The art of cryptography, summer 2013

Lattices and cryptography

Prof. Dr. Joachim von zur Gathen
Dr. Daniel Loebenberger

ALGORITHM 1. Basis reduction.

Input: Linearly independent row vectors $a_1, \dots, a_\ell \in \mathbb{Z}^n$.
Output: A reduced basis $b_1, \dots, b_\ell$ of the lattice
$L = \sum_{1 \le i \le \ell} \mathbb{Z} a_i \subseteq \mathbb{Z}^n$.

1. For $i = 1, \dots, \ell$ do $b_i \leftarrow a_i$.
2. Compute the GSO $B^* \in \mathbb{Q}^{\ell \times n}$, $M \in \mathbb{Q}^{\ell \times \ell}$,
3. $i \leftarrow 2$.
4. While $i \le \ell$ do 5–10
5. For $j = i-1, i-2, \dots, 1$ do step 6–6
6. $b_i \leftarrow b_i - \lceil \mu_{ij} \rfloor b_j$, update the GSO, { replacement step }
7. If $i > 1$ and $\|b_{i-1}^*\|^2 > 2\|b_i^*\|^2$ then
8. exchange b_{i-1} and b_i and update the GSO, { exchange step }
9. $i \leftarrow i - 1$.
10. Else $i \leftarrow i + 1$.
11. Return $b_1, \dots, b_\ell$.

THEOREM 2. *Algorithm 1 correctly computes a reduced basis of* $L \subseteq \mathbb{Z}^n$ *and runs in polynomial time. It uses* $O(n^4 m)$ *arithmetic operations on integers whose bit length is* $O(nm)$*, if the norm of each given generator for* L *has bit length at most* m*.*

LEMMA 3. i. *We consider one execution of step 6, for i, j with $1 \leq j < i \leq \ell$. Let $B, B^* \in \mathbb{Q}^{\ell \times n}, M \in \mathbb{Q}^{\ell \times \ell}$ and $C, C^* \in \mathbb{Q}^{\ell \times n}, N \in \mathbb{Q}^{\ell \times \ell}$ be the matrices of the b_k, b_k^*, μ_{kh} before and after the replacement, respectively, and $E = (e_{kh}) \in \mathbb{Z}^{\ell \times \ell}$ the matrix which has $e_{kk} = 1$ for all k, $e_{ij} = -\lceil \mu_{ij} \rfloor$, and $e_{kh} = 0$ otherwise. Then*

$$C = EB, \; C^* = B^* \text{ and } N = EM.$$

ii. *The following invariant holds before each execution of step 6:*

$$|\mu_{ih}| \leq \frac{1}{2} \text{ for } j < h < i.$$

iii. *The Gram-Schmidt orthogonal basis $b_1^*, \ldots, b_\ell^*$ does not change in step 6, and after the loop in steps 5–6 we have $|\mu_{ih}| \leq 1/2$ for $1 \leq h < i$.*

$$
\begin{pmatrix}
1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
\cdot & 1 & \ddots & & & & & \vdots \\
\cdot & \cdot & 1 & \ddots & & & & \vdots \\
\cdot & \cdot & \cdot & 1 & \ddots & & & \vdots \\
\cdot & \cdot & \cdot & \cdot & 1 & \ddots & & \vdots \\
\circ & \circ & \bullet & \cdot & \cdot & 1 & \ddots & \vdots \\
* & * & * & * & * & * & 1 & 0 \\
* & * & * & * & * & * & * & 1
\end{pmatrix}
$$

Figure: The effect of one replacement step on the μ_{ij}.

LEMMA 4. *Suppose that b_{i-1} and b_i are exchanged in step 8, and denote by $c_1, \ldots, c_\ell$ and $c_1^*, \ldots, c_\ell^*$ the values of the vectors and their Gram-Schmidt orthogonal basis after the exchange, respectively. Then*

i. $c_k^* = b_k^*$ *for* $k \in \{1, \ldots, \ell\} \setminus \{i-1, i\}$,

ii. $\|c_{i-1}^*\|^2 < \frac{3}{4}\|b_{i-1}^*\|^2$,

iii. $\|c_i^*\| \leq \|b_{i-1}^*\|$.

LEMMA 5. *At the beginning of each iteration of the loop in steps 4–10, the following invariants hold:*

$$|\mu_{kh}| \leq \frac{1}{2} \text{ for } 1 \leq h < k < i, \quad \|b^*_{k-1}\|^2 \leq 2\|b^*_k\|^2 \text{ for } 1 \leq k < i.$$

At any stage in the algorithm and for $1 \le k \le \ell$, we consider the matrix

$$B_k = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} \in \mathbb{Z}^{k \times n}$$

comprising the first k vectors, their Gram matrix $B_k \cdot B_k^T = (b_j \star b_h)_{1 \le j,h \le k} \in \mathbb{Z}^{k \times k}$, and the *Gram determinant* $d_k = \det(B_k \cdot B_k^T) \in \mathbb{Z}$. For convenience, we let $d_0 = 1$.

LEMMA 6. *For* $1 \le k \le \ell$, *we have* $d_k = \prod_{1 \le h \le k} \|b_h^*\|^2 > 0$.

LEMMA 7. i. *In steps 5–6, none of the d_k changes.*

ii. *If b_{i-1} and b_i are exchanged in step 7–10 and d_k^* denotes the new value of d_k, for any k, then $d_k^* = d_k$ for $k \neq i-1$ and $d_{i-1}^* \leq \frac{3}{4} d_{i-1}$.*

step	$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$	$\begin{pmatrix} \mu_{21} & \\ \mu_{31} & \mu_{32} \end{pmatrix}$	$\begin{pmatrix} \|b_1^*\|^2 \\ \|b_2^*\|^2 \\ \|b_3^*\|^2 \end{pmatrix}$	d_1, d_2 D	action
4	$\begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 2 \\ 3 & 5 & 6 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{3} & \\ \frac{14}{3} & \frac{13}{14} \end{pmatrix}$	$\begin{pmatrix} 3 \\ \frac{14}{3} \\ \frac{9}{14} \end{pmatrix}$	$3, 14$ 42	rep$(3,2)$
4	$\begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 2 \\ 4 & 5 & 4 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{3} & \\ \frac{13}{3} & \frac{-1}{14} \end{pmatrix}$	$\begin{pmatrix} 3 \\ \frac{14}{3} \\ \frac{9}{14} \end{pmatrix}$	$3, 14$ 42	rep$(3,1)$
5	$\begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{3} & \\ \frac{1}{3} & \frac{-1}{14} \end{pmatrix}$	$\begin{pmatrix} 3 \\ \frac{14}{3} \\ \frac{9}{14} \end{pmatrix}$	$3, 14$ 42	ex$(3,2)$
5	$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 2 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{3} & \\ \frac{1}{3} & \frac{-1}{2} \end{pmatrix}$	$\begin{pmatrix} 3 \\ \frac{2}{3} \\ \frac{9}{2} \end{pmatrix}$	$3, 2$ 6	ex$(2,1)$
4	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ -1 & 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & \\ 0 & \frac{1}{2} \end{pmatrix}$	$\begin{pmatrix} 1 \\ 2 \\ \frac{9}{2} \end{pmatrix}$	$1, 2$ 2	rep$(2,1)$
6	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ -1 & 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 0 & \\ 0 & \frac{1}{2} \end{pmatrix}$	$\begin{pmatrix} 1 \\ 2 \\ \frac{9}{2} \end{pmatrix}$	$1, 2$ 2	

Table: Trace of the basis reduction Algorithm 1 on the lattice $L = \mathbb{Z}(1,1,1) + \mathbb{Z}(-1,0,2) + \mathbb{Z}(3,5,6)$.

COROLLARY 8. *Given linearly independent vectors $a_1, \ldots, a_\ell \in \mathbb{Z}^n$ whose norm has bit length at most m, the basis reduction algorithm Algorithm 1 computes a reduced basis $b_1, \ldots, b_\ell$ of $L = \sum_{1 \le i \le \ell} \mathbb{Z} a_i$. Furthermore, b_1 is a "short" nonzero vector in L with*

$$\|b_1\| \le 2^{(\ell-1)/2} \lambda_1(L) = 2^{(\ell-1)/2} \min\{\|y\| \colon 0 \ne y \in L\}.$$

It uses $O(n^6 m^3)$ bit operations.