ELSEVIER

Theoretical Computer Science 255 (2001) 641–648

Theoretical Computer Science

www.elsevier.com/locate/tcs

Note

On the unique shortest lattice vector problem ☆

S. Ravi Kumar, D. Sivakumar *

IBM Almaden Research Center, Department K-53/B-1, 650 Harry Road, San Jose, CA 95120-6099, USA

Received 15 August 1998; revised 10 August 2000; accepted 31 August 2000
Communicated by O. Watanabe

Abstract

We show that the problem of deciding whether a given rational lattice L has a vector of length less than some given value r is NP-hard, even under the promise that L has exactly zero or one vector of length less than r. © 2001 Published by Elsevier Science B.V.

Keywords: Integer lattices; Shortest vector problem; Unique solutions

1. Introduction

Is it easier to decide instances of NP-hard problems when they are given with the additional promise that the associated search problem has exactly *zero* or *one* solution? Over a decade ago, Valiant and Vazirani [10] proved a beautiful result that shows that this is not the case. More formally, they gave a probabilistic many–one reduction from the NP-complete Boolean formula satisfiability problem to the problem of deciding whether a Boolean formula is satisfiable under the *promise* that it has either zero or one satisfying assignment. Virtually all known NP-complete decision problems are known to be NP-complete under polynomial-time many–one reductions that preserve the number of solutions (often called *parsimonious* reductions, see [7, pp. 441–442]). Therefore, it follows that the zero-or-one promise version of most NP-complete decision problems are also NP-hard.

In a recent breakthrough, Ajtai [1] showed that the problem of finding shortest vectors in rational lattices is NP-hard under randomized reductions (see also [4, 6]). Recall

☆ Most of this work was done while the second author was at the University of Houston.

* Corresponding author.
E-mail addresses: ravi@almaden.ibm.com (S.R. Kumar), siva@almaden.ibm.com (D. Sivakumar).

0304-3975/01/$ - see front matter © 2001 Published by Elsevier Science B.V.
PII: S0304-3975(00)00387-X

that, for n linearly independent vectors $b_1, b_2, \ldots, b_n \in \boldsymbol{R}^n$, $L(b_1, b_2, \ldots, b_n)$ denotes the (discrete) set of all vectors expressible as integral linear combinations of the b_i's, that is, $L(b_1, \ldots, b_n) = \{\sum_{i=1}^{n} c_i b_i \mid c_i \in \boldsymbol{Z}\}$. Let $\|v\|_2$ denote the Euclidean norm of v. Ajtai showed that the following decision problem associated with shortest lattice vectors is NP-complete under randomized many–one reductions.

Short lattice vector problem (SVP):

Input: A lattice $L = L(b_1, b_2, \ldots, b_n) \subseteq \boldsymbol{R}^n$ specified by linearly independent vectors $b_1, b_2, \ldots, b_n \in \boldsymbol{Q}^n$, and a rational number $r > 0$.

Question: Is there a non-zero vector $v \in L$ such that $\|v\|_2 < r$?

However, a remarkable feature of Ajtai's reduction from the NP-complete subset sum problem to the (decision version of) the shortest lattice vector problem is that it is not parsimonious. Specifically, it maps instances of the subset sum problem to instances (L, r) of the short lattice vector problem where every solution of the subset sum problem is mapped to one or more vectors of length $< r$ in the lattice L.

Thus, it appears that we have an NP-complete problem whose structural properties are very different from standard NP-complete problems. Specifically, the lack of an NP-hardness proof via parsimonious reductions leaves the question of whether the following zero-or-one version of the short lattice vector problem is also NP-hard.

Unique short lattice vector problem (USVP):

Input: A lattice $L = L(b_1, b_2, \ldots, b_n) \subseteq \boldsymbol{R}^n$ specified by linearly independent vectors $b_1, b_2, \ldots, b_n \in \boldsymbol{Q}^n$, and a rational number $r > 0$.

Promise: The number of vectors $v \in L$ such that $\|v\|_2 < r$ is either zero or one. [1]

Question: Is there a non-zero vector $v \in L$ such that $\|v\|_2 < r$?

In particular, the non-parsimoniousness of the reduction used in the NP-completeness of the short lattice vector problem rules out the following straightforward reduction from SAT to USVP: given an instance φ of SAT, apply the reduction of [10] and produce an instance ψ of SAT that has either zero or one satisfying assignment, then map it to an instance (L, r) of the shortest lattice vector problem by applying Ajtai's reduction. The difficulty is that (L, r) may have more than one vector of length $< r$ even though ψ has only one satisfying assignment.

In this note, we show that, notwithstanding the fact that Ajtai's reduction is not parsimonious (and the possibility that a parsimonious reduction may not exist at all), the promise problem USVP is still NP-hard under randomized reductions. Our proof is essentially an encoding of the reduction of Valiant and Vazirani into instances of SVP. Given an instance (L, r) of SVP that is produced by Ajtai's reduction, we show

[1] *Remarks*: (1) This uniqueness, of course, is modulo a factor of ± 1, for if $\|v\|_2 < r$ for some non-zero $v \in L$, then also $\| - v\|_2 < r$ and $-v$ is a non-zero point of L. (2) This notion of uniqueness bears a resemblance to the notion of "β-unique shortest vector problem" that has significance to lattice-based cryptography [2, 3]. In the latter problem, the promise is that every non-zero vector of length at most β times the length of the shortest vector in L must be parallel to the shortest vector. The connection appears to be only superficial, however; in particular, we see no application of our reduction to the problem of establishing hardness of finding approximately short vectors in lattices.

how to produce an instance (L', r) of SVP, where $L' \subseteq L$ is a "random" sublattice of L that has the following two properties:

(1) if there is no vector in L of length $< r$, then there is no vector in L' of length $< r$ (since L' will be a sublattice of L);
(2) if L has one or more vectors of length $< r$, then with probability $n^{-O(1)}$, L' has exactly one vector of length $< r$.

In Section 2, we briefly explain the reason why Ajtai's reduction from subset sum to SVP may not be parsimonious. In Section 3, we sketch our main result. We conclude this Introduction with the following open questions that are suggested by the non-parsimoniousness of Ajtai's reduction.

(1) Is there a parsimonious reduction from some well-known NP-complete problem to the short lattice vector problem?
(2) Is the problem of counting the number of points in a lattice L within a certain length bound, under the promise that $\lambda_1(L) \geqslant 1$, complete for ♯P?

2. The non-parsimoniousness of Ajtai's reduction

In his proof of the NP-hardness of SVP, Ajtai gives a reduction from the NP-complete subset sum problem to the decision problem SVP. Given an instance $\langle a_1, a_2, \ldots, a_\ell; A\rangle$ of the subset problem (where the question is whether there is a subset of the set $\{a_1, a_2, \ldots, a_\ell\}$ that sums up to A), first a value $m = \ell^{\Theta(1)}$ is chosen appropriately, and a lattice $L^{(m)} \subseteq \boldsymbol{R}^m$ is constructed. The idea is to search for the solution to the subset sum problem (viewed as a 0–1 vector) from the set of the coefficient sequences of short vectors in $L^{(m)}$. A technical masterpiece that is crucial to achieving this is the family of lattices $L^{(m)}$ (for an appropriate sequence of integers m) that has the following properties:

(1) there is a polynomial-time computable set of basis vectors $b_1, \ldots, b_m$ for $L^{(m)}$;
(2) every non-zero vector of $L^{(m)}$ has length at least 1;
(3) for some absolute constants $\varepsilon > 0$ and $\delta > 0$ there are at least 2^{m^ε} vectors in $L^{(m)}$ of length at most $1 + 2^{-m^\delta}$, and for every such vector all but the last two coefficients w.r.t. the basis $b_1, \ldots, b_m$ are either zero or one.

By property (3) of L_m, there are at least $2^{m^\varepsilon} = 2^{\ell^{O(1)}}$ vectors of length at most $1+2^{-m^\delta}$ and every such vector has $m-2$ coefficients that are zero or one. Let X denote the set of coefficient sequences of these short vectors. A combinatorial lemma of Sauer [8] guarantees that if m^ε is sufficiently large with respect to ℓ, then there is some subset of ℓ coefficient positions such that the projection of the set X of sequences on these positions contains every one of the 2^ℓ 0–1 patterns of length ℓ. The idea will be to search for the solution to the subset sum problem from among these sequences.

Since Sauer's lemma is not constructive, Ajtai presents another technical masterpiece, a probabilistic construction whose effect is similar to the conclusion of Sauer's lemma. Specifically, Ajtai shows that if m^ε is sufficiently large with respect to ℓ, then with good probability, a random collection of ℓ disjoint sets $P_1, P_2, \ldots, P_\ell \subseteq \{1, \ldots, m-2\}$

of coefficient positions has the following property: for every $z \in \{0,1\}^{\ell}$, there exists an $x \in X$ such that for each i, $1 \leqslant i \leqslant \ell$, the number of 1's in the restriction of x to P_i is precisely z_i. We say that x is a representative of z. Ajtai then proceeds to embed the lattice $L^{(m)}$ linearly as a lattice L in a higher dimensional space with a new Euclidean norm on this space (that suitably encodes the subset sum instance) that ensures the following conditions:

(1) every non-zero vector of L has length at least one;
(2) the subset sum problem embedded has a solution iff L has a vector of norm $< \sqrt{1+\zeta}$ for some ζ, $0 < \zeta < 1$;
(3) the number of vectors of norm $< \sqrt{1+\zeta}$ that correspond to any particular solution $z \in \{0,1\}^{\ell}$ to the subset sum problem is *precisely* the number of representatives that z has, in the application of Ajtai's lemma.

It is property (3) that violates parsimoniousness. If the solution z to the subset sum problem being reduced to SVP has more than one representative, then the reduction produces an instance (L,r) of SVP that has at least two vectors u, v, $u \neq \pm v$, of length $< r$.

It is not clear if Ajtai's proof could be modified to ensure that each z has a *unique* representative in X. Of course, if one could come up with a magical lattice construction that, for every integer ℓ, gives a lattice $L^{(\ell)} \subseteq \boldsymbol{R}^{\ell}$ s.t. every one of the 2^{ℓ} 0–1 combinations of the basis vectors is a lattice point of shortest length, then a parsimonious reduction would become possible. However, the construction of such lattices would be a tremendous breakthrough (see the book of Conway and Sloane [5] for much related work that has fallen well short of achieving anything close to this). In fact, the best known lattice construction in this spirit is a construction from the 1950s, called the Barnes–Wall lattice, that has $2^{(\log \ell)^2}$ points of shortest length.

3. USVP is NP-hard

In this section, we present our reduction from any NP decision problem to the promise problem USVP. By combining Ajtai's result [1] with a series of reductions between NP-complete problems, we know that there is a polynomial-time computable randomized many–one reduction h from the NP-complete problem SAT to SVP. Given a Boolean formula φ, $h(\varphi)$ is an instance (L,r) of SVP that has the following properties:

(1) L is a lattice in m dimensions such that every non-zero vector of L has length at least 1.
(2) L has a vector whose length is less than $r = \sqrt{1+\zeta}$, where $0 < \zeta < 1$ is some fixed small number, if and only if φ is satisfiable.

Our randomized procedure takes the instance (L,r) and first produces a sequence of lattices $L = L_0, L_1, L_2, \ldots, L_{2m}$. Then it randomly and uniformly chooses one of the $2m+1$ lattices, say L_k, and outputs the instance (L_k, r) of SVP. We will then argue that the following two conditions hold:

(1) If L has no point of length $<r$, then L_k has no point of length $<r$.
(2) If L has one or more points of length $<r$, then with probability at least $2/(3(2m+1)) - o(1) = \Omega(m^{-1})$, L_k has exactly one point of length $<r$.

Our procedure is very similar in spirit to the reduction of Valiant and Vazirani from SAT to the promise problem Unique SAT. The key part is to show that the reduction can be naturally encoded into instances of SVP, and to handle some technical complications that arise out of probabilistic dependencies.

Suppose that we have produced lattices $L = L_0, \ldots, L_k$ for some $0 \leqslant k < 2m$. We will now show how to produce L_{k+1}. Let $b_1, \ldots, b_m$ be a basis for L_k. Pick a subset $W \subseteq [m] = \{1, 2, \ldots, m\}$ uniformly at random from all subsets of $[m]$.[2] If $W = \emptyset$, let $L_{k+1} = L_k$. Otherwise, pick an element $i \in W$ arbitrarily. For $j \notin W$, let $b'_j = b_j$, and for every $j \in W \setminus \{i\}$, let $b'_j = b_j - b_i$. Finally, let $b'_i = 2b_i$. Now L_{k+1} is defined to be the lattice spanned by the vectors $b'_1, b'_2, \ldots, b'_m$.

This completes the description of our procedure. It is clear that this can be accomplished in time polynomial in the dimension of the lattice L and the bit-length of the representation of L and r. We now proceed to prove the correctness of the procedure; our proof is an adaptation of the proof of Valiant and Vazirani, together with a simple but crucial lemma. The lemma essentially sets the stage for the application of the lemma of Valiant and Vazirani; however, we are unable to apply to the result from [10] as a black-box because of some probabilistic dependencies. Therefore, we give a simple adaptation of a proof of this lemma from Sipser's lecture notes on complexity theory [9].

We first define a technical notion that is helpful in describing our proof. Let U be a lattice in some d dimensions, given by a set of basis vectors $u_1, u_2, \ldots, u_d$. For a lattice point $v \in U$ given by $v = \sum_i c_i u_i$, $c_i \in \boldsymbol{Z}$ for $i = 1, \ldots, d$, we define the parity vector of v with respect to the basis $u_1, \ldots, u_d$ to be the vector $p(v) \in \boldsymbol{Z}_2^d$ whose ith coordinate is $c_i \bmod 2$. Also, as a matter of convention, we often write "point in lattice" to mean a *non-zero* vector in a lattice; since the zero vector doesn't play any role in the results of this paper, we omit the explicit qualification "non-zero". Also, even where it is not stated explicitly, all references to uniqueness of a lattice point is up to multiplication by ± 1.

We begin with a simple geometric lemma.

Lemma 1. *If $u, v \in \boldsymbol{R}^d$ satisfy $\|u\|_2 < \alpha$ and $\|v\|_2 < \alpha$, then either $\|u + v\|_2 < \sqrt{2}\alpha$ or $\|u - v\|_2 < \sqrt{2}\alpha$.*

Proof. $\|u + v\|_2^2 + \|u - v\|_2^2 = \|u\|_2^2 + \|v\|_2^2 + 2\langle u, v\rangle + \|u\|_2^2 + \|v\|_2^2 - 2\langle u, v\rangle = 2(\|u\|_2^2 + \|v\|_2^2) < 4\alpha^2$. Thus, either $\|u + v\|_2^2 < 2\alpha^2$ or $\|u - v\|_2^2 < 2\alpha^2$, and the lemma follows. (Geometrically, the lemma is very clear: if the angle between u and v is $< \pi/2$, then

[2] Technically, we should write something like $b_1^{(k)}, \ldots, b_m^{(k)}$ and $W^{(k)}$ to make the association of the b_i's and W with k clearer; however, we will suppress the superscripting by k for ease of reading. The dependence should be clear from context.

$\|u-v\|_2<\sqrt{2}\alpha$, and if the angle between u and v is $>\pi/2$, then $\|u+v\|_2<\sqrt{2}\alpha$; if the angle $=\pi/2$, $u+v$ and $u-v$ have the same length $<\sqrt{2}\alpha$.) □

Lemma 2. *Let U be a lattice in $\boldsymbol{R}^d$ and let $\lambda_1(U)$ denote the length of the shortest vector of U. If u and v are two points of U such that $u\neq v$, $u\neq -v$, $\|u\|_2<\sqrt{2}\lambda_1(U)$ and $\|v\|_2<\sqrt{2}\lambda_1(U)$. Then for every basis $u_1,\ldots,u_d$ of U, the parity vectors of u and v with respect to the basis $u_1,\ldots,u_d$ are different.*

Proof. Suppose not, and let u and v be lattice points that violate the lemma. Let $u_1,u_2,\ldots,u_d$ be a basis for U, and let $u=\sum_i c_i u_i$ and $v=\sum_i d_i u_i$. Since the parity vectors of u and v w.r.t. the fixed basis are identical, (c_i+d_i) and (c_i-d_i) are both even for every i, $1\leqslant i\leqslant d$. Thus, $(u+v)/2$ and $(u-v)/2$ are both vectors in the lattice U. Furthermore, since $u\neq\pm v$, both of these points are non-zero. Now, by Lemma 1, one of these points has norm $<\frac{1}{2}(\sqrt{2}\sqrt{2}\lambda_1(U))=\lambda_1(U)$, which is a contradiction. □

Corollary 3. *In any lattice $U\subseteq\boldsymbol{R}^d$, the number of points of length $<\sqrt{2}\lambda_1(U)$ is at most 2^d.*

Armed with Lemma 2 and Corollary 3, we are now ready for the analysis of the correctness of our procedure. To do this, we focus on the following question: when we go from a lattice L_k in our sequence to L_{k+1}, exactly which points of L_k of norm $<r$ survive, and how many of these are there?

We begin our analysis by recalling that the instance of SVP that we started with is (L,r), and it was produced by applying Ajtai's reduction.

First we note that for every k, $0\leqslant k<2m$, L_k is a sublattice of L. Indeed, in going from L_k to L_{k+1}, the vectors $b'_1,b'_2,\ldots,b'_{i-1},b_i,b'_{i+1},\ldots,b'_m$ are still a basis of L_k because each b'_j is either b_j or b_j-b_i (this constitutes a unimodular transformation of the basis, which does not change the lattice). This set of vectors, with b_i replaced by $b'_i=2b_i$ span a sub-lattice of L_k of the same dimension.

Consider a vector $v\in L_k$, let $v=\sum_j c_j b_j$. After replacing the basis vectors b_j, $j\in W\setminus\{i\}$ by $b'_j=b_j-b_i$ (and before replacing b_i by $2b_i$), the (unique) representation of v in the new basis $b'_1,b'_2,\ldots,b'_{i-1},b_i,b'_{i+1},\ldots,b'_m$ of L_k is $\sum_j c'_j b'_j$, where $c'_j=c_j$ for all $j\neq i$, and $c'_i=\sum_{j\in W} c_j$. Now the point v is also present in L_{k+1} precisely if $c'_i=\sum_{j\in W} c_j$ is even. This is equivalent to the following: Let $w\in\boldsymbol{Z}_2^m$ denote the characteristic vector of the set W, and let $\cdot$ denote inner product mod 2; then $v\in L_{k+1}$ if and only if $p(v)\cdot w=0$, where $p(v)$ denotes the parity vector of v with respect to the basis $b_1,\ldots,b_m$ of L_k.

Since W was chosen uniformly at random, for any point $v\in L_k$, the probability that $v\in L_{k+1}$ is exactly $\frac{1}{2}$. Moreover, if u and v are distinct points of L_k of length at most $r<\sqrt{2}\leqslant\sqrt{2}\lambda_1(L_k)$, by Lemma 2, u and v have distinct parity vectors w.r.t. any basis of L_k. This implies that the events "$u\in L_{k+1}$" and "$v\in L_{k+1}$" are independent, since whether or not u and v belong to L_{k+1} depends only on their parity vectors.

At this point, the analysis bears a very strong resemblance to the analysis of Valiant and Vazirani [10], who showed the following: If we start with a set $\emptyset\neq S\subseteq\boldsymbol{Z}_2^n$,

randomly pick $w_1, w_2, \ldots, w_n \in \mathbf{Z}_2^n$ and define S_k, for $k = 1, \ldots, n$ by $S_k = \{x \in S \mid x \cdot w_j = 0 \text{ for } j = 1, 2, \ldots, k\}$, then with constant probability one of the S_k's has exactly one element.

We may let $S = \{p(v) \mid v \in L, v \neq 0, \text{ and } \|v\|_2 \leqslant r\}$, and for $1 \leqslant k \leqslant 2m$, $S_k = \{p(v) \mid v \in L_k \text{ and } \|v\|_2 \leqslant r\}$, and attempt to apply the lemma of [10] directly (as a black-box). However, it turns out that we have to be a little more careful. This is because as the basis changes in going from L_k to L_{k+1}, the parity vectors of lattice points keep changing. In particular, it is no longer true that the S_k's, as defined above, are all subsets of S.

On the other hand, we notice that it is only the "names" (parity vectors) of lattice points that change, the actual points themselves behave much better (that is, they either survive or are thrown out). Precisely, let us define the set T_k, $1 \leqslant k \leqslant 2m$, to be the set of non-zero lattice points of length $< r$ in L_k. This set does satisfy the nested subset property: $T = T_0 \supseteq T_1 \supseteq \cdots \supseteq T_{2m}$. It is immediately clear that if $T = \emptyset$, then every T_k is also empty. Moreover, the essential aspects of the [10] lemma remain true: $|T| \leqslant 2^m$ (by Corollary 3); for every k and any $v \in T_k$, $\Pr[v \in T_{k+1}] = \frac{1}{2}$; for every $v \in T$ and any $k < \ell$, the events "$[v \in T_{k+1} \mid v \in T_k]$" and "$[v \in T_{\ell+1} \mid v \in T_\ell,\ v \in T_{k+1}]$" are independent; and, finally, for $u \neq v \in T_k$, the events "$u \in T_{k+1}$" and "$v \in T_{k+1}$" are independent. These crucial statements are true for the following reasons: regardless of what happens in previous rounds, at the beginning of round k, u and v have (fixed) distinct parity vectors w.r.t. the basis for L_k; while these parity vectors may depend on the random choices made in the previous rounds, they may be considered fixed (and distinct) with respect to the choice of the set W (equivalently, its characteristic vector w) which is made uniformly at random and independently of the W's picked for earlier rounds. For the sake of completeness, we present the remainder of the proof, adapted from Sipser's complexity theory notes [9].

Lemma 4. *Let $T \neq \emptyset$ be a finite set of size at most 2^m, and let $T = T_0 \supseteq T_1 \supseteq \cdots \supseteq T_{2m}$ be a sequence of subsets of T defined by some probabilistic process that satisfies the following three properties*: (1) *for every k, $0 \leqslant k < 2m$, and every $x \in T$, $\Pr[x \in T_{k+1} \mid x \in T_k] = \frac{1}{2}$*; (2) *for every $x \in T$ and any $k < \ell$, the events "$[x \in T_{k+1} \mid x \in T_k]$" and "$[x \in T_{\ell+1} \mid x \in T_\ell, x \in T_{k+1}]$" are independent*; *and* (3) *for every k, $0 \leqslant k < 2m$, and elements $x, y \in T_k$, $x \neq y$, the events "$x \in T_{k+1}$" and "$y \in T_{k+1}$" are independent. Then, with probability at least $(\frac{2}{3}) - 2^{-m}$, one of the T_k's has exactly one element.*

Proof. First, we note that with probability $1 - 2^{-m}$, $T_{2m} = \emptyset$. This is because, by properties (1) and (2), for every $x \in T$, $\Pr[x \in T_{2m}] = \prod_{k=1}^{2m} (\frac{1}{2}) = 2^{-2m}$, and therefore, the probability that some x belongs to T_{2m} is at most $2^m 2^{-2m} = 2^{-m}$.

Assuming that $T_{2m} = \emptyset$, let k be the largest index such that T_k has at least two points. Thus $|T_{k+1}|$ is either zero or one. We will upper bound the probability that it is zero. Let u and v be two distinct elements of T_k. The probability that $|T_{k+1}| = 0$ is clearly upper bounded by the probability that neither of u and v belongs to T_{k+1}. Since the events "$u \in T_{k+1}$" and "$v \in T_{k+1}$" are independent, all four possibilities for

the memberships of u and v in T_{k+1} occur with probability $\frac{1}{4}$. Since $|T_{k+1}|$ is either zero or one, it is not true that both u and v belong to T_{k+1}. Conditioned on this event, the probability that neither belongs to T_{k+1} is exactly $\frac{1}{3}$. The proof of the lemma is complete. □

Acknowledgements

We are grateful to Daniele Micciancio for a very helpful conversation, and to the referees for helpful comments and suggestions on the presentation.

References

[1] M. Ajtai, The shortest vector problem in L_2 is NP-hard for randomized reductions, Proc. 30th Annu. ACM Symp. on the Theory of Computing, 1998, pp. 10–19.
[2] M. Ajtai, C. Dwork, A public-key cryptosystem with worst-case/average-case equivalence, Proc. 29th Annu. ACM Symp. on the Theory of Computing, 1997, pp. 284–293.
[3] J. Cai, A relation of primal–dual lattices and the complexity of shortest lattice vector problem, Theoret. Comput. Sci. 207 (1998) 105–116.
[4] J. Cai, A. Nerurkar, Approximating the SVP to within a factor $(1 + 1/(\dim^{\varepsilon}))$ is NP-hard under randomized reductions, J. Comput. System Sci. 59 (1999) 221–239.
[5] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices, and Groups, Springer, Berlin, 2nd (Ed.), 1993, 3rd (Ed.), 1998.
[6] D. Micciancio, The shortest vector in a lattice is hard to approximate to within some constant, Technical Report TR 98-016, Electronic Colloq. on Computational Complexity, 1998, available at `www.eccc.uni-trier.de`.
[7] C. Papadimitriou, Computational Complexity, Addison-Wesley, Reading, MA, 1994.
[8] N. Sauer, On the density of families of sets, J. Combin. Theory Ser. A 13 (1972) 145–147.
[9] M. Sipser, Lecture notes on advanced complexity theory, MIT/LCS course 18.405, 1996, available by anonymous ftp at `theory,lcs.mit.edu/pub/classes/18.405.`
[10] L. Valiant, V. Vazirani, NP is as easy as detecting unique solutions, Theoret. Comput. Sci. 47 (1986) 85–93.