Quantum Pseudo-Telepathy and the Kochen-Specker Theorem

Renato Renner * Stefan Wolf †

Abstract

According to results by Specker, Bell, and Kochen and Specker—among others—, quantum mechanical systems can generally not be described by *hidden variables*, i.e., classical parameters determining the system's behavior under all possible measurements. Kochen and Specker's result implies that three- or higher-dimensional systems cannot be deterministically and consistently prepared in a classical way for all possible alternative measurements simultaneously, whereas Bell showed that the behavior of entangled parts of a quantum system can be *non-local*: classically, it could be explained only by communication between the parts, not by shared information. *Pseudo-telepathy games*, which have been introduced as a deterministic version of non-local behavior, are distributed tasks that can be fulfilled with shared quantum—but not classical—information. We show a close connection between the results of Kochen and Specker on one side, and non-locality, i.e., pseudo telepathy, on the other: Every set of alternative measurements of a quantum system which is "unpredictable" in the sense of the Kochen-Specker theorem leads to a pseudo-telepathy game, and *vice versa*. It is a consequence of our results that pseudo-telepathy games exist that use a maximally entangled quantum trit pair as a resource, whereas there is no such game requiring a quantum bit pair only.

1 Quantum Mechanics and Hidden Variables

1.1 The Kochen-Specker Theorem: Weak and Strong Kochen-Specker Sets

It has been a central objective in the history of quantum mechanics to embed quantum theory into a classical theory, based on so-called *hidden variables*. The fundamental impossibility of this approach was shown roughly forty years ago by Specker [8], Bell [1], and Kochen and Specker [6]. In [8] and [6] it was shown—by a purely algebraical proof—that the behavior of a three- (or higher-) dimensional quantum system cannot be described in a consistent way by hidden variables. Roughly speaking, they proved that somebody who claims to be able to predict the behavior of such a system under all possible alternative measurements can be forced into a contradiction—all these alternative outcomes do simply not co-exist in a deterministic and consistent way. More precisely, Specker's and Kochen and Specker's results imply that any attempt of determining a definite measurement outcome for any possible measurement basis must necessarily be *contextual*: It is impossible to assign values 0 and 1 to all unit vectors in the three-dimensional Hilbert space $\mathcal{H} = \mathbf{C}^3$ in such a way that every orthonormal basis contains *exactly one* vector with value 1—this vector would be the corresponding measurement outcome. Interestingly, Kochen and Specker showed that this impossibility can already hold with respect to a finite set of vectors.

Definition 1. A *Kochen-Specker set* (*KS set* for short) in $\mathcal{H} = \mathbf{C}^n$ is a set $S \subseteq \mathcal{H}$ of unit vectors such that there exists no function $f : S \to \{0, 1\}$ with the property that if $b \subseteq S$ is an

*Department of Computer Science, ETH Zürich, Switzerland. Email: renner@inf.ethz.ch .

†Département d'Informatique et recherche opérationnelle, Université de Montréal, Canada. E-mail: wolf@iro.umontreal.ca .

orthonormal basis of $\mathcal{H}$, then

$$\sum_{u \in b} f(u) = 1$$

holds.

Theorem 1. [8], [6] *There exists a finite KS set $S \subseteq \mathcal{H} = \mathbf{C}^n$ for $n \geq 3$. There exists no KS set $S \subseteq \mathcal{H} = \mathbf{C}^2$ (in other words, $S = \mathcal{H} = \mathbf{C}^2$ is not a KS set).*

The impossibility of consistently predicting—or predetermining—the outcomes of a set of alternative measurements can in fact be derived from a slightly weaker notion than the one of a KS set—namely from a set of vectors on which any "prediction function" f inevitably assigns the value 1 to two orthogonal vectors.

Definition 2. A *weak Kochen-Specker set* (*weak KS set* for short) in $\mathcal{H} = \mathbf{C}^n$ is a set $S \subseteq \mathcal{H}$ of unit vectors such that for every function $f : S \to \{0, 1\}$ satisfying that for every orthonormal basis $b \subseteq S$ of $\mathcal{H}$

$$\sum_{u \in b} f(u) = 1$$

holds, there exist vectors $u, v \in S$ with $\langle u|v\rangle = 0$ and $f(u) = f(v) = 1$.

Clearly, every KS set is a weak KS set (since *no* function f with the mentioned property exists *at all*); on the other hand, every weak set S can be extended to a KS set S' with $O(|S|^2 n)$ additional vectors. In particular, there exists a KS set in some Hilbert space $\mathcal{H}$ if and only if there exists a weak KS set in $\mathcal{H}$.

Lemma 2. *Let $\mathcal{H} = \mathbf{C}^n$ and let $S \subseteq \mathcal{H}$ be a finite weak KS set. Then there exists a finite KS set S', $S \subseteq S' \subseteq \mathcal{H}$ with*

$$|S' \setminus S| \leq \frac{|S|(|S| - 1)}{2} (n - 2) \ . \tag{1}$$

Proof. Every pair of orthonormal vectors in S can be extended to an orthonormal basis by adding $n - 2$ vectors. Hence there exists a set $S' \supseteq S$ satisfying inequality (1) and such that every pair of orthogonal vectors in S is contained in some orthonormal basis $b \subseteq S'$. Let f be a function $f : S' \to \{0, 1\}$ with $\sum_{u \in b} f(u) = 1$ for every orthonormal basis $b \subseteq S'$. Clearly, the restriction of f to S has the same property, hence there exist $u, v \in S$ with $\langle u|v\rangle = 0$ and $f(u) = f(v) = 1$. For the basis $b \subseteq S'$ containing u and v we have $\sum_{w \in b} f(w) \geq f(u) + f(v) = 2$. □

1.2 Non-Locality, Bell's Inequality, and Pseudo-Telepathy

A different approach to showing the impossibility of hidden-variable explanations for the behavior of quantum systems was taken by Bell [1]. According to quantum mechanics, two two-dimensional systems, called *quantum bits* or *Qbits* for short, can—even when physically separated—be in a joint state which cannot be completely described by giving the states of the two Qbits separately; such a state is called *entangled*. An example was given by Einstein, Podolsky, and Rosen [3] as

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \ .$$

Bell showed that the joint behavior with respect to different measurements on the two subsystems of this state cannot be explained by shared classical information under the assumption that no communication is allowed between the two parts of the system. More precisely, Bell derived certain inequalities—the *Bell inequalities*—that are satisfied for all systems the behavior of which *do* have a classical explanation; he then showed that they are violated by the behavior of the EPR state $|\Phi^+\rangle$. This *non-locality* or "Spukhafte Fernwirkung—spooky action

at a distance—", although it does not allow the parties controlling the distant systems for (instant) message transmission, implies that no classical hidden-variable theory can explain their behavior.

"Pseudo-telepathy" [2] is a deterministic version of non-local behavior: Two distant parties unable to communicate but sharing a certain entangled quantum state—for instance n copies of the state $|\Phi^+\rangle$—can satisfy some *deterministic* condition on their mutual input-output behavior with certainty, whereas parties *without* shared entanglement—even when having agreed on a "classical" strategy beforehand—cannot.

Definition 3. Let $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, and let $|\Psi\rangle \in \mathcal{H}$ be a pure state. A *pseudo-telepathy game with respect to* $|\Psi\rangle$ ($|\Psi\rangle$-*PT game* for short) is a pair (B_1, B_2), where B_i is a set of orthonormal bases of $\mathcal{H}_i$, such that the following holds. Let g be the following function defined on $B_1 \times B_2$: $g((b_1, b_2))$ is the set of pairs $(u_1, u_2) \in b_1 \times b_2$ satisfying

$$\langle \Psi | u_1, u_2 \rangle \neq 0 \ ;$$

the latter condition means that the measurement outcome (u_1, u_2) has non-zero probability if $|\Psi\rangle$ is measured with respect to the basis $b_1 \times b_2$ of $\mathcal{H}$. Then we must have that, for every pair of functions (s_1, s_2)—a classical strategy—, where s_i is defined on B_i and $s_i(b_i) \in b_i$ holds for all $b_i \in B_i$, there must exist particular bases $b_1 \in B_1$ and $b_2 \in B_2$ such that

$$(s_1(b_1), s_2(b_2)) \notin g((b_1, b_2))$$

holds.

It is the goal of this paper to show a close connection between PT games and the Kochen-Specker theorem. More precisely, we show that every weak KS set leads to a PT game (Section 2.1), and that every PT game with respect to a maximally entangled state leads to a KS set in some Hilbert space (Section 2.2). Two consequences are that there exists a PT game between two parties sharing only one maximally entangled "Qtrit"—i.e., the state $(|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$—, but that no such game exists (at least if only so-called *von Neumann measurements*, i.e., measurements with respect to an orthonormal basis of $\mathbf{C}^2$, are carried out) when only an EPR state $|\Phi^+\rangle$ is shared.

2 Linking the Kochen-Specker Theorem and Pseudo-Telepathy Games

2.1 Pseudo-Telepathy from any Weak Kochen-Specker Set

Definition 4. Let $\mathcal{H} = \mathbf{C}^n$, and let $c = \{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$ and $b = \{u_0, u_1, \ldots, u_{n-1}\}$ be orthonormal bases of $\mathcal{H}$. Then the *complex conjugate basis* $\overline{b}$ of b (with respect to c) is $\overline{b} = \{\overline{u_0}, \overline{u_1}, \ldots, \overline{u_{n-1}}\}$ with $\overline{u_i} = \overline{U}|i\rangle$, where U is the unitary operator on $\mathcal{H}$ satisfying $b = Uc$, i.e., $u_i = U|i\rangle$ for $i = 0, 1, \ldots, n-1$. For a set B of bases, we denote by $\overline{B}$ the set of complex conjugate bases.

Theorem 3. *Let* $\mathcal{H} = \mathbf{C}^n$, $S \subseteq \mathcal{H}$, $c = \{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$ *and* $b = \{u_0, u_1, \ldots, u_{n-1}\}$ *be orthonormal bases of* $\mathcal{H}$, *and let*

$$B = \{b \subseteq S \,|\, b \text{ is an orthonormal basis of } \mathcal{H}\} \ .$$

Consider the state

$$|\Psi\rangle := \frac{1}{\sqrt{n}}(|00\rangle + |11\rangle + \cdots + |n-1, n-1\rangle) \in \mathcal{H} \otimes \mathcal{H} \ .$$

If S *is a weak KS set in* $\mathcal{H}$, *then* $(B, \overline{B})$ *is a* $|\Psi\rangle$-*PT game.*

Proof. Let s_1 and s_2 be two functions such that for all $b \in B$ and $\overline{b'} \in \overline{B}$, we have $s_1(b) \in b$ and $s_2(\overline{b'}) \in \overline{b'}$. Let now for $u \in S$

$$f(u) := \begin{cases} 1 & \text{if there exists } u \in b \in B \text{ such that } s_1(b) = u \ , \\ 0 & \text{otherwise} \ . \end{cases}$$

Clearly, we have for every $b \in B$ that

$$\sum_{u \in b} f(u) \geq 1$$

holds. Since S is a weak KS set, there exist $u, u' \in S$ with $\langle u|u' \rangle = 0$ and $f(u) = f(u') = 1$. Let $b, b' \in B$ such that $s_1(b) = u$, $s_1(b') = u'$. Clearly, we have either $s_2(\overline{b'}) \neq \overline{u'}$ or $s_2(\overline{b'}) = \overline{u'}$. We show that the condition for a PT game is satisfied in both cases.

Assume first $s_2(\overline{b'}) := \overline{u''} \neq \overline{u'}$. Then u' and u'', which both belong to b', are orthogonal vectors and we get

$$\langle \Psi | u', \overline{u''} \rangle = \frac{1}{\sqrt{n}} \sum_i \langle i|u' \rangle \langle i|\overline{u''} \rangle = \frac{1}{\sqrt{n}} \overline{\langle u'|u'' \rangle} = 0 \ ;$$

hence,

$$(s_1(b'), s_2(\overline{b'})) = (u', \overline{u''}) \notin g((b', \overline{b'}))$$

holds since the probability of this output is 0.

If we have, on the other hand, $s_2(\overline{b'}) = \overline{u'}$, we can conclude

$$(s_1(b), s_2(\overline{b'})) = (u, \overline{u'}) \notin g((b, \overline{b'}))$$

in a similar way since u and u' are orthogonal. □

A consequence of Theorems 1 and 3 is that there exists a PT game between parties sharing only one Qtrit pair. A game using such a small amount of entanglement has not been proposed previously.

Corollary 4. *There exists a* $((|00\rangle + |11\rangle + |22\rangle)/\sqrt{3})$*-PT game.*

In [6], a KS set in $\mathcal{H} = \mathbf{C}^3$ with 117 elements is given. It has been shown later that there exist much smaller such sets; for instance, there exists a KS set with 33 vectors belonging to 16 different orthonormal bases of $\mathcal{H}$. According to Theorem 3, this leads to a PT game where each party gets one of 16 possible inputs—one of the 16 bases; the condition for "winning the game" is that identical bases must be answered by identical vectors, whereas bases that have a vector in common must be answered by the overlapping vector by both parties, or *not* by this vector by both parties.

2.2 Kochen-Specker Sets from Pseudo-Telepathy Games

Theorem 5. *Let* $\mathcal{H} = \mathbf{C}^n$, $c = \{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$ *be an orthonormal basis of* $\mathcal{H}$, *let* B_1 *and* B_2 *be two sets of orthonormal bases of* $\mathcal{H}$, *and let*

$$|\Psi\rangle = \frac{1}{\sqrt{n}}(|00\rangle + |11\rangle + \cdots + |n-1, n-1\rangle) \in \mathcal{H} \otimes \mathcal{H} \ .$$

Let finally S *be the set*

$$S := \bigcup_{b \in B_1} b \ \cup \bigcup_{b \in B_2} \overline{b} \quad \subseteq \mathcal{H} \ .$$

If (B_1, B_2) *is a* $|\Psi\rangle$*-PT game, then* S *is a weak KS set in* $\mathcal{H}$.

Proof. Let $f : S \to \{0,1\}$ be a function such that for all orthonormal bases $b \subseteq S$, we have $\sum_{u \in b} f(u) = 1$.

Let, for any $b_1 \in B_1$ and $b_2 \in B_2$, $s_1(b_1)$ and $s_2(b_2)$ be the elements u_1 and u_2 of b_1 and b_2, respectively, satisfying $f(u_1) = f(\overline{u_2}) = 1$. Because (B_1, B_2) is a $|\Psi\rangle$-PT game, there exist particular bases $b_1 \in B_1$ and $b_2 \in B_2$ with

$$(s_1(b_1), s_2(b_2)) \notin g((b_1, b_2)) \ .$$

Let $u_i = s_i(b_i)$. Now, $(u_1, u_2) \notin g((b_1, b_2))$ implies that this output pair occurs with probability 0, i.e.,

$$0 = \langle \Psi | u_1, u_2 \rangle = \frac{1}{\sqrt{n}} \sum_i \langle i | u_1 \rangle \langle i | u_2 \rangle = \frac{1}{\sqrt{n}} \overline{\langle u_1 | \overline{u_2} \rangle} \ .$$

We conclude that there exist two orthogonal vectors u_1 and $\overline{u_2}$ in S with $f(u_1) = f(\overline{u_2}) = 1$, and this concludes the proof. □

Theorem 5 implies that any PT game between parties sharing a state of the given form (for instance, k copies of $|\Phi^+\rangle$) leads to a weak KS set in the corresponding Hilbert space (e.g., $\mathcal{H} = \mathbf{C}^{2^k}$). It is, however, not clear how such a set can be derived from a PT game using a state of a different form.

Corollary 6, which is an immediate consequence of Theorem 5 and Lemma 2, implies that given the existence of a PT game, the corresponding Hilbert space contains a KS set (of limited size).

Corollary 6. *Let $\mathcal{H} = \mathbf{C}^n$, $c = \{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$ be an orthonormal basis of $\mathcal{H}$, let B_1 and B_2 be two sets of orthonormal bases of $\mathcal{H}$, and let*

$$|\Psi\rangle = \frac{1}{\sqrt{n}}(|00\rangle + |11\rangle + \cdots + |n-1, n-1\rangle) \in \mathcal{H} \otimes \mathcal{H} \ .$$

Let S be the set

$$S := \bigcup_{b \in B_1} b \ \cup \bigcup_{b \in B_2} \overline{b} \quad \subseteq \mathcal{H} \ .$$

If (B_1, B_2) is a $|\Psi\rangle$-PT game, then there exists a KS set S' with $S \subseteq S' \subseteq \mathcal{H}$ and such that

$$|S' \setminus S| \leq |B_1| \cdot |B_2| \cdot n^3$$

holds.

Proof. According to Theorem 5, S is a weak KS set; more precisely, there exist, for every "KS function" f, $u \in b \in B_1$ and $v \in b' \in B_2$ with $\langle u | v \rangle$ and $f(u) = f(v) = 1$. As in Lemma 2, S can be extended by at most

$$\left| \bigcup_{b \in B_1} b \right| \cdot \left| \bigcup_{b' \in B_2} b' \right| \cdot (n-2) \leq |B_1| n \cdot |B_2| n \cdot (n-2)$$

vectors to a set S' such that every orthogonal pair u, v with $u \in b \in B_1$ and $v \in b' \in B_2$ is in an orthonormal basis $b \subseteq S'$ of $\mathcal{H}$. Hence S' is a KS set. □

Corollary 7 is a consequence of Corollary 6 and Theorem 1 and suggests—together with Corollary 4—that the minimal quantum primitive allowing for a PT game is a maximally entangled Qtrit pair. (Note that Corollary 7 does *not* imply that the behavior of $|\Phi^+\rangle$ is *local*: This state *does* violate Bell's inequality.)

Corollary 7. *There exists no* $((|00\rangle + |11\rangle)/\sqrt{2})$*-PT game.*

Theorem 5 can be used to construct new KS sets from PT games. In Example 1, this is done for a game proposed by Brassard, Cleve, and Tapp [2] (see also [4]), which uses 4 EPR pairs as a resource. The resulting KS set in $\mathcal{H} = \mathbf{C}^{16}$ is highly symmetric (but rather large).

Example 1. In [2], the following PT game was introduced. For $n \in \mathbf{N}$, $N = 2^n$, let

$$B_1 = B_2 = \left\{ \left\{ \frac{1}{\sqrt{N}} \sum_{i \in \{0,1\}^n} (-1)^{i \cdot j \oplus z(i)} |i\rangle \;\middle|\; j \in \{0,1\}^n \right\} \;\middle|\; z : \{0,1\}^n \to \{0,1\} \right\} ;$$

these bases arise when the Hadamard transform is applied to the bases $\{\pm|i\rangle\}$ of $\mathcal{H} = \mathbf{C}^N$. In [4] it was shown that for

$$|\Psi\rangle = |\Phi^+\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{i \in \{0,1\}^n} |i, i\rangle ,$$

and for $N \geq 16$, this is a $|\Psi\rangle$-PT game. Hence Theorem 5 implies that in this case the set

$$S = \bigcup_{b \in B_1} b \;\cup \bigcup_{b \in B_2} \overline{b} \;= \left\{ \frac{1}{\sqrt{N}} \sum_{i \in \{0,1\}^n} (-1)^{z(i)} |i\rangle \;\middle|\; z : \{0,1\}^n \to \{0,1\} \right\}$$

is a weak KS set. It is in fact a KS set since every pair of orthogonal vectors can be extended to an orthonormal basis of $\mathcal{H}$ with vectors in S: The idea is, given two orthogonal vectors u and v corresponding to N-bit strings z_1 and z_2, respectively, with $d_H(z_1, z_2) = N/2$—which holds because u and v are orthogonal—, to choose $N - 2$ additional strings z such that the strings $z_1 \oplus z$ are the code words of a dual Hamming code. Hence, for instance, the set

$$S = \left\{ \frac{1}{4} \sum_{i=0}^{15} \pm|i\rangle \right\}$$

is a—highly symmetric—KS set in $\mathcal{H} = \mathbf{C}^{16}$ with 2^{16} elements (corresponding to the different choices of the 16 signs).

References

[1] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, *Physics*, Vol. 1, pp. 195–200, 1964.

[2] G. Brassard, R. Cleve, and A. Tapp, The cost of exactly simulating quantum entanglement with classical communication, *Physical Review Letter*, Vol. 83, No. 9, pp. 1874–1878, 1999.

[3] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, *Phys. Rev.*, Vol. 41, 1935.

[4] V. Galliard, A. Tapp, and S. Wolf, The impossibility of pseudo-telepathy without quantum entanglement, *Proceedings of ISIT 2003*, 2003.

[5] V. Galliard and S. Wolf, Pseudo-telepathy, entanglement, and graph colorings, *Proceedings of ISIT 2002*, 2002.

[6] S. Kochen and E. Specker, The problem of hidden variables in quantum mechanics, *Journal of Mathematics and Mechanics*, Vol. 17, No. 1, 1967.

[7] A. Peres, *Quantum theory: concepts and methods*, Kluwer Academic Publishers, 1993.

[8] E. Specker, Die Logik nicht gleichzeitig entscheidbarer Aussagen, *Dialectica*, Vol. 14, pp. 239–246, 1960.