Geometry of Numbers:

Field was developed by Minkowski in the late 19th century & combines number theory and geometry. Many of the important contributions are due to Minkowski.

Lattices:

An integer lattice, $\mathcal{L}_k \in \mathbb{R}^k$ is the integer combinations of k linearly independant vectors in $\mathbb{R}^k$.

The k vectors are the basis of $\mathcal{L}_k$, the parallelotope generated by the basis vectors is called the fundamental parallelotope.

volume of fundamental parallelotope = $d(\mathcal{L}_k)$

determinant of matrix made up of basis

The vectors in $\mathcal{L}_k$ are called lattice points and $\bar{0} \in \mathcal{L}_k$, always.

Def: C is a compact convex subset of $\mathbb{R}^k$

a) C is convex; $x, y \in C \Rightarrow xp + y(1-p) \in C$ $\quad 0 \le p \le 1$
b) C has at least one interior point
c) C is compact, i.e. closed & bounded

Def: A body is 0-symmetric if it is symmetric w.r.t. the origin.

Theorem: Let C be an o-symmetric convex body and $\mathcal{L}_k$ be a lattice, both in $\mathbb{R}^k$

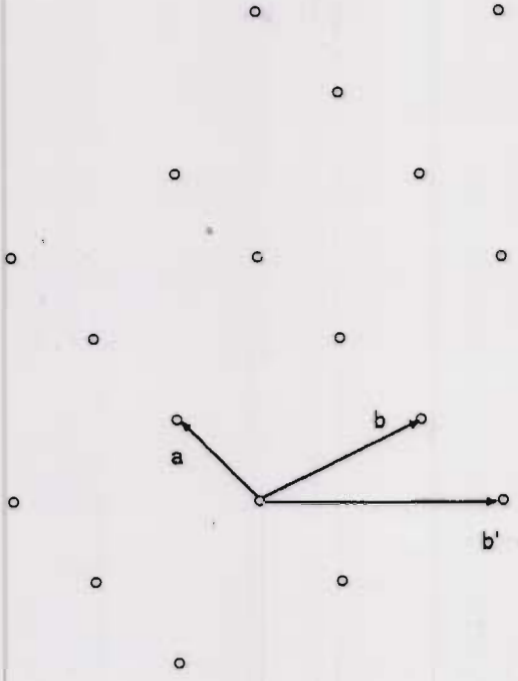
If $V(C) \geq 2^k d(\mathcal{L}_k)$

↑ Lebesgue measure

then C contains at least one pair of lattice points other than the origin

This means that regardless of $\mathcal{L}_k$, you can take a sphere or cube big enough to contain a point.

This is a lower bound to where points can be



Picture

Note: $(\bar{a}, \bar{b})$ are a basis, as is $(a, \bar{b}')$, in fact so is $(\bar{b}, \bar{b}')$!

Def: C, convex, $\in \mathbb{R}^k$ is a star body if the origin is an interior point of C

Def: Let C be a star body, $\mathcal{L}_k \in \mathbb{R}^k$, the minima

$\lambda_i = \lambda_i(C, \mathcal{L}_k)$, $i = 1, \dots, k$ of C w.r.t. $\mathcal{L}_k$

$\lambda_i = \inf\{\lambda > 0 \mid \lambda C$ contains i lin. indep. points of $\mathcal{L}_k\}$

Clearly $0 < \lambda_1 \le \dots \le \lambda_k$

⊛: Minkowski fundamental theorem can be rewritten:

Theorem: Let C be o-symmetric, convex, $\mathcal{L}_k \in \mathbb{R}^k$

$$\lambda_1^k V(C) \le 2^k d(\mathcal{L}_k)$$

volume of C that contains first point other than origin

expanded volume of lattice parallelotope where C contains one point from previous result

Theorem: (Minkowskiis second theorem); Let C be convex, o-symmetric, $\mathcal{L}_k \in \mathbb{R}^k$, then

$$\left(\prod_{i=1}^{k} \lambda_i\right) V(C) \le 2^k d(\mathcal{L}_k)$$

note $\lambda_i^k \le \prod_{i=1}^{k} \lambda_i$, so this is a sharper version.

If C is an o-symmetric ellipsoid, then can be replaced by $\gamma_k^k d(\mathcal{L}_k)$

γ_k are the Hermite constants.

k	γ_k^{2k}
1	1
2	$4/3$
3	2
4	4
5	8
6	$64/3$
7	64
8	256

$$\gamma_k^{2k} = \left(\frac{2}{\pi}\right)^k \Gamma\left(\frac{k}{2}+2\right)^2$$

$\Gamma(0) = \infty$, $\Gamma(1) = 1$

$\Gamma(x+1) = x\,\Gamma(x)$

$\Gamma(n) = (n-1)!$ $\quad n \in \mathbb{Z}^+$

$\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$

The Hermite constants are the best possible in the inequality

A related result of Minkowski is Theorem:

For any convex, o-symmetric C, $\mathcal{L}_k \in \mathbb{R}^k$

$$\frac{2^k}{k!}\, d(\mathcal{L}_k) \le \left(\prod_{i=1}^{k} \lambda_i\right) V(C)$$

Here equality hold if C is a cross polytope

$$C = \left\{ \bar{x} \;\middle|\; \sum_{i=1}^{k} |x_i| \le 1 \right\},$$ unit ball in l^1.

Def: Let C be a star body in $\mathbb{R}^k$, the polar body C^* of C, $C^* = \{ \bar{x} \mid \langle \bar{x}, \bar{y} \rangle \le 1 \;\forall\, \bar{y} \in C \}$

$\langle \bar{x}, \bar{y} \rangle$ is the Euclidean inner product

Properties of C^* with C a star body:

- C^* is a star body
- $C^{**} = C$
- $C \subset D \Rightarrow D^* \subset C^*$ if D, star
- If C is a polytope so is C^*

Theorem: Let C be convex, 0-symmetric, then

$$\frac{\kappa_k^2}{k^{k/2}} \leq V(C)\, V(C^*) \leq \kappa_k^2$$

$\kappa_k = \pi^{k/2} / \Gamma(\frac{k}{2}+1)$ is volume of unit ball in $\mathbb{R}^k$

Def: Let $\mathcal{L}_k \in \mathbb{R}^k$, then the dual lattice

$$\mathcal{L}_k^* = \{ \bar{x} \mid \langle \bar{x}, \bar{y} \rangle \in \mathbb{Z} \ \forall\, y \in \mathcal{L}_k \}$$

B is $k \times k$ with basis of $\mathcal{L}_k$, $d(\mathcal{L}_k) = |\det(B)|$

$\mathcal{L}_k$ is an integer combination of the columns of B, and so

$\mathcal{L}_k^*$ is an integer combination of the columns of $B^* = (B^t)^{-1}$, $B^{*t} B = I$ (why?)

$$|\det(B^{*t}B)| = 1 = |\det(B^{*t})|\, d(\mathcal{L}_k)$$
$$= |\det(B^*)|\, d(\mathcal{L}_k)$$
$$= d(\mathcal{L}_k^*)\, d(\mathcal{L}_k)$$

So $d(\mathcal{L}_k^*) = d(\mathcal{L}_k)^{-1}$

Theorem (Mahler): C is convex, o-symmetric, $\mathcal{L}_k \in \mathbb{R}^k$ and $\lambda_1, \dots, \lambda_k$ are as above. $\lambda_1^*, \dots, \lambda_k^*$ are the successive minima of C w.r.t. $\mathcal{L}_k^*$, then

$$1 \le \lambda_i \lambda_{k+1-i}^* \le (k!)^2 \quad \forall i = 1, 2, \dots, k$$

Note: for an o-symmetric ellipsoid we get

$$1 \le \lambda_i \lambda_{k+1-i}^* \le k^2 \quad i = 1, 2, \dots, k$$

From now on we assume C is the unit ball, and so $C^* = C$.

Def: When C is the unit ball, $\lambda_1^{\mathcal{L}_k}$ is the length of the shortest, nonzero vector, $b_1 \in \mathcal{L}_k$.

For $i > 1$, $\lambda_i^{\mathcal{L}_k}$ is the length of the shortest vector b_i, linearly indep. of $b_1, \dots, b_{i-1}$, over $\mathbb{R}$ (not $\mathbb{Z}$).

Examples: $\mathcal{L}_k \in \mathbb{R}^5$ $b_i = e_i$ $i = 1, \dots, 4$

$b_5 = (1, 1, 1, 1, 1) \cdot \frac{1}{2}$

Successive minima of $\mathcal{L}_R$ are $\lambda_i = 1$ $\forall i$ & correspond to b_i, $2b_5 - (b_1 + b_2 + b_3 + b_4) = e_5$. These vectors are linearly independent over $\mathbb{R}^5$ but do not form a basis for $\mathcal{L}^4$.

Need a more general concept to successive minima, called the reduced basis.

First, let's review quadratic forms:

Def: $\bar{\bar{A}}$ is a real, symmetric $k \times k$ matrix, then

$$g(x) = x^t A x = \sum_{1 \le i \le j \le k} a_{ij} x_i x_j \quad \text{is a (real) quadratic form}$$
$$= \langle x, Ax \rangle$$

$\mathbb{R}^k \xrightarrow{g} \mathbb{R}$

If $g(x) > 0 \quad \forall x \neq 0$ $g(x)$ is positive definite.

Let T be $k \times k$, $t_{ij} \in \mathbb{Z}$, $\det(T) = \pm 1$, this is an integer unimodular matrix & is like a rotation/reflection.

If $\exists$ T integer unimodular $\Rightarrow g_1(x) = g_2(Tx)$ $\forall x \in \mathbb{R}^k$ g_1 and g_2 are equivalent. We would like a reduced form for all equivalent quadratic forms.

Def: $g(x)$ is reduced a la Minkowski if $\forall i = 1, \ldots, k$

$$g(x_1, \ldots, x_k) \ge a_{ii} = g(\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0)$$

$\forall x \in \mathbb{Z}^k$ with $\gcd(x_i, \ldots, x_k) = 1$, this implies $a_{11} \le a_{22} \le \ldots \le a_{kk}$

Let $\mathcal{L}^k$ be a lattice w/ basis $b_1, \ldots, b_k$ & B is the matrix $[b_1, b_2, \ldots, b_n]$ columns. Define the

$$q(x) = x^t B^t B x = \langle Bx, Bx \rangle = x^T A x \text{ for } \mathcal{L}^k$$

A is symmetric, positive definite, $k \times k$.

Note, if A is symm. p.d. the B can uniquely be computed from A as a Cholesky factor.

Equiv. Def: $b_1, \ldots, b_k$ basis for $\mathcal{L}^k$ is reduced in the Minkowski sense if b_1 is the shortest (nonzero) vector in $\mathcal{L}^k$, and if b_i, $i = 2, \ldots, k$ is the shortest vector that can be extended to a basis of $\mathcal{L}^k$.

Minkowski reduced basis is successively the shortest vector $\Rightarrow$ a basis can be formed, and may not be unique.

Example: Hexagonal lattice in $\mathbb{R}^3$ with basis

$x = (1,0,0)$; $y = (\frac{1}{2}, \frac{\sqrt{3}}{2}, 0)$; $z = (\frac{1}{2}, \frac{\sqrt{3}}{6}, \frac{\sqrt{6}}{3})$

$|x| = |y| = |z| = \langle z, z \rangle = 1$; $\langle x, y \rangle = \langle x, z \rangle = \langle y, z \rangle = \frac{1}{2}$

Thus this is a Minkowski reduced basis; however

$x, y-z, z = (1,0,0), (0, \frac{\sqrt{3}}{3}, -\frac{\sqrt{6}}{3}); (\frac{1}{2}, \frac{\sqrt{3}}{6}, \frac{\sqrt{6}}{3})$ is also Minkowski reduced but not isomorphic as

$\langle x, y-z \rangle = 0$, $\langle x, z \rangle = \langle z-y, z \rangle = \frac{1}{2}$.

Theorem: Let b_i $i = 1 \ldots k$ be the Minkowski reduced basis $\mathcal{L}^k$, and λ_i be the successive minima. Then

$|b_i| = \lambda_i$ $1 \le i \le \min(4, k)$, $\lambda_i \le |b_i| \le (\frac{3}{4})^{\frac{i-1}{2}} \lambda_i$ $\min(4,k) \le i \le k$.

Another reduced basis, Korkin & Zolotarev, is based on Gram-Schmidt. Let $b_1, \dots, b_k$ be a basis for $\mathcal{L}^k$ with $|b_1| \le \dots |b_k|$, $\hat{b}_1, \dots \hat{b}_k$ be the G-S reduced basis:

$$b_i := \sum_{j=1}^{i} \mu_{ij} \hat{b}_j \quad i = 1, \dots, n$$

$\mu_{ij} = \langle b_i, \hat{b}_j \rangle / |\hat{b}_j|^2$, assume $\hat{b}_1 = b_1$

$\mu_{ii} = 1$, $\mu_{ij} = 0$ $i < j$. The basis $b_1, \dots, b_k$ is proper if $|\mu_{ij}| \le \frac{1}{2}$ $1 \le j < i \le k$

Def: A basis $b_1, \dots, b_k$ of $\mathcal{L}^k$ is reduced a la Korkin-Zolotarev if it is a proper basis, b_1 is a shortest nonzero vector $\in \mathcal{L}^k$, and if $b_i \in \mathcal{L}^k$ has component orthogonal to $b_1, \dots, b_{i-1}$ that is shortest while allowing $\{b_1, \dots b_i\}$ to be extended to a basis for $\mathcal{L}^k$.

The K-Z reduced basis will help us define the classic Lenstra-Lenstra-Lovász (LLL) reduced basis which is the preferred reduction.

Theorem: Every K-Z r-b $b_1, \dots, b_k$ satisfies

$$\frac{4}{i+3} \le \frac{|b_i|^2}{\lambda_i} < \frac{i+3}{4}, \quad i = 1, \dots, k$$

$A = [a_1, \ldots, a_k]$ is $k \times k$, then

$$|\det(A)| \leq \prod_{i=1}^{k} |a_i|$$ where equality holds when $\langle a_i, a_j \rangle = 0$ $i \neq j$

Since the Gram-Schmidt procedure produces orthonormal or orthogonal vectors, equality holds there, thus

Def: Let $B = [b_1, \ldots, b_k]$ be $k \times k$, with these the $\mathcal{L}^k$ bases, the orthogonal defect of $\mathcal{L}^k$ is

$$OD(b_1, \ldots, b_k) \triangleq \prod_{i=1}^{k} |b_i| \Big/ |\det(B)|$$

$OD(\cdot) \geq 1$, for K-Z $OD(\,) \leq k^{k}$

Minkowski $OD(\,) \leq 2^{O(k^2)}$

Polynomial Lattices

$\mathcal{L}^k \in GF\{q,z\}^k$ (k-dimensional vectorspace of polynomials w/coeffs $\in GF(q)$ or rational functions)

$\mathcal{L}^k$ is linear combinations, w/ polynomial coefficients of linearly independent basis vectors in $GF\{q,z\}^k$ There are countably many sets of bases for $\mathcal{L}^k$. The vectors of $\mathcal{L}^k$ are also called lattice points, 0 is a lattice pt.

For $f_i(z) \in GF\{q,z\}$, $f = (f_1, \ldots, f_k)$

$$|f| = \max_{1 \leq i \leq k} \nu(f_i)$$

Where $r(f_k)$ was defined before (largest nonzero power).

To define successive minima we need to define a star body, but here $C = X \Rightarrow |X| < 0$

Def: $\lambda_1 = |b_1|$, the shortest $\neq 0 \in \mathcal{L}^k$. λ_i is recursively defined to be $|b_i|$ shortest vector linearly independent from $b_1, \dots, b_{i-1}$, $i = 2, \dots, k$.

Thus $-\infty < \lambda_1 \leq \dots \leq \lambda_k$

Theorem: The vectors $b_1, \dots, b_k$ from the def. form a basis for $\mathcal{L}^k \in GF\{2\}$

$C_l^{(k)} = \{X \mid |X| < l, l \in \mathbb{Z}\}$ is a cube, contains finitely many pts. of $\mathcal{L}^k$, thus this basis always exists via exhaustion, is a reduced basis of $\mathcal{L}^k$

Minkowski #1: $B = [b_1, \dots, b_k]$, $k \times k$, basis $\mathcal{L}^k$.

$d(\mathcal{L}^k) = |\det(B)|$: $k\lambda_1 \leq d(\mathcal{L}^k)$

Minkowski #2: $\lambda_1 + \dots + \lambda_k \leq d(\mathcal{L}^k)$

$\mathcal{L}^{k*} = \{x \mid \langle x, y \rangle$ is a poly. $\forall y \in \mathcal{L}^k\}$

$\mathcal{L}^k$ is a lin. comb. of $[b_1, \dots, b_k] = B$

$\mathcal{L}^{\perp}$ is a lin. comb. of the columns of $(B^t)^{-1}$

$R \equiv (B^t)^{-1}$, $B^t B = I$ $d(\mathcal{L}^{\perp}) \cdot d(\mathcal{L}^k) = 0$

Theorem: $\lambda_1, \dots, \lambda_k$ of $\mathcal{L}^k$, $\lambda_1^{\perp}, \dots, \lambda_n^{\perp}$ of $\mathcal{L}^{\perp}$

$$\lambda_i \cdot \lambda_{k+1-i}^{\perp} = 0 \quad \forall i = 1, \dots, k.$$

Def: $OD(b_1, \dots, b_k) = \sum_{i=1}^{k} |b_i| - |\det(B)|$

Theorem: $b_1, \dots, b_k$ basis of $\mathcal{L}^k$ with

$OD(b_1, \dots, b_k) = 0$, $|b_1| \le \dots \le |b_k|$, then $\lambda_i = |b_i|$

Thus the K-Z & Minkowski reduced bases for polynomials are equivalent.

Basis Reduction Algorithms:

We begin to study basis reduction algorithms with SOLEQX (listed on next page), which finds all $x \in \mathbb{Z}^k$ satisfying $g(x) = x^T A x \le C > 0$.

This algorithm, due to Fincke & Pohst, is based on Cholesky factorization of A

$$g(x) = \sum_{i=1}^{k} g_{ii} \left(x_i + \sum_{j=i+1}^{k} g_{ij} x_j \right)^2$$

This algorithm can be used in

1. Compute shortest nonzero vector in $\mathcal{L}^k$
2. Enumerate all $x \in \mathbb{Z}^k \ni 0 < C' \le x^t A x \le C$
3. Compute the closest point $\in \mathcal{L}_k$ to a given pt.

RBASIS, Pohst & Zassenhaus, finds the Minkowski reduced basis using SOLVEQX to solve #2 above

Def. We define the follow partial ordering in $\mathbb{R}^+$

$$\bar{a} < \bar{b} \iff |\bar{a}| < |\bar{b}| \quad \forall \bar{a}, \bar{b} \in \mathbb{R}^k$$

We can use this partial ordering to order the bases of $\mathcal{L}^k$: $(b_1, \ldots, b_k) < (a_1, \ldots, a_k) \iff \exists i \ni |b_i| = |a_i|$ $\forall 0 \le i \le j-1 < k$ & $b_j < a_j$ where we assume in RBASIS that $|a_0| = |b_0| = 0$

Procedure SOLVEQX
input: A positive definite matrix A and a constant $c > 0$
output: All nonzero $\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{Z}^k$ satisfying $q(\mathbf{x}) \equiv \mathbf{x}^t A \mathbf{x} \le c$
begin
  Set $q_{ij} = a_{ij}$ $(1 \le i \le j \le k)$; read half
  for $i = 1, 2, \ldots, k-1$ **do**
    for $j = i+1, \ldots, k$ **do**
      $q_{ji} = q_{ij}$; $q_{ij} = q_{ij}/q_{ii}$; symmetrize + normalize
    end
    for $m = i+1, \ldots, k$ **do**
      for $l = m, \ldots, k$ **do**
        $q_{ml} = q_{ml} - q_{mi} q_{il}$; LU decomp
      end
    end
  end
  Set $q_{ij} = 0$ $(1 \le j < i \le k)$;
  Set $i = k$, $T_i = c$, and $U_i = 0$; solve the quadratic
  label0: $Z = \sqrt{T_i/q_{ii}}$; $UB(x_i) = \lfloor Z - U_i \rfloor$; $x_i = \lceil -Z - U_i \rceil - 1$;
  label1: $x_i = x_i + 1$;
  if $x_i > UB(x_i)$ **then**
    $i = i + 1$; **goto** label1;
  if $i > 1$ **then**
    $i = i - 1$; $U_i = \sum_{j=i+1}^{k} q_{ij} x_j$; $T_i = T_{i+1} - q_{i+1,i+1}(x_{i+1} + U_{i+1})^2$;
    goto label0;
  else
    if $\mathbf{x} \neq 0$ **then**
      print $\mathbf{x}$, $-\mathbf{x}$, and $q(\mathbf{x}) = c - T_1 + q_{11}(x_1 + U_1)^2$; **goto** label1;
end

SUCC (two pages on) computes successive minima for a lattice, is simpler than RBASIS, and uses SOLVEQX as a subroutine, this time for problem #3.

Note: The integer unimodular matrix U needed in RBASIS & SUCC can be constructed with the help of

Lemma

Let $\xi_1, \cdots, \xi_k$ be integers with $\gcd(\xi_1, \cdots, \xi_r) = d_r$, $r = 1, \cdots, k$. Also $\gcd(d_{r-1}, \xi_r) = d_r$, $d_1 = \xi_1$, let $d_r = u_r d_{r-1} + v_r \xi_r$ and $m_{11} = \xi_1 / d_k$. For $r = 2, \cdots, k$ we define

$$m_{rr} = u_r, \quad m_{rj} = -(\xi_j / d_{r-1}) v_r, \quad 1 \le j \le r-1, \quad m_{ir} = 0 \quad (2 \le r \le n-1)$$

Then $U_{n \times k} = (m_{ij})$ is a $k \times k$ integer unimodular matrix with

$$(d_k, 0, \cdots, 0) \, U = (\xi_1, \cdots, \xi_k)$$

Procedure RBASIS
input: $\mathbf{b}_1, \ldots, \mathbf{b}_k$ a basis of rank $k \ge 2$
output: $\mathbf{b}_1, \ldots, \mathbf{b}_k$ a Minkowski reduced basis
begin
  $r = 1$; $\Lambda_r = \mathbb{Z}\mathbf{b}_1$; $\hat{\mathbf{b}}_1 = \mathbf{b}_1$;
  while $r < k$ **do**
    Compute $\mu_{r+1,j} = \langle \mathbf{b}_{r+1}, \hat{\mathbf{b}}_j \rangle / |\hat{\mathbf{b}}_j|^2$ for $1 \le j \le r$;
    Set $\hat{\mathbf{b}}_{r+1} = \mathbf{b}_{r+1} - \sum_{j=1}^{r} \mu_{r+1,j} \hat{\mathbf{b}}_j$;
    Compute $\beta_{r+1,j}$ such that $\hat{\mathbf{b}}_{r+1} = \mathbf{b}_{r+1} - \sum_{j=1}^{r} \beta_{r+1,j} \mathbf{b}_j$;
    Set $B_{r+1} = \lfloor |\mathbf{b}_{r+1}| / |\hat{\mathbf{b}}_{r+1}| \rfloor$ and $\xi_{r+1} = 1$;
    while $\xi_{r+1} \le B_{r+1}$ **do**
      Set $B(\xi_{r+1}) = |\mathbf{b}_{r+1}|^2 - \xi_{r+1}^2 |\hat{\mathbf{b}}_{r+1}|^2$;
      Call **SOLVEQX** to compute $\mathcal{M}$ defined by
      $\mathcal{M} = \{\mathbf{x} = \sum_{i=1}^{r+1} \xi_i \mathbf{b}_i \in \Lambda_r + \mathbb{Z}\mathbf{b}_{r+1} \mid |\mathbf{x} - \xi_{r+1}\hat{\mathbf{b}}_{r+1}|^2 \le B(\xi_{r+1})\}$;
      if $\mathcal{M} \ne \phi$ **then**
        for $j = 1, \ldots, r+1$ **do**
          Let $\mathbf{x}_j$ be minimal in $\mathcal{M}$ such that $\gcd(\xi_j, \ldots, \xi_{r+1}) = 1$ and $\mathbf{x}_j < \mathbf{b}_j$;
          if no such $\mathbf{x}_j$ exists **then** $\mathbf{x}_j = 0$;
        end
        if $\mathbf{x}_j \ne 0$ exists for some j $(1 \le j \le r+1)$ **then**
          for each j with $\mathbf{x}_j \ne 0$ **do**
            Let U be a unimodular matrix of size $r + 2 - j$ over integers,
            whose first column is $(\xi_j, \ldots, \xi_{r+1})$;
            Transform the bases $\mathbf{b}_j, \ldots, \mathbf{b}_{r+1}$ into the new ones $\mathbf{b}'_j = \mathbf{x}_j$, $\mathbf{b}'_{j+1}$,
            $\ldots, \mathbf{b}'_{r+1}$, by using $(\mathbf{b}'_j, \ldots, \mathbf{b}'_{r+1}) = (\mathbf{b}_j, \ldots, \mathbf{b}_{r+1})U$;
            Update $\hat{\mathbf{b}}_i$ $(j \le i \le r+1)$ and the coordinates of $\mathbf{x}_i$ $(i > j)$;
          end
          Let j_0 be the smallest index for which a transformation occurred;
          if $j_0 \le r$ **then** $r = j_0$; $\Lambda_r = \mathbb{Z}\mathbf{b}_1 + \cdots + \mathbb{Z}\mathbf{b}_r$; **goto** label0;
        else $\xi_{r+1} = \xi_{r+1} + 1$;
      end
      $\Lambda_{r+1} = \Lambda_r + \mathbb{Z}\mathbf{b}_{r+1}$; $r = r + 1$;
    label0: **end**
end

Def: $b_1, \cdots, b_k$ is an LLL reduced basis with $\frac{1}{4} < \delta < 1$ if it is proper and if

$$\delta |\hat{b}_i|^2 \le |\hat{b}_{i+1} + \mu_{i+1,i} \hat{b}_i|^2, \quad i = 1, \ldots, k$$

and the "hat" are Gram-Schmidt orthogonal.

The LLL Reduced Basis Properties:

- $|b_1| \le 2^{(k-1)/4} \det(\mathcal{L}_k)^{1/k}$

LLL Reduced Basis: Props. Cont.

- $|b_1| \le 2^{(k-1)/2} \min\{|x| \mid x \in \mathcal{L}_k, x \neq 0\}$
- $\det(\mathcal{L}_k) \le |b_1| \cdots |b_k| \le 2^{k(k-1)/4} \det(\mathcal{L}_k)$

$$OD(b_1, \ldots, b_k) \le 2^{k(k-1)/4}$$

Theorem: Every LLL reduced basis $b_1, \ldots, b_k$ with δ:

$$\alpha^{1-i} \le |b_i|^2 / \lambda_i^2 \le \alpha^{k-1}, \quad i = 1, \ldots, k \qquad \alpha = (\delta - \tfrac{1}{4})^{-1}$$

This means that LLL bases have relatively short vectors.

In comparison w/ K-Z:

$$\hat{b}_{i,j} = \frac{\langle b_i, \hat{b}_j \rangle}{|\hat{b}_j|}$$

$b_{i,j} = 0, \; i < j$

$b_1, \ldots, b_k$ is a K-Z basis:

Procedure SUCC
input: $\mathbf{b}_1, \ldots, \mathbf{b}_k$ a basis of rank $k \ge 2$
output: $|\mathbf{y}_1|, \ldots, |\mathbf{y}_k|$ the successive minima
begin
  $r = 1$; $\Lambda_r = \mathbb{Z}\mathbf{b}_1$; $\hat{\mathbf{b}}_1 = \mathbf{b}_1$; $\mathbf{y}_j = \mathbf{b}_j$ $(1 \le j \le k)$;
  while $r < k$ **do**
    Compute $\mu_{r+1,j} = \langle \mathbf{b}_{r+1}, \hat{\mathbf{b}}_j \rangle / |\hat{\mathbf{b}}_j|^2$ for $1 \le j \le r$;
    Set $\hat{\mathbf{b}}_{r+1} = \mathbf{b}_{r+1} - \sum_{j=1}^{r} \mu_{r+1,j} \hat{\mathbf{b}}_j$;
    Compute $\beta_{r+1,j}$ such that $\hat{\mathbf{b}}_{r+1} = \mathbf{b}_{r+1} - \sum_{j=1}^{r} \beta_{r+1,j} \mathbf{b}_j$;
    Set $B_{r+1} = \lfloor |\mathbf{b}_{r+1}| / |\hat{\mathbf{b}}_{r+1}| \rfloor$ and $\xi_{r+1} = 1$;
    while $\xi_{r+1} \le B_{r+1}$ **do**
      Call **SOLVEQX** to compute $\mathbf{b} \in \Lambda_r + \xi_{r+1}(\mathbf{b}_{r+1} - \hat{\mathbf{b}}_{r+1})$ of shortest length;
      Set $\mathbf{x} = \mathbf{b} + \xi_{r+1} \hat{\mathbf{b}}_{r+1}$;
      Compute m_i $(1 \le i \le r+1)$ such that $\mathbf{x} = \sum_{i=1}^{r+1} m_i \mathbf{b}_i$;
      if $|\mathbf{x}| < |\mathbf{y}_{r+1}|$ **then**
        Let $j \in \{1, \ldots, r+1\}$ be minimal with $|\mathbf{x}| < |\mathbf{y}_j|$;
        Set $a = \gcd(m_j, \ldots, m_{r+1})$;
        Let U be a unimodular matrix of size $r+2-j$ over integers,
        whose first column is $(m_j/a, \ldots, m_{r+1}/a)$;
        Transform the bases $\mathbf{b}_j, \ldots, \mathbf{b}_{r+1}$ into the new ones $\mathbf{b}'_j = \frac{1}{a}(\mathbf{x} - \sum_{i=1}^{j-1} m_i \mathbf{b}_i)$,
        $\mathbf{b}'_{j+1}, \ldots, \mathbf{b}'_{r+1}$, by using $(\mathbf{b}'_j, \ldots, \mathbf{b}'_{r+1}) = (\mathbf{b}_j, \ldots, \mathbf{b}_{r+1})U$;
        Update $\hat{\mathbf{b}}_i$ $(j \le i \le r+1)$;
        Set $\mathbf{y}_j = \mathbf{x}$ and $r = j$;
        goto label0;
      else $\xi_{r+1} = \xi_{r+1} + 1$;
    end
    $\Lambda_{r+1} = \Lambda_r + \mathbb{Z}\mathbf{b}_{r+1}$; $r = r + 1$;
  label0: **end**
end

$$b_{i,i}^2 \le b_{i+1,i}^2 + b_{i+1,i+1}^2, \quad i = 1, \ldots, k-1$$

Since $|b_{i,i}|$ is the length of the shortest vector $\begin{pmatrix} 1 & \cdots \\ \vdots & \\ (k-i+1) & \end{pmatrix}^{\frac{k}{i+1}}$ and the basis is proper, $|b_{i,i}| \ge 2|b_{i+1,i}|$ or

$$\tfrac{3}{4} b_{i,i}^2 \le b_{i+1,i+1}^2 \iff b_{i,i}^2 \le b_{i+1,i+1}^2 + \tfrac{1}{4} b_{i,i}^2$$

which is LLL basis w/ $\delta = 1$, $\mu_{k+1,i} = \frac{1}{2}$

Below LLLBASIS computes the LLL basis for a given lattice where $\lceil x \rfloor$ is the nearest integer to x.

We use $\delta = 1 = 0.999$, $B_{max} = \max_{1 \le i \le k} |b_i|$. To hold the b_i's, μ_{ij} we may need $O(k \ln B_{max})$ bits for multiprecision.

Note: Schnorr proposed a Floating-Point version so no multiprecise arithmetic needed

Procedure LLLBASIS
input: $b_1, \ldots, b_k \in \mathbb{Z}^k$ a basis of rank $k \geq 2$
output: $b_1, \ldots, b_k$ a LLL basis with $\frac{1}{4} < \delta < 1$
begin
  $m = 2$;
  Compute the Gram-Schmidt coefficients μ_{ij} $(1 \leq j < i \leq k)$ and $|\hat{b}_1|^2, \ldots, |\hat{b}_k|^2$;
  while $m \leq k$ **do**
    for $j = m-1, \ldots, 1$ **do**
      if $|\mu_{m,j}| > 1/2$ **then**
        $b_m = b_m - \lceil \mu_{m,j} \rfloor b_j$;
        for $i = 1, \ldots, j$ **do**
          $\mu_{m,i} = \mu_{m,i} - \lceil \mu_{m,j} \rfloor \mu_{j,i}$;
        end
    end
    if $\delta |\hat{b}_{m-1}|^2 > |\hat{b}_m|^2 + \mu_{m,m-1}^2 |\hat{b}_{m-1}|^2$ **then**
      Swap b_m and b_{m-1}, where $\hat{b}_{m-1}$ is replaced by $\hat{b}_m + \mu_{m,m-1} \hat{b}_{m-1}$;
      $m = \max(m-1, 2)$;
    else $m = m + 1$;
  end
end

Polynomial Lattices: LENSTRA (next page) for lattices in $GF\{q, z\}^k$.

Prop: $b_1, \ldots, b_k$ basis of lattice in $GF\{q, z\}^k$ $[b_1, \ldots, b_k]$ = D, if the rows can be permuted so that the result:

$$|\bar{b}_{ii}| \leq |\bar{b}_{ij}| \quad 1 \leq i < j \leq k$$
$$|\bar{b}_{ii}| \geq |\bar{b}_{ij}| \quad " \quad "$$
$$|\bar{b}_{ii}| \geq |b_{ij}| \quad 1 \leq j < i \leq k$$

Proof: $b_1, \dots, b_k$ in this way satisfies $OD(b_1, \dots, b_k) = 0$ $\#|b_i|$ is the ith successive minimum, $i = 1, \dots, k$.

At each stage $m \in \{0, \dots, k\}$ (see code)

$|b_i| \le |b_j|$, $1 \le i < j \le m$, $|b_m| = |b_j|$, $m < j \le k$

$|b_{ii}| \ge |b_{ij}|$, $1 \le i \le m$, $i < j \le k$, $|b_{ii}| > |b_{ij}|$, $1 \le j < i \le m$

$\Rightarrow A$, $a_{ii} \neq 0$, $a_{ij} = 0$, $1 \le j < i \le m$, so A is nonsingular.

Procedure LENSTRA
input: $\mathbf{b}_1, \dots, \mathbf{b}_k \in GF[q, z]^k$ a basis of rank $k \ge 2$
output: $\mathbf{b}_1, \dots, \mathbf{b}_k$ a reduced basis permuted so that (2.4)–(2.6) hold
begin
  $m = 0$; $|\mathbf{b}_0| = -\infty$;
  while $m < k$ **do**
    Renumber $\{\mathbf{b}_{m+1}, \dots, \mathbf{b}_k\}$ in such a way that $|\mathbf{b}_{m+1}| = \min_{m+1 \le i \le k} |\mathbf{b}_i|$;
    if $m > 0$ **then**
      Construct $A = (a_{ij})_{1 \le i,j \le m}$ be an $m \times m$ matrix such that $a_{ij} \in GF(q)$
      be the coefficient of $z^{|\mathbf{b}_i|}$ in b_{ij} for $1 \le i \le m+1$ and $1 \le j \le m$;
      Let $\mathbf{x} = {}^t(x_1, \dots, x_m)$ and $\mathbf{b} = {}^t(a_{m+1,1}, \dots, a_{m+1,m})$ be in $GF(q)^m$;
      Solve $A\mathbf{x} = \mathbf{b}$;
    Put $\hat{\mathbf{b}}_{m+1} = \mathbf{b}_{m+1} - \sum_{i=1}^{m} x_i \mathbf{b}_i z^{|\mathbf{b}_{m+1}| - |\mathbf{b}_i|}$;
    if $|\hat{\mathbf{b}}_{m+1}| = |\mathbf{b}_{m+1}|$ **then**
      $\mathbf{b}_{m+1} = \hat{\mathbf{b}}_{m+1}$;
      Permute the coordinates of $\mathbf{b}_1, \dots, \mathbf{b}_k$ so that $|b_{m+1,m+1}| = |\mathbf{b}_{m+1}|$;
      $m = m + 1$;
    else
      $\mathbf{b}_{m+1} = \hat{\mathbf{b}}_{m+1}$;
      $m = \max\{l \mid |\mathbf{b}_l| \le |\mathbf{b}_{m+1}|, l = 0, 1, \dots, m\}$;
  end
end

This algorithm runs in $O(k^3 B_{max}(OD(b_1, \dots, b_k) + 1))$ unit is operation in $GF(q)$ $B_{max} = \max |b_i|$, since $OD(b_1, \dots, b_k) \le k B_{max}$: $O(k^4 B_{max}^2)$,

but Gaussian elimination would be $O(k^4 B_{max}^3)$