Algorithms for minimal staggered linear bases

Amir Hashemi[2], Nicolas Jagersma[1], **Matthias Orth**[1], Werner M. Seiler[1]

[1]University of Kassel, Germany [2]Isfahan University of Technology, Iran

Computer Algebra in Scientific Computing (CASC)
Rennes, 4 September 2024

Table of Contents

Motivation

- Many different approaches to optimising Gröbner basis computations:
  - Use of criteria for useless pairs (Gebauer–Möller algorithm)
  - Use of syzygies (Möller–Mora–Traverso algorithm)
  - Linear algebra methods (F_4 algorithm)
  - Signature-based methods (F_5 algorithm)
  - Combinatorial structures (involutive bases)

Motivation

- Many different approaches to optimising Gröbner basis computations:
  - Use of criteria for useless pairs (Gebauer–Möller algorithm)
  - Use of syzygies (Möller–Mora–Traverso algorithm)
  - Linear algebra methods (F_4 algorithm)
  - Signature-based methods (F_5 algorithm)
  - Combinatorial structures (involutive bases)
- Staggered linear bases, by concept of *allowed and forbidden terms*
  - Directly incorporate criteria for useless pairs
  - Lead naturally to bases for syzygy modules
  - Are generalisation of involutive and related (Janet-like...) bases

Historical remarks

Gröbner and related bases:

- Janet (1920, 1929): Janet bases for linear partial differential equations
- Buchberger (1965): Gröbner bases
- Buchberger (1979): Criteria for useless pairs
- Gebauer and Möller (1988): Algorithm using criteria efficiently
- Schreyer (1993): Gröbner bases for syzygy modules
- Zharkov and Blinkov (1996): Involutive bases
- Faugère (1999): F_4, (2002): F_5
- Other signature-based: e.g. Gao, Volny, and Wang (2016)

Historical remarks

Gröbner and related bases:

- Janet (1920, 1929): Janet bases for linear partial differential equations
- Buchberger (1965): Gröbner bases
- Buchberger (1979): Criteria for useless pairs
- Gebauer and Möller (1988): Algorithm using criteria efficiently
- Schreyer (1993): Gröbner bases for syzygy modules
- Zharkov and Blinkov (1996): Involutive bases
- Faugère (1999): F_4, (2002): F_5
- Other signature-based: e.g. Gao, Volny, and Wang (2016)

Staggered linear bases in particular:

- Gebauer and Möller (1986): First definition
- Möller (1992): Algorithm using intermediate syzygies
- Hashemi and Javanbakht (2021): Incremental signature-based algo.
- Hashemi and Möller (2023): Algorithm using Möller's lifting theorem

Notation

- Polynomial ring: $\mathcal{P} = \mathcal{K}[x_1, \ldots, x_n]$ over field $\mathcal{K}$
- Set of terms: $\mathbb{T} = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha_i \geq 0\}$
- Term ordering $\prec$ on $\mathbb{T}$

Notation

- Polynomial ring: $\mathcal{P} = \mathcal{K}[x_1, \ldots, x_n]$ over field $\mathcal{K}$
- Set of terms: $\mathbb{T} = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha_i \geq 0\}$
- Term ordering $\prec$ on $\mathbb{T}$
- For polynomial $0 \neq f = \sum_{i=1}^{m} c_i \cdot t_i \neq 0$, where $c_i \in \mathcal{K}$ and $t_i \in \mathbb{T}$
  - Support: $\operatorname{supp}(f) = \{t_i \mid c_i \neq 0\}$
  - Leading term: $\operatorname{lt}(f) = \max_{\prec}(\operatorname{supp}(f))$
  - Leading coefficient: $\operatorname{lc}(f) = c_{\operatorname{lt}(f)}$
  - Leading monomial: $\operatorname{lm}(f) = \operatorname{lc}(f)\operatorname{lt}(f)$

Notation

- Polynomial ring: $\mathcal{P} = \mathcal{K}[x_1, \ldots, x_n]$ over field $\mathcal{K}$
- Set of terms: $\mathbb{T} = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha_i \geq 0\}$
- Term ordering $\prec$ on $\mathbb{T}$
- For polynomial $0 \neq f = \sum_{i=1}^{m} c_i \cdot t_i \neq 0$, where $c_i \in \mathcal{K}$ and $t_i \in \mathbb{T}$
  - Support: $\operatorname{supp}(f) = \{t_i \mid c_i \neq 0\}$
  - Leading term: $\operatorname{lt}(f) = \max_\prec(\operatorname{supp}(f))$
  - Leading coefficient: $\operatorname{lc}(f) = c_{\operatorname{lt}(f)}$
  - Leading monomial: $\operatorname{lm}(f) = \operatorname{lc}(f)\operatorname{lt}(f)$
- For finite set $F = \{f_1, \ldots, f_s\} \subseteq \mathcal{P}$
  - Ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ generated by F
  - Write $\mathrm{T}(i) = \operatorname{lt}(f_i)$ and $\mathrm{T}(i,j) = \operatorname{lcm}(\operatorname{lt}(f_i), \operatorname{lt}(f_j))$
  - $\operatorname{lt}(F) = \{\mathrm{T}(1), \ldots, \mathrm{T}(s)\}$
  - Leading term ideal: $\operatorname{lt}(\mathcal{I}) = \langle \operatorname{lt}(f) \mid 0 \neq f \in \mathcal{I} \rangle$
  - finite set $G \subset \mathcal{I}$ is a *Gröbner basis* for $\mathcal{I}$ if $\operatorname{lt}(\mathcal{I}) = \langle \operatorname{lt}(G) \rangle$

Notation

- Polynomial ring: $\mathcal{P} = \mathcal{K}[x_1, \ldots, x_n]$ over field $\mathcal{K}$
- Set of terms: $\mathbb{T} = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha_i \geq 0\}$
- Term ordering $\prec$ on $\mathbb{T}$
- For polynomial $0 \neq f = \sum_{i=1}^{m} c_i \cdot t_i \neq 0$, where $c_i \in \mathcal{K}$ and $t_i \in \mathbb{T}$
  - Support: $\mathrm{supp}(f) = \{t_i \mid c_i \neq 0\}$
  - Leading term: $\mathrm{lt}(f) = \max_{\prec}(\mathrm{supp}(f))$
  - Leading coefficient: $\mathrm{lc}(f) = c_{\mathrm{lt}(f)}$
  - Leading monomial: $\mathrm{lm}(f) = \mathrm{lc}(f)\,\mathrm{lt}(f)$
- For finite set $F = \{f_1, \ldots, f_s\} \subseteq \mathcal{P}$
  - Ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ generated by F
  - Write $\mathrm{T}(i) = \mathrm{lt}(f_i)$ and $\mathrm{T}(i,j) = \mathrm{lcm}(\mathrm{lt}(f_i), \mathrm{lt}(f_j))$
  - $\mathrm{lt}(F) = \{\mathrm{T}(1), \ldots, \mathrm{T}(s)\}$
  - Leading term ideal: $\mathrm{lt}\,(\mathcal{I}) = \langle \mathrm{lt}(f) \mid 0 \neq f \in \mathcal{I} \rangle$
  - finite set $G \subset \mathcal{I}$ is a *Gröbner basis* for $\mathcal{I}$ if $\mathrm{lt}\,(\mathcal{I}) = \langle \mathrm{lt}(G) \rangle$
- S-polynomial of polynomials f_i and f_j:
  $\mathrm{Spoly}(f_i, f_j) = \frac{\mathrm{T}(i,j)}{\mathrm{lm}(f_i)} \cdot f_i - \frac{\mathrm{T}(i,j)}{\mathrm{lm}(f_j)} \cdot f_j$.

Table of Contents

Staggered linear bases

Given an ideal $\mathcal{I} \subset \mathcal{P}$, can consider it as a $\mathcal{K}$-linear subspace of $\mathcal{P}$.
A staggered linear basis is a special basis for this vector space:

Definition

Given ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$, then $\mathbf{B} = \bigcup_{i=1}^{s} \mathbb{A}_i \cdot f_i$ with $\mathbb{A}_1, \ldots, \mathbb{A}_s \subseteq \mathbb{T}$ is a staggered linear basis for $\mathcal{I}$, if:

(1) $\forall \; t_j \in \mathbb{T} \setminus \mathbb{A}_j \; \exists \; t_i \in \mathbb{A}_i$ with $i < j$ such that $t_i \cdot \mathrm{lt}(f_i) = t_j \cdot \mathrm{lt}(f_j)$,

(2) $\forall \; t_j \in \mathbb{T} \setminus \mathbb{A}_j \, , t \in \mathbb{T}$ it holds $t \cdot t_j \in \mathbb{T} \setminus \mathbb{A}_j$,

(3) $\forall \; t_i \in \mathbb{A}_i, t_j \in \mathbb{A}_j$ with $i \neq j$ we have $t_i \cdot \mathrm{lt}(f_i) \neq t_j \, \mathrm{lt}(f_j)$.

Staggered linear bases

Given an ideal $\mathcal{I} \subset \mathcal{P}$, can consider it as a $\mathcal{K}$-linear subspace of $\mathcal{P}$.
A staggered linear basis is a special basis for this vector space:

Definition

Given ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$, then $\mathbf{B} = \bigcup_{i=1}^{s} \mathbb{A}_i \cdot f_i$ with $\mathbb{A}_1, \ldots, \mathbb{A}_s \subseteq \mathbb{T}$ is a staggered linear basis for $\mathcal{I}$, if:

(1) $\forall \ t_j \in \mathbb{T} \setminus \mathbb{A}_j \ \exists \ t_i \in \mathbb{A}_i$ with $i < j$ such that $t_i \cdot \mathrm{lt}(f_i) = t_j \cdot \mathrm{lt}(f_j)$,

(2) $\forall \ t_j \in \mathbb{T} \setminus \mathbb{A}_j, t \in \mathbb{T}$ it holds $t \cdot t_j \in \mathbb{T} \setminus \mathbb{A}_j$,

(3) $\forall \ t_i \in \mathbb{A}_i, t_j \in \mathbb{A}_j$ with $i \neq j$ we have $t_i \cdot \mathrm{lt}(f_i) \neq t_j \, \mathrm{lt}(f_j)$.

- $\mathbb{A}_i \rightsquigarrow$ set of allowed terms of f_i
- $\mathbb{T} \setminus \mathbb{A}_i \rightsquigarrow$ set of forbidden terms for f_i
- Write $\mathbb{F}_i$ for the minimal generating system of $\mathbb{T} \setminus \mathbb{A}_i$
- Thus, $\mathbb{A}_i = \mathbb{T} \setminus \langle \mathbb{F}_i \rangle$

Structure of forbidden terms

Notation

- We use the abbreviation SLB for "staggered linear basis".
- For SLB $\mathbf{B}$, instead of $\mathbf{B} = \mathbb{A}_1 \cdot f_1 \cup \cdots \cup \mathbb{A}_s \cdot f_s$, also write $\{(f_1, \mathbb{F}_1), \ldots, (f_s, \mathbb{F}_s)\}$. (Where the $\mathbb{F}_i$ are finite.)

Structure of forbidden terms

Notation

- We use the abbreviation SLB for "staggered linear basis".
- For SLB $\mathbf{B}$, instead of $\mathbf{B} = \mathbb{A}_1 \cdot f_1 \cup \cdots \cup \mathbb{A}_s \cdot f_s$, also write $\{(f_1, \mathbb{F}_1), \ldots, (f_s, \mathbb{F}_s)\}$. (Where the $\mathbb{F}_i$ are finite.)

Example

The monomial ideal $\mathcal{I} = \langle x_1x_3^3, x_1x_2, x_2^2, x_1^2x_3 \rangle$ has an SLB

$$\mathbf{B} = \left\{(x_1x_3^3, \emptyset),\ (x_1x_2, \{x_3^3\}),\ (x_2^2, \{x_1\}),\ (x_1^2x_3, \{x_3^2, x_2\})\right\}\ .$$

Structure of forbidden terms

Notation

- We use the abbreviation SLB for "staggered linear basis".
- For SLB $\mathbf{B}$, instead of $\mathbf{B} = \mathbb{A}_1 \cdot f_1 \cup \cdots \cup \mathbb{A}_s \cdot f_s$, also write $\{(f_1, \mathbb{F}_1), \ldots, (f_s, \mathbb{F}_s)\}$. (Where the $\mathbb{F}_i$ are finite.)

Example

The monomial ideal $\mathcal{I} = \langle x_1x_3^3, x_1x_2, x_2^2, x_1^2x_3 \rangle$ has an SLB

$$\mathbf{B} = \left\{(x_1x_3^3, \emptyset), (x_1x_2, \{x_3^3\}), (x_2^2, \{x_1\}), (x_1^2x_3, \{x_3^2, x_2\})\right\} .$$

Lemma

Let $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ be an ideal and $\{f_1, \ldots, f_s\}$ a Gröbner basis for $\mathcal{I}$. Then, $\mathbf{B} = \{(f_1, \mathbb{F}_1), \ldots, (f_s, \mathbb{F}_s)\}$ is an SLB for $\mathcal{I}$ $\iff$ Each $\mathbb{F}_i$ is the minimal generating set of $\langle \mathrm{T}(1), \ldots, \mathrm{T}(i-1) \rangle : \mathrm{T}(i)$.

Minimal SLBs

Definition

SLB $\mathbf{B} = \{(f_1, \mathbb{F}_1), \ldots, (f_s, \mathbb{F}_s)\}$ for ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ is minimal, if

- for each i, j with $i \neq j$ the leading term of f_i does not divide that of f_j,
- for each i, we have $\mathrm{lc}(f_i) = 1$.

Minimal SLBs

Definition

SLB $\mathbf{B} = \{(f_1, \mathbb{F}_1), \ldots, (f_s, \mathbb{F}_s)\}$ for ideal $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ is minimal, if

- for each i, j with $i \neq j$ the leading term of f_i does not divide that of f_j,
- for each i, we have $\operatorname{lc}(f_i) = 1$.

Can minimize a given SLB:

Proposition

Given: Monic, non-minimal SLB $\mathbf{B} = \{(f_1, \mathbb{F}_1), \ldots, (f_s, \mathbb{F}_s)\}$ for $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$. Let $j > i$ with $\mathrm{T}(j) \mid \mathrm{T}(i)$.
Get new SLB for $\mathcal{I}$ by removing $(f_i, \mathbb{F}_i)$ and updating $\mathbb{F}_\ell$ for $\ell \neq i$:

- *If $\ell < i$ or $\ell > j$ or $\mathrm{T}(i,\ell)/\mathrm{T}(\ell) \notin \mathbb{F}_\ell$, don't change $\mathbb{F}_\ell$*
- *Otherwise, new forbidden terms $\mathbb{F}'_\ell$ are the minimal generators of $\left\langle \mathbb{F}_\ell \setminus \{\mathrm{T}(i,\ell)/\mathrm{T}(\ell)\} \cup_{k=1}^{\ell-1} \{\mathrm{T}(k,\ell)/\mathrm{T}(\ell) \mid k \neq i \wedge \mathrm{T}(i) \mid \mathrm{T}(k,\ell)\} \right\rangle$.*

SLB minimisation

Remark

Another way to update $\mathbb{F}_i$'s is as follows.

- *Can work with non-minimal sets* $\mathbb{F}_i = \{\mathrm{T}(1,i)/\mathrm{T}(i), \ldots, \mathrm{T}(i-1,i)/\mathrm{T}(i)\}$ *throughout.*
- *Now can simply update* $\mathbb{F}_\ell$ *for each* $\ell = i+1, \ldots, j$ *to* $\{\mathrm{T}(1,\ell)/\mathrm{T}(\ell), \ldots, \mathrm{T}(\ell-1,\ell)/\mathrm{T}(\ell)\} \setminus \{\mathrm{T}(i,\ell)/\mathrm{T}(\ell)\}$.

Example

In $\mathcal{P} = \mathcal{K}[x_1, x_2]$, $\mathcal{I} = \langle x_1^3, x_1x_2, x_2^2 \rangle$ has SLB

$$\mathbf{B} = \{(x_1^3, \emptyset), (x_1x_2^2, \{x_1^2\}), (x_2^2, \{x_1\}), (x_1x_2, \{x_1^2, x_2\})\}.$$

Removing the second element using the last one, obtain a minimal SLB

$$\mathbf{B}' = \{(x_1^3, \emptyset), (x_2^2, \{x_1^3\}), (x_1x_2, \{x_1^2, x_2\})\}.$$

Syzygies from SLBs

From Gröbner basis $F = \{f_1, \ldots, f_s\}$, can get Gröbner basis for the first syzygy module $\mathrm{Syz}(F)$ by well-known Schreyer's construction.
We derive the following analogous result for SLBs:

Syzygies from SLBs

From Gröbner basis $F = \{f_1, \ldots, f_s\}$, can get Gröbner basis for the first syzygy module $\mathrm{Syz}(F)$ by well-known Schreyer's construction.
We derive the following analogous result for SLBs:

Theorem

Let $\mathbf{B} = \{(f_1, \mathbb{F}_1), \ldots, (f_s, \mathbb{F}_s)\}$ *be an SLB for the ideal* $\mathcal{I} \subset \mathcal{P}$. *Write* $\mathbf{s}_{ij}$ *for the syzygy induced by* $\mathrm{Spoly}(f_i, f_j)$. *Minimal SLB for* $\mathrm{Syz}(f_1, \ldots, f_s)$*:*

$$\mathbf{S} = \{(\mathbf{s}_{ij}, \mathbb{H}_{ij}) \mid i < j \text{ and } \mathrm{T}(i,j)/\mathrm{T}(j) \in \mathbb{F}_j\},$$

where $\mathbb{H}_{ij}$ *is the minimal generating set of*

$$\langle \mathrm{T}(i,j,\ell)/\mathrm{T}(i,j) \mid \ell < i < j \text{ and } \mathrm{T}(i,j)/\mathrm{T}(j), \mathrm{T}(\ell,j)/\mathrm{T}(j) \in \mathbb{F}_j \rangle.$$

Table of Contents

Algorithm for minimal SLBs

We have designed an algorithm for computing a minimal SLB for an ideal given by a finite set of generators. Its main operations are:

Algorithm for minimal SLBs

We have designed an algorithm for computing a minimal SLB for an ideal given by a finite set of generators. Its main operations are:

- The algorithm is incremental. The polynomials (also from the input set) are added one at a time to the candidate SLB.

Algorithm for minimal SLBs

We have designed an algorithm for computing a minimal SLB for an ideal given by a finite set of generators. Its main operations are:

- The algorithm is incremental. The polynomials (also from the input set) are added one at a time to the candidate SLB.
- When adding a new polynomial f_s (i.e., after precomputation, the remainder of an S-Polynomial),
  - Compute: $A = \{\mathrm{T}(i,s)/\mathrm{T}(s) \mid i = 1,\ldots,s-1, \mathrm{T}(i,s)/\mathrm{T}(i) \notin \langle \mathbb{F}_i \rangle\}$
  - Extract minimal generating set of A and store involved indices (i,s)
  - Add pair (f_i, f_s)
  - In case $\mathrm{T}(s) \mid \mathrm{T}(i)$, remove all old pairs involving f_i, update $\mathbb{F}_j$'s
  - Else, add $\mathrm{T}(i,s)/\mathrm{T}(s)$ to the forbidden terms $\mathbb{F}_s$ and add pair (f_i, f_s), unless $\mathrm{T}(i)$ and $\mathrm{T}(s)$ are coprime

Differences to basic SLB algorithm

In contrast to Algorithms 1 and 2 in [Hashemi and Möller 2023]:

- We initialise the forbidden term sets as empty.
- Thus we first keep $\mathrm{T}(i,j)/\mathrm{T}(j)$ in A when $\mathrm{T}(i)$ and $\mathrm{T}(j)$ are co-prime, enabling the removal of more redundant critical pairs later on.
- If a pair (f_i, f_j) satisfies Buchberger's first criterion, we remove it later.
- When $\mathrm{T}(j)$ divides $\mathrm{T}(i)$, we can not only eliminate f_i from F, but also all critical pairs in which one component is f_i, except for (f_i, f_j).

Timings: Methodology

- We have implemented a preliminary version of the improved algorithm described in [Hashemi and Möller 2023], which we call *SLB* here.
- Implementation in the C++ library `CoCoALib` (v. 0.99818).
- We compare *SLB* to `CoCoA`'s built-in function *GBasis* (*GB* for short).

Timings: Methodology

- We have implemented a preliminary version of the improved algorithm described in [Hashemi and Möller 2023], which we call *SLB* here.
- Implementation in the C++ library `CoCoALib` (v. 0.99818).
- We compare *SLB* to `CoCoA`'s built-in function *GBasis* (*GB* for short).
- Test examples from Database of Polynomial Systems (Verschelde).
- Always used graded reverse lexicographic order.

Timings: Methodology

- We have implemented a preliminary version of the improved algorithm described in [Hashemi and Möller 2023], which we call *SLB* here.
- Implementation in the C++ library `CoCoALib` (v. 0.99818).
- We compare *SLB* to `CoCoA`'s built-in function *GBasis* (*GB* for short).
- Test examples from Database of Polynomial Systems (Verschelde).
- Always used graded reverse lexicographic order.
- Hardware: Intel(R) Core(TM) i5-10400F processor, 2.90 GHz, 2904 MHz, 6 cores, 12 logical processors, 16 GB RAM and 64 bits.

Timings

SLB vs GBasis over $\mathbb{Z}$ mod 32003						
	time (sec)			number of (zero-)reductions		
Poly set	**SLB**	**GB**	**ratio**	**SLB**	**GB**	**ratio**
Chemkin	0.095	0.089	1.07	488 (412)	488 (403)	1.00
Eco7	0.014	0.024	0.58	168 (131)	159 (117)	1.06
Eco8	0.081	0.095	0.85	362 (295)	358 (281)	1.01
Noon4	0.003	0.005	0.60	77 (53)	75 (47)	1.03
Noon5	0.019	0.025	0.76	280 (213)	267 (195)	1.05
Cyclic5	0.011	0.002	5.50	127 (86)	113 (75)	1.12
Cyclic6	0.111	0.042	2.64	758 (579)	344 (245)	2.20
Katsura6	0.037	0.046	0.80	164 (128)	169 (128)	0.97
Katsura7	0.264	0.273	0.97	378 (310)	381 (307)	0.99
Katsura8	1.873	1.964	0.95	882 (746)	886 (743)	1.00

Table: Comparison of *SLB* and *GBasis* over $\mathbb{Z}/32003\mathbb{Z}$.

Timings

SLB vs GBasis over $\mathbb{Z}$ mod 32003						
	time (sec)			number of (zero-)reductions		
Poly set	**SLB**	**GB**	**ratio**	**SLB**	**GB**	**ratio**
Chemkin	0.095	0.089	1.07	488 (412)	488 (403)	1.00
Eco7	0.014	0.024	0.58	168 (131)	159 (117)	1.06
Eco8	0.081	0.095	0.85	362 (295)	358 (281)	1.01
Noon4	0.003	0.005	0.60	77 (53)	75 (47)	1.03
Noon5	0.019	0.025	0.76	280 (213)	267 (195)	1.05
Cyclic5	0.011	0.002	5.50	127 (86)	113 (75)	1.12
Cyclic6	0.111	0.042	2.64	758 (579)	344 (245)	2.20
Katsura6	0.037	0.046	0.80	164 (128)	169 (128)	0.97
Katsura7	0.264	0.273	0.97	378 (310)	381 (307)	0.99
Katsura8	1.873	1.964	0.95	882 (746)	886 (743)	1.00

Table: Comparison of *SLB* and *GBasis* over $\mathbb{Z}/32003\mathbb{Z}$.

Timings

SLB vs GBasis over $\mathbb{Z}$ mod 32003						
	time (sec)			number of (zero-)reductions		
Poly set	**SLB**	**GB**	**ratio**	**SLB**	**GB**	**ratio**
Chemkin	0.095	0.089	1.07	488 (412)	488 (403)	1.00
Eco7	0.014	0.024	0.58	168 (131)	159 (117)	1.06
Eco8	0.081	0.095	0.85	362 (295)	358 (281)	1.01
Noon4	0.003	0.005	0.60	77 (53)	75 (47)	1.03
Noon5	0.019	0.025	0.76	280 (213)	267 (195)	1.05
Cyclic5	0.011	0.002	5.50	127 (86)	113 (75)	1.12
Cyclic6	0.111	0.042	2.64	758 (579)	344 (245)	2.20
Katsura6	0.037	0.046	0.80	164 (128)	169 (128)	0.97
Katsura7	0.264	0.273	0.97	378 (310)	381 (307)	0.99
Katsura8	1.873	1.964	0.95	882 (746)	886 (743)	1.00

Table: Comparison of *SLB* and *GBasis* over $\mathbb{Z}/32003\mathbb{Z}$.

Timings

SLB vs GBasis over $\mathbb{Z}$ mod 32003						
	time (sec)			number of (zero-)reductions		
Poly set	**SLB**	**GB**	**ratio**	**SLB**	**GB**	**ratio**
Chemkin	0.095	0.089	1.07	488 (412)	488 (403)	1.00
Eco7	0.014	0.024	0.58	168 (131)	159 (117)	1.06
Eco8	0.081	0.095	0.85	362 (295)	358 (281)	1.01
Noon4	0.003	0.005	0.60	77 (53)	75 (47)	1.03
Noon5	0.019	0.025	0.76	280 (213)	267 (195)	1.05
Cyclic5	0.011	0.002	5.50	127 (86)	113 (75)	1.12
Cyclic6	0.111	0.042	2.64	758 (579)	344 (245)	2.20
Katsura6	0.037	0.046	0.80	164 (128)	169 (128)	0.97
Katsura7	0.264	0.273	0.97	378 (310)	381 (307)	0.99
Katsura8	1.873	1.964	0.95	882 (746)	886 (743)	1.00

Table: Comparison of *SLB* and *GBasis* over $\mathbb{Z}/32003\mathbb{Z}$.

Table of Contents

Complementary decompositions

Definition

- A *generalised cone* $(t, \mathbb{F})$ for some $t \in \mathbb{T}$ is a set $\{t \cdot u \mid u \in \mathbb{T} \setminus \langle \mathbb{F} \rangle\}$.
- A (generalised) *complementary decomposition* (CD) of the monomial ideal $\mathcal{I}$ is a finite set $\{(t_1, \mathbb{F}_1), \ldots, (t_r, \mathbb{F}_r)\}$ of disjoint generalised cones such that $\mathbb{T} \setminus \mathcal{I} = \cup_{i=1}^{r} (t_i, \mathbb{F}_i)$.

Complementary decompositions

Definition

- A *generalised cone* $(t, \mathbb{F})$ for some $t \in \mathbb{T}$ is a set $\{t \cdot u \mid u \in \mathbb{T} \setminus \langle \mathbb{F} \rangle\}$.
- A (generalised) *complementary decomposition* (CD) of the monomial ideal $\mathcal{I}$ is a finite set $\{(t_1, \mathbb{F}_1), \ldots, (t_r, \mathbb{F}_r)\}$ of disjoint generalised cones such that $\mathbb{T} \setminus \mathcal{I} = \cup_{i=1}^{r} (t_i, \mathbb{F}_i)$.

Lemma

Given monomial ideal $\mathcal{I} \lhd \mathcal{P}$ *and* $\{t_1, \ldots, t_r\} \subseteq \mathbb{T} \setminus \mathcal{I}$ *with* $t_r = 1$.
$\rightsquigarrow$ *CD* $\mathbf{C} := \{(t_i, \mathbb{F}_i) \mid 1 \leq i \leq r\}$ *of* $\mathcal{I}$, *where* $\mathbb{F}_i$ *minimally generates*

$$(\mathcal{I} + \langle t_1, \ldots, t_{i-1} \rangle) : t_i.$$

Irreducible SLBs

- Aim: CDs preserving properties of the SLB.
- Intermediate structure between general SLBs and involutive bases:

Definition

The monomial SLB $\mathbf{B} = \{(t_1, \mathbb{F}_1), \dots, (t_s, \mathbb{F}_s)\}$ for $\mathcal{I} = \langle t_1, \dots, t_s \rangle$ is irreducible, if each $\mathbb{F}_i$ consists of pure powers of variables.

Irreducible SLBs

- Aim: CDs preserving properties of the SLB.
- Intermediate structure between general SLBs and involutive bases:

Definition

The monomial SLB $\mathbf{B} = \{(t_1, \mathbb{F}_1), \ldots, (t_s, \mathbb{F}_s)\}$ for $\mathcal{I} = \langle t_1, \ldots, t_s \rangle$ is irreducible, if each $\mathbb{F}_i$ consists of pure powers of variables.

An irreducible SLB can be obtained by splitting a non-irreducible one.

Example

From $\mathbf{B} = \left\{ \begin{array}{lll} (z^4, \emptyset), & (yz^3, \{z\}), & (y^3z^2, \{z\}), \\ (xyz, \{y^2z, z^2\}), & (x^3z, \{y, z^3\}), & (x^3y^3, \{z\}) \end{array} \right\}$,
adding zt_4, eliminate mixed term $y^2z \in \mathbb{F}_4$,

Irreducible SLBs

- Aim: CDs preserving properties of the SLB.
- Intermediate structure between general SLBs and involutive bases:

Definition

The monomial SLB $\mathbf{B} = \{(t_1, \mathbb{F}_1), \ldots, (t_s, \mathbb{F}_s)\}$ for $\mathcal{I} = \langle t_1, \ldots, t_s \rangle$ is irreducible, if each $\mathbb{F}_i$ consists of pure powers of variables.

An irreducible SLB can be obtained by splitting a non-irreducible one.

Example

From $\mathbf{B} = \left\{ \begin{array}{lll} (z^4, \emptyset), & (yz^3, \{z\}), & (y^3z^2, \{z\}), \\ (xyz, \{y^2z, z^2\}), & (x^3z, \{y, z^3\}), & (x^3y^3, \{z\}) \end{array} \right\}$,
adding zt_4, eliminate mixed term $y^2z \in \mathbb{F}_4$, get irreducible SLB
$$\mathbf{B}' = \left\{ \begin{array}{llll} (z^4, \emptyset), & (yz^3, \{z\}), & (y^3z^2, \{z\}), & (xyz^2, \{y^2, z\}), \\ (xyz, \{z\}), & (x^3z, \{y, z^3\}), & (x^3y^3, \{z\}) & \end{array} \right\}.$$

Decompositions from irreducible SLBs

We are interested in irreducible CDs from irreducible monomial SLBs.

Construction

Given SLB $\mathbf{B} = \{(t_1, \mathbb{F}_1), \ldots, (t_s, \mathbb{F}_s)\}$, $B = \{t_1, \ldots, t_r\}$, $\mathcal{I} = \langle B \rangle$.
For $d_j, \ldots, d_n \in \mathbb{Z}_{\geq 0}$, *define Janet classes of* B*:*

$$[d_j, \ldots, d_n] := \{t \in B \mid \deg_k(t) = d_k \text{ for } j \leq k \leq n\}.$$

Let $M_i := \max\{\deg_i(t) \mid t \in B\}$*. For* $c = [d_j, \ldots, d_n]$*, we define the terms:*

$$S(c) = x_{j+1}^{d_{j+1}} \cdots x_n^{d_n} \quad \text{and} \quad U(c) = x_1^{M_1} \cdots x_{j-1}^{M_{j-1}} x_j^{d_j - 1} \cdots x_n^{d_n}.$$

$C := \{S(c) \mid d_j \neq 0 \wedge U(c) \notin \mathcal{I}\}$. $\rightsquigarrow$ *CD* $\mathbf{C} = \{(s, \mathbb{F}(s)) \mid s \in C\}$*, where*

$$\langle \mathbb{F}(s) \rangle = (\mathcal{I} + \langle \hat{s} \in C \mid \hat{s} \succ_{lex} s \rangle) : s.$$

Decompositions from irreducible SLBs

We are interested in irreducible CDs from irreducible monomial SLBs.

Construction

Given SLB $\mathbf{B} = \{(t_1, \mathbb{F}_1), \ldots, (t_s, \mathbb{F}_s)\}$, $B = \{t_1, \ldots, t_r\}$, $\mathcal{I} = \langle B \rangle$.
For $d_j, \ldots, d_n \in \mathbb{Z}_{\geq 0}$, *define Janet classes of* B:

$$[d_j, \ldots, d_n] := \{t \in B \mid \deg_k(t) = d_k \text{ for } j \leq k \leq n\}.$$

Let $M_i := \max\{\deg_i(t) \mid t \in B\}$. *For* $c = [d_j, \ldots, d_n]$, *we define the terms:*

$$S(c) = x_{j+1}^{d_{j+1}} \cdots x_n^{d_n} \quad \text{and} \quad U(c) = x_1^{M_1} \cdots x_{j-1}^{M_{j-1}} x_j^{d_j - 1} \cdots x_n^{d_n}.$$

$C := \{S(c) \mid d_j \neq 0 \wedge U(c) \notin \mathcal{I}\}$. $\rightsquigarrow$ *CD* $\mathbf{C} = \{(s, \mathbb{F}(s)) \mid s \in C\}$, *where*

$$\langle \mathbb{F}(s) \rangle = (\mathcal{I} + \langle \hat{s} \in C \mid \hat{s} \succ_{lex} s \rangle) : s.$$

Caveat

This construction does not in all cases preserve irreducibility.

Example decomposition (1)

Example

An irreducible lexicographically ordered SLB **B** is given by

$$\begin{aligned}
(t_1, \mathbb{F}_1) &= (z^4, \emptyset), & (t_2, \mathbb{F}_2) &= (yz^3, \{z\}), \\
(t_3, \mathbb{F}_3) &= (y^3z^2, \{z\}), & (t_4, \mathbb{F}_4) &= (xyz^2, \{y^2, z\}), \\
(t_5, \mathbb{F}_5) &= (xyz, \{z\}), & (t_6, \mathbb{F}_6) &= (x^3z, \{y, z^3\}), \\
(t_7, \mathbb{F}_7) &= (x^3y^3, \{z\}).
\end{aligned}$$

Example decomposition (1)

Example

An irreducible lexicographically ordered SLB **B** is given by

$$\begin{array}{ll}
(t_1, \mathbb{F}_1) = (z^4, \emptyset), & (t_2, \mathbb{F}_2) = (yz^3, \{z\}), \\
(t_3, \mathbb{F}_3) = (y^3z^2, \{z\}), & (t_4, \mathbb{F}_4) = (xyz^2, \{y^2, z\}), \\
(t_5, \mathbb{F}_5) = (xyz, \{z\}), & (t_6, \mathbb{F}_6) = (x^3z, \{y, z^3\}), \\
(t_7, \mathbb{F}_7) = (x^3y^3, \{z\}). &
\end{array}$$

Let $\mathcal{I} = \langle t_1, \ldots, t_7 \rangle$ and $B = \{t_1, \ldots, t_7\}$. Only five Janet classes ($[1, 1, 2], [1, 1, 1], [3, 0, 1], [3, 3, 0], [3, 0]$) meet the criterion $U(c) \notin \mathcal{I}$.

Example decomposition (1)

Example

An irreducible lexicographically ordered SLB **B** is given by

$$
\begin{aligned}
(t_1, \mathbb{F}_1) &= (z^4, \emptyset), & (t_2, \mathbb{F}_2) &= (yz^3, \{z\}),\\
(t_3, \mathbb{F}_3) &= (y^3z^2, \{z\}), & (t_4, \mathbb{F}_4) &= (xyz^2, \{y^2, z\}),\\
(t_5, \mathbb{F}_5) &= (xyz, \{z\}), & (t_6, \mathbb{F}_6) &= (x^3z, \{y, z^3\}),\\
(t_7, \mathbb{F}_7) &= (x^3y^3, \{z\}).
\end{aligned}
$$

Let $\mathcal{I} = \langle t_1, \ldots, t_7 \rangle$ and $B = \{t_1, \ldots, t_7\}$. Only five Janet classes ($[1,1,2], [1,1,1], [3,0,1], [3,3,0], [3,0]$) meet the criterion $U(c) \notin \mathcal{I}$. Obtain vertex set $C = \{yz^2, yz, z, y^3, 1\}$. Computing the colon ideals, then obtain the irreducible CD with

$$
\begin{aligned}
(s_1, \mathbb{F}(s_1)) &= (yz^2, \{x, y^2, z\}), & (s_2, \mathbb{F}(s_2)) &= (yz, \{x, z\}),\\
(s_3, \mathbb{F}(s_3)) &= (z, \{x^3, y, z^3\}), & (s_4, \mathbb{F}(s_4)) &= (y^3, \{x^3, z\}),\\
(s_5, \mathbb{F}(s_5)) &= (1, \{y^3, z\}).
\end{aligned}
$$

Standard pairs

Definition (Sturmfels et al. 1995)

Let $\mathcal{I} \subseteq \mathcal{P}$ be a monomial ideal.

- Pair $(t, \mathbb{V}(t))$ with $t \in \mathbb{T}$ and $\mathbb{V}(t) \subseteq \{x_1, \ldots, x_n\}$ is *admissible*, if $\deg_x t = 0$ for all $x \in \mathbb{V}(t)$.
- $(t, \mathbb{V}(t)) \leq (u, \mathbb{V}(u)) :\Longleftrightarrow \mathbb{T} \cap (u \cdot \mathcal{K}[\mathbb{V}(u)]) \subseteq \mathbb{T} \cap (t \cdot \mathcal{K}[\mathbb{V}(t)])$.
- $(t, \mathbb{V}(t))$ standard, if it is minimal admissible with $t \cdot \mathcal{K}[\mathbb{V}(t)] \cap \mathcal{I} = \emptyset$.
- Write $\mathcal{S}_{\mathcal{I}}$ for the set of all standard pairs of $\mathcal{I}$.

Standard pairs

Definition (Sturmfels et al. 1995)

Let $\mathcal{I} \subseteq \mathcal{P}$ be a monomial ideal.

- Pair $(t, \mathbb{V}(t))$ with $t \in \mathbb{T}$ and $\mathbb{V}(t) \subseteq \{x_1, \ldots, x_n\}$ is *admissible*, if $\deg_x t = 0$ for all $x \in \mathbb{V}(t)$.
- $(t, \mathbb{V}(t)) \leq (u, \mathbb{V}(u)) :\Longleftrightarrow \mathbb{T} \cap (u \cdot \mathcal{K}[\mathbb{V}(u)]) \subseteq \mathbb{T} \cap (t \cdot \mathcal{K}[\mathbb{V}(t)])$.
- $(t, \mathbb{V}(t))$ standard, if it is minimal admissible with $t \cdot \mathcal{K}[\mathbb{V}(t)] \cap \mathcal{I} = \emptyset$.
- Write $\mathcal{S}_{\mathcal{I}}$ for the set of all standard pairs of $\mathcal{I}$.

Proposition (Sturmfels et al. 1995)

Any monomial ideal $\mathcal{I}$ has an irreducible primary decomposition via $\mathcal{S}_{\mathcal{I}}$:

$$\mathcal{I} = \bigcap_{(t, \mathbb{V}(t)) \in \mathcal{S}_{\mathcal{I}}} \left\langle x^{\deg_x(t)+1} \mid x \notin \mathbb{V}(t) \right\rangle . \tag{1}$$

We give an algorithm computing $\mathcal{S}_{\mathcal{I}}$ from an irreducible CD.

Example decomposition (2)

Recall the irreducible complementary decomposition **C** of $\mathbb{T} \setminus \mathcal{I}$ given by

$$\begin{aligned}
&(s_1, \mathbb{F}(s_1)) = (yz^2, \{x, y^2, z\}), && (s_2, \mathbb{F}(s_2)) = (yz, \{x, z\}),\\
&(s_3, \mathbb{F}(s_3)) = (z, \{x^3, y, z^3\}), && (s_4, \mathbb{F}(s_4)) = (y^3, \{x^3, z\}),\\
&(s_5, \mathbb{F}(s_5)) = (1, \{y^3, z\}).
\end{aligned}$$

Example decomposition (2)

Recall the irreducible complementary decomposition **C** of $\mathbb{T} \setminus \mathcal{I}$ given by

$$\begin{array}{ll} (s_1, \mathbb{F}(s_1)) = (yz^2, \{x, y^2, z\}), & (s_2, \mathbb{F}(s_2)) = (yz, \{x, z\}), \\ (s_3, \mathbb{F}(s_3)) = (z, \{x^3, y, z^3\}), & (s_4, \mathbb{F}(s_4)) = (y^3, \{x^3, z\}), \\ (s_5, \mathbb{F}(s_5)) = (1, \{y^3, z\}). & \end{array}$$

Our algorithm computes admissible pairs as follows:

- for $(s_1, \mathbb{F}(s_1))$ the two pairs $(yz^2, \emptyset)$ and $(y^2z^2, \emptyset)$,
- for $(s_2, \mathbb{F}(s_2))$ the pair $(z, \{y\})$,
- for $(s_3, \mathbb{F}(s_3))$ the nine pairs $(x^\ell z^{m+1}, \emptyset)$, where $1 \leq \ell, m \leq 2$,
- for $(s_4, \mathbb{F}(s_4))$ the three pairs $(1, \{y\})$, $(x, \{y\})$, and $(x^2, \{y\})$,
- for $(s_5, \mathbb{F}(s_5))$ the three pairs $(1, \{x\})$, $(y, \{x\})$, and $(y^2, \{x\})$.

Of the 18 admissible pairs, only $(z, \emptyset)$ is non-standard and removed.

Example decomposition (2)

Recall the irreducible complementary decomposition **C** of $\mathbb{T} \setminus \mathcal{I}$ given by

$$\begin{array}{ll} (s_1, \mathbb{F}(s_1)) = (yz^2, \{x, y^2, z\}), & (s_2, \mathbb{F}(s_2)) = (yz, \{x, z\}), \\ (s_3, \mathbb{F}(s_3)) = (z, \{x^3, y, z^3\}), & (s_4, \mathbb{F}(s_4)) = (y^3, \{x^3, z\}), \\ (s_5, \mathbb{F}(s_5)) = (1, \{y^3, z\}). & \end{array}$$

Our algorithm computes admissible pairs as follows:

- for $(s_1, \mathbb{F}(s_1))$ the two pairs $(yz^2, \emptyset)$ and $(y^2z^2, \emptyset)$,
- for $(s_2, \mathbb{F}(s_2))$ the pair $(z, \{y\})$,
- for $(s_3, \mathbb{F}(s_3))$ the nine pairs $(x^\ell z^{m+1}, \emptyset)$, where $1 \leq \ell, m \leq 2$,
- for $(s_4, \mathbb{F}(s_4))$ the three pairs $(1, \{y\})$, $(x, \{y\})$, and $(x^2, \{y\})$,
- for $(s_5, \mathbb{F}(s_5))$ the three pairs $(1, \{x\})$, $(y, \{x\})$, and $(y^2, \{x\})$.

Of the 18 admissible pairs, only $(z, \emptyset)$ is non-standard and removed. The five maximal pairs $(y^2z^2, \emptyset)$, $(z, \{y\})$, $(x^2z^3, \emptyset)$, $(x^2, \{y\})$, and $(y^2, \{x\})$ induce the irredundant irreducible decomposition

$$\mathcal{I} = \langle x, y^3, z^3 \rangle \cap \langle x, z^2 \rangle \cap \langle x^3, y, z^4 \rangle \cap \langle x^3, z \rangle \cap \langle y^3, z \rangle .$$

Hilbert and volume functions

Given: *Homogeneous* SLB $\{(f_1, \mathbb{F}_1), \ldots, (f_s, \mathbb{F}_s)\}$ of ideal $\mathcal{I}$.
The *volume* and *Hilbert function*, respectively, of $\mathcal{I}$ are the numerical functions $\mathbb{N}_0 \to \mathbb{N}_0$ defined by

$$V_{\mathcal{I}}(q) = \dim_{\mathcal{K}} \mathcal{I}_q\,, \qquad H_{\mathcal{I}}(q) = \dim_{\mathcal{K}} (\mathcal{P}_q/\mathcal{I}_q)\,, \tag{2}$$

where $\mathcal{I}_q$ and $\mathcal{P}_q$ denote homogeneous components of degree q.

Hilbert and volume functions

Given: *Homogeneous* SLB $\{(f_1,\mathbb{F}_1),\dots,(f_s,\mathbb{F}_s)\}$ of ideal $\mathcal{I}$.
The *volume* and *Hilbert function*, respectively, of $\mathcal{I}$ are the numerical functions $\mathbb{N}_0 \to \mathbb{N}_0$ defined by

$$V_{\mathcal{I}}(q) = \dim_{\mathcal{K}} \mathcal{I}_q\,, \qquad H_{\mathcal{I}}(q) = \dim_{\mathcal{K}} (\mathcal{P}_q/\mathcal{I}_q)\,, \tag{2}$$

where $\mathcal{I}_q$ and $\mathcal{P}_q$ denote homogeneous components of degree q.
Since $V_{\mathcal{I}}(q) + H_{\mathcal{I}}(q) = \dim_{\mathcal{K}} \mathcal{P}_q = \binom{n+q-1}{q}$, it suffices to know $V_{\mathcal{I}}$.

Proposition

Let $\{(f_1,\mathbb{F}_1),\dots,(f_s,\mathbb{F}_s)\}$ be a homogeneous SLB of $\mathcal{I}$. Then

$$V_{\mathcal{I}}(q) = \sum_{i=1}^{s} [q \geq \deg f_i] H_{\langle \mathbb{F}_i \rangle}(q - \deg f_i)\,. \tag{3}$$

Here the Iverson bracket $[A]$ equals 1, if A is true, and 0 otherwise.

Thank you for your attention!