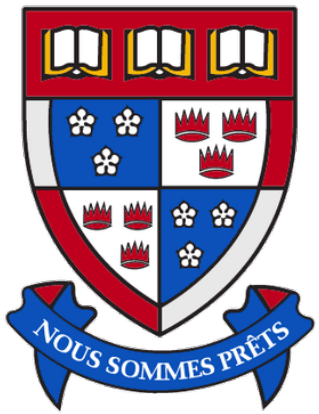
Project Meeting with Maplesoft

Mahsa Ansari
Michael Monagan

Department of Mathematics,
Simon Fraser University,
Canada



Outline

Previous Work

Let $f_1, f_2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)[x_1, \ldots, x_k]$.

1. We designed a modular gcd algorithm called MGCD to compute the monic $\gcd(f_1, f_2)$.
2. To speed up our algorithm, we use linear algebra to map $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ into $\mathbb{Q}(\gamma)$, where γ is a primitive element. We do this mod a prime to avoid expression swell.
3. A Maple implementation using a recursive dense representation for polynomials.
4. Analysis of the expected time complexity.

Our paper is published in CASC 2023, Havana, Cuba.

MGCD

Let $f_1, f_2 \in L[x_1, \ldots, x_k]$, MGCD computes $g = monic \gcd(f_1, f_2)$.

$$
\begin{array}{ccc}
\check{f}_1, \check{f}_2 \in L_{\mathbb{Z}}[x_1, \ldots, x_k] & \longrightarrow & \gcd(f_1, f_2) \in L[x_1, \ldots, x_k] \\
\phi_p \text{ for } p \in \{p_1, p_2, \ldots\} \Big\downarrow p \nmid \prod_{i=1}^{n} \mathrm{lc}(\check{M}_i) \cdot \mathrm{lc}(\check{f}_1) & & \Big\uparrow \textit{CRT, RNR, Division test} \\
\check{f}_1, \check{f}_2 \in L_p[x_1, \ldots, x_k] & & \gcd(\check{f}_1, \check{f}_2) \in L_p[x_1, \ldots, x_k] \\
\Big\downarrow \phi_\gamma & & \Big\uparrow \phi_\gamma^{-1} \\
\check{f}_1, \check{f}_2 \in \bar{L}_p[x_1, \ldots, x_k] & \xrightarrow{PGCD} & \gcd(\check{f}_1, \check{f}_2) \in \bar{L}_p[x_1, \ldots, x_k]
\end{array}
$$

$L = \mathbb{Q}[z_1, \ldots, z_n] / \langle M_1(z_1), \ldots, M_n(z_n) \rangle$
$L_{\mathbb{Z}} = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$
$L_p = \mathbb{Z}_p[z_1, \ldots, z_n] / \langle m_1(z_1), \ldots, m_n(z_n) \rangle$ s.t $m_i(z_i) = \check{M}_i(z_i) \mod p$
$\bar{L}_p = \mathbb{Z}_p[z] / \langle M(z) \rangle$

Benchmark

Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$ have degree 16. The input polynomials $f_1, f_2 \in L[x, y]$ have degree d in x and y.

d	New MGCD			Old MGCD	
	time	LAMP	PGCD	time	PGCD
4	0.119	0.023	0.027	0.114	0.100
6	0.137	0.016	0.034	0.184	0.156
8	0.217	0.018	0.045	0.330	0.244
10	0.252	0.018	0.087	0.479	0.400
12	0.352	0.018	0.078	0.714	0.511
16	0.599	0.017	0.129	1.244	1.008
20	0.767	0.017	0.161	1.965	1.643
24	1.103	0.019	0.220	2.896	2.342
28	1.890	0.023	0.358	4.487	3.897
32	2.002	0.020	0.392	5.416	4.454
36	2.461	0.017	0.595	6.944	5.883
40	3.298	0.019	0.772	9.492	7.960

Outline

Current work

1. Modifying the Monic Euclidean Algorithm, we designed a new algorithm to compute the resultant of univariate polynomials. Let $f_1, f_2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)[x_1, \ldots, x_k, y]$.
2. We designed a modular resultant algorithm called MRES to compute the $\mathrm{res}(f_1, f_2, y)$.
3. To speed up our algorithm, we use linear algebra to map $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ into $\mathbb{Q}(\gamma)$, where γ is a primitive element. We do this mod a prime to avoid expression swell.
4. A Maple implementation using a recursive dense representation for polynomials.
5. Analysis of the expected time complexity.

We plan to submit a paper to CASC 2024, taking place in Rennes, France.

Computing the resultant over $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$

Let $f_1, f_2 \in L[x_1, \ldots, x_k, y]$, MRES computes $\text{res}(f_1, f_2, y)$.

$$
\begin{array}{ccc}
\check{f}_1, \check{f}_2 \in L_{\mathbb{Z}}[x_1, \ldots, x_k, y] & \longrightarrow & \text{res}(f_1, f_2, y) \in L[x_1, \ldots, x_k] \\
\Big\downarrow \phi_p \text{ for } p \in \{p_1, p_2, \ldots\} \; p \nmid \prod_{i=1}^{n} \text{lc}(\check{M}_i) \cdot \text{lc}(\check{f}_1) & & \Big\uparrow \textit{CRT, RNR} \\
\check{f}_1, \check{f}_2 \in L_p[x_1, \ldots, x_k, y] & & \text{res}(\check{f}_1, \check{f}_2, y) \in L_p[x_1, \ldots, x_k] \\
\Big\downarrow \phi_\gamma & & \Big\uparrow \phi_\gamma^{-1} \\
\check{f}_1, \check{f}_2 \in \bar{L}_p[x_1, \ldots, x_k, y] & \xrightarrow{\textit{PRES}} & \text{res}(\check{f}_1, \check{f}_2, y) \in \bar{L}_p[x_1, \ldots, x_k]
\end{array}
$$

$L = \mathbb{Q}[z_1, \ldots, z_n] / \langle M_1(z_1), \ldots, M_n(z_n) \rangle$
$L_{\mathbb{Z}} = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$
$L_p = \mathbb{Z}_p[z_1, \ldots, z_n] / \langle m_1(z_1), \ldots, m_n(z_n) \rangle$ s.t $m_i(z_i) = \check{M}_i(z_i) \mod p$
$\bar{L}_p = \mathbb{Z}_p[z] / \langle M(z) \rangle$

Benchmark

We give one benchmark for resultant computations in $L[x, y]$ where the number field $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$ has degree 16. In the table, the input polynomials f_1 and f_2 have degree d in x and y.

d	MRS 1			MRS 2	
	time	LAMP	PRS	time	PRS
2	0.156	0.076	0.064	0.578	0.578
4	0.578	0.062	0.454	5.656	5.625
6	2.875	0.172	2.375	45.359	45.156
8	11.438	0.205	9.625	208.844	207.891
10	35.563	0.562	30.549	721.766	717.892
12	96.468	0.578	83.363	1995.484	1984.204

Outline

My Future Work

There are still problems waiting to be solved:

1. Failure Probability of MRES (In progress).
2. Failure Probability of MGCD.

Thank you!