Signature-based criteria for computing weak Gröbner bases over PIDs

Maria Francis[1,2], Thibaut Verron[1]

1. Institute for Algebra, Johannes Kepler University, Linz, Austria
2. Indian Institute of Technology, Hyderabad, India

Special session *"Algorithms for zero-dimensional ideals"*, ACA 2018,
20 June 2018, Santiago de Compostela

Introduction and notations

Gröbner bases

- Valuable tool for many questions related to polynomial equations (resolution, elimination, dimension of the solutions...)
- Classically used for polynomials over fields
- Some applications with coefficients in general rings (elimination, combinatorics...)

Definition (Leading term, monomial, coefficient)

R ring, $A = R[X_1, \ldots, X_n]$ with a monomial order $<$, $f = \sum a_i \mathbf{X}^{b_i}$

- Leading term $\mathrm{LT}(f) = a_i \mathbf{X}^{b_i}$ with $\mathbf{X}^{b_i} > \mathbf{X}^{b_j}$ if $j \neq i$
- Leading monomial $\mathrm{LM}(f) = \mathbf{X}^{b_i}$
- Leading coefficient $\mathrm{LC}(f) = a_i$

Definitions for fields

For now $R = K$ is a field.

Definition (reduction)

f reduces to h mod G if there exists $g \in G$ and $a\mathbf{X}^b$ such that

- $\mathrm{LT}(f) = a\mathbf{X}^b \mathrm{LT}(g)$
- $h = f - a\mathbf{X}^b g$

By extension, f reduces to h mod G if there exists a chain of such reductions from f to h.

Definition (Gröbner basis)

$I \subset A$ ideal, a Gröbner basis of I is a finite set $G \subset I$ such that

- $\forall f \in I, f$ reduces to 0 mod G

or equivalently

- $\langle \mathrm{LT}(f) : f \in I \rangle = \langle \mathrm{LT}(g) : g \in G \rangle$

Buchberger's algorithm

- Input: $F = (f_1, \ldots, f_m) \subset \mathbb{K}[X_1, \ldots, X_n]$
- Output: G Gröbner basis of $\langle F \rangle$

1. $G \leftarrow \{f_i : i \in \{1, \ldots, m\}\}$
2. $\mathcal{P} \leftarrow$ pairs of elements of G
3. **while** $\mathcal{P}$ is not empty **do**
4.   Pick (i, j) from $\mathcal{P}$
5. $M(i,j) \leftarrow \mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$
6. $p \leftarrow \text{S-Pol}(g_i, g_j) = \frac{M(i,j)}{\mathrm{LM}(g_i)} g_i - \frac{M(i,j)}{\mathrm{LM}(g_j)} g_j$ (S-polynomial)
7. $r \leftarrow \textsc{Reduce}(p, G)$
8.   **if** $r \neq 0$ **then**
9.   Update G and $\mathcal{P}$ using r
10. **return** G

Signature improvements

[Faugère 2002 ; Gao, Guan, Volny 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

- Idea: keep track of the representation $g = \sum_i q_i f_i$ for $g \in \langle f_1, \ldots, f_m \rangle$
- The algorithm could keep track of the full representation... but it is expensive
- Instead define a signature $\mathfrak{s}(g)$ of g as

$$\mathfrak{s}(g) = \mathrm{LT}(q_j) e_j \text{ for some representation } g = \sum_{i=1}^{m} q_i f_i,\ q_j \text{ being the last non-zero coef.}$$

- Signatures are ordered by

$$a\mathbf{X}^b e_i < a' \mathbf{X}^{b'} e_j \iff i < j \text{ or } i = j \text{ and } \mathbf{X}^b < \mathbf{X}^{b'}$$

- If we never add together two elements with similar signature (regular S-polynomials) and only reduce by polynomials with smaller signature (regular reductions), then keeping track of the signature is free!
- Example: signature of a regular S-polynomial, $\text{S-Pol}(g_i, g_j) = \frac{M(i,j)}{\mathrm{LM}(g_i)} g_i - \frac{M(i,j)}{\mathrm{LM}(g_j)} g_j$:

$$\mathfrak{s}(\text{S-Pol}(g_i, g_j)) = S(i,j) = \max\left(\frac{M(i,j)}{\mathrm{LM}(g_i)}\mathfrak{s}(g_i), \frac{M(i,j)}{\mathrm{LM}(g_j)}\mathfrak{s}(g_j)\right)$$

Signature improvements

[Faugère 2002 ; Gao, Guan, Volny 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

- Idea: keep track of the representation $g = \sum_i q_i f_i$ for $g \in \langle f_1, \ldots, f_m \rangle$
- The algorithm could keep track of the full representation... but it is expensive
- Instead define a signature $\mathfrak{s}(g)$ of g as

$$\mathfrak{s}(g) = \mathrm{LT}(q_j)e_j \text{ for some representation } g = \sum_{i=1}^{m} q_i f_i,\ q_j \text{ being the last non-zero coef.}$$

- Signatures are ordered by

$$a\mathbf{X}^{b} e_i < a' \mathbf{X}^{b'} e_j \iff i < j \text{ or } i = j \text{ and } \mathbf{X}^{b} < \mathbf{X}^{b'}$$

- If we never add together two elements with similar signature (regular S-polynomials) and only reduce by polynomials with smaller signature (regular reductions), then keeping track of the signature is free!
- Example: signature of a regular S-polynomial, $\text{S-Pol}(g_i, g_j) = \frac{M(i,j)}{\mathrm{LM}(g_i)} g_i - \frac{M(i,j)}{\mathrm{LM}(g_j)} g_j$:

$$\mathfrak{s}(\text{S-Pol}(g_i, g_j)) = S(i,j) = \max\left(\frac{M(i,j)}{\mathrm{LM}(g_i)}\mathfrak{s}(g_i), \frac{M(i,j)}{\mathrm{LM}(g_j)}\mathfrak{s}(g_j)\right)$$

Signature improvements

[Faugère 2002 ; Gao, Guan, Volny 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

- Idea: keep track of the representation $g = \sum_i q_i f_i$ for $g \in \langle f_1, \ldots, f_m \rangle$
- The algorithm could keep track of the full representation... but it is expensive
- Instead define a signature $\mathfrak{s}(g)$ of g as

$$\mathfrak{s}(g) = \mathrm{LT}(q_j) e_j \text{ for some representation } g = \sum_{i=1}^{m} q_i f_i,\ q_j \text{ being the last non-zero coef.}$$

- Signatures are ordered by

$$a \mathbf{X}^b e_i < a' \mathbf{X}^{b'} e_j \iff i < j \text{ or } i = j \text{ and } \mathbf{X}^b < \mathbf{X}^{b'}$$

- If we never add together two elements with similar signature (regular S-polynomials) and only reduce by polynomials with smaller signature (regular reductions), then keeping track of the signature is free!
- Example: signature of a regular S-polynomial, $\text{S-Pol}(g_i, g_j) = \frac{M(i,j)}{\mathrm{LM}(g_i)} g_i - \frac{M(i,j)}{\mathrm{LM}(g_j)} g_j$:

$$\mathfrak{s}(\text{S-Pol}(g_i, g_j)) = S(i,j) = \max\left(\frac{M(i,j)}{\mathrm{LM}(g_i)} \mathfrak{s}(g_i), \frac{M(i,j)}{\mathrm{LM}(g_j)} \mathfrak{s}(g_j)\right)$$

Buchberger's algorithm with signatures

- Input: $F = (f_1, \ldots, f_m) \subset \mathbb{K}[X_1, \ldots, X_n]$
- Output: G Gröbner basis of $\langle F \rangle$

1. $G \leftarrow \{f_i$ with signature $e_i : i \in \{1, \ldots, m\}\}$
2. $\mathcal{P} \leftarrow$ (regular) pairs of elements of G
3. while $\mathcal{P}$ is not empty do
4. Pick (i, j) from $\mathcal{P}$ with smallest signature $S(i, j)$
5. $M(i, j) \leftarrow \mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$
6. $p \leftarrow \text{S-Pol}(g_i, g_j) = \frac{M(i,j)}{\mathrm{LM}(g_i)} g_i - \frac{M(i,j)}{\mathrm{LM}(g_j)} g_j$ (S-polynomial)
7. $r \leftarrow$ Regular-Reduce(p, G)
8. if $r \neq 0$ then
9. Update G and $\mathcal{P}$ using r with signature $\mathfrak{s}(r) = S(i, j)$
10. return G

Features of signatures

Key property

Buchberger's algorithm with signatures computes GB elements with increasing signatures.

Then we can add criteria...

Singular criterion: eliminate some redundant computations

If $\mathfrak{s}(g) \simeq \mathfrak{s}(g')$ then after regular reduction, $\mathsf{LM}(g) = \mathsf{LM}(g')$.

F5 criterion: eliminate Koszul syzygies $f_i f_j - f_j f_i = 0$

If $\mathfrak{s}(g) = \mathsf{LT}(g') e_j$ for some $g' \in G$ with $\mathfrak{s}(g') = \star e_i$ with $i < j$,
then g reduces to 0 modulo the already computed basis.

What about signatures for rings?

Main difficulty: how to order the signatures?

Over fields

$$a\mathbf{X}^b e_i < a' \mathbf{X}^{b'} e_j \iff i < j \text{ or } i = j \text{ and } \mathbf{X}^b < \mathbf{X}^{b'}$$

is a partial order but we can always normalize

Over rings, we need to take the coefficients into account.

Over Euclidean rings [Eder, Pfister, Popescu 2017]

- Possible to break ties with the absolute value of the coefficients
- Problem: signature drops = regular reductions leading to a smaller signature
- The algorithm can detect that it happens and serve as a preprocess
- Impossible to avoid signature drops?

In this work

- We use a partial order on the signatures: don't break the ties
- Advantages: no signature drops
- Risk: maybe we forbid too many reductions?
- **Main result:** the algorithm is correct and terminates

What about signatures for rings?

Main difficulty: how to order the signatures?

Over fields

$$a\mathbf{X}^b e_i < a'\mathbf{X}^{b'} e_j \iff i < j \text{ or } i = j \text{ and } \mathbf{X}^b < \mathbf{X}^{b'}$$

is a partial order but we can always normalize

Over rings, we need to take the coefficients into account.

Over Euclidean rings [Eder, Pfister, Popescu 2017]

- Possible to break ties with the absolute value of the coefficients
- Problem: signature drops = regular reductions leading to a smaller signature
- The algorithm can detect that it happens and serve as a preprocess
- Impossible to avoid signature drops?

In this work

- We use a partial order on the signatures: don't break the ties
- Advantages: no signature drops
- Risk: maybe we forbid too many reductions?
- **Main result:** the algorithm is correct and terminates

Definitions for rings

Definition (strong and weak reduction)

f strongly reduces to h mod G if there exists $g \in G$ and $a\mathbf{X}^b$ such that

- $\mathrm{LT}(f) = a\mathbf{X}^b \mathrm{LT}(g)$
- $h = f - a\mathbf{X}^b g$

f weakly reduces to h mod G if there exists $\{g_1, \ldots, g_r\} \subset G$, $a_1\mathbf{X}^{b_1}, \ldots, a_r\mathbf{X}^{b_r}$ such that

- $\mathrm{LT}(f) = \sum a_j \mathbf{X}^{b_j} \mathrm{LT}(g_j)$
- $h = f - \sum a_j \mathbf{X}^{b_j} g_j$

Definition (strong and weak Gröbner basis)

$I \subset A$ ideal, a strong Gröbner basis of I is a finite set $G \subset I$ such that

- $\forall f \in I, f$ strongly reduces to 0 mod G

A weak Gröbner basis of I is a finite set $G \subset I$ such that

- $\langle \mathrm{LT}(f) : f \in I \rangle = \langle \mathrm{LT}(g) : g \in G \rangle$

or equivalently

- $\forall f \in I, f$ weakly reduces to 0 mod G

Definitions for rings

Definition (strong and weak reduction)

f strongly reduces to h mod G if there exists $g \in G$ and $a\mathbf{X}^b$ such that

- $\mathrm{LT}(f) = a\mathbf{X}^b \mathrm{LT}(g)$
- $h = f - a\mathbf{X}^b g$

f weakly reduces to h mod G if there exists $\{g_1, \ldots, g_r\} \subset G$, $a_1\mathbf{X}^{b_1}, \ldots, a_r\mathbf{X}^{b_r}$ such that

- $\mathrm{LT}(f) = \sum a_j \mathbf{X}^{b_j} \mathrm{LT}(g_j)$
- $h = f - \sum a_j \mathbf{X}^{b_j} g_j$

Definition (strong and weak Gröbner basis)

$I \subset A$ ideal, a strong Gröbner basis of I is a finite set $G \subset I$ such that

- $\forall f \in I, f$ strongly reduces to 0 mod G

A weak Gröbner basis of I is a finite set $G \subset I$ such that

- $\langle \mathrm{LT}(f) : f \in I \rangle = \langle \mathrm{LT}(g) : g \in G \rangle$

or equivalently

- $\forall f \in I, f$ weakly reduces to 0 mod G

Definitions for rings

Definition (strong and weak reduction)

f strongly reduces to h mod G if there exists $g \in G$ and $a\mathbf{X}^b$ such that

- $\mathrm{LT}(f) = a\mathbf{X}^b \mathrm{LT}(g)$
- $h = f - a\mathbf{X}^b g$

f weakly reduces to h mod G if there exists $\{g_1, \ldots, g_r\} \subset G$, $a_1\mathbf{X}^{b_1}, \ldots, a_r\mathbf{X}^{b_r}$ such that

- $\mathrm{LT}(f) = \sum a_j \mathbf{X}^{b_j} \mathrm{LT}(g_j)$
- $h = f - \sum a_j \mathbf{X}^{b_j} g_j$

Definition (strong and weak Gröbner basis)

$I \subset A$ ideal, a strong Gröbner basis of I is a finite set $G \subset I$ such that

- $\forall f \in I, f$ strongly reduces to 0 mod G

A weak Gröbner basis of I is a finite set $G \subset I$ such that

- $\langle \mathrm{LT}(f) : f \in I \rangle = \langle \mathrm{LT}(g) : g \in G \rangle$

or equivalently

- $\forall f \in I, f$ weakly reduces to 0 mod G

Strong vs weak Gröbner bases

	Strong Gröbner basis	Weak Gröbner basis
Exists?	Only for PIDs	Always
Defines a normal form?	Yes	Almost
Can test ideal membership?	Yes	Yes

From strong to weak

If G is a strong Gröbner basis of I, then G is a weak Gröbner basis of I.

From weak to strong

If R is a PID and G is a weak Gröbner basis of I, then a strong Gröbner basis can be obtained by forming "GCD-polynomials" with elements of G, without any reduction.

Algorithms for strong Gröbner bases:

- Variants of Buchberger [Buchberger 1984 ; Kandri-Rody, Kapur 1988 ; Möller 1988...]

Algorithms for weak Gröbner bases:

- Algorithm for generalized Noetherian rings [Möller 1988]

Möller's algorithm for weak Gröbner bases

- Input: $F = (f_1, \ldots, f_m) \subset R[X_1, \ldots, X_n]$
- Output: G weak Gröbner basis of $\langle F \rangle$

$G \leftarrow \{f_i : i \in \{1, \ldots, m\}\}$
$\mathcal{S} \leftarrow$ possible saturated sets
while $\mathcal{S}$ is not empty **do**
    Pick a J from $\mathcal{S}$
    $p \leftarrow \text{S-Pol}(J) = \sum_{j \in J} a_j \mathbf{X}^{b_j} g_j$
    $r \leftarrow \textsc{WeaklyReduce}(p, G)$
    if $r \neq 0$ **then**
        Update G and $\mathcal{S}$ using r
return G

Saturated sets

Definition (Saturated set)

Given a basis $\{g_1, \ldots, g_s\}$, saturated sets are constructed as follows:

1. Pick $J \subset \{1, \ldots s\}$
2. $M(J) \leftarrow \operatorname{lcm}\{\mathrm{LM}(g_j) : j \in J\}$
3. Add to J all $j \in \{1, \ldots, s\}$ such that $\mathrm{LM}(g_j)$ divides $M(J)$

Then there exists $(a_i)_{i \in J}$ such that the S-polynomial

$$\text{S-Pol}(J) = \sum_{i \in J} a_i \frac{M(J)}{\mathrm{LM}(g_i)} g_i$$

has leading term $< M(J)$.

Regular saturated sets and their signatures

Definition (Saturated set)

Given a basis $\{g_1, \dots, g_s\}$, saturated sets are constructed as follows:

1. Pick $J \subset \{1, \dots s\}$
2. $M(J) \leftarrow \operatorname{lcm}\{\mathrm{LM}(g_j) : j \in J\}$
3. Add to J all $j \in \{1, \dots, s\}$ such that $\mathrm{LM}(g_j)$ divides $M(J)$

Then there exists $(a_i)_{i \in J}$ such that the S-polynomial

$$\text{S-Pol}(J) = \sum_{i \in J} a_i \frac{M(J)}{\mathrm{LM}(g_i)} g_i$$

has leading term $< M(J)$.

The signature of a saturated set is

$$S(J) = \max\left(a_i \frac{M(J)}{\mathrm{LM}(g_i)} \mathfrak{s}(g_i)\right)_{i \in J}$$

A regular saturated set is constructed such that this max is reached only once. Then

$$S(J) = \mathfrak{s}(\text{S-Pol}(J))$$

Möller's algorithm for weak Gröbner bases with signatures

- Input: $F = (f_1, \ldots, f_m) \subset R[X_1, \ldots, X_n]$
- Output: G weak Gröbner basis of $\langle F \rangle$

```
G ← {f_i with signature e_i : i ∈ {1, ..., m}}
𝒮 ← possible regular saturated sets
while 𝒮 is not empty do
        Pick a J from 𝒮 with smallest signature S(J)
        p ← S-Pol(J) = ∑_{j∈J} a_j X^{b_j} g_j
        r ← Regular-WeaklyReduce(p, G)
        if r ≠ 0 then
                Update G and 𝒮 using r with signature S(J)
return G
```

Are we doing the right thing?

By disregarding the coefficients when comparing the signatures:

- Signature drops cannot happen by definition
- We eliminate more "S-pairs"
- We form more S-polynomials (with smaller J's)

So... We don't have signature drops, but maybe we eliminate too much? Or not enough?

Main result

If the coefficient ring is a PID, then:

- The algorithm terminates
- The algorithm computes a Gröbner basis with non-decreasing signatures
- If the input is a regular sequence, all reductions to zero are eliminated by criteria

Idea of the proof of correctness

Theorem

Assume that all regular S-polynomials weakly reduce to 0 modulo G,
then all polynomials $f \in I$ weakly reduce to 0 modulo G, *i.e.* G is a weak Gröbner basis of I.

Key lemma

Let $p \in I$ with signature s, then there exists $g \in G$ such that:

- $s = \mathfrak{s}(p) = a\mathbf{X}^b\mathfrak{s}(g)$ for some $a \in R$, $b \in \mathbb{N}^n$;
- $a\mathbf{X}^b g$ is regularly weak-reduced modulo G.

Main difficulty : handling this a !

Conclusion and future work

What was done

- Proof-of-concept algorithm for computing Gröbner bases with signatures over PIDs
- Proved to be correct and terminate, criteria still work

The future

- Strong Gröbner bases for PIDs: appears to be possible to implement signatures in Buchberger's algorithm + optimizations such as Gebauer-Möller's criteria
- Getting rid of the combinatorical bottleneck?
- What about other rings? The algorithm can input polynomials in any effective ring!
  - Fields, PID: done
  - UFD : appears to work experimentally!
- What about even more general rings?
  - Non UFD, non GCD domain : would require very different proofs
  - Rings with divisors of zero : there we cannot even guarranty that

$$\mathrm{LM}(a\mathbf{X}^b g) = \mathbf{X}^b \mathrm{LM}(g)!$$

Conclusion and future work

What was done

- Proof-of-concept algorithm for computing Gröbner bases with signatures over PIDs
- Proved to be correct and terminate, criteria still work

The future

- Strong Gröbner bases for PIDs: appears to be possible to implement signatures in Buchberger's algorithm + optimizations such as Gebauer-Möller's criteria
- Getting rid of the combinatorical bottleneck?
- What about other rings? The algorithm can input polynomials in any effective ring!
  - Fields, PID: done
  - UFD : appears to work experimentally!
- What about even more general rings?
  - Non UFD, non GCD domain : would require very different proofs
  - Rings with divisors of zero : there we cannot even guarranty that

$$\mathrm{LM}(a\mathbf{X}^b g) = \mathbf{X}^b \mathrm{LM}(g)!$$

Conclusion and future work

What was done

- Proof-of-concept algorithm for computing Gröbner bases with signatures over PIDs
- Proved to be correct and terminate, criteria still work

The future

- Strong Gröbner bases for PIDs: appears to be possible to implement signatures in Buchberger's algorithm + optimizations such as Gebauer-Möller's criteria
- Getting rid of the combinatorical bottleneck?
- What about other rings? The algorithm can input polynomials in any effective ring!
  - Fields, PID: done
  - UFD : appears to work experimentally!
- What about even more general rings?
  - Non UFD, non GCD domain : would require very different proofs
  - Rings with divisors of zero : there we cannot even guarranty that

$$\mathsf{LM}(a\mathbf{X}^b g) = \mathbf{X}^b \mathsf{LM}(g)!$$

Thank you for your attention!

More information and references:

- Maria Francis and Thibaut Verron (2018). ‘Signature-based Criteria for Möller’s Algorithm for Computing Gröbner Bases over Principal Ideal Domains’. In: *ArXiv e-prints.* arXiv: 1802.01388 [cs.SC]