Some applications of LLL

a. Factorization of polynomials

As the title *Factoring polynomials with rational coefficients* of the original paper in which the LLL algorithm was first published (Mathematische Annalen **261** (1982), 515–534) suggests, the initial motivation was the proof of the following result.

Theorem *There exists an algorithm that factors any primitive polynomial $f \in \mathbb{Z}[x]$ in polynomial time ($\mathcal{O}(n^{12} + n^9(\log |f|)^3$ bit operations).*

The main steps of the algorithm are

1. Use the subresultant algorithm to compute common factors of f and f', and replace f by its squarefree part.

2. Find a suitable prime p and factor $f \bmod p$ in $\mathbb{F}_p[x]$ into irreducibles using Berlekamp's algorithm.

3. For an irreducible factor $h \in \mathbb{F}_p[x]$ and a suitable k use Hensel lifting modulo p^k to find a factor of $f \bmod p^k$; now use LLL to find the unique factor $h_0 \in \mathbb{Z}[x]$ of f such that $h_0 \equiv h \bmod p$. Repeat this for remaining factors.

An algorithm for the factorization of polynomials with coefficients in a number field uses two rounds of applications of LLL.

b. Diophantine approximation

Another application that is found in the original LLL-paper is to the problem of *(simultaneous) Diophantine approximation*: given $n \in \mathbb{N}$, real numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $0 < \epsilon < 1$, there exist integers $p_1, p_2, \ldots, p_n$ and q such that

$$|p_i - q\alpha_i| \leq \epsilon, \quad 1 \leq q \leq \epsilon^{-n},$$

or

$$|\frac{p_i}{q} - \alpha_i| \leq \frac{1}{q^{n+1}}.$$

Applying LLL to the columns of

$$\begin{pmatrix} 1 & 0 & \cdots 0 & -\alpha_1 \\ 0 & 1 & \cdots 0 & -\alpha_2 \\ \vdots & \vdots & \ddots \vdots & \\ 0 & 0 & \cdots 1 & -\alpha_n \\ 0 & 0 & \cdots 0 & 2^{-n(n+1)/4}\epsilon^{n+1} \end{pmatrix}$$

we obtain a polynomial-time algorithm that produces an LLL-reduced basis $b_1, b_2, \ldots, b_{n+1}$. Then

$$|b_1| \leq 2^{n/4} \cdot d^{1/(n+1)} = \epsilon,$$

and by construction $b_1 =$

$$(p_1 - q\alpha_1, p_2 - q\alpha_2, \ldots, p_n - q\alpha_n, q \cdot 2^{-n(n+1)/4}\epsilon^{n+1})^{\mathsf{T}},$$

for certain integers p_i, q. Then certainly all components are less than ϵ and $q \leq 2^{n(n+1)/4}\epsilon^{-n}$.

With $n = 1$ we find the (nearest integer) continued fraction convergents.

c. Sums of squares

Every prime that is 1 mod 4 can be written as sum of two squares. Let $h \in \mathbb{F}_p$ satisfy $h^2 \equiv -1 \bmod p$; for example

$$h = g^{\frac{p-1}{4}} \in \mathbb{F}_p$$

if g is a primitive root modulo p.

Consider the lattice L in $\mathbb{R}^2$ spanned by the vectors $v_1 = \begin{pmatrix} p \\ 0 \end{pmatrix}$, and $v_2 = \begin{pmatrix} h \\ 1 \end{pmatrix}$. The determinant of this lattice is $d(L) = p$. With $b_1 = \begin{pmatrix} u \\ v \end{pmatrix}, b_2$ an LLL-reduced basis for the lattice we get

$$|b_1|^2 \leq (2^{\frac{1}{4}}\sqrt{p})^2 < 2p,$$

so: $u^2 + v^2 < 2p$. On the other hand, for vectors w_1, w_2 in the lattice it holds that the inner product $< w_1, w_2 >$ is divisible by p (as it holds for both basis vectors). Hence $u^2 + v^2 \equiv 0 \bmod p$. Together these imply $u^2 + v^2 = p$.

d. Algebraic dependencies

Suppose that real numbers approximated by $\alpha_1, \alpha_2, \ldots, \alpha_n$ are given. Choose a suitably big integer N and apply LLL-reduction to the lattice spanned by the columns of

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 \\ N\alpha_1 & N\alpha_2 & \cdots & N\alpha_n \end{pmatrix}$$

in $\mathbb{R}^{n+1}$. Then the first vector in a reduced basis of this lattice will be the column

$$(m_1, m_2, \ldots, m_n, N\cdot(m_1\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n))^{\mathsf{T}}$$

of 'small length', which implies that the m_i are not too large while the last component much be close to zero: the corresponding expression $\sum m_i\beta_i$ for the true real numbers β_i will have to be zero.

Special case: minimal polynomials

In the special case that $\alpha_i = \alpha^{i-1}$ for $i = 1, 2, \ldots, n$ and n is the degree of the minimal irreducible polynomial f_α, we will (most likely) recover this!

If the degree of α is not known, we may start with a small choice and increment until we find a solution.

There are slightly different algorithms, devised especially to solve this type of problem: PSLQ, and HJLS. Using this, identities like

$$\pi = \sum_{i=0}^{\infty} \frac{1}{16^i} \left(\frac{4}{8i+1} - \frac{2}{8i-4} - \frac{1}{8i+5} - \frac{1}{8i+6} \right),$$

were discovered.

e. Knapsack

For a while, cryptographic systems based on a version of the *knapsack* problem have been popular. This particular version (called the *subset sum* problem) asks, for given positive integers $m_1, m_2, \ldots, m_n$ and s for an answer to the decision problem: do there exist $z_1, z_2, \ldots, z_n$ in $\{0, 1\}$ such that $s = z_1 m_1 + \cdots + z_n m_n$ (is s a subset sum of the m_i?

In crypto applications the moduli were first chosen superincreasing, that is, for all i it holds that $m_i > \sum_{j<i} m_j$. Next this additional structure is hidden from the user by multiplication and modular reduction.

Now apply lattice basis reduction to the columns

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \\ 0 & 0 & \cdots & 1 & 0 \\ N \cdot m_1 & N \cdot m_2 & \cdots & N \cdot m_n & -Ns \end{pmatrix}$$

for suitable N, will produce a linear combination

$$z_1 \cdot N \cdot m_1 + z_2 \cdot N \cdot m_2 + \cdots + z_n \cdot N \cdot m_n = Ns$$

as desired.

f. abc

The abc-conjecture is a deep, yet easily formulated, problem in number theory. For positive integers a, b, c we define the *radical* $\text{rad}(a, b, c)$ as the product of the distinct prime factors of a, b, c:

$$\text{rad}(a, b, c) = \prod_{\substack{p \text{ prime} \\ p \mid abc}} p.$$

The *quality* q of a, b, c is

$$q(a, b, c) = \frac{\log c}{\log \text{rad}(a, b, c)}.$$

We will assume that $\gcd(a, b, c) = 1$.

abc-**Conjecture** *For every $\eta > 1$ there exist only finitely many a, b, c with $\gcd(a, b, c) = 1$ and $a + b = c$ such that $q(a, b, c) > \eta$.*

There exist infinitely many abc-triples of quality exceeding 1; for example $1+(9^n-1) = 9^n$, then $\mathrm{rad}(abc) = 3 \cdot \mathrm{rad}(b) < c$.

The best known example is $2+3^{10}\cdot 109 = 23^5$ (Reyssat) with $q = 1.629\ldots$.

Triples with $q(a,b,c) > 1.4$ are commonly called *good abc-triples*.

Similarly, one can define *Szpiro triples* as coprime a, b, c with $a+b=c$ for which

$$\rho(a,b,c) = \frac{\log abc}{\log \mathrm{rad}(a,b,c)}$$

is large. Such triples are *good* when $\rho > 4.4$. The best known example was found by Nitaj and has $\rho = 4.419\ldots$:

$$13 \cdot 19^6 + 2^{30} \cdot 5 = 3^{13} \cdot 11^2 \cdot 31.$$

One way to search for examples systematically uses LLL. First generate (many) numbers A, B, C built up from large powers of relatively small primes (to produce small radical) and of comparable size, Then use LLL to find small x, y, z (in absolute value) such that $xA + yB + zC = 0$.

Dokchitser observes that the smallest x, y, z not necessarily produce the best abc triples; it may be necessary to look at small linear combinations in the lattice of solutions.