Power Round

CHMMC 2016

November 20, 2016

1 The Magic Square Game (24 pts)

Alice and Bob tell their friend Eve that they have a magic 3×3 square of numbers with the following properties:

- Every entry is either 1 or -1
- The product of each column is 1
- The product of each row is -1.

Problem 1.1. (5 pts) Exhibit such a square or prove that none exists.

Solution 1. Consider the product of all 9 numbers. Since the product of each row is -1 and there are three rows, the product of the whole square must be -1. Since the product of each column is 1, the product of the whole square must be 1. Therefore, the square doesn't exist.

Eve refuses to believe her friends, and they refuse to show their square to Eve. To resolve the dispute, they have the idea to play the following game.

Definition 1.1 (Magic Square Game)**.**

1. Eve randomly generates two numbers $x, y \in \{0, 1, 2\}$ independently and uniformly at random. She gives x to Alice and y to Bob.
2. Without communicating, Alice and Bob each produce a triple of ± 1 numbers (a_0, a_1, a_2) and (b_0, b_1, b_2).
3. Eve checks that $a_0 a_1 a_2 = 1$, $b_0 b_1 b_2 = -1$.
4. Eve checks that $a_y = b_x$.

Alice and Bob win if they pass both of Eve's checks. They lose if they fail either of them.

Problem 1.2. (6 pts) Alice, Bob, and Eve play three instances of the game. In each instance, decide whether Alice and Bob win or lose the game. Either show that they fail one of the checks or that they pass both.

1. Eve asks $x = 0$, $y = 1$. Alice answers $a = (1, 1, 1)$, while Bob answers $b = (-1, -1, -1)$.

2. Eve asks $x = 1$, $y = 0$. Alice answers $a = (1, -1, -1)$, while Bob answers $b = (-1, 1, -1)$.

3. Eve asks $x = 2$, $y = 2$. Alice answers $a = (1, -1, -1)$, while Bob answers $b = (1, 1, -1)$.

Solution 2.

1. They fail since Alice and Bob disagree: $a_y = 1 \neq -1 = b_x$.

2. They fail since Bob's row does not have a product of -1: $b_0 b_1 b_2 = 1$.

3. They pass both conditions: Alice's column has a product of 1, Bob's row has a product of -1, and we have $a_2 = -1 = b_2$.

Problem 1.3. (8 pts) Give a deterministic strategy that wins with probability $\frac{8}{9}$.

Solution 3. Alice uses the matrix

$$A = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix};$$

Box uses the matrix

$$B = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 1 & -1 \\ 1 & 1 & -1 \end{pmatrix}.$$

When Alice is asked question x, she responds with the x^{th} column of A. Likewise, when Bob is asked question y, he responds with the y^{th} row of B. They fail only on the question $x = 2, y = 2$.

Problem 1.4. (5 pts) Suppose for the sake of this problem that a square of numbers

$$\begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{10} & m_{11} & m_{12} \\ m_{20} & m_{21} & m_{22} \end{pmatrix}$$

satisfying the conditions of problem 1.1 does exist (regardless of your answer to problem 1.1), and that Alice and Bob have access to this square. Show how they can use this square to make a winning strategy in Eve's game.

Solution 4. *(Note: If you pointed out that the premise was false, you received full credit.)* Alice should respond with a column of the magic square $a = (m_{0x}, m_{1x}, m_{2x})$ and Bob should respond with a row of the magic square $b = (m_{y0}, m_{y1}, m_{y2})$. Then we'll have $a_y = m_{yx} = b_x$ and the product of Alice's answer is 1 while the product of Bob's answer is -1.

Eve is happy because she thinks that if they play this game many times and Alice and Bob always win, then they must have the square. Alice and Bob are happy because they only have to reveal part of their square at a time. In order to avoid letting Eve learn the square, they can change which square they use each time they play the game. In section 3, you'll see that in a classical theory of physics, Eve's intuition is correct. In section 2, you'll see that with quantum mechanics, Alice and Bob can fool Eve.

2 A Quantum Strategy for the Magic Square Game (49 pts)

Now we'll show that if we allow Alice and Bob to take advantage of quantum mechanical phenomena, they have a winning strategy for the Magic Square game. First, we'll need some properties of the *Pauli group*.

2.1 The Pauli Group

Definition 2.1. The Pauli group on one qubit (which we'll now denote by $\mathcal{P}_1$) is a multiplicative structure consisting of the four Pauli operators I, X, Y, Z together with multiplicative constants $1, -1, i, -i$. Explicitly, the sixten elements of the Pauli group are

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} \tag{1}$$

We say that elements A and B *commute* if $AB = BA$. We say they *anti-commute* if $AB = -BA$.

The Pauli group obeys the following relations:

- The Pauli group is *closed under multiplication*, i.e. every product of two Pauli operators is a Pauli operator times a constant.
- Multiplication is associative. That is, $(AB)C = A(BC)$ for any $A, B, C \in \mathcal{P}_1$. We'll write ABC without ambiguity.
- I is the identity element. In other words, if A is any element of $\mathcal{P}_1$, then $IA = AI = A$.
- $X^2 = Y^2 = Z^2 = I$.
- $XYZ = -iI$.
- The multiplicative constants $\pm 1, \pm i$ act like they do in the complex numbers, i.e. $i^2 = -1$ and $(-1)^2 = 1$.
- The multiplicative constants commute with everything. (More formally, we should say that $\pm I$ and $\pm iI$ commute with everything.)

Problem 2.1. (9 pts) Prove that X, Y, and Z are *pairwise anti-commuting*. That is, for every pair $A, B \in \{X, Y, Z\}$ with $A \neq B$, we have $AB = -BA$.

Solution 5. Start from $XYZ = -iI$. First, multiply on the left first by X and then by Y. This results in the equation $Z = -iYX$. Starting again from $XYZ = -iI$, multiply on the right by iZ. This results in the equation $iXY = Z$. Thus we conclude $iXY = -iYX$; multiplying by i yields that X and Y anticommute.

We can use this to show more easily that Z anticommutes with X and Y:

$$\begin{aligned} YZ &= Y(iXY) = iY(XY) = -iY(YX) = -iY^2X \\ &= -iXY^2 = -(iXY)Y = -ZY. \end{aligned} \tag{2}$$

In the fifth equality, we used that $Y^2 = I$ commutes with everything. Similarly,

$$XZ = X(iXY) = iX(XY) = -iX(YX) = -(iXY)X = -ZX. \tag{3}$$

Remark 2.2. There are four 2×2 matrices over the complex numbers that obey the same relations as the I, X, Y, Z given here. You are *not* asked to find them.

Definition 2.3. The *Pauli group on two qubits*, denoted $\mathcal{P}_2$, consists of pairs of elements from the Pauli group on one element, together with multiplicative constants $\{1, i, -1, -i\}$. We think of the first part of the pair as being a Pauli operator acting on the first qubit and and the second as being a Pauli operator acting on the second qubit. We write the pair using the tensor product notation $\otimes$. Explicitly, every element of the Pauli group can be written like $cA \otimes B$, where A and B are Pauli operators and $c \in \{\pm 1, \pm i\}$, because multiplication obeys the following relations:

$$(i^n A) \otimes (i^m B) = i^{n+m}(A \otimes B); \quad (i^n A \otimes B)(i^m C \otimes D) = i^{n+m}(AC \otimes BD). \tag{4}$$

Some typical elements of $\mathcal{P}_2$ are $X \otimes X$, $-iI \otimes Z$, and $Y \otimes Z$. (Note that the notation $-iI \otimes Z$ is well-defined by the first equation above.)

Problem 2.2. (22 pts)

a) Show that $X \otimes X$ commutes with $Z \otimes Z$.

b) Compute the product $(X \otimes X)(Y \otimes Z)(Z \otimes Y)$ as a tensor of two one-qubit Pauli operators, possibly with a multiplicative constant.

c) Of the 16 two-qubit Pauli operators of the form $U \otimes V$, where $U, V \in \{I, X, Y, Z\}$, how many commute with $X \otimes X$? How many anticommute? Give proof for your answer.

Solution 6. a) We use the fact that X and Z anti-commute to compute

$$\begin{aligned} (X \otimes X)(Z \otimes Z) &= (XZ \otimes XZ) = (-ZX \otimes -ZX) \\ &= (-1)^2(ZX \otimes ZX) = (Z \otimes Z)(X \otimes X). \end{aligned} \tag{5}$$

b) First, we note that $XZY = -XYZ = iI$ by the anticommutation of Z and Y. Next, we compute

$$\begin{aligned} (X \otimes X)(Y \otimes Z)(Z \otimes Y) &= (XYZ \otimes XZY) = (-iI \otimes iI) \\ &= -i^2 I \otimes I = I \otimes I. \end{aligned} \tag{6}$$

c) First, notice that every one-qubit Pauli operator either commutes with X (X and I do) or anticommute with X (Y and Z do). It follows that an operator $A \otimes B$ commutes with $X \otimes X$ iff either A and B both commute with X or A and B both anticommute with X. In particular, notice that every two-qubit Pauli operator either commutes or anticommutes with $X \otimes X$.

There are $2^2 = 4$ operators with both tensor factors commuting with X ($I \otimes I, I \otimes X, X \otimes I, X \otimes X$) and $2^2 = 4$ with both tensor factors anticommuting with X ($Y \otimes Y, Y \otimes Z, Z \otimes Y, Z \otimes Z$).

The other 8 operators have exactly one tensor factor commuting and one tensor factor anticommuting. We conclude that 8 of the two qubit operators commute with $X \otimes X$ and 8 of them anticommute.

Problem 2.3. (13 pts) Find, with proof, a 3×3 square of two-qubit Pauli operators such that:

- In each row, the three operators pairwise commute and their product is $-I \otimes I$.
- In each column, the three operators pairwise commute and their product is $I \otimes I$.

(Hint: There is such a square with the property that every single-qubit operator (including I) appears at least once. You may need to include -1 coefficients.)

Solution 7. One such square is

$$\begin{pmatrix} -I \otimes Z & X \otimes I & X \otimes Z \\ -Z \otimes I & I \otimes X & Z \otimes X \\ Z \otimes Z & X \otimes X & Y \otimes Y \end{pmatrix}. \tag{7}$$

The column products are

$$\begin{aligned} (-I \otimes Z)(-Z \otimes I)(Z \otimes Z) &= ZZ \otimes ZZ = I \otimes I \\ (X \otimes I)(I \otimes X)(X \otimes X) &= XX \otimes XX = I \otimes I \\ (X \otimes Z)(Z \otimes X)(Y \otimes Y) &= I \otimes I, \end{aligned}$$

where the last equality is proved just as part 2 of problem 2.2. The row products are

$$\begin{aligned} (-I \otimes Z)(X \otimes I)(X \otimes Z) &= -XX \otimes ZZ = -I \otimes I \\ (-Z \otimes I)(I \otimes X)(Z \otimes X) &= -ZZ \otimes XX = -I \otimes I \\ (Z \otimes Z)(X \otimes X)(Y \otimes Y) &= ZXY \otimes ZXY = (-i)^2 I \otimes I = -I \otimes I. \end{aligned}$$

The commutation relations can be checked with the observations from the last part of the previous problem.

Another such square is

$$\begin{pmatrix} X \otimes X & Y \otimes Z & Z \otimes Y \\ Y \otimes Y & Z \otimes X & X \otimes Z \\ Z \otimes Z & X \otimes Y & Y \otimes X \end{pmatrix}. \tag{8}$$

Problem 2.4. (5 pts) Why doesn't your proof from Problem 1.1 apply to the square you found in Problem 2.3?

Solution 8. Because the nine operators do not pairwise commute, multiplying them by rows and multiplying them by columns need not give the same answer.

Theorem 2.4. *If Alice and Bob have access to quantum-mechanical devices, they can use the magic square found in Problem 2.3 to win the Magic Square Game with certainty.*

(A treatment of this theorem can be found at `https://pdfs.semanticscholar.org/33bf/805817648a88f06707dde3e627bfdd74945a.pdf`)

3 A Bell Inequality (27 pts)

First, we need to formalize the notion of a game. Let $X = Y = \{0, 1, 2\}$ and let

$$\begin{aligned} A = B = \{&(+1, +1, +1), (+1, +1, -1), (+1, -1, +1),\\ &(+1, -1, -1), (-1, +1, +1), (-1, +1, -1), (-1, -1, +1), (-1, -1, -1)\}. \end{aligned} \tag{9}$$

We'll think of X and Y as sets of questions by Eve and A and B as the set of valid answers by Alice and Bob.

Definition 3.1. A *strategy* for Alice and Bob is a function $p : A \times B \times X \times Y \to [0, 1]$ such that for each fixed x, y, $\sum_{ab} p(a, b\|x, y) = 1$.

If Eve asks question x to Alice and question y to Bob, then the probability that Alice produces answer a while Bob produces answer b is $p(a, b\|x, y)$. (The symbol $\|$ should be read as "given" or "conditioned on".) Let $V : A \times B \times X \times Y \to \{0, 1\}$ be the *valuation* for the game, i.e. the function that tells whether Alice and Bob win the game. That is,

$$V(a, b, x, y) = \begin{cases} 1, & \text{if } a_y = b_x,\ a_0a_1a_2 = 1, \text{ and } b_0b_1b_2 = -1 \\ 0, & \text{otherwise} \end{cases} \tag{10}$$

Problem 3.1. (12 pts) Show that the probability that Alice and Bob win the game is given by

$$\omega(p) := \frac{1}{9} \sum_{\substack{a\in A, b\in B\\ x\in X, y\in Y}} p(a, b\|x, y)V(a, b, x, y). \tag{11}$$

(Remember that Eve picks x and y independently and uniformly at random.)

Solution 9. Suppose Eve asks fixed questions x and y to Alice and Bob. Then the probability that they win is the probability that they give answers a and b such that $V(a, b, x, y) = 1$. In other words, their win probability is

$$\omega(p \mid xy) = \sum_{\substack{a,b:\\ V(a,b,x,y)=1}} p(a, b\|x, y). \tag{12}$$

We can rewrite this as

$$\omega(p \mid xy) = \sum_{\substack{a,b:\\ V(a,b,x,y)=1}} p(a, b\|x, y) + \sum_{\substack{a,b:\\ V(a,b,x,y)=0}} 0, \tag{13}$$

which is then equal to

$$\omega(p \mid xy) = \sum_{a,b} p(a, b\|x, y)V(a, b, x, y). \tag{14}$$

Since each pair (x, y) is asked with equal probability, we have that $\omega(p)$ is the average of the $\omega(p \mid x, y)$. This recovers equation (5).

Definition 3.2. A strategy is *local* if it decomposes as a product of one strategy for Alice and one strategy for Bob. Explicitly, p is local if there exist $p_A : A \times X \to [0,1]$ and $p_B : B \times Y \to [0,1]$ such that

$$p(a, b \| x, y) = p_A(a, x) \cdot p_B(b, y). \tag{15}$$

A strategy is *classical* if it is a convex combination of local strategies. Explicitly, p is classical if there exist local strategies $p_1, \ldots, p_n$ and nonnegative real numbers $c_1 \ldots c_n$ such that $\sum_{i=1}^n c_i = 1$ and such that for all a, b, x, y,

$$p(a, b \| x, y) = \sum_{i=1}^{n} c_i p_i(a, b \| x, y). \tag{16}$$

Intuitively, we say that a strategy is classical if Alice and Bob can implement it by making use of classically correlated[1] random variables. For example, they might both look at the weather reports for Pasadena and choose to make their first bits equal to 0 if it's sunny, or make them equal to 1 if it's *extra* sunny.

Problem 3.2. (15 pts) Prove that no classical strategy achieves a win probability strictly greater than $\frac{8}{9}$. In other words, assuming that p is classical, prove the following *Bell inequality:* $\omega(p) \leq \frac{8}{9}$, where ω is as defined in equation (5).

Solution 10. Any deterministic strategy is of the following form: Alice has a matrix A which she pulls a row from and Bob has a matrix B which he pulls a column from. The consistency condition $a_y = b_x$ forces that if Alice and Bob always win, then $A = B$. But then this matrix cannot satisfy all of the row product and column product conditions, as we proved in problem 1.1, so there must be some x and y such that Alice and Bob lose. Thus Alice and Bob win with probability at most $\frac{8}{9}$.

Next, note that any local strategy is of the following form: with some probabilities $q_1, \ldots, q_k$ summing to 1, Alice plays the corresponding deterministic strategy $A_1, \ldots, A_k$, and with some probabilites $s_1, \ldots, s_l$ summing to 1, Bob plays the corresponding deterministic strategy $B_1, \ldots, B_l$. These probabilites are independent between Alice and Bob, so for $1 \leq i \leq k$, $1 \leq j \leq l$, we see that with probability $q_i s_j$, Alice and Bob play the deterministic strategy (A_i, B_j). But by the above paragraph, in any such strategy, Alice and Bob win with probability at most $\frac{8}{9}$ as x and y vary, so the local strategy wins with probability at most $\frac{8}{9}$ as well.

Now we will make use of convexity to bound the probability of a general classical strategy. Let p be a general classical strategy. Then $p = \sum c_i p_i$ where

[1]Here, *classically correlated* means something like "obeying a naïve interpretation of physics widely regarded as an accurate model of the real world before the discovery of quantum mechanics in the 1930s." For more precise definitions and theorems, see Bell's seminal paper.

the p_i are local strategies. Then we have

$$\begin{aligned}
\omega(p) &= \frac{1}{9} \sum_{\substack{a\in A, b\in B \\ x\in X, y\in Y}} p(a,b\|x,y)V(a,b,x,y) \\
&= \frac{1}{9} \sum_{\substack{a\in A, b\in B \\ x\in X, y\in Y}} \sum_{i=1}^{n} c_i p_i(a,b\|x,y)V(a,b,x,y) \\
&= \sum_{i=1}^{n} c_i \left(\frac{1}{9} \sum_{\substack{a\in A, b\in B \\ x\in X, y\in Y}} p_i(a,b\|x,y)V(a,b,x,y) \right) \\
&= \sum_{i=1}^{n} c_i \omega(p_i) \\
&\le \frac{8}{9} \sum_{i=1}^{n} c_i = \frac{8}{9}.
\end{aligned}$$