The art of cryptography, summer 2013

Lattices and cryptography

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

Given an arbitrary basis $(b_1, \ldots, b_\ell)$ of an ℓ-dimensional subspace of $\mathbb{R}^n$, it computes an orthogonal basis $(b_1^*, \ldots, b_\ell^*)$ of the same subspace.
The b_i^* are defined inductively as follows.

$$b_i^* = b_i - \sum_{1 \le j < i} \mu_{ij} b_j^*, \text{ where } \mu_{ij} = \frac{b_i \star b_j^*}{\|b_j^*\|^2} \text{ for } 1 \le j < i. \qquad (1)$$

In particular, $b_1^* = b_1$. Then $(b_1^*, \ldots, b_\ell^*)$ is the *Gram-Schmidt orthogonal basis* of $(b_1, \ldots, b_\ell)$, and the b_i^* together with the μ_{ij} form the *Gram-Schmidt orthogonalization* (or GSO for short) of $b_1, \ldots, b_\ell$.
The cost for computing the GSO is $O(n^3)$ arithmetic operations in $\mathbb{Q}$, since $\ell \le n$.

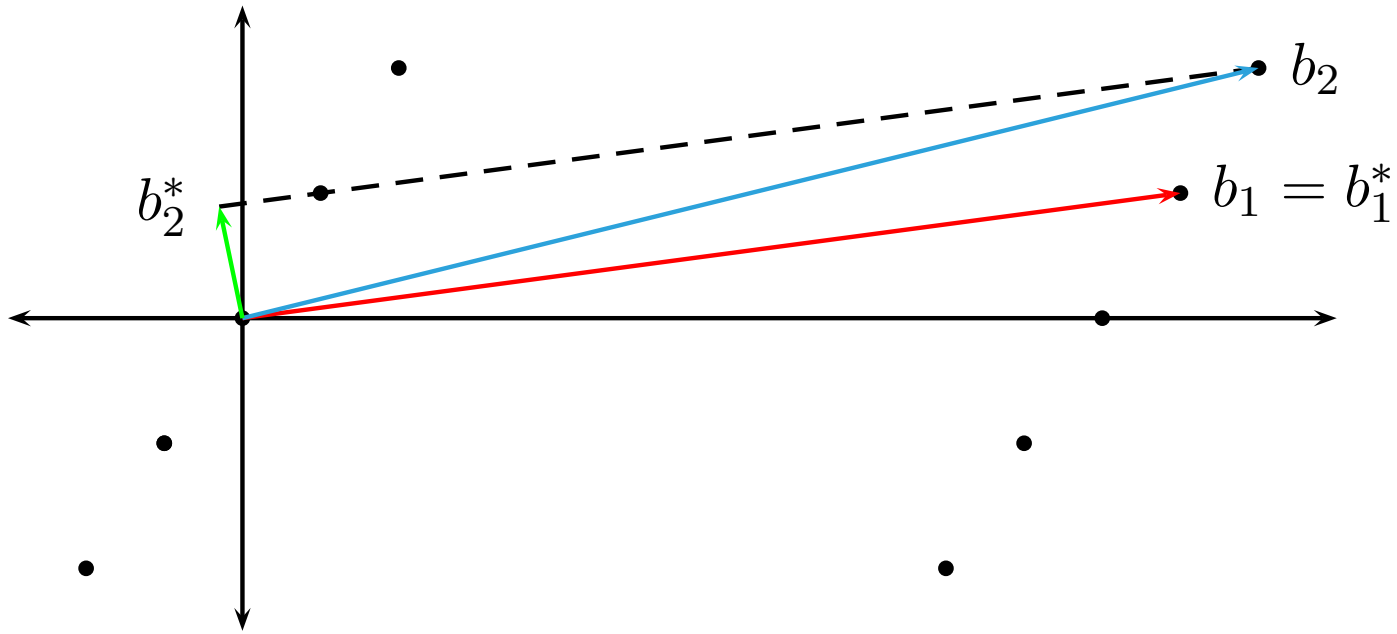

Figure: The Gram-Schmidt orthogonal basis of $(12, 2)$ and $(13, 4)$.

We have $b_1^* = b_1 = (12, 2)$,

$$\mu_{21} = \frac{b_2 \star b_1^*}{b_1^* \star b_1^*} = \frac{41}{37}, \quad b_2^* = b_2 - \mu_{21} b_1^* = \Big(-\frac{11}{37}, \frac{66}{37} \Big).$$

The vector b_2^* (green) is the projection of b_2 (blue) onto the orthogonal complement of b_1 (red).

We can rewrite (1) as

$$b_i = \sum_{1 \le j \le i} \mu_{ij} b_j^* \text{ with } \mu_{ii} = 1. \tag{2}$$

Since the b_j^* are linearly independent, the $\mu_{ij} \in \mathbb{R}$ are uniquely determined by (2).
We consider the b_i and b_i^* to be row vectors in $\mathbb{R}^n$, and define two matrices $B, B^* \in \mathbb{R}^{\ell \times n}$ and a matrix M in $\mathbb{R}^{\ell \times \ell}$:

$$B = \begin{pmatrix} b_1 \\ \vdots \\ b_\ell \end{pmatrix}, \; B^* = \begin{pmatrix} b_1^* \\ \vdots \\ b_\ell^* \end{pmatrix}, \; M = (\mu_{ij})_{1 \le i,j \le \ell}, \tag{3}$$

where $\mu_{ii} = 1$ for $i \le \ell$, and $\mu_{ij} = 0$ for $1 \le i < j \le \ell$. Then M is lower triangular with ones on the diagonal, and (1) reads:

$$B = \begin{pmatrix} b_1 \\ \vdots \\ b_\ell \end{pmatrix} = \begin{pmatrix} 1 & & 0 \\ \vdots & \ddots & \\ \mu_{n1} & \cdots & 1 \end{pmatrix} \begin{pmatrix} b_1^* \\ \vdots \\ b_\ell^* \end{pmatrix} = M \cdot B^*. \tag{4}$$

EXAMPLE 5. We let $\ell = n = 3$, $b_1 = (1,1,0)$, $b_2 = (1,0,1)$, $b_3 = (0,1,1)$, and calculate $b_1^* = b_1 = (1,1,0)$,

$$\mu_{21} = \frac{b_2 \star b_1^*}{b_1^* \star b_1^*} = \frac{1}{2}, \quad b_2^* = b_2 - \mu_{21} b_1^* = \left(\frac{1}{2}, -\frac{1}{2}, 1\right),$$

$$\mu_{31} = \frac{b_3 \star b_1^*}{b_1^* \star b_1^*} = \frac{1}{2}, \ \ \mu_{32} = \frac{b_3 \star b_2^*}{b_2^* \star b_2^*} = \frac{1}{3},$$

$$b_3^* = b_3 - \mu_{31} b_1^* - \mu_{32} b_2^* = \left(-\frac{2}{3}, \frac{2}{3}, \frac{2}{3}\right),$$

$$B = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & 1 & 0 \\ \frac{1}{2} & \frac{1}{3} & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ \frac{1}{2} & -\frac{1}{2} & 1 \\ -\frac{2}{3} & \frac{2}{3} & \frac{2}{3} \end{pmatrix} = M \cdot B^*.$$

We have $\|b_1\|^2 = \|b_2\|^2 = \|b_3\|^2 = 2$, $\|b_1^*\|^2 = 2$, $\|b_2^*\|^2 = 3/2$, $\|b_3^*\|^2 = 4/3$ and $\det B^* = -2$.

THEOREM 6. *Let $b_1, \ldots, b_\ell \in \mathbb{R}^n$ be linearly independent, and $b_i^*, \ldots, b_\ell^*$ their Gram-Schmidt orthogonalization. For $0 \leq k \leq \ell$ let $U_k = \sum_{1 \leq i \leq k} \mathbb{R} b_i \subseteq \mathbb{R}^n$ be the $\mathbb{R}$-subspace spanned by $b_1, \ldots, b_k$.*

i. $\sum_{1 \leq i \leq k} \mathbb{R} b_i^* = U_k$.

ii. b_k^* *is the projection of* b_k *onto the orthogonal complement*

$$U_{k-1}^\perp = \{b \in \mathbb{R}^n : b \star u = 0 \text{ for all } u \in U_{k-1}\}$$

of U_{k-1}, *and hence in particular* $\|b_k^*\| \leq \|b_k\|$.

iii. $b_1^*, \ldots, b_\ell^*$ *are pairwise orthogonal, that is,* $b_i^* \star b_j^* = 0$ *if* $i \neq j$.

iv. $$\det \begin{pmatrix} b_1 \\ \vdots \\ b_\ell \end{pmatrix} = \det \begin{pmatrix} b_1^* \\ \vdots \\ b_\ell^* \end{pmatrix}.$$

THEOREM 7. *Let $L \subseteq \mathbb{R}^n$ be a lattice with basis $b_1, \ldots, b_\ell \in \mathbb{R}^n$, Gram-Schmidt orthogonal basis $b_1^*, \ldots, b_\ell^* \in \mathbb{R}^n$, and successive minima $\lambda_1(L), \ldots, \lambda_\ell(L)$. Then for any $1 \leq i \leq \ell$ we have*

$$\min\{||b_i^*||, ||b_{i+1}^*||, \ldots, ||b_\ell^*||\} \leq \lambda_i(L).$$

COROLLARY 8. *Let $L \subseteq \mathbb{R}^n$ be a lattice with basis $(b_1, \ldots, b_\ell)$ and Gram-Schmidt orthogonal basis $(b_1^*, \ldots, b_\ell^*)$. Then for any nonzero $x \in L$ we have*

$$\min\{\|b_1^*\|, \ldots, \|b_\ell^*\|\} \leq \|x\|.$$

DEFINITION 9. *Let $b_1, \ldots, b_\ell \in \mathbb{R}^n$ be linearly independent and $b_1^*, \ldots, b_\ell^*$ the corresponding Gram-Schmidt orthogonal basis. Then $b_1, \ldots, b_\ell$ is reduced if and only if $\|b_i^*\|^2 \leq 2\|b_{i+1}^*\|^2$ for $1 \leq i < \ell$.*

THEOREM 10. *Let $b_1, \ldots, b_\ell \in \mathbb{R}^n$ be a reduced basis of the lattice L and $\lambda_1(L)$ the length of a shortest nonzero vector x in L. Then $\|b_1\| \leq 2^{(\ell-1)/2} \cdot \lambda_1(L)$.*

ALGORITHM 11. Basis reduction.

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

1. For $i = 1, \ldots, \ell$ do $b_i \leftarrow a_i$.
2. Compute the GSO $B^* \in \mathbb{Q}^{\ell \times n}$, $M \in \mathbb{Q}^{\ell \times \ell}$, as in (1) and (3),
3. $i \leftarrow 2$.
4. While $i \le \ell$ do 5–10
5. For $j = i-1, i-2, \ldots, 1$ do step
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 $b_1, \ldots, b_\ell$.

step	$\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$	M	$\begin{pmatrix} b_1^* \\ b_2^* \end{pmatrix}$	action
6	$\begin{pmatrix} 12 & 2 \\ 13 & 4 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ \frac{41}{37} & 1 \end{pmatrix}$	$\begin{pmatrix} 12 & 2 \\ -\frac{11}{37} & \frac{66}{37} \end{pmatrix}$	row $2 \leftarrow$ row $2 -$ row 1
7	$\begin{pmatrix} 12 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ \frac{4}{37} & 1 \end{pmatrix}$	$\begin{pmatrix} 12 & 2 \\ -\frac{11}{37} & \frac{66}{37} \end{pmatrix}$	exchange rows 1 and 2
6	$\begin{pmatrix} 1 & 2 \\ 12 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ \frac{16}{5} & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ \frac{44}{5} & -\frac{22}{5} \end{pmatrix}$	row $2 \leftarrow$ row $2 - 3 \cdot$ row 1
11	$\begin{pmatrix} 1 & 2 \\ 9 & -4 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ \frac{1}{5} & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ \frac{44}{5} & -\frac{22}{5} \end{pmatrix}$	

Table: Trace of the basis reduction Algorithm 11.

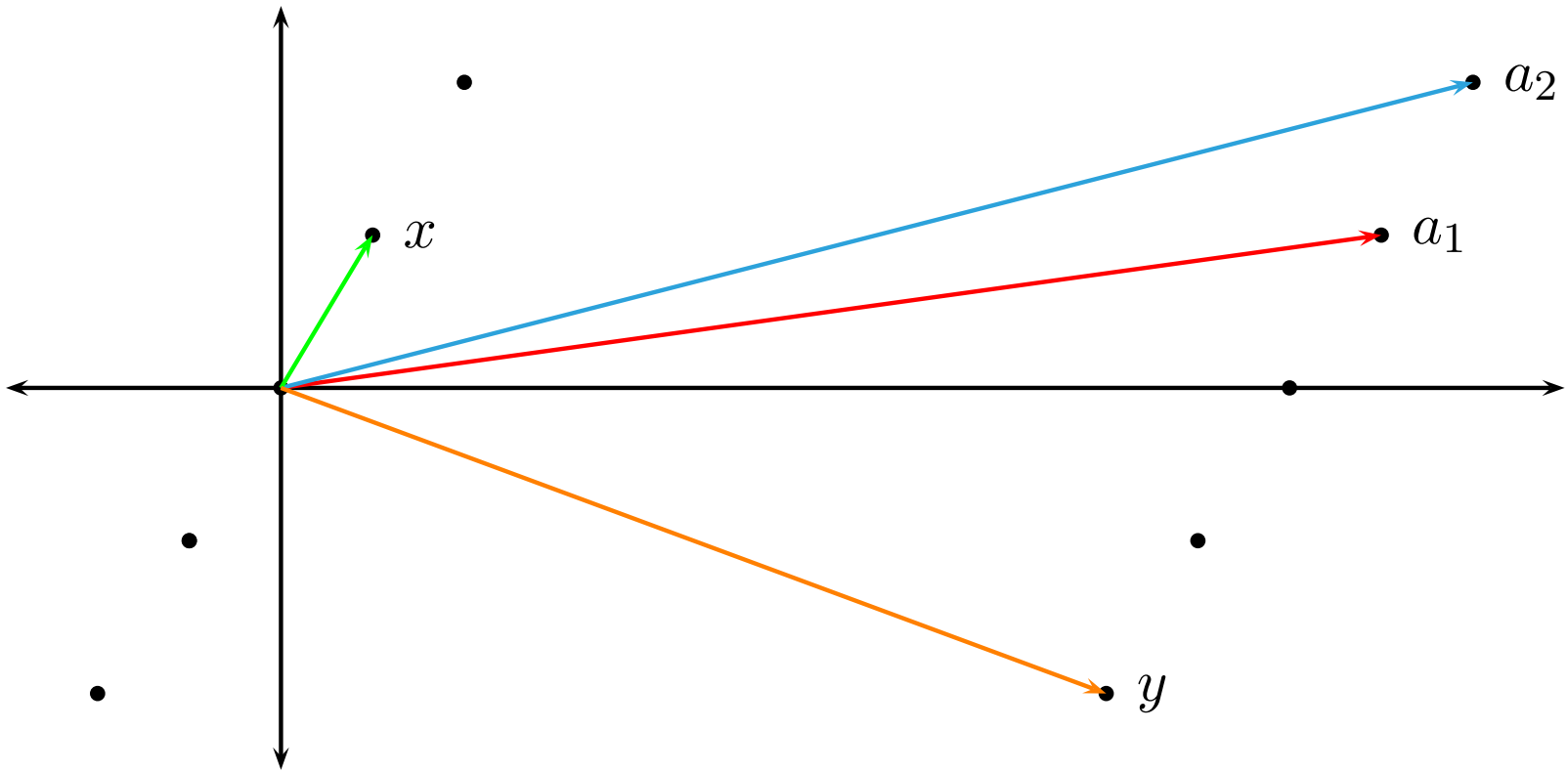

Figure: The vectors computed by the basis reduction Algorithm 11.