Two Bit Quantum Protocol for a Three Party Modular Function

Bhagaban Swain
Department of Information Technology
Assam University,
Silchar

Sudipta Roy
Department of Information Technology
Assam University,
Silchar

ABSTRACT
Communicational complexity problem among three parties for the calculation of a three party inner product modular function is discussed, where each party possess some of the function's input. Classical communicational complexity of this function can be evaluated by three classical bits. In classical theory, the three party modular function can't be evaluated by two classical bits, but using quantum entanglement in quantum theory two classical bits are sufficient to calculate the three party problem.

Keywords
Theoretical Computer Science, Communicational complexity, Quantum Computing.

1. INTRODUCTION
Entanglement [1] [2] is the most distinctive feature of quantum physics with respect to classical world. It provides powerful computation, establishes secure communication, maximize the classical channel capacity [3] (called entangled-assistant classical capacity) and also reduces the communicational complexity in a distributed system as compared to the classical theory.

Bhurman, Cleave and Van Dam [4] discussed two-party quantum communicational complexity (QCC) problem, where the value of a particular function is calculated with high probability of success as compared to classical theory Brukner, Cleave, Zukowski and Zeilinger [5] discussed a two-party QCC problem for qutrit system. Cleave and Buhrman [6] discussed a three-party problem, where the three parties receives n-bit strings x, y, z, respectively, which are subject to the condition x + y + z = 0, where the addition is modulo 2. The function $f(x, y, z) = x_1.y_1.z_1 + x_2.y_2.z_2 + \ldots + x_n.y_n.z_n$ is evaluated by one of the party with two classical bits of communication. In this paper a three-party QCC problem is discussed and solved using a new function.

Alice, Bob and Carol are considered here as three parties in a distributed computer system. Each of them are given n bits of binary string $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ and $z = (z_1, z_2, \ldots, z_n)$, respectively. Let x_i, y_i and z_i are the Alice, Bob and Carol bits respectively, where i = 1, 2, . . . n. The condition on their binary string is

$$x_i + y_i + z_i = 0 \quad (1)$$

The aim is to calculate the function $f(x_i, y_i, z_i)$ given as

$$f(x, y, z) = \Sigma_i \; |x_i - y_i| . |x_i - z_i| \quad (2)$$

with the condition as given in equation(1) where addition is modulo 2.

Here Alice will calculate the value of the function. The function has a binary value 0 or 1. Without quantum entanglement, i.e. by classical theory, three classical bits are communicated to Alice in order to calculate the value of the function. Using quantum theory, i.e., by prior quantum entanglement Alice can calculate the function by two classical bits communicated to her.

The organization of the paper is as below:

1. In section 2, Two bit quantum protocol is discussed to

solve the problem function.

2. The solution of the problem function by three bits classical protocol is discussed in section 3.
3. The solution of the problem function is not possible by two bit classical protocol and is discussed in section 4.
4. Conclusion is discussed in section 5.

2. TWO BIT QUANTUM PROTOCOL
If Alice, Bob and Carol initially share n entangled qubits, then there should be a protocol in which Bob and Carol both send one classical bit to Alice, which enables Alice to determine the binary value of the function f(x, y, z) as defined by equation (2) with the condition defined by equation (1). The entangled involve 3n qubits and each party having n of them. The shared entangled qubits are in the quantum state $1/2(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$. Here first qubit is Alice's, second one is Bob's and third one is Carol's. Let the n qubits of Alice, Bob and Carol are $(A_1,A_2, \ldots ,A_n)$, $(B_1,B_2, \ldots .B_n)$ and $(C_1,C_2, \ldots .C_n)$ respectively. The input strings of Alice, Bob and Carol are $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ and $z = (z_1, z_2, \ldots, z_n)$ respectively. The Protocol is given bellow.

Protocol for Alice

1. for $i \leftarrow 1$ to n
2. do if $x_i = 1$
3. then
4. apply Hadamard transformation H to A_i
5. else
6. do nothing i.e., apply I to her own qubit
7. measure the qubit A_i producing the bit S_{A_i}
8. Calculate $S_A = \overline{S}_{A_1} + \overline{S}_{AB_2} + \cdots + \overline{S}_{A_n}$

Protocol for Bob

1. for $i \leftarrow 1$ to n
2. do if $y_i = 1$
3. then
4. apply rotation $R(\pi/4)$ to B_i
5. else
6. do nothing i.e., apply I to his own qubit
7. measure the qubit B_i producing the bit S_{B_i}
8. Calculate $S_B = \overline{S}_{B_1} + \overline{S}_{B_2} + \cdots + \overline{S}_{B_n}$

Protocol for Carol

1. for $i \leftarrow 1$ to n
2. do if $z_i = 1$
3. then
4. apply rotation $R(\pi/4)$ to C_i
5. else
6. do nothing i.e., apply I to his own qubit
7. measure the qubit C_i producing the bit S_{C_i}
8. Calculate $S_C = \overline{S}_{C_1} + \overline{S}_{C_2} + \cdots + \overline{S}_{C_n}$

Here I is the identity operator, and *H* is the Hadamard Unitary transformation

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

It acts on basis vector as

$$\mathrm{H}|0\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

and

$$\mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The rotational operator R(π/4) is given as

$$R(\pi/4) = \begin{pmatrix} \cos(\pi/4) & -\sin(\pi/4) \\ \sin(\pi/4) & \cos(\pi/4) \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

$$R(\pi/4)|0\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle))$$

and

$$R(\pi/4)|0\rangle = \tfrac{1}{\sqrt{2}}(-|0\rangle + |1\rangle))$$

Now, under the condition given in equation (1) the possible input $x_i\, y_i z_i \in \{000, 011, 101, 110\}$. In the 000 case no unitary transformation is applied The final state in this case is same as initial state $1/2(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$. The equation $f(x_i, y_i, z_i) = S_A + S_B + S_C = S_{A_i} + S_{B_i} + S_{C_i}$ is satisfied by all four possible states.

In the case 101 Alice will apply Hadamard transformation *H*, Bob will apply *I* and Carol will apply $R(\pi/4)$. So the whole system is changed under the transformation $H \otimes I \otimes R(\pi/4)$. Hence the final state of the system is:

$$\begin{aligned}
\mathrm{H} \otimes \mathrm{I} \otimes \mathrm{R}(\pi/4)\, 1/2(|000\rangle - |011\rangle - |101\rangle - |110\rangle) \\
&= \frac{1}{2}\Big\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle \\
&+ |1\rangle) - \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle \otimes \frac{1}{\sqrt{2}}(-|0\rangle \\
&+ |1\rangle) - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle \otimes \frac{1}{\sqrt{2}}(-|0\rangle \\
&+ |1\rangle) - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |1\rangle \\
&\otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\Big\} \\
&= \frac{1}{4}\{|000\rangle + |001\rangle + |100\rangle + |101\rangle \\
&+ |010\rangle - |011\rangle + |110\rangle - |111\rangle + |000\rangle \\
&- |001\rangle - |100\rangle + |101\rangle - |010\rangle - |011\rangle \\
&+ |110\rangle + |111\rangle\} \\
&= 1/2(|000\rangle + |110\rangle + |101\rangle - |011\rangle)
\end{aligned}$$

Here all the four possible states satisfy the equation $f(x_i, y_i, z_i) = S_A + S_B + S_C$. The case 110 is symmetric to case 101

In the case 011 Alice will apply I, Bob will apply $R(\pi/4)$ transformation to his qubit and Carol will apply $R(\pi/4)$ transformation to his qubit. So, the whole system is changed under the unitary transformation $I \otimes R(\pi/4) \otimes R(\pi/4)$. Hence, the final state of the system is:

$$\begin{aligned}
\mathrm{I} \otimes \mathrm{R}(\pi/4) \otimes \mathrm{R}(\pi/4)\, 1/2(|000\rangle - |011\rangle - |101\rangle \\
- |110\rangle) \\
&= \frac{1}{2}\Big\{|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle \\
&+ |1\rangle) - |0\rangle \otimes \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) \\
&\otimes \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) - |1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle \\
&+ |1\rangle) \otimes \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) - |1\rangle \\
&\otimes \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\Big\} \\
&= \frac{1}{4}\{|000\rangle + |001\rangle + |010\rangle + |011\rangle \\
&- |000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle \\
&- |101\rangle + |110\rangle - |111\rangle + |100\rangle + |101\rangle \\
&- |110\rangle - |111\rangle\} \\
&= 1/2(|001\rangle + |010\rangle + |100\rangle - |111\rangle)
\end{aligned}$$

Here again all the four possible states satisfying the equation $f(x_i, y_i, z_i) = S_A + S_B + S_C$.
Hence, Bob will give S_B and Carol will give S_C and finally Alice will calculate the value of the function $f(x, y, z) = S_A + S_B + S_C$. Hence, a two bit quantum protocol is sufficient to calculate the value of the function.

3. THRE BIT CLASSICAL PROTOCOL

It can be proved that three bit classical protocol is able to calculate the function given by equation (2) with the condition given by equation (1).The theoretical intuition is given as:

They can easily calculate the value of the function, if they can know how many ones are used to produce the function $|x_i - y_i|.|x_i - z_i|$ as one. Let m be the number generated by dividing the number of ones used to produce the function $|x_i - y_i|.|x_i - z_i|$ as one by 2. If m is even then the value of the function *f(x, y, z)* is zero otherwise the value of f(x, y, z) is one. Now from the four possible values of the input, Bob and Carol will conform that for their zero input the function $|x_i - y_i|.|x_i - z_i|$ will be zero and for their one input the value of the function $|x_i - y_i|.|x_i - z_i|$ may be zero or one. Hence Bob and Carol will calculate and send all their number of ones assuming that these ones are producing one. Let *a* be the number of one inputs of Alice. But Alice already knows that *a* numbers of ones that both Bob and Carol send to her which are not producing one. Let *b* is the total number of one inputs of both Bob and Carol. The actual number of ones that are producing the function $|x_i - y_i|.|x_i - z_i|$ as one is $k = |b - a|$. Hence, Alice calculates the value of *k*, by which she can easily calculate the value of the function *f(x, y, z)*.

Therefore, in order to send the total number of ones Bob and Carol each will send $log_2 n$ number of bits to Alice. They together will send at most $2log_2 n$ number of bits. Since Alice wants the parity of *m*, only needs the value of *b* in modulo 4 arithmetic. Thus, Bob and carol each will send the two bits taking modulo 4 to his calculated number of ones, instead of $log_2 n$ bits. Alice also calculates the value of *a* by taking modulo 4 to her total number of ones. Again, if *a* is odd, then *b* is odd or if *a* is even, then *b* is even. If any one of them(Bob or Carol) will send his lower bit, then Alice must able to know the lower bit of other. Hence one from Bob or Carol will send his/her higher bit and other one will send both the bits to Alice. Hence, both Bob and Carol together send three bits to Alice so that Alice can easily calculate the value of the function *f(x, y, z)*. So, three bit classical protocol is able to calculate the function.

4. NON-EXISTANCE OF TWO BIT CLASSICAL PROTOCOL

Now, in the case where n = 3 without the use of entangled quantum particle two bits of communication among Alice, Bob and Carol is insufficient to Alice to calculate the valve of the function *f(x, y, z)* [6]

For this two bit protocol if Alice is sending any bit, the function will be a two-party function. The other possibilities are

1) Bob and Carol each will send one bit to Alice
2) Bob will broadcast one bit, then Carol will send one bit to Alice
3) Carol will broadcast one bit, then Bob will send one bit to Alice.

Let, at first Bob broadcasts his bit *y*. The bit that is broadcasted by Bob can be defined by the function $y = \phi : \{1, 0\}^3 \rightarrow \{1, 0\}$.The function ϕ partitions *{0, 1}* into two classes $\phi^{-1}(0)$ and $\phi^{-1}(1)$. These two classes can be called as s_0 and s_1 respectively, and without loss of generality, it is assumed that $000 \in s_0$. Now, Carol gets y and he will broadcast one bit *z* which may depend only on his inputs or Bob's broadcast bit and his inputs. After Alice getting Bob's bit and Carol's bit, she will produce the result. Since the function is a binary function she wants to divide each party's inputs into binary partition.

Let, first Alice partitioning Bob's inputs, and no input condition (equation(1)) is required. Now, there are seven possible cases where Alice can partition Bob's inputs. In each case She will partition Carol's possible (satisfying input condition (1)) inputs. But in all cases she will be failure and hence can't calculate the value of f(x, y, z) . If she want to partition Bob inputs after partitioning Carol inputs, then she will take the Bob's possible inputs satisfying equation (1). There is no difference in partitioning Bob's or Carol's inputs first.

Case 1 $(|s_0| \leq 2)$: In the convention that $000 \in s_0$ if there is a second element then by symmetric it is either 100, 110 or 111. Hence, 001, 010, $011 \in s_1$. Now Alice will do binary partition to Carol inputs. Let $y \in s_1$, when Alice inputs are 010.So the possible values of (x_i, y_i, z_i) are (010, 001, 011), (010, 010, 000), (010, 011, 001) and the respective values of f is 1, 0, 1. In order the protocol to be right, Alice decided that (011) and (001) of Carol's inputs set in same category. When Alice has input (000) now the possible values of (x_i, y_i, z_i) are (000, 001, 001), (000, 010, 010), (000, 011, 011) and the respective values of f is 1, 1, 0. In order the protocol to be right Alice must take (011) and (001) of Carol's inputs set in different categories. This generates the contradiction. Thus, Alice can't divide Carol's possible inputs into binary partition. Hence Alice can't calculate the value of the function exactly.

Case 2 $(|s_0| \geq 2)$: For this case consider the sub cases where s_0 contains a string of weight one or does not.

case 2.1 (s_0 contains a string of weight one) : $(000) \in$ s0 without loss of generality $001 \in s_0$, the possible third element of s0 are 010, 011, 110 and 111, the possible cases are consider below.

case 2.1.1 (000, 001, $010 \in s_0$) : Now Alice will do binary partition to Carol's inputs. Let $y \in$ s0, when Alice input is 010 now the possible values of (x_i, y_i, z_i) are (010, 000, 010), (010, 001, 011), (010, 010, 000) and the respective values of f is 0, 1, 0. In order the protocol to be right Alice decided that (010) and (000) of Carol's inputs set in same category. When Alice has input is (000) now the possible values of (x_i, y_i, z_i) are (000, 000, 000), (000, 001, 001), (000, 010, 010) and the respective values of f is 0, 1, 1. In order the protocol to be right Alice must take (010) and (000) of Carol's inputs set in different categories. Which is a contradiction.

case 2.1.2 (000, 001, $011 \in s_0$) : Now Alice will do binary partition to Carol's inputs. Let $y \in s_0$, when Alice input is 010 now the possible values of (x_i, y_i, z_i) are (010, 000, 010), (010, 001, 011), (010, 011, 001) and the respective values of f is 0, 1, 1. In order the protocol to be right Alice decided that (011) and (001) of Carol's inputs set in same category. When Alice has input (000) now the possible values of (x_i, y_i, z_i) are (000, 000, 000), (000, 001, 001), (000, 011, 011) and the respective values of f is 0, 1, 0. In order the protocol to be right Alice must take (001)and (011) of Carol's inputs set in different categories. Which is a contradiction.

case 2.1.3 (000, 001, $110 \in s_0$) : Now Alice will do binary partition to Carol inputs let $y \in s_0$, when Alice input is 101 now the possible values of (x_i, y_i, z_i) are (101, 000, 101), (101, 001,

100), (101, 110, 011) and the respective values of f is 0, 0, 1 in order the protocol to be right Alice decided that (101) and (100) of Carol's inputs set in one category But when Alice has input (100) now the possible values of (x_i, y_i, z_i) are (100, 001, 101), (100, 000, 100), (100, 110, 010)and the respective values of f is 0, 1, 0 in order the protocol to be right Alice must take (101) and (100) of Carol's inputs set in different categories. Which is a contradiction.

case 2.1.4 (000, 001, $111 \in s_0$) : Now Alice will do binary partition to Carol inputs let y∈ s0, when Alice input is 101 now the possible values of (x_i, y_i, z_i) are (101, 000, 101), (101, 001, 100), (101, 111, 010)and the respective values of f is 0, 0, 1. In order the protocol to be right Alice decided that (101) and (100) of Carol's input set in one category . When Alice has inputs (100), now the possible values of (x_i, y_i, z_i) are (100, 001, 101), (1000, 000, 100), (100, 111, 011) and the respective values of f is 1, 0, 0. In order the protocol to be right Alice must take (101) and (100) of Carol's inputs set in different categories. Which is a contradiction.

case 2.2 ($|s_0|$ contains no string of weight 1) : The following sub cases are considered:

case 2.2.1 ($111 \in s_0$) : In this case 000, 011, $111 \in s_0$. Now Alice will do binary partition to Carol inputs. Let y∈ s0, when Alice input is 010 now the possible values of (x_i, y_i, z_i) are (010, 000, 010), (010, 011, 001), (010, 111, 101) and the respective values of f is 0, 1, 0. In order the protocol to be right Alice decided that (101) and (010) of Carol's inputs set in same category. When Alice has input (101) , the possible values of (x_i, y_i, z_i) are (101, 000, 101), (101, 011, 110), (101, 111, 010) and the respective values of f is 0, 1, 1. In order the protocol to be right Alice must take (101) and (010) of Carol's inputs set in different categories. Which is a contradiction.

case 2.2.2 ($111 \notin s_0$) : In this case 011, 010, 100, $111 \in s_1$. Now Alice will do binary partition to Carol's inputs. Let y∈ s1, when Alice input is 010, possible values of (x_i, y_i, z_i) are (010, 011, 001), (010, 010, 000), (010, 100, 110) and (010, 111, 101) the respective values of f is 1,0, 1, 0. In order the protocol to be right Alice decided that (001) and (110) of Carol's input set in same category. When Alice has inputs (101) now the possible values of (x_i, y_i, z_i) are (101, 011, 110), (101, 010, 111) , (101, 100, 001), (101, 111, 010) and the respective values of f is 1, 1, 0, 1. In order the protocol to be right Alice must take (110) and (001) of Carol's inputs set in different categories. Which is a contradiction again.

In all the possible cases it is impossible for Alice to calculate the value of f(x, y, z) using two bit classical protocol. Hence Two bit protocol for this function doesn't exit.

5. CONCLUSION

For three party communication two bit quantum protocol is sufficient where as in classical protocol 3 bits communication are necessary. 2 bit classical protocol among 3 parties are not possible at all.

These observations are proved in this paper using a new problem function and their corresponding two bit quantum protocol and three bit classical protocol.

6. REFERENCES

[1] Einstein, A., Prodolsky, B., and Rosen, N. 1935. Can quantum mechanical description of physical reality be considered complete?

[2] Bell, J. S. 1964. On the einstein-podolsky-rosen paradox.

[3] Benne, C. H. and Wiesner, S. J. 1992. . Communication via one and two-particle operators on einstein-podolsky-rosen states.

[4] Buhrman, H., Cleve, R. and Dam, W. V. 1997. Quantum Entanglement and Communication Complexity, arxiv:quant-ph/9705033.

[5] Bruknerand , C., Zukowski, M. and Zeilinger, A. 2002 Quantum communication complexity protocol with two entangled qutrits.

[6] Cleve, R. and Buhrman, H. 1997. Substituting quantum entanglement for communication.