Branching proofs of infeasibility in low density subset sum problems

Gábor Pataki [*] and Mustafa Tural [†]
Technical Report 2008-03
Department of Statistics and Operations Research, UNC Chapel Hill

Abstract

We prove that the subset sum problem

$$\begin{array}{rcl} ax & = & \beta \\ x & \in & \{0,1\}^n \end{array} \qquad (SUB)$$

has a polynomial time computable certificate of infeasibility for all a with density at most $1/(2n)$, and for almost all β integer right hand sides. The certificate is branching on a hyperplane, i.e. by a methodology dual to the one explored by Lagarias and Odlyzko [6]; Frieze [3]; Furst and Kannan [4]; and Coster et. al. in [1].

The proof has two ingredients. We first prove that a vector that is near parallel to a is a suitable branching direction, regardless of the density. Then we show that for a low density a such a near parallel vector can be computed using diophantine approximation, via a methodology introduced by Frank and Tardos in [2].

We also show that there is a small number of long intervals whose disjoint union covers the integer right hand sides, for which the infeasibility of (SUB) is proven by branching on the above hyperplane.

Key words Subset sum problems, proof of infeasibility, almost all instances

1 Introduction, and main results

The subset sum problem (SUB) is one of the original NP-complete problems introduced by Karp [5]. A particular reason for its importance is its applicability in cryptography. With a being a public key, and x the message, one can transmit $\beta = ax$ instead of x. An eavesdropper would need

[*] Department of Statistics and Operations Research, UNC Chapel Hill, **gabor@unc.edu**
[†] Department of Statistics and Operations Research, UNC Chapel Hill, **tural@email.unc.edu**

to find x from the intercepted β, and the public a, i.e. solve (SUB), while a legitimate receiver can use a suitable private key to decode the message. In cryptography applications, instances with low density are of interest, with the density of $a \in \mathbb{Z}^n$ defined as

$$d(a) = \frac{n}{\log_2 \| a \|_\infty}. \tag{1.1}$$

A line of research started in the seminal paper of Lagarias and Odlyzko [6], focused on solving such instances. In [6] the authors proved that the solution (SUB) can be found for all but at most a fraction of $1/2^n$ a vectors with $d(a) < c/n$, and assuming that the solution exists. Here c is a constant approximately equal to 4.8. Frieze in [3] gave a simplified algorithm to prove their result.

From now on we will say that a statement is true for almost all elements of a set S, if it is true for all, but at most a fraction of $1/2^n$ of them, with the value of n always clear from the context.

Furst and Kannan in [4] pursued an approach that looked at both feasible, and infeasible instances. In [4] they showed that for some $c > 0$ constant, if $M \geq 2^{cn \log n}$, then for almost all $a \in \{ 1, \dots, M \}^n$ and all β the problem (SUB) has a polynomial size proof of feasibility or infeasibility. Their second result shows that for some $d > 0$ constant, if $M \geq 2^{dn^2}$, then for almost all $a \in \{ 1, \dots, M \}^n$ and all β the problem (SUB) can be *solved* in polynomial time.

All the above proofs construct a candidate solution to (SUB) as a short vector in a certain lattice. Finding a vector whose length is off by a factor of at most $2^{(n-1)/2}$ from the shortest one is done utilizing the famed basis reduction method of Lenstra, Lenstra, and Lovász [7].

Assuming the availability of a *lattice oracle*, which finds the shortest vector in a lattice, Lagarias and Odlyzko in [6] show a similar result under weaker assumption $d(a) < 0.6463$. The current best result on finding the solution of almost all solvable subset sum problems using a lattice oracle is by Coster et al [1]: they require only $d(a) < 0.9408$. It is an open question to prove the infeasibility of almost all subset sum problems with density upper bounded by a constant, without assuming the availibility of an oracle. For more references, we refer to [1] and [8].

In this work we look at the structure of low density subset sum problems from a complementary, or dual viewpoint. With P a polyhedron and v an integral vector, it is clear that P has no integral point, if vx is nonintegral for all $x \in P$. We will examine such proofs of infeasibility of (SUB). Let

$$G(a, v) \quad = \quad \{ \beta \in \mathbb{Z} \,|\, vx \notin \mathbb{Z} \text{ for all } x \,\text{with}\, ax = \beta, \, 0 \leq x \leq e \}, \tag{1.2}$$

where e denotes a column vector of all ones. We will say that for the right hand sides β in $G(a, v)$ the infeasibility of (SUB) is proven by branching on vx. The reason for this terminology is that letting $P = \{ x \,|\, ax = \beta, \, 0 \leq x \leq e \}$, β is in $G(a, v)$ iff the maximum and the minimum of vx over P is between two consecutive integers.

We shall write $\mathbb{Z}^n_+$, and $\mathbb{Z}^n_{++}$, for the set of nonnegative, and positive integral n-vectors, respectively. We will throughout assume $n \geq 10$, and that the components of a are relatively prime. We only consider nontrivial right hand sides of (SUB), i.e. right hand sides from $\{ 0, 1, \dots, \| a \|_1 \}$.

Our first main result is:

Theorem 1. *Suppose $d(a) \leq 1/(2n)$. Then we can compute in polynomial time an integral vector v, such that for almost all right hand sides the infeasibility of (SUB) is proven by branching on vx.*

Also, $G(a, v)$ can be covered by the disjoint union of at most 2^{2n^2} intervals, each of length at least 2^n.

□

Note that Theorem 1 further narrows the range of hard instances from the work of Furst and Kannan in [4].

There are at most 2^n right hand sides for which (SUB) is feasible, so most right hand sides lead to an infeasible instance, when $d(a)$ is small. However, in principle, it may be difficult to *prove* the infeasibility of many infeasible instances. Fortunately, this is not the case, as shown by the following corollary.

Corollary 1. *Let a and v be as in Theorem 1. Then for almost all right hand sides for which (SUB) is infeasible, its infeasibility is proven by branching on vx.*

□

There is an interesting duality and parallel between the results on low density subset sum in [6, 4, 1] and Theorem 1. The proofs in [6, 4, 1] work by constructing a candidate solution, while ours by branching, i.e. by a dual method. At the same time, they all rely on basis reduction. In our proof we find v by a method of Frank and Tardos in [2], which uses the simultaneous diophantine approximation method of Lenstra, Lenstra, and Lovász [7], which in turn, also uses basis reduction.

Theorem 1 will follow from combining Theorems 2 and 3 below. Theorem 2 proves that a "large" fraction of righ hand sides in (SUB) have their infeasibility proven by branching on vx, if v is relatively short, and near parallel to a. Theorem 3 will show that such a v can be found using diophantine approximation, when $d(a) \leq 1/(2n)$.

Theorem 2. *Let $v \in \mathbb{Z}^n_+$, $\lambda \in \mathbb{R}$, $r \in \mathbb{R}^n$ with $\lambda \geq 1$, $\| r \|_1 / \lambda < 1$, and*

$$a = \lambda v + r.$$

Then the infeasibility of all, but at most a fraction of

$$\frac{2(\| r \|_1 + 1)}{\lambda} \tag{1.3}$$

right hand sides is proven by branching on vx.

In addition, $G(a, v)$ can be covered by the disjoint union of at most $\| v \|_1$ intervals, each of length at least $\lambda - \| r \|_1$.

□

Theorem 3. *Suppose $d(a) \leq 1/(2n)$. Then we can compute in polynomial time $v \in \mathbb{Z}_+^n$, $\lambda \in \mathbb{Q}$, $r \in \mathbb{Q}^n$ with $a = \lambda v + r$, and*

(1) $\| v \|_1 \leq 2^{2n^2}$*;*

(2) $\| r \|_1 / \lambda \leq 1/2^{n+2}$*;*

(3) $\lambda \geq 2^{n+2}$.

□

Remark 2. In this discussion we clarify what we mean by the v vector of Theorem 3 being near parallel to a.

Given $v, \lambda,$ and r in Theorem 3, assume

$$\lambda v = \operatorname{Proj}\{ a \mid \operatorname{lin}\{v\}\},\ r = a - \lambda v. \tag{1.4}$$

Then

$$\sin(a, v) = \frac{\| r \|}{\| a \|} \leq \frac{\| r \|}{\| \lambda v \|} \leq \frac{\| r \|}{\| \lambda \|}. \tag{1.5}$$

So a small upper bound on $\| r \| / \lambda$ will force $\sin(a, v)$ to be small as well, i.e. v to be near parallel to a. Some of the inequalities in (1.5) can be strict. For instance, letting $a = (m^2, m^2 + 1)$, $v = (m, m+1)$, and defining λ and r as in (1.4), it is easy to check that $r/\lambda \to (1/2, -1/2)$, as $m \to \infty$, but obviously $\sin(a, v) \to 0$.

2 Proofs

Proof of Theorem 2 Let us fix a and v. Since a and v are nonnegative, and e is a column vector of all ones, it holds that

$$\| a \|_1 = ae, \text{ and } \| v \|_1 = ve,$$

and we will use the latter notation for brevity.

For a row-vector w, and an integer ℓ we write

$$\begin{aligned} \max(w, \ell) &= \max\{ wx \mid vx \leq \ell,\ 0 \leq x \leq e \}, \\ \min(w, \ell) &= \min\{ wx \mid vx \geq \ell,\ 0 \leq x \leq e \}. \end{aligned} \tag{2.6}$$

The dependence on v, and on the sense of the constraint (i.e. $\leq$, or $\geq$) is not shown by this notation; however, we always use $vx \leq \ell$ with "max", and $vx \geq \ell$ with "min", and v is fixed.

Claim 1. *We have*

$$\begin{aligned} \min(a,k) &\leq \max(a,k) \text{ for } k \in \{0,\dots,ve\}, & (2.7)\\ \max(a,k) - \min(a,k) &\leq \|r\|_1 \text{ for } k \in \{0,\dots,ve\}, \text{ and} & (2.8)\\ \min(a,k+1) - \max(a,k) &\geq -\|r\|_1 + \lambda > 0 \text{ for } k \in \{0,\dots,ve-1\}. & (2.9) \end{aligned}$$

Proof The feasible sets of the optimization problems defining $\min(a,k)$, and $\max(a,k)$ contain $\{ x \mid vx = k,\ 0 \leq x \leq e \}$, so (2.7) follows.

The decomposition of a shows that for all ℓ_1 and ℓ_2 integers for which the expressions below are defined,

$$\begin{aligned} \max(a,\ell_1) &\leq \max(r,\ell_1) + \lambda\ell_1, \text{ and}\\ \min(a,\ell_2) &\geq \min(r,\ell_2) + \lambda\ell_2, \end{aligned} \tag{2.10}$$

hold. Therefore

$$\begin{aligned} \min(a,\ell_2) - \max(a,\ell_1) &\geq \min(r,\ell_2) - \max(r,\ell_1) + \lambda(\ell_2 - \ell_1)\\ &\geq -\|r\|_1 + \lambda(\ell_2 - \ell_1). \end{aligned} \tag{2.11}$$

follows, and (2.11) with $\ell_2 = \ell_1 = k$ implies (2.8), and with $\ell_2 = k+1,\ \ell_1 = k$ yields (2.9).

Hence

$$\min(a,0) \leq \max(a,0) < \min(a,1) \leq \max(a,1) < \min(a,2) \leq \dots < \min(a,ve) \leq \max(a,ve). \tag{2.12}$$

We will call the intervals

$$[\min(a,0),\max(a,0)],\dots,[\min(a,ve),\max(a,ve)]$$

bad, and the intervals

$$G_0 := (\max(a,0),\min(a,1)),\dots,G_{ve-1} := (\max(a,ve-1),\min(a,ve))$$

good.

The nonnegativity of v and of a imply $\min(a,0) = 0$, and $\max(a,ve) = ae$, so the bad, and good intervals partition $[0,ae]$: the pattern is bad, good, ..., good, bad. Some of the bad intervals may have zero length, but by (2.9) none of the good ones do.

Next we show that the good intervals contain exactly the right hand sides for which the infeasibility of (SUB) is proven by branching on vx.

Claim 2.

$$G(a,v) = \cup_{i=0}^{ve-1} G_i \cap \mathbb{Z}. \tag{2.13}$$

Proof By definition $\beta \in G(a, v)$ iff for some ℓ integer with $0 \leq \ell < ve - 1$, and for all x with $0 \leq x \leq e$, $ax = \beta$

$$\ell < vx < \ell + 1 \tag{2.14}$$

holds. We show that for this ℓ

$$\begin{aligned} \max(a, \ell) &< \beta \text{ and} && (2.15) \\ \min(a, \ell + 1) &> \beta. && (2.16) \end{aligned}$$

First, assume to the contrary that (2.15) is false, i.e. there exists x_1 with

$$ax_1 \geq \beta,\ vx_1 \leq \ell,\ 0 \leq x_1 \leq e. \tag{2.17}$$

Since $\ell \geq 0$, denoting by x_2 the all-zero vector, it holds that

$$ax_2 \leq \beta,\ vx_2 \leq \ell,\ 0 \leq x_2 \leq e. \tag{2.18}$$

Looking at (2.17) and (2.18) it is clear that a convex combination of x_1 and x_2, say $\bar{x}$ satisfies

$$a\bar{x} = \beta,\ v\bar{x} \leq \ell,\ 0 \leq \bar{x} \leq e, \tag{2.19}$$

which contradicts (2.15). Showing (2.16) is analogous.

End of proof of Claim 2

To summarize, Claim 2 implies that $G(a, v)$ is covered by the disjoint union of ve intervals. By (2.9) their length is lower bounded by $\lambda - \| r \|_1$.

Let us denote by b the number of integers in bad intervals, and by g the number of integers in good intervals, i.e. $g = |G(a, v)|$. Using (2.8) and (2.9), and the fact that there are ve good intervals, and $ve + 1$ bad ones, we get

$$\begin{aligned} g &\geq ve(\lambda - \| r \|_1 - 1), \\ b &\leq (ve + 1)(\| r \|_1 + 1), \end{aligned} \tag{2.20}$$

so

$$\begin{aligned} \frac{g}{b} &\geq \frac{ve}{ve+1} \frac{\lambda - (\| r \|_1 + 1)}{\| r \|_1 + 1} && (2.21) \\ &\geq \frac{1}{2} \frac{\lambda - (\| r \|_1 + 1)}{\| r \|_1 + 1} && (2.22) \\ &\geq \frac{\lambda}{2(\| r \|_1 + 1)} - 1, && (2.23) \end{aligned}$$

and from here

$$\begin{aligned} \frac{b}{g + b} &\leq \frac{1}{1 + g/b} && (2.24) \\ &\leq \frac{2(\| r \|_1 + 1)}{\lambda}. && (2.25) \end{aligned}$$

follows. □

Proof of Theorem 3

We will use a methodology due to Frank and Tardos introduced in [2]. Here the authors employ simultaneous diophantine approximation to decompose a vector with large norm into the weighted sum of smaller norm vectors. We will only need one vector that approximates a, and the parameters will be somewhat differently chosen in the diophantine approximation.

We will rely on the following result of Lenstra, Lenstra, and Lovász from [7]:

Theorem 4. *Given a positive integer N, and $\alpha \in \mathbb{Q}^n$, we can compute in polynomial time $v \in \mathbb{Z}^n$, $q \in \mathbb{Z}_{++}$ such that*

$$\begin{aligned} \| q\alpha - v \|_\infty &\leq \frac{1}{N} \text{ and} && (2.26) \\ q &\leq 2^{n(n+1)/4} N^n. && (2.27) \end{aligned}$$

□

We will use Theorem 4 with

$$\alpha = \frac{a}{\| a \|_\infty},$$

then set

$$\lambda = \frac{\| a \|_\infty}{q}, \; r = a - \lambda v.$$

We have the following estimates with ensuing explanation:

$$\begin{aligned} \| v \|_1 &\leq n \| v \|_\infty \leq nq \leq n 2^{n(n+1)/4} N^n, && (2.28) \\ \frac{\| r \|_1}{\lambda} &\leq \frac{n \| r \|_\infty}{\lambda} \leq \frac{n}{N}, && (2.29) \\ \lambda &\geq \frac{\| a \|_\infty}{2^{n(n+1)/4} N^n} \geq \frac{2^{2n^2 - n(n+1)/4}}{N^n}. && (2.30) \end{aligned}$$

Here (2.28) follows from using (2.26), since $\| q\alpha \|_\infty = q$, and v is integral. The second inequality in (2.29) is actually equivalent to (2.26); and (2.30) comes from the definition of λ, and (2.27). Hence (1), (2), and (3) in Theorem 3 are satisfied when

$$\begin{aligned} n 2^{n(n+1)/4} N^n &\leq 2^{2n^2}, && (2.31) \\ \frac{n}{N} &\leq \frac{1}{2^{n+2}}, && (2.32) \\ \frac{2^{2n^2 - n(n+1)/4}}{N^n} &\geq 2^{n+2}. && (2.33) \end{aligned}$$

But (2.31) through (2.33) are equivalent to

$$n 2^{n+2} \leq N \leq 2^{2n - (n+1)/4 - 1 - 2/n}, \qquad (2.34)$$

and such an integer N exists, when $n \geq 10$. □

Proof of Corollary 1 Let $I(a)$ be the set of right hand sides for which (SUB) is infeasible. Theorem 1 states

$$\frac{|G(a,v)|}{\|\, a \,\|_1 + 1} \geq 1 - \frac{1}{2^n}. \tag{2.35}$$

Since $I(a) \subseteq \{\, 0, \ldots, \|\, a \,\|_1 \,\}$, Theorem 1 implies

$$\frac{|G(a,v)|}{I(a)} \geq 1 - \frac{1}{2^n}; \tag{2.36}$$

and since $G(a,v) \subseteq I(a)$, (2.36) means the desired conclusion. □

Remark 3. One can use a different methodology to find a near parallel vector to a, which we quote from [9]:

Theorem 5. *Suppose $d(a) \leq 1/(n/2+1)$. Let U be a unimodular matrix such that the columns of*

$$\begin{pmatrix} a \\ I \end{pmatrix} U$$

are reduced in the sense of Lenstra, Lenstra, and Lovász, and v the last row of U^{-1}. Define r and λ to satisfy (1.4), and let $f(a) \;=\; 2^{n/4} / \,\|\, a \,\|^{1/n}$.

Then

(1) $\|\, v \,\| \; (1 + \|\, r \,\|^2)^{1/2} \leq \|\, a \,\| \; f(a)$;

(2) $\lambda \geq 1/f(a)$;

(3) $\|\, r \,\| \,/\lambda \leq 2f(a)$.

□

These bounds also suffice to prove the first part of Theorem 1; however, the bound we get on $\|\, v \,\|$ involves $\|\, a \,\|$ as well, not just the dimension.

Acknowledgement Thanks are due to Ravi Kannan, and Laci Lovász for helpful discussions; to Fritz Eisenbrand for discussions on the connection with diophantine approximation; and to Jeff Lagarias and Andrew Odlyzko for pointing out reference [1].

References

[1] M. J. Coster, A. Joux, B. A. LaMacchia, A. M. Odlyzko, C. P. Schnorr, and J. Stern. Improved low-density subset sum algorithms. *Computational Complexity*, 2:111–128, 1992.

[2] András Frank and Éva Tardos. An application of simultaneous diophantine approximation in combinatorial optimization. *Combinatorica*, 7(1):49–65, 1987.

[3] Alan Frieze. On the Lagarias-Odlyzko algorithm for the subset sum problem. *SIAM Journal on Computing*, 15:536–540, 1986.

[4] Merrick Furst and Ravi Kannan. Succinct certificates for almost all subset sum problems. *SIAM Journal on Computing*, 18:550 – 558, 1989.

[5] Richard Karp. Reducibility among combinatorial problems. In J.W. Thatcher R.E. Miller, editor, *Complexity of Computer Computations*. Plenum Press, 1972.

[6] Jeffrey C. Lagarias and Andrew M. Odlyzko. Solving low-density subset sum problems. *Journal of ACM*, 32:229–246, 1985.

[7] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[8] D. Micciancio. *Complexity of lattice problems: a cryptographic perspective.* Kluwer Academic Publishers, 2002.

[9] Gábor Pataki and Mustafa Tural. Parallel approximation and integer programming reformulation. *Technical Report 2007-07, Dept of Statistics and Operations Research, UNC Chapel Hill, submitted.*