Computing multivariate polynomial GCDs using sparse interpolation:

the problem of unlucky evaluation points and evaluation cost.

Michael Monagan

SCG, October 5th, 2015.

This is joint work with Adriano Aarce, Lucas Hu, John Kluessner and Hao Zhuang.

The GCD Problem

Input: A and B in $\mathbb{Z}[x_0, x_1, \ldots, x_n]$. **Output:** $G = \gcd(A, B)$.

Assume: $G = x_0^d + \sum_{i=0}^{m-1} c_i(x_1, \ldots, x_n) x_0^i$.
For prime p and points $\alpha_j \in \mathbb{Z}_p^n$ interpolate c_i from images

$$\gcd(A(x_0, \alpha_j), B(x_0, \alpha_j)) = G(x_0, \alpha_j) = x_0^m + \sum_{i=0}^{m-1} c_i(\alpha_j) x_0^i.$$

The GCD Problem

Input: A and B in $\mathbb{Z}[x_0, x_1, \ldots, x_{\mathbf{n}}]$. **Output:** $G = \gcd(A, B)$.

Assume: $G = x_0^d + \sum_{i=0}^{m-1} c_i(x_1, \ldots, x_n) x_0^i$.
For prime p and points $\alpha_j \in \mathbb{Z}_p^n$ interpolate c_i from images

$$\gcd(A(x_0, \alpha_j), B(x_0, \alpha_j)) = G(x_0, \alpha_j) = x_0^m + \sum_{i=0}^{m-1} c_i(\alpha_j) x_0^i.$$

Sparse interpolation: Let $\mathbf{t} = \max_i \#c_i$ and $d_i = \deg_{x_i} G$ and $\mathbf{d} = \max_i d_i$ and $\mathbf{D} = \deg G$.
Large GCD example: $n = 8$, $t = 1000$, $d = 20$ and $D = 60$.

Zippel [1979]	$O(ndt)$ points	$p > 2nd^2t^2 = 6.4 \times 10^9$.
BenOr/Tiwari [1988]	$O(t)$ points	$p > p_n^D = 19^{60} = 5.3 \times 10^{77}$.
Discrete Logs	$O(t)$ points	$p > (d+1)^n = 21^8 = 3.7 \times 10^{10}$.

The GCD Problem

Input: A and B in $\mathbb{Z}[x_0, x_1, \ldots, x_{\mathbf{n}}]$. **Output:** $G = \gcd(A, B)$.

Assume: $G = x_0^d + \sum_{i=0}^{m-1} c_i(x_1, \ldots, x_n) x_0^i$.
For prime p and points $\alpha_j \in \mathbb{Z}_p^n$ interpolate c_i from images

$$\gcd(A(x_0, \alpha_j), B(x_0, \alpha_j)) = G(x_0, \alpha_j) = x_0^m + \sum_{i=0}^{m-1} c_i(\alpha_j) x_0^i.$$

Sparse interpolation: Let $\mathbf{t} = \max_i \#c_i$ and $d_i = \deg_{x_i} G$ and $\mathbf{d} = \max_i d_i$ and $\mathbf{D} = \deg G$.
Large GCD example: $n = 8$, $t = 1000$, $d = 20$ and $D = 60$.

Zippel [1979]	$O(ndt)$ points	$p > 2nd^2t^2 = 6.4 \times 10^9$.
BenOr/Tiwari [1988]	$O(t)$ points	$p > p_n^D = 19^{60} = 5.3 \times 10^{77}$.
Discrete Logs	$O(t)$ points	$p > (d+1)^n = 21^8 = 3.7 \times 10^{10}$.

1. The Ben-Or/Tiwari method and discrete logarithms
2. Unlucky evaluation points and Kronecker substitutions
3. Cost of evaluating $A(x, \alpha_j)$ and $B(x, \alpha_j)$
4. Cilk C implementation and benchmarks.

Ben-Or Tiwari Sparse Interpolation

Let $C(x_1, \ldots, x_n) = \sum_{i=1}^{\mathbf{t}} a_i M_i(x_1, \ldots, x_n)$ where $a_i \in \mathbb{Z}$.
Input: $v_j = C(2^j, 3^j, 5^j, \ldots, p_n^j)$ for $j = 0, 1, \ldots, 2t-1$.
Let $m_i = M_i(2, 3, 5, \ldots, p_n) \in \mathbb{Z}$ and $\lambda(z) = \prod_{i=1}^{t}(z - m_i)$.

Step 1 Compute $\lambda(z)$ from v_j using the BM algorithm.

Step 2 Factor $\lambda(z)$ to determine the $m_i \in \mathbb{Z}$.

Step 3 Factor the integers m_i.

E.g. if $M_1 = {x_1}^3 {x_2}^2 {x_3}^4$ then $m_1 = 2^3 3^2 5^4 = 45000$

Step 4 Solve the transposed Vandermonde system

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ m_1 & m_2 & \ldots & m_t \\ {m_1}^2 & {m_2}^2 & \ldots & {m_t}^2 \\ \vdots & \vdots & \vdots & \vdots \\ {m_1}^{t-1} & {m_2}^{t-1} & \ldots & m_t^{t-1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_t \end{bmatrix} = \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ \vdots \\ v_{t-1} \end{bmatrix}.$$

Problem: A severe expression swell occurs in step 1 over $\mathbb{Q}$

Ben-Or Tiwari Sparse Interpolation

Let $C(x_1, \ldots, x_n) = \sum_{i=1}^{\mathbf{t}} a_i M_i(x_1, \ldots, x_n)$ where $a_i \in \mathbb{Z}$.
Input: $v_j = C(2^j, 3^j, 5^j, \ldots, p_n^j)$ for $j = 0, 1, \ldots, 2t-1$.
Let $m_i = M_i(2, 3, 5, \ldots, p_n) \in \mathbb{Z}$ and $\lambda(z) = \prod_{i=1}^{t}(z - m_i)$.

Step 1 Compute $\lambda(z)$ from v_j using BM _____ $O(t^2)$

Step 2 Factor $\lambda(z)$ to determine the $m_i \in \mathbb{Z}$ _____ $O(t^2 \log p)$

Step 3 Factor the integers m_i _____ $O(dt)$

E.g. if $M_1 = x_1^3 x_2^2 x_3^5$ then $m_1 = 2^3 3^2 5^4 = 45000$

Step 4 Solve the transposed Vandermonde system _____ $O(t^2)$

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ m_1 & m_2 & \ldots & m_t \\ {m_1}^2 & {m_2}^2 & \ldots & {m_t}^2 \\ \vdots & \vdots & \vdots & \vdots \\ {m_1}^{t-1} & {m_2}^{t-1} & \ldots & m_t^{t-1} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_t \end{bmatrix} = \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ \vdots \\ v_{t-1} \end{bmatrix}$$

Problem: A severe expression swell occurs in step 1 over $\mathbb{Q}$
Compute mod a prime $p > p_n^d$ (m_i unique mod p) $= 19^{60} = 5.3 \times 10^{77}$.

Ben-Or/Tiwari using discrete logarithms in $\mathbb{Z}_p$

[GLL 2006] Symbolic-numeric sparse interpolation of multivariate polynomials.

- Pick a prime $p = q_1 q_2 q_3 \ldots q_n + 1$ with $\gcd(q_i, q_j) = 1$ and $q_i > \deg_{x_i} G \implies p > (d+1)^n$.
- Pick a random primitive element $\alpha \in \mathbb{Z}_p$ and set $\omega_i := \alpha^{(p-1)/q_i} \implies \omega_i^{q_i} = 1$.
- Replace $(2^j, 3^j, \ldots, p_n^j)$ with $(\omega_1^j, \omega_2^j, \ldots, \omega_n^j)$ in BT. Hence if $M_i = \prod_{k=1}^n x_k^{d_k}$ we have $m_i = \prod_{k=1}^n \omega_k^{d_k}$.

Ben-Or/Tiwari using discrete logarithms in $\mathbb{Z}_p$

[GLL 2006] Symbolic-numeric sparse interpolation of multivariate polynomials.

- Pick a prime $p = q_1 q_2 q_3 \dots q_n + 1$ with $\gcd(q_i, q_j) = 1$ and $q_i > \deg_{x_i} G \implies p > (d+1)^n$.
- Pick a random primitive element $\alpha \in \mathbb{Z}_p$ and set $\omega_i := \alpha^{(p-1)/q_i} \implies \omega_i^{q_i} = 1$.
- Replace $(2^j, 3^j, \dots, p_n^j)$ with $(\omega_1^j, \omega_2^j, \dots, \omega_n^j)$ in BT. Hence if $M_i = \prod_{k=1}^n x_k^{d_k}$ we have $m_i = \prod_{k=1}^n \omega_k^{d_k}$.

Step 3 Compute the discrete logarithm $x := \log_\alpha m_i$. Solve $\alpha^x = m_i \bmod p$ for $0 \le x < p-1$ using Pohlig-Hellman + Shanks in $O(\sum_i \sqrt{q_i})$.

$$\log_\alpha m_i = \log_\alpha \prod_{k=1}^n \omega_k^{d_k} = \sum_{k=1}^n d_k \log_\alpha \omega_k = \sum_{k=1}^n d_k \frac{p-1}{q_k}$$

Hence

$$x = d_1(q_2 q_3 \dots q_n) + d_2(q_1 q_3 \dots q_n) + \dots + d_n(q_1 q_2 \dots q_{n-1})$$

Solve this mod q_i for d_i for $1 \le i \le n$.

Unlucky Evaluation Points

Let $\bar{A} = A/G$ and $\bar{B} = B/G \implies \gcd(\bar{A}, \bar{B}) = 1$.
Assume $\bar{A}$ and $\bar{B}$ are monic in x_0.

Definition. A point $\alpha \in \mathbb{Z}_p^n$ is unlucky if $\gcd(\bar{A}(x_0, \alpha), \bar{B}(x_0, \alpha)) \neq 1$.

Example. $\bar{A} = x_0^2 + (x_1 - 1)(x_2 - 9)x_0 + 1$ Unlucky α?
$\bar{B} = x_0^2 + 1$

Unlucky Evaluation Points

Let $\bar{A} = A/G$ and $\bar{B} = B/G \implies \gcd(\bar{A}, \bar{B}) = 1$.
Assume $\bar{A}$ and $\bar{B}$ are monic in x_0.

Definition. A point $\alpha \in \mathbb{Z}_p^n$ is unlucky if $\gcd(\bar{A}(x_0, \alpha), \bar{B}(x_0, \alpha)) \neq 1$.

Example.
$\bar{A} = x_0^2 + (x_1 - 1)(x_2 - 9)x_0 + 1$
$\bar{B} = x_0^2 + 1$

Unlucky α?
$(1, \blacksquare)$ and $(\blacksquare, 9)$

Theorem: If $D \geq \max(\deg \bar{A}, \deg \bar{B})$ then Prob[α is unlucky] $\leq \frac{D^2}{p}$.

Zippel pick $p > 2^k(d^2 n(d+1)t = 7.5 \times 10^8)$ and use **random** $\alpha \in \mathbb{Z}_p^n$.
Proof:

$$\begin{aligned} \gcd(\bar{A}(x, \alpha), \bar{B}(x, \alpha)) \neq 1 &\iff res_x(\bar{A}(x, \alpha), \bar{B}(x, \alpha)) = 0 \\ &\iff \underbrace{res_x(\bar{A}, \bar{B})}_{R \in \mathbb{Z}_p[x_1, \ldots, x_n]}(\alpha) = 0 \end{aligned}$$

We have $\deg R \leq \deg(\bar{A}) \deg(\bar{B}) = D^2$ from Sylvester's matrix.
The theorem follows from the Schwarz-Zippel Lemma.

Unlucky Evaluation Points

Example. $\bar{A} = x_0^2 + (x_1 - 1)(x_2 - 9)x_0 + 1$
$\bar{B} = x_0^2 + 1$

Ben-Or/Tiwari $\alpha_j = (2^j, 3^j, 5^j, \ldots, p_n^j)$ for $0 \leq j < 2t$.
Need $2t$ consecutive lucky evaluation points.

Unlucky Evaluation Points

Example. $\bar{A} = x_0^2 + (x_1 - 1)(x_2 - 9)x_0 + 1$
$\bar{B} = x_0^2 + 1$

Ben-Or/Tiwari $\alpha_j = (2^j, 3^j, 5^j, \ldots, p_n^j)$ for $0 \leq j < 2t$.
Need $2t$ consecutive lucky evaluation points.

Pick first $2^s > p$ and use $s \leq j < 2t + s$. To solve the shifted transposed Vandermonde system

$$\begin{bmatrix} m_1^s & m_2^s & \ldots & m_t^s \\ {m_1}^{s+1} & {m_2}^{s+1} & \ldots & {m_t}^{s+1} \\ \vdots & \vdots & \vdots & \vdots \\ {m_1}^{s+t-1} & {m_2}^{s+t-1} & \ldots & m_t^{s+t-1} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_t \end{bmatrix} = \begin{bmatrix} v_s \\ v_{s+1} \\ \vdots \\ v_{s+t-1} \end{bmatrix}$$

$$\mathbf{W} \qquad \mathbf{c} = \mathbf{u}$$

we first solve the transposed Vandermonde system

$$\underbrace{\begin{bmatrix} 1 & 1 & \dots & 1 \\ m_1 & m_2 & \dots & m_t \\ \vdots & \vdots & \vdots & \vdots \\ {m_1}^{t-1} & {m_2}^{t-1} & \dots & m_t^{t-1} \end{bmatrix}}_{\mathbf{V}} \underbrace{\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_t \end{bmatrix}}_{\mathbf{b}} = \underbrace{\begin{bmatrix} v_s \\ v_{s+1} \\ \vdots \\ v_{s+t-1} \end{bmatrix}}_{\mathbf{u}}$$

using the $O(t^2)$ method to obtain $b = V^{-1}u$. Observe that the matrix $W = DV$ where D be the t by t diagonal matrix with $D_{i,i} = m_i^s$.
To solve $Wc = u$ we have

$$(DV)c = u \implies c = (V^{-1}D^{-1})u = D^{-1}(V^{-1}u) = D^{-1}b$$

Thus $c_i = um_i^{-s}$ and we can solve $Wc = u$ in $O(t^2 + t \log s)$ multiplications.

Unlucky Evaluation Points

Example. $\bar{A} = x_0^2 + (x_1 - 1)(x_2 - 9)x_0 + 1$
$\bar{B} = x_0^2 + 1$

Discrete logs uses $\alpha_j = (\omega_1^j, \omega_2^j, \ldots, \omega_n^j)$ for $1 \leq j \leq 2t$.
But $\omega_i^{q_i} = 1$.

Unlucky Evaluation Points

Example. $\bar{A} = x_0^2 + (x_1 - 1)(x_2 - 9)x_0 + 1$
$\bar{B} = x_0^2 + 1$

Discrete logs uses $\alpha_j = (\omega_1^j, \omega_2^j, \ldots, \omega_n^j)$ for $1 \leq j \leq 2t$.
But $\omega_i^{q_i} = 1$.

Pick $q_i > 2t \implies p > (2t)^n = (2000)^8 = 2.5 \times 10^{27}$.
But we don't know t!
The bound $t < \binom{D+n}{n} = \binom{68}{8} = 7.4 \times 10^9$ is too big.

Unlucky Evaluation Points

Example. $\bar{A} = x_0^2 + (x_1 - 1)(x_2 - 9)x_0 + 1$
$\bar{B} = x_0^2 + 1$

Discrete logs uses $\alpha_j = (\omega_1^j, \omega_2^j, \ldots, \omega_n^j)$ for $1 \leq j \leq 2t$.
But $\omega_i^{q_i} = 1$.

Pick $q_i > 2t \implies p > (2t)^n = (2000)^8 = 2.5 \times 10^{27}$.
But we don't know t!
The bound $t < \binom{D+n}{n} = \binom{68}{8} = 7.4 \times 10^9$ is too big.

Start with $q_i > d$.
If $j = q_i$ is unlucky, probably $x_j = 1$ is unlucky, so restart with new p with q_i doubled in length.

Kronecker Substitutions

For $r > 0$ define $K_r : R[x_0, x_1, \ldots, x_n] \to R[x, y]$ by

$$K_r(f) = f(x, y, y^r, y^{r^2}, \ldots, y^{r^{n-1}}).$$

If $d = \deg f$ then K_r is invertible if $r > d$.

Example: GCD in $\mathbb{Z}_p[x, y, z]$.

$$G = x^2 + y^2 + z^2 \qquad K_3(G) = x^2 + y^2 + y^6$$
$$\bar{A} = x^2 - y^2 \qquad K_3(\bar{A}) = x^2 - y^2$$
$$\bar{B} = x^4 - yz \qquad K_3(\bar{B}) = x^4 - y^4$$

Kronecker Substitutions

For $r > 0$ define $K_r : R[x_0, x_1, \ldots, x_n] \to R[x, y]$ by

$$K_r(f) = f(x, y, y^r, y^{r^2}, \ldots, y^{r^{n-1}}).$$

If $d = \deg f$ then K_r is invertible if $r > d$.

Example: GCD in $\mathbb{Z}_p[x, y, z]$.

$$G = x^2 + y^2 + z^2 \qquad K_3(G) = x^2 + y^2 + y^6$$
$$\bar{A} = x^2 - y^2 \qquad K_3(\bar{A}) = x^2 - y^2$$
$$\bar{B} = x^4 - yz \qquad K_3(\bar{B}) = x^4 - y^4$$

Definition: K_r is unlucky if $\gcd(K_r(\bar{A}), K_r(\bar{B})) \neq 1$

Theorem: If $r > d$ the number of unlucky K_r is
$\leq \dfrac{n-1}{d+1} \deg(\mathrm{res}_{x_0}(\bar{A}, \bar{B}))$.

For $d \geq \deg G$ try K_r for $r = d+1, d+2, \ldots$ until we get a lucky one.
Pick $p = 2^k s + 1$ prime with $p > r^n$ and s small for PH.
Use $\alpha_j = (\beta^j, (\beta^r)^j, \ldots, (\beta^{r^{n-1}})^j)$ for $1 \leq j \leq 2t$.

Kronecker Substitutions

For $r > 0$ define $K_r : R[x_0, x_1, \ldots, x_n] \to R[x, y]$ by

$$K_r(f) = f(x, y, y^r, y^{r^2}, \ldots, y^{r^{n-1}}).$$

If $d = \deg f$ then K_r is invertible if $r > d$.

Example: GCD in $\mathbb{Z}_p[x, y, z]$.

$G = x^2 + y^2 + z^2$	$K_3(G) = x^2 + y^2 + y^6$
$\bar{A} = x^2 - y^2$	$K_3(\bar{A}) = x^2 - y^2$
$\bar{B} = x^4 - yz$	$K_3(\bar{B}) = x^4 - y^4$

Definition: K_r is unlucky if $\gcd(K_r(\bar{A}), K_r(\bar{B})) \neq 1$

Theorem: If $r > d$ the number of unlucky K_r is
$\leq \dfrac{n-1}{d+1} \deg(\mathrm{res}_{x_0}(\bar{A}, \bar{B}))$.

For $d \geq \deg G$ try K_r for $r = d+1, d+2, \ldots$ until we get a lucky one.
Pick $p = 2^k s + 1$ prime with $p > r^n$ and s small for PH.
Use $\alpha_j = (\beta^j, (\beta^r)^j, \ldots, (\beta^{r^{n-1}})^j)$ for $1 \leq j \leq 2t$.

For random $\alpha \in \mathbb{Z}_p^n$ compute $D_x = \deg_{x_0} \gcd(A(x_0, \alpha), B(x_0, \alpha))$.

Kronecker substitutions and unlucky evaluation points

Example

$$\bar{A} = x_0 + x_1 + \cdots + x_{n-1} + x_n^d$$
$$\bar{B} = x_0 + x_1 + \cdots + x_{n-1} + 1$$

$$res_{x_0}(\bar{A}, \bar{B}) = 1 - x_n^d$$
$$K_{d+1}(1 - x_n^d) = 1 - y^{d(d+1)^{n-1}} \neq 0$$

Kronecker substitutions and unlucky evaluation points

Example

$\bar{A} = x_0 + x_1 + \cdots + x_{n-1} + x_n^d$
$\bar{B} = x_0 + x_1 + \cdots + x_{n-1} + 1$

$res_{x_0}(\bar{A}, \bar{B}) = 1 - x_n^d$
$K_{d+1}(1 - x_n^d) = 1 - y^{d(d+1)^{n-1}} \neq 0$

Theorem

Let $A = x^m + \sum_{i=0}^{m-1} a_i(y)x^i$
and $B = x^l + \sum_{i=0}^{l-1} b_i(y)x^i$ in $\mathbb{Z}_p[x, y]$

Let $X = |\{0 \leq \beta < p : \gcd(A(x, \beta), B(x, \beta)) \neq 1\}|$. Then

(i) $E[X] =$

Kronecker substitutions and unlucky evaluation points

Example

$\bar{A} = x_0 + x_1 + \cdots + x_{n-1} + x_n^d$
$\bar{B} = x_0 + x_1 + \cdots + x_{n-1} + 1$

$res_{x_0}(\bar{A}, \bar{B}) = 1 - x_n^d$
$K_{d+1}(1 - x_n^d) = 1 - y^{d(d+1)^{n-1}} \neq 0$

Theorem

Let $A = x^m + \sum_{i=0}^{m-1} a_i(y)x^i$
and $B = x^l + \sum_{i=0}^{l-1} b_i(y)x^i$ in $\mathbb{Z}_p[x, y]$

Let $X = |\{0 \leq \beta < p : \gcd(A(x, \beta), B(x, \beta)) \neq 1\}|$. Then

(i) $E[X] = 1$.
(ii) $Var[X] = 1 - 1/p$ if $\deg a_i, b_i > 0$.

Evaluating the input polynomials A and B.

Evaluate $K_r(A)(x, y)$ at $y = \alpha^j$ for $j = 1, 2, \ldots, 2t$.

Evaluating the input polynomials A and B.

Evaluate $K_r(A)(x, y)$ at $y = \alpha^j$ for $j = 1, 2, \ldots, 2t$.

Write $\boxed{Kr(A) = \sum_{i=1}^{\mathbf{s}} c_i x^{d_i} y^{e_i}}$ in **lex order** with $x > y$.

If $\deg A \leq d$ and $r = d + 1$ then $e_i < (d + 1)^n$.

Evaluating the input polynomials A and B.

Evaluate $K_r(A)(x, y)$ at $y = \alpha^j$ for $j = 1, 2, \ldots, 2t$.

Write $\boxed{Kr(A) = \sum_{i=1}^{\mathbf{s}} c_i x^{d_i} y^{e_i}}$ in **lex order** with $x > y$.

If $\deg A \leq d$ and $r = d + 1$ then $e_i < (d + 1)^n$.

for $j = 1, 2, \ldots 2t$ **in parallel** do

compute $\beta := \alpha^j$

assemble $Kr(A)(\alpha^j)$ from $\sum_{i=1}^{\mathbf{s}} (c_i \cdot \beta^{e_i}) x^{d_i}$ _____ $O(\mathbf{s}n \log d)$

Total cost: $O(\mathbf{s}tn \log d) \implies$ all the time in GCD(A, B) is in evaluation!

Evaluating the input polynomials A and B.

Evaluate $K_r(A)(x, y)$ at $y = \alpha^j$ for $j = 1, 2, \ldots, 2t$.

Write $\boxed{Kr(A) = \sum_{i=1}^{\mathbf{s}} c_i x^{d_i} y^{e_i}}$ in **lex order** with $x > y$.

If $\deg A \leq d$ and $r = d + 1$ then $e_i < (d + 1)^n$.

for $j = 1, 2, \ldots 2t$ **in parallel** do

compute $\beta := \alpha^j$

assemble $Kr(A)(\alpha^j)$ from $\sum_{i=1}^{\mathbf{s}} (c_i \cdot \beta^{e_i}) x^{d_i}$ _____ $O(\mathbf{s}n \log d)$

Total cost: $O(\mathbf{s}tn \log d) \implies$ all the time in GCD(A, B) is in evaluation!

But $(\alpha^j)^{e_i} = (\alpha^{e_i})^j$ so

Precompute $B = [\alpha^{e_1}, \alpha^{e_2}, \ldots, \alpha^{e_{\mathbf{s}}}]$ _____ $O(\mathbf{s}n \log d)$

Initialize $C = [c_1, c_2, \ldots, c_{\mathbf{s}}]$

Evaluating the input polynomials A and B.

Evaluate $K_r(A)(x, y)$ at $y = \alpha^j$ for $j = 1, 2, \ldots, 2t$.

Write $\boxed{Kr(A) = \sum_{i=1}^{\mathbf{s}} c_i x^{d_i} y^{e_i}}$ in **lex order** with $x > y$.

If $\deg A \leq d$ and $r = d + 1$ then $e_i < (d+1)^n$.

for $j = 1, 2, \ldots 2t$ **in parallel** do
  compute $\beta := \alpha^j$
  assemble $Kr(A)(\alpha^j)$ from $\sum_{i=1}^{\mathbf{s}} (c_i \cdot \beta^{e_i}) x^{d_i}$ ——— $O(\mathbf{s}n \log d)$

Total cost: $O(\mathbf{s}tn \log d) \implies$ all the time in GCD(A, B) is in evaluation!

But $(\alpha^j)^{e_i} = (\alpha^{e_i})^j$ so
  Precompute $B = [\alpha^{e_1}, \alpha^{e_2}, \ldots, \alpha^{e_{\mathbf{s}}}]$ ——— $O(\mathbf{s}n \log d)$
  Initialize $C = [c_1, c_2, \ldots, c_{\mathbf{s}}]$
  for $j = 1, 2, \ldots, 2t$ **in serial** do
    compute $C := [B_i \times C_i \mod p \text{ for } 1 \leq i \leq \mathbf{s}]$ **afap** ——— $O(\mathbf{s})$
    assemble $Kr(A)(\alpha^j) = \sum_{i=1}^{\mathbf{s}} C_i x^{d_i}$ ——— $O(\mathbf{s})$

Total cost: $O(\mathbf{s}n \log d + \mathbf{s}t) \implies$ evaluation is quadratic in t.

Evaluating the input polynomials A and B.

Evaluate $K_r(A)(x,y)$ at $y = \alpha^j$ for $j = 1, 2, \ldots, 2t$.

Write $\boxed{Kr(A) = \sum_{i=1}^{\mathbf{s}} c_i x^{d_i} y^{e_i}}$ in **lex order** with $x > y$.

If $\deg A \leq d$ and $r = d + 1$ then $e_i < (d+1)^n$.

for $j = 1, 2, \ldots 2t$ **in parallel** do
  compute $\beta := \alpha^j$
  assemble $Kr(A)(\alpha^j)$ from $\sum_{i=1}^{\mathbf{s}} (c_i \cdot \beta^{e_i}) x^{d_i}$ ——— $O(\mathbf{s}n \log d)$

Total cost: $O(\mathbf{s}tn \log d) \implies$ all the time in GCD(A, B) is in evaluation!

But $(\alpha^j)^{e_i} = (\alpha^{e_i})^j$ so
  Precompute $B = [\alpha^{e_1}, \alpha^{e_2}, \ldots, \alpha^{e_{\mathbf{s}}}]$ ——— $O(\mathbf{s}n \log d)$
  Initialize $C = [c_1, c_2, \ldots, c_{\mathbf{s}}]$
  for $j = 1, 2, \ldots, 2t$ **in serial** do
    compute $C := [B_i \times C_i \mod p \text{ for } 1 \leq i \leq \mathbf{s}]$ **afap** ——— $O(\mathbf{s})$
    assemble $Kr(A)(\alpha^j) = \sum_{i=1}^{\mathbf{s}} C_i x^{d_i}$ ——— $O(\mathbf{s})$

Total cost: $O(\mathbf{s}n \log d + \mathbf{s}t) \implies$ evaluation is quadratic in t.

For N cores do N evaluations at a time using $B = [\alpha^{Ne_1}, \alpha^{Ne_2}, \ldots, \alpha^{Ne_s}]$

Benchmarks

Cilk C codes for 31 bit primes and 63 bit primes.

Benchmarks

Cilk C codes for 31 bit primes and 63 bit primes.

$G = x^d + c + \sum_{i=1}^{100d-1} c_i x^{d_i} y^{e_i} z^{f_i}$ with $0 \le d_i, e_i, f_i < d$
$\#\bar{A} = \#\bar{B} = 100$ terms.
So t is about 100 and $\#A, \#B \le 10^4 d$ terms.

3 variables, $p = 15 \times 2^{27} + 1$.

d	1 core	eval	4 cores	16 cores	Zippel	Magma
20	0.208	65%	0.073	0.031	0.385	0.89
50	1.004	80%	0.301	0.108	5.174	20.00
100	2.736	85%	0.792	0.262	72.461	228.84
200	6.026	86%	1.723	0.578	693.088	3003.23
500	16.0117	87%	4.492	1.550	10946.081	–

Timings (in seconds) on two Xeon E5-2680 CPUs, 8 cores, 2.2GHz/3.0GHz.

Maximum parallel speedup $= 16 \times 2.2/3.0 = 11.7$ x

Benchmarks

6 variables, $p = 29 \times 2^{57} + 1$.

d	1 core	eval	4 cores	16 cores	Zippel	Magma
10	0.660	72%	0.225	0.096	48.05	106.23
20	1.463	74%	0.473	0.187	191.28	7179.01
50	3.387	72%	1.050	0.397	1191.00	–
100	7.010	73%	2.126	0.760	6415.17	
200	15.031	74%	4.522	1.629	–	
500	41.101	74%	12.389	4.425		

9 variables, $p = 29 \times 2^{57} + 1$.

d	1 core	eval	4 cores	16 cores	Zippel	Magma
5	0.353	70%	0.133	0.065	30.87	14.15
10	0.656	71%	0.221	0.089	138.41	69.12
20	1.439	72%	0.466	0.176	664.33	705.84
50	3.654	73%	1.102	0.410	6390.22	3932.64
100	7.320	73%	2.168	0.792	–	–
200	need 127 bit primes					

Thank you!

Kronecker substitutions and unlucky evaluation points

Example: $p = 7$

$A = x^2 + (a_{11}y + a_{10})x + (a_{22}y^2 + a_{21}y + a_{20})$

$B = x^2 + (b_{11}y + b_{10})x + (a_{22}y^2 + b_{21}y + b_{20})$

k	0	1	2	3	4	5	6	7
F_k	96606636	110666892	56053746	17287200	1728720	0	0	132055
B_k	96018048	112021056	56010528	15558480	2593080	259308	14406	343

F_k counts over p^{10} polynomials the number of polynomials with k unlucky $\beta's$.

$B_k = p^{10}[\binom{n}{k} q^k (1-q)^{n-k}]$ is a binomial distribution with $q = 1/p$ and $n = p$.