PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
S 0002-9939(09)10131-4
Article electronically published on September 17, 2009

LLL REDUCTION AND A CONJECTURE OF GUNNELLS

DARRIN DOUD AND RUSSELL RICKS

(Communicated by Ken Ono)

Abstract. Paul Gunnells has developed an algorithm for computing actions of Hecke operators on arithmetic cohomology below the cohomological dimension. One version of his algorithm uses a conjecture concerning LLL-reduced matrices. We prove this conjecture for dimensions 2 through 5 and disprove it for all higher dimensions.

1. Introduction

Let Γ be a torsion-free finite-index subgroup of $SL_n(\mathbb{Z})$ or $GL_n(Z)$. In [5], Paul Gunnells describes algorithms to compute the action of the Hecke operators on the cohomology groups $H^{\nu-1}(\Gamma, \mathbb{Z})$ when $n = 2, 3$, or 4, where ν is the cohomological dimension of Γ. Such computations are useful in testing conjectures concerning relationships between arithmetic cohomology and Galois representations [1, 2, 3]. Gunnells' algorithms use either a conjecture concerning Voronoi reduction [5, Conj. 3.5], or a conjecture concerning LLL reduction [5, Conj. 3.9], both of which he states for arbitrary n. The version using Voronoi reduction generalizes more easily to other contexts, but the version using LLL reduction is computationally more convenient, due to the easy availability of high-quality code for LLL reduction. In this paper, we prove the conjecture involving LLL reduction for $n =$ 2, 3, 4, and 5 (using a computer calculation in dimensions 4 and 5), and we produce a counterexample for it in each dimension higher than five. Note that the fact that the conjecture is false in dimensions greater than 5 does not take away from its usefulness in computing with cohomology in dimensions 2, 3, and 4.

2. LLL-reduced bases

We recall the definitions of Gram-Schmidt orthogonalization and LLL-reduced bases from [4] (see also [6]).

Definition 2.1. Let $b_1, \dots, b_m$ be an ordered basis for a subspace V of $\mathbb{R}^n$. Define $b_1^* = b_1$, and inductively define b_i^* (for $1 < i \leq m$) by

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*,$$

Received by the editors December 31, 2008.
2000 *Mathematics Subject Classification.* Primary 11H55; Secondary 11F75.
Key words and phrases. LLL-reduced lattices.

where, for $1 \leq j < i$,

$$\mu_{ij} = \frac{b_i \cdot b_j^*}{|b_j^*|^2}.$$

We note that the basis $\{b_1^*, \dots, b_m^*\}$ is orthogonal but not orthonormal. In addition, we see that the orthogonalization depends strongly on the ordering of the original basis. In what follows, we will use the convention that, when given an ordered basis $\{b_i\}$, the vectors $\{b_i^*\}$ are the basis obtained by applying Gram-Schmidt orthogonalization and the constants μ_{ij} are the constants defined above.

Definition 2.2 (LLL-reduced)**.** We say that a basis $\{b_1, \dots, b_m\}$ for a subspace V of $\mathbb{R}^n$ is *LLL-reduced* if

(1) for $1 \leq j < i \leq m$, we have $|\mu_{ij}| \leq \frac{1}{2}$,
(2) for $2 \leq i \leq m$, we have $|b_i^* + \mu_{i,i-1} b_{i-1}^*|^2 \geq \frac{3}{4}|b_{i-1}^*|^2$.

Because the b_i^* are orthogonal, the second condition is easily seen to be equivalent to the condition

$$|b_i^*|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right)|b_{i-1}^*|^2.$$

Given a basis for a lattice V of $\mathbb{R}^n$, there is a fast (polynomial time) algorithm for computing an LLL-reduced basis for V [4, Section 2.6]. We will not describe this algorithm, as we do not need it, but it is used in Gunnells' algorithm for computing with modular symbols. We will need the following elementary bounds on LLL-reduced bases.

Proposition 2.3. *Let $b_1, \dots, b_m$ be an LLL-reduced basis for a subspace of $\mathbb{R}^n$. Then for $i \geq j$, the following inequalities hold:*

(1) $|b_j^*|^2 \leq 2^{i-j}|b_i^*|^2$,
(2) $|b_j|^2 \leq (2^{i-2} + 2^{i-j-1})|b_i^*|^2$.

Proof. We take our proof directly from [4, p. 85]. Since the b_i are LLL-reduced, we have that

$$|b_i^*|^2 \geq (3/4 - \mu_{i,i-1}^2)|b_{i-1}^*|^2 \geq \frac{1}{2}|b_{i-1}^*|^2.$$

Induction yields (1).

Since $b_j = b_j^* + \sum_{k=1}^{j} \mu_{jk} b_k^*$, and the b_k^* are orthogonal, we see (using (1)) that

$$|b_j|^2 = |b_j^*|^2 + \sum_{k=1}^{j-1} \mu_{jk}^2 |b_k^*|^2 \leq |b_j^*|^2 + \frac{1}{4}\sum_{k=1}^{j-1} 2^{j-k}|b_j^*|^2 = \left(\frac{2^{j-1}+1}{2}\right)|b_j^*|^2.$$

Combining this with (1), we obtain (2). □

Definition 2.4. Let B be an $n \times n$ matrix with integer entries. We say that B is *reduced* if

(1) $|\det(B)| > 1$,
(2) the rows of B form an LLL-reduced basis for $\mathbb{R}^n$.

3. Candidates for modular symbols

Definition 3.1. Let B be an $n \times n$ matrix with integer entries. A *candidate* for B is a vector $v \in \mathbb{R}^n$, so that for each matrix $B_i(v)$ formed by replacing the ith column of B with v $(1 \leq i \leq n)$, we have $|\det(B_i(v))| < |\det(B)|$.

Gunnells' algorithm requires us to find candidates for large numbers of matrices. In order to do this, Gunnells uses LLL reduction on the rows of a matrix, finds a candidate for the reduced matrix, and reverses the transformation giving the LLL-reduced basis to obtain a candidate for the original matrix. In order to quickly find a candidate for the LLL-reduced matrix, Gunnells stated the following conjecture.

Conjecture 3.2 ([5, Conj. 5.9])**.** *Let B be a reduced $n \times n$ matrix. Then one of the standard basis elements $e_1, \dots, e_n$ of $\mathbb{R}^n$ is a candidate for B.*

Gunnells gave extensive computational evidence for the conjecture with n up to 20. He also proved the conjecture for $n \times n$ matrices B with $|\det(B)| > 2^{n(n-1)/2}$, and for certain other cases. He did not, however, claim to have proved the conjecture completely for any specific value of n. In what follows, we will prove the conjecture for $2 \leq n \leq 5$ and disprove it for $n \geq 6$.

We begin by giving two restatements of the conjecture, which we will use in place of the original conjecture.

Conjecture 3.3. *For a reduced $n \times n$ matrix B, all the entries of some column of $\operatorname{adj}(B)$ have absolute value strictly less than $|\det(B)|$.*

Conjecture 3.4. *For a reduced $n \times n$ matrix B, all the entries of some column of B^{-1} have absolute value strictly less than 1.*

These two versions of the conjecture are easily seen to be equivalent to each other, since $\det(B)B^{-1} = \operatorname{adj}(B)$. To see that they are equivalent to the original conjecture, we note that if we denote by B_{ij} the matrix obtained by replacing the jth column of B by e_i, then the ji entry of $\operatorname{adj}(B)$ is (up to sign) the same as $\det(B_{ij})$. Hence, e_i is a candidate for B if and only if all entries of the ith column of $\operatorname{adj}(B)$ have absolute value less than $|\det(B)|$. Our computations will be done to investigate Conjecture 3.4.

4. Bounds for reduced bases

Throughout the rest of this paper, B is an $n \times n$ reduced matrix with rows b_i, the b_i^* are the vectors obtained from the b_i by Gram-Schmidt orthogonalization, and the μ_{ij} are the scalars obtained from Gram-Schmidt orthogonalization.

We begin by proving an elementary bound which guarantees that for certain reduced bases, e_n is a candidate. Note that this lemma is just Lemma 3.13 in [5].

Lemma 4.1. *Let B be an $n \times n$ reduced matrix. If $|b_n^*| > 1$, then e_n is a candidate for B.*

Proof. We begin by noting that, for $|b_n^*| > 1$, we have

$$|\det(B)| = \prod_{i=1}^{n} |b_i^*| > \prod_{i<n} |b_i^*|.$$

Now, for each standard basis vector e_k of $\mathbb{R}^n$, let B_k be the matrix obtained by replacing the last row of B by e_k. We will denote by e_k^* the final vector obtained by performing Gram-Schmidt orthogonalization on the rows of B_k. Clearly, $|e_k^*| \leq |e_k| = 1$, so we have that

$$|\det(B_k)| = |e_k^*| \prod_{i<n} |b_i^*| \leq \prod_{i<n} |b_i^*| < |\det(B)|,$$

for each k with $1 \leq k \leq n$.

Now we note that $\det(B_k)$ has the same absolute value as the determinant of the matrix obtained by replacing the kth column of B by e_n. Hence, since each $|\det(B_k)| < |\det(B)|$, we see that e_n is a candidate for B. □

Lemma 4.2. *If B is reduced, and $|b_{n-1}^*|^2 > (1 - \frac{4}{3}\mu_{n,n-1}^2)^{-1}$, then e_{n-1} is a candidate for B.*

Proof. We define C_k to be the matrix obtained from B by replacing the $(n-1)$st row by the standard basis vector e_k, and we define D_k to be the matrix obtained by swapping the last two rows of C_k. Note that e_{n-1} is a candidate for B exactly when each $|\det(D_k)| = |\det(C_k)| < |\det(B)|$. Applying Gram-Schmidt orthogonalization to the rows of D_k, we obtain an orthogonal set

$$b_1^*, \ldots, b_{n-2}^*, d_{n-1}^*, d_n^*.$$

Note that $|d_n^*| \leq |e_k| = 1$. Hence, we see that

$$|\det D_k| = |d_{n-1}^*||d_n^*| \prod_{i=1}^{n-2} |b_i^*| \leq |d_{n-1}^*| \prod_{i=1}^{n-2} |b_i^*|,$$

and this will be less than $|\det B|$ if $|d_{n-1}^*| < |b_{n-1}^*||b_n^*|$.

Examining the definition of the Gram-Schmidt process, we see that

$$d_{n-1}^* = b_n - \sum_{j=1}^{n-2} \mu_{nj} b_j^* = b_n^* + \mu_{n,n-1} b_{n-1}^*,$$

and, since b_n^* and b_{n-1}^* are orthogonal, we have that

$$|d_{n-1}^*|^2 = |b_n^*|^2 + \mu_{n,n-1}^2 |b_{n-1}^*|^2,$$

so e_{n-1} will be a candidate if

$$|b_n^*|^2 + \mu_{n,n-1}^2 |b_{n-1}^*|^2 < |b_{n-1}^*|^2 |b_n^*|^2.$$

Now under the assumption that $|b_{n-1}^*|^2 > (1 - \frac{4}{3}\mu_{n,n-1}^2)^{-1}$, and using that $\{b_1, \ldots, b_n\}$ are LLL-reduced, we have that

$$|b_n^*|^2 \geq \left(\frac{3}{4} - \mu_{n,n-1}^2\right) |b_{n-1}^*|^2 > \frac{\frac{3}{4} - \mu_{n,n-1}^2}{1 - \frac{4}{3}\mu_{n,n-1}^2} = 3/4.$$

Hence,

$$|b_{n-1}^*|^2 > \frac{1}{1 - \frac{4}{3}\mu_{n,n-1}^2} > \frac{1}{1 - \frac{1}{|b_n^*|^2}\mu_{n,n-1}^2} = \frac{|b_n^*|^2}{|b_n^*|^2 - \mu_{n,n-1}^2}.$$

Since, in an LLL-reduced basis, $\mu_{n,n-1}^2 \leq 1/4$, we have that $|b_n^*|^2 - \mu_{n,n-1}^2 > 0$. Multiplying by it, we see that $|b_{n-1}^*|^2(|b_n^*|^2 - \mu_{n,n-1}^2) > |b_n^*|^2$, so that

$$|b_n^*|^2 + \mu_{n,n-1}^2 |b_{n-1}^*|^2 < |b_{n-1}^*|^2 |b_n^*|^2.$$

As we have seen, this implies that e_{n-1} is a candidate for B. □

Corollary 4.3. *If B is reduced and $|b_{n-1}^*|^2 > 3/2$, then e_{n-1} is a candidate for B.*

Proof. If B is reduced, $\mu_{n,n-1}^2 \le 1/4$. Hence, $(1 - \frac{4}{3}\mu_{n,n-1}^2)^{-1} \le 3/2$. □

Corollary 4.4. *If B is reduced, and no standard basis vector is a candidate for B, then for $i < n$, $|b_i^*|^2 \le 3 \cdot 2^{n-i-2}$, and $\det(B)^2 \le 3^{n-1} 2^{(n-1)(n-4)/2}$.*

Proof. By Lemma 4.1, $|b_n^*|^2 \le 1$, and by Proposition 2.3 and Corollary 4.3, $|b_i^*|^2 \le 2^{n-i-1}|b_{n-1}^*|^2 \le 3 \cdot 2^{n-i-2}$ for $i < n$. Hence

$$\det(B)^2 = \prod_{i=1}^{n} |b_i^*|^2 \le \prod_{i=1}^{n-1} 3 \cdot 2^{n-i-2} = 3^{n-1} 2^{(n-1)(n-4)/2}.$$

□

Corollary 4.5. *If B is reduced, and no standard basis vector is a candidate for B, then for $i < n$, $|b_i|^2 \le \frac{3}{4}(2^{n-2} + 2^{n-i-1})$ and $|b_n|^2 \le \frac{5}{8} + 3 \cdot 2^{n-4}$.*

Proof. By Proposition 2.3 and Corollary 4.3, for $i < n$,

$$|b_i|^2 \le (2^{n-3} + 2^{n-i-2})|b_{n-1}^*|^2 \le \frac{3}{4}(2^{n-2} + 2^{n-i-1}).$$

Since $\{b_i^*\}$ is an orthogonal basis, $\mu_{ij}^2 \le \frac{1}{4}$, $|b_n^*|^2 \le 1$, and $|b_i^*|^2 \le 3 \cdot 2^{n-i-2}$, we see that

$$|b_n|^2 = |b_n^*|^2 + \sum_{i=1}^{n-1} \mu_{n,i}^2 |b_i^*|^2 \le 1 + \sum_{i=1}^{n-1} \frac{1}{4} \cdot 3 \cdot 2^{n-i-2} = 1 + \frac{3}{8}(2^{n-1} - 1) = \frac{5}{8} + 3 \cdot 2^{n-4}.$$

□

5. Dimensions two and three

Theorem 5.1. *Conjecture 3.2 is true in dimensions two and three.*

Proof. In the two-dimensional case ($n = 2$), we find from Corollary 4.4 that any counterexample to the conjecture would have $1 < \det(B)^2 \le 3/2$. Since $\det(B)$ must be an integer, no such counterexample can exist.

In three dimensions, we see that any counterexample would have $1 < \det(B)^2 \le 9/2$. Hence, it must be the case that $\det(B)^2 = 4$. In addition, Lemma 4.1 and Corollary 4.3 show that

$$|b_1|^2 = |b_1^*|^2 = \frac{\det(B)^2}{|b_2^*|^2 |b_3^*|^2} \ge \frac{8}{3} > 2.$$

However, by Corollary 4.5, $|b_2|^2 \le 9/4 < 3$. Hence, $|b_2|^2 \le 2$, and we have, from Definitions 2.1 and 2.2, that

$$|b_1|^2 = |b_1^*|^2 \le \frac{4}{3}|b_2^* + \mu_{21} b_1^*|^2 = \frac{4}{3}|b_2|^2 \le \frac{8}{3} < 3.$$

This implies that $2 < |b_1|^2 < 3$, which is impossible. Hence, there can be no counterexamples to the conjecture in three dimensions. □

6. Dimensions four and five

For dimension four, Corollary 4.5, together with the fact that each $|b_i|^2$ must be an integer, yields the following bounds on the size of the $|b_i|^2$ for any counterexample to the conjecture:

$$|b_1|^2 \leq 6, \quad |b_2|^2 \leq 4, \quad |b_3|^2 \leq 3, \quad |b_4|^2 \leq 3.$$

For dimension five, similar considerations yield the bounds

$$|b_1|^2 \leq 12, \quad |b_2|^2 \leq 9, \quad |b_3|^2 \leq 7, \quad |b_4|^2 \leq 6, \quad |b_5|^2 \leq 6$$

for any counterexample to the conjecture. For each of these cases, we wrote a computer program (in GP/PARI [7]) which searched through all LLL-reduced bases consisting of vectors satisfying the bounds in Corollary 4.5, Lemma 4.1, and Lemma 4.2, and checked whether the conjecture was true for each such basis. Since any counterexample to the conjecture must satisfy these bounds, finding no counterexamples proves the theorem. We also used symmetry to reduce the search space, as described in the following paragraphs.

We noted that any counterexample could have the entries of the b_i permuted (for instance, swapping the third and fourth coordinates of all the b_i) and would still yield a counterexample. In addition, multiplying a fixed coordinate of each b_i by -1 would also yield a counterexample. Applying permutations and negations of coordinates allowed us to look only at bases for which b_1 had non-negative, non-increasing entries. This greatly reduced the number of possibilities for b_1.

After selecting a vector for b_1, we looked at possibilities for b_2. If an entry of b_1 was 0, we looked only at b_2 in which that coordinate was non-negative (since negating a coordinate does not affect a counterexample, this is justified). We then checked that b_2^* was smaller than $3 \cdot 2^{n-4}$, as required by Corollary 4.4, and that the combination of b_1 and b_2 satisfied the properties of an LLL-reduced basis.

We then selected vectors $b_3, b_4, \ldots$, in turn, at each stage checking that the given vector satisfied the length bounds and the conditions to be part of an LLL-reduced basis, and that the resulting b_i^* satisfied the length requirements of Corollary 4.4 and Lemma 4.2 for a counterexample.

Once all the b_i were chosen, we checked to see if the resulting matrix B was a counterexample to Conjecture 3.4.

The degree-four computation checked a total of 1,280 reduced bases in 1.1 seconds, and found that no counterexamples exist. The degree-five computation checked a total of 1,469,824 reduced bases in 1.82 hours and found that no counterexamples exist. Hence, the following theorem is proved.

Theorem 6.1. *Conjecture* 3.2 *is true in dimensions four and five.*

7. Dimension six and higher

In dimension six, a computer search similar to that used for dimensions four and five proved impractical, since the search space is much larger. However, in checking the size of the search space, a preliminary computation yielded the following result after less than one day of computer time.

Theorem 7.1. *Conjecture* 3.2 *is false in dimensions six and higher.*

Proof. In dimension six, we examine the following matrix:

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

We note that its rows form an LLL-reduced basis of $\mathbb{R}^6$, and its determinant is -8. No standard basis vector is a candidate for A, since replacing the fifth column of A by any standard basis vector gives a matrix with determinant ± 8. Alternatively, we note that every entry in the fifth row of A^{-1} has absolute value 1, so that Conjecture 3.4 fails for A. Hence, Conjecture 3.2 is false in dimension six.

If $n > 6$, let A_n be the block diagonal matrix $A \oplus I_{n-6}$, where I_k denotes the $k \times k$ identity matrix. Then the rows of A_n are easily seen to be LLL-reduced, since the rows of A are, and the conjecture clearly fails for A_n. Indeed, we see that $A_n^{-1} = A^{-1} \oplus I_{n-6}$, and since every column of A^{-1} has an entry of absolute value 1, every column of A_n^{-1} has an entry of absolute value 1. Hence, no standard basis vector is a candidate for A_n, and Conjecture 3.2 is false in every dimension higher than 6. □

We remark that even though [5, Conj. 3.9] is false in dimension six and higher, it may still be possible to use LLL reduction to find candidates for matrices in these dimensions. Applying LLL reduction to a basis that is already LLL-reduced can change the basis. For instance, as was pointed out by the referee, applying LLL reduction (as implemented in GP/PARI [7]) to the rows of the matrix in our counterexample yields a matrix which does have a standard basis vector as a candidate. Hence, some adjustment to the algorithm could yield a method of using LLL reduction to find candidates for matrices in arbitrary dimension.

References

1. Avner Ash, Darrin Doud, and David Pollack, *Galois representations with conjectural connections to arithmetic cohomology*, Duke Math. J. **112** (2002), no. 3, 521–579. MR1896473 (2003g:11055)
2. Avner Ash, Paul E. Gunnells, and Mark McConnell, *Cohomology of congruence subgroups of* $\mathrm{SL}_4(\mathbb{Z})$, J. Number Theory **94** (2002), no. 1, 181–212. MR1904968 (2003f:11072)
3. ———, *Cohomology of congruence subgroups of* $\mathrm{SL}(4,\mathbb{Z})$. *II*, J. Number Theory **128** (2008), no. 8, 2263–2274. MR2394820
4. Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR1228206 (94i:11105)
5. Paul E. Gunnells, *Computing Hecke eigenvalues below the cohomological dimension*, Experiment. Math. **9** (2000), no. 3, 351–367. MR1795307 (2001k:11092)
6. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534. MR682664 (84a:12002)
7. The PARI-Group, Bordeaux, PARI/GP, Version 2.3.3, 2007, available from http://pari.math.u-bordeaux.fr/.

Department of Mathematics, Brigham Young University, Provo, Utah 84602
E-mail address: doud@math.byu.edu

Department of Mathematics, Brigham Young University, Provo, Utah 84602
E-mail address: russellricks@byu.edu