Gröbner Bases over Algebraic Number Fields

Andreas Steenpass

joint work with
Dereje K. Boku, Wolfram Decker, and Claus Fieker

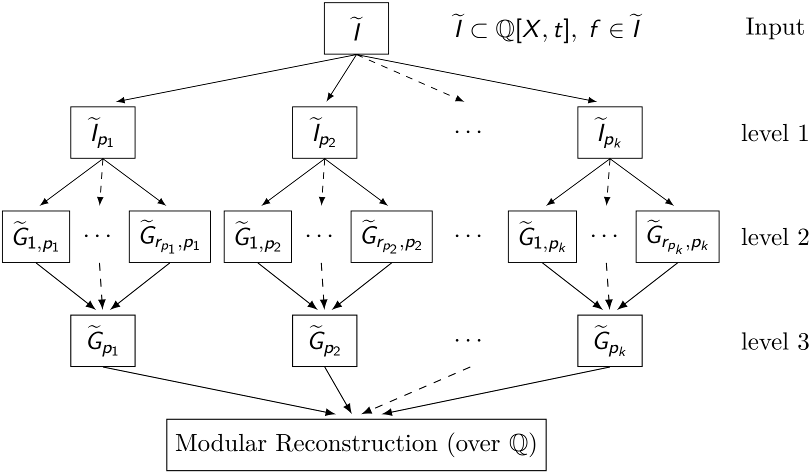
University of Kaiserslautern

October 1, 2015

Problem

Given an ideal $I \subseteq K[x_1, \ldots, x_n]$ where $K = \mathbb{Q}(\alpha)$ is a number field, what is an efficient way to compute a Gröbner basis of I?

Overview of the New Method



Notation

- Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field;

Notation

- Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field;
- let $X = \{x_1, \ldots, x_n\}$ be a set of variables, and let t be an extra variable;

Notation

- Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field;
- let $X = \{x_1, \ldots, x_n\}$ be a set of variables, and let t be an extra variable;
- let $f \in \mathbb{Q}[t]$ be the minimal polynomial of the algebraic number α;

Notation

- Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field;
- let $X = \{x_1, \ldots, x_n\}$ be a set of variables, and let t be an extra variable;
- let $f \in \mathbb{Q}[t]$ be the minimal polynomial of the algebraic number α;
- consider the polynomial rings $S = \mathbb{Q}(\alpha)[X]$, $T = \mathbb{Q}[X, t]$, and $\mathbb{Q}[t]$;

Notation

- Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field;
- let $X = \{x_1, \ldots, x_n\}$ be a set of variables, and let t be an extra variable;
- let $f \in \mathbb{Q}[t]$ be the minimal polynomial of the algebraic number α;
- consider the polynomial rings $S = \mathbb{Q}(\alpha)[X]$, $T = \mathbb{Q}[X, t]$, and $\mathbb{Q}[t]$;
- fix a global product ordering $\succ_K := (\succ_1, \succ_2)$ on $\mathrm{Mon}(X, t)$; this is an elimination ordering w.r.t. X;

Notation

- Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field;
- let $X = \{x_1, \ldots, x_n\}$ be a set of variables, and let t be an extra variable;
- let $f \in \mathbb{Q}[t]$ be the minimal polynomial of the algebraic number α;
- consider the polynomial rings $S = \mathbb{Q}(\alpha)[X]$, $T = \mathbb{Q}[X, t]$, and $\mathbb{Q}[t]$;
- fix a global product ordering $\succ_K := (\succ_1, \succ_2)$ on $\mathrm{Mon}(X, t)$; this is an elimination ordering w.r.t. X;
- for a polynomial $q \in S$ and a set $G \subseteq S$, we write:

  $\mathsf{lm}(q)$: the *leading monomial* of q,
  $\mathsf{Lm}(G)$: the *set of leading monomials* of the elements in G.

- Let $I \subseteq S$ be an ideal, given by a set of generators $H = \{g_1(X, \alpha), \ldots, g_s(X, \alpha)\}$, with polynomials $g_i(X, t) \in T$;

- Let $I \subseteq S$ be an ideal, given by a set of generators $H = \{g_1(X, \alpha), \ldots, g_s(X, \alpha)\}$, with polynomials $g_i(X, t) \in T$;
- set $\widetilde{H} = \{g_1(X, t), \ldots, g_s(X, t)\} \subset T$, and let $\widetilde{I} \subset T$ be the ideal generated by $\widetilde{H}$ and f.

- Let $I \subseteq S$ be an ideal, given by a set of generators $H = \{g_1(X, \alpha), \ldots, g_s(X, \alpha)\}$, with polynomials $g_i(X, t) \in T$;
- set $\widetilde{H} = \{g_1(X, t), \ldots, g_s(X, t)\} \subset T$, and let $\widetilde{I} \subset T$ be the ideal generated by $\widetilde{H}$ and f.

Theorem

Let $\widetilde{G}$ be the reduced Gröbner basis of $\widetilde{I}$ w.r.t. $\succ_K$. Then, if $\widetilde{I} \neq \langle 1 \rangle$, we have $f \in \widetilde{G}$. In any case, all elements $m(X, t) \in \widetilde{G} \setminus \{f\}$ are monic if considered as elements in $\mathbb{Q}[t][X]$. Furthermore, $(\widetilde{G} \setminus \{f\})|_{t=\alpha}$ is the reduced Gröbner basis of I w.r.t. $\succ_1$.

Previous Work

- Noro has presented a modified version of Buchberger's algorithm [Masayuki Noro, 2006].

Previous Work

- Noro has presented a modified version of Buchberger's algorithm [Masayuki Noro, 2006].
- He noticed that during the execution of Buchberger's algorithm applied to $\widetilde{I}$, many superfluous intermediate basis elements of the form $t^b X^a + \text{(lower terms)}$ are computed before a monic element $X^a + \text{(lower terms)}$ is generated.

Previous Work

- Noro has presented a modified version of Buchberger's algorithm [Masayuki Noro, 2006].
- He noticed that during the execution of Buchberger's algorithm applied to $\widetilde{I}$, many superfluous intermediate basis elements of the form $t^b X^a +$ (lower terms) are computed before a monic element $X^a +$ (lower terms) is generated.
  - ∗ The superfluous elements yield new S-pairs which usually make the subsequent computations inefficient.

Previous Work

- Noro has presented a modified version of Buchberger's algorithm [Masayuki Noro, 2006].
- He noticed that during the execution of Buchberger's algorithm applied to $\widetilde{I}$, many superfluous intermediate basis elements of the form $t^b X^a + (\text{lower terms})$ are computed before a monic element $X^a + (\text{lower terms})$ is generated.
  - The superfluous elements yield new S-pairs which usually make the subsequent computations inefficient.
  - Noro's modification: Each generated basis element is made monic in $(\mathbb{Q}[t])[X]$ before it is added to the basis, that is, the inverse of an algebraic number is computed.

Previous Work

- Noro has presented a modified version of Buchberger's algorithm [Masayuki Noro, 2006].
- He noticed that during the execution of Buchberger's algorithm applied to $\widetilde{I}$, many superfluous intermediate basis elements of the form $t^b X^a + \text{(lower terms)}$ are computed before a monic element $X^a + \text{(lower terms)}$ is generated.
  - The superfluous elements yield new S-pairs which usually make the subsequent computations inefficient.
  - Noro's modification: Each generated basis element is made monic in $(\mathbb{Q}[t])[X]$ before it is added to the basis, that is, the inverse of an algebraic number is computed.
  - However, this is in general computationally expensive.

Our New Approach

- We use a different approach to reduce the number of basis elements which are computed before a monic element $X^a +$ (lower terms) is generated.

Our New Approach

- We use a different approach to reduce the number of basis elements which are computed before a monic element $X^a + (\text{lower terms})$ is generated.
- Our approach makes use of
  - modular methods w.r.t. different prime numbers to avoid intermediate coefficient swell;

Our New Approach

- We use a different approach to reduce the number of basis elements which are computed before a monic element $X^a + \text{(lower terms)}$ is generated.
- Our approach makes use of
  - modular methods w.r.t. different prime numbers to avoid intermediate coefficient swell;
  - factorization of the minimal polynomial in positive characteristic to considerably reduce the degree of the field extensions.

Theorem

Let $p_1, \ldots, p_k$ be distinct prime numbers, and let $N = p_1 \cdots p_k$ be their product. Then we have the ring isomorphism:

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{F}_{p_1} \times \ldots \times \mathbb{F}_{p_k}.$$

Two Variants of the Chinese Remainder Theorem

Theorem

Let $p_1, \ldots, p_k$ *be distinct prime numbers, and let* $N = p_1 \cdots p_k$ *be their product. Then we have the ring isomorphism:*

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{F}_{p_1} \times \ldots \times \mathbb{F}_{p_k}.$$

Theorem

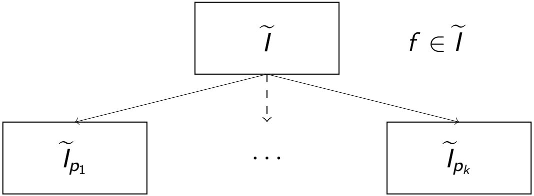
Let $f_{1,p}, \ldots, f_{r_p,p} \in \mathbb{F}_p[t]$ *be pairwise coprime polynomials, and let* $f_p = f_{1,p} \cdots f_{r_p,p}$ *be their product. Then we have the ring isomorphism*

$$\mathbb{F}_p[t]/\langle f_p \rangle \cong \mathbb{F}_p[t]/\langle f_{1,p} \rangle \times \ldots \times \mathbb{F}_p[t]/\langle f_{r_p,p} \rangle.$$

Level 1: Compute modulo several prime numbers

$\boxed{\widetilde{I}}$ $\quad f \in \widetilde{I}$ Input

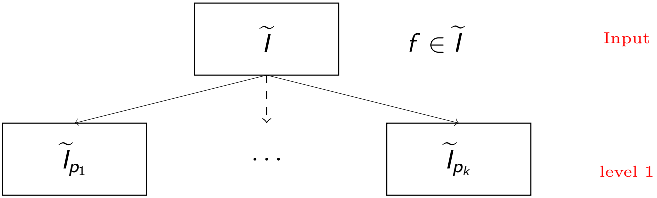
Level 1: Compute modulo several prime numbers



$f \in \widetilde{I}$

Input

level 1



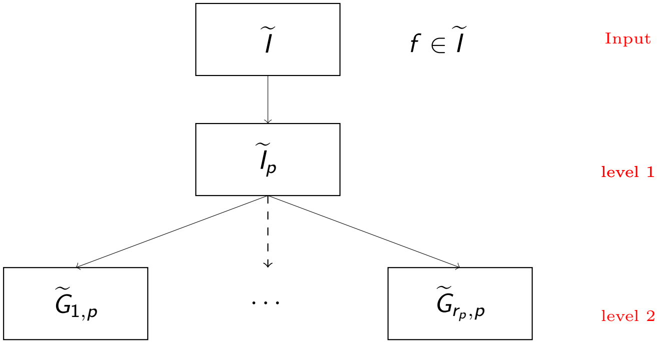
Definition

Let $f \in \mathbb{Q}[t]$ be as given above. Let p be a prime not dividing any numerator or denominator of the coefficients occurring in f. We say that p is *admissible of type* A w.r.t. f if the reduction f_p is reducible and square-free over $\mathbb{F}_p$. In this case, we write $f_p = \prod_{1 \le i \le r_p} f_{i,p}$.

Level 2: Compute modulo the factors of f_p

$$\begin{array}{ccc}
\boxed{\widetilde{I}} & f \in \widetilde{I} & \text{Input} \\
\downarrow & & \\
\boxed{\widetilde{I}_p} & & \text{level 1}
\end{array}$$

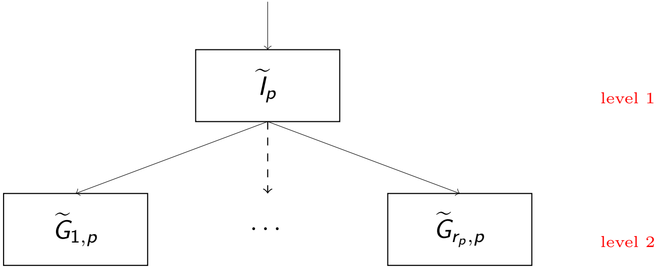
Level 2: Compute modulo the factors of f_p



Level 2: Compute modulo the factors of f_p

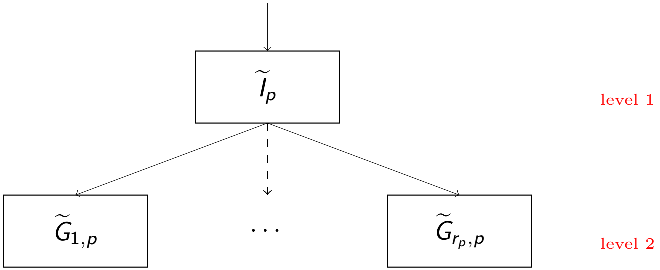
$$\begin{tikzcd}
{} \arrow[d] & & \\
& \widetilde{I}_p \arrow[dl] \arrow[d, dashed] \arrow[dr] & & \text{level 1} \\
\widetilde{G}_{1,p} & \cdots & \widetilde{G}_{r_p,p} & \text{level 2}
\end{tikzcd}$$

Level 2: Compute modulo the factors of f_p



- Let $f_p = \prod_{1 \le i \le r_p} f_{i,p}$ be the irreducible factorization of f_p over $\mathbb{F}_p$, with $r_p > 1$.

Level 2: Compute modulo the factors of f_p

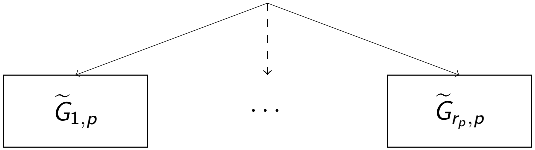


- Let $f_p = \prod_{1 \le i \le r_p} f_{i,p}$ be the irreducible factorization of f_p over $\mathbb{F}_p$, with $r_p > 1$.
- For each $i \in \{1, \dots, r_p\}$, we compute the reduced Gröbner basis $\widetilde{G}_{i,p}$ of the ideal $\widetilde{I}_{i,p} := \langle \widetilde{H}_p \cup \{f_{i,p}\} \rangle$.

Level 2: Compute modulo the factors of f_p

$$
\begin{tikzcd}
 & \bullet \arrow[dl] \arrow[d, dashed] \arrow[dr] & \\
\boxed{\widetilde{G}_{1,p}} & \cdots & \boxed{\widetilde{G}_{r_p,p}}
\end{tikzcd}
$$

level 2

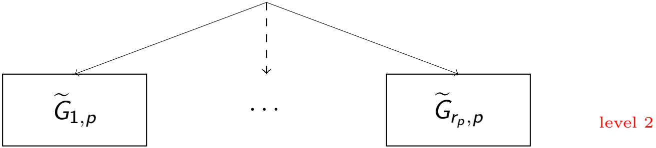


level 2

Definition

Let p be a prime as in the previous definition. In addition, suppose that p does not divide any numerator or denominator of the coefficients occurring in $\widetilde{H}$. Then we say that p is *admissible of type* B w.r.t. f and $\widetilde{H}$ if for all indices i, j with $i \neq j$

Level 2: Compute modulo the factors of f_p



Definition

Let p be a prime as in the previous definition. In addition, suppose that p does not divide any numerator or denominator of the coefficients occurring in $\widetilde{H}$. Then we say that p is *admissible of type* B w.r.t. f and $\widetilde{H}$ if for all indices i, j with $i \neq j$

1. the sizes of $\widetilde{G}_{i,p}$ and $\widetilde{G}_{j,p}$ coincide, and

Level 2: Compute modulo the factors of f_p

$\widetilde{G}_{1,p}$ $\quad\cdots\quad$ $\widetilde{G}_{r_p,p}$

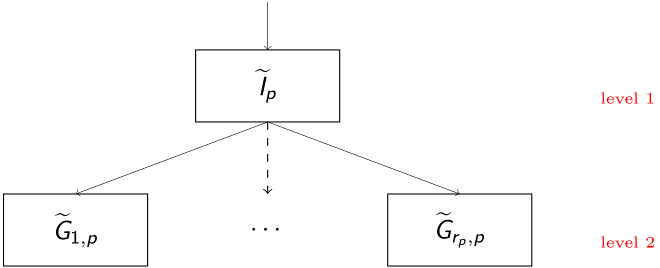
level 2

Definition

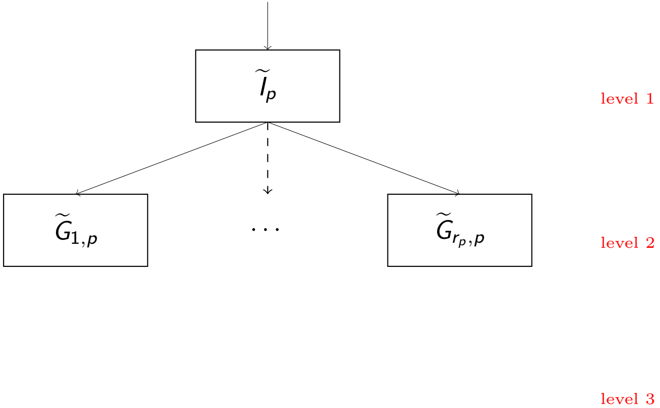
Let p be a prime as in the previous definition. In addition, suppose that p does not divide any numerator or denominator of the coefficients occurring in $\widetilde{H}$. Then we say that p is *admissible of type* B w.r.t. f and $\widetilde{H}$ if for all indices i, j with $i \neq j$

1. the sizes of $\widetilde{G}_{i,p}$ and $\widetilde{G}_{j,p}$ coincide, and
2. $\mathrm{Lm}(\widetilde{G}_{i,p} \setminus \{f_{i,p}\}) = \mathrm{Lm}(\widetilde{G}_{j,p} \setminus \{f_{j,p}\})$.

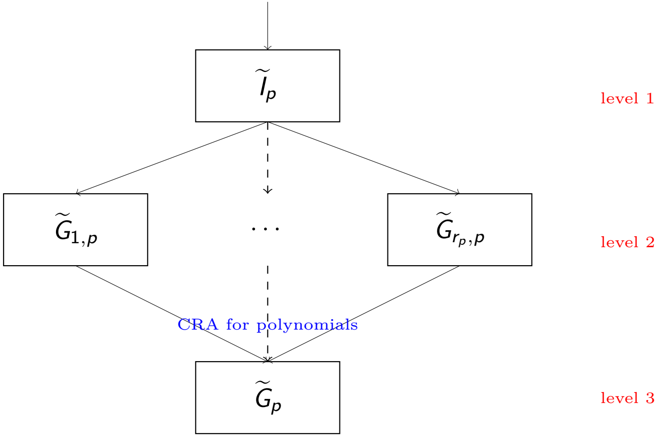
Level 3: Reconstruct $\widetilde{G}_p$



Level 3: Reconstruct $\widetilde{G}_p$



Level 3: Reconstruct $\widetilde{G}_p$



Delete Unlucky Primes

Definition

Let $\widetilde{I}$ be an ideal given as above and let p be a prime number. Furthermore, let $\widetilde{G}$ be the reduced Gröbner basis of $\widetilde{I}$ and let $\widetilde{G}_p$ be the reduced Gröbner basis of $\widetilde{I}_p$. Then p is called *lucky* for $\widetilde{I}$ if and only if $\mathsf{Lm}(\widetilde{G}_p) = \mathsf{Lm}(\widetilde{G})$. Otherwise p is called *unlucky* for $\widetilde{I}$. [Idrees, Pfister, and Steidel, 2011]

Delete Unlucky Primes

Definition

Let $\widetilde{I}$ be an ideal given as above and let p be a prime number. Furthermore, let $\widetilde{G}$ be the reduced Gröbner basis of $\widetilde{I}$ and let $\widetilde{G}_p$ be the reduced Gröbner basis of $\widetilde{I}_p$. Then p is called *lucky* for $\widetilde{I}$ if and only if $\mathsf{Lm}(\widetilde{G}_p) = \mathsf{Lm}(\widetilde{G})$. Otherwise p is called *unlucky* for $\widetilde{I}$. [Idrees, Pfister, and Steidel, 2011]

$$\boxed{\widetilde{G}_{p_1}} \qquad \cdots \qquad \boxed{\widetilde{G}_{p_k}}$$

each p_i is a prime which is admissible of type B

Delete Unlucky Primes

Definition

Let $\widetilde{I}$ be an ideal given as above and let p be a prime number. Furthermore, let $\widetilde{G}$ be the reduced Gröbner basis of $\widetilde{I}$ and let $\widetilde{G}_p$ be the reduced Gröbner basis of $\widetilde{I}_p$. Then p is called *lucky* for $\widetilde{I}$ if and only if $\mathsf{Lm}(\widetilde{G}_p) = \mathsf{Lm}(\widetilde{G})$. Otherwise p is called *unlucky* for $\widetilde{I}$. [Idrees, Pfister, and Steidel, 2011]

$$\boxed{\widetilde{G}_{p_1}} \quad \cdots \quad \boxed{\widetilde{G}_{p_k}}$$

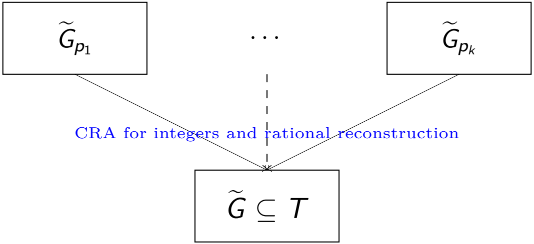
each p_i is a prime which is admissible of type B

DeleteUnluckyPrimes: *If $\mathcal{P}$ is the set of selected primes, with corresponding Gröbner bases collected in $\mathcal{GP}$, define an equivalence relation on $(\mathcal{GP}, \mathcal{P})$ by*

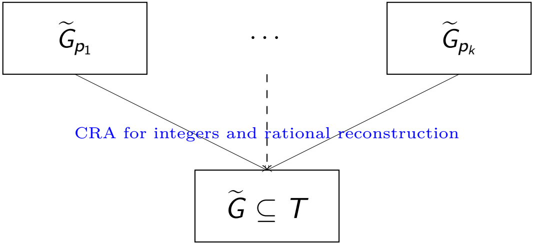
$$(\widetilde{G}_p, p) \sim (\widetilde{G}_q, q) :\Longleftrightarrow \mathsf{Lm}(\widetilde{G}_p) = \mathsf{Lm}(\widetilde{G}_q).$$

Store the equivalence class of largest cardinality in $(\mathcal{GP}, \mathcal{P})$, and delete the others [Idrees, Pfister, and Steidel, 2011].

A Test in Positive Characteristic: pTestSB



A Test in Positive Characteristic: pTestSB



pTestSB: *We randomly choose a prime* $p \notin \mathcal{P}$ *which is admissible of type* B *w.r.t.* f *and* $\widetilde{H}$. *We test if including this prime in the set* $\mathcal{P}$ *would improve the result. That is, we explicitly test whether* $\widetilde{I}_p$ *reduces to zero w.r.t* $\widetilde{G}$ *mapped to* $\mathbb{F}_p[X, t]$, *and vice-versa, whether* $\widetilde{G}$ *mapped to* $\mathbb{F}_p[X, t]$ *reduces to zero w.r.t.* $\widetilde{G}_p$. [Idrees, Pfister, and Steidel, 2011].

Final Test

For homogeneous ideals or for local monomial orderings, we have the following result:

Theorem (Arnold 2003 and Pfister 2007)

If $\widetilde{\mathsf{I}}$ reduces to zero w.r.t. $\widetilde{\mathsf{G}}$ and if $\widetilde{\mathsf{G}}$ is the reduced Gröbner basis of $\langle \widetilde{\mathsf{G}} \rangle$, then $\widetilde{\mathsf{I}} = \langle \widetilde{\mathsf{G}} \rangle$.

Theorem

Let $\widetilde{G}$ be the reduced Gröbner basis of $\widetilde{I}$ with respect to $\succ_K$. Then $(\widetilde{G} \setminus \{f\})|_{t=\alpha}$ is the reduced Gröbner basis of I with respect to $\succ_1$.

Theorem

Let $\widetilde{G}$ be the reduced Gröbner basis of $\widetilde{I}$ with respect to $\succ_K$. Then $(\widetilde{G} \setminus \{f\})|_{t=\alpha}$ is the reduced Gröbner basis of I with respect to $\succ_1$.

---

nfmodStd

Input: $I = \langle g_1(X,\alpha), \ldots, g_s(X,\alpha) \rangle \subseteq S = K[X]$.

Output: $G \subseteq S$, a Gröbner basis of I w.r.t. $\succ_1$.

1: map I to $\langle \widetilde{H} \rangle$ via the map sending α to t

2: $\widetilde{I} \longleftarrow \langle \widetilde{H} \rangle + \langle f \rangle$

3: compute the reduced Gröbner basis $\widetilde{G}$ of $\widetilde{I}$ w.r.t. $\succ_K = (\succ_1, \succ_2)$

4: lift $\widetilde{G}$ to G via the map sending t to α

5: **return** G

Implementation and Timings

- Our algorithm is implemented in SINGULAR in the library `nfmodstd.lib`.
  http://www.singular.uni-kl.de
  [Boku, Decker and Fieker, 2015].

	Magma	Singular					
deg	GB	std	modStd		nfmodStd		
			1 core	32 cores	1 core	32 cores	
2	1241.98	1.51	1.24	0.37	0.22	0.13	
5	error	70.55	19.59	4.79	1.89	0.61	
7	-	0.90	143.79	9.34	3.27	0.51	
7	-	314.00	11212.00	1118.78	97.43	19.23	
6	-	265.53	9163.38	567.03	686.01	99.41	
12	-	2061.95	3321.28	256.58	430.23	71.47	
2	2.93	8931.13	197.20	47.54	24.26	8.99	
8	-	0.90	2044.08	195.41	8.54	1.87	
7	-	15477.87	15274.97	4787.49	92.99	23.89	

GB = GroebnerBasis

Advantages of the New Method

Why is the new algorithm much faster than other known methods?

Advantages of the New Method

Why is the new algorithm much faster than other known methods?

- We do not directly use the computationally expensive arithmetic in K.

Advantages of the New Method

Why is the new algorithm much faster than other known methods?

- We do not directly use the computationally expensive arithmetic in K.
- The computations are carried out over finite fields which avoids coefficient swell.

Advantages of the New Method

Why is the new algorithm much faster than other known methods?

- We do not directly use the computationally expensive arithmetic in K.
- The computations are carried out over finite fields which avoids coefficient swell.
- Modulo p, we compute in rings with minimal polynomials of degree much less than $\mathsf{deg}(f)$.

Advantages of the New Method

Why is the new algorithm much faster than other known methods?

- We do not directly use the computationally expensive arithmetic in K.
- The computations are carried out over finite fields which avoids coefficient swell.
- Modulo p, we compute in rings with minimal polynomials of degree much less than $\mathsf{deg}(f)$.
- The algorithm is parallel in nature.