LATTICE BASIS REDUCTION AND SHORT VECTORS

NILS BRUIN

Disclaimer: This is a first draft which hasn't even been carefully proofread–you guys will be doing that! There could be gross typos here.

1. A little motivation: rational and integer approximations

Sometimes surprising relations between mathematical constants arise. For instance, we have

$$\zeta(2) = \frac{1}{6}\pi^2, \ \int_{-\infty}^{\infty} e^{-x^2}dx = \sqrt{\pi}$$

and, if $\{F_n\}_n = \{1, 1, 2, 3, 5, 8, 11, 13, \ldots\}$ is the fibonacci series then

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \frac{1+\sqrt{5}}{2}$$

Each of these relations has its own proof. However, before you can set of to find a proof, you'd first need to *find* the relation that you're trying to prove. In each of these cases, it is fairly easy to find numerical approximations to the constants involved. So perhaps we can try and let a computer try and find likely relations from these approximations?

Definition 1. Let $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$. We say that $\alpha_1, \ldots, \alpha_r$ are *linearly dependent* over $\mathbb{Q}$ (or $\mathbb{Z}$) if there are $x_0, \ldots, x_r \in \mathbb{Q}$ (or $\mathbb{Z}$), not all zero, such that

$$x_0 + x_1\alpha_1 + \cdots + x_r\alpha_r = 0$$

Lemma 2. *The numbers $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ are linearly dependent over $\mathbb{Q}$ if and only if they are over $\mathbb{Z}$.*

Proof. Since $\mathbb{Z} \subset \mathbb{Q}$, we see that a $\mathbb{Z}$-linear dependency is also a $\mathbb{Q}$-linear dependency. It remains to show that a $\mathbb{Q}$-linear dependency gives rise to a $\mathbb{Z}$-linear dependency. But this is straightforward by clearing denominators: For each $x_i \in \mathbb{Q}$ there is a denominator, i.e., a number $d_i \in \mathbb{Z}$ such that $d_i x_i \in \mathbb{Z}$. But then for $d = \mathrm{lcm}(d_0, \ldots, d_r)$ we have $dx_i \in \mathbb{Z}$ for all i, and if the x_i is non-zero then so is dx_i. Hence

$$(dx_0) + (dx_1)\alpha_1 + \cdots + (dx_r)\alpha_r = d0 = 0$$

yields a $\mathbb{Z}$-linear dependency. □

Finding a linear dependency is now a matter of finding a vector $(x_0, \ldots, x_r) \in \mathbb{Z}^r$ such that

$$x_0 + x_1\alpha_1 + \cdots + x_r\alpha_r = 0.$$

That's a useful formulation to have, but it does not help us much with actually *solving* the problem. We would like to be able to find likely solutions to this equation using *approximations* of the α_i. That means we can only hope for the equation to *approximately* hold too. That's a problem: we can make that value as small as we like:

Date: July 15, 2014.

Theorem 3. *Let $\alpha_0, \ldots, \alpha_r \in \mathbb{R}$ with $M = \max_i |a_i|$. Let $B > 1$. Then there are $x_0, \ldots, x_i \in \mathbb{Z}$ with $|x_i| \leq B$ such that*

$$|x_0\alpha_0 + \cdots + x_r\alpha_r| < \epsilon = \frac{(r+1)M}{B^{r-1}(B+r+1)}$$

Proof. First consider $x_i \in \{0, \ldots, B\}$. Then

$$|x_0\alpha_0 + \cdots + x_r\alpha_r| < (r+1)MB$$

Note that if we split the interval $(0, (r+1)MB)$ into subintervals of length ϵ, then we end up with less than $(B+1)^{r+1}$ intervals. That is less than the number of choices we have for the x_i. Hence, two choices $y_0, \ldots, y_r$ and $z_0, \ldots, z_r$ must yield a value in the same interval and hence we have

$$|y_0\alpha_0 + \cdots + y_r\alpha_r| - |z_0\alpha_0 + \cdots + z_r\alpha_r| < \epsilon$$

Hence, taking $x_i = y_i - z_i$ gives us the desired solution. □

Remark 4. Note that $\epsilon \sim 1/B^r$ as $B \to \infty$.

Results like this are basically quantitative versions of the statement that $\mathbb{Q}$ lies dense in $\mathbb{Z}$: they give you a sense of *how* dense they are. Indeed, the first proof of density usually gives you a result using rational numbers where the denominators are only, say, powers of 10. Quantitative version of that are not good enough for our application.

Corollary 5 (Dirichlet)**.** *Let $\alpha \in \mathbb{R}$ be an irrational number. Then there are infinitely many fractions $p/q \in \mathbb{Q}$ such that*

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2}$$

Exercise 1. Prove this. Beware that it's more a corollary of the method of proof than of the actual statement here. The most direct application would be from considering $|q\alpha - p|$ and then divide by q. That would give the right kind of result if $q = B$. So in particular, you shouldn't bound the numerator p (which indeed Dirichlet doesn't say anything about).

It may be worth observing too that Dirichlet's result is not *quite* the sharpest possible: Continued fractions give approximations with $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$. Lagrange proved that $|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$ is in fact possible and for $\alpha = \frac{1+\sqrt{5}}{2}$ this is best possible. In that sense, the golden ratio is the worst rationally approximable number.

Anyway, for us the main lesson from this is that we shouldn't just look for integers that make $|x_0\alpha_0 + \cdots + x_r\alpha_r|$, we should be looking for integers $x_0, \ldots, x_r$ that make this expression small *compared to the size of* $x_0, \ldots, x_r$. One way of doing that is by choosing $N > 0$ and trying to find integers $x_0, \ldots, x_r$ (not all zero) that make the following expression small:

$$x_0^2 + x_1^2 + \cdots + x_r^2 + (N\sum_{i=0}^{r} x_i\alpha_i)^2$$

Note that this amounts to finding a vector of small norm, i.e., a *short vector*. The set in which we try to find such a vector can be written using linear algebra as a set of row-vectors:

$$\{(x_0, \ldots, x_r) \begin{pmatrix} 1 & 0 & \cdots & 0 & N\alpha_0 \\ 0 & 1 & \cdots & 0 & N\alpha_1 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 1 & N\alpha_r \end{pmatrix} : x_0, \ldots, x_r \in \mathbb{Z}^{r+1}\}$$

2. Lattices

In the previous section we saw that we are interested in finding short vectors in sets that are described by integer linear combinations over vectors in $\mathbb{R}^n$. We refer to this vector space as the *ambient vector space*.

Definition 6. A *lattice* $\Lambda \subset \mathbb{R}^n$ is a finitely generated discrete subgroup of $\mathbb{R}^n$. Equivalently, (this uses the structure theorem for finitely generated abelian groups!) a lattice is a group $\mathbb{Z}^r$, together with a group homomorphism $\mathbb{Z}^r \to \mathbb{R}^n$ such that the image is discrete.

The *discrete* part is important, For instance, $\{a + \sqrt{2}b : a, b \in \mathbb{Z}\} \subset \mathbb{R}^1$ is a finitely generated subgroup of the 1-dimensional vector space $\mathbb{R}^1$, but, as we've seen, it contains arbitrarily short vectors, so it isn't a *discrete* subgroup.

Remark 7. Note that $\mathbb{R}^n$ as an additive group doesn't contain any finite order elements (when you add a nonzero vector to itself repeatedly, you never get the zero vector), so any subgroup is also *torsion-free*. The structure theorem for finitely generated abelian groups tells us then that the subgroup is isomorphic to $\mathbb{Z}^r$, and also that $\mathbb{Z}^r$ and $\mathbb{Z}^s$ are isomorphic if and only if $r = s$. This is called the *rank* of a lattice.

Given a lattice $\Lambda \subset \mathbb{R}^n$ of rank r, we can consider the $\mathbb{R}$-*span* of Λ: the set of $\mathbb{R}$-linear combinations of elements of Λ. This is the smallest $\mathbb{R}$-sub vector space of $\mathbb{R}^n$ that contains Λ. We write $\mathbb{R}\Lambda$ for this.

Lemma 8. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice of rank r. Then* $\dim_{\mathbb{R}} \mathbb{R}\Lambda = r$.

Exercise 2. Prove this. You can do so by adapting the proof strategy of Theorem 3: assume that $\dim_{\mathbb{R}} \mathbb{R}\Lambda < r$ and show that the number of lattice elements that you can make using $\mathbb{Z}$-linear combinations of bounded size from generators grows faster than the volume of the ball in which you know they lie, so they need to accumulate somewhere.

For now we will concentrate on *full rank* lattices, i.e., lattices $\Lambda \subset \mathbb{R}^n$ with rank n. Lattices like this can be represented by a square $n \times n$ matrix, of rank n, such that Λ consists exactly of the $\mathbb{Z}$-linear combinations of the rows of the matrix. We say that the rows for a *lattice basis* of Λ. As we have formulated above, the discreteness of the basis implies thatr the lattice basis is also $\mathbb{R}$-linearly independent, and hence a basis for $\mathbb{R}\Lambda$. For a full rank lattice, a lattice basis is also a basis of the ambient vector space.

Almost all elementary linear algebra algorithms depend on gaussian elimination: Performing elementary row operations on a matrix to get the matrix in a particular form. The key is that row operations do not change the vector space spanned by the row vectors. We can do something similar with lattice bases:

Proposition 9. *Let $\{\mathbf{b}_1, \ldots, \mathbf{b}_r\} \subset \mathbb{R}^n$ be a lattice basis. The following operations do not change the lattice generated by these vectors:*

1. *Replace $\mathbf{b}_i$ by $\mathbf{b}_i + c\mathbf{b}_j$, where $j \neq i$ and $c \in \mathbb{Z}$*
2. *Swap $\mathbf{b}_j$ with $\mathbf{b}_j$*
3. *Replace $\mathbf{b}_i$ by $-\mathbf{b}_i$.*

These are almost the same row operations as in linear algebra, except that we can only add an *integer* multiple of one row to another and that we can't scale basis vectors: we can only multiply by ± 1. That is of course because ± 1 are the only invertible elements in $\mathbb{Z}$.

Proposition 10. *Let B be a square $n \times n$ matrix, whose rows span a lattice $\Lambda \subset \mathbb{R}^n$. Let C be another $n \times n$ matrix. Then the rows of C span Λ if and only if there is an integer valued matrix A with* $\det(A) = \pm 1$ *such that $C = BA$.*

In particular, we see that the (absolute) determinant $|\det(B)|$ is a property of Λ itself.

3. Inner products and orthogonalization

In the previous section we have seen that the (squared) norm function on $\mathbb{R}^n$ is important for us. In fact, the standard *inner product* is even more important. One can be derived from the other, though. Let $\mathbf{v} = (v_1, \ldots, v_n), \mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{R}^n$ and consider

$$||\mathbf{v}||^2 = v_1^2 + \cdots + v_n^2$$
$$\mathbf{v} \cdot \mathbf{w} = v_1 w_1 + \cdots + v_n w_n$$

Naturally, the norm can be recovered from the dot product via $||\mathbf{v}|| = \mathbf{v} \cdot \mathbf{v}$. The converse also works:

$$\mathbf{v} \cdot \mathbf{w} = \frac{1}{2}||\mathbf{v} + \mathbf{w}||^2 - ||\mathbf{v}||^2 - ||\mathbf{w}||^2$$

Definition 11 (Gram-Schmidt)**.** Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be an independent set of vectors. We defined the associated *Gram-Schmidt* basis by

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^* \text{ where } \mu_{i,j} = \frac{\mathbf{b}_i \cdot \mathbf{b}_j^*}{\mathbf{b}_j^* \cdot \mathbf{b}_j^*} \text{ for } 1 \leq j < i \leq n$$

Proposition 12. *The subspace spanned by $\mathbf{b}_1, \ldots, \mathbf{b}_r$ equals the subspace spanned by $\mathbf{b}_1^*, \ldots, \mathbf{b}_r^*$. Furthermore, $||\mathbf{b}_i^*||^2 \leq ||bb_i||^2$. If B is a square matrix with rows $\mathbf{b}_1, \ldots, \mathbf{b}_n$ and B^* is the matrix with rows $\mathbf{b}_1, \ldots, \mathbf{b}_n^*$ then $\det(B) = \det(B^*)$.*

Lemma 13. *Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be orthogonal non-zero vectors in $\mathbb{R}^n$, i.e., $\mathbf{b}_i \cdot \mathbf{b}_j = 0$ for $i \neq j$. Then*

$$\det(B)^2 = ||\mathbf{b}_1||^2 \cdots ||\mathbf{b}_n||^2$$

Proof. Use that $\det(B^2) = \det(BB^T)$. □

Theorem 14 (Hadamard's inequality)**.**

$$\det(B)^2 \leq ||\mathbf{b}_1||^2 \cdots ||\mathbf{b}_n||^2$$

Proof. Use Gram-Schmidt orthogonalization. □

This gives us an important hint on how to find short vectors in a lattice: The determinant is a property of the lattice and the product of the norms of a $\mathbb{Z}$-basis of the lattice will never be smaller than the determinant and, if we can find an orthogonal basis, then we have equality. We even have a way of getting an orthogonal set of vectors out of a given set: Apply Gram-Schmidt orthogonalization. The problem is that Gram-Schmidt does not apply lattice-preserving operations: The multiple $\mu_{i,j}$ is likely not an integer.

4. LLL-reduced basis

In general it is too much to ask that we find an orthogonal basis for a lattice: there may just not exist one. Therefore, we formulate a weaker property, in the hope that it is still good enough for our applications and that it is still attainable:

Definition 15. Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a lattice basis and let $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ be the corresponding orthogonalized basis (which is not a basis of the same lattice!). We say the basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is *LLL-reduced* if

$$|\mu_{i,j} \leq \frac{1}{2}| \text{ for } 1 \leq j < i \leq n$$

and

$$||\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*||^2 \geq \frac{3}{4}||\mathbf{b}_{i-1}^*||^2$$

or equivalently

$$||\mathbf{b}_i^*||^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)||\mathbf{b}_{i-1}^*||^2$$

We'll see later that every lattice indeed has an LLL-reduced basis, but first we show that we have the right properties.

Theorem 16. *Suppose $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is an LLL-reduced basis of a lattice $\Lambda \subset \mathbb{R}^n$. Then*

(1) $\det(\Lambda)^2 \leq \prod_{i=1}^n ||\mathbf{b}_i||^2 \leq 2^{n(n-1)/2} \det(\Lambda)^2$
(2) $||\mathbf{b}_j||^2 \leq 2^{i-1}||\mathbf{b}_i^*||$ *for* $1 \leq j < i <\leq n$
(3) $||\mathbf{b}_1||^2 \leq 2^{(n-1)/2} \det(\Lambda)^{2/n}$
(4) *For every non-zero vector* $\mathbf{v} \in \Lambda$ *we have* $||\mathbf{b}_1||^2 \leq 2^{n-1}||\mathbf{v}||^2$.
(5) *For any linearly independent vectors* $\mathbf{v}_1, \ldots, \mathbf{v}_t \in \Lambda$ *we have*

$$||\mathbf{b}_j||^2 \leq 2^{n-1} \max(||\mathbf{v}_1||^2, \ldots, ||\mathbf{v}_t||^2) \text{ for } 1 \leq j \leq t$$

So we see that, in a very precise sense, $\mathbf{b}_1$ is not too much bigger than the shortest vector in Λ.

The algorithm is now quite straightforward, although the proof that it actually terminates and does so quickly, is quite involved. We write $\lfloor \alpha \rceil$ for the *nearest* integer to α (break tie however you like).

LLL-algorithm

Input: Sequence of independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \subset \mathbb{R}^m$
Output: LLL-reduced basis for lattice spanned by input.

(1) Set $k = 2$
(2) Ensure first LLL-condition holds at k: Set

$$\mathbf{b}_k := \mathbf{b}_k - \left\lfloor \frac{\mathbf{b}_k \cdot \mathbf{b}_{k-1}^*}{||\mathbf{b}_{k-1}^*||^2} \right\rceil \mathbf{b}_{k-1}$$

(3) Swap if second condition requires it: If $||\mathbf{b}_k||^2 < (3/4 - \mu_{k,k-1}^2)||\mathbf{b}_{k-1}^*||^2$, swap $\mathbf{b}_{k-1}$ and $\mathbf{b}_k$, decrease k (unless k was already 2), and go to step (3). Otherwise set

$$\mathbf{b}_k := \mathbf{b}_k - \sum_{i=1}^{k-2} \left\lfloor \frac{\mathbf{b}_k \cdot \mathbf{b}_i^*}{||\mathbf{b}_i^*||^2} \right\rceil \mathbf{b}_i$$

and increment k.
(4) If $k \leq n$ go to step 2. Otherwise the $\mathbf{b}_i$ form an LLL-reduced basis.

It is fairly easy to check that *if* this algorithm finishes, then the returned basis does satisfy the LLL properies. So the art is in proving that the algorithm finishes.

We will not do the proof in detail (you can look it up!). The trick is to show that the number of swaps that occur (in step (3)) must be finite. That means that k only gets decreased a finite number of times, and since the alternative is increasing k, we see that $k > n$ at some point.

The trick is to look at

$$d_i = \det(\mathbf{b}_r \cdot \mathbf{b}_s)_{1 \leq r,s \leq i}$$

It is straightforward to check that

$$d_i = \prod_{j=1}^{i} ||\mathbf{b}_j^*||^2$$

and in particular that $d_0 = 1, d_n = \det(\Lambda)^2$. One now needs to show that the d_i are bounded below in terms of Λ and that step (3) will decrease d_i by a non-negligible amount.

Remark 17. Note that the above asserts that we can find *a* LLL-reduced basis; not that such a basis is in any way unique. The result one gets back in practice is quite dependent on the basis you start with.

Remark 18. The argument above gives a suggestion that the algorithm finishes. In fact, one of the key results is that it does so *fairly quickly*: The runtime can be proven to be $O(n^6 \ln^3 B)$ if $|\mathbf{b}_i|^2 \leq B$ for all i and the vectors are integer valued (this is less of a restriction than it may seem), and in practice is often much better.

The algorithm above can be tweaked quite a bit. There is a large literature on finding optimized algorithms to compute reduced bases.

5. Applications to finding integer relations

Going back to the original problem, say for finding an integer relation between $1, \pi, \pi^2, \zeta(2)$, we set up a matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & N \\ 0 & 1 & 0 & 0 & N\pi \\ 0 & 0 & 1 & 0 & N\pi^2 \\ 0 & 0 & 0 & 1 & N\zeta(2) \end{pmatrix}$$

for some large number N (perhaps $N = 10^{100}$ if we can get 100 digits for each?). The larger N, the less our concept of "short vector" is influenced by the size of the integers x_0, x_1, x_2, x_3 that we hope to find.

We take the lattice generated by the rows of this matrix and compute an LLL-reduced basis for it. If there is a relation

$$x_0 + x_1\pi + x_2\pi^2 + x_3\zeta(2) = 0$$

with the x_i much smaller than N, then this relation would likely show up as the first vector in an LLL-reduced basis.

In many implementations of the LLL algorithm, an integer-valued matrix is required. Note that once N is chosen large enough, rounding the last column to integers should hardly affect the shape of the lattice.

6. Further exercises

Exercise 3. The extended Euclidean algorithm, which takes as input $a, b \in \mathbb{Z}$ and produces $x, y \in \mathbb{Z}$ such that $xa + yb = \gcd(a, b)$, can also be considered as finding a $\mathbb{Z}$-linear dependence between $a, b, 1$. Take your favourite a, b and try and determine x, y using LLL. How does that compare to running the Euclidean algorithm? (the Euclidean algorithm is a source of inspiration for LLL)

Exercise 4. You may know that $\arctan(1) = \pi/4$ and that the taylor-series obtained from $\arctan(x) = \int_0^x \frac{1}{1+t^2} dt$ converges for $x = 1$. This gives a series that converges to $\pi/4$ and hence gives a way to approximate π. The series only converges conditionally as a harmonic series, though, so convergence is quite slow. Much better results arise from

$$\pi/4 = \arctan(1/2) + \arctan(1/3)$$

(can you prove that identity?) because for $x = 1/2$ and $x = 1/3$ the series converge geometrically (and hence quite well). Even better results can be obtained from *Machin's formula*:

$$\frac{\pi}{4} = 4\arctan(1/5) - \arctan(1/239)$$

(convergence is better for smaller numbers).

Can you find similar formulas? Can you find better ones?

Look up the Borwein-Borwein-Plouffe formula. It is a similar formula for π but with some extra, interesting (binary) property. Integer relation finding algorithms played an important role in finding this formula.

Exercise 5. Experiment with trying to (re)discover relations between multiple zeta values. The recipe is simple: Concoct a nice collection of values you conjecture an integer relation between (make sure you can compute plenty of digits of each of these values!), place them into a matrix in the appropriate way, and try and find relations.

Exercise 6. Look up the PSLQ algorithm by Ferguson-Bailey-Arno. It is a close cousin to LLL, but it is purpose-built for finding integer relations, so it may do a more efficient job at it.

References

Further reading: The first reference is a comprehensive, basic description of the LLL basis reduction algorithm, together with several improvements and variants.

The original article by Lenstra, Lenstra and Lovazs is quite readable as well.

A little literature search will show ample references. Lattice basis reduction is a very active field with many applications, including cryptography (some of the most promissing post-quantum cryptosystems are based on lattices).

[1] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR1228206 (94i:11105)

[2] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534, DOI 10.1007/BF01457454. MR682664 (84a:12002)