Quantum Algorithm for Appointment Scheduling

Wenbin Yu[1, 2, 3, *], Yinsong Xu[1, 2, 3], Wenjie Liu[1, 2, 3], Alex Xiangyang Liu[4] and Baoyu Zheng[5]

Abstract: Suppose a practical scene that when two or more parties want to schedule an appointment, they need to share their calendars with each other in order to make it possible. According to the present result the whole communication cost to solve this problem should be their calendars' length by using a classical algorithm. In this work, we investigate the appointment schedule issue made by N users and try to accomplish it in quantum information case. Our study shows that the total communication cost will be quadratic times smaller than the conventional case if we apply a quantum algorithm in the appointment-scheduling problem.

Keywords: Quantum algorithm, appointment scheduling, quantum speed-up.

1 Introduction

Communication complexity mainly deals with the following problems: Two independent parties want to calculate a common task based on their input, and make the communication between them as little as possible. This model was first proposed by Yao [Yao (1979)]. Subsequent studies show that the communication complexity of some bilateral and tripartite computational problems will be reduced when quantum computing and communication are allowed, which is proved impossible by classical algorithms [Yao (1993); Brassard (2003)]. In addition, in the field of quantum algorithm research, Shor [Shor (1997)] proposed a quantum algorithm for decomposition of large number prime factors, which transformed the classical NP problem into P problem.

Grover [Grover (1996, 1998, 2005)] proposed that the quadratic polynomial acceleration of classical algorithms could be achieved by applying quantum mechanism to the search

[1] Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology, Nanjing University of Information Science & Technology, Nanjing, 210044, China.

[2] Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing, 210044, China.

[3] School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, 210044, China.

[4] Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824-1266, USA.

[5] National Engineering Research Center for Communications and Network Technology, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China.

[*] Corresponding Author: Wenbin Yu. Email: ywb1518@126.com.

JQC. doi:10.32604/jqc.2019.07412

of disordered databases. This algorithm is studied in Høyer et al. [Høyer (2000); Mosca (1998); Younes, Rowe and Miller (2003); Younes, Rowe and Miller (2004)], and various improved algorithms under specific conditions are given. Subsequently, a series of novel quantum methods have been proposed [Liu, Wang, Yuan et al. (2016); Liu, Gao, Yu et al. (2018); Liu, Xu, Yang et al. (2018); Liu, Chen, Liu et al. (2018); Qu, Wu, Wang et al. (2017); Qu, Zhu, Wang et al. (2018); Qu, Li, Xu et al. (2019); Qu, Cheng and Wang (2019); Wang, Yang and Mousoli (2018)].

At present, the research on the complexity of quantum communication begins to go deep into multi-party Computation (MPC) [Shakshuki, Koo, Benoit et al. (2008); Wang, Venkataraman, Wang et al. (2009); Han, Kim, Choi et al. (2007)].

Here we consider the following multi-user computing model with arbitrary number of users. A calendar is a tool commonly used in people's daily life. Many people use different ways or tools to remind themselves of upcoming appointments. The determination of itinerary requires users to agree on their respective schedules in order to have the right time to participate in common affairs. The process of user multi-party pre-negotiation and schedule determination can be seen as a typical multi-party Dating (MPD) problem. Han et al. [Han, Kim, Choi et al. (2007)] gives some application models and performance improvements on MPD in classical communication.

In this paper, we study the classical communication complexity and quantum communication complexity of MPD without sharing any information resources shared in advance.

2 The multi-party dating based on the composite Boolean-valued function

We describe the MPD model based on the composite Boolean-valued function. Supposing that there are K users, marked as user 1 to user K, provided with the function

$$\begin{cases} user1: & y_1 = g_1(x) \\ user2: & y_2 = g_2(x) \\ \vdots & \vdots \\ userK: & y_K = g_K(x) \end{cases} \tag{1}$$

in turn. The kth user wants to compute the function $g_k(x)$, $1 \le k \le K$. The function $\{g_k(x)|1 \le k \le K\}$ could be arbitrary function in the application, but only satisfying that they share the same function domain and codomain. Besides, denote the function $F(y_1, y_2, \cdots, y_K)$ as an arbitrary K-ary Boolean-valued function, only to satisfy that $F(y_1, y_2, \cdots, y_K) \in \{0,1\}$ and $y_k = g_k(x)$, $1 \le k \le K$.

Without loss of generality, denote the domain of function $g_k(x)$ as $\boldsymbol{X} = \{x|0 \le x \le N-1, x \in \mathbb{Z}\}$, the length of X is N. For the convenience let N be an integer that satisfies $N = 2^n$ (As for the case of $2^n < N < 2^{n+1}$, simply have $N = 2^{n+1}$, the expanded part of X does not influence on the solving of the problem), therefore it is feasible to use the length of $n = \log N$ bits information to describe the function domain. And similarly, supposing that the codomain of $g_k(x)$ is $\boldsymbol{Y} = \{y|0 \le y \le H-1, y \in \mathbb{Z}\}$, and the length to store the codomain information is $h = \log H$ bits. So we have

$$g_k(x): \boldsymbol{X} \to \boldsymbol{Y} \tag{2}$$

$$F(y_1, y_2, \cdots, y_K): \boldsymbol{Y}^K \to \{0,1\} \tag{3}$$

$$F\big(g_1(x), g_2(x), \cdots, g_K(x)\big): \boldsymbol{X} \to \{0,1\} \tag{4}$$

In summary, the goal of our research on the multiparty computation task is to find a solution x to equation $F\big(g_1(x), g_2(x), \cdots, g_K(x)\big) = 1$ by comparing the results of K arbitrary functions $\{g_k(x) | 1 \leq k \leq K\}$ calculation held by the multi-users.

3 Method: the distributed Oracle operator and quantum distributed algorithm

Based on the foregoing MPD model, we construct the quantum distributed (QD) algorithm with distributed Oracle operator (DOO) and Grover's iteration [Grover (1996)].

3.1 The function and operator definitions related to the QD Algorithm

The initialization of the algorithm starts with user 1. First, user 1 needs to prepare an n qubits state $|0\rangle^{\otimes n}$, then apply the Hadamard transformation $\boldsymbol{H}^{\otimes n}$ on it, which will make the n qubits at an uniform superposition state $|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$. Quantum state $|\Psi\rangle$ is used to save the N values of the user function domain, where $|x\rangle = |0\rangle, |1\rangle, \cdots, |N-1\rangle$ are the N eigenstates corresponding to the indices of the N values in the function domain. The quantum state $|\Psi\rangle$ is the initial input of user 1, the h qubits $|g_k(x)\rangle$ is used to save the calculated message about x for the kth user.

Second, define the quantum state sequence $\{|\varphi_k\rangle | 1 \leq k \leq K\}$ and $\{|\psi_k\rangle | 1 \leq k \leq K\}$, where

$$|\varphi_k\rangle = |x\rangle |g_1(x)\rangle |g_2(x)\rangle \cdots |g_{k-1}(x)\rangle \tag{5}$$

$$|\psi_k\rangle = |x\rangle |g_1(x)\rangle |g_2(x)\rangle \cdots |g_{K-k}(x)\rangle \tag{6}$$

It can be seen that $|\varphi_k\rangle$ and $|\psi_k\rangle$ are $n + (k-1)h$ and $n + (K-k)h$ qubits respectively. Especially we have $|\varphi_1\rangle = |x\rangle$ when $k = 1$ and $|\psi_K\rangle = |x\rangle$ when $k = K$, both of which are of n qubits length.

Moreover, define the unitary operator sequence $\{\boldsymbol{U}_k | 1 \leq k \leq K-1\}$, where $\boldsymbol{U}_k$ is a $n + kh$ dimensional operator.

It is used to operate on the last qubit of the input states, add it to $g_k(x)$ with the mod H. Especially when $k = 1$, $\boldsymbol{U}_1$ is an n dimensional unitary operator.

It can be verified that the operator $\boldsymbol{U}_k$ is a reversible unitary transformation, and the reversible operator of $\boldsymbol{U}_k$ satisfies the condition $\boldsymbol{U}_k^{-1} = \boldsymbol{U}_k^{H-1}$. The same type of operators with $\boldsymbol{U}_k$ is applied in the Deutsch-Jozsa algorithm once. In the quantum computation, the quantum calculation circuits which satisfy the reversible transformation condition are proved to be physically realizable.

Still, define the $n + (k-1)h$ dimensional unitary operator Oracle, which is an expansion of the Oracle operator in the Grover's quantum search algorithm [Grover (1996)], that is

$$|x\rangle |g_1(x)\rangle |g_2(x)\rangle \cdots |g_{K-1}(x)\rangle \xrightarrow{Oracle} (-1)^{F(g_1(x), g_2(x), \cdots, g_K(x))} |x\rangle |g_1(x)\rangle |g_2(x)\rangle \cdots |g_{K-1}(x)\rangle \tag{7}$$

Obviously, the Oracle operator is unitary as well as reversible, therefore is physically realizable.

Finally, apply the operator sequence $\{\boldsymbol{U}_k | 1 \leq k \leq K-1\}$ and operator Oracle we defined to the quantum state sequence $\{|\varphi_k\rangle | 1 \leq k \leq K\}$ and $\{|\psi_k\rangle | 1 \leq k \leq K\}$, then there are

$$|\varphi_k\rangle |0\rangle^{\otimes h} \overset{\boldsymbol{U}_k}{\to} |\varphi_{k+1}\rangle \tag{8}$$

$$|\psi_k\rangle \xrightarrow{\boldsymbol{U}_{K-k}^{H-1}} |\psi_{k+1}\rangle|0\rangle^{\otimes h} \tag{9}$$

$$|\varphi_K\rangle \xrightarrow{Oracle} |\psi_1\rangle \tag{10}$$

We separate the DOO algorithm into three phases. Phase 1 is a forward communication process from user 1 to user *K*. During this phase, every user applies the unitary operator in the sequence $\{\boldsymbol{U}_k|1 \le k \le K-1\}$ to the quantum states in the sequence $\{|\varphi_k\rangle|1 \le k \le K\}$ in order, and transfers the result to the next user one by one. Therefore, the result of each user's calculation will finally be transferred to user *K*.

In the second phase, user *K* applies the Oracle operator to quantum state $|\varphi_K\rangle$ and gets the quantum state $|\psi_1\rangle$. Meanwhile, all the quantum states corresponding to the solution of the MPD model will get a phase reverse, so that the solution can be marked.

The third phase is the reverse communication process from user *K* to user 1. Every user applies the unitary operator in the sequence $\{\boldsymbol{U}_k^{-1}|1 \le k \le K-1\}$ to the quantum states in the sequence $\{|\psi_k\rangle|1 \le k \le K\}$ in turn, and transfers the result to the next user, then the quantum states carrying the solution mark will be delivered to user 1. So the entire process of DOO algorithm is as follows.

3.1.1 DOO algorithm

(1) The forward communication phase from user 1 to user *K*.

Step 1: The initial input is that user 1 receives the quantum state $|\varphi_1\rangle$.

Step 2: The current user receives quantum state $|\varphi_K\rangle$, then adds *h* qubits $|0\rangle^{\otimes h}$ to its last qubit as the auxiliary quantum state.

Step 3: The current user applies operator $\boldsymbol{U}_k$ to the outcome of Step 2 to get quantum state $|\varphi_{k+1}\rangle$.

Step 4: The current user transfers quantum state $|\varphi_{k+1}\rangle$ to the next user.

Step 5: The next user goes to Step 2 to start. Repeating this process till the quantum state $|\varphi_K\rangle$ is transferred to the last user *K*.

(2) User K executes the Oracle operator on the received quantum state $|\varphi_K\rangle$, gets state $|\psi_1\rangle$. Sends $|\psi_1\rangle$ to user $K-1$.

(3) The backward communication phase from user $K-1$ to user 1

Step 1: The initial input is that user $K-1$ receives the quantum state $|\psi_1\rangle$.

Step 2: The current user receives the quantum state $|\psi_k\rangle$, applies the operator $\boldsymbol{U}_{K-k}^{-1}$ to it and gets state $|\psi_{k+1}\rangle|0\rangle^{\otimes h}$.

Step 3: The current user removes the last h qubits $|0\rangle^{\otimes h}$ from the quantum state $|\psi_{k+1}\rangle|0\rangle^{\otimes h}$ and gets the state $|\psi_{k+1}\rangle$.

Step 4: The current user sends $|\psi_{k+1}\rangle$ to the previous user.

Step 5: The previous user goes to Step 2 and start operating. Repeating this process till the quantum state $|\psi_{K-1}\rangle$ is transferred to user 1.

Step 6: User 1 gets the quantum state $|\psi_{K-1}\rangle$, applies the operator $\boldsymbol{U}_1^{-1}$ to it and gets the state $|\psi_K\rangle|0\rangle^{\otimes h}$; Then removes the last h qubits $|0\rangle^{\otimes h}$ and gets $|\psi_K\rangle$.

Algorithm ends.

3.1.2 QD algorithm

In the DOO algorithm, we take the quantum state as the information carrier. Through the process of delivering and sharing quantum states within multi users, each user executes the corresponding operation on the quantum state signal to cooperate with a joint distributed computation task. As for the MPD model, the operation the DOO algorithm performs on the input quantum state $|\varphi_1\rangle$ can be written as:

$$\mathrm{DOO}: |x\rangle \rightarrow (-1)^{F(g_1(x),g_2(x),\cdots,g_K(x))}|x\rangle. \tag{11}$$

This means when every turn of DOO algorithm is carried out, the quantum eigenstates corresponding to the solutions will get a phase reverse.

In order to implement QD algorithm, we need to apply the aforementioned DOO algorithm to the Grover iteration. Here we present one time of the Grover iteration steps:

Step 1: Applying the DOO algorithm. Check whether each value index is the solution of MPC model or not.

Step 2: Apply Hadamard transform $\boldsymbol{H}^{\otimes n}$ to the result of Step 1.

Step 3: Carry on conditional phase shift to the outcome of Step 2, so as to make every base state other than $|0\rangle$ gets -1 phase shift, i.e. $|x\rangle \rightarrow -(-1)^{\delta_{x,0}}|x\rangle$.

Step 4: Apply the Hadamard transform $\boldsymbol{H}^{\otimes n}$ to the result of Step 3.

According to the features of the Grover's algorithm, we notice that as the iteration times approach $\mathrm{O}(\sqrt{N})$ the weights of some eigenstates of the n qubits representing the function domain will grow big enough, where these eigenstates are all solutions to the MPD model. If we measure the eigenstates on the n qubits after iteration, we will obtain the solution to the problem with an ultimately large probability.

3.2 Lemma and theorems

Lemma 1: $\log_{1-2^{-K}}^{1-P}$ *and* 2^K *is of the same order of infinity.*

Proof:

$$\because \lim_{x\to+\infty}\left(\frac{\log_{1-2^{-K}}^{1-P}}{2^K}\right)=\lim_{x\to+\infty}\left(\log^{1-P}_{\left(1-2^{-K}\right)^{2^K}}\right)=-\ln\left(1-P\right) \tag{12}$$

$$\therefore O\left(\log_{1-2^{-K}}^{1-P}\right)=O\left(2^K\right) \tag{13}$$

Theorem 1: *The classical communication complexity required for the worst case of MPD is* $O\left(K\cdot 2^K\right)$.

Proof: We can conclude that the amount of information communicated in classical algorithm is

$$n\left(K-1\right)+CK=\left(K-1\right)\log_{1-2^{-K}}^{1-P}+CK\,. \tag{14}$$

where C is a constant, CK denotes the amount of ancillary communication which prepares for communication and sends back the final result.

Applying the result of Lemma 1, we obtain the communication complexity of classical algorithm to be

$$O\left(K \cdot 2^K\right). \tag{15}$$

Theorem 2: *Employing quantum algorithm, the worst case communication complexity is* $O\left(K^2\sqrt{2^K}\right)$.

Proof: One time of iteration process consists of transmission from user 1 to user K each sends a quantum state to its next one by one in turn, of which the amount of communication is $\left(K-1\right)\log N + K\left(K-1\right)/2$, and the reverse transmission phase from user K to user 1 feeding back their quantum states one by one in turn, of which the amount of communication is the same as above.

So one time of complete iteration claims the communication cost of $2\left(K-1\right)\log N + K\left(K-1\right)$.

Overall the algorithm needs iterations of $O\left(\sqrt{N}\right)$ times, henceforth, the communication complexity of quantum algorithm amounts to $O\left(\left(2\left(K-1\right)\log N + K\left(K-1\right)\right)\sqrt{N}\right)$.

Due to the conclusion of Lemma 1, it results in $O\left(K^2\sqrt{2^K}\right)$.

4 Conclusion

According to Theorem 1 and 2, we can conclude that the communication complexity of appointment scheduling is able to get $O\left(K^2\sqrt{2^K}\right)$ by using quantum algorithm, which is comprehensively lower than $O\left(K \cdot 2^K\right)$ by handling it in classical way. So we can figure that the highest speed-up made by quantum algorithm can reach the quadratic level when the users' number increases large sufficiently.

Acknowledgement: Supported by the National Natural Science Foundation of China under Grant Nos. 61501247, 61373131 and 61702277, the Six Talent Peaks Project of Jiangsu Province (Grant No. 2015-XXRJ-013), Natural Science Foundation of Jiangsu Province (Grant No. BK20171458), the Natural Science Foundation of the Higher Education Institutions of Jiangsu Province (China under Grant No. 16KJB520030), the NUIST Research Foundation for Talented Scholars under Grant No. 2015r014, PAPD and CICAEET funds.

References

Brassard, G. (2003): Quantum communication complexity. *Foundations of Physics*, vol. 33, no. 11, pp. 1593-1616.

Grover, L. (1996): A fast quantum mechanical algorithm for database search. *Proceedings* *of the 28th Annual ACM Symposium on the Theory of Computing*, pp. 212-219.

Grover, L. (1998): Quantum computers can search rapidly by using almost any transformation. *Physical Review Letters*, vol. 80, no. 19, pp. 4329-4332.

Grover, L. (2005): Fixed-point quantum search. *Physical Review Letter*, vol. 95, no. 15, pp. 150501-150507.

Han, S.; Kim, N.; Choi, K.; Kim, J. (2007): Design of multi-party meeting system for interactive collaboration. *Proceedings of the 2nd International Conference on Communication Systems Software and Middleware*, pp. 1-8.

Høyer, P. (2000): On arbitrary phases in quantum amplitude amplification. *Physical Review A*, vol. 62, no. 5, pp. 052304-052309.

Liu, W.; Chen, Z.; Liu, J.; Su, Z.; Chi, L. (2018): Full-blind delegating private quantum computation. *Computers, Materials & Continua*, vol. 56, no. 2, pp. 211-223.

Liu, W.; Gao, P.; Yu, W.; Qu, Z.; Yang, C. (2018): Quantum relief algorithm. *Quantum Information Processing*, vol. 17, no. 10, pp. 1-15.

Liu, W.; Wang, H.; Yuan, G.; Xu, Y.; Chen, Z. et al. (2016): Multiparty quantum sealed-bid auction using single photons as message carrier. *Quantum Information Processing*, vol. 15, no. 2, pp. 869-879.

Liu, W.; Xu, Y.; Yang, C.; Gao, P.; Yu, W. (2018): An efficient and secure arbitrary n-party quantum key agreement protocol using Bell states. *International Journal of Theoretical Physics*, vol. 57, no. 1, pp. 195-207.

Mosca, M. (1998): Quantum searching, counting and amplitude amplification by eigenvector analysis. *Proceedings of Randomized Algorithms, Workshop of Mathematical Foundations of Computer Science*, pp. 90-100.

Qu, Z.; Cheng, Z.; Wang, X. (2019): Matrix coding-based quantum image steganography algorithm. *IEEE Access*, vol. 7, pp. 35684-35698.

Qu, Z.; Li, Z.; Xu, G.; Wu, S.; Wang, X. (2019): Quantum image steganography protocol based on quantum image expansion and Grover search algorithm. *IEEE Access*, vol. 7, pp. 50849-50857.

Qu, Z.; Wu, S.; Wang, M.; Sun, L.; Wang, X. (2017): Effect of quantum noise on deterministic remote state preparation of an arbitrary two-particle state via various quantum entangled channels. *Quantum Information Processing*, vol. 16, no. 306, pp. 1-25.

Qu, Z.; Zhu, Z.; Wang, J.; Wang, X. (2018): A novel quantum steganography based on brown states. *Computers, Materials & Continua*, vol. 56, no. 1, pp. 47-59.

Shor, P. W. (1997): Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal of Computer*, vol. 26, no. 5, pp. 1484-1590.

Shakshuki, E.; Koo, H.; Benoit, D.; Silver, D. (2008): A distributed multi-agent meeting scheduler. *Journal of Computer and System Sciences*, vol. 74, no. 2, pp. 279-296.

Wang, D.; Venkataraman, V.; Wang, Z.; Qin, W.; Wang, H. et al. (2009): Accelerating multi-party scheduling for transaction-level modeling. *Proceedings of the 19th ACM Great Lakes Symposium on VLSI*, pp. 339-344.

Wang, M.; Yang, C.; Mousoli, R. (2018): Controlled cyclic remote state preparation of arbitrary qubit states. *Computers, Materials & Continua*, vol. 55, no. 2, pp. 321-329.

Yao, A. C. (1979): Some complexity questions related to distributed computing. *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*, pp. 209-213.

Yao, A. C. (1993): Quantum circuit complexity. *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, pp. 352-361.

Younes, A.; Rowe, J.; Miller, J. (2003): A hybrid quantum search engine: a fast quantum algorithm for multiple matches. *Proceedings of the 2nd International Computer Engineering Conference*. https://arxiv.org/abs/quant-ph/0311171.

Younes, A.; Rowe, J.; Miller, J. (2004): Quantum search algorithm with more reliable behaviour using partial diffusion. *Proceedings of the 7th International Conference on Quantum Communication, Measurement and Computing*, vol. 734, no. 1, pp. 171-174.