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

John Perry

University of Southern Mississippi

ACA 2014
The skeletons you find when you order your ideal's closet

John Perry

Overview

1. Ordering your ideal’s closet
2. Sorting the closet
3. Skeletons in the closet
4. Conclusion
§1. Ordering your ideal’s closet
Buchberger’s algorithm

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

Ordering your ideal's closet

Sorting the closet

Skeletons in the closet

Conclusion

Different orders

\[ x^2 + y^2 \]

\[ xy \]

\[ y^3 \]

\[ x \]

\[ y \]

\[ 1 \]

\[ x \]

\[ y \]

\[ x^3 \]

\[ y^3 \]

\[ x^2 \]

\[ y^2 \]

\[ y \]

\[ x \]

\[ xy \]

\[ x^3 \]
Some orderings “better”

Cyclic-5

\[
\begin{cases}
    x_1 + x_2 + \cdots + x_5, \\
    x_1x_2 + x_2x_3 + \cdots + x_5x_1, \\
    x_1x_2x_3 + x_2x_3x_4 + \cdots + x_5x_1x_2, \\
    x_1x_2x_3x_4 + x_2x_3x_4x_5 + \cdots + x_5x_1x_2x_3, \\
    x_1x_2x_3x_4x_5 - 1
\end{cases}
\]

lex order: 11
grevlex order: 20
The skeletons you find when you order your ideal's closet

John Perry

Ordering your ideal's closet

Sorting the closet

Skeletons in the closet

Conclusion

Another example

Cyclic-7 homogeneous

\[
\begin{align*}
    x_1 + x_2 + \cdots + x_7, \\
    x_1x_2 + x_2x_3 + \cdots + x_1x_1, \\
    x_1x_2x_3 + x_2x_3x_4 + \cdots + x_7x_1x_2, \\
    \vdots \\
    x_1x_2x_3x_4x_5x_6x_7 - h^7
\end{align*}
\]

lex order: 985
grevlex order: 443
The skeletons you find when you order your ideal’s closet

John Perry

Ordering your ideal’s closet

Sorting the closet

Skeletons in the closet

Conclusion

Another example

Cyclic-7 homogeneous

\[
\left\{
\begin{array}{l}
x_1 + x_2 + \cdots + x_7, \\
x_1x_2 + x_2x_3 + \cdots + x_1x_1, \\
x_1x_2x_3 + x_2x_3x_4 + \cdots + x_7x_1x_2, \\
\vdots \\
x_1x_2x_3x_4x_5x_6x_7 - b^7
\end{array}
\right.
\]

lex order: 985
grevlex order: 443
mystery order: 118
The skeletons you find when you order your ideal's closet

John Perry

Ordering your ideal’s closet

Sorting the closet

Skeletons in the closet

Conclusion

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 $\Rightarrow$ easier to work with

• less computation $\Rightarrow$ quicker result

• applied mathematicians $\Rightarrow$ much happier
"Short" example

\[ F = \begin{cases}
  x^3 y^2 + 5776x^2 y^3 + 1230x^4 + 4073x^2 y^2 - 1332xy^3, \\
  x^4 y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725
\end{cases} \]
“Short” example

\[ F = \begin{cases} 
  x^3 y^2 + 5776x^2 y^3 + 1230x^4 + 4073x^2 y^2 - 1332xy^3, \\
  x^4 y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725 
\end{cases} \]

for \( f_1 \),

- only \( x^3 y^2, x^2 y^3, x^4 \) possible
- \( x^4 \) more attractive…

1, 2, 3, 4, 5, …  
1, 2, 3, 4, 5, …  
1, 2, 3, 4, 4, …
“Short” example

\[
F = \begin{cases} 
  x^3y^2 + 5776x^2y^3 + 1230x^4 + 4073x^2y^2 - 1332xy^3, \\
  x^4y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725
\end{cases}
\]

for \( f_2 \),

- only \( x^4y \), \( xy^2 \) possible
- \( xy^2 \) more attractive…

…but incompatible w/ choice of \( x^4 \)
§2. Sorting the closet
The skeletons you find when you order your ideal's closet

John Perry

Ordering your ideal’s closet

Sorting the closet

Skeletons in the closet

Conclusion

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

John Perry

Ordering your ideal's closet

Sorting the closet

Skeletons in the closet

Conclusion

Refining v. general

<table>
<thead>
<tr>
<th>Ordering</th>
<th>Refining</th>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>new polys</td>
<td>partial</td>
<td>partial or total</td>
</tr>
<tr>
<td>leading mons</td>
<td>refine ordering</td>
<td>re-evaluate</td>
</tr>
<tr>
<td>preserved</td>
<td></td>
<td>can change</td>
</tr>
</tbody>
</table>
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
The skeletons you find when you order your ideal's closet

Ordering your ideal's closet

Sorting the closet

Skeletons in the closet

Conclusion

Algebra of orderings

ordering

\[ \downarrow \]

vector \((\omega)\)
Algebra of orderings

ordering

↓

vector (ω)

\[ x^2 > y^2 \iff \omega \cdot (2,0) > \omega \cdot (0,2) \]
Algebra of orderings

ordering

\[ \downarrow \]

vector \((\omega)\)

\[ x^2 > y^2 \iff \omega \cdot (2, 0) > \omega \cdot (0, 2) \]

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

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

\[ \omega = (0, 1) \quad x^3 + x^2y^2 + y^3 \]
Clutter in the closet

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

John Perry

Ordering your ideal’s closet

Sorting the closet

Skeletons in the closet

Conclusion

\[x^5 + x^4 y^2 + wz^3 + w^3 z + wx^4 + w^2 yz^2 + x^2\]

new leading polynomial \(\rightarrow\) new constraints

many/large polynomials \(\rightarrow\) many constraints

more constraints \(\rightarrow\) more computation

more computation \(\rightarrow\) unhappy applied mathematicians
Clutter in the closet

\[ x^5 + x^4 y^2 + wz^3 + w^3 z + wx^4 + w^2 yz^2 + x^2 \]

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

John Perry

Ordering your ideal’s closet

Sorting the closet

Skeletons in the closet

Conclusion

Many closet elements “strung together”

Some elements drag others along

\[ x^5 \quad \text{-----} \quad x^2 \]

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

Ordering your ideal’s closet

Sorting the closet

Skeletons in the closet

Conclusion

Geometric view

linear inequalities → polyhedral cone

\[ \tau \]

\[ \mu \]

\[ \sigma \]

2d

3d

Definition

**Skeleton**: extreme vectors & adjacency relationship
Fact

*Skeleton identifies minimal set of closet elements*

(“Easily” proved from Corner Point Theorem)
The skeletons you find when you order your ideal’s closet

Ordering your ideal’s closet

Sorting the closet

Skeletons in the closet

Conclusion

Example

\[ F = \begin{cases} 
  x^3 y^2 + 5776x^2 y^3 + 1230x^4 + 4073x^2 y^2 - 1332xy^3, \\
  x^4 y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725
\end{cases} \]

Select \( x^4 = \text{lm} \left( f_1 \right) \)
The skeletons you find when you order your ideal's closet

John Perry

Ordering your ideal’s closet

Sorting the closet

Skeletons in the closet

Conclusion

Example

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

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

- Skeleton: $\{(1, 0), (2, 1)\}$
  - let $\sigma = (1, 0) + (2, 1) = (3, 1)$
The skeletons you find when you order your ideal’s closet

John Perry

Ordering your ideal’s closet

Sorting the closet

Skeletons in the closet

Conclusion

Example

\[ F = \begin{cases} 
  x^3y^2 + 5776x^2y^3 + 1230x^4 + 4073x^2y^2 - 1332xy^3, \\
  x^4y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725 
\end{cases} \]

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

- 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 \)
The skeletons you find when you order your ideal's closet

John Perry

Ordering your ideal's closet

Sorting the closet

Skeletons in the closet

Conclusion

Example

\[
F = \begin{cases} 
  x^3y^2 + 5776x^2y^3 + 1230x^4 + 4073x^2y^2 - 1332xy^3, \\
  x^4y + 3199x^3 + 11994xy^2 - 8996y^2 - 10725 
\end{cases}
\]

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

- **Skeleton:** \( \{(1,0),(2,1)\} \)
  - let \( \sigma = (1,0) + (2,1) = (3,1) \)
  - \( f_2 \mapsto 2784x^3y^3 + 14878x^2y^4 + 10170x^2y^3 - 13675xy^4 \)
    + \( 3199x^3 + 11994xy^2 - 8996y^2 - 10725 \)
  - \( \text{lm}_\sigma (f_2) = x^3y^3 \)
    - \( t \not\succ_{\tau} \text{lm}_\sigma (f_2) \) 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 $\omega_i$

Disallow some needed, allow only needed

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

<table>
<thead>
<tr>
<th></th>
<th>#constraints</th>
<th>size of basis (polys × mons)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>div only</td>
<td>app skel</td>
</tr>
<tr>
<td>Caboara 1</td>
<td>29</td>
<td>20</td>
</tr>
<tr>
<td>Caboara 2</td>
<td>17</td>
<td>26</td>
</tr>
<tr>
<td>Cyclic-5</td>
<td>61</td>
<td>31</td>
</tr>
<tr>
<td>Cyclic-6</td>
<td>250</td>
<td>56</td>
</tr>
<tr>
<td>Cyclic-7</td>
<td>&gt;1000</td>
<td>63</td>
</tr>
<tr>
<td>Cyclic-5 hom</td>
<td>60</td>
<td>33</td>
</tr>
<tr>
<td>Cyclic-6 hom</td>
<td>303</td>
<td>39</td>
</tr>
<tr>
<td>Cyclic-7 hom</td>
<td>&gt;1000</td>
<td>105</td>
</tr>
</tbody>
</table>

- 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)
Use *entire* skeleton?

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)

#boundary vectors

- Evolution of skeleton
- Finding leading monomials
- Larger GB than using approximate skeleton
- Greedy algorithm does not pay here
- Still smaller than static (grevlex)
- Similar for Caboara 2
Evolution of skeleton (1)

坏消息:
- 找到主导元法 $\gg$ 减法
- 集合比使用近似骨架更大
- 贪婪算法不在此处支付
- 还比静态 (grevlex) 小
- 相似于 Caboara 2
Evolution of skeleton (2)

#boundary vectors

Cyclic-5  Cyclic-6  Cyclic-7
(all homogeneous)
The skeletons you find when you order your ideal's closet

Ordering your ideal's closet

Sorting the closet

Skeletons in the closet

Conclusion

Yes, entire skeleton!

Cylic-7 homogeneous

<table>
<thead>
<tr>
<th></th>
<th>grevlex</th>
<th>app skel</th>
<th>ent skel</th>
</tr>
</thead>
<tbody>
<tr>
<td>#polys</td>
<td>443</td>
<td>222</td>
<td>126*</td>
</tr>
<tr>
<td>#mons</td>
<td>3395</td>
<td>5181</td>
<td>4312</td>
</tr>
<tr>
<td>#vectors</td>
<td>N/A</td>
<td>4</td>
<td>11</td>
</tr>
<tr>
<td>#constraints</td>
<td>N/A</td>
<td>105</td>
<td>74</td>
</tr>
</tbody>
</table>

Using entire skeleton:

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

*118 non-redundant
§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
The skeletons you find when you order your ideal’s closet

John Perry

Ordering your ideal’s closet

Sorting the closet

Skeletons in the closet

Conclusion

Future

- Efficient implementation
  - Hilbert polynomial & series
  - Double description method
  - Compiled (*not Cython, or better Cython*)
- Better (?) criteria to select ordering
- Combine w/modern techniques
The skeletons you find when you order your ideal's closet

John Perry

Ordering your ideal’s closet

Sorting the closet

Skeletons in the closet

Conclusion

Thank you!

Massimo Caboara

Anonymous referee

Николай Юрьевич Золотых

University of Southern Mississippi

Галина Валеревна Заморий
Further reading


