Abstract

We show how Frieze’s analysis of subset sum solving using lattices can be done without any large constants and without flipping. We apply the variant without the large constant to inputs with noise.

1 Introduction

In [4], Lagarias and Odlyzko introduce a lattice based method for efficiently solving subset sum problems with large integers, with high probability. In [2], Frieze applies two slight alterations to the method of Lagarias and Odlyzko, and is then able to provide a very simple proof of the high probability correctness of the altered method. The first alteration, as we describe below is the introduction of a large constant in their lattice construction. The second introduction is testing a certain condition on the input and if this condition fails, instead solving a suitably “flipped” problem.

In this note we first show that one can avoid the use of this large constant without sacrificing the result or making the proof (much) more complicated. We next show that if we alter the problem by adding one extra row to the lattice construction, we can avoid the test-and-flip step.

Our motivation for removing the large constant comes from our desire to deal with slightly noisy input. In [3, 6], the authors further altered Frieze’s lattice construction to deal with noisy input. In this note we also show, that once the large constant is removed, small noise can be dealt with without any alterations at all.

The ideas in this note have been applied in [1] where we use a lattice based approach to reconstruct a one-dimensional point configuration from an unlabeled subset of the interpoint distances.

This text will be borrow quite heavily from Frieze’s language verbatim throughout, without further specific attribution, and we will assume the reader is quite familiar with that paper.

2 Basic Lattice Construction

Let $\mathbf{e} = [e_1; e_2; \ldots; e_n] \in \{0,1\}^n$ be fixed. Let $B_1, B_2, \ldots, B_n$ be positive integers and $B_0 = \sum_{i=1}^n B_i e_i$. We will assume that $B_1, B_2, \ldots, B_n$ are independently chosen at random from 1, \ldots, $B = 2^{cn^2}$ with $c = 1/2 + \epsilon$ for $\epsilon > 0$. The given SUBSET-SUM problem is to find $\mathbf{e}$ given $B_0, B_1, \ldots, B_n$.

Adapting the method of [4], Frieze assumes that

$$B_0 \geq \frac{1}{2} \sum_{i=1}^n B_i \quad (1)$$

If this doesn’t hold, he instead replaces $B_0$ by

$$\left( \sum_{i=1}^n B_i \right) - B_0$$
Plainly, this new problem has a solution iff the original does, and one can easily determine \( e \) from the solution to the new problem. We call this step “test-and-flip”.

Adapting the method of \([4]\), Frieze then defines the integer lattice that is generated by the \((n + 1)\)-by\((n + 1)\) matrix:

\[
\begin{pmatrix}
  pB_0 & -pB_1 & -pB_2 & \ldots & -pB_{n-1} & -pB_n \\
  0 & 1 & 0 & \ldots & 0 & 0 \\
  0 & 0 & 1 & \ldots & 0 & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
  0 & 0 & 0 & \ldots & 1 & 0 \\
  0 & 0 & 0 & \ldots & 0 & 1 \\
\end{pmatrix}
\]

where the integer \( p > n^{2n/2} \) plays the role of a “large constant”.

The LLL algorithm \([5]\), (an efficient algorithm) is then run to find a small vector in this lattice.

We will state the main result of Frieze in the following form:

**Theorem 2.1.** For all \( \epsilon > 0 \), there is an \( n_0(\epsilon) \in \mathbb{N} \), such that if \( n > n_0 \), the algorithm returns a vector that is a scale factor of \( e \) with probability at least \( 1 - 2^{-\epsilon n^2/2} \).

(The use of \( n_0 \) mirrors the use in \([4]\) immediately following their Theorem 3.5.)

### 3 Removing the large constant

Here we show that the large constant can be removed without changing the correctness of the method, and without changing the proof too much.

Without the large constant, similarly to \([4]\), the lattice \( L \) will be generated by the columns of the \((n + 1)\)-by\((n + 1)\) matrix:

\[
\begin{pmatrix}
  B_0 & -B_1 & -B_2 & \ldots & -B_{n-1} & -B_n \\
  0 & 1 & 0 & \ldots & 0 & 0 \\
  0 & 0 & 1 & \ldots & 0 & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
  0 & 0 & 0 & \ldots & 1 & 0 \\
  0 & 0 & 0 & \ldots & 0 & 1 \\
\end{pmatrix}
\]

with columns \( b_0, \ldots, b_n \).

The LLL algorithm is guaranteed to find us \( x \in L, x \neq 0 \) satisfying

\[
||x|| \leq 2^{n/2}||e|| \leq 2^{n/2}n^{1/2} =: m
\]

If \( x = [x_0; x_1; \ldots; x_n] \in L \) then we have

\[
x = x'_0b_0 + x_1b_1 + \ldots + x_nb_n
\]

where

\[
x_0 = \left( B_0x'_0 - \sum_{i=1}^{n} B_ix_i \right)
\]

Let \( A = \{x \in L, ||x|| \leq m, x \neq k[0; e] \} \) for any \( k \in \mathbb{Z} \). This is the set that can give rise to algorithmic failure.
But if \( x \in A \) then
\[
|B_0x'_0| = |x_0 + \sum_{i=1}^{n} B_i x_i| \leq |x_0| + \sum_{i=1}^{n} B_i |x_i|
\]

Using (1), this gives us
\[
|x'_0| \leq \frac{|x_0|}{B_0} + \frac{\sum_{i=1}^{n} B_i |x_i|}{B_0} \leq \frac{|x_0|}{B_0} + 2|x| \leq 3m
\]

Note that we get a 3\( m \) instead of Frieze’s 2\( m \) but this will not be material, as we shall see below.

So if \( A \neq \emptyset \) there exists \( x = [x_0; x_1; x_2; \ldots; x_n] \in \mathbb{Z}^{n+1} \) and \( y \in \mathbb{Z} \) satisfying
\[
||x|| < m, \quad |y| \leq 3m \quad (a)
\]
\[
x \neq k[0; e] \quad \text{for any } k \in \mathbb{Z} \quad (b)
\]
\[
\sum_{i=1}^{n} B_i x_i = yB_0 - x_0 \quad (c)
\]

Consider now a fixed \((x, y)\) satisfying (a) and (b), we will prove that
\[
\Pr(x, y \text{ satisfy (c)}) \leq 1/B
\]

To prove this, note that (c) is equivalent to \( \sum_{i=1}^{n} B_i z_i = -x_0 \) where \( z_i = x_i - ye_i \). This is simply a non-trivial (due to (b)) inhomogeneous linear equation over the \( \{B_1, \ldots, B_n\} \).

**Lemma 3.1.** Let \( H \) be a \( d \)-dimensional affine subset of \( \mathbb{R}^n \). The number of points in the discrete cube \([1...B]^n\) intersected with \( H \) is at most \( B^d \).

**Proof.** Let \( C^n \) be the discrete cube of the statement. Define \( C^d \) similarly. The projection of \( H \) onto the the first \( d \) coordinates by forgetting the last \( n - d \) coordinates is a bijective (if not, pick a different coordinate subspace), and in particular injective, affine map that sends points in \( H \cap C^n \) to points \( C^d \). It follows that \( |H \cap C^n| \leq |C^d| = B^d \).

Since we have one equation, we get \( d = n - 1 \) in our application of Lemma 3.1, giving us \( \frac{B^{n-1}}{B^n} = 1/B \).

**Remark 3.2.** In Frieze’s original method, he gets \( x_0 = 0 \), and so his linear equation is guaranteed to be homogeneous. This does not effect the count of Lemma 3.1. Frieze states his argument for this step probabilistically, but we prefer the more general linear algebraic interpretation. Note the Frieze’s probabilistic argument could have worked in the inhomogeneous case as well.

Letting \( A_1 = \{ x \in \mathbb{Z}^{n+1} : ||x|| \leq m \} \) and summing over all \( A_1 \) and \( y \), we get a failure probability bound of
\[
\frac{(6n+1)|A_1|}{B} \leq \frac{(6n+1)(2m+1)^n+1}{B} \leq \frac{2n^22^O(n \log n)}{B} \leq O(2^{-\alpha n^2/2}) \quad (3)
\]

We get \((2m + 1)^n+1\) instead of \((2m + 1)^n\) as in [2], but this is subsumed into the \( 2^O(n \log n) \) in the next step. We expand on the last inequality in the following lemma.
Lemma 3.3. For fixed $\epsilon > 0$. For $n$ sufficiently large (depending on $\epsilon$), the probability of failure is at most $\frac{1}{2^{n^2/2}}$

Proof. Recall $B = 2^n$ where $c = 1/2 + \epsilon$ for $\epsilon > 0$. For sufficiently large $n$, the quantity $2^{n^2/2}2^{O(n \log n)}$ is bounded by $2^{(\frac{1}{2} + \frac{\epsilon}{2})n^2}$. The probability of the event in the statement is then at most

$$\frac{2^{(\frac{1}{2} + \frac{\epsilon}{2})n^2}}{2^{(\frac{1}{2} + \epsilon)n^2}} = \frac{1}{2^{n^2/2}}$$

This Lemma then establishes the result of Theorem 2.1.

In summary, Frieze’s argument goes through without the use of the large constant. The bound on $y$ becomes slightly worse, as does a term in the count of Equation 3, but all of this is swallowed up by the $2^{O(n \log n)}$ term. Perhaps the biggest difference is that his original homogeneous linear constraint becomes inhomogeneous, but both cases are covered by Lemma 3.1.

4 Removing the flip

Here we show that the assumption of Equation 1 can be removed if we add one more row to our lattice generating matrix.

We will leave the big constant out.

So now our lattice $L$ will be generated by the columns of the $(n+2)$-by-$(n+1)$ matrix:

$$
\begin{pmatrix}
B_0 & -B_1 & -B_2 & \cdots & -B_{n-1} & -B_n \\
1 & 0 & 0 & \cdots & 0 & 0 \\
0 & 1 & 0 & \cdots & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 \\
\end{pmatrix}
$$

Note the new second row.

The LLL algorithm will find us $x \in L$, $x \neq 0$ satisfying

$$||x|| \leq 2^{(n+1)/2}||[1; e]|| \leq 2^{(n+1)/2}(n+1)^{1/2} \leq 2 \cdot 2^{n/2}n^{1/2} =: m$$

This $m$ is slightly larger than that of the previous section, but not in a way that will prove material. If $x = [x_0; x'_0; x_1; \ldots; x_n] \in L$ then we have

$$x = x'_0 b_0 + x_1 b_1 + \ldots + x_n b_n$$

where

$$x_0 = \left( B_0 x'_0 - \sum_{i=1}^{n} B_i x_i \right)$$

The main idea here is that the $x'_0$ data will show up in the lattice vector. We will bounding the size of the lattice vectors, so we will not need any extra bounding for $x'_0$, hence no need for a flip.

Let $A = \{ x \in L, ||x|| \leq m, x \neq k[0; 1; e] \}$ for any $k \in \mathbb{Z}$.
So if $A \neq \emptyset$ there exists $x = [x_0; x_0'; x_1; x_2; \ldots; x_n] \in \mathbb{Z}^{n+2}$ satisfying

$$||x|| < m,$$

(a')

$$x \neq k[0; 1; e] \text{ for any } k \in \mathbb{Z}$$

(b')

$$\sum_{i=1}^{n} B_i x_i = x_0' B_0 - x_0$$

(c')

Consider now a fixed $x$ satisfying (a') and (b'), we prove, as above, that

$$\Pr(x \text{ satisfy (c')}) \leq 1/B$$

To prove this, note that (c') is equivalent to $\sum_{i=1}^{n} B_i z_i = -x_0$ where $z_i = x_i - x_0' e_i$. Again, this is an inhomogeneous linear equation over $\{B_1 \ldots B_n\}$.

Letting $A_1 = \{x \in \mathbb{Z}^{n+2} : ||x|| \leq m\}$ and summing over all $A_1$, we get

$$\frac{|A_1|}{B} \leq \frac{(2m + 1)^{n+2}}{B} \leq \frac{2^{n/2} O(n \log n)}{B} \leq O(2^{-cn^2/2})$$

Note that we get an $n+2$ exponent in the second term instead of Frieze's $n$, but this is not material for the third term.

From what we have gleamed from [4] (which has its own version of flipping), we suspect that the test-and-flip step can be omitted, and no extra row needs to be added, without impacting the success of the algorithm. (This is also consistent with our experiments, below.) But proving this might require going back to the proof methods of [4], which are more involved.

5 Adding Noise

Let $\varepsilon$ be a $\{-1, 0, 1\}^n$ be a fixed noise vector. And suppose that instead of the correct $B_i$, we are given $\{B_0, B_1 + \varepsilon_1, \ldots B_2 + \varepsilon_n\}$. ($B_0$ itself is given without noise.) We will see that whp, we can still solve the underlying subset sum problem.

Our lattice will now be generated by the columns of the matrix

$$M := \begin{pmatrix} B_0 & -B_1 - \varepsilon_1 & -B_2 - \varepsilon_2 & \ldots & -B_{n-1} - \varepsilon_{n-1} & -B_n - \varepsilon_n \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

Consider the vector $f := M[1; e]$ in the lattice. We have $f = [f_0; 1; e]$, Because $e$ solved the subset sum problem, we have an error term $|f_0| \leq n$ and thus $||f|| \leq (2n + 1)^{1/2}$.

The LLL algorithm will find us $x \in L$, $x \neq 0$ satisfying

$$||x|| \leq 2^{(n+1)/2}(2n + 1)^{1/2} \leq 3 \cdot 2^{n/2} n^{1/2} =: m$$

If $x = [x_0; x_0'; x_1; \ldots x_n] \in L$ then we have

$$x = x_0' b_0 + x_1 b_1 + \ldots + x_n b_n$$
where

\[ x_0 = \left( B_0 x'_0 - \sum_{i=1}^{n} B_i x_i - \sum_{i=1}^{n} \varepsilon_i x_i \right) \]

Let \( A = \{ x \in L, \| x \| \leq m, x \neq k[f_0; 1; e] \} \) for any \( k \in \mathbb{Z} \).
So if \( A \neq \emptyset \) there exists \( x = [x_0; x'_0; x_1; x_2; \ldots; x_n] \in \mathbb{Z}^{n+2} \) satisfying

\[ \| x \| < m, \quad (a'') \]
\[ x \neq k[f_0; 1; e] \text{ for any } k \in \mathbb{Z}, \quad (b'') \]
\[ \sum_{i=1}^{n} B_i x_i = x'_0 B_0 - x_0 - \sum_{i=1}^{n} \varepsilon_i x_i, \quad (c'') \]

Consider now a fixed \( x \) satisfying \((a'')\) and \((b'')\). We prove, as above, that

\[ \Pr( x \text{ satisfies } (c'')) \leq 1/B \]

To prove this, note that \((c'')\) is equivalent to \( \sum_{i=1}^{n} B_i z_i = -x_0 - E \) where \( z_i = x_i - x'_0 e_i \) and \( E = \sum_{i=1}^{n} \varepsilon_i x_i \). This is simply a non-trivial (due to \((b'')\)) inhomogeneous linear equation over the \( \{B_1, \ldots, B_n\} \).

Letting \( A_1 = \{ x \in \mathbb{Z}^{n+2} : \| x \| \leq m \} \) and summing over all \( A_1 \), and all possible error vectors we get

\[ \frac{3^n |A_1|}{B} \leq \frac{3^n (2m + 1)^{n+2}}{B} \leq \frac{2^n/2 O(n \log n)}{B} \leq O(2^{-cn^2/2}) \]

Again, our second term is larger than that of Frieze, but not materially so.

In this section on input errors we have also used the lattice where an extra second row was added to the lattice generating matrix as in the previous section. This second row could have been omitted as long we applied Frieze’s test-and-flip step. The correctness of this is left as an exercise.

### 6 Experiments

We implemented methods described above and experimented with random inputs. We investigated a number of different variants: The original Frieze method with test-to-flip, the original Frieze method with no test-to-flip and our method with the introduced second row. For all of these three methods, we tried with, and without, the introduction of the large constant. In total this gave us 6 methods to work with. We have found that when using the theoretically prescribed input magnitude size, \( B = 2^{n^2/2} \), all 6 methods work without any detected failures. Indeed, all 6 methods continued to work when using much smaller values for \( B \).

To push the methods, we kept dropping \( B \) until we came near a phase transition, where failures began to appear. We found that, at this point, the 6 different methods all failed randomly, but there was no discernible difference in their success rates.

We then experimented with the introduction of \( \{-1, 0, 1\} \) noise in the input. Here, we found that all three methods worked as expected as long as no large constant was used. When the large constant was introduced, all three methods failed consistently.
References

[1] R. Connelly, S. J. Gortler, and L. Theran. Reconstruction in one dimension from unlabeled euclidean lengths. *arXiv preprint arXiv:2007.06550*, 2020.

[2] A. M. Frieze. On the Lagarias-Odlyzko algorithm for the subset sum problem. *SIAM J. Comput.*, 15(2):536–539, 1986. doi: 10.1137/0215038.

[3] D. Gamarnik, E. C. Kızıldağ, and I. Zadik. Inference in high-dimensional linear regression via lattice basis reduction and integer relation detection. *arXiv preprint arXiv:1910.10890*, 2019.

[4] J. C. Lagarias and A. M. Odlyzko. Solving low-density subset sum problems. *J. Assoc. Comput. Mach.*, 32(1):229–246, 1985. doi: 10.1145/2455.2461.

[5] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982. doi: 10.1007/BF01457454.

[6] I. Zadik and D. Gamarnik. High dimensional linear regression using lattice basis reduction. In *Advances in Neural Information Processing Systems 31*, pages 1842–1852. 2018.