Extended Euclidean Algorithm

Johannes Middeke

Summer Term 2019

Notation 1. Let $A \in R^{m \times n}$ be an m-by-n matrix with entries in a commutative ring R. We denote by $\gcd(A)$ the greatest common divisor of all the entries of A.

Notation 2. We use $\mathit{Swap}_{j,k}$ to refer to the (unimodular[1]) elementary matrix which swaps the j^{th} with the k^{th} row. We write $\mathit{Add}_{j,k}(x)$ for the (unimodular) elementary matrix which adds x times the k^{th} row to the j^{th} row.

Theorem 3. *Let R be a commutative ring. Let $A \in R^{m \times n}$ and $B \in R^{n \times p}$. Then*

$$\gcd(A)\gcd(B) \mid \gcd(AB).$$

Proof. Write $A = \gcd(A)\tilde{A}$ and $B = \gcd(B)\tilde{B}$ for some $\tilde{A} \in R^{m \times n}$ and $\tilde{B} \in R^{n \times p}$. Then

$$AB = \gcd(A)\gcd(B)\tilde{A}\tilde{B},$$

implying that $\gcd(A)\gcd(B) \mid AB$ which proves the theorem. □

Corollary 4. *Let $A \in R^{m \times n}$, $P \in \mathrm{GL}_m(R)$, and $Q \in \mathrm{GL}_n(R)$. Then*

$$\gcd(PA) = \gcd(A) = \gcd(AQ).$$

Proof. By Theorem 3,

$$\gcd(A) \mid \gcd(PA) \mid \gcd(P^{-1}PA) = \gcd(A).$$

Thus, $\gcd(A) = \gcd(PA)$. The other identity is proved in the same way. □

Algorithm 5 (Extended Euclidean Algorithm).

Input $v \in R^n$ where R is a Euclidean ring with degree $\deg\colon R \setminus \{0\} \to \mathbb{N}$.

Output $Q \in \mathrm{GL}_n(R)$ such that $Qv = (\gcd(v), 0, \ldots, 0)^t$.

Procedure

(a) If $v = 0$, then return $Q = \mathbf{1}_n$.

(b) If v has only one non-zero entry v_j, then return $Q = \mathit{Swap}_{1,j}$.

(c) If v has at least two different non-zero components v_j and v_k where $\deg v_j \leqslant \deg v_k$, then:

[1] A matrix with entries in R is unimodular if and only if its determinant is a unit in R if and only if it has an inverse with entries in R.

(1) Let $v_k = qv_j + r$ with $r = 0$ or $\deg r < \deg v_j$.
(2) Apply the algorithm recursively $v' = Add_{k,j}(-q)\,v$ obtaining Q'.
(3) Return $Q = Q'\,Add_{k,j}(-q)$.

Theorem 6. *Algorithm 5 is correct and terminates.*

Proof. We first check the correctness: If the algorithm terminates in step (a) or (b), then the output is obviously correct. It it reaches step (c), then $Qv = Q'\,Add_{k,j}(-q)\,v = Q'v' = (\gcd(v'), 0, \ldots, 0)^t = (\gcd(v), 0, \ldots, 0)^t$ where the last identity follows from Theorem 3 since $Add_{k,j}(-q)$ is unimodular.

We now check termination: Here, we only need to consider step (c). For $w \in R^n$ and $w \neq 0$, define a *size* $\delta(w) = \sum_{j, w_j \neq 0}(1 + \deg w_j) \geqslant 0$. We claim that $\delta(v) > \delta(v')$: The only entry of v' which changes compared to v is its k^{th} entry where v_k is replaced by $r = v_k - qv_j$. Since either $r = 0$ or $\deg r < \deg v_k$, we have indeed $\delta(v) > \delta(v')$. That means, that in every recursive call the size of the argument decreases which can only happen finitely often. Thus, step (c) cannot be executed infinitely often meaning that eventually one of the conditions in the previous two steps must hold and the algorithm terminates. □

Note 7. For actual computations, the following variant of Algorithm 5 is useful:

(a) Form the extended matrix $A = (v \mid \mathbf{1}_n)$.

(b) If $A = \left(\begin{array}{c|c} x & \multirow{2}{*}{Q} \\ 0 & \end{array}\right)$ with $x \in R$, then return Q.

(c) Let k be such that $A_{k,1}$ is a non-zero entry of the first column of A of minimal degree.[2] Exchange the k^{th} and first row of A.

(d) For $j = 2, \ldots, n$ such that $v_j \neq 0$: Let $v_j = qv_1 + r$ where $r = 0$ or $\deg r < \deg v_j$; and subtract q times the first row of A from the j^{th} row.

(e) Go to step (b).

It is easy to check that the above steps do the same computations as Algorithm 5 unrolled into an imperative programming style and with a stricter order of the eliminations. The first column of A corresponds to the (current instance of the) vector v while the identity matrix is used to record the row transformations.

Example 8. For $R = \mathbb{Z}$, consider

$$\left(\begin{array}{c|ccc} 33 & 1 & 0 & 1 \\ 55 & 0 & 1 & 0 \\ 121 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{c|ccc} 33 & 1 & 0 & 1 \\ 55 & 0 & 1 & 0 \\ 11 & 0 & -2 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{c|ccc} 33 & 1 & 0 & 1 \\ 0 & 0 & 11 & -5 \\ 11 & 0 & -2 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{c|ccc} 0 & 1 & 6 & -3 \\ 0 & 0 & 11 & -5 \\ 11 & 0 & -2 & 1 \end{array}\right)$$

which implies that $\gcd(33, 55, 121) = 11$.

[2] That is, $A_{k,1} \neq 0$ and $\deg A_{j,1} \geqslant \deg A_{k,1}$ for all $= 1, \ldots, n$.