Notes on Lattices and Integer Linear Algebra

Brandon Dutra

Department of Mathematics, University of California, Davis
E-mail address: bedutra@ucdavis.edu

Contents

CHAPTER 1

Book: Integer Points in Polyhedra

Most text/math came from [1].

Definition 1. Let V be a vector space, then $\Lambda \subset V$ is a lattice if

(1) Λ is an additive subgroup of V w.r.t +.
(2) Λ is discrete: A) every bounded set B in V, the intersection $B \cap \Lambda$ is finite OR B) there is a neighborhood of the orgin that does not contain any lattice point other than the origin.
(3) $span(\Lambda) = V$.

Lemma 2. *Let $\Lambda \subset V$ be a lattice and $L \subset V$ a vector subspace spanned by some points from Λ. Then among all the lattice points that are not in L there exist a bpoint v closest to L. That is, ther exist a point v such that*
$v \in \Lambda - L; dist(V, L) \leq dist(w, L)\ \forall w \in \Lambda - L$

Proof. Let k = dim(L), and let $u_1, \ldots, u_k$ be a basis for L consisting of lattice points in Λ. Define (not this is not the fundamental parallelepiped b/c of the 1.

$$\Pi = \{\sum_{i=1}^{k} \lambda_i u_i : 0 \leq \lambda_i \leq 1\}$$

Pick a ρ large enough so that $\Pi_p = \{x \in V : dist(x, \Pi) \leq \rho\}$ contains a lattice point not in L. B/c Λ is discrete $\Pi_p \cap \Lambda$ is finite. Out of all the points in $\Pi_p \cap (\Lambda - L)$ let v be the closest to Π. It is clear $dist(v, \Pi) \leq dist(a, \Pi)\ \forall a \in \Lambda - L$. But WTS $dist(v, L) \leq dist(w, L)\ \forall w \in \Lambda - L$. For a contradiction assume such a w exist with >.

Let $x \in L$ be the closest point to w (so then dist(w, x) = dist(w, L)). Because $x \in L$ write x in the basis:

$$x = \sum \alpha_i u_i = u + y\ where$$
$$u = \sum \lfloor \alpha_i \rfloor\ u_i$$
$$y = \sum \{\alpha_i\} u_i$$

Note that $u \in \Lambda \cap L; y \in \Pi; w - y \in \Lambda - L$. Thus

$$\begin{aligned} dist(w-u,\Pi) &\leq dist(w-u, x-u)(b/cx - u \in \Pi) \\ &= dist(w,x) \\ &= dist(w,L) \\ &< dist(v,L) \text{assumption for a contradiction} \\ &\leq dist(v,\Pi). \end{aligned}$$

but v (not w-u) is the closest point to Λ, a contradiction. □

Corollary 3. *Let $\Lambda \subset V$ be a lattice and $L \subset V$ a vector subspace spanned by some points from Λ. Let $V = L \bigoplus W$, and $pr : V \to W$ be the project with the kernel L. Then $pr(\Lambda)$ is a lattice in W.*

Proof. It is clear $\Lambda_1 = pr(\Lambda)$ is an additive subgroup in W which spans W as a vector space. By the last lemma, there exist the minimum positive distance from a point in $\Lambda - L$ to L. So there exist the minimum positive distance from a point in $\Lambda_1 - \{0\}$ to the origin in W. This shows that Λ_1 is discrete. Not that if L is not spanned by lattice points, then $\Lambda_1 = pr(\Lambda)$ may get everywhere dense in W, this is why we assume L is spanned by lattice points. □

Theorem 4. *(The basis representation) let dim(V) = d ¿ 0.*

1)There exist vectors $u_1, \ldots, u_d$ in Λ such that every $u \in \Lambda$ admits a unique decomposition:

$$u = \sum m_i u_i \text{ where } m_i \in \mathbb{Z}$$

The set $u_i, \ldots, u_d$ is called a basis for Λ.

2) Let $u_1, \ldots, u_d$ be a basis for Λ and let

$$\Lambda = \{\sum m_i u_i \text{ where } m_i \in \mathbb{Z}\}$$

then $\Lambda \subset V$ is a lattice.

Proof. 1) By induction on d. If d = 1, V = $\mathbb{R}$. B/c Λ is discrete, pick the smallest positive number $a \in \Lambda$. Show every point in the lattice is a multiple of a: let x be a lattice point and write $x = ma, m \, in\mathbb{R}$. Then $x = \lfloor m \rfloor a + \{m\}a$. By subtraction, $\{m\}a \in \Lambda$ but $\{m\} < 1$, so $\{m\} = 0$. So every lattice point is a integer mult. of a.

Let d ¿ 1. Pick any d-1 linearly indepen. points and let L be the subspace spanned by those points. Hence dimL = d-1 and $\Lambda_1 = \Lambda \cap L$ is a lattice in L. B y the induction hypothesis, there is a basis $u_1, \ldots, u_{d-1}$ of Λ_1. By a lambda above, there is a vector $u_d \in \Lambda - L$ such that $dist(u_d, L) \leq dist(u, L)\ \forall u \in \Lambda - L$.

claim: $u_1, \ldots, u_{d-1}, u_d$ is a basis of Λ. Pick any $u \in \Lambda$ write u as a linear comb: $u = \sum^d \alpha_i u_i$. WTS $\alpha_d \in \mathbb{Z}$.

For a contradiction, assume $\alpha_d \notin \mathbb{Z}$ *so* $\{\alpha_d\} > 0$. Then the point $v = u - \lfloor \alpha_d \rfloor u_d = \{\alpha_d\}u_d + \sum^{d-1} \alpha_i u_i \in \Lambda - L$. Then

$$dist(v, L) = dist(\{\alpha_d\}u_d, L) = \{\alpha_d\}dist(u_d, L) < dist(u_d, L)$$

, a contradiction. Now, $\alpha_1, \ldots, \alpha_{d-1}$ are integers too because the point $u - \alpha_d u_d$ is a lattice point.

2) Let $T : \mathbb{R}^d \to V; T(\alpha_1, \ldots, \alpha_d) = \sum^d \alpha_i u_i$. Then $\Lambda = T(\mathbb{Z}^d)$. B/c T is an invertible linear transformation, Λ is a discrete additive subgroup of V which spans V. □

Lemma 5. *Let* Π *be a fundamental parallelepiped (1/2 open) of* Λ. *Then every point* $x \in V$ *can be uniquely written as* $x = y + u$ *where* y *is in the fun. parallelepiped and* u *is a lattice point.*

Proof. Let $u_1, \ldots, u_d$ be a basis for the lattice. that spans the parallelepiped. Write $x = \sum a_i u_i; a_i \mathbb{R}$. Write $y = \sum \{a_i\}u_i; u = \sum \lfloor a_i \rfloor u_i$.

Now show this is unique. Let $x = y_1 + u_1 = y_2 + u_2$, then $y_1 - y_2 = u_2 - u_1 \in \Lambda$ So $y_1 - y_2$ can be written as an integer comb. of the lattice basis vectors, AND $u_2 - u_1$ is written as a fractional < 1 comb. of the lattice basis, hence $u_2 - u_1 = 0$. And $y = y, u = u$ follows.

□

Theorem 6. *All the fundamental parallelepipeds (1/2 open)* Π *of* Λ *have the same volume, called the determinant of* Λ *written* $det\Lambda$. *Let* B_ρ *be a all of a radius of* ρ *centered at the origin. Then*

$$lim_{p\to\infty} \frac{|B_\rho \cap \Lambda|}{volB_\rho} = 1/det\Lambda$$

Proof. Pick a fund. para. Π. the translates $\Pi + u : u \in \Lambda$ cover V w/o overlapping. Let $\Pi \subset B_\alpha$ for some $\alpha > 0$. Pick $\rho > \alpha$, and let $X_\rho = \cup_{u \in B_\rho}(\Pi|u)$. Then it is clear $X_\rho \subset B_{\rho+\alpha}$.

Now show $B_{\rho-\alpha} \subset X_\rho$. Let $x \in B_{\rho-\alpha}$, the it has to be covered by some translation $\Pi + u$ for $u \in \Lambda \subset B_\rho$. Then

$$volB_{\rho-\alpha} \leq volX_\rho = |B_\rho \cap \Lambda| vol\Pi \leq volB_{\rho+\alpha}$$

Because

$$lim_{\rho\to\infty} \frac{volB_{\rho+/-\alpha}}{volB_\rho} = 1$$

we have that

$$lim_{p\to\infty} \frac{|B_\rho \cap \Lambda|}{volB_\rho} = 1/vol\Pi$$

More generally, for any a in V with $\alpha = \|a\|$, we have the containment

$$a + (B_{\rho-\alpha} \cap \Lambda) \subset B_\rho \cap (a + \Lambda) \subset a + (B_{\rho+\alpha} \cap \Lambda)$$

Which implies

$$|B_{\rho-\alpha} \cap \Lambda| \leq | \subset B_\rho \cap (a+\Lambda)| \leq | \subset (B_{\rho+\alpha} \cap \Lambda|$$

and hence

$$lim_{\rho\to\infty} \frac{|B_\rho \cap (a+\Lambda)|}{volB_\rho} = 1/det\Lambda$$

□

Theorem 7. *(Volume and lattice point count). Let $\Lambda_o \subset \Lambda$ be lattices and let Π be a fund. paallelepiped of λ_o. Then the sets $\Pi \cap \Lambda$ contains each coset Λ/Λ_o representative exactly once. Also*

$$|\Pi \cap \Lambda| = |\Lambda/\Lambda_o| = det\Lambda_o/det\Lambda$$

PROOF. By lemma 5 every $x \in \Lambda$ has a unique representation $x = y+u; y \in \Pi; u \in \Lambda_o$. But $y \in \Lambda$ so $y = xmod\Lambda_o$. Thus $|\Pi \cap \Lambda| = |\Lambda/\Lambda_o|$.

Let S be a set of all the cosets, $|S| = |\Lambda/\Lambda_o|$. Because $\Lambda = \cup_{a\in S}(a+\Lambda_o)$, we have that $|B_\rho \cap \Lambda| = \cup_{a\in S}(B_\rho \cap (a+\Lambda_0))$.

By theorem 6, we have that

$$lim_{\rho\to\infty} \frac{|B_\rho \cap (a+\Lambda_o)|}{volB_\rho} = 1/det\Lambda_o lim_{\rho\to\infty} \frac{|B_\rho \cap \Lambda|}{volB_\rho} = 1/det\Lambda.$$

Then but each $a+\Lambda_0$ is disjoint and

$$lim_{\rho\to\infty} \frac{\cup_{b\in S} B_\rho \cap (b+\Lambda_o)}{B_\rho \cap (a+\Lambda_0)} = det\Lambda_0/det\Lambda$$

for any fixed $a \in S$. Hence $B_\rho \cap (a+\Lambda_0)$ must be the same for each a, hence the LHS is equal to $|S|$. □

Remark 8. In the last result, let $V = \mathbb{R}^d, \Lambda = \mathbb{Z}^d$ and Λ_0 be the lattice generated by some linearly independent integer vectors $u_1, \ldots, u_d$. Then the number of integer points in the fun. parallelepiped is equal to the volume of the parallelepiped!!!

1.1. Minkowski Convex Body Theorem

Theorem 9. *(Blichfeldt's Theorem) $\Lambda \subset V$ be a lattice and $X \subset V$ be a Lebesgue measurable set sucht that* $\operatorname{vol} X > \det \Lambda$. *Then there exist two distinct points $x, y \in X$ s.t. $x - y \in \Lambda$*

PROOF. Pick a fun. parallelepiped Π of Λ, so $\operatorname{vol}\Pi = \det\Lambda$. For each $u \in \Lambda$ let $X_u = \{x \in \Pi : x+u \in X\}$. In words, we consider the translates $\Pi + u : u \in \Lambda$ which cover V w/o overlapping . Then for every translate, we find the intersection $(\Pi + u) \cap X$ and get X_u by translating i5 back into Π by $-u$.

B/c $(\Pi + u) \cap X$ cover X w/o overlapping we have

$$\sum_{u\in\Lambda} \operatorname{vol} X_u = \sum_{u\in\Lambda} \operatorname{vol}((\Pi + u) \cap X) = \operatorname{vol} X$$

Claim: some sets $X_u, X_v, v \neq u$ must intersect. For a contradiction, assume all the sets are disjoint, then

$$\operatorname{vol}(\cup_{u\in\Lambda} X_u) = \sum_{u\in\Lambda} X_u = \operatorname{vol} X > \operatorname{vol} \Pi$$

, which is a contradiction b/c

$$\cup_{u\in\Lambda} X_u \subset \Pi$$

.

This shows that there are two lattice pints $u \neq v$ and a point a s.t. $a \in X_v \cap X_u$. In other words, $a + u \in X_u$, and $a + v \in X_v$. Let $x = a + u; y = a + v$, let us obtain two distinct points from X s.t. $x - y = u - v$ is a non-zero lattice point. □

Theorem 10. *(Minkowski First Convex Body Theorem) Let $B \subset V$ be a Labesgue measurable set such that the following holds*

(1) for every $x, y \in B$ we have $(x + y)/2 \in B$
(2) for every $x \in B$ we have $-x \in B$
(3) $vol B > 2^d \det \Lambda$ where it is a lattice in V.

Then B contains a non-zero point from Λ. Moreover, if B is compact, the the last condidtion can be replaced by $vol B \geq 2^d \det \Lambda$

Proof. Let $X = 1/2B = \{1/2 * x : x \in B\}$. Then

$$\operatorname{vol} X = \frac{1}{2^d} \operatorname{vol} B = \det \Lambda > 1.$$

By Blichfeldt's Theorem, there are two points $x, y \in B$ s.t. $u = 1/2x - 1/2y$ is a non-zero lattice point. Rewrite $u = 1/2x + 1/2(-y)$ and note $-y \in B$ we have the $u \in B$.

Now assume B is compact and $\operatorname{vol} B = 2^d \det \Lambda$. Then for every $\varepsilon > 0$, the set

$$B_\varepsilon = \{(1 + \varepsilon)x : x \in B\}$$

satisfies the condidtions of the theorem and

$$\operatorname{vol} B_\varepsilon = (1 + \varepsilon)^d \operatorname{vol} B > 2^d \det \Lambda.$$

Hence B_ε contains a non-zero lattice point u_ε. A limit point u of $\{u_\varepsilon\}$ is a non-zero lattice point in B. □

1.2. Basis Reduction

Let $u_1, \ldots, u_k$ be a basis. Let $L_0 = \{0\}, L_k = span(u_1, \ldots, u_k)$. Let w_k be the orthogonal complement of the projection of u_k onto L_{k-1}. The vectors $w_1, \ldots w_k$ are the Gram-Schmidt orthogonalization of the u's w/o normalization: $dist(u_k, L_{k-1}) = \|w_k\|$.

Note that $\det \Lambda = \Pi_{k=1}^d \|w_k\|$. Define $\Lambda_k = \Lambda \cap L_k$, and $\det \Lambda_k = \Pi_{i=1}^k \|w_i\|$.

1.2.1. weakly reduced. Write $u_k = w_k + \sum_{i=1}^{k-1} \alpha_{ij} w_i$ for real α.

The basis is weakly reduced iff $|\alpha_{ij}| \leq 1/2$

If $|\alpha_{ij}| > 1/2$, replace $u'_k = u_k - m_{ki} u_i$ where m is the integer s.t. $|\alpha_{ki} - m_{ki}| \leq 1/2$.

It is clear $u_1, \ldots, u_{k-1}, u'_k, u_{k+1}, \ldots, u_d$ is still a bnasis for Λ. Also, the subspaces $L_0, \ldots, L_k$ and the vectors $w_1, \ldots, w_k$ do not change. On the α_{kj} with $j \leq i$ change and $|\alpha'_{ki}| = |\alpha_{ki} - m_{ki}| \leq 1/2$. So we have to apply this update at most $d(d-1)/2$ times (lower triangular).

1.2.2. reduced. A basis $u_1, \ldots, u_k$ is reduced iff it is weakly reduced and

$$dist^2(u_k, L_{k-1}) \leq 4/3 dist^2(u_{k+1}, L_{k-1}; k = 1, \ldots, d-1$$

This means that u_{k+1} is not much closer to L_{k-1} than u_k.

1.2.3. Algorithm. Start with $u_1, \ldots, u_k$. Make it weakly reduced. If it is not reduced, (the condition above is false for some k) then change the order of the basis vectors switching u_k, and u_{k+1}. Now the basis may not be weakly reduced, so start over.

1.2.4. Remarks.

Corollary 11. *Let $u_1, \ldots, u_d$ be a reduced basis of Λ. Then*

$$\Pi_{i=1}^d \|u_i\| \leq 2^{d(d-1)/4} \det \Lambda.$$

Corollary 12. *Let $u_1, \ldots, u_d$ be a reduced basis of Λ. Let*

$$\lambda = min_{u \in \Lambda - \{0\}} \|u\|$$

be the min. length of a non-zero vector from Λ. Assume that $\|u\| \leq \beta\lambda$ for some $u \in \Lambda$ and some $\beta \geq 1$. Then in the representation $u = \sum_1^d m_i u_i$ one must have

$$|m_k| \leq 2^{(d-1)/2} (3/2)^{d-k} \beta \leq 3^d \beta; \; k = 1, \ldots d.$$

CHAPTER 2

Book: Integer and Combinatorial Optimization

Most text/math came from [3].

2.1. Euclidean Algorithm

Algorithm 1 Euclidean Algorithm

Input: $b \leq a$.
Output: $c = gcd(a, b)$
  $(c_{-1}, c_0) = (a, b)$
  $(p_{-1}, p_0) = (1, 0)$
  $(q_{-1}, q_0) = (0, 1)$
  $t = 1$
  $d_t = \lfloor c_{t-2}/c_{t-1} \rfloor$
  while $c_t \neq 0$ **do**
    $c_t = c_{t-2} - d_t c_{t-1}$
    $p_t = p_{t-2} + d_t p_{t-1}$
    $q_t = q_{t-2} + d_t q_{t-1}$
    $t = t + 1$
    $d_t = \lfloor c_{t-2}/c_{t-1} \rfloor$
  end while
  $T = t$
  return $gcd(a, b) = c_{T-1}$

Corollary 13. *For $t = -1 \ldots T$ we have that 1) $c_t = (-1)^{t+1}(p_t a - q_t b)$; 2) $p_t q_{t+1} - p_{t+1} q_t = (-1)^{t+1}$; 3) $gcd(p_t, q_t) = 1$; 4) $a/b = q_T/p_T$*

Proof. 1) by induction: for t=-1, 0 it is clear by how we define p, t, etc. assume it is true up to some $t - 1$. Then

$$\begin{aligned} c_t &= c_{t-2} - d_t c_{t-1} \\ &= (-1)^{t-1}(p_{t-2}a - q_{t-2}b) - (-1)^t d_t (p_{t-1}a - q_{t-1}b) \\ &= (-1)^{t+1}[(p_{t-2} + d_t p_{t-1})a - (q_{t-2} + d_t q_{t-1})b] \\ &= (-1)^{t+1}(p_t a - q_t b) \end{aligned}$$

2) by induction again
3) b/c $p_{t-1}q_t - p_tq_{t-1} = (-1)^t$ and $p, d > 0$, we have the $gcd(p_t, q_t) = 1$
4) b/c $c_T = 0 = p_Ta - q_Tb$, $a/b = q_T/p_T$ □

So the EA above gives the gcd AND the extended result.

2.2. Hermite Normal Form

Definition 14. A is an $m \times n$ inteer matrix. The lattice $L(A) = \{Ax : x \in \mathbb{Z}^n\}$

Definition 15. C is unimodular if it is integer and $|detC| = 1$.

Lemma 16. *A is integer, C is unimodular, then $L(AC) = L(A)$.*

PROOF. It is enough to show that $\{Cw : w \in \mathbb{Z}^n\} = \{w : w \in \mathbb{Z}^n\}$.
$\subseteq$: C is integer, so $Cw \in \mathbb{Z}^n$.
$\supseteq$: C is unimodular, so C^{-1} is integer matrix so $C^{-1}w$ is integer and so $C(C^{-1}w)$ is in the RHS. □

Definition 17. $m \times m$ matrix H is in Hermite normal form if

(1) H is lower triangular: $h_{ij} = 0$ for $i < j$.
(2) $h_{ii} > 0$
(3) $h_{ij} \leq 0$ and $|h_{ij}| < h_{ii}$ for $i > j$. So the off diag is negative and the elements on the diagonal is the largest number per row absolutely.

Theorem 18. *(Main HNF theorem) Let A be a $m \times n$ matrix and let A have full row rank (note: $m \leq n$), then there exist an $n \times n$ unomodular matirx C s.t. $AC = (H, O)$ where H is the HNF and $H^{-1}A$ is an integer matrix. Sometimes we will write $C = (C_1, C_2)$ where C_1 is a $n \times m$ and C_2 is a $n \times (n - m)$ matrix. The proof is in the polynomial-time algorithm.*

Corollary 19. *L(H) = L(A).*

Definition 20. If L(A) = L(B) and B is nonsingular, then B is a basis for the lattice L(A). Every full row rank matrix A has a basis.

Theorem 21. *(Linear Equation Integer Feasibility Problem) Let $S = \{x \in \mathbb{Z}^n : Ax = b\}$.*
1) $S \neq \emptyset$ iff $H^{-1}b \in \mathbb{Z}^n$
2) if $S \neq \emptyset$ then every solution in S is in the form $x = C_1H^{-1}b + C_2z, z \in Z$

PROOF. 1) $\Rightarrow$: let Ax = b. Then $ACw = b$ for $x = Cw, w \in Z^n$. Then $(H, O)w = b$
$\Leftarrow$: Let $w = H^{-1}b$, then let $x = Cw$.
2)

$$\begin{aligned} S &= \{x \in \mathbb{Z}^n : Ax = b\} \\ &= \{x : x = Cw, ACw = b, w \in Z^n\} \\ &= \{x : x = Cw, (H, O)w = b, w \in Z^n\} \\ &= \{x : x = C_1w_1 + C_2w_2, Hw_1 = b, w_1 \in Z^m, w_2 \in \mathbb{Z}^{n-m}\} \end{aligned}$$

□

Example 22. Find integer solutions to

$$2x_1 + 6x_2 + x_3 = 7$$
$$4x_1 + 7x_2 + 7x_3 = 4$$

$$H = \begin{pmatrix} 1 & 0 \\ -3 & 5 \end{pmatrix}, H = 1/5 \begin{pmatrix} 5 & 0 \\ 3 & 1 \end{pmatrix}, C = \begin{pmatrix} 1 & 3 & -7 \\ 0 & -1 & 2 \\ -1 & 0 & 2 \end{pmatrix}$$

The solution space is not empty b/c $H^{-1}b = \binom{7}{5} \in \mathbb{Z}^2$.
The general solution is $C_1\binom{7}{5} + C_2 w_2$ which is

$$\begin{pmatrix} 1 & 3 \\ 0 & -1 \\ -1 & 0 \end{pmatrix} \binom{7}{5} + \begin{pmatrix} -7 \\ 2 \\ 2 \end{pmatrix} w_2$$

Corollary 23. *(Integer Farkas Lemma) Either $S \neq \emptyset$ or exclusively there exist $u \in \mathbb{R}^m$ s.t. $uA \in \mathbb{Z}^m, ub \notin \mathbb{Z}^m$.*

Proof. Both cannot be true because $uAx = ub$ would be a contradiction. If S is empty, then $H^{-1}b \notin \mathbb{Z}^m$. Let the ith coefficient of $H^{-1}b$ not be integer then take u to be the ith row of H^{-1} □

Lemma 24. *Let $A = (a_1, \ldots, a_n)$ be an $m \times n$ matrix, $gcd(a_{is}, a_{it}) = r, pa_{is} + qa_{ir} = r$. Then exists an $n \times n$ unimodular integer matrix C s.t. $AC = A'$ where*

$$a'_l = a_l for l \neq s, t$$
$$a'_s = pa_s + qa_t$$
$$a'_t = -\frac{a_{it}}{r}a_s + \frac{a_{is}}{r}a_t$$

Note: $a'_{is} = r, a'_{it} = 0$. So we just perfomed elementary column operations so that $a_{is} \leftarrow gcd(a_{is}, a_{it}), a_{it} \leftarrow 0$ $(s < t)$.

Proof. Let C be the identity matrix with $c_{ss} = p, c_{ts} = q, c_{st} = -a_{it}/r, c_{tt} = a_{is}/r$. Then $AC = A'$ and $detC = pa_{is}/r + qait/r = 1$. □

2.3. Hermite Normal Form Algorithm

Proof. (the NHF Alg. is correct) All the operations performed are column operations corresponding to right multiplication by a unimodular matrix. Hence the produce C of these matrices is unimodular. Let $H' = AC$. Note that after step 2, $h'_{ij} = 0$ for all $j > i$; after step 3, $h'_{ii} \geq 0$; and after step 4 $h'_{ij} < 0$ and $|h'_{ij}| < h'_{ii}$ for $j < i$ unless $h'_{ii} = 0$. These values are never changed in later steps. Hence we only need to show that after step 2 for row i, $|h'_{ii}| > 0$. For a contradiction, assume $h'_{jj} > 0$ for $j < i$ and $h'_{ii} = 0$. Let A_1 be the first i

Algorithm 2 HNF Algorithm

$i = 1$

1) work on row i. Set $j = i + 1$

2) work on row i and columsn i and $j > i$. If $a_{ij} = 0$ do nothing. Else use the EA to find $r = gcd(a_{ii}, a_{ij})$, and p, q relatively prime s.t. $pa_{ii} + qa_{ij} = r$. Set $A = AC$ where C is the unimodular matrix described in the last lemma with $s = i, t = j$. If $j < n$ set $j = j + 1$ and return to step 2, else goto step 3 ($j = n$).

3) work on row i and column i. If $a_{ii} < 0$ multiply column i by -1.

4) work on row i and column $j < i$. Set $A = AC$ where C replaces column a_j by $a_j - \left\lceil \frac{a_{ij}}{a_{ii}} \right\rceil a_i$. If $j = i - 1$ then increase i. If $i > m$ stop, else goto step 1. If $j < i - 1$, then increase j and goto step 4.

rows of A. Then let $H^* = A_1 C^*$ where C^* is the unimodular matrix produced so far. Note $h^*_{kj} = 0$ for $k \leq i$ and $j \geq i$. Hence rank(H^*) = i-1. So $rank(A_1) = rank(A_1 C^*) = i - 1$, which contradicts rank(A) = m. □

The number of iterations of the NHF is polynomially bounded, it is not known whether the size of the numbers is polynomially bounded. The numbers can be very large.

Example 25.

$$A = \begin{pmatrix} 2 & 6 & 1 \\ 4 & 7 & 7 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{matrix} i = 1, j = 2 \\ (a_{11}, a_{12}) = 2, 6 \\ (p, q) = 1, 0; r = 2 \end{matrix} \quad C^1 = \begin{pmatrix} 1 & -3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$A = \begin{pmatrix} 2 & 0 & 1 \\ 4 & -5 & 7 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{matrix} i = 1, j = 3 \\ (a_{11}, a_{13}) = 2, 1 \\ (p, q) = 1, 0; r = 1 \end{matrix} \quad C^2 = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 7 & -5 & 10 \\ 1 & 0 & 2 \end{pmatrix} \quad \begin{matrix} i = 1, j = 1, no - change \\ i = 2, j = 3 \\ (a_{22}, a_{23}) = -5, 10 \\ (p, q) = -1, 0; r = 5 \end{matrix} \quad C^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -2 \\ 0 & 0 & -1 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 7 & 5 & 2 \\ 1 & 0 & -2 \end{pmatrix} \quad \begin{matrix} i = 2, j = 2, no - change \\ i = 2, j = 1 \end{matrix} \quad C^4 = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 0 & 0 \\ -3 & 5 & 0 \\ 1 & 0 & -2 \end{pmatrix} \quad i = 3, j = 3 \quad C^5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 0 & 0 \\ -3 & 5 & 0 \\ 1 & 0 & 2 \end{pmatrix} \quad i = 3, j = 1 \quad C^6 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 0 & 0 \\ -3 & 5 & 0 \\ -1 & 0 & 2 \end{pmatrix} \quad i = 3, j = 2, no - change \quad H = \begin{pmatrix} 1 & 0 & 0 \\ -3 & 5 & 0 \\ -1 & 0 & 2 \end{pmatrix}$$

Finally, $C = \Pi_1^6 C^k = \begin{pmatrix} 1 & 3 & -7 \\ 0 & -1 & 2 \\ -1 & 0 & 2 \end{pmatrix}$

We can modify the algorithm to guarantee that the numbers remain small.

Lemma 26. *Assume A is square matrix and full rank. let $d_i = \Pi_{k=i}^m h_{kk}$ for $i = 1 \dots m$. Then $d_i e_k \in L(A)$ for $k = i \dots m$.*

PROOF. The vector $x = (d_1 A^{-1}) e_k$ is integer b/c $d_1 A^{-1}$ is integer. Also $Ax = d_1 e_k \in L(A)$. Now note that $h_i, \dots h_m$ (col vectors.) are in the lattice L(A). Then $d_i e_k$ is in the lattice $L(h_i, \dots, h_m) \subseteq L(A)$ (WHY? replace A with $\hat{H} = (h_i, \dots, h_m)$ and note that the top $i-1$ rows are zero, so remove these rows to get a square matrix and $\hat{H}^{-1}$ is now defined and repeat the above argument). □

To apply this lemma, first find $d_1 = det(H) = det(A)$. Add $d_1 e_k$ for $k = 1 \dots m$ to the columns of A. Once you find h_1 you can divide and find d_2 and then all $d_2 e_k$ for $k = 2 \dots m$ in A and repeat. This allows you to reduce all elements in rows $i \dots m$ modulo d_i. With this no intermediate number in the HNF exceeds $2d_1^2$ is absolute value, yet is still a poly-time algo.

If A does not have full row rank, we can find a unimodular $n \times n$ C s.t.

$$AC = \begin{pmatrix} H & 0 \\ 0 & 0 \end{pmatrix}$$

Definition 27. A is $m \times m$ nonsingular integer matrix, there exist unimodular matrices R and C s.t.

(1) $RAC = \Delta$
(2) Δ is a diagonal matrix with diagonal entries in $\mathbb{Z} - \{0\}$.
(3) $\delta_1 | \delta_2| \dots | \delta_m$
(4) Δ is unique and is called the Smith normal form of A.

2.4. Reduced Basis of a Lattice

Definition 28. Gram-Schmidt Orthogonalization of a basis B

(1) $b_1^* = b_1$
(2) $b_k^* = b_k - \sum_{j=1}^{k-1} \alpha_{ij} b^* j$.
(3) where $\alpha_{ij} = b_j^* b_j / \left\| b_j^* \right\|^2$ for $i < j$.

Remark 29. Gram-Schmidt Orthogonalization of a basis B

(1) GS makes an orthogonal basis B^* but it is NOT normal.

(2) b_k^* is the component of b_k orthogonal to the subspace generated by $b_1^*, \ldots, b_{k-1}^*$.
(3) $|det(B)| = |det(B^*)| = \Pi_{j=1}^n \left\|b_j^*\right\|$ (WHY: write $B^* = BL$ where L is lower triangular with 1's on the diagonal. The 2nd equality comes from the geometric meaning of det).

Definition 30. $|det(b_1, \ldots, b_k)| = \Pi_{j=1}^k \|b_k^*\|$ for all $k \leq n$.

Note that because b_j^* is the component of b_j orthogonal to the subspace generated by $b_1^*, \ldots, b_{j-1}^*$ we have that $\left\|b_j^*\right\| \leq \|b_j\|$.

Given a full-dim lattice L we know by the GS remark above that —det(B)— as the same value for all basis B of a lattice. Let d(L) be this common value and let $\alpha(B) = \Pi_1^n \|b_j\|$. Then we have

Remark 31. (The Hadamard Inequality) For all bases B of L, we have $\alpha(B) \geq d(L)$.

All of this is related to the shortest vector problem:

Theorem 32. *Given a full-dim lattice L and a basis B of L, let y be the solution to*

$$min\{\|Bx\| : |x_j| \leq \frac{\alpha(B)}{|det(B)|}, x \in \mathbb{Z}^n - \{0\}\}$$

Then $v = By$ is the shortest vector in the lattice L.

Proof. Let v = By be the shortest nonzero vector with $y \neq 0$. Use Cramer's rule $|x_j| = |det(B_j)|/|det(B)|$ where B_j has the jth column replaced by v.

Then by Hadamard's Ineq.: $|det(B_j)| \leq \|b_1\| \cdots \|v\| \cdots \|b_n\|$ but each $b_j \in L$ and so b/c v is the shortest vector $\|v\| \leq \|b_j\|$. Then $|det(B_j)| \leq |\alpha(B)|$

Thus, $|x_j| \leq \frac{\alpha(B)}{|det(B)|}$ □

So, now we want to find a basis where $\frac{\alpha(B)}{|det(B)|}$ is small. But first here is a lower bound on the shortest vector:

Theorem 33. *If b is in the lattice and nonzero, B is a lattice of L, B^* is the GS, then $\|b\| \geq min_j \left\|b_j^*\right\|$*

Proof. b/c b is in the lattice, write $b = \sum_j^k b_j z_j$ with z_j integer and $z_k \neq 0$ ($k \leq n$).

Plug in $b_j = b_j^* + \sum_{i=1}^{j-1} stuff \times b_i^*$ to write $b = \sum_j^k b_j^* z_j^*$ and notice that $z_k^* = z_k$.

Then because the B^* are orthogonal we get: $\|b\| \geq |z_k| \left\|b_k^*\right\| \geq min_j \left\|b_j^*\right\|$. □

Note that B^* may not a lattice basis (even if integer) b/c not all the α_{ij} are integer.

Definition 34. Let L be a full dim lattice, B is a basis of L, and B^* is obtained from GS. B is a reduced basis if

1) $\alpha_{ij} \leq 1/2$
2) $\left\|b^* j + 1 + \alpha_{j,j+1} b_j^*\right\|^2 \geq 3/4 \left\|b_j^*\right\|^2$ for j = 1..(n-1).

Theorem 35. *B is a reduced basis for the full dim lattice L then*

(1) $\left\|b_j^*\right\|^2 \leq 2\left\|b_{j+1}^*\right\|$
(2) $\|b_1\| \leq 2^{(n-1)/4} d(L)^{1/n}$
(3) $\|b_1\| \leq 2^{(n-1)/2} min\{\|b\|, b \in L - 0\}$
(4) $\alpha(B) \leq 2^{n(n-1)/4} d(L)$

PROOF. 1): b/c B* is orthogonal, be the def. of reduced basis:

$$\left\|b^* j + 1 + \alpha_{j,j+1} b_j^*\right\|^2 = \left\|b_{j+1}^*\right\|^2 + \alpha_{j,j+1}^2 \left\|b_j^*\right\|^2 \geq 3/4 \left\|b_j^*\right\|^2$$

But $\alpha_{j,j+1}^2 \leq 1/4$, thus $\left\|b_j^*\right\|^2 \leq 2\left\|b_{j+1}^*\right\|$
2) by (1) $\left\|b_j^*\right\|^2 \geq 2^{-(j-1)} \|b_1 = b_1^*\|^2$ So then

$$d(L)^2 = \Pi_{j=1}^n \left\|b_j^*\right\|^2 \leq 2^{-\sum(j-1)} \|b_1\|^{2n} = 2^{-n(n-1)/2} \|b_1\|^{2n}$$

3) From 2 we have

$$\left\|b_j^*\right\|^2 \geq 2^{-(j-1)} \|b_1\|^2 \geq 2^{-(n-1)} \|b_1\|^2$$

Using the last theorem

$$\|b\| \geq min_j(\left\|b_j^*\right\|) \geq 2^{-(n-1)/2} \|b_1\|^2$$

for any nonzero b in the lattice.
4) Write $b_j = \sum_1^j \alpha ij b_j^*$. B/c B* is orthogonal,

$$\begin{aligned}
\|b_j\|^2 &= \sum_{i=1}^{j} \alpha_{ij}^2 \|b_i^*\| \, (note : \alpha_{jj} = 1) \\
&\leq \left\|b_j^*\right\|^2 + 1/4 \sum_{i=1}^{j-1} \|b_i^*\|^2 \, (b/c \, \alpha_{ij} \leq 1/2) \\
&\leq \left\|b_j^*\right\|^2 (1 + 1/4 \sum_{i=1}^{j-1} 2^{j-1}) (from \, 1 \, \|b_i^*\|^2 \leq 2^{j-i} \left\|b_j^*\right\|^2 \\
&\leq 2^{j-1} \left\|b_j^*\right\|^2
\end{aligned}$$

Finally,

$$\alpha(B)^2 = \Pi_{j=1}^n \|b_j\|^2 \leq (use - above - ineq) = 2^{n(n-1)/2} d(L)^2$$

□

The last part of the last theorem gives a way to search for the shortest lattice vector (use the 2nd to last theorem and $\alpha(B)/|det(B)| \leq 2^{n(n-1)/4}$

Example 36.

$$B = \begin{pmatrix} 0 & 2 & 1 \\ 0 & -1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$$

Then from the GS we get $b_1^* = (0, 0, 2)$ From this, we compute $\alpha_{12} = 0, \alpha_{13} = 1/2$.

Then $b_2^* = (2, -1, 0)$ and we find $\alpha_{23} = 0$ which gives $b_3^* = (1, 2, 0)$.

We can also check the 2nd condition in a reduced basis. This basis is reduced.

Now find the shortest vector in the lattice. So we find Bx for every x with $|x_i| \leq \lfloor 2^3(3-1)/4 = 2 \rfloor$. So we have to look at $5^3 - 1$ different x's and times by B and compute the resulting length. The shortest vector found this way is $Bx = (0, 0, 2)$.

2.5. Basis Reduce Algorithmm for full dimensional lattice

This algorithm find a reduced basis for L in polynomial time.

Algorithm 3 Basis Reduction

Input: B be a basis of a lattice L

Output: $c = gcd(a, b)$

1) $(b_1^*, \ldots, b_n^*)$ be the GS of B with $\alpha_{ij} = b_i^* b_j / \left\|b_i^*\right\|^2$

2) for j = 2..n, for i=j-1..1, replace b_j with $b_j - \hat{\alpha}_{ij} b_i$ where $\hat{\alpha}$ is the integer closest to α.

3) If $\left\|b_{j+1}^* + \alpha_{j,j+1} b_j^*\right\|^2 < 3/4 \left\|b_j^*\right\|^2$ for some j, interchange b_j, and b_{j+1} and goto step 1 with the new basis B.

2.6. Simultaneous Diophantine Approximation Feasibility Problem

Definition 37. Simultaneous Diophantine Approximation Feasibility Problem: given rationals $a_1, \ldots, a_n, \varepsilon$ and integer $K > 0$, decide if there exist integers $q_1, \ldots, q_n$ and $0 < p \leq K$ s.t. $|pa_i - q_i| \leq \varepsilon$ for i=1..n.

Theorem 38. *There is a poly-time algorithm which either 1) determines theat SDAF is infeasible OR 2) finds integers $q_1, \ldots, q_n$ and $p > 0$ s.t.t $|pa_i - q_i| < 2^{n/2}\varepsilon(n+1)^{1/2}$ for i=1..n and $p < 2^{n/2}K(n+1)^{1/2}$.*

Proof. Let $a = (a_1, \ldots, a_n, \varepsilon/K) \in \mathbb{R}^{n+1}$ and let e_i be the std unit vector in $\mathbb{R}^{n+1}$. Consider the lattice generated by $(e_1, \ldots, e_n, -a)$. For any $(q_1, \ldots, q_n, p) \in \mathbb{Z}^{n+1}$ we have $w = \sum_1^n q_i e_i - pa \in L$. If $(q_1, \ldots, q_n, p)$ is a solution to SDAF then $|w_i| = |q_i - a_i p| \leq \varepsilon$ and for i=1..n and $|w_{n+1}| = |p\varepsilon/k| \leq \varepsilon$. Hence $\|w\| \leq \varepsilon(n+1)^{1/2}$.

Now let B be a reduced basis for L with b_1 being the 1st column. This can be done in poly-time.

Recall from part (3) of a theorem above not-too-long-ago that $\|b_1\| \leq 2^{(n-1)/2} min\{\|b\|, b \in L - 0\}$. So, IF $\|b_1\| > 2^{(n-1)/2}\varepsilon(n+1)^{1/2}$, then $\|b\| \geq 2^{-(n-1)/2}\|b_1\| > \varepsilon(n+1)^{1/2}$ for all nonzero b in the lattice. Thus the SDAF has no solution.

IF $\|b_1\| \leq 2^{(n-1)/2}\varepsilon(n+1)^{1/2}$, choose $(q', p') \in \mathbb{Z}^{n+1}$ s.t. $b_1 = \sum_1^n q'_i e_i - p'a$. Now there are two more chases. If $p' \neq 0$, then (q', p') is a solution b/c

$$|q'_i - p'a_i| \leq 2^{(n-1)/2}\varepsilon(n+1)^{1/2}, i = 1, \ldots, n$$

and

$$|p'\varepsilon/K| \leq 2^{(n-1)/2}\varepsilon(n+1)^{1/2}$$

If $p' = 0$ then $b_1 = (q'_1, \ldots, q'_n, 0)$ and $\|b_1\| \geq 1$. Thus $2^{(n-1)/2}\varepsilon(n+1)^{1/2} \geq 1$ and $p = 1, q_i = \lfloor a_i \rfloor$ □

CHAPTER 3

Book: Theory of Linear and Integer Programming

Most text/math came from [4].

3.1. Theory of lattices and linear diophantine equations

Definition 39. Elementary unimodular column operations

(1) swap two columns
(2) multiplying a column by -1
(3) adding an integral multiple of one column to another column.

Definition 40. A full row rank matrix is in Hermite normal form if it is the form [B 0] where B is nonsingular, lower triangular, nonnegative matrix, and each row has a unique maximum entry located on the main diagonal.

Theorem 41. *(Hermite normal form theorem) Each rational matrix of full row rank can be brought into Hermite normal form by a series of elementary column operations.*

PROOF. Let A be integral, wlog. By induction, assume we transformed A by elementary column operations to the form $\begin{pmatrix} B & 0 \\ C & D \end{pmatrix}$ where B is lower triangular and with positive diagonal. With elm. column operations we can modify D so its first row is nonegative and the sum $d_{11} + \cdots + d_{1k}$ is as small as possible. Assume that $d_{11} \leq \cdots \leq d_{1k}$. Then $d_{11} > 0$ b/c A is full row rank. If $d_{12} > 0$ then subtract the 2nd column of D from the first, then the first row will have smaller sum, a contradiction, and so $d_{12} = \cdots = d_{1k} = 0$. By repeating for each row, we transform A into [B 0] where B is lower triangular. Then add multiple of column j to $i < j$ to get it in HNF. □

Corollary 42. *Let A be rational, b is rational. The System $Ax = b$ as in integral solution x iff yb is an integer for each rational row vector y for which yA is integral.*

PROOF. $\Leftarrow$: For a contradiction, assume yA is integral, but yb is not. But x is integer and yAx = yb so (integer) = non-integer.

$\Rightarrow$: Assume yb is integer when yA is integral. Ax = b has a real solution, otherwise we could find y s.t. yA = 0, yB = 1/2 (by linear algebra). So we can now assume A has full row rank. Because both sides of the equivalence are invariant under elm column operations, we can assume A is in HNF [B 0]. B/c $B^{-1}[B0] = [I0]$ is integral, $B^{-1}b$ is integral by assumption (applied to each row).

So $x = (B^{-1}b, 0)^T$ is the integral solution to $[B\ 0] = b$. □

Corollary 43. *Let A be integral $m \times n$ full row rank matrix. The following are equivalent*

(1) the gcd of the subdeterminants of A or order m is 1.
(2) the system Ax=b has an integral solution x, for each integral vector b.
(3) for each vector y, if yA is integral then y is integral

PROOF. 1,2,3 are invariant under elm column operations on A. So assume A is in HNF [B 0]. 1,2,3 are equivalent to B=I. □

Theorem 44. *The following are equivalent for a nonsingular rational matrix U of order n*

(1) U is unimodular.
(2) U^{-1} is unomdular
(3) the lattice generated by the columns of U is $\mathbb{Z}^n$
(4) U has the identity matrix as HNF.
(5) U comes from I by elm column operations.

PROOF. $1 \leftrightarrow 2$ is clear.
$3 \leftrightarrow 4 \leftrightarrow 5$ is clear by taking the HNF.
$5 \leftrightarrow 1$ is clear.
$1 \leftrightarrow 4$: if B is the HNF of U then B is integral and $|det(B)| = |det(U)| = 1$ But B is triangular. Thus $B = I$. □

Corollary 45. *A and A' are nonsingular. The following are equivalent*

(1) columns of A and A' generate the same lattice.
(2) A' comes from A by elm. column operations.
(3) A'=AU for some unimodular matrix U.

PROOF. $2 \leftrightarrow 3$ is clear.
$1 \leftrightarrow 3$: let B, B' be the HNF of A, A'. so let A = BU, A'=B'U'. But HNF is unique (we skipped the proof) for the lattice so B = B'. Then $AU^{-1}U' = BU' = A'$ □

Corollary 46. *If A, B are nonsingular, and each column of B is in the lattice generated by the columns of A, then det(B) is an integral multiple of det(A). Furthermore, $|det(A)| = |det(B)|$ iff the lattice generated by the columns of A = lattice generated by B.*

PROOF. So $B = AU$ where U is just integral. So $|det(B)| = |det(A)||det(U)|$. And $|det(A)| = |det(B)|$ iff U is unimodular. □

3.2. Algorithms for linear diophantine equations

3.2.1. EA. This is done for $k = 1..N$ when $a_N = 0$ or $b_N = 0$. The gcd of the first row of A does not change. We also get the extended EA form. To see this, note that $(1, -a, -b)A_k = (0, 0)$. This means

$$y_k a + e_k b = a_k$$
$$g_k a + z_k b = b_k$$

Algorithm 4 (Rational) Euclidean Algorithm

Input: rationals a, b.
Output: $gcd(a, b)$

1) let $A = \begin{pmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$

2) Let $A_k = \begin{pmatrix} a_k & b_k \\ y_k & g_k \\ e_k & z_k \end{pmatrix}$. Then find A_k by the following rule

If k is even and $b_k > 0$: subtract $\lfloor a_k/b_k \rfloor$ times the second column of A_k from the 1st.

If k is odd and $a_k > 0$: subtract $\lfloor b_k/a_k \rfloor$ times the first column of A_k from the 2nd.

and so depending on if $a_N = 0$ or $b_N = 0$ one equation gives the gcd in terms of a and b.

Corollary 47. *A linear diophantine equation with rational coefficients can be solved in polynomial time.*

PROOF. Let $a_1 z_1 + \cdots + a_n z_n = b$. (the a's are known and scaled to integers). If n=1, this is easy. For $n \geq 2$, let $a' = gcd(a_1, a_2) = a_1 y + a_2 e$, where y and e are integers. Now solve $a' z' + a_3 z_3 + \cdots + a_n z_n = b$. If this has no integral solution, neither does the first one. If $(z', z_3, \ldots, z_n)$ is a solution, then the first solution is $z_1 = yz', z_2 = ez', z_i = z_i$. □

3.2.2. HNF. We will describe the algo to find the HNF.

Let A be $m \times n$ of full row rank. Let M be the abs. value of the determinant of an arbitarary submatrix of A or rank m. The columns of A generate the same lattice as $A' = [A|M * I]$ (Why: A has full rank square submatrix B with det(B) = +-B, and $det(B)B^{-1}$ is integral. So BX=MI has an integer solution X.)

My elm. col. operations, we can reduce a_{ij} mod M. For k = 0..m consider the matrix

$$\left(\begin{array}{c|c|ccc} \text{B} & 0 & 0 & \ldots & 0 \\ \text{C} & \text{D} & 0 & \ldots & 0 \\ & & \text{M} & 0 & 0 \\ & & 0 & \ddots & 0 \\ & & 0 & \ldots & \text{M} \end{array}\right)$$

Where B is lower triangular $k \times k$, C is $(m-k) \times k$, D is $(m-k) \times (n+1)$, and the whole matrix is $m \times (m+n)$ (so the first row of d is $(stuff, M)$.

Then, repeatedly do while the first row of D contains more than 1 non-zero: if there are $d_{1i} \geq d_{1j} > 0$ then subtract $\lfloor d_{1i}/d_{1j} \rfloor$ times the jth column of D from the ith column

of D. Then add integral multiples of the last $m-k-1$ columns to reduce all entries in D modulo M.

Then increase k. When k=m, $A' = [B, 0]$. Then we can make B nonnegative and each row mod the diagional.

Deleting the last m columns (which are now zero) give the HNF of A.

3.3. Basis reduction

We will prove the main algorithm all in 1 shot!

Theorem 48. *(Basis reduction method) there exists a polynomial algorithm which, for given positive definite rational matrix D, finds a basis $b_1, \ldots, b_n$ for the lattice $\mathbb{Z}^n$. st*

$$//b_1// \ldots //b_n// \leq 2^{n(n-1)/4} det(D)^{1/2}$$

where $//x// = \sqrt{x^T D x}$.

PROOF. We can assume D is integer. Also, we also define orthogonality w.r.t. $x^T D y = 0$ and take inner products w.r.t. D.

Start off with b_i the std. basis vectors.

Step 1: Let B^* be the GS of B (take inner products w.r.t D).

Step 2: Write $B = B^* V$ for some upper triangular matrix V with 1's on the diagonal (b/c $b_i = \lambda_1 b_1^* + \ldots \lambda_{i-1} b_{i-1}^* + b_i^*$). Then do elm column operations that change V into an upper triangular with 1's on the diagonal and all other entries at most 1/2 is absolute value. This does not change the GS orthogonalization of the b's.

Step 3: If $//b *_i //^2 \geq 2//b_{i+1}^*//^2$ then exchange b_i and b_{i+1} and goto step 1. Else stop.

The author goes on to prove the algorithm stops, is correct, is polynomial time, and gives the same identities as other others (in more generality). But I stop here–BD. □

Corollary 49. *There exists a polynomial algo which, for given nonsingular rational matrix A, finds a basis $b_1, \ldots, b_n$ for the lattice generated by the columns of A s.t.*

$$\|b_1\| \ldots \|b_n\| \leq 2^{n(n-1)/4} |det(A)|$$

PROOF. Set $D = A^T A$ and apply the last theorem. This gives a basis $b_1, \ldots, b_n$ for $\mathbb{Z}^n$ s.t.

$$\|Ab_1\| \ldots \|Ab_n\| = \sqrt{b_1^T D b_1} \ldots \sqrt{b_n^T D b_n} \quad \leq 2^{n(n-1)/4} det(D)^{1/2} = 2^{n(n-1)/4} |det(A)|$$

The vectors $\|Ab_1\|, \ldots, \|Ab_n\|$ form a basis for the lattice. □

3.3.1. Application: Finding shortest nonzero vector in a lattice. From Minkowski, any n-dim lattice has a nonzero vector b with

$$\|b\| \leq 2(\frac{det(\Lambda)}{V_n})^{1/n}$$

where V_n is the volume of the n-dim unit ball. No poly-time algo is know to find this b. It is thought that finding the shortest nonzero vector in a lattice is NP-complete. But

we can find a 'longer short vector' in a lattice, by taking the shortest vector in the basis constructed there.

Corollary 50. *There exists a poly-algo which, given a nonsingular rational matrix A, finds a nonzero vector b in the lattice generated by the columns of A with $\|b\| \leq 2^{n(n-1)/4} det(\Lambda)^{1/n}$*

PROOF. From the last corollary,

$$\|Ab_1\| = //b_1// \ = (\Pi_{k=1}^n //b *_1 //^{1/n} \leq (\Pi_{k=1}^n 2^{(k-1)/2} //b_k^*//)^{1/n} \ = (2^{n(n-1)/4} det(\Lambda))^{1/2}$$

□

So we can use LLL to find a short vonzero vector, but generally NOT THE SHORTEST.

3.3.2. Application: Finding shortest nonzero vector in a lattice. We saw this one in the other book already. Nothing new.

3.3.3. Application: Finding HNF. Let A be a nonsingular integral matrix of order n. Let $M = \lceil 2^{n(n-1)/4} |det(A)| \rceil$. Let C arise from A by multiplying the ith row of A by M^{n-i} for $i = 1, \ldots, n$.

We can find in poly-time a basis $b_1, \ldots, b_n$ for the lattice generated by the columns of C s.t.

$$\|b_1\| \ldots \|b_n\| \leq 2^{n(n-1)/4} |det(C)| = 2^{n(n-1)/4} M^{n(n-1)/2} |det(A)|$$

These vectors can be reordered in such a way that the matrix $[b_1, \ldots, b_n]$ is lower triangular. We can assume (by reordering) the jth corrdinate of b_j is at least M^{n-j} in abs. value, and so $\|b_j\| \geq M^{n-j}$. Why?: Assume the ith coordinate of b_k is nonzero for some $1 \leq i < k \leq n$. Then $\|b_k\| > M^{n-i} M \geq M^{n-k} M$ and

$$\|b_1\| \ldots \|b_n\| > (\Pi_{j=1}^n M^{n-j}) M \geq 2^{n(n-1)/2} M^{n(n-1)/2)} |det(A)|$$

a contradiction to what is above.

So $b_1, \ldots, b_n$ can be reordered s.t. the matrix B is lower triangular. Then we can multiply by elm. column operations to make B in HNF (nonnegagive, largest row element on the diagional,etc).

Dividing the HNF's jth row by M^{n-j} for each j gives the HNF of A.

CHAPTER 4

Book: Lattice Basis Reduction: LLL and its Applications.

Most text/math came from [2].

In this book, lattice generating points are placed in a row of a matrix and not its columns.

I just want to list the names of some algorithms that LLL is part of or improves on.

4.1. Fincke-Pohst Algorithm

We want to find all lattice points inside a box by looking inside an ellipsoid.

Let columns of lattice be in B. Let $G = B^T B$ be the Gramm matrix. The Cholesky decomposition is $G = U^T D U$.

The FP Algorithm is to find $\|Bx\|^2 \leq C$. Note that

$$\begin{aligned}\|Bx\|^2 &= (Bx)^T(Bx)\\ &= x^T(B^T B)x\\ &= x^T G x\\ &= \sum_{i=1}^{m} d_i(x_i + \sum_{j=i+1}^{m} u_{ij}x_j)^2 \leq C\end{aligned}$$

where $x = (x_1, \cdots, x_m) \in \mathbb{R}^m$.

Look at $i = m$ first then we bounds on what integers x_m could be

$$\left\lceil -\sqrt{C/d_m} \right\rceil \leq x_m \leq \left\lfloor \sqrt{C/d_m} \right\rfloor.$$

Then for each x_m loop over what x_{m-1}.

In general, let $S_k = \sum_{i=k+1}^{m} d_i(x_i + \sum_{j=i+1}^{m} u_{ij}x_j)^2$, and $T_k = \sum_{j=k+1}^{m} u_{kj}x_j$.Then

$$\left\lceil -\sqrt{\frac{C - S_k}{d_k}} \right\rceil \leq x_k \leq \left\lfloor \sqrt{\frac{C - S_k}{d_k}} \right\rfloor.$$

Now lets use LLL. Write $G = U^T D U = R^T R$.

Find R^{-1}, and think of its rows as a lattice. Do LLL on the rows and save the result in the rows of S^{-1}. Find x^{-1} st $S^{-1} = X^{-1}R^{-1}$. Let P be a permutation matrix s.t. the rows of $(SP)^{-1}$ has decreasing Euclidean norm. Make the Gram matrix $H = (SP)^T(SP)$.

Apply Fincke-Pohst to H. If z is one of the coeff. vectors, let $y = Pz$, then change the basis to $x = Xy$. Then the short lattice vectors are $w = Bx$.

4.2. Polynomial Factorization

Let $f \in \mathbb{F}_{p^n}[x]$ be square-free, because this is a UFD, $f = \Pi g_i$. Group producds of distince irreducible factors of d into h_d.

Definition 51. distinct-degree decomposition of f (which is sqare-free) is the seq. ddd(f)=$[h_1, h_2, \cdots, h_d]$.

We can find the square-free part of f by dividing by f by the GCD(f, f').

Theorem 52. *$q = p^n$,p is prime. $i \geq 1$.In $\mathbb{F}_q[x]$,$x^{q^i} - x = \prod_{d \| i} \prod_{deg(f)=d} f$ where the 2nd product is over all f monic irreducibles.*

This thorem gives us $h1 = GCD(f, x^q - x)$, then divide $f_1 := f/h_1$ and find $h_2 = gcd(f_1, x^{q^2} - x)$. Then divide and let $f_2 := f_1/h_2$ and find $h_3 = GCD(f_2, x^{q^3} - x)$, and so on

4.2.1. Equal degree decomposition. Given a h_d, want to find $h_d = \prod_{j=1}^{l_d} h_{dj}$ where $deg(h_{dj}) = d$.

Theorem 53. *g be a randomrniformly distributed non-constannt polynomial with $deg(g) < deg(h)$.*

If $gcd(g, h) \neq 1$, then $gcd(g, h)$ is a proper factor of h. If $gcd(g, h) = 1$, then $\bar{g} = GCD(\overline{g^e} - 1, h), e = (q^d - 1)/2$, where the bar denotes remainder mod h, is a proper factor of h with probability $\geq 1/2$.

4.2.2. Hensel lifting of a polynomial factorizatoin. Let $f \in \mathbb{F}[x]$, let p be prime and not divide the leading coeff. of f. Assume we have $\bar{f} = \bar{g}_1 \bar{h}_1$ in $\mathbb{F}[x]$ with $g_1, h_1 \in \mathbb{Z}[x]$, where the bar is taking the coeff. mod p. We want to find $g_2, h_2 \in \mathbb{Z}[x]$ s.t. $deg(g_1) = deg(g_2)$ and $deg(h_1) = deg(h_2)$ and $f = g_2 h_2 \mod p^2$. We want to lift the factorization from the ring $(\mathbb{Z}/p\mathbb{Z})[x]$ to $(\mathbb{Z}/p^2\mathbb{Z})[x]$ (which is not a field because $p * p = 0 \mod p^2$). Repeating this lifting we can get $f = g_n h_n \mod p^{2^n}$. See Algorithm 5.

4.2.3. Polynomial factorizatoin over $\mathbb{Z}[x]$ and not just $(\mathbb{Z}/m\mathbb{Z})[x]$. There is something called the Zassenhaus factorization algorithm (for finite fields?). Then von zur Gathen and Gerhard developed the following

It is clear Algorithm 6 is exponential in the worst case because of the "every subset" loop, but this is where LLL comes to save the day.

Theorem 54. *$f, g \in \mathbb{Z}[x]$ where f is deg $n > 0$ and g is degree $m > 0$. Let $u \in \mathbb{Z}[x]$ be monic and nonconstant and $f = uv_1 \mod m$ and $g = uv_2 \mod m$ for some $v_1, v_2 \in \mathbb{Z}[x]$. Assume $m > \|f\|_2^k \|g\|_2^n$. Then $GCD(f, g)$ is nonconstant.*

Algorithm 5 Hensel lifting

Input: Polynomials $f, g_1, h_2 \in \mathbb{Z}[x]$ s.t $f = g_1 h_1 \mod m$,

Input: Polynomials $s_1, t_1 \in \mathbb{Z}[x]$ s.t. $s_1 g_1 + t_1 h_1 = 1 \mod m$, $deg(s_1) < deg(h1)$, $deg(t_1) < deg(g_1)$.

Output: Polynomials $g_2, h_2 \in \mathbb{Z}[x]$,s.t. $f = g_2 h_2 \mod m^2$ and the deg's of the g's are equal and $g_2 = g_1 \mod m$ and likewise for the h's.

Output: Polynomials $s_2, t_t \in \mathbb{Z}[x]$ s.t. $s_2 g_2 + t_2 h_2 = 1 \mod m^2$ and $s_2 = s_1 \mod m$ and $deg(s_2) < deg(h_2)$ and likewise for the t's.

$e := f - g_1 h_1 \mod m^2$

Find $q, r \in \mathbb{Z}[x]$ s.t $s_1 e = q h_1 + r \mod m^2$

$g_2 := g_1 + t_1 e + q g_1 \mod m^2$

$h_2 := h_1 + r \mod m^2$

$e^* := s_1 g_2 + t_1 h_2 - 1 \mod m^2$

Find $q*, r* \in \mathbb{Z}[x]$ s.t. $s_1 e^* = q^* h_2 + r^* \mod m^2$

$s_2 := s_1 - r^* \mod m^2$

$t_1 := t_1 - t_1 e^* - q * g_2 \mod m^2$

return g_2, h_2, s_2, t_2

Let f be squarefree and primative of deg n. Let u be monic and nnonconstant with $d = deg(g) < n$ and $f = uv \mod m$ where $m = p^k$. We want to find a poly $g \in \mathbb{Z}[x]$ s.t. $m > \|g\|_2^n \|f\|_2^{deg(g)}$. Then by the lemma $GCD(f, g)$ is nonconstant and hence a factor in $\mathbb{Z}[x]$.

Let $j \in \{d+1, \ldots, n\}$ We want to find g of deg $< j$. Write a polynomal as a list of its coefficient vector. Let $L \subset \mathbb{Z}^j$ be the lattice with a basis consisting of the coefficient vectors of polynomials

$$\{u, xu, x^2 u, \cdots, x^{j-d-1} u\} \cup \{m, mx, \ldots, mx^{d-1}\}$$

There are $j - d + d$ elements of this basis and they are lin independent b/c each has a unique degree (m in an integer and u has deg d). A general $g \in L$ has the from $\sum q_i x^i u + \sum r_i m x^i = qu + mr$. Hence $g = qu \mod m$.So u divides g mod m. Therefore, $g \in L \Rightarrow deg(g) < j$ and u divides $g \mod m$.

Conversely, assume $deg(g) < j$ and u divides $g \mod m$. Then $g = q_1 u + m r_1$. B/c u is monic, $r_1 = q_2 u + r_2$ for some q_2, r_2. Then

$$(q_1 + m q_2) u + m r_2 = q_1 u r_1 m = g.$$

It is clear that $deg(r_2) < deg(u)$, $deg(q_1) \leq deg(g) - deg(u) < j - d$ and $deg(q_2) \leq deg(r_1) - deg(u) < j - d$. Thus $g \in L$.

Hence gŁ $\Leftrightarrow deg(g) < j, u \mid g \mod m$.

Algorithm 6 Polynomial Factoring

Input: Squarefree primative non-constant poly $f \in \mathbb{Z}[x]$.
Output: The factors of f over $\mathbb{Z}[x]$.

$n = deg(f)$
$C := (n+1)^{2n} \|f\|_\infty^{2n-1}$
$B := (n+1)^{1/2} 2^n \|f\|_\infty * L(f)$ where $L(f)$ is leading coeff of f.
$r := \lceil 2 \log C \rceil$
Find prime s.t. $p < 2r \ln r$, p does not divide $L(f)$ nor the polynomial discriminant (det of Sylvester matrix of polynomials) of f.
$k := \lceil \log_p(2B+1) \rceil$
Factor $\bar{f} = \bar{L}(f)\bar{h}_1 \cdots \bar{h}_r$ in $\mathbb{F}_p[x]$ using symmetric representatives $\|h_i\|_\infty < p/2$. I think this uses Zassenhaus.
Use Hensal to find monic polynomials $f = L(f)g_1 \cdots g_r \mod p^k$ and $g_i = h_i \mod p$ while using symmetric representatives $\|g_i\|_\infty < p^k/2$.
$T := \{1, 2, \cdots, r\}; s := 1; F := f$
while $2s \leq size(T)$ **do**
  for every s-slement subtset of T called S **do**
    Find $G, H \in \mathbb{Z}[x]$ s.t. $\|G\|_\infty, \|H\|_\infty < p^k/2$
    s.t. $G = L(F) \prod_{i \in S} g_i \mod p^k$
    and $H = L(F) \prod_{i \in T-S} g_i \mod p^k$
    if $\|G\|_1 \|H\|_1 \leq B$ **then**
      Append $prim(G)$ to result.
      $T := T - S$
      $F := prim(H)$
    end if
  end for
end while
Append F to result
return result.

This justifies the use of LLL, but we also want $\|g\|_2^n < m \|f\|_2^{-deg(g)}$. Use LLL with $\alpha = 3/4$ we get that for any g in the lattice $\|g_1\|_2 \leq 2^{(j-1)/2} \|g\|_2 \leq 2^{n/2} \|g\|_2$. But Mignotte's bound lemma gives that $\|g\|_\infty \leq \|g\|_2 \leq B$ where $B = (n+1)^{1/2} 2^n \max(\|f\|_\infty, \|g\|_\infty)$.

Then $\|g_1\|_2 \leq 2^{n/2} B$. Hence

$$\|g_1\|_2^{j-1} \|g\|_2^{deg(g_1)} < (2^{n/2}B)^n B^n = 2^{n^2/2}(n+1)^{1/2} 2^{2n^2} \max(\|f\|_\infty, \|g\|_\infty)^{2n} \leq p^k,$$

by the choice of k in the factorication algorithms. By the lemma above, $GCD(g, g_1)$ is nonconstant in $\mathbb{Z}[x]$.

Hence in the factorization algorithm, we can replace the "every subset" loop with a call to LLL for every monic divisor h_d ??? (I'm not sure exactly).

Bibliography

[1] A. I. Barvinok, *Integer points in polyhedra*, Zürich Lectures in Advanced Mathematics, European Mathematical Society (EMS), Zürich, Switzerland, 2008.

[2] M. Bremner, *Lattice basis reduction: introduction to the lll algorithm and its applications*, Pure and Applied Mathematics, CRC Press: Chapman and Hall book, Boca Raton, FL, 2012.

[3] W. L. Nemhauser, George, *Iteger and combinatorial optimization*, Wiley-Interscience series in discrete mathematics and optimization, Wiley-Interscience, New York, 1988.

[4] A. Schrijver, *Theory of linear and integer programming*, Wiley-Interscience, 1986.