Discrete Math, Seventh Problem Set (July 2)

REU 2003

Instructor: Laszlo Babai
Scribe: Varsha Dani

Exercise 0.1. Consider an infinite checkerboard. We will associate a cost of \$1 to each black square, and \$(−1) to each white square. We say that a rectangle is "aligned" if its sides are parallel to the axes of the checkerboard. For an aligned rectangle, we can define its cost to be the sum of the costs of the checkerboard squares that it intersects. Partially covered squares are evaluated proportionally; e. g. if say 70% of a black square is covered, the associated cost is \$ -0.7. Show that the following are equaivalent for an aligned rectangle R:

1. the cost of every translate[1] of R is zero;
2. R has a side of even integer length. (The unit of length is the sidelength of a square in the checkerboard.)

Exercise 0.2. If vertex v in the graph G has odd degree then there is a vertex $w \neq v$, also of odd degree, such that G contains a $v - w$ path.

Exercise 0.3. Let R be a rectangle. Consider a tiling of R by non-overlapping axis-parallel rectangles. Suppose each rectangle in the tiling has at least one side of integer length. Then R also has at least one side of integer length.

1. Prove this using Exercise 1.
2. Prove this using Exercise 2.

We now turn our attention to an algorithmic problem. Consider a lattice in $\mathbb{R}^n$, specified by a basis. We want to find the shortest non-zero vector in the lattice. Moreover, we would like to be able to do this "efficiently," in the sense that the number of steps taken by the algorithm should be bounded by a polynomial function of the bit-length of the input (number of zeros and ones needed to describe the input).

Let $L = \sum_{i=1}^{n} \mathbb{Z}\mathbf{b}_i$ where the $\mathbf{b}_i \in \mathbb{Z}^n$ are linearly independent. Note that we restrict our attention to bases in $\mathbb{Z}^n$ rather than $\mathbb{R}^n$ because we need the number of bits in the input to be finite. The length is the total number of bits needed to describe all entries of the matrix $[b_1, b_2, \dots, b_n]$.

[1] The statement is not true with the words "every translate of" removed. Why not?

Exercise 0.4. Show that the number of bits in the binary expansion of a positive integer N is $\lfloor \log N \rfloor + 1$.

So for example if each coordinate has m bits, then the input length is mn^2.

A *polynomial time algorithm* is one that takes at most $C_1(\text{input length})^{C_2}$ steps to execute. For example an algorithm that runs in $C(\text{input length})^3$ steps is a cubic algorithm.

The shortest vector in a lattice is the zero vector. When we talk about "the shortest vector" in a lattice, we mean the shortest non-zero vector.

Finding the shortest vector in a lattice is *NP-hard* (Ajtai, 2000). Roughly speaking this means that the problem is at least as hard as any combinatorial search problem: if we could solve it in polynomial time, we could use that to solve any other combinatorial search problem in polynomial time. For example we could factor large numbers in polynomial time.

Lovász's lattice reduction algorithm (1980) which we are about to see is a polynomial time algorithm, and it does *not* find the shortest vector in the lattice. What it *does* find is a vector in the lattice that is "short enough." Specifically, it finds a vector $x \in L$ with $\|x\| \leq 2^{(n-1)/2}\text{min}L$ where n is the dimension and

$$\text{min}L := \min\{\|\mathbf{v}\| \,:\, \mathbf{v} \in L, \mathbf{v} \neq 0\}.$$

In fact it does more; it finds a certain "nice" basis for the lattice, called a *Lovász-reduced basis.* A "nice" basis is one that is "close" to being orthogonal in some vague sense. It will turn out that the first vector of a Lovász-reduced basis is a $2^{(n-1)/2}$-approximation to the shortest vector in the lattice.

First we need to define a Lovász-reduced basis. Recall the Gram-Schmidt orthogonalization process for obtaining an orthogonal basis for the span of a set of linearly independent vectors. If $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is the original basis, and $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ is the orthogonalized basis then we have

$$(\forall i, 1 \leq i \leq n) \left(\mathbf{b}_i = \mathbf{b}_i^* + \sum_{j<i} \mu_{i,j} \mathbf{b}_j^* \right).$$

Now if the given basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is orthogonal then $(\forall i, j)\,(\mu_{i,j} = 0)$. One possible meaning of being "close to orthogonal" is that all the $\mu_{i,j}$ are small in absolute value; a Lovász-reduced basis intends to meet this objective.

Additionally, we do not want the basis vector $\mathbf{b}_i$ to be too close to the subspace $\mathcal{U}_{i-1}$, the span of $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$, i. e., we do not want $\mathbf{b}_i^*$ to have too small norm.

The following definition gives a prcise meaning to these two requirements:

Definition 0.5. A basis $\mathbf{b}_1, \ldots, \mathbf{b}_n \in R^n$ is *Lovász-reduced* if after performing the Gram-Schmidt orthogonalization process on it, the following conditions hold:

1. $(\forall i, j)\left(|\mu_{i,j}| \leq \frac{1}{2}\right)$;

2. $(\forall i)\left(\|\mathbf{b}_{i+1}^*\| \geq \frac{1}{\sqrt{2}}\|\mathbf{b}_i^*\|\right)$.

Note that the definition is sensitive to order: the same basis vectors in a different order may not form a Lovász-reduced basis.

The following lemma applies to all bases, not only to L-reduced ones. The lemma will be our key tool to proving that in a L-reduced basis, the first basis vector is not much longer than $\min L$.

Lemma 0.6. *For all lattices and bases,* $\min L \geq \min_{1\leq i\leq n} \|\mathbf{b}_i^*\|$.

Proof: Let $\mathbf{x} \in L$, $\mathbf{x} \neq 0$. Then there exist $\alpha_i \in \mathbb{Z}$ not all zero, such that $\mathbf{x} = \sum_{i=1}^n \alpha_i \mathbf{b}_i$. Let t be the largest index for which $\alpha_t \neq 0$, i. e., $\alpha_t \neq 0$ and $\alpha_i = 0$ for all $i > t$. Then $\mathbf{x} = \sum_{i=1}^t \alpha_i \mathbf{b}_i$. Now recall that the Gram-Schmidt process on $\mathbf{b}_1, \ldots, \mathbf{b}_n$ produces orthogonal vectors $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ with the property that for all i with $1 \leq i \leq n$, $\mathrm{Span}(\mathbf{b}_1, \ldots, \mathbf{b}_i) = \mathrm{Span}(\mathbf{b}_1^*, \ldots, \mathbf{b}_i^*)$. Thus there exist $\beta_i \in \mathbb{R}$ such that $\mathbf{x} = \sum_{i=1}^t \beta_i \mathbf{b}_i$. Note that while the β_i do not have to be integers, the last one, β_t *is* an integer. To see this, note that for all i with $1 \leq i \leq t$,

$$\alpha_i \mathbf{b}_i = \alpha_i \mathbf{b}_i^* + \sum_{j<i} \alpha_i \mu_{i,j} \mathbf{b}_j^*.$$

Summing this up for $i \leq t$, we obtain

$$\mathbf{x} = \sum_{i=1}^t \alpha_i \mathbf{b}_i = \sum_{i=1}^t \alpha_i \mathbf{b}_i^* + \sum_{i=1}^t \sum_{j<i} \alpha_i \mu_{i,j} \mathbf{b}_j^*.$$

The second term on the right hand side does not contain $\mathbf{b}_t^*$, so $\mathbf{b}_t^*$ occurs only once, with coefficient α_t. Since the $\mathbf{b}_i^*$ are linearly independent and $\mathbf{x} = \sum_{i=1}^t \beta_i \mathbf{b}_i^*$ it follows that $\beta_t = \alpha_t \in \mathbb{Z}$. Now since the $\mathbf{b}_i^*$ are orthogonal,

$$\|\mathbf{x}\|^2 = \sum_{i=1}^t \beta_i^2 \|\mathbf{b}_i^*\|^2 \;\geq\; \beta_t^2 \|\mathbf{b}_t^*\|^2 \;\overset{(*)}{\geq}\; \|\mathbf{b}_t^*\|^2 \;\geq\; \min_{1\leq i\leq n} \|\mathbf{b}_i^*\|^2,$$

where inequality (*) follows from the fact that if $\beta \in \mathbb{Z}$ and $\beta \neq 0$ then $|\beta| \geq 1$. Taking the minimum over all $\mathbf{x} \in L$ now completes the proof. □

Observation 0.7. If $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is a Lovász-reduced basis for the lattice L then for all i, $\|\mathbf{b}_1^*\| \leq 2^{(i-1)/2}\|\mathbf{b}_i^*\|$ (by induction, using property (2) of such a basis). Therefore

$$\|\mathbf{b}_1^*\| \leq 2^{(n-1)/2} \min_{1\leq i\leq n} \mathbf{b}_i^* \leq 2^{(n-1)/2} \min L.$$

Since $\mathbf{b}_1^* = \mathbf{b}_1$ we have

Corollary 0.8. *If* $\mathbf{b}_1, \dots, \mathbf{b}_n$ *is a Lovász-reduced basis for lattice* L *then* $\|\mathbf{b}_1\| \le 2^{(n-1)/2}\min L$.

We still have to find a Lovász-reduced basis in L.

Lovász's Algorithm

Input: $[\mathbf{b}_1, \dots, \mathbf{b}_n] \in \mathbb{Z}^{n\times n}$, non-singular.
Output: $[\mathbf{b}'_1, \dots, \mathbf{b}'_n] \in \mathbb{Z}^{n\times n}$, a Lovász-reduced basis of the same lattice, i. e., $L = \sum_{i=1}^n \mathbb{Z}\mathbf{b}_i = \sum_{i=1}^n \mathbb{Z}\mathbf{b}'_i$.

The algorithm will make two kinds of steps, which try to achieve the two conditions in the definitions. The first kind will perform elementary transformations on the basis (replacing $\mathbf{b}_i$ by $\mathbf{b}_i - \alpha\mathbf{b}_j$ for a suitable scalar α) with the goal to make the condition $|\mu_{i,j}| \le \frac{1}{2}$ hold. We repeat this type of steps until all $\mu_{i,j}$ satisfy this inequality (so condition (1) holds).

Once condition (1) has been achieved, we check for condition (2) and will switch the order of a pair of consecutive basis vectors where violation is found. We perform this operation only once per round. While it is not immediately clear how this kind of rearrangement is of any help, it is clear that such a rearrangement may destroy the condition $|\mu_{i,j}| \le \frac{1}{2}$ we have labored hard to achieve, so we must return to the elementary transformations to restore condition (1).

All in all, it is not evident that such an approach will converge to anything at all; but if it does converge, the result is a Lovász-reduced basis.

Making the $\mu_{\mathbf{i,j}}$ s small
Let $\mathcal{U}_i$ denote Span$(\mathbf{b}_1, \dots, \mathbf{b}_i)$. If $\mathbf{b}^*_1, \dots \mathbf{b}^*_n$ are the vectors produced by the Gram-Schmidt process, then for all i, Span$(\mathbf{b}^*_1, \dots, \mathbf{b}^*_i) = \mathcal{U}_i$ and $\mathbf{b}_i - \mathbf{b}^*_i \in \mathcal{U}_{i-1}$; and these two conditions determine the $\mathbf{b}^*_i$. So the elementary transformations $\mathbf{b}_i \mapsto \mathbf{b}_i - \alpha\mathbf{b}_j$ $(j < i)$ do not change any of the $\mathbf{b}^*_i$. $\mathbf{b}'_1, \dots \mathbf{b}'_n$ will produce the same vectors $\mathbf{b}^*_i$. On the other hand, the $\mu_{i,j}$ will change; we need to calculate this change to see that with the appropriate choice of the coefficient $\alpha \in \mathbb{Z}$, the condition $|\mu_{i,j}| \le 1/2$ will be achieved.

Here is then the first procedure:

```
Procedure "coefficient reduction"
    for $i = 2$ to $n$
        for $j = i - 1$ downto 1
            $\mathbf{b}_i := \mathbf{b}_i - \lfloor \mu_{i,j} \rceil \, \mathbf{b}_j$
```

Here $\lfloor x \rceil$ denotes the integer nearest to x. Ties are broken arbitrarily.

Exercise 0.9. Prove that the basis produced by this procedure satisfies condition (1).

Exercise 0.10. Why do we need to have the inner loop go **down**? Show that the procedure would fail to achieve codition (1) if we had "**for** $j = 1$ **to** $i - 1$" in the inner loop. – Does the order in which the outer loop goes matter? Could we use the "**downto**" command in the outer loop?

Complexity analysis: "coefficient reduction" requires $\binom{n}{2}$ elementary basis transformations, each of which takes $O(n)$ arithmetic operations. One more thing to worry about: do the integers involved grow in the process?

Exercise 0.11. Construct a simple sequence of n arithmetic operations which do not constitute a polynomial-time algorithm when started from an n-digit input. *Hint.* Make the numbers grow too fast.

Swapping

Now we check property 2. If it is violated, we swap a violating pair $\mathbf{b}_i$ and $\mathbf{b}_{i+1}$. Then we start over with coefficient reduction again. If property 2 is ever satisfied after coefficient reduction then we are done. Here is the full algorithm in pseudocode:

```
Procedure "Lattice Reduction"
    while basis not Lovász-reduced
        if $(\exists i > j)(|\mu_{i,j}| > 1/2)$ then do coefficient reduction
        else find first $i$ such that $\|\mathbf{b}^*_{i+1}\| < \frac{1}{\sqrt{2}}\|\mathbf{b}^*_i\|$;
            swap $\mathbf{b}_i$ and $\mathbf{b}_{i+1}$;
            update orthogonalized sequence.
```

To prove that this algorithm terminates, we use a **potential function** argument, a general method of algorithm analysis which assigns a value (the "potential") to each "configuration" of variables in such a way that each phase of the algorithm reduces the potential.

The *Lovász potential* of a basis $\mathbf{b}_1, \dots, \mathbf{b}_n$ is defined to be the quantity

$$\mathrm{vol}\,(\mathbf{b}_1) \cdot \mathrm{vol}\,(\mathbf{b}_1, \mathbf{b}_2) \cdot \dots \cdot \mathrm{vol}\,(\mathbf{b}_1, \dots, \mathbf{b}_n),$$

where vol refers to the appropriate dimensional volume of the parallelepiped spanned by the vectors in the argument.

Exercise 0.12. Show that the following quantity is equal to the Lovász potential:

$$\|\mathbf{b}^*_1\|^n \|\mathbf{b}^*_2\|^{n-1} \dots \|\mathbf{b}^*_n\|.$$

It follows from the exercise that the Lovász potential does not change under the "coefficient reduction" procedure. (Why?)

Exercise 0.13. Prove that each execution of the "swap" command in the main algorithm reduces the Lovász potential at least by a fixed constant factor, say 0.9.

Exercise 0.14. Show that for integral lattices (where all cordinates of the input vectors are integers), the Lovász potential is the sqaure root of an integer.

Therefore, for integral lattices, the Lovász potential is ≥ 1. It follows that the algorithm terminates in $O(\log I)$ phases, where I is the initial potential. Since each phase takes $O(n^2)$ steps, the algorithm takes $\log I O(n^2)$ steps.

Exercise 0.15. Estimate the initial potential I. Show that $\log I$ is polynomially bounded as a function of the bit-length of the input.

Exercise 0.16. Does the preceding exercise complete the polynomial-time analysis of the basis reduction algorithm? *Hint.* No, we have only estimated the number of arithmetic operations, and not the bit-size of the numbers on which they need to be performed. Take care of this missing part of the analysis.