Some comments about Indefinite LLL

Mark Watkins

Magma Computer Algebra Group, School of Mathematics and Statistics, Carslaw Building F07, University of Sydney, NSW 2006, AUSTRALIA

E-mail address: watkins@maths.usyd.edu.au

1. Review of LLL

One rendition of the classical LLL algorithm [**10**] takes as an input a symmetric, nonsingular, and definite Gram matrix G of dimension n, and from this computes a Gram matrix corresponding to a reduced basis. More specifically, given a parameter $1/4 < \delta \leq 1$, a definite nonsingular Gram matrix is LLL-reduced if

- $|\mu_{i,j}| \leq \frac{1}{2}$ for all $1 \leq j < i \leq n$ (size reduction);
- $\delta B(k-1) \leq B(k) + \mu_{k.k-1}^2 B(k-1)$ for all $2 \leq k \leq n$ (Lovász condition).

Here $B(i)$ and $\mu_{i.j}$ are defined[1] recursively by

$$\mu_{i,j} B(j) = G_{i,j} - \sum_{k=1}^{j-1} \mu_{j,k}\mu_{i,k} B(k) \quad \text{and} \quad B(i) = G_{i,i} - \sum_{j=1}^{i-1} \mu_{i,j}^2 B(j).$$

The fact that $B(i) \neq 0$ for all $1 \leq i \leq n$ follows from the definiteness and nonsingularity of G.

One significant property of a LLL-reduced Gram matrix is that we have

$$B(k-1) \leq \gamma B(k) \text{ for all } k,$$

where $\gamma = (\delta - 1/4)^{-1}$. Since we have that $\det(G) = \prod_i B(i)$, by induction this yields the bound $G_{1,1}^n = B(1)^n \leq \gamma^{n(n-1)/2} \det(G)$. Note that $\gamma \to 4/3$ as $\delta \to 1$.

When $\delta < 1$, the LLL algorithm can compute such a reduction (via an integral transformation) in polynomial time. It proceeds by recursively considering larger and larger submatrices, first size-reducing them, and then deciding whether the Lovász condition is met (if not, the last two rows/columns are swapped). The proof that LLL works as desired usually proceeds by first noting that $\prod_{i=1}^k B(i)$ is the determinant of the upper-left k-by-k submatrix G_k of G, and that this determinant is reduced by a factor of at least $1/\delta$ by each swap, with the other minors remaining constant. We thus get a bound on how many swaps must be made before termination, perhaps most conveniently described in terms of $\prod_k \det(G_k) = \prod_i B(i)^{n+1-i}$.

For nonsingular matrices, we can use (for instance) the MLLL algorithm [**16**]. We wish to also be able to handle indefinite matrices.

[1]These quantities correspond to a Gram-Schmidt orthogonalisation (see [**14**, §3.2] for instance), though there is no explicit reference to any underlying vectors (only the inner products).

1.1. Indefinite LLL. The Lovász condition can be readily generalised to the indefinite case via putting absolute values around both sides. This seems to be first noted in [**9**]. The principal difficulty arises when an isotropic vector is detected, that is, a vector of norm zero. The same proof as with the LLL algorithm yields that: either an isotropic (norm 0) vector is found (which is often the desired output in any event); or the resulting output satisfies the above inequalities with absolute values in place.

In fact, Simon shows [**21**] that we have $|G_{1,1}|^n \leq \frac{3}{4}\gamma^{n(n-1)/2}|\det(G)|$ in the indefinite case, and in general we do better when there are many sign-changes on successive $B(k)$, especially for the smaller indices. He also shows [**22**] that when G is integral, unimodular, and indefinite, and $n \leq 9$ with $\delta > 193/196$, a modified algorithm returns either an isotropic vector, or a diagonal Gram matrix with ± 1 entries.[2] He then uses this to show how to solve quadratic equations.

Herein we give an exposition of Simon's work, with a few additional comments of our own.

1.1.1. *Acknowledgments.* The author thanks T. A. Fisher for indicating some bugs with one of the versions of the Magma implementation [**1**] of Simon's algorithm, C. Fieker and A. K. Steel for their comments about Grassl's application, and D. Simon, D. R. Heath-Brown, and H. W. Lenstra Jr. for various comments. He also thanks BIRS for hosting the workshop, and the referee for a proper reading of the paper and many useful comments.

2. Quadratic equations

Let G be a symmetric indefinite integral matrix of dimension n. We write (r, s) for its signature, and can assume that $r \geq s \geq 1$. We want to find a vector $\vec{v} \neq \vec{0}$ that satisfies $\vec{v}G\vec{v}^T = 0$, and indeed would like to determine a space of such solutions that is of as large as dimension as possible. Here this "space" is a quadratic space over $\mathbf{Z}$. As noted by Simon [**23**], when $\det(G) = 0$ we can use linear algebra to determine a suitable kernel, which reduces the problem to a smaller one. So we will assume that $\det(G) \neq 0$. This implies that there is no nonzero $\vec{v}$ with $\vec{v}G\vec{u}^T = 0$ for all $\vec{u}$.

Such a subspace of solutions $\vec{v}_i G\vec{v}_i^T = 0$ with $\vec{v}_i G\vec{v}_j^T = 0$ for all i, j is termed a (totally) isotropic subspace.[3] Note that in general there will be no "best answer" other than the maximal dimension of such a totally isotropic subspace (called the isotropy index), as can be seen from the case of $n = 3$ with conics; namely, a solvable conic has infinitely many solutions, any of which generates a 1-dimensional totally isotropic subspace which cannot be extended.

2.1. Reduction in dimension. We recall how basic linear algebra allows us to reduce to a case of smaller dimension once we have found an isotropic vector. In particular, letting $\vec{v}$ be isotropic for G, we can find $\vec{w}$ with $\vec{v}G\vec{w}^T = \gcd_{\vec{u}}\big(\vec{v}G\vec{u}^T\big)$, the latter being nonzero since $\vec{v} \notin \ker(G)$. We can then choose $(\vec{e}_i)_i$ with $\vec{v}G\vec{e}_i^T = 0$ for $3 \leq i \leq n$, via simply taking any spanning set and then subtracting suitable

[2] An isotropic vector can trivially be found from the latter; indeed, the principal effort beyond [**21**, Theorems 1.6,1.8] in [**22**] considers linear combinations of basis vectors in more cases.

[3] When using the term isotropic, we exclude kernel vectors $\vec{v}$ that have $\vec{v}G\vec{w}^T = 0$ for all $\vec{w}$.

multiples of $\vec{w}$ so as to make the inner products be zero.[4] We can then consider the Gram submatrix corresponding to the $\vec{e}_i$, and all isotropic vectors for it will be orthogonal to $\vec{v}$. In this way we reduce the dimension of the problem by 2, and so once a method for finding isotropic vectors is given, we can use it recursively.

We can show that this method finds an isotropic subspace of maximal dimension as follows. Let $\vec{v}$ be isotropic for G, with $\vec{w}$ and $(\vec{e}_i)_i$ as above completing a basis for the quadratic space, and denote by E the subspace spanned by the $(\vec{e}_i)_i$. Let S be a totally isotropic subspace (for G) of maximal dimension s. Since $\vec{v}G\vec{w}^T \neq 0$, there is some $\vec{u} \in \langle\vec{v}\rangle \oplus \langle\vec{w}\rangle$ such that $\vec{u} \notin S$, namely (at least) one of $\vec{v}$ or $\vec{w}$ will work. We then note that $\langle\vec{u}\rangle \oplus E$ has codimension 1, and thus its intersection with S has dimension at least $(s-1)$. However, this latter intersection is the same as $(\langle\vec{u}\rangle \cap S) \oplus (E \cap S)$, and the former is empty. Thus $E \cap S$ has dimension $(s-1)$ as desired – the iteration will now break off $\vec{v}$ and $\vec{w}$ and proceed to E (which is orthogonal to $\vec{v}$), and this has an isotropic subspace of the desired dimension.

2.2. The unimodular case. In the unimodular case with signature (r, s), we can obtain a totally isotropic subspace of dimension s. A more specific statement is given in [**19**, V,§2.2], where when G is odd (that is, it has vectors of odd norm), we have $G \cong I_+^{\oplus r} \oplus I_-^{\oplus s}$, and from this one easily obtains an isotropic subspace of dimension s by pairing each I_- with a different I_+ (here $I_\pm$ is the 1-dimensional quadratic space with determinant ± 1). When G is even we get $G \cong U^{\oplus s} \oplus \Gamma_8^{\oplus t}$ for some t, where U is the hyperbolic plane with Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and Γ_8 is the unique 8-dimensional positive definite quadratic space that is even and unimodular. Again we readily get an isotropic subspace of dimension s via taking one vector from each U-component.

Remark 2.2.1. One can note that Simon calls the quadratic space with Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ a *hyperbolic plane*, though the referee indicates this is not always termed as such. We use H to denote a quadratic space whose Gram matrix is either U or the above.

Simon gives an algorithm for computing such a maximal totally isotropic subspace which relies (inductively) on other parts of his work. As above, once we find a vector of norm zero, we can readily use linear algebra to break off a hyperbolic plane corresponding to it. Thus, by the above stated consequence [**22**] of indefinite LLL (with $\delta > 193/196$), we can compute a maximal totally isotropic space for $n \leq 9$, as his algorithm will always directly yield an isotropic vector. Similarly, for larger n we can assume that an application of indefinite LLL does not produce an isotropic vector, as otherwise we could inductively reduce to a smaller dimension.

In this alternative case (when indefinite LLL does not produce an isotropic vector), Simon considers various 5-by-5 submatrices of the resulting Gram matrix, looking for ones that are indefinite. By Meyer's theorem [**11**], the quadratic form associated to such a submatrix has a nontrivial zero, and a solution can be found as described below – the method for this does use the unimodular step given here, but only in dimension 7. So we are always able to obtain an isotropic vector, and can thus inductively compute a totally isotropic subspace corresponding to a unimodular Gram matrix.

[4]When $\vec{v}G\vec{w}^T = 1$ we can additionally require that $\vec{w}G\vec{e}_i^T = 0$ for all $3 \leq i \leq n$, in this case subtracting suitable multiples of $\vec{v}$. We can also note that this will always be the case whenever $\det(G)$ is squarefree, as the square of $\vec{v}G\vec{w}^T$ will divide $\det(G)$.

We make some comments about the efficacy of this method below. As noted by Simon, finding a solution to a form of dimension 5 requires factorisation of its discriminant, but this does not seem to be too problematic. Furthermore, if such a factorisation looks to be difficult in any given case, we could (say) consider a different 5-by-5 indefinite submatrix (perhaps with smaller entries in its Gram-Schmidt orthogonalisation), or pre-transform G by a random unimodular matrix.

2.3. Minimisation. When G is not unimodular, we can first try to transform it (over $\mathbf{Q}$) to an equivalent form that has smaller determinant. Here we work on a prime-by-prime basis, and so will want to reduce the valuation at each prime as much as possible.

Simon gives a procedure for minimisation in general, consisting mainly of finding kernel vectors mod p, and transforming suitably before applying $\mathrm{diag}(\frac{1}{p}, 1, \ldots 1)$. These intermediate transformations can indeed introduce large numbers, but the indefinite LLL routine will readily handle them. As a result of his minimisation process, we obtain a matrix G_m with the following properties:

- When n is odd, $\det(G_m)$ is odd and squarefree.
- When n is even, $v_p\big(\det(G_m)\big) \leq 2$ for all p, and $v_2\big(\det(G_m)\big) \leq 1$.
- The kernel of G_m mod p has dimension $v_p\big(\det(G_m)\big)$.

Furthermore, when n is odd, the maximal dimension of a totally isotropic subspace (after removing the kernel) at a prime $p|\det(G_m)$ is $(n-3)/2$. When n is even and $p^2|\det(G_m)$ this local isotropy index is $(n-4)/2$ (see [**23**, Lemmata 2,9]). Although Simon does not mention it explicitly, when n is even and $p\|\det(G_m)$, the local isotropy index is $(n-2)/2$; upon removing the 1-dimensional kernel, we are left with a nonsingular odd-dimensional form, to which we can apply [**23**, Lemma 2].

2.4. Conics. The case of $n = 3$ is mostly solved by Gauss [**6**, §272,274,294], and indeed Simon in essence generalises his work when dealing with higher dimension. Namely, prime divisors of the determinant/discriminant are removed via a minimisation technique at each such prime, leaving us with a unimodular matrix. Then a reduction technique is used to bring the result into the form $\mathrm{diag}(1, -1, \pm 1)$, from which a solution is readily determined. The solutions are then back-tracked to the original form.

2.5. Dimension 4. The Hasse-Minkowski theorem [**8, 12**] states that to determine if an integral quadratic form has a global solution, we need only check whether it is everywhere locally solvable. For $n = 4$, we can first note that G_m is unsolvable at an odd prime p only when $v_p\big(\det(G_m)\big) = 2$, while local solubility at 2 occurs except when $\det(G_m) \equiv 1 \pmod 8$ with Witt invariant $\epsilon_2(G_m) = +1$ (see [**19**, Ch. IV, Th. 6]).

In this $n = 4$ case, Cassels [**3**, §14.7] gives a proof of the Hasse-Minkowski theorem that avoids the use[5] of Dirichlet's theorem for primes in arithmetic progressions (see also [**4**]), and Simon is able to suitably algorithmise this idea.

Namely, in the (more difficult) case where $\det(G_m) \neq \pm 1$, one considers the direct sum $D = G_m \oplus Q_2$ where Q_2 is a suitable binary quadratic form (having the

[5]Simon calls Dirichlet's theorem "highly ineffective" but it seems as though he means only for the practical algorithmic aspects. Cassels [**4**] places Dirichlet's theorem as being "of a fairly deep nature", noting that Skolem had used a weaker form, while Siegel had instead used the Hardy-Littlewood circle method (see references therein). More recently, O'Meara [**15**] has given a proof using class field theory.

right Witt invariants); this will be a 6-dimensional form that can be readily minimised to a unimodular form, having signature $(3,3)$. Thus we get a 3-dimensional isotropic subspace for D as above, and by intersecting with G we find a solution.

The construction of Q_2 is effected by computing[6] generators of the 2-Sylow part of the class group of $\mathbf{Z}[\sqrt{4\det(G_m)}]$ and then using linear algebra over $\mathbf{F}_2$ to find a suitable form that will yield the desired Witt invariants. Explicitly we want[7]

$$\frac{\epsilon_p(Q_2)}{\epsilon_p(G_m)} = \big(-1,-4\det(G_m)\big)_p \quad \text{or} \quad \frac{\epsilon_p(Q_2)}{\epsilon_p(G_m)} = \big(-1,-4\det(G_m)\big)_p\big(2,4\det(G_m)\big)_p,$$

where $(x,y)_p$ is a Hilbert symbol (and indeed, the Witt invariants themselves can be computed in terms of such [**19**, IV, §2.1]). Note also that Q_2 is either indefinite or negative definite, depending on the sign of $\det(G_m)$.

Remark 2.5.1. It is not clear to me whether this idea of Cassels can be made to work in general over number fields, either theoretically or in practice.

2.6. Dimension 5 and above. For dimension 5 and higher, Meyer's theorem [**11**] implies that an indefinite quadratic form represents zero, and thus there is no obstruction to solving the equation. Simon proceeds to again use the summand idea of Cassels, though the efficacy of his method depends on whether the dimension is odd or even.

2.6.1. *Odd dimension.* For n odd, we write the signature as (r,s) with $r > s$. We then take the direct sum of G_m with a suitable Q_2, again having the right Witt invariants to be minimised to a unimodular matrix (see [**23**, Propositions 14-15]). Here we work with the 2-Sylow part of the class group of $\mathbf{Q}(\sqrt{-8|\det(G_m)|})$, and desire

$$\epsilon_p(Q_2) = -\big(-1,2(-1)^{(n-1)/2+s}\big)_p.$$

Note that this does not particularly depend on the Witt invariants of G_m, and recall also that $\det(G_m)$ is odd and squarefree.

We can ensure that the resulting direct sum has signature $(r,s+2)$, and the application of indefinite LLL as above then yields a totally isotropic subspace of dimension $\min(r,s+2)$. Upon intersecting back to G, we get a totally isotropic subspace of dimension $\min(r,s+2)-2$, and this dimension is equal to $\min(r,s)=s$ except in the case $r=s+1$.

However, in this latter case Simon shows that when G_m is not unimodular, the isotropy index is only $(s-1)$. The argument for this notes that such an isotropic subspace of dimension s would allow us to write $G \cong H^{\oplus s} \oplus (-1)^s\det(G_m)I_1$ (where H is a generalized hyperbolic plane as in §2.2.1); but then at every prime p we would obtain a (local) totally isotropic subspace of dimension $s=(n-1)/2$ over $\mathbf{F}_p$, which implies $p \nmid \det(G_m)$ by the properties given in §2.3. Thus G_m is unimodular.

Simon notes that the multiplication of the discriminant by a factor of 8 is in general necessary here, for when $|\det(G_m)| \equiv 7 \pmod 8$ there will be no binary quadratic form of smaller discriminant that has the correct Witt invariant at 2.

---

[6]The algorithm of Bosma and Stevenhagen [**2**] can be used to do this. Amusingly, one can note that some early work of Shanks [**20**] already related the underlying problem (of computing square roots in the class group) back to the ternary form reduction of Gauss.

[7]The splitting of possibilities here is related to integrality and primitivity issues, when we deal with nonfundamental discriminants.

One could presumably append a different form in various cases, but as the method here generates a maximal totally isotropic subspace, such is unnecessary.

2.6.2. *Even dimension.* The case of even dimension is more difficult, firstly as one cannot always exploit inequalities in the signature, and secondly since Simon does not specifically attempt to take a direct sum with the most suitable quadratic form, but rather simply increases the dimension by 1 (reducing to the previous odd dimension case). He does this via summing with the quadratic space with Gram matrix $-I_1$, but it seems to me that other summands can be superior.

The upshot is, when the resulting minimisation is not unimodular (the worst case), from Simon's algorithm we obtain: a totally isotropic subspace of dimension s when $r > s+2$; of dimension $(s-1)$ when $r = s+2$; and dimension $(s-2)$ when $r = s$. In the worst case of $n = 6$, we are still always able to obtain a solution to the original equation. Simon leaves it as an open question as to whether this version of his algorithm always finds a totally isotropic subspace of maximal dimension.

As with the odd-dimensional case above, when $\det(G_m) \neq \pm 1$ is squarefree the isotropy index cannot exceed $(n/2-1)$, and this is a nontrivial bound when the signature is (s,s).

This argument can be extended to the case where $\det(G_m)$ is not squarefree. We can assume that the signature is (s,s), that there is an isotropic subspace of dimension s, and $p^2 | \det(G_m)$ for some prime p. We write S for some isotropic subspace of dimension s. By the third condition enumerated in §2.3 the kernel of G_m at p is 2-dimensional, and we take it to be generated by some $\vec{v}$ and $\vec{w}$, writing G' for the complement. By [**23**, Lemma 9], the fact that G_m is minimised implies that G' has a local isotropy index of $(s-2)$ at p. This is also an upper bound for the global isotropy index of G', and since S has dimension s, the isotropy index must increase by 2 upon adjoining $\vec{v}$ and $\vec{w}$. This implies we must have $\ker_p(G_m) \subseteq S$. In particular, this implies that $\vec{v}$ and $\vec{w}$ are themselves (globally) isotropic, and that $\vec{v}G_m\vec{w}^T = 0$. We can then (unimodularly) transform G_m to a Gram matrix $\tilde{G}$ corresponding to a basis $\{\vec{v}, \vec{w}, \vec{e}_3, \dots, \vec{e}_{2s}\}$, and can ensure that $\vec{v}\tilde{G}\vec{e}_i^T = 0$ for all $i \geq 4$ and $\vec{w}\tilde{G}\vec{e}_i^T = 0$ for all $i \geq 5$. This then implies the determinant of $\tilde{G}$ is divisible by p^4, since $p | \vec{v}\tilde{G}\vec{e}_3^T$ and $p | \vec{w}\tilde{G}\vec{e}_4^T$, with these being the only applicable entries in the first and second row/column when computing the determinant. This contradicts Simon's second property of a minimised matrix, namely that $p^3 \nmid \det(G_m)$. Thus a totally isotropic subspace of dimension s cannot exist in this case.

We can also note (if others have not already done so) that Simon's algorithm does not always determine a maximal isotropic subspace.[8] For instance, it is possible to have a 2-dimensional maximal isotropic subspace in the case of signature $(4,2)$, even when the relevant minimisation is not unimodular. One explicit example here has $Q_4 = \mathrm{diag}(1,1,1,-3)$ and U the standard hyperbolic plane, and then Simon's algorithm (as given) only returns one isotropic vector for the 6-dimensional form $U \oplus Q_4$, since the minimisation of $U \oplus Q_4 \oplus -I_1$ is not unimodular. An example with the other signature has $\tilde{Q}_4 = \mathrm{diag}(1,1,-2,-3)$, where again $U \oplus \tilde{Q}_4$ has isotropy index 2.

[8]This answers *strictu sensu* the first part of the second Remark after [**23**, Algorithm 7], while for the second part Simon himself gives a feasible modification at the beginning of the first Remark therein.

I do not see any immediate way to modify Simon's algorithm (at the level of summands) to ensure that a maximal isotropic subspace is returned. In the first example above, we can simply sum with $-6I_1$, and the resulting form will minimise to a unimodular form of signature $(3,4)$, inducing a 2-dimensional solution space upon intersection. The same is true for the second example, where $3I_1$ also suffices (for the first example, summing with $3I_1$ does not work since the resulting signature of $(2,5)$ is inefficacious). However, I do not know how far such ideas can be taken in general, and it appears that a more thorough analysis of Witt invariants would be necessary.

An alternative process for computing a maximal isotropic subspace is to iteratively find isotropic vectors and break off hyperbolic planes; following the last paragraph of §2.1, this should always work. The current Magma implementation [**1**] (in version 2.18) first finds a large isotropic subspace via Simon's method, then breaks off the corresponding hyperbolic planes, and finally looks for more isotropic vectors in the resulting subspace (necessarily of dimension 4). Explicitly, one can transform to $\left(\begin{smallmatrix} 0 & L & 0 \\ L & * & * \\ 0 & * & X \end{smallmatrix}\right)$ where L is lower triangular and $\dim(X) = 4$. This is already noted by Simon in the Remark after [**23**, Algorithm 7].

Experimentation on many even-dimensional examples of near-balanced signature shows that typically the maximal isotropic dimension is 1 more than Simon's estimate, the only obstacle being the solvability of the final 4-dimensional subspace.[9]

2.7. Exhibiting rational equivalence. We can adapt Simon's algorithm to demonstrate a transformation between two rationally equivalent forms. Explicitly, given two symmetric matrices X and Y over $\mathbf{Q}$ with the same Witt invariants and signature, we write $M = -Y \oplus X$, and then find a totally isotropic subspace S for M. The dimension d of S will be equal to that of X. We then echelonise a (rational) basis for S as $[I_d|U]$, so that $Y = UXU^T$.

One application of this (as suggested by Grassl [**7**]) is to computing orthogonal (or unitary) representations. For this, we are given X, and typically want Y to be diagonal with simple entries. In the Fi_{22} example of dimension 78 given by Grassl, we have $Y = \mathrm{diag}(1,\ldots,1,3)$, and would need to apply Simon's algorithm in dimension 156.[10] As noted by Grassl, to achieve orthonormalisation, a post-processing to extend to $\mathbf{Q}(\sqrt{3})$ is necessary.

Remark 2.7.1. The generalisation here to number fields might be nontrivial. For instance, taking a totally real cubic field where 2 is inert, with ϵ_1, ϵ_2 totally positive (independent) units, I do not see how to adapt Simon's algorithm to transform $\mathrm{diag}(1, -\epsilon_1, -\epsilon_2, 1/\epsilon_1\epsilon_2)$ into $\mathrm{diag}(+1,+1,-1,-1)$, though these have the same invariants. Nor it is clear how to find isotropic vectors for the former, nor how to pass from these to a desired diagonalisation.

2.8. Recent work of Castel for dimension 5. In his recent Ph. D. thesis, Castel [**5**] has shown how one can solve quadratic equations in dimension 5 without factorising the determinant.[11] He does this by extending G to a 6-dimensional form M_6 whose determinant has a known factorisation (for instance, twice a prime).

[9] The frequency of this occurrence presumably relates to the $(n,d) = (3,2)$ case of [**18**].

[10] It may be possible to work in smaller dimension either via building up an orthogonal vector sequence with norms in appropriate square classes, or (as noted by Grassl) by considering subforms.

[11] Of course, one can assume $\det(G)$ has no small prime divisors, and in particular is odd.

Writing $M_6 = \left(\begin{smallmatrix} G & \vec{v}^T \\ \vec{v} & z \end{smallmatrix}\right)$ and $X = -\vec{v}G^{\mathrm{adj}}\vec{v}^T$, we have $\det(M_6) = z\det(G) + X$. In particular, $\det(M_6)$ is congruent to X modulo $\det(G)$, and given $\vec{v}$ we can choose z to ensure $\det(M_6) > 0$ (implying its signature is beneficial for our purposes).

Castel first shows that we can minimise G (without factorisation) so that its Smith form is $\mathrm{diag}\big(\det(G_m), 1, 1, 1, 1\big)$. The final case in this minimisation analysis reduces to a problem essentially considered by Pollard and Schnorr [**17**], that of solving a conic $ax^2 + by^2 + cz^2 \equiv 0 \pmod{n}$ without factorising n. He then shows when G_m has such a Smith form, there is some δ (coprime to $\det(G_m)$) such that all choices of $\vec{v}$ yield X-values with X/δ a square modulo $\det(G_m)$. One can then use theorems on primes in arithmetic progressions to deduce that there are choices of $\vec{v}$ and z with $\det(M_6)$ as desired.[12] Finally, Castel shows that M_6 has two independent solutions,[13] which can be found as above.

We thus have at least one solution upon intersection with G. Unless G has signature $(2, 3)$ and the minimisation (using factorisation) of G is unimodular, this is a maximal isotropic subspace. In the alternative case, we can break off a (generalised) hyperbolic plane with the found solution, but then we just seem to have reduced to the problem of determining whether the resulting conic is solvable, and this is thought to be difficult to do without factorising the determinant.

It is not apparent to me whether Castel's technique will generalise to higher dimensions. For instance, in the 6-dimensional case, one can presumably have a Smith form of $\mathrm{diag}(d, d, 1, 1, 1, 1)$ with the factorisation of d unknown. The difficulties appear to grow as the dimension goes up. On the other hand, his method should work for squarefree determinant, when the Smith form must be as desired.

Remark 2.8.1. As noted by both Simon and independently Heath-Brown, one could also try to find a solution to a 5-dimensional indefinite form by taking random restrictions to indefinite forms of dimension 3 or 4, hoping that the obtained determinant can be easily factored. This is likely a good procedure in practice, but it seems difficult to prove that this will indeed always work.

3. Back to indefinite LLL

One of the classical goals of LLL is to find short vectors. Another idea is to get a basis that is as orthogonal as possible. These goals tend to cooperate in the definite case, but need not do so in the indefinite case.

For instance, the matrix $\left(\begin{smallmatrix} 0 & 100 \\ 100 & 9 \end{smallmatrix}\right)$ has an isotropic vector visibly apparent, but a superior representation for orthogonality is $\left(\begin{smallmatrix} 9 & 1 \\ 1 & -1111 \end{smallmatrix}\right)$. Obviously one can interpolate between these extremes.[14] In this 2-dimensional case, we typically have 2 possibilities for the LLL output (meeting the Lovász condition), corresponding to the two smallest possible norms from independent vectors. The number of such

[12] As he is concerned with the algorithmic aspects, for his runtime analysis Castel assumes GRH for the associated Dedekind L-functions so as to ensure enough uniformity, and then applies the Chebotarëv density theorem.

[13] The only obstacle is the 2-adic solubility of a 4-dimensional subspace that results after breaking off an isotropic vector paired with a nonorthogonal vector; this seems to be why he requires $\det(M_6)$ to be *twice* a prime, though I think one could alternatively require $\det(M_6)$ to be a prime that is not 7 mod 8.

[14] The second corresponds to making the sum (trace) of the roots of the associated quadratic be close to zero, while the first is related to extreme values for the ratio of these roots.

possibilities tends to grow rapidly with the dimension (much more so than in the definite case), but I have not explored this question in any depth.

3.1. Considerations of output. When $\det(G)$ is squarefree, via the method of finding isotropic vectors and breaking off associated spaces as in §2.1, we can reduce to the situation of $G \cong H^{\oplus s} \oplus Q$, where H is a generalized hyperbolic plane as in §2.2.1. Since Q here has no isotropic vectors, it must either be definite or have $\dim(Q) \leq 4$. Upon applying LLL to Q, we obtain a form that is reasonable for algorithmic output. However, the isotropic vectors obtained from the above method typically have quite large coefficients (particularly when the determinant is large), and it can be beneficial to first reduce the size of the coefficients of the basis of the isotropic subspace by applying LLL to its basis. It still does not seem that this will necessarily yield vectors that are anywhere near as small (in the standard L^1 or L^2 norm say) as possible.[15]

When $\det(G)$ is not squarefree, the value of this process is not that clear. Given an isotropic vector $\vec{v}$ such that $\vec{v}G\vec{u}^T \equiv 0 \pmod{p}$ for all $\vec{u}$, one can find a basis $(\vec{e}_i)_i$ with $\vec{e}_1 = \vec{v}$ such that $\vec{v}G\vec{e}_j^T = 0$ for $3 \leq j \leq n$, but there is no reason that the inner products $\vec{e}_2 G \vec{e}_j^T$ need be small, and the effect on these inner products when reducing the resulting restriction to dimension $(n-2)$ must be considered as well.[16]

Ivanyos and Szánto [**9**] give an alternative method of dealing with isotropic vectors in the LLL procedure, namely to avoid them via adding suitable (small) basis elements so as to make them anisotropic. The resulting output has similar quality to LLL when bounding the entry sizes, though one does not directly obtain any isotropic vectors. This still, however, can be a useful output when isotropic vectors are not of primary interest (and indeed, are perhaps to be avoided from the standpoint of analogy to the classical LLL reduction).

3.2. Diagonalisation in the unimodular case. We conclude with some comments about diagonalising the Gram matrix of an (odd) indefinite quadratic space in the unimodular case.

Suppose that we start with a quadratic space with unimodular Gram matrix G of signature (r, s), with $r \geq s \geq 1$. Via the algorithm of Simon as explained above, we can find an isotropic vector $\vec{v}$. We then pair it with a nonorthogonal vector $\vec{w}$ of odd norm. This allows us to write $G = X \oplus G'$ where X has Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, and X can then be transformed to $\mathrm{diag}(+1, -1)$.

The above reduces the signature (r, s) to $(r-1, s-1)$. When $s = 1$, we can break off the $+1$ component while retaining the -1 component (reducing the signature $(r, 1)$ to $(r-1, 1)$), and can continue in various ways. For instance, we can randomly perturb the matrix and apply LLL again, or we could also try to use the vector of norm -1 more directly, say to decrease the diagonal entries of the Gram matrix by any square amount (in particular, if any diagonal entry is square, we immediately obtain another isotropic vector). With the random perturbation, one method is to take an upper-triangular transformation matrix T with

[15] Already in the 3-dimensional case, finding a point on a conic and finding such a point of relatively small height can be two rather different problems, though the existence of a parametrisation of the conic can ameliorate this to some degree.

[16] Note that in the previous section, for the purpose of solving quadratic equations we were more concerned with *rational* equivalence of forms, but now we must return to integral equivalence, and so cannot simply skirt the issue here via minimisiation.

random elements in $\{0, \pm 1\}$ above the diagonal, and then apply LLL to TGT^T. The Magma code does something akin to this, but limits the row/column operations (swapping/addition) to about n operations in dimension n, rather than the n^2 operations as would be implied by a full upper-triangular matrix.

So once we find an isotropic vector, we are essentially done. This is borne out in practice to some degree. For instance, we ran this code in Magma 2.17:

```
SetSeed(1); // to ensure reproducibility
D:=DiagonalMatrix([1 : i in [1..99]] cat [-1]);
R:=RandomSLnZ(100,100,10^3); M:=R*D*Transpose(R);
SetVerbose("IsotropicLLL",1); // SetVerbose("LLL",1);
time _:=LLLGram(M : Isotropic);
```

This takes a random unimodular matrix of signature $(99, 1)$ with entries of size 269 bits. The initial indefinite LLL call took about 40 seconds. It turned out that the resulting matrix was rather difficult to use, in that finding a suitable 5-by-5 submatrix was not immediate. For instance, the smallest diagonal entry was[17] of size 192. The initial attempt at taking a 5-by-5 submatrix resulted in a Gram orthogonalisation with entries of 50 digits. However, after 5 random perturbations (taking a total of 10-15 seconds), a much nicer orthogonalisation appeared, with an entry of -6. This also produced an isotropic vector, and the rest of the routine took only 2-3 seconds (and much of this likely in keeping track of the transformation matrices, which tend to get quite large).

[17]The Magma LLL implementation [**13**] by default uses $\delta = 0.76$ internally; upon increasing this to be quite close to 1, the LLL reduction takes about twice as long, but the resulting diagonal entries are all smaller than 50, and indeed, one of them is equal to -1.

Bibliography

[1] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language.* In *Computational algebra and number theory* Proceedings of the 1st MAGMA Conference held at Queen Mary and Westfield College, London, August 23–27, 1993. Edited by J. Cannon and D. Holt, Elsevier Science B.V., Amsterdam (1997), 235–265. Cross-referenced as J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Online at `http://magma.maths.usyd.edu.au`

[2] W. Bosma, P. Stevenhagen, *On the computation of quadratic 2-class groups.* J. Théor. Nombres Bordeaux **8**, no. 2 (1996), 283–313; erratum *ibid.* **9**, no. 1 (1997), 249. `http://jtnb.cedram.org/item?id=JTNB_1996__8_2_283_0`

[3] J. W. S. Cassels, *Rational Quadratic Forms.* LMS Monographs **13**, 1978.

[4] J. W. S. Cassels, *Note on quadratic forms over the rational field.* Proc. Cambridge Philos. Soc. **55** (1959), 267–70; addendum *ibid.* **57** (1961), 697. `http://journals.cambridge.org/article_S0305004100034009`

[5] P. Castel, *Un algorithme de résolution des équations quadratiques en dimension 5 sans factorisation.* (French) [An algorithm for solving 5-dimensional quadratic equations without factorisation]. Thèse under D. Simon, Caen, 2011. Related work to appear in ANTS-X proceedings.

[6] C. F. Gauss, *Disquisitiones Arithmeticae.* (Latin) [Arithmetical investigations] (1801). Online from his complete works (1863): `http://resolver.sub.uni-goettingen.de/purl?PPN235993352`
English translation: A. A. Clarke, *Disquisitiones Aritmeticae*, Yale Univ. Press (1965).

[7] M. Grassl, *Constructing Matrix Representations of Finite Groups in Characteristic Zero.* Proceedings of the 10th Rhine Workshop on Computer Algebra (RWCA 2006). Universität Basel (2006), 143–48.

[8] H. Hasse, *Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen.* (German) [On the representability of numbers by quadratic forms over the rationals]. J. reine angew. Math. **152** (1923), 129–48. `http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0152`

[9] G. Ivanyos, Á. Szánto, *Lattice basis reduction for indefinite forms and an application.* Discrete Math. **153** (1996), 177–88. `http://dx.doi.org/10.1016/0012-365X(95)00135-J`

[10] A. K. Lenstra, H. W. Lenstra Jr., L. Lovász, *Factoring polynomials with rational coefficients.* Math. Ann. **261**, no. 4 (1982), 515–534. `http://dx.doi.org/10.1007/BF01457454`

[11] A. Meyer, *Mathematische Mittheilungen.* (German) [Mathematical communications]. Vierteljahrschrift der Naturforschenden Gesellschaft in Zürich **29** (1884), 209–22. `http://www.biodiversitylibrary.org/item/34517#page/217/mode/1up`

[12] H. Minkowski, *Über die Bedingungen, unter welchen zwei quadratischen Formen mit rationalen Koeffizienten ineinander rational transformiert werden können.* (German) [On the conditions under which two quadratic forms rational coefficients can be rationally transformed into each other]. J. reine angew. Math. **106** (1890), 5–26. `http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0106`

[13] P. Q. Nguyen, D. Stehlé, *Floating-point LLL Revisted.* In *Advances In Cryptology* (EUROCRYPT 2005, Aarhus). Edited by R. Cramer, Springer LNCS **3494** (2005), 215–33. `http://dx.doi.org/10.1007/11426639_13`
See also `http://perso.ens-lyon.fr/damien.stehle/FPLLL.html`

[14] P. Q. Nguyen, D. Stehlé, *An LLL Algorithm with Quadratic Complexity.* SIAM J. Comput. **39** (2009), 874–903. `http://dx.doi.org/10.1137/070705702`

[15] O. T. O'Meara, *Introduction to Quadratic Forms*. Originally published as *Grundlehren der mathematischen Wissenscahften* **117**, Springer-Verlag, 1963.
http://www.springer.com/mathematics/numbers/book/978-3-540-66564-9

[16] M. Pohst, *A modification of the LLL reduction algorithm.* J. Symbolic Comp. **4**, no. 1 (1987), 123–7. http://dx.doi.org/10.1016/S0747-7171(87)80061-5

[17] J. M. Pollard, C. P. Schnorr. *An efficient solution of the congruence* $x^2 + ky^2 = m \pmod n$. IEEE Transactions on Information Theory **33**, no. 5 (1987), 702–9.
http://dx.doi.org/10.1109/TIT.1987.1057350

[18] B. Poonen, J. F. Voloch, *Random diophantine equations.* In *Arithmetic of higher-dimensional algebraic varieties,* B. Poonen and Yu. Tschinkel (eds.), Progress in Math. **226** (2004), Birkhäuser, 175–84.

[19] J.-P. Serre, *A Course in Arithmetic*, Springer GTM **7**, 1973.

[20] D. Shanks, *Gauss's ternary form reduction and the 2-Sylow subgroup.* Math. Comp. **25** (1971), 837–53; corrigendum *ibid.* **32** (1978), 1328–9.
http://www.ams.org/journals/mcom/1971-25-116/S0025-5718-1971-0297737-4/

[21] D. Simon, *Solving quadratic equations using reduced unimodular quadratic forms.* Math. Comp. **74** (2005), 1531–43.
http://www.ams.org/journals/mcom/2005-74-251/S0025-5718-05-01729-1/home.html

[22] D. Simon, *Formes quadratiques unimodulaires réeduites en petite dimension.* (French) [Reduced unimodular quadratic forms in small dimension]. Preprint (2005).
http://www.math.unicaen.fr/~simon/maths/det1.html

[23] D. Simon, *Quadratic equation in dimension 4, 5 and more.* Preprint (2005).
http://www.math.unicaen.fr/~simon/maths/dim4.html