ON THE LAGARIA–ODLYZKO ALGORITHM FOR THE SUBSET SUM PROBLEM

A. M. FRIEZE†

Abstract. We give a simple analysis of an algorithm for solving subset-sum problems proposed Lagarias and Odlyzko [2].

Key words. complexity, lattice algorithm, random problems

Suppose \( \mathbf{e} = (e_1, e_2, \ldots, e_n) \in \{0, 1\}^n \), \( B_1, B_2, \ldots, B_n \) are positive integers and \( B = \sum_{i=1}^{n} B_i e_i \). Then clearly \( \mathbf{e} \) is a solution of

\[
\sum_{i=1}^{n} B_i x_i = B_0, \quad x_i = 0 \text{ or } 1, \quad i = 1, 2, \ldots, n.
\]

The following problem arises in cryptography [4]: given \( B_0, B_1, \ldots, B_n \), find \( \mathbf{e} \) solving (1).

Solving (1) is a well-known NP-complete problem and Lagarias and Odlyzko [2] describe an algorithm which almost surely\(^1\) finds \( \mathbf{e} \) assuming

\[
B_1, B_2, \ldots, B_n \text{ are independently chosen at random from } 1, \ldots, B = 2^m,
\]

c sufficiently large.

In this paper we show that \( c = 1 + \epsilon, \epsilon > 0 \) is sufficient. The main point of this paper is to give a simple proof of their result.

In the following analysis \( \mathbf{e} \) is fixed and \( B_1, B_2, \ldots, B_n \) are randomly generated. We note that we can assume

\[
B_0 \equiv \sum_{i=1}^{n} B_i / 2
\]

for if not, we can put \( y_i = 1 - x_i \) and try to solve

\[
\sum_{i=1}^{n} B_i y_i = \sum_{i=1}^{n} B_i - B_0, \quad y_i = 0 \text{ or } 1, \quad i = 1, 2, \ldots, n.
\]

Now let \( p = \lceil \frac{n2^{n/2}}{2} \rceil \), \( Z \) be the set of integers and

\[
\begin{align*}
&b_0 = (pB_0, 0, \ldots, 0) \in \mathbb{Z}^{n+1}, \\
&b_1 = (-pB_1, 1, 0, \ldots, 0), \\
&\vdots \\
&b_n = (-pB_n, 0, 0, \ldots, 1).
\end{align*}
\]

Let \( L = \{z = \sum_{i=0}^{n} \xi_i b_i : \xi_i \in \mathbb{Z}, i = 0, 1, \ldots, n\} \) be the lattice generated \( b_0, b_1, \ldots, b_n \).

Let \( \mathbf{e} = (0, e_1, e_2, \ldots, e_n) = b_0 + \sum_{i=1}^{n} e_i b_i \in L \). Note that \( \|\mathbf{e}\| \leq n^{1/2} \), using the euclidean norm. Thus \( \mathbf{e} \) is a "short" vector of \( L \).

\(^{-1}\) Received by the editors April 24, 1985, and in revised form February 15, 1985.

† Graduate School of Industrial Administration, Carnegie-Mellon University, Pittsburgh, Pennsylvania 15213. Current address, Department of Computer Science and Statistics, Queen Mary College, London 4NS, England.

1 By almost surely (a.s.) we mean with probability tending to 1.
Let \( \| x^* \| = \min \{ \| x \| : x \neq 0, x \in L \} \). It is not known at present whether it is possible to find a shortest nonzero vector in \( L \) in polynomial time. However, using the Basis Reduction Algorithm (BRA) of Lenstra, Lenstra and Lovász [3], we can in polynomial time find \( \hat{x} \in L \), \( \hat{x} \neq 0 \) satisfying
\[
\| \hat{x} \| \leq 2^{n/2} \| x^* \| \leq 2^{n/2} \| \hat{e} \| \leq m = 2^{n/2} n^{1/2}.
\]

Thus we can try to solve (1) by applying BRA to \( L \) and seeing if it produces \( \pm \hat{e} \). There is of course the possibility that there is more than one solution to (1); however the analysis below shows this to be unlikely.

So let \( \hat{x} \) be the shortest vector produced by BRA and assume that \( B_1, B_2, \ldots, B_n \) are distributed as in (2). We will show
\[
\Pr (\hat{x} \neq \pm \hat{e}) \leq (4m + 1)(2m + 1)^n / B = O(2^{-en^{1/2}}) \quad \text{if } B \geq 2^{(n+1)+(n+1)/2}.
\]

If \( x = (x_0, x_1, \ldots, x_n) \in L \), then we have
\[
x = x_0b_0 + x_1b_1 + \cdots + x_nb_n \quad \text{where } x_0 = p \left( B_0x_0 - \sum_{i=1}^{n} B_ix_i \right).
\]

Let \( L_0 = \{x \in L : x_0 = 0\} \). It follows that
\[
x \in L - L_0 \implies \| x \| \geq p.
\]
Thus (5) and (7) imply that \( \hat{x} \in L_0 \). The lattice used in [2] has \( p = 1 \). Taking \( p \) large allows us to restrict our attention to \( L_0 \). It also allows us to solve one lattice problem in place of the two solved in [2]. We can prove (6) by showing
\[
\Pr (A_0 \neq \emptyset) \leq (4m + 1)(2m + 1)^n / B
\]
where \( A_0 = \{ x \in L_0 : \| x \| \leq m, x \neq k\hat{e} \quad \text{for any } k \in Z \} \). (Note that \( \hat{x} = k\hat{e} \) for any \( k \in Z \) implies \( k = \pm 1 \) if \( \hat{x} \) is part of a basis.)

But if \( x \in A_0 \) then
\[
\| B_0x_0 \| = \left| \sum_{i=1}^{n} B_ix_i \right| \leq \sum_{i=1}^{n} B_i \| x \|
\]
and so \( \| x \| \leq 2\| x \| \leq 2m \), using (3). So if \( A_0 \neq \emptyset \) there exist \( x = (x_1, x_2, \ldots, x_n) \in Z^n \) and \( y \in Z \) satisfying
\begin{align*}
\| x \| &\leq m, \quad |y| \leq 2m, \\
x \neq k\hat{e} \quad \text{for any } k \in Z, \\
\sum_{i=1}^{n} B_ix_i &= yB_0.
\end{align*}

Consider now a fixed \( x, y \) satisfying (10a) and (10b) and let \( A_1 = \{ x \in Z^n : \| x \| = m \} \).
We will prove that
\[
\Pr (x, y \text{ satisfy (10c)}) \leq 1 / B
\]
and then
\[
\Pr (\exists x, y \text{ satisfying (10)}) \leq (4m + 1)|A_1| / B \leq (4m + 1)(2m + 1)^n / B
\]
and (8) follows.

To prove (11), note that (10c) is equivalent to \( \sum_{i=1}^{n} B_ix_i = 0 \) where \( z_i = x_i - ye_i \). Since (10b) holds, we can assume, without loss of generality, that \( z_i \neq 0 \). Letting \( \xi \)
denote \(-\sum_{i=1}^{n} Bz_i / z_1\),

\[ \Pr \left( \sum_{i=1}^{n} Bz_i = 0 \right) = \Pr (B_1 = \xi) = \sum_{j=1}^{n} \Pr (B_1 = j | \xi = j) \Pr (\xi = j) \]

\[ = \sum_{j=1}^{n} \frac{1}{B} \Pr (\xi = j) \quad \text{as } B_1 \text{ and } \xi \text{ are independent} \]

\[ \equiv \frac{1}{B}. \]

This completes the proof of the main result.

Schnorr [5] has recently built on the ideas in [3] and Kannan [1] to construct a family of basis reduction algorithms, so that for any \( \sigma > 1 \) there is an algorithm BRA, in the family which runs in polynomial time (the degree of the polynomial depends on \( \sigma \)) which guaranteed to find a vector of length no more than \( \sigma^{n-1} \|x^*\| \). Using BRA, in place of BRA means that we can take \( c = \sigma + \epsilon \) in (3) and still a.s. solve the problem.

Now Lagarias and Odlyzko also show that if \( B = 2^m \), where \( c > c_0 = 1.54725 \), then

\[ \epsilon \text{ a.s. the shortest vector of } L. \]

It is not difficult to see first that \( B = 2^m \) gives (12) for some \( c > 0 \) assuming we proceed exactly as above. Let \( m = n^{1/2} \) and \( x^* \) be the shortest vector of \( L \). If \( x^* \neq \pm \epsilon \) then (10) again holds. It is easy to show that \( |A_i| \leq 2^m \) for some \( c > 0 \) and this \( c \) will suffice.

To get \( c \) as small as \( c_0 \), we have to assume that \( \sum_{i=1}^{n} e_i \leq n/2 \). This is true for one of the problems (3) and (4) and so, as in [2], we solve both of these. We can now take \( m = (n/2)^{1/2} \) in our analysis.

We cannot assume (3) for the problem in which \( \sum_{i=1}^{n} e_i \leq n/2 \) but as \( B_0 \equiv \min \{B_i; i = 1, 2, \ldots, n \} \geq B/n^2 \) a.s. we can assume this instead. Using this in (9) gives \( |x_0| \leq n^2 m \) and so we take \( |y| \leq n^3 m \) in (10a). Theorem 3.2 of [2] is that \( |A_i| \leq 2^{n^2} \) and so (12) holds as

\[ \Pr ((12) \text{ fails}) \equiv \Pr ((10) \text{ holds}) + \Pr (B_0 < B/n^2). \]

(i) Problems with \( r > 1 \) constraints. Here one replaces \( c \) by \( c/r \) in the theorems. By multiplying the \( r \)th constraint by \( B^{-1} \) and then adding all these constraints together we have a subset sum problem in which the coefficients are very close to being randomly chosen uniformly from \( 1, \ldots, B' \).

(ii) \( B_0 \) an independent random variable. Suppose that instead of \( c \) being an a priori solution, \( B_0 \) is randomly generated in \( 1, \ldots, [\lambda n B] \) where \( 0 < \lambda \leq 1 \) is some constant. It is not difficult to show for \( B = 2^m, c > \frac{1}{2} \), that if (1) has a solution then it is a.s. unique and this approach a.s. finds it.

Acknowledgment. I am grateful to Ravi Kannan for interesting discussions on this topic.

REFERENCES
