The skeletons you find when you order your ideal's closet

John Perry

University of Southern Mississippi

ACA 2014

Overview

Ordering your ideal's closet

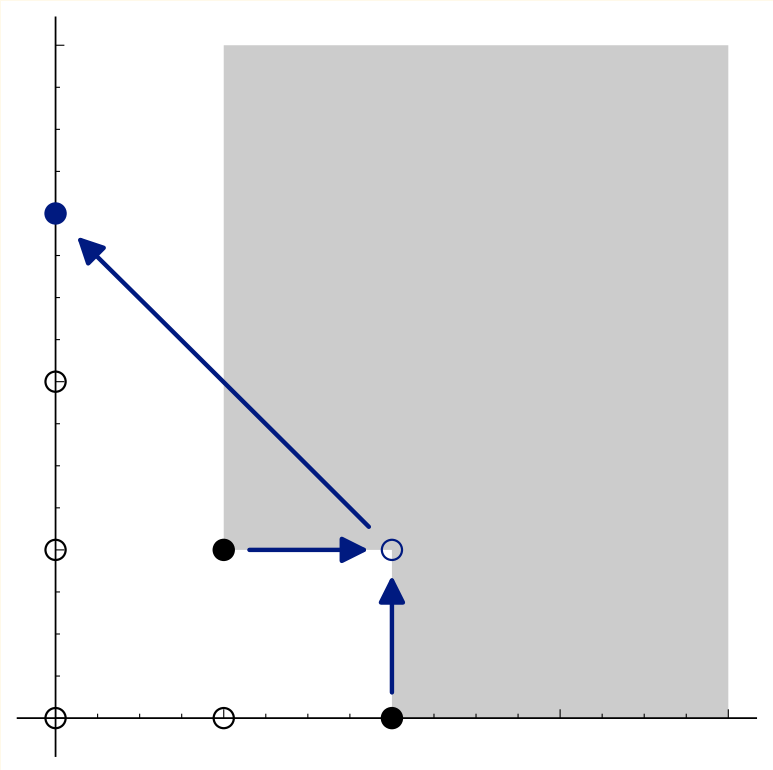
Sorting the closet

Skeletons in the closet

Conclusion

§1. Ordering your ideal's closet

New elements come from ideal's "closet"

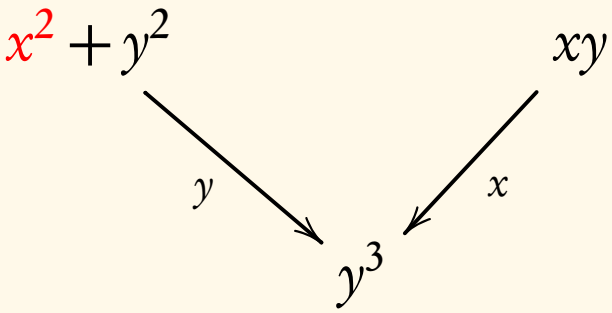


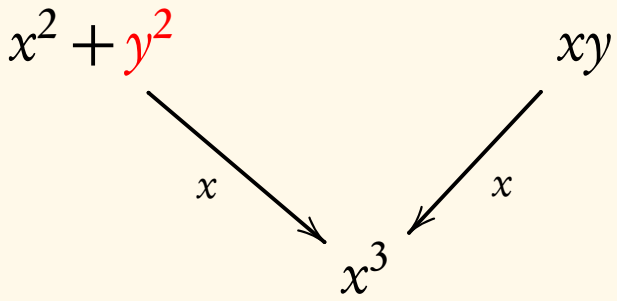
(Ideal of leading terms)

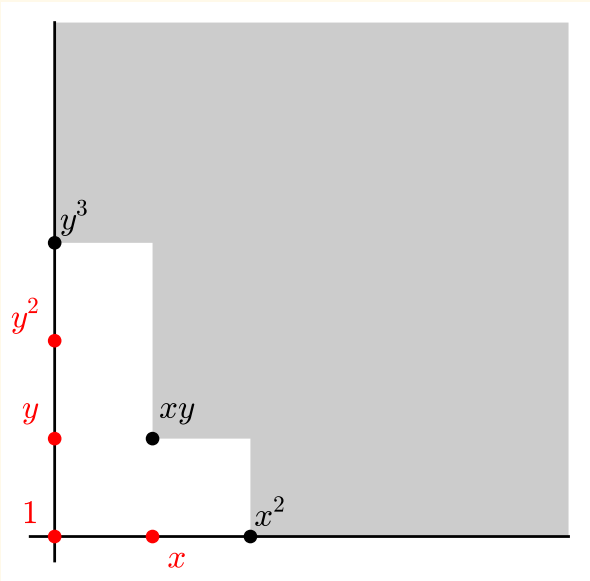
Usefulness

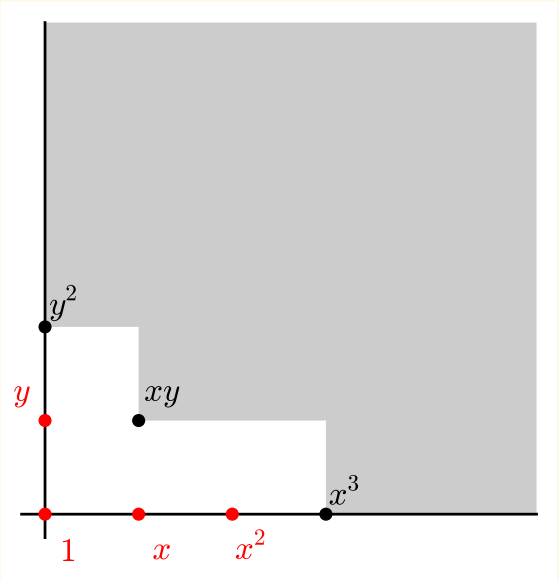
- algebraic geometry
- analysis of codes
- astrophysics
- commutative algebra
- computing discrete logarithms
- cryptanalysis
- learning with errors
- …

Different orders









Some orderings "better"

Cyclic-5

$$\left\{ \begin{array}{c} x_1 + x_2 + \cdots + x_5, \\ x_1x_2 + x_2x_3 + \cdots + x_5x_1, \\ x_1x_2x_3 + x_2x_3x_4 + \cdots + x_5x_1x_2, \\ x_1x_2x_3x_4 + x_2x_3x_4x_5 + \cdots + x_5x_1x_2x_3, \\ x_1x_2x_3x_4x_5 - 1 \end{array} \right\}$$

lex order: 11
grevlex order: 20

Another example

Cyclic-7 homogeneous

$$\left\{ \begin{array}{c} x_1 + x_2 + \cdots + x_7, \\ x_1x_2 + x_2x_3 + \cdots + x_1x_1, \\ x_1x_2x_3 + x_2x_3x_4 + \cdots + x_7x_1x_2, \\ \vdots \\ x_1x_2x_3x_4x_5x_6x_7 - h^7 \end{array} \right\}$$

lex order: 985
grevlex order: 443

Another example

Cyclic-7 homogeneous

$$\left\{ \begin{array}{c} x_1 + x_2 + \cdots + x_7, \\ x_1x_2 + x_2x_3 + \cdots + x_1x_1, \\ x_1x_2x_3 + x_2x_3x_4 + \cdots + x_7x_1x_2, \\ \vdots \\ x_1x_2x_3x_4x_5x_6x_7 - h^7 \end{array} \right\}$$

lex order: 985
grevlex order: 443
mystery order: 118

Question

Find ~~*best*~~ "good" ordering *while* sorting?

Find ~~*best*~~ "good" ordering *while* sorting?

Dynamic Gröbner basis computation

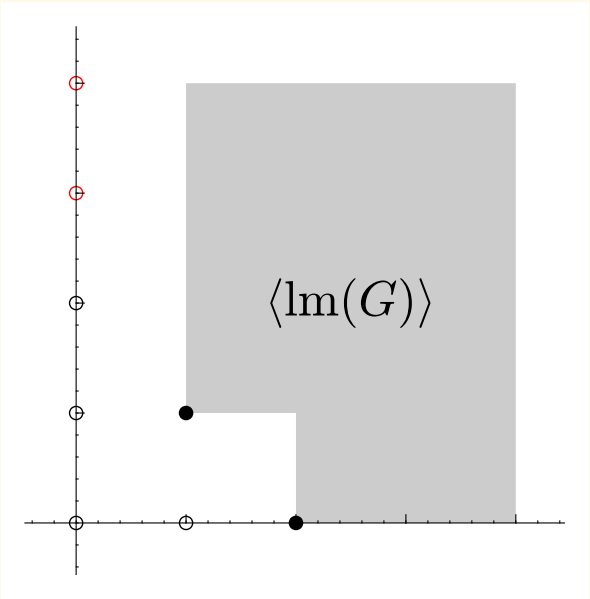
("sorting ideal's closet")
(reorder Macaulay matrix during reduction)

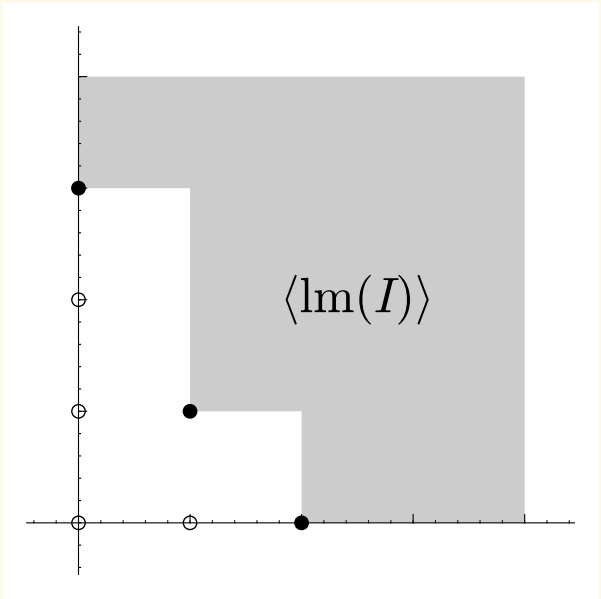
Find ~~*best*~~ "good" ordering *while* sorting?

Dynamic Gröbner basis computation

("sorting ideal's closet")
(reorder Macaulay matrix during reduction)

"Tentative" Hilbert function selects ordering





Usefulness

- smaller basis $\Longrightarrow$ easier to work with
- less computation $\Longrightarrow$ quicker result
- applied mathematicians $\Longrightarrow$ much happier

“Short” example

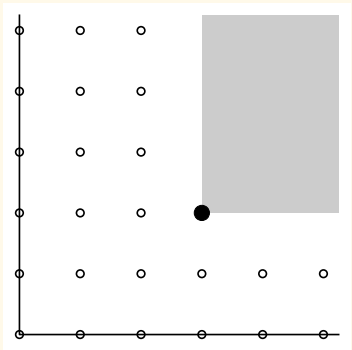
$$F = \left\{ \begin{array}{c} x^3y^2 + 5776x^2y^3 + 1230x^4 + 4073x^2y^2 - 1332xy^3, \\ \\ x^4y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725 \end{array} \right\}$$

"Short" example

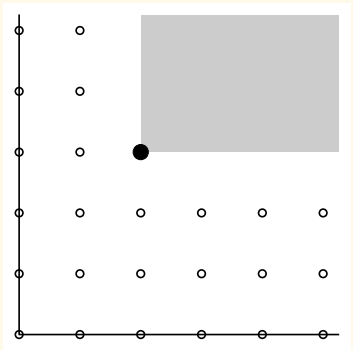
$$F = \left\{ \begin{array}{c} x^3y^2 + 5776x^2y^3 + 1230x^4 + 4073x^2y^2 - 1332xy^3, \\ \\ x^4y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725 \end{array} \right\}$$

for f_1,

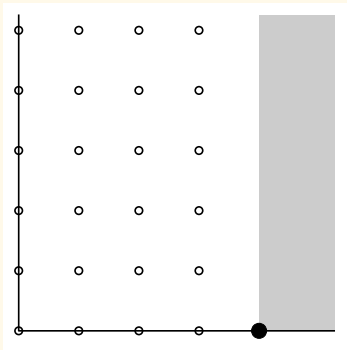
- only x^3y^2, x^2y^3, x^4 possible
- x^4 more attractive...



1,2,3,4,5,...



1,2,3,4,5,...



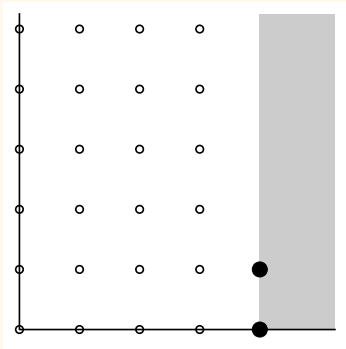
1,2,3,4,4,...

"Short" example

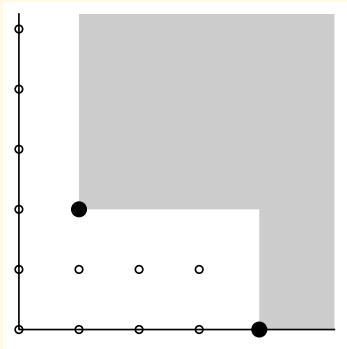
$$F = \left\{ \begin{array}{c} x^3y^2 + 5776x^2y^3 + 1230x^4 + 4073x^2y^2 - 1332xy^3, \\ \\ x^4y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725 \end{array} \right\}$$

for f_2,

- only x^4y, xy^2 possible
- xy^2 more attractive...



1,2,3,4,4,...



1,2,3,3,2,1,1,...

...but *incompatible* w/choice of x^4

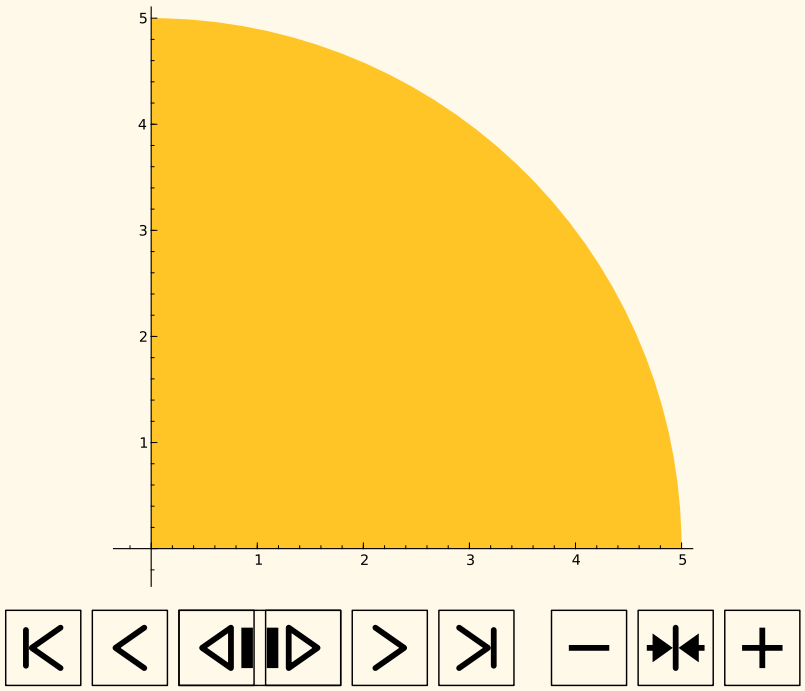
§2. Sorting the closet

Previous work

- Mora and Robbiano (1988)
  . . . pose question
- Gritzmann and Sturmfels (1993)
  . . . describe *general* algorithm w/convex geometry
- Caboara (1993)
  . . . describes, implements *refining* algorithm w/simplex
- Oleg Golubitsky (preprint)
  . . . describes, implements (?) *general* algorithm

. . . nothing else!

Refining v. general



	Refining	**General**
ordering	partial	partial or total
new polys	refine ordering	re-evaluate
leading mons	preserved	can change

Refinement: pros, cons

Cons

- sometimes forego best orderings

Pros

- no need to re-evaluate previous polynomials
- no need to re-evaluate *S*-polynomials
- can still predict zero reductions
- warm-start simplex algorithm, not cold-start

Algebra of orderings

ordering

$\downarrow$

vector (ω)

Algebra of orderings

ordering

$\downarrow$

vector (ω)

$$x^2 > y^2 \qquad \Longleftrightarrow \qquad \omega \cdot (2,0) > \omega \cdot (0,2)$$

Algebra of orderings

ordering

$\downarrow$

vector (ω)

$$x^2 > y^2 \qquad \Longleftrightarrow \qquad \omega \cdot (2,0) > \omega \cdot (0,2)$$

$$\omega = (1,0) \quad x^3 + x^2y^2 + y^3$$

$$\omega = (1,1) \quad x^3 + x^2y^2 + y^3$$

$$\omega = (0,1) \quad x^3 + x^2y^2 + y^3$$

Clutter in the closet

$$x^5 + x^4y^2 + wz^3 + w^3z + wx^4 + w^2yz^2 + x^2$$

new leading polynomial	$\longrightarrow$	new constraints
many/large polynomials	$\longrightarrow$	many constraints
more constraints	$\longrightarrow$	more computation
more computation	$\longrightarrow$	unhappy applied mathematicians

Clutter in the closet

$$x^5 + x^4y^2 + wz^3 + w^3z + wx^4 + w^2yz^2 + x^2$$

new leading polynomial	$\longrightarrow$	new constraints
many/large polynomials	$\longrightarrow$	many constraints
more constraints	$\longrightarrow$	more computation
more computation	$\longrightarrow$	unhappy applied mathematicians

Big-time question

How can we reduce the number of constraints?

Many closet elements “strung together”

Some elements drag others along

$$x^5 \text{———} x^2$$

Divisibility criterion

$t \mid u$? no need to consider t.

(Caboara, 1993)

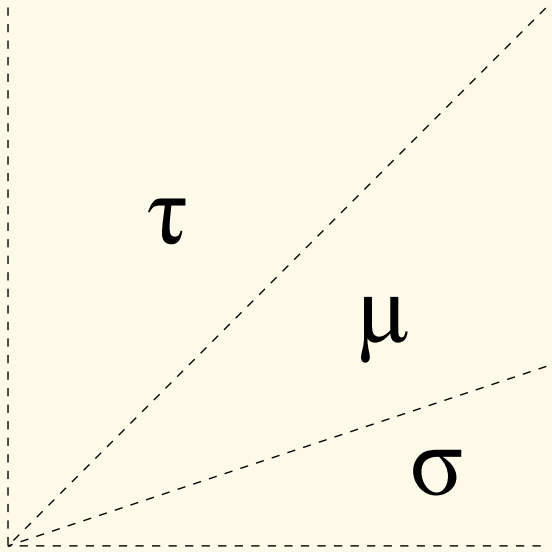
Limited usefulness

- homogeneous polynomials
- not-so-homogeneous polynomials

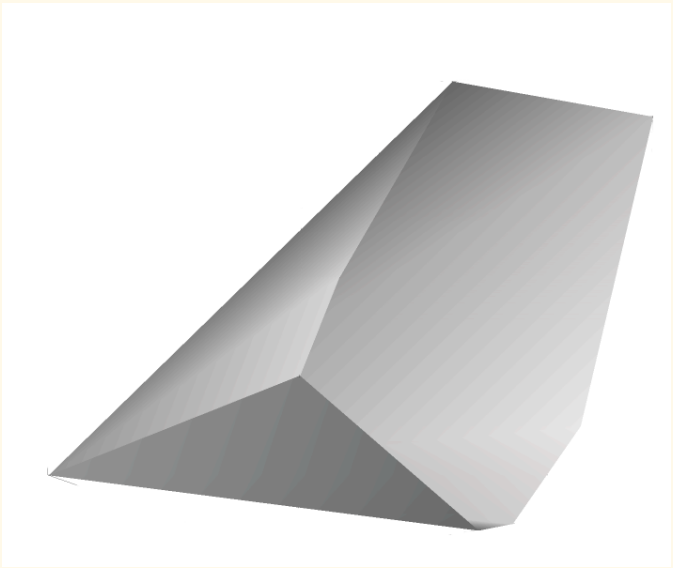
§3. Skeletons in the closet

Geometric view

linear inequalities $\longrightarrow$ polyhedral cone



2d



3d

Definition

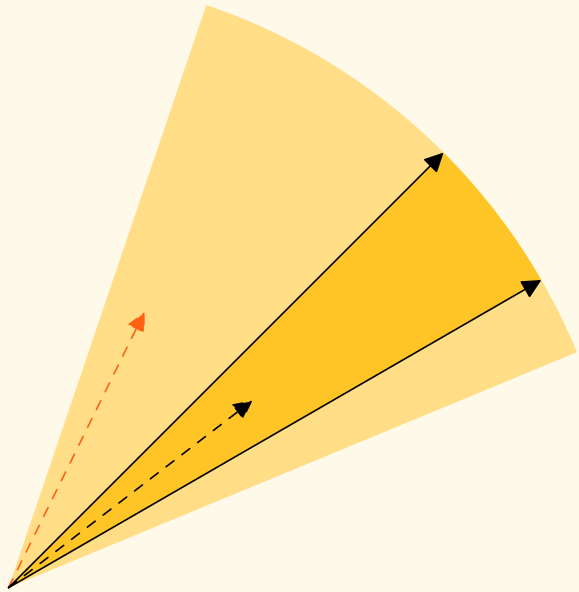
Skeleton: extreme vectors & adjacency relationship

Usefulness

Fact

Skeleton identifies minimal set of closet elements

("Easily" proved from Corner Point Theorem)



Example

$$F = \left\{ \begin{array}{c} x^3y^2 + 5776x^2y^3 + 1230x^4 + 4073x^2y^2 - 1332xy^3, \\ \\ x^4y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725 \end{array} \right\}$$

Select $x^4 = \mathrm{lm}(f_1)$

Example

$$F = \left\{ \begin{array}{c} x^3y^2 + 5776x^2y^3 + 1230x^4 + 4073x^2y^2 - 1332xy^3, \\ \\ x^4y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725 \end{array} \right\}$$

Select $x^4 = \mathrm{lm}(f_1)$

- Skeleton: $\{(1,0),(2,1)\}$
  - let $\sigma = (1,0)+(2,1) = (3,1)$

Example

$$F = \left\{ \begin{array}{c} x^3y^2 + 5776x^2y^3 + 1230x^4 + 4073x^2y^2 - 1332xy^3, \\ \\ x^4y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725 \end{array} \right\}$$

Select $x^4 = \mathrm{lm}(f_1)$

- Skeleton: $\{(1,0),(2,1)\}$
  - let $\sigma = (1,0) + (2,1) = (3,1)$
- $f_2 \xrightarrow[f_1]{} 2784x^3y^3 + 14878x^2y^4 + 10170x^2y^3 - 13675xy^4$
  $+ 3199x^3 + 11994xy^2 - 899y^2 - 10725$

Example

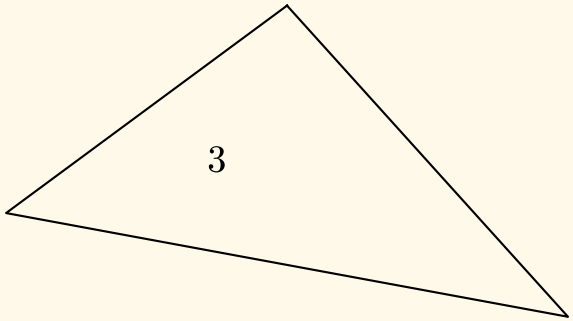
$$F = \left\{ \begin{array}{c} x^3y^2 + 5776x^2y^3 + 1230x^4 + 4073x^2y^2 - 1332xy^3, \\ \\ x^4y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725 \end{array} \right\}$$

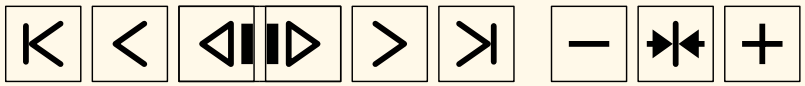
Select $x^4 = \mathrm{lm}(f_1)$

- Skeleton: $\{(1,0),(2,1)\}$
  - let $\sigma = (1,0) + (2,1) = (3,1)$
- $f_2 \xrightarrow[f_1]{} 2784x^3y^3 + 14878x^2y^4 + 10170x^2y^3 - 13675xy^4 + 3199x^3 + 11994xy^2 - 899y^2 - 10725$
- $\mathrm{lm}_\sigma(f_2) = x^3y^3$
  - $t \not> _\tau \mathrm{lm}_\sigma(f_2)$ for $t \in f_2$, $\tau \in \{(1,0),(2,1)\}$

  $\therefore$ no other possible lms

Should we use the *entire* skeleton?

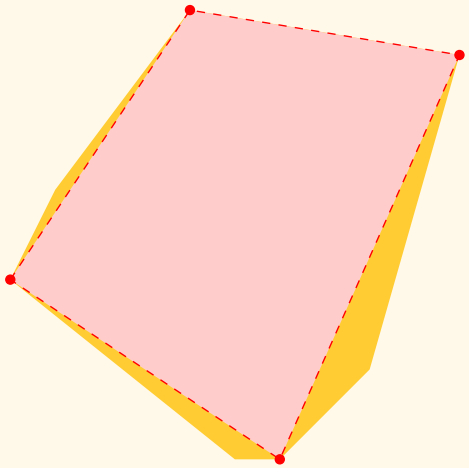




- Explosion in # of vectors?
- "Hard" to compute? (rel. simplex)

“Approximate” skeleton?

compute only max, min ω_i



disallow some needed, allow only needed

- $O(n)$ space
- $O(n)$ “easy” calls to simplex: change objective function

Practical results

	#constraints		size of basis (pols × mons)	
	div only	app skel	dyn	grevlex
Caboara 1	29	20	35 × 137	239 × 478
Caboara 2	17	26	21 × 42	553 × 1106
Cyclic-5	61	31	11 × 68	20 × 85
Cyclic-6	250	56	20 × 129	45 × 199
Cyclic-7	>1000	63	63 × 1049	209 × 1134
Cyclic-5 hom	60	33	11 × 98	38 × 197
Cyclic-6 hom	303	39	33 × 476	99 × 580
Cyclic-7 hom	>1000	105	222 × 5181	443 × 3395

- Able to compute dyn GB we could not do before!
- Reduction consumes most time (usually)
- Katsura-n: similar size basis as static, fewer constraints

(Caboara & Perry, 2014)

You knew there was a penalty somewhere

CAS's require *integer* orderings

- simplex *fast* when *inexact*
- *integer* solutions ***slower than molasses in winter***
    - narrow cone? large integer entries

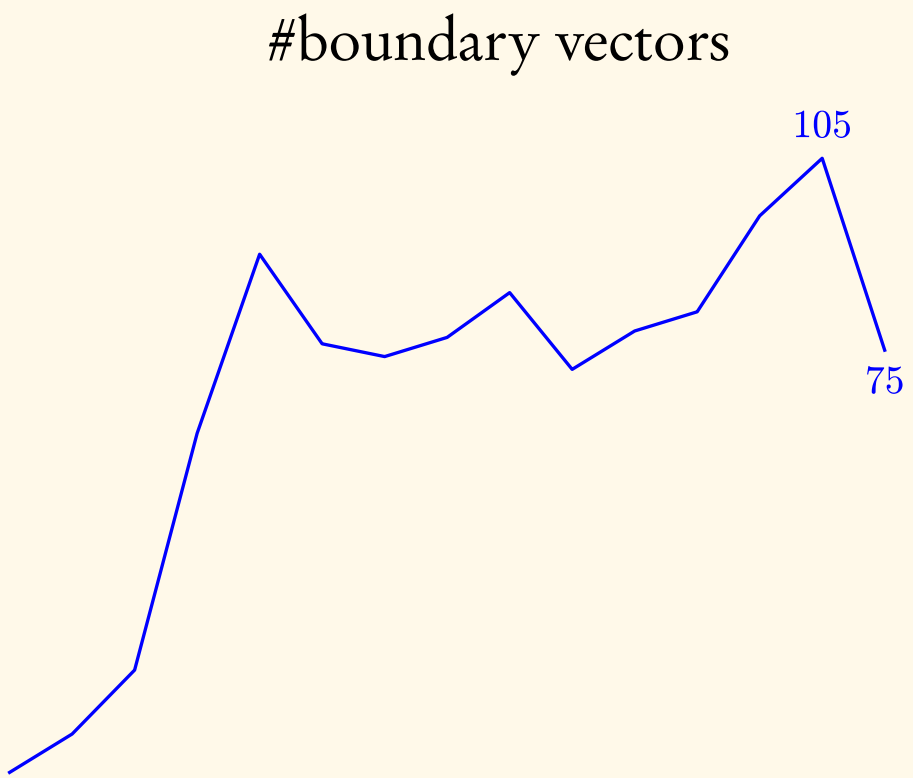
(CAS also don't like *large* integer products)

Life is short. Why not?

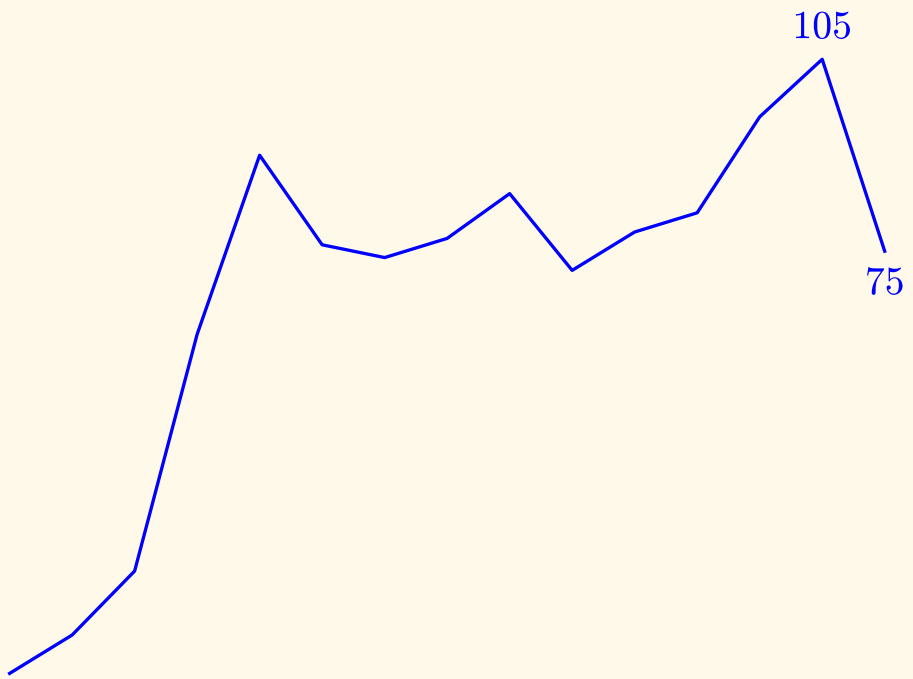
Double description method

- Exact
- Iterative: well-suited for refinement!
  - add constraints as needed
  - detects, discards redundant constraints
- Well-studied
  - Motzkin et al., 1953
  - Fukuda and Prodon, 1996
  - Zolotych, 2012

Evolution of skeleton (1)



Evolution of skeleton (1)

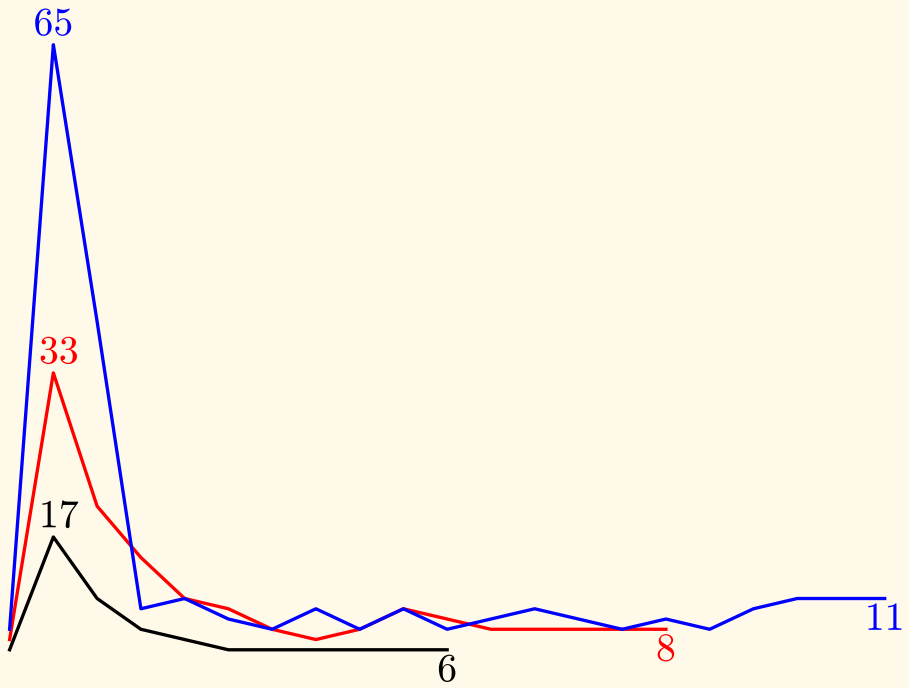


bad news:

- finding leading monomials $\gg$ reduction
- larger GB than using approximate skeleton
  - greedy algorithm does not pay here
  - still smaller than static (grevlex)
- similar for Caboara 2

Evolution of skeleton (2)

#boundary vectors



Cyclic-5 Cyclic-6 Cyclic-7

(all homogeneous)

Yes, entire skeleton!

Cylic-7 homogeneous

	grevlex	app skel	ent skel
#polys	443	222	126*
#mons	3395	5181	4312
#vectors	N/A	4	11
#constraints	N/A	105	74

*118 non-redundant

Using entire skeleton:

- *much* smaller basis
- costliest stage? reduction!
  - *not* selecting ordering!
  - *no integer programming*
- not many boundary vectors!

§4. Conclusion

The perfect is the enemy of the good

- We obtain *good* orderings from dynamic algorithm
  - not necessarily *best* ordering
  - what makes "best"? shortest? fastest?
- Approximate v. exact skeleton

Challenges

Data structures

- Integer orderings grow large
- CAS require integer orderings
- Implemented as "marked" polynomials

Reduction

- not all CAS use Sugar

Choosing good heuristic

Future

- Efficient implementation
  - Hilbert polynomial & series
  - Double description method
  - Compiled (*not Cython*, or *better Cython*)
- Better (?) criteria to select ordering
- Combine w/modern techniques

Thank you!

Massimo Caboara

Anonymous referee

Николай Юрьевич Золотых

University of Southern Mississippi

Галина Валеревна Заморий

Further reading

- Mora and Robbiano, "The Gröbner fan of an ideal." *JSC* 6 (1988) 183–208.
- Grtizmann and Sturmfels, "Minkowski Addition of Polytopes: Computational Complexity and Applications to Gröbner Bases." *SIAM J. Disc. Math* 6 (1993) 246–269.
- Caboara, "A Dynamic Algorithm for Gröbner basis computation." *ISSAC '93*, ACM Press, 275–283.
- O. Golubitsky, "Converging term order sequences and the dynamic Buchberger algorithm." In preparation, preprint received via private communication.
- Caboara and Perry, "Reducing the size and number of linear programs in a dynamic Gröbner basis algorithm." *AAECC* 25 (2014) 99–117.