CS855: Parallel GCD Algorithms

Marc Moreno Maza

February 19, 2008

- Why are GCD algorithms difficult to parallelize?
- Parallel GCD algorithm for integers.
- GCDs of univariate polynomials.
- Parallel polynomial GCD algorithms based on Linear Algebra.

- Specifying the input.
- Notion of a reduction.
- The algorithms of Kannan, Miller and Rudolph.

Notations 1 *Let $u \geq v$ be positive integers. We define:*

$$n = \ell_2(u) \quad \text{and} \quad m = \ell_2(v). \tag{1}$$

where

$$\ell_2(x) = \begin{cases} \lfloor \log_2(x) \rfloor + 1 & \text{if} \quad x \geq 1, \\ 1 & \text{if} \quad x = 0. \end{cases} \tag{2}$$

Hence we have

$$2^{n-1} \leq u < 2^n \quad \text{and} \quad 2^{m-1} \leq u < 2^m. \tag{3}$$

We define

$$\rho = \rho(u, v) = \ell_2(u) - \ell_2(v) + 1. \tag{4}$$

We have

$$2^{\rho-2} < u/v < 2^{\rho}. \tag{5}$$

Definition 1 *A* reduction *is a map*

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N}^{\times} & \rightarrow & \mathbb{N} \times \mathbb{N} \\ (u, v) & \longmapsto & (v, R(u, v)) \end{array} \tag{6}$$

such that the following holds for every $(u, v) \in \mathbb{N} \times \mathbb{N}^{\times}$*:*

1. $0 \leq R(u, v) < v$,
2. *there exists* $\alpha \in \mathbb{N}^{\times}$ *such that* $\gcd(v, R(u, v)) = \alpha \gcd(u, v)$.

- In practice, the coefficient α can be easily computed.
- Computing $\gcd(u, v)$ reduces to a finte sequence of transformations $(u, v) \longmapsto (v, R(u, v))$.
- The idea of parallel algorithms for computing integer GCDs is to find a reduction such that
  - $R(u, v)$ can be computed in $O(\mathrm{loglog}(n))$ (with $n = \ell_2(u) \geq \ell_2(v)$).
  - few transformations $(u, v) \longmapsto (v, R(u, v))$ are needed, say $O(n/\log(n))$ of them.

Example 1 The *Euclidean* reduction:

$$R(u,v) = u - qv \quad \text{where} \quad q = \lfloor u/v \rfloor. \tag{7}$$

In this case $\alpha = 1$.

Example 2 The well-known *Binary* reduction is based on:

$$R(u,v) = (u-v)/2 \quad \text{where} \quad u \equiv v \mod 2 \tag{8}$$

In this case $\alpha = 2$.

Example 3 The popular *bmod* reduction is based on:

$$R(u,v) \;= \mid u - xv \mid /2^{\rho(u,v)} \quad \text{where} \quad v \equiv 1 \mod 2 \tag{9}$$

and

$$x \equiv (u/v) \mod 2^{\rho(u,v)}. \tag{10}$$

In this case $\alpha = 2^{\rho(u,v)}$. This reduction is sometimes unproperly presented. So, let us show that the above division by $2^{\rho(u,v)}$ is exact. There exists

$a, b \in \mathbb{Z}$ such that we have:

$$av + b2^{\rho(u,v)} = 1. \tag{11}$$

Hence, we have:

$$x \equiv ua \mod 2^{\rho(u,v)}. \tag{12}$$

We can choose x such that the Euclidean division of ua by $2^{\rho(u,v)}$ returns some y as quotient and x as remainder. Thus, we have:

$$ua = x + y2^{\rho(u,v)}. \tag{13}$$

Therefore, we have:

$$\begin{aligned} u - xv &= u - (ua - y2^{\rho(u,v)})v \\ &= u - uav + y2^{\rho(u,v)}v \\ &= u(1 - av) + y2^{\rho(u,v)}v \\ &= ub2^{\rho(u,v)} + y2^{\rho(u,v)}v \\ &= (ub + vy)2^{\rho(u,v)}. \end{aligned} \tag{14}$$

- The principle of this algorithm.
- The Pigeonhole Principle.
- The reduction of Kannan, Miller and Rudolph.
- The algorithm of Kannan, Miller and Rudolph.

For $p = 1 \cdots n$, compute q the quotient in the division of pu by v. Hence we have:

$$0 \leq pu - qv < v. \tag{15}$$

Using the *pigeonhole principle*, the algorithm exhibits two pairs (p_1, q_1) and (p_2, q_2) such that

- the numbers $p_1 u - q_1 v$ and $p_2 u - q_2 v$ agree at least on $\log(n)$ leading bits (where $n = \ell_2(u)$), and thus,
- the difference $(p_1 - p_2)u - (q_1 - q_2)v$ has at most $n - \log(n)$ bits.

Define the reduction $R(u, v) = (p_1 - p_2)u - (q_1 - q_2)v$.

- It turns out that $R(u, v)$ can be computed in parallel in $O(\log \log n)$ machine-word operations using $O(n^2 \log^2 n)$ processors.
- Leading to a *sublinear time* algorithm running in $O(n \log \log n / \log n)$ machine-word operations.

There are mainly two difficulties with this approach.

- We may have $\gcd(u,v) \neq \gcd(R(u,v),v)$.
- How to find the numbers $p_1u - q_1v$ and $p_2u - q_2v$ fast enough?

The first difficulty is solved by the following result.

Lemma 1 *If $g = \gcd(u,v)$ and $h = \gcd(pu - qv, v)$ then $g \mid h$ and $(h/g) \mid p$ both hold.*

Proof. Let d be a divisor of u and v. Then d divides $pu - qv$ and v, and thus, their GCD. Hence, g divides h. Now, let us define $h/g = f$. Observe that f divides both v and $pu - qv + qv = pu$. Let e be an irreducible factor of f. If e divides u then it divides v and u, and thus, it divides g; a contradiction. Hence e does not divides u, showing that f must divide p. $\square$

Since $\mid p \mid \leq n$, then p is **small** comparing to u. Thus the factor f is small too and the following trick can be used:

- Removing (in advance) from u and v all common prime factors less than n guarantees $f = 1$ and thus $h = g$.
- Can be done in parallel time $O(\log(n))$ using $O(n^2 \log^2 n)$ processors.

Lemma 2 (Pigeonhole Principle) *Let α and β be two positive integers. Let f be a map from $[0,\alpha]\cap\mathbb{Z}$ to $[0,\beta]\cap\mathbb{Z}$. Then, there exists $x_1, x_2 \in [0,\alpha]\cap\mathbb{Z}$ with $x_1 \neq x_2$ such that we have:*

$$\mid f(x_1) - f(x_2) \mid \leq \frac{\beta}{\alpha}. \tag{16}$$

PROOF. By contradiction, we assume that the conclusion is false. Let $y_0 \leq \cdots \leq y_\alpha$ be the values taken by f in $[0,\beta]$. Then we have

$$\begin{array}{rcl} y_\alpha - y_0 & \geq & \sum_{i=0}^{i=\alpha-1} y_{i+1} - y_i \\ & > & \alpha\frac{\beta}{\alpha} \\ & > & \beta \end{array} \tag{17}$$

A contradiction. $\square$

Note that if $\alpha > \beta$, then there exists $x_1, x_2 \in [0,\alpha]\cap\mathbb{Z}$ such that we have $f(x_1) = f(x_2)$. That is the usual formulation of the *Pigeonhole Principle.*

Lemma 3 (Kannan, Miller and Rudolph) *Assume that $u \leq vn$ holds. Then, there exists $p, q \in \mathbb{Z}$ with $(p, q) \neq (0, 0)$ such that we have*

$$\mid p \mid \leq \frac{nv}{u}, \ \mid q \mid \leq n \ \text{ and } \ 0 \leq pu - qv \leq \frac{2u}{n}. \tag{18}$$

Proof. By Euclidean division, for every $p \in \mathbb{Z}$ there exists $q \in \mathbb{Z}$ s. t.:

$$0 \leq pu - qv < v. \tag{19}$$

Then, assuming $\mid pu \mid \leq nv$, one deduces $\mid q \mid \leq n$, as required.

We observe also that for every p satisfying $0 \leq p \leq \frac{nv}{u}$, we obatin a unique q satisfying (19). Hence, the number of couples (p, q) with $0 \leq p \leq \frac{nv}{u}$ and satisfying (19) is $\lfloor nv/u \rfloor + 1$. For each of them, the value of $pu - qv$ belongs to $[0, v]$. By *Pigeonhole Principle* there exist two different couples (p_1, q_1) and (p_2, q_2) with $0 \leq p_i \leq \frac{nv}{u}$ and $\mid q_i \mid \leq n$, for $i = 1, 2$ and satisfying

$$0 \leq (p_1 u - q_1 v) - (p_2 u - q_2 v) \leq \frac{v}{\lfloor nv/u \rfloor} \leq \frac{2v}{nv/u} = \frac{2u}{n} \tag{20}$$

Finally, $(p_1 - p_2)u - (q_1 - q_2)v$ is the desired combination. $\square$

We do not give the full details but only the key points.

- The reduction $R(u, v) = (p_1 - p_2)u - (q_1 - q_2)v$ assumes $u \leq vn$.
- If this consition does not hold, then a *Long Division* is used.
- It is clear that $R(u, v)$ achieves its goal: we obtain an integer whose length has reduced at least by $\log(n)$ bits.
- Analyzing the complexity of computing $R(u, v)$:
  - Observe that the number of couples (p, q) with $0 \leq p \leq \frac{nv}{u}$ and satisfying (19) is in $O(n)$.
  - Thus the number of $(p_1u - q_1v) - (p_2u - q_2v)$ is in $O(n^2)$.
  - The algorithm calls $R(u, v)$ only with input u and v of length at most $2\log^2(n)$. (We have to admit that.) Then, the parallel time for one addition/multiplication of two numbers of such length is in $O(\log\log n)$ and requires $O(\log^2(n))$ processors.
  - Therefore, $R(u, v)$ can be computed in parallel time $O(\log\log n)$ using $O(n^2\log^2(n))$ processors.

- The resultant.
- The GCDs.
- Computing GCDs via Linear Algebra.

Proposition 1 *Let $f, g \in \mathbb{K}[x]$ be two polynomials of positive degree. The following conditions are equivalent.*

1. *The polynomials f, g have a common factor of positive degree.*
2. *There exists $(u, v) \in \mathbb{K}[x] \times \mathbb{K}[x]$, with $(u, v) \neq (0, 0)$, such that*

$$uf + vg = 0, \; \deg(u) < \deg(g) \; \text{ and } \; \deg(v) < \deg(f). \tag{21}$$

Proof. First assume that there exists $d \in \mathbb{K}[x]$ with positive degree and dividing f and g. Let $f_1, g_1 \in \mathbb{K}[x]$ be such that $f = f_1 d$ et $g = g_1 d$. Then $(u, v) := (g_1, -f_1)$ satisfies Relation (21).

Assume now that Relation (21) holds for a couple $(u, v) \in \mathbb{K}[x] \times \mathbb{K}[x]$. We may assume $u \neq 0$. In addition, we assume that f and g does not have a common factor of positive degree. This implies that f and g are relatively prime. Hence, there exist $a, b \in \mathbb{K}[x]$ such that $af + bg = 1$ and we have:

$$u = (af + bg)u = afu + bgu = -agv + bgu = (bu - va)g.$$

Since $u \neq 0$, we deduce $\deg(u) \geq \deg(g)$. A contradiction. $\square$

Definition 2 *Let $f = a_m x^m + \cdots + a_1 x + a_0$ and $g = b_n x^n + \cdots + b_1 x + b_0$ be non-zero polynomials of respective degrees m and n such that $n + m > 0$.*

$$\begin{pmatrix}
a_m & 0 & \cdots & 0 & b_n & 0 & \cdots & 0 \\
a_{m-1} & a_m & \ddots & \vdots & b_{n-1} & b_n & \ddots & \vdots \\
a_{m-2} & a_{m-1} & \ddots & 0 & b_{n-2} & b_{n-1} & \ddots & 0 \\
\vdots & & \ddots & a_m & \vdots & & \ddots & b_n \\
 & \vdots & & a_{m-1} & & \vdots & & b_{n-1} \\
a_0 & & & & b_0 & & & \\
0 & a_0 & & \vdots & 0 & b_0 & & \vdots \\
\vdots & \ddots & \ddots & & \vdots & \ddots & \ddots & \\
0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & b_0
\end{pmatrix}$$

is the Sylvester matrix *of f and g; it is a square matrix of order $n + m$*

with coefficients in $\mathbb{K}$*, denoted by* $\text{sylv}(f, g)$*. Its determinant is denoted by* $\text{res}(f, g)$ *and called the* resultant *of* f *and* g*.*

Now, we assume $n < m$*. For* $0 \leq i \leq n$*, we consider the* $(n + m - 2i) \times (n + m + 2i)$*-submatrix of* $\text{sylv}(f, g)$ *which consists of*

- *the first* $(n + m - 2i)$ *rows from the first* $n - i$ *columns of the* f*'s, followed by*
- *the first* $(n + m - 2i)$ *rows from the first* $m - i$ *columns of the* g*'s.*

This matrix is denoted by $\text{psubres}(f, g, i)$ *and is called often the* i*-th* principal subresultant *of* f *and* g*.*

Proposition 2 *Let $f, g \in \mathbb{K}[x]$ be two polynomials of positive degrees. Then, the following conditions are equivalent.*

1. *The polynomials f, g have a common factor of positive degree.*
2. $\mathrm{res}(f, g) = 0$.

Proof. We can turn the problem (21) into a linear system. Indeed, let

$$u = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \quad \text{and} \quad v = d_{m-1}x^{m-1} + \cdots + d_1 x + d_0$$

Then, the equation $uf + vg = 0$ becomes the linear system below

$$\left\{ \begin{array}{ccccccccc} a_m c_{n-1} & & & + & b_n d_{m-1} & & & = & 0 \\ a_{m-1} c_{n-1} & + & a_{m-} c_{n-2} & + & b_{n-1} d_{m-1} & + & b_n d_{m-2} & = & 0 \\ & \ddots & & & & \ddots & & & \vdots \\ & & a_0 c_0 & + & & & b_0 d_0 & = & 0 \end{array} \right. \tag{22}$$

with $\mathrm{sylv}(f, g)$ as matrix and with $w = {}^t(c_{n-1}, \ldots, c_1, c_0, d_{m-1}, \ldots, d_1, d_0)$ as unknown vector. The trivial solution ${}^t(0, \ldots, 0)$ is the unique one if and only its determinant $\mathrm{res}(f, g)$ is not zero. Therefore, by virtue of Proposition 1, we have $\deg(\gcd(f, g)) > 0$ if and only $\mathrm{res}(f, g) = 0$. $\square$

Proposition 3 *The polynomials $f, g \in \mathbb{K}[x]$ with positive degrees are relatively prime iff there exists a unique $(u, v) \in \mathbb{K}[x] \times \mathbb{K}[x]$ such that*

$$uf + vg = 1, \ (u, v) \neq (0, 0), \ \deg(u) < \deg(g) \ \text{ and } \ \deg(v) < \deg(f). \quad (23)$$

Proof. The condition is sufficient. Let us prove it is necessary. By running the EEA, one can compute $s, t \in \mathbb{K}[x]$ such that $sf + tg = 1$. Let q_s and r_s be the quotient and the remainder of s w.r.t. g. Then, we define

$$u = r_s \ \text{ and } \ v = fq_s + t.$$

We obtain

$$uf + vg = fr_s + (fq_s + t)g = f(q_s g + r_s) + tg = 1$$

In addition, we have $\deg(u) < \deg(g)$. Since we have $\deg(uf) = \deg(vg)$ we deduce $\deg(v) < \deg(f)$. Therefore, the couple (u, v) can be viewed as a solution of the linear system obtained from Relation (22) by replacing the last 0 (in the right-hand sides of the equalities) by 1. The determinant of this new linear system is $\mathrm{res}(f, g)$. We conclude with Proposition 2. $\square$

Let $r_0 = f, r_1 = g, \ldots, r_\ell \neq 0, r_{\ell+1}$ the sequence of the **monic** remainders in the EEA applied to (f, g); thus r_ℓ is a GCD of f and g. Let $(s_0, t_0), (s_1, t_1), \ldots, (s_\ell, t_\ell), (s_{\ell+1}, t_{\ell+1})$ be the sequence of *Bézout coefficients* computed by the EEA applied to (f, g). Hence, we have $s_i f + t_i g = r_i$ for $0 \leq i \leq \ell + 1$. We define $n_i = \deg(r_i)$ for $0 \leq i \leq \ell + 1$. Then, the following is well known: for $2 \leq i \leq \ell + 1$ we have

$$\deg s_i = n_1 - n_{i-1} \quad \text{and} \quad \deg t_i = n_0 - n_{i-1}. \tag{24}$$

The sequence $n_0, n_1, n_2, \ldots, n_\ell$ is the *degree sequence* of the the EEA applied to (f, g). We will use another property of the EEA in $\mathbb{K}[x]$. Let $r, s, t \in \mathbf{k}[x]$, with $t \neq 0$, be polynomials such that

$$r = sf + tg \quad \text{and} \quad \deg r + \deg t < \deg f. \tag{25}$$

Let $j \in \{1, \ldots, k+1\}$ be such that $\deg r_j \leq \deg r < \deg r_{j-1}$. Then, there exists a non-zero $\alpha \in \mathbf{k}[x]$ such that we have

$$r = \alpha r_j, s = \alpha s_j \quad \text{and} \quad t = \alpha t_j. \tag{26}$$

Proposition 4 *Let $0 \leq k \leq n \leq m$ be a non-negative integer. Then k does not appear in the degree sequence if and only if there exists $s, t \in \mathbb{K}[x]$ satisfying*

$$t \neq 0, \quad \deg s < \deg g - k, \quad \deg t < \deg f - k, \quad \deg(sf + tg) < k. \tag{27}$$

Proof. First, suppose that k does not appear in the degree sequence. Then, there exists an i with $2 \leq i \leq \ell + 1$ such that $n_i < k < n_{i-1}$. We claim that $s = s_i$ and $t = t_i$ do the job. We have:

$$sf + tg = r_i \;\text{ and }\; \deg(r_i) = n_i < k. \tag{28}$$

We deduce: $\deg s = n_1 - n_{i-1} < n - k$ and $\deg t = n_0 - n_{i-1} < m - k$. Second, suppose there exist $s, t \in \mathbb{K}[x]$ satisfying (27). Define $r = sf + tg$. Then we have $\deg r + \deg t < m = \deg f$. Appying one of the properties recalled above, there exists $\alpha \in \{1, \ldots, \ell + 1\}$ and $\alpha \in \mathbb{K}[x] \; \{0\}$ such that $t = \alpha t_i$ and $r = \alpha r_i$. We deduce:

$$m - n_{i-1} \leq \deg\alpha + n - n_{i-1} = \deg(\alpha t_i) = \deg t < m - k, \tag{29}$$

and:

$$n_i \leq \deg\alpha + n_i = \deg(\alpha r_i) = \deg r < k. \tag{30}$$

Together these imply $n_i < k < n_{i-1}$, as required. $\square$

As we did, for the resultant, we shall translate Proposition 4 into the language of linear algebra. We consider the map

$$\phi_{f,g} : \begin{array}{lcl} \mathbb{K}[x] \times \mathbb{K}[x] & \to & \mathbb{K}[x] \\ (s,t) & \longmapsto & sf + tg \end{array} \tag{31}$$

For $d \in \mathbb{N}$ we let $P_d = \{a \in \mathbb{K}[x] \mid \deg a < d\}$ and we define $P_0 = \{0\}$.

The restriction of $\phi_{f,g}$ to $\phi_0 : P_n \times P_m \to P_{n+m}$ is a $\mathbb{K}$-linear mapping between vector spaces of the same dimension and we have:

1. $\gcd(f,g) = 1 \iff \phi_0$ isomorphism,
2. If $\gcd(f,g) = 1$, then the Bézout coefficients (s_ℓ, t_ℓ) computed by the EEA are the unique solution in $P_n \times P_m$ of the linear system $\phi_0(s,t) = 1$.

Consider k as in Proposition 4 with $k > 0$. The restriction of $\phi_{f,g}$ to $P_{n-k} \times P_{m-k} \to P_{n+m-k}$ is a $\mathbb{K}$-linear mapping between vector spaces of **different** dimension. In fact, we consider

$$\phi_k : \begin{array}{ccc} P_{n-k} \times P_{m-k} & \to & P_{n+m-2k} \\ (s,t) & \longmapsto & (sf + tg) \text{ quo } x^k \end{array} \tag{32}$$

Proposition 5 *Let $0 \leq k \leq n \leq m$ and $0 \leq i \leq \ell$. Then, we have:*

(i) k appears in the degree sequence of the EEA applied to (f,g) if and only if ϕ_k is an isomorphism,

(ii) If $k = n_i$, then the Bézout coefficients (s_i, t_i) computed by the EEA are the **unique** *solution (s,t) of the linear system of $\phi_k(s,t) = 1$.*

PROOF. From Proposition 4 we have $k \notin \{n_i \ \mid \ \{0 \leq i \leq \ell\}$ if and only if there exists a nonzero couple $(s,t) \in P_{n-k} \times P_{m-k}$ such that $\phi_k(s,t) = 0$, that is, if and only if ϕ_k is not injective. Note that we have used the fact:

$$s \neq 0 \ \text{ and } \ \phi_k(s,t) = 0 \quad \Rightarrow \quad t \neq 0. \tag{33}$$

This proves (i). We note that if $k = n_i$, then we have $s_i \in P_{n-k}$, $t_i \in P_{m-k}$ and $\phi_k(s_i, t_i) = 1$. Since ϕ_k is an isomorphism in thsi case, we proved (ii).
$\square$

$$\begin{pmatrix}
a_m & 0 & \cdots & 0 & b_n & 0 & \cdots & 0 \\
a_{m-1} & a_m & \ddots & \vdots & b_{n-1} & b_n & \ddots & \vdots \\
\vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\
a_{n-m+k+1} & & & a_m & b_{n-m+k+1} & & & b_n \\
\vdots & & & \vdots & \vdots & & & \vdots \\
a_{k+1} & & & a_n & b_{k+1} & & & b_n \\
\vdots & & & \vdots & \vdots & & & \vdots \\
\vdots & & & \vdots & \vdots & & & \vdots \\
a_{2k-n+1} & \cdots & \cdots & a_k & b_{2k-m+1} & \cdots & \cdots & b_k
\end{pmatrix}$$

Proposition 6 *For* $0 \leq i \leq n$, *let* $p_i = \det \operatorname{psubres}(f, g, i)$. *Define*

$$n_1, \ldots, n_k = i \;\mid\; 0 \leq i \leq n \quad \text{with} \quad p_i \neq 0. \tag{34}$$

Then, we have

$$n = n_1 > n_2 > \cdots > n_k = \deg(f, g). \tag{35}$$

For $1 \leq d \leq k$, let $i := n_d$. Consider the linear system

$$\operatorname{psubres}(f, g, i) \begin{pmatrix} y_{n-i-1} \\ \vdots \\ y_1 \\ y_0 \\ z_{m-i-1} \\ \vdots \\ z_1 \\ z_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \tag{36}$$

Define $s_d = y_{n-i-1}x^{n-i-1} + y_0$, $t_d = z_{m-i-1}x^{m-i-1} + z_0$ and $r_d = s_d f + t_d g$. Then, $r_d = s_d f + t_d g$ is (up to a non-zero scalar) the d-th row in the Extended Euclidean Algorithm and r_k is a GCD of f and g.