SIAM J. COMPUT.
Vol. 15, No. 2, May 1986

ON THE LAGARIAS–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 $\mathbf{e}=(e_1, e_2, \cdots, e_n)\in\{0,1\}^n$, $B_1, B_2, \cdots, B_n$ are positive integers and $B_0 = \sum_{i=1}^n B_ie_i$. Then clearly $\mathbf{e}$ is a solution of

$$\sum_{i=1}^{n} B_ix_i = B_0, \qquad x_i = 0 \text{ or } 1, \quad i=1,2,\cdots,n. \tag{1}$$

The following problem arises in cryptography [4]: given $B_0, B_1, \cdots, B_n$, find $\mathbf{e}$ l 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

$$B_1, B_2, \cdots, B_n \text{ are independently chosen at random from } 1, \cdots, B=2^{cn^2}, \; c \text{ sufficiently large.} \tag{2}$$

In this paper we show that $c=\frac{1}{2}+\varepsilon$, $\varepsilon>0$ is sufficient. The main point of th paper is to give a simple proof of their result.

In the following analysis $\mathbf{e}$ is *fixed* and $B_1, B_2, \cdots, B_n$ are randomly generate We note that we can assume

$$B_0 \geqq \sum_{i=1}^{n} B_i/2 \tag{3}$$

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

$$\sum_{i=1}^{n} B_iy_i = \sum_{i=1}^{n} B_i - B_0, \qquad y_i=0 \text{ or } 1, \quad i=1,2,\cdots,n. \tag{4}$$

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

$$\begin{aligned}
\mathbf{b}_0 &= (pB_0, 0, \cdots, 0)\in Z^{n+1},\\
\mathbf{b}_1 &= (-pB_1, 1, 0, \cdots, 0),\\
&\;\;\vdots\\
\mathbf{b}_n &= (-pB_n, 0, 0, \cdots, 1).
\end{aligned}$$

Let $L=\{\mathbf{z}=\sum_{i=0}^n \xi_i\mathbf{b}_i \colon \xi_i\in Z, i=0,1,\cdots,n\}$ be the lattice generated $\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_n$.

Let $\hat{\mathbf{e}}=(0, e_1, e_2, \cdots, e_n)=\mathbf{b}_0+\sum_{i=1}^n e_i\mathbf{b}_i\in L$. Note that $\|\hat{\mathbf{e}}\|\leqq n^{1/2}$, using the euclidean norm. Thus $\hat{\mathbf{e}}$ is a "short" vector of L.

* Received by the editors April 24, 1985, and in revised form February 15, 1985.

† Graduate School of Industrial Administration, Carnegie-Mellon University, Pittsburgh, Pennsylva 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

$$\|\hat{x}\| \leqq 2^{n/2}\|x^*\| \leqq 2^{n/2}\|\hat{e}\| \leqq m = 2^{n/2}n^{1/2}. \tag{5}$$

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 $B_1, B_2, \cdots, B_n$ are distributed as in (2). We will show

$$\Pr(\hat{x} \neq \pm\hat{e}) \leqq (4m+1)(2m+1)^n/B = O(2^{-\varepsilon n^2/2}) \quad \text{if } B \geqq 2^{(1/2+\varepsilon)n^2} \tag{6}$$

If $x = (x_0, x_1, \cdots, x_n) \in L$, then we have

$$x = x_0'b_0 + x_1b_1 + \cdots + x_nb_n \quad \text{where } x_0 = p\left(B_0x_0' - \sum_{i=1}^n B_ix_i\right).$$

Let $L_0 = \{x \in L : x_0 = 0\}$. It follows that

$$x \in L - L_0 \text{ implies } \|x\| \geqq p. \tag{7}$$

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

$$\Pr(A_0 \neq \varnothing) \leqq (4m+1)(2m+1)^n/B \tag{8}$$

where $A_0 = \{x \in L_0 : \|x\| \leqq m, x \neq k\hat{e} \text{ for any } k \in Z\}$. (Note that $\hat{x} = k\hat{e}$ for $k \in Z$ implies $k = \pm 1$ if $\hat{x}$ is part of a basis.)

But if $x \in A_0$ then

$$|B_0x_0'| = \left|\sum_{i=1}^n B_ix_i\right| \leqq \sum_{i=1}^n B_i\|x\| \tag{9}$$

and so $|x_0'| \leqq 2\|x\| \leqq 2m$, using (3). So if $A_0 \neq \varnothing$ there exist $x = (x_1, x_2, \cdots, x_n) \in Z^n$ and $y \in Z$ satisfying

$$\|x\| \leqq m, \qquad |y| \leqq 2m, \tag{10a}$$

$$x \neq ke \quad \text{for any } k \in Z, \tag{10b}$$

$$\sum_{i=1}^n B_ix_i = yB_0. \tag{10c}$$

Consider now a *fixed* x, y satisfying (10a) and (10b) and let $A_1 = \{x \in Z^n : \|x\| \leqq m\}$. We will prove that

$$\Pr(x, y \text{ satisfy (10c)}) \leqq 1/B \tag{11}$$

and then

$$\Pr(\exists x, y \text{ satisfying (10)}) \leqq (4m+1)|A_1|/B \leqq (4m+1)(2m+1)^n/B$$

and (8) follows.

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

denote $-(\sum_{i=2}^n B_i z_i / z_1)$,

$$\Pr\left(\sum_{i=1}^n B_i z_i = 0\right) = \Pr(B_1 = \xi) = \sum_{j=1}^B \Pr(B_1 = j | \xi = j) \Pr(\xi = j)$$

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

$$\leqq \frac{1}{B}.$$

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_σ in the family which runs in polynomial time (the degree of the polynomial depends on σ) which guaranteed to find a vector of length no more than $\sigma^{n-1}\|\mathbf{x}^*\|$. Using BRA_σ in place of BRA means that we can take $c = \sigma + \varepsilon$ in (2) and still a.s. solve the problem.

Now Lagarias and Odlyzko also show that if $B = 2^{cn}$, where $c > c_0 = 1.54725$, then

(12) $\hat{\mathbf{e}}$ is a.s. the shortest vector of L.

It is not difficult to see first that $B = 2^{cn}$ gives (12) for some $c > 0$ assuming we proceed exactly as above. Let $m = n^{1/2}$ and $\mathbf{x}^*$ be the shortest vector of L. If $\mathbf{x}^* \neq \pm\hat{\mathbf{e}}$ then (10) again holds. It is easy to show that $|A_1| \leqq 2^{cn}$ for some $c > 0$ and this c will suffice.

To get c as small as c_0, we have to assume that $\sum_{i=1}^n e_i \leqq n/2$. This is true for one of the problems (1) 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 $\sum_{i=1}^n e_i \leqq n/2$ but as $B_0 \geqq \min\{B_i: i = 1, 2, \cdots, n\} \geqq B/n^2$ a.s. we can assume this instead. Using this in (9) gives $|x_0| \leqq n^2 m$ and so we take $|y| \leqq n^2 m$ in (10a). Theorem 3.2 of [2] is that $|A_1| \leqq 2^{c_0 n}$ and so (12) holds as

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

(i) *Problems with $r > 1$ constraints.* Here one replaces c by c/r in the theorems. By multiplying the ith constraint by B^{i-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 $1, \cdots, B^r$.

(ii) *B_0 an independent random variable.* Suppose that instead of $\mathbf{e}$ being an a priori solution, B_0 is randomly generated in $1, \cdots, \lceil \lambda n B \rceil$ where $0 < \lambda \leqq 1$ is some constant. It is not difficult to show for $B = 2^{cn^2}$, $c > \frac{1}{2}$, 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

[1] R. Kannan, *Improved algorithms for integer programming and related problems,* in Proc. 24th IEEE Symposium on Foundations of Computer Science, 1983.

[2] J. C. Lagarias and A. M. Odlyzko, *Solving low density subset sum problems,* Proc. 25th Annual IEEE Symposium on Foundations of Computer Science, 1983, pp. 1-10.

[3] A. K. LENSTRA, H. W. LENSTRA, JR. AND L. LOVÁSZ, *Factoring polynomials with rational coefficients*, Math. Ann., 26 (1982), pp. 515–534.

[4] R. C. MERKLE AND M. E. HELLMAN, *Hiding information and signatures in trap-door knapsacks*, IEEE Trans. Inform. Theory, IT-24 (1978), pp. 525–530.

[5] C. P. SHNORR, *A hierarchy of polynomial time basis reduction algorithms*, Proc. Symposium on the Theory of Algorithms, Pe'cs, Hungary, 1984, to appear.