Gdańsk, 10.03.2014

Marcin Markiewicz, MSc
Institute of Theoretical Physics and Astrophysics
University of Gdańsk
Wita Stwosza 57, 80-952 Gdańsk

Abstract of PhD Thesis:

Characterization and detection of multipartite entanglement

1 Summary

The aim of this Thesis is to investigate the structure of multipartite entanglement, and to find efficient criteria for its experimental detection, and its impact on practical applications.

If one considers many subsystems, quantum correlations can be distributed in several different ways, and in the case of more than two subsystems, n-partite entanglement is not in one-to-one correspondence with n-partite correlations. This complicates the analysis. In this Thesis we apply a geometric approach. The structure of a multipartite quantum state is mapped into a multidimensional real euclildean space of correlations. Such an approach has two advantages. First, a theoretical one: one can use simple geometrical tools, like metrics and inner products. This makes the considerations much simpler than a direct analysis on the level of a Hilbert space. The second advantage is purely practical. Namely the basic objects in this analysis – the correlations – are directly measurable in experiments. We propose several correlation-based criteria for detection of multipartite entanglement, which, in contrast to earlier criteria, demand very limited number of measurements.

Further, we analyze the role of a multipartite entanglement as a basic resource in the field of quantum metrology and quantum distributed computing. We show that multipartite GHZ states enable better than classical scaling of precision in parameter estimation in the presence of decoherence, and can reduce computation complexity of distributed computing.

2 Quantum entanglement and quantum correlations – introduction

Quantum entanglement, almost 80 years after it was first discussed [1, 2], can be treated as a trademark of quantum physics, being called *the essence of quantum mechanics* in numerous papers. In modern terms the phenomenon of entanglement can be described in terms of information: two particles are entangled if their state contains more information about the entire system than about the separate subsystems [3].

In quantum mechanics, the state of a composite system can be at the same time *pure* – that is with maximal possible knowledge – and correlated. This situation is impossible in classical physics, where the state is *either* pure *or* correlated [4]. Therefore classical correlations always arise due to some ignorance about the global state, which is not the case for pure entangled states. This fact indicates that the nature of quantum correlations is completely different from that of classical ones. The *non-classicality* of quantum correlations can be considered from two different perspectives: within the formalism of quantum theory and from outside.

The nature of states and observables in quantum formalism is revealed by two properties. First, in quantum physics, the composite system is described by a tensor product of subsystems, and not by the Cartesian product as in the classical counterpart. Second, quantum observables, as opposite to classical ones, can be noncommutative. Both features are essential for the entanglement to exist, since entangled states exist only in the theory which assumes noncommuting observables for each separate subsystem [5, 6].

Non-classicality of quantum correlations can be described without resort to quantum formalism in terms of violation of Bell inequalities [7, 8]. They provide restrictions on probabilistic or information theoretic description of outcomes of measurements performed on separated subsystems. For example the most famous CHSH inequality [9] is expressed in terms of correlation functions. Its violation, indicating non-classical behaviour of the system, is related to the non-existence of a joint probability distribution for measurement outcomes of all possible measurements. In case of violation of inequalities expressed in terms of Shannon entropy [10] or Kolmogorov complexity [11], more subtle classical properties are not fulfilled [12].

Quantum incompatibility [13, 14, 15] is a general property which connects the above discussed ways of understanding non-classicality of quantum entanglement. Every commutatitve set of observables can be endowed with classical probabilistic model: there exists joint probability distribution for outcomes of all possible measurements from this set. However, two or more different sets of such a kind can be mutually incompatible. This implies that mixing the corresponding models for measurements on entangled states inevitably leads to contradictions on probabilistic and logical level [15, 14]. These contradictions have provoked a long debate on their impact for the structure, foundations and philosophical implications of quantum theory. This debate is still continuing [16].

Quantum entanglement has been put in the context of computation and communication tasks, giving rise to a new interdisciplinary field of *quantum information science*. This field covers a very broad class of problems, and the

results lead to many applications, such as quantum communication [17, 18, 19, 20], quantum cryptography [21], quantum metrology [22] and perhaps in a remote future quantum computation [23].

3 Detailed description of results

In this section I present a summary of results of my research projects published in works [A],[B],[C],[D],[E],[F].

3.1 The structure of multipartite entanglement and multipartite correlations

Multipartite entanglement can be thought of as a manifestation of *quantum inseparability* in the case of many subsystems. Intuitively, entanglement between n parties indicates some sort of strong non-classical correlations between all of them. Whereas this intuition turns out to be perfectly valid in the case of pure states, it breakes down when mixed states are considered [24], [25], [C]. Therefore, in a general case a multipartite entanglement has to be defined by rejecting separability of investigated state. In this chapter we describe a general characterization of a partial separability. Further on, we investigate the relation between multipartite entanglement, lower order correlations and possibility of simulating these correlations with classical models.

3.1.1 Geometrical characterization of partial separability

In general terms separability is a property of a composite system indicating that the overall state is a convex probabilistic mixture of pure states that are product with respect to some partitions [26]. In case of a bipartite system this reduces to a convex mixture of bi-product states. Operationally, this means that every possible correlation function of local measurements can be simulated by local operations and shared randomness, but without communication.

For more than two parties, the notion of separability is much richer, because the system can be partitioned into subsystems in many ways. The most natural extension of the notion of separability is *partial separability with respect to a partition* [27, 4]. An n-partite state ρ is called k-separable with respect to a partition $\mathcal{S}$ of n particles into k subsystems $\{s_1, \ldots, s_k\}$, if it can be expressed as a probabilistic mixture of pure states $|\psi_{(k-\mathrm{pr}|\mathcal{S})}\rangle = \bigotimes_{l=1}^{k} |\psi_{r_l \in s_l}\rangle$, which are k-product with respect to $\mathcal{S}$:

$$\rho_{(k-\mathrm{sep}|\mathcal{S})} = \sum_i p_i |\psi^i_{(k-\mathrm{pr}|\mathcal{S})}\rangle\langle\psi^i_{(k-\mathrm{pr}|\mathcal{S})}|, \tag{1}$$

where subscripts 'k–sep' and 'k–pr' denote 'k–separable' and 'k–product', respectively. The operational interpretation of the above is in a direct analogy to the one from the bipartite case. Unfortunatelly, partial separability (1) does not give rise to partially ordered classes of separability. Therefore it cannot be used to quantify the degree of separability, since different classes are incomparable. To avoid this difficulty we consider the unconditioned k-separability. Namely, we say that the n-partite state ρ is called k-separable if it can be expressed as

a probabilistic mixture of pure k-product states $|\psi_{k-\mathrm{pr}}\rangle = |\psi_{r_1}\rangle \otimes \ldots \otimes |\psi_{r_k}\rangle$:

$$\rho_{k-\mathrm{sep}} = \sum_i p_i |\psi^i_{k-\mathrm{pr}}\rangle\langle\psi^i_{k-\mathrm{pr}}|. \tag{2}$$

The difference with respect to the previous definition is that now the pure states entering the mixture can be k-product with respect to different partitions. Sets S_{k-sep} of k-separable states are convex and partially ordered by inclusion:

$$S_{n-sep} \subseteq S_{(n-1)-sep} \subseteq \ldots \subseteq S_{3-sep} \subseteq S_{2-sep}. \tag{3}$$

Testing whether given state is k-separable directly from the definition (2) is analytically hard and in many cases intractable. There were given several sufficient conditions for testing k-separability in case of qubits [27]. For systems of arbitrary dimensions only full separability has been completely characterized [28].

In [A] we give a general characterization of k-separability for arbitrary finite dimensional systems. It has a form of a necessary and sufficient geometrical condition for refuting k-separability of a given state. Since the k-separable states form a partially ordered familly of sets (3), our condition gives a complete characterization.

Our condition is expressed in terms of the so called *generalized correlation tensor* of a quantum state, which in case of qubits is defined as:

$$T_{\mu_1,\ldots,\mu_n} = \langle \sigma_{\mu_1} \otimes \ldots \otimes \sigma_{\mu_n} \rangle_\rho = \mathrm{Tr}\left(\rho\, \sigma_{\mu_1} \otimes \ldots \otimes \sigma_{\mu_n}\right), \tag{4}$$

where σ_μ for $\mu = 1, 2, 3$ denotes Pauli matrices, and σ_0 denotes identity matrix. For non-zero indices this object transforms like a tensor. In case of states of arbitrary dimension one can use any Hermitian operator basis (eg. generalized Gell-Mann matrices) instead of $\{\sigma_\mu\}_{\mu=0}^3$ to define the correlation tensor. The generalized correlation tensor gives a unique description of a quantum state:

$$\rho = \frac{1}{2^n} \sum_{\mu_1,\ldots,\mu_n=0,1,2,3} T_{\mu_1,\ldots,\mu_n} \sigma_{\mu_1} \otimes \ldots \otimes \sigma_{\mu_n}. \tag{5}$$

For the sake of simplicity we will often denote $T_{\mu_1,\ldots,\mu_n}$ as $T_{\vec{\mu}}$.

Using correlation tensors instead of density matrices has two main advantages. First, their elements, as expectation values of Hermitian operators, are directly measureable. Second, correlation tensors belong to a family of real inner product spaces, with generalized inner products defined as:

$$(X, Y)_G = \sum_{\vec{\mu},\vec{\nu}} X_{\vec{\mu}} G_{\vec{\mu}\vec{\nu}} Y_{\vec{\nu}}, \tag{6}$$

where G is a positive semidefinite operator acting on a vector space of correlation tensors. This inner product induces a G-seminorm[1]:

$$||T||^2_G = (T, T)_G. \tag{7}$$

[1] A seminorm is a non-negative function of a vector space, which is absolutely homogeneous, and fulfills the triangle inequality, but need not to *separate points*, which means $||T||_G = 0$ does *not* necesserilly imply $T = 0$. In fact correlation tensor T of a quantum state is never a zero vector, however for suitably chosen metric it can happen, that $||T||_G = 0$.

In this sense a space of correlation tensors with fixed G is a pseudo-metric space. We will refer to operators G simply as *metrics*, having in mind that they define a pseudo-metric.

The machinery of an inner product space allows to formulate a very simple condition for refuting that a given vector $\vec{a}$ belongs to a set S [29]:

$$\max_{\vec{b}\in S} \vec{a}\cdot\vec{b} < \vec{a}\cdot\vec{a} \Longrightarrow \vec{a}\notin S. \tag{8}$$

Applying this condition to the set of k-separable states we obtain the following condition, which generalizes the full separability condition in [29]:

$$\begin{gathered} \textit{If there exists a metic } G\textit{, for which:} \\ \max_{T^{k\text{-}sep}}(T^{k\text{-}sep},T)_G < ||T||^2_G, \\ \textit{the state described by correlation tensor } T \textit{ is not } k\textit{-separable.} \end{gathered} \tag{9}$$

This condition is in a sense tautological, since it demands optimization over all k-separable states to prove that some state is not in this class. However, due to convexity of this set we have:

$$\max_{T^{k\text{-}sep}}(T^{k\text{-}sep},T)_G = \max_{\{\{p_i\},T^{k\text{-}pr}\}}\left(\sum_i p_i T^{k\text{-}pr}_{(i)},T\right)_G \leq \max_{T^{k\text{-}pr}}(T^{k\text{-}pr},T)_G, \tag{10}$$

which allows to perform the maximization in (9) over pure k-product states. The set of k-product states can be uniquely decomposed into the set of states, which are k-product with respect to all k-partitions $\mathcal{S}$. Therefore, the condition (9) can be reformulated, such that the maximization is performed separately for each partition:

$$\begin{gathered} \textit{If for every partition } \mathcal{S} \textit{ there exists a metric } G_{\mathcal{S}} \textit{ such that:} \\ \max_{T^{(k\text{-}pr|\mathcal{S})}}(T^{(k\text{-}pr|\mathcal{S})},T)_{G_{\mathcal{S}}} < ||T||^2_{G_{\mathcal{S}}}, \\ \textit{the state described by correlation tensor } T \textit{ is not } k\textit{-separable.} \end{gathered} \tag{11}$$

Moreover, we show in [A], that the above condition is also a necessary one, which means, that for every non-k-separable state ρ, and every k-partition $\mathcal{S}$ there exists a metric $G_{\mathcal{S}}$, such that the inequality (11) is fulfilled. This leads to a general characterization of k-separability [A]:

$$\begin{gathered} \textit{An } n\textit{-partite state endowed with correlation tensor } T \textit{ is not } k\textit{-separable} \\ \textit{if and only if for every partition } \mathcal{S} \textit{ into } k \textit{ subsystems,} \\ \textit{there exists a metric } G_{\mathcal{S}} \textit{ such that the following inequality holds:} \\ \max_{T^{(k\text{-pr}|\mathcal{S})}}(T^{(k\text{-pr}|\mathcal{S})},T)_{G_{\mathcal{S}}} < (T,T)_{G_{\mathcal{S}}}. \end{gathered} \tag{12}$$

The above characterization is very important, since it gives a complete description of the degree of separability, and a partial characterization of multipartite entanglement. Indeed, since k-separable states form a partially oredered sets (3), they naturally characterize the degree of separability: the most separable states are n-separable ones, also called fully separable, and the least separable states are *biseparable*. States which are fully separable contain no entanglement, states that are not k-separable contain entanglement between at least $\lceil \frac{n}{k-1} \rceil$ parties, and states that are not biseparable, are genuinely n-partite entangled.

3.1.2 Multipartite entanglement deduced from bipartite correlations

In the case of multipartite systems there is no one-to-one correspondence between entanglement and correlations, namely, states that are n-partite entangled need not give rise to n-partite correlations [24, 25]. In [B] we investigate to what extent multipartite entanglement of pure states can be derived from bipartite correlations. The considerations are based on the phenomenon called *monogamy of correlations*, which relies on the fact, that if many systems are correlated, the distribution of these correlations is strongly bounded by physical properties of the entire system. In the case of three qubits this phenomenon implies, that if any two of the systems are strongly quantumly correlated, they cannot be strongly correlated with the third subsystem [30]. This intuition is the basic idea behind device-independent quantum cryptography [31, 32, 33].

In our considerations we use the correlation tensor representation (5) of a quantum state of n qubits. The elements of a correlation tensor (4), which contain only k non-zero indices correspond to k-partite correlations. Single particle expectations (T_x, T_y, T_z) form a three dimensional real vector. We conventionally call the local measurements of σ_x, σ_y and σ_z as measurements in $\hat{x}$, $\hat{y}$ and $\hat{z}$ direction respectively.

Our characterization of multipartite entanglement of pure qubit states is based on the following monogamy relation:

For any n-qubit state (pure or mixed) the following tight bound holds:

$$\mathcal{M} = \sum_{1\leq k<l\leq n} \mathcal{M}_{kl} \leq \begin{cases} 2 \text{ if } n = 2 \\ \binom{n}{2} \text{ if } n \geq 3 \end{cases}, \tag{13}$$

with $\mathcal{M}_{kl} = \sum_{i,j=1,2} T^2_{0,\ldots,0,i_{(k)},0,\ldots,0,j_{(l)},0,\ldots,0}$, where subscripts (k) and (l) denote k-th and l-th subsystem, and i, j are two pairs of Cartesian coordinate indices. For simplicity, we shall assume that they always represent coordinates related with measurement directions $\hat{x}$ and $\hat{y}$.

The condition (13) states that the sum of squares of all possible bipartite correlations in an n qubit state with respect to two different orthogonal directions i, j is bounded by the factor $\binom{n}{2}$, which is 4 times less than the algebraic bound of this expression. In this form the proposition is useless for detection of entanglement, since $\mathcal{M}$ contains terms related to classical correlations. To remove them, we define a *preffered basis* for the k-th observer, as a measurement basis in which the local Bloch vector is pointing in $\hat{z}$ direction. The quantity $\mathcal{M}$ in these new coordinates, which we denote by $\mathcal{M}^{(pb)}$ gives rise to two entanglement criteria:

For $n \geq 5$, and for any n-qubit pure state $|\psi\rangle$, if:

$$\mathcal{M}^{(pb)}(|\psi\rangle) > \tbinom{n-1}{2} \tag{14}$$

then $|\psi\rangle$ is genuinely n-partite entangled. For n=3 and n=4 we have:

$$\mathcal{M}^{(pb)}(|\psi\rangle) > 2 \Longrightarrow |\psi\rangle \text{ is genuinely 3-partite entangled.}$$

$$\mathcal{M}^{(pb)}(|\psi\rangle) > 4 \Longrightarrow |\psi\rangle \text{ is genuinely 4-partite entangled.}$$

and:

$$\begin{gathered}\textit{For any } n\textit{-qubit pure state } |\psi\rangle, \textit{ with } n \geq 5, \\ \textit{and for any } m \leq \left\lfloor \tfrac{n}{2} \right\rfloor - 1 \textit{ the following holds:} \\ \textit{if } \mathcal{M}^{(pb)}(|\psi\rangle) > \tbinom{m}{2} + \tbinom{n-m}{2} + \delta_{m,2}, \\ \textit{where } \delta_{m,2} \textit{ denotes the Kronecker delta,} \\ \textit{the state } |\psi\rangle \textit{ is genuinely } m\textit{–partite entangled.}\end{gathered} \tag{15}$$

We illustrate the above criteria using Dicke states [34]:

$$|D_n^e\rangle = \frac{1}{\sqrt{\binom{N}{e}}} \sum_{\pi} |\pi(1 \ldots 10 \ldots 0)\rangle\,, \tag{16}$$

where π denotes permutations of local subsystems and e is the number of excitations (states $|1\rangle$). Applying condition (14) we obtain, that states D_3^1 and D_5^2 are genuinely multipartite entangled, whereas applying condition (15) we get that states $D_n^{(n-1)/2}$, where n is odd, contain entanglement between at least $(n+3)/2$ parties.

These results, although not optimal from the point of view of entanglement detection (it is known that all Dicke states are truly n-partite entangled) are nevertheless quite important. First, they do not follow usual intuitions about Dicke states. Namely, Dicke states D_n^e are known to be the only states compatible with its $2e$-qubit reduced states [35]. Therefore intuitively the greater is the number of excitations e, the more dependent D_n^e are on higher-partite correlations. However condition (15), based solely on bipartite correlations, detects higher-partite entanglement for higher e. This shows that quantifying multipartite entanglement is completely different task from the so called *quantum marginal problem* [36], that is determining unique global state given its marginals. Second, condition (15) applied to Dicke states gives an interesting illustration of *quantum de Finetti theorem* [37], which in the simplest version states, that the reduced k-partite state of every permutationally invariant finite dimensional state of n parties is for sufficiently large n arbitrary close to a separable state. Condition (15) detects entanglement of $D_n^{(n-1)/2}$ for arbitrary n, however the efficiency of this condition tends to zero with $n \to \infty$. This is in accordance with *quantum de Finetti theorem* which indicates, that bipartite reduced states of D_n^e are asymptotically separable, hence asymptotically they should not contain any information about entanglement of D_n^e.

3.1.3 Incompatibility of classical models for multipartite entangled states

As mentioned in the introduction, the characterization of multipartite quantum correlations can be done without resort to quantum formalism. This is done by investigating, to what extent correlations arising from measurements on quantum particles can be described with classical statistical models [15]. The impossibility of the classical description can be confirmed by a violation of a Bell inequality [8], as it is derivable under the assumption that such a model exists. The necessary condition for non-existence of such models for measurements on quantum particles, is that the particles are entangled and the sets

of measurements of at least two observers are non-commuting. However, this condition is not sufficient, as shown by Werner [26].

Let us consider a distributed scenario, called n-partite Bell-type scenario with m settings per observer, in which n parties perform local binary[2] measurements, and k-th party locally chooses her observable from the set $\mathcal{A}_1^{[k]}, \ldots, \mathcal{A}_m^{[k]}$. We say that there exists a *classical model for probabilities* of measurement outcomes in defined scenario, if and only if every observable $\mathcal{A}_{x^{[k]}}^{[k]}$ can be represented as a random variable on a global sample space of all possible events, and this assignment is *noncontextual*, which means that it does not depend on which of the observables are chosen to be measured in a given experiment. It is assumed that all these random variables admit a joint probability distribution. This model is a simple example of a *Kolmogorovian probabilistic model* [38, 15], and has (at least) three different interpretations:

- *local hidden variable (LHV) model* [7, 39, 8]; here we assume, that the joint probability distribution of outcomes $y^{[1]}, \ldots, y^{[n]}$ on condition the local measurements $\mathcal{A}_{x^{[1]}}^{[1]}, \ldots, \mathcal{A}_{x^{[n]}}^{[n]}$ were chosen can be presented in the form [26, 8]:

$$p(y^{[1]}, \ldots, y^{[n]}|x^{[1]}, \ldots, x^{[n]}) = \int_{\lambda \in \mathcal{O}} \rho(\lambda) \cdot p(y^{[1]}|x^{[1]}, \lambda) \cdot \ldots \cdot p(y^{[n]}|x^{[n]}, \lambda)\, \mathrm{d}\lambda; \tag{17}$$

  this corresponds to the original notion of classicality, that has arisen after the original EPR [1] and Bell [7] discussions; it emphasizes the role of λ as a hidden parameter not present in quantum formalism, which affects the probabilities of local events; the idea assumes that when the physical system is initially prepared, it is assigned some value of λ, and after the system is already distributed in space, all its parts carry the information about λ; moreover λ can have different values at each preparation round; this is described by the distribution $\rho(\lambda)$;

- *local realistic model* [39]; the classical model is understood as coming from joint assumptions of *realism*, which guarantees the existence of all values of all involved observables, and *locality*, which justifies the noncontextual assignment; it is a special, extremal case of the local hidden variable model (in which the values are hidden variables).

- *randomized algorithm in distributed computational model* [39],[F]; this interpretation is the most operational one; n distributed processors with unbounded local computational capabilities share random sequences λ and are given distributed inputs $x^{[1]}, \ldots, x^{[n]}$; it is assumed that there exists an algorithm, such that the processors output bit values $y^{[1]}, \ldots, y^{[n]}$ with desired probability distribution (17); the output bits depend only on their local inputs and the shared random numbers λ, whereas no communication between the processors is allowed.

To avoid endless disputes on the problem which of the above three interpretations is the most appropriate one, we will simply refer to (17) as a *classical model*.

[2] We use the convention, that binary observables take values $\{-1, 1\}$ instead of bit values $\{0, 1\}$.

We can define a weaker version of the classical model in the above sense, called a *classical model for correlations* [26, 40], the existence of which, in several important cases, is much easier to check. Namely we say that such a model exists if and only if the correlation function of the measurement outcomes is given by:

$$E(x^{[1]},\ldots,x^{[n]}) = \langle \mathcal{A}^{[1]}_{x^{[1]}} \ldots \mathcal{A}^{[n]}_{x^{[n]}} \rangle_\rho = \int_{\lambda\in\mathcal{O}} \rho(\lambda)\cdot I^{[1]}_{x^{[1]}}(\lambda)\cdot\ldots\cdot I^{[n]}_{x^{[n]}}(\lambda)\,\mathrm{d}\lambda, \quad (18)$$

where the binary functions $I^{[k]}_{x^{[k]}}(\lambda)$, called *response functions* [41, 26], denote (predefined) outcomes of the observables $\mathcal{A}^{[k]}_{x^{[k]}}$ measured by the k-th observer for a given value of λ.

The difference between the conditions (17) and (18) is that (17) is much more restrictive. For a given definite scenario, existence of a model for probabilities (17) uniquely determines the model for correlations (18), however the converse is not true. Given a model for correlations one can always determine (usually not unique) *hidden probability distribution* for all possible outcomes [42], however this distribution, when treated as a joint probability distribution, can give rise to wrong correlations between fewer number of parties.

A theorem by Żukowski and Brukner [42] gives a sufficient condition for existence of such a model, when the measurements are performed on qubits. Let us consider an n-partite Bell-type scenario, in which each observer can choose between two different projective measurements on a qubit. If for any set of local orthogonal coordinate systems $\{x_1,\ldots,x_n\}$ the following condition holds [42]:

$$\sum_{x_1,\ldots,x_n=1,2} T^2_{x_1,\ldots,x_n} \leq 1, \quad (19)$$

then the correlation function for arbitrary local measurements in this scenario admits a classical description in terms of (18).

When characterizing the nonclassicality of multipartite quantum correlations, one usually investigates the non-existence of a global model for probabilities (17) or a model for full n-partite correlations (18). As we show in [C] this approach is insufficient to reveal the entire structure of nonclassical correlations.

Let us consider the following class of mixed entangled states:

$$\rho^e_n = \frac{1}{2}\,|D^e_n\rangle\,\langle D^e_n| + \frac{1}{2}|D^{n-e}_n\rangle\langle D^{n-e}_n|, \quad (20)$$

where $|D^e_n\rangle$ denotes Dicke states (16). States ρ^e_n are genuinely n-partite entangled, although for odd n they have vanishing correlations between odd number of subsystems, including the n-point ones. This means, that correlations between odd number of subsystems trivially admit classical models for correlations (18). However, as we point out in [C], the state ρ^2_5 admits a classical models for correlations (18) between any two subsystems, and between any four subsystems. This can be directly proven using the condition (19). Therefore, the state ρ^2_5 admits classical models for correlations between any fixed number of subsystems, however the global classical model for probabilities (17) does not exist for this state, which we verified numerically.

Operationally this means, that for each subset of observers $\{a_{i_1},\ldots,a_{i_k}\}$, where $k\leq 5$ it is possible to construct a procedure, which allows to simulate k-partite correlations arising from measurements on ρ^2_5, and uses only the local inputs (the settings) and some shared random numbers.

Since the global classical model for probabilities in Bell scenario with two settings per observer does not exist in this case, the classical models for correlations between any fixed number of parties must be mutually incompatible. This means, that the *hidden probability distributions* arising from these models cannot be extended to a single model for probabilities (17). This incompatibility can arise inbetween models for bipartite and four-partite correlations, as well as inbetween models for a fixed number of parties but for different choices of subsystems. The incompatibility can be directly proven by demonstrating a violation of a Bell inequality involving both bipartite and four-partite correlations for all possible permutations of subsystems:

$$E_{\pi(11110)} + E_{\pi(22220)} + E_{\pi(12220)} - E_{\pi(21110)} - E_{\pi(11000)} - E_{\pi(22000)} \leq 6, \quad (21)$$

where the subscripts 1 and 2 denote settings for given observers, subscripts 0 denote σ_0 "measurements" (that is lower order correlations) and $E_{\pi(ijklm)}$ denotes the sum of all correlation functions obtained by permuting positions of the settings i, j, k, l, m. We have found settings:

$$\vec{s}_1 = (\cos\tfrac{\pi}{5}, -\sin\tfrac{\pi}{5}, 0), \quad (22)$$

$$\vec{s}_2 = (\cos\tfrac{\pi}{20}, \sin\tfrac{\pi}{20}, 0), \quad (23)$$

which give rise to a violation of (21). The left-hand-side of (21) for ρ_5^2 equals 7.7831, which is almost equal to the maximal value, which we have found numerically to be 7.8217.

The discussed example shows that if one investigates multipartite entangled states from the perspective of classical models, their *nonclassicality* is a very subtle point. Even though ρ_5^2 is genuinely 5-partite entangled, and as such highly non-classical, its correlations between any fixed number of parties in a scenario of two settings per observer are classical in terms of (18). This indicates, that correlations do not give a full description of *quantum incompatibility*, and in some cases direct investigation of the classical models for probability (eg. using the software described in [43]) is necessary.

3.2 Efficient experimental detection of multipartite entanglement with non-linear entanglement identifiers

The main difficulty in detecting multipartite entanglement stems from the fact that sets of k-partite entangled states are not convex. In general proving that some vector belongs to a non-convex set is a hard task. It is therefore much more efficient to characterize relation of a given state with respect to sets of k-separable states (3). By rejecting different classes of k-separability (3), we get information about entanglement, namely an n-partite state which is not k-separable must involve entanglement between at least $\lceil \frac{n}{k-1} \rceil$ parties.

Precise geometrical characterization of S_{k-sep} is difficult. Since this set is not a polytope – it cannot be effectively described by a finite number of linear equations. On the other hand, due to Hahn-Banach theorem, such a set can be characterized using a continuous set of linear functionals, called in this context *entanglement witnesses* [44, 4]. Every such functional can be represented by an Hermitian operator[3], hence is directly measureable, at least in principle.

[3]This happens since the set of all linear continuous functionals on the space of trace class operators is isomorphic to algebra of bounded operators on a system's Hilbert space.

In practice, this method is very problematic for several reasons. First, the operator representing the witness has to be decomposed into locally measurable observables [4] in such a way, that the number of local measurements needed for detection of entanglement is reasonably small. Second, the witness has to be precisely adjusted to the state under investigation, which demands some initial knowledge about the state. The first problem has been solved only for a few low-dimensional cases [45, 46], whereas the second one has been partially solved in a bipartite case by non-linear improvements to the witness [47].

In works [A] and [D] we propose a much more versatile method of entanglement detection, based on condition (12). First, our method is by definition adjusted to the scenario of local measurements performed on arbitrary number of subsystems. Second, our entanglement identifiers have form of nonlinear functionals, which makes them more universal and less dependent on the initial knowledge of the state. Finally, our method often requires only few measurements to detect entanglement.

In [A] we derived several nonlinear entanglement identifiers directly based on condition (12). In the case of three qubits, we derived criteria, which are unbiased with respect to any family of entagled states. Using the inner product (6) based on the metric $G_{\vec{\mu}\vec{\nu}}$ (7) in the standard form of a Kronecker delta, we obtained:

If the following inequality holds:

$$\max_{\pi,\pi\left(\hat{O}\otimes\hat{O}',\mathbb{1}\right)} \sqrt{\sum_{i=1}^{3}\left(\left|T_{\pi(11i)}-T_{\pi(22i)}\right|+\left|T_{\pi(33i)}\right|\right)^2} < ||T||^2, \qquad (24)$$

then the state described by T is genuinely 3-partite entangled.

The maximization of the left-hand-side is performed over all permutations π of the indices, and over local rotations applied to fixed indices for a given permutation. This condition is very versatile, since it allows for detection of genuine 3-partite entanglement of both GHZ and W states, despite the fact, that they belong to two completely different families of states, and their entanglement is of a very different nature [48].

We can modify the metric (hence also the norm (7)) to get rid of terms of the $T_{\pi(33i)}$ type, thus we put:

$$||T||_{\pi}^2 = \sum_{i,j,k=1}^{3} T_{ijk}^2 - \sum_{l=1}^{3} T_{\pi(33l)}^2. \qquad (25)$$

In this way we obtain a condition with fewer number of measurements:

If the following inequalities hold:

$$\forall_{\pi} \max_{\pi\left(\hat{O}\otimes\hat{O}',\mathbb{1}\right)} \sqrt{\sum_{i=1}^{3}\left(T_{\pi(11i)}-T_{\pi(22i)}\right)^2} < ||T||_{\pi}^2, \qquad (26)$$

where $||T||_{\pi}^2 = \sum_{i,j,k=1}^{3} T_{ijk}^2 - \sum_{l=1}^{3} T_{\pi(33l)}^2$,

then the state described by T is genuinely 3-partite entangled.

Since the square root in (26) is not greater than 2, the former condition can be simplified to a weaker one:

$$\forall_{\pi} ||T||_{\pi}^2 > 2,$$

which is experimentally very efficient. Namely one measures the components of T which enter $||T||^2_\pi$ untill for all permutations π the sum (25) exceeds 2. In this way a 3-partite entanglement can be confirmed with few measurements.

We also provide an example of condition that favours generalized GHZ states of n qubits:

$$|GHZ_\alpha\rangle = \cos\alpha\,|0\ldots0\rangle + \sin\alpha\,|1\ldots1\rangle\,, \tag{27}$$

Our condition with a diagonal metric $G_{\vec{\mu}\vec{\nu}} = \delta_{\vec{\mu},\vec{\nu}}|G^{\rm GHZ}_{\vec{\mu}}|$, where $G^{\rm GHZ}_{\vec{\mu}}$ denotes a correlation tensor of a GHZ state (27), but with $G^{GHZ}_{0,\ldots,0} = 0$, leads to an optimal detection of a genuine multipartite entanglement of noisy GHZ states. Namely, generalized GHZ state mixed with white noise:

$$\rho = v|GHZ\rangle\langle GHZ| + (1-v)\frac{1}{2^n}\mathbb{1}. \tag{28}$$

is n-partite entangled for $v > \frac{2^n\cos^2\alpha - 1}{2^n - 1}$. Note that this state is fully separable only for $\alpha = 0$, which indicates a very interesting feature of sets of k-separable states, that in an infinitesimal neighbourhood of the fully separable states there are states with entanglement between an arbitrary number of subsystems.

The criteria presented in [A] do not demand the exact knowledge of the state which is experimentally tested, hence they can be used for testing entanglement without any knowledge of the preparation procedure. However, one often faces a different experimental problem, in which one aims at producing a definite entangled state, and wants to check, whether the noise that appeares during this stage spoiles the entanglement. As we discussed before, the earlier approach of entanglement witnesses encounters several difficulties. In [D] we proposed an approach to the witness method, which can be applied succesfully, whenever we can find a nearest separable (or in general k-separable) state, further denoted as ρ_0, to the state ρ under investigation.

The construction comes from the "*only if*" part of condition (12), which states that for each state ρ, that is not k-separable, there exists a metric G, such that for every partition $\mathcal{S}$ of the subsystems, the inequality (12) is fulfilled. Such a metric is given by:

$$G_{\vec{\mu}\vec{\nu}} = D_{\vec{\mu}}D_{\vec{\nu}} \tag{29}$$

where vector indices denote coordinates in some Hermitian operator basis, and $D_{\vec{\mu}}$ is a correlation tensor (4) of operator $\rho - \rho_0$. Putting this specific metric into the condition (12) we obtain the following criterion:

$$\max_{T^{k-pr}} \sum_{\vec{\mu}\vec{\nu}} T_{\vec{\mu}}D_{\vec{\mu}}D_{\vec{\nu}}T^{k-pr}_{\vec{\nu}} < \sum_{\vec{\mu}\vec{\nu}} T_{\vec{\mu}}D_{\vec{\mu}}D_{\vec{\nu}}T_{\vec{\nu}}. \tag{30}$$

The value L_G of the left-hand-side gives us the following entanglement identifier:

$$\sum_{\vec{\mu}\vec{\nu}} T_{\vec{\mu}}D_{\vec{\mu}}D_{\vec{\nu}}T_{\vec{\nu}} > L_G \Longrightarrow \rho \textit{ described by } T \textit{ is not separable}, \tag{31}$$

which in the case of rejecting full separability is equivalent to a standard entanglement witness [29]. The numbers entering this condition can be negative, thus all the corresponding correlations have to be measured. This assumption can be relaxed by erasing all off-diagonal terms of the metric G, which defines a new metric:

$$H_{\vec{\mu}\vec{\nu}} = D^2_{\vec{\mu}}\delta_{\vec{\mu}\vec{\nu}} \tag{32}$$

where $\delta_{\vec{\mu}\vec{\nu}} = \delta_{\mu_1\nu_1} \cdot \ldots \cdot \delta_{\mu_n\nu_n}$ denotes the product of point-wise Kronecker deltas of all possible pairs of coordinates. The new metric H gives rise to an analogous condition:

$$\max_{T^{k-pr}} \sum_{\vec{\mu}} T_{\vec{\mu}} D^2_{\vec{\mu}} T^{k-pr}_{\vec{\mu}} < \sum_{\vec{\mu}} T^2_{\vec{\mu}} D^2_{\vec{\mu}}. \tag{33}$$

If we calculate the numerical value of the left-hand-side, L_H, we obtain a quadratic generalization of an entanglement witness:

$$\sum_{\vec{\mu}} T^2_{\vec{\mu}} D^2_{\vec{\nu}} > L_H \Longrightarrow \rho \textit{ described by } T \textit{ is not separable.} \tag{34}$$

The sensitivity of this condition with respect to the white noise is different than in the case of standard witnesses. In contradistinction to (31), it contains summation of positive numbers only. This allows an efficient experimental detection of entanglement, since once the condition is fulfilled we do not need to perform further measurements, as they can only increase the left-hand-side of (34). Our work [D] includes applications of the above two identifiers (31) and (34) for several states, which are interesting from quantum information perspective.

The presented approach to entanglement witnesses is very general. It works for states of arbitrary dimension, and it can be used to test if a given state does not belong to any other class of convex states, like PPT ones [4].

3.3 Applications of multipartite entanglement in various physical scenarios

Here we present an analysis of applications of multipartite entanglement in the context of metrology and distributed computing.

3.3.1 Precise parameter estimation

One of the most significant applications of multipartite entanglement is *quantum metrology* [22]. This field originates from investigations on precise phase-shift estimation in interferometers [49] and has been generalized to a theory of precise estimation of more general physical parameters. Nowadays a development of these techniques is crucial in atomic spectroscopy [50], in constructing atomic clocks [51] and in detection of gravitational waves [52].

General metrological setup is theory-independent, and consists of four stages: three experimental ones and one theoretical. In the experiment, one first prepares an initial system of n particles – the probe. Then the system undergoes a local unitary evolution, which depends on some unknown parameter ω, which is estimated. Finally, the evolved system undergoes some local POVM measurements[4], and the results are processed so as to estimate the parameter ω, with the best possible precision.

Intuitively, the bigger the initial system, the higher the precision of estimation. It turns out, that when the initial system consists of n classically correlated particles, the best possible precision of estimation scales like $1/\sqrt{n}$, which is a direct consequence of a *Cramer-Rao bound* [53, 54] in estimation theory. However, when the initial state is multipartite entangled, it turns out

[4]This assumption is not restrictive, since it is proved that global measurements do not enhance the precision of estimation.

that the precision of estimation can achieve scaling of $1/n$, called the *Heisenberg limit*. The intuitive reason for this improvement is that the correlation function of local measurements on a highly entangled state is much more sensitive to a unitary dynamics than the classical correlation function. Unfortunatelly this *quantum gain* in precision is extremely fragile to decoherence. Let us assume that each qubit from the initial n-partite system undergoes a local unitary ω-dependent rotation and simultaneously is exposed to a general local noise. This kind of evolution is formally described by the Kossakowski-Lindblad equation [55, 56]:

$$\frac{\partial \rho\left(t\right)}{\partial t} = -i[H,\rho] + \mathcal{L}\left(\rho\right), \tag{35}$$

where the Hamiltonian $H = \frac{1}{2}\omega\sigma_{\vec{r}}$ is a *generator of unitary rotation* around axis $\vec{r}$, whereas the Liouvillian:

$$\mathcal{L}(\rho) = -\frac{1}{2}\gamma\left[\rho - \alpha_x\sigma_x\rho\sigma_x - \alpha_y\sigma_y\rho\sigma_y - \alpha_z\sigma_z\rho\sigma_z\right], \tag{36}$$

describes a noise generated by $\{\sigma_x, \sigma_y, \sigma_z\}$. The entire evolution can be transformed into the quantum channel formalism [57, 58, 59]:

$$\rho(t) = \sum_{i=1}^{4} K_i(t)\rho K_i^{\dagger}(t), \tag{37}$$

where the evolution operators K_i are called Kraus operators. Recently it has been shown that an arbitrary noise described by full rank channels (which means all Kraus operators in (37) are non-zero) reduces the scaling of precision to $1/\sqrt{n}$ [60], which is the classical scaling. Thus, realistic quantum metrology turns out to be very limited.

In [E] we propose a slightly modified metrological scenario, which allows to overcome this problem in a special case, of the generator of noise, which is perpendicular to the generator of evolution. Our idea is based on the following observation. The uncertainty of estimation of a parameter ω fulfills the quantum Cramer-Rao bound [61]:

$$\delta\omega \geq \frac{1}{\sqrt{(\mathcal{F}(\rho_\omega)\cdot T)/t}}, \tag{38}$$

where T is the total time of the experiment, t is a time of a single round (which is the time the system evolves) and $\mathcal{F}(\rho_\omega)$ is the so called quantum Fisher information (QFI) [62]. QFI is a function of the evolved state and describes the amount of information about the parameter ω that can be extracted from measurements on the final state, assuming that the entire estimation procedure is optimal. Typically one assumes, that T and t are fixed, and one maximizes the QFI over input states. Then it turns out, that taking eg. n-partite GHZ state as an input state, the quadratic scaling $\mathcal{F}(\rho_\omega) \propto n^2$ of the QFI as a function of input size can be attained, which gives the best quantum gain in precission. Unfortunatelly, in this case also the *no-go* result of Ref. [60] holds, which states, that in the presence of any decoherence, such that the entire quantum channel (37) is full-rank, the classical scaling $\mathcal{F}(\rho_\omega) \propto n$ is assymptotically unavoidable. To cope with this problem we utilize a modified approach to parameter estimation, in which only the entire experiment time T is fixed, whereas the evolution

time t is optimized for each n separately, so as to maximize[5] $\mathcal{F}(\rho_\omega)/t$. This approach has been considered before in a very restricted case of collinear noise and evolution generators [50, 63].

We show [E], that if the generator of noise is perpendicular to the generator of evolution, the initial n-partite GHZ state gives rise to QFI scaling asymptotically as $\mathcal{F}(\rho_\omega) \propto n^{\frac{5}{3}}$. This implies the uncertainty $\delta\omega \propto n^{-\frac{5}{6}}$, which beats the classical scaling, though not achieving the quantum Heisenberg limit.

In our investigations we assume that the generator of evolution is σ_z, whereas the generator of noise in (36) is set to be σ_x. The input state is an n-partite GHZ state (27) with $\alpha = \frac{\pi}{4}$. We find analytic form of Kraus operators (37) for this channel. Although we obtained analytic form of the QFI, we were forced to calculate $\max_t \mathcal{F}(\rho_\omega)/t$ numerically, because of the very complicated and intractable form of $\mathcal{F}(\rho_\omega)$. Performing the t-maximization for $n = 2, \ldots, 5000$ we numerically found the precision scaling to be $\delta\omega \propto n^{-\frac{5}{6}}$. We confirmed this scaling for n up to 10^8, using the numerical channel extension method proposed in [60, 64].

We also investigated the case, in which the generator of noise is slightly deviated from the direction perpendicular to the evolution generator σ_z, namely we assumed $\alpha_x = 1 - \epsilon$ and $\alpha_z = \epsilon$ in (36). In this case, our numerical analysis shows that the uncertainty of the frequency estimation $\delta\omega$ initially scales super-classicaly, however for higher n the scaling goes back to a classical one. We found numerically, that the critical n, for which the scaling starts to return to a classical one can be approximated by $n_{crit} \approx 3\omega/(8\gamma\epsilon^{3/2})$.

Our analysis gives a strong numerical evidence, that if the noise is perpendicular to the evolution, the precision of frequency estimation scales better than classically for $n \to \infty$, however an arbitrarilly small deviation from this perpendicularity brings the precision scaling back to the classical one. Although we do not have a formal analytical proof, and the result seems very restrictive from the experimental perspective, it allows to treat quantum metrology not only as a pure theoretical exercise, and gives a motivation for finding new effective realistic protocols for an ultra precise parameter estimation [65].

3.3.2 Quantum Distributed Computing

Distributed computing is a broad class of computational models, the common feature of which is the existence of several autonomous computational units, which have local memories and can communicate with each other in order to solve some common problem. In [F] we focus on a distributed graph models called $\mathcal{LOCAL}$ models [66]: such models assume that one has n distributed processors (nodes), which operate in *synchronous* rounds, each round consisting of a local computation and communication with nodes linked as nearest neighbours. The local computational power of each node and the amount of communication between adjacent nodes are unbounded. The input is defined as a labeled graph G_x and has two tasks: it defines a local numerical inputs $x(v)$ and the topology of communication links between the nodes. The output is simply defined as a vector of local variables $y(v)$ given by each node. A *problem* is defined as a map from the inputs G_x into the set of acceptable outputs. The complexity of a problem is measured by the *minimal number of rounds* needed to obtain an

[5] Note that $\mathcal{F}(\rho_\omega)$ is an implicit funtion of t, via dependence on ρ_ω.

acceptable output with certainty.

Several works produced over the last few years attempt to incorporate quantum effects, like entanglement or quantum communication, to the scenario of distributed computing, and the set of these hybrid models is referred to as *quantum distributed computing* [67]. All these attempts are lacking a consistent framework, which leads to an overestimation of the role of quantumness in solving some distributed problems[6][69, 70, 71].

In [F] we systematically introduced several quantum extensions of a $\mathcal{LOCAL}$ model and found a hierarchy of these extensions with respect to their computational power. We have also defined a resource-independent model φ-$\mathcal{LOCAL}$, containing all the quantum extensions, which represents the intuition of physical locality in a distributed computational scenario.

Round-based distributed computing is one of the three basic computational models, in which adding quantum resources significantly decreases complexity of solving particular problems. The nature of this *quantum reduction in complexity* is even today not fully understood, however some intuitive approaches have been suggested. Namely, in the *decision tree model of computations*, which involves the most famous quantum algorithms, like Deutsch-Jozsa algorithm [72] or Simon's algorithm [73], the quantum gain is thought to come from the fact, that the quantum oracle can be fed with lengthy superposition of computational basis states [74]. In the *communication complexity* scenario [75, 20], which is a model of distributed systems, in which the complexity is measured by the minimal number of total communication between the nodes, the *quantum reduction in communication complexity* comes in two different scenarios. In the first one, the power of quantum communication is compared with the classical communication and the fairness of this comparison is based on Holevo bound [76], which states, in the simplest version, that by communicating n qubits one can directly communicate at most n bits of classical message. In the second scenario one compares the computational power of a distributed system with classically communicating nodes with and without access to entangled quantum particles. Here, the reduction in communication complexity can be treated as a manifestation of nonclassicality of quantum correlations [39].

We show that in the model of round based distributed computing, the quantum reduction in the number of rounds can be attributed to reduction in communication complexity in both above discussed versions. Although we do not prove any sort of equivalence between these two different notions of complexity in distributed systems, we indicate a deep conection between them, which demands further analysis. We also demonstrate, that the computational power of all quantum extensions is significantly bounded by the principle of *physical locality*.

At first stage we define [F] two extensions of $\mathcal{LOCAL}$ model which introduce aditional resources at the initialization of the distributed algorithm, that is before the input G_x is given to the nodes. In the first extension, $\mathcal{LOCAL}^{+}\mathcal{S}$, we assume that the set of initial states of each processor is chosen randomly according to some probability distribution. In physical terms this corresponds to a creation of a separable state shared by the nodes, whereas in computational terms it can be interpreted as a *shared randomness*. Note that the $\mathcal{LOCAL}$

[6]Note that a similar problem occured in the context of so called *Static Quantum Games*, cf. [68].

model does not assume any bounds on local memory and local computational procedures, hence the amount of shared randomness in the $\mathcal{LOCAL}^+\mathcal{S}$ model is unbounded. In the second extension, $\mathcal{LOCAL}^+\mathcal{E}$, each node is equipped with a quantum register of arbitrary dimension, and the initialization relies on creating an n-partite, possibly entangled state, which is shared by all the parties.

The second type of extension, $\mathcal{LOCAL}^+\mathcal{Q}$ allows for unbounded communication of quantum particles inbetween nodes which are connected by a link, according to the input graph G_x.

Let us denote by $\mathcal{LOCAL}[t]$ the complexity class of problems, that can be solved within a $\mathcal{LOCAL}$ model in at most t rounds of computation. Analogically we define complexity classes for $\mathcal{LOCAL}^+\mathcal{S}[t]$, $\mathcal{LOCAL}^+\mathcal{E}[t]$ and $\mathcal{LOCAL}^+\mathcal{Q}[t]$. The hierarchy of the above defined models can be determined by the following intuitive arguments:

- $\mathcal{LOCAL} \subsetneq \mathcal{LOCAL}^+\mathcal{S}$; trivially all problems in $\mathcal{LOCAL}[t]$ belong to $\mathcal{LOCAL}^+\mathcal{S}[t]$ with trivial initialization; however, the problem of assigning unique node identifiers to all the processors assuming empty input, cannot be solved in $\mathcal{LOCAL}[t]$ for any t, but can be solved in $\mathcal{LOCAL}^+\mathcal{S}[0]$.

- $\mathcal{LOCAL}^+\mathcal{S} \subsetneq \mathcal{LOCAL}^+\mathcal{E}$; trivially any problem in $\mathcal{LOCAL}^+\mathcal{S}$ belongs to $\mathcal{LOCAL}^+\mathcal{E}$ by choosing a separable state at the initialization; however, the 3-partite modulo-4 problem [77, 78] in the setting with empty initial graph, cannot be solved in $\mathcal{LOCAL}^+\mathcal{S}[t]$ for any t, whereas it can be solved in $\mathcal{LOCAL}^+\mathcal{E}[0]$ by preparing a 3-partite GHZ state inbetween the nodes; this fact can be seen as a distributed-computing version of a GHZ paradox [79]; note that this argument can be understood in terms of communication complexity, namely that the correlations of GHZ state cannot be simulated by a locally computable functions with access to unbounded shared randomness, but without communication.

- $\mathcal{LOCAL} \subsetneq \mathcal{LOCAL}^+\mathcal{Q}$; trivially all problems in $\mathcal{LOCAL}[t]$ belong to $\mathcal{LOCAL}^+\mathcal{Q}[t]$ without quantum communication; consider now a problem defined on $n = 3k + 1$ nodes, and the input graph as a uniformly subdivided star with central node of degree 3; the problem relies on solving a modulo-4 problem by 3 external nodes of the star; within $\mathcal{LOCAL}^+\mathcal{Q}$ this can be done in k rounds by creating a GHZ state in the central node and sending it to three external nodes by quantum communication links; this process cannot be simulated by communicating arbitrary number of classical information from the central node, and needs direct communication between the three leaves of the star which demands $2k$ rounds; in this example, the discrepancy inebetween the models can be attributed to quantum communication complexity argument, that sending away entangled qubits cannot be simulated by sending away arbitrary number of correlated bits.

- $\mathcal{LOCAL}^+\mathcal{Q} \subsetneq \mathcal{LOCAL}^+\mathcal{E}$; the distributed modulo-4 problem with empty graph, which is in $\mathcal{LOCAL}^+\mathcal{E}[0]$ cannot be solved in $\mathcal{LOCAL}^+\mathcal{Q}[t]$ since there is no communication between the nodes; on the other hand, quantum communication links can be simulated in the $\mathcal{LOCAL}^+\mathcal{E}$ model by quantum teleportation [19], hence every problem solvable in $\mathcal{LOCAL}^+\mathcal{Q}[t]$ can be solved in $\mathcal{LOCAL}^+\mathcal{E}[t]$.

- $\mathcal{LOCAL}^{+}\mathcal{Q}$ and $\mathcal{LOCAL}^{+}\mathcal{S}$ are incomparable.

All of the above extensions are fully consistent with the intuitive notion of *physical locality*, which in the context of $\mathcal{LOCAL}$ model means, that the input of each node v after t rounds of executing an algorithm can affect the probabilities of outcomes of nodes, which are within distance of at most t edges from the node v, and this property must hold for arbitrary input graph G_x. This intuition corresponds to the notion of a finite speed of propagation of information in lattice models with nearest-neighbour interaction [80]. We define φ-$\mathcal{LOCAL}$ model as the set of all models that preserve the above defined notion of locality. In the extended version of the article [81] we show that the models $\mathcal{LOCAL}$, $\mathcal{LOCAL}^{+}\mathcal{S}$, $\mathcal{LOCAL}^{+}\mathcal{Q}$ and $\mathcal{LOCAL}^{+}\mathcal{E}$ belong to φ-$\mathcal{LOCAL}$ and leave as an open question, whether this inclusion is strict. Note that the φ-$\mathcal{LOCAL}$ model is defined in a theory-independent way, that is it does not directly specify the allowed resources. The definition of φ-$\mathcal{LOCAL}$ restricted to $t = 0$ is equivalent to the notion of *non-signalling* in generalized probabilistic teories [82].

The introduction of φ-$\mathcal{LOCAL}$ model, apart from its intuitive meaning, significantly simplifies proving lower bounds on computation complexity of several problems within quantum extensions. Namely, it is much easier to prove, that every solution to a given problem after k rounds violates physical locality, than directly prove, that the problem cannot be solved by some quantum extension within k rounds of computation. In this way we prove, that *distributed consensus*[83][7] $\notin \varphi$-$\mathcal{LOCAL}$[0], which implies it cannot be solved by any quantum extension without communication, since existence of such a solution would imply violation of physical locality.

Apart from this intuitive exposition, in an extended version [81] of the work [F], we provide a formal mathematical characterization of all the quantum extensions. This is done in the language of local C^* algebras, and is motivated by the approach presented in [84, 80, 85]. Within this formalization we provide a general proof of the fact, that all considered extensions of a $\mathcal{LOCAL}$ model belong to φ-$\mathcal{LOCAL}$.

PhD Thesis Publications

[A] W. Laskowski, M. Markiewicz, T. Paterek and M. Żukowski, *Correlation tensor criteria for genuine multiqubit entanglement*, Phys. Rev. A **84**, 062305 (2011).

[B] M. Markiewicz, W. Laskowski, T. Paterek and M. Żukowski, *Detecting genuine multipartite entanglement of pure states with bipartite correlations*, Phys. Rev. A. **87**, 034301 (2013).

[C] W. Laskowski, M. Markiewicz, T. Paterek and M. Wieśniak, *Incompatible local hidden-variable models of quantum correlations*, Phys. Rev. A **86**, 032105 (2012).

[D] W. Laskowski, M. Markiewicz, T. Paterek and R. Weinar, *Entanglement witnesses with variable number of local measurements*, Phys. Rev. A. **88**, 022304 (2013).

[7] A *distributed consensus* is a problem, in which n nodes are given input labels $\{x_i\}_{i=1}^n$, and their task is to output the same number $y \in \{x_i\}_{i=1}^n$.

[E] R. Chaves, J. B. Brask, M. Markiewicz, J. Kołodyński and A. Acín, *Noisy metrology beyond the standard quantum limit*, Phys. Rev. Lett. **111**, 120401 (2013).

[F] C. Gavoille, A. Kosowski and M. Markiewicz, *What Can Be Observed Locally? Round Based Models for Quantum Distributed Computing*, Springer Lecture Notes in Computer Science **5805**, pp. 243-257 (2009).

References

[1] A. Einstein, B. Podolsky, and N. Rosen. *Phys. Rev.*, 47:777, 1935.

[2] E. Schrödinger. Probability relations between separated systems. *Proc. Camb. Phil. Soc.*, 32:446, 1936.

[3] R. Horodecki and P. Horodecki. *Phys. Lett. A*, 197:147, 1994.

[4] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. *Rev. Mod. Phys.*, 81:865942, 2009.

[5] W. A. Majewski. Separable and entangled states of composite quantum systems; rigorous description. *quant-ph/9711051*, 1997.

[6] I. Cuculescu. Some remarks on tensor products of standard forms of von neumann algebras. *Bolletino U.M.I.*, 7:907–919, 1993.

[7] J.S. Bell. *Physics*, 1:195, 1964.

[8] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. *arXiv[quant-ph]:1303.284*, 2013.

[9] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt. *Phys. Rev. Lett.*, 23:880–884, 1969.

[10] R. Chaves. *Phys. Rev. A*, 87:022102, 2013.

[11] P. Kurzynski, M. Markiewicz, and D. Kaszlikowski. *arXiv[quant-ph]:1310.5644*, 2013.

[12] P. Kurzynski and D. Kaszlikowski. *Phys. Rev. A*, 89:012103, 2013.

[13] R. Omnès. *Rev. Mod. Phys.*, 64:339, 1992.

[14] R. B. Griffiths. *Consistent Quantum Theory*. Cambridge University Press, 2003.

[15] R. F. Streater. *Lost Causes in and beyond Physics*. Springer-Verlag, 2007.

[16] B.-G. Englert. *Eur. Phys. J. D*, 67:238, 2013.

[17] C. H. Bennett, G. Brassard, C. Crpeau, R. Jozsa, A. Peres, and W. K. Wootters. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[18] M. Żukowski, A. Zeilinger, M. Horne, and A. Ekert. *Phys. Rev. Lett.*, 71:4297, 1993.

[19] L. Accardi and M. Ohya. *arXiv:quant-ph/9912087*, 1999.

[20] G. Brassard. *arXiv:quant-ph/0101005*, 2001.

[21] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev. *Rev. Mod. Phys.*, 81:1301, 2009.

[22] V. Giovannetti, S. Lloyd, and L. Maccone. *Nature Photonics*, 5:222, 2011.

[23] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press.

[24] D. Kaszlikowski, A. Sen(De), U. Sen, V. Vedral, and A. Winter. *Phys. Rev. Lett.*, 101:070502, 2008.

[25] C. H. Bennett, A. Grudka, M. Horodecki, P. Horodecki, and R. Horodecki. *Phys. Rev. A*, 83:012312, 2011.

[26] R. F. Werner. *Phys. Rev. A*, 40:4277–4281, 1989.

[27] M. Seevinck and J. Uffink. *Phys. Rev. A*, 78:032101, 2008.

[28] M. Horodecki, P. Horodecki, and R. Horodecki. *Phys. Lett. A*, 283:1, 2001.

[29] P. Badziąg, Č. Brukner, W. Laskowski, T. Paterek, and M. Żukowski. *Phys. Rev. Lett.*, 100:140403, 2008.

[30] V. Coffman, J. Kundu, and W. K. Wootters. *Phys. Rev. A*, 61:052306, 2000.

[31] N. Gisin A. Acin and L. Masanes. *Phys. Rev. Lett.*, 97:120405, 2006.

[32] M. Pawlowski. *Phys. Rev. A*, 82:032313, 2010.

[33] P. Kurzynski, M. Markiewicz, and D. Kaszlikowski. *arXiv[quant-ph]:1312.5263*, 2013.

[34] R. Dicke. *Phys. Rev.*, 93:99, 1954.

[35] P. Parashar and S. Rana. *Phys. Rev. A*, 80:012319, 2009.

[36] A. Klyachko. *arXiv:quant-ph/0409113*, 2004.

[37] M. Christandl, R. Koenig, G. Mitchison, and R. Renner. *Comm. Math. Phys.*, 273:473–498, 2007.

[38] R. F. Streater. *arXiv:math-ph/0002049*, 2000.

[39] C. Brukner and M. Żukowski. *Bell's Inequalities: Foundations and Quantum Communication in Handbook of Natural Computing*. Springer, 2010.

[40] K. Nagata, W. Laskowski, M. Wiesniak, and M. Żukowski. *Phys. Rev. Lett.*, 93:230403, 2004.

[41] A. Fine. *Phys. Rev. Lett.*, 48:291, 1982.

[42] M. Żukowski and C. Brukner. *Phys. Rev. Lett.*, 88:210401, 1990.

[43] J. Gruca, W. Laskowski, M. Żukowski, N. Kiesel, W. Wieczorek, C. Schmid, and H. Weinfurter. *Phys. Rev. A*, 82:012118, 2010.

[44] M. Horodecki, P. Horodecki, and R. Horodecki. *Phys. Lett. A*, 223:1, 1996.

[45] O. Gühne, P. Hyllus, D. Bru, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera. *Phys. Rev. A*, 66:062305, 2002.

[46] O. Gühne, P. Hyllus, D. Bru, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera. *J. Mod. Opt.*, 50:1079, 2003.

[47] O. Gühne and N. Lütkenhaus. *Phys. Rev. Lett.*, 96:170502, 2006.

[48] W. Dür, G. Vidal, and J. I. Cirac. *Phys. Rev. A*, 62:062314, 2000.

[49] M. Holland and K. Burnett. *Phys. Rev. Lett.*, 71:1355, 1993.

[50] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac. *Phys. Rev. Lett.*, 79:3865, 1997.

[51] V. Buzek, R. Derka, and S. Massar. *Phys. Rev. Lett.*, 82:2207–2210, 1999.

[52] The LIGO Scientific Collaboration. *Nat. Phys.*, 7:962, 2011.

[53] H. Cramer. *Mathematical Methods of Statistics*. Princeton Univ. Press, 1946.

[54] C.R. Rao. *Bulletin of the Calcutta Mathematical Society*, 37:81–89, 1945.

[55] A. Kossakowski. *Rep. Math. Phys.*, 3:247, 1972.

[56] G. Lindblad. *Commun. Math. Phys.*, 48:119, 1976.

[57] E. C. G. Sudarshan et al. *Phys. Rev.*, 121:920–924, 1961.

[58] K. Kraus. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. Springer Verlag, 1983.

[59] E. Andersson, J. D. Cresser, and M. J. W. Hall. *J. Mod. Opt.*, 54:1695, 2007.

[60] J. Kolodyński R. Demkowicz-Dobrzański and M. Guta. *Nature Communications*, 3:1063, 2012.

[61] S. L. Braunstein and C. M. Caves. *Phys. Rev. Lett.*, 72:3439, 1994.

[62] A. S. Holevo. *Probabilistic and Statistical Aspect of Quantum Theory*. North-Holland, Amsterdam, 1982.

[63] B. M. Eschera, R. L. de Matos Filho, and L. Davidovich. *Nat. Phys.*, 7:406, 2011.

[64] J. Kolodyński and R. Demkowicz-Dobrzański. *New J. Phys.*, 15:073043, 2013.

[65] W. Dür, M. Skotiniotis, F. Fröwis, and B. Kraus. *arXiv:1310.3750 [quant-ph]*, 2013.

[66] N. Linial. *28th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 331–335, 1987.

[67] V. S. Denchev and G. Pandurangan. Distributed quantum computing: A new frontier in distributed systems or science fiction? *ACM SIGACT News - Distributed Computing Column*, 39:77–95, 2008.

[68] M. Markiewicz, A. Kosowski, T. Tylec, J. Pykacz, and C. Gavoille. *arXiv:1001.2257 [quant-ph]*, 2010.

[69] S. P. Pal, S. K. Singh, and S. Kumar. *arXiv:quant-ph/0306195*, 2003.

[70] E. D'Hondt and P. Panangaden. *Quant. Inf. Comp.*, 6:173–183, 2006.

[71] L. Helm. Brief announcement: Quantum distributed consensus. *27th Annual ACM Symposium on Principles of Distributed Computing (PODC)*, page 445, 2008.

[72] D. Deutsch and R. Jozsa. *Proceedings of the Royal Soci- ety of London A*, 439, 1992.

[73] D.R. Simon. *Siam J. Comp.*, 26:1474, 1997.

[74] F. Brandao and M. Horodecki. *Q. Inf. Comp.*, 13:0901, 2013.

[75] A. Yao. *Proceedings of the 11th Annual ACM Sympo- sium on Theory of Computing*, 209, 1979.

[76] A. Holevo. *Problems of Information Transmission*, 9:177–183, 1973.

[77] P. Trojek, Ch. Schmid, M. Bourennane, C. Brukner, M. Żukowski, and H. Weinfurter. *Phys. Rev. A*, 72:050305(R), 2005.

[78] M. Żukowski. On bells theorem, quantum communication, and entanglement detection. *Foundations of Probability and Physics*, 5, 2008.

[79] D. M. Greenberger, M. A. Horne, and A. Zeilinger. *Bells Theorem, Quantum Theory, and Conceptions of the Universe*. Kluwer, 1989.

[80] O. Bratelli and D. W. Robinson. *Operator algebras and quantum statistical mechanics, volume II*. Springer-Verlag, 1981.

[81] C. Gavoille, A. Kosowski, and M. Markiewicz. *arXiv: quant-ph/0903.1133*, 2009.

[82] A.J. Short and J. Barrett. *New J. Phys.*, 12:033034, 2010.

[83] N. Lynch. *Distributed Algorithms*. Morgan Kaufmann Publishers, 1997.

[84] O. Bratelli and D. W. Robinson. *Operator algebras and quantum statistical mechanics, volume I*. Springer-Verlag, 1979.

[85] R. Haag. *Local Quantum Physics: Fields, Particles, Algebras*. Springer, 1992.