Computer-assisted Studies in Algebraic Combinatorics

Dissertation
zur Erlangung des akademischen Grades
"Doktor der technischen Wissenschaften"

Eingereicht von
Dipl.-Ing. Petr Lisoněk

September 1994

Erster Begutachter:	O.Univ.-Prof. Dr. Bruno Buchberger
Zweiter Begutachter:	A.Univ.-Prof. Dr. Günter Pilz

Angefertigt am Forschungsinstitut für Symbolisches Rechnen
Technisch-Naturwissenschaftliche Fakultät
Johannes Kepler Universität Linz

Eidesstattliche Erklärung

Ich versichere, daß ich die Dissertation selbständing verfaßt habe, andere als die angegebenen Quellen und Hilfsmittel nicht verwendet und mich auch sonst keiner unerlaubten Hilfe bedient habe.

Linz, am 19. September 1994 Petr Lisoněk

This work was partially supported

by the Austrian Federal Ministry for Science and Research
(doctoral scholarship)

and by Austrian Science Foundation Grant P7220.

Abstract

The main objective of the thesis is to develop and evaluate a variety of computer-aided experimental methods that yield insight for discovering and proving theorems in combinatorics. We contribute to the methodology of the "creativity spiral" paradigm.

We present nine studies, most of which rely on replacing equivalence of discrete structures by a finite group action.

Throughout the thesis we make much use of computer algebra systems. In particular, the first core chapter is completely devoted to an improvement of an algorithm that frequently occurs in proving combinatorial identities, namely Gosper's algorithm.

The enumerative part of the thesis is centered around the concept of quasi-polynomials. We show that many interesting combinatorial quantities, typically depending on two parameters, possess a quasi-polynomial closed form if one of the parameters becomes fixed. Then we derive an algorithm for computing the values of one special kind of quasi-polynomials, namely the number of restricted partitions.

In the constructive part of the thesis we subsequently focus our attention on different kinds of discrete structures. We start with two chapters on graphs, disproving a graph-theoretical conjecture in the first one and extending the classification theory of chordal rings in the second one. Then we switch to necklaces and bracelets. We develop an algorithm that generates bracelets and then we improve known bounds on the relation between local and global bead proportionalities in bracelets. The rest of the constructive part is devoted to finite geometries and linear codes. We build catalogs of two kinds of configurations in projective planes over finite fields, namely the semiovals and the arcs. We develop general constructions of semiovals in Desarguesian planes of arbitrary odd orders. At the end we classify certain optimal ternary linear codes.

The majority of our studies improves or extends results of other authors. This was achieved by thoroughly planned interlacing of human thinking steps and machine computing. Hence, our main conclusion is that this strategy inevitably contributes to the research in combinatorics.

Kurzreferat

Das Thema der Dissertation ist die Entwicklung und Auswertung verschiedener computerunterstützter experimenteller Methoden hinsichtlich des Findens und Beweisens von Sätzen in der Kombinatorik. Wir tragen zur Methodologie des Prinzips der "Kreativitätsspirale" bei.

Wir stellen neun Studien vor, von denen die meisten darauf beruhen, die Äquivalenz von diskreten Strukturen durch Operation einer endlichen Gruppe zu ersetzen.

Der intensive Gebrauch von Computeralgebra-Systemen war eine wesentliche Voraussetzung, um die Ergebnisse dieser Dissertation zu erzielen. Das erste Kapitel ist einer Verbesserung von Gospers Algorithmus gewidmet, mit dem sich eine Reihe kombinatorischer Identitäten beweisen lassen.

Das Konzept der Quasipolynome ist das Kernstück des enumerativen Teils der Arbeit. Wir zeigen, daß zahlreiche interessante kombinatorische Größen sich durch Quasipolynome geschlossen darstellen lassen. Darüberhinaus entwickeln wir einen Algorithmus zur Berechnung einer speziellen Art von Quasipolynomen, welche die Anzahl von eingeschränkten Partitionen beschreiben.

Im konstruktiven Teil diskutieren wir unterschiedliche Arten von diskreten Strukturen. Zwei Kapitel beschäftigen sich mit Graphen, wobei im ersten eine graphentheoretische Vermutung widerlegt wird und im zweiten eine Theorie zur Klassifizierung von chordialen Ringen aufgestellt wird. Danach folgt ein Kapitel über die kombinatorischen Modelle "Halsketten" und "Armbänder". Wir entwickeln einen Algorithmus, der Armbänder auflistet, und verbessern bekannte Schranken für das lokal-globale Verhältnis der Perlenanzahl in Armbändern. Dann erstellen wir Listen zweier Arten von Konfigurationen in projektiven Ebenen über endliche Körper: Semiovale und Bögen. Weiters entwickeln wir eine Methode, um in Desarguesschen Ebenen beliebiger ungerader Ordnung Semiovale zu konstruieren. Abschließend klassifizieren wir bestimmte optimale triadische lineare Codes.

Der Großteil unserer Studien verbessert oder erweitert Ergebnisse anderer Autoren. Das wurde ermöglicht durch wohlüberlegtes Verbinden von menschlichen Denkschritten und Computerberechnungen. Als Hauptschlußfolgerung daraus ergibt sich, daß diese Strategie essentiell für die kombinatorische Forschung ist.

To my parents

Preface

We live in a stormy period when computers have begun to invade the sacred ground of classical mathematics. A dangerous polarization has become visible between the classical, "rigorous" mathematicians on one side and mathematicians proposing "semi-rigorous", "experimental" methods on the other side. Wide-spread journals such as *Notices of the A.M.S.* or *Bulletin of the A.M.S.* initiated discussion about these issues on their pages.

While the discussion goes on and the end is not in sight, we feel that any attempt to reconcile both sides is worth a try. The main goal of our thesis is to deliver a modest but sincere contribution to this process. In the specific field of combinatorics, which offers perhaps the largest computational playground among all corners of mathematics, we will try to show that the "silicon savior" need not be an enemy of the mathematical rigorousness. Our belief is that, in particular in combinatorics, both the rigorous proving methods *and* the insight gained from thoroughly planned computer experiments are inevitable for achieving a continuous progress. We explain our views in more detail in the introductory chapter of the thesis.

Rather than speculating in general, we present nine case studies that roughly correspond to the chapters of the thesis. Each chapter ends with a section called "Methodological Aspects" where we analyze the relation between experimenting and proving. The chapters are relatively independent; about half of them was accepted for publishing as journal papers while some more will be submitted for publication soon.

The thesis is divided in three parts. After a short excursion in computer algebra we enter the two core parts, reflecting this way the common division of combinatorics into enumerative and constructive problems. In these two parts we replace equivalence of discrete structures by a finite group action. At the beginning of either part we recall how to use group action for enumerative and constructive purposes (Chapters 2 and 6, respectively). A skilled reader can skip these introductory chapters as well as the chapter on Hadamard patterns (Chapter 3), since the last one is meant mainly as a warm-up example on Pólya's counting theory.

Throughout the thesis, the word "we" means "the reader and the author". Wherever "we" stays in place of other co-authors as well, the names are mentioned explicitly. Theorems reproduced from other sources are always accompanied with the most appropriate reference known to us.

Not only finishing but even beginning of my thesis work would have been impossible without a help of many. My first and most sincere thanks go to Bruno Buchberger who taught me so much, who substantially helped me to get a doctoral scholarship over a period of three years and who brought to life the wonderful research environment called RISC-Linz. Thank you very much, Bruno, I will never forget what you did for me.

I am extremely grateful to Peter Paule who greatly intensified my original interest in combinatorics, who gave me a freedom to choose the research topics but at the same time was always ready to answer my questions, and who carefully read my manuscripts and helped to improve them a lot. I am happy that we found two occasions to have a joint paper, I really enjoyed that work. When speaking about joint papers, I appreciated that Volker Strehl formed a trio with Peter and me to investigate Gosper's algorithm.

Many thanks are due to Günter Pilz who kindly agreed to be a referee of this thesis and who was providing me with informal and friendly help over the years.

Special thanks are addressed to John Cannon and his co-workers in the computer algebra team at the University of Sydney who granted me access to their wonderful systems Cayley and Magma which I thankfully used on many places in this thesis, and who listened to my outsider thoughts about Magma, making many of them into a reality.

I can hardly tell how much I appreciated the opportunity of exciting and fruitful discussions with all members of RISC-Linz, and I thank to all of them. In particular I enjoyed the everyday collaboration with my closest colleagues and friends Kurt Eichhorn, István Nemes and Roberto Pirastu.

I wish to express my gratitude to Adalbert Kerber, Reinhard Laue and Ronald C. Read who grew my passion for combinatorial constructions by saying to me the right words at the right time. The same is true about Professor Kerber's students Bernd Schmalz and Roland Grund.

I am happy that during my short but intensive visits to Eindhoven and Ghent I met Marijn van Eupen and Leo Storme, which in both cases resulted in a very interesting collaboration.

Many more people contributed by pointing me to references, giving me worthy advices, or even inviting me to visit their universities. I wish to thank to Gert Almkvist, Aart Blokhuis, Joel Brawley Jr., Gunnar Brinkmann, Frank De Clerck, Reinhard Folk, Roberto Frucht, Poul Hjorth, Frank K. Hwang, Steen Markvorsen, Brendan D. McKay, Simon Plouffe and Neil J. Sloane.

September 14, 1994 Petr Lisoněk

Symbols and Conventions

In the following table we include a list of symbols that are used widely in the thesis. Symbols specific to certain chapters are introduced at the beginning of the respective chapter.

$\mathbb{N}$	set of non-negative integers
$\mathbb{N}^+$	set of positive integers
$\mathbb{Z}$	set of integers
$\mathbb{Q}$	set of rational numbers
$\lvert X\rvert$, $\lvert G\rvert$	number of elements of the finite set X, order of the finite group G
Y^X	$\{f \mid f : X \to Y\}$, set of all mappings from X to Y
$\mathcal{P}(X)$	power set of the set X
χ_S	characteristic function of the set S; $\chi_S(x) = 1$ if $x \in S$, 0 otherwise
$\underline{n}$	set $\{1, 2, \ldots, n\}$ where n is a positive integer
S_X	symmetric group on the set X (acting naturally on X)
$G \leq H$	G is a subgroup of H
$G \oplus H$	direct sum of the groups G and H
$GF(q)$	finite field with q elements, q a prime power
U^T	transposition of the matrix U
$\deg(p)$	degree of the polynomial p
$K[x_1, \ldots, x_n]$	ring of n-variate polynomials over K
$K[[x_1, \ldots, x_n]]$	ring of n-variate formal power series over K
$K(x)$	field of univariate rational functions over K
$\lfloor x \rfloor$	floor of x (integer part)
$\lceil x \rceil$	ceiling of x
$n \bmod k$	modulo function with the range $\{0, 1, \ldots, k-1\}$
$a \vdash n$	a is a partition of n; $a = (a_i)_{1 \leq i \leq n}$ with $\sum_{i=1}^{n} i \cdot a_i = n$, $a_i \in \mathbb{N}$
$f(n) = O(g(n))$	there is a constant C such that $f(n) \leq C\lvert g(n)\rvert$ for all $n \in \mathbb{N}$; analogously for sequences in more variables

Contents

Chapter 0

Methodological Background

Science walks forward on two feet,
namely theory and experiment.
Sometimes it is one foot which is put forward first,
sometimes the other,
but continuous progress is only made by the use of both.

— R. Millikan

These remarkable words, which we would like to have as the *motto* of our thesis, belong to a famous physicist and 1923 Nobel prize winner. Unlike physics, mathematics is known for the *rigorousness* as its absolute principle. Hence, much caution is needed if we want to take a moral from the motto. We feel that a detailed explanation of our views is in place before starting anything else, and the present chapter is devoted to this.

0.1 The Creativity Spiral

Once we begin to formulate a research plan, we need a rigorous mathematical description of the ideas that are approximated in Millikan's quotation. Among those known to us, the most refined such plan is the *iteration through the "creativity spiral"* as described by Buchberger (1993). The basic idea of this principle is expressed in Figure 0.1.

Following Buchberger (1993), the concept of *spiral* has two ingredients: proceeding through a *circle* one arrives at a *higher level*. In the bottom level (base) of the spiral, it does not matter which step of the four possible ones we take as the point of the departure for the first iteration.

Typically, we would start with some (say, given) algorithm and generate experimental data that are related to the problem under examination. By observing the common structure "hidden" in the experimental

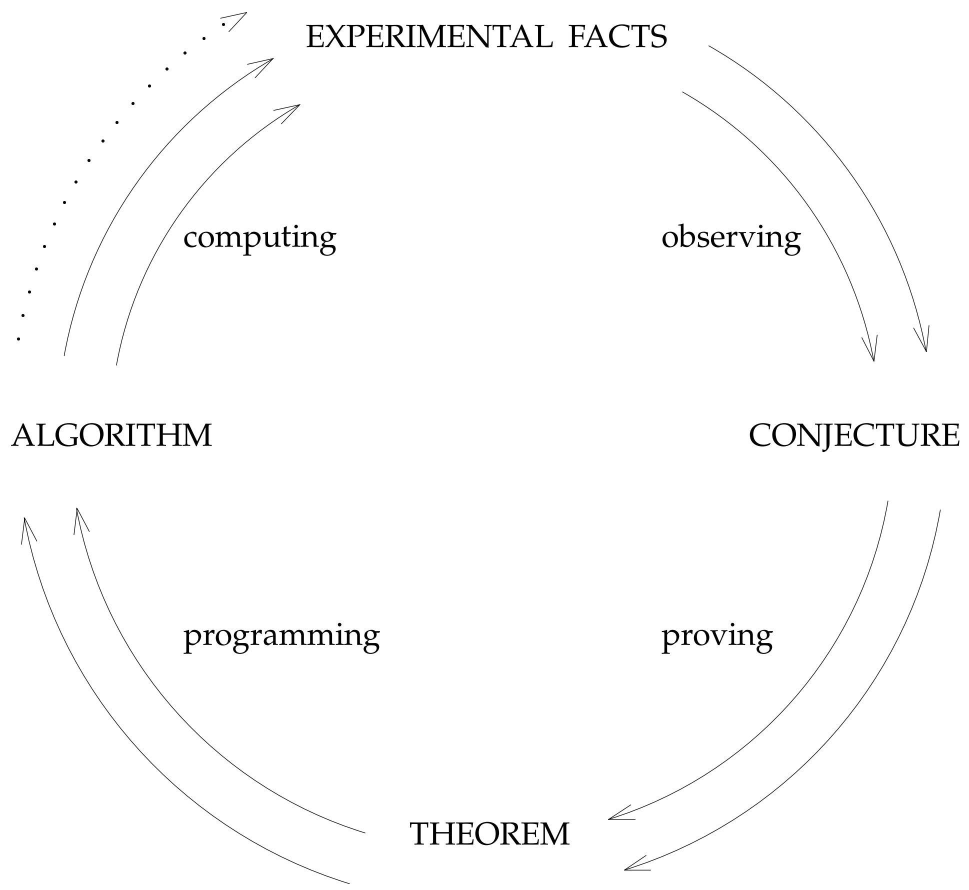


Figure 0.1: The creativity spiral (Buchberger).

facts we may get a new insight in the problem and formulate a conjecture. Our main aim, however, is to turn this conjecture into a theorem, i.e., to prove that the conjectured assertion is not only true in the cases observed in the computational experiments but is necessarily true in all possible cases. In the case of proving, again, the insight obtained in the computational experiments may be crucial for discovering the sequence of thinking steps needed in order to obtain a complete proof.

At this point, Buchberger puts much emphasis on *algorithmic mathematics*. This means that one should always try to formulate and prove theorems that can be easily converted into algorithms, which then enable to continue smoothly in the circle movement. Now, one circle of the spiral is closed and we are, again, in the position where we can apply the algorithm to collect more experimental data and, hopefully, get new insight. Since the new algorithm incorporates more insight and knowledge, we may hope that it is more efficient for solving our problem, which means that the *next pass through the circle may proceed on a higher level.*

We may summarize that the creativity spiral is marked by an interlaced sharpening of its two essential components, namely results (theorems) and methods (algorithms).

It is the ultimate goal of our thesis to *contribute to the specific aspects of the "creativity spiral"* when it is applied as a methodology for research in *combinatorics* and *closely neighboring fields*. For this purpose, at the end of each chapter (except for the introductory ones) we insert a section called "Methodological Aspects". In each such section we discuss the creativity spiral of the respective chapter, in particular we analyze the relation between experiments and proofs. Some general remarks about these issues follow in the next section.

0.2 Experiments and Proofs

The concept of the creativity spiral seems to be so natural that we can adopt the idea that it governs all progress in mathematics. While the proving side of the spiral is relatively transparent because the proofs are usually published in full detail, it may be less transparent what happens on the experimental part.

The last sentence of course does not imply that proving is easy—typically proofs are products of hard mental work, and *the essence of mathematics is proving.* We just want to remark that, after having read a paper written by someone else, we usually know much better how the theorem was proved than in which way it was discovered. Some authors intentionally skip the latter information because they hope to exploit it further, and because only the former information (the proof) is normally required to get the theorem published.

Hence, apart for giving perfect proofs, it will also be our concern in this thesis to develop good methods of experimenting.

The dramatic progress in computer technology over the past decade was paralleled by equally dramatic statements about the changing role of computers in mathematics. One of them reads as follows:

> *There are writings on the wall that,*
> *now that the silicon savior has arrived,*
> *a new testament is going to be written.*

This quotation is taken from a controversial paper by Zeilberger (1993). While we find this particular sentence very appealing (let us make it, say, to a *sub-motto* of our thesis), it should be noted that the rest of the paper provoked a lot of (mostly negative) discussion. Zeilberger argues that in the future computers will overwhelm us with so many new exciting facts that we simply will not have time to prove them. He predicts the dawn of "semi-rigorous mathematics" in which propositions will be stated only with limited certainty, based on computer experiments. Things went even further in a Scientific American essay by Horgan (1993) who speculated about "the death of proof". Technical flaws in Horgan's pamphlet were pointed out by many authors; see, for example, the response by MacLane (1994).

In these days, for many mathematicians the main source of irritation is the appearance of computerized experiments as substitutes for proofs. As a consequence, the pure mathematical community in its vast majority still regards computers as invaders, despoilers of "the sacred ground".

To our opinion, the way out of this unpleasant and dangerous polarization is to clearly state *in which parts of the creativity spiral is the* *use of computers highly profitable* and *from which parts it should be eliminated whenever possible.*

Since our main concern is to study the creativity spiral in combinatorics, we will now turn our attention to this specific field.

0.2.1 Combinatorial Computing

Massive combinatorial computations were performed to establish the following results:

- *Every plane map is four-colorable.* See (Appel, Haken, 1986) for a historical account and a defense of their method.
- *There is no projective plane of order 10,* by Lam, Thiel and Swiercz (1989).
- *The Ramsey number* $R(4,5)$ *is equal to 25,* by McKay and Radziszowski (1993).

The common characteristic of all three cases is that a computer was used to "prove" a result by separately verifying a myriad of possible subcases at the total cost of months or years of computing time.

The main objection raised by the rigorous mathematicians is that such proofs cannot be checked by humans. For example, to establish the equality $R(4,5) = 25$, a separate consideration of more than 350,000 twenty-four-vertex graphs was necessary. In the proof by Appel and Haken, even minor errors had to be corrected over the years. Recently, Sanders (1994) and his colleagues have simplified the Appel-Haken proof, which now requires "only" 24 hours on a Sun Sparc 10 workstation.

The second objection is that the computer proofs may rely on error-prone software, not to speak about possible hardware failures.

It is then no wonder that, given this state of affairs, the rigorous mathematicians tend to believe that the computer is a false Messiah.

Our main concern in this thesis is to show that computer-assisted mathematics need not be "speculative" or "semi-rigorous". One possible *recipe* to have the computer as a honest, harmless tool of rigorous mathematics is to use it freely on the experimental side of the creativity spiral, while the usage on the proving side should be limited to cases that are intractable by humans (e.g., because of immense complexity).

(*Remark.* Even in those cases, one should try to get such computer-generated proofs that have short (i.e., human-verifiable) "certificates". For an excellent example of certified computer proving, see Zeilberger (1990*a*), (1990*b*) and Wilf and Zeilberger (1992).)

In other words, we aim at a rehabilitation of *"experimental mathematics"* by giving this term a proper content, as outlined by J. Borwein and P. Borwein (1992) or by Kerber (1991) in the final comments to his recent book (pages 425–426).

As far as experimenting is considered, combinatorics and its neighbors seem to be a paradise landscape. Combinatorial objects are usually easy to represent in a computer, and the numbers involved in the problems usually are integers or rationals.

In our thesis, we present nine studies of doing *rigorous* experimental combinatorics. In the great majority of cases we are able to provide transparent proofs that are logically independent of computer results. Only in the last two chapters (constructions in finite projective planes and classifications of ternary codes) we sometimes have to "believe the computer" in the instances when the number of classified objects is too big to have a human proof for it.

0.3 The Role of Symbolic Computation

Symbolic computation software is a useful tool that changes the way we teach, apply and *invent* mathematics. In particular, the computer algebra systems provide wonderful environments for experimenting. Bergeron (1993) shows how surprising can be the results discovered this way.

Computer algebra plays an immense role also in our investigations. Part I deals entirely with computer algebra algorithms. In Part II, computational manipulations of formal power series provide us with a lot of insight in certain enumerative problems. In Part III, we study problems that have symmetries described by permutation groups. In order to efficiently cope with these problems we need a certain preprocessing of these groups. In cases when these groups grow very large (such as in Chapters 10 and 11), a powerful computational system is inevitable to handle them. A standard instance for the application of computer algebra also is provided by the study of algebraic curves in Section 10.4.

Part I

Computer Algebra in Combinatorics

Chapter 1

Improvement in Gosper's Algorithm

1.1 About Symbolic Summation

In this chapter our interest will be focussed on "simplification" of *finite* sums

$$\sum_{i=a}^{b} t_i. \tag{1.1}$$

Usually, the main goal is elimination of the $\sum$ symbol in (1.1) under the assumption that the resulting formula is "simpler" then the original sum. As an example, take

$$a(n) = \sum_{k=0}^{n} \frac{1}{4k^2 + 8k + 3}$$

and

$$b(n) = \frac{n+1}{2n+3}.$$

For all non-negative integers n, $a(n) = b(n)$ holds. But evaluating $b(n)$ takes constant time (when n is "not too big") while for computing $a(n)$ we must do $O(n)$ arithmetic operations. Moreover, from $b(n)$ we get more knowledge—for instance,

$$\lim_{n\to\infty} a(n) = \lim_{n\to\infty} b(n) = \frac{1}{2}.$$

Thus the main reasons for performing symbolic summation are

- achieving more mathematical insight,
- obtaining better or unique algebraic representations,
- reduction of evaluation time and/or escape from complicated numerical evaluations.

It has been recognized in the course of years that for certain classes of functions, the sums are found in other certain classes of functions. For example, sums of polynomials are polynomials, sums of rational functions are rational functions plus a transcendental part. This leads to the formal specification of our problem, see also (Gärtner, 1986):

Definition 1.1.1 *Let K be a ring (field) and $K \subseteq F(t) \subseteq G(t)$ be extensions of K such that all elements of $F(t)$ and $G(t)$ are functions from $\mathbb{Z}$ to K. The problem of* summation in finite terms *is as follows:*

Given: *an element $f \in F(t)$ (the "summand expression").*
Find: *an element $g \in G(t)$ in "closed form" such that for all $n, m \in \mathbb{Z}, n \leq m$, the following holds:*

$$\begin{aligned}(\forall\ i = n, n+1, \dots, m)\ (f(i) \text{ is defined}) \Longrightarrow \\ (g(n) \text{ is defined} \wedge g(m+1) \text{ is defined} \wedge \\ \textstyle\sum_{i=n}^{m} f(i) = g(m+1) - g(n)).\end{aligned} \tag{1.2}$$

Return "no closed formula exists" if there is no function $g \in G(t)$ with this property.

Hence, given a function $f(n)$, $n \in \mathbb{Z}$, we look for corresponding $g(n)$ such that

$$(\forall n \in \mathbb{Z})\,(\Delta g(n) := g(n+1) - g(n) = f(n))\,.$$

The implication (1.2) is then easily satisfied. Thus the indefinite summation reduces to solving the first-order difference equation

$$g(n+1) - g(n) = f(n). \tag{1.3}$$

The solution is unique up to the addition of a constant sequence.

The term "closed form" is to be understood in accordance with the achievement that we expect from the summation act. For example, if we intend to reduce the amount of computation, the "closed form" is an expression that is *considerable easier to evaluate* than the sum itself.

Sometimes, we speak about *indefinite summation* instead of "summation in finite terms" because of the parallel to the indefinite integration problem. See Chapter 2.6 of (Graham, Knuth and Patashnik, 1989) for a discussion of analogy to the continuous case. In fact, success with symbolic integration in the late 60s motivated progress in the discrete case as well.

Sometimes, we cannot find $g(n)$ satisfying (1.2) but for some $I \subseteq \mathbb{Z}$, evaluation of $\sum_{n \in I} f(n)$ is possible. Then we perform the *definite summation*. In this case often one of the summation limits appears as a parameter of the summand. As a well-known example, consider $f(k) = \binom{n}{k}$, $n \in \mathbb{N}$. We cannot simplify the symbolic sum $\sum_{k=0}^{m} \binom{n}{k}$ for arbitrary m but we know that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

In particular, symbolic methods can be used for proving (and also rediscovering) of a great majority of identities involving factorials and binomial coefficients. Nowadays they present a standard tool for research in combinatorics.

In the history of indefinite summation, four large classes of functions were subsequently mastered, namely polynomial, rational, hypergeometric and special functions. The hypergeometric case is treated by the algorithm invented by Gosper (1978). In the following sections, a detailed study of the degree setting for Gosper's algorithm is presented. In particular, we discriminate between rational and proper hypergeometric input. As a result, the critical degree bound can be improved in the former case.

The work described in subsequent sections originated by two independent publications: Paule and Strehl (1991) described the K_0-case arising in proof of Apéry's recurrence (see Section 1.7.2), and Lisoněk (1991) found the improvement of the degree setting in the rational input case. The algebraic theory of the degree setting was then developed in collaboration of Lisoněk, Paule and Strehl (1993).

1.2 Gosper's Algorithm

Gosper's algorithm for *indefinite* hypergeometric summation (see Gosper (1978), Lafon (1983) or Graham, Knuth and Patashnik (1989)) belongs to the standard methods implemented in most computer algebra systems. Current interest in this algorithm is mainly due to the fact that it can also be used for *definite* hypergeometric summation (e.g., verifying binomial identities "automatically", finding recurrence operators annihilating hypergeometric sums) in a non-obvious and nontrivial way (see Zeilberger (1990*a*), (1990*b*), Wilf and Zeilberger (1992) and the references given in the latter).

One of the steps in Gosper's algorithm, crucial for its running time and memory requirement, is the determination of a degree bound for a possible polynomial solution of a certain difference equation - the so-called "key equation", see (GE) in Section 1.5. In this chapter a detailed analysis of this degree setting is given. It turns out that the situation for rational sequences is different from that for proper, i.e., non-rational hypergeometric input. Besides several theoretical results one practical implication of our discussion is an improvement for the degree setting in Gosper's algorithm in the rational case. At first glance, this improvement might seem to be of minor interest since Gosper's algorithm is not primarily intended for the special case of rational summation. But we have to stress that in many computer algebra systems it is the *only* summation algorithm available. (The single exception from this situation is probably Maple providing a variety of summation algorithms and choosing the appropriate one depending on the particular form of the input.) This motivates a study of the behavior of Gosper's algorithm for different classes of inputs in order to make it *input-sensitive* as a balance to having more algorithms at hand.

After the basic definitions, in Sections 1.3 and 1.4 algebraic relations between rational and hypergeometric sequences are discussed. Two representations (Gosper form and Petkovšek's normal form) of rational functions are introduced which are crucial for our investigation. In Section 1.5 a brief outline of Gosper's algorithm is given, including information on the solution space of the key equation (GE). Section 1.6 presents the careful analysis of the degree setting for polynomial solutions of (GE). The difference between rational and hypergeometric input sequences is made explicit. For example, if an indefinite sum over a regular rational sequence again is rational then there exist at least two polynomial solutions of the key equation with different degrees. The one with the higher degree corresponds to the "K_0-case" in Gosper's original degree setting. This is different from the situation for proper hypergeometric input. Based on the degree setting analysis, a suggestion for a corresponding improvement in Gosper's algorithm is made.

In Section 1.7 two examples illustrating the difference between rational and proper hypergeometric situation are given. One of them is related to the famous Apéry recurrence.

In Section 1.8 we include a brief survey of other methods for rational sequence summation.

1.3 Rational and Hypergeometric Sequences

Definition 1.3.1 *Let Q be a field of characteristic* 0. *A sequence $(a_k)_{k\geq 0}$ in Q is called*

- rational, *if there exist relatively prime polynomials $s, t \in Q[x]$ such that*

$$a_k = \frac{s(k)}{t(k)} \qquad (k \in \mathbb{N}) \tag{1.4}$$

  (in particular: $t(k) \neq 0$ for all $k \in \mathbb{N}$)

- hypergeometric, *if there exist relatively prime polynomials $\sigma, \tau \in Q[x]$ such that*

$$a_k = \frac{\sigma(k)}{\tau(k)} \cdot a_{k-1} \qquad (k \geq 1) \tag{1.5}$$

  where $\tau(k) \neq 0$ for all $k \geq 1$.

A rational sequence $(a_k)_{k\geq 0}$ is called regular rational *if* $\deg(s) < \deg(t)$ *in equation (1.4) holds.*

Note that once a term a_n of some hypergeometric sequence vanishes, all the subsequent terms a_{n+k} $(k \geq 0)$ will automatically vanish too, i.e., $(a_k)_{k\geq 0}$ has only a finite number of non-zero terms in this case. This degenerate situation is obviously not of much interest as far as *indefinite* hypergeometric summation is concerned. On the other hand, rational sequences can only have a finite number of vanishing terms, hence rational sequences with at least one vanishing term cannot be hypergeometric. Again, since we are interested in indefinite summation, we can always dispense with a finite initial segment of a sequence to be summed by shifting indices.

Hence, for the remainder of this chapter *rational sequence* will always mean "rational sequence without vanishing terms" and *hypergeometric sequence* will always mean "hypergeometric sequence without vanishing terms".

Under this convention, every rational sequence is a hypergeometric one, since

$$a_k = \frac{s(k)}{t(k)} \cdot \frac{t(k-1)}{s(k-1)} \cdot a_{k-1} = \frac{\sigma(k)}{\tau(k)} \cdot a_{k-1}$$

with

$$\begin{aligned}\sigma(x) &= s(x)\cdot t(x-1)/d(x)\\ \tau(x) &= t(x)\cdot s(x-1)/d(x)\end{aligned}$$

where $d(x) = \gcd(s(x)\cdot t(x-1), t(x)\cdot s(x-1))$. Thus it makes sense to introduce the concept of *proper hypergeometric sequence* which means hypergeometric sequence that is not a rational one.

Conversely, if $(a_k)_{k\geq 0}$ is a hypergeometric sequence as in (1.5) such that the rational function $\sigma(x)/\tau(x)$ can be written as

$$\frac{\sigma(x)}{\tau(x)} = \frac{p_1(x)}{p_1(x-1)}\cdot\frac{p_2(x-1)}{p_2(x)}$$

for (relatively prime, w.l.o.g.) polynomials $p_1, p_2 \in Q[x]$, then $(a_k)_{k\geq 0}$ is rational because

$$a_k = \frac{\prod_{i=1}^k \sigma(i)}{\prod_{j=1}^k \tau(j)}\cdot a_0 = \frac{p_1(k)\cdot p_2(0)}{p_1(0)\cdot p_2(k)}\cdot a_0,$$

i.e., we have (1.4) with $s(x) = a_0\cdot p_2(0)\cdot p_1(x)$ and $t(x) = p_1(0)\cdot p_2(x)$.

We may summarize this discussion in

Proposition 1.3.2 *Let $(a_k)_{k\geq 0}$ be a hypergeometric sequence with rational function certificate $\lambda(x) = \sigma(x)/\tau(x) \in Q(x)$, i.e.,*

$$a_k = \lambda(k)\cdot a_{k-1} \quad \textit{for all } k\geq 1.$$

The sequence $(a_k)_{k\geq 0}$ is rational if and only if there exist polynomials p_1, $p_2 \in Q[x]$ such that

$$\lambda(x) = \frac{p_1(x)}{p_1(x-1)}\cdot\frac{p_2(x-1)}{p_2(x)}.$$

1.4 Representations of Rational Functions

Gosper's algorithm makes essential use of the following fact about rational functions:

Proposition 1.4.1 (Gosper) *Every non-zero rational function* $\lambda(x) \in Q(x)$ *can be written as*

$$\lambda(x) = \frac{p(x)}{p(x-1)} \cdot \frac{q(x)}{r(x)}, \tag{G1}$$

where $p, q, r \in Q[x]$ *are polynomials such that*

$$\gcd(q(x), r(x+j)) = 1 \qquad \textit{for all } j \in \mathbb{N}. \tag{G2}$$

A triple (p, q, r) satisfying (G1) and (G2) will be called a G-form of $\lambda(x)$. Gosper (1978) outlines an algorithm for the computation of a G-form. Note that such a form is not unique. As a simple example: in

$$\lambda(x) = \frac{(x+1)^2}{x} = \frac{x+1}{x} \cdot \frac{x+1}{1} = \frac{(x+1)^2}{x^2} \cdot \frac{x}{1}$$

both the third and the fourth term are G-forms with

$$p(x) = x+1,\ \ q(x) = x+1,\ \ r(x) = 1$$

and

$$p(x) = (x+1)^2,\ \ q(x) = x,\ \ r(x) = 1,$$

respectively.

It was shown by Petkovšek (1992) that uniqueness for this kind of form can be enforced by imposing two more conditions.

Proposition 1.4.2 (Petkovšek) *Every non-zero rational function* $\lambda(x) \in Q(x)$ *can be written uniquely as*

$$\lambda(x) = c \cdot \frac{p(x)}{p(x-1)} \cdot \frac{q(x)}{r(x)}, \tag{P1}$$

where $0 \neq c \in Q$ *and where* $p, q, r \in Q[x]$ *are monic polynomials such that*

$$\gcd(q(x), r(x+j)) = 1 \qquad \textit{for all } j \in \mathbb{N}, \tag{P2}$$

$$\gcd(p(x), r(x)) = 1, \tag{P3a}$$

$$\gcd(p(x-1), q(x)) = 1. \tag{P3b}$$

Petkovšek also gives an algorithm for computing what we will call the P-form (p, q, r) of a rational function.

As an immediate simple consequence of Petkovšek's representation we note:

Proposition 1.4.3 *Let* $\alpha, \beta \in Q[x]$. *If the equation*

$$\beta(x) \cdot y(x) - \alpha(x) \cdot y(x-1) = 0 \tag{1.6}$$

admits a non-trivial polynomial solution $y \in Q[x]$, *then all polynomial solutions of (1.6) are precisely given by the scalar multiples* $c \cdot y(x),\ c \in Q$, *of* $y(x)$.

Proof. If $y(x)$ is any monic solution of the equation, then view the r.h.s. of

$$\frac{\alpha(x)}{\beta(x)} = \frac{y(x)}{y(x-1)}$$

as the P-form $(p(x) = y(x), q(x) = r(x) = 1)$ of the l.h.s. By the uniqueness assertion of Proposition 1.4.2, any polynomial solution of equation (1.6) must be a scalar multiple of $y(x)$. □

As a further consequence of Petkovšek's result we get information about the possible G-forms of rational sequence certificates. (Cf. Proposition 1.3.2 for the notion of the certificate.)

Proposition 1.4.4 *Let* $\rho(x) = \sigma(x)/\tau(x) \in Q(x)$ *be a rational function with* $\gcd(\sigma(x),\ \tau(x)) = 1$, *and let* $(p(x), q(x), r(x))$ *be any G-form of* $\rho(x)/\rho(x-1)$. *Then*

1. *if* $q(x) = r(x) = 1$, *then* $\rho(x)$ *is a polynomial, i.e.,* $\tau(x) = 1$;
2. *if* $p(x) = 1$, *then* $\rho(x)$ *is the reciprocal of a polynomial, i.e.,* $\sigma(x) = 1$;
3. *in the general situation:* $\sigma(x) \mid p(x)$.

Proof. 1. For $q = r = 1$

$$\frac{\sigma(x)}{\sigma(x-1)} = \frac{(\tau \cdot p)(x)}{(\tau \cdot p)(x-1)}.$$

Both sides are in P-form, thus $\sigma = \tau \cdot p$, which implies $\tau = 1$ by $\gcd(\sigma, \tau)$ $= 1$.

2. Representing $\tau(x-1)/\tau(x)$ in P-form as

$$\frac{\tau(x-1)}{\tau(x)} = \frac{u(x)}{u(x-1)} \cdot \frac{v(x)}{w(x)}$$

implies $v(x) \mid \tau(x-1)$ and $w(x) \mid \tau(x)$ by considering

$$\tau(x-1) \cdot u(x-1) \cdot w(x) = \tau(x) \cdot u(x) \cdot v(x)$$

together with the Petkovšek conditions. But then both sides of

$$\frac{(\sigma \cdot u)(x)}{(\sigma \cdot u)(x-1)} \cdot \frac{v(x)}{w(x)} = \frac{q(x)}{r(x)}$$

are in P-form. E.g., $\gcd(w, \sigma \cdot u) = 1$, the Petkovšek condition (P3a), holds because of $w \mid \tau$, $\gcd(\sigma, \tau) = 1$, and $\gcd(u, w) = 1$. Analogously the other "diagonal" Petkovšek condition (P3b) is verified using $v(x) \mid \tau(x-1)$.
Thus we have $v = q$, $w = r$, $\sigma \cdot u = 1$, and thus $u = \sigma = 1$.

3. For $\tilde{\rho} = \sigma/(p \cdot \tau)$ the G-form of $\tilde{\rho}(x)/\tilde{\rho}(x-1)$ is

$$\frac{\tilde{\rho}(x)}{\tilde{\rho}(x-1)} = \frac{q(x)}{r(x)}.$$

It follows from 2. that $\tilde{\rho}(x)$ is the reciprocal of a polynomial. This, together with $\gcd(\sigma, \tau) = 1$, implies $\sigma \mid p$. □

We use this assertion in the following result which is crucial for discussing the behavior of Gosper's algorithm on rational sequences.

Proposition 1.4.5 *Let $\lambda(x) \in Q(x)$ be a rational function, and let (p, q, r) be any G-form of $\lambda(x)$. Then the following assertions are equivalent:*

1. *We have*

$$\lambda(x) = \frac{\rho(x)}{\rho(x-1)}$$

for some rational function $\rho(x) \in Q(x)$.

2. *The equation*

$$q(x+1) \cdot y(x) - r(x) \cdot y(x-1) = 0$$

admits a non-trivial polynomial solution $y \in Q[x]$.

Proof. Let $\rho(x) = \sigma(x)/\tau(x) \in Q(x)$ with $\gcd(\sigma(x), \tau(x)) = 1$. Then $\sigma(x) \mid p(x)$ by the general part of the previous proposition. We may thus rewrite the G-form of

$$\lambda(x) = \frac{\rho(x)}{\rho(x-1)} = \frac{\sigma(x)}{\sigma(x-1)} \cdot \frac{\tau(x-1)}{\tau(x)}$$

as

$$\frac{\tau(x-1)}{\tau(x)} = \frac{(p/\sigma)(x)}{(p/\sigma)(x-1)} \cdot \frac{q(x)}{r(x)}$$

or

$$q(x) \cdot \left(\frac{p \cdot \tau}{\sigma}\right)(x) - r(x) \cdot \left(\frac{p \cdot \tau}{\sigma}\right)(x-1) = 0. \tag{1.7}$$

Now $\gcd(q(x), r(x)) = 1$ by property (G2), hence $q(x) \mid (p \cdot \tau/\sigma)(x-1)$, i.e.,

$$\left(\frac{p \cdot \tau}{\sigma}\right) \sigma(x) = q(x+1) \cdot y(x)$$

for some non-zero polynomial $y \in Q[x]$. Dividing both sides of (1.7) by $q(x)$ then gives

$$q(x+1) \cdot y(x) - r(x) \cdot y(x-1) = 0.$$

For the other direction, let $y(x)$ be a non-trivial solution of this previous equation, then

$$\frac{q(x)}{r(x)} = \frac{q(x)}{q(x+1)} \cdot \frac{y(x-1)}{y(x)},$$

and

$$\lambda(x) = \frac{p(x)}{p(x-1)} \cdot \frac{q(x)}{q(x+1)} \cdot \frac{y(x-1)}{y(x)},$$

i.e., we have $\lambda(x) = \rho(x)/\rho(x-1)$ with

$$\rho(x) = \frac{p(x)}{q(x+1) \cdot y(x)}.$$

□

1.5 Uniqueness of Solutions

The essence of Gosper's algorithm (see Gosper (1978) or Section 5.7 in Graham, Knuth and Patashnik (1989)) can be shortly described as follows:

Given a hypergeometric sequence $(a_k)_{k\geq 0}$ with values from the field Q. Let us assume that the sequence $(s_n)_{n\geq 0}$ defined as

$$s_n = \sum_{k=0}^{n} a_k,$$

for all non-negative integers n, again is hypergeometric. Then to solve the summation problem is equivalent to find the hypergeometric solution $(s_k)_{k\geq 0}$ of the difference equation

$$s_k - s_{k-1} = a_k \qquad\qquad k \geq 1 \tag{DE}$$

with the initial condition $s_0 = a_0$. If exists, this solution can be expressed as

$$s_n = \frac{q(n+1)}{p(n)} \cdot f(n) \cdot a_n,$$

where $f(x)$ is a polynomial satisfying the *key equation*

$$p(x) = q(x+1) \cdot f(x) - r(x) \cdot f(x-1) \tag{GE}$$

and where (p, q, r) is a G-form of the rational function certificate determined by a_k/a_{k-1} $(k \geq 1)$. In order to discuss the set of all possible polynomial solutions $f \in Q[x]$ of the key equation (GE) we make use of the following proposition which is evident:

Proposition 1.5.1 *Given polynomials* $\alpha, \beta, \gamma \in Q[x]$ *with* $\gamma \neq 0$, *then the set of all polynomial solutions of*

$$\gamma(x) = \alpha(x) \cdot y(x) - \beta(x) \cdot y(x-1) \tag{1.8}$$

consists precisely of all expressions of the form

$$y \; + \; z,$$

where $y \in Q[x]$ *is a solution of (1.8) and* $z \in Q[x]$ *runs through all polynomial solutions of the homogeneous equation*

$$0 = \alpha(x) \cdot z(x) - \beta(x) \cdot z(x-1). \tag{1.9}$$

A similar statement is proven as Lemma 3.7 in (Koornwinder, 1992). However, no further investigations appear there. On the contrary, here we proceed by showing that there is an intimate connection between the situation described in the previous proposition and the two principal classes of input sequences:

Let us assume that a polynomial solution $f \in Q[x]$ of (GE) exists. Then, by Proposition 1.5.1 we have to consider two different cases, *(A)* and *(B)*, induced by the structure of the corresponding homogeneous equation

$$0 = q(x+1) \cdot y(x) - r(x) \cdot y(x-1). \tag{1.10}$$

(A) If (1.10) admits no non-trivial solution, then $f(x)$ is the only solution of the key equation (GE).

(B) If there exists a non-trivial solution h of (1.10), then due to Propositions 1.5.1 and 1.4.3 the polynomial solution set of the key equation (GE) consists precisely of all polynomials of the form

$$f(x) + c \cdot h(x),$$

where c is running through all the elements of Q.

We show that the cases *(A)* and *(B)* correspond to $(a_k)_{k\geq 0}$ being either a *proper* hypergeometric sequence (i.e., not a rational one), or being a rational sequence:

Proposition 1.5.2 *Let $(a_k)_{k\geq 0}$ be a hypergeometric sequence with rational function certificate $\lambda(x) \in Q(x)$, i.e., $a_k = \lambda(k) \cdot a_{k-1}$ for all $k \geq 1$, and let (p, q, r) be a G-form of λ. Then the key equation*

$$p(x) = q(x+1) \cdot f(x) - r(x) \cdot f(x-1)$$

arising in Gosper's algorithm admits

1. *at most one polynomial solution, if $(a_k)_{k\geq 0}$ is a proper hypergeometric sequence;*

2. *none or a one-parameter family of polynomial solutions, if $(a_k)_{k\geq 0}$ is a rational sequence.*

Proof. By Proposition 1.4.5 the homogeneous form of the key equation

$$0 = q(x+1) \cdot f(x) - r(x) \cdot f(x-1)$$

admits a non-trivial solution if and only if $\lambda(x) = \rho(x)/\rho(x-1)$ for some rational function $\rho \in Q(x)$. By Proposition 1.3.2 this representation of λ is possible if and only if $(a_k)_{k\geq 0}$ is rational. The rest of the proposition is implied by the analysis of the cases *(A)* and *(B)* above. □

We conclude this section by a proposition describing how, in the rational input case, a polynomial solution of the homogeneous form of the key equation (GE) can be computed from the corresponding G-form. The special form of this solution implies a degree relation which turns out to be fundamental for the analysis of the degree setting (see Section 1.6.4).

Definition 1.5.3 *We define the* degree of a rational function

$$F(x) = f_1(x)/f_2(x)$$

as

$$\mathrm{Deg}(F(x)) \quad := \quad \deg(f_1(x)) - \deg(f_2(x)).$$

Proposition 1.5.4 *Let $(F(k))_{k\geq 0}$ be a rational sequence, $F(x) = f_1(x)/f_2(x)$ with $f_1, f_2 \in Q[x]$ and $\gcd(f_1, f_2) = 1$, and let (p, q, r) be a G-form of $F(x)/F(x-1)$. Suppose that the key equation (GE) admits a one-parameter family of polynomial solutions (cf. Proposition 1.5.2.2). Then the following holds:*

1. *We have that $P(x) := p(x)/f_1(x)$ and $z(x) := f_2(x)P(x)/q(x+1)$ are polynomials in $Q[x]$.*

2. *The polynomial $z \in Q[x]$ is a solution of the homogeneous form of the key equation (GE), i.e.,*

$$0 = q(x+1) \cdot z(x) - r(x) \cdot z(x-1) \tag{1.11}$$

   holds.

3. *For $\mathrm{Deg}(F(x)) = \deg(f_1(x)) - \deg(f_2(x))$ we have*

$$\deg(p(x)) - \deg(q(x)) - \mathrm{Deg}(F(x)) = \deg(z(x)).$$

Proof. By Proposition 1.4.4.3 we know that $f_1(x) \mid p(x)$, hence from the G-form representation

$$\frac{f_2(x-1)}{f_2(x)} = \frac{P(x)}{P(x-1)} \cdot \frac{q(x)}{r(x)}.$$

From Proposition 1.4.5 we know there must exist a non-trivial solution of (1.11). Suppose $Z \in Q[x]$ is such a solution. Then by rewriting (1.11) as

$$\frac{q(x)}{r(x)} = \frac{Z(x-1)}{Z(x)} \cdot \frac{q(x)}{q(x+1)}$$

and corresponding replacement of $q(x)/r(x)$ in the equation above, after some rearrangements we obtain

$$\frac{f_2(x)P(x)}{Z(x)q(x+1)} = \frac{f_2(x-1)P(x-1)}{Z(x-1)q(x)}.$$

This equation implies that for some non-zero constant $c \in Q$

$$f_2(x) \cdot P(x) = c \cdot Z(x) \cdot q(x+1).$$

Consequently $z(x) := f_2(x)P(x)/q(x+1)$ must be a polynomial and a solution of (1.11), too.

The assertion on degrees follows immediately from 1. $\square$

Later (in Proposition 1.6.1) we shall see that the critical value of K_0 is just the degree of the non-zero homogeneous solution $z \in Q[x]$.

1.6 The Degree Setting

We resume the discussion of Gosper's algorithm at the point where a G-form has been computed. Then the remaining task in Gosper's algorithm is to solve the key equation (GE).

To be specific, let $(a_k)_{k\geq 0}$ be a hypergeometric sequence with rational function certificate $\lambda(x) \in Q(x)$, i.e., $a_k = \lambda(k) \cdot a_{k-1}$ for all $k \geq 1$, and let (p, q, r) be a G-form of λ. One possibility to compute a polynomial solution $f(x)$ of Gosper's key equation (GE) is by coefficient comparison. This can be carried out algorithmically once an upper bound K

for the degree of $f(x)$ is known. As Gosper (1978) showed, K can be derived from an analysis of the following equation, which is equivalent to (GE):

$$p(x) = (q(x+1) - r(x))\frac{f(x) + f(x-1)}{2} + (q(x+1) + r(x))\frac{f(x) - f(x-1)}{2}.$$

The following two cases may arise: (The degree of the zero polynomial is set to -1.)

Case 1: If $\deg(q(x+1) + r(x)) \leq \deg(q(x+1) - r(x)) =: M$, then K is uniquely determined as $K := \deg(p) - M$.

Case 2: $\deg(q(x+1) - r(x)) < \deg(q(x+1) + r(x)) =: m$. This case appears exactly if $\deg(q) = \deg(r)$ and, moreover, the leading coefficients of q and r are equal. Thus by the Gosper-type representation (G1) we may assume that these leading coefficients are equal to 1. Let $f(x) = f_K x^K + O(x^{K-1})$, $f_K \in Q \setminus \{0\}$, be a polynomial solution f of (GE). (In this particular case, the notation $O(x^d)$ stays for a polynomial of degree at most d.) Then the rest of the degree analysis can be read off the observation that

$$p(x) = f_K \cdot L(K) \cdot x^{K+m-1} + O(x^{K+m-2}), \tag{1.12}$$

with $L(K)$ being a linear polynomial of the form $L(K) = K - K_0$, where K_0, the root of $L(K)$, is determined as the coefficient of x^{m-1} in $r(x) - q(x+1)$, in usual notation

$$K_0 := [x^{m-1}]\,(r(x) - q(x+1)). \tag{1.13}$$

According to the degree comparison of both sides of (1.12) the set of polynomial solutions f of (GE) splits into two classes: those solutions f with $\deg(f) = K_0$, which is just possible for K_0 being an integer greater than $\deg(p) - m + 1$, and those solutions f with $\deg(f) \neq K_0$, which corresponds to $K := \deg(p) - m + 1$. Recalling that $m = \deg(q)$, one has

Case 2a: if K_0 is not an integer, then K is uniquely determined as $K := \deg(p) - \deg(q) + 1$,

Case 2b: if K_0 is an integer, take $K := \max(K_0, \deg(p) - \deg(q) + 1)$.

It may happen that K is determined to be a negative integer. This means that no hypergeometric sequence $(s_n)_{n \geq 0}$ solving the difference equation (DE) exists and Gosper's algorithm terminates.

1.6.1 K_0-cases

In his survey on indefinite summation algorithms, Lafon (1983) writes about Gosper's algorithm: "We have never observed that (the degree) ... was set to K_0; here some improvements may be possible."

This remark is a bit confusing. Actually such a "K_0-example" is provided by Lafon himself on the same page (Lafon, 1983, p. 75): For the (regular rational) input $a_n = 1/(n(n+2))$, $K := K_0$ $(= 2)$ is set by Gosper's algorithm as the degree for the polynomial $f(n)$.

Moreover, there are prominent *proper hypergeometric* sequences for which exactly the K_0-setting yields a solution. One of such sequences arises from the famous Apéry recurrence, see Section 1.7.2.

1.6.2 Rational Sequence Summation

Suppose we run Gosper's algorithm on the rational sequence input $(F(n))_{n\geq 0}$ of the form $F(x) = f_1(x)/f_2(x)$; $f_1, f_2 \in Q[x]$.

Let (1.14) be Gosper's representation of the quotient $F(x)/F(x-1)$:

$$\frac{f_1(x)f_2(x-1)}{f_2(x)f_1(x-1)} = \frac{p(x)}{p(x-1)} \cdot \frac{q(x)}{r(x)}. \tag{1.14}$$

From (1.14) we have

$$f_1(x)f_2(x-1)p(x-1)r(x) = f_2(x)f_1(x-1)p(x)q(x). \tag{1.15}$$

We see that $\deg(q(x)) = \deg(r(x)) =: m$ and $[x^m]\, q(x) = [x^m]\, r(x)$. Thus Case 2 of Gosper's degree analysis applies. We have to look for the value of K_0:

Proposition 1.6.1 *For each non-zero rational function $F(x)$ we have*

$$K_0 = \deg(p(x)) - \deg(q(x)) - \mathrm{Deg}(F(x)), \tag{1.16}$$

where K_0 is the value computed by Gosper's algorithm in Case 2 and $p(x)$, $q(x)$, $r(x)$ are the polynomials arising in Gosper's representation (1.14).

Proof. Denote $f_1(x) = \sum_{i=0}^{s} a_i x^i$, $f_2(x) = \sum_{i=0}^{t} b_i x^i$, $p(x) = \sum_{i=0}^{d} p_i x^i$, $q(x) = \sum_{i=0}^{m} q_i x^i$, $r(x) = \sum_{i=0}^{m} r_i x^i$ with $a_s\, b_t\, p_d\, q_m\, r_m \neq 0$. Note that $q_m = r_m$.

By coefficients comparison at $x^{s+t+d+m-1}$ in (1.15) we obtain (remember that $q_m = r_m$)

$$a_{s-1}b_t p_d r_m + a_s(-tb_t + b_{t-1})p_d r_m + a_s b_t(-dp_d + p_{d-1})r_m + a_s b_t p_d r_{m-1} = \\ b_{t-1}a_s p_d r_m + b_t(-sa_s + a_{s-1})p_d r_m + b_t a_s p_{d-1} r_m + b_t a_s p_d q_{m-1},$$

hence

$$(s-t-d)a_s\, b_t\, p_d\, r_m = a_s\, b_t\, p_d\,(q_{m-1} - r_{m-1})$$

and

$$(-d+m-t+s)r_m = mr_m + q_{m-1} - r_{m-1}.$$

Thus

$$d-m+t-s = -\frac{mr_m + q_{m-1} - r_{m-1}}{r_m},$$

which together with $q_m = r_m$ yields

$$\deg(p(x)) - \deg(q(x)) - \operatorname{Deg}(F(x)) = -2\frac{mq_m + q_{m-1} - r_{m-1}}{q_m + r_m}.$$

On the r.h.s. of the last equation we have the value

$$-2\frac{[x^{m-1}]\,(q(x+1) - r(x))}{[x^m]\,(q(x) + r(x))}. \tag{1.17}$$

W.l.o.g. we can assume q and r to be monic. Then (1.17) is precisely equal to the value K_0 (cf. (1.13)) in Gosper's degree analysis. Thus we have proved that (1.16) holds for each rational input sequence. □

1.6.3 Description of the K_0-case in Rational Summation

With respect to our result, the "$K \leftarrow K_0$"-case in rational summation occurs if and only if

$$\deg(p(x)) - \deg(q(x)) - \operatorname{Deg}(F(x)) \geq \deg(p(x)) - \deg(q(x)) + 1 \tag{1.18}$$

iff

$$\operatorname{Deg}(F(x)) \leq -1$$

iff the summation input $(F(k))_{k\geq 0}$ is a regular rational sequence.

If this is the case, the solution to the summation problem is given by

$$R(x) = \frac{q(x+1)f(x)}{p(x)}F(x)$$

with $\deg(f(x)) := K_0 = \deg(p(x)) - \deg(q(x)) - \mathrm{Deg}(F(x))$. (It follows from Gosper's precise analysis that this degree bound is accurate.) We compute

$$\begin{aligned}\mathrm{Deg}(R(x)) &= \deg(q(x)) + (\deg(p(x)) - \deg(q(x)) - \mathrm{Deg}(F(x))) \\ &\quad - \deg(p(x)) + \mathrm{Deg}(F(x)).\end{aligned}$$

Hence, $\mathrm{Deg}(R(x)) = 0$.

1.6.4 A Better Degree Setting

We learned that for regular rational function inputs $F(x)$, the solution function $R(x)$ of (DE) computed by Gosper's algorithm arises from the K_0-case and, moreover, $\mathrm{Deg}(R(x)) = 0$ holds. Let $R(x) = r_1(x)/r_2(x)$, $\deg(r_1(x)) = \deg(r_2(x))$. Then $r_1(x)/r_2(x) = c + r_3(x)/r_2(x)$, $c \in Q \setminus \{0\}$ with $r_3 = 0$ or $\deg(r_3(x)) < \deg(r_2(x))$. From this we get another solution of the difference equation (DE), namely

$$\frac{r_3(x)}{r_2(x)} - \frac{r_3(x-1)}{r_2(x-1)} = F(x). \tag{1.19}$$

Since $\mathrm{Deg}(r_3(x)/r_2(x)) < 0$, we see that this solution cannot correspond to the K_0-case. Moreover, (1.19) implies $\mathrm{Deg}(r_3(x)/r_2(x)) = \mathrm{Deg}(F(x)) + 1$ for the regular rational solution of (DE) from which we calculate the degree of the respective polynomial $f(x)$ to be

$$\mathrm{Deg}(F(x)) + 1 - \mathrm{Deg}(F(x)) + \deg(p(x)) - \deg(q(x))$$

which is the second alternative of Case 2b of Gosper's algorithm.

For the practical applications we note that the degree of $f(x)$ (and so the order of the linear system for coefficients of $f(x)$) decreases by the same value as the rational function degree of the resulting sum does, i.e., by $-\mathrm{Deg}(F(x)) - 1$.

1.6.5 Non-regular Rational Input

The last class of inputs that has not been treated yet is the set of non-regular rational sequences. We show that no improvement of degree setting is possible here:

From Proposition 1.5.4.3 we have that

$$\mathrm{Deg}(F(x)) \geq 0 \qquad \Longleftrightarrow \qquad \deg(z(x)) < \deg(p(x)) - \deg(q(x)) + 1$$

for any non-zero solution $z(x) \in Q[x]$ of the homogeneous form of the key equation (GE). Due to Gosper's degree analysis this also implies

$$\deg(z(x)) < \deg(y(x))$$

where $y \in Q[x]$ solves (GE). This means that in the case of the non-regular rational input, all solutions of (GE) are of the same degree. In particular, we see that this degree is $\deg(p(x)) - \deg(q(x)) + 1$ since Proposition 1.5.4.3 and Proposition 1.6.1 yield together

$$K_0 = \deg(z(x))$$

and so K_0 is less than $\deg(p(x)) - \deg(q(x)) + 1$ here.

1.6.6 "Plain" and "Hidden" Rational Sequences

We should be aware of the fact that the input sequence actually might be a rational one but in a disguised form. For example,

$$a_k = k!/(k+6)! \tag{1.20}$$

is a rational sequence.

Such cases are recognized easily when processed by humans but need more care when we implement summation in a computer algebra system. Success with the rationality test allows us to reduce computation time by taking the better degree setting instead of the maximum in Case 2b.

Here we meet central issues of symbolic computation, namely simplification and canonical forms.

However, even if we do not simplify the input completely, there is a guideline that can help us:

Proposition 1.6.2 *Let m be the value computed in Case 2 of Gosper's algorithm (cf. Section 1.6). If we get into Case 2b with $m = 1$ (q and r are linear polynomials), then the input sequence is rational.*

Proof. We can make q and r monic. Suppose $q(x) = x + q_0$, $r(x) = x + r_0$. Then $K_0 = r_0 - q_0 - 1$ must be a non-negative integer. Denote the summation input by $(a_k)_{k\geq 0}$. Then the G-representation is

$$\frac{a_k}{a_{k-1}} = \frac{p(k)}{p(k-1)} \cdot \frac{k+q_0}{k+r_0}$$

for some $p(x) \in Q[x]$. Now the result follows directly from Proposition 1.3.2 applied with $p_1(x) := p(x)$ and $p_2(x) := \prod_{i=q_0+1}^{r_0}(x+i)$. □

Based on our results given up to now, *we suggest the following improvement of the degree setting in Gosper's algorithm by regrouping the two subcases of Case 2:*

If K_0 is not an integer **or** the input sequence is rational **or** $m = 1$
then $K := \deg(p(n)) - m + 1$ $\{$*Case 2a*$\}$
else $K := \max(K_0, \deg(p(n)) - m + 1)$ $\{$*Case 2b*$\}$

1.7 Other K_0-examples

We have shown how to improve the degree reasoning for rational inputs. In this section we present some proper hypergeometric K_0-cases documenting that no general improvement is possible here.

1.7.1 A "Simple" Proper Hypergeometric K_0-case

It is hard to find a "nice" example with binomials or even with (integer) factorials and not to fall into the rational case at the same time. This is the reason why we use somewhat cumbersome fractions and raising factorials here:

Let $x^{\overline{n}} = x(x+1)\ldots(x+n-1)$ be the raising factorial and let $\tilde{p}(n) = \frac{1}{36}(-35n^2 - 20n + 65)$. We want to sum

$$a_n = \tilde{p}(n) \frac{{(-5/2)^{\overline{n+1}}}^2}{(-1/3)^{\overline{n+1}}(-2/3)^{\overline{n+1}}}.$$

Gosper's representation here is $p(n) = \tilde{p}(n)$, $q(n) = (n-5/2)^2$, $r(n) = (n-1/3)(n-2/3)$, so $\deg(q(n)) = \deg(r(n))$ and leading coefficient of q is equal to the leading coefficient of r. We have that $m = 2$ and the degree bounds for polynomial $f(n)$ are

$$\deg(p) - m + 1 = 2 - 2 + 1 = 1$$

and

$$K_0 = 2.$$

Thus we are in the K_0-case with a balanced linear system for unknown coefficients c_2, c_1, c_0 of polynomial $f(n)$. The system has exactly one solution because its determinant is different from zero. The solution is $(c_2, c_1, c_0) = (1, 0, 1)$, thus we are in the proper hypergeometric K_0-case with $f(n) = n^2 + 1$. The sum is

$$s_n = (n-3/2)^2(n^2+1)\frac{(-5/2)^{\overline{n+1}^2}}{(-1/3)^{\overline{n+1}}(-2/3)^{\overline{n+1}}}.$$

Remark. We note that for $m = 1$ and $K = K_0$, the linear system for coefficients of $f(x) = c_{K_0}x^{K_0} + \ldots + c_0$ is underdetermined. It has K_0 equations and $K_0 + 1$ unknowns. This fact just supports the claim of Proposition 1.5.2.2.

Generally, in the "$K = K_0$" case the linear system for coefficients of $f(x)$ arises from coefficient comparisons at $\deg(q(x+1)) + \deg(f(x)) + 1 - 1 = K_0 + m$ different powers of x in (GE). (The $+1$ counts the absolute term whereas -1 discounts the vanishing leading term, cf. Gosper's degree analysis.). Hence, the system has $K_0 + m$ equations and $K_0 + 1$ unknowns. Thus it is the value of m that influences whether the system is underdetermined, balanced or overdetermined ($m = 1$, $m = 2$, $m > 2$). The value $m = 1$ means rational input, hence the value $m = 2$ from the previous example is minimal for presentation of a *proper hypergeometric K_0-case.*

1.7.2 Apéry's Recurrence

Finally we present a nice proper hypergeometric K_0-example. The value of m is equal to 4 here. The example is taken from (Paule, Strehl, 1991).

For non-negative integers n, k let

$$F_{n,k} = \binom{n}{k}^2 \binom{n+k}{k}^2. \tag{1.21}$$

Let us recall the famous Apéry recurrence

$$\forall n \in \mathbb{N} \qquad c_0(n) \cdot S_n + c_1(n) \cdot S_{n+1} + c_2(n) \cdot S_{n+2} = 0, \tag{1.22}$$

where

$$\begin{aligned} &c_0(n) = (n+1)^3, \quad c_1(n) = -(2n+3)(17n^2+51n+39), \\ &c_2(n) = (n+2)^3, \end{aligned} \tag{1.23}$$

and

$$S_n = \sum_{k=0}^{n} F_{n,k}. \tag{1.24}$$

Remark. For an excellent account on how this recurrence is used to prove the irrationality of $\zeta(3)$ see (van der Poorten, 1979).

Note that the double-indexed sequence $(F_{n,k})_{n\geq 0, k\geq 0}$ is hypergeometric in both variables. Under slight side-conditions (see Zeilberger (1990*a*), (1990*b*) or Wilf and Zeilberger (1992)) for such sequences there exist a non-negative integer d, polynomials $c_0(n), \ldots, c_d(n)$ being independent of k, and a double-indexed sequence $(G_{n,k})_{n\geq 0, k\geq 0}$, again hypergeometric in both variables, such that

$$\begin{aligned} c_0(n) \cdot F_{n,k} + c_1(n) \cdot F_{n+1,k} + \ldots + c_d(n) \cdot F_{n+d,k} \\ = G_{n,k} - G_{n,k-1}. \end{aligned} \tag{1.25}$$

Since the l.h.s. of the equation above can be rewritten as $F_{n,k}$ times a rational function in the two variables n, k, i.e., the resulting expression is hypergeometric in k (actually it is hypergeometric in both variables), it is possible to compute $G_{n,k}$ and the coefficient polynomials $c_i(n)$ by executing Gosper's algorithm once the order d is known.

Now running this procedure in the Apéry situation, i.e., with choosing $F_{n,k}$ as defined in (1.21) and setting $d = 2$, produces exactly the situation of Case 2b described above. In the following we give the details of that computation.

The left-hand-side of equation (1.25) can be rewritten as the following rational function multiple of $F_{n,k}$:

$$\frac{p_0(n,k)\cdot c_0(n) + p_1(n,k)\cdot c_1(n) + p_2(n,k)\cdot c_2(n)}{(n-k+1)^2(n-k+2)^2}\cdot F_{n,k} = a_k, \tag{1.26}$$

where

$$\begin{aligned} p_0(n,k) &= (n-k+2)^2(n-k+1)^2,\\ p_1(n,k) &= (n-k+2)^2(n+k+1)^2,\\ p_2(n,k) &= (n+k+2)^2(n+k+1)^2. \end{aligned}$$

The polynomials corresponding to a G-form of the quotient a_k/a_{k-1} are computed as

$$\begin{aligned} &p(x) = c_0(n)p_0(n,x) + c_1(n)p_1(n,x) + c_2(n)p_2(n,x),\\ &q(x) = (n+x)^2(x-n-3)^2,\\ &r(x) = x^4. \end{aligned}$$

In addition, we find that

$$\deg(p(x)) = 4,\ \deg(q(x+1)-r(x)) = 3,\ \text{and}\ \deg(q(x+1)+r(x)) = 4.$$

One can observe that

$$K_0 = 2 \text{ and } \deg(p(x)) - m + 1 = 1.$$

Thus we are in Case 2b, where now the degree setting K for $f(x)$ has to be set to K_0, i.e., $K := 2$.

Following that pattern, i.e., that of the polynomials p, q, r, it is easy to construct further examples where exactly the same instance of Case 2b occurs.

For the sake of completeness we want to remark that by running Gosper's algorithm one gets for the coefficient polynomials $c_i(n)$, $i = 0,1,2$, the same values (1.23) as in Apéry's recurrence, $f(x) = 4(2n+3)(2x^2+x-(2n+3)^2)$ and thus

$$G_{n,k} = \frac{q(k+1)}{p(k)}\cdot f(k)\cdot a_k = \frac{(n+k+1)^2}{(n-k+1)^2}\cdot f(k)\cdot F_{n,k}.$$

With these substitutions Apéry's recurrence (1.22) follows from (1.25) by "telescoping", i.e., summation w.r.t. k. (If n is fixed then $G_{n,k}$ as a function in k has finite support, as it is a rational function multiple of $F_{n,k}$.)

1.8 More on Rational Summation

To conclude this degree analysis we briefly comment on other methods for rational function summation.

The (probably) first method for rational sequence summation was designed by Abramov (1971). Nowadays it can be viewed as a special version of Gosper's algorithm adjusted for rational sequences. Abramov solves an equation which is similar to Gosper's equation (GE), however, he considers only Case 2a in degree setting since, in his approach, it leads to the solution if there is any. It follows from (1.18) that Case 2a delivers a better setting than Case 2b if and only if the degree of the numerator of the input sequence is less than the degree of the denominator. This can be always done by putting the polynomial part of the input aside. There are considerably easier methods for summing polynomials. (E.g., transformation in the falling factorial base.)

On the other hand, Gosper stuck to the higher degree setting because he wanted to ensure that no solution is lost. Sometimes we pay for this comfort by unnecessary computations.

As far as we know, neither of them considered or discussed the approach of the other one.

Summation analogs of Hermite integration of rational functions have been provided by Abramov (1975) and Moenck (1977). Since both methods are iterative and based on gcd-computations, they cannot be compared to the two mentioned above.

Paule (1992), in an effort to close gaps in Moenck's work, introduced the concept of greatest-factorial factorization. In that paper a new approach to rational sequence summation is given including a summation analog of Horowitz's method for rational function integration.

For a detailed comparison of the last three approaches mentioned see Pirastu (1992).

Recently Pirastu and Strehl (1994) invented a rational summation algorithm which for any given input finds the optimal solution, where optimality is defined in terms of degrees of the polynomials that appear as denominators in the solution (both in the rational and in the transcendental part).

1.9 Methodological Aspects

Gosper's approach involved testing many cases with Macsyma until a pattern emerged that worked for all cases and led to the discovery of the algorithm. Following Gosper's own words (1976), "if Stirling had been granted access to a computerized symbolic mathematic system, he would probably have done most of this work before 1750." Our approach was basically the same, namely experimenting with Gosper's algorithm and observing carefully what happens at the point where it comes to the degree setting. Based on these observations we then rigorously proved theorems characterizing the degree setting.

Computer algebra systems stimulate research on efficient symbolic algorithms that make them more powerful. At the same time these systems yield a wonderful environment for experimenting with symbolic algorithms which in turn leads to further improvements in the theory. Hence, this field provides an excellent playing ground for climbing up the creativity spiral (Section 0.1).

Part II

Enumerative Combinatorics

Chapter 2

Symmetry Classes of Mappings

This is a preparatory chapter for Part II of our thesis. We shortly recall basic definitions in *finite group actions*, in particular the statements concerning the enumeration of the symmetry classes of mappings. The reader may find more information in the first two chapters of the book (Kerber, 1991).

2.1 Definitions

Definition 2.1.1 *Let $(a_i)_{i\geq 0}$ be a sequence. The formal power series*

$$\sum_{i=0}^{\infty} a_i z^i$$

is called the (ordinary) generating function *for the sequence (a_i).*

For an excellent textbook on generating functions we refer to (Wilf, 1993).

Definition 2.1.2 *Let G be a finite group and X a finite set. Suppose the mapping*

$$G \times X \to X, \quad (g, x) \mapsto gx$$

fulfills two axioms:

$A1.$ $(\forall x \in X) \quad 1_G x = x$
$A2.$ $(\forall g_1, g_2 \in G)(\forall x \in X) \quad (g_1 g_2)x = g_1(g_2 x)$

where 1_G is the unit element of G. Then we call this mapping finite group action *of G on X. We abbreviate this by saying that X is a G-set or by simply writing ${}_G X$.*

Remark. Let us emphasize that in Definition 2.1.2 both the group G and the set X are *finite.* The definition for infinite groups and/or infinite sets is completely analogous. However, we do not study infinite actions in our thesis since we do not really use them here. The only infinite action, which occurs in Section 4.3, will be transformed to a limit of a sequence of finite actions.

Let S_X denote the symmetric group on X, i.e., the group of all bijections from X to X and let X be a G-set. The homomorphism

$\delta : G \to S_X$, $\delta(g) := \bar{g}$ where $\bar{g} : x \mapsto gx$, is a permutation representation of G. (One has to verify that $\bar{g} \in S_X$ and $\overline{g_1 \cdot g_2} = \overline{g_1} \cdot \overline{g_2}$, which is easy.) The image of the permutation representation of G is denoted by $\bar{G}$:

$$\delta : G \mapsto \bar{G} \leq S_X.$$

Remark. Later on, we will stick to the common abuse in the terminology by identifying the permutation representation (as a mapping) with the image of a group under this mapping.

Definition 2.1.3 *The* natural action *of the symmetric group S_X on its underlying set X is defined by*

$$(\pi, x) \mapsto \pi(x).$$

Definition 2.1.4 *If $G \leq S_X$ for some set X then we will say that G is a* permutation group. *The* degree *of G is $|X|$.*

Fact 2.1.5 *Let ${}_GX$ be a finite action. The relation $\sim_G$ defined by*

$$x_1 \sim_G x_2 \ :\Longleftrightarrow (\exists g \in G) \quad x_2 = gx_1$$

is an equivalence relation on X.

Proof. $A1$ gives reflexivity while $A2$ assures transitivity. Finally, $A1$ and $A2$ together yield symmetry. □

Definition 2.1.6 *The equivalence classes of $\sim_G$ are called* orbits. *The orbit of x is denoted by*

$$G(x) := \{gx \mid g \in G\}.$$

If $G \times X \to X$ is a finite action and $H \leq G$ then we obtain the *subaction* $H \times X \to X$ by mapping restriction.

Another way to define a subaction of the action ${}_GX$ is to take a union of several G's orbits on X (let us call this union Y) and to consider the action ${}_GY$ defined again by mapping restriction.

Definition 2.1.7 *A subset $\mathcal{T}$ of X such that*

$$X = \dot{\bigcup_{t \in \mathcal{T}}} G(t)$$

(on the right-hand side we have a disjoint union) is called a transversal *of the orbits.*

Definition 2.1.8 *The set of all orbits will be denoted by*

$$G \backslash\backslash X := \{G(x) \mid x \in X\}.$$

Definition 2.1.9 *Let $G \times X \to X$ and $H \times Y \to Y$ be two actions such that there is an isomorphism $\tau : G \to H$ and a bijection $\omega : X \to Y$ with $\tau(g)\omega(x) = \omega(gx)$ for any $g \in G$, $x \in X$. Then we say that the actions ${}_GX$ and ${}_HY$ are* isomorphic.

Obviously, ω induces a bijection between G-orbits and H-orbits.

Definition 2.1.10 *Let X be a G-set. For each $x \in X$ we introduce its* stabilizer

$$G_x := \{g \in G \mid gx = x\}.$$

Clearly, $G_x \leq G$ for any $x \in X$.

Definition 2.1.11 *With each group element $g \in G$ we associate its* fixed point set

$$X_g := \{x \in X \mid gx = x\}.$$

Fact 2.1.12 *Let X be a G-set, $x \in X$. Then $|G(x)| = |G|/|G_x|$.*

Proof. For arbitrary $g, g' \in G$ we have

$$gx = g'x \iff g^{-1}g' \in G_x \iff g'G_x = gG_x.$$

This implies that the mapping

$$\begin{array}{rcl} G(x) & \to & G/G_x \\ gx & \mapsto & gG_x, \end{array}$$

where G/G_x denotes the set of left cosets of G_x in G, is a bijection. $\square$

The value $|G(x)|$ is usually called *length* of the orbit $G(x)$.

Lemma 2.1.13 (Cauchy-Frobenius) *Let ${}_GX$ denote a finite action and $w : X \to R$ a map from X into a commutative ring R containing $\mathbb{Q}$ as a subring. If w is constant on the orbits of G on X, then we have for any transversal $\mathcal{T}$ of the orbits:*

$$\sum_{t\in\mathcal{T}} w(t) = \frac{1}{|G|}\sum_{g\in G}\sum_{x\in X_g} w(x) = \frac{1}{|\bar{G}|}\sum_{\bar{g}\in\bar{G}}\sum_{x\in X_{\bar{g}}} w(x). \tag{2.1}$$

Proof. We have

$$\sum_{g\in G}\sum_{x\in X_g} w(x) = \sum_{x}\sum_{g\in G_x} w(x)$$
$$= \sum_x |G_x| w(x) = |G|\sum_x |G(x)|^{-1} w(x) = |G|\sum_{t\in\mathcal{T}} w(t).$$

The last equation follows from the assumption that w is constant on orbits. □

This is the so-called weighted form of Cauchy-Frobenius Lemma as it allows us to enumerate orbits by weight. By taking the constant weight $w \equiv 1$ we obtain the unweighted form of the Lemma which then states that the total number of orbits is equal to the average cardinality of fixed point sets.

Remark. Lemma 2.1.13 is often incorrectly called "Burnside's Lemma", see (Kerber, 1991), p. 407 for a historical account.

Definition 2.1.14 *Let X be a G-set and let Y be a finite set. The* induced action *of G on Y^X is defined by*

$$\begin{array}{rcl} G \times Y^X & \to & Y^X \\ (g, f)(x) & := & f(g^{-1}x), \end{array}$$

i.e., (g, f) is mapped to $\tilde{f}$, where $\tilde{f}(x) := f(g^{-1}x)$. The orbits of G on Y^X will be called symmetry classes of mappings.

Definition 2.1.15 *Given a weight mapping $W : Y \to R$, where R is a commutative ring containing $\mathbb{Q}$ as a subring, we define the* multiplicative weight *$w : Y^X \to R$ by*

$$w(f) := \prod_{x\in X} W(f(x)) \tag{2.2}$$

for each $f \in Y^X$. Clearly, w is constant on G-orbits.

In order to use Lemma 2.1.13 for enumeration of symmetry classes of mappings by their weight we need to know the sum of the weights of mappings fixed by a given $g \in G$. To this end we have to define the cycle type of a permutation.

Definition 2.1.16 *Let $_GX$ be a finite action. Each permutation $\bar{g} \in \bar{G}$ can be decomposed in a product of pairwise different disjoint cycles; this factorization is unique up to the relative order of the cycles in the product, which is of no consequence. For each $1 \leq i \leq |X|$, let $a_i(\bar{g})$ denote the number of cycles of length i occurring in this factorization. The $|X|$-tuple*

$$a(\bar{g}) := (a_1(\bar{g}), a_2(\bar{g}), \ldots, a_{|X|}(\bar{g}))$$

we be called the cycle type *of $\bar{g}$.*

Obviously, $\sum_{i=1}^{|X|} i \cdot a_i(\bar{g}) = |X|$ for any $\bar{g}$.

Lemma 2.1.17 *Let $_GX$ be a finite action, Y be a finite set and let the weight of functions in Y^X be defined as in (2.2). For each $\bar{g} \in \bar{G}$ we have*

$$\sum_{f \in (Y^X)_{\bar{g}}} w(f) = \prod_{i=1}^{|X|} \left(\sum_{y \in Y} W(y)^i \right)^{a_i(\bar{g})}. \tag{2.3}$$

Proof. If $f \in (Y^X)_{\bar{g}}$ then f must be constant on $\bar{g}$'s cycles. For each $1 \leq i \leq |X|$ there are precisely $a_i(\bar{g})$ cycles of length i and each such cycle contributes to f's weight by a factor of $W(y)^i$ for some $y \in Y$. Summing over all possible combinations gives exactly the right-hand side of (2.3). □

Theorem 2.1.18 *Let $_GX$ be a finite action, Y be a finite set, $W : Y \mapsto R$ be a weight function and let the multiplicative weight function w be defined as in (2.2). The sum of w's values on a transversal of the orbits is equal to*

$$\frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{|X|} \left(\sum_{y \in Y} W(y)^i \right)^{a_i(\bar{g})}. \tag{2.4}$$

Proof. This follows from Lemmas 2.1.13 and 2.1.17. □

Definition 2.1.19 *Let X and Y be finite sets and let $f \in Y^X$. We define the* content *of f to be the mapping*

$$c(f, y) := |f^{-1}(y)|,$$

i.e., $c(f, y)$ is the multiplicity with which f takes the value $y \in Y$.

In the special case $Y = \{0, 1, \ldots, m\}$ we will occasionally write the content of f as $(k_0, k_1, \ldots, k_m)$ where $k_i = |f^{-1}(i)|$.

We have now the following consequence of Theorem 2.1.18:

Corollary 2.1.20 *Let Y be a finite set of indeterminates. The number of G-orbits on Y^X, the elements of which have the same content as $f \in Y^X$, is equal to the coefficient of the monomial $\prod_{y \in Y} y^{c(f,y)}$ in the polynomial*

$$\frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{|X|} \left(\sum_{y \in Y} y^i \right)^{a_i(\bar{g})}.$$

Proof. We identify each element of Y with its weight, i.e., we put $W : y \mapsto y$ for each $y \in Y$. □

Definition 2.1.21 *Let ${}_GX$ be a finite action. The* cycle index *(sometimes called* cycle indicator polynomial*) of ${}_GX$ is the polynomial*

$$C(G, X) := \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{|X|} (z_i)^{a_i(\bar{g})} \in \mathbb{Q}[z_1, z_2, \ldots, z_{|X|}]. \tag{2.5}$$

The intuition behind the name of the cycle index is that $C(G, X)$ "knows" the cycle type of all elements of $\bar{G}$.

Definition 2.1.22 *Let $C(G, X)$ be the cycle index of ${}_GX$ as in (2.5) and let $p \in \mathbb{Q}[u_1, u_2, \ldots, u_m]$ be a polynomial. The* Pólya-substitution *of p in $C(G, X)$ is defined by*

$$C(G, X | p(u_1, u_2, \ldots, u_m)) := \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{|X|} p(u_1^i, u_2^i, \ldots, u_m^i)^{a_i(\bar{g})} \in \mathbb{Q}[u_1, u_2, \ldots, u_m].$$

This definition naturally generalizes to the *Pólya-substitution* of a formal power series $f \in \mathbb{Q}[[u_1, u_2, \ldots, u_m]]$ in the cycle index, yielding another formal power series from $\mathbb{Q}[[u_1, u_2, \ldots, u_m]]$.

Theorem 2.1.23 (Pólya) *The generating function for the enumeration of G-classes on Y^X by content can be obtained from the cycle index of ${}_GX$ by Pólya-substituting $\sum_{y \in Y} y$ into the cycle index $C(G, X)$. Hence this generating function is equal to*

$$C(G, X | \sum_{y \in Y} y).$$

A generalized version of this theorem gives us a freedom to determine which orbits should be considered together for enumeration purposes.

Theorem 2.1.24 (Pólya) *Let ${}_GX$ be a finite action and let Y be a finite set. Let $R = \mathbb{Q}[t_1, \ldots, t_l]$, let $W : Y \to R$ be a weight function such that $W(y)$ is a monomial in $\mathbb{Q}[t_1, \ldots, t_l]$ for any $y \in Y$, and let the multiplicative weight of functions from Y^X be defined as in (2.2). Let z be a monomial in $\mathbb{Q}[t_1, \ldots, t_l]$. The number of G's orbits of weight z on Y^X is equal to the coefficient of z in*

$$C(G, X | \sum_{y \in Y} W(y)).$$

The *unweighted version* of the last theorem is obtained by setting $W(y) = 1$ for each $y \in Y$. It allows us to count the *total* number of orbits (disregarding the content).

Theorem 2.1.25 (Pólya) *The total number of G's orbits of on Y^X is equal to*

$$C(G, X \mid |Y|).$$

Hence the enumeration task is reduced to the computation of the cycle index for the given action. Examples of cycle indices for the most common group actions can be found on pages 72–73 of (Kerber, 1991). The definition of the cycle index given in equation (2.5) can be substantially simplified by recalling that the cycle type of $\bar{g}$ is invariant on conjugacy classes of the group $\bar{G}$.

Pólya's Theorem is the essential tool for class enumeration. We will see many its applications in the forthcoming chapters of our thesis.

Chapter 3

Symmetries in Neural Networks

This chapter develops mathematical methods for studying Hadamard pattern sets which are currently used as models of neural networks. Two applications are presented: the enumeration of equivalence classes of Hadamard pattern sets and the evaluation of orbit lengths. The chapter provides a standard application of finite group action and is intended as an introductory example for definitions and theorems from Chapter 2. Hence, it can be skipped by those readers who are well-acquainted with these topics.

Our work was motivated by theoretical physics scientists who are currently introducing and investigating a new model for neural networks involving the so-called Hadamard patterns. Global properties of an individual network can be found from symmetry considerations of the invariance group of the specific pattern set stored by some learning rule. Theoretical physics background of our investigations in explained in (Folk, Kartashov and Ortbauer, 1992). The summary of our results and their physical implications can be found in (Folk, Kartashov, Lisoněk and Paule, 1993). Technical details of the isomorphism between G_n's and $GL(n,2)$'s actions (Section 3.3) were worked out by Brawley and Lisoněk (1992).

3.1 Definitions

Let X be a set. A k-subset of X (k natural) is any subset of X with cardinality k. The set of all k-subsets of X is denoted as $X^{[k]}$:

$$X^{[k]} := \{S \mid S \subseteq X\ ,\ |S| = k\}.$$

Let $t = (t_0, \ldots, t_{m-1})$ and $s = (s_0, \ldots, s_{m-1})$ be two m-tuples. We define

$$t \cdot s := (t_0, \ldots, t_{m-1}, s_0, \ldots, s_{m-1}).$$

To make the equations more readable we will sometimes write $t[i]$ instead of t_i but we will always keep in mind that these two symbols denote the same object, namely the i-th component of the vector t.

Let $GF(2)^m$ be the m-dimensional vector space over $GF(2)$. The elements of $GF(2)^m$ will be considered as row vectors. The coordinates of these vectors will be numbered by $0, 1, \ldots, m-1$. For each $n \geq 1$, let

$\{e_{0,n}, \ldots, e_{n-1,n}\}$ be the standard basis of $GF(2)^n$ where

$$e_{i,n} := (\underbrace{0, \ldots, 0}_{i}, 1, \underbrace{0, \ldots, 0}_{n-i-1}).$$

Definition 3.1.1 *For* $u \in GF(2)^m$, $u = (u_0, \ldots, u_{m-1})$, *we define its* complement $\overline{u} := (1 - u_0, \ldots, 1 - u_{m-1})$.

Thus $\overline{\overline{u}} = u$.

Definition 3.1.2 *Let* $H_n \subseteq GF(2)^{2^n}$ *be defined inductively as follows:*

$$H_0 := \{(0)\}$$

and for $i \geq 0$,

$$H_{i+1} := \{p \cdot q \mid p \in H_i \wedge (q = p \vee q = \overline{p})\}.$$

The elements of H_n *are called* Hadamard patterns of length 2^n.

For example,

$$H_2 \;=\; \{\ (0,0,0,0),\ (0,0,1,1),\ (0,1,0,1),\ (0,1,1,0)\ \}.$$

We introduce the sequence of mappings $(\Phi_n)_{n \geq 1}$

$$\Phi_n \;:\; H_n \to GF(2)^n$$

where

$$\Phi_n(p) := (p[2^0], p[2^1], \ldots, p[2^{n-1}]).$$

E.g.,

$$\Phi_3(0,1,0,1,1,0,1,0) = (1,0,1),$$

$$\Phi_2^{-1}(1,0) = (0,1,0,1).$$

Lemma 3.1.3 *For each* $n \geq 1$, Φ_n *is a bijection between* H_n *and* $GF(2)^n$.

Proof. The statement follows easily from the definition of H_n. $\square$

We also introduce the bijections $(\phi_n)_{n\geq 1}$

$$\phi_n : \{0, 1, \ldots, 2^n - 1\} \to GF(2)^n$$

such that for $0 \leq k \leq 2^n - 1$

$$\phi_n(k) := \sum_{i \in I} e_{i,n}$$

where I is the unique subset of $\{0, 1, \ldots, n-1\}$ such that

$$k = \sum_{i \in I} 2^i.$$

Thus $\phi_n(k)$ is the coefficient vector of the dyadic representation of k. For example, $\phi_4(13) = (1, 0, 1, 1) = e_{0,4} + e_{2,4} + e_{3,4}$ because $13 = 2^0 + 2^2 + 2^3$.

3.1.1 Automorphism Group of H_n

The automorphism group of H_n will be denoted G_n and is defined as the group consisting of all permutations that map Hadamard patterns to Hadamard patterns:

$$G_n := \{\pi \in S_{\{0,1,\ldots,2^n-1\}} \mid \pi H_n = H_n\}$$

where

$$\pi H_n = \{\pi h \mid h \in H_n\}$$

and for $h \in H_n$, $h = (h_0, h_1, \ldots, h_{2^n-1})$,

$$\pi h := (h[\pi^{-1}(0)], h[\pi^{-1}(1)], , \ldots, , h[\pi^{-1}(2^n - 1)]). \qquad (3.1)$$

Lemma 3.1.4 *G_n acts on H_n by the mapping (3.1).*

From definition of H_n it is clear that each element of G_n must fix the position 0, i.e., $G_n \leq S_{\{0\}} \oplus S_{\{1,\ldots,2^n-1\}}$. Obviously, $G_1 = S_{\{0\}} \oplus S_{\{1\}}$. We invite the reader to convince herself/himself that $G_2 = S_{\{0\}} \oplus S_{\{1,2,3\}}$. Actually, $n = 1, 2$ are the only trivial cases with $G_n = S_{\{0\}} \oplus S_{\{1,\ldots,2^n-1\}}$. For example, $|G_3| = 168$ whereas $|S_{\{0\}} \oplus S_{\{1,\ldots,7\}}| = 5040$.

3.1.2 The Group $GL(n, 2)$

The group of all $n \times n$ non-singular matrices over $GF(2)$ is usually called the *nth general linear group* over $GF(2)$ and denoted by $GL(n, 2)$. The group operation is matrix multiplication. Each matrix from $GL(n, 2)$ can be thought of as an n-tuple of non-zero rows $(r_1, \ldots, r_n)$ such that r_i does not belong to the subspace of $GF(2)^n$ spanned by $r_1, \ldots, r_{i-1}$. Hence, the order of $GL(n, 2)$ is equal to $\prod_{i=1}^{n}(2^n - 2^{i-1})$.

$GL(n, 2)$ acts on $GF(2)^n$ by multiplication:

$$\begin{array}{l} GL(n,2) \times GF(2)^n \to GF(2)^n \\ (M, f) \mapsto (M \cdot f^T)^T = f \cdot M^T. \end{array}$$

Observing the orders of first few stabilizers G_n, Paule stated a conjecture that G_n is isomorphic to $GL(n, 2)$. In the next section we show that this is true and, moreover, we provide the isomorphism which carries over the respective group actions. Before stating the two main theorems, we prove some important lemmas about the objects introduced so far.

3.2 Preparatory Statements

Lemma 3.2.1 *Let* $\pi \in S_{\{0,1,\ldots,2^n-1\}}$ *and consider the action*

$$\pi f := (f[\pi^{-1}(0)], f[\pi^{-1}(1)], \ldots, f[\pi^{-1}(2^n - 1)])$$

of π *on* $GF(2)^{2^n}$. *Then* π *acts as an invertible linear operator on* $GF(2)^{2^n}$, *i.e.,* π *acts as an automorphism of* $GF(2)^{2^n}$. *(A* linear operator *on a vector space W is a linear transformation from W to W.)*

Proof. Let f and g be two members of $GF(2)^{2^n}$, i.e., $f + g$ is in $GF(2)^{2^n}$. Then for $0 \le i \le 2^n - 1$ we have

$$\begin{aligned} \pi(f+g)[i] &= (f+g)(\pi^{-1}[i]) = f(\pi^{-1}[i]) + g(\pi^{-1}[i]) = \pi f[i] + \pi g[i] \\ &= (\pi f + \pi g)[i]. \end{aligned}$$

Thus, $\pi(f + g) = \pi f + \pi g$. The invertibility follows from the definition of group action. □

Lemma 3.2.2 *The set H_n of Hadamard patterns of length 2^n is an n-dimensional subspace of $GF(2)^{2^n}$. Further, if for $k = 0, \ldots, n-1$ the vector $v_{k,n}$ is defined as*

$$v_{k,n} := \Phi_n^{-1}(\underbrace{0, \ldots, 0}_{k}, 1, \underbrace{0, \ldots, 0}_{n-k-1}) = \Phi_n^{-1}(e_{k,n})$$

(i.e., $v_{k,n}$ has alternately 2^k zeros followed by 2^k ones and so on), then set

$$\{v_{k,n} \mid 0 \leq k \leq n-1\}$$

is a basis for H_n.

Proof. (Induction on n.) The statement is clear for $n = 0$ and 1; thus, assume it is true for H_n, consider H_{n+1}. Each of the members of H_{n+1} is of the form (x, x) or $(x, \bar{x})$, where x is in H_n. Since H_n is a subspace, it is easily seen that the sum of two elements of this form is again of the form; i.e., $(x \cdot x) + (y \cdot y) = ((x+y) \cdot (x+y))$, $(x \cdot x) + (y \cdot \bar{y}) = ((x+y) \cdot (\overline{x+y}))$, $(x \cdot \bar{x}) + (y \cdot \bar{y}) = ((x+y) \cdot (x+y))$. Closure under scalar multiplication is trivial since the only scalars are 0 and 1 so H_{n+1} is a subspace. Since H_{n+1} has 2^{n+1} members and is a vector space over $GF(2)$, a counting argument shows its dimension must be $n+1$. Finally, since $\{v_{k,n} \mid 0 \leq k \leq n-1\}$ is a basis for H_n, it follows that the vectors $(v_{k,n}, v_{k,n})$, $0 \leq k \leq n-1$, are n independent elements of H_{n+1}. Further, the 2^{n+1}-long vector $v_{n,n+1}$ of 2^n zeros followed by 2^n ones is in H_{n+1} and is independent of the $(v_{k,n}, v_{k,n})$. Then the set of $n+1$ vectors taken together is a basis for H_{n+1} and the proof is complete. □

Example. For H_3, the basis is $v_{0,3} = (0,1,0,1,0,1,0,1)$, $v_{1,3} = (0,0,1,1,0,0,1,1)$, $v_{2,3} = (0,0,0,0,1,1,1,1)$. Thus, $H_3 = \{b_0 v_{0,3} + b_1 v_{1,3} + b_2 v_{2,3} \mid b_i \in GF(2)\}$.

Now consider the $n \times 2^n$ matrix V_n whose i-th row, $0 \leq i \leq n-1$, is the vector $v_{i,n}$. It is easily seen that the k-th column, $0 \leq k \leq n-1$, of V_n is

$$u_{k,n} := (\phi_n(k))^T.$$

For example, with $n = 3$ we have

$$V_3 = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

whose columns are, respectively, the binary representations of the numbers 0, 1, 2, 3, 4, 5, 6, 7.

Since the elements of H_n are precisely the set of vectors of the form

$$h = b_0 v_{0,n} + \ldots + b_{n-1} v_{n-1,n} = bV_n$$

where $b = (b_0, \ldots, b_{n-1}) \in GF(2)^n$, we see that the k-th component of the vector $h = bV_n$ is the scalar product $b \cdot u_{k,n} = b \cdot (\phi_n(k))^T$, i.e.,

$$H_n = \{(b \cdot u_{0,n}, b \cdot u_{1,n}, \ldots, b \cdot u_{2^n-1,n}) \mid b \in GF(2)^n\}.$$

For example,

$$\begin{aligned} H_3 &= \{b_0 v_{0,3} + b_1 v_{1,3} + b_2 v_{2,3} \mid b_i \in GF(2)\} = \\ &= \{(0, b_0, b_1, b_0 + b_1, b_2, b_0 + b_2, b_1 + b_2, b_0 + b_1 + b_2) \mid b_i \in GF(2)\}. \end{aligned}$$

Lemma 3.2.3 *The bijection Φ_n is an invertible linear transformation from H_n to $GF(2)^n$.*

Proof. Each h can be written uniquely in the form $h = b_0 v_{0,n} + \ldots + b_{n-1} v_{n-1,n}$ where b_i is in $GF(2)$. By definition of Φ_n, we have $\Phi_n(h) = (b_0, \ldots, b_{n-1})$ which is clearly a linear, bijective mapping. (Actually the fact is obvious as Φ_n maps the base vectors of H_n to those of $GF(2)^n$.) □

Lemma 3.2.4 *Let $h \in GF(2)^{2^n}$ and let $\Phi_n(h) = (b_0, \ldots, b_{n-1})$. Then $h \in H_n$ if and only if*

$$h = b_0 v_{0,n} + b_1 v_{1,n} + \ldots + b_{n-1} v_{n-1,n}.$$

Proof. If $h \in H_n$, then by Lemma 3.2.3, $h = b_0 v_{0,n} + b_1 v_{1,n} + \ldots + b_{n-1} v_{n-1,n}$ where $\Phi_n(h) = (b_0, b_1, \ldots, b_{n-1})$. The converse is clear. □

Lemma 3.2.5 *If π is in G_n, then π acts on H_n as an invertible linear operator.*

Proof. From Lemma 3.2.1, any $\pi \in S_{\{0,1,\ldots,2^n-1\}}$ when restricted to H_n acts as an invertible linear transformation. The fact that π is in G_n simply means that the image of H_n is H_n. □

Lemma 3.2.6 *For each π in G_n, the mapping $L_\pi : GF(2)^n \to GF(2)^n$ defined by the composition*

$$L_\pi(x) \ := \ \Phi_n \cdot \pi \cdot \Phi_n^{-1}(x)$$

is an invertible linear operator. Further, if π_1 and π_2 are in G_n, then

$$L_{\pi_1\pi_2} = L_{\pi_1} L_{\pi_2}$$

and if $\pi_1 \neq \pi_2$, then $L_{\pi_1} \neq L_{\pi_2}$.

Proof. Note that $L_{\pi_1\pi_2}(x) = \Phi_n \cdot \pi_1 \cdot \pi_2 \cdot \Phi_n^{-1}(x) = \Phi_n \cdot \pi_1 \cdot \Phi_n^{-1} \cdot (\Phi_n \cdot \pi_2 \cdot \Phi_n^{-1}(x)) = L_{\pi_1}(L_{\pi_2}(x))$ so $L_{\pi_1\pi_2} = L_{\pi_1} L_{\pi_2}$. The remaining statements are immediate from properties of linear transformations. □

3.3 Isomorphism between G_n's and $GL(n,2)$'s Actions

Let n be an arbitrary but fixed positive integer. In this section we establish an isomorphism between G_n's action on H_n and $GL(n,2)$'s action on $GF(2)^n$.

Consider a linear operator L_π corresponding to π in G_n (cf. Lemma 3.2.6) and set

$$R_k \ := \ L_\pi(e_{k,n}).$$

Then for $x = (x_0, \ldots, x_{n-1})$ in $GF(2)^n$, we may write (by linearity)

$$L_\pi(x) = x_0 R_0 + \ldots + x_{n-1} R_{n-1} = x M^T,$$

where M^T is the $n \times n$ matrix whose k-th row is R_k, $0 \leq k \leq n-1$. We use this relation to associate with each π in G_n an invertible matrix $M \in GL(n,2)$; i.e., we use the relation to define a function

$$I_n : G_n \to GL(n,2)$$

where $I_n(\pi) := M$. Clearly, the function I_n is one-to-one (since $\Phi_n \cdot \pi_1 \cdot \Phi_n^{-1} = \Phi_n \cdot \pi_2 \cdot \Phi_n^{-1}$ implies $\pi_1 = \pi_2$).

Moreover, if $I_n(\pi_1) = M_1$ and $I_n(\pi_2) = M_2$, then it is easily checked that $I_n(\pi_1\pi_2) = M_1M_2$: Let $I_n(\pi_1\pi_2) = M_3$, then

$$\begin{aligned} xM_3^T &= \Phi_n \cdot (\pi_1 \cdot \pi_2) \cdot \Phi_n^{-1}(x) = \Phi_n \cdot \pi_1 \cdot \Phi_n^{-1}(\Phi_n \cdot \pi_2 \cdot \Phi_n^{-1}(x)) \\ &= \Phi_n \cdot \pi_1 \cdot \Phi_n^{-1}(xM_2^T) = (xM_2^T)M_1^T = x(M_1M_2)^T \end{aligned}$$

Thus, $M_3 = M_1M_2$.

Finally, we show that I_n is onto; i.e., for each M in $GL(n,2)$ there is a π in G_n such that $I_n(\pi) = M$. To this end, let $M \in GL(n,2)$ be given, let C_k denote the k-th column of M^T, and consider the linear operator Π on H_n defined by the composition

$$\Pi = \Phi_n^{-1} L \Phi_n,$$

where $L(x) = xM^T$.

For each $h \in H_n$ we may write (recall the definition of base vectors $v_{k,n}$ in Lemma 3.2.2) $h = b_0v_{0,n} + \ldots + b_{n-1}v_{n-1,n}$ and $\Phi_n(h) = (b_0, \ldots, b_{n-1})$. Hence,

$$\begin{aligned} \Phi_n^{-1}L\Phi_n(h) &= \Phi_n^{-1}L(b_0, \ldots, b_{n-1}) = \Phi_n^{-1}(bM^T) = \Phi_n^{-1}(bC_0, \ldots, bC_{n-1}) = \\ &= (0, bC_0, bC_1, bC_0 + bC_1, \\ &\quad bC_2, bC_0 + bC_2, bC_1 + bC_2, bC_0 + bC_1 + bC_2, bC_3, \ldots). \end{aligned}$$

But this is exactly the result one gets from πh, the action of π on h, where π is that member of G_n such that $\pi^{-1}[2^i] = \phi_n^{-1}(C_i)$. We have now established the following two theorems.

Theorem 3.3.1 *For each $n \geq 1$, the mapping I_n is an isomorphism between G_n and $GL(n,2)$.*

Theorem 3.3.2 *For each $n \geq 1$, the action of G_n on H_n and the action of $GL(n,2)$ on $GF(2)^n$ are isomorphic in the sense of Definition 2.1.9.*

Proof. Let n be an arbitrary but fixed positive integer. In Definition 2.1.9 we put $\tau := I_n$ and $\omega := \Phi_n$. Our theorem then follows from the fact that the following diagram commutes:

$$\begin{tikzcd} H_n \arrow[r, "\pi"] \arrow[d, "\Phi_n"'] & H_n \arrow[d, "\Phi_n"] \\ GF(2)^n \arrow[r, "I_n(\pi)"'] & GF(2)^n \end{tikzcd} .$$

□

Before coming to applications, we provide two examples illustrating Theorems 3.3.1 and 3.3.2.

Example 1. Let $n_0 = 3$, $\pi_0 = (1,2,5)(3,7,4) \in G_3$. We have

$$\begin{aligned} L_{\pi_0}(e_{0,3}) &= (1,1,1), \\ L_{\pi_0}(e_{1,3}) &= (0,0,1), \\ L_{\pi_0}(e_{2,3}) &= (1,0,1). \end{aligned}$$

Thus

$$I_3(\pi_0) := \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}^T = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} .$$

Example 2. Let us have n_0, π_0 and $I_3(\pi_0)$ as in Example 1 and additionally take the Hadamard pattern $h_0 = (0,0,1,1,1,1,0,0) \in H_3$. We compute

$$\pi_0 h_0 = (0,1,0,1,0,1,0,1),$$

$$\Phi_3(\pi_0 h_0) = (1,0,0).$$

On the other hand,

$$\Phi_3(h_0) = (0,1,1)$$

and

$$(0,1,1) \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} = (1,0,0).$$

Indeed, $\Phi_3(\pi_0 h_0) = \Phi_3(h_0) \cdot (I_3(\pi_0))^T$.

3.4 Orbits of Hadamard Pattern Sets

To stay consistent with the physical model of Folk, Kartashov and Ortbauer (1992) we will now exclude from our investigations the exceptional Hadamard pattern $(0, 0, \ldots, 0)$:

$$\mathcal{H}_n := H_n \setminus \{(\underbrace{0, \ldots, 0}_{2^n})\} \quad \text{for each } n.$$

Since this pattern forms a singleton orbit in G_n's action on H_n, we can change to the action

$$G_n \times \mathcal{H}_n \to \mathcal{H}_n$$

merely by mapping restriction.

In this section we study the induced action

$$G_n \times \mathcal{H}_n^{[k]} \to \mathcal{H}_n^{[k]} \tag{3.2}$$

of G_n-permutations on k-subsets of $\mathcal{H}_n$, i.e., on pattern sets with cardinality k:

$$\pi\{h_1, \ldots, h_k\} := \{\pi h_1, \ldots, \pi h_k\}$$

for $\pi \in G_n$ and $\{h_1, \ldots, h_k\} \subseteq \mathcal{H}_n$, where

$$\pi h_i := (h_i[\pi^{-1}(0)], h_i[\pi^{-1}(1)], \ldots, h_i[\pi^{-1}(2^n - 1)])$$

for each h_i, cf. (3.1).

Our ultimate goal is to learn as much as possible about (3.2) because this action answers many questions about neural networks storing Hadamard patterns. See (Folk, Kartashov, Lisoněk and Paule, 1993) for the discussion of physical implications that follow from our results.

The crucial point in studying (3.2) is to realize the natural correspondence between the k-subsets of $\mathcal{H}_n$ and functions from $\{0,1\}^{\mathcal{H}_n}$ with content $(n-k, k)$, i.e., with $n-k$ zeros and k ones. We can now move to the action

$$G_n \times \{0,1\}^{\mathcal{H}_n} \to \{0,1\}^{\mathcal{H}_n}$$

that fits perfectly the "symmetry classes of mappings" paradigm introduced in Chapter 2. In order to apply Pólya's Theorem (Theorem 2.1.23) we need the cycle index of G_n's action on $\mathcal{H}_n$. By Theorem 3.3.2 this cycle index is equal to the index of $GL(n,2)$'s action on $\mathcal{F}_n$ where

$$\mathcal{F}_n := GF(2)^n \setminus \{(\underbrace{0, \ldots, 0}_{n})\}.$$

3.4.1 Cycle Indices of Linear Groups

The cycle types of $GL(n,2)$-matrices acting on $GF(2)^n$ have been studied by Lidl and Niederreiter (1983), pp. 523–525. The authors call them *"cycle sums"* and give an algorithm to compute the cycle sum for a given matrix. Since for increasing n the order of $GL(n,2)$ grows rapidly, this method is not suitable for evaluating the whole cycle index.

Accidentally, another kind of "cycle indices" of linear groups was defined by Kung (1981) and refined slightly by Stong (1988). Their cycle index characterizes properties of decomposition of invertible linear transformation into direct sums of cyclic linear transformations. Both authors give generating functions for their indices but they do not believe in an immediate link between their view of cycle index and the cycle index used in Pólya's Theorem.

We developed our own method for computing the (Pólya) cycle index. Since cycle types are invariant on conjugacy classes, it is enough to solve the following tasks *(I)* and *(II)* for each conjugacy class:

(I) Evaluate the cycle type. This can be done by
  (Ia) constructing a class representative and
  (Ib) using the Lidl-Niederreiter algorithm.

(II) Evaluate the class length.

The number Conj(n) of conjugacy classes of $GL(n,2)$, which clearly puts a limitation on the applicability of our method, can be evaluated from (Brawley, 1967), p. 177. For small values of n it is close to 2^n:

n	Conj(n)
5	27
10	1002
15	32559
20	1047690

All three issues *(Ia)*, *(Ib)*, *(II)* can be solved using the *Smith normal form* (SNF) of matrices which is invariant on conjugacy classes.

The SNF of an $n \times n$ non-singular matrix M over $GF(2)$ is an n-tuple of monic polynomials $f_1, \ldots, f_n \in GF(2)[x]$ such that

$\sum_{i=1}^{n} \deg(f_i) = n$,

$f_i \mid f_{i+1}$ for $i = 1, \ldots, n-1$, all f_i's have non-zero constant terms,

M is similar to the direct sum of companion matrices of polynomials $f_1, \ldots, f_n$.

The Smith normal form enables us to cope with tasks *(Ia)*, *(Ib)*, *(II)* in the following way:

(Ia) A class representative is the direct sum of companion matrices of polynomials $f_1, \ldots, f_n$.

(Ib) The cycle sum is determined from *elementary divisors* which are irreducible factors of polynomials f_i. See (Lidl, Niederreiter, 1983), p. 526.

(II) Also the class length can be figured out from elementary divisors. See (Hodges, 1958), pp. 291–2.

3.5 Computation of Orbit Numbers

The coding was done in computer algebra system Maple. We used the method described above (computing cycle index by decomposition to conjugacy classes and evaluating cycle type and class length for each conjugacy class, and finally using Pólya's Theorem). The cycle indices of groups up to $GL(5,2)$ have been verified by computational group theory system Cayley. The linear groups of higher degree could not have been checked by Cayley because of their huge orders. (The order of $GL(6,2)$ is about $2 \cdot 10^{10}$.)

A table summarizing the number of orbits of

$$GL(n,2) \times \mathcal{F}_n^{[k]} \to \mathcal{F}_n^{[k]} \tag{3.3}$$

(and hence also the number of orbits of (3.2)) for modest values of n and k can be found in (Folk, Kartashov, Lisoněk and Paule, 1993).

3.6 Length of the Winning Orbit

For each k, $n \in \mathbb{N}$ such that $k \leq n$ we single out one special orbit of the action (3.3), namely the orbit of the set

$$\{e_{0,n}, e_{1,n}, \ldots, e_{k-1,n}\}. \tag{3.4}$$

Folk, Kartashov and Ortbauer (1992) showed that, for any fixed k, the length of this orbit approaches the cardinality of $\mathcal{F}_n^{[k]}$ as n approaches infinity. Hence, they call it the *winning orbit*.

To establish the cardinality of this orbit we just need to find the order of the stabilizer of (3.4). We will denote this stabilizer by $St_{n,k}$.

Obviously, each matrix in $St_{k,n}$ is of the form

$$\left(\begin{array}{c|c} \multirow{2}{*}{M_1} & M_2 \\ \cline{2-2} & M_3 \end{array}\right)$$

where

M_1 is an $n \times k$ matrix obtained as a permutation of the column vectors $e_{0,n}^T, e_{1,n}^T, \ldots, e_{k-1,n}^T$,

M_2 is *any* $k \times (n-k)$ matrix over $GF(2)$ and

M_3 is an $(n-k) \times (n-k)$ matrix from $GL(n-k, GF(2))$.

Thus the order of the stabilizer is $k! \cdot 2^{k(n-k)} \cdot |GL(n-k, GF(2))|$ and the length of the winner's orbit is by Fact 2.1.12

$$\frac{(2^n - 1) \cdot \ldots \cdot (2^n - 2^{n-1})}{k! \cdot 2^{k(n-k)} \cdot (2^{n-k} - 1) \cdot \ldots \cdot (2^{n-k} - 2^{n-k-1})} = \frac{(2^n - 1) \cdot \ldots \cdot (2^n - 2^{k-1})}{k!}.$$

Let us point out that just the case study of $k = 1, 2$ takes one page in (Folk, Kartashov and Ortbauer 1992).

3.7 Methodological Aspects

Folk, Kartashov and Ortbauer (1992) attempted to distinguish the equivalence classes of Hadamard pattern sets by defining a heuristic set of invariants. Unfortunately, these invariants were not powerful enough to split all classes apart, as was found by our later study, in particular after computing the table of orbit numbers.

We approached the same problem by methods of finite group action. To find the correct group, we experimented with small cases. Then, after proving the correctness of the group action setting, we applied standard methods of group action which gave more powerful and transparent solution methods. This setting seems to be appropriate for solving problems related to symmetries in neural networks.

Since the original problem was rephrased in the paradigm of symmetry classes of mappings, also the *construction* of orbit representatives was an easy task. (We deal with constructional issues in Part III of our thesis.) We regret that this information was not used when the results were transformed back to the level of neural network theory.

Chapter 4

Quasi-polynomials

Much effort was put into answering the question if a given sequence has a generating function within a specific domain or not. In this chapter we prove that certain interesting combinatorial quantities (typically depending on two parameters) possess compact closed forms when one of the parameters becomes fixed. The examples include necklaces, $0,1$-matrices, bipartite graphs, multigraphs and polygon dissections. A subset of the examples can be treated in a uniform way which resides in the generalization of restricted partitions by instruments of finite group action.

In Section 4.1 we recall some concepts from enumerative combinatorics. In particular, we define quasi-polynomials as a natural generalization of polynomials and show the form of their generating functions. Later on, we explain how the *experimental* methods were used by other authors to conjecture generating functions of various sequences. This approach has a twofold effect: *(i)* We can collect together more examples of quasi-polynomials comparing to what the textbooks normally present. *(ii)* We can try proving quasi-polynomiality of other sequences, which is the main objective of this chapter.

It turns out that a certain subset of examples can be treated in a uniform way by generalizing the concept of so-called "restricted partitions" by instruments of finite group action. Section 4.3 is devoted to this topic. However, there still remain sequences that probably cannot be handled this way, and different methods must be taken to prove that they have generating functions of the desired form. An example of such situation is given in Section 4.4.

In Section 4.5 we briefly introduce a computer algebra package for efficient computations in the domain of quasi-polynomials. This tool may be used to convert generating functions for quasi-polynomial sequences into corresponding closed forms. Consequently, it may produce the closed form for any sequence studied in this chapter. Only few samples are included in order to keep the modest size of this section. However, it should be noted that long tables of generating functions and/or quasi-polynomial closed forms could be manufactured in a routine way.

4.1 Definitions

For a polynomial (formal power series) $P(x)$, let $[x^s]P(x)$ be the coefficient of x^s in P.

In this chapter we study a natural generalization of polynomials, namely so-called *quasi-polynomials*. In the sequel, we will be using the word quasi-polynomial both as a noun and as an adjective.

Definition 4.1.1 *Let $(a_n)_{n\geq 0}$ (or simply (a_n)) be an integral sequence, $a_n \in \mathbb{Z}$ for all $n \in \mathbb{N}$. We say that (a_n) is* quasi-polynomial *if and only if there are integers $p \geq 1$, $n_0 \geq 0$ and polynomials $P_0(n), P_1(n), \ldots, P_{p-1}(n) \in \mathbb{Q}[n]$ such that for each $n \geq n_0$*

$$a_n = P_k(n) \qquad \text{where } k = n \bmod p. \tag{4.1}$$

There are two differences of this definition from the usual one, see for example (Stanley, 1986), p. 210: In our setting it suffices that the polynomials P_k determine the sequence's values only from some point onwards. Later the reader may recognize why this comes useful: Consider, for example, the sequences of Section 4.4. The second difference is that we define the quasi-polynomiality only for sequences with integral entries. The reason for this limitation is that in this chapter we deal exclusively with sequences that count combinatorial objects.

Definition 4.1.2 *The number p will be called the* quasi-period *of the sequence. The polynomials $P_0, \ldots, P_{p-1}$ will be called the* class polynomials *of the sequence because they determine its entries on residue classes of the index.*

Let D be the maximum degree amongst polynomials P_k and suppose $P_k = \sum_{l=0}^{D} c_{k,l} n^l$. Instead of equation (4.1) one usually writes

$$a_n = [c_{0,D}, c_{1,D}, \ldots, c_{p-1,D}]n^D + \ldots + [c_{0,0}, c_{1,0}, \ldots, c_{p-1,0}].$$

Further abbreviation is achieved by writing $[c_0, \ldots, c_t]$ instead of $[c_0, \ldots, c_t, c_0, \ldots, c_t, \ \ldots \ , c_0, \ldots, c_t]$ and c instead of $[c, c, \ldots, c]$. We will use such notation in Section 4.5.1.

Let $\lfloor x \rfloor$ denote the floor function. The reader may verify that also each equation of the following form

$$a_n = \lfloor P(n) \rfloor, \qquad P(n) \in \mathbb{Q}[n] \tag{4.2}$$

defines a quasi-polynomial sequence. Unfortunately, the converse does not hold in general.

We start with two warm-up examples: The sequence $(2, 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots)$ of terms in the continued fraction expansion of the well-known number $e = 2 + 1/(1 + 1/(2 + 1/(1 + 1/(1 + 1/(4 + 1/\ldots)))))$ is quasi-polynomial with $p = 3$, $n_0 = 1$ and $P_1 = 1$, $P_2 = 2/3(n+1)$, $P_0 = 1$.

The (sorted) sequence of numbers k such that $\lfloor\sqrt{k}\rfloor$ divides k (AMM problem E 2491) is the sequence of numbers of the form m^2, $m^2 + m$, $m^2 + 2m$ with $m \geq 1$. Indexing these items by $0, 1, \ldots$ we get a quasi-polynomial sequence with $p = 3$, $n_0 = 0$, $P_0 = (n/3 + 1)^2$, $P_1 = ((n+2)/3)^2 + (n+2)/3$ and $P_2 = ((n+1)/3)^2 + 2(n+1)/3$.

For a more general example of a quasi-polynomial quantity we recall the number of *restricted partitions* of a given positive integer n into parts of possible sizes $s_1, \ldots, s_k$. Comtet (1974) calls this number the *denumerant* $N(n; s_1, \ldots, s_k)$. (See also Definition 5.1.1.) The denumerant is quasi-polynomial in n. It is common to use the notation $p_k(n)$ as an abbreviation for $N(n; 1, 2, \ldots, k)$ and we will do so in Section 4.5. We will learn more about denumerants in Chapter 5 of our thesis.

For an introduction on quasi-polynomials we recommend (Ehrhart, 1977) or (Stanley, 1986).

4.1.1 Generating Functions

Lemma 4.1.3 *The integral sequence (a_n) is quasi-polynomial (in the sense of the preceding section) if and only if the following two conditions hold.*

(QP1) *The generating function for (a_n) is rational, $\sum_{n\geq 0} a_n x^n = P(x)/Q(x)$ with $P(x), Q(x) \in \mathbb{Z}[x]$, $\gcd(P(x), Q(x)) = 1$.*

(QP2) *All roots of the polynomial $Q(x)$ are roots of unity (not necessarily with same primitive periods). This can be rephrased by saying that all irreducible factors of $Q(x)$ are* cyclotomic polynomials, *see (Lang, 1984), p. 316.*

Proof. The proof of this statement relies on Proposition 4.4.1 in (Stanley, 1986) which in our setting reads as follows: "The integral sequence (a_n) is quasi-polynomial with $n_0 = 0$ if and only if (QP1) and (QP2) hold and, moreover, $\deg P < \deg Q$." In the general case (no restriction on degrees of P and Q) we can always find polynomials $R, S \in \mathbb{Z}[x]$ such that $P/Q = R + S/Q$ with $\deg S < \deg Q$. Let $r := \deg R$ and $S/Q = \sum_{n \geq 0} a'_n x^n$. Then $a_n = [x^n]R(x) + a'_n$ for $n \leq r$ while $a_n = a'_n$ for $n \geq r+1$. Hence, (a_n) is quasi-polynomial (in our sense) with $n_0 = r + 1$. $\square$

Definition 4.1.4 *We will say that a generating function has* (QP)-form *if it fulfills both conditions (QP1) and (QP2).*

Quasi-polynomials are closed under addition, convolution and indefinite summation. They are also closed under multiplication, as may be seen by a direct argument (without consideration of generating functions).

4.1.2 Closed Forms

Mathematicians like to see things in "closed forms". For example, the following three equations (equation systems) define the same sequence $(a_n)_{n \geq 0}$, cf. Exercise 5.15 in (Graham, Knuth and Patashnik, 1989):

$$\begin{aligned} a_n &= (-1)^m (3m)!/m!^3 \qquad \text{for } n \text{ even}, \ n = 2m \\ a_n &= 0 \qquad \text{for } n \text{ odd} \end{aligned} \tag{4.3}$$

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^3 (-1)^k \tag{4.4}$$

$$(n+2)^2 a_{n+2} + 3(3n+4)(3n+2)a_n = 0, \qquad a_0 = 1, \ a_1 = 0. \tag{4.5}$$

For many reasons (computation complexity, getting more mathematical insight, asymptotic analysis, or even aesthetic reasons etc.) we prefer the definition (4.3) to the other two cases. (Cf. also the discussion in Section 1.1.) No fixed definition exists that would specify which operations are allowed to appear in a "closed form expression". Typically, closed forms may include addition, multiplication, exponentiation and factorials. In the present chapter we adopt quasi-polynomials as "closed forms", since they very well meet all demands listed at the beginning of this paragraph.

4.2 On the Search for Quasi-polynomials

Recently, Bergeron and Plouffe (1992) as well as Salvy and Zimmermann (1993) developed Maple programs that, among other things, can guess the generating function for a sequence from its initial terms. Using these programs, Plouffe (1992) computed an amazingly large catalog of more than one thousand conjectured generating functions or recurrence relations. His work will be incorporated into the second edition of (Sloane, 1973).

(*Remark.* Meanwhile, this second edition of Sloane's famous Handbook (1973), now called The Encyclopedia, is available electronically by sending an e-mail request to

`superseeker@research.att.com`.

Such request is handled not only by a table look-up in the Encyclopedia but also by activating the aforementioned Maple programs for guessing the explanation of the sequence.)

Interestingly enough, more than 60 guess entries of (Plouffe, 1992) have (QP)-form. (Recall Definition 4.1.4.) Based on the references provided with each such entry, one can track down the circumstances under which the respective sequence appears in the literature, and find out if its suspected quasi-polynomiality has been recognized by the author(s) introducing this sequence. Depending on whether the answer to the last question is positive or negative, one can

(i) add the sequence to a data base of quasi-polynomials, and hence collect more examples of quasi-polynomials than is usually listed in the textbooks, i.e., *organize the knowledge*,

(ii) try to *rigorously prove* that the respective sequence indeed is quasi-polynomial, i.e., *extend the knowledge*.

It is a pleasure for us to note that in the course of our work with Plouffe's list (1992) we did not meet any wrong guess, i.e., each sequence that we picked for a detailed study turned out to be an instance for task *(i)* or *(ii)*. Moreover, a great majority of items falling in class *(ii)* was generalized by showing not only the quasi-polynomiality of the particular sequence appearing in (Plouffe, 1992), which typically is a specialization of some general quantity for a small concrete value of some parameter, but also the quasi-polynomiality of the respective sequence in general, i.e., for *any* value(s) of the parameter(s).

Since task *(i)* is better suited for a textbook, we concentrate on task *(ii)*. This is done in Sections 4.3 and 4.4.

4.3 G-partitions of Numbers

As mentioned at the beginning of this chapter, some instances of quasi-polynomials can be gathered together by viewing them as restricted partitions under an action of a permutation group.

Let $\underline{n} := \{1, 2, \ldots, n\}$ and let G be a subgroup of $S_{\underline{n}}$ acting naturally on $\underline{n}$. Then $\bar{G}$, the permutation representation of G, is identical with G itself and we will not distinguish between them in this chapter. After putting $Y = \mathbb{N}$ in the "symmetry classes of mappings" paradigm (Chapter 2) we arrive at the action

$$G \times \mathbb{N}^{\underline{n}} \to \mathbb{N}^{\underline{n}} \tag{4.6}$$

defined by $(\pi f)(x) := f(\pi^{-1}(x))$ for $\pi \in G$, $f \in \mathbb{N}^{\underline{n}}$.

Definition 4.3.1 *Let n be a positive integer and let $G \leq S_{\underline{n}}$. For an $f \in \mathbb{N}^{\underline{n}}$, let*

$$c_f := \sum_{x \in \underline{n}} f(x)$$

and let

$$G(f) := \{\pi f \mid \pi \in G\}$$

be the orbit of f w.r.t. G's action on $\mathbb{N}^{\underline{n}}$. We say that $G(f)$ is a G-partition *of the number c_f.*

This definition is sound, since the value $\sum_{i=1}^{n} f(i)$ is obviously invariant on G's orbits.

Informally, given a natural number c and a permutation group $G \leq S_{\underline{n}}$, then a G-partition of the number c is a set T of n-tuples over $\mathbb{N}$ where each tuple sums up to c, and for any two n-tuples $t_1, t_2 \in T$ there is a permutation $\pi \in G$ such that $t_2 = \pi t_1$. Since the length of tuples must be equal to n, we speak about restricted partitions. We note that zero parts are allowed as well, a fact that fits the combinatorial applications and ensures that the set of G-partitions of c is always non-empty.

Definition 4.3.2 *Let n be a positive integer and let $G \leq S_{\underline{n}}$. For any $c \in \mathbb{N}$, the number of G-partitions of c will be denoted by $P_G(c)$.*

Lemma 4.3.3 *Let n be a positive integer and let $G \leq S_{\underline{n}}$. For any $c \in \mathbb{N}$, the value $P_G(c)$ is equal to the coefficient of t^c in*

$$C(G, \underline{n} | \frac{1}{1-t}). \tag{4.7}$$

In words, $P_G(c)$ is equal to the coefficient of t^c in the formal power series that results from Pólya-substitution of the series

$$\frac{1}{1-t} = 1 + t + t^2 + \dots$$

in the cycle index of G's action on $\underline{n}$.

Proof. By introducing the weight mapping $W : \mathbb{N} \to \mathbb{Z}[t]$, $W(i) = t^i$ and considering the multiplicative weight of functions as defined in (2.2) we see that $P_G(c)$ is equal to the number of orbits of weight t^c in (4.6).

In order to use group action methods for enumeration of these orbits we use a little trick. The theory of Chapter 2 applies only to finite actions, which is not the case in (4.6). However, orbits of weight t^c in (4.6) are identical with orbits of weight t^c in

$$G \times \{0, 1, \dots, c\}^{\underline{n}} \to \{0, 1, \dots, c\}^{\underline{n}}$$

and we can use Theorem 2.1.24 for the latter action. We get that $P_G(c)$ is equal to the coefficient of t^c in

$$C(G, \underline{n} | \sum_{i=0}^{c} t^i). \tag{4.8}$$

where $C(G, \underline{n})$ is the cycle index of G's action on $\underline{n}$ and expression (4.8) means Pólya-substitution. Furthermore, the coefficient of t^c in (4.8) is clearly equal to the coefficient of t^c in

$$C(G, \underline{n} | \sum_{i=0}^{\infty} t^i)$$

because introducing powers with exponents greater than c is of no consequence. The last expression is equal to (4.7). $\square$

As an immediate application of Lemma 4.3.3 we note a quick proof of the following identity.

Theorem 4.3.4 *For each positive integer n we have*

$$\sum_{a \vdash n} \prod_{k} \frac{1}{a_k!} \left(\frac{1}{k(1-x^k)} \right)^{a_k} = \prod_{k=1}^{n} \frac{1}{1-x^k} \tag{4.9}$$

where the sum extends over all $a = (a_1, a_2, \ldots)$ such that $a_1 \cdot 1 + a_2 \cdot 2 + \ldots = n$ and $a_i \in \mathbb{N}$ for $1 \leq i \leq n$.

Proof. The left-hand side of (4.9) is exactly $C(S_{\underline{n}}, \underline{n}|1/(1-x))$. (For the cycle index of $S_{\underline{n}}$'s natural action, see (Kerber, 1991), p. 72.) The right-hand side is the well-known generating function for the number of (unordered) partitions in parts of size $1, 2, \ldots, n$, which in our terminology are the $S_{\underline{n}}$-partitions. The identity now follows from Lemma 4.3.3. □

The identity (4.9) appears in MacMahon (1984), Vol. II, p. 62. It is normally used as the first step in a partial fraction decomposition of its right-hand side. This identity is typically derived using symmetric functions, even in the textbooks that introduce Pólya's counting theory, see for example (Riordan, 1958), pp. 118–119.

The following theorem will be later used to prove quasi-polynomiality of diverse combinatorial quantities.

Theorem 4.3.5 *Let n be a positive integer. For each permutation group $G \leq S_{\underline{n}}$, the number $P_G(c)$ of G-partitions of c is quasi-polynomial in c.*

Proof. The generating function for the sequence $(P_G(c))_{c \geq 0}$ is (4.7). Since $C(G, \underline{n})$ is a polynomial in all its indeterminates, the Pólya-substitution of $\frac{1}{1-t}$ in $C(G, \underline{n})$ clearly yields a generation function in (QP)-form. □

By taking suitable subgroups of $S_{\underline{n}}$, we can prove quasi-polynomiality of various combinatorial quantities. All of the following examples were treated elsewhere but only occasionally the quasi-polynomial closed forms for some special cases were recognized. We aim at a unifying treatment of all situations.

4.3.1 Necklaces and Bracelets

Taking $G = C_{\underline{n}}$ to be the cyclic group acting naturally on $\underline{n}$, the $C_{\underline{n}}$-partitions of a number m are models for *two-colored necklaces* (black and white, say) with the fixed number n of black beads and a varying number m of white beads. The bijection between these two sets is as follows: For a given $C_{\underline{n}}$-partition of the number m with a representative $(m_1, m_2, \ldots, m_n)$ we construct a necklace with n black beads and n blocks of white beads (of sizes $m_1, m_2, \ldots, m_n$, respectively) by inserting one white block between each consecutive pair of black beads, keeping the cyclic order of the m_i's unchanged. Thus the black beads provide the "marks" between consecutive parts in the $C_{\underline{n}}$-partition.

Similarly, if $G = D_{\underline{n}}$ is the dihedral group acting naturally on $\underline{n}$ then the $D_{\underline{n}}$-partitions of a number m are models for *two-colored bracelets* with the fixed number n of black beads and a varying number m of white beads. (Chapter 9 is entirely devoted to necklaces and bracelets.)

From Theorem 4.3.5 we obtain:

Proposition 4.3.6 *Let $N_n(m)$ denote the number of necklaces with n black and m white beads. and let $B_n(m)$ denote the number of bracelets with n black and m white beads. For each fixed $n \in \mathbb{N}$, the functions $N_n(m)$ and $B_n(m)$ are quasi-polynomial in m.*

The values involved in Proposition 4.3.6 are of interest in diverse applications, see (Hoskins, Penfold Street, 1982) or (Ethier, Hodge, 1985).

For quasi-polynomials enumerating $C_{\underline{n}}$- and $D_{\underline{n}}$-partitions, the class polynomials can be expressed explicitly by binomial sums, providing this way an *alternative* proof of the quasi-polynomiality of the quantities under examination. This approach is less elegant (comparing to the argument using generating functions). Pólya's Theorem is now applied for the cyclic and dihedral group of degree $m + n$, respectively.

Next we show these computations for the case of $C_{\underline{n}}$-partitions. The number of necklaces with n black and m white beads is the coefficient of x^m in

$$\frac{1}{m+n} \sum_{d|(m+n)} \phi(d)(x^d + 1)^{(m+n)/d}$$

which by the binomial theorem turns out to be

$$\frac{1}{m+n}\sum_{d\,|\,\gcd(m,n)}\phi(d)\binom{(m+n)/d}{n/d}. \tag{4.10}$$

The basic property of greatest common divisor

$$\gcd(m,n)=\gcd(m \bmod n, n)$$

allows us to change the description of summation range in a convenient way: It is now clear that the summation range depends just on the value of $m \bmod n$, i.e., on the residue class of m, and that (4.10) is polynomial in m on each such residue class. This means that $N_n(m)$ is quasi-polynomial with quasi-period n.

4.3.2 $0,1$-matrices and Bipartite Graphs

Many problems in switching theory can be recast as problems involving $0,1$-matrices. Harrison (1973) develops methods for finding number of equivalence classes of $0,1$-matrices with m rows and n columns under two definitions of equivalence:

(E1) equivalent matrices are obtained by row and column permutations;

(E2) equivalent matrices are obtained by row permutations together with column permutations and/or complementations.

For the equivalence (E1), the number $s_{m,n}$ of classes of $m \times n$ matrices may be determined as follows: Consider the action (cf. Definition 2.1.14)

$$S_{\underline{n}} \times \{0,1\}^{\underline{n}} \to \{0,1\}^{\underline{n}}. \tag{4.11}$$

If we introduce some bijection $\{0,1\}^{\underline{n}} \to \underline{2^n}$ then (4.11) induces $S'_n \leq S_{\underline{2^n}}$, a permutation representation of $S_{\underline{n}}$ in $S_{\underline{2^n}}$. Then each (E1)-equivalence class of $m \times n$ binary matrices is in an obvious correspondence with one S'_n-partition of the number m. The formula for the cycle index of S'_n appears in (Harrison, 1965). For example, $C(S_{\underline{2}},\{0,1\}^{\underline{2}}) = C(S'_2,\underline{2^2}) =$

$1/2(s_1^4 + s_1^2 s_2)$ and so the generating function for (E1)-classes of $m \times 2$ matrices is

$$\begin{aligned} \sum_{m \geq 0} s_{m,2} x^m &= \frac{1}{2}\left((\frac{1}{1-x})^4 + (\frac{1}{1-x})^2 \frac{1}{1-x^2} \right) \qquad (4.12) \\ &= \frac{1}{(1-x)^3(1-x^2)} = 1 + 3x + 7x^2 + 13x^3 + \ldots \end{aligned}$$

In order to find $t_{m,n}$, the number of classes under (E2), Harrison (1973) proceeds in a similar way, arriving at the group S_n'' which is the exponentiation group ${S_{\{0,1\}}}^{S_{\underline{n}}}$.

Putting $G = S_n'$ and $G = S_n''$ in Theorem 4.3.5 we obtain:

Proposition 4.3.7 *Let $s_{m,n}$ and $t_{m,n}$ be number of classes of $m \times n$ 0,1-matrices under the equivalence (E1) and (E2), respectively. For fixed n, the sequences $s_{m,n}$ and $t_{m,n}$ are quasi-polynomial in m.*

It is worth mentioning that for $m \neq n$, $s_{m,n}$ gives also the number of bipartite graphs with vertex set partition (m, n). The bijection is achieved by viewing $0,1$-matrices of the shape $m \times n$ as a special kind of incidence matrices for bipartite graphs with m and n vertices. Thus (4.12) tells us that we have thirteen non-isomorphic bipartite graphs with the vertex partition (3,2). They are drawn in (Harary, Palmer, 1973), p. 95 as an illustration for their enumeration via the cycle index of $S_{\underline{m}} \times S_{\underline{n}}$. The case $m = n$ needs a different treatment, see (Harary, Palmer, 1973), pp. 97–99.

4.3.3 Multigraphs

Consider the symmetric group $S_{\underline{n}}$ acting on pairs from $\underline{n}$. Viewing these pairs as unordered (ordered) and introducing a numbering of them, we obtain two permutation representations of $S_{\underline{n}}$ in $S_{\underline{\binom{n}{2}}}$ and $S_{\underline{n(n-1)}}$, respectively. (Let us call the first one $S_n^{(2)}$.) Taking these two representations for group G in Theorem 4.3.5 we obtain:

Proposition 4.3.8 *For fixed n, the number of (unoriented, oriented) multigraphs on n points with e edges is quasi-polynomial in e.*

The Pólya-substitution of $\frac{1}{1-x}$ into the cycle index of $S_n^{(2)}$ is (without any further comments) mentioned in (Harary, Palmer, 1973), p. 88.

4.4 Polygon Dissections

There are some examples of quasi-polynomials that we could not adjust into the framework of G-partitions. Instead, we had to use other methods in our proofs. One prominent example is presented in this section.

By a *polygon dissection* we mean each subdivision of the interior of a convex s-gon into smaller polygons by means of non-intersecting diagonals. The enumeration of dissections was treated by many authors. In the special case when all parts happen to be triangles, the number of *triangulations* of the s-gon is well-known to be the Catalan number C_{s-2}, see Exercise 7.22 in (Graham, Knuth and Patashnik, 1989). Up to now, no symmetries have been considered so that, for example, the two possible triangulations of the square are regarded as distinct.

Restricting the attention to regular s-gons, one can make the problem more natural by viewing two dissections as identical if one can be obtained from the other by rotating and/or reflecting the s-gon. Depending on whether the reflection is or is not allowed as a possible symmetry, we come to two different problems, and the counted objects will be called "dissections with reflection" and "dissections without reflection", respectively.

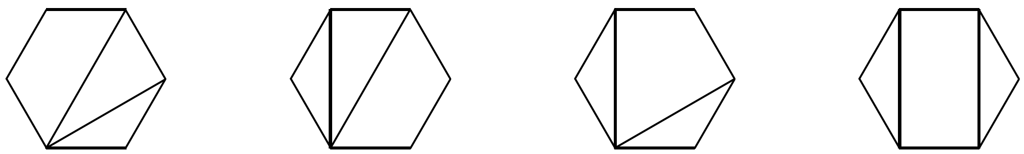
In the general setting when the regular s-gon is to be divided into r polygons, the symmetry classes of dissections were enumerated by Read (1978*b*). We will extend the results of this article by showing that for fixed r, all arising quantities happen to be quasi-polynomials in the variable s.

First of all, we introduce Read's notation and illustrate it on a simple example. Since the general idea of (Read, 1978*b*) is to turn the dissection problem into a cell-growth problem, we will use the term *cells* for the polygons arising in the dissection. With each pair (r, s) we associate five numbers counting different kinds of dividing up the regular s-gon into r polygons:

$V_{r,s}$	number of dissections without reflection rooted at an edge
$F_{r,s}$	number of dissections without reflection rooted at a cell
$H_{r,s}$	number of unrooted dissections without reflection
$f_{r,s}$	number of dissections with reflection rooted at a cell
$h_{r,s}$	number of unrooted dissections with reflection

Obviously, these values are non-zero exactly if $s \geq r+2$. Additionally, we set $V_{0,1} := 1$.

To enlighten the definition of these sequences, let us have a look at their values for $(r,s) = (3,6)$. The following picture will help us:



A B C D

Since each dissection of the hexagon into 3 parts is rotationally equivalent to one of A, B, C, D, we have $H_{3,6} = 4$. Under reflection, A and B fall into one class, hence $h_{3,6} = 3$. If the reflection is not allowed, we may root each of A, B and C at 3 cells and D at 2 cells, which together gives $F_{3,6} = 11$. Allowing the reflection, we must give up one rooting of C and all rootings of B, hence $f_{3,6} = 7$. Finally, under rotational symmetry we may root A, B, C at any outer edge and D at half of its outer edges which implies $V_{3,6} = 21$.

Since we deal with double-indexed sequences, their generating functions are bivariate:

$$V(x,y) := \sum_r \sum_s V_{r,s} x^r y^s.$$

Similarly we define $F(x,y)$, $H(x,y)$, $f(x,y)$ and $h(x,y)$. We recall the formulas derived by Read, for detailed proofs see (Read, 1978*b*):

$$V_{r,s} = \frac{1}{r}\binom{s-2}{r-1}\binom{r+s-1}{s} \qquad (r \geq 1) \tag{4.13}$$

$$F(x,y) = x \sum_{k \geq 3} C(C_{\underline{k}}, \underline{k} | V(x,y)) \tag{4.14}$$

$$H(x,y) = F(x,y) - \frac{1}{2}\left(U^2(x,y) - U(x^2,y^2)\right) \tag{4.15}$$

$$f(x,y) = \frac{1}{2}F(x,y) + \frac{1}{4}\left(2T(x,y) + V(x^2,y^2) + T^2(x,y)\right) R(x,y) \tag{4.16}$$

$$h(x,y) = f(x,y) - \frac{1}{4}\left(U^2(x,y) - 2U(x^2,y^2) + W^2(x,y)\right) \tag{4.17}$$

where $U(x,y) = V(x,y) - y$, $xR(x,y) = (1+x^2)V(x^2,y^2) - y^2$ and $W(x,y) = T(x,y) - y$ with

$$T(x,y) = \frac{y + R(x,y)}{1 - R(x,y)}. \tag{4.18}$$

In the equation (4.14), the expression $C(C_{\underline{k}}, \underline{k}|V(x,y))$ denotes the Pólya-substitution of the formal power series $V(x,y)$ in

$$C(C_{\underline{k}}, \underline{k}) = \frac{1}{k} \sum_{d|k} \phi(d) z_d^{k/d}.$$

Here $C(C_{\underline{k}}, \underline{k})$ denotes the cycle index of the cyclic group $C_{\underline{k}}$ in its natural action on $\underline{k}$ and ϕ is the Euler function. See (Kerber, 1991), pp. 70–72 for details.

We will now show that, for each fixed r, the five enumerating sequences $(V_{r,s})$, $(F_{r,s})$, $(H_{r,s})$, $(f_{r,s})$ and $(h_{r,s})$ (all viewed as single-indexed) are quasi-polynomial in s. To this end, for each r we introduce five univariate generating functions V_r, F_r, H_r, f_r and h_r in the variable y:

$$V(x,y) =: \sum_r V_r(y) \cdot x^r$$

and analogously for the other four functions. Clearly, our goal is to show that for any r, each of these five univariate functions meets the conditions (QP1), (QP2), see Section 4.1.1.

This statement is trivial for the functions V_r because for $r \geq 1$, $V_{r,s}$ is polynomial in s of degree $2r-2$, hence

$$V_r(y) = \frac{P_r(y)}{(1-y)^{2r-1}} \qquad (r \geq 1) \tag{4.19}$$

for some polynomial P_r. For $r = 0$ we have

$$V_0(y) = y. \tag{4.20}$$

This simple form of V_0 will consequently play a notable role in our computations.

The series F_r is obtained by a rearrangement of (4.14):

$$\begin{aligned} F_r(y) &= [x^r]\, F(x,y) = [x^{r-1}] \sum_{k\geq 3}\sum_{d|k} \frac{\phi(d)}{k} V^{k/d}(x^d, y^d) \\ &= [x^{r-1}] \sum_{d'|(r-1)} \sum_{md'\geq 3} \frac{\phi(d')}{md'} V^m(x^{d'}, y^{d'}). \end{aligned}$$

By multinomial theorem and another rearrangement we find

$$\begin{aligned} F_r(y) &= \sum_{d'|(r-1)} \sum_{(a_1,a_2,\ldots)\vdash \frac{r-1}{d'}} \sum_{m=\left\lceil \frac{\max(3,\sum a_i)}{d'} \right\rceil}^{\infty} \\ &\quad \frac{\phi(d')}{md'} \frac{m!}{a_1!a_2!\ldots(m-\sum a_i)!} V_0^{m-\sum a_i}(y^{d'}) \cdot V_1^{a_1}(y^{d'}) \cdot V_2^{a_2}(y^{d'}) \cdot \ldots \end{aligned}$$

where the second sums extends over all sequences $(a_1, a_2, \ldots)$ such that $a_1 \cdot 1 + a_2 \cdot 2 + \ldots = (r-1)/d'$, $\lceil x \rceil$ is the ceiling of x and $\sum a_i = a_1 + a_2 + \ldots$. The multinomial coefficient multiplied by $\phi(d')/md'$ is a polynomial in m of degree $(\sum a_i) - 1$, let us call it $A(m)$. Due to (4.20), the innermost sum in the last equation is

$$\sum_{m=m_0}^{\infty} A(m) \cdot y^{d'm-(d'\sum a_i)} \cdot V_1^{a_1}(y^{d'}) \cdot V_2^{a_2}(y^{d'}) \cdot \ldots$$

where the summation bound was replaced by a symbol. The factors independent of m may be put apart, which gives

$$C(y) \cdot \sum_{m=m_0}^{\infty} A(m) \cdot y^{d'm} \tag{4.21}$$

with $C(y)$ in (QP)-form because of (4.19). Hence, the expression (4.21) meets (QP)-form and finally the generating function F_r, being a finite sum of expressions of the type (4.21), must also fit (QP)-form. Hence, we have proved that for any fixed r, the sequence $F_{r,s}$ is quasi-polynomial in s. Taking $r = 3$ as an easy example, we compute

$$F_3(y) = \sum_{m\geq 3} y^{m-1} V_2(y) + \sum_{m\geq 3} \frac{m-1}{2} y^{m-2} V_1^2(y) + \sum_{m\geq 2} \frac{1}{2} (y^2)^{m-1} V_1(y^2)$$

$$\begin{aligned} &= V_2(y) \cdot \frac{y^2}{1-y} + V_1^2(y) \cdot \frac{y(2-y)}{2(y-1)^2} + V_1(y^2) \cdot \frac{y^2}{2(1-y^2)} \\ &= -\frac{(y^3+y^2-5y-3)y^5}{(1-y^2)^2(1-y)^2} = 3y^5 + 11y^6 + 24y^7 + 46y^8 + 75y^9 + \ldots, \end{aligned}$$

cf. Table 2 in (Read, 1978*b*).

The functions H_r give little trouble since from (4.15) we directly obtain

$$H_r(y) = F_r(y) - \frac{1}{2}\left(\sum_{i=1}^{r-1} V_i(y) \cdot V_{r-i}(y) - \left\{V_{r/2}(y^2)\right\}\right)$$

where the term in curly brackets is (or is not) present depending on if r is even (odd). In both cases, the yet known forms of F_r and V_i imply that H_r meets (QP)-form for any r.

Next we must deal with the functions $f_r(y)$. We will show that also the functions $R_r(y)$ and $T_r(y)$ happen to be in (QP)-form which obviously will settle the problem for f_r, see (4.16).

We observe that $R_r(y) = 0$ for r even and

$$R_r(y) = V_{(r+1)/2}(y^2) + V_{(r-1)/2}(y^2)$$

for r odd which again meets (QP)-form. The treatment of T_r needs a bit of rewriting of (4.18):

$$T_r(y) = y \cdot R'_r(y) + \sum_{k=0}^{r} R_k(y) \cdot R'_{r-k}(y)$$

where

$$\begin{aligned} R'_l(y) &:= [x^l] \sum_{i=0}^{\infty} R^i(x,y) \;=^{(*)}\; [x^l] \sum_{i=0}^{l} R^i(x,y) \\ &= \sum_{(a_1,a_2,\ldots)\vdash l} \frac{(a_1+a_2+\ldots)!}{a_1!a_2!\ldots} \cdot R_1^{a_1}(y) \cdot R_2^{a_2}(y) \ldots . \end{aligned}$$

The step $^{(*)}$ is possible due to $R_0(y) = 0$. We conclude that each R'_l is in (QP)-form. Thus, also T_r fulfills (QP)-form. Now f_r can be expressed as a finite sum of products involving constants, F_r, V_i's, T_i's and R_i's. Hence, f_r meets (QP)-form.

The last remaining series is h_r. Again, h_r can be written a finite sum of products involving constants, f_r, V_i's and T_i's. Hence, also h_r meets (QP)-form.

Theorem 4.4.1 *For any fixed $r \geq 1$, the enumerating sequence $(V_{r,s})$ is polynomial in s and the four enumerating sequences $(F_{r,s})$, $(H_{r,s})$, $(f_{r,s})$ and $(h_{r,s})$ are quasi-polynomial in s.*

Proof. The statement about $(V_{r,s})$ follows clearly from Read's formula (4.13). Concerning the other four sequences, we have recently shown that their generating functions, i.e., the functions F_r, H_r, f_r and h_r, have (QP)-form. □

Finally, we would like to remark that the change from bivariate to univariate generating functions not only proves the existence of certain closed forms for the studied sequences but also provides a practical method for computing these closed forms and hence the terms of the respective sequences. To our opinion, this computational method is more straightforward than the somewhat cumbersome evaluations of coefficients of bivariate power series as suggested in (Read, 1978*b*). Using computer algebra systems it is very easy to compute explicitly the generating functions F_r, H_r, f_r and h_r for modest values of r along the preceding lines.

While doing so, we had the pleasure to verify the huge amount of data contained in (Read, 1978*b*), Tables 2 to 5 with the exception of the three positions $f_{3,16}$, $f_{6,16}$ and $h_{8,15}$ that according to our results should hold the values 372, 624355 and 384035, respectively. (*Remark.* The quasi-polynomial closed form for the sequence $(f_{3,s})$, deduced from the generating function f_3, is shown in Section 4.5.1.) For each of these three entries, the value given in (Read, 1978*b*) and our value disagree only at a single decimal position so the difference clearly should be accounted to a transcription mistake rather than to a mathematical error.

4.5 Computational Considerations

We shortly introduce the Maple package `QP` which we developed for easy computations with quasi-polynomials.

This package, as each computer algebra product, is *not supposed to replace the knowledge* (of working with generating functions, in this case). Rather, it should support tedious computations by saving time and human energy. For an interesting discussion on usage of such systems, see (Buchberger, 1991).

We give an idea about the package by a very brief survey of its functions:

`gf2qp` takes a rational generating function and decides whether the underlying sequence is quasi-polynomial. If this is the case, the quasi-polynomial coefficients are computed.

`eval_qp` evaluates the given quasi-polynomial at a given integer.

`denumerant` computes the denumerant from given part sizes.

`p` computes $p_k(n)$.

A special message is printed if the result may be represented in terms of the floor function.

To give some feeling about the performance, we include three examples with their reference and CPU time needed to compute the quasi-polynomial closed form (i.e., the class polynomials) by our package on a DEC-5200 running Maple V Release 2.

problem	reference	CPU time
$p_3(n)$	S, p. 211	1.0 sec
$p_6(n)$	S, p. 211	3.5 sec
$N(n; 1, 5, 10, 25, 50)$	GKP, p. 331	37.9 sec

Abbreviations:

S (Stanley, 1986)

GKP (Graham, Knuth and Patashnik, 1989)

4.5.1 Examples of Closed Forms

Finally, we tabulate a couple of quasi-polynomial closed forms for some of the sequences treated in this chapter. In front of each sequence we include the number of the section where it was introduced. The bracket and ceiling notations for quasi-polynomials were explained in Section 4.1.

4.3.1	$B_4(m)$	$=$	$\frac{1}{48}m^3 - \frac{1}{16}m^2 + [\frac{1}{6}, -\frac{1}{48}, \frac{1}{6}, -\frac{1}{48}]m + [0, \frac{1}{16}, -\frac{1}{4}, \frac{1}{16}]$
4.3.2	$s_{m,2}$	$=$	$\lfloor \frac{1}{24}(m+2)(m+4)(2m+3) \rfloor$
4.4	$f_{3,s}$	$=$	$\frac{1}{8}s^3 - \frac{1}{2}s^2 + [-1, -\frac{9}{8}]s + [4, \frac{9}{2}] \quad (s \geq 5)$

4.6 Methodological Aspects

The combinatorial theory given in this chapter bases on (yet unexploited) empiric results of other authors. The essential methodological issues of the approach taken in this chapter were discussed in Section 4.2. The usefulness of this approach is documented by theorems proved in Sections 4.3 and 4.4.

Chapter 5

Denumerants

In Chapter 4 of our thesis we dealt with various quasi-polynomial quantities that appear in combinatorial enumeration. Many of our examples were in some way related to number partitions.

In the present chapter we restrict our attention to partitions with prescribed part sizes. More specifically, let a, b, c be fixed, pairwise relatively prime integers. We investigate the number of non-negative integral solutions of the equation $ax + by + cz = n$ as a function of n.

We present a new algorithm that computes the "closed form" of this function. This algorithm is simple and its time performance is better than the performance of yet known algorithms. We also recall how to approximate the aforementioned function by a polynomial and we derive bounds on the "error" of this approximation for the case $a = 1$.

5.1 Definitions

We recall that $\lfloor x \rfloor$ means the *integer part* of x. Let $\{x\} := x - \lfloor x \rfloor$ denote the *fractional part* of x.

Definition 5.1.1 *Let m be a positive integer and let $(a_1, \ldots, a_m)$ be an m-tuple of positive integers. Let n be a non-negative integer. Each m-tuple of non-negative integers $(x_1, \ldots, x_m)$ such that*

$$\sum_{i=1}^{m} a_i x_i = n$$

is called a partition of the number n into parts of size $a_1, \ldots, a_m$. *For a given n, let $N(n; a_1, \ldots, a_m)$ denote the number of all such partitions.*

The number $N(n; a_1, \ldots, a_m)$ will be called the denumerant *of n with respect to the sequence $(a_i)_{1 \le i \le m}$.*

The term "denumerant" appears in (Comtet, 1974), p. 108. The generating function for the denumerant is well-known to be

$$\sum_{n=0}^{\infty} N(n; a_1, \ldots, a_m) t^n = \prod_{i=1}^{m} \frac{1}{1 - t^{a_i}}. \tag{5.1}$$

We deal with the problem of determining N as a function of n for certain sequences (a_i). This issue is also known as the *money changing* *problem* (when we consider n as an amount to be changed in coins or bills of size a_i).

In this chapter we extend several results of Popoviciu (1953) who studied the case $m = 3$ in a great detail. His work is quoted in most textbooks on combinatorial enumeration, such as (Comtet, 1974) or (Stanley, 1986). While Popoviciu's paper is more static (aiming at isolating denumerants with a certain property), we advance its results for dynamic purposes, namely for computing arbitrary denumerants with $m = 3$ and a_1, a_2, a_3 pairwise relatively prime.

5.2 Facts about Denumerants

We begin our investigations with recalling several known facts.

Fact 5.2.1 *Let k be a non-negative integer. With the notation as above, we have*

$$N(n + ka_m; a_1, \dots, a_m) - N(n; a_1, \dots, a_m) = \sum_{i=1}^{k} N(n + ia_m; a_1, \dots, a_{m-1}). \tag{5.2}$$

Proof. Consider the the following equation with unknowns $x_1, \dots, x_m$

$$a_1 x_1 + \ldots + a_m x_m = n + ka_m.$$

The solutions of this equation are of two types: *(i)* those with $x_m \geq k$, *(ii)* those with $x_m < k$. Each solution $(x_1, \dots, x_{m-1}, x_m)$ of the type *(i)* is in a one-to-one correspondence with the non-negative solution

$$(y_1, \dots, y_m) = (x_1, \dots, x_{m-1}, x_m - k)$$

of the equation

$$a_1 y_1 + \ldots + a_m y_m = n.$$

Each solution of the type *(ii)* is in a one-to-one correspondence with the non-negative solution

$$(y_1, \dots, y_{m-1}) = (x_1, \dots, x_{m-1})$$

of the equation

$$a_1 y_1 + \ldots + a_{m-1} y_{m-1} = n + (k - x_m) a_m.$$

The formula (5.2) now follows by summation. □

In the present paper we study the denumerants in the case *when the part sizes a_i are pairwise relatively prime.* From the theory of rational generating functions it follows that $N_m(n) := N(n; a_1, \ldots, a_m)$ is then expressible in the nice form

$$N_m(n) = R_m(n) + G_m(n)$$

where R_m is a polynomial of degree $m-1$ in n whose coefficients are symmetric functions in the parameters a_i and G_m is a periodic sequence with the period $\prod_{i=1}^{m} a_i$. The coefficients of R_m for $m \le 4$ can be found in (Comtet, 1974), p. 113.

In the case $m = 1$ we have $R_1(n) = 1/a_1$ and $G_1(n) = -1/a_1 + 1$ or $-1/a_1$ according as a_1 divides or does not divide n.

Definition 5.2.2 *For relatively prime numbers p, q, let the symbol*

$$\left(\frac{n}{q} \mid p \right)$$

denote the unique integer $x \in \{0, \ldots, p-1\}$ such that

$$qx \equiv n \pmod{p}.$$

Fact 5.2.3 *In the case $m = 2$ we have*

$$R_2(n) = \frac{n}{a_1 a_2}, \qquad G_2(n) = -\frac{1}{a_1}\left(\frac{n}{a_2} \mid a_1 \right) - \frac{1}{a_2}\left(\frac{n}{a_1} \mid a_2 \right) + 1. \tag{5.3}$$

Proof. (Popoviciu, 1953), pp. 24–25. □

The interesting cases are $m \ge 3$ where it becomes less trivial to determine the periodic part $G_m(n)$. The rest of this chapter deals with the instance $m = 3$. For the sake of brevity, we will use the letters a, b, c instead of a_1, a_2, a_3. The polynomial part of the denumerant can be extracted from the formulas in (Comtet, 1974), p. 113:

Fact 5.2.4 *Let a, b and c be pairwise relatively prime positive integers and let $N_3(n) := N_3(n; a, b, c)$ be the denumerant of n w.r.t. (a, b, c). Then*

$$N_3(n) = R_3(n) + G_3(n)$$

where

$$R_3(n) = \frac{n(n + a + b + c)}{2abc}$$

and $G_3(n)$ is a periodic sequence with period abc.

Fact 5.2.5 *With the notation introduced in Fact 5.2.4, let $r = abc - (a + b + c)$. For each $i = 1, 2, \ldots, a + b + c - 1$ we have*

$$G_3(r + i) = \frac{i(a + b + c - i)}{2abc}.$$

Proof. (Popoviciu, 1953), p. 38. □

5.3 Algorithms for Computing Denumerants

5.3.1 Known Methods

The traditional methods for computing denumerants are typically based on the partial fraction decomposition which is costly. For details see (Comtet, 1974), p. 109.

Another solution approach, which is of great advantage when many of the part sizes a_i have a non-trivial common divisor, is shown in (Graham, Knuth and Patashnik, 1989), Section 7.3, Example 4.

In our restricted case when the part sizes a_i are pairwise relatively prime, we may observe that the periodic part G_m is expressible as a sum $\sum_{i=1}^{m} G^{(i)}$ where each $G^{(i)}$ is periodic with period a_i. Then we may set up a linear system for the unknowns $G^{(i)}(j)$, $1 \leq i \leq m$, $0 \leq j \leq a_i - 1$, see (Comtet, 1974), p. 114. Solving this system by Gaussian elimination requires $O((\sum_{i=1}^{m} a_i)^3)$ elementary arithmetic operations (addition, subtraction, multiplication and division). Moreover, we need to compute the vector of right-hand sides for this linear system. To this end we must evaluate $N(n)$ at $(\sum_{i=1}^{m} a_i) - m$ contiguous points. This subgoal may further increase the total time complexity.

5.3.2 The New Algorithm

We now present a new algorithm whose time complexity is better than the complexity of yet known methods and which uses only elementary arithmetic operations. We add the fifth "elementary" arithmetic operation in our computational model, namely the binary modulo function $(\bmod)$. In the complexity analysis we will assume that all five operations are performed at the unit cost.

As before, let a, b, c be three fixed pairwise relatively prime positive integers and let $a \leq b \leq c$. Our goal is to compute $N_3(n; a, b, c)$ as a function of n. It should be noted that this problem actually includes *two* different tasks:

(I) Compute the "closed form" of N, i.e., obtain a representation of N that will allow us to evaluate $N(n)$ for any given n in a constant number of arithmetic operations, i.e., in time independent of n, a, b and c.

(II) Evaluate $N(n)$ for *one* given n.

As we already know, the central issue that we have to cope with is to evaluate the periodic part $G_3(n)$ on the interval $0 \leq n < abc$, say. Fact 5.2.5 states that the last $a + b + c - 1$ points of this interval are handled with a quadratic formula, whereas we do not know anything about the remaining points yet. After some experimenting (cf. Figure 5.1) one gets the idea that the values of G_3 on the rest of the interval can be obtained by horizontal and vertical "shifts" of the parabola that covers the end of the interval. In the next lemmas we prove that this is indeed true and we show how this knowledge leads to a simple algorithm for computing denumerants.

Definition 5.3.1 *For every non-negative integer t we denote*

$$g(t) := G_3(t + c) - G_3(t).$$

Lemma 5.3.2 *For any two non-negative integers k, l such that $k \equiv l \pmod{ab}$ we have*

$$g(k) = g(l).$$

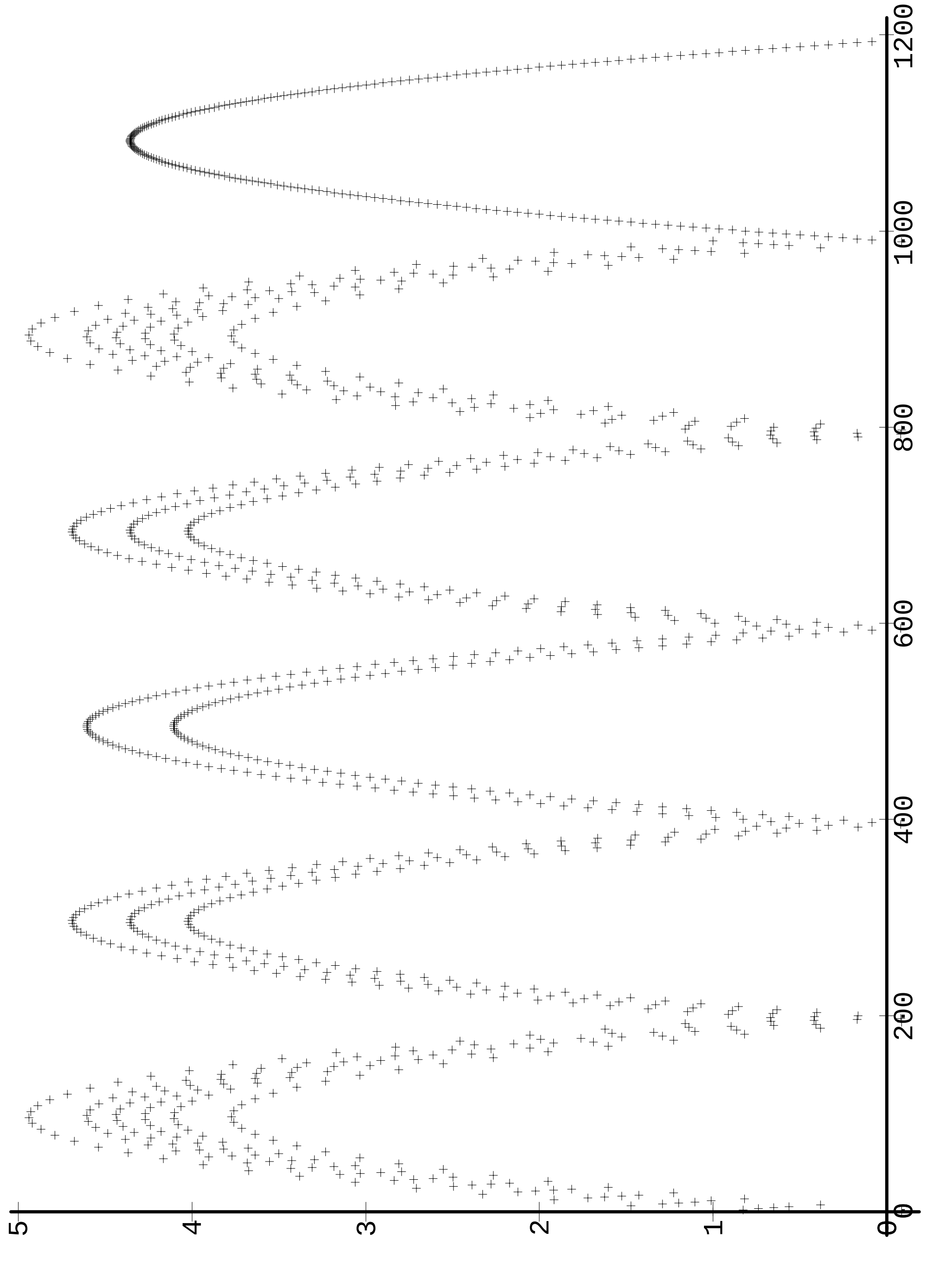


Figure 5.1: The values of $G_3(n; 2, 3, 199)$ for $0 \le n < 2 \cdot 3 \cdot 199$.

Proof. Let $t \in \{k, l\}$. We have

$$G_3(t+c) - G_3(t) = N_3(t+c) - N_3(t) + R_3(t) - R_3(t+c).$$

From Facts 5.2.1, 5.2.3 and 5.2.4 we obtain

$$N_3(t+c) - N_3(t) = \frac{t+c}{ab} + G_2(t+c)$$

$$R_3(t) - R_3(t+c) = -\frac{t+c}{ab} - \frac{1}{2a} - \frac{1}{2b}.$$

Hence,

$$\begin{aligned} g(t) &= G_3(t+c) - G_3(t) \\ &= -\frac{1}{a}\left(\frac{t+c}{b} \mid a\right) - \frac{1}{b}\left(\frac{t+c}{a} \mid b\right) + 1 - \frac{1}{2a} - \frac{1}{2b}. \end{aligned} \tag{5.4}$$

It is easily seen that $n' \equiv n'' \pmod p$ implies $(n'/q \mid p) = (n''/q \mid p)$, hence $k \equiv l \pmod{ab}$ implies $g(k) = g(l)$. □

Lemma 5.3.3 *Let $k \equiv l \pmod{ab}$ and let q be an integer. Then*

$$G_3(k+qc) - G_3(k) = G_3(l+qc) - G_3(l).$$

Proof. This is an easy consequence of Lemma 5.3.2. □

Lemma 5.3.4 *There are $(ab)^2$ rational numbers Δ_i^j, $0 \le i < ab$, $0 \le j < ab$ such that for any k we have*

$$G_3(i \cdot c + k) = G_3((ab-1) \cdot c + k) + \Delta_i^j \quad \textit{whenever } k \equiv j \pmod{ab}.$$

Proof. Put $\Delta_i^j = G_3(i \cdot c + j) - G_3((ab-1) \cdot c + j)$. Using Lemma 5.3.3 we conclude that $k \equiv j \pmod{ab}$ implies $\Delta_i^j = G_3(i \cdot c + k) - G_3((ab-1) \cdot c + k)$. □

Lemma 5.3.4 is the basis for the following simple *algorithm* which computes $G_3(n_0)$ for given $0 \le n_0 < abc$:

1. Set $i_0 := \lfloor n_0/c \rfloor$.
2. Set $k_0 := n_0 \bmod c$.
3. Set $j_0 := k_0 \bmod ab$.
4. Evaluate $G_3((ab-1)\cdot c + k_0)$ by Fact 5.2.5.
5. Return $G_3(n_0) := G_3((ab-1)\cdot c + k_0) + \Delta_{i_0}^{j_0}$.

Theorem 5.3.5 *Let a, b, c be pairwise relatively prime positive integers. If $ab \geq c$ then the task (I) can be solved in time $O(abc)$. If $ab \leq c$ then the task (I) can be solved in time $O((ab)^2)$.*

Proof. The values $\left(\frac{n}{a} \mid b\right)$ and $\left(\frac{n}{b} \mid a\right)$ for all residue classes of n can be identified by computing the values

$$az \bmod b \qquad (0 \leq z < b)$$

and

$$bz \bmod a \qquad (0 \leq z < a)$$

using $O(b)$ arithmetic operations (cf. the description of our computational model).

Then we can compute $g(t)$ for any t in constant time using (5.4). Now we employ two sets of equations

$$\Delta_0^j = g((ab-1)c + j) \tag{5.5}$$

and

$$\Delta_i^j = \Delta_{i-1}^j + g((i-1)c + j), \qquad 1 \leq i < ab. \tag{5.6}$$

Using (5.5) and (5.6) we determine Δ_i^j for all indices in the range $0 \leq i < ab$ and $0 \leq j < \min(ab, c)$ in constant time per item. If $ab \geq c$ then we compute abc such values, if $ab \leq c$ then we need $(ab)^2$ values. Knowing these Δ_i^j allows us to evaluate $G_3(t)$ and hence also $N_3(t)$ for any t in constant time. □

Theorem 5.3.6 *Let a, b, c be pairwise relatively prime positive integers. Then the task (II) can be solved in time $O(ab)$.*

Proof. Again we start by computing the values $\left(\frac{n}{a} \mid b\right)$ and $\left(\frac{n}{b} \mid a\right)$ in $O(b)$ time. Now for any given t, we compute $G_3((ab-1)c + (t \bmod c))$ by Fact 5.2.5. Then we "jump" to the value $G_3(t)$ in at most $ab-1$ steps described by equation (5.4), in a constant time per each step. Actually at most $ab/2$ such steps are always sufficient since we can do the steps in both "directions". $\square$

5.3.3 Comparison with Other Algorithms

From Theorem 5.3.5 it follows immediately that our algorithm for task *(I)* is asymptotically better than the linear system approach described in Section 5.3.1 since the latter one needs at least order of c^3 operations if Gaussian elimination is used.

Task *(II)* is treated in (Popoviciu, 1953), p. 27 with a formula which has time complexity $O(c)$. If $ab > c$ then this formula is more efficient while our approach (Theorem 5.3.6) is asymptotically better in the case $ab < c$.

We also have to emphasize the *simplicity* of our algorithms as they do not use any procedure other than the basic arithmetic (no linear systems, no partial fraction decompositions etc.).

5.4 Approximations

The main goal of (Popoviciu, 1953) was to determine all pairwise relatively prime triples (a, b, c) such that the denumerant $N(n) = N_3(n; a, b, c)$ is expressible as the floor of some polynomial $P(n)$, i.e., $N(n) = \lfloor P(n) \rfloor$. This is possible exactly if

$$\max_{0 \le n < abc} G_3(n) - \min_{0 \le n < abc} G_3(n) < 1. \tag{5.7}$$

For the sake of completeness we mention that there are 18 such triples (a, b, c). The equality $a = 1$ turns out to be a necessary condition for (5.7) to hold.

In our study we extend these investigations by giving bounds on the values of $G_3(n)$ for all cases with $a = 1$, $(b, c) = 1$. Hence, we give bounds on the "error" that occurs if the denumerant $N_3(n)$ is approximated by the polynomial $R_3(n)$.

Theorem 5.4.1 *Let b and c be pairwise relatively prime positive integers, $b < c$. For any non-negative n we have*

$$\frac{b+c+1}{2bc} - \frac{b}{8} \leq N_3(n;1,b,c) - R_3(n;1,b,c) \leq \frac{((b+c+1)/2)^2}{2bc} + \frac{b}{8}.$$

Proof. Recall that $\{x\}$ means the fractional part of x. From equation (5.4) it follows that

$$G_3(n+c;1,b,c) - G_3(n;1,b,c) = \frac{b-1}{2b} - \left\{\frac{n+c}{b}\right\}$$

for any n. For the rest of the chapter, let $G(n)$ denote $G_3(n;1,b,c)$. For any $1 \leq k \leq b$ we have

$$G(n+kc) - G(n) = k \cdot \frac{b-1}{2b} - \sum_{j=1}^{k} \left\{\frac{n+jc}{b}\right\}.$$

Let us examine the function

$$F(k) = k(b-1)/2 - \sum_{j=1}^{k} (n+jc) \bmod b.$$

One can write $F(k) = \sum_{j=1}^{k} f_j$ where

$$f_j = (b-1)/2 - (n+jc) \bmod b.$$

From $(b,c) = 1$ it follows that

$$\{f_j \mid 1 \leq j \leq b\} = \{\ -(b-1)/2,\ \ -(b-3)/2,\ \ \ldots,\ \ (b-3)/2,\ \ (b-1)/2\}.$$

Denote

$$f_- = \{f_j \mid f_j < 0\}, \quad f_+ = \{f_j \mid f_j > 0\}.$$

For any value of b we have

$$-\frac{b^2}{8} \leq \sum_{x \in f_-} x, \qquad \sum_{x \in f_+} x \leq \frac{b^2}{8}.$$

Hence,

$$-\frac{b^2}{8} \leq F(k) \leq \frac{b^2}{8}.$$

Incidentally, these bounds are indeed achieved for certain choices of n, b, c and k. (The proof is left as an exercise.) Coming back to the definition of $F(k)$, we see that

$$-\frac{b}{8} \leq \Delta_i^j \leq \frac{b}{8}$$

for all i, j. By Fact 5.2.5 we have

$$\frac{b+c+1}{2bc} \leq G(n) \leq \frac{((b+c+1)/2)^2}{2bc}$$

for all $bc-(b+c) \leq n \leq bc-1$. The rest follows from Lemma 5.3.4. □

Remark. A slight refinement of the last theorem can be achieved by splitting it in three statements according to the parity of b and c.

5.5 Methodological Aspects

The investigations presented in this chapter represent one circle on the creativity spiral (Section 0.1). Using Maple code described in Section 4.5 we examined one special type of quasi-polynomials, and collected very appealing experimental data, such as for example the drawing in Figure 5.1. From these data we gained an idea how the function G_3 behaves in general, and we succeeded to prove the corresponding theorems. These theorems gave us a new, more efficient algorithm for computing denumerants.

Part III

Constructive Combinatorics

Chapter 6

Group Action and Constructions

In Part II of our thesis we approached the problem of counting combinatorial objects, mainly in the presence of an equivalence relation. The general method of solving the counting problem, both in the unweighted and in the weighted case, was to replace the equivalence by a finite group action and to apply algebraic tools like the Cauchy-Frobenius Lemma and its refinements.

The present part of the thesis is centered around the methods for constructing unique representatives of equivalence classes of discrete structures. We will be mainly concerned with the study how constructing discrete structures can give us intuition for rigorous proofs of combinatorial theorems involving these structures. Since the power of modern computers is exploding continuously, the constructive methods are becoming an extremely important tool for getting insight in combinatorial problems.

Also this part starts with a preparatory chapter introducing the concepts and methods that we will be using later on. Since there is an obvious relation between counting and constructing, we will build on the definitions and statements about finite group actions as we learned them in Chapter 2. Due to a huge variety of possible approaches to the construction problem, the introduction to it will be done in a very pragmatic style; only topics relevant to our work will be presented in some detail. We will try to balance this drawback by pointing to other reading whenever possible. In particular, for excellent surveys of construction methods we refer the reader to Chapter 7 of (Kerber, 1991) and to (Laue, 1993).

6.1 Problem Specification

Definition 6.1.1 *Let X be a G-set, Y be a finite set and consider G's induced action on Y^X as in Definition 2.1.14. The* construction problem *related to this induced action is to find a transversal of G–orbits on Y^X, i.e., to find a subset $\mathcal{T}(G \,\backslash\backslash\, Y^X)$ of Y^X such that*

$$Y^X = \dot{\bigcup_{f \in \mathcal{T}(G \,\backslash\backslash\, Y^X)}} G(f).$$

We will write just $\mathcal{T}$ instead of $\mathcal{T}(G \,\backslash\backslash\, Y^X)$ if no confusion can arise.

We have to emphasize that the union in the last equation is disjoint, i.e., $\mathcal{T}$ contains exactly one element from each G-orbit.

Definition 6.1.2 *The elements of the transversal $\mathcal{T}$ will be called* representatives *of G-orbits.*

It should be noted that until now the transversal is by no means unique. The uniqueness, which is of great importance for computational methods, can be achieved by imposing additional conditions concerning certain properties of the representatives. Section 6.2.1 will discuss this issue in more detail.

Instead of "construction" one sometimes says *listing* or *generation* of class representatives. The transversal may also be called list of representatives or, as we will mostly say, the *catalog of representatives.*

It should be also pointed out that some authors use the word "enumeration" as a synonym for counting while others use it in context of constructions. To resolve this ambiguity, we declare that in our thesis "enumeration" always means counting while the possible synonyms for "construction" are listed in the preceding paragraph.

It may be surprising that we bound the construction problem to the "symmetry classes of mappings" paradigm. We will try to convince the reader in subsequent chapters that this setting covers a big portion of the problems that may generally be addressed as "constructional". One of the reasons for this fact is the bijection

$$\begin{array}{rcl} \mathcal{P}(X) & \to & \{0,1\}^X \\ Y & \mapsto & \chi_Y \end{array} \tag{6.1}$$

between the power set of X and the set of all $0,1$-functions on X. This means that, among others, also all problems related to constructing symmetry classes of X's subsets are covered by our definition.

Another advantage of our setting is that we can compute the cardinality of the transversal (i.e., we can cross-check the length of the output of the listing program) by Pólya's Theorem 2.1.25. Indeed, there is a close relationship between the enumerative applications of finite group action (as we learned them in Chapter 2) and the constructive applications which we are learning now.

Of course, there are some other constructive tasks lying beyond our paradigm. One of well-known examples is Lam and others' (1989) search for a projective plane of order 10. See (Lam, 1993) for a more general setting of a combinatorial search (construction) problem.

6.1.1 Small and Large Problems

Analogous to different methods for multiplying "short" and "long" integers, for example, there are also different methods for handling "small" and "large" construction problems. The size of a construction problem is determined by the order of G and by the cardinalities of sets Y and X. If both $|G|$ and $|Y^X|$ are small then we can afford to completely evaluate G–orbits, see Section 7.1 of (Kerber, 1991) for methods how to do that.

What is sufficiently "small" depends on computational means that we have at our disposal. Problems where the order of G is 10^{10}, say, will probably never belong to this scope, i.e., they are inherently large. Still one can handle such large actions algorithmically. Let us note that many construction tasks discussed in subsequent chapters have this or similar size. Hence, also in this preparatory chapter we will restrict our attention to large problems.

6.2 Orderly Methods

Orderly methods of generation were invented by Read (1978*a*). According to some references, for example (Walsh, 1983) or (Brinkmann, 1992), similar ideas were independently used by Faradzhev around 1976. Orderly methods belong to the family of branch and bound methods.

Before we can explain the orderly algorithm, we need two technical definitions:

Definition 6.2.1 *Let $T = (t_i)_{1 \leq i \leq r}$ be a sequence (list) over a set U and let $u \in U$. We will say that u* occurs *in T if there is an index $j \in \underline{r}$ such that $z = t_j$.*

Definition 6.2.2 *Let $T = (t_i)_{1 \leq i \leq r}$ be a sequence (list) over a set U. The set of all elements of U that occur in T will be denoted by* $\mathrm{Set}(T)$.

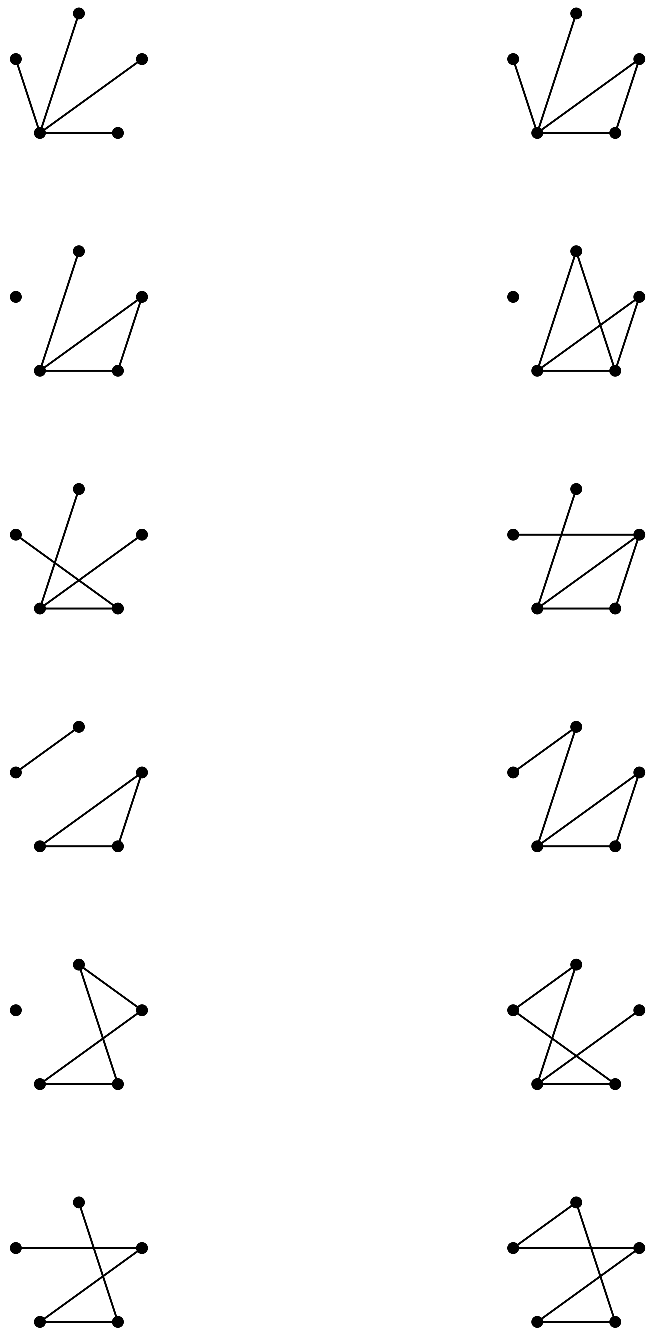


Figure 6.1: One augmentation step in orderly generation.

We describe the orderly methods for a special case when we look for the transversal of G–orbits on the set $\{0,1\}^{\underline{n}}$ for some $G \leq S_{\underline{n}}$, $n \in \mathbb{N}^+$. In our thesis we use the orderly approach only for this kind of actions.

Definition 6.2.3 *Let $G \leq S_{\underline{n}}$ be acting naturally on $\underline{n}$ and let $>$, $\geq$ be the lexicographic orderings induced on $\{0,1\}^{\underline{n}}$ by the total ordering $1 > 0$ of $\{0,1\}$. For each orbit of G on $\{0,1\}^{\underline{n}}$ we define its* canonical representative *to be the lexicographically greatest element in that orbit, i.e.,*

$$f \ \textit{canonical} \ :\Longleftrightarrow (\forall \pi \in G)(f \geq \pi f).$$

Definition 6.2.4 *With the assumptions of Definition 6.2.3, the G–transversal of $\{0,1\}^{\underline{n}}$ consisting entirely of canonical representatives will be called the* canonical G–transversal of $\{0,1\}^{\underline{n}}$.

Definition 6.2.5 *Let $f \in \{0,1\}^{\underline{n}}$ and let $k := \max\{j \in \underline{n} \mid f(j) = 1\}$. We define the* augmentation of f *to be the sequence (list)*

$$\operatorname{aug}(f) \ := \ \left(f^{(k+1)}, f^{(k+2)}, \ldots, f^{(n)}\right),$$

where for any $l \in \underline{n}$ and $f \in \{0,1\}^{\underline{n}}$, $f^{(l)}$ is defined by

$$f^{(l)} \in \{0,1\}^{\underline{n}}, \qquad f^{(l)}(m) = f(m) \ \text{if} \ m \neq l \quad \text{and} \ f^{(l)}(l) = 1.$$

If $k = n$ then $\operatorname{aug}(f)$ *is the empty list.*

The idea behind the name "augmentation" is the following: Let $f \in \{0,1\}^{\underline{n}}$ and let $S \subseteq \underline{n}$ such that $f = \chi_S$. Then the list $\operatorname{aug}(f)$ consists of all functions f' such that $f' = \chi_{S'}$ where $S' = S \cup \{l\}$ for some $l > \max S$.

Definition 6.2.6 *For any non-empty sequence (list) L, let* $\operatorname{last}(L)$ *denote the last element in L.*

Definition 6.2.7 *Let $L = (f_i)_{1 \leq i \leq r}$ be a sequence (list) of functions from $\{0,1\}^{\underline{n}}$. We define the* augmentation *of L to be the sequence (list)* $\operatorname{Aug}(L)$ *obtained by the following algorithm:*

1. Put $L' := (\ )$, the empty list.
2. For $i := 1$ to r do
   $A := \operatorname{aug}(f_i)$; let $A = (a_j)_{1 \leq j \leq s}$

For $j := 1$ to s do
  If a_j canonical and (L' is empty
      or $a_j > \text{last}(L')$)
   then append a_j at the end of L'.
3. Return $\text{Aug}(L) := L'$.

An example illustrating Definition 6.2.7 will follow soon.

The essence of the orderly approach (here for cataloging 0, 1-function representatives) is contained in the following theorem.

Theorem 6.2.8 (Read) *Let G be acting on $\{0,1\}^{\underline{n}}$. The following algorithm delivers the canonical G–transversal of $\{0,1\}^{\underline{n}}$:*

1. Put $L_0 := ((0,0,\ldots,0))$.
2. For $i := 1$ to n do $L_i := \text{Aug}(L_{i-1})$.
3. Return $\mathcal{T}(G \backslash\backslash \{0,1\}^{\underline{n}}) := \bigcup_{i=0}^{n} \text{Set}(L_i)$.

In particular, L_i is the canonical G–transversal of functions with content $(n-i,i)$, i.e., with $n-i$ zeros and i ones.

Proof. (Read, 1978*a*), Section 2. □

The adjective *orderly* means that the method under description produces canonical representatives ordered by content and, moreover, the representatives of the same content are ordered lexicographically.

As an example illustrating Definition 6.2.7 and Theorem 6.2.8, consider listing of (simple, undirected) graphs on 5 vertices. Each *labeled* graph on 5 vertices is in an obvious one-to-one correspondence with a function from $\{0,1\}^{\underline{10}}$: The numbers $1,\ldots,10$ denote edges $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{1,5\}$, $\{2,3\}$, ..., $\{4,5\}$, respectively, and for any $f \in \{0,1\}^{\underline{10}}$, $f(i) = 1$ exactly if the edge number i is present in the graph encoded by f. An *unlabeled* graph on 5 vertices is then a G–orbit on $\{0,1\}^{\underline{10}}$ where $G \leq S_{\underline{10}}$ is the permutation representation of $S_{\underline{5}}$ in its action on unordered pairs $\{i,j\}$, $1 \leq i < j \leq 5$.

In Figure 6.1 we see one augmentation step in the orderly generation of unlabeled graphs on 5 vertices. In each graph, vertex numbering starts at the lower left vertex of the pentagon and proceeds counter-clockwise. The labeling of edges is then derived from vertex numbers as explained in the preceding paragraph. We invite the reader to check that the displayed graphs are canonical representatives of orbits with content $(6,4)$ and $(5,5)$ and also to check the augmentation $L_5 := \mathrm{Aug}(L_4)$, see Definition 6.2.7 and Theorem 6.2.8.

6.2.1 Canonical Forms

The only difficult step in the orderly algorithm is to check if a given function $f \in \{0,1\}^{\underline{n}}$ is the canonical representative of its G–orbit. Read (1978*a*) in his historical paper does not address this problem in much detail, and indeed the time complexity of the *canonicity check* has been for a long time the limiting issue for the applicability of orderly methods. The naive approach would be to test the inequality

$$f \geq \pi f \tag{6.2}$$

for *all* $\pi \in G$. This is of course prohibitive if $|G|$ is large.

A fast canonicity check was developed by Grund (1992). The group G is stored in a tree form using coset representatives in the Sims chain of stabilizers. (See (Kerber, 1991), p. 330.) The main goal is to cut this tree efficiently so that the inequality (6.2) has to be tested for as few permutations π as possible. In the general case, Grund's method requires some preprocessing of the group G which can be done using systems for computational group theory such as Cayley or Magma, see (Bosma, Cannon, 1993). In our constructions we have used Grund's canonicity check for large groups such as $PGL(5,3)$ or $PGL(3,16)$, see Chapters 10 and 11.

For another solution to the canonicity testing problem see (Hager, Kerber, Laue, Moser and Weber, 1991), p. 163.

Finally, we have to point out the essential difference between mathematical and algorithmic understanding of the adjective "canonical". The canonical forms as discussed here have algorithmic meaning only. This means that most probably they are difficult to "digest", i.e., it is difficult to understand on their basis the (mathematical) properties of the classes that these canonical functions represent. Consider, for example, the canonical graphs in Figure 6.1: A graph theorist would draw most of these pictures in a different way. We will return to this problem in more detail at the end of Chapter 7.

6.2.2 Restricted Generation

It occurs very often that we are not interested in exhaustive catalogs of class representatives but rather we want to list only the representatives satisfying a given property P. We will show that, for certain "nice" properties P, the orderly methods can be used for generation of restricted catalogs.

Definition 6.2.9 *Let Z be a G–set and let P be a predicate defined on Z. We say that the action ${}_G Z$* preserves the predicate P *if for each $g \in G$ and each $z \in Z$ we have $P(z) \iff P(gz)$.*

Obviously, if a predicate is not constant on orbits then it makes no sense to consider it in the frame of group action.

Definition 6.2.10 *Let P be a predicate defined on $\{0,1\}^{\underline{n}}$ and let for any $f \in \{0,1\}^{\underline{n}}$ the sequence* $\mathrm{aug}(f)$ *be as in Definition 6.2.5. We say that P is* consistent with augmentation *if the following holds for any $f, f' \in \{0,1\}^{\underline{n}}$:*

$$(P(f) \;\wedge\; f \text{ occurs in } \mathrm{aug}(f')) \implies P(f').$$

It is now easy to see that if a predicate P possesses both properties defined above then it can be used for restricting the generation process:

Theorem 6.2.11 *Let ${}_G(\{0,1\}^{\underline{n}})$ be an action that preserves the predicate P and let P be consistent with augmentation. Let* Restr_Ord *be Read's orderly algorithm (as described in Theorem 6.2.8) modified by inserting the condition $P(a_j)$ in the if-statement in Definition 6.2.7, and suppose that $P(0,\dots,0)$ is true. Let L be the canonical G–transversal of $\{0,1\}^{\underline{n}}$. Then the algorithm* Restr_Ord *outputs the set L' such that*

$$L' = \{f \in \{0,1\}^{\underline{n}} \mid f \in L \wedge P(f)\}\,.$$

Proof. For this and many more thoughts on restricted generation we refer to the papers (Colbourn, Read, 1979) and, in particular, (Brinkmann, 1992). □

Remark. In our statement of the last theorem, some of the assumptions can be weakened or rephrased. For example, in Definition 6.2.10 it is enough to require that the implication holds if f, f' are canonical.

As the first example of restricted orderly generation, consider the generation of unlabeled triangle-free graphs on v vertices. As explained earlier in this chapter, unlabeled simple graphs on v vertices are G–orbits on $\{0,1\}^{\underline{n}}$ where $n = \binom{v}{2}$ and G (the "graph group") is a subgroup of $S_{\underline{n}}$ isomorphic to $S_{\underline{v}}$. Each element of $f \in \{0,1\}^{\underline{n}}$ is a unique encoding of a unique labeled graph on v vertices; with a slight abuse of notation we will speak about the labeled graph f. Let us put $P(f) :\Longleftrightarrow$ "f is triangle-free". It is straightforward to verify that P satisfies the assumptions of Theorem 6.2.11, and so we can use restricted orderly generation in this case.

For a more involved example, consider generation of graphs on v vertices with girth equal to 6. (Girth of a graph Γ is the length of the shortest cycle in Γ. If there are no cycles in Γ then we put $\text{girth}(\Gamma) = \infty$.) We note that the predicate $P(f) :\Longleftrightarrow$ "$\text{girth}(f) = 6$" is not consistent with augmentation because adding an edge to a given graph may decrease its girth. What we can do is to use the predicate $P'(f) :\Longleftrightarrow$ "$\text{girth}(f) \geq 6$" which *is* consistent with augmentation, construct the catalog L' of all graphs on v vertices with girth greater or equal 6 and finally single out from L' those items whose girth is 6.

In general, if we aim at a restricted generation w.r.t. predicate P that is not consistent with augmentation, a way out is to find a weaker predicate P' (i.e., $P(f) \Longrightarrow P'(f)$ for all f) such that P' is consistent with augmentation, use the restricted orderly generation controlled by P' and then extract from the resulting list the entries that satisfy P.

We would like to emphasize that the last two examples are somewhat artificial because more efficient methods exist for graph generation restricted by girth. We took these examples because they are easy to present and understand.

6.3 Other General Methods

After the detailed presentation of the orderly methods, we recall very briefly some other constructive methods that are applicable for any finite G, X and Y.

6.3.1 Recursive Methods

These methods apply to cases when Y has more than two elements. The recursion is by cardinality of Y and relies on the homomorphism principle, see (Kerber, 1991). For many other applications of the homomorphism principle in construction problems see (Laue, 1993).

6.3.2 Double Coset Representatives

Construction of (non-canonical) transversals can be reduced to construction of double coset representatives:

Theorem 6.3.1 (Ruch) *Let $G \leq S_{\underline{n}}$ and let $m \in \mathbb{N}$. Let $\sum_{i=0}^{m} \lambda_i = n$, $\lambda_i \in \mathbb{N}$ for $0 \leq i \leq m$. There is a one-to-one correspondence between double cosets $S_\lambda \backslash S_{\underline{n}}/G$ and G–orbits on $\{0, 1, \ldots, m\}^{\underline{n}}$ with content $(\lambda_0, \ldots, \lambda_m)$. (Here S_λ means the Young subgroup determined by the partition λ, i.e., $S_\lambda = S_{\lambda_0} \oplus \ldots \oplus S_{\lambda_m}$.)*

Proof. E.g., (Krishnamurthy, 1986), pp. 185–189. □

A construction method relying on double cosets was invented by Schmalz (1990). He calls his method "ladder game" (Leiterspiel). A slight drawback of this approach in computer applications is a high requirement on computer memory which makes the program applicable only for values of n up to 50 or so.

6.3.3 Combined Methods

Hager, Kerber, Laue, Moser and Weber (1991) present two combined methods for transversal construction. The ingredients are orderly approach, recursion and homomorphism principle.

6.3.4 Generation by Stabilizer Type

Suppose that X is a G–set, Y is a finite set and let $f \in Y^X$. The subgroup G_f of G which fixes f is called the stabilizer of f, see Definition 2.1.10. If f and f' belong to the same G–orbit then G_f and $G_{f'}$ are conjugate subgroups of G. By Burnside's Lemma, see Chapter 3 of (Kerber, 1991), it is possible to determine the number of G–orbits with stabilizers in the given conjugacy class of subgroups of G. Laue (1989) refined this counting lemma to a constructive method, i.e., to an algorithm that constructs class representatives with a given stabilizer.

6.3.5 Random Generation

Dixon and Wilf (1983) invented an algorithm that generates orbit representatives uniformly at random, i.e., a representative of any orbit is likely to appear with equal probability.

Kerber, Laue, Hager and Weber (1990) showed how to use this method for building exhaustive catalogs: The number of orbits computed by Pólya's Theorem serves as a stopping rule, and canonical representatives of yet constructed orbits can be efficiently maintained for later comparisons in an AVL-tree. In this case, for the "canonical form" w.r.t. the action ${}_GZ$ we may use *any* mapping $\mathrm{can}: Z \to Z$ such that $\mathrm{can}(z) = \mathrm{can}(gz)$ for all g and z, i.e., we are not restricted to special canonical forms like it was in the case of orderly generation.

It is known from statistics that the expected number of random "drawings" necessary to build in this way the catalog of length L is approximately $L \log L$. For the calculation see, e.g., (Nijenhuis, Wilf, 1978), p. 40.

6.4 Specialized Listing Methods

In Sections 6.2 and 6.3 we focused our attention on general constructive methods that are applicable to *any* action ${}_G(Y^X)$, $G \leq S_{\underline{n}}$. It often happens that for special permutation groups G and special restrictive properties (Section 6.2.2) more efficient methods exist. A brief survey of several selected cases follows.

6.4.1 Graphs

The best known method for exhaustive generation of simple unlabeled graphs is due to B.D. McKay (1990). It is a great service to the mathematics community that the author makes the algorithms available as C language code in the form of *nauty* package which can operate on different computing platforms. Among *nauty*'s features we find *makeg*, the program for graph generation, as well as the procedure *nauty* itself, which can compute canonical forms of graphs (in the sense of Section 6.3.5) and the automorphism groups of graphs.

Using *nauty* for computing canonical forms of graphs ("practical graph isomorphism") has been of great help for us for getting insight in classification of chordal rings as presented in Chapter 8 of our thesis.

6.4.2 Rooted and Unrooted Trees

An algorithm for generation of unlabeled rooted trees in constant time per tree was developed by Beyer and Hedetniemi (1980) and later extended by Wright, Richmond, Odlyzko and McKay (1986) for the case of unlabeled free trees.

6.4.3 Regular Graphs

Brinkmann (1992) invented a fast, orderly-like method for generation of unlabeled 3-regular (cubic) graphs. Beezer (1991) developed an algorithm that is applicable for unlabeled r-regular graphs, $r \geq 3$. It should be mentioned, however, that for $r \geq 4$ the number of unlabeled r–regular graphs grows very quickly with the number of vertices so cataloging such graphs is not very practical.

Some thoughts about building catalogs of cubic graphs will be presented in Section 7.4 of our thesis.

6.4.4 Necklaces

If we take the cyclic group $C_{\underline{n}}$ for G in Definition 6.1.1 then the $C_{\underline{n}}$–orbits on $Y^{\underline{n}}$ are called *necklaces* with n beads. Similarly, the $D_{\underline{n}}$–orbits on $Y^{\underline{n}}$ are called *bracelets* with n beads. Generation of necklaces and bracelets will be treated in much detail in Chapter 9 of our thesis.

Chapter 7

On a Conjecture of Graffiti

A graph is r-regular if each its vertex has degree (valence) r. Regular graphs occur so often in graph theory that they deserve special interest; many of them serve as counterexamples to conjectures or play crucial role in proofs.

In this chapter we will see a particular 3-regular (cubic) graph disprove one of the recent conjectures of Graffiti, a computer system which is designed for making graph-theoretical hypotheses. We present an entire family of counterexamples. The way in which the counterexamples were derived bases both on the search of the catalogs of cubic graphs and on mathematical understanding and generalization of the search results.

7.1 About Graffiti

Graffiti is a computer system which makes graph-theoretical conjectures. The system was developed by S. Fajtlowicz at the University of Houston. The main principles of Graffiti are described in (Fajtlowicz, 1988). There have been several updates to this paper, which have reported on new conjectures as well as on the status of old ones. The state of the art is periodically resumed in the report (Fajtlowicz, 1991).

In the present chapter we deal with one of the recent conjectures which was recorded with number 750 in October 1992.

7.2 The Conjecture

Let $G = (V, E)$ be a connected simple undirected graph. The distance of two vertices $u, v \in V$ is the number of edges on any shortest path from u to v and will be denoted as $\mathrm{dist}(u, v)$. Any set $X \subseteq V$ with the property $(\forall w, z \in X)(\{w, z\} \notin E)$ is an *independent set* of G. If Y is an independent set of G such that for each other independent set Z the inequality $|Z| \leq |Y|$ holds, then Y is a *largest independent set* of G.

Definition 7.2.1 *The cardinality of any of G's largest independent sets will be denoted by* $\mathrm{Indep}(G)$.

Definition 7.2.2 *Let v be a vertex of G. The number of vertices at odd distance from v will be denoted by* $\mathrm{odd}(v)$*:*

$$\mathrm{odd}(v) \;:=\; |\{w \in V \,|\, \mathrm{dist}(v,w) \text{ is odd}\}|.$$

Definition 7.2.3 *If both endpoints of an edge $e \in E$ happen to have the same distance from a vertex $v \in V$, then e is a* horizontal edge *w.r.t. v.*

Definition 7.2.4 *The number of edges that are horizontal with respect to a given vertex v is denoted by* $\mathrm{horiz}(v)$*:*

$$\mathrm{horiz}(v) \;:=\; |\{\{x,y\} \in E \,|\, \mathrm{dist}(v,x) = \mathrm{dist}(v,y)\}|.$$

Graffiti made the following conjecture (Fajtlowicz, 1992):

Conjecture 750. For every connected graph $G = (V,E)$,

$$\max_{v \in V} \mathrm{odd}(v) - \min_{v \in V} \mathrm{horiz}(v) \;\leq\; \mathrm{Indep}(G). \tag{7.1}$$

The author of the program mentioned that this conjecture is in fact not very likely to be true, and asked for counterexamples that would enrich Graffiti's knowledge base and prevent the system from generating other weak conjectures. In the next section we describe how an entire family of such examples was obtained.

7.3 Derivation of Counterexamples

In the run for counterexamples we first examined some small graphs which led to no results. Afterwards, we turned to a systematic inspection of regular graphs, and soon a cubic graph on 10 vertices popped up as a counterexample to (7.1). For the reasons that become clear later, we will call it G_3. See Figure 7.1.

We invite the reader to investigate on her/his own why G_3 does refute (7.1). Let us just mention that the "error" in Conjecture 750 (difference between the left-hand side and the right-hand side in (7.1)) is equal to 1 for our graph. One may ask whether there are graphs for which this "error" takes larger values, and now the creative part of our deal comes.

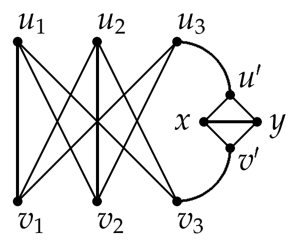


Figure 7.1: The graph G_3

We show that (7.1) cannot be "repaired by an additive constant", i.e., it keeps false even if the right-hand side is replaced by the term $\mathrm{Indep}(G) + p$, where p is a fixed positive integer.

To this end, we introduce and study the following sequence of graphs $(G_n)_{n \geq 3}$:

$$\begin{aligned} G_n &:= (V_n, E_n)\ , \text{ where} \\ V_n &:= \{u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_n, u', x, y, v'\}\ , \\ E_n &:= \{\{u_i, v_j\} \mid 1 \leq i \leq n,\, 1 \leq j \leq n\} \setminus \{\{u_n, v_n\}\} \\ &\quad \cup \{\{u_n, u'\}, \{u', x\}, \{u', y\}, \{v_n, v'\}, \{v', x\}, \{v', y\}, \{x, y\}\}\ . \end{aligned}$$

Informally, G_n is obtained from the complete bipartite graph $K_{n,n}$ by inserting a "diamond" (two triangles glued together along a common edge) at one of its edges.

Proposition 7.3.1 *For each $n \geq 3$, the following holds for the graph G_n:*

1. $\mathrm{Indep}(G_n) = n + 1$.
2. $\max_{v \in V_n} \mathrm{odd}(v) \geq 2n + 1$.
3. $\min_{v \in V_n} \mathrm{horiz}(v) \leq 2$.

Proof. 1. Note that the graph G_n is symmetric w.r.t. the mutual exchange of u- and v-vertices. Let I be one of G_n's independent sets. If both u_n and v_n belong to I, then I is one of $\{u_n, v_n\}$, $\{u_n, v_n, x\}$, $\{u_n, v_n, y\}$ and so $|I| \leq 3$. If just one of them (u_n, say) belongs to I, then I can be as large as $\{u_1, u_2, \ldots, u_n, x\}$, i.e., $|I| \leq n + 1$. If none of u_n, v_n is in I, then w.l.o.g. $I \subseteq \{u_1, ..., u_{n-1}, u', v'\}$ or $I \subseteq \{u_1, ..., u_{n-1}, z\}$ where z is one of x, y. We see that $\mathrm{Indep}(G_n) = n + 1$.

2. This follows easily from $\mathrm{odd}(x) = 2n + 1$. The $2n + 1$ vertices at an odd distance from x are $u', y, v', u_1, u_2, \ldots, u_{n-1}, v_1, v_2, \ldots, v_{n-1}$.

3. This follows easily from $\mathrm{horiz}(u_n) = 2$. Consider that none of the edges $\{u_i, v_j\}$ is horizontal w.r.t. u_n. The examination of the remaining edges shows that $\{x, y\}$ and $\{v_n, v'\}$ are the only two edges in E_n that are horizontal w.r.t. u_n. □

Corollary 7.3.2 *In G_n, the difference between left-hand side and right-hand side of (7.1) is at least* $(2n + 1) - 2 - (n + 1) = n - 2$, *i.e.,*

$$\left(\max_{v \in V_n} \mathrm{odd}(v) \; - \; \min_{v \in V_n} \mathrm{horiz}(v)\right) \; - \; \mathrm{Indep}(G_n) \geq n - 2.$$

The author of Graffiti wrote about our constructions: "Your counterexamples can be easily modified to get other useful examples. By attaching the path with two vertices to the vertex x one gets arbitrarily large difference for the even version of the conjecture. ... So your examples are indeed very valuable."

7.4 Methodological Aspects

We used computer-generated catalogs of cubic graphs to find our graph G_3 as a simple counterexample to (7.1). The full understanding of underlying graph-theoretical mechanisms allowed us to derive generalizations of G_3 into G_n. Since both computer search and human mind were inevitable to end up with the family $(G_n)_{n \geq 3}$—which disproves not only the original conjecture but also any conjectures resulting from it by including an additive constant—the material presented in this chapter is a good example of experimental combinatorics as discussed in Section 0.2.

While the discovery (and correctness proof) of the general pattern G_n certainly belongs to the human part of the deal, we have to stress that *another* human step was necessary at the earlier stages of the work: This was the "perception" of the graph G_3. As we explained at the end of Section 6.2.1, the "canonical" forms that appear in the process of graph generation are far from what a graph theorist would understand as a canonical drawing of the respective graph. While this issue was not that critical in the case of G_3 which has only 10 vertices, it may become a real obstacle for larger graphs. The problem "how to decipher a given cryptic isomorph of some interesting graph" may be very difficult in general. At least in the case of cubic graphs, however, a practical solution may be possible.

As early as 1889 it was proven by de Vries that each cubic graph can be obtained from the complete graph K_4 (tetrahedron) by juxtaposition of three simple augmentation operations. A modern account of de Vries' theorem was given by Gropp (1992). Hence, one could think of "illustrated catalogs" of cubic graphs in the following sense: One takes a certain set of well-understood cubic graphs as a basis set; the remaining cubic graphs are then "illustrated" or "explained" in terms of the basis graphs and de Vries' augmentation operations. The total number of cubic graphs on v vertices is known for all meaningful values of v, which may serve as a stopping rule (criterion of completeness). (For a table see (Robinson, Wormald, 1983).) Avoiding duplicates can be easily done by McKay's isomorphism code (see Section 6.4.1).

Production of such "illustrated" catalogs would certainly take much longer than for example Brinkmann's (1992) fast algorithm and in certain sense this process would never be finished because we may always try to improve the "readability" of the catalog. (With each entry in the catalog one may store the "complexity" of its illustration; if a simpler illustration pops up then it replaces the old one.) On the other hand, such a catalog would probably provide a graph theorist with a more valuable information than the "canonical" forms produced by standard generation methods.

Chapter 8

Chordal Rings

A Hamiltonian circuit in a graph is a closed path (circle) that passes through each vertex of the graph exactly once. A *chordal ring* is a bipartite cubic graph obtained by adjoining k chords of equal length to a Hamiltonian circuit formed by $2k$ vertices. We are dealing with the problem of determining the isomorphism types of the chordal rings for given k and varying chord length. The solution has been known for k prime while it was conjectured that the problem is difficult if k is composite. We develop theory that allows us to approach the problem for composite values of k, and on a particular example ($k = 2^e p$, e a positive integer, p an odd prime) we show how to use this machinery in proving a classification theorem.

This means that in the present chapter we deal with a task that slightly reminds us about the constructive problem (Chapter 6) in the sense that also here we are interested in producing redundancy-free (isomorphism-free) lists of certain structures. However, due to the relatively small universe of these structures we can afford to determine the entire isomorphism classes which are also very small (none of them contains more than three objects).

After presenting definitions and motivations, the exact statement of the problem is given in Section 8.3. In Sections 8.4 and 8.5 we present graph-theoretic and number-theoretic results, and in Section 8.6 we show how to use them in proving a classification theorem.

Our contribution is an extension of the work by Boreham, Bouwer and Frucht (1974) who solved the classification problem in the case when k is a prime. Wherever we use a result of these authors, we present it as a "fact" while our own results are called "lemma" or "theorem". This terminology is used throughout the chapter.

8.1 Definitions

By the term "graph" we mean a simple undirected graph. As always in our thesis, the edge joining vertices x and y is denoted by $\{x, y\}$. Moreover, we use various terms from graph theory in their usual meaning.

Definition 8.1.1 *Let k and m be integers with $k \geq 3$ and $2 \leq m \leq k-1$. The* chordal ring *with parameters k and m is the graph* $\mathrm{CR}(k,m) := (V(k,m), E(k,m))$ *where*

$$V(k,m) := \{i \mid 0 \leq i \leq k-1\} \ \dot{\cup} \ \{\bar{i} \mid 0 \leq i \leq k-1\}$$

(to be understood as a disjoint union of two copies of $\mathbb{Z}/k\mathbb{Z}$) and

$$E(k,m) := \bigcup_{i=0}^{k-1} \{\{i, \bar{i}\}\} \ \cup \ \bigcup_{i=0}^{k-1} \{\{i, \overline{i+1}\}\} \ \cup \ \bigcup_{i=0}^{k-1} \{\{i, \overline{i+m}\}\}$$

where addition is taken modulo k.

In definitions and theorems involving two or more chordal rings, we will use the *extended notation* for vertices: we will write (k,m,i) and $(k,m,\bar{i})$ instead of i and $\bar{i}$ to emphasize the parameters of the chordal ring that the vertex in question belongs to. If, however, only one chordal ring is involved in the discussion then we will use the short notation without danger of confusion.

Informally, the graph $\mathrm{CR}(k,m)$ may be viewed as derived from the $2k$-gon with vertices (in an order of transversal)

$$\bar{0},\ 0,\ \bar{1},\ 1,\ \bar{2},\ 2,\ \ldots,\ \overline{k-1},\ k-1$$

by the adjunction of the chords

$$\{i,\ \overline{i+m}\} \qquad (i = 0,1,2,\ldots,k-1).$$

Hence, $\mathrm{CR}(k,m)$ is a bipartite cubic Hamiltonian graph.

Please note that throughout this chapter, all arithmetic concerning vertex numbering is—in accordance with Definition 8.1.1—performed modulo k.

For first examples of chordal rings we refer the reader to the drawings in Figures 8.1 and 8.2.

Definition 8.1.2 *By* $\mathrm{Aut}(\mathrm{CR}(k,m))$ *we will denote the automorphism group of* $\mathrm{CR}(k,m)$.

8.1.1 Alternating Paths and Alternating Cycles

By definition, in the graph $\mathrm{CR}(k, m)$ we have edges of three types. Hence, it is natural to think of $\mathrm{CR}(k, m)$ as an edge-colored graph and assign the edges of the type $\{i, \bar{i}\}$, $\{i, \overline{i+1}\}$ and $\{i, \overline{i+m}\}$ the colors a, b and c, respectively. We introduce the function $C : E(k, m) \to \{a, b, c\}$ that maps each edge to its color.

Definition 8.1.3 *Let $I : V(k, m_1) \to V(k, m_2)$ be an isomorphism between* $\mathrm{CR}(k, m_1)$ *and* $\mathrm{CR}(k, m_2)$ *and let I' be the bijection between $E(k, m_1)$ and $E(k, m_2)$ induced by I. We say that I is* color-faithful *if*

$$(\forall e, f \in E(k, m_1)) \qquad (C(e) = C(f)) \implies (C(I'(e)) = C(I'(f))).$$

Definition 8.1.4 *Let x, y be two different colors, i.e., $\{x, y\} \subset \{a, b, c\}$, $x \neq y$. The* alternating path *$A(x, y)$ in* $\mathrm{CR}(k, m)$ *is the (doubly infinite) sequence of vertices $(v_i)_{i \in \mathbb{Z}}$ such that $v_1 = 0$, $\{v_i, v_{i+1}\} \in E(k, m)$ for all i and $C(\{v_{2j-1}, v_{2j}\}) = x$, $C(\{v_{2j}, v_{2j+1}\}) = y$ for all $j \in \mathbb{Z}$.*

The uniqueness of $A(x, y)$ follows easily from the definition of $\mathrm{CR}(k, m)$.

We will now examine the alternating paths algebraically.

1. The path $A_1 := A(b, a)$ obtained by alternating the colors b and a. Let $A_{1,n}$ be the n-th node on this path. We get $A_{1,2i} = \bar{i}$, $A_{1,2i+1} = i$. This is the outer polygon of $\mathrm{CR}(k, m)$.

2. The path $A_2 := A(c, b)$. Here $A_{2,2i} = \overline{i(m-1)+1}$, $A_{2,2i+1} = i(m-1)$ for each i.

3. The path $A_3 := A(c, a)$. Here $A_{3,2i} = \overline{im}$, $A_{3,2i+1} = im$.

We now invite the reader to consult the drawing in Figure 8.3, attach properly the colors a, b and c to the edges in this drawing and examine the segments of the paths A_1, A_2 and A_3 in this drawing.

From the algebraic description it is clear that each of the three paths A_1, A_2 and A_3 consists of a simple cycle which is repeated infinitely many times. The lengths l_1, l_2 and l_3 of these three cycles are even numbers and they all divide $2k$. More precisely,

$$\begin{aligned} l_1 &= 2 \cdot k, \\ l_2 &= 2 \cdot k / \gcd(k, m-1), \\ l_3 &= 2 \cdot k / \gcd(k, m). \end{aligned}$$

Moreover, it is clear that for any two colors x and y, $A(y,x)$ is obtained from $A(x,y)$ by changing the orientation of the path. Since we are dealing with undirected graphs, we can identify $A(y,x)$ with $A(x,y)$ and speak of the (finite) *alternating cycle* instead of the (infinite) alternating path.

Definition 8.1.5 *By C_1, C_2, C_3 we will denote the three alternating cycles obtained from A_1, A_2, A_3, respectively. In Section 8.5 we will speak about the first, second and third alternating cycle, respectively.*

8.2 Motivations

The motivation for the study of chordal rings is twofold:

8.2.1 Combinatorics

Chordal rings were introduced by Coxeter (1950), pp. 426ff. Coxeter himself did not propose any name for $\mathrm{CR}(k,m)$ while Foster later called them "graphs of equal-chord type". Coxeter (1950) pointed out that many chordal rings represent interesting combinatorial objects, for example $\mathrm{CR}(7,3)$ which is at the same time the (3,6)-cage (smallest cubic graph of girth 6) and the point-line graph (Levi graph) of Fano's plane $PG(2,2)$.

8.2.2 Distributed Computing

Independently, chordal rings have enjoyed much attention in the context of distributed computing. Arden and Lee (1981) showed that with a suitable choice of m, the diameter of $\mathrm{CR}(k,m)$ is $O(\sqrt{k})$, yielding a design for dense processor (workstation) interconnection networks. The past decade has seen as many as several dozens of articles examining other aspects of chordal ring architectures (such as reliability) and generalizing chordal rings in various directions.

8.3 Problem Statement

Before stating the problem exactly, we note:

Fact 8.3.1 *We have* $\mathrm{CR}(k,m) \simeq \mathrm{CR}(k,k+1-m)$.

Proof. The mapping $I : V(k,m) \to V(k,k+1-m)$

$$I: \quad \begin{array}{l} (k,m,i) \mapsto (k,k+1-m,\overline{i+1}) \\ (k,m,\bar{i}) \mapsto (k,k+1-m,i) \end{array}$$

provides the isomorphism. □

Hence, we will restrict our attention to the following values of m:

$$2 \le m \le \left\lfloor \frac{k+1}{2} \right\rfloor . \tag{8.1}$$

With respect to Fact 8.3.1 it makes sense to introduce the following definition:

Definition 8.3.2 *For each* $2 \le m \le k-1$ *we define its* normalized value

$$\mathrm{norm}(m) := \min\{m, k+1-m\}.$$

We will use the function "norm" in Sections 8.5 and 8.6.

The inequality (8.1) still does not ensure that the graphs are pairwise non-isomorphic. We can illustrate this with the example of graphs $\mathrm{CR}(9,3)$ and $\mathrm{CR}(9,4)$, see Figures 8.1 and 8.2. We invite the reader to prove that these two chordal rings are isomorphic.

For any fixed positive integer $k \ge 3$, *we will address the problem of determining the isomorphism classes of* $\mathrm{CR}(k,m)$ $(2 \le m \le \lfloor (k+1)/2 \rfloor)$ *as* classification of chordal rings.

Frucht (1976) writes about this problem: "An easy answer can be given only for $k = p$ (prime)." The paper by Boreham, Bouwer and Frucht (1974) contains the classification for k prime, and announces a paper by Foster that will treat the general case. However, according to R. Frucht (personal communication, April 1993) the second paper never appeared.

With the modern computing devices and appropriate software ("practical graph isomorphism", see Section 6.4.1) it is possible to approach the classification problem computationally for values $k \le 500$ or so. Interestingly, the results reveal highly regular patterns also for

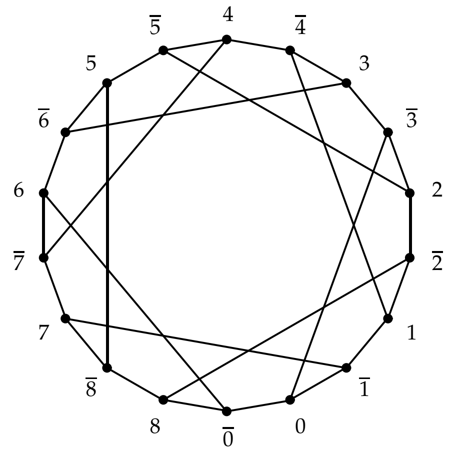


Figure 8.1: CR$(9, 3)$

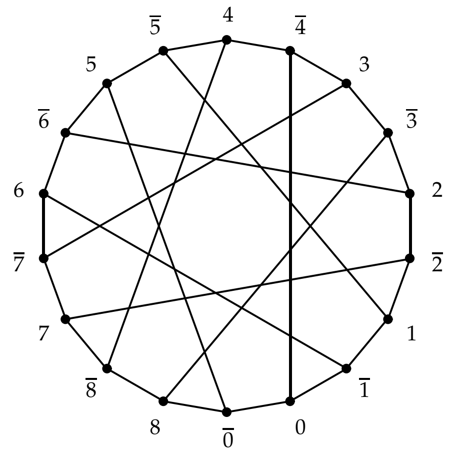


Figure 8.2: CR$(9, 4)$

non-prime values of k. Based on, but independent of the computational experience, we prove rigorous theorems that allow us to theoretically solve the classification problem for wider ranges of the parameter k. In Section 8.6.2, we give as an example the full classification for values $k = 2^e p$ where e is a positive integer and p an odd prime, and we explain that also classifications for other families of k can be obtained easily.

8.4 Initial Results

Fact 8.4.1 *For each k and m, the graph $\mathrm{CR}(k,m)$ is vertex-transitive, i.e., $\mathrm{Aut}(\mathrm{CR}(k,m))$ acts transitively on the set of vertices of $\mathrm{CR}(k,m)$.*

Proof. The graph $\mathrm{CR}(k,m)$ admits (among others) the following two automorphisms: Cyclic shift of the outer polygon

$$S: \begin{array}{l} i \mapsto i+1 \\ \bar{i} \mapsto \overline{i+1} \end{array}$$

and reflection of the outer polygon

$$R: \begin{array}{l} i \mapsto \overline{k-i} \\ \bar{i} \mapsto k-i. \end{array}$$

The subgroup of $\mathrm{Aut}(\mathrm{CR}(k,m))$ generated by S and R is transitive. Hence is $\mathrm{Aut}(\mathrm{CR}(k,m))$ transitive. □

8.4.1 Local Structure of $\mathrm{CR}(k,m)$

In the following investigations we will often make use of the drawing in Figure 8.3.

Fact 8.4.2 *Let $k \geq 3$ be an integer and m an integer subject to (8.1). If $2 < m < k/2$ then girth of $\mathrm{CR}(k,m)$ is 6.*

Proof. Let T be the shortest cycle in $\mathrm{CR}(k,m)$. By vertex transitivity we may assume that T contains 0. It follows from Figure 8.3 that in the case $3 \leq m < k/2$ there cannot be cycle of length less than 6 while there are cycles of length 6. Hence the girth is 6. □

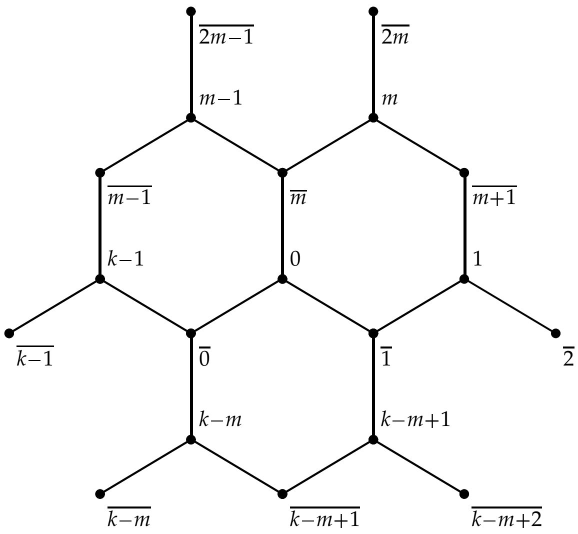


Figure 8.3: Neighborhood of 0 in CR(k, m).

Fact 8.4.3 *Let $k \geq 3$ be an integer and m an integer such that*

$$3 < m < k/3 \quad \text{or} \quad k/3 + 1 < m < (k-1)/2. \tag{8.2}$$

Then each edge of CR(k, m) *belongs to exactly two hexagons (cycles of length 6).*

Proof. Let e be the edge in question. By vertex transitivity we may assume that one of the endpoints of e is 0. If m is as in (8.2) then all 19 vertices in Figure 8.3 are pairwise different. Obviously, each edge incident with 0 belongs to exactly two hexagons. □

Definition 8.4.4 *Let e_1, e_2 be two adjacent edges in* CR(k, m) *with m subject to (8.2). The* Petrie path $P(e_1, e_2)$ *is defined as the (doubly infinite) path containing e_1, e_2 as consecutive edges, such that no three consecutive edges belong to the same hexagon.*

From Fact 8.4.3 it follows readily that the definition is sound. Moreover, it is clear that each Petrie path consists of a simple cycle which is repeated infinitely many times and that these simple cycles are identical with alternating cycles.

8.4.2 Singular Cases

In order to solve the classification problem, we will make much use of the alternating cycles. In the preceding section we saw that if m is as in (8.2) then the alternating cycles have a very natural description using incidence with hexagons. The cases not covered by (8.2) will be called "singular" since the local structure of $\mathrm{CR}(k, m)$ is different from the general pattern exhibited in Figure 8.3.

Fact 8.4.5 *Let $k \geq 3$ be a positive integer and m an integer subject to (8.1). If $m \in \{2,\ k/2,\ (k+1)/2\}$ then girth of $\mathrm{CR}(k, m)$ is 4.*

Proof. Clearly is $\mathrm{CR}(k, m)$ triangle-free for each m. Vertices (in shortened notation) forming the cycles of length four are, for example,

$\overline{0},\ 0,\ \overline{1},\ k-1,\ \overline{0}$	in $\mathrm{CR}(k, 2)$,
$\overline{0},\ 0,\ \overline{k/2},\ k/2,\ \overline{0}$	in $\mathrm{CR}(k, k/2)$,
$\overline{0},\ 0,\ \overline{(k+1)/2},\ (k-1)/2,\ \overline{0}$	in $\mathrm{CR}(k, (k+1)/2)$.

The local structure of these three graphs is shown in Figures 8.4 to 8.6. $\square$

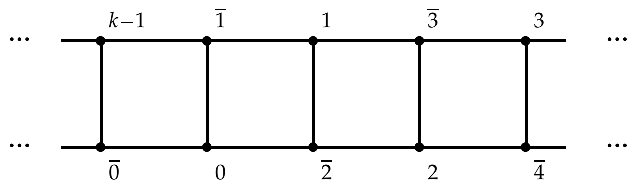


Figure 8.4: $\mathrm{CR}(k, 2)$

Lemma 8.4.6 *If k is odd then* $\mathrm{CR}(k, 2) \simeq \mathrm{CR}(k, (k+1)/2)$. *If k is even then* $\mathrm{CR}(k, 2) \not\simeq \mathrm{CR}(k, k/2)$.

Proof. Let k be odd. The isomorphism I between $\mathrm{CR}(k, 2)$ and $\mathrm{CR}(k, (k+1)/2)$ is given by

$$
\begin{array}{lll}
I: & (k, 2, i) \mapsto (k, (k+1)/2, i/2), & i \text{ even} \\
 & (k, 2, \overline{i}) \mapsto (k, (k+1)/2, \overline{i/2}), & i \text{ even} \\
 & (k, 2, i) \mapsto (k, (k+1)/2, (k+i)/2), & i \text{ odd} \\
 & (k, 2, \overline{i}) \mapsto (k, (k+1)/2, \overline{(k+i)/2}), & i \text{ odd.}
\end{array}
$$

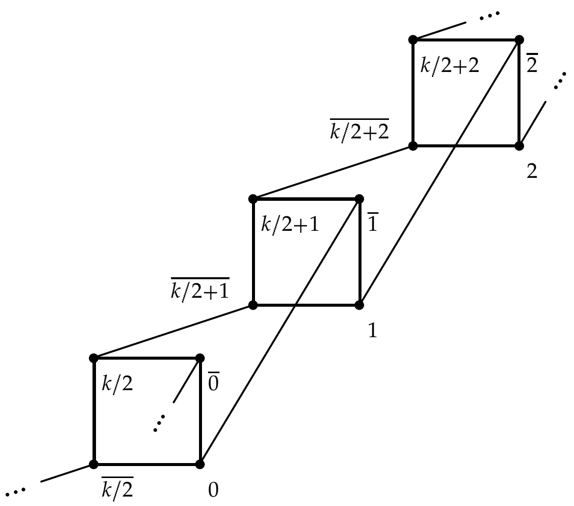


Figure 8.5: $\mathrm{CR}(k, k/2)$

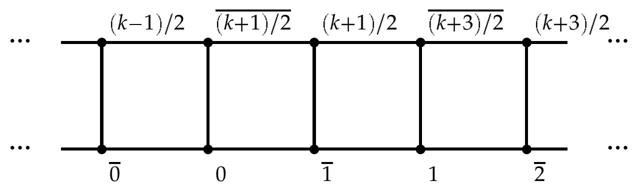


Figure 8.6: $\mathrm{CR}(k, (k+1)/2)$

We note that I is color-faithful.

Next we show $\mathrm{CR}(k,2) \not\simeq \mathrm{CR}(k,k/2)$ for k even. To this end, observe that for any fixed vertex $v \in V(k,2)$ there are exactly four vertices at distance 2 from v in $\mathrm{CR}(k,2)$ whereas for any fixed vertex $w \in V(k,k/2)$, there are exactly five vertices at distance 2 from w in $\mathrm{CR}(k,k/2)$. Obviously the graphs cannot be isomorphic. □

In the following proofs we will be constructing isomorphisms between various chordal rings. In order to ensure the bijectivity of these isomorphisms we note this simple fact:

Lemma 8.4.7 *Let $k \in \mathbb{N}^+$, $c,d \in \mathbb{Z}$ and consider the mapping $h : \mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ defined by $h : i \mapsto c \cdot i + d$. If $\gcd(k,c) = 1$ then h is a bijection.*

Proof. We show that h is injective: Let i_1, i_2 be representatives of two residue classes and suppose $h(i_1) = h(i_2)$. By definition of h we have $k \mid c \cdot (i_1 - i_2)$. Since $\gcd(k,c) = 1$, k must divide $i_1 - i_2$. Hence, i_1 and i_2 are representatives of the same class and h is injective. Since the domain and the codomain of h have the same cardinality, the surjectivity of h follows from its injectivity. Hence, h is a bijection. □

Using the last lemma, one can prove the bijectivity of all graph isomorphisms (defined as mappings between vertex sets) that appear in the subsequent proofs. (Checking the property $\gcd(k,c) = 1$ amounts in all cases to just one or two iterations of the Euclidean algorithm.) To show that these mappings also preserve incidence of vertices one has to consult the definition of $\mathrm{CR}(k,m)$ and do some easy computations modulo k. As by-products of these computations one obtains proofs of the color-faithfulness of the respective isomorphisms.

Lemma 8.4.8 *If k is not divisible by 3 then* $\mathrm{CR}(k,3) \simeq \mathrm{CR}(k, \lfloor (k+2)/3 \rfloor)$.

Proof. Let $k \equiv 1 \pmod 3$. The bijection $I : V(k,3) \to V(k,(k+2)/3)$

$$I : \begin{array}{l} (k,3,i) \mapsto (k,(k+2)/3, i(k-1)/3) \\ (k,3,\bar{i}) \mapsto (k,(k+2)/3, \overline{i(k-1)/3+1}) \end{array}$$

is an isomorphism.

If $k \equiv 2 \pmod 3$ then the bijection $I : V(k,3) \to V(k,(k+1)/3)$

$$I: \quad \begin{array}{l}(k,3,i) \mapsto (k,(k+1)/3, i(k+1)/3) \\ (k,3,\bar{i}) \mapsto (k,(k+1)/3, \overline{i(k+1)/3})\end{array}$$

is an isomorphism.

In both cases is the mapping I color-faithful. $\square$

Lemma 8.4.9 *If k is odd then* $\mathrm{CR}(k,3) \simeq \mathrm{CR}(k,(k-1)/2)$.

Proof. The bijection $I : V(k,3) \to V(k,(k-1)/2)$

$$I: \quad \begin{array}{l}(k,3,i) \mapsto (k,(k-1)/2, -i(k-1)/2) \\ (k,3,\bar{i}) \mapsto (k,(k-1)/2, \overline{(1-i)(k-1)/2})\end{array}$$

is an isomorphism. Also here is I color-faithful. $\square$

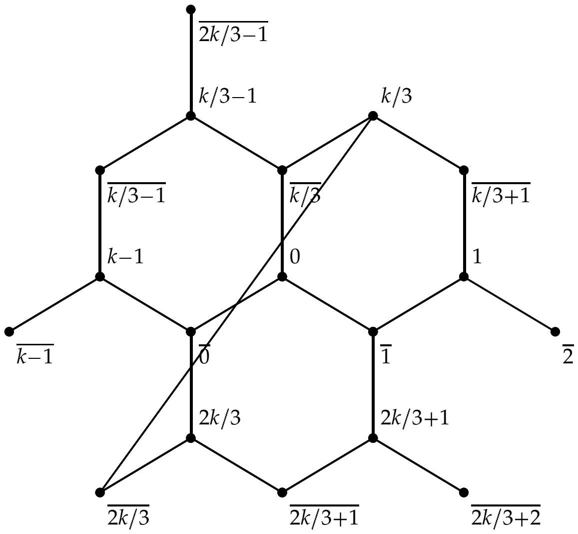


Figure 8.7: Neighborhood of 0 in $\mathrm{CR}(k,k/3)$.

Lemma 8.4.10 *Let m be a positive integer greater than 3. Let v be any vertex of* $\mathrm{CR}(3m,m)$ *and denote S_v the stabilizer of v in* $\mathrm{Aut}(\mathrm{CR}(3m,m))$. *The group S_v is non-trivial if and only if $m \equiv -1 \pmod 3$.*

Proof. Due to vertex transitivity we can assume w.l.o.g. that $v = 0$. We have $k = 3m$.

First we observe that if $k/3 \equiv -1 \pmod 3$ then the mapping $A : V(k, k/3) \to V(k, k/3)$ given by the equations

$$A(i) = i(2k/3 + 1) \qquad \text{and} \qquad A(\bar{i}) = \overline{i(2k/3 + 1) + k/3}$$

is a non-trivial automorphism of $\mathrm{CR}(k, k/3)$ such that $A(0) = 0$. A is color-faithful.

We will prove by contradiction that no non-trivial automorphism stabilizing 0 exists if $k/3 \not\equiv -1 \pmod 3$.

Suppose that A is such an automorphism. We will use the drawing in Figure 8.7. We invite the reader to check that in the graph $\mathrm{CR}(k, k/3)$, each edge $\{i, \overline{i+1}\}$ belongs to exactly two hexagons while each other edge belongs to exactly three hexagons. Hence, the set of $\{i, \overline{i+1}\}$-edges must be mapped onto itself by A. This means $A(\overline{1}) = \overline{1}$ because $A(0) = 0$ by assumption. The further discussion will be split into two cases.

(i) $A(\overline{0}) = \overline{0}$, $A(\overline{k/3}) = \overline{k/3}$. This implies $A(\overline{k/3+1}) = \overline{k/3+1}$, $A(1) = 1$ and $A(\overline{2}) = \overline{2}$ where the later statements follow from the earlier ones (and from the assumptions). We can repeat the argument to show $A(i) = i$ and $A(\bar{i}) = \bar{i}$ for all i. Hence, A is the trivial automorphism.

(ii) $A(\overline{0}) = \overline{k/3}$, $A(\overline{k/3}) = \overline{0}$. We will use the abbreviation $x \leftrightarrow^A y$ to denote $A(x) = y$, $A(y) = x$. We derive

$\overline{k/3+1} \leftrightarrow^A \overline{2k/3+1}$,
$k/3 \leftrightarrow^A 2k/3$,
$1 \leftrightarrow^A 2k/3+1$,
$\overline{2} \leftrightarrow^A \overline{2k/3+2}$ and
$A(2k/3+2) = 2k/3+2$

where again the later statements follow from the earlier ones (and from the assumptions).

We can now consider the neighborhood of $2k/3 + 2$ instead of that of 0 by merely adding $2k/3 + 2$ to all vertices. By repeating the process we prove that all vertices of the form $t(2k/3 + 2)$ for some integer $t \geq 0$ are fixed by A.

Since $\gcd(k, 2k/3 + 2) = \gcd(6, k/3 - 2)$ and $3 \not| (k/3 - 2)$ by assumption, we have $\gcd(k, 2k/3 + 2) = 1$ (k odd) or $\gcd(k, 2k/3 + 2) = 2$

(k even). In both cases the congruence $t(2k/3+2) \equiv k/3 \pmod{k}$ is solvable. Hence, the vertex $k/3$ is fixed by A, a contradiction to $k/3 \leftrightarrow^A 2k/3$. $\square$

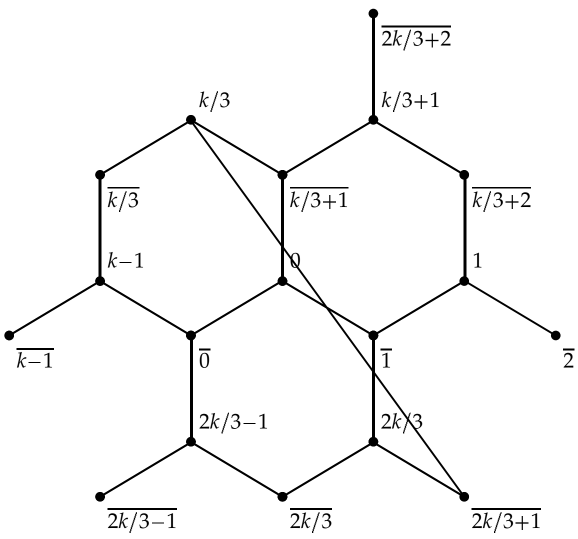


Figure 8.8: Neighborhood of 0 in $\mathrm{CR}(k, k/3+1)$.

Lemma 8.4.11 *Let l be a positive integer greater than 2. Let v be a vertex of $\mathrm{CR}(3l, l+1)$ and denote S_v the stabilizer of v in $\mathrm{Aut}(\mathrm{CR}(3l, l+1))$. The group S_v is non-trivial if and only if $l \equiv 1 \pmod{3}$.*

Proof. The reasoning is very analogous to that in the previous proof.

Now $k = 3l$, $m = l+1$. First we note that if $k/3 \equiv 1 \pmod{3}$ then the mapping A defined by

$$A(i) = i(k/3+1) \qquad \text{and} \qquad A(\bar{i}) = \overline{i(k/3+1)}$$

is a non-trivial automorphism of $\mathrm{CR}(3l, l+1)$ stabilizing 0. Also this mapping is color-faithful.

We will prove by contradiction that no non-trivial automorphism stabilizing 0 exists if $k/3 \not\equiv 1 \pmod{3}$.

Suppose that A is such an automorphism. Guided by the drawing in Figure 8.8 we can easily prove that in the graph $\mathrm{CR}(k, k/3+1)$, each edge $\{i, \bar{i}\}$ belongs to exactly two hexagons while each other edge belongs to exactly three hexagons. Hence, the set of $\{i, \bar{i}\}$-edges must be mapped onto itself by A. This means $A(\overline{0}) = \overline{0}$. The further discussion will be again split into two cases.

(i) $A(\overline{1}) = \overline{1}$, $A(\overline{k/3+1}) = \overline{k/3+1}$. As in the previous proof we derive that A must be the trivial automorphism.

(ii) $\overline{1} \;\leftrightarrow^A\; \overline{k/3+1}$. We derive

$\overline{k/3} \;\leftrightarrow^A\; \overline{2k/3}$,
$k/3 \;\leftrightarrow^A\; 2k/3$,
$k-1 \;\leftrightarrow^A\; 2k/3-1$,
$\overline{k-1} \;\leftrightarrow^A\; \overline{2k/3-1}$ and
$A(2k/3-2) = 2k/3-2$

where again the later statements follow from the earlier ones (and from the assumptions).

Hence, all vertices of the form $t(2k/3-2)$ for some integer $t \geq 0$ are fixed by A.

Since $\gcd(k, 2k/3-2) = \gcd(6, k/3+2)$ and $3 \nmid (k/3+2)$ by assumption, we have $\gcd(k, 2k/3-2) = 1$ (k odd) or $\gcd(k, 2k/3-2) = 2$ (k even). In both cases the congruence $t(2k/3-2) \equiv k/3 \pmod{k}$ is solvable. Hence, the vertex $k/3$ is fixed by A, a contradiction to $k/3 \;\leftrightarrow^A\; 2k/3$. □

Lemma 8.4.12 *If $k > 9$, k is divisible by 3 and not divisible by 9 then* $\mathrm{CR}(k, k/3) \not\simeq \mathrm{CR}(k, k/3+1)$.

Proof. Suppose $k > 9$, $3 \mid k$, $9 \nmid k$, $\mathrm{CR}(k, k/3) \simeq \mathrm{CR}(k, k/3+1)$. The isomorphism between $\mathrm{CR}(k, k/3)$ and $\mathrm{CR}(k, k/3+1)$ would naturally induce an isomorphism between the groups $\mathrm{Aut}(\mathrm{CR}(k, k/3))$ and $\mathrm{Aut}(\mathrm{CR}(k, k/3+1))$.

Let $m = k/3$. Since $9 \nmid k$, we have $m \equiv \pm 1 \pmod{3}$. In either case we obtain $\mathrm{Aut}(\mathrm{CR}(k, k/3)) \not\simeq \mathrm{Aut}(\mathrm{CR}(k, k/3+1))$ from conjunction of Lemmas 8.4.10 and 8.4.11. This is a contradiction. □

Lemma 8.4.13 *If k is divisible by 9 then* $\mathrm{CR}(k, k/3) \simeq \mathrm{CR}(k, k/3+1)$.

Proof. If $3 \mid k/3$ then the bijection $I : V(k, k/3) \to V(k, k/3+1)$

$$\begin{aligned} I : \quad & (k, k/3, i) \mapsto (k, k/3+1, -(i+1)(k/3+1)) \\ & (k, k/3, \bar{i}) \mapsto (k, k/3+1, \overline{-i(k/3+1)}) \end{aligned}$$

is a color-faithful isomorphism. □

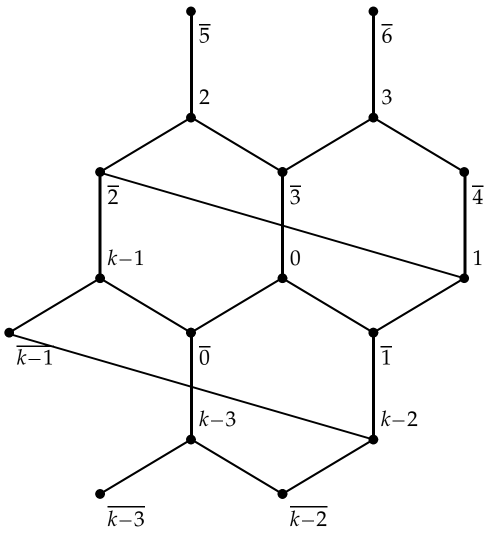


Figure 8.9: Neighborhood of 0 in $\mathrm{CR}(k, 3)$.

Lemma 8.4.14 *If k is divisible by 3, $k > 9$, then* $\mathrm{CR}(k, 3) \not\simeq \mathrm{CR}(k, k/3)$.

Proof. If $k > 9$ then all vertices in Figure 8.9 are pairwise different. For any fixed vertex $v \in V(k, 3)$ there are exactly seven vertices at distance 3 from v in $\mathrm{CR}(k, 3)$ whereas for any fixed vertex $w \in V(k, k/3)$, there are exactly eight vertices at distance 3 from w in $\mathrm{CR}(k, k/3)$. Obviously the graphs cannot be isomorphic. □

Lemma 8.4.15 *If k is divisible by 3, $k > 9$, then* $\mathrm{CR}(k, 3) \not\simeq \mathrm{CR}(k, k/3+1)$.

Proof. The argument is the same as in the proof of the preceding lemma. □

8.5 Alternating Cycles and Isomorphism

Lemma 8.5.1 *Let* $2 \leq m_1, m_2 \leq (k+1)/2$ *and let* $\mathrm{CR}(k, m_1) \simeq \mathrm{CR}(k, m_2)$. *Let* C'_1, C'_2 *and* C'_3 *be the three alternating cycles incident with* $(k, m_1, 0)$ *and let* C''_1, C''_2 *and* C''_3 *be the three alternating cycles incident with* $(k, m_2, 0)$. *Then there exists an isomorphism* $I : V(k, m_1) \to V(k, m_2)$ *and a permutation* $\pi : \{1, 2, 3\} \to \{1, 2, 3\}$ *such that* $I(C'_i) = C''_{\pi(i)}$ *(as graphs) for* $i = 1, 2, 3$.

Proof. The lemma says that if two chordal rings are isomorphic then there must be an isomorphism that maps the alternating cycles of the first chordal ring on the alternating cycles of the second chordal ring.

For m_1 subject to (8.2) this follows from the fact that *each* isomorphism must map Petrie cycles on Petrie cycles. For the remaining ("singular") values of m_1 this follows from the statements of Section 8.4.2 where we proved that whenever the graphs are isomorphic, there is a color-faithful isomorphism. Obviously, a color-faithful isomorphism maps an alternating cycle onto an alternating cycle. □

Next we will show that the pairwise correspondence of alternating cycles in chordal rings $\mathrm{CR}(k, m_1)$ and $\mathrm{CR}(k, m_2)$ provides a strong information concerning the values of m_1 and m_2.

Fact 8.5.2 *Let* $2 \leq m_1, m_2 \leq k - 1$ *be integers. Let* $\mathrm{CR}(k, m_1) \simeq \mathrm{CR}(k, m_2)$ *and let* $I : V(k, m_1) \to V(k, m_2)$ *be an isomorphism. Let* C'_1 *(respectively,* C''_1*) be the first alternating cycle in* $\mathrm{CR}(k, m_1)$ *(respectively,* $\mathrm{CR}(k, m_2)$*). If* $I(C'_1) = C''_1$ *(as graphs) then* $m_1 = m_2$ *or* $m_1 = k + 1 - m_2$.

Proof. Suppose $I(C'_1) = C''_1$. By vertex transitivity we may assume that $I(k, m_1, 0) = (k, m_2, 0)$. Then either $I(k, m_1, 1) = (k, m_2, 1)$ or $I(k, m_1, 1) = (k, m_2, \overline{0})$. One sees easily that the first case necessarily leads to $m_2 = m_1$ while in the second case $m_2 = k + 1 - m_1$ must hold. □

Lemma 8.5.3 *Let* $2 \leq m_1, m_2 \leq (k+1)/2$ *with* $m_1 \neq m_2$. *Then* $\mathrm{CR}(k, m_1) \simeq \mathrm{CR}(k, m_2)$ *if and only if at least one of the following cases occurs:*

(i) *k and $m_1 - 1$ are relatively prime and* $m_2 = \mathrm{norm}(s)$ *for an s such that* $s(m_1 - 1) \equiv -1 \pmod{k}$.

(ii) *k and m_1 are relatively prime and* $m_2 = \mathrm{norm}(t)$ *for a t such that* $tm_1 \equiv 1 \pmod{k}$.

Proof.

(A) The part "$\Rightarrow$":

Let $I : V(k, m_1) \to V(k, m_2)$ be an isomorphism. By vertex transitivity we may assume $I(k, m_1, 0) = (k, m_2, 0)$.

Let the notation for alternating cycles and alternating paths be as introduced in Section 8.1.1 and let C'_i and A'_i be the cycles (paths) in $\mathrm{CR}(k, m_1)$ while C''_i and A''_i are the cycles (paths) in $\mathrm{CR}(k, m_2)$. By Fact 8.5.2, $I(C'_1) \neq C''_1$. However, I must map alternating cycles to alternating cycles, hence either *(i)* $I(C'_2) = C''_1$ or *(ii)* $I(C'_3) = C''_1$.

Ad (i): The length of C'_2 in $\mathrm{CR}(k, m_1)$ must be $2k$, hence $\gcd(k, m_1 - 1) = 1$ (see the algebraic description of alternating paths). Moreover, $I(k, m_1, \overline{m}) = (k, m_2, \overline{1})$ or $I(k, m_1, \overline{m}) = (k, m_2, \overline{0})$. In the first case we must have $I(k, m_1, \overline{0}) = (k, m_2, \overline{m_2})$, the latter being $A''_{1,2m_2}$, hence $A'_{2,2m_2} = \overline{0}$. By algebraic description of A_2, $A_{2,2m_2} = \overline{m_2(m_1 - 1) + 1}$ and we are left with the congruence

$$m_2(m_1 - 1) + 1 \equiv 0 \pmod{k}. \tag{8.3}$$

If $I(k, m_1, \overline{m}) = (k, m_2, \overline{0})$, then we again derive $I(k, m_1, \overline{0}) = (k, m_2, \overline{m_2})$, the latter being now $A_{1,2(k+1-m_2)}$ (now we run through A_2 and A_1 in different directions). This leads to the congruence

$$(k + 1 - m_2)(m_1 - 1) + 1 \equiv 0 \pmod{k}. \tag{8.4}$$

Since we suppose $2 \leq m_2 \leq (k+1)/2$, indeed $m_2 = \mathrm{norm}(s)$ where $s(m_1 - 1) + 1 \equiv 0 \pmod{k}$.

Ad (ii): The length of A_3 in $\mathrm{CR}(k, m_1)$ must be $2k$, hence $\gcd(k, m_1) = 1$ (see the algebraic description of alternating paths). The desired result for m_2 follows from algebraic description of A_3 in a manner similar to the case *(i)*.

(B) The part "$\Leftarrow$":

Suppose that *(i)* holds, i.e., k and $m_1 - 1$ are relatively prime and one of the congruences (8.3), (8.4) is fulfilled. If (8.3) holds, then we construct the mapping $I : V(k, m_1) \to V(k, m_2)$ via alternating paths $I(k, m_1, \overline{i}) = A''_{2,2i}$ and $I(k, m_1, i) = A''_{2,2i+1}$ and we check easily that this mapping is an isomorphism. If (8.4) holds, then the same construction works, taking the path A_2 in the opposite order.

The case *(ii)* is treated analogously. □

The graph-theoretical classification problem has now been to a great extent transformed in a number-theoretical problem (solving congruences). In order to support further investigations we need some statements about polynomial congruences.

8.5.1 Solving the Congruences

Lemma 8.5.4 (i) *If $e \geq 3$ is an integer, then $x^2 \equiv 1 \pmod{2^e}$ has exactly four solutions $1, 2^{e-1}-1, 2^{e-1}+1, 2^e-1$.*

(ii) *If p is a prime greater than 2 and e is a positive integer, then $x^2 \equiv 1 \pmod{p^e}$ has exactly two solutions $1, p^e - 1$.*

Proof. (i) The statement is true for $e = 3$. Suppose it is true for some $e \geq 3$. The induction step is done easily by a direct application of material in Section 8.3 of (Hardy, Wright, 1990).

(ii) If p is an odd prime, then $x^2 \equiv 1 \pmod{p}$ has exactly two solutions (i.e., 1 and -1) by Theorem 109 of (Hardy, Wright, 1990). The induction step again follows directly from Section 8.3 of (Hardy, Wright, 1990). □

Lemma 8.5.5 (i) *If e is a positive integer, then $x(x-1) \equiv -1 \pmod{2^e}$ has no solutions.*

(ii) *If e is a positive integer greater than 1, then $x(x-1) \equiv -1 (\mathrm{mod}\, 3^e)$ has no solutions.*

(iii) *If p is a prime, $p \equiv 1 \pmod{6}$ and e a positive integer, then $x(x-1) \equiv -1 \pmod{p^e}$ has exactly two solutions.*

(iv) *If p is a prime, $p \equiv -1 \pmod{6}$ and e a positive integer, then $x(x-1) \equiv -1 \pmod{p^e}$ has no solutions.*

Proof. (i) The congruence $x(x-1)+1 \equiv 0 \pmod{2}$ has no solutions. Hence, $x(x-1)+1 \equiv 0 \pmod{2^e}$ has no solutions for any $e \geq 1$.

(ii) The congruence $x(x-1)+1 \equiv 0 \pmod{3^2}$ has no solutions. It follows that $x(x-1)+1 \equiv 0 \pmod{3^e}$ has no solutions for any $e \geq 2$.

(iii) Proof by induction: For $e = 1$ the statement follows from observing that for any odd prime p,

$$x^2 - x \equiv -1 \pmod{p}$$

is equivalent to

$$(2x-1)^2 \equiv -3 \pmod{p}$$

and from Theorem 96 of (Hardy, Wright, 1990). The induction step again easily follows from the theory in Section 8.3 of (Hardy, Wright, 1990).

(iv) For $e = 1$ the proof goes like in *(iii)*. Since there are no solutions $\pmod{p}$, there can be no solutions $\pmod{p^e}$, $e \geq 1$. □

Fact 8.5.6 *Let $m = \prod_{i=1}^{t} p_i^{e_i}$ where p_i are pairwise different primes and e_i are positive integers. Let c be an integer and let $c_i = c \bmod p_i^{e_i}$ for each $1 \leq i \leq t$. Let the congruence $f(x) \equiv c_i \pmod{p_i^{e_i}}$ has s_i solutions for each $1 \leq i \leq t$. Then the number of solutions of $f(x) \equiv c \pmod{m}$ is equal to $\prod_{i=1}^{t} s_i$.*

Proof. This is a consequence of the Chinese Remainder Theorem. See (Hardy, Wright, 1990), Theorems 121 and 122. □

8.6 Classifications

We have now collected all necessary knowledge to efficiently handle the classification problem stated in Section 8.3.

Fact 8.6.1 *Let $k \geq 3$ is an integer and consider the isomorphism classes of graphs $\mathrm{CR}(k, m)$, $2 \leq m \leq (k+1)/2$. Each such class consists of at most 3 graphs.*

Proof. Let m_0 be an integer with $2 \leq m_0 \leq (k+1)/2$. By Lemma 8.5.3 there can be at most two chordal rings $\mathrm{CR}(k, m)$, $2 \leq m \leq (k+1)/2$, $m \neq m_0$, that are isomorphic to $\mathrm{CR}(k, m_0)$. This follows from the fact that either of the congruences in Lemma 8.5.3 has none or one solution. □

For the sake of completeness we briefly recall the classification in the case k prime, as derived in (Boreham, Bouwer and Frucht, 1974). In this case, for any $2 \leq m \leq p-1$ we have $\gcd(p, m-1) = \gcd(p, m) = 1$. Hence, by Lemma 8.5.3, we may have isomorphic triples of graphs.

8.6.1 The Case $k = p$

Fact 8.6.2 *Let p be a prime greater than 7 and let m be an integer, $3 < m < (p-1)/2$, $m \neq \lfloor (p+2)/3 \rfloor$. Let s, t be integers such that $s(m-1) \equiv -1 \pmod p$ and $tm \equiv 1 \pmod p$. Then the three numbers* $\text{norm}(m)$, $\text{norm}(s)$ *and* $\text{norm}(t)$ *are either all equal or pairwise different. Moreover, there is at most one value $3 < z < (p-1)/2$ such that $z = \text{norm}(m) = \text{norm}(s) = \text{norm}(t)$, and it occurs if and only if $p \equiv 1 \pmod 6$.*

Proof. (Boreham, Bouwer and Frucht, 1974), pp. 220–221. □

This fact completes the classification of isomorphism types in the case p prime, see Table 8.1 for a global scheme. (For more details, see the aforementioned reference.)

number of types	description of types (values of m)	remarks
1	$\{2,\ (p+1)/2\}$	
1	$\{3,\ \lfloor (p+2)/3 \rfloor,\ (p-1)/2\}$	
$\lfloor p/6 \rfloor - 1$	$\{\text{norm}(m), \text{norm}(s), \text{norm}(t)\}$	one singleton if $p \equiv 1 \pmod 6$

Table 8.1: Isomorphism types of $\text{CR}(p, m)$, p prime > 7

8.6.2 The Case $k = 2^e p$

Now let $k = 2^e p$ where e is a positive integer and p is an odd prime.

Lemma 8.6.3 *Let $k = 2^e p$ where e is a positive integer and p is an odd prime and consider the isomorphism classes of graphs* $\text{CR}(k, m)$ *where m is as in (8.1), i.e., $2 \leq m \leq 2^{e-1} p$. Each such class consists of one or two graphs. The one-graph classes will be called singletons. There are exactly*

2 singletons	*if $e = 1$,*
5 singletons	*if $e = 2$,*
$2^{e-1} + 7$ *singletons*	*if $e \geq 3$.*

Proof. It follows from Fact 8.6.1 and Lemma 8.5.3 that a three member class can occur only if $\gcd(k, m-1) = \gcd(k, m) = 1$ for some m. This clearly cannot be the case if k is even.

Now we determine the number of singletons. If $\{\mathrm{CR}(k, m)\}$ is a singleton then according to Lemma 8.5.3 the following two conditions must hold *simultaneously:*

(i) $\gcd(2^e p, m-1) > 1$ or the solution of $x(m-1) \equiv -1 \pmod{2^e p}$ satisfies $\mathrm{norm}(x) = m$

and

(ii) $\gcd(2^e p, m) > 1$ or the solution of $xm \equiv 1 \pmod{2^e p}$ satisfies $\mathrm{norm}(x) = m$.

These conditions can be rewritten as

$$\begin{aligned} (i) \quad &\iff \quad 2 \mid m-1 \;\vee\; p \mid m-1 \;\vee\; m(m-1) \equiv -1 \pmod{2^e p} \\ & \qquad\quad \vee\; (2^e p + 1 - m)(m-1) \equiv -1 \pmod{2^e p} \end{aligned}$$

$$\begin{aligned} (ii) \quad &\iff \quad 2 \mid m \;\vee\; p \mid m \;\vee\; m^2 \equiv 1 \pmod{2^e p} \\ & \qquad\quad \vee\; (2^e p + 1 - m)m \equiv 1 \pmod{2^e p}. \end{aligned}$$

This can be further simplified to

$$(i) \quad \iff \quad 2 \mid m-1 \;\vee\; p \mid m-1 \;\vee\; (m-1)^2 \equiv 1 \pmod{2^e p}$$

$$(ii) \quad \iff \quad 2 \mid m \;\vee\; p \mid m \;\vee\; m^2 \equiv 1 \pmod{2^e p}.$$

In the last two equivalences, we will denote the subformulas on the right-hand sides by *(ia)*, *(ib)*, *(ic)* and *(iia)*, *(iib)*, *(iic)*, respectively.

Taking into account what was said about solutions of congruences, we find that only the following four combinations can lead to an m satisfying $(i) \wedge (ii)$:

$(ia) \wedge (iib)$: Here m must be of the form $o \cdot p$ where o is an odd number $\leq 2^{e-1}$.

$(ib) \wedge (iia)$: Here m must be of the form $o \cdot p + 1$ where o is an odd number $< 2^{e-1}$.

(ic): it implies (iia).

(iic): it implies (ia).

Further we note that no m can satisfy more than one of these four combinations and that the solutions m of (ic) satisfying $m \leq 2^{e-1}p$ are in a one-to-one correspondence with solutions m' of (iic) satisfying

$m' > 2^{e-1}p$ via $m = \mathrm{norm}(m')$. Hence, we can discard (ic) by considering (iic) on the "doubled" interval $2 \le m \le 2^e p - 1$ and taking norms of the solutions. Finally we note that the solution $m = 1$ of (iic) does not lead to a chordal ring, see the definition of $\mathrm{CR}(k, m)$.

The rest of the proof will be split according to the value of e.

$e = 1$: *(iic)* has two solutions $m \equiv 1, -1 \pmod{2p}$ whose norms are 1 and 2. This gives us one singleton $(m = 2)$. There is one more singleton with $m = p$ (case $(ia) \wedge (iib)$). There are no more singletons.

$e = 2$: There are $2 \cdot 2 = 4$ solutions of (iic) yielding three singletons after we disregard $m = 1$. Further we have singletons for $m = p$ and $m = p + 1$, giving a total of 5 singletons.

$e \ge 3$: There are $4 \cdot 2 = 8$ solutions of (iic) yielding seven singletons. Further we get 2^{e-2} singletons for $m = o \cdot p$ $(o = 1, 3, \ldots, 2^{e-1} - 1)$, and 2^{e-2} more singletons for $m = o \cdot p + 1$, o as before. This gives a total of $2^{e-1} + 7$ singletons. □

Theorem 8.6.4 *Let $k = 2^e p$ where e is a positive integer and p is an odd prime and consider the isomorphism classes of graphs $\mathrm{CR}(k, m)$ for $2 \le m \le 2^{e-1}p$. The number of these classes is*

$$\begin{array}{ll} (p+1)/2 & \textit{if } e = 1, \\ p + 2 & \textit{if } e = 2, \\ 2^{e-2}(p+1) + 3 & \textit{if } e \ge 3. \end{array}$$

Proof. Lemma 8.6.3 and easy computations. □

8.7 Notes on Other Values of k

Apparently, the classification problem can be decided for many other families of the parameter k in a similar fashion. In general, simple formulas like those of Theorem 8.6.4 should exist whenever k contains at least one of the factors 2, 3^2 or a prime of the form $6t - 1$ since we do not need to care about the congruence $x(x-1) \equiv -1 \pmod{k}$ in those cases, and the other congruences do not disturb us much as we have seen lately. If k does not contain any of such factors, the additional congruence will mess up the things a little bit but a general answer should still be possible by a proper case distinction.

8.8 Methodological Aspects

It was conjectured by Frucht (1976) that determining the number of chordal ring isomorphism types is difficult if k is not a prime. We begun attacking this problem by using *nauty* package (see Section 6.4.1) to investigate rings of modest size. McKay's code proved to be extremely useful for these computations. The results gave us good hope that simple classifications exist even for composite values of k.

In order to enable the theoretic classification for k composite, we had to extend the theory of (Boreham, Bouwer and Frucht, 1974) in two directions: First, graph-theoretical treatment of issues that do *not* arise for prime k was necessary. Second, statements concerning solvability of congruences developed in (Boreham, Bouwer and Frucht, 1974) had to be proven for cases when the modulus is composite.

Finally, we picked the case $k = 2^e p$ to give an easy example demonstrating how to use this machinery in proving a classification theorem for k composite.

We are completely convinced that if *nauty* were accessible to the authors whose work was mentioned earlier, much more progress would have been done on the subject in the past two decades. Still, we are pleased that the problem has remained open until now, since it offered us a delicious example how experimental and raw data can inspire proving rigorous theorems of general validity.

Chapter 9

Necklaces and Bracelets

Rotation and reflection belong to the most natural symmetries in the world of discrete structures. Orbits of functions whose domain possesses the rotational symmetry are known as *necklaces*. In this chapter we recall the recent algorithm for generating canonical representatives of necklaces due to Wang and Savage. We will refer to it as the "WS algorithm".

We study the generation problem in the similar setting when, additionally, reflection is allowed. The symmetry then is described by the dihedral group and the arising orbits will be called *bracelets*.

This chapter consists of two closely related parts:

In Sections 9.2 through 9.4 we examine the distribution of bracelets in the necklace tree that is formed by the WS algorithm and we show how this knowledge can be used to develop an algorithm for bracelet generation. After presenting the WS-type algorithms we note their apparent resemblance to orderly-type methods. In Section 9.5 we emphasize this relationship by showing that WS-like algorithms can be modified for the purpose of restricted generation in a fashion similar to restricted orderly generation as we saw it in Section 6.2.2.

In Sections 9.6 through 9.9 we recall an interesting open problem concerning local and global proportionality of the number of black and white beads in two-color necklaces (bracelets). We use our bracelet generation algorithm to obtain examples of bracelets that improve the upper bound on global proportionality for fixed local proportionality. Starting from these examples we derive theorems that simplify and improve the bounds obtained by other authors.

9.1 Definitions

Let n be an arbitrary but fixed positive integer. By $<, \leq$ we mean the lexicographic order on $\{0,1\}^{\underline{n}}$ induced by $0 < 1$. Each function $f \in \{0,1\}^{\underline{n}}$ will be viewed as a string of zeros and ones of length n. This uncommon treatment of functions, which does not appear in other chapters of our thesis, will greatly simplify the description of algorithms that we will be studying and developing.

In this chapter we will often write f_i instead of $f(i)$. Along with a string (function) $f \in \{0,1\}^{\underline{n}}$, $f = f_1 \dots f_n$, we will often consider its substrings $f_i \dots f_j$ for some $i, j \in \underline{n}$. The concatenation of two strings x and y is denoted by simply writing xy. The notation a^k will be used to denote the string consisting of k symbols a ($a = 0, 1$), and $\{0,1\}^k$ will denote the set of all strings of length k over $\{0,1\}$. Hence, in the special case $k = n$ we can now identify $\{0,1\}^{\underline{n}}$ with $\{0,1\}^n$ although we will prefer the former notation.

When describing the listing algorithms we will need various functions from $\{0,1\}^k$ to $\{0,1\}^k$. Some of these functions are permutations (i.e., elements of the acting groups) while some other are not. To avoid the confusion in notation, we will consequently denote the function application by $\alpha(x)$ for any function $\alpha\colon \{0,1\}^k \to \{0,1\}^k$ and any $x \in \{0,1\}^k$. We will use this symbolics no matter whether it refers to group action or not.

Definition 9.1.1 *The* reversal *of* $z = z_1 \dots z_l$ *is* $z^R := z_l \dots z_1$.

Some of the following definitions have appeared already in Section 4.3.1 which deals with counting necklaces and bracelets.

Let $\sigma := (1, n, n-1, \dots, 2) \in S_{\underline{n}}$ and let $\rho \in S_{\underline{n}}$ such that $\rho : i \mapsto n - i$ for all $i \in \underline{n}$. By Definition 2.1.14, $\sigma(z)$ is the left cyclic shift of z and $\rho(z)$ is the reversal of z. The subgroup of $S_{\underline{n}}$ generated by σ has n elements and is called the *cyclic group* $C_{\underline{n}}$. The group generated by σ and ρ is the symmetry group of the regular n-gon and is called the *dihedral group* $D_{\underline{n}}$. This group has $2n$ elements $1, \sigma, \dots, \sigma^{n-1}$ and $\rho, \rho\sigma, \dots, \rho\sigma^{n-1}$. The action of the former elements on $x \in \{0,1\}^{\underline{n}}$ is described by

$$\sigma^t(x_1 \dots x_n) = x_{t+1} \dots x_n x_1 \dots x_t \tag{9.1}$$

while the latter elements are involutions and act as follows:

$$\rho\sigma^t(x_1 \dots x_n) = x_t \dots x_1 x_n \dots x_{t+1}. \tag{9.2}$$

Definition 9.1.2 *The orbits of* $C_{\underline{n}}$ *on* $\{0,1\}^{\underline{n}}$ *will be called* n-bead necklaces (in two colors).

Definition 9.1.3 *For each necklace, we define its* canonical representative *to be the lexicographically smallest element in the orbit.*

Remark. We should emphasize that in the description of the orderly methods (Section 6.2), the lexicographically largest element in each orbit was taken for the canonical representative. On the contrary, in this chapter the lexicographically smallest elements will represent their orbits. The reason for this confusing setting is that we would like to be consistent with the original papers, i.e., with (Read, 1978*a*) and (Ruskey, Savage and Wang, 1992).

Necklaces are models for patterns that are allowed to be rotated but cannot be reflected, such as neckties with parallel strips, some necklace-like accessories or musical chords, see (Gilbert, Riordan, 1961) for the last example.

Definition 9.1.4 *The orbits of $D_{\underline{n}}$ on $\{0,1\}^{\underline{n}}$ will be called n-*bead bracelets *(in two colors).*

Definition 9.1.5 *For each bracelet, we define its* canonical representative *to be the lexicographically smallest element in the orbit.*

It should be stressed that the terms "necklace" and "bracelet" are by no means stable, which often causes confusion. So, for example, Graham, Knuth and Patashnik (1989) use the term "necklace" for $C_{\underline{n}}$–orbits while in (Harary, Palmer, 1973) the same word denotes $D_{\underline{n}}$–orbits. Although some attempts were made to distinguish the names by extra tags ("one-sided necklaces" in (Riordan, 1958)), in our thesis we decided to have a completely different term for the $D_{\underline{n}}$–orbits. This name was suggested to us by Terry Wang (personal communication) and was already used by other authors for the same combinatorial paradigm, for example by Whitworth (1959), p. 20, and by Stockmeyer (1974).

Bracelets are models for objects which can be rotated *and* reflected. For many applications in sciences (Artemi, Alexandru, 1987) the bracelet paradigm is appropriate. Other applications involve twill manufacturing (Hoskins, Penfold Street, 1982) and music (Reiner, 1985). Bracelets certainly deserve as much interest as necklaces do, and Section 9.4 is devoted to an algorithm which lists the canonical representatives of all two-colored bracelets for a given number of beads n.

9.2 Necklace Generation

Algorithms for producing catalogs of necklaces (bracelets) that we discuss in this chapter belong to the class of specialized listing algorithms, see Section 6.4.

Recalling the confusion of $C_{\underline{n}}$– and $D_{\underline{n}}$–actions (see the preceding section), we emphasize that the papers dealing with the "necklace" generation (surveyed in the next paragraph) consider the orbits w.r.t. $C_{\underline{n}}$–action. Early motivation for that task came already in the ancient years of computing from the study of *shift registers* and *de Bruijn sequences*, see (Fredricksen, 1982) for a historical account.

The first algorithm was designed by Fredricksen and Kessler (1986) based on work by Fredricksen and Maiorana (1978). We will refer to it as the "FKM algorithm". Its careful time analysis is due to Ruskey, Savage, and Wang (1992) who showed that FKM generates necklaces in the constant amortized time, i.e., in total time $O(N(n))$ where $N(n)$ is the number of two-colored necklaces of n beads. In this chapter we focus on the recent algorithm due to Wang and Savage (WS algorithm). We restrict our description to the two-color case as it was done in (Ruskey, Savage, and Wang, 1992). For the the details on k colors, i.e., on constructing the transversal of $C_{\underline{n}} \backslash\backslash \{0, 1, \ldots, k-1\}^{\underline{n}}$, see (Wang, Savage, 1990).

9.3 The WS Algorithm

For the sake of brevity, instead of saying "x is the canonical representative of its orbit" we will sometimes say simply "x is canonical". Also, instead of "canonical representative" we will say only "representative".

It will be of some use to keep in mind the following facts about representatives of two-colored necklaces: The only representative ending with a zero is 0^n. The only representative starting with a one is 1^n. If x is canonical and x starts with exactly s zeros then all runs of contiguous zeros inside x have length at most s.

Let $\tau : \{0, 1\}^{\underline{n}} \to \{0, 1\}^{\underline{n}}$ be the involution defined by

$$\tau(x_1 \ldots x_n) := x_1 \ldots x_{n-1}\overline{x_n}$$

where $\overline{x_n} := 1 - x_n$ is the complement of the last bit. We now rephrase the main theorem (Theorem 5) of Ruskey, Savage and Wang (1992) with an alternative proof.

Theorem 9.3.1 *Let $x \in \{0,1\}^{\underline{n}}$, $x = 0z1$ (i.e., $z \in \{0,1\}^{n-2}$). If x is not canonical, then $y := \tau\sigma\tau(x)$ is also not canonical.*

Proof. Suppose x is not canonical while y is canonical. Let

$$x = 0^s x_1 \dots x_{n-s-t-1} 0^t 1$$

with $s > 0$, $t \geq 0$ and $x_1 = x_{n-s-t-1} = 1$. Then

$$y = \tau\sigma\tau(x) = 0^{s-1} x_1 \dots x_{n-s-t-1} 0^{t+1} 1.$$

There is an r, $0 < r < n$, such that $\sigma^r(x)$ is canonical. For this r we have (i) $\sigma^r(x) < x$ and (ii) $\sigma^{r-1}(y) \geq y$. It must be $s < r \leq n-t-1$ for otherwise $\sigma^r(x)$ would end by a zero. Now (i) implies that

$$\sigma^r(x) = x_{r-s+1} \dots x_{n-s-t-1} 0^t 1 0^s x_1 \dots x_{r-s}$$

starts with at least s zeros which means that

$$\sigma^{r-1}(y) = x_{r-s+1} \dots x_{n-s-t-1} 0^{t+1} 1 0^{s-1} x_1 \dots x_{r-s}$$

starts with at least s zeros, too, which is a contradiction to (ii). □

We now describe the WS algorithm as introduced in (Ruskey, Savage and Wang, 1992), p. 426. This algorithm produces the canonical representative for each necklace orbit.

Starting with the string $w = 0^n$ as root, we generate as the children of w all those *canonical* strings of the form $\tau\sigma(w)$, $\tau\sigma^2(w) = \tau\sigma\tau(\tau\sigma(w))$, $\tau\sigma^3(w) = (\tau\sigma\tau)^2(\tau\sigma(w))$, etc. We keep generating until the smallest j is reached for which $\tau\sigma^j(w)$ is not canonical. This procedure is applied recursively to each canonical child of w.

In Figure 9.1 we see the trace of the algorithm for $n = 5$. The non-canonical strings examined by the algorithm are typeset in italics.

Theorem 9.3.2 (Wang, Savage) *Each canonical representative is generated by the WS algorithm.*

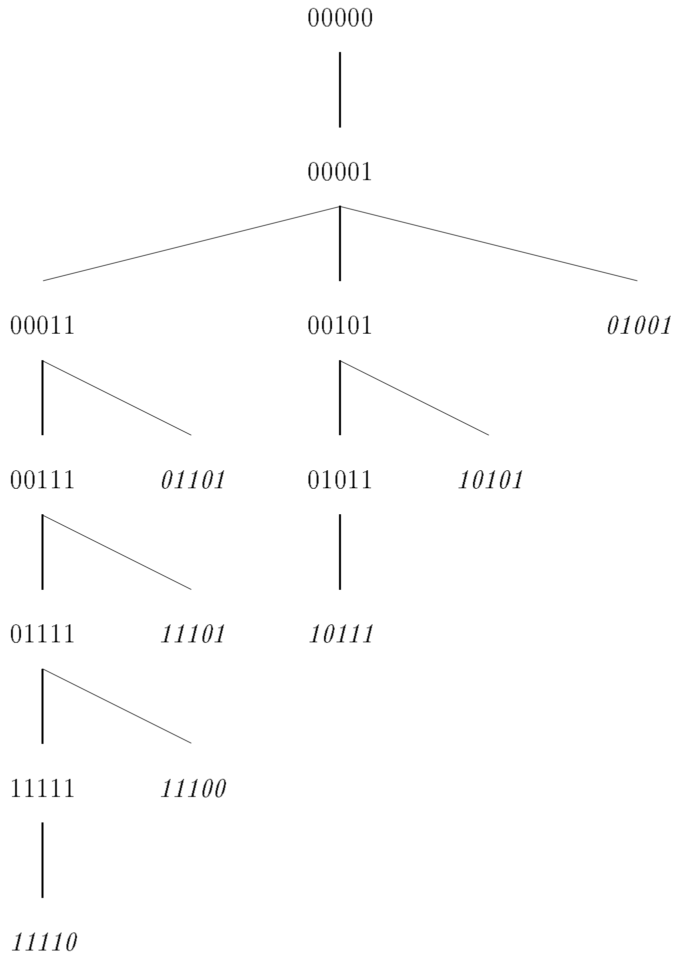


Figure 9.1: Trace of the WS algorithm for two colors and 5 beads.

Proof. Let y be canonical and let a be the number of ones in y. We will show by induction on a that y is generated by the algorithm: The case $a = 0$ is trivial. For $a > 0$, let us assume that all canonical representatives with $a - 1$ ones are generated. The string $y' := \tau(y)$ has $a - 1$ ones. Let $y' = 0^s z 0^t$, where $z \in \{0,1\}^{n-s-t}$ begins and ends with a 1. Then $s + t$ is the length of longest possible run of contiguous zeros in any string that belongs to the $C_{\underline{n}}$–orbit of y'. (Note that $t \geq 1$.) Let $\bar{y}$ be the canonical representative of that orbit. Since z does *not* contain 0^{s+t} as a substring (otherwise y would not be canonical), clearly $\bar{y} = 0^{s+t}z$. Hence, $y = \tau\sigma^t(\bar{y})$. By the induction assumption, $\bar{y}$ is generated by the WS algorithm. Since $\tau\sigma^{j+1}(\bar{y}) = \tau\sigma\tau(\tau\sigma^j(\bar{y}))$ for each $j \geq 1$, it follows from Theorem 9.3.1 that all strings $\tau\sigma(\bar{y})$, $\tau\sigma^2(\bar{y})$, $\ldots$, $\tau\sigma^t(\bar{y})$ are canonical representatives and hence, by the description given above, all of them are generated by the WS algorithm. In particular, $y = \tau\sigma^t(\bar{y})$ is generated. □

Lemma 9.3.3 *Let $x \in \{0,1\}^{\underline{n}}$. We can test in $O(n)$ time if x is the canonical representative of its $C_{\underline{n}}$–orbit.*

Proof. Shiloach (1981) gives an algorithm that finds for each $x \in \{0,1\}^{\underline{n}}$ in time $O(n)$ an integer t such that

$$\sigma^t(x) = \min_{0 \leq t' < n} \sigma^{t'}(x).$$

Now x is canonical if and only if $x = \sigma^t(x)$ which again can be checked in $O(n)$ time. □

9.3.1 Time Complexity of the WS Algorithm

Recall that, in this chapter, $N(n)$ denote the number of two-color necklaces of n beads. The running time of the WS algorithm can be measured by the number of nodes visited by the algorithm because at each node we need $O(n)$ time to generate the respective string and test if it is canonical or not. We note that while generating the children of the canonical string y, at most one non-canonical string is examined. (Precisely, expansion of *each* canonical node in the tree should end in a non-canonical string. However, we can avoid certain tests by noting that a string x starting with a 1 is canonical if and only if $x = 1^n$.) Consequently, the number of nodes visited by the algorithm is at most $2 \cdot N(n)$ and the running time is $O(n \cdot N(n))$.

From the formula for the cycle index of $C_{\underline{n}}$'s natural action, see (Kerber, 1991), p. 72, we find the total number of two-color necklaces by unweighted Pólya's Theorem 2.1.25:

$$N(n) = \sum_{d|n} \phi(d) \cdot 2^{n/d}$$

where ϕ is the Euler totient function. It turns out that with growing n the number of visited nodes approaches the value $2 \cdot N(n)$ very quickly. For example, in the case of 20 beads about $1.97 \cdot N(20)$ strings are examined (Wang, Savage, 1990).

9.4 Bracelet Generation

From now on, we deal with the natural action of the dihedral group $D_{\underline{n}}$ on $\{0,1\}^{\underline{n}}$. Unless stated otherwise, the terms "canonical" and "canonical representative" *are from now on meant with respect to $D_{\underline{n}}$–orbits.*

The basis of our algorithm is the bracelet analog of Theorem 9.3.1:

Theorem 9.4.1 *Let $x \in \{0,1\}^{\underline{n}}$, $x = 0z1$ (i.e., $z \in \{0,1\}^{n-2}$). If x is not canonical, then $y := \tau\sigma\tau(x)$ is also not canonical.*

Proof. Suppose x is not canonical while $\tau\sigma\tau(x)$ is canonical. Let $x = x_1 \dots x_n$ so that $x_1 = 0$, $x_n = 1$. There is an $\omega \in D_{\underline{n}}$ such that $\omega(x)$ is canonical, $\omega(x) < x$. According to Theorem 9.3.1, x is the representative of its $C_{\underline{n}}$–orbit, hence $\omega \neq \sigma^r$ and so $\omega = \rho\sigma^r$. If we had $r = 0$ then $\omega(x) = \rho(x)$ starts with a 1 which is impossible. For $r = 1$ we would have $x_1 x_n \dots x_2 < x_1 x_2 \dots x_n$ implying $x_2 = 1$. In this case $\tau\sigma\tau(x)$ starts with a 1 which again is not possible.

Thus $r \geq 2$ must hold. By rewriting $\rho\sigma^r(x) < x$ in explicit form we obtain

$$x_r \dots x_2 0 1 x_{n-1} \dots x_{r+1} \quad < \quad 0 x_2 \dots x_{n-1} 1. \tag{9.3}$$

We have $y = \tau\sigma\tau(x) = x_2 \ldots x_{n-1}01$. Since y is assumed to be canonical, we must have $\rho\sigma^{r-1}(y) \geq y$ which reads as

$$x_r \ldots x_2 10 x_{n-1} \ldots x_{r+1} \quad \geq \quad x_2 x_3 \ldots x_{n-1}01. \tag{9.4}$$

Now (9.3) and (9.4) must hold simultaneously. This together with $x_1 = 0$, $x_n = 1$ gives strong restrictions on the x_i's: From (9.3) we have $x_r = 0$ which implies $x_2 = 0$ because of (9.4). Inductively we get $x_i = 0$ for all $1 \leq i \leq r$. The system (9.3,9.4) now looks as follows:

$$\underbrace{00\ldots0}_{r}1x_{n-1}\ldots x_{r+1} \quad < \quad \underbrace{00\ldots0}_{r}x_{r+1}\ldots x_{n-1}1 \tag{9.5}$$

$$\underbrace{00\ldots0}_{r-1}10x_{n-1}\ldots x_{r+1} \quad \geq \quad \underbrace{00\ldots0}_{r-1}x_{r+1}\ldots x_{n-1}01. \tag{9.6}$$

Equation (9.5) yields $x_{r+1} = 1$. Then we get $x_{r+2} = 0$ from (9.6) which results in $x_{n-1} = 0$ because of (9.5). By iteration, $x_j = 0$ for $r + 2 \leq j \leq n - 1$. After all these substitutions, (9.5) has the form

$$0^r 10^{n-r-2} 1 < 0^r 10^{n-r-2} 1$$

which is a contradiction. □

Definition 9.4.2 *The canonical representatives of $C_{\underline{n}}$–orbits will be called* N-representatives (necklace representatives) *and the canonical representatives of $D_{\underline{n}}$–orbits will be called* B-representatives (bracelet representatives).

Corollary 9.4.3 (Two-Block Theorem) *In the WS necklace generation tree, any B-representative appears to the left of any N-representative that is not a B-representative.*

9.4.1 The Bracelet Algorithm

Basically, we can exploit the Two-Block Theorem when we like to list representatives of *both* necklaces and bracelets. However, if we want to generate *only* bracelets then a more efficient method is possible, namely our *bracelet analog of the WS algorithm* which generates the canonical representative of each bracelet orbit:

Starting with the string $w = 0^n$ as root, we generate as the children of w all those *B-representatives* of the form $\tau\sigma(w)$, $\tau\sigma^2(w)$, etc. We keep generating until the smallest j is reached for which $\tau\sigma^j(w)$ is not canonical. Additionally, if $w = 0^q z$ (where $z \in \{0,1\}^{n-q}$ starts with a 1) and $z \neq z^R$ then we also generate all *B-representatives* of the form $\tau\sigma(0^q z^R)$, $\tau\sigma^2(0^q z^R)$, etc. Again, we keep doing this until the smallest j is reached for which $\tau\sigma^j(0^q z^R)$ is not canonical. This procedure is applied recursively to each bracelet child of w.

In Figure 9.3 we see the trace of our algorithm for $n = 8$. Only a subtree of the generation tree is displayed. Branches that are omitted from the picture are indicated by dots, and the strings failing the canonicity test are again typeset in italics. For the sake of brevity, also the strings beginning with 1 are omitted from the picture. (In fact, they need not to be tested by the algorithm, see above.) To improve the readability, for each string $w = 0^q z$ the children of the form $\tau\sigma^j(0^q z^R)$ are emphasized by an R at the end of the tree edge.

Theorem 9.4.4 *Each B-representative is generated by our algorithm.*

Proof. Let y be canonical and let a be the number of ones in y. We will show by induction on a that y is generated by the algorithm: The cases $a = 0, 1$ are trivial. For $a > 1$, let us assume that all B-representatives with $a - 1$ ones are generated. The string $y' := \tau(y)$ has $a - 1$ ones. Let $y' = 0^s z 0^t$, where $z \in \{0,1\}^{n-s-t}$ begins and ends with a 1. Then $s + t$ is the length of longest possible run of contiguous zeros in any string that belongs to the $D_{\underline{n}}$–orbit of y'. Let $\bar{y}$ be the B-representative (lexicographically smallest string) in that orbit. Since z does *not* contain 0^{s+t} as a substring (otherwise y would not be canonical), clearly (i) $\bar{y} = 0^{s+t} z$ or (ii) $\bar{y} = 0^{s+t} z^R$. It follows from Theorem 9.4.1 that in the case (i) all strings $\tau\sigma(0^{s+t}z)$, $\tau\sigma^2(0^{s+t}z)$, ..., $\tau\sigma^t(0^{s+t}z)$ are B-representatives while in the case (ii) all strings $\tau\sigma(0^{s+t}z^R)$, $\tau\sigma^2(0^{s+t}z^R)$, ..., $\tau\sigma^t(0^{s+t}z^R)$ are B-representatives. By the induction assumption, $\bar{y}$ is generated by our algorithm and, hence, so is y. Note that the test $z \neq z^R$ in the expansion step of our algorithm is necessary to avoid duplicate generation. □

Two Color Bracelets

```
procedure reverse_tail(x);
    find s such that x starts with exactly s zeros;
    find z such that x = 0^s z;
    return concat(0^s, reverse(z));

procedure search(y);
output(y);
done := false;
while not(done) do
    v := σ(y);
    x := τ(v);
    if x is canonical
        then search(x);
        else done := true;
if y ≠ reverse_tail(y)
    then v := reverse_tail(y);
        done := false;
        while not(done) do
            v := σ(v);
            x := τ(v);
            if x is canonical
                then search(x);
                else done := true;

main;
output(00...00);
search(00...01);
```

Figure 9.2: The algorithm to generate n-bead bracelets in two colors.

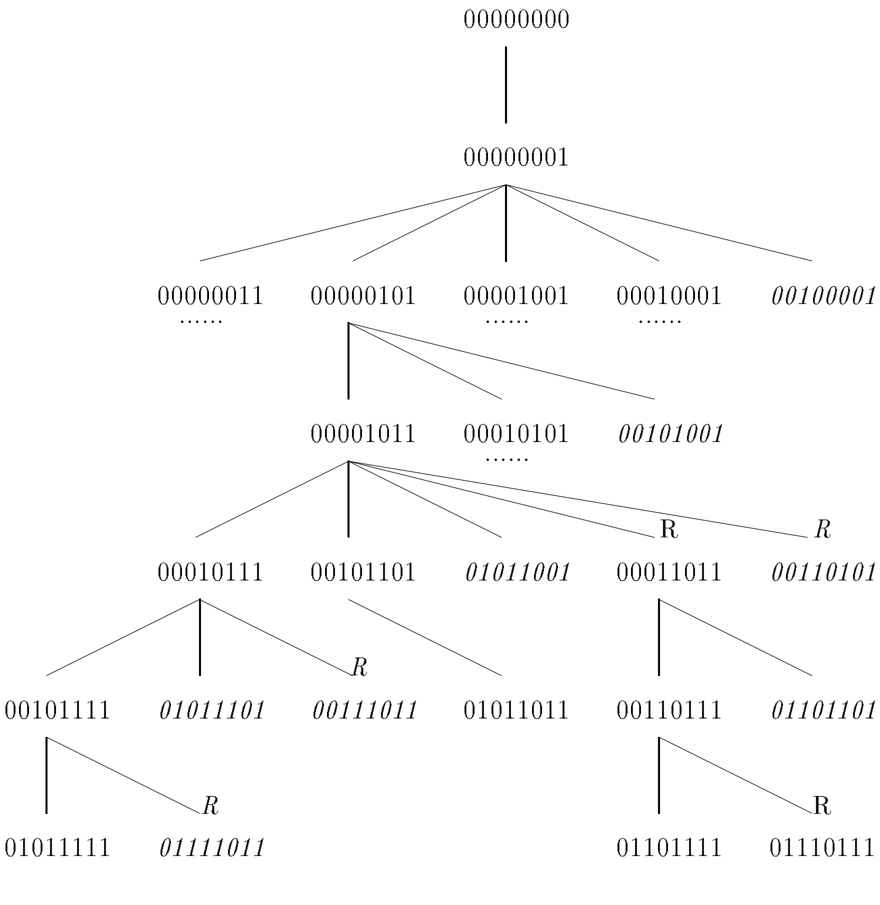


Figure 9.3: A subtree of the bracelet generation tree for $n = 8$.

9.4.2 Time Complexity

With each B-representative $y = 0^q z$ we examine at most two non-canonical strings. Hence, the total number of strings (tree nodes) examined by our algorithm is at most $3 \cdot B(n)$ where $B(n)$ is the number of two-color bracelets of n beads. Using formulas for the cycle index of $D_{\underline{n}}$'s natural action, see (Kerber, 1991, p. 72), $B(n)$ can be expressed as

$$\begin{array}{rcll} B(n) & = & 1/2 \cdot N(n) + 2^{\frac{n-1}{2}} & \text{if } n \text{ is odd,} \\ B(n) & = & 1/2 \cdot N(n) + 3/4 \cdot 2^{\frac{n}{2}} & \text{if } n \text{ is even.} \end{array}$$

Combining with $N(n) \geq 2^n/n$, the last two equations give the obvious asymptotic result $\lim_{n\to\infty} B(n)/N(n) = 1/2$. Hence, the ratio of strings examined by WS and by our algorithm is approximately

$$\frac{3 \cdot B(n)}{2 \cdot N(n)} \sim \frac{3}{4}.$$

This means that if we aim at *bracelet* generation then the use of our algorithm asymptotically saves about 25% of the number of vertices that have to be visited, when compared to the "brute force" approach which resides in generating all N-representatives by WS necklace algorithm and select the B-representatives from them. In fact, the ratio 3/4 between the numbers of vertices visited by the respective algorithms is approached already for small values of n, as can be seen from the table:

	WS algorithm		our algorithm	
beads	nodes examined	number of $C_{\underline{n}}$–orbits	nodes examined	number of $D_{\underline{n}}$–orbits
10	186	108	165	78
15	4196	2192	3347	1224
20	103444	52488	79017	27012

Another reduction is possible if we do not insist on *canonical* representatives. In this case, the representatives of orbits with $m > n/2$ ones are found as pointwise complements of the representatives with $n - m$ ones, saving about a half of the generation time. In general, the generation of canonical representatives with $m \leq M$ ones is possible for any M by cutting the WS tree at level M.

9.5 Restricted Generation

There is an apparent resemblance between WS-type algorithms and the orderly generation methods (Section 6.2). In particular, in the Wang-Savage algorithm the sequence of children of each N-representative reminds (to some extent) of the augmentation of that string (function) as introduced in Definition 6.2.5. This gives us hope that certain features of orderly approach may project to the WS-type algorithms, in particular the restricted generation should be possible. (See Section 6.2.2 for exposition on restricted listing.)

In the context of necklaces and bracelets, the restrictive predicate P often has the form "The given (fixed) string u is not allowed to appear as a substring in the generated object." Such restrictions typically arise in sciences (chemistry etc.) It should be clear that this kind of requirements can be easily embedded into our algorithms since we have a direct control over the adjacency relations in the process of generation.

More precisely, if x is a N-representative (B-representative), $x = 0^t y$ where y begins with a 1, and if a "forbidden" string u appears as a substring of y then u appears as a substring of every child of x in the generation tree. Hence, if we detect u to be a suffix of y, then we can cut off the whole branch of the tree descending from x.

We now present an example of restricted bracelet generation. El-Basil (1988) studies so-called *Clar structures* which are binary strings not containing 0^2 or 1^3 as substrings. If we wish to list all bracelets subject to these conditions (let us call them *Clar bracelets*) then the following table shows the notable reduction in the number of strings to be examined. The entry in the column "full tree" indicates the number of nodes to be visited in the unrestricted generation whereas the column "pruned tree" shows the size of the tree in restricted generation, where pruning proceeds using the idea from the preceding paragraph.

beads	full tree	pruned tree	Clar bracelets
10	165	23	3
15	3347	77	5
20	79017	278	14
25	$\sim 2 \cdot 10^6$	1025	31
30	$\sim 5.4 \cdot 10^7$	3992	104

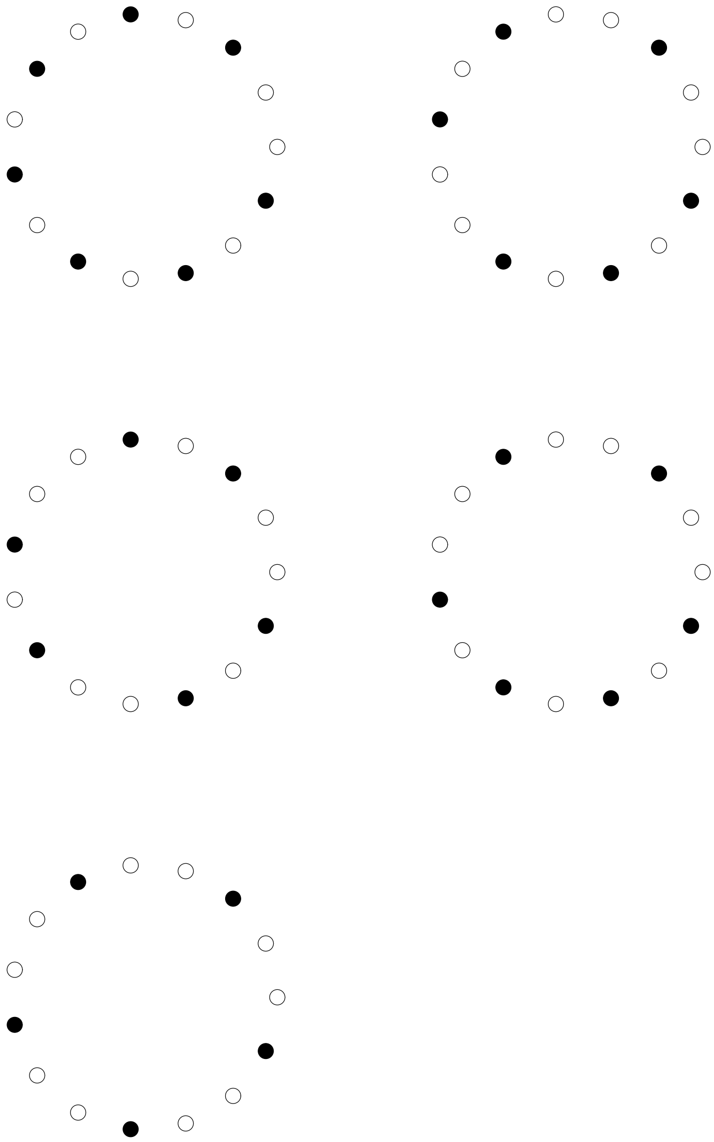


Figure 9.4: Clar bracelets of 15 beads.

For an illustration, in Figure 9.4 we see the five Clar bracelets of 15 beads. Zeros are displayed as black circles, ones correspond to white circles.

9.6 Proportionalities in Ball Rings

In the preceding sections we have proven correctness of algorithms for generating necklaces and bracelets. In the rest of the chapter we will see an application of bracelet listing. We will recall the interesting problem about local and global proportionalities in ball rings posed by Fishburn, Hwang and Lee (1986). For the symmetric neighborhood case, we decrease the upper bounds (which were conjectured to be tight) by giving a uniform construction for the three subcases distinguished in the original paper. Furthermore, we describe our technique of obtaining upper bounds because it may be re-used for the study of other instances of the original problem.

9.6.1 Local and Global Majorities

Suppose a ring $\mathcal{R}$ of n balls

$$\mathcal{R} = (B_0, B_1, \ldots, B_{n-1}),$$

each of which is either black or white, contains at least one white ball. Denote by $\mathrm{wh}(\mathcal{R})$ and $\mathrm{bl}(\mathcal{R})$ the number of white and black balls in $\mathcal{R}$, respectively.

Definition 9.6.1 *For given integers $r \geq l \geq 0$ define for each ball B_i its* (l,r)-ball neighborhood

$$N_{l,r}(B_i) := (B_{i-l}, \ldots, B_{i-1}, B_{i+1}, \ldots, B_{i+r})$$

where indices are taken modulo n if necessary.

Definition 9.6.2 *Let $r \geq l \geq 0$ be given integers and let c be an integer, having the same parity as $l+r$ and satisfying $-(l+r) \leq c \leq l+r$. We say that $\mathcal{R}$ is* (l,r,c)-admissible *if it satisfies the following local condition: For every white ball B in $\mathcal{R}$, $N_{l,r}(B)$ contains at least c more white balls than black balls.*

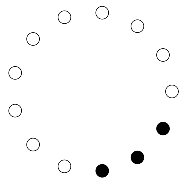


Figure 9.5: A $(6,6,6)$-admissible ring.

For example, the ring in Figure 9.5 is $(6,6,6)$-admissible but not $(6,6,8)$-admissible.

Fishburn, Hwang and Lee (1986) studied the function

$$R(l,r,c) := \inf_{\mathcal{R}} \frac{\mathrm{wh}(\mathcal{R})}{\mathrm{bl}(\mathcal{R})}$$

where the infimum is taken over all (l,r,c)-admissible rings $\mathcal{R}$. Thus Figure 9.5 shows us that $R(6,6,6) \le 10/3$.

Special interest was paid to the *symmetric case*, where $l = r = k$, $0 < c \le 2k$ and c is even since it must have the same parity as $l + r = 2k$. We will assume these additional conditions throughout the rest of this chapter. Fishburn, Hwang and Lee (1986) derived the lower bound

$$R(k,k,c) \ge \frac{2k+c}{2k-c}$$

and they showed that $R(k,k,c) = (2k+c)/(2k-c)$ if k and $\frac{c}{2}$ have the same parity. For the remaining case when

$$0 < c \le 2k \qquad \text{and} \qquad k \not\equiv \frac{c}{2} \pmod 2 \tag{9.7}$$

three upper bounds were constructed (together with respective rings) for various combinations of values k and c:

Fact 9.6.3 *Suppose* $k \not\equiv \frac{c}{2} \pmod 2$. *Then*

$$R(k,k,c) \le \frac{2k+c+2}{2k-c} \qquad \text{if } k \le c < 2k, \tag{9.8}$$

$$R(k,k,c) \le \frac{2k^2+2k+ck}{2k^2+2k-ck-2c} \quad \text{if } 0 < c \le k \text{ and } k \text{ is even}, \tag{9.9}$$

$$R(k,k,c) \le \frac{2k^2+4k+2+ck+c}{2k^2+4k+2-ck-3c} \quad \text{if } 0 < c \le k \text{ and } k \text{ is odd}. \tag{9.10}$$

The right-hand sides of inequalities (9.8)–(9.10) will be denoted by $U_1(k,c)$, $U_2(k,c)$ and $U_3(k,c)$, respectively.

Fishburn, Hwang and Lee (1986) conjectured that the bounds in (9.9) and (9.10) are tight, i.e., that $R(k,k,c)$ is equal to $U_2(k,c)$ or $U_3(k,c)$ in those cases. As for the first bound, it was conjectured that it is "best-possible".

In the rest of this chapter we show that these conjectures are not valid by presenting a *uniform* construction which covers all three subcases distinguished above. We show that our bound is strictly better than (9.8)–(9.10) except for certain rare cases where both bounds are equal. Finally, we give a detailed description of the method that led to our results. It can be easily adapted for other values of l, r and c.

There is no overlap between our results and the work by Woodall (1992) who developed the ideas of Fishburn, Hwang and Lee (1986) in a different direction.

9.7 Models for Ball Rings

Obviously, both informations that are of interest to us (admissibility and global proportionality) are invariant under rotation of the ball ring. In the symmetric neighborhood case ($l = r$) these properties are invariant under reflection, too. This means that in the case $l \neq r$ we can take *necklaces* as the proper model for ball rings, whereas in the case $l = r$, *bracelets* will serve us well.

In our work we concentrate on the symmetric case ($l = r$) since it was treated in big detail in the original paper introducing the problem. Hence, we can use our algorithm to generate bracelet representatives and run it subsequently for increasing number of beads. While doing so, we check if we can detect a bracelet that would improve some of the bounds (9.8)–(9.10).

Surprisingly, we indeed came across such bracelets. Although we found only a couple of them, the careful study of their properties was motivating enough to give us an idea how to proceed further. In Section 9.8 we show the improved upper bound and in Section 9.9 we sketch how this bound was found. The whole way from bracelet listing to the pattern (9.11) is then summarized in Section 9.10.

9.8 A New Upper Bound for the Symmetric Case

Let p be a non-negative integer such that $p \le k-2$ and consider the following $(k-p-1) \times 6$ array.

$$\begin{array}{cccccc} p & k-p & p & 1 & 1 & k-p-2 \\ p & k-p & p & 2 & 1 & k-p-3 \\ \vdots & & & & & \\ p & k-p & p & k-p-2 & 1 & 1 \\ p & k-p & p & k-p-1 & p+1 & k-p-1 \end{array} \tag{9.11}$$

(If $p = k-2$ then just the last row of (9.11) should be present.) Construct a ring $\mathcal{R}$ in which the lengths of successive runs of consecutive balls of the same color are given by concatenating the rows of (9.11), with each entry being the length of a run of consecutive black or white balls according as it occurs in an odd-numbered or an even-numbered column. Note that $\mathcal{R}$ is symmetrical about the run of $p+1$ consecutive black balls. It is lengthy but straightforward to prove that for each white ball B, $N_{k,k}(B)$ contains exactly $2p+1$ black balls.

As before, let k and c be as in (9.7). Then

$$p := \frac{2k-c-2}{4} \tag{9.12}$$

is a non-negative integer. Moreover, $p < k-2$ in all cases except for $(k,c) = (2,2)$, when $p = k-2$. In all cases we construct the ring $\mathcal{R}$ from the array (9.11) with p determined by (9.12). We can easily check that $\mathcal{R}$ is (k,k,c)-admissible.

As an example, for $(k,c) = (6,6)$ we get $p = 1$ and the ring $\mathcal{R}$ as depicted in Figure 9.6.

In the array (9.11) we have altogether $(k-p-1)(k-p) + (k-p-2)(k-p-1) + 2(k-p-1) = 2(k-p-1)(k-p)$ white beads and $2(k-p-1)p + (k-p-2) + (p+1) = 2(k-p-1)p + k - 1$ black beads. After substitution from (9.12), the global proportionality of white and black beads in $\mathcal{R}$ is

$$U(k,c) := \frac{4k^2+4ck+c^2-4}{4k^2-c^2-4}. \tag{9.13}$$

We arrive at the following theorem:

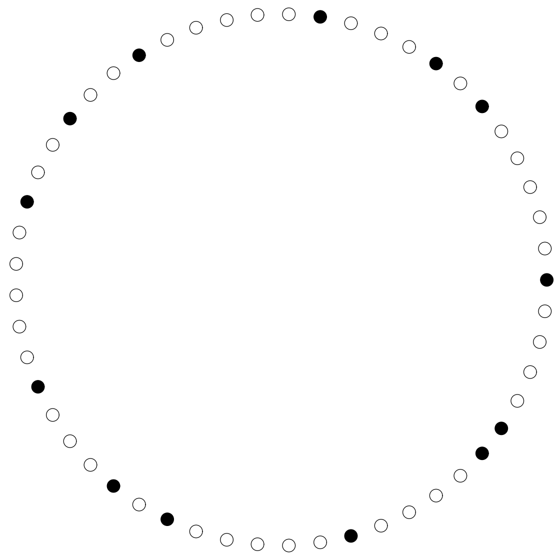


Figure 9.6: $R(6,6,6) \leq 40/13$.

Theorem 9.8.1 *Let* $k \not\equiv \frac{c}{2} \pmod 2$ *and* $0 < c < 2k$. *Then*

$$R(k,k,c) \leq \frac{4k^2 + 4ck + c^2 - 4}{4k^2 - c^2 - 4}.$$

An easy computation yields the comparison of this (uniform) bound and bounds due to Fishburn, Hwang and Lee (1986):

Theorem 9.8.2 *Let* $k \not\equiv \frac{c}{2} \pmod 2$ *and* $0 < c < 2k$.

(i) If $k \leq c < 2k$ *then* $U(k,c) \leq U_1(k,c)$. *Equality holds if and only if* $c = 2k - 2$.

(ii) If $0 < c \leq k$ *and* k *is even then* $U(k,c) \leq U_2(k,c)$. *Equality holds if and only if* $c = 2$.

(iii) If $0 < c \leq k$ *and* k *is odd then* $U(k,c) \leq U_3(k,c)$. *Equality holds if and only if* $c = 4$.

One may note that the equality takes place for the extreme values of c. (In fact, for $c = 2$ and $c = 4$ the rings drawn by our scheme (9.11) coincide with those constructed by Fishburn, Hwang and Lee (1986).) The smallest instance where the bounds are different is $(k,c) = (6,6)$. Here Figure 9.5 shows (the period of) the ring suggested by Fishburn, Hwang and Lee (1986) whereas Figure 9.6 presents the ring resulting from our arrangement.

9.9 Deriving Upper Bounds

We now describe the way in which the scheme (9.11) was discovered. Unfortunately, the paper (Fishburn, Hwang and Lee, 1986) is lacking any information of this kind.

Again, let k and c be as in (9.7).

Definition 9.9.1 *A (k,k,c)-admissible ring will be called a (k,k,c)-*dense ring *if the (k,k)-ball neighborhood of every white ball contains precisely c more white balls than black balls.*

The intuition suggests that density decreases the ratio of white and black balls and good upper bounds on $R(k,k,c)$ might be obtained this way. The definition of density as given above is compatible with the concept of (k,k,c)-admissibility. However, for our purposes it will be reasonable to introduce the *dual definition:*

Definition 9.9.2 *Let $q := k - c/2$. A ring is (k,k,c)-*dense *if for each white ball B there are precisely q black balls $C_1, \ldots, C_q$ such that B is contained in the (k,k)-ball neighborhood of each C_i ($1 \le i \le q$) and B is not contained in the (k,k)-ball neighborhood of any other black ball.*

Note that $q = 2p + 1$ where p is as in (9.12).

Our approach was, for certain values of k and c, to list all different dense rings. (By "different" rings we mean such rings that cannot be transformed into each other by a cyclic shift.) We need some more definitions in order to describe how this task was accomplished.

Definition 9.9.3 *Each finite or infinite sequence of black and white balls (b's and w's) beginning with a black ball will be called* ball sequence.

Definition 9.9.4 *For a ball sequence, we define its* gap sequence *as the sequence of lengths of white ball runs between consecutive black balls.*

For example, the gap sequence of $(b, w, w, w, b, b, w, b, \ldots)$ is $(3, 0, 1, \ldots)$. Obviously, there is a one-to-one correspondence between ball sequences and gap sequences.

Definition 9.9.5 *A sequence $(a_i)_{i\in\mathbb{N}}$ is* periodic *if there is a positive integer P such that $a_i = a_{i+P}$ for each i.*

Definition 9.9.6 *A sequence $(a_i)_{i\in\mathbb{N}}$ is* eventually periodic *if there are integers $P \neq 0$ and T such that $a_i = a_{i+P}$ for each $i \geq T$.*

Definition 9.9.7 *Two sequences $(a_i)_{i\in\mathbb{N}}$ and $(b_i)_{i\in\mathbb{N}}$ are* similar, *$a \sim b$, if there are integers S, T such that $a_i = b_{i+S}$ for each $i \geq T$.*

Hence, two eventually periodic sequences are similar if their periods have the same pattern. Clearly, $\sim$ is an equivalence relation.

Definition 9.9.8 *The $\sim$-equivalence classes of eventually periodic gap sequences will be called* clusters.

Further we note that each ball ring (when unfolded infinitely many times) gives rise to a periodic (and, *a fortiori*, eventually periodic) ball sequence and, conversely, each eventually periodic ball sequence gives rise to a ball ring by folding its period.

Let $(g_j)_{j\geq 0}$ be a gap sequence and let $(B_i)_{i\geq 0}$ be the corresponding ball sequence. Let $(b_j)_{j\geq 0}$ be the sequence of black ball indices,

$$b_0 = 0 \quad \text{and} \quad b_j - b_{j-1} = g_{j-1} + 1 \text{ for } j > 0. \tag{9.14}$$

As before, let $q := k - c/2$.

Definition 9.9.9 *We will say that $(g_j)_{j\geq 0}$ is* (k, c)-tight *if $g_0, g_1, \ldots, g_{q-2}$ are arbitrary non-negative integers less than or equal to $2k - q$ and for each $j \geq q - 1$, g_j is the* least *non-negative integer such that $N_{0,k}(B_{b_{j-q+1}})$ and $N_{k,0}(B_{b_{j+1}})$ have no white ball in common.*

(Recall (9.14). In the one case $g_{j-q+1} = \ldots = g_{j-1} = 0$, we must specify also that $N_{0,k}(B_{b_{j-q+1}})$ contains at least one white ball.)

For each tight sequence this gives a recurrence relation of order $q - 1$

$$g_j = f(g_{j-q}, g_{j-q+1}, \ldots, g_{j-1}) \tag{9.15}$$

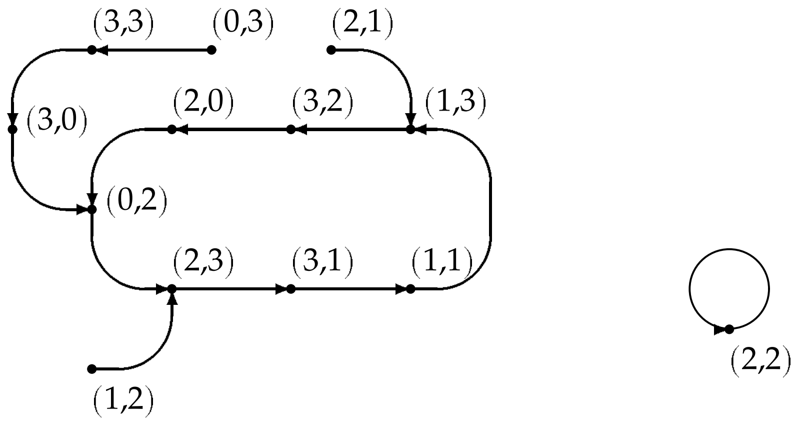


Figure 9.7: A part of the digraph G for $(k, c) = (4, 2)$.

with initial values $g_0, \ldots, g_{q-2}$. Since also for each $j \geq q - 1$ we have $g_j \leq 2k - q$, each tight sequence is bounded. The last two properties together imply that each tight sequence is eventually periodic. Folding the period, we get a (k, k, c)-dense ring. Conversely, each (k, k, c)-dense ring may be unfolded to a (k, c)-tight sequence.

Thus the problem of construction of all dense rings reduces to examination of all clusters of tight sequences. The recurrence (9.15) induces the mapping

$$F : (x_0, x_1, \ldots, x_{q-2}) \mapsto (x_1, x_2, \ldots, x_{q-2}, f(x_0, \ldots, x_{q-2}))$$

between $(q-1)$-tuples over $\{0, \ldots, 2k-q\}$. We may visualize F as the directed graph $G = (V, E)$, where $V = \{0, \ldots, 2k-q\}^{q-1}$ and $(x, F(x)) \in E$ for each $x \in V$. Clusters of tight sequences correspond to connected components of G, which are easily found algorithmically.

We invite the reader to try this method on the particular case $k = 4$, $c = 2$ and $q = 3$. A part of the digraph G is drawn in Figure 9.7. (The entire digraph has $(2k - q + 1)^{q-1} = 36$ vertices.) In the picture we see two clusters, each giving rise to one (4,4,2)-dense ring: The left-hand cluster leads to the dense ring with white ball runs $0, 2, 3, 1, 1, 1, 3, 2$ which is just the ring with proportionality $17/12$ from Figure 1 in (Fishburn, Hwang and Lee, 1986). The right-hand cluster implies the (4,4,2)-dense ring with two white balls and one black ball, which is not optimal.

Thus, for given k and c subject to (9.7), we may construct all (k,k,c)-dense rings and single out the optimal one(s). In the course of experimentation, we proceeded by fixing $p = 1,2,3,\ldots$ $(q = 3,5,7,\ldots)$ and finally we derived the pattern (9.11) which covers all optimal dense rings known to us. It is very likely that this general scheme gives the optimal ball proportionality amongst the dense rings and subsequently we may conjecture that $U(k,c)$ is the value of $R(k,k,c)$ when k and $c/2$ have different parities.

In our work, we have treated the open part of the symmetric case $l = r = k$ because this subproblem was studied in great detail in (Fishburn, Hwang and Lee, 1986). Nevertheless, our approach may be used to derive upper bounds for any l, r and c.

9.10 Methodological Aspects

From Section 0.1 we recall that the creativity spiral is marked by an interleaved sharpening of results (theorems) and methods (algorithms). The research described in this chapter provides an example of ascending the creativity spiral in several iterations. In each iteration, the insight gained from computer-aided experiments was inevitable for forming concepts and proving rigorous theorems.

We based our spiral when we developed the bracelet listing algorithm. Using this method, we found first few examples of bracelets that revealed that the bounds (9.8)–(9.10) are not tight. A careful examination of these initial results led us to the concept of dense rings (cf. Definition 9.9.1). To generate the dense rings was the next algorithmic challenge and once we mastered this problem, we could get ourselves a load of them. Once more we had results to analyze, and finally the pattern (9.11) popped up, giving us hints how to prove a rigorous theorem which simplifies and improves the proportionality bounds.

Chapter 10

Configurations in Finite Geometries

In Section 6.2 we paid much attention to the description of orderly listing methods. In this chapter and in Chapter 11 we will see how restricted orderly generation can be used to look for interesting objects in finite geometry and in coding theory.

In the present chapter we focus on configurations in finite projective planes. In particular, we will be dealing with the Desarguesian planes over the field $GF(q)$, i.e., with the planes $PG(2,q)$. We will also call them "classical planes".

The symbolics and also some statements are introduced in Section 10.1. However, the presentation of all definitions and preparatory theorems would be far beyond our possibilities, hence the basic knowledge of projective geometry will be assumed. In Section 10.2 we establish a link between configurations in finite planes and the "symmetry classes of mappings" paradigm (Chapter 2). This link allows us to apply the theory of Chapter 6. Introductory remarks on this particular application of constructive methods are in Section 10.3. Then in Sections 10.4 and 10.5 we use the orderly methods to compile catalogs of *semiovals* and *arcs*, respectively. After describing how the concrete generation task was accomplished, we analyze the outputs (catalogs) and evaluate their geometric meaning.

10.1 Definitions and Facts

Throughout this chapter, let $GF(q)$ denote the finite field with q elements, q being a prime power, and let $PG(2,q)$ be the projective plane over $GF(q)$.

We regret that a detailed exposition on classical projective planes is beyond the possibilities of our thesis. For this purpose we can recommend (Hughes, Piper, 1982). For an introduction on finite classical planes we refer to (Hirschfeld, 1979), or to Chapters 19, 23 and 26 in (van Lint, Wilson, 1992).

10.1.1 Finite Fields

Definition 10.1.1 *Let $GF(q)^*$ be the cyclic multiplicative group of non-zero elements of $GF(q)$. We say that t is* a square *in $GF(q)$ if there exists*

$u \in GF(q)$ such that $t = u^2$ holds in $GF(q)$. Otherwise we say that t is non-square *in $GF(q)$.*

We will write $1/y$ instead of y^{-1} and x/y instead of xy^{-1} for $x \in GF(q)$, $y \in GF(q)^*$.

Fact 10.1.2 *Let q be an odd prime power. Then -1 is a square in $GF(q)$ if and only if $q = 4r + 1$, $r \in \mathbb{N}^+$. Consequence: Let t be square in $GF(q)$, q an odd prime power. Then $-t$ is a square in $GF(q)$ if and only if $q = 4r + 1$, $r \in \mathbb{N}^+$.*

Proof. (Biggs, 1989), p. 365. □

Fact 10.1.3 *Let q be an odd prime power. Then 2 is a square in $GF(q)$ if and only if $q = 8r \pm 1$, $r \in \mathbb{N}^+$. Consequence: If $q = 8r - 1$ or $q = 8r - 3$, $r \in \mathbb{N}^+$, q a prime power, then -2 is non-square in $GF(q)$.*

Proof. (Lidl, Niederreiter, 1986), p. 182. □

10.1.2 Finite Field Planes

Definition 10.1.4 *Let $S(2, q)$ denote the point set of $PG(2, q)$.*

Definition 10.1.5 *Let $F = F(x, y, z)$ be a trivariate homogeneous polynomial over $GF(q)$. Then $\mathcal{F} = V(F)$ will denote the* variety *of F, i.e., the set of points from $PG(2, q)$ on which F vanishes,*

$$V(F) = \{P \in S(2, q) \mid F(P) = 0\}.$$

If F is linear then $\mathcal{F}$ is a line having $q + 1$ points.

Definition 10.1.6 *If S is any set of two or more collinear points then $l(S)$ will denote the line containing S. For any two different points $P \neq Q$, the notation $l(PQ)$ will serve as shorthand for $l(\{P, Q\})$.*

If the polynomial F in Definition 10.1.5 is quadratic then $\mathcal{F}$ is a *conic.* The conic can be either *singular* (in which case it is a point, a repeated line, or two lines) or non-singular, in which case it consists of $q + 1$ points, none three of them being collinear.

Fact 10.1.7 *Let $K = GF(q)$ and let $F \in K[x_0, x_1, x_2]$, $F = \sum_{0 \leq i,j \leq 2} a_{ij}x_ix_j$. As before, let $\mathcal{F} = V(F)$. Then $\mathcal{F}$ is singular if and only if $\delta = 0$ where*

$$\delta = 4a_{00}a_{11}a_{22} + a_{01}a_{02}a_{12} - a_{00}a_{12}^2 - a_{11}a_{02}^2 - a_{22}a_{01}^2.$$

Proof. (Hirschfeld, 1979), p. 144. □

Definition 10.1.8 *Let $\mathcal{F}$ be a non-singular conic in $PG(2,q)$, q odd. The line l is called an* external line, *a* unisecant *or a* bisecant *of $\mathcal{F}$ according as it has 0, 1 or 2 common points with $\mathcal{F}$.*

Definition 10.1.9 *Let $\mathcal{F}$ be a non-singular conic in $PG(2,q)$, q odd, and let P be a point in $PG(2,q)$, $P \notin \mathcal{F}$. The point P is called* external *or* internal *to the conic $\mathcal{F}$ according as it lies on two or none of the unisecants (tangents) of $\mathcal{F}$.*

Fact 10.1.10 *Let $\mathcal{F}$ be a non-singular conic in $PG(2,q)$, q odd, let P be a point in $PG(2,q)$, and let l be the polar of P with respect to $\mathcal{F}$. Then l is the tangent to $\mathcal{F}$ at P, an external line, or a bisecant according as P is a point of $\mathcal{F}$, a point internal to $\mathcal{F}$, or a point external to $\mathcal{F}$.*

Proof. (Hirschfeld, 1979), p. 170. □

As a special case we have:

Fact 10.1.11 *Let $\mathcal{F} = V(x^2 - yz)$ in $PG(2,q)$, q odd. The point (x_0, y_0, z_0) is on $\mathcal{F}$, external to $\mathcal{F}$, or internal to $\mathcal{F}$, according as $x_0^2 - y_0z_0$ is zero, a non-zero square or non-square in $GF(q)$.*

Proof. (Hirschfeld, 1979), p. 171. □

Definition 10.1.12 *Let $\mathcal{F}$ and $\mathcal{G}$ be two non-singular conics. If each point of $\mathcal{F} \setminus \mathcal{G}$ is internal to the conic $\mathcal{G}$ then we say that the conic $\mathcal{F}$ is* internal *to the conic $\mathcal{G}$.*

Definition 10.1.13 *Let $\mathcal{F}$ and $\mathcal{G}$ be two non-singular conics. If $\mathcal{F}$ is internal to $\mathcal{G}$ and $\mathcal{G}$ is internal to $\mathcal{F}$ then we say that $\mathcal{F}$ and $\mathcal{G}$ are* mutually internal.

10.2 Group Action Setting

Let $GL(3,q)$ denote the group of all 3×3 non-singular matrices over $GF(q)$ and let $Z(GF(3,q))$ be its center, which is the group of all $GF(q)^*$-scalar multiples of the 3×3 identity matrix.

The group of all projectivities of $PG(2,q)$ is denoted by $PGL(3,q)$ (projective general linear group). We have

$$PGL(3,q) \simeq GL(3,q)/Z(GL(3,q)). \tag{10.1}$$

Hence, to each projectivity $\Pi \in PGL(3,q)$ there correspond $q-1$ matrices from $GL(3,q)$. We can take any of them to represent Π.

Definition 10.2.1 *Let V^T denote the transpose of the vector V and let $\Pi \in PGL(3,q)$ be a projectivity represented by the matrix*

$$M(\Pi) = \begin{pmatrix} t_{00} & t_{01} & t_{02} \\ t_{10} & t_{11} & t_{12} \\ t_{20} & t_{21} & t_{22} \end{pmatrix}.$$

Let X be a point in $PG(2,q)$. The projectivity Π acts on points by matrix multiplication:

$$\Pi : \; X \mapsto (M(\Pi) \cdot X^T)^T. \tag{10.2}$$

Remark. It may be of some use to notice how the action of Π on *varieties* follows from the action on points:

$$\Pi : \; V(F) \mapsto V(F')$$

where $F'(x,y,z) = F(x',y',z')$ is the polynomial obtained from F via the substitution $\{x \mapsto x', y \mapsto y', z \mapsto z'\}$ defined by

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = (M(\Pi))^{-1} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Fact 10.2.2 *The mapping (10.2) is a group action.*

Definition 10.2.3 *Each bijection $C : PG(2,q) \to PG(2,q)$ that preserves collinearity (i.e., C maps lines to lines) is called a* collineation *of the plane.*

Definition 10.2.4 *The group of all collineations of* $PG(2,q)$ *is called the* collineation group *of* $PG(2,q)$.

An automorphism σ of $GF(q)$ acts on points of $PG(2,q)$ by $\sigma(x,y,z) = (\sigma x, \sigma y, \sigma z)$.

Theorem 10.2.5 (Fundamental Theorem of Projective Geometry) *Let* K *be a field. Each collineation of the projective plane over* K *is a composition of a projectivity and an automorphism of* K.

Proof. (Hirschfeld, 1979), p. 30. □

The collineation group of $PG(2,q)$ is denoted by $P\Gamma L(3,q)$ (projective semilinear group).

Let $q = p^r$ where p is a prime. Since non-trivial automorphisms of $GF(q)$ exist exactly if $r > 1$, we have $PGL(3,p) = P\Gamma L(3,p)$ for $r = 1$. In general, $PGL(3,p^r)$ is a normal subgroup of $P\Gamma L(3,p^r)$.

The geometric properties of objects in $PG(2,q)$ are mostly defined using line incidence (cf. Definitions 10.4.1 and 10.5.1). Hence, these properties are invariant under collineation and it makes good sense to study the objects "up to collineation".

In particular, if the objects that we wish to study are simply point sets in $PG(2,q)$ then we can use the correspondence (6.1) to define the geometric problems in the frame of the "symmetry classes of mappings" paradigm.

Which subgroup of $P\Gamma L(3,q)$ we take for the acting group depends on the particular motivation. In geometric studies we typically choose $PGL(3,q)$, since the collineations arising from field automorphisms usually do not have a good geometric meaning. If, however, we do not care about how objects get screwed by field automorphisms then we may take the entire $P\Gamma L(3,q)$. The former approach *(reasoning "up to projectivity")* may be considered a more geometrical one while the latter *(reasoning "up to collineation" = "up to automorphism")* would be more combinatorial, viewing $PG(2,q)$ merely as a design and somewhat hiding its geometric origin.

In this chapter we work "up to projectivity", i.e., we construct representatives of $PGL(3,q)$-orbits.

plane	total number of configurations
$PG(2,5)$	7,152
$PG(2,7)$	25,598,921,348

Table 10.1: Number of configurations in some small planes.

Definition 10.2.6 *Recall that $S(2,q)$ means the point set of $PG(2,q)$. Let G be the projective group $PGL(3,q)$ and let $f \in \{0,1\}^{S(2,q)}$. The orbit $G(f)$ is called a* configuration *in $PG(2,q)$.*

Fact 10.2.7 *The order of $PGL(3,q)$ is*

$$|PGL(3,q)| = (q^3-1)(q^2-1)q^3.$$

Proof. Each matrix from $GL(3,q)$ can be thought of as an ordered triple of non-zero rows (r_1, r_2, r_3) such that r_i does not belong to the subspace of $GF(q)^3$ spanned by $r_1, \ldots, r_{i-1}$. Hence, the order of $GL(3,q)$ is equal to $(q^3-1)(q^3-q)(q^3-q^2)$. The order of $PGL(3,q)$ is then $|GL(3,q)|/(q-1)$ by (10.1). □

10.3 Configuration Listing

In the last section we have explained that, in geometric reasoning on subsets of $PG(2,q)$, it is enough to work with configurations rather than with the sets themselves. A single configuration may comprise as many as $|PGL(3,q)|$ subsets of $PG(2,q)$. Hence, it follows from Fact 10.2.7 that a considerable reduction of the amount of data is possible even for small values of q.

Moreover, since we succeeded to define geometric configurations in terms of the symmetry classes of mappings, we can use the theory of Chapter 6 to list the configurations. The total number of configurations in $PG(2,q)$ can be evaluated by unweighted Pólya's Theorem 2.1.25 using the cycle index of $PGL(3,q)$'s action on $S(2,q)$.

Table 10.1 shows that the exhaustive (unrestricted) listing of configurations is possible exactly if $q \leq 5$.

Fortunately, in geometric applications only configurations satisfying certain given predicate P are of interest. Hence, we can use restricted generation (Section 6.2.2) which further reduces the number of data to be processed.

Furthermore, it is usual that we know in advance some facts about the number of points in the configurations that are to be listed, see for example Facts 10.4.2 and 10.5.4. Since orderly generation proceeds by content (i.e., by the number of points in the configurations), we have an easy stopping condition.

The ideas from last two paragraphs make it possible to list configurations also in planes of order $q > 5$. In Sections 10.4 and 10.5 we document this by showing how restricted orderly generation was used to obtain new examples of two geometric phenomena, namely *semiovals* ($q \leq 7$) and *arcs* ($q \leq 16$). Then in Chapter 11 we use the same approach to list certain optimal ternary linear codes. The details of the listing task are discussed in each of the three cases separately.

10.4 Semiovals

Definition 10.4.1 *Let T be a set of points of $PG(2,q)$. We say that T is a* semioval *if and only if for each point $P \in T$ there is a unique line l of $PG(2,q)$ such that $T \cap l = \{P\}$. This line l is called the* tangent *to T at P.*

Thas (1974) proved the following lower and upper bounds on the size of semiovals in the plane of order q:

Fact 10.4.2 *If T is a semioval in the finite projective plane of order q, then*

$$q+1 \leq |T| \leq q\sqrt{q}+1.$$

The bounds are achieved when T is an oval or an unital, respectively.

M. de Finis wrote in (1987): "The existence of semiovals whose sizes are neither maximum nor minimum is still an open problem." Blokhuis (1991) gave two constructions of distinguished semiovals (satisfying certain additional property) with sizes $2(q-1)$ and $3/2 \cdot (q-1)$, respectively.

In our work we could find much more examples of semiovals in $PG(2,q)$. Table 10.2 reveals that semiovals are not at all rare phenomena. Rather, they include a broad kaleidoscope of shapes, probably an interesting subject for a classification theory.

10.4.1 Constructions

Following Definition 10.4.1, if $\chi_T \in \{0,1\}^{S(2,q)}$ is a characteristic function of a set T which is a semioval then this function satisfies the predicate $P(\chi_T)$:="T has *exactly* one tangent at each point."

This predicate P, however, is not consistent with augmentation (Definition 6.2.10) and so it cannot be used to restrict the orderly generation. Instead, we have to look for a weaker predicate P' that is consistent with augmentation and then follow the idea from the end of Section 6.2.2. In our case we can use the predicate $P'(\chi_T)$:="T has *at least* one tangent at each point."

As we already know, in planes of order $q \leq 5$ we can easily list all configurations, hence also the determination of all semiovals is easy. In case $q = 7$, listing semiovals by restricted orderly generation using predicate P' is still a manageable task whereas the order $q = 8$ lies beyond our computational possibilities. In Table 10.2 we summarize the results for planes of order less or equal to 7.

10.4.2 Analysis of Results

Definition 10.4.3 *We say that a semioval T is* regular *if it is of the type $(0,1,n)$, i.e., if each line of the plane intersects T in 0, 1 or n points for some $n \in \mathbb{N}$.*

It was conjectured by Blokhuis and Szőnyi (1992) that the only regular semiovals in the Desarguesian plane are the ovals ($n = 2$) and the unitals ($n = \sqrt{q} + 1$). We can support this conjecture with the observation that the only regular semiovals in $PG(2,q)$, $q \leq 7$, are ovals and unitals.

Also, the low appearance of semiovals of small size attracts one's eyes. It follows from the results of Blokhuis (1991) that semiovals of size $q + 2$ can exist in planes of order 4 and 7 only. A subclass of semiovals of size $q + 4$ is discussed in Section 10.4.3.

k \ q	2	3	4	5	7
3	1	-	-	-	-
4	-	1	-	-	-
5	-	0	1	-	-
6	-	1	1	1	-
7	-	-	0	0	-
8	-	-	1	1	1
9	-	-	1	2	1
10	-	-	-	3	0
11	-	-	-	2	0
12	-	-	-	1	10
13	-	-	-	-	21
14	-	-	-	-	69
15	-	-	-	-	118
16	-	-	-	-	82
17	-	-	-	-	21
18	-	-	-	-	7
19	-	-	-	-	1

Table 10.2: Number of k-point semiovals in $PG(2, q)$ up to projectivity.

Each semioval on our list was tested for diverse patterns to appear in it (few intersection numbers, large collinear sets, large arcs, etc.) In particular, for any semioval that could be completely decomposed into a union of several ovals, the permutation group facilities of Cayley (the new version known as Magma) were employed to find all projectivities that would transform one of the ovals into the canonical form $V(x^2 - yz)$. The analytic representation of the transformed semioval was then studied to possibly extract the desired relative position of its ovals in general.

This approach resulted in an intimate interplay between the constructive combinatorics (permutation groups) on one side and the algebraic geometry over finite fields on the other side. Several general constructions obtained in this way can be found in Section 10.4.4. One of them led to the rediscovery of the construction of a non-classical unital that was first discovered by Hirschfeld and Szőnyi (1991).

10.4.3 Semiovals and Regular Arrangements

Blokhuis (1991) gives the complete characterization of semiovals consisting of $q + a$ points in Desarguesian plane of order q, with one additional condition imposed, namely that through each point of the semioval there is exactly one $a + 1$-secant. He proves that each such semioval is a union of two or three large sets of collinear points.

In our work, we have concentrated on the possibility of obtaining semiovals as unions of several ovals. A couple of theorems in this direction can be found in Section 10.4.4. Before coming to that, we note another interesting possibility to obtain semiovals, namely as realizations of regular arrangements.

Definition 10.4.4 *An* n_3-arrangement $\mathcal{A}$ *is a pair* $\mathcal{A} = (\mathcal{P}, \mathcal{B})$ *where* $\mathcal{P}$ *is a set of* n points, *and* $\mathcal{B}$ *is a set of* n point blocks *such that each block contains exactly three points from* $\mathcal{P}$ *and each point is contained in exactly three blocks from* $\mathcal{B}$*. Moreover, any two blocks intersect in at most one point.*

Hence, n_3-arrangements are special instances of $(n, 3, 3)$-designs.

Remark. Instead of n_3-arrangements, one usually speaks of n_3-*configurations*. However, in this chapter we use the word "configuration" to mean something else, so we had to pick a different name in order to avoid confusion.

Definition 10.4.5 *As before, let $S(2,q)$ be the point set of $PG(2,q)$. A* realization *of the arrangement $\mathcal{A} = (\mathcal{P}, \mathcal{B})$ in the plane $PG(2,q)$ is an injective map $R : \mathcal{P} \to S(2,q)$ such that for any block $\mathcal{B}_0 \in \mathcal{B}$, $\mathcal{B}_0 = \{X,Y,Z\}$, the points $R(X)$, $R(Y)$ and $R(Z)$ are collinear.*

Several algorithms for deciding realizability of a given arrangement in a given geometric space are developed in the book by Bokowski and Sturmfels (1989).

When moving from the arrangement $(\mathcal{P}, \mathcal{B})$ to its realization, we may loose some information. For example, if $|\mathcal{P}| = n \leq q+1$ and $P_1, \ldots,$ P_n are n collinear points in $PG(2,q)$ then any bijection between $\mathcal{P}$ and $\{P_1, \ldots, P_n\}$ is a realization of $(\mathcal{P}, \mathcal{B})$. Hence, it makes sense to distinguish some "nice" realizations.

Definition 10.4.6 *We say that a realization $R : \mathcal{P} \to S(2,q)$ is* faithful *if the following holds for any three points $P_1, P_2, P_3 \in R(\mathcal{P})$: If P_1, P_2 and P_3 are collinear then $\{R^{-1}(P_1), R^{-1}(P_2), R^{-1}(P_3)\} \in \mathcal{B}$.*

Very informally, faithful realizations are those which do not introduce any "additional collinearities" (apart from those collinearities that are present in the arrangement). The next proposition shows that faithful realizations are of some interest to us.

Proposition 10.4.7 *Let $\mathcal{A} = (\mathcal{P}, \mathcal{B})$ be an n_3-arrangement. If $n = q+4$ and $R(\mathcal{A})$ is a faithful realization of $\mathcal{A}$ in $PG(2,q)$ then $R(\mathcal{P})$ is a semioval in $PG(2,q)$.*

Proof. Let $S = R(\mathcal{P})$ and let S_0 be an arbitrary point from S. Let $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ be those blocks from $\mathcal{B}$ which contain $R^{-1}(S_0)$. Let $Q = R(\mathcal{B}_1) \cup R(\mathcal{B}_2) \cup R(\mathcal{B}_3)$ and let $S' = S \setminus Q$. Hence, $|S'| = n - 7$. Consider the $q+1$ lines of $PG(2,q)$ going through S_0. Three of them are $l(R(\mathcal{B}_1))$, $l(R(\mathcal{B}_2))$ and $l(R(\mathcal{B}_3))$. There are $n - 7 = q - 3$ other lines connecting S_0 with points from S' since, for any $S'_1, S'_2 \in S'$, $S'_1 \neq S'_2$ implies $l(S_0S'_1) \neq l(S_0S'_2)$. Hence, there is exactly one unisecant of S at S_0. Since S_0 was an arbitrary point, S is a semioval. $\square$

To have some illustration, we will discuss faithful realizations of several n_3-arrangements.

An n_3-arrangement exists only for $n \geq 7$. The only 7_3-arrangement up to isomorphism is the Fano plane (if we take its lines as the blocks). This arrangement can be realized only in planes of even order, hence it does not lead to a semioval in $PG(2,3)$.

The 8_3-Arrangement

Also for $n = 8$, there is (up to isomorphism) just one 8_3-arrangement, see (Vajda, 1967), p. 69.

Proposition 10.4.8 *The 8_3-arrangement can be faithfully realized in $PG(2,4)$.*

Proof. Take three non-concurrent lines l_1, l_2 and l_3. Each l_i contains two points where it intersects the other two lines, and three more points which we shall call *inner* points. Let S bet a point set composed of three inner points of l_1, three inner points of l_2 and two inner points of l_3. We check easily that S is a faithful realization of an 8_3-arrangement. □

Remark. This is in fact the only semioval in a plane of an even order that we meet. Everywhere else, we consider only semiovals in planes of odd order. The main reason is that certain parts of the theory of conics are different for planes of odd and even order.

The 9_3-Arrangements

There are three essentially different 9_3-arrangements, see (Vajda, 1967), p. 69. Among them, the prominent one is the Pappus arrangement so we will deal with it first.

Proposition 10.4.9 *The Pappus 9_3-arrangement cannot be realized as a semioval in $PG(2,5)$.*

Proof. Let the nine points forming a realization of the Pappus arrangement consist of two collinear triples P_1, P_2, P_3 and Q_1, Q_2, Q_3 together with the three points R_{12}, R_{13}, R_{23} lying on the Pappus line. We will label the points so that $R_{12} = l(P_1Q_2) \cap l(P_2Q_1)$, $R_{13} = l(P_1Q_3) \cap l(P_3Q_1)$, $R_{23} = l(P_2Q_3) \cap l(P_3Q_2)$.

W.l.o.g. we may assume that $P_1 = (1,0,0)$, $P_2 = (0,1,0)$, $Q_1 = (0,0,1)$, $Q_2 = (1,1,1)$. Then $P_3 = (1,a,0)$ for some $a \in GF(5)^*$ and $Q_3 = (b,b,1)$ for some $b \in GF(5)^*$. Also, $a \neq 1$ and $b \neq 1$ for otherwise the realization would not be faithful. We compute $R_{12} = (0,1,1)$, $R_{13} = (b, ab, a)$, $R_{23} = (b, ab - a + 1, 1)$. Apart from the nine collinear triples that are always present in any Pappus configuration, some additional collinearities may arise in non-faithful realizations. Our realizations are parameterized by two parameters a and b. The following table lists the conditions under which certain triples in a particular realization happen to be collinear:

triple	collinearity condition
P_1, Q_1, R_{23}	$a = 1/(1-b)$
P_2, Q_2, R_{13}	$a = b$
P_3, Q_3, R_{12}	$a = (b-1)/b$

Consider the three values $1/(1-b)$, b, $(b-1)/b$. Recalling that $b \notin \{0,1\}$ it is easy to prove that *(i)* all of them are pairwise different, *(ii)* none of them is 0, *(iii)* none of them is 1.

This means that for any fixed $b \in GF(5) \setminus \{0,1\}$,

$$\{\ 1/(1-b),\ b,\ (b-1)/b\ \} = GF(5) \setminus \{0,1\}.$$

Hence, for any admissible choice of a and b, exactly one of the triples listed in the table will be collinear, additionally to the nine default collinearities. Two unisecants exist at each point which belongs to this additional collinear triple. Hence the Pappus arrangement cannot be realized as a semioval in $PG(2,5)$. □

Proposition 10.4.10 *The other two 9_3-arrangements can be faithfully realized in $PG(2,5)$.*

Proof. For the sake of brevity, we show only the easier case and we will omit the other one.

Let $C = \{1,2,3\} \subset GF(5)$ and put

$$S\ =\ \{(0,1,c) \mid c \in C\}\ \cup\ \{(c,0,1) \mid c \in C\}\ \cup\ \{(1,c,0) \mid c \in C\}.$$

The points $(x,0,1)$, $(1,y,0)$ and $(0,1,z)$ are collinear if and only if $xyz+1=0$. For the points belonging to S, this is only possible when $\{x,y,z\} = \{1,2,2\}$ or $\{x,y,z\} = \{1,3,3\}$ (as multisets). From this we easily deduce that each point from S belongs to exactly three collinear triples and that S is a faithful realization of a 9_3-arrangement. $\square$

10.4.4 Semiovals Built from Conics

Theorem 10.4.11 (General construction of semiovals from conics.) *Let $(\mathcal{F}_i)_{1\le i\le m}$ be a family of non-singular conics. Denote $\mathcal{S} = \cup_{1\le i\le m}\mathcal{F}_i$. Moreover, let the following two conditions be fulfilled:*

(i) For any subset $I \subseteq \{1,\dots,m\}$ and point P such that $P \in \cap_{i\in I}\mathcal{F}_i$, all *conics $\mathcal{F}_i$ with $i \in I$ have the same tangent at P.*

(ii) For any $1 \le i,j \le m$, $i \ne j$, $\mathcal{F}_i$ is internal to $\mathcal{F}_j$.

Then $\mathcal{S}$ is a semioval.

Proof. (i): Existence of tangents. Let S_0 be an arbitrary point of $\mathcal{S}$. If S_0 belongs to a unique conic $\mathcal{F}$ then the tangent t to $\mathcal{F}$ at S_0 becomes also the tangent to $\mathcal{S}$ at S_0 since $\mathcal{F}'$ is internal to $\mathcal{F}$ for any $\mathcal{F}' \ne \mathcal{F}$, hence $t \cap \mathcal{F}' = \emptyset$. If S_0 lies in the intersection $\cap_{i\in I}\mathcal{F}_i$ then the common tangent t' to all $\mathcal{F}_i$ at S_0 is also the tangent to $\mathcal{S}$ at S_0 since $t' \cap \mathcal{F}_j = \emptyset$ for each $j \notin I$.

(ii): Uniqueness of tangents at their respective points of contact. Let t, t' be two different tangents at S_0 and w.l.o.g. let $S_0 \in \mathcal{F}_1$. Then at least one of t, t' intersects $\mathcal{F}_1$ in two points. Since $\mathcal{F}_1 \subseteq \mathcal{S}$, this bisecant cannot be a tangent to $\mathcal{S}$, a contradiction. $\square$

Planes of Order $q = 2r+1$

Proposition 10.4.12 *Let q be an odd prime power. In $PG(2,q)$, let $\mathcal{F} = V(x^2-yz)$ and $\mathcal{G} = V((a-1)x^2+yz)$ where $a \in GF(q)$ such that a is non-square and $a-1$ is square. Then $\mathcal{F}$ and $\mathcal{G}$ are non-singular conics and $\mathcal{F} \cup \mathcal{G}$ is a semioval in $PG(2,q)$ consisting of $2q$ points.*

Proof. Since a is non-square, $a \neq 0$. Clearly, there are exactly two common points of $\mathcal{F}$ and $\mathcal{G}$, namely $(0,1,0)$ and $(0,0,1)$. At these points have $\mathcal{F}$ and $\mathcal{G}$ common tangents (namely, $V(z)$ and $V(y)$). Both $\mathcal{F}$ and $\mathcal{G}$ are non-singular since $\delta = 1-a$ for the conic $\mathcal{G}$ and, since a is non-square, $1-a \neq 0$.

In order to show that $\mathcal{G}$ is internal to $\mathcal{F}$ it is enough to notice that $(a-1)x^2 + yz = 0$ implies $ax^2 = x^2 - yz$. Since a is non-square, ax^2 must be non-square whenever non-zero.

Conversely, to show that $\mathcal{F}$ is internal to $\mathcal{G}$ we consider the projectivity Π given by the matrix

$$M(\Pi) = \begin{pmatrix} b & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where $b \in GF(q)$ such that $a-1 = b^2$. Π maps $\mathcal{G}$ to $V(x^2-yz)$ and $\mathcal{F}$ to $\mathcal{F}' = V(1/(a-1)x^2 + yz)$. Now $1/(a-1)x^2 + yz = 0$ implies $a \cdot (x/b)^2 = x^2 - yz$. Since a is non-square, $a \cdot (x/b)^2$ must be non-square whenever non-zero, which means that $\mathcal{F}'$ is internal to $V(x^2-yz)$. Hence $\mathcal{F}$ is internal to $\mathcal{G}$. □

Proposition 10.4.13 *Let q be an odd prime power. In $PG(2,q)$, let $\mathcal{F} = V(x^2 - yz)$, $\mathcal{G} = V(ax^2 + yz)$ and $\mathcal{H} = V(b_1x^2 + b_2y^2 + b_2z^2 + yz)$ where $a, b_1, b_2 \in GF(q)$, $a \neq 1$, a is a square, $a+1$ non-square and*

$$\begin{array}{rcrcr} b_1 & + & 2b_2 & = & -1 \\ b_1 & + & 2ab_2 & = & a. \end{array}$$

Then $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are non-singular conics and $\mathcal{F} \cup \mathcal{G} \cup \mathcal{H}$ is a semioval in $PG(2,q)$ consisting of $3(q-1)$ points.

Proof. (i) Common points and tangents. We note that $a \neq 0$. Let $t \in GF(q)^*$ such that $a = t^2$. Since $a \neq 1$, $t \neq \pm 1$. Each pair of conics has two common points with common tangents at these points:

conics	common point common tangent	common point common tangent
$\mathcal{F}$ and $\mathcal{G}$	$(0,1,0)$ $V(z)$	$(0,0,1)$ $V(y)$
$\mathcal{F}$ and $\mathcal{H}$	$(1,1,1)$ $V(2x-y-z)$	$(1,-1,-1)$ $V(2x+y+z)$
$\mathcal{G}$ and $\mathcal{H}$	$(1,t,-t)$ $V(2ax-ty+tz)$	$(1,-t,t)$ $V(2ax+ty-tz)$

(ii) Non-singularity.

conic	value of δ (Fact 10.1.7)
$\mathcal{F}$	-1
$\mathcal{G}$	$-a$
$\mathcal{H}$	$b_1(4b_2^2-1)$

We only have to clarify that $b_1(4b_2^2-1) \neq 0$. First of all, $b_1 \neq 0$, for $b_1 = 0$ would imply $2b_2 = -1$ and $2ab_2 = a$, which is impossible due to $a \neq 0$. Next, $4b_2^2 - 1 = 0$ would mean $b_2 = \pm 1/2$. Both eventualities would imply $b_1 = 0$ and hence lead to a contradiction. Therefore, $b_1(4b_2^2-1) \neq 0$.

(iii) $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$ pairwise mutually internal. We first show that $\mathcal{F}$ and $\mathcal{G}$ are mutually internal. To this end, we notice that $ax^2 + yz = 0$ implies $(a+1)x^2 = x^2 - yz$ and that $a+1$ is non-square, making $(a+1)x^2$ non-square if non-zero. Hence $\mathcal{G}$ is internal to $\mathcal{F}$. In order to show that $\mathcal{F}$ is internal to $\mathcal{G}$ we write

$$\mathcal{F} = \{(0,1,0)\} \cup \{(s,s^2,1) \mid s \in GF(q)\}.$$

$(0,1,0)$ lies in the intersection $\mathcal{F} \cap \mathcal{G}$ so it cannot be an external point. The polar of $(s,s^2,1)$ with respect to $\mathcal{G}$ has the equation $2asx + y + s^2z = 0$. Let us examine the possible intersections of this line with the conic $\mathcal{G}$. This leads us to the system

$$\begin{array}{rcrcrcl} ax^2 & + & yz & & & = & 0 \\ 2asx & + & y & + & s^2z & = & 0 \end{array}$$

Let $(\bar{x},\bar{y},\bar{z})$ be a solution of this system. If $\bar{z} = 0$ then $\bar{x} = 0$ and $\bar{y} = 0$ which does not correspond to a point in $PG(2,q)$. If $\bar{z} = 1$ then we eliminate $\bar{y}$ from the first equation and substitute it in the second, obtaining

$$a\bar{x}^2 - 2as\bar{x} - s^2 = 0.$$

Viewing this as a quadratic equation in $\bar{x}$, we compute its discriminant to be

$$4a^2s^2 + 4as^2 = (2s)^2 a(a+1).$$

The value $s = 0$ leads to the point $(0,0,1) \in \mathcal{F} \cap \mathcal{G}$. If $s \neq 0$, the whole expression is non-square since a is square while $a+1$ is non-square. Hence none of the points $(s, s^2, 1)$ is external to $\mathcal{G}$. Hence $\mathcal{F}$ is internal to $\mathcal{G}$. This concludes the proof that $\mathcal{F}$ and $\mathcal{G}$ are mutually internal.

In order to prove that also the remaining two pairs of conics are mutually internal, we notice the existence of the helpful projectivity Π with the matrix

$$M(\Pi) = \begin{pmatrix} 0 & 1 & 1 \\ 2t & -1 & 1 \\ -2t & -1 & 1 \end{pmatrix}.$$

Using a computer algebra system it is straightforward to verify that this projectivity performs the cyclic shift of the three conics $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$. More precisely, $\Pi(\mathcal{F}) = \mathcal{H}$, $\Pi(\mathcal{H}) = \mathcal{G}$ and $\Pi(\mathcal{G}) = \mathcal{F}$. Since $\mathcal{F}$ and $\mathcal{G}$ are mutually internal, any two conics out of $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$ must be mutually internal, too. $\square$

Remark. Due to many conditions imposed on values a, b_1 and b_2, the very existence of the configuration may not be obvious. However, for $q > 5$ it is always possible to find an $a \in GF(q)$ such that $a \neq 1$, a is square and $a+1$ non-square. The determinant of the 2×2 linear system for b_1 and b_2 is then equal to $2(t^2 - 1) = 2(a-1)$, and hence for each such a there do exist (uniquely determined) values for parameters b_1 and b_2.

Planes of Order $q = 4r + 1$

Proposition 10.4.14 *Let q be a prime power with $q \equiv 1 \pmod 4$. Let $A = \{a_1, \ldots, a_m\}$ be a subset of $GF(q)$ such that $a_i \neq 0$ for $1 \leq i \leq m$ and $a_i^2 - a_j^2$ is non-square for each $1 \leq i, j \leq m$, $i \neq j$. In $PG(2, q)$, let $\mathcal{F}_i = V((a_i x)^2 - yz)$. Then each $\mathcal{F}_i$ is a non-singular conic and $\mathcal{S} = \cup_{1 \leq i \leq m} \mathcal{F}_i$ is a semioval in $PG(2, q)$. $\mathcal{S}$ consists of $m(q-1)+2$ points.*

q	m	A
5	2	$\{1,2\}$
9	2	$\{\xi,\xi^2\}$ (ξ prim. el. of $GF(9)$, $\xi^2=\xi+1$)
13	3	$\{1,3,4\}$
17	3	$\{1,2,7\}$
25	3	$\{\xi,\xi^2,\xi^6\}$ (ξ prim. el. of $GF(25)$, $\xi^2=\xi+3$)
29	4	$\{1,3,7,12\}$

Table 10.3: Examples of sets A applicable in Proposition 10.4.14.

Proof. Let $F_i=(a_ix)^2-yz$. The value of δ from Fact 10.1.7 is $a_i^2\neq 0$, hence $\mathcal{F}_i$ is non-singular. For $1\leq i<j\leq m$, the conics $\mathcal{F}_i$ and $\mathcal{F}_j$ have exactly two common points, namely $(0,0,1)$ and $(0,1,0)$. At both points have $\mathcal{F}_i$ and $\mathcal{F}_j$ common tangents ($V(y)$ and $V(z)$, respectively). Let Π be the projectivity given by the matrix

$$M(\Pi)=\begin{pmatrix} a_i & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

Π maps $\mathcal{F}_i$ to $V(x^2-yz)$ and $\mathcal{F}_j$ to $V((a_j/a_i)^2x^2-yz)$. Since $a_i^2-a_j^2$ is non-square, also $(a_i^2-a_j^2)/a_i^2$ is non-square and hence $(-(a_j/a_i)^2+1)\bar{x}^2$ is non-square for any $\bar{x}\in GF(q)^*$. But $(-(a_j/a_i)^2+1)\bar{x}^2$ is the value of the polynomial x^2-yz on a point $(\bar{x},\bar{y},\bar{z})\in V(((a_j/a_i)^2x^2-yz)$. Hence, $\mathcal{F}_j$ is internal to $\mathcal{F}_i$. Similarly we can show that $\mathcal{F}_i$ is internal to $\mathcal{F}_j$. Hence, $\mathcal{F}_j$ and $\mathcal{F}_i$ are mutually internal for any $i\neq j$, $\{i,j\}\subseteq\{1,\ldots,m\}$. Hence, $\mathcal{S}$ is a semioval. $\square$

Some maximal index sets A for initial values of q are shown in Table 10.3.

Proposition 10.4.15 *Let q be a prime power with $q\equiv 1 \pmod 4$. Let $A=\{a_1,\ldots,a_m\}$ be a subset of $GF(q)$ such that a_i-a_j is non-square for each $1\leq i,j\leq m$, $i\neq j$. In $PG(2,q)$, let $\mathcal{F}_i=V(x^2-a_iy^2-yz)$. Then each $\mathcal{F}_i$ is a non-singular conic and $\mathcal{S}=\cup_{1\leq i\leq m}\mathcal{F}_i$ is a semioval in $PG(2,q)$. $\mathcal{S}$ consists of $mq+1$ points.*

Proof. Let $F_i=x^2-a_iy^2-yz$. The value of δ from Fact 10.1.7 is equal to 1, hence $\mathcal{F}_i$ is non-singular. For $1\leq i<j\leq m$, the conics $\mathcal{F}_i$ and $\mathcal{F}_j$

q	m	A
5	2	$\{0,2\}$
9	3	$\{0,\xi,2\xi\}$ (ξ prim. el. of $GF(9)$, $\xi^2=\xi+1$)
13	3	$\{0,2,7\}$
17	3	$\{0,3,6\}$
25	5	$\{0,\xi,2\xi,3\xi,4\xi\}$ (ξ prim. el. of $GF(25)$, $\xi^2=\xi+3$)
29	4	$\{0,2,10,12\}$

Table 10.4: Examples of sets A applicable in Proposition 10.4.15.

have exactly one common point, namely $(0,0,1)$. At this point have $\mathcal{F}_i$ and $\mathcal{F}_j$ the common tangent $V(y)$. Let Π be the projectivity given by the matrix

$$M(\Pi)=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & a_i & 1 \end{pmatrix}.$$

Π maps $\mathcal{F}_i$ to $V(x^2-yz)$ and $\mathcal{F}_j$ to $V(x^2+(a_i-a_j)y^2-yz)$. Since a_j-a_i is non-square, also $(a_j-a_i)\bar{y}^2$ is non-square for any $\bar{y}\in GF(q)^*$. But $(a_j-a_i)\bar{y}^2$ is the value of the polynomial x^2-yz on a point $(\bar{x},\bar{y},\bar{z})\in V(x^2+(a_i-a_j)y^2-yz)$. Hence, $\mathcal{F}_j$ is internal to $\mathcal{F}_i$. Similarly we can show that $\mathcal{F}_i$ is internal to $\mathcal{F}_j$. Hence, $\mathcal{F}_j$ and $\mathcal{F}_i$ are mutually internal for any $i\neq j$, $\{i,j\}\subseteq\{1,\ldots,m\}$. Hence $\mathcal{S}$ is a semioval. $\square$

We display some maximal index sets A for initial values of q in Table 10.4. In this table, the rows corresponding to the order $q=p^2$ deserve special interest. We will need one technical lemma.

Lemma 10.4.16 *Let p be an odd prime, $q=p^2$ and let ξ be a primitive element of $GF(q)$. Consider $GF(p)$ as a subfield of $GF(q)$ with $GF(p)\cap GF(q)=\{0,1,\ldots,p-1\}$. For each $k\in GF(p)^*$, $k\xi$ is a non-square element of $GF(q)$.*

Proof. Let $\alpha=\xi^{p+1}$. Then $\alpha^{p-1}=\xi^{p^2-1}=1$ and $\alpha^i\neq\alpha^j$ for $1\leq i<j\leq p-1$. Hence, α is a primitive element of $GF(p)$. Hence,

$$\{1,2,\ldots,p-1\}=GF(p)^*=\{\xi^{t(p+1)}\mid 1\leq t\leq p-1\}.$$

It follows that

$$\{\xi,2\xi,\ldots,(p-1)\xi\}=\{\xi^{t(p+1)+1}\mid 1\leq t\leq p-1\}.$$

Since p is odd, $t(p+1)+1$ must be odd, too. Since ξ is primitive in $GF(q)$, ξ^s is non-square for any odd s. □

Proposition 10.4.17 *Let p be an odd prime, $q = p^2$. In $PG(2,q)$, Proposition 10.4.15 yields semiovals of size $q\sqrt{q}+1$.*

Proof. In Proposition 10.4.15, take $A = \{k\xi \mid k \in GF(p)\}$ where ξ is a primitive element of $GF(q)$. Then $m = |GF(p)| = \sqrt{q}$ and $|\mathcal{S}| = q\sqrt{q}+1$. Moreover, for any $a_i, a_j \in A$, $a_i \neq a_j$, we have $a_i - a_j = l\xi$ for some $l \in GF(p)^*$, hence $a_i - a_j$ is non-square. □

Remark. The construction given in Proposition 10.4.17 was first published (with a different proof) by Hirschfeld and Szőnyi in 1991, see Corollary 5.6 in (Hirschfeld, Szőnyi, 1991). It can be shown that the resulting semioval is regular and that it is a non-classical unital, see (Hirschfeld, Szőnyi, 1991) for details.

Planes of Order $q = 8r - 1$

Proposition 10.4.18 *Let q be a prime power with $q \equiv -1 \pmod 8$. In $PG(2,q)$, let $\mathcal{F} = V(x^2 - yz)$ and $\mathcal{G} = V(2x^2 + y^2 + z^2)$. Then $\mathcal{F}$ and $\mathcal{G}$ are non-singular conics and $\mathcal{F} \cup \mathcal{G}$ is a semioval in $PG(2,q)$ consisting of $2(q+1)$ points.*

Proof. First we examine common points of $\mathcal{F}$ and $\mathcal{G}$: From the system

$$\begin{array}{ccccccccc} 2x^2 & & & & & - & 2yz & = & 0 \\ 2x^2 & + & y^2 & + & z^2 & & & = & 0 \end{array}$$

we obtain

$$(y+z)^2 = 0.$$

Suppose $(\bar{x}, \bar{y}, \bar{z}) \in \mathcal{F} \cap \mathcal{G}$. Then $\bar{z} = -\bar{y}$ and so $\bar{x}^2 + \bar{y}^2 = 0$. Since $q = 8r - 1 = 4r' + 3$ ($r' \in \mathbb{N}$), -1 is non-square in $GF(q)$ by Fact 10.1.2. Hence, the last equation has the only solution $(\bar{x}, \bar{y}) = (0,0)$ implying $\bar{z} = 0$. But $(0,0,0)$ is not a point of $PG(2,q)$ and thus $\mathcal{F}$ and $\mathcal{G}$ are disjoint.

Using Fact 10.1.7 it is easy to verify that both $\mathcal{F}$ and $\mathcal{G}$ are non-singular. Next we want to show that $\mathcal{F}$ and $\mathcal{G}$ are mutually internal. We proceed in two steps.

(i) $\mathcal{F}$ is internal to $\mathcal{G}$. We have

$$\mathcal{F} = \{(0,1,0)\} \cup \{(s,s^2,1) \mid s \in GF(q)\}.$$

The polar of $(0,1,0)$ w.r.t. $\mathcal{G}$ is $V(y)$. We must decide the relative position of $V(y)$ and $\mathcal{G}$. The system

$$\begin{array}{ccccccc} 2x^2 & + & y^2 & + & z^2 & = & 0 \\ & & y & & & = & 0 \end{array}$$

leads to $2x^2 + z^2 = 0$. Since -2 is non-square (Fact 10.1.3), this system has none but the trivial solution. Hence $(0,1,0)$ is internal to $\mathcal{G}$.

The polar of $(s,s^2,1)$ w.r.t. $\mathcal{G}$ is $V(2sx + s^2y + z)$. We are about to solve the system

$$\begin{array}{ccccccc} 2x^2 & + & y^2 & + & z^2 & = & 0 \\ 2sx & + & s^2y & + & z & = & 0 \end{array}$$

Let $(\bar{x},\bar{y},\bar{z})$ be the solution. If $\bar{x} = 0$ then we obtain by substitution

$$\bar{y}^2 + (-s^2\bar{y})^2 = 0$$

which leads only to the trivial solution (and hence no crossing point). If $\bar{x} = 1$ then we eliminate $\bar{z}$ from the second equation and by substituting in the first we get

$$2 + \bar{y}^2 + (-2s - s^2\bar{y})^2 = 0.$$

This can be viewed as a quadratic equation in $\bar{y}$

$$(s^4+1)\bar{y}^2 + 4s^3\bar{y} + (4s^2+2) = 0.$$

The discriminant of this equation is

$$16s^6 - 4(s^4+1)(4s^2+2) = (-2) \cdot 2^2 \cdot (s^2+1)^2.$$

Since -1 is non-square, the discriminant is non-zero for any value of s. Moreover, since -2 is non-square, the entire discriminant is non-square and so the polar does not intersect $\mathcal{G}$. Thus, for any $s \in GF(q)$, the point $(s,s^2,1)$ is internal to $\mathcal{G}$.

(ii) Now we prove that $\mathcal{G}$ is internal to $\mathcal{F}$. The equation

$$2x^2 + y^2 + z^2 = 0$$

is equivalent to
$$-1/2(y+z)^2 = x^2 - yz.$$
Since -2 is non-square, $-1/2$ must be non-square, too. Hence for any point $(\bar{x}, \bar{y}, \bar{z}) \in V(2x^2 + y^2 + z^2)$ the value $\bar{x}^2 - \bar{y}\bar{z}$ is non-square which means that $\mathcal{G}$ is internal to $\mathcal{F}$. □

10.4.5 Semiovals with Deleted Points

It was observed by several authors that a new semioval may be obtained from a given one by deleting some of its points as long as no new tangents are introduced. This paradigm often applies to the configurations that we described in the preceding propositions. We include just one illustrative example.

Proposition 10.4.19 *Let q be an odd prime power and let $\mathcal{F}$ and $\mathcal{G}$ be conics in $PG(2,q)$ as in Proposition 10.4.12. Let $\mathcal{F} \cap \mathcal{G} = \{P, Q\}$. Then $\mathcal{F} \cup \mathcal{G} \setminus \{P, Q\}$ is a semioval in $PG(2,q)$.*

Proof. Let $\mathcal{S} = \mathcal{F} \cup \mathcal{G}$, $\mathcal{S}' = \mathcal{S} \setminus \{P, Q\}$ and similarly $\mathcal{F}' = \mathcal{F} \setminus \{P, Q\}$, $\mathcal{G}' = \mathcal{G} \setminus \{P, Q\}$. Let S_0 be any point in $\mathcal{S}'$. Clearly, the tangent t to $\mathcal{S}$ at S_0 is also a tangent to $\mathcal{S}'$. Suppose there is another tangent t' to $\mathcal{S}'$ at S_0. W.l.o.g. we may assume that $t' = l(PS_0)$ and that $S_0 \in \mathcal{F}'$. Since t' is a tangent, $t' \cap \mathcal{G}' = \emptyset$. Recall that $\mathcal{F}$ and $\mathcal{G}$ have a common tangent at P, hence $\{l(PX) \mid X \in \mathcal{F}'\} = \{l(PY) \mid Y \in \mathcal{G}'\}$. Hence t' must intersect $\mathcal{G}'$, a contradiction. □

10.5 Arcs

We now turn our attention to another geometric phenomenon, namely to the *arcs*.

Definition 10.5.1 *Let A be a point set in $PG(2,q)$. If no three points of A are collinear then the set A is called an* arc.

Definition 10.5.2 *Let A be an arc in $PG(2,q)$. We say that A is a* complete arc *if there is no arc A' in $PG(2,q)$ such that A is a proper subset of A'.*

Definition 10.5.3 *If A is an arc in $PG(2,q)$, $|A| = k$, then A is sometimes also called a k-*arc.

Fact 10.5.4 *Let A be an arc in $PG(2,q)$. If q is odd then $|A| \leq q+1$. If q is even then $|A| \leq q+2$.*

Proof. Hirschfeld (1979), pp. 164. □

If q is odd then any $(q+1)$-arc is a non-singular conic.

If q is even then a $(q+2)$-arc is called a *hyperoval.* Each hyperoval is either *regular* in which case it is the union of a conic and its nucleus (a point where all tangents meet), or *irregular*. The complete classification of hyperovals in $PG(2,2^r)$ is known only for $r \leq 4$. If $r \leq 3$ then each hyperoval is regular. For $r = 4$ an irregular hyperoval was found by Lunelli and Sce in 1957 using a computer. Later it was shown that (up to projectivity) there are no more hyperovals in $PG(2,16)$.

The catalogs of *all* arcs in $PG(2,q)$ (up to projectivity) have been known for $q \leq 13$. For $q \leq 9$, the lists can be found in (Hirschfeld, 1979), pp. 387–414. For $q = 11$ and $q = 13$ the lists were computed by Gordon (1993).

10.5.1 Constructions

Following Definition 10.5.1, if $\chi_A \in \{0,1\}^{S(2,q)}$ is a characteristic function of a set A which is an arc then this function satisfies the predicate $P(\chi_A)$:="No three points of A are collinear."

This predicate P is consistent with augmentation (Definition 6.2.10) and hence we can use it to control the restricted orderly generation (Section 6.2.2).

Using restricted orderly generation, we have listed the full catalog of arcs in $PG(2,16)$. The statistics on them is in Table 10.5.

Just before finishing the thesis we learned that Tim Penttila (personal communication, August 1994), Gordon Royle and Michael Simpson at the University of Western Australia recently used the same idea (orderly generation) to compile the catalogs of arcs for $q = 16, 17, 19$.

k	number of k-arcs	number of complete k-arcs
1	1	0
2	1	0
3	1	0
4	1	0
5	4	0
6	61	0
7	454	0
8	2633	0
9	6014	6
10	4899	1944
11	1171	113
12	587	32
13	260	1
14	100	0
15	30	0
16	9	0
17	3	0
18	2	2

Table 10.5: Number of k-arcs in $PG(2, 16)$ up to projectivity.

10.5.2 Analysis of Results

It has been known that, in $PG(2, 16)$, the second greatest value of k for which a complete k-arc exists is $k = 13$. A complete 13-arc in $PG(2, 16)$ was constructed by Fisher, Hirschfeld and Thas (1986). From our catalog it follows that this complete 13-arc is unique.

The analysis of the catalogs by Penttila, Royle and Simpson is currently undertaken by de Resmini and Scipioni. Our catalogs will be analyzed in our cooperation with Storme.

10.6 Methodological Aspects

In this chapter we have proven that the restricted orderly generation is a useful approach for listing interesting configurations in finite classical planes. We applied this approach for computer-aided study of two geometric phenomena in classical planes of small orders. It was not surprising that the constructive methods have produced many yet unknown instances of these phenomena. It was more pleasant to observe that these concrete instances can be developed to rigorous theorems of general nature.

Chapter 11

Linear Codes

In this chapter we will be using orderly generation to classify (up to equivalence) certain optimal ternary linear codes. After giving all necessary definitions from coding theory we explain the classification problem in Section 11.2. Then in Section 11.3 we embed this classification task in the "symmetry classes of mappings" paradigm. In the last two sections we discuss the relevancy of computer-aided methods for classifications in coding theory.

11.1 Definitions

Let $GF(q)^n$ denote the n-dimensional vector space over $GF(q)$. Let $\mathbf{0} \in GF(q)^n$ be the zero vector.

Definition 11.1.1 *Let $x \in GF(q)^n$ and let $\mathrm{wt}(x)$ denote the number of non-zero coordinates in x. We say that $\mathrm{wt}(x)$ is the* weight *of the vector x.*

Definition 11.1.2 *Let $x, y \in GF(q)^n$. We define the* Hamming distance *of x and y by*

$$d(x,y) := \mathrm{wt}(x-y).$$

The value $d(x,y)$ is equal to the number of coordinates in which x and y differ. Hamming distance is a metric on $GF(q)^n$.

Definition 11.1.3 *We say that C is an $[n,k,d]$* linear code over *$GF(q)$ if C is a k-dimensional subspace of $GF(q)^n$ and*

$$\min_{x \in C,\ x \neq \mathbf{0}} \mathrm{wt}(x) = d.$$

For a classical textbook on linear codes we refer to (MacWilliams, Sloane, 1977).

In this chapter we deal only with linear codes, hence we will omit this adjective in the following. The codes over $GF(q)$ for $q = 2, 3, \ldots$ are called *binary, ternary,...* (in general *q-ary*) codes.

Fact 11.1.4 *Let C be an $[n,k,d]$ q-ary code. Then*

$$\min_{x,y \in C,\ x \neq y} d(x,y) = d.$$

The values n, k, d in Definition 11.1.3 are called *length*, *dimension* and *minimum distance* of the code C. The elements of C are called *codewords*.

The minimum distance of C is of essential importance when C is used for information transmission. Roughly spoken, the greater the distance between the codewords is, the better chances we have to properly recognize the codewords at the receiving end even if they are spoiled by noise that occurred during the transmission.

Definition 11.1.5 *Let C be an $[n,k,d]$ q-ary code. The polynomial $\sum_{i=0}^{n} A_i y^i$, where A_i is the number of weight i codewords in C, will be called the* weight enumerator *of C.*

Definition 11.1.6 *Let C be an $[n,k,d]$ q-ary code. We say that C is an* optimal code *if there is no $[n,k,d']$ q-ary code with $d' > d$.*

Definition 11.1.7 *Let C be an $[n,k,d]$ q-ary code and let M be a $k \times n$ matrix over $GF(q)$ such that C is generated by the rows of M. We say that M is a* generator matrix *for C.*

Definition 11.1.8 *Let C be an $[n,k,d]$ q-ary code. If there exists a matrix M such that M a is generator matrix for C and the columns of M are n pairwise different points in $PG(k-1,q)$ then we say that C is a* projective code*.*

Fact 11.1.9 *Let C be a projective $[n,k,d]$ q-ary code. Then the columns of any generator matrix for C are pairwise different points in $PG(k-1,q)$.*

The following fact can be used to prove that certain codes must be projective (in the case that they exist at all).

Fact 11.1.10 *Let C be an $[n,k,d]$ q-ary code and let M be a generator matrix for C. Suppose that no coordinate of C is identically zero, i.e., M does not contain a zero column. If C is not projective then there exists an $[n-2,k-1,d']$ q-ary code with $d' \geq d$.*

Proof. (MacWilliams, Sloane, 1977), p. 592. □

Definition 11.1.11 *A* permutation matrix *is any $n \times n$ matrix P that has exactly one 1 in each row and each column; other entries of P are all 0. A* diagonal matrix *is any $n \times n$ matrix $D = (l_{i,j})$ such that $d_{i,j} \neq 0$ exactly if $i = j$.*

Definition 11.1.12 *Let C_1, C_2 be two $[n,k,d]$ q-ary codes. We say that the codes C_1 and C_2 are* equivalent *if there exists a generator matrix M_1 for C_1 and a generator matrix M_2 for C_2 such that $M_2 = M_1 DP$ for some diagonal matrix D and for some permutation matrix P.*

Informally, if codes C_1 and C_2 are equivalent then C_2 can be obtained from C_1 by multiplying the i-coordinate of each codeword by a non-zero scalar a_i and applying one arbitrary but fixed permutation $\pi \in S_{\underline{n}}$ to all vectors.

11.2 Classification of Optimal Codes

There are two classical problems related to optimal codes:

(i) Given n, k and q, determine

$$d_q(n,k) := \max\{d \mid \text{an } [n,k,d] \ q\text{-ary code exists}\}.$$

(ii) Given n, k, q and $d_q(n,k)$, determine (up to equivalence) all $[n,k,d_q(n,k)]$ q-ary codes.

Much more is known about *(i)* as compared to *(ii)*. For example, in the case $q = 2$ the exact value of $d_2(n,k)$ is known for any pair (n,k) such that $k \leq 7$, and for many more combinations of n and k. A table of known lower and upper bounds on d_2 is periodically published, see (Brouwer, Verhoeff, 1993) for the most recent edition. An up-to-date on-line data base of known lower and upper bounds on $d_q(n,k)$ for $q = 2,3,4$ and $n \leq 130$ ($n \leq 255$ for $q = 2$) is maintained by Brouwer. This data base can be accessed by sending an e-mail message to `aeb@cwi.nl` with subject line `exec lincodbd`.

In this chapter we are concerned with the problem *(ii)*, i.e., with *classification* of certain optimal codes (namely those optimal codes that are projective). We will be particularly dealing with the case $q = 3$ (ternary codes) and $k = 4, 5$.

Before approaching the classification task, we will rephrase it in terms of the "symmetry classes of mappings" paradigm which will then let us exploit the methods of Chapter 6.

11.3 Group Action Setting

Definition 11.3.1 *Let $S(k-1,q)$ denote the point set of $PG(k-1,q)$.*

We denote by $PGL(k,q)$ the group of all projectivities of $PG(k-1,q)$. We now think of the projective points as *column* vectors, hence the action of a projectivity $\Pi \in PGL(k,q)$ on a point $X \in S(k-1,q)$ is simply $\Pi : X \mapsto M(\Pi) \cdot X$ where $M(\Pi)$ is a matrix representing Π.

Definition 11.3.2 *Let $P = \{P_1,\dots,P_n\}$ and $Q = \{Q_1,\dots,Q_n\}$ be two subsets of $S(k-1,q)$. We say that P and Q are* projectively equivalent sets *if their characteristic functions $\chi_P, \chi_Q \in \{0,1\}^{S(k-1,q)}$ belong to the same $PGL(k,q)$-orbit on $\{0,1\}^{S(k-1,q)}$.*

Fact 11.3.3 *Let C_1 and C_2 be two projective $[n,k,d]$ q-ary codes. Let C_1 have a generator matrix M_1 whose columns are points $P_1,\dots,P_n \in S(k-1,q)$ and let C_2 have a generator matrix M_2 whose columns are points $Q_1,\dots,Q_n \in S(k-1,q)$. The codes C_1 and C_2 are equivalent (Definition 11.1.12) if and only if the sets $\{P_1,\dots,P_n\}$ and $\{Q_1,\dots,Q_n\}$ are projectively equivalent.*

Proof. If C_1 and C_2 are equivalent then there is a matrix M_2' such that (i) M_2' can be obtained from the matrix M_2 by permuting its columns and multiplying them by $GF(q)$-scalars, (ii) M_2' generates the code C_1. From (ii) it follows that there is a $k \times k$ invertible matrix L over $GF(q)$ such that $L \cdot M_1 = M_2'$. Since L is invertible, it represents a projectivity, hence the set $\{P_1,\dots,P_n\}$ is projectively equivalent to the set of columns of M_2' (regarded as projective points). But the latter one is equal to $\{Q_1,\dots,Q_n\}$, hence $\{P_1,\dots,P_n\}$ and $\{Q_1,\dots,Q_n\}$ are projectively equivalent.

Now suppose that the sets $\{P_1,\dots,P_n\}$ and $\{Q_1,\dots,Q_n\}$ are projectively equivalent. Then there is a projectivity $\Pi \in PGL(k,q)$ such that $\Pi\chi_P = \chi_Q$. Let $M(\Pi)$ be one of the $q-1$ matrices representing Π. Since

$M(\Pi)$ is invertible, $M(\Pi) \cdot M_1$ generates the code C_1. The columns of $M(\Pi) \cdot M_1$ are the projective points $M(\Pi) \cdot P_1, \ldots, M(\Pi) \cdot P_n$. Moreover, we know that $\{M(\Pi) \cdot P_1, \ldots, M(\Pi) \cdot P_n\} = \{Q_1, \ldots, Q_n\}$ (as sets of projective points). This means that the columns of M_2 are obtained by permuting columns of $M(\Pi) \cdot M_1$ and multiplying them by $GF(q)$-scalars. Since $M(\Pi) \cdot M_1$ generates C_1 and M_2 generates C_2, the codes C_1 and C_2 are equivalent. □

We now introduce the notion of a configuration in $PG(k-1, q)$ similarly as we did it in Definition 10.2.6 for $PG(2, q)$.

Definition 11.3.4 *Recall that $S(k-1, q)$ means the point set of $PG(k-1, q)$. Let G be the projective group $PGL(k, q)$ and let $f \in \{0, 1\}^{S(k-1,q)}$. The orbit $G(f)$ is called a* configuration *in $PG(k-1, q)$.*

The relation between finite spaces and projective codes is widely used. To document this, we refer at least to a long series of papers by Hamada and co-workers who related certain optimal projective codes (namely those meeting the Griesmer bound) to certain geometric configurations (so-called "minihypers"), see (Hamada, Helleseth, 1990), (Hamada, Helleseth, 1992), (Hamada, Helleseth and Ytrehus, 1993) as well as about 20 other papers in that series. For other examples of geometric proofs in classification of codes see (van Eupen, 1993).

11.4 Constructions

Fact 11.3.3 states that equivalence classes of k-dimensional q-ary projective codes are in a one-to-one correspondence with configurations in $PG(k-1, q)$. From Chapter 10 we know that orderly methods can be used for (possibly restricted) generation of configurations, hence we will be able to use these methods for classification of projective codes.

In this chapter we deal with ternary codes, i.e., we will be listing configurations in $PG(k-1, 3)$. We restrict our attention to the *optimal* codes (see Definition 11.1.6).

Using Fact 11.1.10 and tables of values of $d_3(n, k)$ (see, e.g., Table I in (van Eupen, 1993)) we can determine whether, for given n and k, all $[n, k, d_3(n, k)]$ ternary codes must be projective. If so, then we can generate all n-point configurations in $PG(k-1,3)$, for each configuration compute the minimum distance of the corresponding projective code, and single out the codes with minimum distance equal to $d_3(n,k)$. This way we can list all pairwise non-isomorphic $[n,k,d_3(n,k)]$ codes.

The total number of configurations in $PG(k-1,3)$ can be evaluated by unweighted Pólya's Theorem 2.1.25 using the cycle index of $PGL(k,3)$'s action on $S(k-1,3)$.

space	total number of configurations
$PG(3,3)$	111,832
$PG(4,3)$	11,180,165,801,375,240,179,617,696

Table 11.1: Total number of configurations in some $GF(3)$-spaces.

Table 11.1 reveals that *all* configurations in $PG(3,3)$ can be listed without problems. The orderly generation of l-point configurations in $PG(3,3)$ for $l \leq 20$ takes about 8 CPU hours on an SGI workstation. The (non-canonical) representatives of the remaining configurations are obtained by complementation.

Hence, we can classify up to equivalence all optimal 4-dimensional ternary codes if these happen to be projective. The upper part of Table 11.2 shows the statistics.

In the case of $PG(4,3)$, Table 11.1 documents that generation of all configurations is impossible. Since the orderly generation proceeds by content (Theorem 6.2.8) and taking into account the unimodality of the number of symmetry classes of mappings (see (Kerber, 1991), p. 237 for details on this), we might want to undertake the full generation of l-point configurations for some $l \leq l_{\max}$ and then proceed by restricted generation. Pólya's Theorem 2.1.23 for enumeration of symmetry classes by content can help us to find a feasible value of $l_{\max}$. For example, there are exactly 9,260 eleven-point configurations in $PG(4,3)$. By a complete generation of all l-point configurations ($1 \leq l \leq 11$) we classify the optimal projective codes with parameters [6,5,2] up to [11,5,6], see the lower part of Table 11.2.

From this place on, the full generation would be very time and space consuming. Fortunately, we note that the next three triples of optimal projective code parameters (namely, [14,5,7], [15,5,8] and [16,5,9]) all satisfy the equality $n - d_3(n,k) = 7$ which proposes an idea for a predicate that would control the restricted generation. This predicate, however, is not consistent with augmentation (Definition 6.2.10) because the value $n - d$ can increase when we lengthen the code. On the other hand, the difference $n - d$ can never decrease by augmentation, because, when adding one coordinate to a given code, its minimum distance cannot increase by more than 1. Hence, the weaker predicate $P'(\chi_S)$:="parameters n, d of the code corresponding to the projective set S satisfy $n - d \leq 7$" is consistent with augmentation, and we can use it to control the restricted orderly generation (Section 6.2.2) to determine the bottom three rows of Table 11.2.

11.5 Analysis of Results

In Table 11.2 we display the basic statistics of the classifications that we obtained.

In collaboration with van Eupen we collected references on the codes and/or geometric descriptions of them, see the last column of Table 11.2.

Most of the references contain the complete classification proof (theoretical or computer-based); in general they give geometric description of the code(s) or at least geometric constraints on the corresponding configurations in $PG(k-1,3)$.

In the trivial cases when there is no particular paper dealing with the respective triple of parameters we include the geometric description of the code, i.e., we characterize the set of points in $PG(k-1,3)$ which form the columns of the generator matrix for the respective code. To keep Table 11.2 in a modest size we allowed us a little sloppiness in these descriptions: For example, the phrase "$PG(3,3)$ minus a hyperplane" should be interpreted as

$$S(3,3) \setminus \{P \in S(3,3) \,|\, P \in H\}, \qquad H \text{ a fixed hyperplane in } PG(3,3).$$

(Cf. Definition 11.3.1.) The remaining descriptions should be interpreted in a similar manner.

In the current collaboration of Lisoněk and van Eupen (1994) we look for theoretical proofs for some of the computer-based classifica-

$[n,k,d]$	number of classes	reference or description
[5,4,2]	1	
[7,4,3]	4	
[8,4,4]	3	
[9,4,5]	1	(van Eupen, 1993), Lemma 3
[10,4,6]	1	(van Eupen, 1993), Lemma 3
[17,4,10]	18	
[18,4,11]	2	
[19,4,12]	1	(Hamada, Helleseth, 1990)
[25,4,16]	1	(Hamada, Helleseth, 1992)
[26,4,17]	1	(Hamada, 1993), Theorem 3.1
[27,4,18]	1	$PG(3,3)$ minus a hyperplane
[30,4,19]	8	(Hamada, Helleseth, Ytrehus, 1993)
[31,4,20]	2	(Hamada, 1993), Theorem 3.4.(7)
[32,4,21]	1	(Hamada, 1993), Theorem 3.1
[34,4,22]	3	(Helleseth, 1992), Theorem 2
[35,4,23]	1	(Hamada, 1993), Theorem 3.1
[36,4,24]	1	$PG(3,3)$ minus a line
[38,4,25]	1	$PG(3,3)$ minus two points
[39,4,26]	1	$PG(3,3)$ minus a point
[40,4,27]	1	$PG(3,3)$
[6,5,2]	1	
[8,5,3]	3	
[9,5,4]	1	
[10,5,5]	1	(van Eupen, 1993), Lemma 4
[11,5,6]	1	dual of the Golay code
[14,5,7]	236	
[15,5,8]	4	
[16,5,9]	1	(van Eupen, Hill, 1994), Lemma 10

Table 11.2: Number of some optimal ternary codes (up to equivalence).

tions from Table 11.2 in the cases that have not been treated in the literature yet.

For example, the computer-based result that there are exactly two [18,4,11] codes together with the fact that Hamada-Helleseth (1990) uniqueness construction of the [19,4,12] code uses one distinguished point (point Q in their paper) inspired us to the following theoretic classification of [18,4,11] codes:

(i) One shows that any [18,4,11] code is obtained by puncturing the [19,4,12] code. (Puncturing a code means simply deleting one coordinate from it.)

(ii) One shows that the automorphism group of the [19,4,12] code has two orbits; one of them being the singleton $\{Q\}$, the other one being the set of the remaining 18 points. This means that there are (up to equivalence) two ways to puncture the [19,4,12] code. Finally one shows that these two puncturings give non-equivalent codes. (The resulting codes have different weight enumerators.)

11.6 Methodological Aspects

Similarly as in Chapter 10 we found the concept of configurations and their orderly generation to be a fruitful approach to obtain new results in the respective field. In coding theory this approach seems to be a novelty application of the "symmetry classes of mappings" paradigm. Computer-based results inspire theoretical proofs, moreover the methods of these proofs may be reusable also for other instances. For example, the idea of [18,4,11] code classification (see the end of the preceding section) can be modified for the purpose of [19,5,11] code classification, i.e., for parameters that are out-of-reach of the direct computer approach (orderly generation). Hence, also in this field we succeeded to ascend the creativity spiral of computer-assisted algebraic combinatorics.

References

Abramov, S.A. (1971). On the summation of rational functions. *Zh. vycisl. matem. i matem. fiz.* **11**, 1071–1075. (In Russian.)

Abramov, S.A. (1975). The rational component of the solution of a first-order linear recurrence relation with a rational right-hand side. *Zh. vycisl. matem. i matem. fiz.* **15**, 1035–1039. (In Russian.)

Appel, K., Hakken, W. (1986). The Four Color proof suffices. *Math. Intell.* **8**, 10–20.

Arden, B.W., Lee, H. (1981). Analysis of chordal ring network. *IEEE Trans. Comp.* **30**, 291–295.

Artemi, C., Alexandru, T. (1987). Mathematical modeling of polymers, Part II. *Match* **22**, 33–66.

Beezer, R.A. (1991). *Generating Catalogs of Regular Graphs.* Technical Report 91-1. Department of Mathematics and Computer Science, The University of Puget Sound, Tacoma.

Bergeron, F. (1993). Surprising mathematics using a computer algebra system. *J. Symb. Comp.* **15**, 365–370.

Bergeron, F., Plouffe, S. (1992). Computing the generating function of a series given its first few terms. *Experimental Mathematics* **1**, 307–312.

Beyer, T., Hedetniemi, S.M. (1980). Constant time generation of rooted trees. *SIAM J. Comput.* **9**, 706–712.

Biggs, N.L. (1989). *Discrete Mathematics.* Oxford: Clarendon Press.

Blokhuis, A. (1991). Characterization of seminuclear sets in a finite projective plane. *J. Geometry* **40**, 15–19.

Blokhuis, A., Szőnyi, T. (1992). Note on the structure of semiovals in finite projective planes. *Discr. Math.* **106/107**, 61–65.

Bokowski, J., Sturmfels, B. (1989). *Computational Synthetic Geometry.* Lecture Notes in Mathematics 1355. Berlin: Springer.

Boreham, T.G., Bouwer, I.Z., Frucht, R. (1974). *A Useful Family of Bicubic Graphs.* In *Graphs and Combinatorics,* 213–225. Berlin: Springer.

Borwein, J., Borwein, P. (1992). Some observations on computer aided analysis. *Not. Amer. Math. Soc.* **39**, 825–829.

Bosma, W., Cannon, J. (1993). *Handbook of Magma Functions.* Department of Pure Mathematics, University of Sydney.

Brawley, J.V. Jr. (1967). Enumeration of canonical sets by rank. *Amer. Math. Monthly* **74**, 175–177.

Brawley, J.V. Jr., Lisoněk, P. (1992). *Counting Equivalence Classes of Hadamard Pattern Sets by Group Action Methods.* Technical Report. RISC-Linz Series 92-28.

Brinkmann, G. (1992). *Generating Cubic Graphs Faster than Isomorphism Checking.* Technical Report 92-047. Department of Mathematics, University of Bielefeld.

Brouwer, A.E., Verhoeff, T. (1993). An updated table of minimum-distance bounds for binary linear codes. *IEEE Trans. Inform. Theory*, **IT-33**, 662–677.

Buchberger, B. (1991). Should students learn integration rules? *SIGSAM Bull.* **24**, 10–17.

Buchberger, B. (1993). *Mathematica: A System for Doing Mathematics by Computer?* Invited talk at DISCO'93, Gmunden, Austria, September 1993. RISC-Linz Series 93-50.

Colbourn, C.J., Read, R.C. (1979). Orderly algorithms for generating restricted classes of graphs. *J. Graph Th.* **3**, 187–195.

Comtet, L. (1974). *Advanced Combinatorics.* Dodrecht: D.Riedel.

Coxeter, H.S.M. (1950). Self-dual configurations and regular graphs. *Bull. Amer. Math. Soc.* **56**, 413–455.

de Finis, M. (1987). On semiovals in projective planes. *Ars Comb.* **24A**, 65–70.

Dixon, J.D., Wilf, H.S. (1983). The random selection of unlabeled graphs. *J. Algorithms* **4**, 205–213.

Ehrhart, E. (1977). *Polynômes Arithmétiques et Méthode des Polyèdres en Combinatoire.* Basel: Birkhäuser Verlag. (In French.)

El-Basil, S. (1988). Binomial-combinatorial properties of Clar structures. *Discr. Appl. Math.* **19**, 145–156.

Ethier, S.N., Hodge, S.E. (1985). Identity by descent analysis of sibship configurations. *Amer. J. of Medical Genetics* **22**, 263–272.

Fajtlowicz, S. (1988). On conjectures of Graffiti. *Discr. Math.* **72**, 113–118.

Fajtlowicz, S. (1991). *Written on the Wall.* Technical Report, Department of Mathematics, University of Houston.

Fajtlowicz, S. (1992). Personal communication.

Fishburn, P.C., Hwang, F.K., Lee, H. (1986). Do local majorities force a global majority? *Discr. Math.* **61**, 165–179.

Fisher, J.C., Hirschfeld, J.W.P., Thas, J.A. (1986). Complete arcs in planes of square order. *Ann. Discrete Math.* **30**, 243–250.

Folk, R., Kartashov, A., Lisoněk, P., Paule, P. (1993). Symmetries in neural networks: a linear group action approach. *J. Phys. A: Math. Gen.* **26**, 3159–3164.

Folk, R., Kartashov, A., Ortbauer, M. (1992). *Equivalence Classes of Hadamard Pattern Sets for Hebbian Networks.* Institute for Theoretical Physics, J. Kepler University Linz.

Fredricksen, H. (1982). A survey of full length nonlinear shift register algorithms. *SIAM Review* **24**, 195–221.

Fredricksen, H., Kessler, I. (1986). An algorithm for generating necklaces of beads in two colors. *Discr. Math.* **61**, 181–188.

Fredricksen, H., Maiorana, J. (1978). Necklaces of beads in k colors and k-ary de Bruijn sequences. *Discr. Math.* **23**, 207–210.

Frucht, R. (1976). A canonical representation of trivalent Hamiltonian graphs. *J. Graph Th.* **1**, 45–60.

Gärtner, J. (1986). *Summation in Finite Terms—Presentation and Implementation of M. Karr's Algorithm.* Diploma Thesis. RISC-Linz Series 86-10.

Gilbert, E.N., Riordan, J. (1961). Symmetry types of periodic sequences. *Ill. J. Math.* **5**, 657–665.

Gordon, C.E. (1993). *Orbits of Arcs in Projective Spaces.* In *Finite Geometry and Combinatorics,* 161–174. (F. De Clerck, ed.) Cambridge: Cambridge University Press.

Gosper, R. Wm. Jr. (1976). *A Calculus of Series Rearrangements.* In *Proceedings of Algorithms and Complexity.* New York: Academic Press.

Gosper, R.W. (1978). Decision procedures for indefinite hypergeometric summation. *Proc. Natl. Acad. Sci. U.S.A.* **75**, 40–42.

Graham, R.L., Knuth, D.E., Patashnik, O. (1989). *Concrete Mathematics. A Foundation for Computer Science*. Second Printing, December 1988. Reading: Addison-Wesley.

Gropp, H. (1992). Enumeration of regular graphs 100 years ago. *Discr. Math.* **101**, 73–85.

Grund, R. (1992). Symmetrieklassen von Abbildungen und die Konstruktion von diskreten Strukturen. *Bayreuther Math. Schriften* **31**, 19–54. (In German.)

Hager, R., Kerber, A., Laue, R., Moser, D., Weber, W. (1991). Construction of orbit representatives. *Bayreuther Math. Schriften* **35**, 157–169.

Hamada, N. (1993). A survey of recent work on characterization of minihypers in $PG(t,q)$ and nonbinary linear codes meeting Griesmer bound. *J. Combin. Inform. Syst. Sci.* **18**, 161–191.

Hamada, N., Helleseth, T. (1990). A characterization of some $\{3v_2, 3v_1; t, q\}$-minihypers and some $\{2v_2 + v_{\gamma+1}, 2v_1 + v_\gamma; t, q\}$-minihypers ($q = 3$ or 4, $2 \leq \gamma < t$) and its applications to error-correcting codes. *Bulletin of Osaka Women's University* **27**, 49–107.

Hamada, N., Helleseth, T. (1992). A characterization of some $\{2v_{\alpha+1} + v_{\gamma+1}, 2v_\alpha + v_\gamma; k-1, 3\}$-minihypers and some $(n, k, 3^{k-1} - 2 \cdot 3^\alpha - 3^\gamma; 3)$-codes meeting the Griesmer bound. *Discr. Math.* **104**, 67–81.

Hamada, N., Helleseth, T., Ytrehus, Ø. (1993). Characterization of $\{2(q+1)+2, 2; t, q\}$-minihypers in $PG(t,q)$ $(t \leq 3,\ q \in \{3,4\})$. *Discr. Math.* **115**, 175–185.

Harary, F., Palmer, E. (1973). *Graphical Enumeration.* New York: Academic Press.

Hardy, G.H., Wright, E.M. (1990). *Introduction to the Theory of Numbers.* Fifth Print. Oxford: Clarendon Press.

Harrison, M.A. (1965). *Introduction to Switching and Automata Theory.* New York: McGraw-Hill.

Harrison, M.A. (1973). On the number of classes of binary matrices. *IEEE Trans. Comp.* **C-22**, 1048–1052.

Helleseth, T. (1992). Projective codes meeting the Griesmer bound. *Discr. Math.* **106/107**, 265–271.

Hirschfeld, J.W.P. (1979). *Projective Geometries over Finite Fields.* Oxford: Clarendon Press.

Hirschfeld, J.W.P., Szőnyi, T. (1991). Sets in a finite plane with few intersection numbers and a distinguished point. *Discr. Math.* **97**, 229–242.

Hodges, J.H. (1958). Scalar polynomial equations for matrices over a finite field. *Duke Math. Journal* **25**, 291–296.

Horgan, J. (1993). The death of proof. *Scientific American* **269**, 74–82.

Hoskins, W.D., Penfold Street, A. (1982). Twills on a given number of harnesses. *J. Austral. Math. Soc. (A)* **33**, 1–15.

Hughes, D.R., Pipper, F.C. (1982). *Projective Planes.* New York: Springer.

Kerber, A. (1991). *Algebraic Combinatorics via Finite Group Action.* Mannheim: BI Wissenschaftsverlag.

Kerber, A., Laue, R., Hager, R. and Weber, W. (1990). Cataloging graphs by generating them uniformly at random. *J. Graph Th.* **14**, 559–563.

Knuth, D.E. (1981). *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms.* Second Edition. Reading: Addison-Wesley.

Koornwinder, T.H. (1992). *On Zeilberger's Algorithm and Its q-analogue: A Rigorous Description.* Report AM-R9207. CWI, Amsterdam.

Krishnamurthy, V. (1986). *Combinatorics: Theory and Applications.* Chichester: Ellis Horwood Ltd.

Kung, J.P.S. (1981). The cycle structure of a linear transformation over a finite field. *Lin. Alg. Appl.* **36**, 141–155.

Lafon, J.C. (1983). *Summation in finite terms.* In *Computer Algebra and Symbolic Computation*, 71–77. Second Edition. Wien: Springer.

Lam, C.W.H. (1993). *Application of Group Theory to Combinatorial Searches.* In *Groups and Computation*, 133-138. (Finkelstein, L., Kantor, W.M., eds.) DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Volume 11. Rutgers University.

Lam, C.W.H., Thiel, L.H., Swiercz, S. (1989). The non-existence of finite projective planes of order 10. *Canad. J. of Math.* **XLI**, 1117–1123.

Lang, S. (1984). *Algebra. Second Edition.* Redwood City: Addison-Wesley.

Laue, R. (1989). Eine konstruktive Version des Lemmas von Burnside. *Bayreuther Math. Schriften* **28**, 111-125. (In German.)

Laue, R. (1993). Construction of combinatorial objects—a tutorial. *Bayreuther Math. Schriften* **43**, 53–96.

Lidl, R., Niederreiter, H. (1983). *Finite Fields.* Encyclopedia of Mathematics, Vol. 20. Reading: Addison-Wesley.

Lidl, R., Niederreiter, H. (1986). *Introduction to Finite Fields and their Applications.* Cambridge: Cambridge University Press.

Lisoněk, P. (1991). *The Performance of Gosper's Algorithm on Rational Function Inputs.* Technical Report, RISC-Linz Series 91-31.

Lisoněk, P., Paule, P., Strehl, V. (1993). Improvement of the degree setting in Gosper's algorithm. *J. Symb. Comp.* **16**, 243–258.

Lisoněk, P., van Eupen, M. (1994). Classifications of some optimal ternary codes. In preparation.

MacLane, S. (1994). Response to Horgan's "Death of proof". *Not. Amer. Math. Soc.* **41**, 573.

MacMahon, P.A (1984). *Combinatory Analysis.* Third Edition. New York: Chelsea.

MacWilliams, F.J., Sloane, N.J.A. (1977). *The Theory of Error-Correcting Codes.* Eight Printing. Amsterdam: North-Holland.

McKay, B.D. (1990). *nauty User's Guide*. Technical Report TR-CS-90-02, Australian National University, Department of Computer Science.

McKay, B.D., Radziszowski, S.P. (1993). *New Ramsey Number:* $R(4,5) = 25$. Communicated by electronic means on March 19, 1993.

Moenck, R. (1977). *On Computing Closed Forms for Summations.* In *Proceedings of MACSYMA users' conference*. Berkeley.

Nijenhuis, A., Wilf, H.S. (1978). *Combinatorial Algorithms for Computers and Calculators.* Orlando: Academic Press.

Paule, P. (1992). Greatest-factorial factorization and symbolic summation I. *J. Symb. Comp.,* submitted. Technical Report. RISC-Linz Series 93-02.

Paule, P., Strehl, V. (1991). *A Remark on an Instance of Gosper's Algorithm.* Technical Report. RISC-Linz Series 91-14.

Petkovšek, M. (1992). Hypergeometric solutions of linear recurrences with polynomial coefficients. *J. Symb. Comp.* **14**, 243–264.

Pirastu, R. (1992). *Algorithmen zur Summation rationaler Funktionen*. Diploma Thesis, Univ. Erlangen-Nürnberg. (In German.)

Pirastu, R., Strehl, V. (1994). Rational summation and Gosper-Petkovšek representation. *J. Symb. Comp.*, submitted.

Plouffe, S. (1992). *Approximations de Séries Génératrices et Quelques Conjectures*. Montréal, Bordeaux: Master's Thesis. (In French.)

Popoviciu, T. (1953). Asupra unei probleme de partiţie a numerelor. *Acad. R.P.R., Filiala Cluj, Studie şi cercetari şiintifice* **4**, 7–58. (In Rumanian.)

Read, R.C. (1978*a*). Every one a winner. *Ann. Discr. Math.* **2**, 107–120.

Read, R.C. (1978*b*). On general dissections of a polygon. *Aeq. Math.* **18**, 370–388.

Reiner, D.L. (1985). Enumeration in music theory. *Amer. Math. Monthly* **92**, 51–54.

Riordan, J. (1958). *An Introduction to Combinatorial Analysis.* New York: John Wiley & Sons.

Robinson, R.W., Wormald, N.C. (1983). Numbers of cubic graphs. *J. Graph Th.* **7**, 463–467.

Ruskey, F., Savage, C., Wang, T.M. (1992). Generating necklaces. *J. Algorithms* **13**, 414–430.

Salvy, B., Zimmermann, P. (1993). Gfun: A Maple package for the manipulation of generating and holonomic functions in one variable. To appear in *ACM Trans. in Math. Software.*

Sanders, D.P. (1994). A new proof of the Four Color Theorem. *Newsletter of the SIAM Activity Group on Discrete Mathematics* **4**, No. 4 (Summer 1994), 6–7.

Schmalz, B. (1990). Verwendung von Untergruppenleitern zur Bestimmung von Doppelnebenklassen. *Bayreuther Math. Schriften* **31**, 109–143. (In German.)

Shiloach, Y. (1981). Fast canonization of circular strings. *J. Algorithms* **2**, 107–121.

Sloane, N.J.A. (1973). *A Handbook of Integer Sequences*. New York: Academic Press. Second Edition, to appear.

Stanley, R.P. (1986). *Enumerative Combinatorics. Volume I.* Monterey: Wadsworth & Brooks.

Stockmeyer, P.K. (1974). *The Charm Bracelet Problem and its Applications.* In *Graphs and Combinatorics*, Proceedings Capital Conference, Washington, DC 1973, 339–349, Lecture Notes in Mathematics Vol. 406. Berlin: Springer.

Stong, R. (1988). Some asymptotic results on finite vector spaces. *Adv. Appl. Math.* **9**, 167–199.

Thas, J.A. (1974). On semi ovals and semi ovoids. *Geom. Dedicata* **3**, 229–231.

Vajda, S. (1967). *Patterns and Configurations in Finite Spaces.* New York: Hafner.

van der Poorten, A. (1979). A proof that Euler missed ... Apéry's proof of the irrationality of $\zeta(3)$. *Math. Intell.* **1**, 195–203.

van Eupen, M. (1993). Four non-existence results for ternary linear codes. *IEEE Trans. Inform. Th.,* submitted.

van Eupen, M., Hill, R. (1994). An optimal ternary $[69, 5, 45]$ code and related codes. *Designs, Codes and Cryptography* **4**, 271–282.

van Lint, J.H., Wilson, R.M. (1992). *A Course in Combinatorics.* Cambridge: Cambridge University Press.

Walsh, T.R. (1983). Generating non-isomorphic maps without storing them. *SIAM J. Alg. Disc. Math* **4**, 161–178.

Wang, T.M., Savage, C.D. (1990). *A New Algorithm for Generating Necklaces.* In *Proceedings of the Twenty-eighth Annual Allerton Conference on Communication, Control, and Computing.* October 1990, 72–81.

Whitworth, W.A. (1959). *Choice and Chance.* Fifth Edition. New York: Hafner.

Wilf, H.S. (1993). *generatingfunctionology.* Second Edition. Boston: Academic Press.

Wilf, H.S., Zeilberger, D. (1992). An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities. *Invent. Math.* **108**, 575–633.

Woodall, D.R. (1992). Local and global proportionality. *Discr. Math.* **102**, 315–328.

Wright, R.A., Richmond, B., Odlyzko, A., McKay, B. (1986). Constant time generation of free trees. *SIAM J. Comput.* **15**, 540–548.

Zeilberger, D. (1990*a*). A holonomic systems approach to special function identities. *J. Comp. Appl. Math.* **32**, 321–368.

Zeilberger, D. (1990*b*). A fast algorithm for proving terminating hypergeometric identities. *Discr. Math.* **80**, 207–211.

Zeilberger, D. (1993). Theorems for a price: Tomorrow's semi-rigorous mathematical culture. *Not. Amer. Math. Soc.* **40**, 978–981.

Curriculum Vitae

Personal

name	Petr Lisoněk
born	April 17, 1964
marital status	single, no children
citizenship	Czech Republic
languages	English, German (fluent)

Education

1970–1978	ground school, Olomouc, Czech Republic
1978–1982	high school, Olomouc, Czech Republic
1982–1987	undergraduate studies in Computer Science Palacký University, Olomouc, Czech Republic M.Sc. with honors
1990–1994	graduate studies Research Institute for Symbolic Computation, J. Kepler University, Linz, Austria

Employment

1987–1990	assistant professor Department of Computer Science, Palacký University, Olomouc, Czech Republic
1993	development of CAD/CAM software (5 months, full-time) Gödel School Ges.m.b.H., Hagenberg, Austria
1993–1994	teaching assistant Software Engineering College, Hagenberg, Austria

Conferences, Lectures

August 1993	contributed talk *CAYLEY/MAGMA Conference on Computational Algebra*, Queen Mary and Westfield College, London, Great Britain

September 1993	contributed talk *Workshop "Symbolic Computation in Combinatorics"* Cornell University, Ithaca, NY, U.S.A.
March 1994	invited lectures Technical University Eindhoven, The Netherlands University of Ghent, Belgium
June 1994	invited lecture Technical University of Denmark, Lyngby

Papers Related to Ph.D. Thesis

Lisoněk, P., Paule, P., Strehl, V. (1993). Improvement of the degree setting in Gosper's algorithm. *J. Symb. Comp.* **16**, 243–258.

Lisoněk, P. (1993*a*). Local and global majorities revisited. *Discr. Math.,* accepted.

Lisoněk, P. (1993*b*). Denumerants and their approximations. *Journal of Comb. Math. and Comb. Computing,* accepted.

Folk, R., Kartashov, A., Lisoněk, P., Paule, P. (1993). Symmetries in neural networks: a linear group action approach. *J. Phys. A: Math. Gen.* **26**, 3159–3164.

Lisoněk, P. (1994*a*). Closed forms for the number of polygon dissections. *J. Symb. Comp.,* submitted.

Lisoněk, P., van Eupen, M. (1994). Classifications of some optimal ternary codes. In preparation.

Lisoněk, P. (1994*b*). Some constructions of semiovals in $PG(2,q)$. In preparation.

Other Research Papers

Bajer, J., Lisoněk, P. (1991). Symbolic computation approach to nonlinear dynamics. *Journal of Modern Optics* **38**, 719–729.