

# Random lattices and a conjectured 0 – 1 law about their polynomial time computable properties

Miklós Ajtai

IBM Almaden Research Center

## Abstract

We formulate a conjecture about random  $n$ -dimensional lattices with a suitable distribution. The conjecture says that every polynomial time computable property of a random lattice holds with a probability either close to 0 or close to 1. Accepting the conjecture we get a large class of hard lattice problems. We describe an analogy between our conjecture and a set theoretical axiom, which cannot be proved in ZFC. This axiom says that there exists a nontrivial  $\sigma$ -additive 0 – 1 measure defined on the set of all subsets of some set  $S$ .

**Introduction.** A measure  $\mu_n$  on  $n$ -dimensional lattices with determinant 1 was introduced about fifty years ago to prove the existence of lattices which contain points from certain sets.  $\mu_n$  is the unique probability measure on lattices with determinant 1 which is invariant under linear transformations with determinant 1, where a linear transformation acts point by point on lattices.

Our main goal is to formulate a conjectured 0 – 1 law about  $\mu_n$ . We will also give a method for generating a random lattice with the distribution  $\mu_n$ . As we will see, there are many proven 0 – 1 laws concerning random structures, but they are valid for a much smaller set of properties, e.g. first-order definable properties. The infinite sequence  $\langle P_n \mid n = 1, 2, \dots \rangle$  is a property of lattices if for each  $n$ ,  $P_n$  is a set of  $n$ -dimensional lattices with determinant 1. We say that a property  $P_n$ ,  $n = 1, 2, \dots$  is polynomial time computable (p.t.c.) if there is a probabilistic Turing machine  $T$  so that given a lattice with any basis as an input  $T$  decides with high probability in polynomial time whether  $P_n$  holds. The conjecture states that for any p.t.c property  $P_n$ ,  $n = 1, 2, \dots$  we have that either  $\lim_{n \rightarrow \infty} \mu_n(P_n) = 0$  or  $\lim_{n \rightarrow \infty} \mu_n(P_n) = 1$ . The conjecture implies  $P \neq NP$  so there is not much hope for proving it, but it gives a way to create a large number of hard lattice problems. (E.g. it implies that for any fixed set  $H$  of volume 1 in  $\mathbf{R}^n$  it cannot be decided in polynomial time whether a lattice contains a nonzero point from  $H$ .) We do not think that there is any reason to believe that it is easier to prove  $P \neq NP$  through

the conjecture than in any other way. Our goal is rather to give a way to create a large collection of computationally hard problems (by accepting a single statement.) As we will show some of these problems may be useful for cryptographic purposes.

We also describe an analogy between our conjecture and a famous set theoretical axiom, which cannot be proved in ZFC, the usual system of axioms for set theory. (This axiom states that there exists a nontrivial  $\sigma$ -additive 0 – 1 measure defined on the set of all subsets of some set  $S$ .) This analogy served as a motivation for the formulation of the conjecture and it also makes more likely that the conjecture cannot be disproved. (J. H. Lutz and E. Mayordomo formulated a conjecture, implying  $P \neq NP$ , which also has a measure theoretic motivation although in a somewhat different sense, see [12]).

We formulate the conjecture about lattices over the field of real numbers, so each point of the lattice is presented as a sequence of real numbers. The length of the sequence is the dimension of the lattice. We will use a computational model where to access the  $i$ th bit of a real number requires about  $i$  time units, so during a polynomial time computation we can access the first polynomial number of bits of each real number. Still, as we will explain later, the randomization itself cannot be done on lattices over the rationals. However the consequences of the conjecture can be translated into hardness statements about rational or integer lattices.

*Notation.* We will write p.t. for “polynomial time” and p.t.c. for “polynomial time computable” throughout the paper.

**The definition of a measure on lattices.** The topology and measure on lattices described in this section was introduced by Mahler around 1946. The measure first was used by him to prove the Minkowski-Hlawka theorem about the existence of lattices that do not contain points from certain sets. The proof used an averaging argument on lattices according to this measure (See [8]). Although  $\mu_n$  is a probability measure it was used only for existence proofs and not for probabilistic constructions of lattices. No connection between  $\mu_n$  and probabilistic notions were investigated.

**Definition.** If  $n$  is a positive integer then an  $L \subseteq \mathbf{R}^n$  is

an  $n$ -dimensional lattice if there are  $n$  linearly independent vectors  $a_1, \dots, a_n \in \mathbf{R}^n$  so that for all  $x \in L$  there are integers  $\alpha_1, \dots, \alpha_n$  with  $x = \sum_{i=1}^n \alpha_i a_i$ . A linearly independent system of vectors  $a_1, \dots, a_n$  with the described property will be called a basis of  $L$ . The absolute value of the determinant whose columns are  $a_1, \dots, a_n$ , where  $a_1, \dots, a_n$  is a basis of  $L$  is called the determinant of  $L$ . Clearly the determinant of the lattice does not depend on the choice of the basis  $a_1, \dots, a_n$ . We will denote the set of all  $n$  dimensional lattices whose determinant is one by  $\text{lattice}_n$ .

First we define a measure (and a topology) on the set of all sequences consisting of  $n$  linearly independent vectors in  $\mathbf{R}^n$ . This space consists of all of the possible bases of lattices so it helps in the formulation of the final definition of  $\mu_n$ .

Definitions. 1. Let  $\text{basis}_n$  be the set of all sequences  $a_1, \dots, a_n \in \mathbf{R}^n$  so that  $a_1, \dots, a_n$  are linearly independent and the matrix formed from them has determinant 1 or  $-1$ . We will consider each  $\langle a_1, \dots, a_n \rangle \in \text{basis}_n$  as an  $n \times n$  matrix whose columns are  $a_1, \dots, a_n$  and therefore we may assume that  $\text{basis}_n \subseteq \mathbf{R}^{n^2}$ .

2. If  $a = \langle a_1, \dots, a_n \rangle \in \text{basis}_n$  then let  $\psi(a)$  be the lattice whose basis is  $a_1, \dots, a_n$ .

We will define a topology on  $\text{lattice}_n$  and our measure will be defined on the Borel sets of this topological space. The set  $\text{basis}_n$  has a topology on it induced by the topology of  $\mathbf{R}^{n^2}$ . (We get all of the open sets in the form  $\text{basis}_n \cap H$  where  $H$  is an open set of  $\mathbf{R}^{n^2}$ .) This induces a topology on  $\text{lattice}_n$ , namely  $G \subseteq \text{lattice}_n$  will be open iff  $\psi^{-1}(G)$  is open in  $\text{basis}_n$ . The Borel sets of  $\text{lattice}_n$  are the elements of the smallest  $\sigma$ -algebra on  $\text{lattice}_n$  which contains all open subsets. It is easy to see that a  $B \subseteq \text{lattice}_n$  is a Borel set iff  $\psi^{-1}(B)$  is a Borel set of  $\text{basis}_n$  (or of  $\mathbf{R}^{n^2}$ ).

We want to define a measure on the Borel sets of  $\text{lattice}_n$  which is invariant under linear transformations with determinant 1. First we define a measure with this property on  $\text{basis}_n$ .

1. If  $V \subseteq \mathbf{R}^n$  then  $V^\circ$  will denote the set of all vectors  $\gamma v$  where  $\gamma \in \mathbf{R}$ ,  $|\gamma| \leq 1$  and  $v \in V$ .

2. On the Borel sets of  $\mathbf{R}^n$  the  $n$  dimensional volume is a measure which will be denoted by  $\text{vol}_n$ .

3. If  $A \subseteq \text{basis}_n$  is a Borel set then let  $\rho_n(A) = \text{vol}_{n^2}(A^\circ)$

It is easy to see that  $\rho_n$  is a measure with the required property, namely, if  $T$  is a linear transformation on  $\mathbf{R}^n$  with determinant 1 or  $-1$  and  $A \subseteq \text{basis}_n$  then  $\rho_n(TA) = \rho_n(A)$ . (Here we apply  $T$  to  $A$  point by point and for each  $a = \langle a_1, \dots, a_n \rangle \in \text{basis}_n$ ,  $Ta = \langle Ta_1, \dots, Ta_n \rangle$ .) The reason for the equality  $\rho_n(TA) = \rho_n(A)$  is that  $A$  acts on the elements of  $\text{basis}_n$  as a linear transformation of  $\mathbf{R}^{n^2}$ , namely the tensor product of  $T$  with the identity matrix and

so the determinant of this linear transformation on  $\mathbf{R}^{n^2}$  is  $\pm 1$ .

The measure  $\rho_n$  is *not* a probability measure e.g.  $\rho_n(\text{basis}_n) = \infty$ .

Since a lattice has infinitely many different bases,  $\psi^{-1}\{L\}$  is an infinite set for each  $L \in \text{lattice}_n$ . For the definition of the measure  $\mu_n$  we select an element  $\varphi(L)$  of  $\psi^{-1}(L)$  arbitrarily for each  $L \in \text{lattice}_n$ . In other words  $\varphi(L)$  is a basis of  $L$ . There are an infinite number of functions  $\varphi$  with this property and we fix one so that for each Borel set  $B \subseteq L$  the set  $\varphi(B)$  is also a Borel set.

E.g. the following definition of  $\varphi(L) = \langle a_1, \dots, a_n \rangle$  meets this requirement. We define  $a_i$  by recursion on  $i$ .  $a_i$  will be a vector in the lattice which is linearly independent from the vectors  $a_1, \dots, a_{i-1}$  and of minimal length with this property. If there are more then one such vector then  $a_i$  will be the smallest according to lexicographic ordering.

Definition. If  $A$  is a Borel subset of  $\text{lattice}_n$  then let  $\mu'(A) = \rho_n(\varphi(A))$  and let  $\mu_n(A) = (\mu'(\text{lattice}_n))^{-1} \mu'(A)$ .

It is easy to see that  $\mu'$  is a measure on the Borel sets of  $\text{lattice}_n$  and  $\mu'$  does not depend on the choice of the function  $\varphi$  with the mentioned properties. It can be proved that that  $\mu'(\text{lattice}_n) < \infty$  and actually there is an explicit formula for  $\mu'(\text{lattice}_n)$  (see [8]). Clearly  $\mu_n$  is a probability measure defined on the Borel sets of  $\text{lattice}_n$ . The most important property of this measure is the following: if  $T$  is a linear transformation with determinant  $\pm 1$  and  $A$  is a Borel set of lattices then  $\mu_n(A) = \mu_n(TA)$ . (If  $L$  is a lattice then  $TL = \{Tx | x \in L\}$  is also a lattice, and if  $A$  is a set of lattices then  $TA = \{TL | L \in A\}$ .) This property easily follows from the corresponding property of  $\rho_n$ .

All of the definitions and theorems that we described up to this point were already known for more than fifty years. The definition of  $\mu_n$  is not satisfactory from a computational point of view. (E.g. there is no known p.t.c. choice for the function  $\varphi$ .) After formulating the conjecture we will give an equivalent definition which can be used for generating a random lattice with the distribution  $\mu_n$  in polynomial time.

Before we formulate our conjecture we list a few facts about random lattices which may help to "visualize" them. A random lattice  $L$  with distribution  $\mu_n$  has the following properties with a probability higher than  $1 - n^{-c}$ . ( $\gamma_n$  denotes the radius of the  $n$  dimensional ball whose volume is 1.  $\gamma_n$  is about  $n^{\frac{1}{2}}$ .  $c' > 0$  is sufficiently large with respect to  $c$ .)

1. The length of the shortest vector is about  $\gamma_n$  with a multiplicative error of at most  $1 \pm c'n^{-1} \log n$ .

2. There is a basis of  $L$  where the maximal lengths of the basis vectors is less than  $\gamma_n(1 + c'n^{-1} \log n)$ .

3. In a ball of radius  $\gamma_n(1 + c'n^{-1} \log n)$  the number of lattice points is asymptotically the volume of the ball, that

is,  $n^{c'}$ . For any fixed set  $S$  with larger than  $n^{c'}$  volume the number of lattice points in  $S$  is about  $n^{c'}$ .

**Conjectures in complexity theory and set theory.** Complexity theory is full of unsolved problems, in particular unproved lower bounds about the resources needed to solve computational tasks in various models. We frequently try to make some order among the many undecided questions by an “axiomatic” method. E.g. as a consequence of the assumption  $P \neq NP$  we get that all of the  $NP$ -hard problems are computationally hard. The assumption that there is no efficient algorithm for factoring long integers (or finding short vectors in a large dimensional lattice) have consequences in cryptography. In these cases we accept a few unproved statements as axioms and with their help we are able to decide a large number of interesting questions. A very large part of cryptography (both theoretical and practical) has been built around these type of axioms. We accept these axioms (at least temporarily) on various grounds. E.g. many researchers feel, based on some “philosophical” argument, that the statement  $P \neq NP$  must be true. In other cases (e.g. the hardness of factoring) we may have more pragmatic reasons. The problem remained unsolved for centuries although the best scientists of the world tried to solve it, so it must be hard. Naturally different people would put the same problem in different categories according to this classification.

Altogether we may say that in complexity theory (and in particular in the theory of lower bounds) this axiomatic approach is successful in the sense that with a relatively small number of axioms we are able to decide a large number of interesting and open problems. On the other hand the method is also very incomplete. Namely there are many interesting problems in this area which are not  $NP$ -hard, cannot be reduced to factoring or any other famous unsolved problem so we do not have a firm ground to tell whether they are probably hard or not.

To make some order among a lot of different unsolved problems by this axiomatic method were also tried in certain branches of mathematics. (E.g. in prime number theory Riemann hypothesis serves as an axiom). In set theory (about infinite sets) there was a similar situation about fifty years ago. Here it is important to note that the word “axiom” in the context of set theory usually means the simple “self-evident” statements about the existence of sets on which the whole set theory (including everything in mathematics) is built. Such a system is  $ZFC$  the Zermelo-Fraenkel system of axioms with the Axiom of Choice (see [9]). We are not using now the word in this sense but rather we are referring to set theoretical conjectures like the continuum hypothesis, which can be added to  $ZFC$  as additional axioms. The basic notions of set theory were introduced by Cantor toward the end of the nineteenth century and he also formulated the continuum hypothesis. In addition to the contin-

uum hypothesis many basic questions in set theory were later formulated which remained open and it seemed that there is no hope of deciding them. About fifty years ago Kurt Gödel has shown that the continuum hypothesis cannot be disproved and later Paul Cohen has proved that it cannot be proved in  $ZFC$ . (For the proof of these facts they used as an additional axiom that  $ZFC$  is consistent.) Apart from the continuum hypothesis there were a very large number of other set theoretical questions which remained open and set theorists started to use some of them as new axioms. Another question of this type is the so-called measure problem. We describe here the problem since our goal is to formulate a finite analogue.

**The measure problem.** *Is there a set  $S$  and a  $\sigma$ -additive  $0, 1$ -measure defined on all subsets of  $S$ , which takes the value  $0$  on all singletons and the value  $1$  on  $S$ ?*

It can be proved that if such a set  $S$  exists then its cardinality must be very large in some sense. Because of this the axiom stating that there exists such a measure is usually stated in the form “there exists a measurable cardinal”. This is one of the so called “large cardinal” axioms (see [9]).

This situation in the fifties of the last century in set theory was somewhat similar to the situation of the described state of “axiomatic” complexity theory right now. Later however a few very powerful axioms have been found (e.g. the so called large cardinal axioms, we have seen one of them) which seem to decide almost any interesting set theoretical question (see [7]). (Of course this is not a mathematical statement. It is always possible to create questions which are undecidable in a given system of axioms; we are speaking about only “natural” set theoretical questions.)

A similar development would be desirable in complexity theory as well since it would eliminate the mentioned incompleteness of the axiomatic method in complexity theory. We do not have any methods of showing that a statement like “ $P = NP$ ” cannot be proved or disproved in  $ZFC$ , still we may try to come up with new, more powerful conjectures which as axioms decide more and more problems. This is one of the motivations of this work. We will describe a conjecture (concerning random lattices) which we think is pointing in the described direction.

The mentioned conjecture about random lattices has a direct analogue in infinite set theory. Perhaps this analogy makes it more likely that the conjecture is valid (or at least it will not be disproved) so we describe it briefly. Our starting point is the “Measure problem” formulated earlier. For the motivation of the original measure problem we note that a finitely additive  $0, 1$ -measure is the same as an ultrafilter which is frequently used in model theoretic constructions. The sets of measure  $1$  belong to the ultrafilter. So a  $\sigma$ -additive  $0, 1$ -measure defines an ultrafilter closed under countable intersections so the corresponding model theoretic construction (ultraproduct) becomes much more pow-

erful. It was shown that the existence of such a measure implies that *ZFC* is consistent so by Gödel's incompleteness theorem this statement cannot be proved in *ZFC*. However accepting the existence of such a measure as an axiom proved to be very fruitful in set theory.

Our goal is to give a finite analogue of this axiom. Of course a literal translation is not possible since on a finite set if a measure is 0 on the singletons then it is 0 everywhere. In our finite version of the problem we will think that a positive integer  $n$  is fixed, and we will translate the phrase "the measure defined on all subsets of  $S$ " into "the measure defined on all p.t. definable subsets of  $S$ ". (Or alternatively on all sets defined by a polynomial size circuit.) This makes sense only if the elements of  $S$  can serve as an input to a p.t. algorithm so they have a (not necessarily unique) representation by a 0, 1 sequence of polynomial length. Another change will be that for a fixed  $n$  the measure may take any value in the  $[0, 1]$  interval, only the asymptotic values will be strictly 0s and 1s. (Asymptotic in the sense that the p.t. definition of the set is fixed and we tend to infinity with  $n$ .) Surprisingly, there are theorems about finite random structures, which are formulated along these lines with the exception that instead of p.t.c. sets the measure is defined on first-order definable sets (some type of second-order definitions may be also allowed). These theorems are the 0 – 1 laws for finite structures. The first theorem of this type, was formulated and proved by R. Fagin (see [5]). These 0 – 1 laws serve both as a motivation and a model for formulating our conjecture.

Finite analogues of set theoretical notions/techniques have already been used in complexity theory. The set theoretical technique "forcing" was created by Paul Cohen to show that the continuum hypothesis cannot be proved in *ZFC* and later used by many other mathematicians for proving most of the independence results. The author of the present paper used a finite analogue of this method to show that the Pigeonhole Principle has no polynomial size constant depth propositional proof (the journal version of the paper [2] contains the complete description of the set theoretic connection). In a similar sense there is a technical connection between the infinite and finite statements in the present case as well. Namely the set theoretic technique "ultraproduct" which is the main tool of the proofs concerning the measure problem, has a finite analogue. More precisely working with fragments of Peano Arithmetic in a similar way as in [2] we may define the finite version of the ultraproduct and our finite conjecture has similar effect on it as the infinite version. We do not need this for the formulation of our conjecture or for the proof of any of the stated results. We mention this here only to point out that the analogy between the finite and infinite measure problems is not superficial, but has a substantial technical content.

**0-1 laws.** Assume that we pick a random graph on a

vertex set consisting of  $n$  elements so that for each pair of vertices  $\{a, b\}$  the probability that the unordered pair  $\{a, b\}$  is an edge of the graph is  $\frac{1}{2}$ , moreover all of these events for the various pairs of vertices are independent. For any first-order formula  $\varphi$  in the language of graphs let  $p(\varphi, n)$  be the probability that  $\varphi$  holds on the random graph on  $n$  vertices. Ron Fagin has proved (see [5]) in a more general form that for any fixed first-order formula  $\varphi$  either  $\lim_{n \rightarrow \infty} p(\varphi, n) = 0$  or  $\lim_{n \rightarrow \infty} p(\varphi, n) = 1$ , that is, the 0 – 1 law holds for the first-order properties of random graphs. The theorem gives a surprisingly complete picture about the behaviour of first-order formulae on random graphs at least in an asymptotic sense. It has been generalized in many directions. E.g. we may pick the probabilities of the individual edges in a more general way or instead of first-order formulae we may allow second-order formulae with some strong restrictions on the second-order quantifiers. A third possibility is that instead of the binary relations of the graphs we pick random relations of larger arities. All of these directions were very thoroughly investigated and led to many interesting results (see [10], [4]).

From the point of view of constructing graphs (or other structures) with interesting properties, all of these 0-1 laws have a common deficiency, namely the class of properties for which the 0-1 law holds, e.g. first-order definable properties in the case of random graphs, is very limited. The really interesting properties of graphs usually cannot be defined by a first-order formula. The mentioned generalizations for wider classes of formulae does not change this picture.

Our finite analogue for the measure problem will be a statement which says that on a certain class of random structures (random lattices) a 0–1 law holds for the p.t. definable properties.

First we note that such a 0-1 law does not hold for random graphs with the described randomization. Indeed if  $n$  is the number of vertices then e. g. the property "the number of edges is less than  $\frac{1}{2} \binom{n}{2}$ " always holds with about probability  $\frac{1}{2}$ . We may try to avoid this problem by restricting our attention to graphs with a fixed number of edges, but then we may easily find some other parameter (e.g. the number of triangles in the graph) which will have a nontrivial distribution. We may describe this phenomenon in a more general framework.

**Definitions.** 1. Suppose that for each  $n$ ,  $\mathcal{S}_n$  is a set of structures and  $\mu_n$  is a probability measure defined on the set of all subsets of  $\mathcal{S}_n$ . Assume that each element of  $\mathcal{S}_n$  can be uniquely represented by a 0, 1-sequence of polynomial lengths. (For the sake of simplicity we identify now the structure with this representation.) Assume further that there is a p.t. probabilistic algorithm which generates the distribution  $\mu_n$ , that is, given  $n$  as an input it provides structure  $S \in \mathcal{S}_n$  as an output with probability  $\mu_n(\{S\})$ . In this

case we will say that  $\mu_n$  is a p.t.c. distribution on the set of the uniquely represented structures  $\mathcal{S}_n$ ,  $n = 1, 2, \dots$ . We will call the sequence of measures  $\mu_n$  trivial if there is a sequence of structures  $X_n$ , with  $X_n \in \mathcal{S}_n$ , so that  $\lim_{n \rightarrow \infty} \mu_n(X_n) = 1$ . (In other words  $\mu_n$  is trivial if for all large enough  $n$  it is essentially concentrated on a single structure  $X_n$ ).

2. We say that the property  $P_n$  on  $\mathcal{S}_n$ ,  $n = 1, 2, \dots$  is p.t. definable if there is a p.t. algorithm  $\mathcal{A}$  which for all  $n$ , at the input  $\langle n, S \rangle$  where  $S \in \mathcal{S}_n$  decides whether  $S$  has property  $P_n$  or not. If  $\lim_{n \rightarrow \infty} \mu_n(P_n) = 1$  or  $\lim_{n \rightarrow \infty} \mu_n(P_n) = 0$  then we say that the 0 – 1 law holds for property  $P_n$ ,  $n = 1, 2, \dots$ .

**Lemma 1** *Suppose that  $\mu_n$  is a non-trivial polynomial time computable distribution on the set of the uniquely represented structures  $\mathcal{S}_n$  for  $n = 1, 2, \dots$ . Then there is a polynomial time definable property  $P_n$  on  $\mathcal{S}_n$ ,  $n = 1, 2, \dots$  so that the 0 – 1 law does not hold for property  $P_n$ ,  $n = 1, 2, \dots$ .*

We will give the proof later. There are two consequences of this lemma which are important from our point of view. (1) We cannot consider lattices together with a fixed basis since this would provide a unique representation. Therefore we will consider a lattice just as a set of points in the  $n$  dimensional space which can be given with any (not too long) basis and will require that the fact whether lattice  $L$  has property  $P_n$  or not can be decided in p.t. starting from any basis of  $L$ .

(2) We cannot consider lattices consisting of points with integer (or rational) coordinates. It is easy to see that there is a p.t. algorithm which given any integer lattice as an input, presented with an arbitrary basis  $B$  with a polynomial number of bits, selects a unique basis of  $L$  which does not depend on  $B$ . Indeed, let  $e_i$  be the  $i$ th unit vector and let  $c_i$  be the smallest positive integer so that  $c_i e_i \in L$ . In this case the vectors  $c_i e_i$  are in the lattice and they are also linearly independent. Moreover the sequence  $c_i e_i$  is uniquely determined by the lattice. It is easy to see that a uniquely determined basis can be constructed from them.

Because of (2) we will give our probability distribution on the set of all lattices whose elements are arbitrary vectors in  $\mathbf{R}^n$ . This causes a substantial complication in the way of presenting lattices (we have to deal with the representations of real numbers), however (2) shows that there is no 0 – 1 law for lattices consisting of integer vectors. Naturally when we use a random lattice, presented by a basis, as an input for our computation will use a rational approximation of the basis, however such an approximations will not determine the lattice uniquely.

**The formulation of the conjecture.** Definitions. 1. If  $L \subseteq \mathbf{R}^n$  is a lattice and  $a_1, \dots, a_n$  is a basis of  $L$  then the length of the basis  $a_1, \dots, a_n$  will be  $\max_{i=1}^n \|a_i\|$ .

2. We will assume that the input of a Turing machine can be a real number or a finite sequence of real numbers. (Alternately the reader who is familiar with the oracle representation of real numbers may think that each real number is represented by an oracle and the cost of getting a rational approximation of it with precision  $2^{-i}$  is  $i$  time units.) A real number  $\alpha$ ,  $0 \leq \alpha < 2$  is given as an infinite sequence of rationals  $r_0, r_1, \dots, r_k, \dots$  so that  $|r_k - \alpha| \leq 2^{-k+1}$  and  $r_k$  has at most  $k + 2$  binary bits. (This representation is not unique but has the property that an  $r_k$  can be computed if  $\alpha$  is known approximately with an error of at most  $2^{-k-1}$ . In contrast the binary bits of a real number in certain cases cannot be decided knowing only an approximation of the number.) An arbitrary real number  $\beta$  is represented by a pair  $\langle \beta_0, \beta_1 \rangle$ , where  $\beta = \beta_0 + \beta_1$ ,  $\beta_0$  is an integer given in binary form and  $\beta_1 \in [0, 2)$  is a real given in the form described above. (The reason why we pick  $\beta_1$  from an interval of length 2, instead of the interval  $[0, 1)$ , is that this way  $\beta_0$  can be selected even if only an approximation of  $\beta$  is known.) This way, in time polynomial in  $k$ , we can get an approximation of  $\beta$  with a precision of  $2^{-k}(|\beta| + 1)$ . Conversely if we are able to compute an approximation of  $\beta$  in polynomial time then we are also able to compute the corresponding initial segment of a representation. If a sequence of real numbers  $\alpha_1, \dots, \alpha_i$  is given as input then  $\alpha_j$  is given on the cells  $j + ti$ ,  $t = 1, 2, \dots$ . We assume that at the beginning of the computation the head of the Turing machine is at the first cell. Therefore, although a real number as an input is an infinite 0, 1 sequence, during a p.t. computation only a polynomial number of bits will be accessed.

3. Suppose that  $\mathbf{P} = \langle P_n \mid n = 1, 2, \dots \rangle$ , is a property of lattices with determinant 1. (That is,  $P_n \subseteq \text{lattice}_n$ ). We say that  $\mathbf{P}$  is p.t.c. if there is a probabilistic Turing machine  $T$  so that for all  $c' > 0$  there is a  $c > 0$  so that if  $n$  is sufficiently large and  $L$  is a random lattice chosen with the distribution  $\mu_n$ , then for any basis  $a_1, \dots, a_n$  of  $L$  with length less than  $2^n$  if  $T$  gets  $n, c', a_1, \dots, a_n$  as input then in time  $n^c$  it provides an output  $x$  so that with a probability of at least  $1 - n^{-c'}$  (for the randomization of  $L$  and the random steps of  $T$ ) we have  $x = 1$  iff  $L \in P_n$ .

**Conjecture 1** *Suppose that  $\mathbf{P} = \langle P_n, n = 1, 2, \dots \rangle$  is a p.t.c. lattice property. Then either  $\lim_{n \rightarrow \infty} \mu_n(P_n) = 0$  or  $\lim_{n \rightarrow \infty} \mu_n(P_n) = 1$ . Moreover for all  $c > 0$  if  $n$  is sufficiently large then either  $\mu_n(P_n) < n^{-c}$  or  $\mu_n(P_n) > 1 - n^{-c}$ .*

We may replace the condition p.t.c. by “definable by a polynomial size circuit”, then we get a somewhat stronger and perhaps more natural statement.

The conjecture seems to be compatible with every known lattice algorithm. (The conjecture was presented in a talk at the MSRI Workshop on Number Theory and Cryptography in the fall of 2000 and since then there was no indication that

the conjecture may be false.) Another argument in favor of the conjecture is the following. The same general principle about lattices, namely that from an algorithmic point of view (that is, if we perform computations about a lattice starting from an arbitrarily given large basis) almost every lattice looks the same, lead the author to theorems about the equivalence of worst-case and average-case lattice problems (see [1]).

This conjecture implies  $P \neq NP$ . Indeed if  $P = NP$  then the shortest vector in a lattice can be found in p.t. moreover there is a p.t.c. rational  $\alpha(n) > 0$  so that in a random lattice  $L$  the probability that the shortest nonzero vector is shorter than  $\alpha(n)$  is about  $\frac{1}{2}$ . If this property is  $P_n$  then the  $0 - 1$  law clearly does not hold.

There is no reason to think that to prove that  $P \neq NP$  through the conjecture is easier than any other possible of proof. However unlike the statement  $P \neq NP$  the Conjecture has special cases which are not lower bounds concerning some computational model but “ordinary” mathematical statements. (Of course these statements may not have any computational consequences.) Namely for any property  $P_n$  (once we have proved that  $P_n$  is p.t.c.) the statement of the conjecture has nothing to do with lower bounds it is a mathematical statement in a classical sense. E.g. we know that there is a p.t.c. algorithm which approximates the number of lattice points in a large ball (large compared to a known basis). Based on this and the conjecture we expect that the number of lattice points of a random lattice in the ball will be always (approximately) the same and indeed this can be proved. (We can prove a similar theorem for random lattices about  $k$ -tuples in a large ball, where  $1 \leq k \leq n - 1$ . The proof of the general statement is more difficult than the  $k = 1$  special case.) Another consequence of the conjecture where we do not have a proof is the following. Let us consider a p.t. algorithm computing a relatively short vector in the lattice e.g. the LLL algorithm (cf. [11]). If we have a fixed lattice  $L$  then we are able to pick a random basis  $b$  from a large cube (large relative to a known basis). Starting with different random choices for  $b$  the length of the short vector that our algorithm produces has a distribution. It is a consequence of the conjecture that this distribution is essentially independent of the lattice in the sense that if we pick various random lattices  $L$  then with a probability close to 1 they will provide distributions which are indistinguishable by p.t.c. We do not have a proof for this statement but its proof may be very much easier than either the conjecture in general or the statement  $P \neq NP$ .

Remarks. 1. The Conjecture implies that there is no p.t. algorithm that selects a uniquely defined nonzero element from each lattice (or selects) a unique basis.

2. We do not know whether  $P \neq NP$  implies the conjecture.

3. Based on the conjecture we can create a large number

of computationally hard lattice problems. If  $S \subseteq \mathbf{R}^n \setminus \{0\}$  let  $p_S$  be the probability that a random lattice with distribution  $\mu_n$  has a point in  $S$ . We show that if the volume of  $S$  is 1 then both  $p_S$  and  $1 - p_S$  is bounded from below by a positive constant. Therefore according to the conjecture there is no polynomial time algorithm which decides whether a given lattice has a point in  $S$ . (We used a similar argument to show that the conjecture implies  $P \neq NP$ .) Since  $S$  now can be a set of any shape (there is no assumption about convexity or connectivity) this creates a huge number of computationally hard problems. Based on the  $P \neq NP$  assumption we have similar conclusions only for spheres (in various metrics) and to expand it to other type of sets seems very difficult and probably requires proofs for each new type of sets  $S$ . The assumption  $\text{vol}_n(S) = 1$  can be substituted by  $n^{-c} \leq \text{vol}_n(S) \leq n^c$ .

4. In the set theoretical axiom about the existence of a  $\sigma$ -additive 0, 1-measure the measure is not defined explicitly unlike in the finite analogue. This is not really a difference since in our finite world we consider only p.t.c. sets so already every set is explicitly defined. The analogue of  $\sigma$ -additivity is additivity for a polynomial number of terms, which holds if the conjecture is true. It is true however that in the finite case by naming a measure we are making a somewhat arbitrary decision.

5. Even in the case of the set theoretical measure problem (or other large cardinal axioms) we do not have any guarantee that these statements are really consistent to  $ZFC$ . (Actually we know that this consistency cannot be proved in  $ZFC$  even if in the proof we can use the additional axiom that  $ZFC$  is consistent.) In this sense the finite case is worse only because our intuition is weaker and perhaps we have less experience in the subject. Experience seems to be important since in the early history of large cardinals sometimes it was assumed that the smallest strongly inaccessible cardinal is measurable, which simply turned out to be false. The experience in the finite case is provided by the history of lattice problems.

**Lattices over the reals and integers.** Our conjecture is formulated about lattices over the reals, that is, the lattice points may have arbitrary real coordinates. In contrast most of the computational problems concerning lattices are about lattices where the coordinates are integers or at least rationals. There is no essential difference between the integer and rational case, because for each rational lattice  $L$  there is a single integer  $m$  so that  $mL$  is an integer lattice. (Naturally if we change the “scaling” this way we change the determinant as well.)

If we have a real lattice we can always approximate it with a rational lattice. Actually our definition of a lattice property implies that we are using only lattice properties which can be decided by knowing only a good enough rational approximation. As a consequence, although our inputs

are real numbers given by infinite 0, 1-sequences, we use only a finite initial segment (of length  $n^c$ ) in our computation. The reason why we do not cut down the remaining part in advance is that in the conjecture the value of  $c$  is not fixed but depends on other quantified parameters. (Lemma 1 shows that the conjecture modified for a fixed length is not true.) In principle we could cut down the sequence representing the real numbers after the first  $f(n)$  bits where  $f(n)$  grows faster than polynomial. This would mean that we are working with rational lattices but there may not be basis with polynomial size representation. This solution does not seem to offer any advantage compared to the real lattices and makes the definition of the distribution  $\mu_n$  more complicated.

Since we use only polynomial size initial segments of the 0, 1-sequences representing the real numbers every conclusion of our conjecture which says that it is hard to decide whether the real lattice has property  $P_n$  is actually a hardness statement about rational approximating lattices. The following (trivial) observation is helpful in making connection between the properties of the random lattice and of the approximating rational lattices. In this statement we are referring to the representation of a lattice as used in the conjecture, that is, it is given by an arbitrary basis of length not greater than  $2^n$  and the basis vectors and their coordinates are coded by a single 0, 1 sequence.

(1) If  $c_1 > 0$  is sufficiently large with respect to  $c_2 > 0$  and  $c_3 > 0$  then the first  $n^{c_1}$  bits of the representation of a lattice  $L$  with determinant 1 determines the location of the lattice points in a ball around 0 with radius  $2^{n^{c_2}}$  with an (additive) precision of  $2^{-n^{c_3}}$ .

The following lemma is also useful in this context. We will sketch the proof of this lemma later when we provide alternative definitions for the measure  $\mu_n$ .

**Lemma 2** If  $X \subseteq \mathbf{R}^n$  is a Borel set, and  $L$  is a random lattice with distribution  $\mu_n$  then the expected number of nonzero lattice points in  $X$  is  $\text{vol}_n(X)$ .

The lemma implies that if  $H \subseteq \mathbf{R}^n$  is a Borel set then the probability that there is a nonzero lattice point in  $H$  is at most  $\text{vol}_n(H)$ . Assume now that our lattice property is of the type “there is a nonzero lattice point in the set  $G$ ”. Suppose further that  $G$  has a “small boundary”, more precisely if  $c > 0$  is sufficiently large with respect to  $c' > 0$  the volume of the set of points which are closer than  $2^{-n^c}$  to both  $G$  and  $\mathbf{R}^n \setminus G$  is smaller than  $2^{-n^{c'}}$ . (E.g. a convex set  $G$  in a ball of radius  $2^{n^{c_1}}$  always satisfies this condition.) Then Lemma 2 implies that for a random lattice  $L$  and for a good rational approximation  $L'$  with high probability the property holds for  $L$  and  $L'$  at the same time.

**A stronger version of the conjecture.** We have formulated the conjecture in a weak form in the sense that small

probability means smaller than  $n^{-c}$  for any constant  $c > 0$ . However a stronger form where small means smaller than  $e^{-cn \log n}$  has more interesting consequences. The modified version of the conjecture can be stated as follows.

**Conjecture 2** Suppose that  $\mathbf{P} = \langle P_n, n = 1, 2, \dots \rangle$  is a p.t.c. lattice property. Then either  $\lim_{n \rightarrow \infty} \mu_n(P_n) = 0$  or  $\lim_{n \rightarrow \infty} \mu_n(P_n) = 1$ . Moreover for all  $c > 0$  if  $n$  is sufficiently large then either  $\mu_n(P_n) < e^{-cn \log n}$  or  $\mu_n(P_n) > 1 - e^{-cn \log n}$ .

Remark. Note that in this form of the conjecture only the probabilities has changed compared to the original version but the running times of the algorithms involved remained polynomial.

This form of the conjecture still seems to be consistent with all known facts. It can be proved that this stronger conjecture implies that the length of the shortest vector cannot be approximated in p.t. upto a polynomial factor. Indeed using the techniques for the proof of  $\mu_n(\text{lattice}_n) < \infty$  (see [8]) it is possible to show that for any fixed  $r$  with  $0 < r < \gamma_n$ , the probability that there is a nonzero lattice point in a ball of radius  $r$  around the origin is at least  $c_0 \gamma_n^{-n} r^n$  where  $c_0 > 0$  is an absolute constant. Assume now that there is a polynomial time algorithm  $\mathcal{A}$  which approximates the length of the shortest vector in any lattice within a factor of  $n^{c_1}$  for some  $c_1 > 0$ . We can argue the same way as in the proof of “Conjecture 1 implies  $P \neq NP$ ”. Namely there will be a rational  $r > 0$  so that if  $\lambda_0$  is the length of the shortest vector in a random lattice then the probabilities of both  $r < n^{-c_1} \lambda_0$  and  $r > n^{c_1} \lambda_0$  are greater than  $e^{-c' n \log n}$  for some  $c' > 0$ . Therefore the property “the approximated value of  $L$  provided by  $\mathcal{A}$  is greater than  $r$ ” does not satisfy the requirements of Conjecture 2 because it can be true of false both with a non-negligible probability.

The proof which gives that the probability that there is a nonzero lattice vector in the ball of radius  $r$  around the origin is at least  $c_0 \gamma_n^{-n} r^n$ , where  $c_0 > 0$  and  $r < \gamma_n$ , also guarantees that for all  $r < \frac{\gamma_n}{2}$  if there is such a vector then with high probability it is unique. (Unique in the sense that every such vector is parallel to it.) As a consequence, Conjecture 2 implies that it is hard to approximate the length of the shortest vector upto a polynomial factor even if we restrict our attention to lattices where the shortest vector is unique upto a polynomial factor. This also implies that it is not possible to find the shortest vector in polynomial time even in lattices where it is unique upto a factor of  $n^c$ . (We say that the shortest nonzero  $v$  vector in the lattice is unique upto a factor of  $\lambda$  if for all lattice vector  $u$ ,  $\|u\| \leq \lambda \|v\|$  implies that  $u$  and  $v$  are parallel.) Moreover from this proof we also get a method of constructing hard instances of the  $n^c$ -unique shortest vector problem. We describe how to construct the dual of such a lattice (this is what actually needed

in the cryptosystem described in [3].) First we take a random  $n - 1$  dimensional hyperplane  $H$  in  $\mathbf{R}^n$  through the origin. We choose it in a way that the normal vector of the hyperplane is taken with uniform distribution from the sphere around the origin with radius 1. Next we take a random  $n - 1$  dimensional lattice  $L_0$ , with distribution  $\mu_{n-1}$  in the hyperplane  $H$  (whose shortest vector will be of length about  $\gamma_{n-1}$ ). Multiplying every point in  $L_0$  by  $(n^{-c-1})^{\frac{1}{n}}$ , we get an  $n - 1$  dimensional lattice  $L_1$  in  $H$  whose determinant is  $D = n^{-c-1}$ . Now we take a hyperplane  $K$  parallel to  $H$  and from distance  $D^{-1}$  from it. We pick an arbitrary point  $x \in K$  and a random point  $a_n$  of the  $n - 1$  dimensional parallelepiped which has edges pointing from  $x$  to  $x + a_1, \dots, x + a_{n-1}$ , where  $a_1, \dots, a_{n-1}$  is a basis of  $L_1$ .  $L$  will be the lattice whose basis is  $a_1, \dots, a_n$ . It is easy to see that  $\det(L) = 1$  and the lattice points are located on hyperplanes parallel to  $H$  so that the distance of the consecutive hyperplanes is  $D^{-1} = n^{c+1} > 2n^c \gamma_{n-1}$  while the lattice  $L_1$  has a basis shorter than  $2\gamma_n$ . This implies that the dual  $L_2$  of  $L_1$  has an  $n^c$ -unique shortest vector. It is not difficult to see that Conjecture 2 implies that it is not possible to find the shortest vector in  $L_2$  or the hyperplane structure of  $L_1$  in p.t. with a polynomially large probability.

The described construction can be used in the public-key cryptosystem given by Ajtai and Dwork in [3] where a lattice is needed with the properties of  $L_1$ . In [3] instead of constructing such a lattice an alternative way is provided to use only the hyperplane structure associated with the lattice and it is shown that if the worst-case  $n^c$ -shortest vector problem is hard then it is also hard to break the cryptosystem. Now we provided an alternative “guarantee”, Conjecture 2, for the cryptosystem. The conjecture also implies that the version of the cryptosystem where not the hyperplanes but an actual lattice is used is also safe provided that we pick the lattice in the described manner. This has the advantage that the parameters (e.g. size of the key) are better than in the version based only on the hyperplane structure. (We intend to return to this question in a separate paper.) The reason is that for the proof which reduces the security of the hyperplane system to the worst-case problem we need a bigger ratio between the distance of the neighboring hyperplanes and the shortest vector in the lattice  $L_0$ . It is not clear whether the difference is just an imperfection of the mentioned proof or for the reduction to the worst case problem we really need a bigger ratio than for the random construction.

**A probabilistic definition of  $\mu_n$ .** In this section we give equivalent definitions for the probability measure  $\mu_n$  which are more satisfactory from a computational point of view than the original definition. These theorems give a definition of  $\mu_n$  based on probabilistic concepts and they make it possible to generate a random lattice in p.t.

The theorem defines the value of  $\mu_n$  on open sets through

a random process. The basic idea is that we start to “shake” a lattice by applying random linear transformations on it. After a time the distribution of the lattice, at least approximately, will not depend on the distribution of the linear transformations. (We exclude the possibility that there are not enough linear transformations.) These distributions converge to  $\mu_n$ .

**Definition.** The group of linear transformations of  $\mathbf{R}_n$  whose determinant is  $\pm 1$  will be denoted by  $\mathcal{G}_n$ . There is a natural topology on  $\mathcal{G}_n$  induced by its matrix representation.

**Theorem 1** *Suppose that  $n$  is a positive integer and the finite set  $X \subseteq \mathcal{G}_n$  meets the following requirements.*

(1) *the group of linear transformations generated by  $X$  is dense in  $\mathcal{G}_n$ .*

(2)  *$T \in X$  implies  $T^{-1} \in X$ .*

*Assume further that a distribution  $\kappa$  is given on  $X$  so that the probability of each singleton is positive. Let  $T_1, \dots, T_m, \dots$  be an infinite random sequence whose elements are picked independently and with the distribution  $\kappa$  from  $X$  and let  $L_i = T_i \cdot \dots \cdot T_1 L$ . Assume that for all  $L \in \text{lattice}_n$  and for all open  $G \subseteq \text{lattice}_n$ ,  $N(L, G, m)$  denotes the number of integers  $i = 1, \dots, m$  with  $L_i \in G$ , then*

$$\lim_{m \rightarrow \infty} \frac{1}{m} N(L, G, m) = \mu_n(G)$$

The following theorem gives a direct method for picking a random lattice in polynomial time with distribution  $\mu_n$  (with a polynomially small error). (Actually Theorem 1 can be modified so that it gives a polynomial time method for generating random lattices, however it involves some technical complications since for such a modified version we cannot pick the linear transformations from a finite set but must choose them e.g. from a ball.)

**Definition.** Assume that  $n$  is a positive integer and  $R > 0$ . We define a random variable  $\chi^{(R,n)}$  whose values are lattices. We pick at random and with uniform distribution  $n - 1$  vectors  $a_1, \dots, a_{n-1}$  from the ball with radius  $R$  centered around the origin in  $\mathbf{R}^n$ . With probability 1 the vectors  $a_1, \dots, a_{n-1}$  are linearly independent. Let  $D$  be the  $n - 1$  dimensional volume of the  $n - 1$  dimensional parallelepiped determined by the vectors  $a_1, \dots, a_{n-1}$ . Let  $x \in \mathbf{R}^n$  be a point whose distance from the hyperplane generated by  $a_1, \dots, a_{n-1}$  is  $D^{-1}$ . Let  $\mathcal{P}$  be the  $n - 1$  dimensional parallelepiped so that  $x$  is a vertex of  $\mathcal{P}$  and the neighbouring vertices are  $x + a_1, \dots, x + a_{n-1}$ . Finally let  $a_n$  be a random point of  $\mathcal{P}$  picked by uniform distribution. The lattice  $L$  whose basis is  $a_1, \dots, a_n$  is the value of the random variable  $\chi^{(R,n)}$ . (It is easy to see that the distribution of  $L$  does not depend on the choice of  $x$ .)

**Theorem 2** *For all  $c > 0$  there is a  $c_1 > 0$  so that if  $n$  is a positive integer and  $R > 0$  so that the volume of a ball with*

radius  $R$  is at least  $n^{c_1}$  then the distance of the distribution of  $\chi^{(R,n)}$  from the distribution  $\mu_n$  is at most  $n^{-c}$ .

**Sketch of the proofs.** Before we give the idea of the proofs of the individual theorems we describe another alternative definition for the probability measure  $\mu_n$  on  $\text{lattice}_n$ . This motivates some of the steps in the proofs.

Our goal is to define a measure  $\mu_n$  on the Borel sets of  $\text{lattice}_n$  so that for each linear transformation  $T$  with determinant 1 and each Borel set  $B$  we have  $\mu_n(B) = \mu_n(TB)$ . That is, we have a group  $\mathcal{G}_n$ , the group of linear transformations with determinants  $\pm 1$  which acts on a topological space  $\text{lattice}_n$ . The group also has its natural topology (defined by e.g. a matrix representation) which is locally compact. The space  $\text{lattice}_n$  is also locally compact. There are general theorems which guarantee the existence of an invariant measure (the Haar measure) in such a situation if the action of the group on the topological space satisfies certain additional conditions (see [6]). Usually these additional requirements are easier to meet if at least one of the two topological spaces is not only locally compact but compact. In this case it is not clear whether we can get the existence of the measure from a general theorem but anyhow essentially the same techniques as in the proofs of the general theorems leads to a proof of the existence and uniqueness (upto a constant factor) of the required measure. This definition in itself does not guarantee that  $\mu_n(\text{lattice}_n)$  is finite. We have to prove it the same way as in the case of the first definition.

This proof and particularly the part that the invariant measure is unique plays a role in the proof of Theorem 2 (the proof of Theorem 1 will be based on Theorem 2). We start with the proof of Lemma 2, that is, by showing that for any Borel set  $S \subseteq \{\mathbf{R}^n \setminus \{0\}\}$  if we take a random lattice  $L$  with distribution  $\mu_n$  then the expected value of the number of lattice points in  $S$  is  $\text{vol}_n(S)$ . Let  $\lambda(S)$  be this expected value. We show first that  $\lambda$  is a measure on the Borel subsets of  $\mathbf{R}^n \setminus \{0\}$  which is invariant under multiplication by elements of  $\mathcal{G}_n$ . This invariance follows from the corresponding invariance of the measure  $\mu_n$ . Once we have established the invariance of the measure  $\lambda$  we may apply the uniqueness theorem about invariant measures. (Again there seems to be no general theorem which implies this particular case but the methods used in the general theorem give the uniqueness of  $\lambda$ .) However  $\text{vol}_n$  is also an invariant measure with respect to  $\mathcal{G}_n$  (since the determinants of the elements of  $\mathcal{G}_n$  has values  $\pm 1$ ) so we get that the two measures  $\lambda$  and  $\text{vol}_n$  are identical upto a constant factor. We can show that this factor is 1 from the fact that in a ball of radius  $R$  the number of lattice points of a lattice with determinant 1 is asymptotically the volume of the ball, when  $R \rightarrow \infty$ .

The next step is to show that for any Borel set  $S \subseteq \mathbf{R}^n$  if  $\text{vol}_n(S)$  is large enough (larger than polynomial in  $n$ )

then with a high probability if we pick a random lattice then the number of lattice points in  $S$  is approximately  $\text{vol}_n(S)$ . Since we know already that the expected value is the correct one we can prove this by estimating the standard deviation of the number of lattice points in  $S$ . To do this we estimate the expected value of the number of pairs of lattice points in  $S$ . More precisely we will take only those pairs which are contained in some basis of the lattice. For any pair of sets  $U, V \subseteq \mathbf{R}^n \setminus \{0\}$  we may consider the expected value of the number of pairs of lattice points  $(u, v)$  (so that there is a basis containing  $u, v$ ) with  $u \in U, v \in V$ . Let  $\kappa(U \times V)$  be this expected value. It is easy to see that  $\kappa$  can be extended into a measure defined on the Borel sets of  $\mathbf{R}^n \times \mathbf{R}^n$  and  $\kappa$  is invariant under multiplication by elements of  $\mathcal{G}_n$ . Using a similar argument than in the case of  $\lambda$ , we get that  $\kappa$  differs from  $\text{vol}_{2n}$  only by a constant factor. (In this case the constant factor is not 1 because of our restriction on the pair  $u, v$  but it will be exponentially close to 1. The word "constant" here means only that the value does not depend on the set where the measures are taken, but it will depend on  $n$ .) From this estimate we get that the standard deviation is so small that the number of lattice points in a large set is almost always close to the expected value.

We may conclude from this that if we have a fixed set  $S \subseteq \mathbf{R}^n$  in a large ball  $B$  then for almost all lattices  $L$  if we take a random lattice point  $x$  from  $B$  then the probability that  $x \in S$  is about the same as the probability that an arbitrary random point of  $B$  is in  $S$ . Based on this we can show that the first element of the basis randomized in Theorem 2 has approximately the same distribution as if we pick a random lattice first and then a random lattice point from the ball with radius  $R$  with uniform distribution.

This is the starting step in an inductive proof where we show that the distribution described in Theorem 2 is approximately the same as the distribution that we get in the following way. First we pick a random lattice  $L$ , then we pick a basis  $d_1, \dots, d_n$  in it recursively so that if  $i < n$  then  $d_i$  is a random point of  $L$  in the ball with radius  $R$  around the origin so that  $d_1, \dots, d_i$  is contained in a basis of  $L$  (and  $d_i$  is uniformly distributed on the set of lattice points with these properties).  $d_n$  is picked with uniform distribution from the lattice points of a parallelepiped defined in the same way as in the theorem.

The general step in the induction can be accomplished in a similar way as the first step, with some additional technical complications. We will have the following situation. We have already selected the first  $k$  element  $d_1, \dots, d_k$  of a basis of a random lattice for some  $1 \leq k < n - 1$ . We will consider now the distribution  $\mu_n$  with the condition that " $d_1, \dots, d_k$  are contained in a basis of  $L$ ". Let  $\mu'$  be this conditional distribution. We show that if  $Z$  is the subspace generated by  $d_1, \dots, d_k$  then for any Borel set  $X \subseteq \mathbf{R}^n$  the expected number of lattice points in  $X \setminus Z$ , where the lat-

tice is picked by  $\mu'$ , is  $\text{vol}_1(X)$ . The proof of this fact is similar to the  $k = 1$  case. Now we consider only the subgroup of  $\mathcal{G}_n$  whose elements leave each  $d_i$  in place. The same argument about invariant measures remains valid. The transfer from expected values to actual values with high probability is more difficult if  $k > \frac{n}{2}$ . (We cannot simply take pairs of sequences of length  $k$  because if  $k > \frac{n}{2}$  the combined sequence of length  $2k$  cannot be linearly independent.) Still with a more careful counting argument it is possible to prove that with high probability the actual value is close to the expected value.

The proof of Theorem 1 is based on Theorem 2. First we consider what can we tell about the path of a fixed element  $w \in \mathbf{R}_n$  that is about the sequence  $w_i = T_i \cdots T_1 w$ . We show that the logarithm of  $\|w_i\|$  performs a random walk on the line with a positive shift and so  $\|w_i\| \rightarrow \infty$ . Estimating more precisely the probabilities in this random walk we can conclude that as long as the shortest vector of the lattice is much shorter than  $\gamma_n$  (the radius of the ball with volume 1) the length of the shortest vector will increase (on the long run), even the rate of increase can be estimated. Therefore after a time with high probability the length of the shortest vector will be close to  $\gamma_n$ . Since this is also true for the dual lattice we get that after a time with high probability the lattice will have a basis of polynomial length. Of course the distribution of such a basis is not necessarily close to the distribution of a basis described in Theorem 2. Still if we start from a polynomial size basis and follow its path we can show that it is getting closer to the required distribution. Unfortunately it is not true that for a fixed basis the path of the basis converges to the required distributions. However if we follow a fixed basis only for a short time, we can show that we are getting closer somewhat to the required distribution while the length of our basis is increasing. Then we pick new shorter basis and repeat the process.

*Proof of Lemma 1.* Assume that each structure in  $\mathcal{S}_n$  is represented by a 0, 1 sequence  $x_0^{(n)}, \dots, x_{k_n}^{(n)}$  where  $k_n = n^c$ . Suppose that for infinitely many integers  $n$  we have e.g.  $\mu_n(x_0^{(n)} = 1) \geq \frac{1}{2}$  and assume that such an  $n$  is fixed. We pick a 0, 1-sequence  $\delta_t, t = 0, \dots, k_n$  by recursion on  $i$  so that  $\delta_0 = 1$  and for all  $t = 1, \dots, k_n$  we have  $\mu_n(x_0 = 1 \wedge x_t = \delta_t \wedge \bigwedge_{j=1}^{t-1} x_j = \delta_j) \geq \mu_n(x_0 = 1 \wedge x_t = 1 - \delta_t \wedge \bigwedge_{j=1}^{t-1} x_j = \delta_j)$ , that is, we always pick  $\delta_t$  from the two possibilities so that the initial sequence  $\delta_0, \dots, \delta_t$  get the greater probability. The nontriviality of the sequence  $\mu_n$  implies that there is a  $0 < \alpha < 1$  so that for an infinite number of integers we have  $\mu_n(x_0 = \delta_0^{(n)} \wedge \dots \wedge x_{k_n} = \delta_{k_n}^{(n)}) < \alpha$ . For such an integer  $n$  let  $t_n$  be the smallest integer so that  $\mu_n(x_0 = \delta_0^{(n)} \wedge \dots \wedge x_{k_n} = \delta_{t_n}^{(n)}) < \alpha$ . The minimality of  $t_n$  implies that  $\mu_n(x_0 = \delta_0^{(n)} \wedge \dots \wedge x_{k_n} = \delta_{t_n}^{(n)}) > \frac{\alpha}{2}$  (since  $x_{t_n}$  has only two possible values). Therefore the 0-1 law does not hold for the property  $P_n \equiv$

$\delta_0^{(n)} \wedge \dots \wedge x_{k_n} = \delta_{t_n}^{(n)}$ . As we defined  $P_n$  it is definable by a polynomial size circuit but it is not necessarily p.t.c. since the sequence  $\delta_0, \dots, \delta_{k_n}$  may not be p.t.c. However if we change the defining inequality of  $\delta_t$  into  $\mu_n(x_0 = 1 \wedge x_t = \delta_t \wedge \bigwedge_{j=1}^{t-1} x_j = \delta_j) \geq -n^{-c-1} + \mu_n(x_0 = 1 \wedge x_t = 1 - \delta_t \wedge \bigwedge_{j=1}^{t-1} x_j = \delta_j)$  then the sequence  $\delta_i, i = 1, \dots, k_n$  is p.t.c. (although it is not necessarily unique.) This completes the proof of Lemma 1.

## References

- [1] M. Ajtai, *Generating Hard Instances of Lattice Problems*, In Proc. of 28th ACM STOC 1996 or Electronic Colloquium on Computational Complexity, 1996, <http://www.eccc.uni-trier.de/eccc/>
- [2] M. Ajtai *The Complexity of the Pigeonhole Principle*, *Combinatorica* 14 (4), (1994) 417-433. 1993.
- [3] M. Ajtai and C. Dwork *In A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence*, In Proc. of 29th ACM STOC 1997 or Electronic Colloquium on Computational Complexity, 1996, <http://www.eccc.uni-trier.de/eccc/>
- [4] K. J. Compton *0-1 laws in logic and combinatorics*, In *Nato Adv. Study Inst. on Algorithms and Order*, Ed. I. Rival. D. Reidel, 1988, pages 353-383.
- [5] R. Fagin, *Probabilities on Finite models*, *Journal of Symbolic Logic*, 41, 1, March 1976, pp. 50-58.
- [6] H. Federer *Geometric measure theory*, Section 2.7, Springer, 1969, (Grundlehren der mathematischen Wissenschaften; Vol. 153).
- [7] M. Foreman. *Generic Large Cardinals: New Axioms for Mathematics?* In Proc. International Congress of Mathematicians, Vol. II, pages 11-23, 1998.
- [8] P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers*, Chapter 3. North Holland 1987.
- [9] T. Jech. *Set Theory*, Academic Press, 1978.
- [10] P. G. Kolaitis and M. Vardi, *0-1 Laws for Fragments of Existential Second-Order Logic: A Survey*. In MFCS 2000. Lecture Notes in Computer Science 1893, Springer 2000, ISBN 3-540-67901-4, pp. 82-89.
- [11] A. K. Lenstra, H. W. Lenstra, L. Lovász *Factoring polynomials with rational coefficients*, *Math. Ann.* 261, 515-534 (1982).
- [12] J. H. Lutz, E. Mayordomo, *Cook versus Karp/Levin: separating completeness notions in if NP is not small*. *Theoretical Computer Science*, 164 (1996), pp. 141-163.