Electronic Colloquium on Computational Complexity, Report No. 61 (2002)

A conjectured $0-1$ law about the polynomial time computable properties of random lattices, I.

Preliminary Version

Miklós Ajtai
IBM Almaden Research Center

Correction. In the FOCS'02 paper of the author (see [3]) the formulations of both conjectures contained trivial errors, which made the conjectures trivially false. In this paper we correct these errors.

Abstract. A measure μ_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. μ_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 on a lattice point by point. Our main goal is to formulate a conjectured $0-1$ law about μ_n. In the second part of the paper we will also give a method for generating a random lattice with the distribution μ_n. As we will see, there are many known and proven $0-1$ laws concerning random structrues, but they are valid for a much smaller set of properties, e.g. first-order definable properties. The infinite sequence $\langle P_n \mid , n = 1, 2, \ldots \rangle$ 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, $n = 1, 2, \ldots$ 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 if the integer n is sufficiently large then the probability $\mu_n(P_n)$ is either close to 0 or close to 1. More precisely we have $\lim_{n\to\infty} \max\{\mu_n(P_n), \mu_n(\neg P_n)\} = 1$. 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 belive 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.

Remark In the FOCS'02 paper of the author ([3]) the conjecture mentioned in the abstract has been formulated. This formulation contains an error. Namely instead of

ISSN 1433-8092

$\lim_{n\to\infty} \max\{\mu_n(P_n), \mu_n(\neg P_n\} = 1$ (as stated in the present abstract) it said "either $\lim_{n\to\infty}(P_n) = 1$ or $\lim_{n\to\infty}(P_n) = 0$". This is trivially false for the property P_n which holds for all lattices if n is even and does not hold for any if n is odd. The FOCS'02 paper also describes connections of the stated conjecture with conjectures of axiomatic set theory and gave methods for generating the distribution of the random lattices. In this part of the paper we describe the statement of the conjecture and the mathematical problems related to it in greater detail. We will deal with the other two topics in the second part of this paper. In the FOCS paper a stronger version of the conjecture, Conjecture 2 was also formulated (with the same error). The definition of a polynomial time computable property for Conjecture 2 was missing from the paper. Here we give the complete definition. (The definition used for Conjecture 1 is not applicable because in this case it makes the error term larger than the main term.)

Introduction. Definition. If $a_1, ..., a_n \in \mathbf{R}^n$ are linearly independent vectors then the set of all of their linear combinations with integer coefficients is a lattice. $a_1, ..., a_n$ is a basis of the lattice (if $n > 1$ then a lattice has many different bases). If L is a lattice then the determinant of L, that is, $\det(L)$ is the absolute value of the determinant of the matrix whose columns are $a_1, ..., a_n$ where $a_1, ..., a_n$ is an arbitrary basis of L.

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

Random structures has a useful role in theoretical computerscience and in many branches of mathematics. There are several examples where with probabilistic methods we are able to construct structures with certain desirable properties but there is no known explicit construction for the same task. Nonconstructive proofs were known in mathematics for a long time. E.g. Dirichlet's theroems about simultaneous Diophantine approximation or Minkowski's convex body theorem about the existence of lattice points are based on the Pigeonhole principle and so they do not give a method of constructing the object whose existence has been proved. Another example from the theory of lattices is Mahler's proof of the Minkowski-Hlawka theorem [9] about the existence of lattices that do not contain points from certain sets. This example is especially important for us because for the proof Mahler has introduced a measure μ_n defined on the Borel measurable subsets of $\texttt{lattice}_n$, where $\texttt{lattice}_n$ is the set of all lattices in $\mathbf{R}^n$ whose determinant is 1. He proved essentially (in the form of an averageing argument) that the set of lattices with the desirable property has a nonzero measure. μ_n is a measure defined on the Borel measurable subsets on $\texttt{lattice}_n$, with the following properties:

(1) it is invariant under linear transformations with determinant ± 1,

(2) each compact set has a finite measure, and

(3) for any Borel set B we have $\mu_n(B) = \sup\{\mu_n(C) \mid C \subseteq B \text{ and } C \text{ is compact }\}$ and $\mu_n(B) = \inf\{\mu_n(G) \mid B \subseteq G \text{ and } G \text{ is open }\}$.

(In other words μ_n is a regular Borel measure.) Moreover μ_n is unique with these properties apart from a constant factor. We will show later that there is a natural topology on the set of lattices. The Borel sets are the elements of the smallest σ-algebra consisting of subsets of $\mathtt{lattice}_n$ which contains all of the closed sets according to this topology. A measure μ is invariant under linear transformations with determinant ± 1 if for every Borel set $X \subseteq \mathtt{lattice}_n$ and for every linear transformation A on $\mathbf{R}^n$ with determinant ± 1, we have $\mu(X) = \mu\{AL \mid L \in X\}$, where for each lattice L, $AL = \{Av \mid v \in L\}$. This invariance property and μ_n's uniqueness with respect to it means that μ_n is not only a possible measure on the set of lattices, but it is *the* natural measure on them in the same sense as the n-dimensional volume (i.e. the Lebesgue measure) is the natural measure on $\mathbf{R}^n$.

Mahler also proved that $\mu_n(\mathtt{lattice}_n) < \infty$, so $\mu_n(\mathtt{lattice}_n)^{-1}\mu_n$ is a probability measure, however this measure was not investigated from a probabilistic point of view. (In the follwing μ_n will denote the probability measure.) The systematic use of probabilistic notions for proving existence theorems was introduced by Erdős for combinatorial problems and lead to the solution of many problems both in combinatorics and in other fields. In particular in theoretical computerscience the technique of probabilistic construction is widely used and it is closely connected to the notion of probabilistic algorithm. This and the existence of many unsolved algortihmic questions about lattices would in itself be sufficient motivation to investigate μ_n as a probability measure from an algorithmic point of view. E.g. we can ask whether a random lattice with the distribution μ_n can be generated algorithmically in polynomial time (as we will see the answer is yes), then we may also ask what are the properties of a random lattice in the same sense as Erdős and Rényi studied the properties of a random graph. Our conjecture says that this second question has a surpsirsing answer namely for each $\varepsilon > 0$ and for each fixed property which can be tested by a polynomial time algortihm if n is sufficiently large then the property holds either with a probability of at least $1 - \varepsilon$ or with a probability less than ε (the choice of the two possiblities may depend on n). This type of phenomenon for first-order definable properties on certain random structure has been known and studied in great detail for a long time as we describe it below. (In the case of first-order definability the an even stronger statement is true, namely the fact whether the probability is close to 0 or 1 does not depend on n.) Before we describe the known $0-1$ laws we note only that the exact formulation of the conjecture, namely what is a polynomial time coputable property for lattices is not easy. We have to deal with three different and probably unavoidable

difficulties.

(1) a latttice is usually presented by a basis, however a lattice has many different bases and to decide whether a property holds or not can be easy starting from one bases and difficult starting from another. We avoid this problem by defining a property as polynomial time computable if there is an algorithm which if gets a lattice L represented by *any* basis (which consists of not too long vectors), is able to decide with high probability whether L has the property or not.

(2) the points of a lattice and so the basis vectors as well which represent the lattice are points $\mathbf{R}^n$, therefore they are sequences of real numbers and each real number is an infinite sequence of bits so it cannot be an input of a polynomial time algorithm. We use here a well-known solution, that is, we consider each real number as an oracle which gives an approximation of the real number α with precision 2^i to the algorithm at a cost i (counted in the time of the algorithm). A consequence of this solution is that in any fixed algorithm we use only a polynomial number of bits of the real numbers used in the representation of the input lattice. This seems to indicate that we actually do not need real numbers and perhaps we can reformulate the conjecture speaking about lattices with integer or rational points. As we will prove later this is not possible.

(3) We cannot expect that an algorithm will decide for all lattices whether a property P holds or not. This is again a consequence of the fact that the lattices are defined over the reals and so two lattices one with P the other with $\neg P$ can be arbitrary close to eachother. Therefore getting the lattice only with a finite precision may not be enough. In fact our representation of lattices with an arbitrary basis, as described in (1), implies that for every nontrivial property P there is no polynomial time algorithm which decides whether P holds or not for every L. Moroever an algorithm may give different answers for the same lattice if it is presented with different bases. Therefore our final definition of what is a property and an algorithm which tests it in polynomial time will be a probabilistic one which takes into account the mentioned error possibilities in a quantitative sense.

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 φ in the language of graphs let $p(\varphi, n)$ be the probability that φ holds on the random graph on n vertices. Ron Fagin has proved (see [6]) in a more general form that for any fixed first-order formula φ either $\lim_{n\to\infty} p(\varphi, n) = 0$ or $\lim_{n\to\infty} p(\varphi, n) = 1$, that is, the $0-1$ law holds for the first-order properties of random graphs. The theorem gives a surpirsingly 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 [11], [5]).

From the point of view of constructing graphs (or other structures) with interesting porperties, 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 conjecture 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.c. properties (although in a somewhat weaker sense, since the fact whether the probability is close ot 0 or close to 1 mat depend on n). 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) wich will have a nontrivial distribution. Actually, as we will prove later, if each structure has a unique polynomial size reperesentation which can be computed in polynomial time from the representation used by the algorithm then there is no $0-1$-law for p.t.c. properties. This excludes the existence for such a $0-1$-law for most of the well-studied classes of random structures and also for lattices over the integers or rationals.

The conjecture has a motivation in measure theory, more presisely an analogy with the axiom of the existence of a measurable cardinal, as we will describe it in the second part of the paper. J. H. Lutz and E. Mayordomo fomulated a conjecture, implying $P \neq NP$, which also has a measure theoretic motivation although in a somewhat different sense, see [13]).

The statement of the conjecture. In this section we give the necessary definitions for the formulation of the conjectured $0-1$-law. We describe the complete definition of the measure μ_n, still, to show that this really defines a measure and especially to show that $\mu_n(\texttt{lattice}_n)$ is finite, requires some extra work. This is described e.g. in [9] but to make the paper more self-contained we will also give the proofs

of these facts in the last section. Some of the definitions were already given in the introduction but we repeat them here.

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 $a_1, \ldots, a_n \in \mathbf{R}^n$ so that for all $x \in L$ there are integers $\alpha_1, \ldots, \alpha_n$ with $x = \sum_{i=1}^n \alpha_i a_i$. A linearly independent system of vectors $a_1, \ldots, a_n$ with the described property will be called a basis of L. The absolute value of the determinant whose columns are $a_1, \ldots, a_n$, where $a_1, \ldots, a_n$ 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 $a_1, \ldots, a_n$. We will denote the set of all n dimensional lattices whose determinant is one by $\mathtt{lattice}_n$.

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 μ_n.

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

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

We will define a topology on $\mathtt{lattice}_n$ and our measure will be defined on the Borel sets of this topological space. The set $\mathtt{basis}_n$ has a toplogy on it induced by the topology of $\mathbf{R}^{n^2}$. (We get all of the open sets in the form $\mathtt{basis}_n \cap H$ where H is an open set of $\mathbf{R}^{n^2}$.) This induces a toplogy on $\mathtt{lattice}_n$, namely $G \subseteq \mathtt{lattice}_n$ will be open iff $\psi^{-1}(G)$ is open in $\mathtt{basis}_n$. (In the last section of this part of the paper we describe this topology and its most important properties in greater detail.) The Borel sets of $\mathtt{lattice}_n$ are the elements of the smallest σ-algebra on $\mathtt{lattice}_n$ which contains all closed subsets. It is easy to see that a $B \subseteq \mathtt{lattice}_n$ is a Borel set iff $\psi^{-1}(B)$ is a Borel set of $\mathtt{basis}_n$ (or of $\mathbf{R}^{n^2}$).

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

1. If $V \subseteq \mathbf{R}^n$ then V° will denote the set of all vectors γv 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 $\mathtt{vol}_n$. (This is the the Lebesgue measure restricted to the σ-algebra of Borel sets. The Lebesgue measure itself is defined on a larger σ-algebra, the σ-algebra of the Lebesgue measurable sets. Each Lebesgue measurable set X can be written int he form of $X = Y \Delta S$ (symmetric difference), where Y is Borel measurable and

$S \subseteq Z$ for a suitably chosen Borel measurable set Z with $\mathtt{vol}_n(Z) = 0$. In this case the Lebesgue measure of X is $\mathtt{vol}_n(Y)$.)

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

It is easy to see that ρ_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 $A \subseteq \mathtt{basis}_n$ is a Borel set, then $\rho_n(TA) = \rho_n(A)$. (Here we apply T to A point by point and for each $a = \langle a_1, \ldots, a_n \rangle \in \mathtt{basis}_n$, $Ta = \langle Ta_1, \ldots, Ta_n \rangle$.) The reason for the equality $\rho_n(TA) = \rho_n(A)$ is that A acts on the elements of $\mathtt{basis}_n$ 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 ± 1.

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

Since a lattice has infinitely many different bases, $\psi^{-1}(L)$ is an infinite set for each $L \in \mathtt{lattice}_n$. For the definition of the measure μ_n we select an element $\varphi(L)$ of $\psi^{-1}(L)$ arbitrarily for each $L \in \mathtt{lattice}_n$. In other words $\varphi(L)$ is a basis of L. There are an infinite number of functions φ 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 $\varphi(L) = \langle a_1, \ldots, a_n \rangle$ meets this requirement. We define a_i by recursion on i. Assume that $a_1, ..., a_{i-1}$ has been already defined with the property that there is at least one basis of L containing $a_1, ..., a_{i-1}$. a_i will be a vector in the lattice L so that there is at least one basis of L containing $a_1, ..., a_i$ and a_i is of minimal length with this property. If there are more than one such vector then a_i will be the smallest according to lexicographic ordering.

Definition. If A is a Borel subset of $\mathtt{lattice}_n$ then let $\tilde{\mu}_n(A) = \rho_n(\varphi(A))$. (It is easy to see that $\tilde{\mu}_n(\mathtt{lattice}_n) > 0$.) Finally let $\mu_n(A) = (\tilde{\mu}_n(\mathtt{lattice}_n))^{-1}\tilde{\mu}_n(A)$.

We will show that $\tilde{\mu}_n$ is a measure on the Borel sets of $\mathtt{lattice}_n$ and $\tilde{\mu}_n$ does not depend on the choice of the function φ with the mentioned properties. We will also show that that $\tilde{\mu}_n(\mathtt{lattice}_n) < \infty$. Actually there is an explicit formula for $\tilde{\mu}_n(\mathtt{lattice}_n)$ (see [9]). The inequality $\tilde{\mu}_n(\mathtt{lattice}_n) < \infty$ implies that μ_n is a probability measure defined on the Borel sets of $\mathtt{lattice}_n$. The most important property of this measure is the following: *if T is a linear transformation with determinant ± 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 $TA = \{TL \mid L \in A\}$.) This property easily follows from the corresponding property of ρ_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 μ_n is not satisfactory from a computational point of view. (E.g. there is no known p.t.c. choice for the function φ). In the second part of the paper we will give an equivalent definition which can be used

for generating a random lattice with the distribution μ_n in polynomial time.

Definitions. 1. If $L \subseteq \mathbf{R}^n$ is a lattice and $a_1, \ldots, a_n$ is a basis of L then the length of the basis $a_1, \ldots, a_n$ 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 α, $0 \leq \alpha < 2$ is given as an infinite sequence of rationals $r_0, r_1, \ldots, r_k, \ldots$ 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 α 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 β is represented by a pair $\langle \beta_0, \beta_1 \rangle$, where $\beta = \beta_0 + \beta_1$, β_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 β_1 from an interval of length 2, instead of the interval $[0, 1)$, is that this way β_0 can be selected even if only an approximation of β is known.) This way, in time polynomial in k, we can get an approximation of β with a precision of $2^{-k}(|\beta|+1)$. Conversely if we are able to compute an approximation of β in polynomial time then we are also able to compute the corresponding initial segment of a representation. If a sequence of real numbers $\alpha_1, \ldots, \alpha_i$ is given as input then α_j is given on the cells $j+ti$, $t = 1, 2, \ldots$. 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. When we say that a Turing machine solves a problem with a given input containing real numbers we mean that it solves the problem with each of the possible representations of the real numbers in the input.

3. Suppose that $\mathbf{P} = \langle P_n \mid n = 1, 2, \ldots \rangle$, is a property of lattices with determinant 1. (That is, $P_n \subseteq \mathtt{lattice}_n$). 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 μ_n, then for any basis $a_1, \ldots, a_n$ of L with length less than 2^n if T gets n, c', $a_1, \ldots, a_n$ 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* $\mathbf{P} = \langle P_n,\ n = 1, 2, \ldots \rangle$ *is a p.t.c. lattice property. Then* $\lim_{n\to\infty} \max\{\mu_n(P_n), \mu_n(\neg(P_n))\} = 1$, *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 then $\alpha(n)$ is about $\frac{1}{2}$. If this porperty 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 then 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 mathamatical 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. [12]). 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 then 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 $S \subseteq \mathbf{R}^n \backslash \{0\}$ let p_S be the probability that a random lattice with distribution μ_n has a point in S. We will 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 of 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 to be very difficult and probably different proofs for each of sets S. The assumption $\mathtt{vol}_n(S) = 1$ can be substituted by $n^{-c} \leq \mathtt{vol}_n(S) \leq n^c$.

Random structures without $0-1$-laws for p.t.c. properties. In this section we show that if each structure has a p.t.c. unique representation then there is no $0-1$-law for p.t.c. properties.

Definitions. 1. Suppose that for each n, $\mathcal{S}_n$ is a set of structures and ν_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 ν_n, that is, given n as an input it provides structure $S \in \mathcal{S}_n$ as an output with probability $\nu_n(\{S\})$. In this case we will say that ν_n is a p.t.c. distribution on the set of the uniquely represented structures $\mathcal{S}_n$, $n = 1, 2, \ldots$. We will call the sequence of measures ν_n trivial if there is a seqeunce of structures X_n, with $X_n \in S_n$, so that $\lim_{n\to\infty} \nu_n(X_n) = 1$. (In other words ν_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 $\mathcal{S}_n$, $n = 1, 2, \ldots$ 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 $\lim_{n\to\infty} \max\{\nu_n(P_n), \nu_n(\neg P_n)\} = 1$ then we say that the $0-1$ law holds for property P_n, $n = 1, 2 \ldots$

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

Before we start the proof we describe a consequence of this lemma which are important from our point of view.

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 ith 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.

This is the reason why we gave our probability distribution on lattices whose points are arbitrary vectors in $\mathbf{R}^n$. This caused a substantial complication in the way of presenting lattices (we had to deal with the representations of real numbers), however the lemma 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, we will use a rational approximation of the basis, however such an approximation will not determine the lattice uniquely.

Proof of Lemma 1. Assume that each structure in $\mathcal{S}_n$ is represented by a $0,1$ sequence $x_0^{(n)}, \ldots, x_{k_n}^{(n)}$ where $k_n = n^c$. Suppose that for infinitely many integers n we have e.g. $\nu_n(x_0^{(n)} = 1) \geq \frac{1}{2}$ and assume that such an n is fixed. We pick a $0,1$-sequence δ_t, $t = 0, \ldots, k_n$ by recursion on i so that $\delta_0 = 1$ and for all $t = 1, \ldots, k_n$ we have $\nu_n(x_0 = 1 \wedge x_t = \delta_t \wedge \bigwedge_{j=1}^{t-1} x_j = \delta_j) \geq \nu_n(x_0 = 1 \wedge x_t = 1 - \delta_t \wedge \bigwedge_{j=1}^{t-1} x_j = \delta_j)$, that is, we always pick δ_t from the two possibilities so that the initial sequence $\delta_0, \ldots, \delta_t$ get the greater probability. The nontriviality of the sequence ν_n implies that there is a $0 < \alpha < 1$ so that for an infinite number of integers n we have $\nu_n(x_0 = \delta_0^{(n)} \wedge \ldots \wedge x_{k_n} = \delta_{k_n}^{(n)}) < \alpha$. For such an integer n let t_n be the smallest integer so that $\nu_n(x_0 = \delta_0^{(n)} \wedge \ldots \wedge x_{k_n} = \delta_{t_n}^{(n)}) < \alpha$. The minimality of t_n implies that $\nu_n(x_0 = \delta_0^{(n)} \wedge \ldots \wedge x_{t_n} = \delta_{t_n}^{(n)}) > \frac{\alpha}{2}$ (since x_{t_n} has only two possible values). Therefore the $0-1$ law does not hold for the property $P_n \equiv (x_0 = \delta_0^{(n)} \wedge \ldots \wedge x_{t_n} = \delta_{t_n}^{(n)})$. As we defined P_n it is definable by a polynomial size circuit but it is not necessaryly p.t.c. since the sequence $\delta_0, ..., \delta_{k_n}$ may not be p.t.c. However if we change the defining inequality of δ_t into $\nu_n(x_0 = 1 \wedge x_t = \delta_t \wedge \bigwedge_{j=1}^{t-1} x_j = \delta_j) \geq -n^{-c-1} + \nu_n(x_0 = 1 \wedge x_t = 1 - \delta_t \wedge \bigwedge_{j=1}^{t-1} x_j = \delta_j)$ then the suequence δ_i, $i = 1, \ldots k_n$ is p.t.c. (although it is not necessarily unique.) This completes the proof of Lemma 1.

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, besause 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 wich 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 then polynomial. This would mean that we are working with rational lattices but there may not be a 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 μ_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 the 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 refering 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 μ_n.

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

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 $\mathtt{vol}_n(H)$. 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 precisley 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 $\mathbf{R}^n \backslash G$ is smaller that $2^{-n^{c'}}$. (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. We will prove this lemma in the second part of the paper.

Stronger versions of the conjecture. In the definition of a p.t.c. lattice property we allowed a polynomial size error in the choice of lattices. That is, we required only that the algorithm produces a good answer with the exception of a set of lattices S, where $\mu_n(S)$ could be as large as n^{-c} for some large constant c. A consequence of this is that if a lattice property P_n holds only on a smaller set then the algorithm which always says that the property does not hold makes P_n p.t.c. in spite of the fact that it does not give any information about it. E.g. if $P_n \equiv$"the shortest nonzero vector is of length at most 1" then $\mu_n(P_n)$ is about $e^{-\frac{1}{2}n \log n}$. So according to our original definition the property P_n is p.t.c. The new definition will take into account the size of the set, more precisely the probability of an erroneous answer for lattices with propety P_n resp. $\neg P_n$ must be small compared $\mu(P_n)$ resp $\mu_n(\neg P_n)$. We formulate a conjecture with this modified notion of p.t.c. property. This conjecture will be stronger in the sense that it says something about properties which are satisfied only on an exponentially small set.

Definition. Suppose that $\mathbf{P} = \langle P_n \mid n = 1, 2, \ldots \rangle$, is a property of lattices with determinant 1 and for each $n = 1, 2, ...$, $P_n \subseteq \mathtt{lattice}_n$ is a Borel set. We say that $\mathbf{P}$ is p.t.c. with small relative error 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 μ_n then for any basis $a_1, \ldots, a_n$ of L with length less than 2^n if T gets $n, c', a_1, \ldots, a_n$ as input then in time n^c it provides an output x so that the following holds:

(1) with the condition $L \in P_n$ we have that with a probability of at least $(1 - n^{-c'})\mu(P_n)$ for the randomization of L and the randomization in T the output is $x = 1$.

(2) with the condition $L \notin P_n$ we have that with a probability of at least $(1 - n^{-c'})\mu(\neg P_n)$ for the randomization of L and the randomization in T the output is $x = 0$.

Conjecture 2 *Suppose that* $\mathbf{P} = \langle P_n \text{ — } n = 1, 2, \ldots \rangle$ *is a lattice property which is polynomial time computable with small relative error. Then* $\lim_{n\to\infty} \max\{\mu_n(P_n), \mu_n(\neg(P_n)) = 1$. *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.

The definition of polynomial time property in Conjecture 2 seems somewhat less natural than in Conjecture 1 because of the two different types of errors. However we can reformulate the conjecture in a stronger form which avoids this asymmetry. In the earlier definitions we assumed that the lattice is presented with an arbitrary basis B of length 2^n. It is easy to see that starting from an arbitrary basis B of L of length at most 2^n we are able to generate in polynomial time a distribution D_L on the set of bases of L whose length is at most 2^{2n} so that D_L does not depend on B. (This is a consequence of the fact that we are able to pick a random lattice point from a cube of size 2^{2n} with uniform distribution.) When we reformulate the conjecture we assume that such a distribution D_L is fixed and the lattice L is now always presented by a random basis chosen by distribution D_L. In a similar way we assume that in the reperesentation of each real number included in the input, the approximating rationals are chosen according to a fixed distribution (which can be generated in polynomial time from an arbitrary representation of the real number). In both cases we cannot expect that the distributions in question can be generated exactly, we will assume that the error (that is, the maximal distance of the various generated distributions from eachother) is less than e^{-n^2}.

Definition. Assume that a $c > 0$ and probabilistic Turing machine T is fixed so that for each positive integer n if T gets n and a lattice $L \in \texttt{lattice}_n$ as an input then it always returns a $0-1$ output in time at most n^c. For a lattice $L \in \texttt{lattice}_n$ let $p_{L,T}$ be the probability that if T gets as input the lattice L, (presented by a random basis as described above) then the ouput of T is 1, where the probability is taken together for the randomization of the representation of L and for the randomization in T. For each real number $\alpha \in [0, 1]$ let $S_{\alpha,T}$ be the set of all lattices $L \in \texttt{lattice}_n$ so that $p_{L,T} \leq \alpha$.

Conjecture 3 *Suppose that* c_1 *is a positive integer and* T *is a Turing machine which, given* n *and an* n*-dimensional lattice* L *with a basis of length at most* 2^{2n} *as an input, always returns a* $0-1$ *output in time* n^{c_1}. *Then for all* $c_2, c_3 > 0$ *and for all sufficiently large* n *the following holds:*

If $\alpha, \beta \in (0,1)$ *so that* $\alpha + n^{-c_2} \leq \beta$ *then either* $\mu_n(S_{\alpha,T}) \leq e^{-c_3 n \log n}$ *or* $\mu_n(S_{\beta,T}) \geq 1 - e^{-c_3 n \log n}$.

We show that Conjecture 3 implies Conjecture 2. Indeed if Conjecture 2 does not hold then there is a lattice property $\mathbf{P} = \langle P_n \mid n = 1, 2, ... \rangle$ and an infinite set X of integers so that for all $n \in X$, P_n is polynomial time computable with small relative error, by the Turing machine T. This implies that if $\alpha = \frac{1}{2}$ and $\beta = \frac{1}{2} + n^{-c_2}$ then the requirements of Conjecture 3 are violated by, T if c_1, c_2, c_3 are sufficiently large.

Remarks. 1. It is not clear whether there is a proof of "Conjecture 2 implies Conjecture 3". (Of course if both conjectures are true then the implication holds.) The answer is probably "no" since in Conjecture 3 the Turing machine works only for a fixed time n^{c_1}.

2. We may replace the expression $e^{-c_3 n \log n}$ at both places in the conclusion of the conjecture by n^{-c_3}. We get a conjecture which implies Conjecture 1. Again we don't know whether the implication in the other direction can be proved

We describe below briefly some cryptographic consequences of Conjecture 2. We will give a more detailed account in a separate paper. 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 as we will show in the second part of this paper for any $r > 0$ the probability that in a random lattice $L \in \texttt{lattice}_n$ there is a nonzero lattice point in the 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 and γ_n is the radius of the n dimensional ball with volume 1. 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 λ_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 then $e^{-c' n \log n}$ for some $c' > 0$. Therefore the property "the approximated value of L provided by $\mathcal{A}$ is greater than r" does not statisfy 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 approximtate the length of the shortest nonzero vector upto a polynomial factor even if we restrict our attention to lattices where the

shortest nonzero vector is unique upto a polynomial factor. This also implies that it is not possible to find the nonzero 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 λ if for all lattice vector u, $\|u\| \leq \lambda\|v\|$ implies that u and v are parallel.) Moreover form 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 [4].) 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 μ_{n-1} in the hyperplane H (whose shortest vector will be of length about γ_{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 wich has edges pointing from x to $x + a_1, ..., x + a_{n-1}$, where $a_1, ..., a_{n-1}$ is a basis of L_1. L will be the lattice whose basis is $a_1, ..., a_n$. 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 [4] where a lattice is needed with the properties of L_1. In [4] 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.

Topology on the set of lattices. In this section we describe the properties of the natural toplogy on the set of lattices. To make the picture more complete we will consider also lattices whose determinant is not 1. Actually, as we have seen already, this helps in the definition of the measure μ_n.

Definitions. $\mathcal{L}_n$ will denote the set of all lattices $L \subseteq \mathbf{R}^n$. $\mathcal{B}_n$ will denote the set of all linearly independent sequence of vectors $a_1, ..., a_n$ so that $a_i \in \mathbf{R}^n$ for $i = 1, ..., n$. In other words $\mathcal{B}_n$ is the set of all possible bases for n dimensional lattices. (According to our earlier definition $\mathtt{basis}_n \subseteq \mathcal{B}_n$ is the set of all bases for lattices with determinant 1.)

According to our definitions the elements of $\mathcal{B}_n$ and $\mathtt{basis}_n$ are sequences of length n whose elements are n-dimensional vectors. We may identify such a sequence $a_1, ..., a_n$ with the $n \times n$ matrix, whose ith column is a_i. This way each basis uniquely defines an invertable $n \times n$ matrix over $\mathbf{R}$ and conversely the columns of each invertable matrix from a basis of a lattice.

Definition. $\mathcal{G}_n$ will be the group of all invertible n by n matrices whose entries are real numbers, $\mathcal{S}_n$ will be the subgroup of $\mathcal{G}_n$ consisting of the matrices with determinants ± 1, and $\mathcal{Z}_n$ will be the subgroup of $\mathcal{S}_n$ consisting of all matrices in $\mathcal{S}_n$ which have only integer entries. (So we have $\mathcal{Z}_n \subseteq \mathcal{S}_n \subseteq \mathcal{G}_n$.)

According to our earlier remark we will identify $\mathcal{B}_n$ with $\mathcal{G}_n$ and $\mathtt{basis}_n$ with $\mathcal{S}_n$. In the definition of a lattice we represented a lattice as a subset of $\mathbf{R}^n$. Our identification of a basis with an element of the group $\mathcal{G}_n$ provides an alternative representation which makes it easier to define topolgy and measure on sets of lattices. Namely we can represent the lattice L as the set of set of all elements in $\mathcal{G}_n$ whose columns form a basis of L. Suppose that $U, V \in \mathcal{G}_n$ are two bases of the same lattice L. Then there is a $Z \in \mathcal{Z}_n$ so that $U = VZ$. This is the consequence of the fact that any two bases of the same lattice can be transformed into eachother by a linear transformation with integer entries and with determinant ± 1. We have that $U, V \in \mathcal{G}_n$ are the bases of the same lattice iff they are in the same left-coset of the subgroup $\mathcal{Z}_n$. Therefore each lattice L, that is, every element of $\mathcal{L}_n$ is represented by a left-coset of the subgroup $\mathcal{Z}$ in the group $\mathcal{G}_n$, and in a similar way every element of $\mathtt{lattice}_n$ can be uniquely represented as a left coset of $\mathcal{Z}_n$ in $\mathcal{S}_n$.

Remark. The reason why we have left-cosets and not right-cosets is that the basis vectors are columns and not rows of the matrix representing the basis. It is important that if the matrix B is a basis of the lattice L then multiplying it from the right or

left act differently on the corresponding lattices. Namely if A is an invertible linear transformation then AB will be the basis of a lattice $AL = \{Ax \mid x \in L\}$, that is, we apply A on the lattice point by point. On the other hand BA will be a lattice which has a basis that we get from the basis B by taking linear combinations of the basis elements, where the coefficients for each new basis element, with respect to the old basis, form a column of the matrix A.

The coset representation of lattices motivates the following definition.

Definitions. 1. The set of left cosets of the subgroup $\mathcal{Z}_n$ in $\mathcal{G}_n$ will be denoted by $\mathcal{L}_n^c$. The one-to-one map of $\mathcal{L}_n$ onto $\mathcal{L}_n^c$ which takes every lattice L into the corresponding coset of $\mathcal{Z}_n$ will be denoted by ξ_n. We will denote by $\mathtt{lattice}_n^c$ the set of all left-cosets of the subgroup $\mathcal{Z}_n$ in $\mathcal{S}_n$. ξ restricted to $\mathtt{lattice}_n$ is a one-to-one map of $\mathtt{lattice}_n$ onto $\mathtt{lattice}_n^c$. (Since both $\mathcal{L}_n$ and $\mathcal{L}_n^c$ are essentially the set of lattices it seems tempting to simply consider the two sets as identical. However this would create a confusion since each $L \in \mathcal{L}_n$ is a set of points in $\mathbf{R}^n$ while each $L \in \mathcal{L}_n^c$ is a set of n by n matrices.)

2. If $V \in \mathcal{G}_n$ then $\Psi_n(V) \in \mathcal{L}_n$ will denote the lattice whose basis consists of the columns of V, while $\psi_n(V)$ will denote the coset representation of the same lattice. That is, $\psi_n(V) = \xi(\psi_n(V))$. According to the definition of the coset representation we also have $\psi_n(V) = V\mathcal{Z}_n$.

3. If f is an arbitrary function defined on a set X and $Y \subseteq X$ then $f''(Y)$ will denote the set $\{f(y) \mid y \in Y\}$.

4. $\mathcal{G}_n$ is a topological space with respect to the topology induced by the Euclidean topology of $\mathbf{R}^{n^2}$. In fact $\mathcal{G}_n$ is an open subset the n^2 dimensional Euclidean space. As a consequence a set G is open in $\mathcal{G}_n$ iff it is open in $\mathbf{R}^n$. $\mathcal{L}_n^c$ is a topological space with repsect to the factor topology, that is, the strongest topology so that the canonical map of $\mathcal{G}_n$ onto $\mathcal{L}_n^c$ is continuous. In other words a set $H \subseteq \mathcal{L}_n^c$ is open in $\mathcal{L}_n^c$ iff $\psi_n^{-1}(H)$ is open in $\mathcal{G}_n$. We will always consider this topology on $\mathcal{L}_n^c$. On $\mathcal{L}_n$ we will always consider the unique topology so that ξ is a homeomorohism between $\mathcal{L}_n$ and $\mathcal{L}_n^c$.

5. Since $\mathtt{lattice}_n^c \subseteq \mathcal{L}_n^c$ the topolgy on $\mathcal{L}_n^c$ induces a topolgy on $\mathtt{lattice}_n^c$. This toplogy can also be defined in a similar way as we did it on $\mathcal{L}_n^c$ namely it will be the strongest topology on $\mathtt{lattice}_n^c$ so that the restriction of the function ψ_n onto $\mathcal{S}_n$ is continuous. Moreover a set $H \subseteq \mathtt{lattice}_n^c$ is open iff $\psi_n^{-1}(H)$ is open in $\mathcal{S}_n$. The topolgy on $\mathcal{S}_n$ is induced by the topoly of $\mathbf{R}^n$. A $G \subseteq \mathcal{S}_n$ is open in $\mathcal{S}_n$ iff there is a $G' \subseteq \mathbf{R}^n$ which is open in $\mathbf{R}^n$ so that $G = G' \cap \mathcal{S}_n$. ($\mathcal{S}_n$ is closed but not open in $\mathbf{R}^n$.) We define a topology on $\mathtt{lattice}_n$ as the unique topology so that the map ξ restricted to $\mathtt{lattice}_n$ is a homeomorphism.

The following lemma describes the most important properties of the topologies on

$\mathcal{L}_n^c$ and $\mathtt{lattice}_n^c$.

Lemma 3 *Let n be a positive integer. The topology defined on $\mathcal{L}_n^c$ meets the following requirements:*

(1) if $G \subseteq \mathcal{G}_n$ is open, then $\psi_n''(G)$ is also open.

(2) each $x \in \mathcal{L}_n^c$ has a basis of neighborhoods consisting of compact sets.

(3) any two points of $\mathcal{L}_n^c$ have disjoint closed neighborhoods.

(4) every $V \in \mathcal{G}_n$ has a neighborhood T so that ψ_n is one-to-one on T.

(5) There is a partition of $\mathcal{G}_n$ onto countably many sets $C_1, C_2, ...$ so that for each fixed $i = 1, 2, ...$ ψ_n is one-to-one on C_i and C_i is the difference of two open sets.

(6) $\mathcal{L}_n^c$ is a locally compact Hausdorff space.

All of the statements of the lemma remain true if we substitute $\mathcal{L}_n^c$ by $\mathtt{lattice}_n^c$, $\mathcal{G}_n$ by $\mathcal{S}_n$, and ψ_n by $\psi_n|_{\mathcal{S}_n}$ where $\psi_n|_{\mathcal{S}_n}$ is the restriction of ψ_n to $\mathcal{S}_n$.

Remark. Naturally properties (2),(3) and (6) hold for $\mathcal{L}_n$ (and $\mathtt{lattice}_n$) as well without any changes, while the remaining ones become valid if we replace ψ_n by Ψ_n.

Proof. (1) We will say that an $X \subseteq \mathcal{G}_n$ is full, if it is the union of all left cosets of $\mathcal{Z}_n$ intersecting X. We prove first that if $A \subseteq \mathcal{G}_n$ is the smallest full subset of $\mathcal{G}_n$ containing an open set G, then A is open. Indeed, for any fixed $Z \in \mathcal{Z}_n$ the set GZ is open since the multiplication by Z is a homeomorphism. Therefore $A = \bigcup_{Z \in \mathcal{Z}_n} GZ$ is open.

By the definition of the factor topology every full open subset of $\mathcal{G}_n$ has an open image and therefore $\psi_n(G) = \psi_n(A)$ is open.

(2) Let $x = \psi_n(y)$. y has a basis of neighborhoods consisting of compact sets. We claim that their images will form the required basis of x. Indeed by (1) the images are neighborhoods of x, by the continuity of ψ_n they form a basis of neighborhoods, and again by the continuity of ψ_n, they are compact.

(3) We will prove this part of the lemma later, after the proof of Lemma 5.

(4). First we note that for all $U, W \in \mathcal{G}_n$, $\psi_n(U) = \psi_n(W)$ iff $U^{-1}W \in \mathcal{Z}_n$. Assume now that contrary to our assertion V has no neighborhood with the required property. Then there are two sequences $\langle U_i \rangle$, $\langle W_i \rangle$, so that both converges to V and $U_i \neq W_i$, but $\psi_n(U_i) = \psi_n(W_i)$ for $i = 1, 2, ...$ According to our observation $U_i^{-1}W_i = \mathcal{Z}_n$ for $i = 1, 2, ...$ On the other hand $U_i^{-1}W_i$ converges to $V^{-1}V = 1$. Since $\mathcal{Z}_n$ contains only matrices with integer entries this means that $U_i^{-1}V_i = 1$ for all sufficiently large i in contradiction to the assumption $U_i \neq V_i$.

(5). By (4) every compact subset of $\mathcal{G}_n$ can be covered by a finite number of open sets so that ψ_n is one-to-one on each of them. Since $\mathcal{G}_n$ is the union of a countble

set of compact subsets, $\mathcal{G}_n$ can be covered by a sequence G_i $i = 1, 2, ...$ of open sets sets so that ψ_n is one-to-one on each of them. $C_i = G_i - \bigcup_{j<i} G_j$ meets all of the requirements.

(6) is an immdediate consequence of (2) and (3).

The corresponding properites of the topolgy on $\texttt{lattice}_n^c$ follow easily from the properties of $\mathcal{L}_n^c$. This concludes the proof of Lemma 3 with the exception of property (3) with will be proved later.

Definitions. 1. Assume that $B \in \mathcal{G}_n$. If $L \in \mathcal{L}_n$ then let $BL = \{Bx \mid x \in L\}$. Obvoiusly $BL \in \mathcal{L}_n$.

2. If $B \in \mathcal{G}_n$ and $a \in \mathcal{L}_n^c$ then we define Ba in the following way: $Ba = \xi(B\xi^{-1}(a))$. We also can describe this more directly. By definition $a = W\mathcal{Z}_n$ for some $W \in \mathcal{G}_n$. We define Ba as the left coset $BW\mathcal{Z}_n$. This coset is clearly independent of the choice of the representative W. With these definitions we have $B\xi_n(L) = \xi_n(BL)$ for all $B \in \mathcal{G}_n$, $L \in \mathcal{L}_n$.

3. If $W \in \mathcal{G}_n$ then $\|W\|$ will denote the Euclidean norm on the n^2 dimensional space, that is if $W = \{w_{i,j}\}$, then $\|W\| = (\sum w_{i,j}^2)^{\frac{1}{2}}$.

The following lemma says that if we take lattice bases from a compact set Φ and consider the coefficients (in these bases) of points from a bounded set X then the set of all of these coefficients is bounded.

Lemma 4 *Let n be a positive integer and let Φ be a compact subset of $\mathcal{G}_n$. Suppose that $X \subseteq \mathbf{R}^n$ is bounded. Then there is an $N > 0$ so that for all $V \in \Phi$ if $x \in X$, and $x = \sum_i^n \alpha_i v_i$ where $v_1, ..., v_n$ are the columns of V, then $|\alpha_i| \leq N$ for $i = 1, ..., n$.*

Proof. We define $\alpha_i(x, V)$ if $i = 1, ...n$, if x is in the closure $\bar{X}$ of X and $V \in \Phi$, by $x = \sum_{i=1}^n \alpha_i(x, V)v_i$. ($\alpha_i(x, V)$ is not necessarily an integer.) This implies that $V^{-1}x = \langle \alpha_1(x, V), ..., \alpha_n(x, V)\rangle$. Since the function V^{-1} is continuous on $\mathcal{G}_n$ we have that for each fixed i the function $|\alpha_i(x, V)|$ is continuous on the compact set $\bar{X} \times \Phi$ therefore it has a finite upper bound. Let N be the maximum of these upper bounds taken for all $i = 1, ..., n$. *Q.E.D.*(Lemma 4)

According to the following lemma if we take a small enough neighborhood of a basis of the lattice L (in the topology of $\mathcal{G}_n$) then all of the lattices generated by bases in this neighborhood will be pointwise close to the lattice L in some sense.

Lemma 5 *Assume that $W \in \mathcal{G}_n$, $K > 0$ and $\varepsilon > 0$. Then there exists a neighborhood T of W so that for all $V \in T$ if $x \in \Psi_n(V)$ and $\|x\| \leq K$ then there is an $y \in \Psi_n(W)$ with $\|x - y\| \leq \varepsilon$.*

Proof. (2) of Lemma 3 implies that W has a compact neighborhood $\Phi \subseteq \mathcal{G}_n$. According to Lemma 4, for all $V \in \Phi$, $x \in \Psi_n(V)$, $\|x\| \leq K$, the absolute value of the coefficients of x in the basis $v_1, ..., v_n$ consisting of the columns of V, remain below a bound N. Suppose that $\delta > 0$ is sufficiently small with respect to ε, N, K and $\|W\|$. Let T be the neighborhood of V with radius δ and assume that $v_1, ..., v_n$ are the columns of V and $w_1, ..., w_n$ are the columns of W. Suppose that $x \in \Psi_n(V)$ with $\|x\| \leq K$ is fixed. Let $x = \sum_{i=1}^n \alpha_i(x, V)v_i$ $y = \sum_{i=1}^n \alpha_i(x, V)w_i$. Since x is a lattice point in $\Psi_n(V)$ the numbers $\alpha_i(x, V)$ are integers and so $y \in \Psi_n(W)$. Since $\|V - W\| \leq \delta$ and δ is sufficiently small with respect to ε, N, K and $\|W\|$, we have that $\|x - y\| \leq \varepsilon$. *Q.E.D.*(Lemma 5)

Proof of (3) of Lemma 3. By (1) and (2) it is enough to show that if $U, V \in \mathcal{G}_n$ so that $\psi_n(U) \neq \psi_n(V)$, then they have neighborhoods S, T so that $\psi_n(U')$ and $\psi_n(V')$ are distinct for all $U' \in S$, $V' \in T$. Since $\psi_n(U)$ and $\psi_n(V)$ are distinct so are $\Psi_n(U)$ and $\Psi_n(V)$. $\Psi_n(U)$ and $\Psi_n(V)$ are discrete subsets of $\mathbf{R}^n$. Therefore their distinctness implies that one of them e.g. $\Psi_n(U)$ contains a point x with the property that there is a $\delta > 0$ so that the distance of x from any element of $\Psi_n(V)$ is at least δ. (We will assume that δ is sufficiently small with respect to $\|x\|$.) Let $K = 2\|x\|$. Applying lemma 5 with both $W \to V$ and $W \to U$, K, $\varepsilon \to \frac{\delta}{4}$ we pick neighborhoods S, T of U, V. Assume that $U' \in S$, $V' \in T$. We claim that $\Psi_n(U')$ and $\Psi_n(V')$ are distinct. By Lemma 5 there is an $y \in \Psi_n(U')$ so that $\|x - y\| < \frac{\delta}{4}$. We claim that $y \notin \Psi_n(V')$. Indeed $y \in \Psi_n(V')$, $\|y\| \leq \|x\| + \frac{\delta}{4} < K$ would imply by Lemma 5 that there is a $z \in \Psi_n(V)$ so that $\|y - z\| \leq \frac{\delta}{4}$. That is, we would get $\|x - z\| \leq \frac{\delta}{2}$ in contradiction to the assumption that the distance of x from $\Psi_n(V)$ is at least δ. *Q.E.D.*((3) of Lemma 3)

The measure μ_n. In this section we show that the function μ_n as defined earlier is indeed a measure on the Borel sets of $\mathtt{lattice}_n$.

Definitions. 1. $\mathtt{vol}_n(X)$ will denote the n-dimensional volume of the Borel set $X \subseteq \mathbf{R}^n$. We consider $\mathcal{G}_n$ as a subset of $\mathbf{R}^{n^2}$, therefore $\mathtt{vol}_{n^2}$ is defined on the Borel measurable subsets of $\mathcal{G}_n$.

2. If $A \subseteq \mathcal{S}_n$ then A° will denonte the set $\{\alpha X | -1 \leq \alpha \leq 1, X \in A\}$.

Lemma 6 *If n is a positive integer then for each Borel set B of $\mathcal{S}_n$ let $\rho_n(B) = \mathtt{vol}_{n^2}(B^\circ)$. Then the following conditions are satisfied:*

(a) $\rho_n(G) > 0$ if G is open in $\mathcal{S}_n$.

(b) $\rho_n(C) < \infty$ if C is compact in $\mathcal{S}_n$.

(c) for all $g \in \mathcal{S}_n$ and for all Borel sets B of $\mathcal{S}_n$ we have $\rho_n(gB) = \rho_n(B) = \rho_n(Bg)$, where $gB = \{gX \mid X \in B\}$

Proof. (a) if G is open then G° contains the open set $X = \{\alpha x | x \in G, 0 < \alpha < 1\}$. Since X is open in $\mathbf{R}^{n^2}$ we have $\rho_n(G) = \mu_{n^2}(G^\circ) \geq \mu_{n^2}(X) > 0$.

(b) If C is compact then C° is also compact, so we have $\rho_n(C) = \mathtt{vol}_{n^2}(C^\circ) < \infty$

(c) For each $g \in \mathcal{S}_n$, the map $x \to gx$, where x is an arbitrary $n \times n$ matrix, is a linear transformation of $\mathbf{R}^{n^2}$ into itself. In the basis consisting of matrices with a single entry 1 and $n^2 - 1$ entries 0 the matrix of this linear transformation is the tensor product of x and the $n \times n$ identity matrix, therefore its determinant is 1, which implies $\mathtt{vol}_{n^2}(gX) = \mathtt{vol}_{n^2}(X)$ for all Borel sets $X \subseteq \mathbf{R}^{n^2}$. For any $B \subseteq \mathcal{S}_n$ we clearly have $g(B^\circ) = (gB)^\circ$, therefore $\rho_n(gB) = \mathtt{vol}_{n^2}((gB)^\circ) = \mathtt{vol}_{n^2}(g(B^\circ)) = \mathtt{vol}_{n^2}(B^\circ) = \rho_n(B)$. The equality $\rho_n(B) = \rho_n(Bg)$ can be proved in a similar way. *Q.E.D.*(Lemma 6)

Property (5) of Lemma 3 implies that $\mathcal{S}_n$ can be partitioned into a countable number of Borel sets so that on each one the map ψ_n is one-to-one. The following lemma is a consequence of this fact and says that if ψ_n is one-to-one on a Borel set then its range can be arbitrarily extended in a way that ψ_n still remains one-to-one.

Lemma 7 *Assume that $D \subseteq \mathcal{L}_n^c$, $F_0 \subseteq \mathcal{G}_n$ are Borel sets, ψ_n is one-to-one on F_0 and $\psi_n''(F_0) \subseteq D$. Then there is a Borel set $F \supseteq F_0$ of $\mathcal{G}_n$ so that ψ_n is one-to-one on F and $\psi_n''(F) = D$. Moreover if $H \subseteq \mathcal{G}_n$ is an arbitrary Borel set with $\psi_n''(H) \supseteq D$, then the set F with the properties described above can be chosen so that $F \subseteq H$. In particular if $D \subseteq \mathtt{lattice}_n^c$ then we may pick F with the additional property $F \subseteq \mathcal{S}_n$.*

Proof. By recursion on i we define a sequence of Borel sets $F_0, F_1, F_2, ...$ so that $F_i \supseteq F_{i-1}$, $i = 1, 2, ...$ The set F_0 is already given. We want do define F_i so that ψ_n is one-to-one on F_i, $\psi_n''(F_i) \subseteq D$ and $\psi_n''(F_i) \supseteq \bigcup_{j=1}^{i} D \cap \psi_n''(C_j)$ for $i = 1, 2, ...$, where the sequence C_i, $i = 1, 2, ...$ is defined in (5) of Lemma 3. Assume that $F_0, ..., F_{i-1}$ has been already defined with these properties. F_i will be the union of F_{i-1} and $\psi_n^{-1}(D) \cap (C_i - \psi_n^{-1}(F_{i-1}))$. Finally let $F = \bigcup_{i=0}^{\infty} F_i$. Clearly $F \supseteq F_0$ is a Borel set and it is easy to check that ψ_n is one-to-one on F and $\psi_n''(F) = D$. If the set H is given with the properties listed in the lemma then we may repeat the proof using $H \cap C_i$ instead of C_i. *Q.E.D.*(Lemma 7)

The following corollary of the lemma says that on each Borel set Y of $\mathtt{lattice}_n^c$ we can choose a one-to-one inverse of ψ_n so that the range of this inverse is a Borel set in $\mathcal{S}_n$.

Corollary 1 *There is a function ϑ defined on the set of all Borel sets $Y \subseteq \mathtt{lattice}_n^c$, with properties (a) and (b) described below:*

(a) each value of ϑ is a Borel set in $\mathcal{S}_n$,

(b) for any Borel set Y of $\mathtt{lattice}_n^c$*, we have* $\psi_n''(\vartheta(Y)) = Y$ *and* ψ_n *is one-to-one on* $\vartheta(Y)$*.*

If we fix a ϑ with the properties in the corollary then starting from an arbitrary measure κ on the Borel sets on $\mathcal{S}_n$ we may define a function κ' on the Borel sets of $\mathtt{lattice}_n^c$ by $\kappa'(Y) = \kappa(\vartheta(Y))$ for all Borel set $Y \subseteq \mathcal{S}_n$. In particular we will get the definition of $\tilde{\mu}_n$ if $\kappa = \rho_n$, $\kappa' = \tilde{\mu}_n$. However κ' will not be a measure for each choice of κ and ϑ. In the following lemma we will show that under certain conditions on κ (which are met by ρ_n) the defined function κ' does not depend on the choice of ϑ and in this case κ' is indeed a measure. This will guarantee that $\tilde{\mu}_n$ is a measure and it does not depend on the choice of ϑ.

Lemma 8 *Assume that κ is a measure defined on the Borel sets of $\mathcal{S}_n$ so that for each Borel set B of $\mathcal{S}_n$ and for each $Z \in \mathcal{Z}_n$ we have $\kappa(B) = \kappa(BZ)$, where $BZ = \{xZ \mid x \in B\}$. Then for any function ϑ with propreties (a) and (b) of Corollary 1 the number $\kappa(\vartheta(Y))$ depends only on κ and the Borel set $Y \subseteq \mathtt{lattice}_n^c$, but not on ϑ. If we define the function κ' on the set of all Borel set $Y \subseteq \mathtt{lattice}_n^c$ by $\kappa'(Y) = \kappa(\vartheta(A))$, then κ' is a measure (which depends only on κ but not on ϑ).*

Proof. First we prove that the value of $\kappa(\vartheta(Y))$ does not depend on the choice of ϑ. Suppose that a Borel set $Y \subseteq \mathtt{lattice}_n^c$ is fixed and we have two sets A_i, $i = 1, 2$ (the values of $\vartheta(Y)$ for two differnet choices of ϑ) so that

(a) $A_i \subseteq \mathcal{S}_n$, *$A_i$ is a Borel set, ψ_n is one-to-one on A_i and* $\psi_n''(A_i) = Y$ *for* $i = 1, 2$

We show that $\kappa(A_1) = \kappa(A_2)$. We define a one-to-one map f of A_1 onto A_2. For each $U \in A_1$, $f(U)$ will be the unique element of A_2 with $\psi_n(U) = \psi_n(f(U))$. This last equality implies that U and $f(U)$ are bases of the same lattice therefore there is a unique element $Z_U \in \mathcal{Z}_n$ with $f(U) = UZ_U$. We partition A_1 into countably many sets according to the value of Z_U. We claim that each class of this partition is a Borel set. Indeed for a fixed possible value $Z \in \mathcal{Z}_n$ of Z_U this class is $(A_1Z \cap A_2)Z^{-1}$. A_i, $i = 1, 2$ are Borel sets in $\mathcal{S}_n$, the multiplications by Z or by Z^{-1} are homeomorphisms of $\mathcal{S}_n$ onto itself therefore A_1Z, $A_1Z \cap A_2$ and $(A_1Z \cap A_2)Z^{-1}$ are also a Borel sets, which proves our claim.

Let R be an arbitrary but fixed class of this partition. Clearly it is enough to show that $\kappa(R) = \kappa(f''(R))$. By the definition of R there is an $Z \in \mathcal{Z}_n$ so that for all $U \in R$ we have $f(U) = UZ$ and therefore $f''(R) = RZ$. According to an assumption of the lemma $\kappa(B) = \kappa(BZ)$ for all Borel sets B and $Z \in \mathcal{Z}_n$, therefore $\kappa(R) = \kappa(RZ) = \kappa(f''(R))$.

Clearly the values of κ' are nonnegative reals. To show that it is σ-additive let $Y_1, Y_2, ...$ be pairwise disjoint Borel sets in $\texttt{lattice}_n^c$ and for each fixed i we pick a Borel set A_i in $\mathcal{S}_n$ so that $\psi_n''(A_i) = Y_i$ and ψ_n is one-to-one on A_i. Since the sets Y_i are pairwise disjoint, the sets A_i are pairwise disjoint too. Therefore if $Y = \bigcup_{i=1}^{\infty} Y_i$ then $A = \bigcup_{i=1}^{\infty} A_i$ will satisfy the requirements of the lemma and since κ is σ-additive we get that $\kappa'(\bigcup Y_i) = \kappa(A) = \sum \kappa(A_i) = \sum \kappa'(Y_i)$ *Q.E.D.*(Lemma 8)

By Lemma 6 the measure ρ_n meets the requirements of Lemma 8 with $\kappa \to \rho_n$. Therefore ρ_n' is a measure on the Borel sets of $\mathcal{S}_n$.

Definition. Let $\tilde{\mu}_n^c$ be the measure ρ_n' on the Borel sets of $\texttt{lattice}_n^c$. $\tilde{\mu}_n$ is defined by $\tilde{\mu}_n(X) = \tilde{\mu}_n^c(\xi''(X))$ for each Borel set $X \subseteq \mathcal{L}_n$.

Lemma 9 *Suppose that $D \subseteq \texttt{lattice}_n^c$, $F \subseteq \mathcal{S}_n$ are Borel sets, $\psi_n''(F) = D$ and ψ_n is one-to-one on F. Then $\tilde{\mu}_n^c(D) = \rho_n(F)$.*

Proof. We can choose the function ϑ with the properties in the Corollary of Lemma 7 so that $\vartheta(D) = F$. Therefore $\tilde{\mu}_n^c(D) = \rho_n(\vartheta(D)) = \rho_n(F)$. *Q.E.D.*(Lemma 9)

Lemma 10 *If n is a positive integer then the measure $\tilde{\mu}_n$ satisfies the following conditions*

(a) $\tilde{\mu}_n(G) > 0$ if G is open in $\texttt{lattice}_n$.

(b) $\tilde{\mu}_n(C) < \infty$ if C is compact in $\texttt{lattice}_n$.

(c) for all $A \in \mathcal{S}_n$ and for all Borel sets B of $\texttt{lattice}_n$ we have $\tilde{\mu}_n(AB) = \tilde{\mu}_n(B)$, where $AB = \{AL \mid L \in B\}$

Proof. We prove the corresponding properties for $\tilde{\mu}_n^c$.

(a) The coninuity of ψ_n implies that $H = \psi_n^{-1}(G)$ is open in $\mathcal{S}_n$. Therefore by Lemma 6 we have $\rho_n(H) > 0$. Let ϑ be a function whose existence is stated in the corollary of Lemma 7. Let $K = \vartheta^{-1}(G)$, where K is a Borel set in $\mathcal{S}_n$. Since $\psi_n''(H) = \psi_n''(K)$ and H is maximal with this property we have $H = \bigcup_{Z \in \mathcal{Z}_n} KZ$. Since all of the sets KZ, $Z \in \mathcal{Z}_n$ are Borel sets and $\mathcal{Z}$ is countable we have $\rho_n(H) \leq \sum_{Z \in \mathcal{Z}_n} \rho_n(KZ)$. By (c) of Lemma 6 $\rho_n(K) = \rho_n(KZ)$ for all $Z \in \mathcal{Z}_n$, therefore the inequlity $\rho_n(H) \leq \sum_{Z \in \mathcal{Z}_n} \rho_n(KZ)$, $\rho_n(H) > 0$ and the σ-additivity of ρ_n implies that $\rho_n(K) > 0$ and therefore $\tilde{\mu}_n^c(G) = \rho_n(K) > 0$.

(b) For each positive integer i let H_i be the set of all matrices in $\mathcal{S}_n$ whose each entry in absolulte value is strictly less then i. Clearly H_i is open in $\mathcal{S}_n$. By (1) of Lemma 3 $\psi_n''(H_i)$ is open in $\texttt{lattice}_n^c$ and obvioiusly $\bigcup_{i=1}^{\infty} \psi_n''(H_i) = \texttt{lattice}_n \supseteq C$. Therefore the compactness of C implies that it is covered by a finite number of these sets, that is, there is a positive integer i so that $C \subseteq \psi_n''(H_i)$. Applying Lemma 7

with $H \to H_i$ we get that there is a function ϑ with the properties in the corollary of Lemma 7 so that $\vartheta(C) \subseteq H_i$. Therefore $\tilde{\mu}_n^c(C) \leq \rho_n(H_i)$. Since H_i is bounded, so is H_i° and therefore $\tilde{\mu}_n^c(C) \leq \rho_n(H_i) = \mathtt{vol}_{n^2}(H_i^\circ) < \infty$.

(c) Assume that $B \subseteq \mathtt{lattice}_n^c$ is a Borel set and for some choice of the function ϑ we have $\vartheta(B) = F$, $\tilde{\mu}_n^c(B) = \rho_n(F)$. ψ_n is one-to-one on F and its image there is B. Let $K = AF$, where $A \in \mathcal{S}_n$ is fixed. We will show that ψ_n is one-to-one on K and its image there is AB. This is suffient for the proof of (c) since, by Lemma 6 and Lemma 9 this would imply $\tilde{\mu}_n^c(AB) = \rho_n(K) = \rho_n(AF) = \rho_n(F) = \tilde{\mu}_n^c(B)$.

Now we show that ψ_n is one-to-one on K and its image there is AB. Indeed each $T \in K$ is of the form Ax for some $x \in F$. Therefore $\psi_n(T) = T\mathcal{Z}_n = Ax\mathcal{Z}_n = A(x\mathcal{Z}_n)$ where $x\mathcal{Z}_n = \psi_n(x) \in B$. Suppose that $\psi_n(T_1) = \psi_n(T_2)$ where $T_1, T_2 \in K$. Then $T_i = Ax_i$ for $x_i \in F$, $i = 1, 2$. Therefore $\psi_n(T_1) = \psi_n(T_2)$ implies that $Ax_1\mathcal{Z}_n = Ax_2\mathcal{Z}_n$ and so $x_1\mathcal{Z}_n = x_2\mathcal{Z}_n$, that is, $\psi_n(x_1) = \psi_n(x_2)$. Since ψ_n is one-to-one on F this implies $x_1 = x_2$ and so $T_1 = T_2$, that is, ψ_n is one-to-one on K. Assume that $z = AB$. Then $z = Ay$ where $y \in B$ and since $B = \psi_n''(F)$ we have $y = f\mathcal{Z}_n$ for some $f \in F$. Therefore $z = Af\mathcal{Z}_n$ wher $Af \in K$ thus $z \in \psi_n''(K)$. *Q.E.D.*(Lemma 10)

Property (b) of Lemma 10 implies that $\tilde{\mu}_n(\mathtt{lattice}_n) > 0$. This makes possible the following definition.

Definition. If n is a positive integer then for all Borels sets $B \subseteq \mathtt{lattice}_n$ let $\mu_n(B) = (\tilde{\mu}_n(\mathtt{lattice}_n))^{-1}\tilde{\mu_n}(B)$.

We show now that $\tilde{\mu}_n(\mathtt{lattice}_n) < \infty$. This guarantees that the measure μ_n is not identically 0 and as a consequence it is a probabillity measure.

Lemma 11 *There is a function $c(n)$ defined for all posititve integer n so that the following holds. For each positive integer n and for each positive real number r there is a Borel set $B_n^{(r)}$ in $\mathcal{G}_n$ so that*

(1) $\Psi_n''(B_n^{(r)})$ contains all lattices with determinant 1 whose shortest nonzero vectors are of length at most r.

(2) $\mathtt{vol}_{n^2}(B_n^{(r)}) \leq c(n)r^n$

(3) $(B_n^{(r)})^\circ = B_n^{(r)}$

Proof. For the description of the set $B_n^{(r)}$ we need the following definition.

Definitions 1. Let $b_1, ..., b_n$ be a basis of the lattice $L \subseteq \mathbf{R}^n$. Applying the Gram-Schmidt orthogonalization procedure to this basis we get a sequence of vectors $b_1^*, ..., b_n^*$ with the property that b_i^*, $i = 1, 2, ..., n$ are pairwise orthogonal, $b_1 = b_1^*$ and for all $i = 1, ..., n$ we have $b_i^* = b_i - \sum_{i=1}^n \mu_{i,j} b_j^*$ where $\mu_{i,j} = (b_i \cdot b_j^*)/(b_j^* \cdot b_j^*)$. If P_i is the orthogonal projection of the n-dimensional space onto the subspace orthogonal to

$b_1, ..., b_{i-1}$ then $b_i^* = P_i b_i$. We call the basis $b_1, ..., b_n$ size-reduced if $|\mu_{i,j}| \leq \frac{1}{2}$ for all $1 \leq j < i \leq n$. For each $i = 1, ..., n$, $P_i L$ is an $n - i + 1$ dimensional lattice in $P_i \mathbf{R}^n$. We say that $b_1, ..., b_n$ is a Korkine-Zolotareff basis if $P_i b_i$ is a shortest nonzero vector in $P_i L$ for all $i = 1, ..., n$.

2. The set $B_n^{(r)}$ will be the set of all bases $b_1, ..., b_n$ which generate a lattice L with determinant at most 1 so that $b_1, ..., b_n$ is a size reduced Korkine-Zolotareff basis, and $\|b_1\| \leq r$. (We also include the 0 vector of $\mathbf{R}^{n^2}$ in $B_n^{(r)}$ for the sake of property (3) of the Lemma.)

We claim that every lattice has a size reduced Korkine-Zolotareff basis. We may prove this fact by induction on the dimension of the lattice. Let L be an n dimensional lattice, let b_1 be a shortest vector in L and let P_1 be the orthogonal projection of $\mathbf{R}^n$ onto the subspace orthogonal to b_1. $P_1 L$ is an $n-1$ dimensional lattice. Let $d_1, ..., d_{n-1}$ be a size reduced Korkine-Zolotareff basis in $P_1 L$. For each $i = 2, ..., n$ let b_i be an element of L so that $P b_i = d_{i-1}$ and $\|b_i - d_{i-1}\|$ is minimal. (The latter condition implies that $\|b_i - d_{i-1}\| \leq \frac{1}{2}\|b_1\|$.) It is easy to see that $b_1, ..., b_n$ is a size reduced Korkine-Zolotareff basis.)

Since every lattice has a Korkine-Zolotareff basis condition (1) is satisfied by $B_n^{(r)}$. By Minkowski's convex body theorem we have that for each $x \in \mathcal{Y}_n$, $\xi^{-1}(x)$ contains a nonzero vector shorter than $\sigma_n = c_M n^{\frac{1}{2}}$, where c_M is a constant. This implies that will define $B_n^{(r)} = B_n^{(\sigma_n)}$ for all $r \geq \sigma_n$. We will use the notation $B_n^{(\infty)} = \bigcup_{r>0} B_n^{(r)} = B_n^{(\sigma_n)}$.

Condition (3) holds since by multiplying a lattice L by a positive constant $\alpha \leq 1$ any size reduced Korkine-Zolotareff lattice L will go into a size reduced Korkine-Zolotareff basis of αL, and the length of a shortest nonzero vector is also multiplied by $\alpha \leq 1$.

We prove the existence of the real number $c(n)$ with property (2) by induction on n. For $n = 1$ condition (2) is trivially satisfied by $c(n) = 2$ (2 is the length of the interval $[-1, 1]$.) Assume that condition (2) is satisfied for $n - 1$ with a real number $c(n-1)$ for any $r > 0$.

First we note that our inductive assumption implies the following:

(*) *If $H \subseteq \mathcal{G}_{n-1}$ is the set of all size reduced Korkine-Zolotareff basis which generate a lattice with determinant at most D then* $\mathtt{vol}_{(n-1)^2}(H) \leq D^{n-1} c(n-1) \sigma_{n-1}^{n-1}$.

Indeed we know this for $D = 1$ and we have to multiply all of the $n-1$ components of all of the $n - 1$ basis vector by $D^{\frac{1}{n-1}}$ to get a lattice with determinant D from a lattice with determinant 1. During this transformation in the $(n-1)^2$ dimensional space al of the $(n-1)^2$ dimensional volumes are multiplied by $(D^{\frac{1}{n-1}})^{(n-1)^2} = D^{n-1}$.

Suppose that an $r \in (0, \sigma_n)$ is fixed. We estimate the volume of the set $B_n^{(r)}$. Let $\chi(b_1, ..., b_n)$ be the characteristic function of the set $B_n^{(r)}$ where $\langle b_1, ..., b_n \rangle$ now represents a basis $b_1, ..., b_n$, that is, the comlumns of the corresponding matrix. We

get the n^2 dimensional volume of $B_n^{(r)}$ by integrating χ on $\mathbf{R}^{n^2}$.

We compute this integral by integrating first by $b_2, ..., b_n$ and then by b_1. For the elements of $B_n^{(r)}$, b_1 is a vector whose length is at most r so we may assume that b_1 is restricted to a ball S with radius r around the origin. Let's assume that b_1 is a fixed point of this ball and we integrate χ according to the remaining variables. Let $\rho = \|b_1\|$. We want to determine the $n(n-1)$ dimensional volume of the set $X_{b_1} = B_{n^{(r)}} \cap V_{b_1}$ set where $V_{b_1} = \langle \langle b_1, w_2, ..., w_n \rangle | w_2, ..., w_n \in \mathbf{R}^n \rangle$. We can do this by a simple geometric argument based on the inductive assumption. For an arbitrary basis $b_1, ..., b_n$ let $d_i = P_1 b_i$ for $i = 2, ..., n$, where P_1 is the orthogonal projection of $\mathbf{R}^{n^2}$ onto the subspace orthogonal to b_1 and let $f_i = b_i - d_i$. The sequence $b_1, d_2, ..., d_n, f_2, ..., f_n$ uniquely determines the basis $b_1, ..., b_n$. Moreover if $b_1, ..., b_n$ is Korkine-Zolotareff basis then $d_2, ..., d_n$ is also a Korkine-Zolotareff basis of the lattice $P_a L$ in the $n-1$ dimensional subspace $P_1 \mathbf{R}^n$, and $f_i = \tau_i b_i$ for $i = 2, ..., n$ where $|\tau_i| \leq \frac{1}{2}$. For any fixed choice of $\tau_2, ..., \tau_n$, the $(n-1)^2$ dimensional volume of all of the points in $\langle b_1, \tau_2, ..., \tau_n, d_2, ..., d_n \rangle \in X_{b_1}$ is at most $c(n-1)\rho^{-(n-1)}\sigma_{n-1}^{n-1}$ since $d_2, ..., d_n$ is a Korkine-Zolotareff basis of a lattice with determinant ρ^{-1}. (Here we used (*).) Therefore using that each τ_i is chosen from an interval of length ρ we get that $\mathtt{vol}_{n(n-1)}(X_{b_1}) \leq c(n-1)\rho^{n-1}\rho^{-(n-1)}\sigma_{n-1}^{n-1}$. Since this is true for every fixed b_1 in the sphere with radius r we get that $\mathtt{vol}_{n^2}(B_n^{(r)}) \leq \int_0^r \gamma_n \rho^{n-1} c(n-1)\sigma_{n-1}^{n-1} d\rho = c(n) r^n$, where γ_n is the surface area of the n dimensional unit sphere and $c(n) = \frac{1}{n}\gamma_n c(n-1)\sigma_{n-1}^{n-1}$. *Q.E.D.*(Lemma 11)

Lemma 12 *$\tilde{\mu}_n(\mathtt{lattice}_n) < \infty$ for all $n = 1, 2, ...$*

Proof. By Lemma 11 we have $\tilde{\mu}_n(\mathtt{lattice}_n) = \mathtt{vol}_{n^2}(B_n^{(\infty)})^\circ = \mathtt{vol}_{n^2}(B_n^{(\sigma_n)}) \leq c_n \sigma_n^n < \infty$, where σ_n is defined in the proof of Lemma 11. *Q.E.D.*(Lemma 12)

Lemma 13 *μ_n is a probability measure defined on the Borel sets of $\mathtt{lattice}_n$ for every positive integer n, moreover μ_n satisfies the following conditions:*

(a) For every linear transformation A of $\mathbf{R}^n$ with determinant ± 1 and for every Borel set $B \subseteq \mathtt{lattice}_n$ we have $\mu_n(AB) = \mu_n(B)$.

(b) if G is an open subset of $\mathtt{lattice}_n$ then $\mu_n(G) > 0$.

(c) there is a positive real number $c(n)$, depending only on n, so that for all $r > 0$ if X is the set of all lattices with determinant 1 whose shortest nonzero vector is at most of length r then $\mu_n(X) \leq c(n) r^n$

(d) for any Borel set $B \subseteq \mathtt{lattice}_n$, we have

$\mu_n(B) = \sup\{\mu_n(C) \mid C \subseteq B$ and C is compact $\}$ and

$\mu_n(B) = \inf\{\mu_n(G) \mid B \subseteq G$ and G is open $\}$.

Proof. (a) and (b) are immediate consequences of the corresponding properties of $\tilde{\mu}_n$ stated in Lemma 10.

(c) follows from Lemma 11. Indeed using the notation of Lemma 11 we have that $\Psi_n''(B_n^{(r)}) \supseteq X$ and so $\mu_n(X) = \tilde{\mu}_n(\xi(X)) \leq \mathtt{vol}_{n^2}((B_n^{(r)})^\circ) = \mathtt{vol}_{n^2}(B_n^{(r)}) \leq c(n)r^n$.

Fore the proof of property (d) we need the following Lemma.

Definition. We say that a set $X \subseteq \mathbf{R}^n$ is symmetric if $x \in X$ imples $-x \in X$ for all $x \in X$.

Lemma 14 *Assume that $X \subseteq \mathcal{S}_n$ is a symmetric Borel set so that $\mathtt{vol}_{n_2}(X^\circ) < \infty$. Then for all $\varepsilon > 0$ there is a symmetric compact set $C \subseteq X$ and a symetric set $G \subseteq X$ which is open in $\mathcal{S}_n$, so that $\mathtt{vol}_{n^2}(X^\circ) - \mathtt{vol}_{n^2}(C^\circ) < \varepsilon$ and $\mathtt{vol}_{n^2}(G^\circ) - \mathtt{vol}_{n^2}(X^\circ) < \varepsilon$.*

Proof. Since $\mathtt{vol}_{n^2}(X^\circ) < \infty$, there is a compact $C' \subseteq X^\circ$ and an open (in $\mathbf{R}^{n^2}$) $G' \supseteq X^\circ$ so that $\mathtt{vol}(X^\circ) - \mathtt{vol}(C') < \varepsilon$ and $\mathtt{vol}(G') - \mathtt{vol}(X^\circ) < \varepsilon/2$. The set $\mathcal{S}_n$ is closed therefore its distance from 0 is positive. Assume that $\delta > 0$ is smaller than this distance and that the volume of the (open) ball B_δ with radius δ around 0 has volume less than $\varepsilon/2$. $W = C' \backslash B_\delta$ is a compact symmetric set. We define a function f on W in the following way. If $x \in W$ then let $f(x)$ be the unique element of X so that $x = \alpha f(x)$ for some $\alpha \in (0, 1]$. The existence of such an $f(x)$ follows from $C' \subseteq X^\circ$ and the symmetricity of X, the uniqueness follows from $X \subseteq \mathcal{S}_n$. It is easy to see that the function $f(x)$ is continuous on W. Therefore the image $C = f''(C_1)$ of the compact set C_1 is also compact (and obviously symmetric). Clearly $C \subseteq X$ and $C^\circ \supseteq C_1 = C' \backslash B_\delta$. Therefore $\mathtt{vol}_{n_2}(C) \leq \mathtt{vol}_{n^2}(C') - \frac{\varepsilon}{2} \geq \mathtt{vol}_{n^2}(X) - \varepsilon$.

Let $G = \{x \in G' \cap \mathcal{S}_n \mid \forall \alpha \in [0, 1],\ \alpha x \in G'\}$. $G' \supseteq X^\circ$ implies that $G \supseteq X$. The definition of G' implies that $(G)^\circ \subseteq G'$ and so $\mathtt{vol}(G^\circ) \leq \mathtt{vol}(G') \leq \mathtt{vol}(X^\circ) + \varepsilon$. Since G is obviously symmetric we have to prove only that G is open.

Assume that $g \in G$. By the definition of G the complete line segment $K_g = \{\alpha g \mid \alpha \in [0, 1]\}$ is in G'. Therefore there is a $\delta > 0$ so that the distance of K_g from the complement of G' is positive. Let $\delta' > 0$ be sufficiently small with respect to δ. Then for any $x \in \mathcal{S}_n$ with $\|x - g\| \leq \delta'$, the complete line segment $K_x = \{\alpha x \mid \alpha \in [0, 1]\}$ is also included in G', therfore $x \in G$. *Q.E.D.*(Lemma 14)

Now we continue the proof of Lemma 13. Let Y be a Borel set in $\mathcal{S}_n$ so that ψ_n is one-to-one on Y and $\psi_n''(Y) = \xi(B)$. Lemma 7 and its Corollary guarantee the existence of such a set Y. By the definition of $\tilde{\mu}_n$ we have that $\tilde{\mu}_n(\xi(B)) = \mathtt{vol}_{n^2}(Y^\circ)$. According to Lemma 12 $\tilde{\mu}_n$ is finite and so $\mathtt{vol}_{n^2}(Y^\circ) < \infty$. Let $X = Y \cup (-Y)$. $X \subseteq \mathcal{S}_n$ is a symmetric Borel set and $X^\circ = Y^\circ$. We apply Lemma 14 to the set X. Let $\bar{C} \subseteq X$ be the compact set and $\bar{G} \supseteq X$ the open (in $\mathcal{S}_n$) set whose existence are guaranteed by Lemma 14. Finally let $C = \Psi_n''(\bar{C})$ and $G = \Psi_n''(\bar{G})$. Clearly

$C \subseteq B \subseteq G$. By property (1) of Lemma 3 the set G is open in $\texttt{lattice}_n$ and by the continuity of the map Ψ_n'' the set C is compact in $\texttt{lattice}_n$. Since $\mu_n(C) = \mu_n(\bar{C}\circ)$ and $\mu_n(G) \leq \mu_n(\bar{G}^\circ)$ we have $\mu_n(B) - \mu_n(C) \leq \varepsilon$ and $\mu_n(G) - \mu_n(B) \leq \varepsilon$. *Q.E.D.*(Lemma 13)

References

[1] M. Ajtai, *Generating Hard Instances of Lattice Problems*, 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, *Random lattices and a conjectured 0-1 law about their polynomial time properties*, Proc. of 43rd IEEE FOCS 2002

[4] 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/

[5] 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.

[6] R. Fagin, *Probabilities on Finite models*, Journal of Symbolic Logic, 41, 1, March 1976, pp. 50-58.

[7] H. Federer *Geometric measure theory*, Section 2.7, Springer, 1969, (Grundleheren der matematischen Wissenschaften; Vol. 153).

[8] M. Foreman. *Generic Large Cardinals: New Axioms for Mathematics?* In Proc. International Congress of Mathematicians, Vol. II, pages 11–23, 1998.

[9] P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers*, Chapter 3. North Holland 1987.

[10] T. Jech. *Set Theory*, Academic Press, 1978.

[11] 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.

[12] A. K. Lenstra, H. W. Lenstra, L. Lovász *Factoring polynomials with rational coefficients*, Math. Ann. 261, 515-534 (1982).

[13] 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.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'