A layered LLL algorithm

Erwin L. Torreao Dassen
Universiteit Leiden, The Netherlands

Bordeaux, December 2, 2008

Outline

- Review what the LLL algorithm is and does.
- Example of its use: computing kernels and images of groups.
- The idea of the layered setting.
- Layered Euclidean spaces and layered lattices.
- Our example in the layered setting.

LLL Introduction I

Recall:

A lattice is a finitely generated abelian group L together with a map $q : L \to \mathbb{R}$ such that for all $x, y \in L$ and all $r \in \mathbb{R}$ we have

- $x \neq 0 \implies q(x) \neq 0$
- $q(x + y) + q(x - y) = 2q(x) + 2q(y)$
- $\forall r \in \mathbb{R},\ \{x \in L : q(x) \leqslant r\}$ is finite

Giving (L, q) is equivalent to giving a discrete subgroup of a Euclidean space. $(\langle x, y\rangle = \frac{1}{4}q(x + y) + \frac{1}{4}q(x - y))$

The *rank* of a lattice is its rank as an abelian group. We denote by $d(L)$ the discriminant of L (the volume spanned by a basis of L).

LLL Introduction II

- In many applications of lattice theory one is interested in finding "short" vectors in a given lattice.
- This stems from the fact that in many cases, by constructing an appropriate lattice, one can read off solutions of the given problem from these short vectors.
- In this direction the main theoretical result is Minkowski's theorem:

Each lattice L of positive rank n contains a non-zero element x with

$$q(x) \leqslant \frac{4}{\pi}\Gamma(1+n/2)^{2/n} d(L)^{2/n} \leqslant n \cdot d(L)^{2/n}.$$

LLL Introduction III

- Every lattice has a basis consisting of optimally short vectors (take the smallest ball containing a basis).
- LLL is a family of polynomial time algorithms that from an arbitrary basis constructs a *c-reduced* basis which is “nearly” optimal by successively applying “rank 2” reductions at each step.
- The parameter c is a real number $> 4/3$ encoding more or less the quality of this basis (how smaller the c the better the quality).

Lattices of rank 2

Let L be a lattice of rank 2 and $\{b_1, b_2\}$ a basis of L. We say L is *reduced* if

$$q(b_1) = \min_{x \in L - \{0\}} q(x) \qquad q(b_2) = \min_{x \in L - \mathbb{Z} b_1} q(x).$$

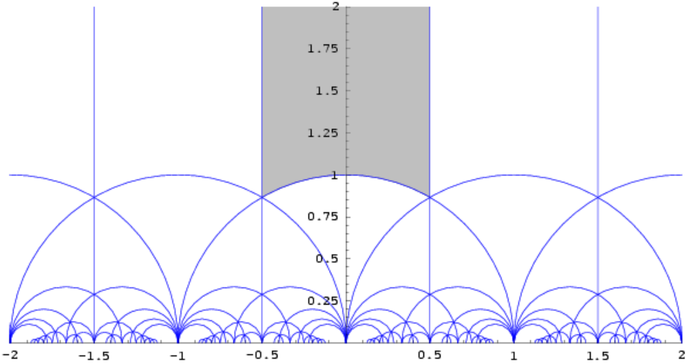
If one defines

$$a = q(b_1) \quad b = 2\langle b_1, b_2 \rangle \quad c = q(b_2)$$

then $\{b_1, b_2\}$ is reduced if and only if

$$|b| \leqslant a \leqslant c.$$

Reduced basis



If $b_1 = (1, 0)$ then $\{b_1, b_2\}$ is reduced if b_2 lies in the shaded region.

Lattice basis reduction in rank 2

The following procedure is due to Gauss. Given a basis $\{b_1, b_2\}$ of L it computes a reduced basis.

1. $m \leftarrow \lfloor \langle b_1, b_2 \rangle / q(b_1) \rceil$ (*nearest integer*)
2. $b_2 \leftarrow b_2 - m b_1$ (*we now have* $2|\langle b_1, b_2 \rangle| \leqslant q(b_1)$)
3. if $q(b_2) < q(b_1)$ swap b_1, b_2 and iterate else output $\{b_1, b_2\}$

That this procedure is correct follows from the inequalities $|b| \leqslant a \leqslant c$ mentioned before. It terminates since the norm of b_1 decreases through the process.

Reduction in general rank

The idea now is to apply one step of the above procedure to a rank 2 sublattice of our lattice L of rank n at each step.

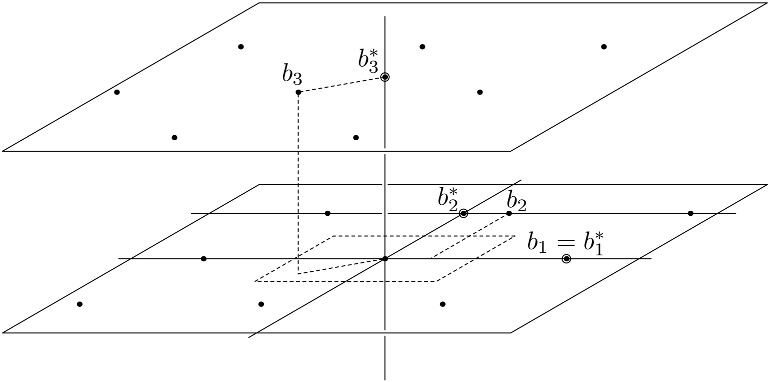
First, given a basis $\{b_1, \ldots, b_n\}$ of L let $\{b_1^*, \ldots, b_n^*\}$ be the associated Gram-Schmidt basis and define

$$L_j = \sum_{i=1}^{j} \mathbb{Z} b_i \quad \text{and} \quad \ell_j = d(L_j/L_{j-1}) \; (= ||b_j^*||).$$

Let $c \geqslant 1$. A basis $\{b_1, \ldots, b_n\}$ is *c-reduced* if for all $0 < j < n$ and all $i < j$ we have

- $2|\langle b_i^*, b_j \rangle| \leqslant q(b_i^*)$ (size-reducedness)
- $\ell_j^2 \leqslant c\ell_{j+1}^2$

What is size-reducedness?



$$|\langle b_i^*, b_j \rangle| \leqslant \frac{1}{2} q(b_i^*).$$

Reduction in general rank

We can now summarize a possible approach as follows:

1. size-reduce $\{b_1, \ldots, b_n\}$
2. if $\{j : c\ell_{j+1}^2 < \ell_j^2\} \neq \varnothing$ choose j in this set, swap b_j, b_{j+1} and iterate, else output $b_1, \ldots, b_n$

- Size-reducedness is easily accomplished by a direct generalization of the rank 2 case.
- It is not clear that this yields a polynomial time algorithm (in fact this is an open problem for $c = 4/3$).
- The classical LLL described in [1] takes the minimum j in step 2. This allows us to size-reduce as needed.
- The output of this procedure is clearly a c-reduced basis.

What about c?

As expected a lattice basis which is "nearly" orthogonal is also "nearly" optimal (in size).

Denote by $\lambda_i(L)$ the ith-successive minimum of L, that is,

$$\lambda_i(L) = \inf\{r \in \mathbb{R} : \exists\{x_1, \ldots, x_i\} \subset L \textit{ lin. indep. with } q(x_j) \leqslant r\}.$$

Theorem

Let $c \geqslant 4/3$ and let $\{b_1, \ldots, b_n\}$ be a c-reduced basis of L. Then for $1 \leqslant i \leqslant n$ we have

$$c^{1-n} q(b_i) \leqslant \lambda_i(L) \leqslant c^{i-1} q(b_i).$$

In particular for the shortest vector ($i = 1$) we have

$$q(b_1) \leqslant c^{n-1} \lambda(L).$$

Example: computing kernels & images

Let $\mathbf{F}$ be the matrix representing $f : \mathbb{Z}^n \to \mathbb{Z}^m$ and $r =$ rank($\mathbf{F}$). Choose

$$F > \max_{i,j} |\mathbf{F}_{ij}| \qquad c \geqslant 4/3 \qquad N > c^{n-1}(r+1)r^r F^{2r}.$$

Consider the lattice $(\mathbb{Z}^n, q)$ where

$$q(x) = ||x||^2 + N||f(x)||^2.$$

Then a c-reduced basis of this lattice satisfies the following.

(a). $\{b_1, \ldots, b_{n-r}\}$ forms a basis for ker f

(b). $\{f(b_{n-r+1}), \ldots, f(b_n)\}$ forms a basis for $f(\mathbb{Z}^n)$ in $\mathbb{Z}^m$.

We only show that $q(b_i) < N$ for $1 \leqslant i \leqslant n - r$. Denote by $\mathbf{F}_i$ the columns of $\mathbf{F}$.

Applications - Linear algebra over $\mathbb{Z}$

Suppose for simplicity that the first r columns of $\mathbf{F}$ are linearly independent.

- For $r < h \leqslant n$ we have a linear dependency among $F_1, \ldots, F_r$ and F_h.
- This dependency, say $x = (x_i)$, satisfies $x \in \ker f,\ x_h \neq 0$ and $x_i = 0$ for $i > r,\ i \neq h$.
- Cramer's rule implies that the x_i are $(r \times r)$ minors of $\mathbf{F}$ hence $|x_i| \leqslant r^{r/2} F^r$ by Hadamard's inequality. Therefore,

$$q(x) = ||x||^2 \leqslant (r+1) r^r F^{2r}.$$

- The $n - r$ vectors obtained in this way are independent so by c-reducedness we have

$$q(b_i) \leqslant c^{n-1} \lambda_i(L) \leqslant c^{n-1} (r+1) r^r F^{2r} < N.$$

Linear algebra over $\mathbb{Z}$

- Solving linear systems

Given $\mathbf{F}$ as before and $b \in \mathbb{Z}^m$ we want to solve $\mathbf{F}x = b$.

We let $N \gg M \gg 1$ be suitable large numbers and consider the lattice $L = \mathbb{Z}^n \times \mathbb{Z}$ with q given by

$$q(x, z) = ||x||^2 + M||z||^2 + N||\mathbf{F}x - zb||^2.$$

Given a c-reduced basis $\{w_1, \dots\}$ one has the following.

- Vectors $w_i = (x_i, z_i)$ with $q(w_i) < M$ form a basis for $\ker \mathbf{F}$.
- $\exists x : \mathbf{F}x = b \iff \exists w_j = (x_j, z_j)$ with $M \leqslant q(w_j) < 4M$.
- In this case $z_j = 1$, x_j is a solution and all solutions are of the form $x_j + \sum_{i<j} c_i x_i, \; c_i \in \mathbb{Z}$.

The idea of the Layered setting

- As $M, N \to \infty$ the reduced basis computed give us the desired solution.
- These constants are “weights” we give to certain directions of the lattice of special interest.
- With big enough weights we get solutions. But to give a lower bound for them is not easy in general.
- Further, being big, they can produce memory overhead.
- We could just as well work with “symbols” that are big enough.
- This is the ideas of the layered setting: We substitute these weights by symbols or, more precisely, infinities in a structured manner.

Totally ordered vector spaces

First step: generalize our ambient spaces, that is, Euclidean spaces.

Totally ordered vector spaces

Let V be a real vector space of finite dimension and $>$ a total order on V. We say that V is a totally ordered vector space if the following holds.

- For all $u, v, w \in V$ with $u > v$ we have $u + w > v + w$.
- For all $u \in V$, $u > 0$ and all $\lambda \in \mathbb{R}_{>0}$ we have $\lambda u > 0$.

Example

Let $V = \mathbb{R}^2$ with the antilexicographical order.

Theorem: Every total order on V is of the "above form", i.e., there is a basis $\{v_i\}$ s.t. $v_i \mapsto e_i$ is an o-isomorphism. We denote $V_i = \oplus_{j \leqslant i} \mathbb{R} v_j$.

Layered Euclidean spaces

Layered Euclidean spaces

A layered Euclidean space is a triple $(E, V, \langle\cdot,\cdot\rangle)$ where E and V are finite dimensional real vector spaces, V is totally ordered and $\langle\cdot,\cdot\rangle : E \times E \to V$ is a bilinear, symmetric map satisfying:

- For all $x \in E, x \neq 0$, we have $\langle x, x\rangle > 0$.
- For all $x, y \in E$, there is a $\lambda \in \mathbb{R}$ such that

$$\langle x, y\rangle \leqslant \lambda\langle y, y\rangle$$

Layered Euclidean spaces

Example

Let $E = \mathbb{R}^2, V = \mathbb{R}^2$ with the antilexicographical order and define

$$\langle x, y \rangle = (x \cdot \mathbf{B}_1 y, x \cdot \mathbf{B}_2 y)$$

where

$$\mathbf{B}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \mathbf{B}_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

One computes: $\langle e_1, e_1 \rangle = (1, 0)$, $\langle e_2, e_2 \rangle = (0, 1)$. So,

$$\forall \lambda \in \mathbb{R} \ : \ q(\lambda e_1) < q(e_2)$$

Layered Euclidean spaces

Layers

- Such a flag induces a filtration $\{0\} = E_0 \subseteq \cdots \subseteq E_n = E$ on E by subspaces which we call the layers of E:

$$E_i = \{x \in E \ : \ \langle x, x \rangle \in V_i\}$$

- An important fact is that $(E_i/E_{i-1}, V_i/V_{i-1}, \langle \cdot, \cdot \rangle)$ is a Euclidean space once we identify $V_i/V_{i-1} \simeq \mathbb{R}$.

Layered Euclidean spaces

Next, we look at the Gram-Schmidt process on which the concept of LLL reducedness depends.

- Perpendicularity: $x \perp y \iff \forall \lambda \in \mathbb{R}_{>0},\ |\langle x, y\rangle| \leqslant \lambda \langle y, y\rangle$.
- This amounts to say that $\langle x, y\rangle$ is an "order of magnitude" smaller than $\langle y, y\rangle$.
- Note that, in general, we can have $x \perp y$ but $y \not\perp x$:

Layered Euclidean spaces

Example

Let $E = \mathbb{R}^2, V = \mathbb{R}^2$ with the antilexicographical order and define

$$\langle x, y \rangle = (x \cdot \mathbf{B}_1 y, x \cdot \mathbf{B}_2 y)$$

where

$$\mathbf{B}_1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \mathbf{B}_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

One calculates: $\langle e_1, e_1 \rangle = \langle e_1, e_2 \rangle = (1, 0)$ and $\langle e_2, e_2 \rangle = (1, 1)$ so $e_1 \perp e_2$ but $e_2 \not\perp e_1$.

Layered Euclidean spaces

Thus, we have two related concepts:

- Perpendicularity: $x \perp y \iff \forall \lambda \in \mathbb{R}_{>0},\ |\langle x, y\rangle| \leqslant \lambda \langle y, y\rangle$.
- Orthogonality: $x \amalg y \iff x \perp y$ and $y \perp x$.

Gram-Schmidt

In the layered setting there is a trade-off: given a basis of E we can:

- Preserve the flag induced by that basis and achieve perpendicularity among the vectors of the resulting basis.

or:

- Achieve orthogonality if the flag structure is not important.

Layered lattices

Layered lattices

A layered lattice is a triple (L, V, q) where L is a finitely generated abelian group, V a finite dimensional, totally ordered, real vector space and $q : L \longrightarrow V$ is a map satisfying:

- For all $x \neq 0$, we have $q(x) \neq 0$.
- For all $x, y \in L$, $q(x+y) + q(x-y) = 2q(x) + 2q(y)$ holds.
- The set $q(L) \subseteq V$ is well-ordered.

Layered lattices

Theorem:

- Every layered lattice can be embedded in a layered Euclidean space.
- Reciprocally, a basis of E compatible with the layer structure of E induces a layered lattice.

Such a basis we call a *layered basis*.

Layered lattices

Counterexample

Take as in our first example $E = \mathbb{R}^2$, $V = \mathbb{R}^2$ with the antilexicographical order and $\langle x, y \rangle = (x \cdot \mathbf{B}_1 y, x \cdot \mathbf{B}_2 y)$ where

$$\mathbf{B}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \mathbf{B}_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

The vectors $b = (1, \sqrt{2})$ and e_2 form a basis for E but their $\mathbb{Z}$-span is not a layered lattice since for $m, n \in \mathbb{Z}$,

$$q(mb, ne_2) = (m^2, (n + m\sqrt{2})^2)$$

so $q(L)$ is not well-ordered.

Linear algebra over $\mathbb{Z}$ revisited

Recall: we have a matrix $\mathbf{F} \in M_{m\times n}(\mathbb{Z})$ representing an homomorphism $f : \mathbb{Z}^n \to \mathbb{Z}^m$ of groups. We want to compute the kernel and image of F. Let $V = \mathbb{R}^3$ and define $q : \mathbb{Z}^n \oplus \mathbb{Z} \to V$ by

$$q(x, z) = (||x||^2, ||z||^2, ||\mathbf{F}x - zb||^2).$$

- A reduced basis in the layered setting is just a layered basis which is reduced in each layer.
- An algorithm that computes an reduced basis in this setting solves our problem.
- The classical LLL algorithm and its invariants (size, successive distance, etc...) can be generalized to this setting.
- We already now that the corresponding algorithm is correct and finishes. We are now attempting to prove it is polynomial time.

Bibliography

[1] H. W. Lenstra Jr.
Lattices.
In *Surveys in algorithmic number theory*, Mathematical Science Research Institute Publications. Cambridge University Press, to appear.

[2] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász.
Factoring polynomials with rational coefficients.
Math. Ann., (261):515–534, 1982.

[3] H. Cohen.
A Course in Computational Algebraic Number Theory, volume 138 of *Graduate Texts in Mathematics*.
Springer, 1993.