# The Impossibility of Pseudo-Telepathy Without Quantum Entanglement

Viktor Galliard[1] Alain Tapp[2] Stefan Wolf[2]

*Abstract* — **In a *pseudo-telepathy game*, communication can be entirely replaced by quantum entanglement. We provide, for the first proposed and simplest two-player game of this type, the proof that communication is indeed necessary to win with certainty if *no* quantum entanglement is shared by the players. This completes the game's analysis and shows its "pseudo-telepathic" properties.**

## I. The Game by Brassard, Cleve, and Tapp

Consider the following simple game. Alice and Bob, unable to communicate, are both given a 16-bit string such that the strings are either equal, or they differ in exactly 8 positions. Both parties are then supposed to output a 4-bit string in such a way that these short strings are equal if and only if the original longer strings given to them were equal as well; if they manage to do this, we say that they *win the game*.

The described game is a special case of so-called *pseudo-telepathy* and was proposed in [1], where it was shown that it can be won without failure by two parties sharing some *quantum entanglement*. Due to the additional fact that the game *cannot* be won otherwise, it can be used as a simple demonstration experiment for the existence of such entanglement. Previously, the impossibility result has, however, been proven only "asymptotically" (i.e., for games where the involved strings are long enough), and no specific parameters have been known for which the game has the described "pseudo-telepathic" property. We provide this proof for the game as described above. Our result, together with the possibility result for the quantum setting, implies that in the context of this particular game, quantum entanglement can *replace* classical communication; note that entanglement does not, however, *allow* for such communication.

## II. A Classical Impossibility Result

**Theorem 1.** *Classically, the described pseudo-telepathy game cannot be won with certainty.*

*Proof Sketch.* Consider the graph $G = (V, E)$ defined by $V = \{0,1\}^{16}$ and $E = \{(v, w) \in V^2 \mid d_H(v, w) = 8\}$. In [2], it was shown that a winning strategy, should it exist, is a coloring of $G$ with 16 colors. We show that its chromatic number $\chi(G)$ is, however, larger than 16, by giving an upper bound on the size $M$ of a maximum independent set $I$ of $G$, and by using $\chi(G) \geq 2^{16}/M$. More precisely, we show that for any independent set $I$ of $G$, we have $|I| \leq 3912$ $(< 2^{16}/16)$.

We simplify this problem step by step. First, we observe that the graph $G$ consists of two isomorphic connected components $G_e$ and $G_o$ (containing the vertices of even and odd Hamming weight, respectively). Secondly, a maximum independent set contains a vertex $v$ if and only if it also contains its bitwise complement $\overline{v}$ since for all vertices $w$, we have $d_H(v, w) = 8 \leftrightarrow d_H(\overline{v}, w) = 8$. Let $G_{e,<8}$ be the subgraph of $G_e$ containing the vertices of Hamming weight less than 8, let, for $i = 0, 2, 4$, and 6 $G_i$ be the subgraph of $G_{e,<8}$ containing the vertices of Hamming weight $i$, and let for a graph $H$ $M(H)$ denote the size of a maximum independent set of $H$. Since $M(G) \leq 4(M(G_0)+M(G_2)+M(G_4)+M(G_6))$, it is sufficient to prove $M(G_0)+M(G_2)+M(G_4)+M(G_6) \leq 3912/4 = 978$. We will show $M(G_0) = 1$, $M(G_2) = 120$, $M(G_4) = 455$, and $M(G_6) \leq 402$.

$M(G_0) = 1$ is trivial. $M(G_2) = \binom{16}{2} = 120$ holds since none of the vertices in $G_2$ are connected. $M(G_4) = \binom{16-1}{4-1} = 455$ follows directly from a combinatorial result by Erdös *et. al.* [3]. Let finally $I$ be an independent set of $G_6$ such that every two vertices $u$ and $v$ of $I$ satisfy $d_H(u, v) \leq 6$. Then the same combinatorial result implies $|I| \leq \binom{16-3}{6-3} = 286$. We hence deal with the remaining cases of independent sets $I$ containing $u, v \in I$ with $d_H(u, v) \in \{10, 12\}$. Let first $u, v \in I$ with $d_H(u, v) = 12$. (Without loss of generality, we can assume $u = 111111 \cdot 000000 \cdot 0000$ and $v = 000000 \cdot 111111 \cdot 0000$.) A third vertex $w \in I$ has to be of one of eight different "types" (where two strings are of the same type if their substrings composed by the first and second group of six bits have the same Hamming weight). Let now, for fixed $u$, $v$, and $w$, $G_{6,uvw}$ be the subgraph of $G_6$ arising when $u$, $v$, $w$, and their neighbors are removed. In order to find an upper bound on $M(G_{6,uvw})$, we decompose the graph into disjoint cliques, the number of which is such a bound. Using a simple greedy algorithm, we found such decompositions for all possible vertices $w$ (or, more precisely, "types" of vertices). For three of the types, the number of cliques is at most 399, whereas the rest of the "type sets" together contain less than 399 vertices in total. (The relevant clique decompositions can be found at [4].) Any independent set $I$ of $G_6$ containing two vertices with Hamming distance 12 is thus of size at most $402 = 399 + 3$. The proof for independent sets $I$ of $G_6$ containing two vertices of Hamming distance 10 is similar and leads to an even smaller bound than 402. □

[1] Untervaz, Switzerland. E-mail: math@galliard.ch. Supported by Canada's NSERC and Swisscom IT Services Ltd.

[2] Département d'Informatique et recherche opérationnelle, Université de Montréal, C.P. 6128 succ Centre-Ville, Montréal, Québec, H3C 3J7, Canada. E-mail: {tappa , wolf}@iro.umontreal.ca. Both authors are supported by Canada's NSERC.

## References

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

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

[3] P. Erdös, C. Ko, and R. Rado, "Intersection theorem for systems of finite sets", *Quarterly journal of mathematics*, Vol. 2, No. 12, pp. 313–320, 1961.

[4] http://math.galliard.ch/Quantum/pseudo-telepathy/data03/ptp_cliques_twg03.txt. In ptp_cliques_twg03_extract.txt, initial vertices and sizes of cliques are given.