Computation of Hilbert bases and Graver bases

Lunch talk, 24-11-2005

Raymond Hemmecke

raymond@hemmecke.de

Let's start with integral bases...

For $S \subseteq \mathbb{Z}^n$ we call $T \subseteq S$ an integral generating set every $s \in S$ can be written as

$$s = \sum \alpha_i t_i, \quad \alpha_i \in \mathbb{Z}_+, t_i \in T.$$

Theorem. (H. & Weismantel) S possesses a finite integral generating set if and only if $\mathrm{cone}(S)$ is a rational polyhedral cone.

Consequence. For every rational pointed cone C, the set $S = C \cap \mathbb{Z}^n$ possesses a finite integral basis called Hilbert basis of S (or of C).

If C is also pointed, there is a unique inclusion-minimal Hilbert basis.

What is a Graver basis?

$\mathbb{O}_j = j^{\text{th}}$ orthant of $\mathbb{R}^n$

$H_j =$ (unique) minimal Hilbert basis of $\ker_{\mathbb{R}^n}(A) \cap \mathbb{O}_j$.

$$G(A) := \bigcup H_j \setminus \{0\}$$

is called the **Graver basis** of A.

$G(A)$ is an integral generating set of $\ker_{\mathbb{Z}^n}(A)$ in every orthant, that is, $G(A) \cap \mathbb{O}_j$ is an integral generating set of $\ker_{\mathbb{Z}^n}(A) \cap \mathbb{O}_j$.

The relation $\sqsubseteq$

For $u, v \in \mathbb{R}^n$ let $u \sqsubseteq v$ iff $u^{(i)} v^{(i)} \geq 0$ and $|u^{(i)}| \leq |v^{(i)}|$ for $i = 1, \ldots, n$.

$G(A)$ is exactly the set of $\sqsubseteq$-minimal elements in $\ker_{\mathbb{Z}^n}(A) \setminus \{0\}$.

$G(A)$ has the positive sum property w.r.t. $\ker_{\mathbb{Z}^n}(A)$, that is, every $z \in \ker_{\mathbb{Z}^n}(A)$ possesses a $\sqsubseteq$-representation w.r.t. $G(A)$:

$$z = \sum \alpha_i g_i, \quad \alpha_i \in \mathbb{Z}_{>0}, g_i \in G(A), g_i \sqsubseteq z.$$

$G(A)$ is the unique inclusion-minimal subset of $\ker_{\mathbb{Z}^n}(A)$ that has the positive sum property w.r.t. $\ker_{\mathbb{Z}^n}(A)$.

Criterion for PSP

Given a lattice $\Lambda \subseteq \mathbb{Z}^n$.

Infinite test. A set symmetric set $G \subseteq \Lambda$ has the p.s.p. w.r.t. Λ if and only if every $z \in \Lambda$ is $\sqsubseteq$-representable w.r.t. G.

Finite test. A set symmetric set $G \subseteq \Lambda$ has the p.s.p. w.r.t. Λ if and only if G generates Λ over $\mathbb{Z}$ and if every sum $u+v$, $u, v \in G$, is $\sqsubseteq$-representable w.r.t. G.

This leads immediately to a finite algorithm due to L. Pottier, which is based on a so-called completion procedure.

Idea of proof

$$z \in \Lambda$$

$$z = \sum \alpha_i g_i, \quad \alpha_i \in \mathbb{Z}_{>0}, g_i \in G$$

$$\sum \alpha_i \|g_i\|_1 \geq \|z\|_1$$ triangle inequality

Equality holds iff and only if $g_i \sqsubseteq z$ for all i.

Idea of proof (2)

Assume $\sum \alpha_i \|g_i\|_1 > \|z\|_1. \longrightarrow \exists g_{i_1}, g_{i_2}, k$ with $g_{i_1}^{(k)} g_{i_2}^{(k)} < 0$

$$g_{i_1} + g_{i_2} = \sum \beta_j \bar{g}_j, \quad \beta_j \in \mathbb{Z}_{>0}, \bar{g}_j \in G, \bar{g}_j \sqsubseteq g_{i_1} + g_{i_2}$$

$$z = \sum_{i \neq i_1, i_2} \alpha_i g_i + (\alpha_{i_1} - 1) g_{i_1} + (\alpha_{i_2} - 1) g_{i_2} + \sum \beta_j \bar{g}_j$$

Pottier's algorithm

In: symmetric generating set F for $\ker(A) \longrightarrow$ Out: Graver basis of A

$G := F \qquad C := \bigcup_{f,g \in G} \{f+g\}$

while $C \neq \emptyset$ do

$\quad s :=$ an element in $C \qquad C := C \setminus \{s\}$

$\quad f := \mathrm{normalForm}(s, G)$

$\quad$ if $f \neq 0$ then

$\qquad C := C \cup \bigcup_{g \in G} \{f+g\} \qquad G := G \cup \{f\}$

return G.

Normal form algorithm

Input: a vector s, a set G of vectors

Output: a normal form of s with respect to G

while there is some $g \in G$ such that $g \sqsubseteq s$ do

$s := s - g$

return s

Termination and Correctness

Correctness upon termination is clear.

Termination follows from the Gordan-Dickson Lemma:

Every sequence $\{p_1, p_2, \ldots\} \subseteq \mathbb{Z}_+^n$ with $p_i \not\leq p_j$ whenever $i < j$ is finite.

Every sequence $\{p_1, p_2, \ldots\} \subseteq \mathbb{Z}^n$ with $p_i \not\sqsubseteq p_j$ whenever $i < j$ is finite.

State-of-the-art algorithm

- Apply Pottier's algorithm to achieve Graver basis property on a subset of all variables.

  All vectors in $\ker(A)$ (in particular: all Graver bases elements) can be generated by increasing norm on these variables.

- Apply Pottier's algorithm again, but to all variables.
  - Fewer sums $f+g$ have to be considered. (f and g should have the same sign pattern on the chosen variables.)
  - Only those sums $f+g$ have to be considered that fulfill upper bound conditions on the chosen variables.

Critical-pair selection strategy

Choose $s \in C$ by increasing norm on the given subset of all variables.

- $G(A)$ is constructed by increasing norm on subset of variables.
- $\mathrm{normalForm}(s, G)$ needs only check reducibility w.r.t. G.
- Exactly $G(A)$ is computed.

Review proof

$$z \in \Lambda$$

$$z = \sum \alpha_i g_i, \quad \alpha_i \in \mathbb{Z}_{>0}, g_i \in G$$

$$\sum \alpha_i \|g_i\|_1 \geq \|z\|_1 \quad \text{triangle inequality}$$

Equality holds iff and only if $g_i \sqsubseteq z$ for all i.

Review proof (2)

Assume $\sum \alpha_i \|g_i\|_1 > \|z\|_1. \longrightarrow \exists g_{i_1}, g_{i_2}, k$ with $g_{i_1}^{(k)} g_{i_2}^{(k)} < 0$

$$g_{i_1} + g_{i_2} = \sum \beta_j \bar{g}_j, \quad \beta_j \in \mathbb{Z}_{>0}, \bar{g}_j \in G$$

$$z = \sum_{i \neq i_1, i_2} \alpha_i g_i + (\alpha_{i_1} - 1) g_{i_1} + (\alpha_{i_2} - 1) g_{i_2} + \sum \beta_j \bar{g}_j$$

Computation of Hilbert bases

To compute Hilbert basis for cone $\{z : Az = 0, z \geq 0\}$ do for $k = 1, \ldots, n$:

- Guarantee PSP on first k variables.
- Extract vectors that fulfill sign conditions $x_i \geq 0$, $i = 1, \ldots, k$.

Applicable also for Hilbert bases of cones $\{z : Az \leq 0\}$. Simply rewrite as $\{z : Az + u = 0, u \geq 0, z \text{ free}\}$.

Theoretically, this approach can compute “any” set inbetween Hilbert basis and Graver basis.

4ti2's function "solve"

Is being implemented by Matthias Walter. This function allows to solve systems of the following form:

$$\begin{aligned} Ax &= a \\ Bx &\leq b \\ Cx &\equiv c \pmod{p} \\ l \leq x &\leq u \end{aligned}$$

Each variable is either of type

- free
- Graver
- Hilbert

Output are two sets I and H such that each solution is the some of one element from I and a nonnegative integer linear combination of elements from H:

$$z = z_{\text{inhom}} + \sum \alpha_i z_{\text{hom},i}.$$

Example

$$\begin{aligned} x + y + 2z &= 3 \\ -3x + y &\leq 7 \\ 4x + z &\equiv 5 \pmod 7 \end{aligned}$$

All variables are free.

Example (2)

Matrix file "example":

```
3 3
 1 1 2
-3 1 0
 4 0 1
```

Right-hand side file "example.rhs":

```
1 3
3 7 5
```

Example (3)

Info file “example.ini”:

```
all free
1 equ
2 leq
3 mod 7
```

Example(4)

“Solve” rewrites the system as:

$$
\begin{array}{rcl}
x + y + 2z - 3s & = & 0 \\
-3x + y - 7s + t & = & 0 \\
4x + z - 5s + 7u & = & 0 \\
s & \geq & 0 \\
t & \geq & 0 \\
s & \leq & 1
\end{array}
$$

x, y, z, u are free, s, t are Hilbert components.

Example(5)

Matrix file “example”:

```
3 6
 1 1 2 -3 0 0
-3 1 0 -7 1 0
 4 0 1 -5 0 7
```

Info file “example.ini”:

```
all free
4 0 1
5 0 inf
all equ
```

Example(6)

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 7 \\ -2 \end{pmatrix} + \alpha \begin{pmatrix} 3 \\ 7 \\ -5 \end{pmatrix} + \beta \begin{pmatrix} 7 \\ 21 \\ -14 \end{pmatrix}, \quad \alpha \in \mathbb{Z}_+, \beta \in \mathbb{Z}$$