Random Witnesses and the Classical Character of Macroscopic Objects

I. Pitowsky

Department of Philosophy, The Hebrew University, Mount Scopus, Jerusalem, Israel, 91905. Electronic mail: itamarp@vms.huji.ac.il

(April 8, 2004)

Typeset using REVTEX

Abstract

An observable W that distinguishes all the unentangled states from some entangled states is called a witness. We consider witnesses on n qbits, and use the following normalization: A witness W satisfies $|tr(W\rho)| \leq 1$ for all separable states ρ, while $\|W\| > 1$, with the norm being the maximum among the absolute values of the eigenvalues of W. Although there are n-qbit witnesses whose norm is exponential in n, we conjecture that for a large majority of n-qbit witnesses $\|W\| \leq O(\sqrt{n \log n})$. We prove this conjecture for the family of extremal witnesses introduced by Werner and Wolf (*Phys. Rev. A* **64**, 032112 (2001)). Assuming the conjecture is valid we argue that multiparticle entanglement can be detected only if a system has been carefully prepared in a very special state. Otherwise, multiparticle entanglement lies below the possibility of detection, even if it exists, and even if decoherence has been "turned off".

I. INTRODUCTION

Why we do not see large macroscopic objects in entangled states? There are two ways to approach this question. The first is dynamic: the coupling of a large object to its surroundings and its constant random bombardment from the environment cause any entanglement that ever existed to disentangle. The second approach- which does not in any way undermine the first- puts the stress on the word *we*. Even if the particles composing the object were all entangled and insulated from the environment, we shall still find it hard to *observe* the superposition. The reason is that as the number of particles n grows we need an ever more precise knowledge of the state, and an ever more carefully designed experiment in order to recognize the entangled character of the state of the object.

In this paper I examine the second approach by considering entanglements of multi particle systems. For simplicity, the discussion concentrates mostly on two-level systems, that is, n-qbit systems where n is large. An observable W that distinguishes all the unentangled states from some entangled states is called a *witness* [1]. I shall use the following normalization: A witness W satisfies $|tr(W\rho)| \leq 1$ for all separable (that is, unentangled) states ρ, while $\|W\| > 1$. Here $\|W\|$ is the operator norm, the maximum among the absolute values of the eigenvalues of W.

For each $n \geq 2$ there is a witness W, called the Mermin-Klyshko operator [2], whose norm, $\|W\| = \sqrt{2^{n-1}}$, increases exponentially with n. The eigenvector at which this norm obtains is called the generalized GHZ state; it represents a maximally entangled system of n qbits. However, we shall see that this large norm is the exception, not the rule. My aim is to show that the norm of a *majority* of the witnesses grows with n very slowly, $\|W\| \leq O(\sqrt{n \log n})$, slower than the growth of the measurement error. We shall prove this with respect to a particular family of witnesses, and formulate it as a conjecture in the general case. This means that unless the system has been very carefully prepared in a very specific state, there is a very little chance that we shall detect multiparticle entanglement, even if it is there.

The paper proceeds as follows: In the next section I shall review some of the known witnesses for n qbits, those associated with the generalized Bell inequalities introduced by Werner and Wolf [3]. The third section examines the typical norm of the Werner Wolf operators, which is closely associated with the shape of the set of quantum correlations for two possible measurements per particle. Subsequently, I formulate the *random witness conjecture*, and examine how it bears on our original question namely, why we do not see large objects in entangled states.

II. WITNESSES AND QUANTUM CORRELATIONS

A. The two particles case

Let A_0, A_1, B_0, B_1 be four Hermitian operators in a finite dimensional Hilbert space $\mathbb{H}$ such that $A_i^2 = B_j^2 = \mathbf{1}$. On $\mathbb{H} \otimes \mathbb{H}$ define the following operator

$$W = \frac{1}{2} A_0 \otimes B_0 + \frac{1}{2} A_0 \otimes B_1 + \frac{1}{2} A_1 \otimes B_0 - \frac{1}{2} A_1 \otimes B_1 \tag{1}$$

It is easy to see that $|tr(W\rho)| \leq 1$ for any separable state ρ on $\mathbb{H} \otimes \mathbb{H}$. This is, in fact, the Clauser Horne Shimony and Holt (CHSH) inequality [4]. Indeed, if X_0, X_1, Y_0, Y_1 are any four random variables taking the values ± 1 then

$$-1 \leq \frac{1}{2} X_0 Y_0 + \frac{1}{2} X_0 Y_1 + \frac{1}{2} X_1 Y_0 - \frac{1}{2} X_1 Y_1 \leq 1 \tag{2}$$

as can easily be verified by considering the 16 possible cases. Hence $c_{ij} = \mathcal{E}(X_i Y_j)$, the correlations between X_i and Y_j, also satisfy the inequalities

$$-1 \leq \frac{1}{2} c_{00} + \frac{1}{2} c_{01} + \frac{1}{2} c_{10} - \frac{1}{2} c_{11} \leq 1 \tag{3}$$

If ρ is a separable state on $\mathbb{H} \otimes \mathbb{H}$ we can represent $tr(\rho\ A_i \otimes B_j)$ as correlations c_{ij} between such X_i's and Y_j's. In other words, the correlations can be recovered in a local hidden variables model.

From Eq (2) three other conditions of the form Eq (3) can be obtained by permuting the two X indecies or the two Y indices. The resulting constraints on the correlations form a necessary and *sufficient* condition for the existence of a local hidden variables model [5,6]. One way to see this is to consider the four-dimensional convex hull C_2 of the sixteen real vectors in $\mathbb{R}^4$:

$$(X_0 Y_0, X_0 Y_1, X_1 Y_0, X_1 Y_1) \quad X_i = \pm 1,\ Y_j = \pm 1 \tag{4}$$

and prove that an arbitrary four-dimensional real vector $(c_{00}, c_{01}, c_{10}, c_{11})$ is an element of C_2 if, and only if, the c_{ij} satisfy $-1 \leq c_{ij} \leq 1$ and all the conditions of type Eq (3). The inequalities, then, are the *facets* of the polytope C_2.

By contrast with the classical case let ρ be a *pure entangled* state on $\mathbb{H} \otimes \mathbb{H}$. Then for a suitable choice of A_i's, and B_j's in Eq (1) we have $|tr(W\rho)| > 1$ [7], so the operators W of this type are sufficient as witnesses for all pure entangled bipartite states. To obtain a geometric representation of the quantum correlations let ρ be any state, denote $q_{ij} = tr(\rho\ A_i \otimes B_j)$, and consider the set Q_2 of all four dimensional vectors $(q_{00}, q_{01}, q_{10}, q_{11})$ which obtain as we vary the Hilbert space and the choice of ρ, A_i, and B_j. The set Q_2 is convex, $Q_2 \supset C_2$ but it is not a polytope. The shape of this set has been the focus of a great deal of interest [8–12]. To get a handle on its boundary we can check how the value of $\|W\|$ changes with the choice of A_i's, and B_j's. Cirel'son [8,9] showed that $\|W\| \leq \sqrt{2}$. This is a tight inequality, and equality obtains already for qbits. In this case, $\mathbb{H} = \mathbb{C}^2$ and $A_i = \sigma(\mathbf{a}_i)$, $B_j = \sigma(\mathbf{b}_j)$ are spin operators, with $\mathbf{a}_0, \mathbf{a}_1, \mathbf{b}_0, \mathbf{b}_1$ four directions in physical space. There is a choice of directions such that $\|W\| = \sqrt{2}$, and the eigenvectors $|\phi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, corresponding to this value are the maximally entangled states.

The condition $\|W\| \leq \sqrt{2}$ while necessary, is not sufficient to determine the boundary of Q_2. As it turns out the boundary is quite complex; the values on the boundary determine the range of violation of the CHSH inequality attainable by quantum systems, and therefore, serves as an important test of quantum theory [10–12].

B. The n particles case - Werner Wolf operators

Some of these results can be extended to n particle systems, provided that the operators are restricted to two binary measurements per particle. To account for classical correlations consider $2n$ random variables $X_0^1, X_1^1; X_0^2, X_1^2; ...; X_0^n, X_1^n$, each taking the two possible values ± 1. We shall parametrize the coordinates of a vector in the 2^n-dimensional real space $\mathbb{R}^{2^n}$ by sequences $\mathbf{s} = (s_1, ..., s_n) \in \{0, 1\}^n$. Now, consider the set of 2^{2n} real vectors in $\mathbb{R}^{2^n}$

$$(a(0, ..., 0), ..., a(s_1, ..., s_n), ...a(1, ..., 1)), \quad a(s_1, ..., s_n) = X_{s_1}^1 X_{s_2}^2 ... X_{s_n}^n \tag{5}$$

Their convex hull in $\mathbb{R}^{2^n}$, denoted by C_n, is the range of values of all possible classical correlations for n particles and two measurements per site. Werner and Wolf [3] showed that C_n is a hyper-octahedron and derived the inequalities of its facets. These are 2^{2^n} inequalities of the form

$$-1 \leq \sum_{s_1,...,s_n=0,1} \beta_f(s_1,...,s_n) X^1_{s_1} X^2_{s_2} ... X^n_{s_n} \leq 1 \tag{6}$$

where each inequality is determined by an arbitrary function $f : \{0,1\}^n \to \{-1,1\}$ with

$$\beta_f(s_1,...,s_n) = \frac{1}{2^n} \sum_{\varepsilon_1,...,\varepsilon_n=0,1} (-1)^{\varepsilon_1 s_1+...+\varepsilon_n s_n} f(\varepsilon_1,...,\varepsilon_n) \tag{7}$$

In other words, to each choice of function f there corresponds a choice of coefficients β_f. Since β_f is the inverse Fourier transform of f on the group $\mathbb{Z}_2^n$ we have by Plancherel's theorem [13]:

$$\sum_{\mathbf{s}} |\beta_f(\mathbf{s})|^2 = \frac{1}{2^n} \sum_{\varepsilon} |f(\varepsilon)|^2 = 1 \tag{8}$$

Using the analogy with the bipartite case let $A^1_0, A^1_1, ..., A^n_0, A^n_1$ be $2n$ arbitrary Hermitian operators in a Hilbert space $\mathbb{H}$, satisfying $(A^j_i)^2 = \mathbf{1}$. The quantum operators corresponding to the classical facets in Eq (6) are the *Werner Wolf operators* on $\mathbb{H}^{\otimes n}$ given by:

$$W_f = \sum_{s_1,...,s_n \in \{0,1\}} \beta_f(s_1,...,s_n) A^1_{s_1} \otimes ... \otimes A^n_{s_n} \tag{9}$$

It is easy to see from Eq (6) that $|tr(\rho W_f)| \leq 1$ for every separable state ρ and all the f's. However, the inequalities may be violated by entangled states. Let Q_n be the set of all vectors in $\mathbb{R}^{2^n}$ whose coordinates have the form $q(s_1,...,s_n) = tr(\rho A^1_{s_1} \otimes ... \otimes A^n_{s_n})$ for some choice of state ρ and operators A^j_i as above. The set Q_n is the range of possible values of quantum correlations, and it is not difficult to see that Q_n is convex and $Q_n \supset C_n$. To obtain information about the boundary of Q_n we can examine how $\|W_f\|$ varies as we change the A^j_i's. In this case too, it was shown [3] that for each fixed f, the maximal value of $\|W_f\|$ is already obtained when we choose $\mathbb{H} = \mathbb{C}^2$, and the A^j_i's to be spin operators. Therefore, without loss of generality, consider

$$W_f = \sum_{s_1,...,s_n \in \{0,1\}} \beta_f(s_1,...,s_n) \sigma(\mathbf{a}^1_{s_1}) \otimes ... \otimes \sigma(\mathbf{a}^n_{s_n}) \tag{10}$$

Where $\mathbf{a}_0^1, \mathbf{a}_1^1, ..., \mathbf{a}_0^n, \mathbf{a}_1^n$ are $2n$ arbitrary directions. We can calculate explicitly the eigenvalues of W_f [3,14]. Let $\mathbf{z}_j$ be the direction orthogonal to the vectors $\mathbf{a}_0^j, \mathbf{a}_1^j,\ j = 1, ..., n$. Denote by $|-1\rangle_j$ and $|1\rangle_j$ the states "spin-down" and "spin-up" in the $\mathbf{z}_j$-direction; so the vectors $|\omega_1, \omega_2, ..., \omega_n\rangle$, $\omega = (\omega_1, \omega_2, ..., \omega_n) \in \{-1, 1\}^n$ form a basis for the n-qbits space. Let $\mathbf{x}_j$ be orthogonal to $\mathbf{z}_j$ and let θ_s^j be the angle between $\mathbf{a}_s^j$ and $\mathbf{x}_j$, $s = 0, 1$. For each f there are 2^n eigenvectors of W_f which have the generalized GHZ form

$$|\Psi_f(\omega)\rangle = \frac{1}{\sqrt{2}}(e^{i\Theta(\omega)} |\omega_1, \omega_2, ..., \omega_n\rangle + |-\omega_1, -\omega_2, ..., -\omega_n\rangle) \tag{11}$$

and the corresponding eigenvalue

$$\lambda_f(\omega) = e^{i\Theta(\omega)} \sum_{s_1,...,s_n \in \{0,1\}} \beta_f(s_1, ..., s_n) \exp i \left(\omega_1 \theta_{s_1}^1 + ... + \omega_n \theta_{s_n}^n\right) \tag{12}$$

where $\Theta(\omega)$ in Eqs (11,12) is chosen so that $\lambda_f(\omega)$ is a real number. Hence

$$\|W_f\| = \max_{\omega} |\lambda_f(\omega)| \tag{13}$$

As in the CHSH case we can check how large $\|W_f\|$ can become as $\mathbf{a}_0^j, \mathbf{a}_1^j$ range over all possible directions. Using Eqs (12,13) we see that

$$\max_{directions} \|W_f\| = \max_{\theta_0^1, \theta_1^1, ...,\ \theta_0^n, \theta_1^n} \left| \sum_{s_1,...,s_n \in \{0,1\}} \beta_f(s_1, ..., s_n) \exp i \left(\theta_{s_1}^1 + ... + \theta_{s_n}^n\right) \right| \tag{14}$$

with the maximum on the left is taken over all possible choices of directions $\mathbf{a}_0^1, \mathbf{a}_1^1, ..., \mathbf{a}_0^n, \mathbf{a}_1^n$. The Mermin-Klyshko operators [2], mentioned previously, correspond to a particular choice of $f_0 : \{0, 1\}^n \to \{-1, 1\}$ and $\mathbf{a}_0^j, \mathbf{a}_1^j$, with the result that $\|W_{f_0}\| = \sqrt{2^{n-1}}$. This is the maximal value of Eq (14) possible. The maximum value is attained by a small minority of the operators W_f, only those which are obtained from W_{f_0} by one of the $n!2^{2n+1}$ symmetry operations of the polytope C_n (as compared with the total of 2^{2^n} of facets in Eq (6)).

In any case, for most f 's there is a choice of angles such that W_f is a witness. This means that in addition to the fact that $|tr(\rho W_f)| \leq 1$ for every separable state ρ, we also have $\|W_f\| > 1$. The 2^n exceptional cases are those in which the inequality in Eq (6) degenerates into the trivial condition $1 \leq X_{s_1}^1 X_{s_2}^2 ... X_{s_n}^n \leq 1$. All the other W_f's are witnesses. The reason is that all inequalities of type Eq (6) are obtained from the basic inequalities for C_2 (including the trivial ones) by iteration [3]. If the iteration contains even one instance of the type Eq (2) the corresponding operator can be chosen to violate the CHSH inequality.

III. RANDOM WITNESSES

A. Typical behavior of $\max\limits_{directions} \|W_f\|$

Although the norm of $\|W_f\|$ can reach as high as $\sqrt{2^{n-1}}$ this is not the rule but the exception. Our aim is to estimate the *typical* behavior of $\max\limits_{directions} \|W_f\|$ as we let f range over all its values. To do that, consider the set of all 2^{2^n} functions $f : \{0,1\}^n \to \{-1,1\}$ as a probability space with a uniform probability distribution $\mathcal{P}$, which assigns probability 2^{-2^n} to each one of the f's. Then, for each set of fixed directions $\mathbf{a}_i^j$ we can look at $\|W_f\|$ as a random variable defined on the space of f's. Likewise, also $\max\limits_{directions} \|W_f\|$ in Eq (14) is a random variable on the space of f's, for which we have

Theorem 1 *There is a universal constant C such that*

$$\mathcal{P}\ \{f;\ \max_{directions} \|W_f\| > C\sqrt{n \log n}\ \} \to 0 \quad as\ n \to \infty \tag{15}$$

The proof of this result is based on the theorem of Salem, Zygmund, and Kahane [15] and is given in the appendix. This means that for the vast majority of the f's the violation of the classical inequalities Eq (6) is small. Accordingly, the boundary of Q_n is highly uneven about the facets of C_n, it does not extend far above most of the facets of C_n, but occasionally it has an extended exponential hump.

The expected growth of $|\lambda_f|$ is even slower when the directions $\mathbf{a}_i^j$ (or the angles θ_i^j) are fixed.As a direct consequence of Tchebychev's inequality [16] we get:

Proposition 2 *For λ_f in Eq (12) we have for all $M > 1$: $\mathcal{P}\ \{f;\ |\lambda_f| > M\} \leq \frac{1}{M^2}$.*

(See the appendix for details). This means that most of the eigenvalues of the W_f's are bounded within a small sphere. The application of a randomly chosen W_f to any of its eigenstates $|\Psi_f(\omega)\rangle$ in Eq (12) is unlikely to reveal a significunt violation of Eq (6).

B. The random witness conjecture

For appropriate choices of angles the Werner-Wolf operators Eq (10) are, with very few exceptions, entanglement witnesses on the space of n q-bits They are very special witnesses for two reasons: firstly, they are local operators. This means that if we posses many copies of a system made of n-qbits, all in the same state $|\Phi\rangle$, we can measure the expectation $\langle\Phi\,|W_f|\,\Phi\rangle$ by performing separate measurements on each qbit of the system. Secondly, even as local observables the Werner Wolf operators are special, because of the restriction to two measurements per particle. Indeed, one would have liked to extend the results beyond this restriction, and obtain all the inequalities for any number of measurement per site, but this problem is NP-hard even for $n = 2$. [17]

However, the W_f's are the most likely to be violated among such local operators, because they are derived from the facets of C_n. There are, therefore, reasons to believe that iMoreover, we already noted that all the norm estimates are also valid for the wider family given in Eq (9), with the A^i_j's acting on any finite dimensional space, and satisfying $(A^i_j)^2 = I$. Hence, the estimate of theorem 1 includes many more witnesses than those given in Eq (10). To an n qbits system we can add auxiliary particles and use quantum and classical communication protocols. As long as our overall measurement retains the structure

$$W = \sum_{s_1,\dots,s_k\in\{0,1\}} \beta_f(s_1,\dots,s_k) A^1_{s_1}\otimes\dots\otimes A^k_{s_k} \tag{16}$$

with the A^i_j's satisfying $(A^i_j)^2 = I$ and $k \leq O(n)$, the estimate of theorem 1 holds.

Hence, there is a reason to suspect that the typical behavior of the Werner Wolf operators is also typical of general random witnesses. A random witness is an observable drawn from the set of all witnesses $\mathcal{W}$ with uniform probability. It is easy to give an abstract description of $\mathcal{W}$: Consider the space of Hermitian operators on $(\mathbb{C}^2)^{\otimes n}$, it has dimension $d_n = 2^{n-1}(2^n + 1)$. For an Hermitian operator A define the norm $[[A]] = \sup \| A \, |\alpha_1\rangle \ldots |\alpha_n\rangle \|$ where the supremum ranges over all choices of unit vectors $|\alpha_i\rangle \in \mathbb{C}^2$. Denote the unit sphere in this norm by $\mathcal{K}_1 = \{A; \; [[A]] = 1\}$. It is a hypersurface of dimension $d_n - 1$, which is equipped with the uniform (Lebesgue) measure, and its total hyper-area is finite. Now, denote by $\mathcal{K}_2$ the normal unit sphere $\mathcal{K}_2 = \{A; \; \|A\| = 1\}$. Here, as usual, $\|A\| = \sup \|A \, |\Phi\rangle \|$ is the operator norm, where the supremum is taken over all unit vectors $|\Phi\rangle$. The set of witnesses is $\mathcal{W} = \mathcal{K}_1 \setminus \mathcal{K}_2$. Note that if $A \in \mathcal{W}$ then necessarily $\|A\| > 1$. It is not difficult to see that $\mathcal{W}$ is relatively open in $\mathcal{K}_1$, and therefore has a non zero measure in $\mathcal{K}_1$. We consider the set of all witnesses $\mathcal{W}$ on $(\mathbb{C}^2)^{\otimes n}$ and the normalized Lebesgue measure $\mathcal{P}$ on it.

Conjecture 3 *There is a universal constant C such that*

$$\mathcal{P} \; \{W \in \mathcal{W}; \quad \|W\| > C\sqrt{n \log n} \; \} \to 0 \quad \textit{as } n \to \infty. \tag{17}$$

C. Discussion

Assume the conjecture is valid and consider the following highly ideal situation: A macroscopic object (a single copy of it) is prepared in a state unknown to us and is carefully kept insulated from environmental decoherence. Since the state is unknown we choose randomly a witness W to examine it. Now, suppose that we hit the pot and the system happens to be in an eigenstate of W; in fact, the eigenstate corresponding to its maximum eigenvalue (in absolute value). This means, in particular, that the state of the system is entangled; but can we detect this fact using W? A measurement of a witness *on a single copy* is a very complicated affair (just think about any one of the W_f's in Eq (10)). Such a measurement invariably involves manipulations of the individual particles. If we make the reasonable assumption that each such manipulation introduces a small independent error, we obtain a total measurement error that grows exponentially with n. By the random witness conjecture, Eq (17), this means that we are unlikely to see a clear non-classical effect. The typical witness is a poor witness.

If this is true in the idealized situation it is all the more true with respect to the "measurements" performed by our sensory organs. Arguably, one can associate with observation, in the everyday non-technical sense, a quantum mechanical operator. However, it is not very likely to be an entanglement witness, and even on the happy occasion that it is, it is not likely to reveal anything. So even if my cat miraculously avoided decoherence and remained in an entangled state, I am unlikely to see anything non classical about him.

Note that this analysis is not meant as a solution to the measurement problem. The measurement problem is a dilemma that concerns the $\psi - realists$, who maintain that the quantum state is a part of physical reality (and not merely our description of it). For the ψ-realists the fact that the cat can be in a dead-alive superposition is itself a problem, regardless of weather we can actually detect such a state in practice. The present discussion is agnostic with respect to the reality of the quantum state, and strives to explain why large things would hardly ever *appear* to us non-classical even if decoherence were turned off.

All this does not mean, of course, that we cannot see large scale entanglements. If a system has been carefully prepared in a known special state (say, the generalized GHZ state Eq (11)) and its coherency has been maintained, we may be able to tailor an experiment to verify this fact. Hopefully, this will happened when quantum computers are developed. However, as n grows the task is becoming exponentially more difficult.

There is some analogy between the present approach to multiparticle systems and the point made by Khinchin on the foundations of classical statistical mechanics [18,19]. While thermodynamic equilibrium has its origins in the dynamics of the molecules, much of the *observable* qualities of multiparticle systems can be explained on the basis of the law of large numbers. The tradition which began with Boltzmann identifies equilibrium with ergodicity. The condition of ergodicity ensures that every integrable function has identical phase-space and long-time averages. However, Khinchine points out that this is an overkill, because most of the integrable functions do not correspond to macroscopic (that is, thermodynamic) observables. If we concentrate on thermodynamic observables, which involve averages over an enormous number of particles, weaker dynamical assumptions will do the job.

I believe that a similar answer can be given to our original question, namely, why we do not see large macroscopic objects in entangled states. Since decoherence cannot be "turned off" the multiparticle systems that we encounter are never maximally entangled. But even if the amount of entanglement that remains in them is still significant, *we* cannot detect it, because the witnesses are simply too weak.

IV. APPENDIX

In the proof of theorem 1 we shall rely on a theorem in Fourier analysis due to Salem, Zygmund and Kahane [15]. Our aim is to consider random trigonometric polynomials. So let $(\Omega, \Sigma, \mathcal{P})$ be a probability space, where Ω is a set, Σ a σ-algebra of subsets of Ω, and $\mathcal{P} : \Sigma \to [0, 1]$ a probability measure. For a random variable ξ on Ω denote by $\mathcal{E}(\xi) = \int_\Omega \xi(\omega) d\mathcal{P}(\omega)$ the expectation of ξ. A real random variable ξ is called *subnormal* if $\mathcal{E}(\exp(\lambda\xi)) \leq \exp(\frac{\lambda^2}{2})$ for all $-\infty < \lambda < \infty$.

A trigonometric polynomial in r variables is a function on the torus $\mathbb{T}^r$ given by

$$g(\mathbf{t}) = g(t_1, t_2, ..., t_r) = \sum b(k_1, k_2, ..., k_r) e^{i(k_1 t_1 +, k_2 t_2 + ... + k_r t_r)} \tag{18}$$

where the sum is taken over all negative and nonnegative integers $k_1, k_2, ..., k_r$ which satisfy $|k_1| + |k_2| + ... + |k_r| \leq N$. The integer N is called *the degree of the polynomial.* Denote $\|g\|_\infty = \max_{t_1,...,t_r} |g(t_1, t_2, ..., t_r)|$.

Theorem 4 *(Salem, Zygmund, Kahane) Let the $\xi_j(\omega)$, $j = 1, 2, ..., J$ be a finite sequence of real, independent, subnormal random variables on Ω. Let $g_j(\mathbf{t})$, $j = 1, 2, ..., J$ be a sequence of trigonometric polynomials in r variables whose degree is less or equal N, and such that $\sum_j |g(\mathbf{t})|^2 \leq 1$ for all $\mathbf{t}$. Then*

$$\mathcal{P} \left\{ \omega; \quad \left\| \sum_{j=1}^{J} \xi_j(\omega) g_j(\mathbf{t}) \right\|_\infty > C\sqrt{r \log N} \right\} \leq \frac{1}{N^2 e^r} \tag{19}$$

for some universal constat C.

Note that the formulation here is slightly different from that in [15], but the proof is identical. Our probability space Ω is the set of all functions $f : \{0,1\}^n \to \{-1,1\}$ with the uniform distribution which assigns each such function f a weight 2^{-2^n}. On this space consider the 2^n random variables $\xi_\varepsilon(f)$ defined for each $\varepsilon = (\varepsilon_1, ..., \varepsilon_n) \in \{0,1\}^n$ by

$$\xi_\varepsilon(f) = f(\varepsilon) \tag{20}$$

Now, note that $f \in \Omega$ iff $-f \in \Omega$ hence for each fixed ε we get $\mathcal{E}(\xi_\varepsilon) = 2^{-2^n} \sum_f f(\varepsilon) = -2^{-2^n} \sum_f f(\varepsilon) = -\mathcal{E}(\xi_\varepsilon)$, and therefore $\mathcal{E}(\xi_\varepsilon) = 0$, similarly, for $\varepsilon, \varepsilon'$ we have $\mathcal{E}(\xi_\varepsilon \xi_{\varepsilon'}) = \delta(\varepsilon, \varepsilon')$ and so on; the 2^n random variables $\xi_\varepsilon(f)$ are independent. Now, by a similar argument

$$\begin{gathered}\mathcal{E}(\exp(\lambda \xi_\varepsilon)) = 2^{-2^n} \sum_f \exp(\lambda f(\varepsilon)) = \\ 2^{-2^n} \sum_f \frac{1}{2}[\exp(\lambda f(\varepsilon)) + \exp(-\lambda f(\varepsilon))] = \frac{1}{2}(e^\lambda + e^{-\lambda}) \leq e^{\frac{\lambda^2}{2}}\end{gathered} \tag{21}$$

To define the trigonometric polynomials note that by Eq (7,20)

$$\begin{aligned}&\sum_{s_1,...,s_n \in \{0,1\}} \beta_f(s_1, ..., s_n) \exp i \left(t^1_{s_1} + ... + t^n_{s_n}\right) = \\ &= \frac{1}{2^n} \sum_\varepsilon f(\varepsilon) \sum_{\mathbf{s}} (-1)^{\varepsilon_1 s_1 + ... + \varepsilon_n s_n} \exp i \left(t^1_{s_1} + t^2_{s_2} + ... + t^n_{s_n}\right) = \\ &= \sum_\varepsilon f(\varepsilon) \frac{1}{2^n} \prod_{j=1}^n \left(\exp it^j_0 + (-1)^{\varepsilon_j} \exp it^j_1\right) = \sum_\varepsilon \xi_\varepsilon(f) g_\varepsilon(\mathbf{t})\end{aligned} \tag{22}$$

with

$$g_\varepsilon(\mathbf{t}) = 2^{-n} \prod_j \left(\exp it^j_0 + (-1)^{\varepsilon_j} \exp it^j_1\right) \tag{23}$$

The polynomials $g_\varepsilon(\mathbf{t})$ do not depend on f, have $2n$ variables $t^j_0,\ t^j_1,\ j = 1, 2, ..., n$, and their degree is n. We shall prove that $\sum_\varepsilon |g_\varepsilon(\mathbf{t})|^2 = 1$ for all $\mathbf{t}$. Indeed, $|g_\varepsilon(\mathbf{t})|^2 = 2^{-2n} \left|\prod_j \left(1 + (-1)^{\varepsilon_j} \exp(i\phi_j)\right)\right|^2$, with $\phi_j = t^j_1 - t^j_0$. But, $|1 + \exp i\phi_j|^2 = 4\cos^2\left(\frac{\phi_j}{2}\right)$ and $|1 - \exp i\phi_j|^2 = 4\sin^2\left(\frac{\phi_j}{2}\right)$ and therefore $\sum_\varepsilon |g_\varepsilon(\mathbf{t})|^2 = \prod_j \left(\cos^2\left(\frac{\phi_j}{2}\right) + \sin^2\left(\frac{\phi_j}{2}\right)\right) = 1$.

From Eqs (14,22) we get

$$\max_{directions} \|W_f\| = \left\| \sum_{\varepsilon} \xi_{\varepsilon}(f) g_{\varepsilon}(\mathbf{t}) \right\|_{\infty} \tag{24}$$

Hence, we can apply the Salem Zygmund Kahane inequality Eq (19) to the present case, with $N = n$ and $r = 2n$, to obtain theorem 1.

To prove proposition 2 consider $|\lambda_f|$ as a random variable on the space of f's. By Eq (12) we get

$$|\lambda_f| = \left| \sum_{s_1,...,s_n \in \{0,1\}} \beta_f(s_1, ..., s_n) \exp i \left(t^1_{s_1} + ... + t^n_{s_n} \right) \right| \tag{25}$$

with $t^j_{s_n} = \omega_j \theta^j_{s_n}$. By Eq (22) we get $|\lambda_f| = |\sum_{\varepsilon} \xi_{\varepsilon}(f) g_{\varepsilon}(\mathbf{t})|$. But $\mathcal{E}(\sum_{\varepsilon} \xi_{\varepsilon} g_{\varepsilon}) = 0$, and $\mathcal{E}(|\sum_{\varepsilon} \xi_{\varepsilon} g_{\varepsilon}|^2) = \sum_{\varepsilon} |g_{\varepsilon}|^2 = 1$. Therefore, by Tchebishev's inequality we have $\mathcal{P}\ \{f;\ |\lambda_f| > M\} \leq \frac{1}{M^2}$ for all $M > 1$.

Acknowledgement 5 *The research for this paper was done while I was visiting the Perimeter Institute, I am grateful for the hospitality. This research is supported by the Israel Science Foundation, grant number 879/02.*

REFERENCES

[1] B. M. Terhal , *J. Theor. Comp. Sci.* **287**, 313 (2002).

[2] N. D. Mermin, *Phys. Rev. Lett.* **65**, 1838 (1990).

[3] R. F. Werner and M. M. Wolf, *Phys. Rev. A* **64**, 032112 (2001).

[4] J.F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys.Rev. Lett.* **23**, 880 (1969).

[5] A. Fine, *Phys. Rev. Lett.* **48**, 291 (1982).

[6] I. Pitowsky, *Quantum Probability-Quantum Logic* (Springer, Berlin, 1989).

[7] N. Gisin, and A. Peres, *Phys. Lett. A* **162**, 15 (1992)

[8] B. S. Cirel'son, *Lett. Math. Phys.* **4**, 93 (1980).

[9] B. S. Tsirel'son, *J. Sov. Math.* **36**, 557 (1987)

[10] S. Phillip and K, Svozil, *Phys. Rev. A* **63**, 032101 (2004).

[11] A. Cabello, *Phys. Rev. Lett.* **92** 060403 (2004)

[12] F. A. Bovino and G. Castagnoli, *Phys.Rev.Lett.* **92**, 060404 (2004)

[13] W. Rudin, *Fourier Analysis on Groups* (Interscience Publishers, New York, 1960).

[14] V. Scarani and N. Gisin, e-print *quant-ph/0103068.*

[15] J. P. Kahane, *Some Random Series of Functions* (Cambridge University Press, Cambridge, second edition, 1985)

[16] Y. S. Chow and H. Teicher, *Probability Theory, Independence, Interchangeability, Martingales* (Springer, Berlin 1978).

[17] I. Pitowsky, *Math. Programming A* **50**, 395 (1991).

[18] A. I. Khinchin, *Mathematical foundations of Statistical Mechanics* (Dover, New-York 1949).

[19] I. Pitowsky, *Studies Hist. Phil. of Mod. Phy.*, **32**, 595 (2001).