Quantum Anonymous Veto with Hardy Paradox

Ramij Rahaman[1] * Marcin Wieśniak[1] † and Marek Żukowski[1] ‡

[1]*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*

Abstract. We present a secure quantum protocol for the Anonymous Veto problem by introducing a new variant of the Hardy's paradox for n qu*D*its case. The Anonymous Veto problem allows a voting party in a jury to anonymously veto a decision, which is to be approved unanimously. Whereas, our multi qu*D*it Hardy paradox satisfies only by a genuine multipartite entangled state and shows a direct contradiction with local realism without any statistical inequalities. Moreover, in some cases, it can distinguish a unique state satisfying all Hardy conditions and the uniqueness of the state allows a secure quantum solution of the problem.

Keywords: Hardy paradox, Multipartite entanglement, Anonymous Veto & dining cryptographers problem

Due to the existence of entanglement in quantum physics, quantum information theory provides a means to perform some tasks that would be impossible in classical information theory. Therefore, entanglement is considered to be the most useful resource in the context of quantum information theory. In 1964, J.S. Bell, proved that correlations, such as the entanglement between two or more particles in quantum mechanics, cannot be reproduced by any local-realistic (LR) theory [1]. This was a first answer to the foundational debate "*Can quantum mechanical description of reality be considered complete*" [2] started by *Einstein* along with *Podolsky* and *Rosen* (EPR). Later, *Hardy* gave an argument which also reveals the same non-LR character of quantum mechanics [3]. His argument, unlike Bell's argument, does not use statistical inequalities involving expectation values. This caused much interest among physicists.

On the other hand, the structure of multipartite entanglement is not a simple extension of the bipartite one. E.g., for three qubits there are two different classes of pure genuinely three-partite entanglement, and also one may have entanglement of just two parties. Most of features of bipartite entanglement are well understood, whereas the multipartite entanglement this is still not the case. The rich structure of the multipartite entanglement can be used for various tasks, such as quantum computation [4], quantum simulation [5], quantum metrology [6]. This inspired broad theoretical and experimental studies, [7, 8]. In this regards, we extend the approach of Hardy [3] to an arbitrary n-partite scenario, and show that only a genuine multipartite entangled state[1] can satisfy our generalized Hardy-type (GHt) argument. Therefore, this can be used as a wittiness for genuine multipartite entanglement. For qubit systems, only a *unique* pure genuinely multipartite entangled state satisfies our GHt argument for two dichotomic observables per site. Thus, an important feature of original Hardy-type two-qubit argument is preserved. This feature is missing in most other multipartite Bell-type tests and totally absent in all the proposed generalizations of Hardy-type argument for more than two-qubit case [9, 10, 11, 12, 13]. We also find that the GHt correlations can be used to construct a quantum protocol for anonymous veto, which is a cryptographic problem with classical solutions, security of which is based on computational hardness, see [14] and [15]. Secure protocols for anonymous veto (or related "dining cryptographers"), allow to take decisions, by some jury, which must be unanimous, without ever revealing the possible vetoing party(-ies). Thus, they are important in many aspects for functioning of human societies.

We now give an overall idea of our Quantum Anonymous Veto Protocol. All other results on GHt argument and the detail of this protocol can be found in Ref. [16].

Quantum Anonymous Veto Protocol: Imagine a jury with N members, who need to take an unanimous decision, but at the same time want their individual decisions to remain secret. N-qubit Hardy argument i.e., the following set of joint probability conditions

$$\begin{aligned} P(\hat{u}_1=+1,\hat{u}_2=+1,....,\hat{u}_N=+1) &= q>0, && (1)\\ \forall\ r\le N:\ P(\hat{v}_r=+1,\hat{u}_{r+1}=+1) &= 0, && (2)\\ P(\hat{v}_1=-1,\hat{v}_2=-1,....,\hat{v}_N=-1) &= 0 && (3)\end{aligned}$$

would allow them to achieve this. Imagine that the observables in the above conditions are, say, $\hat{u}_k=\sigma_z$ and $\hat{v}_k=-\sigma_x$. In such a case only the following state has the properties (1-3)

$$|\phi_N\rangle=\frac{1}{\sqrt{2^N-1}}\left[2^{\frac{N}{2}}|1\rangle^{\otimes N}-|+\rangle^{\otimes N}\right], \qquad (4)$$

where $|+\rangle=\frac{1}{\sqrt{2}}\left[|0\rangle+|1\rangle\right]$. Here the computational basis is the one of σ_z, and $|+\rangle$ is the -1 eigenstate of $-\sigma_x$. Note, that due to the symmetry of the state with respect to any permutation of the qubits, the condition (2) can be replaced by a more general one: $\forall\ r\neq s:\ P(\hat{v}_r=+1,\hat{u}_s=+1)=0$.

Each jury member receives one of the qubits, and can make secret measurements on them. The local measuring devices provide a choice between the two observables

*ramij.rahaman@ug.edu.pl

†marcin.wiesniak@univie.ac.at

‡marek.zukowski@univie.ac.at

[1] The state is not-biseparable with respect to any partition of subsystems.

mentioned above (settings). Choosing $\hat{u}_k$ represents being "in favor", "vetoing" is represented by $\hat{v}_k$.

A high repetition rate (event ready) quantum interferometric device [2], sends qubits in the state to the jury members. Before every run, each of the members randomly chooses whether this run would be a voting one or testing one. The testing runs may use different settings, and their results and settings are announced (after the measurements are done). Testing measurements in principle perform a kind of state tomography, or state witness operation, which assures that the delivered state is indeed (4). Details can be spared. Otherwise, the jury members choose the setting corresponding to his/her own opinion and collect the measurement data. They send data to the referee after a certain data processing, described below.

Each jury member has a list of results under voting settings, correlated with the timing of the measurements. Those who vetoed randomly reject the runs, which yielded the outcome '+1' until the proportion between '+1's and '−1's in their table is $1 : (2^N - 2)$, as such would be the local statistics for those who were in favor. Next, all jury members randomly further reduce their lists by a certain big enough factor to a fixed (for all the same) number of entries. This is to hide how many results were rejected in the first step and hence again hide members' individual decisions. Next, each partner sends the list of their reduced samples (*i.e.*, the timing information of the selected events, but not their results) to the referee. The referee finds a common part of the lists of the timings. The list of common timings must be very large. This can be guaranteed by the high repetition rate of the source.

The referee then asks a random jury member at a time about his/her *result* in a randomly chosen run in the common part, and continues this procedure until in this way patiently collects all the results related with the runs that were sharing timing. The referee has all results for each run associated with a common timing, $x_i(T_k) = \pm 1$, where i denotes a jury member, and T_k is the timing.

If any jury member vetoes, but there was a disagreement, due to the condition (2), one cannot have $\sum_{i=1}^{N} x_i(T_k) = N$ for any k. Thus if in the collected data the referee does not see strings of results related with the same T_k which have all +1's, he/she can safely (high statistics!) conclude that somebody was vetoing. However, if such a string is occurring (many times, we assume big statistics), the vote must be unanimous, because of (1) and the fact that for the state $P(\forall\ i\ :\ \hat{v}_i = +1) > 0$. If there is no string related to a common T_k with all results −1, everybody must have been against, see (3). Otherwise, the vote is unanimously in favour, as for the state $P(\forall\ i\ :\ \hat{u}_i = -1) > 0$.

In summary, our generalized Hardy-type (GHt) argument provides new and interesting results on both the fundamental and the application level. On one side the GHt argument can be used as a tool to study the structure of multipartite entanglement, on the other - it provides us secure protocols for various cryptographic problems. Finally we remark that we also studied the maximum probability of success (MPS) of the GHt argument for three two-level systems under a generalized non-signaling theory (GNST) and in quantum theory. We found that the maximum value of the probability for quantum theory is 0.0181938, and for GNST it is $\frac{1}{3}$. Interestingly, for both cases MPS is lower than for two two-level systems.

Acknowledgments: We thank Guruprasad Kar, Sibasish Ghosh and Mohamed Bourennane for stimulating discussions. R.R. and M.Z. acknowledge support by Foundation for Polish Science (FNP) TEAM/2011-8/9 project co-financed by EU European Regional Development Fund, and ERC grant QOLAPS(291348). M.W. acknowledges support from FNP (HOMING PLUS/2011-4/14) and project QUASAR.

References

[1] J. S. Bell, *Physics* **1**, 195 (1964).

[2] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).

[3] L. Hardy, *Phys. Rev. Lett.* **68**, 2981 (1992).

[4] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).

[5] S. Lloyd, *Science* **273**, 1073 (1996).

[6] L. Pezzé and A. Smerzi, *Phys. Rev. Lett.* **102**, 100401 (2009).

[7] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki, *Rev. Mod. Phys.* **81** 865 (2009).

[8] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Żukowski, *Rev. Mod. Phys.* **84**, 777 (2012).

[9] S. K. Choudhary, S. Ghosh, G. Kar and R. Rahaman, *Phys. Rev. A* **81**, 042107 (2010).

[10] S. Yu, Q. Chen, C. Zhang, C. H. Lai and C. H. Oh, *Phys. Rev. Lett.* **109**, 120402 (2012).

[11] S. Ghosh, G. Kar, and D. Sarkar, *Phys. Lett. A* **243**, 249 (1998); X.-H. Wu and R.-H. Xie, *Phys. Lett. A* **211**, 129 (1996).

[12] S. K. Chudhary, S. Ghosh, G. Kar, S. Kunkri, R. Rahaman, and A. Roy, *Quant. Inf. Comp.* **10**, 0859 (2010); K. S. Parasuram and S. Ghosh, *J. Phys. A: Math. Theor.* **44**, 315305 (2011).

[13] Q. Chen, S. Yu, C. Zhang, C. H. Lai, and C. H. Oh, arxiv.org:1305.4472.

[14] F. Hao and P. Zieliński, *A 2-round anonymous veto protocol, Proc. 14th Works. Secur. Prot.* 2006.

[15] D. Chuam, *Jour. Crypt.* **1**, 65 (1998).

[16] R. Rahaman, M. Wieśniak, M. Żukowski, arXiv:1303.0128.

[2] For a review of such techniques see [8].