H.W. Lenstra Jr. (Lattices)

1) A lattice is a discrete subgroup of a Euclidean vector space.

2) A subgroup L of $\mathbb{R}^m$ is a lattice $\Leftrightarrow$ there are n linearly independent vectors $b_1, b_2 \dots b_n \in \mathbb{R}^m$ with $L = \sum_{i=1}^{n} \mathbb{Z} b_i$

rank $rk(L)$ is n.

abstract: L lattice = L abelian group
1) $q : L \to \mathbb{R}$
$q(x+y) + q(x-y) = 2q(x) + 2q(y)$
3) $\{x \in L \mid q(x) \leq n\}$ is finite
2) $q(x) \neq 0$ for $x \neq 0$

3) Examples of lattices

(a) K be an algebraic number field and $L \subset K$ a finitely generated additive subgroup

eg $\mathbb{Z}_K$ = integers of K $\quad q(x) = \sum_{\sigma} |\sigma x|^2$

σ field embeddings $K \to \mathbb{C}$

Not easy to know a basis!

(b) E elliptic curve over $\mathbb{Q}$ $\quad L = E(\mathbb{Q}) / E(\mathbb{Q})_{Tor}$.

(c) K be an algebraic number field, μ the group of roots of unity in K, and $L = \mathbb{Z}_K^* / \mu$

$\Rightarrow$ L is a lattice with $q(\bar{u}) = \sum_{\sigma} (\log |\sigma u|)^2$

σ ranging over field embeddings $K \to \mathbb{C}$

How to specify a lattice to a computer?

Method 1 give a real (rational) $m \times n$ matrix B of rank n.

The lattice L spanned by colums!

$q(x) = \sum x_i^2$ for $x = (x_i)_{i=1}^{m}$

and elements of L are represented as elements of $\mathbb{R}^m$ (or $\mathbb{Q}^n$)

Method 2

Give a real (rational) positive definite symmetric $n \times n$ matrix A.

$\Rightarrow L = \mathbb{Z}^n$ with $q(x) = x^T A x$.

CONVERSION: Given B (method 1) take $A = B^T B$.

VOW Given A how to find B?

Thm: $\exists$ a polynomial time alg. Given A finds a rational $m \times n$ matrix B with $A = B^T B$

Question: Can one also achieve $m \leq n+3$ even for $n=1$?

IMPORTANT Questions:

1) Given L, find $x \in L$ $x \neq 0$ with $q(x)$ smallest possible. ← THE homogeneous approximation problem

2) Given $L \subset E$, $x \in E$ find $y \in L$ with $\langle x-y, x-y \rangle$ smallest possible ← The inhomogeneous approximation

Applications

1) $L = \mathbb{Z}^2$, $q(x,y) = (N(x-\alpha y))^2 + (y/N)^2$ $\alpha \in [0,1]$ N large

A "small" non-zero vector in L gives a good rational approximation x/y to α.

Similarly can be used to give simultaneous approximations $x_1/y, x_2/y, \ldots, x_k/y$ to k given real numbers $\alpha_1, \ldots, \alpha_k$

2) Le- $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ are they linearly dependent over the rationals?

Use $L = \mathbb{Z}^n$ $q(x) = \sum x_i^2 + \left(N \cdot \sum x_i \alpha_i\right)^2$

for $X = (x_i)_{i=1}^n$ with N Large.

3) Given Lattice $L \subset E$ with
$\operatorname{rk}(L) = \dim E$ find $x \in E$ with
$L \subset (\mathbb{R}x)^\perp + \mathbb{Z}x$
and $\langle x, x\rangle$ largest possible.

{ Distribute points in Lattice in sequence of parallel "planes"

Useful in IP! ← (why?)

Define L^* dual of $L = \{ x \in E : \langle x, L\rangle \subset \mathbb{Z} \}$

$(L^*)^* = L$

If $E = \mathbb{R}^n$, L spanned by the columns of non-singular matrix B $\Rightarrow$ L^* is spanned by the columns of B^{-T}

NOTE: Let $x \in E$, $x \neq 0$. Put $x' = x/\langle x, x\rangle$

Then $\mathbb{R}x' = \mathbb{R}x$

$$\langle x, x'\rangle = \frac{1}{\langle x, x\rangle}$$

$$(\mathbb{R}x')^\perp = (\mathbb{R}x)^\perp$$

$$\langle x', x\rangle = 1$$

$$(\mathbb{R}x)^\perp + \mathbb{Z}x = \{ y \in E : \langle x', y\rangle \in \mathbb{Z} \}$$

It follows that one has

$$L \subset (\mathbb{R}x)^\perp + \mathbb{Z}x \iff x' \in L^*$$

My problem of finding x with $L \subset (\mathbb{R}x)^\perp + \mathbb{Z}x$ and $\langle x, x\rangle$ largest possible amounts to the homogeneous approximation for L^*

Definition: The determinant of a lattice

$$L = \sum_{i=1}^{n} \mathbb{Z} b_i \subset E$$

$$d(L) = \sqrt{\det\left(\langle b_i b_j \rangle\right)}$$

equivalently

1) $d(L) = \mathrm{Vol}\left(E/L\right)$ if $\dim E = n$

- $\#\{x \in L,\ q(x) \le r\} \sim \dfrac{r^{n/2} \cdot \pi^{n/2}/(n/2)!}{d(L)}$

for $r \to \infty$

Thm (Minkowski) Each non-zero lattice L contains a non-zero element x with

$$q(x) \le (\mathrm{rk}\, L) \cdot d(L)^{2/\mathrm{rk}\, L}$$

proof: Let $L \subset \mathbb{R}^n$ $n = r_* L$

$\ell = \min\{q(x) : x \in L,\ x \neq 0\}$ and $C \subset \mathbb{R}^n$ an open n-cube of diameter $\sqrt{\ell}$.

$$\mathrm{VOL}(C) \le \mathrm{VOL}(E/L) = d(L)$$

Corollary: If $L \subset E$ is a lattice with $\dim E = rkL > 0 \Rightarrow$

$\exists\, x \in E \quad x \neq 0$ with $L \subset (\mathbb{R}x)^{\perp} + \mathbb{Z}x$ and

$\langle x, x \rangle \geq (rkL)^{-1} \cdot d(L)^{2/rkL}$

proof Apply Minkowski's theorem to L^*

and use that $d(L^*) = d(L)^{-1}$

Def: Any subgroup of a lattice has lattice structure we call it a SUBLATTICE

$K = (\mathbb{R}K) \cap L$

We say $K \subset L$ is a pure sublattice if L/K has no element of finite order

Orthogonal lattices: Let $L \subset E$ be lattice $K \subset L$ a pure sublattice

$\Rightarrow L/K$ embeds by projection in $(\mathbb{R} \cdot K)^{\perp}$

and it becomes a lattice

Pf: $\bar{x} = x + K \in L/K$

$\langle \bar{x}, \bar{x} \rangle$ is the minimum of all

$\langle y, y \rangle \quad y \in x + (\mathbb{R} \cdot K)$

One has

$$d(L) = d(K) \cdot d(L/K)$$

Flags

A flag F of a lattice L of rank n is

$$0 = F_0 \subset F_1 \subset \dots \subset F_n = L$$

of proper sublattices of L with $\operatorname{rk} F_i = i$

Observe

If $L = \sum \mathbb{Z} b_j$ then $F_i = \sum_{j \le i} \mathbb{Z} b_j$ yields a

flag, and every flag is obtained in this way.

Specifying a basis to specify flag.

It is often desirable to require that the unique

dual vectors

$b_i^* \in (R \cdot F_{i-1})^\perp \cap (b_i + R \cdot F_{i-1})$ satisfy

$b_i - b_i^* \in \sum_{j<i} \left[-\frac{1}{2}, \frac{1}{2}\right] (b_j^*)$

Def: The size of a flag $F = (F_i)_{i=0}^n$ is

$$s(F) = \prod_{i=1}^{n} d(F_i)$$

Theorem: Let L be a lattice and $r \in \mathbb{R}$, then L

has only finitely many flags with $s(F) \le r$

(hint use Minkowski's theorem.

Def: The successive distances

$\ell_1(F), \ell_2(F), \dots, \ell_n(F)$

of a flag are defined by

$$\ell_i(F) = d(F_i / F_{i-1})$$

If $F_i = \sum_{j \le i} \mathbb{Z} b_j$ then $\ell_i(F) =$ the distance of b_i to $\sum_{j<i} \mathbb{R} b_j$ which $= \langle b_i^*, b_i^* \rangle^{1/2}$

Consider $d(L) = \prod_{i=1}^{n} \ell_i(F)$

$s(F) = \prod_{i=1}^{n} \ell_i(F)^{n+1-i}$

A good flag $s(F)$ is small and the sequence $\ell_1(F), \dots, \ell_n(F)$ does not decrease too steeply

Thm: Let $c \in \mathbb{R}$, $c \ge 1$ and let F be a flag with

$$\ell_i(F)^2 \le c\, \ell_{i+1}(F)^2$$

for $1 \le i < n$, and $F_1 = \mathbb{Z} b_1$

$$\Rightarrow \quad q(b_1) \le c^{(n-1)/2} \cdot d(L)^{2/n}$$

$$q(b_1) \le c^{n-1} \cdot q(x)$$

for all $x \in L$, $x \neq 0$

b_1 is an "approximation" to the solution of the homogeneous approximation thm

It also helps to "approximate" a solution to inhomogeneous problems:

Thm Let $c \in \mathbb{R}$, $c \geq 1$ and $F = (F_i)$ flag [illegible] $l_i(F)^2 \leq c \cdot l_{i+1}(F)^2$

[illegible] Let $F_i = \sum_{j<i} \mathbb{Z} b_j$ and $b_i^* \in (\mathbb{R} \cdot F_{i-1})^{\perp} \cap (b_i + \mathbb{R} \cdot F_{i-1})$

[illegible] each $x \in E$ $\exists$ a unique $y \in L$ [illegible]

$$x - y \in \sum_i \left(-\tfrac{1}{2}, \tfrac{1}{2}\right] \cdot b_i^*$$

[illegible]

$$\langle x-y, x-y \rangle \leq \frac{c^n - 1}{c - 1} \cdot \langle x-z, x-z \rangle$$

for all $z \in L$

Exercise!

Thm Any lattice has a flag with $l_i(F)^2 \leq \frac{4}{3} l_{i+1}(F)^2$ [illegible] $0 < i < n = \operatorname{rk} L$

This statement is wrong when $\frac{4}{3}$ is replaced by any smaller constant.

Lemma: If a flag F has

$$\ell_{j+1}(F)^2 < \frac{3}{4} \cdot \ell_j(F)^2$$

for some $j \Rightarrow$ one can find a flag F'

with $s(F') < s(F)$

Moreover $F' = (F_n')_{n=1}^{n}$ can be chosen so that

$F_i' = F_i$ for $i \neq j$

Reduce L by F_{j+1}/F_{j-1} reduces to case $\mathrm{rk} L = 2$

The guts!

Def: L lattice $\mathrm{rk} L = n$. The reduction graph

Γ_L has sets of flags of L as vertices

Edge from $F = (F_i)_{i=0}^{n}$ to $F' = (F_i')_{i=0}^{n}$

$\Leftrightarrow \exists j$ with

a) $F_i' = F_i \quad \forall i \neq j$

b) $F_j' \neq F_j = F_{j+1}$

c) $s(F')$ is minimal given a, b

d) $s(F') < s(F)$

... length of the arc $F \to F'$ is defined ... $\log(s(F)/s(F'))$

... exhibit an isomorphism $\Gamma(L) \cong \Gamma(L^*)$ ... labeled graphs that preserves arc lengths

Theorem ... $\exists\, B(n) > 0$ such that any directed ... $F \to \cdots \to F'$ in $\mathcal{F}(L)$ has length $\geq B(n) + \log(s(F)/s(F'))$.

... starting at any F one finds after "not too many steps" a flag F' with

$$\ell_i(F')^2 \leq \frac{4}{3}\,\ell_{i-1,i+1}(F')^2$$

for $0 < i < n$

Proof ... can take c_3

$$B(n) = \left(\tfrac{4}{3}\right)^{n^3/12n-1}$$ ← Bad for not fixed n !!

... a positive real number ℓ

$\Gamma_\ell(L)$ subgraph of $\Gamma(L)$

... delete edges ...

[illegible]

[illegible] For each $c > 4/3 \Rightarrow \exists$ a polynomial [illegible] algorithm that produces a flag that is [illegible]

SUBSET SUM (knapsack)

[illegible] Given $S, a_1, \ldots, a_n$ find integers

$$\sum_{i=1}^{n} x_i a_i$$

$x_i = 0$ or 1 $\forall i$

[illegible] algorithm $n 2^{n/2}$

[illegible] Alice publishes $a_1, \ldots, a_n$

Bob sends $S = \sum x_i a_i$ $\quad x = 0, 1$

transmit S over a public channel...

[illegible] $a_1, \ldots, a_n$ must have "structure"

Merkle-Hellman $\quad b_1 \simeq 2^n \quad b_j > \sum^{j-1} b_i$

$b_n \approx 2^{2n}$

Alice chooses M & W $\quad M > \sum_{i=1}^{n} b_i \quad (M, W) = 1$

$a_j \equiv b_j w \pmod{M} \quad 0 < a_j < M$

$a_1' \dots a_n'$ is permutation a_j

$$c \equiv s w^{-1} \pmod{M} \quad 0 \le c < M$$

$$\equiv \sum_{j=1}^{n} x_j a_j w^{-1} \pmod{M}$$

$$\equiv \sum x_j a'_{\pi(j)} w^{-1} \pmod{M}$$

$$\equiv \sum x_j b_{\pi(j)} \pmod{M}$$

$M > \sum b_i$

$$c = \sum x_j b_{\pi(j)}$$

$b_1 \dots b_n$ super increasing.

Pomerance (Primality)

Mathematica is happy with "high probability" primality...

Thm: Miller - Oestlé - Bach

If n is an odd composite there is some r, $1 < r < 2\log^2 n$ such that n is not a strong pseudoprime base r

↑ Needs Extended Riemann Hypothesis....

Thm: (Lucas, Pocklington)

Suppose $F \mid n-1$, $F > \sqrt{n}$, $a^{n-1} \equiv 1 \bmod n$

$\gcd(a^{(n-1)/q} - 1, n) = 1$ for all primes $q \mid F$ ← hard part

$\Rightarrow n$ is prime.

Proof: Let p be a prime factor of n.

$\Rightarrow a^{n-1} \equiv 1 \pmod p$

and $a^{(n-1)/q} \not\equiv 1 \bmod p$ for all $q \mid F$.

$\Rightarrow$ order of $a^{(n-1)/F}$ is F in $\mathbb{Z}_p^*$.

so $F \mid p-1$ in particular $p > F > \sqrt{n}$

↑ DONE.

Thm (Hendrik Lenstra) Suppose I, F are integers with $F > \sqrt{n}$

$F \mid n^I - 1$ suppose $f, g \in \mathbb{Z}_n[x]$ $\deg f = I$, f monic

(i) $g^{n^I} \equiv 1 \pmod f$

(ii) $g^{(n^I-1)/q} - 1$ is coprime to f for every prime $q \mid F$.

(iii) Each of the elementary polynomials in $g, g^n, \ldots, g^{n^I-1} \pmod f$ are elements of $\mathbb{Z}_n$

(iv) Each $(n^j \bmod p)$ is not a proper factor of n $j = 1 \ldots I-1$

$\Rightarrow n$ is prime