Elem. Math. 67 (2012) 122 – 133
0013-6018/12/030122-12
DOI 10.4171/EM/201

Elemente der Mathematik

Ernst Specker and the Hidden Variables

Renato Renner and Stefan Wolf

Renato Renner studied theoretical physics at ETH Zürich, and received his PhD in 2005 under the supervision of Ueli Maurer. After a research period at the Centre for Quantum Computation, University of Cambridge UK, he returned to ETH in 2007 as Assistant Professor at the Institute for Theoretical Physics. His research interests are centered around quantum information theory and its applications in physics.

Stefan Wolf obtained his PhD in 1999 from ETH Zürich under the supervision of Ueli Maurer. After a postdoc at McGill University, Montréal, he was an Assistant professor at University of Waterloo, Ontario, and Université de Montréal, Québec, before he became an SNF Professor for Quantum Information at ETH. He is now Professor at the Università della Svizzera italiana, USI. His research domain lies in the fields of cryptography, information theory, and quantum information processing.

Introduction

In 1960, Ernst Specker showed, in an article written in German and entitled *"Die Logik nicht gleichzeitig entscheidbarer Aussagen"* (The logic of not simultaneously decidable propositions) that it is impossible to predict the behavior of a quantum-mechanical system under all possible measurements in a consistent and context-independent way. Later, John Bell showed a similar result based on the joint behavior of entangled pairs of particles, and on the assumption of *locality* instead of *non-contextuality*. We discuss the relevance and applications of these results. Moreover, we prove a rigorous link between the two lines of reasoning or, equivalently, between the assumptions of non-contextuality – which appears hard to translate to an actual experiment –, *versus* locality – which can be quite easily guaranteed in practice by a spacelike separation of the measurement events.

Ernst Speckers Ideen haben nicht nur innerhalb der Mathematik Generationen von Forschern inspiriert, sondern auch in den angrenzenden Gebieten wichtige Spuren hinterlassen. Renato Renner und Stefan Wolf illustrieren dies in der vorliegenden Arbeit am Beispiel der Quantenmechanik respektive der Quanteninformationstheorie.

1 Quantum Logic

When the second author joined ETH to study mathematics, Ernst Specker had already retired, but was still very present at the departement. One reason were numerous stories [1] about the charismatic and inspiring teacher, another was the logic seminar which continued to be held each year, and that had its origin back in the days of Paul Bernays. Since this seminar, which Ernst Specker held together with Hans Läuchli, was worthwhile attending just for Specker's constitutive introductory hours, a small community had gathered around it, and those people attended the event far beyond what was required by their studies' curricula. The seminar's topic changed every year, and the edition on "quantum logic" was the second author's first contact with the topic – the fascination for which, initiated by Specker, has never left him ever since. In his introductory address to the seminar, Specker told, in his very own narrative style, a tale about a wise teacher of an Assyrian prophets' school who was concerned with ruling the contest about the charms of his daughter, for whom he wanted to find a worthy future husband. The prophet showed to every candidate three boxes, each of which either contained a diamond or was empty. The task to be solved, namely to point out two boxes with similar content, seemed doable, but turned out impossible: Whatever pair of boxes was opened, one of them contained a diamond whereas the other was found empty. What was going on?

The tale is taken from Specker's work *"Die Logik nicht gleichzeitig entscheidbarer Aussagen"* (The logic of not simultaneously decidable propositions) [26], in which he discusses a modification of classical propositional logic by dropping the standard assumption that each couple of propositions can both always be assigned a definite truth value. Specker's starting point was his teacher Gonseth's quote *"La logique est d'abord une science naturelle"* – *"Logic is, first of all, a natural science"* [17], in some sense a paradigmatic predecessor of Landauer's *"Information is Physical"* [22], three decades later. In this spirit, the logic of quantum physics has been studied first by Birkhoff and von Neumann [6].

Specker asks: *"Kann die Beschreibung eines quantenmechanischen Systems durch Einführung von zusätzlichen – fiktiven – Aussagen so erweitert werden, dass im erweiterten Bereich die klassische Aussagenlogik gilt?"* – "Is it possible to extend the description of a quantum-mechanical system by adding additional – fictional – propositions in such a way that in the resulting domain, classical propositional logic governs?"

The question is answered to the negative: *"Ein elementargeometrisches Argument zeigt, dass* [. . .] *über ein quantenmechanisches System* (*von Ausnahmefällen abgesehen*) *keine konsistenten Prophezeiungen möglich sind."* – "An elementary-geometric argument shows that in general, no consistent prophecies are possible concerning the behavior of a quantum-mechanical system."

In Specker's own words, every prophet can be led into some sort of contradiction, not when compared to an actual experiment, but due to *unavoidable inner contradictions among his set of prophecies for alternative setups*. There is still a possible way out, namely if the prophet is able to predict *how* the system is measured, i.e., *which* of the alternatives really occurs. We discuss this point further in Section 4.3.

1. It has been reported that whenever someone had forgotten his or her key, yet claimed to have an office space in ETH's "math floor" HG G, Ernst Specker would ask that person "Was gibt i^i?".

2 Hidden Variables?

In 1935, Einstein, Podolsky, and Rosen (in the following, *EPR* for short) [12] have challenged quantum theory by stating that it might only be an incomplete description of nature. More specifically, the authors considered the joint behavior of certain entangled states; the argument has later been simplified by Bohm and Aharanov [7], who considered a maximally entangled state of two two-dimensional quantum systems. The reasoning of EPR was that since given the outcome of a measurement of *one* of the two parts of the entangled system, the outcome of a corresponding measurement of the *other* part can be predicted *with certainty* – and, therefore, must be seen as an "element of reality" –, this outcome must be represented in any complete theory, regardless of whether the measurement is actually carried out or not. In other words, quantum mechanics is incomplete and must be augmented by *hidden variables* predetermining the outcomes of all possible measurements that can be carried out. It should be noted that EPR's claim was, physically speaking, most natural: How else should one explain a correlation in the behavior of possibly distant particles that had been prepared together before they got separated?

Nevertheless, the program suggested by EPR turned out to be infeasible. Indeed, the decades that followed brought a series of results which complement each other up to a quite coherent picture letting it appear rather unnatural (to say the least) that the outcome of quantum measurements be predetermined before they are actually carried out. In this picture, Specker's result is a landmark.

Von Neumann [28] showed that no hidden-variable model was possible for which the expectation values of arbitrary observables depend linearly on the latter. The linearity assumption was dropped with respect to non-commuting observables by Jauch and Piron [20] as well as by Gleason [16]; that result prepared the ground for the work of Specker which is, in some sense, a consequence thereof. Specker's [26] as well as Kochen and Specker's [21] results imply that no *non-contextual* predetermination of all measurement outcomes is possible: Whether a quantum system "replies" by *yes* or *no* to a given "question" would depend on what *other* questions are asked.

In 1964, a breakthrough was achieved by John Bell [5], who showed that the joint behavior of entangled states, such as the singlet, was *beyond the explanatory power of shared randomness* if the measurement outcome was to be determined *locally* from the hidden variables and the choice of the measurement to be performed. These "spooky actions at a distance" have since been experimentally verified with respect to different settings and assumptions, e.g., [1], [27].

In Section 3, we prove a direct connection between the no-hidden-variable results based on *non-contextuality* on the one hand and on *locality* on the other. Our findings have already appeared in part in [24] [2].

2. The authors had proposed, at the time, to Ernst Specker to be a co-author of the work. Specker politely declined and added, smiling: "Das tut mir Leid für Ihre Erdös-Zahlen."

3 Linking the Kochen-Specker Theorem to Non-Locality

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

Specker's [26] and Kochen and Specker's [21] results on the impossibility of hidden-variable models 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, this impossibility even holds 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 orthonormal basis of $\mathcal{H}$, then

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

holds.

Theorem 1. [26], [21] *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, the set S of unit vectors in $\mathcal{H} = \mathbf{C}^2$ 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 $b \subseteq S'$. Assume there exists 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 $\sum_{w \in b'} f(w) \geq f(u) + f(v) = 2$. Therefore, no prediction function f can exist for S', which must thus be a KS set. □

3.2 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 [5]. 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 is

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

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*, even though it does not allow the parties controlling the distant systems for (instant) message transmission, implies that no local hidden-variable theory can explain their behavior.

"Pseudo-telepathy" [8] 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 condition holds. Let g be the function defined on $B_1 \times B_2$ such that $g((b_1, b_2))$ 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.

3.3 Pseudo-Telepathy from any Weak Kochen-Specker Set

We 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 3.3), and that every PT game with respect to a maximally entangled state leads to a KS set in some Hilbert space (Section 3.4). Two consequences are that there exists a PT game between two parties sharing only one maximally entangled *Qtrit* pair, i.e., the state $(|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$, but that no such game exists (at least with respect to *von Neumann measurements*) when only an EPR state $|\Phi^+\rangle$ is shared.

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*

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

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.

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

In [21], 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.

3.4 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

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

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 finishes 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

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

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 various Bell inequalities.)

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 [8] (see also [14]), 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 [8], 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 [14], 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_i, $i = 3, \ldots, N$, such that the strings $z_1 \oplus z_i$, $i = 1, \ldots, N$, 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).

4 What Do the Non-Local Correlations Mean?

The cause and consequences of non-local correlations have been a *mystery* and *challenging problem* up to this day; in addition, the phenomenon has turned out to be a potentially *precious resource* for information processing, as well as a *criterion* for the comparison and discussion of different interpretations of quantum theory.

4.1 Explanations

When faced with the problem of explaining an observed correlation between two events, we are used to choosing one of the two possibilities: Either a common cause explains the correlation, or an influence from one event to the other establishes it. In various experiments, *non-local* correlations between *spacelike separated* measurement events have been observed; this means that *both* our standard explanations of correlations are ruled out in this case. It has, therefore, been suggested that they might arise from some kind of "hidden influence" at finite yet *superluminal* speed (in some preferred reference frame). However, in a series of results [25], [11], [2], such an explanation has been ruled out as well, since it is self-contradictory in multi-partite scenarios.

4.2 Applications

Now, if it is indeed the case that the classical information representing the outcome of a quantum measurement arises spontaneously, and that pieces of such information generated in remote locations can be perfectly correlated, then it is natural to try applying the phenomenon, e.g., for cryptography: If the laboratories of two parties Alice and Bob are secured, and measurements of previously exchanged entangled systems are carried out, then the generated information cannot be known to any outside party, potentially controlling the entire environment.

This paradigm was pioneered in [13], realized in principle in [3], further developed in, e.g., [19], [18], and led to a variant of quantum key distribution where no trust in the manufacturer of the devices is required, nor into the fact that the adversary is limited by quantum physics – as long as superluminal signaling is excluded. The confidentiality of the generated keys is directly related to the impossibility of predicting the future, in principle, as Specker had put it in his seminal work: Pieces of information clearly *are* secret if they cannot be predicted *before* some given point in time, and as long as they are not leaked *after* that.

4.3 Lessons

In related work by the first author, it has been shown that quantum physics is complete if it is correct [10] under the assumption that measurement settings can be chosen freely. In [9], it was shown that this latter assumption can be relaxed to certain only *partially free* choices. This result supports the "all-or-nothing nature" of true randomness, already exposed in Specker's original article: *"In einem gewissen Sinne gehören aber auch die scholastischen Spekulationen über die Infuturabilien hieher, das heisst die Frage, ob sich die göttliche Allwissenheit auch auf Ereignisse erstrecke, die eingetreten wären, falls etwas geschehen wäre, was nicht geschehen ist."* – "In some sense, our statements also deal with the scholastic speculations about the *infuturabili*, i.e., the question whether divine omniscience also covers what would have happened if something had happened that has not happened."

Indeed, Specker's as well as Bell's findings indicate that the answer to this is *no*. Let us put it more explicitly, in Specker's terms: *Either* a prophet can predict which measurement will be carried out by an experimenter, together with its outcome, *or* he cannot predict the measurement choice, in which case, according to Specker's argument, he cannot consistently predict the *outcome* either. In this sense, even divine omniscience can, in principle, not be consistently extended to conditioning on alternatives mutually excluding each other. Roughly speaking, either we fail to be able to make spontaneous choices, or elementary particles must have that ability, too.

In a nutshell, this leaves us with only the extremal options of *no true free randomness at all*, or *omnipresent randomness*. It is unclear whether it is possible in principle to decide which is the case. However, non-local correlations *are* real and might serve as an illustrative criterion in the discussion and evaluation of the different options.

In an inherently random theory, such as the standard (Copenhagen) interpretation of quantum physics, the correlations are surprising and mysterious coïncidences without any "story to tell within space-time" (Nicolas Gisin).

A deterministic hidden-variable theory, e.g., Bohmian mechanics, must be such that the outcomes of one measurement potentially also depend not only on the hidden variables of another particle but also of the apparatus, ultimately even the experimenter, of that other particle. Bell disqualified such a thing as being "even more mind-boggling" than spontaneous correlations of spacelike separated random events [4].

In theories where no collapse and no randomness occurs, and where *decoherence* explains macroscopicity and classicality of information, it remains unexplained why the emerging "pseudo-classical" information perceived by us or observed in the laboratory shows the strange correlations. The mystery cannot be escaped unless the notion of classical information, or logic for that matter, including our assumption of one unique objective reality, is put into question entirely. Yet then, how would we explain our subjective perceptions of classical outcomes and *of their being correlated*, and how would we be to reason about them in the first place?

5 Epilogue

The authors thank Janos Makowsky and Norbert Hungerbühler for their kind invitation to contribute to this special issue. In 2010, the second author discussed the relevance and implications of Specker's work in the field at a workshop organized by Janos Makowsky on the occasion of Ernst Specker's 90th birthday. After the talk, Ernst Specker came up to the speaker and said *"Sie haben schon recht, dies ist dasjenige Resultat, welches mich am längsten überleben wird."* – "You are right, this is the result of mine that I will be remembered for the longest time."

References

[1] A. Aspect, P. Grangier, and G. Roger, Experimental test of realistic local theories via Bell's theorem, *Phys. Rev. Lett.*, Vol. 47, pp. 460–463, 1981.

[2] J.-D. Bancal, S. Pironio, A. Acin, Y.-C. Liang, V. Scarani, and N. Gisin, Quantum nonlocality based on finite-speed causal influences leads to superluminal signaling, quant-ph/arXiv:1110.3795v1, 2011.

[3] J. Barrett, L. Hardy, and A. Kent, No-signalling and quantum key distribution, *Phys. Rev. Lett.*, Vol. 95, No. 010503, 2005. quant-ph/0405101, 2004.

[4] J.S. Bell, Bertlsmann's socks and the nature of reality, in *Spekable and unspeakable in quantum mechanics*, Cambridge University Press, 1987.

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

[6] G. Birkhoff and J. von Neumann, The logic of quantum mechanics, *The Annals of Mathematics*, Second Series, Vol. 37, No. 4, pp. 823–843, 1936.

[7] D. Bohm and Y. Aharanov, Discussion of experimental proof for the paradox of Einstein, Rosen, and Podolsky, *Phys. Rev.*, Vol. 108, pp. 1070–1076, 1957.

[8] 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.

[9] R. Colbeck and R. Renner, Free randomness can be amplified, *Nature Physics*, Vol. 8, pp. 450–454, 2012. quant-ph/arXiv:1105.3195, 2011.

[10] R. Colbeck and R. Renner, No extension of quantum theory can have improved predictive power, *Nature Communications*, Vol. 2, p. 411, 2011. quant-ph/arXiv:1005.5173, 2010.

[11] S. Coretti, E. Hänggi, and S. Wolf, Non-locality is transitive, *Phys. Rev. Lett.*, Vol. 107, No. 100402, 2011.

[12] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, *Phys. Rev.*, Vol. 41, pp. 777–780, 1935.

[13] A. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.*, Vol. 67, pp. 661–663, 1991.

[14] V. Galliard, A. Tapp, and S. Wolf, The impossibility of pseudo-telepathy without quantum entanglement, *Proceedings of ISIT* 2003, p. 457, 2003.

[15] V. Galliard and S. Wolf, Pseudo-telepathy, entanglement, and graph colorings, *Proceedings of ISIT* 2002, p. 101, 2002.

[16] A.M. Gleason, Measures on the closed subspaces of a Hilbert space, *J. Math. Mech.*, Vol. 6, pp. 885–893, 1957.

[17] F. Gonseth, La physique de l'objet quelconque, in *Les mathématiques et la réalité*, 1936.

[18] E. Hänggi, R. Renner, and S. Wolf, Efficient device-independent quantum key distribution, *Proceedings of EUROCRYPT* 2010, LNCS, Springer-Verlag, pp. 216–234, 2010.

[19] E. Hänggi, R. Renner, and S. Wolf, The impossibility of no-signaling privacy amplification to appear in *Theoretical Computer Science* (*Elsevier*), 2012.

[20] J.M. Jauch and C. Piron, Can hidden variables be excluded in quantum mechanics?, *Helv. Phys. Acta*, Vol. 36, pp. 827–837, 1963.

[21] S. Kochen and E. Specker, The problem of hidden variables in quantum mechanics, *Journal of Mathematics and Mechanics*, Vol. 17, No. 1, pp. 59–87, 1967.

[22] R. Landauer, Information is inevitably physical, *Feynman and Computation 2*, Addison Wesley, 1998.

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

[24] R. Renner and S. Wolf, Quantum pseudo-telepathy and the Kochen-Specker theorem, *Proceedings of International Symposium on Information Theory* (*ISIT*) 2004, p. 322, 2004.

[25] V. Scarani and N. Gisin, Superluminal hidden communication as the underlying mechanism for quantum correlations: constraining models, *Braz. J. Phys.*, Vol. 35, pp. 328–332, 2005.

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

[27] A. Stefanov, H. Zbinden, N. Gisin, and A. Suarez, Quantum correlations with spacelike separated beam splitters in motion: Experimental test of multisimultaneity, *Phys. Rev. Lett.*, Vol. 88, No. 120404, 2002.

[28] J. von Neumann, *Mathematische Grundlagen der Quanten-Mechanik*, Verlag Julius-Springer, Berlin, 1932.

Renato Renner
Department of Physics
ETH Zürich
CH-8093 Zürich, Switzerland
e-mail: renner@phys.ethz.ch

Stefan Wolf
Faculty of Informatics
University of Lugano (USI)
CH-6904 Lugano, Switzerland
e-mail: wolfs@usi.ch