Slimgb

Gröbner bases with slim polynomials
The Aim

avoid intermediate expression swell

Classical Buchberger algorithm with parallel reductions guided by new weighted length functions

• Often: big computations -> small results
• experiments show: blow up often avoidable
• use combination of several techniques
• no reduction to other methods (like Walk, homogenization, mod p approaches)
Classical measures of expression swell

- Length (number of terms)
- Ecart (max degree - lead degree)
- Coefficient size

Need them all!!!
Weighted Length

- \( \mathbb{Z}/p[x_1, \ldots , x_n] \): length
- \( \mathbb{Q}[x_1, \ldots , x_n] \): size(lc(p)) * length(p)
- elimination orderings:
  \[
  \sum_{m \in \text{supp}(p)} (1 + | \deg(m) - \deg(\text{lm}(p)) |^+)
  \]
  where supp(p) are the monomials of p
  e.g. for \( x>y \): \( \text{wlen}(x^3+y^5) = 1+(1+5-3)=4 \)
Meaning for slimgb - weighted length controls everything

• sort basis elements for reduction of S-Polynomials

• choice of critical pairs (together with Sugar)

• additional reductors

• exchange basis elements by “w. shorter” ones
Extended product criterion

Theorem: \( f, g, m \) polynomials, \( \gcd(\text{lm}(f),\text{lm}(g)) = 1 \) then \( \text{spoly}(m*f, m*g) \) has standard representation against \( \{m*f, m*g\} \)

Proof:
- apply normal product criterion to \( f,g \)
- multiply with \( m \)
Application of extended product criterion

- common factor $m$ is a monomial
- for every basis $f$ element compute $\gcd(m_f)$ of its terms
- pull out $\gcd(m_f, m_g)$
- $f = x^2y + xy$, $g = xz + x$, $x > y > z$ (lex)
- $m_f = xy$, $m_g = x$, $\gcd(y^2, z) = 1$
nontrivial $t$-representations

- Let $spoly(p,q)=g_1 f_1 + ... + g_n f_n$ (*)
- Let $t$ monomial, $t \geq \text{lm}(g_i) \times \text{lm}(f_i)$ for all $i$
- this is called a $t$-representation
- of course $t \geq \text{lm}(spoly(p,q))$
- $t = \text{lm}(spoly(p,q))$: (*) standard representation
- $t < \text{lcm}(	ext{lm}(p), \text{lm}(q))$: (*) nontrivial $t$-representation (or nontrivial syzygy)
Example

- $f = xy + 1$
  
  $g = x^2 + 1$
  
  $h = x$

- Ordering $lp: x > y$

- $s := spoly(f, g) = x - y$

- $(*)$: $-y*f + (y^2 + 1)*h = s$ is a $xy^2$-representation

- $x < xy^2 < x^2y$: $(*)$ nontrivial, but not standard
Theorem

• Let $G = \{g_1, \ldots, g_n\}$

• $G$ is a Gröbner basis iff for every $i,j$: $\text{spoly}(g_i,g_j)$ has a nontrivial $t$-representation (some $t < \text{lcm}(\text{lm}(g_i),\text{lm}(g_j))$)

• Buchberger criterion: $t = \text{lm}(\text{spoly}(g_i,g_j))$

cf. Becker, Weißpfenning
Algorithm 1 slimgb main procedure, calculates a Gröbner basis of \( F \)

Require: \( F \) finite tuple of polynomials (from \( K[x_1, \ldots, x_n]^r \)).

\[
P := \{(i, j)|1 \leq i < j \leq \#F\}
\]
apply criteria to \( P \)

while \( P \neq \emptyset \) do
   choose \( \emptyset \neq S \subset P \)
   \[
P := P \setminus S
\]
   \[
(R, F) := \text{slimgbReduce}(S, F)
\]
   for \( 0 \neq r \in R \) do
      \[
F := \text{append}(F, r)
\]
      \[
P := P \cup \{(i, \#F)|1 \leq i < \#F\}
\]
      apply criteria to \( P \)
   end for
end while

return \( F \)
slimgbReduce

- reduction of several polynomials
- modifies basis by replacing polynomials by shorter ones with same leading term
- no linear algebra
Axioms for the reduction algorithm

- Input: $F$: Basis, $S$: S-Polynomials
- Output: $F'$ new Basis, $R$: reduced S-Polynomials

1. $\langle F' \cup R \rangle_{K[x_1, \ldots, x_n]} = \langle F \rangle_{K[x_1, \ldots, x_n]}$

2. $\#F = \#F'$,

3. $F'$ preserves the order of $F$: $\forall i: \text{lm}(F[i]) = \text{lm}(F'[i])$ and $\text{spoly}(F[i], F'[i])$ has standard representation w. r. t. $F' \cup R$,

4. each $r \in S$ has a nontrivial $t$-representation w. r. t. $F' \cup R$,

5. and for termination: $R \neq \emptyset \implies \exists r \in R: \text{lm}(r) \notin L(F)$. 
Sketch of proof (main)

- Algorithm terminates as usual: termination property of slimgb reduce
- The algorithm ensures, that every pair gets nontrivial t-representation at some time
- If you exchange an element of F the old one has still a standard representation
- In particular the property of having a nontrivial t-representation is never lost
Gaussian-like algorithm
+ extra operations

Each polynomial in S corresponds to a row in Gauss

• \( f, g \in S, \text{lm}(f) = \text{lm}(g) \): \( g \rightarrow \text{spoly}(f, g) \)

• \( f \in F, g \in S \): \( \text{lm}(f) | \text{lm}(g) \): \( g \rightarrow \text{spoly}(f, g) \)

• \( f \in F, g \in S \): \( \text{lm}(f) = \text{lm}(g) \): replace \( f \) in \( F \) by \( g \), \( g \) in \( S \) by \( \text{spoly}(f, g) \)

Every choice is controlled by the weighted length
Sketch of proof for reduction

• All properties hold at the beginning, except
  \[ R \neq \emptyset \Rightarrow \exists r \in R : \text{lm}(r) \notin L(F) \]

• The other properties are preserved in each step

• No element with leading term in \( L(F) \) can remain, as there is an operation to reduce it
At some points computes
\[ \text{spoly}(a^2b-x^2, abx-1) = x^3 + a \]

Same leading term as \( x^3 - x^2 y + \ldots \)

Put \( x^3 + a \) at the place of \( x^3 - x^2 y + \ldots \) (in the basis) and vice versa

Critical pairs are updated automatically (only indices)

Use \( x^3 + a \) for reduction of \( x^3 - x^2 y + \ldots \)
Strengths of slimgb

- function fields
- elimination orderings
- rational numbers
- noncommutative rings
- treats also the case of modules
Implementation in Singular

- uses same low level functions and data structures as std (Buchberger)
- slightly tuned result of a diploma thesis
- still much room for optimization
- very easy to implement efficiently compared to F4
## rational numbers

<table>
<thead>
<tr>
<th></th>
<th>Var.</th>
<th>Gen.</th>
<th>slimgb</th>
<th>std</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turaev/Viro 3 colors</td>
<td>44</td>
<td>1661</td>
<td>1 min 100MB</td>
<td>&gt; 1d &gt; 400MB</td>
</tr>
<tr>
<td>Turaev/Viro m3n1OrAns+</td>
<td>111</td>
<td>10159</td>
<td>20 min</td>
<td>&gt; 1 week</td>
</tr>
<tr>
<td>Turaev/Viro m4n1UnorAnsSimpl</td>
<td>53</td>
<td>892</td>
<td>1h</td>
<td>&gt; 1 week</td>
</tr>
<tr>
<td>Diaz1</td>
<td>7</td>
<td>9</td>
<td>0.25s 5,8MB</td>
<td>&gt;45h &gt;1GB</td>
</tr>
</tbody>
</table>

Measured on Dual Opteron 2,2GHz 16GB RAM, Singular-3-0-1/CVS
### Smaller Coefficients

<table>
<thead>
<tr>
<th></th>
<th>slimgb</th>
<th>std</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>0.42s</td>
<td>243.49s</td>
</tr>
<tr>
<td>aver. inter.</td>
<td>109</td>
<td>1188</td>
</tr>
<tr>
<td>coeff. size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multiplications</td>
<td>1190</td>
<td>3867</td>
</tr>
</tbody>
</table>

Chou 274 2 over $F_{32003}(p_1, \ldots, p_5)[x_1, \ldots, x_7]$, Singular-2-1-99
# Function fields

<table>
<thead>
<tr>
<th>O.</th>
<th>Ch.</th>
<th>Par.</th>
<th>Var.</th>
<th>Slimgb</th>
<th>Std</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>s</td>
<td>MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>s</td>
<td>MB</td>
</tr>
<tr>
<td>H. Simson 3</td>
<td>dp</td>
<td>p</td>
<td>4</td>
<td>10</td>
<td>128</td>
</tr>
<tr>
<td>H. Butterfly 1</td>
<td>dp</td>
<td>p</td>
<td>4</td>
<td>8</td>
<td>0.86</td>
</tr>
<tr>
<td>Chou 303 1</td>
<td>lp</td>
<td>p</td>
<td>5</td>
<td>8</td>
<td>2.6</td>
</tr>
<tr>
<td>Chou 274 2</td>
<td>lp</td>
<td>p</td>
<td>4</td>
<td>7</td>
<td>102</td>
</tr>
<tr>
<td>Chou 302 1</td>
<td>lp</td>
<td>p</td>
<td>5</td>
<td>8</td>
<td>2.32</td>
</tr>
</tbody>
</table>

\[ p := 32003 \]
# Further Elimination

<table>
<thead>
<tr>
<th>O.</th>
<th>Ch.</th>
<th>Var.</th>
<th>Slimgb</th>
<th>Std</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>s</td>
<td>MB</td>
</tr>
<tr>
<td>Katsura 6</td>
<td>lp</td>
<td>p</td>
<td>7</td>
<td>0.19</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&gt; 1819</td>
</tr>
<tr>
<td>Katsura 5</td>
<td>lp</td>
<td>p</td>
<td>5</td>
<td>0.01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.8</td>
</tr>
<tr>
<td>ZeroDim 57</td>
<td>lp</td>
<td>p</td>
<td>8</td>
<td>0.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&gt;1591</td>
</tr>
<tr>
<td>ZeroDim 29</td>
<td>lp</td>
<td>p</td>
<td>8</td>
<td>0.03</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&gt;1451</td>
</tr>
</tbody>
</table>
# Noncommutative O. Ch. Par. Var. Slimgb Std

<table>
<thead>
<tr>
<th></th>
<th>O.</th>
<th>Ch.</th>
<th>Par.</th>
<th>Var.</th>
<th>Slimgb</th>
<th>Std</th>
</tr>
</thead>
<tbody>
<tr>
<td>ucha 2</td>
<td>prod.</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>5,6s 5,9MB</td>
<td>16m 332MB</td>
</tr>
<tr>
<td>ucha 4</td>
<td>lp</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0.01s 0,6MB</td>
<td>0,27 0,6MB</td>
</tr>
<tr>
<td>tarasov 2</td>
<td>dp</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>1,45min 26MB</td>
<td>&gt;3,5h &gt;2,4GB</td>
</tr>
<tr>
<td>bern5</td>
<td>prod.</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>2,11min 16,8 MB</td>
<td>&gt;2h &gt;7,5GB</td>
</tr>
</tbody>
</table>