Computing polynomial GCDs in $\mathbb{Z}[x_1, x_2, \ldots, x_n]$

Michael Monagan

This is joint work with Qiao-Long Huang from Shandong Univerity.

Let $A, B \in \mathbb{Z}[x_1, \ldots, x_n]$, $G = \gcd(A, B)$, $\bar{A} = A/G$, $\bar{B} = B/G$.

Substitute $x_i = (\gamma_i z - \alpha_i) y^{s_i}$ for $1 \leq i \leq n$ where s_i are chosen at random from $[0, T)$.

For the GCD in $\mathbb{Z}[z, y]$ do it mod 63 bit primes p using evaluation and interpolation on z.

Try this for $T = 2, 4, 8, 16, \ldots$ until $1 + \log_2(T)$ choices for s (same α, γ) are good.

Benchmark 1

G has t terms $\quad \bar{A}, \bar{B}$ have s terms.
Monomials in $n = 9$ variables $\quad G, \bar{A}, \bar{B}$ have total degree 30.

s	t	MGCD	T	eval	Maple	Magma	MonHu
10^5	10^1	11.69	4	10.22	78.92	39.90	0.661
10^4	10^2	13.55	8	10.24	197.6	9.98	1.488
10^3	10^3	29.65	64	10.27	1054.9	37.49	6.868
10^2	10^4	13.43	16	10.24	14568.	27.68	1.087
10^1	10^5	10.67	4	9.47	NA	144.8	0.696

Table: Benchmark 1: Timings in CPU seconds for n=9

Notes: Maple and Magma are using Zippel's algorithm.
MGCD used two 63 bit primes.
MGCD and Monagan/Hu both recover the smaller of G,$\bar{A}$,$\bar{B}$.
Notice T is small.

Benchmark 2

Same as benchmark 1 except $n = 18$.
Here MonHu cannot use a 64 bit prime. It uses a 128 bit prime.

s	t	MGCD	T	eval	Maple	Magma	MonHu
10^5	10^1	38.17	4	22.67	494.9	166.5	310.2
10^4	10^2	48.76	16	24.62	1473.2	79.50	450.8
10^3	10^3	92.60	128	24.68	14287.	447.8	4358.
10^2	10^4	50.54	16	24.64	NA	76.73	605.7
10^1	10^5	39.61	4	22.59	NA	188.1	150.6

Table: Benchmark 2 timings in CPU seconds for n=18

Benchmark 3

Let $\Gamma = \gcd(LC(A, x_1), LC(B, x_1)$ and $\Delta = \Gamma / LC(\gcd(A, B))$.
If $\#\Delta > 1$ then Zippel and Monagan/Hu scale by Γ so interpolate ΔG which is not good if $\#\Delta \gg 1$.
For example

$$G = x + y, \bar{A} = (y^2 - 1)x + y + 1, \bar{B} = (y^3 - 1)x + y - 1$$

Here $\Delta = y - 1$ and $\Delta G = (y - 1)x + y^2 - 1$.
In benchmark 3 $\#\Delta = t/10$.

t	$\#A$	MGCD	T	Maple	Magma	MonHu	tmax
50	22100	0.945	4	82.86	2.17	0.279	150
100	169096	6.359	8	2794.8	6.15	5.718	829
150	573732	21.36	16	25407.	148.2	37.10	1848
200	1352967	46.57	16	NA	1058.9	136.8	3349
300	4538198	143.5	32	NA	13752.	1079.1	7409
500	20849989	671.9	32	NA	NA	12400.	20656