XOR games with no quantum advantage and the Shannon zero-error channel capacity

Ravishankar Ramanathan,[1,*] Alastair Kay,[2,3] Gláucia Murta,[1,4]
Remigiusz Augusiak,[5] Michał Horodecki,[6,7] and Paweł Horodecki[1,8]

[1]*National Quantum Information Center of Gdańsk, 81-824 Sopot, Poland*
[2]*Department of Mathematics, Royal Holloway University of London, Egham, Surrey, TW20 0EX, UK*
[3]*University of Gdańsk, 80-952 Gdańsk, Poland*
[4]*Departamento de Fisica, Universidade Federal de Minas Gerais, Caixa Postal 702, 30123-970, Belo Horizonte, MG, Brazil*
[5]*ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*
[6]*National Quantum Information Center of Gdańsk, 81-824 Sopot, Poland*
[7]*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*
[8]*Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-233 Gdańsk, Poland*

The present abstract concerns the following works:

- R. Ramanathan, A. Kay, G. Murta, P. Horodecki, arXiv:1406.0995 [1].
- R. Augusiak, R. Ramanathan, G. Murta, M. Horodecki, P. Horodecki. *Work in Progress* (attached notes).

A bipartite non-local game is a co-operative game where two players, Alice and Bob, receive questions x and y from a referee and they are supposed to output answers, a and b respectively, with an aim to maximize a pay off function $V(a,b|x,y) \in \{0,1\}$. The score of the players is given by

$$\omega = \sum_{a,b,x,y} p(x,y)V(a,b|x,y)P(a,b|x,y). \tag{1}$$

The players are not allowed to communicate, but can pre-share some classical (shared randomness) or quantum resources (entangled states); with corresponding scores ω_c and ω_q respectively. These "Bell tests" have led to numerous philosophical and practical developments, such as demonstrating the indeterminacy of Nature [2] and providing the vital ingredient in quantum cryptography [3], even in a device-independent scenario. However, it is not only games where quantum theory provides an advantage that are worth considering, the games in which there is no quantum advantage reveal just as much about Nature [4]. The quintessential example of such a task is distributed non-local computation NLC_2, where the parties are required to compute an arbitrary (binary) function with non-locally encoded inputs, such that each party individually learns nothing, yet together an XOR of their outputs equals the correct function output. In [5], it was shown that quantum theory provides no advantage in this task, simply giving the best linear approximation to the function although super-quantum correlations *do* provide an advantage. This is such a powerful statement that the lack of non-local computation has been elevated to the status of an information-theoretic principle akin to the ones proposed in [6–10], with the aim of identifying the set of quantum correlations from among all non-signaling ones.

The NLC_2 games belong to the class of XOR games, where Alice and Bob each receive one among m inputs, $x, y \in [m]$, and the winning condition only depends on the XOR of their outputs, i.e. $V(a,b|x,y) = 1$ iff $a \oplus b = f(x,y)$. Binary XOR games (with $a, b \in \{0,1\}$) can be characterized by the game matrix [5]

$$\tilde{\Phi} = \sum_{x,y \in [m]} (-1)^{f(x,y)} p(x,y) |x\rangle\langle y|. \tag{2}$$

The celebrated theorem of Tsirelson [11] then allows the calculation of ω_q by a simple semi-definite program. The optimal quantum strategy proceeds by Alice and Bob measuring ± 1 observables A_x and B_y on a shared quantum state $|\psi\rangle$ when asked questions x and y respectively. This strategy can be represented in terms of unit vectors in $\mathbb{R}^m$ for each measurement of Alice ($\{|u_x\rangle\}$) and Bob ($\{|v_y\rangle\}$) [11–13]. The inner product $\langle u_x|v_y\rangle$ reproduces the expectation value of the observables. The quantum bias of the game, $\varepsilon_q := 2\omega_q - 1$, is thus given by an optimization over the real vectors, which is phrased as a semi-definite program ($\mathcal{P}$):

$$\begin{aligned} \varepsilon_q = \ \max \quad & \mathrm{Tr}[\tilde{\Phi}_s \mathcal{X}] \\ \text{s.t.} \quad & \mathrm{diag}(\mathcal{X}) = |j\rangle \oplus |j\rangle, \ \ \mathcal{X} \succeq 0, \end{aligned} \tag{3}$$

where $\mathcal{X} = \begin{pmatrix} A & S \\ S^T & B \end{pmatrix}$, $\tilde{\Phi}_s = \begin{pmatrix} 0 & \frac{1}{2}\tilde{\Phi} \\ \frac{1}{2}\tilde{\Phi}^T & 0 \end{pmatrix}$ and $|j\rangle = \sum_{x\in[m]} |x\rangle$ is the all-ones vector. S is the strategy matrix and is defined as an $m \times m$ matrix having entries $S_{x,y} = \langle u_x | v_y \rangle$. The matrices A, B with $A_{x,y} = \langle u_x | u_y \rangle$ and $B_{x,y} = \langle v_x | v_y \rangle$ describe local terms. In a deterministic classical strategy, the vectors $|u_x\rangle$ and $|v_y\rangle$ all equal $\pm|w\rangle$ for a single unit vector $|w\rangle$. The classical strategy matrix S_c is thus a matrix with ± 1 entries with all columns (and rows) being proportional to each other.

We first address the problem of categorizing the two-party binary XOR games which share the property of no quantum advantage, i.e., with $\omega_c = \omega_q$, for which we provide a necessary and sufficient condition, with an aim to identifying new information-theoretic principles and a deeper understanding of the set of quantum correlations. We remark that for every XOR game, there exists a super-quantum no-signaling strategy that wins the game, i.e. one that achieves $\omega_{ns} = 1$.

Theorem 1. *Consider a two-party binary* XOR *game with game matrix $\tilde{\Phi}$ with no all-zero row or column for which $S_c = |s^A\rangle\langle s^B|$ represents the optimal classical strategy. Let $\Sigma = diag(\{\langle i|\tilde{\Phi}|s^B\rangle\langle s^A|i\rangle\}_{i=1}^m)$ and $\Lambda = diag(\{\langle s^A|\tilde{\Phi}|i\rangle\langle i|s^B\rangle\}_{i=1}^m)$. There is no quantum advantage for $\tilde{\Phi}$ if and only if $\Sigma, \Lambda \succ 0$ and $\rho(\Lambda^{-1}\tilde{\Phi}^T\Sigma^{-1}\tilde{\Phi}) = 1$, where $\rho(.)$ denotes the spectral radius.*

As a consequence of Theorem 1, we can also derive a weaker sufficient condition for no quantum advantage:

Corollary 2. *If the maximum singular vectors of $\tilde{\Phi}$ only contain elements that are ± 1, then there is no quantum advantage for players of the game $\tilde{\Phi}$.*

These conditions allow us to single out new families of games with no quantum advantage for arbitrary input probability distributions, up to certain symmetries, see [1]. When considering games with no quantum advantage, it is also of interest to consider whether the corresponding Bell inequalities are tight, i.e., whether they form facets of the polytope of classical correlations. A tight inequality with no quantum advantage implies that the information-theoretic game identifies a portion of the boundary of quantum correlations which is of non-zero measure. By exhibiting an explicit decomposition of the NLC_2 games as sums of CHSH games and games which can be classically won, we show that these games do not constitute facets of the local polytope; we leave as open the question of existence of two-party facet Bell inequalities with no quantum advantage.

Shannon capacity of graphs. A recent interesting development [14–17] is that each non-local game can be associated with a *orthogonality graph* G, and the classical and quantum winning probability of the game are related to the important graph parameters independence number $\alpha(G)$ and the Lovász theta number $\theta(G)$ as

$$m^2\omega_c = \alpha(G) \leq \; m^2\omega_q \; \leq \theta(G). \tag{4}$$

For an XOR game with m inputs on each side, the orthogonality graph consists of $2m^2$ vertices $v \in V$. Each vertex is labeled by (x, y, a) and two vertices are connected by an edge iff ($x = x'$ and $a \neq a'$) or ($y = y'$ and $a \oplus a' \neq f(x, y) \oplus f(x', y)$. A related important information-theoretic quantity is the Shannon zero error capacity $\Theta(G)$ for sequential uses of a memoryless channel which is the maximum rate at which information can be sent through the channel with zero probability of error [18]. This quantity is traditionally described using the confusability graph G of the channel, where the vertices of the graph correspond to the inputs of the channel (letters of the encoding alphabet) and two vertices are connected by an edge if the corresponding inputs can be confused with each other by the receiver upon transmission through the channel. The zero-error Shannon capacity of the graph is then defined as

$$\Theta(G) := \sup_k \sqrt[k]{\alpha(G^k)}, \tag{5}$$

where G^k denotes the k-fold strong product of graph G with itself. Despite the importance of the Shannon capacity, remarkably few classes of graphs, such as perfect graphs [20], Kneser graphs, vertex-transitive self-complementary graphs [19] and König-Egerváry graphs [21–24], are known for which $\Theta(G)$ has been established analytically. In the majority of cases, these satisfy $\Theta(G) = \alpha(G)$, and are said to be class-1 graphs [20]. The Lovász number was introduced as an semi-definite relaxation of $\Theta(G)$ (whose computational complexity is unknown and whose value remains unknown even for graphs as simple as the seven cycle C_7!). Given a graph G we have the following relations [19]

$$\alpha(G) \leq \Theta(G) \leq \theta(G). \tag{6}$$

Our second main result is an identification of a new set of class-1 graphs by looking at the orthogonality graphs of XOR games with no quantum advantage. The adjacency matrix of a graph G associated with the XOR game is conveniently expressed as

$$\mathcal{A}(G) = \mathbb{1} \otimes (|j\rangle\langle j| - \mathbb{1}) \otimes X + \tfrac{1}{2}|j\rangle\langle j| \otimes \mathbb{1} \otimes (\mathbb{1} + X) - \tfrac{1}{2}[D(|j\rangle\langle j| \otimes \mathbb{1})D] \otimes (\mathbb{1} - X) \tag{7}$$

where X is the usual Pauli-X matrix and D is defined as $D = \sum_{x,y\in[m]}(-1)^{f(x,y)}|x,y\rangle\langle x,y|$. This graph is $(2m-1)$ regular, triangle free, and has a perfect matching [27]. We show that its spectrum, and corresponding degeneracies are given by

$$\text{spec}(\mathcal{A}(G)) = \begin{cases} 2m-1 & 1 \\ m-1 & 2m-2 \\ -1 & (m-1)^2 \\ 1-m\pm\lambda_z & 1 \\ 1 & m(m-2) \end{cases} \tag{8}$$

where λ_z denotes the m singular values of $\Phi := \sum_{x,y\in[m]}(-1)^{f(x,y)}|x\rangle\langle y|$. By (4) and (6) we see that a necessary condition for a game graph to be class-1 is that $\omega_q = \omega_c$. Motivated by this we have our main result.

Theorem 3. *Every two-party* XOR *game with m uniformly chosen inputs for each party, and satisfying Cor. 2 has a game graph which is class-1 (has $\Theta(G) = \alpha(G)$).*

We show that the family of game graphs described here is distinct from all previously described classes of graphs for which Shannon capacity has been calculated [19–24]. This result, remarkable simply due to the difficulty in evaluating the Shannon capacity even for very simple graphs, is a classical result derived as a consequence of insight from a study of a quantum-mechanical problem!

XOR games with d outcomes. We now consider d-output XOR games, i.e. those where the winning condition is expressed as $a \oplus b$ mod d $= f(x,y)$ with $a, b \in \{0, \ldots, d-1\}$ and $x, y \in [m]$. Such games were studied in [26]. For these games, we define a set of game matrices $\tilde{\Phi}_k$, with $k \in \{1, \ldots, d-1\}$ as

$$\tilde{\Phi}_k := \sum_{x,y\in[m]} p(x,y)\zeta^{kf(x,y)}\,|x\rangle\langle y|\,, \tag{9}$$

where $\zeta = e^{\frac{2\pi i}{d}}$ is the d-th root of unity, and use them to find an upper bound on their quantum value.

Lemma 4. *The quantum value of any d-output* XOR *game with winning relation $a \oplus b$ mod $d = f(x,y)$ obeys*

$$\omega_q \leq \frac{1}{d}\left(1 + m\sum_{k=1}^{d-1}\|\tilde{\Phi}_k\|\right), \tag{10}$$

where $\|.\|$ denotes the spectral norm of the matrix.

We also present a generalization of the class of non-local computation to the scenario of d outputs for prime d, a problem left as an open question in [5]. In these games which we label NLC_d, Alice and Bob receive n dits $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ respectively and are required to output a, b whose XOR equals the value of

$$f(x,y) = g(x_1 \oplus y_1, \ldots, x_{n-1} \oplus y_{n-1}) \cdot (x_n \oplus y_n) \tag{11}$$

for an arbitrary function g mapping $n-1$ dits to 1 dit. For simplicity, we restrict to the case of uniform probabilities $p(x,y) = \frac{1}{d^{2m}}$ although we expect the extension to arbitrary probabilities is straightforward.

Lemma 5. *The games NLC_d for arbitrary prime d have no quantum advantage, i.e. $\omega_c(NLC_d) = \omega_q(NLC_d)$.*

Work in progress includes an identification of more classes of d-output XOR games with no advantage as well as extending to non-prime d. A further question of current interest is to show a generalization of the norm bound to the class of all *linear* games using a generalization of the Fourier transform from cyclic to arbitrary finite groups. An open question for the future concerns the Shannon capacity of the orthogonality graphs corresponding to the d-output XOR games with no quantum advantage, to identify when these graphs can be categorized as class-1 graphs.

* Electronic address: ravishankar.r.10@gmail.com

[1] R. Ramanathan, A. Kay, G. Murta and P. Horodecki, arXiv: 1406.0995 (2014).
[2] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning and C. Monroe, Nature **464**, 1021 (2010).
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] A. Winter, Nature **466**, 1053 (2010).
[5] N. Linden, S. Popescu, A. J. Short and A. Winter, Phys. Rev. Lett. **99**, 180502 (2007).
[6] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter and M. Zukowski, Nature **461**, 1101 (2009).
[7] G. Brassard, H. Buhrman, N. Linden, A. A. Methot, A. Tapp and F. Unger, Phys. Rev. Lett. **96**, 250401 (2006).
[8] M. Navascúes and H. Wunderlich, Proc. Roy. Soc. Lond. A **466**: 881-890 (2009).
[9] A. Cabello, Phys. Rev. Lett. **110**, 060402 (2013).
[10] T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier and A. Acín, Nature Communications **4**, 2263 (2013).
[11] B. S. Cirelson, Lett. Math. Phys. **4**, 93 (1980).
[12] R. Cleve, P. Hoyer, B. Toner and J. Watrous, Proc. of the 19th IEEE Conf. on Comp. Complexity (CCC 2004), 236 (2004).
[13] S. Wehner, Phys. Rev. A **73**, 022110 (2006).
[14] A. Cabello, S. Severini and A. Winter, arXiv:1010.2163 (2010).
[15] A. Acín, T. Fritz, A. Leverrier and A. B. Sainz, arXiv: 1212.4084 (2012).
[16] A. Chailloux, L. Mančinska, G. Scarpa and S. Severini, arXiv:1404.3640 (2014).
[17] A. Cabello, S. Severini and A. Winter, Phys. Rev. Lett. **112**, 040401 (2014).
[18] C. E. Shannon, IRE Trans. Inform. Th. **2**, 8-19 (1956).
[19] L. Lovász, IEEE Trans. on Inform. Theory, IT-25 (1) (1979).
[20] C. Berge, "Perfect graphs", Six Papers on Graph Theory, Calcutta: Indian Statistical Institute 1 (1963).
[21] C. E. Larson, The 2nd Canadian Discrete and Algorithmic Mathematics Conference, CRM Montreal (2009); arXiv:0912.2260.
[22] D. König, Matematikai Lapok **38**: 116-119 (1931).
[23] E. Egerváry, Matematikai Lapok **38**: 16-28 (1931).
[24] *https://independencenumber.wordpress.com*.
[25] J. Kempe, O. Regev and B. Toner, arXiv: 0710.0655 (2007).
[26] M. Rosicka, *et al. In preparation*.
[27] An example matching is all pairs of vertices $(x, y, 0)$ and $(x, y, 1)$.