

ON MERMIN'S n -PLAYERS PARITY GAME

MICHEL BOYER

AUG 15, 2004

Abstract

An interesting problem solved in Mermin [1990], exhibiting a Bell inequality for n spin- $\frac{1}{2}$ entangled particles, corresponds to what is now called “pseudo-telepathy game” in the quantum information community. Those ideas were revisited recently by Broadbent [2004] and Brassard et al. [2003]. What follows is meant to be a (or yet another) unifying presentation of the relevant concepts. (Those are in fact my working notes before I wrote Boyer [2004]).

§ 1. Introduction: Mermin's parity game

Mermin [1990] proposes a “gedanken experiment” that establishes an exponential gap between expected values obtained in the quantum world and those obtainable in a local theory. That experiment can be viewed as a game between n players (whilst Mermin's “game” is played by n particles in Nature) that goes as follows: each player is given $x_j \in \{0, 1\}$ where x is promised to have a Hamming weight $|x|$ that is even i.e.

$$\sum_{j=1}^n x_j \equiv 0 \pmod{2} \quad (1)$$

Each player is asked to output $y_j \in \{0, 1\}$. The game is won if

$$\sum_{j=1}^n y_j \equiv \frac{1}{2} \sum_{j=1}^n x_j \pmod{2} \quad (2)$$

Condition (1) is a “promise” on the inputs given to the m players and (2) is the winning condition. It means that the parity of the output string y is equal to the parity of $\frac{1}{2} \sum_j x_j$. In fact Mermin's “game” is slightly different: the promise is that $|x|$ is odd and the game is won if the parity of $|y|$ is that of $(|x| - 1)/2$. This game is clearly equivalent to the one we have preferred to present here.

§ 2. The quantum strategy

The players share the state $|\Phi_n^+\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$. Remembering that

$$\begin{aligned} \sigma_1|0\rangle &= |1\rangle & \sigma_2|0\rangle &= i|1\rangle \\ \sigma_1|1\rangle &= |0\rangle & \sigma_2|1\rangle &= -i|0\rangle \end{aligned}$$

and denoting $\sigma_{1+x} = \otimes_j \sigma_{1+x_j}$ we readily obtain that if $|x| \equiv 2 \pmod{4}$ then $\sigma_{1+x}|\Phi_n^+\rangle = -|\Phi_n^+\rangle$ and if $|x| \equiv 0 \pmod{4}$ then $\sigma_{1+x}|\Phi_n^+\rangle = |\Phi_n^+\rangle$. Put differently

$$\sigma_{1+x}|\Phi_n^+\rangle = (-1)^{\frac{|x|}{2}} |\Phi_n^+\rangle \quad (3)$$

This means that if we measure σ_{1+x} on $|\Phi_n^+\rangle$ we get the parity of $\frac{|x|}{2}$. This measurement can be performed bitwise to get a bit y_j and the result of the measurement is the sum modulo 2 of the y_j . This is the physical algorithm.

In order to translate this into a quantum computer algorithm where measurements are performed in a standard basis (a result which was obtained independently by Broadbent [2004]; see Brassard et al. [2003] for a short account) we simply notice that:

$$\begin{aligned} \sigma_1 &= H\sigma_3H \\ \sigma_2 &= S\sigma_1S^\dagger = SH\sigma_3HS^\dagger \end{aligned}$$

Measuring σ_{1+x} on the state $|\Phi_n^+\rangle$ is thus measuring $\sigma_3^{\otimes n}$ i.e. parity on the state obtained from $|\Phi_n^+\rangle$ as follows

- (1) if $x_j = 0$, apply H on qubit j
- (2) if $x_j = 1$, apply HS^\dagger on qubit j

In all cases, player j applies $(S^\dagger)^{x_j}$, then H, and then measures σ_3 i.e. measures in the standard basis to get y_j . From (3)

$$|y| \equiv \frac{|x|}{2} \pmod{2}$$

In Brassard et al. [2003], S^{x_j} is applied by player j instead of $(S^\dagger)^{x_j}$, one reason being that the result was derived independently of Mermin's. In fact the state used by Mermin is not $|\Phi_n^+\rangle$ either, but $\frac{1}{2}(|0^n\rangle + i|1^n\rangle)$ and equality (3) is modified accordingly.

§ 3. A derived expectation

In the previous section, the n bits x_j could be generated equally likely by a quantum circuit (apply $H^{\otimes(n-1)}$ to $|0^{n-1}\rangle$) and then add a parity bit using an $n - 1$ bit

controlled \oplus so as to get an even string and then use the x_j to control S and S^\dagger . The output of the experiment is the parity of $|Y| + \frac{|X|}{2}$, or, equivalently

$$(-1)^{|Y| + \frac{|X|}{2}}$$

In the above experiment, the output is always 1 and so, the expectation or expected value of the measurements is 1. This is a value that is physically significant.

§ 4. Classical strategies

We first give a rough interpretation. In order to compare with the quantum strategy, Mermin essentially calculates the expectation¹

$$\left\langle (-1)^{|Y| + \frac{|X|}{2}} \right\rangle \quad (4)$$

of the random variable $(-1)^{|Y| + \frac{|X|}{2}}$ in the context where $X = (X_1, \dots, X_n)$ is an equally distributed multivariate random variable on strings of even parity in $\{0, 1\}^n$, $Y = (Y_1, \dots, Y_n)$ is a multivariate random variable such that the Y_j are $\{0, 1\}$ valued, independent and depend only on X_j and some shared random variable Λ . The random variable $(-1)^{|Y| + \frac{|X|}{2}}$ takes only two values, 1 and -1 ; it is 1 if the game is won and it is -1 if the game is lost. As a consequence

$$\left\langle (-1)^{|Y| + \frac{|X|}{2}} \right\rangle = P[\text{win}] - P[\text{lose}] = 2P[\text{win}] - 1$$

and

$$P[\text{win}] = \frac{1}{2} + \frac{1}{2} \left\langle (-1)^{|Y| + \frac{|X|}{2}} \right\rangle \quad (5)$$

so that bounding the expectation (4) is essentially nothing but bounding the probability of winning for any local random strategy with shared random value. This is a possible meaning that can be given to Mermin's formulas though, if we are more careful, we can get from them a more useful bound without any assumption on the distribution of X . The details follow.

§ 5. Mermin's bound

The assumption is that we are given random variables (X, Y, Λ) where Λ is shared by all players, $Y = (Y_j)$ is such that the Y_j are $\{0, 1\}$ valued and independent, Y_j

¹The expectation of a random variable Y is denoted $\langle Y \rangle$ or $E[Y]$; the notation $E[Y]$ allows conditional expectations $E[Y | x]$ and will thus be preferred in the next sections.

depending on X_j and the shared Λ . We make no assumption on X . This implies the $(-1)^{Y_j}$ are independent and

$$E[(-1)^{|Y|} | x, \lambda] = \prod_j E[(-1)^{|Y_j|} | x_j, \lambda] \quad (6)$$

For each Y_j we can write

$$E[(-1)^{Y_j} | x_j, \lambda] = P[y_j = 0 | x_j, \lambda] - P[y_j = 1 | x_j, \lambda] \quad (7)$$

and this value lies in the interval $[-1, 1]$ of the real line. Let us now consider

$$\prod_{i=1}^n \{E[(-1)^{Y_i} | x_i = 0, \lambda] + iE[(-1)^{Y_i} | x_i = 1, \lambda]\} \quad (8)$$

Using (6) this product is equal to

$$\sum_{x \in \{0, 1\}^n} i^{|x|} E[(-1)^{|Y|} | x, \lambda]$$

In the same way

$$\prod_{i=1}^n \{E[(-1)^{Y_i} | x_i = 0, \lambda] - iE[(-1)^{Y_i} | x_i = 1, \lambda]\} \quad (9)$$

is equal to

$$\sum_{x \in \{0, 1\}^n} (-i)^{|x|} E[(-1)^{|Y|} | x, \lambda]$$

and if we add (8) and (9) and then divide by 2, we get

$$\sum_{x \in P} (-1)^{|x|/2} E[(-1)^{|Y|} | x, \lambda] \quad (10)$$

where $P = \{x \in \{0, 1\}^n \text{ s.t. } |x| \text{ is even}\}$. This is the value that is effectively bound by Mermin. If we let Lose be the random variable that is 0 if there is a win and 1 if there is a lose, then

$$(-1)^{\text{Lose}} = (-1)^{|Y| + |X|/2}$$

and (10) is then equal to

$$\sum_{x \in P} E[(-1)^{\text{Lose}} | x, \lambda]$$

If we assume $P[X = x] = 2^{-n+1}$, i.e. that the inputs $x \in P$ are all equally likely, than this can be rewritten $2^{n-1} E[(-1)^{\text{Lose}} | \lambda]$ or $2^{n-1} E[(-1)^{|X|/2 + |Y|} | \lambda]$ but there is no need to make that assumption.

The sum (10) is equal by construction to the real part of (8) which is of the form $\prod_j (a_j + i b_j)$ with $a_j \in [-1, 1]$ and $b_j \in [-1, 1]$. We now bound the real value of such

products, this will provide a bound for (8). If n is even, the largest possible norm for $\prod_j (a_j + ib_j)$, which is $2^{n/2}$, can be obtained as the real part of the product by letting half the factors be $1 + i$ and the other half be $1 - i$ (indeed, $(1 + i)(1 - i) = 2 = \|1 + i\| \|1 - i\|$). If n is odd, the maximum real part is $2^{(n-1)/2}$ (the last factor cannot increase the real part) and so

$$\sum_{x \in \mathcal{P}} \mathbb{E} [(-1)^{\text{Lose}} | x, \lambda] \leq 2^{\lfloor n/2 \rfloor} \quad (11)$$

Now

$$\mathbb{E} [(-1)^{\text{Lose}} | x, \lambda] = \mathbb{P}[\text{win} | x, \lambda] - \mathbb{P}[\text{lose} | x, \lambda] = 2\mathbb{P}[\text{win} | x, \lambda] - 1$$

and so (11) is equivalent to

$$\frac{1}{|\mathcal{P}|} \sum_{x \in \mathcal{P}} \mathbb{P}[\text{win} | x, \lambda] \leq \frac{1}{2} + \frac{1}{2^{\lfloor n/2 \rfloor}} \quad (12)$$

for all λ and, in the particular case where X is uniformly distributed, gives a bound on $\mathbb{P}[\text{win} | \lambda]$ and thus on $\mathbb{P}[\text{win}]$. Of course, since (11) holds for all λ we also have

$$\frac{1}{|\mathcal{P}|} \sum_{x \in \mathcal{P}} \mathbb{P}[\text{win} | x] \leq \frac{1}{2} + \frac{1}{2^{\lfloor n/2 \rfloor}} \quad (13)$$

§ 6. Optimal strategies

One relevant question for pseudo-telepathy games is to find all the deterministic strategies for which the bound (12) is effectively reached. For each player j there are four possible deterministic strategies \mathcal{S}_j^s with $s \in \{0, 1, 2, 3\}$:

- (1) \mathcal{S}_j^0 : player j answers $y_j = 0$
- (2) \mathcal{S}_j^1 : player j answers $y_j = \bar{x}_j$
- (3) \mathcal{S}_j^2 : player j answers $y_j = 1$
- (4) \mathcal{S}_j^3 : player j answers $y_j = x_j$

Let us assume that player j uses strategy $\mathcal{S}_j^{s_j}$ and let $\mathcal{S} = (\mathcal{S}_j^{s_j})$ be their global strategy. If we let λ be $s = (s_j)_{1 \leq j \leq n}$, then using (7) and an appropriate polar representation of $\pm 1 \pm i$, we get

$$\mathbb{E} [(-1)^{Y_j} | x_j = 0, s] + i \mathbb{E} [(-1)^{Y_j} | x_j = 1, s] = \sqrt{2} e^{(2s_j+1)i\pi/4}$$

and consequently, product (8) which is equal to

$$\prod_{j=1}^n \{ \mathbb{E} [(-1)^{Y_j} | x_j = 0, s] + i \mathbb{E} [(-1)^{Y_j} | x_j = 1, s] \}$$

gives as a result

$$\sqrt{2}^n e^{i \sum_j (2s_j+1)\pi/4} \quad (14)$$

When n is even, this is exactly $2^{n/2}$ provided $\sum_j (2s_j + 1) \equiv 0 \pmod{8}$ which is equivalent to

$$\sum_j s_j \equiv -n/2 \pmod{4} \quad (15)$$

For n even, there are thus 4^{n-1} (optimal) strategies for which there is equality in (12). We can choose at will the values $s_j \in \{0, 1, 2, 3\}$ for players 1 to $n-1$ and s_n needs to be chosen so that the sum is $-n/2$ modulo 4. We then have, for any such s , denoting $\mathbb{P}_{\mathcal{S}^s}[\text{win}]$ for $\mathbb{P}[\text{win} | x, s]$,

$$\frac{1}{|\mathcal{P}|} \sum_{x \in \mathcal{P}} \mathbb{P}_{\mathcal{S}^s}[\text{win} | x] = \frac{1}{2} + \frac{1}{2^{\lfloor n/2 \rfloor}}$$

When n is odd, (14) cannot be real and the largest real part is obtained when the resulting complex number has a phase of $\pi/4$ or $-\pi/4$ (and of course a norm of $\sqrt{2}^n$). Projecting on the real axis leaves a value of $2^{\lfloor n/2 \rfloor}$ and the condition to be met by the s_j is $\sum_j (2s_j + 1) \equiv \pm 1 \pmod{8}$ which can be written

$$\sum_j s_j \equiv \frac{-n \pm 1}{2} \pmod{4} \quad (16)$$

We can choose at will the $n-1$ first strategies in $\{0, 1, 2, 3\}$ and there are two possible choices for s_n giving a total of $2 \times 4^{n-1}$ strategies that are optimal when n is odd.

§ 7. An optimal probabilistic strategy

Mermin's argument allows bounding the average of $\mathbb{P}[\text{win} | x]$ for all even strings x . If the adversary decides not to send those strings with equal probability, then we may want to know the largest value

$$\min_x \mathbb{P}_{\mathcal{S}}[\text{win} | x] \quad (17)$$

can take for all possible strategies \mathcal{S} . Clearly, (17) cannot be larger than the average of the values $\mathbb{P}_{\mathcal{S}}[\text{win} | x]$ can take and so, for all strategies \mathcal{S} ,

$$\min_x \mathbb{P}_{\mathcal{S}}[\text{win} | x] \leq \frac{1}{2} + \frac{1}{2^{\lfloor n/2 \rfloor}}$$

By strategy is meant in principle any algorithm, deterministic or not, possibly using some shared random generator. This corresponds to the most general situation Mermin analyses, the common random generator corresponding to Λ . However, we can put the random generators of all players in Λ and we will consequently consider only situations where the strategy is deterministic for all λ .

Proposition 7.1 (Broadbent [2004]) *Let \mathcal{S} be the strategy where the players share $\lambda = s$ randomly generated in the set of sequences $s \in [0..3]^n$ satisfying satisfying (15) or (16) and, knowing s , apply the strategy \mathcal{S}^s . Then*

$$\min_x P_{\mathcal{S}}[\text{win} \mid x] = \frac{1}{2} + \frac{1}{2^{\lceil n/2 \rceil}}$$

This is of course equivalent to saying that $P_{\mathcal{S}}[\text{win} \mid x] = \frac{1}{2} + \frac{1}{2^{\lceil n/2 \rceil}}$ for all $x \in \mathcal{P}$. Here is a proof using a different approach than Broadbent's.

Proof. For any optimal strategy defined by s , let $P[\text{win} \mid x, s]$ be the probability of winning if the input is x and the optimal strategy chosen is \mathcal{S}^s . By definition,

$$2^{1-n} \sum_x P[\text{win} \mid x, s] = \frac{1}{2} + \frac{1}{2^{\lceil n/2 \rceil}}$$

and, for the strategy where the s are identically distributed amongst optimal s

$$2^{1-n} \sum_x P[\text{win} \mid x] = \frac{1}{2} + \frac{1}{2^{\lceil n/2 \rceil}}$$

In order to show that $P[\text{win} \mid x] = \frac{1}{2} + \frac{1}{2^{\lceil n/2 \rceil}}$ we need only show that $P[\text{win} \mid x]$ is independent of x i.e.

$$P[(-1)^{|X|/2+|Y|} = 1 \mid x]$$

is independent of x (so that the average is equal to the minimum). This is equivalent to showing that

$$E[(-1)^{|X|/2+|Y|} \mid x]$$

does not depend on x . It suffices to show that if we take two bits that are 1 in x and replace them by 0, then this expectation is left unchanged. We may assume these two bits to be the first ones in x and we thus need only show that

$$E[(-1)^{|Y|} \mid 11x'] = -E[(-1)^{|Y|} \mid 00x']$$

Since all the strategies are equally likely, this is equivalent to showing that

$$\sum_s E[(-1)^{|Y|} \mid 11x', s] = -\sum_s E[(-1)^{|Y|} \mid 00x', s] \quad (18)$$

Since the conditions (15) or (16) for optimality if n is even or odd is on $\sum_j s_j$ modulo 4, we can sum (18) by keeping $s_1 + s_2$ fixed modulo 4 (for each value this sum is allowed to take); we will do so with all the other s_j fixed for $3 \leq j \leq n$: more precisely, let us compare for $b = 0$ and $b = 1$ the value for each $a \in [0..3]$ of

$$\sum_{s_1+s_2 \equiv a \pmod{4}} (-1)^{y_1(b,s_1)+y_2(b,s_2)+y'(x',s')} \quad (19)$$

for some x' and s' fixed for $3 \leq j \leq n$ and the corresponding uniquely defined string $y'(x', s')$ (of length $n-2$). In this notation, $y_j(b, 0) = 0$, $y_j(b, 1) = \bar{b}$, $y_j(b, 2) = 1$, $y_j(b, 3) = b$. It is an easy exercise (might be good for homework) to check that for $a = 0$ and $a = 2$, (19) is 0. For $a = 1$ and $a = 3$, sum (19) for $b = 1$ is equal to the negative of (19) for $b = 0$. Consequently, in all cases (including 0 sums), the sign of (19) is changed when b is flipped. This proves (18) and the theorem. \square

§ 8. Conclusion

Mermin's parity game provides a nice example where the optimal proportion of winning inputs as well as the probability of winning on worst inputs can be precisely characterised. The use of expectations gives an elegant and short proof of the upper bound.

As for the optimality of the probabilistic strategy, it seems to depart sensibly from Mermin's 1990 preoccupations and the result (but not the above proof) belongs to Broadbent [2004]. This proposition shows that there is effectively a classical strategy that wins with a probability equal to the optimum and, in particular, with a probability larger than 1/2 on all inputs. This means that the quantum strategy wins with a probability that is not even twice that of a well chosen classical strategy.

Another reading of Mermin's article can be found in Brassard et al. [2004] where the above proposition is also proved.

References

- Michel Boyer. Extended GHZ n -player games with classical probability of winning tending to 0, 2004. URL <http://arxiv.org/abs/quant-ph/0408090>.
- Gilles Brassard, Anne Broadbent, and Alain Tapp. Multi-party pseudo-telepathy. In F. Dehne, J. R. Sack, and M. Smid, editors, *Proceedings of the 8th International Workshop on Algorithms and Data Structures*, volume 2748 of *Lecture Notes in Computer Sciences*, pages 1–11, 2003. URL <http://arxiv.org/abs/quant-ph/0306042>.
- Gilles Brassard, Anne Broadbent, and Alain Tapp. Recasting mermin's multi-player game into the framework of pseudo-telepathy, 2004. URL <http://arxiv.org/abs/quant-ph/0408052>.
- Anne Lise Broadbent. Quantum pseudo-telepathy games. Master's thesis, DIRO, Université de Montréal, 2004.
- David N. Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, 65(15):1838–1840, 1990.