Scientific Research

Quantum Number Tricks

Takashi Mihara

Department of Information Sciences and Arts, Toyo University, Kawagoe, Japan.
Email: mihara@toyonet.toyo.ac.jp

ABSTRACT

Some results indicate that quantum information based on quantum physics is more powerful than classical one. In this paper, we propose new tricks based on quantum physics. Our tricks are methods inspired by the strategies of quantum game theory. In these tricks, magicians have the ability of quantum physics, but spectators have only classical one. We propose quantum tricks such that, by manipulating quantum coins and quantum cards, magicians guess spectators' values.

1. Introduction

The studies on *quantum information* have succeeded in such as quantum computation, quantum cryptography, quantum communication complexity, and so on. For example, Shor's quantum factoring algorithm is one of representative results in these fields [1]. In addition, quantum game theory has been also proposed and it has been shown that quantum game theory is more powerful than classical one.

In 1998, for a coin flipping game, Meyer proposed a quantum strategy for the first time and showed that the quantum strategy has an advantage over classical ones [2]. Moreover, he also showed the importance of a relationship between quantum game theory and quantum algorithms.

After that, other types of quantum strategies have been also proposed. For example, Eisert *et al.* proposed a quantum strategy with entangled states for a famous two-player game called the *Prisoner's Dilemma* [3] (also see Du *et al.* [4,5], Eisert and Wilkens [6], and Iqbal and Toor [7]). For another famous two-player game called the *Battle of the Sexes*, Marinatto *et al.* also proposed a quantum strategy with entangled states [8]. For these games, they showed quantum Nash equilibriums different from classical ones.

In this paper, we propose quantum tricks based on methods inspired by the strategies of quantum game theory. Magicians have the ability of quantum physics, but spectators have only classical one. By manipulating quantum coins and quantum cards, magicians guess spectators' values. For example, we propose tricks such that by using entangled states, a magician transmits a spectator's value to another magician without communicating between them.

The remainder of this paper has the following organization. In Section 2, we define notations and basic operations used in this paper. In Section 3, we propose quantum coin tricks. In Section 4, we propose quantum card tricks. Finally, in Section 5, we provide some concluding remarks.

2. Preliminaries

First, we denote some basic notations. Let $\mathbf{B} = \{0,1\}$, $\mathbf{Z}_n = \{0,1,...,n-1\}$, and $\mathbf{Z}_n^+ = \{1,2,...,n-1\}$ for a positive integer n. Let a and b be integers. We say that a is congruent to b to modulus n if n is a divisor of $a-b$ and denote by $a \equiv b \pmod n$, and we denote an inner product modulo 2 of a and b by $a \cdot b$. Finally, let $\oplus$ be an exclusive-OR operator, e.g., $(1,1,0,0) \oplus (1,0,1,0) = (0,1,1,0)$.

Next, we define some basic quantum notations. As states of *qubit*, let $|0\rangle = (1 \quad 0)^T$ and $|1\rangle = (0 \quad 1)^T$, where $|\cdot\rangle$ is Dirac notation and A^T is the transposed matrix of matrix A. Throughout this paper, we take $\mathbf{B}_q = \{|0\rangle, |1\rangle\}$ as a computational basis and a measurement basis. Moreover, we denote an n-qubit basis state by $|b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle = |b_1\rangle |b_2\rangle \cdots |b_n\rangle = |b_1, b_2, ..., b_n\rangle$, where $\otimes$ is a tensor product and $|b_i\rangle \in \mathbf{B}_q$ ($i = 1,2,...,n$). In addition, we denote a basis in an N-dimensional system,

a basis of *qudit* states, by $\mathbf{Z}_{N_q} = \left\{ |x\rangle \mid x \in \mathbf{Z}_N \right\}$, where $N\,(\geq 2\,)$ is an integer. We call $|x\rangle$ a *quantum register*.

Finally, we define some unitary matrices used for quantum tricks in this paper. Let I be the 2×2 identity matrix. This operation means no operation. A *Walsh-Hadamard* operation H is

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$(\,H\,|0\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)\,)$

and

$H\,|1\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)\,)$.

Note that $H = H^{-1}$. This operation is used when we make a superposition of states. An operation used when a coin is flipped is X,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$(\,X\,|0\rangle = |1\rangle$ and $X\,|1\rangle = |0\rangle\,)$.

Moreover, we define an operation between two qubits. A *Controlled Not* gate, *CNOT*, is

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$(\,CNOT\,|c,t\rangle = |c, t\oplus c\rangle$, where the first bit c is the controlled bit and the second bit t is the target bit). We denote the operation by $CNOT_{(ij)}$ when the i-th bit is the controlled bit and the j-th bit is the target bit.

Entangled states can be made by using H and $CNOT$. For example,

$$|0\rangle\,|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle$$
$$\xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle).$$

Finally, we define two matrices for N-state transition. Let $x \in \mathbf{Z}_N$. A *quantum Fourier transform* [1], *QFT*, is

$$QFT\,|x\rangle = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{i2\pi xy/N}\,|y\rangle,$$

and

$$QFT^{-1}\,|y\rangle = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{-i2\pi xy/N}\,|x\rangle.$$

3. Quantum Coin Tricks

In this section, we show some quantum coin tricks using quantum states. Throughout this paper, we use Alice and

Bob as names of magicians, and use Carol and Davis as names of spectators participating in a magic show. Moreover, Alice and Bob can cooperate but cannot communicate with each other during each show.

First, we show a simple coin trick using a two-qubit entangled state.

Coincidence: First, Alice prepares one coin and put it in a box. The box is a container such that no one cannot see the state of the coin but can operate it. Next, Carol flips the coin or not. Then, Bob guesses the state of the coin, *i.e.*, either head (H) or tail (T).

Method of Coincidence

We denote H and T by $|0\rangle$ and $|1\rangle$, respectively.

1) Beforehand, Alice and Bob share an entangled state

$$\frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle),$$

where Alice has the first qubit and Bob has the second qubit. Alice's qubit is in a box.

2) Carol flips Alice's coin or not. This means that Carol applies X to Alice's qubit if she wants to flip the coin; otherwise she applies I to it. Then, if she flips it, the state becomes

$$\frac{1}{\sqrt{2}}(|1\rangle\,|0\rangle + |0\rangle\,|1\rangle).$$

3) Alice and Bob apply H to the state. Then it becomes

$$\frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle - |1\rangle\,|1\rangle)$$

if Carol flipped the coin; otherwise the state does not change, *i.e.*,

$$\frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle).$$

4) Bob measures his qubit and announces the value(H or T) to Carol.

5) Carol opens the box and confirms that her value is same as Bob's value.

This trick can be easily extended to multiple coins by preparing the entangled states $(1/\sqrt{2})(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle)$ corresponding to the number of coins.

Next, we show a trick guessing the number of Carol flipping coins.

Flip-Flop1: First, Alice prepares k coins in all the coins being head. Next, Carol flips some coins such that the state of coins is $m \in \mathbf{B}^k$. Alice flips some coins. Carol flips some coins. Alice flips some coins. Then, Carol finds that the state of final coins is *m*.

Method of Flip-Flop1

1) Alice prepares a state $|0^k\rangle$ (all the coins are head), exhibits it to Carol, and puts it in a box.

2) Carol flips some coins and the state becomes $|m\rangle$.

3) Alice applies $H^{\otimes k}$ to it and the state becomes

$$\frac{1}{\sqrt{2^k}}\sum_{x=0}^{2^k-1}(-1)^{m\cdot x}|x\rangle.$$

4) Carol flips some coins and the state becomes

$$\frac{1}{\sqrt{2^k}}\sum_{x=0}^{2^k-1}(-1)^{m\cdot x}|x\oplus r\rangle,$$

where $r\in\mathbf{B}^k$.

5) Alice applies $H^{\otimes k}$ to it and the state becomes

$$\frac{1}{\sqrt{2^{2k}}}\sum_{y=0}^{2^k-1}\sum_{x=0}^{2^k-1}(-1)^{m\cdot x}(-1)^{(x\oplus r)\cdot y}|y\rangle$$

$$=\frac{1}{\sqrt{2^{2k}}}\sum_{y=0}^{2^k-1}(-1)^{r\cdot y}\sum_{x=0}^{2^k-1}(-1)^{(m\oplus y)\cdot x}|y\rangle$$

$$=(-1)^{r\cdot m}|m\rangle.$$

6) Carol opens the box and confirms m.

Finally, we show a trick modifying **Flip-Flop1**.

Flip-Flop2: First, Alice prepares k coins in all the coins being head. Next, Carol flips some coins such that the state of coins is $m_1\in\mathbf{B}^k$. Alice flips some coins. Carol flips some coins such that the added state of coins is $m_2\in\mathbf{B}^k$. Alice flips some coins. Carol flips some coins. Alice flips some coins. Then, Alice guesses the value of m_1 if Carol announces the value of m_2; otherwise, Alice guesses the value of m_2 if Carol announces the value of m_1.

Method of Flip-Flop2

1) Alice prepares a state $|0^k\rangle$, exhibits it to Carol, and puts it in a box.

2) Carol flips some coins and the state becomes $|m_1\rangle$.

3) Alice does not flip them in her turn.

4) Carol flips some coins and the state becomes $|m_1\oplus m_2\rangle$.

5) Alice applies $H^{\otimes k}$ to it and the state becomes

$$\frac{1}{\sqrt{2^k}}\sum_{x=0}^{2^k-1}(-1)^{(m_1\oplus m_2)\cdot x}|x\rangle.$$

6) Carol flips some coins and the state becomes

$$\frac{1}{\sqrt{2^k}}\sum_{x=0}^{2^k-1}(-1)^{(m_1\oplus m_2)\cdot x}|x\oplus r\rangle,$$

where $r\in\mathbf{B}^k$.

7) Alice applies $H^{\otimes k}$ to it and the state becomes

$$\frac{1}{\sqrt{2^{2k}}}\sum_{y=0}^{2^k-1}\sum_{x=0}^{2^k-1}(-1)^{(m_1\oplus m_2)\cdot x}(-1)^{(x\oplus r)\cdot y}|y\rangle$$

$$=\frac{1}{\sqrt{2^{2k}}}\sum_{y=0}^{2^k-1}(-1)^{r\cdot y}\sum_{x=0}^{2^k-1}(-1)^{(m_1\oplus m_2\oplus y)\cdot x}|y\rangle$$

$$=(-1)^{r\cdot y}|m_1\oplus m_2\rangle.$$

Then, Alice measures it and obtains $m_1\oplus m_2$.

8) Carol announces either m_1 or m_2. Then, Alice guesses m_2 if Carol announced m_1; otherwise she guesses m_1.

Let k be the number of coins. Then, the complexity of these methods mentioned in this section is in $O(k)$ time because each operation of X, H, and $CNOT$ can be executed in $O(1)$ time.

4. Quantum Card Tricks

In this section, we show some quantum card tricks using quantum states. Magicians Alice and Bob guesses the numbers selected by spectators Carol and Davis. Throughout this section, let arithmetic operations be executed to modulus a prime integer N.

First, let (Alice, Carol) and (Bob, Davis) be two pairs. Then, we show tricks such that Alice guesses Davis's number and Bob guesses Carol's number.

Telepathy: First, Alice prepares a card written a number, and puts in a box. The number of this card can be rewritten. Next, Carol multiplies it by m and adds a random r to it, where $m,r\in\mathbf{Z}_N^+$. Finally, Bob prepares the $N-1$ numbered cards. Carol opens the box and obtains a number. By turning over Bob's card corresponding the number, Carol confirms that the reverse side of the card is m.

Method of Telepathy

1) Beforehand, Alice and Bob share the following entangled state.

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|x\rangle,$$

where Alice has the first register and Bob has the second register. Alice's register is put in a box.

2) Carol multiplies Alice's register by m, and adds r to it. Then, the state becomes

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|mx+r\rangle|x\rangle.$$

3) Alice and Bob apply QFT to it and the state becomes

$$\frac{1}{\sqrt{N^3}} \sum_{y_1=0}^{N-1} \sum_{y_2=0}^{N-1} \sum_{x=0}^{N-1} e^{i2\pi(mx+r)y_1/N} e^{i2\pi xy_2/N} |y_1\rangle |y_2\rangle$$

$$= \frac{1}{\sqrt{N^3}} \sum_{y_1=0}^{N-1} e^{i2\pi ry_1/N} \sum_{y_2=0}^{N-1} \sum_{x=0}^{N-1} e^{i2\pi(my_1+y_2)x/N} |y_1\rangle |y_2\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{my_1+y_2\equiv 0(\mathrm{mod}\,N)} e^{i2\pi ry_1/N} |y_1\rangle |y_2\rangle.$$

Then, Bob measures it and obtains y_2 satisfying $my_1 + y_2 \equiv 0(\mathrm{mod}\,N)$.

4) Bob prepares a set of pairs (m, y_1) satisfying $my_1 + y_2 \equiv 0(\mathrm{mod}\,N)$. That is, he writes y_1 to the surface of a card and writes m to the reverse side. He makes cards corresponding to all the possible pairs of (m, y_1). Then, he exhibits the set of the cards to Carol.

5) Carol opens the box and knows y_1. Then, she turns over Bob's card written y_1 and confirms that the value of the reverse side is m.

Mutual Telepathy: Let Alice and Carol be one pair, and Bob and Davis be another pair. First, Alice prepares a card written a number, and puts in a box. Bob also prepares a card written a number, and puts in another box. Next, Carol multiplies it by m_1, and adds a random r_1 to it. Davis multiplies it by m_2, and adds a random r_2 to it. Here, $m_1, m_2, r_1, r_2 \in \mathbf{Z}_N^+$. Finally, Bob prepares the $N-1$ numbered cards. Carol opens the box and obtains a number. By turning over Bob's card corresponding the number, Carol confirms that the reverse side of the card is m_1. In addition, Alice prepares the $N-1$ numbered cards. Davis opens the box and obtains a number. By turning over Alice's card corresponding the number, Davis confirms that the reverse side of the card is m_2.

Method of Mutual Telepathy

1) Beforehand, Alice and Bob share the following entangled state.

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |x\rangle,$$

where Alice has the first register and Bob has the second register. Alice's register is put in a box, and Bob's register is put another box.

2) Carol multiplies Alice's register by m_1 and adds r_1 to it. Davis multiplies Bob's register by m_2 and adds r_2 to it. Then, the state becomes

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |m_1 x + r_1\rangle |m_2 x + r_2\rangle.$$

In addition, Davis announces m_2 to Bob.

3) Alice and Bob apply QFT to it and the state becomes

$$\frac{1}{\sqrt{N^3}} \sum_{y_1=0}^{N-1} \sum_{y_2=0}^{N-1} e^{i2\pi(r_1y_1+r_2y_2)/N} \sum_{x=0}^{N-1} e^{i2\pi(m_1y_1+m_2y_2)x/N} |y_1\rangle |y_2\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{m_1y_1+m_2y_2\equiv 0(\mathrm{mod}\,N)} e^{i2\pi(r_1y_1+r_2y_2)/N} |y_1\rangle |y_2\rangle.$$

Then, Alice and Bob measure it and obtain y_1 and y_2, respectively, satisfying $m_1y_1 + m_2y_2 \equiv 0(\mathrm{mod}\,N)$.

4) Bob prepares a set of pairs (m_1, y_1) satisfying $m_1y_1 + m_2y_2 \equiv 0(\mathrm{mod}\,N)$. That is, he writes y_1 to the surface of a card and writes m_1 to the reverse side. He makes cards corresponding to all the possible pairs of (m_1, y_1). Then, he exhibits the set of the cards to Carol.

5) Carol opens the box and knows y_1. Then, she turns over Bob's card written y_1 and confirms that the value of the reverse side is m_1. Note that Alice can also know m_1 here.

6) Alice also prepares a set of pairs (m_2, y_2) satisfying $m_1y_1 + m_2y_2 \equiv 0(\mathrm{mod}\,N)$, and Davis can find the correct pair (m_2, y_2).

Next, we show a card trick similar to **Flip-Flop2**.

Prediction: First, Alice prepares a card written 0, and puts it in a box. Next, Carol adds $m_1 \in \mathbf{Z}_N^+$ to it. Alice executes some operation. Carol multiplies it by m_2 and adds a random r to it, where $m_2, r \in \mathbf{Z}_N^+$. Alice executes some operation, opens the box, and obtains a number. Finally, Alice prepares the $N-1$ numbered cards. By turning over Alice's card corresponding m_1, Carol confirms that the reverse side of the card is m_2.

Method of Prediction

1) Alice prepares a state $|0\rangle$, exhibits it to Carol, and puts it in a box.

2) Carol adds m_1 to it and the state becomes $|m_1\rangle$.

3) Alice applies QFT to it and the state becomes

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{i2\pi m_1 x/N} |x\rangle.$$

4) Carol multiplies it by m_2 and adds r to it. Then, the state becomes

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{i2\pi m_1 x/N} |m_2 x + r\rangle.$$

5) Alice applies QFT to it and the state becomes

$$\frac{1}{\sqrt{N^2}}\sum_{y=0}^{N-1}\sum_{x=0}^{N-1}e^{i2\pi m_1 x/N}e^{i2\pi(m_2 x+r)y/N}\,|\,y\rangle$$

$$=\frac{1}{\sqrt{N^2}}\sum_{y=0}^{N-1}e^{i2\pi ry/N}\sum_{x=0}^{N-1}e^{i2\pi(m_1+m_2 y)x/N}\,|\,y\rangle$$

$$=e^{i2\pi ry'/N}\,|\,y'\rangle,$$

where $m_1+m_2 y'\equiv 0(\text{mod }N)$. Then, Alice measures it and obtains y'.

6) Alice prepares a set of pairs (m_1,m_2) satisfying $m_1+m_2 y'\equiv 0(\text{mod }N)$. That is, she writes m_1 to the surface of a card and writes m_2 to the reverse side. she makes cards corresponding to all the possible pairs of (m_1,m_2). Then, she exhibits the set of the cards to Carol.

7) Carol turns over Alice's card written m_1 and confirms that the value of the reverse side is m_2.

Finally, we show a trick such that Alice guesses the number selected by Carol in a situation that Alice prepares a set of cards beforehand.

Mindreading: Beforehand, Alice prepares a set of $N-1$ cards. She writes each $y\in\mathbf{Z}_N^+$ to each card and writes $\sigma(y)$ to the reverse side, where $\sigma(y)$ is a random permutation of y. First, Carol selects $m\in\mathbf{Z}_N^+$ and announces it to Alice. Alice prepares a card, and puts in a box. Next, Carol adds a random $r\in\mathbf{Z}_N^+$ to it. Alice executes some operation. Finally, Carol opens the box, and obtains a number. By turning over Alice's card corresponding to the number, Carol confirms that the reverse side of the card is m.

Method of Mindreading

1) Carol selects m and announces it to Alice.
2) Alice prepares a state

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{i2\pi wx/N}\,|\,x\rangle,$$

where let $\sigma(w)=m$. This is put in a box.

3) Carol adds a random r to it, and the state becomes

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{i2\pi wx/N}\,|\,x+r\rangle,$$

4) Alice applies QFT^{-1} to it and the state becomes

$$\frac{1}{\sqrt{N^2}}\sum_{y=0}^{N-1}\sum_{x=0}^{N-1}e^{i2\pi wx/N}e^{-i2\pi(x+r)y/N}\,|\,y\rangle$$

$$=\frac{1}{\sqrt{N^2}}\sum_{y=0}^{N-1}e^{-i2\pi ry/N}\sum_{x=0}^{N-1}e^{i2\pi(w-y)x/N}\,|\,y\rangle$$

$$=e^{-i2\pi rw/N}\,|\,w\rangle.$$

5) Carol opens the box, obtains w, and confirms that the value of the reverse side is m.

Let $c(n)$ be the time complexity of arithmetic operations, where n is the size of the input. In addition, let $q(n)$ be the time complexity of QFT. It is know that both $c(n)$ and $q(n)$ are within polynomial of n. Then, the complexity of their methods mentioned in this section is in $O(c(\log N)+q(\log N))$ time.

5. Conclusions

In this paper, we proposed new coin tricks and card tricks based on quantum physics. In these tricks, magicians had the ability of quantum physics, but spectators had only classical one. Therefore, magicians could manipulate coins and cards as quantum states. Moreover, by sharing entangled states, they could transmit spectators' values without communicating between them.

Since our tricks are simple and straightforward ones using quantum states, they are somewhat clumsy. Therefore, it is a future work to construct polished tricks. Moreover, in our tricks, spectators had only classical power. Therefore, it is an interesting problem that we construct quantum tricks when spectators also have quantum power.

REFERENCES

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Journal on Computing, Vol. 26, pp. 1484–1509, 1997.

[2] D. A. Meyer, "Quantum strategies," Physical Review Letters, Vol. 82, pp. 1052–1055, 1999.

[3] J. Eisert, M. Wilkens, and M. Lewenstein, "Quantum games and quantum strategies," Physical Review Letters, Vol. 83, pp. 3077–3080, 1999.

[4] J. Du, H. Li, X. Xu, M. Shi, J. Wu, X. Zhou, and R. Han, "Experimental realization of quantum games on a quantum computer," Physical Review Letters, Vol. 88, 2002.

[5] J. Du, H. Li, X. Xu, X. Zhou, and R. Han, "Entanglement enhanced multiplayer quantum games," Physical Review Letters, Vol. 302, pp. 229–233, 2002.

[6] J. Eisert and M. Wilkens, "Quantum games," Journal of Modern Optics, Vol. 47, pp. 2543–2556, 2000.

[7] A. Iqbal and A. H. Toor, "Evolutionarily stable strategies in quantum games," Physics Letters A, Vol. 280, pp. 249–256, 2001.

[8] L. Marinatto and T. Weber, "A quantum approach to static games of complete information," Physics Letters A, Vol. 272, pp. 291–303, 2000.