Computing with Laminated Integral Lattices.

Richard Parker

Aachen Sept 27 2011

My Background

- In 1977 - 1987 I was working with John H Conway, mainly on the Atlas of Finite Groups.
- This naturally included work with the Conway groups (and hence the Leech Lattice).
- In particular the idea of laminated lattices I got from him.
- Conway also told me to study LLL.
- My knowledge of lattices generally is patchy and idiosynchratic.

What is important in maths?

- To get a job!
- To succeed where other, clever people have failed.
- My approach is different.
- To understand everything possible about major computer algorithms.
- And to extract mathematics from algorithms. . .
- Major algorithms, such as LLL!

What is LLL?

- It takes a (usually positive definite) lattice, and changes the basis to make a “better” basis.
- It is usually used to search for short vectors in the lattice. . . .
- But - following my principle - I want to know what it ***really*** does!
- I think I understand it now.
- Worse . . . I'm going to try to tell you!

LLL - From the beginning

- We take a real n-space equipped with the usual (sum of squares) positive definite quadratic form. Hence m_1, m_2 . . . m_n form an orthonormal basis for the model space M.
- And then we take the lattice we are investigating, with a given basis v_1, v_2, . . . v_n, and find an isometric set in M
- It is natural to take v_1 as the appropriate scalar multiple of m_1, and v_2 in the space $\langle m_1, m_2 \rangle$ etc.

The LLL model for a lattice

g 0 0 0 0 0 0 0 If |b| > a/2, we can fix that

h i 0 0 0 0 0 0 by $v_4 = v_4 \pm v_3$.

j k **a** 0 0 0 0 0 If $b^2 + c^2 < a^2$, we then

l m **b** **c** 0 0 0 0 swap v_3 and v_4

n p d e f 0 0 0

q r s t u v 0 0

* * * * * * w 0

* * * * * * * x

How is the model held?

- Personally I use double-precision floating point numbers.
- Once you have a reasonable basis, you seem to lose about one (decimal) digit of accuracy for each ten dimensions.
- So double precision is good up to about 150-200 dimensions.
- If you need a proof, you get the basis right first and then prove it using exact methods.

What is LLL actually doing?

- Swapping the two vectors naturally reduces a, but cannot change the product a.c, which is the determinant of the 2-dimensional lattice.

- Hence it is reducing the “determinant product”

Determinant product

- Start with a positive definite lattice spanned by a basis $v_1, v_2, \dots v_n$
- We then define λ_i to be the lattice spanned by the first i basis vectors $\lambda_i = \langle v_1, v_2, \dots v_i \rangle$
- The determinant product (DP) of the basis is the products of the determinants of the λ_i, so

  $DP = \det(\lambda_1) * \det(\lambda_2) * \dots * \det(\lambda_n)$
- LLL says . . . “use a basis with minimum DP”.

Determinant product

g 0 0 0 0 0 0 0 Determinant product is

h i 0 0 0 0 0 0 $(g^7.i^6.a^5.c^4.f^3.v^2.w)^2$

j k **a** 0 0 0 0 0

l m **b** **c** 0 0 0 0

n p d e f 0 0 0

q r s t u v 0 0

* * * * * * w 0

* * * * * * * x

“Improving” LLL

- Most attempts are to make it run faster.

- I have made so many “improvements” in my life, all of which made it slower!   :(

- But we **can** make an algorithm that often reduces the DP more than LLL does.

LLL - Not so much a program - more a way of life!

Ever noticed that often one of the later basis vectors has smaller norm than the first one?

- This suggests that bringing it to the front might reduce the DP.
- More generally, we need to understand which basis changes might reduce the DP, and find an intelligent way of looking at them.
- I tried a stupid way. It was slow, but I think there is a faster way.

Reducing the DP

g 0 | 0 0 0 | 0 0 0

h i | 0 0 0 | 0 0 0

j k | a 0 0 | 0 0 0   If we can reduce DP

l m | b c 0 | 0 0 0   in this 3 x 3 block,

n p | d e f | 0 0 0   i.e. a^2c, that

q r | s t u | v 0 0   reduces DP overall

* * | * * * | * w 0 $(g^7.i^6.a^5.c^4.f^3.v^2.w)^2$

* * | * * * | * * x

Look at 3 x 3 more closely

a 0 0

b c 0

d e f

- LLL gives us that $a \geq 2|b|$ and $c \geq 2|e|$
- also $b^2 + c^2 \geq a^2$ and $e^2 + f^2 \geq c^2$.
- LLL therefore gives us that $f^2 \geq 9.a^2/16$ (0.5625) but this cannot be min-DP. I suspect that $f^2 \geq 2.a^2/3$ (0.6667) as happens in A_3

Find the min-DP basis

a 0 0

b c 0

d e f

Naturally take a, c and f positive, and negating v_2 and/or v_3 if necessary, make b and e be ≤ 0.

- Hence I suspect that the only viable vectors for the first one are v_3 or $v_3 + v_2$, possibly with v_1 added or subtracted depending on the sign of the first co-ordinate.

So LLL-3 needs

- A rapid algorithm to put a 3-dimensional lattice into min-DP form.

- I feel sure that some careful thinking, possibly backed up by some computer work with intervals, can provide such an algorithm.

And onward

- For each dimension n we are interested in two related things about lattices in min-DP basis.

1) By what factor can the diagonal entries of the model go down
2) Find a very fast algorithm to put an arbitrary lattice of small dimension n into a min-DP basis

For example

- If one has a min-DP basis for a lattice in 8 dimensions, can the bottom right entry be less than half the first one?
- In other words, is E_8 the best in this sense.
- Similarly one might suspect that the Leech lattice is the most extreme case in 24, where the bottom right is 1/4 of the top left.

Ideas for brute-force classification of Type-II dim-48 det-1?

- Use a min-DP basis for all the lattices we deal with.
- Keep some information on the theta function on all the points of the dual quotient.
- Go up one dimension at a time.

The “Gene”.

- Not sure if this is the genus. Even if it is, my emphasis is completely different.
- The dual quotient is a finite Abelian group G whose order is the determinant of the lattice.
- The norms of elements of G are defined as rational numbers modulo 1 (type I) or modulo 2 (type II)
- (This norm function must satisfy certain bilinearity axioms not discussed further)
- The **gene** of a lattice is this finite abelian group G, and the norms of every element mod 1 (or mod 2).

Example - the E_6 lattice

Determinant is 3, so the gene is a cyclic group of order three. E_6 is an even lattice, so the norms are defined modulo 2.

The Gene of E_6 is this group, along with the norm information, namely

[0] has norm 0 (mod 2) - as always

[1] has norm 4/3 (mod 2)

[2] has norm 4/3 (mod 2)

Genetic theta function

- Take an element of the Gene group G.
- Now consider the coset consisting of the points of the dual lattice congruent to this element modulo the lattice.
- We may list, as a theta function with fractional exponents, how many vectors of this coset have each possible norm.
- We may want this theta function for every element of the gene group.

Partial Genetic Theta function.

- The entire genetic theta function is not always needed.
- It is often sufficient to know the minimum norm of a vector for each element of the gene.
- (e.g. if we want minimum norm 6).
- Or we may be interested, for some small norms, how many dual lattice vectors there are in that coset with that norm.
- We may also hold an example vector of minimum norm.

Gluing

- Given any of these forms of partial genetic theta function, the same information can be readily made for two lattices glued together if it is available for the parts.
- Direct sum . . . OK
- Add some glue vectors . . . OK
- 1-dimensional lattices . . . OK.

So we can laminate

- Given a lattice (with its genetic theta function), for each point of the dual-quotient we can laminate above that point,
- and compute the genetic theta function of the result.
- By gluing with a 1-dimensional lattice.

A way to look for 48 dimensional even unimodular lattices

- Run the procedure so far described with minimum norm 6 and get a million or so lattices of moderate determinant in each dimension up to 24.
- Look through the pairs of 24-dimensional lattices for pairs with complementary gene and minimum norm 6.
- Will it work?   Dunno.

Towards a full classification of unimodular min-6 dim-48.

- Idea is to use the min-DP basis to specify properties of lattices in every dimension P(1), P(2), . . . P(48) such that for all lattices satisfying P(n) in a minimal DP basis, the first n-1 basis vectors span a lattice with P(n-1).
- P(48) is determinant 1, minimum norm 6.
- so what might P(24) look like, and (critically) how many lattices satisfy it?

Research Area

- We therefore seek properties of the DP basis that enable us to get properties in decreasing dimension starting at 48.
- The idea being that if you add some more vectors where the determinant is decreasing rapidly, the fact that the DP cannot be reduced is a property that one should be able to use.