アルゴリズム 84−12
(2002. 5. 23)

通信、そして計算としての量子ゲーム

川上 岳†

†東京大学大学院情報理工学研究科コンピュータ科学専攻
113–0033 東京都文京区本郷 7–3–1
cawakami@is.s.u-tokyo.ac.jp

要旨

囚人のジレンマと呼ばれるゲームにおいて、プレーヤーである囚人は情報交換を許されず、相手がどんな選択をするかがわからないまま自分の選択を行わなければならない。審判としての看守に自分の選択を伝え、看守は両者の選択に従ってそれぞれに利得を与える。自分の選択がわかっているそれぞれの囚人はその利得を得た瞬間に相手がどんな選択をしたかを知る。つまり利得が看守から囚人に与えられた瞬間に囚人間の通信が成立するのである。このような観点から、この論文ではゲームを一種の通信として捉え、主に量子ゲームの中での情報の運び手について考察する。さらにゲームという通信形態を用いた問題解法についても言及し、古典モデルでは解けない問題が量子モデルでは解けることを示す。

Quantum Game as Communication and Computation

Takeshi Kawakami†

†Department of Computer Science, Graduate School of Information Science and Technology, The University of Tokyo
7–3–1 Hongo, Bunkyo-ku, Tokyo 113–0033, Japan
cawakami@is.s.u-tokyo.ac.jp

Abstract

In a game called prisoner's dilemma, each of two prisoners as a player is not permitted to exchange information with the other and has to make his decision without knowing the decision of the opponent. Prisoners tell a jailer as arbitrator their decisions and the jailer gives each of the prisoners appropriate payoff according to his decision. That is, communication between the two is achieved the moment each payoff has been given to each of them by the jailer. From this viewpoint, this paper considers a game as a kind of communication and mainly discussed information carriers in the quantum game. Furthermore, it refers a problem solving by using an aspect as communication of a game and shows a problem which cannot be solved in classical model can be solved in quantum model.

1 Introduction

Game theory is a field in which a process of decision making is analyzed, and a game called "prisoner's dilemma"[4] can directly represent an interest and difficulty of the analysis. But in this paper, the aspect of communication is dicussed, not the equilibrium. In the game, two prisoner, Alice and Bob, are prohibited to communicate each other and forced to decide cooperation(C) or defect(D). After they tell a jailer as an arbitrator their decision, he give each payoff to each prisoner based on Table1. In Table1, a row is Alice's decision and a column is Bob's decision and each cell's left side is Alice's payoff and right side is Bob's. For example,

	C	D
C	3 3	0 5
D	5 0	1 1

Table 1: payoff table

in Alice's position, if she decides C and gains a payoff 3, she can know Bob's decision is C by Table1. That is, a payoff given by a jailer includes information which tells an opponent's decision and this information is 1bit which can determine one of two.

In this following part, the aspect of the quantum game is focused on, and we discuss information exchanged in it and this information carrier. Furthermore, we refer the problem solving using the aspect, and it is showed that the procedure which is impossible in a classical model is possible in a quantum model by this peculiar phenomena.

2 Quatum Game as Communication

2.1 4 Pauli Matrices and Unitary Matrix

An arbitrary unitary matrix $\boldsymbol{U}$ of degree 2 can be represented as follows [3]:

$$\boldsymbol{U} = e^{i\gamma} \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix} \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} e^{i\beta} & 0 \\ 0 & e^{-i\beta} \end{pmatrix} \tag{2.1}$$

If $\gamma = 0$, $\boldsymbol{U}$ can be represented by identity matrix $\boldsymbol{I}$ and Pauli matrices $\boldsymbol{\sigma}_x$, $\boldsymbol{\sigma}_y$, $\boldsymbol{\sigma}_z$ as follows:

$$\boldsymbol{U} = \cos\phi\cos\theta\cdot\boldsymbol{I} + \sin\phi\cos\theta\cdot i\boldsymbol{\sigma}_z + \cos\psi\sin\theta\cdot i\boldsymbol{\sigma}_x + \sin\psi\sin\theta\cdot i\boldsymbol{\sigma}_y \tag{2.2}$$

Each Pauli matrix is as follows:

$$\boldsymbol{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \boldsymbol{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \boldsymbol{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.3}$$

Pauli matrices have following properties:

$$\boldsymbol{\sigma}_j{}^2 = \boldsymbol{I} \quad j \in \{x, y, z\} \qquad \boldsymbol{\sigma}_k\boldsymbol{\sigma}_l = -\boldsymbol{\sigma}_l\boldsymbol{\sigma}_k = i\boldsymbol{\sigma}_m \tag{2.4}$$

(k, l, m) is a cyclic permutation of (x, y, z).

2.2 4 Strategies

In this establishment, each prisoner's strategy (unitary transform $\boldsymbol{U}$) is restricted to $\boldsymbol{I}$, $\boldsymbol{\sigma}_x$, $\boldsymbol{\sigma}'_y\,(= i\boldsymbol{\sigma}_y)$, and $\boldsymbol{\sigma}_z$, and represented as follows:

$$\boldsymbol{U} = \boldsymbol{\sigma}_z{}^j\boldsymbol{\sigma}_x{}^k \tag{2.5}$$

That is, each prisoner can decide j and k. For example, if $j = 1$ and $k = 1$, $\boldsymbol{U}$ is $\boldsymbol{\sigma}_y{}'$. In this game, a matrix $\boldsymbol{J}$ is as follows:

$$\boldsymbol{J} = \frac{1}{\sqrt{2}}\left(\boldsymbol{I}\otimes\boldsymbol{I} + i\boldsymbol{\sigma}_x\otimes\boldsymbol{\sigma}_x\right) \tag{2.6}$$

Alice's strategy $\boldsymbol{U}_A$ and Bob's strategy $\boldsymbol{U}_B$ are represented as follows:

$$\boldsymbol{U}_A = \boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A} \quad \boldsymbol{U}_B = \boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B} \tag{2.7}$$

This game's initial state $\boldsymbol{\varphi}_{in}$ and final state $\boldsymbol{\varphi}_{fin}$ which is an target of measurement are as follows[2, 1]:

$$\boldsymbol{\varphi}_{in} = \boldsymbol{J}|00\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{i}{\sqrt{2}}|11\rangle \qquad \boldsymbol{\varphi}_{fin} = \boldsymbol{J}^*\left(\boldsymbol{U}_A \otimes \boldsymbol{U}_B\right)\boldsymbol{J}|00\rangle \tag{2.8}$$

$\boldsymbol{J}^*\left(\boldsymbol{U}_A \otimes \boldsymbol{U}_B\right)\boldsymbol{J}$ is analyzed as follows.

$$\boldsymbol{J}^*\left(\boldsymbol{U}_A \otimes \boldsymbol{U}_B\right)\boldsymbol{J} = \frac{1}{2}\left(\boldsymbol{I}\otimes\boldsymbol{I} - i\boldsymbol{\sigma}_x\otimes\boldsymbol{\sigma}_x\right)\left(\boldsymbol{U}_A \otimes \boldsymbol{U}_B\right)\left(\boldsymbol{I}\otimes\boldsymbol{I} + i\boldsymbol{\sigma}_x\otimes\boldsymbol{\sigma}_x\right) \tag{2.9}$$

$$=\frac{1}{2}\{\boldsymbol{U}_A\otimes\boldsymbol{U}_B + i\left(\boldsymbol{U}_A\boldsymbol{\sigma}_x\right)\otimes\left(\boldsymbol{U}_B\boldsymbol{\sigma}_x\right) - i\left(\boldsymbol{\sigma}_x\boldsymbol{U}_A\otimes\boldsymbol{\sigma}_x\boldsymbol{U}_B\right) + \left(\boldsymbol{\sigma}_x\boldsymbol{U}_A\boldsymbol{\sigma}_x\right)\otimes\left(\boldsymbol{\sigma}_x\boldsymbol{U}_B\boldsymbol{\sigma}_x\right)\} \tag{2.10}$$

$$=\frac{1}{2}\{\boldsymbol{U}_A\otimes\boldsymbol{U}_B + \left(\boldsymbol{\sigma}_x\boldsymbol{U}_A\boldsymbol{\sigma}_x\right)\otimes\left(\boldsymbol{\sigma}_x\boldsymbol{U}_B\boldsymbol{\sigma}_x\right) + \frac{i}{2}\{\left(\boldsymbol{U}_A\boldsymbol{\sigma}_x\right)\otimes\left(\boldsymbol{U}_B\boldsymbol{\sigma}_x\right) - \left(\boldsymbol{\sigma}_x\boldsymbol{U}_A\otimes\boldsymbol{\sigma}_x\boldsymbol{U}_B\right)\} \tag{2.11}$$

$$\begin{aligned}=&\frac{1}{2}\{\left(\boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A}\right)\otimes\left(\boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B}\right) + \left(\boldsymbol{\sigma}_x\boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A}\boldsymbol{\sigma}_x\right)\otimes\left(\boldsymbol{\sigma}_x\boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B}\boldsymbol{\sigma}_x\right)\}\\ &+\frac{i}{2}\{\left(\boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A}\boldsymbol{\sigma}_x\right)\otimes\left(\boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B}\boldsymbol{\sigma}_x\right) - \left(\boldsymbol{\sigma}_x\boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A}\right)\otimes\left(\boldsymbol{\sigma}_x\boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B}\right)\}\end{aligned} \tag{2.12}$$

$$\begin{aligned}=&\frac{1}{2}\{\left(\boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A}\right)\otimes\left(\boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B}\right) + (-1)^{j_A+j_B}\left(\boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A}\right)\otimes\left(\boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B}\right)\}\\ +&\frac{i}{2}\{\left(\boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A}\boldsymbol{\sigma}_x\right)\otimes\left(\boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B}\boldsymbol{\sigma}_x\right) - (-1)^{j_A+j_B}\left(\boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A}\boldsymbol{\sigma}_x\right)\otimes\left(\boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B}\boldsymbol{\sigma}_x\right)\}\end{aligned} \tag{2.13}$$

$$=\boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A}\otimes\boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B}\left(\frac{1+(-1)^{j_A+j_B}}{2}\boldsymbol{I}\otimes\boldsymbol{I} + i\frac{1-(-1)^{j_A+j_B}}{2}\boldsymbol{\sigma}_x\otimes\boldsymbol{\sigma}_x\right) \tag{2.14}$$

$$=\boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A}\otimes\boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B}\left(\delta_{f(j_A,j_B),0}\boldsymbol{I}\otimes\boldsymbol{I} + i\delta_{f(j_A,j_B),1}\boldsymbol{\sigma}_x\otimes\boldsymbol{\sigma}_x\right) \tag{2.15}$$

Thus, $\boldsymbol{\varphi}_{fin}$ is analyzed as follows.

$$\boldsymbol{\varphi}_{fin} = \boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A}\otimes\boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B}\left(\delta_{f(j_A,j_B),0}\boldsymbol{I}\otimes\boldsymbol{I} + i\delta_{f(j_A,j_B),1}\boldsymbol{\sigma}_x\otimes\boldsymbol{\sigma}_x\right)|00\rangle \tag{2.16}$$

$$= \boldsymbol{\sigma}_z{}^{j_A}\boldsymbol{\sigma}_x{}^{k_A}\otimes\boldsymbol{\sigma}_z{}^{j_B}\boldsymbol{\sigma}_x{}^{k_B}\left(\delta_{f(j_A,j_B),0}|00\rangle + i\delta_{f(j_A,j_B),1}|11\rangle\right) \tag{2.17}$$

A function $f\left(j_A, j_B\right)$ is as follows:

$$f\left(j_A, j_B\right) = \left(j_A + j_B\right) \bmod 2 \tag{2.18}$$

Who computes this function? A jailer or a prisoner? Each prisoner is prohibitted to communicate with other prisoners, so he has no way to compute the function. Although a jailer can apply unitary transforms $\boldsymbol{J}$ and $\boldsymbol{J}^*$ to each qubit, he is only to measure each qubit. That is, the function is computed automatically by the interaction between qubit brought about by a series unitary transform $\boldsymbol{J}^*\left(\boldsymbol{U}_A \otimes \boldsymbol{U}_B\right)\boldsymbol{J}$. The automatical computation like this might mean quantum computation or quantum information processing and we can see the aspect in this game. His/Her payoff which is given to each prisoner on the basis of his/her measured state is in a table 2.

From a formula (2.17) and a table 2, his/her payoff which is given to each prisoner on the basis of his/her strategy is in a table 3. From a formula (2.5), each strategy can be distinguished

	$\|0\rangle$	$\|1\rangle$
$\|0\rangle$	3 3	0 5
$\|1\rangle$	5 0	1 1

Table 2: state

jk	00	10	01	11
00	3 3	1 1	0 5	5 0
10	1 1	3 3	5 0	0 5
01	5 0	0 5	1 1	3 3
11	0 5	5 0	3 3	1 1

Table 3: strategy

by j and k, so each strategy is represented by j and k in a table 3. In Alice's position, if she decides 00 and gains a payoff 5, she can know Bob's decision is 11 by a table 3. In this case, information which is exchanged between them through a jailer is 2 bits which determine one of four.

2.3 Aspect of Communication

As stated above, a game has an aspect of communication. Especially, a quantum game has an ability to communicate 2 bits information by 1 qubit operation while a classical game communicates 1 bit by 1 bit operation. This fact is similar to superdense coding[3] and implies that quantum communication has more computational ability than classical.

In a quantum game, each unitary matrix ${\boldsymbol{\sigma}_z}^j{\boldsymbol{\sigma}_x}^k$ which prisoners can use can be said as follows.

$$\boldsymbol{I}\,(j=0,k=0): \quad |0\rangle \longrightarrow |0\rangle \qquad |1\rangle \longrightarrow |1\rangle \tag{2.19}$$
$$\boldsymbol{\sigma}_x\,(j=0,k=1): \quad |0\rangle \longrightarrow |1\rangle \qquad |1\rangle \longrightarrow |0\rangle \tag{2.20}$$
$$\boldsymbol{\sigma}_z\,(j=1,k=0): \quad |0\rangle \longrightarrow |0\rangle \qquad |1\rangle \longrightarrow -|1\rangle \tag{2.21}$$
$$\boldsymbol{\sigma}'_y\,(j=1,k=1): \quad |0\rangle \longrightarrow -|1\rangle \qquad |1\rangle \longrightarrow |0\rangle \tag{2.22}$$

That is,

$${\boldsymbol{\sigma}_z}^j{\boldsymbol{\sigma}_x}^k: \quad |0\rangle \longrightarrow (-1)^{jk}\,|k\rangle \qquad |1\rangle \longrightarrow (-1)^{j\overline{k}}\,|\overline{k}\rangle \tag{2.23}$$

So, it can be said that ${\boldsymbol{\sigma}_z}^j{\boldsymbol{\sigma}_x}^k$ changes not only a qubit's content but also this phase(coefficient). If there would be a way to distinguish single qubit's phase, a qubit could include infinite information. But we can't distinguish the phase by measuring. For example, assume a state $\boldsymbol{\varphi}$ is as follows.

$$\boldsymbol{\varphi} = a|0\rangle \quad \left(|a|^2 = 1\right) \tag{2.24}$$

You can know easily a complex number which satisfies $|a|^2 = 1$ exists infinitely, but we can only measure a state $|0\rangle$. So, a phase difference has no mean and one qubit includes only one bit information if it cannot be distinguished on measuring. But in a quantum game, 2 bit communication can be done by operating one qubit. This means a phase difference is distinguished in it. How can it be done?

By the way, the initial state $\boldsymbol{\varphi}_{in}$ in a quatum game was as follows.

$$\boldsymbol{\varphi}_{in} = \boldsymbol{J}|00\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{i}{\sqrt{2}}|11\rangle \tag{2.25}$$

That is, a entangled state[3] is made by $\boldsymbol{J}$. One of some properties of tensor product is as follows.

$$(a\boldsymbol{x}) \otimes (b\boldsymbol{y}) = ab\,(\boldsymbol{x} \otimes \boldsymbol{y}) \tag{2.26}$$

Formula (2.26) means phase interaction happens between different qubits. That is, after each prisoner applied each unitary transform to each qubit, different qubits' phases interact each other and in Formula (2.17), it can be said that a $f(j_A, j_B)$'s value is determined by this interaction. In other words, in Formula (2.17), $\delta_{f(j_A,j_B),0}$ or $\delta_{f(j_A,j_B),1}$ represents an interference caused by $\boldsymbol{J^*}$, so it can be said that the interference is controled by the interaction.

To sum up, in a quantum game, a entangled state in which each qubit's content is connected with other's is caused by $\boldsymbol{J}$, the phase interaction between different qubit is caused by each prisoner's unitary transform, and the interference is caused by $\boldsymbol{J'}$. That is, by this process each phase difference in Formulas (2.19)(2.20)(2.21) (2.22) is distinguished. So it can be said that a unitary transform series $\boldsymbol{J^*}\left(\boldsymbol{U}_A \otimes \boldsymbol{U}_B\right)\boldsymbol{J}$ is a kind of procedure to distinguish the phase difference.

For example, Assume Alice decides $\boldsymbol{\sigma}_z\,(10)$ and Bob decides $\boldsymbol{\sigma}'_y\,(11)$. First, the entangled state $\boldsymbol{\varphi}_{in}$ is made by $\boldsymbol{J}$ as follows.

$$\boldsymbol{\varphi}_{in} = \boldsymbol{J}|00\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{i}{\sqrt{2}}|11\rangle \tag{2.27}$$

Then, Alice and Bob apply their unitary transform to their own qubits respectively and cause the phase interaction between qubits as follows.

$$\left(\boldsymbol{U}_A \otimes \boldsymbol{U}_B\right)\boldsymbol{\varphi}_{in} = \frac{1}{\sqrt{2}}\left(\boldsymbol{\sigma}_z|0\rangle\right) \otimes \left(\boldsymbol{\sigma}'_y|0\rangle\right) + \frac{i}{\sqrt{2}}\left(\boldsymbol{\sigma}_z|1\rangle\right) \otimes \left(\boldsymbol{\sigma}'_y|1\rangle\right) \tag{2.28}$$

$$= \frac{1}{\sqrt{2}}|0\rangle \otimes (-|1\rangle) + \frac{i}{\sqrt{2}}(-|1\rangle) \otimes |0\rangle = -\frac{1}{\sqrt{2}}|01\rangle - \frac{i}{\sqrt{2}}|10\rangle \tag{2.29}$$

Finally, the interference is caused by $\boldsymbol{J}^*$ as follows.

$$\boldsymbol{\varphi}_{fin} = \boldsymbol{J}^*\left(-\frac{1}{\sqrt{2}}|01\rangle - \frac{i}{\sqrt{2}}|10\rangle\right) = -\frac{1}{2}|01\rangle - \frac{i}{2}|10\rangle + \frac{i}{2}|10\rangle - \frac{1}{2}|01\rangle \tag{2.30}$$

$$= -\frac{1}{2}(1+1)|01\rangle + \frac{i}{2}(-1+1)|10\rangle = -\frac{1}{2}\cdot 2\cdot|01\rangle + \frac{i}{2}\cdot 0\cdot|10\rangle \tag{2.31}$$

$$= -|01\rangle \tag{2.32}$$

So in this case, a state $|01\rangle$ is measured by a jailer and Alice gains 0 and Bob gains 5 payoff respectively according to Table 2. From each payoff, Alice can know Bob changed his qubit as $|0\rangle \longrightarrow -|1\rangle$ and $|1\rangle \longrightarrow |0\rangle$, and Bob can know Alice changed her qubit as $|0\rangle \longrightarrow |0\rangle$ and $|1\rangle \longrightarrow -|1\rangle$. So, it can be said that the payoff a jailer returns to each prisoner includes phase information of each qubit and that it becomes possible to distinguish the phase difference in quantum game.

3 Quantum Game as Computation

A meaningless communication in a classical model is meaningful in a quantum model. That is, the following problem can be solved in this condition by iterating quantum game n times.

Problem:

M prisoners have 0 or 1. What is the remaider of 2^n of the sum of all prisoners' numbers?

Conditions:

- Each prisoner cannot communicate with other prisoners.

- Each prisoner can deliver to a jailer only an envelope into which his paper on which his decision is written is put.
- Each prisoner knows only how many prisoners there are.
- A jailer cannot open the envelopes which are collected from prisoners.

In this case, there are M prisoners, so $\boldsymbol{J}, \boldsymbol{\varphi}_{in}, \boldsymbol{\varphi}_{fin}$ in section 2 are extended as follows respectively:

$$\boldsymbol{J} = \frac{1}{\sqrt{2}} \bigotimes_{j=1}^{M} \boldsymbol{I} + \frac{i}{\sqrt{2}} \bigotimes_{j=1}^{M} \boldsymbol{\sigma}_x \quad \left(\bigotimes_{j=1}^{M} \boldsymbol{I} = \overbrace{\boldsymbol{I} \otimes \cdots \otimes \boldsymbol{I}}^{M} \right) \tag{3.1}$$

$$\boldsymbol{\varphi}_{in} = \boldsymbol{J} \bigotimes_{j=1}^{M} |0\rangle = \frac{1}{\sqrt{2}} \bigotimes_{j=1}^{M} |0\rangle + \frac{i}{\sqrt{2}} \bigotimes_{j=1}^{M} |1\rangle \quad \left(\bigotimes_{j=1}^{M} |0\rangle = \overbrace{|0 \dots 0\rangle}^{M} \right) \tag{3.2}$$

$$\boldsymbol{\varphi}_{fin} = \boldsymbol{J}^* \left(\bigotimes_{j=1}^{M} \boldsymbol{U}_j(t) \right) \boldsymbol{J} \bigotimes_{j=1}^{M} |0\rangle \tag{3.3}$$

A unitary transform $\boldsymbol{U}_j(t)$ which jth prisoner can apply to his own qubit is as follows:

$$\boldsymbol{U}_j(t) = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(-i\frac{2\pi}{2^t M} r_{t-1}\right) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(i\frac{2\pi}{2^t} b_j\right) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(i\frac{2\pi}{2^t}\left(b_j - \frac{r_{t-1}}{M}\right)\right) \end{pmatrix} \tag{3.4}$$

That is,

$$\boldsymbol{U}_j(t): \quad |0\rangle \longrightarrow |0\rangle \qquad |1\rangle \longrightarrow \exp\left(i\frac{2\pi}{2^t}\left(b_j - \frac{r_{t-1}}{M}\right)\right)|1\rangle \tag{3.5}$$

b_j is a number which jth prisoner has, t is a iteration time, and later I will prove that r_{t-1} becomes 2^{t-1}'s remainder of a sum of all prisoners' number if it is updated every iteration by a recursive formula (3.11) and its initial value r_0 is 0 because. A final state $\boldsymbol{\varphi}_{fin}$ is analyzed as follows.

$$\boldsymbol{\varphi}_{fin} = \boldsymbol{J}^* \left(\bigotimes_{j=1}^{M} \boldsymbol{U}_j(t) \right) \boldsymbol{J} \bigotimes_{j=1}^{M} |0\rangle \tag{3.6}$$

$$= \frac{1}{2}\left[1 + \exp\left(i\pi \frac{\sum_{j=1}^{M} b_j - r_{t-1}}{2^{t-1}}\right)\right] \bigotimes_{j=1}^{M} |0\rangle - \frac{i}{2}\left[1 - \exp\left(i\pi \frac{\sum_{j=1}^{M} b_j - r_{t-1}}{2^{t-1}}\right)\right] \bigotimes_{j=1}^{M} |1\rangle \tag{3.7}$$

$$= \frac{1 + (-1)^{R(t)}}{2} \bigotimes_{j=1}^{M} |0\rangle - i\frac{1 - (-1)^{R(t)}}{2} \bigotimes_{j=1}^{M} |1\rangle \tag{3.8}$$

$R(t)$ is as follows:

$$R(t) = \frac{\sum_{j=1}^{M} b_j - r_{t-1}}{2^{t-1}} \tag{3.9}$$

A function $f_t(b_1, b_2, \dots, b_n)$ is as follows:

$$f_t(b_1, b_2, \dots, b_n) = \left(\sum_{j=1}^{M} b_j \text{ quotient } 2^{t-1} \right) \bmod 2 \tag{3.10}$$

Before starting $t+1\,(t \geq 1)$th game communication, each prisoner updates r_{t-1} to r_t in his own unitary transform as follows.

$$r_t := r_{t-1} + q_j^t \cdot 2^{t-1} \quad (r_0 = 0) \tag{3.11}$$

q_j^t is a measurement result of jth prisoner's qubit after tth game communication which he only can measure.

Proposition

r_t is a 2^t's remaider of the sum of all prisoner's numbers for $t \geq 0$.

Proof

When $t = 0$, it is clear that the proposition holds.
When $t = k\,(\geq 1)$, $R\,(k)$ is as follows.

$$R\,(k) = \frac{\sum_{j=1}^{M} b_j - r_{k-1}}{2^{k-1}} \tag{3.12}$$

So, supposing the proposition holds when $t = k-1$, $R\,(k)$ is as follows.

$$R\,(k) = \sum_{j=1}^{M} b_j \text{ quotient } 2^{k-1} \tag{3.13}$$

Therefore, $f_k\,(b_1, b_2, \ldots, b_n)$ is as follows.

$$f_k\,(b_1, b_2, \ldots, b_n) = R\,(k) \bmod 2 \tag{3.14}$$

After kth game communication, a final state φ_{fin} is as follows.

$$\varphi_{fin} = \delta_{f_k(b_1,\ldots,b_n),0} \bigotimes_{j=1}^{M} |0\rangle - i\delta_{f_k(b_1,\ldots,b_n),1} \bigotimes_{j=1}^{M} |1\rangle \tag{3.15}$$

In jth prisoner's position, he can know whether $f_k\,(b_1, \ldots, b_n)$ is 0 or 1 by measuring his own bit. By the way, the sum can be represented as follows.

$$\sum_{j=1}^{M} b_j = B \cdot 2^k + b \cdot 2^{k-1} + r_{k-1} = (B \cdot 2 + b) \cdot 2^{k-1} + r_{k-1} \tag{3.16}$$

$R\,(k)$ is as follows from a formula (3.13).

$$R\,(k) = B \cdot 2 + b \tag{3.17}$$

And $f_k\,(b_1, b_2, \ldots, b_n)$ can be represented as follows from a formula (3.14).

$$f_k\,(b_1, b_2, \ldots, b_n) = (B \cdot 2 + b) \bmod 2 = b \bmod 2 \tag{3.18}$$

In other words, he can know whether b in above formulas is 0 or 1 by measuring his own qubit. Therefore, when he updates r_{k-1} to r_k according to a formula (3.11), r_k becomes a 2^k's remainder of the sum.
From the mentioned above, it is proved that the proposition holds for $t \geq 0$. □

From the proposition, it can be said that the problem can be solved by iterating quantum game n times. That is, the action that he measure his own qubit after game session, which looks meaningless, is meaningful in quantum model.

4 Conclusion

Why is it meaningful that each prisoner measures his own qubit by himself in quantum game? In classical game, he knows his own decision, so it is meaningless that a jailer returns his decision as it is to him. However in quantum game, he has no way to know what his qubit is after measurement. Since it can be said that it depends on the other prisoner's decision by a series of interactions, entanglement by $\boldsymbol{J}$, phase interaction by $\boldsymbol{U}_A \otimes \boldsymbol{U}_B$, interference by $\boldsymbol{J}^*$.

Next, what are carriers of information in quantum game and quatum game? There are two carriers. Of course one of these is a content of a qubit itself. This can be distinguished by measurement. If it would be only an information carrier, one qubit could include only one bit information. However in quantum game, 2 bit information is exchanged between prisoners by one qubit opperation. This fact implies that there is another information carrier. This is a phase of each qubit. In quatum game in section 2, a unitary transform which each prisoner can use can change not only a qubit content but also this phase. In quantum game in section 3, it can be said that each prisoner represents information which he want to send not by a qubit content, but by this phase. However, phase difference cannot be distinguished by simple measurement. A certain device is necessary to do this and the device is a series of unitary transforms, $\boldsymbol{J}^* \left(\boldsymbol{U}_A \otimes \boldsymbol{U}_B\right) \boldsymbol{J}$ in section 2, or $\boldsymbol{J}^* \left(\bigotimes_{j=1}^{M} \boldsymbol{U}_j\left(t\right)\right) \boldsymbol{J}$ in section 3. It can be said that in section 2, 2 bit information is exchanged between two prisoners by using one qubit content and phase as information carrier, and that in section 3, the problem can be solved by using one qubit phase in the severe condition in which the problem cannot be solved by a classical model.

In a classical model, if a jailer is prohibitted to open envelopes which are collected from prisoners, he have nothing to do. However, in a quantum model, he can apply a unitary transform to a "paper" from the outside of the envelope and bring about the interaction between "papers". This interaction is reflected on measument by each prisoner and he can extract information from something which he can see. We can never see and have never felt the phase in our living world. However in the quantum world, it is a carrier of information and plays an important role in processing information. How we control this carrier, in other words, how we should use a series of unitary transforms as a device to extract information from the carrier is the most important to extract information from a qubit as much as possible and devising the series of unitary transform is equivalent to designing the quantum algorithm.

References

[1] Jiangfeng Du, Hui Li, Xiaodong Xu, Mingjun Shi, Xianyi Zhou, and Rongdian Han. Multi-player and multi-choice quantum game. Los Alamos e-print archive quant-ph/0010092, 2001.

[2] Jens Eisert, Martin Wilkens, and Maciej Lewenstein. Quantum games and quantum strategies. Los Alamos e-print archive quant-ph/9806088, 1999.

[3] Jozef Gruska. *Quantum Computing*. McGraw-Hill, 1999.

[4] William Poundstone. *Prisoner's Dilemma/John Von Neumann, Game Theory and the Puzzle of the Bomb*. Doubleday, 1992.