arXiv:2301.00370v2 [quant-ph] 9 Jan 2023

量子通信复杂度中对称谓词的匹配上界

Daiki Suruga *

2023年1月10日

摘要

本文聚焦于如下形式的函数的量子通信复杂度：$f \circ G = f(G(X_1, Y_1) \ldots, G(X_n, Y_n))$，其中 f：$\{0,1\}^n \to \{0,1\}$ 是对称函数，G：$\{0,1\}^j \times \{0,1\}^k \to \{0,1\}$ 是任意函数；Alice（分别地，Bob）获得 $(X_i)_{i \le n}$（分别地，$(Y_i)_{i \le n}$）。最近，Chakraborty 等人在 [STACS 2022]中证明，当双方可以使用共享纠缠时，$f \circ G$ 的量子通信复杂度为 $O(Q(f)\mathrm{QCC}_{\mathrm{E}}(G))$，其中 $Q(f)$是 f 的查询复杂度，而 $\mathrm{QCC}_{\mathrm{E}}(G)$是 G的精确通信复杂度。本文首先证明，相同结论在 *without shared entanglement* 下也成立，从而推广了他们的结果。基于这一改进结果，我们进一步给出任意对称函数 f 的 $f \circ$与$_2$ 的紧上界，其中 AND_2：$\{0,1\} \times \{0,1\} \to \{0,1\}$ 表示 2 位与函数；这一结论在两种模型下均成立：有共享纠缠和无共享纠缠。这与 Razborov 在 [Izv. Math. 67(1) 145, 2003] 中证明的著名下界相匹配（当允许共享纠缠时），并改进了不允许共享纠缠时 Razborov 的下界。

1 引言

1.1 动机

通信复杂度 （经典）通信复杂度模型最初由 Yao 提出 [1]。在该模型中，有两名参与者：Alice 收到 $x \in \mathcal{X}$，Bob 收到 $y \in \mathcal{Y}$。他们的目标是以尽可能少的通信计算一个已知函数 f：$\mathcal{X} \times \mathcal{Y} \to \{0,1\}$。由于结构简单，通信复杂度问题的下界和上界可应用于许多其他领域，例如超大规模集成电路设计、电路复杂度、数据结构等。（优秀的参考资料见 [2, 3] 。）自通信复杂度提出以来，已有许多研究对其进行了探讨。

在通信复杂度领域，集合不相交问题（DISJ$_n(x,y) = \neg \bigvee_{i \le n} x_i \wedge y_i$）、相等性（EQ$_n(x,y) = \neg \bigwedge_{i \le n} x_i \oplus y_i$）和内积函数（IP$_n(x,y) = \bigoplus_{i \le n} x_i \wedge y_i$）是研究最广泛的三个函数。将函数 f（错误率为 $\le 1/3$）的私有随机通信复杂度记为 CC(f)，已有结果表明，CC(DISJ$_n$) = CC(IP$_n$) = $\Theta(n)$ 且 CC(EQ$_n$) = $\Theta(\log n)$。请注意，如果允许双方使用共享随机性，则 CC$^{\mathrm{pub}}$(DISJ$_n$) = CC$^{\mathrm{pub}}$(IP$_n$) = $\Theta(n)$ 且 CC$^{\mathrm{pub}}$(EQ$_n$) = $\Theta(1)$，其中 CC$^{\mathrm{pub}}(f)$ 表示函数 f 在错误率为 $\le 1/3$ 且使用共享随机性的情况下的随机通信复杂度。由 CC(EQ$_n$) $\neq$CC$^{\mathrm{pub}}$(EQ$_n$) 可知，共享随机性有时能降低通信复杂度。因此，在分析函数的通信复杂度时，我们需要仔细考虑共享随机性的影响。（请注意，如果 CC$^{\mathrm{pub}}(f)$ 严格大于 $O(\log n)$，纽曼定理 [4] 指出 CC$^{\mathrm{pub}}(f) = O(\mathrm{CC}(f))$。）

1993年，Yao [5] 提出了以经典通信复杂度模型为基础的量子通信复杂度模型。经典模型与量子模型的主要区别在于，在量子模型中，Alice 和 Bob 使用量子比特传输信息。随着量子信息科学的迅速发展，量子通信复杂度得到了广泛研究 [6, 7, 8, 9]。在量子

*名古屋大学数学研究生院

通信复杂度中，上述三个函数满足 QCC(DISJ$_n$) $=\Theta(\sqrt{n})$ [10, 11], QCC(IP$_n$) $=\Theta(n)$ [12] 以及 QCC(EQ$_n$) $=\Theta(\log\ n)$ [13] ,，其中 QCC(f) 表示函数 f 的私有量子通信复杂度。如果 Alice 和 Bob 拥有共享纠缠，则有 QCC*(DISJ$_n$) $=\Theta(\sqrt{n})$ [10, 11], QCC*(IP$_n$) $=\Theta(n)$ [12]以及 QCC*(EQ$_n$) $=\Theta(1)$ [13]，其中 QCC*(f) 表示允许使用共享纠缠时函数f的量子通信复杂度。尽管纠缠在这些例子中的作用并不显著，但谨慎处理共享纠缠十分重要，因为人们已经发现了纠缠的许多非平凡性质（例如，[14, 15, 16, 17, 9]），其中包括文献 [17]，该文表明，在共享纠缠的情况下，纽曼定理 [4] 并不成立。

复合函数 在经典和量子通信复杂度中，许多重要函数都具有如下形式

$$f\circ G:(X,Y)\mapsto f((G(X_1,Y_1)),\ldots,G(X_n,Y_n))\in\{0,1\}$$

其中 $X=(X_i)_{i\le n}\in\{0,1\}^{nj}$, $Y=(Y_i)_{i\le n}\in\{0,1\}^{nk}$, f: $\{0,1\}^n\to\{0,1\}$ 且 G: $\{0,1\}^j\times\{0,1\}^k\to\{0,1\}$。这一点已在最受广泛研究的三个函数中得到体现：集合不相交问题（¬或$_n$ ∘与$_2$）、相等性（与$_n$ ∘异或$_2$）以及内积函数（异或$_n$ ∘与$_2$）。鉴于其重要性，这类函数自然在经典和量子通信复杂度领域都得到了深入研究[18, 19, 20] 。尽管这类函数 $f\circ G$ 通常因其一般性而难以进行细致分析，但当 G 具有较简单的形式时，分析可能会变得更容易。下面详细介绍当 G 是简单函数（如与$_2$, 异或$_2$）时，量子通信复杂度的上界和下界。关于上界，Buhrman 等人 [21] 证明，当 $G\in\{$为与$_2$, 异或$_2\}$时，QCC($f\circ G$) $=O$(Q(f) log n)成立，其中 Q(f)表示函数 f的有界错误查询复杂度。应用这一结果，我们立即得到 QCC(DISJ$_n$) $=O(\sqrt{n}\log\ n)$，因为根据 Grover算法，Q(OR$_n$) $=O(\sqrt{n})$成立。这是一项重要结果，因为它表明基本函数 DISJ$_n$ 的计算效率高于经典情形（回顾一下，CC$^{\text{pub}}$(DISJ$_n$) $=\Theta(n)$）。之后，[22] 改进了这一上界 QCC(DISJ$_n$) $=O(\sqrt{n}\log\ n)$，最终由 [11]将其改进为 $O(\sqrt{n})$。参考文献 [21] 给出了关于函数 $f\circ G$的许多重要上界。另一方面，Razborov [10] 研究了 QCC*($f\circ G$)的下界，并在 f 为对称函数且 G 为与$_2$时，证明了若干紧确界。例如，参考文献 [10] 证明了 QCC*(DISJ$_n$) $=\Omega(\sqrt{n})$，以及 QCC*(IP$_n$) $=\Omega(n)$。结合 $O(\sqrt{n})$界 [11] 和 $\Omega(\sqrt{n})$界 [10]，可推出 QCC(DISJ$_n$) $=\Theta(\sqrt{n})$。我们的贡献可以视为对这些工作的推广 [21, 10, 11]。

如上所述，当函数 G 是与 $_2$ 或异或 $_2$ [21], 时，关系 QCC($f\circ G$) $=O$(Q(f) log n) 成立；随后，Aaronson 和 Ambainis [11] 将这一上界改进为 $O(\sqrt{n})$，其中 $f=$ 为或 $_n$。这意味着，对于集合不相交函数，[21] 中的 log n 因子并非必需。鉴于这一事实，我们可能会想知道，当 $G\in\{$为与 $_2$, 异或 $_2\}$ 时，任意函数是否都不需要 log n 的额外开销。Chakraborty 等人 [23] 研究了这一问题，并给出了否定答案。他们展示了一个函数 f，计算 $f\circ$ 异或 $_2$ 需要 $\Omega(Q(f)\log\ n)$ 通信。这意味着，对于一般函数，[21] 中的上界 $O(Q(f)\log\ n)$ 是紧的。有趣的是，他们随后的一项工作 [24] 推广了这一结果，并证明当 f 是对称函数时，不需要 log n 的额外开销。本文聚焦于 SYM $\circ G$ 形式的函数，其中 SYM 是一个对称函数。如下文第 1.2 节和第 1.3 节所述，我们的第一个结果推广了文献 [24]，第二个结果则给出了此类函数 SYM $\circ G$ 在 $G=$ 为与 $_2$ 时量子通信复杂度的紧确下界和上界。

1.2 首个结果：关于改进结果 [24]

如上所述，论文 [24] 证明，当我们关注对称函数 $f=$ SYM 时，$O(Q(f)\log\ n)$ 上界中的对数 n 因子并非必需。更准确地说，参考文献 [24] 证明，对于函数 SYM $\circ G$，存在一个使用共享纠缠的协议，其通信量为 $O(Q$(SYM)QCC$_E(G))$ 个通信量子比特（QCC$_E(G)$ 表示 G 的精确通信复杂度）。尽管他们的协议所需的共享纠缠量不算大，但如 [24, 备注 4]所述，在某些情况下，纠缠量会显著大于通信成本 $O(Q$(SYM)QCC$_E(G))$。因此，一般而言，他们协议中的共享纠缠不能作为通信的一部分。我们改进了他们的结果，并证明即使没有任何共享纠缠，同样的结论依然成立。也就是说，我们证明了以下定理。

定理 1. 对任意对称函数 $f\colon\ \{0,1\}^n \to \{0,1\}$ 以及任意两方函数 $G\colon\ \{0,1\}^j \times \{0,1\}^k \to \{0,1\}$,

$$\mathrm{QCC}(f \circ G) \in O(Q(f)\mathrm{QCC}_{\mathrm{E}}(G)).$$

证明技巧 在论文[24], 中，所需的协议通过一种名为 含噪振幅放大的新技术构造，该技术需要 Alice 和 Bob 共享一定数量的纠缠。基于含噪振幅放大技术，参考文献 [24] 给出了以下定理。

定理（[24, 定理 21]）。假设 Alice（分别地，Bob）获得（X_i）$_{i\le n} \in \{0,1\}^{jn}$（分别地，（$Y_i$）$_{i\le n} \in \{0,1\}^{kn}$）。存在一个满足以下条件的协议：

- 该协议使用 O（$\sqrt{n}$量子通信复杂度$_{\mathrm{E}}$（G））个通信量子比特和 $\lceil \log n \rceil$ 个 EPR 对。
- 当存在满足条件 G（X_i, Y_i）$= 1$ 的坐标 i 时，该协议以概率 $99/100$ 找到该坐标；当不存在这样的 i 时，则以概率 1 输出“否”。

参考文献 [24] 的作者将该协议用作子程序，构造了用于 $f \circ G$ 的主协议，而该主协议本身需要一定数量的纠缠。

另一方面，对于集合不相交问题，Aaronson 和 Ambainis [11] 展示了一种协议，其通信量为 $O(\sqrt{n}$ 个量子比特，且 不使用任何共享纠缠，但能找到一个坐标 i 满足$x_i \wedge y_i = 1$ 的概率为 $99/100$。基于[11] 中的协议构造，而非 [24], 中使用的含噪振幅放大技术，我们成功地在命题 2 中构造了上述定理的一个广义版本，该版本不需要任何共享纠缠。证明了这个广义版本之后，其余部分便可按照 [24], 中的类似方式完成，相关内容见第 4节。因此，我们得到一个用于 SYM $\circ G$的协议，使用 $O(Q(\mathrm{SYM})$量子通信复杂度$_{\mathrm{E}}(G))$ 个量子比特，且不使用任何共享纠缠。

1.3 第二个结果：关于 SYM $\circ$与$_2$的紧上界

在第二个结果中，我们着重研究 SYM $\circ$与$_2$的量子通信复杂度的紧上界。首先注意到，论文 [24] 以及我们的第一个结果已经给出了使用 $O(Q(\mathrm{SYM}))$ 个量子比特的协议，其效率高于 [21] 中使用 $O(Q(\mathrm{SYM})\log n)$ 个量子比特的协议。然而，即使是使用 $O(Q(\mathrm{SYM}))$ 个通信量子比特的协议，通常也无法给出紧上界。例如，$\mathrm{AND}_n \circ$与$_2$ 的量子通信复杂度为 $O(1)$，但 $Q(\mathrm{AND}_n) = \Theta(\sqrt{n})$。因此，我们需要开发另一种技术来证明紧上界。

在这一框架下，Razborov [10] 和 Sherstov [25] 证明了以下强有力的结果。

定理([10, 25])。设$SYM_n\colon\ \{0,1\}^n \to \{0,1\}$ 是一个对称函数，且 $D\colon\ \{0,\ldots,n\} \to \{0,1\}$ 是满足以下条件的函数[1] $SYM_n(x) = D(|x|)$。定义

$$\begin{aligned} l_0(D) &= \max\{l \mid 1 \le l \le n/2 \text{ and } D(l) \ne D(l-1)\}, \\ l_1(D) &= \max\{n-l \mid n/2 \le l < n \text{ and } D(l) \ne D(l+1)\}. \end{aligned}$$

于是我们有 $\mathrm{QCC}^*(\mathrm{SYM}_n \circ$与$_2) \in \Omega(\sqrt{nl_0(D)\overline{+l_1(D)}})$，以及 $\mathrm{QCC}(\mathrm{SYM}_n \circ$与$_2) \in O(\{\sqrt{nl_0(D)+\overline{l_1(D)}}\}\log n)$。

该定理已经给出了近乎紧确的上界 $\mathrm{QCC}^*(\mathrm{SYM}_n \circ$与$_2) = \tilde{\Theta}(\sqrt{nl_0(D)} + l_1(D))$，仅相差一个乘法因子 $\log n$ 。因此，要证明精确的紧确上界，只需通过消去因子 $\log n$，构造一个使用$O(\sqrt{nl_0(D)} + l_1(D))$个通信量子比特的协议。本文成功证明，在共享纠缠模型中不需要这个乘法因子 $\log n$ 。也就是说，我们得到以下定理。

定理 2. 对于任意对称函数 $\mathrm{SYM}_n\colon\ \{0,1\}^n \to \{0,1\}$，$\mathrm{QCC}^*(\mathrm{SYM}_n \circ$与$_2) \in O(\sqrt{nl_0(D)} + l_1(D))$ 成立。

[1]注意，对于任意对称函数 f，都有一个相应的函数 D 满足 $f(x) = D(|x|)$，其中 $|x|$表示比特串 x的汉明重量。

在没有共享纠缠的模型中，我们也证明了一个类似的结论，不过会多出一个加性 $\log\log n$因子。因此我们证明了

定理 3. 对于任意对称函数 $\mathrm{SYM}_n : \{0,1\}^n \to \{0,1\}$，$\mathrm{QCC}(\mathrm{SYM}_n \circ \text{与}_2) \in O(\sqrt{n l_0(D)} + l_1(D) + \log\log n)$ 成立。

这首次揭示了 QCC 之间的紧致关系$^*(\mathrm{SYM}_n \circ \text{与}_2) = \Theta(\sqrt{n l_0(D)} + l_1(D))$，适用于共享纠缠模型，并与 [10, 25] 给出的下界相匹配。然而，在无共享纠缠模型中，我们的协议通信成本与下界 n 之间仍存在 $\log\log$ [10, 25]的差距。为弥合这一差距，我们还证明，无共享纠缠时我们的协议实际上是最优的：

命题 1. 对于任意非平凡对称函数 $f_n : \{0,1\}^n \to \{0,1\}$，

- 如果函数 f_n满足 $l_0(D_{f_n}) > 0$或 $l_1(D_{f_n}) > 1$，则 $\mathrm{QCC}(f_n \circ \text{与}_2) \in \Omega(\sqrt{n l_0(D_{f_n})} + l_1(D_{f_n}) + \log\log n)$ 成立。
- 否则（若 f_n满足 $l_0(D_{f_n}) = 0$且 $l_1(D_{f_n}) \le 1$），则 $\mathrm{QCC}(f_n \circ \text{与}_2) \in \Theta(1)$ 成立。

在命题1的证明中，欺骗集论证这一通信复杂度中的标准技巧发挥了基础性作用。

证明技巧 现在我们来解释定理 2 和定理3中所用的目标协议的主要思路。为了构造 $\mathrm{SYM} \circ \text{与}_2$, 的目标协议，我们首先将对称函数 $\mathrm{SYM}(x) = D(|x|)$ 分解为两个对称函数 $\mathrm{SYM}_0(x) := D_0(|x|)$ 和 $\mathrm{SYM}_1(x) := D_1(|x|)$，如下所示：

$$D_0(m) := \begin{cases} D(m) & \text{if } m \le l_0(D) \\ 0 & \text{otherwise} \end{cases}, \quad D_1(m) = \begin{cases} D(m) & \text{if } m > n - l_1(D) \\ 0 & \text{otherwise} \end{cases}.$$

注意，函数 D 在区间 $[l_0(D)\ n - l_1(D)]$上取常数值。正如第 5节所述，结果表明，分别计算 $\mathrm{SYM}_0 \circ \text{与}_2$ 和 $\mathrm{SYM}_1 \circ \text{与}_2$ 就足以计算整个函数$\mathrm{SYM} \circ \text{与}_2$。因此，我们只需设计两个不同的协议：一个用于 $\mathrm{SYM}_0 \circ \text{与}_2$，另一个用于 $\mathrm{SYM}_1 \circ \text{与}_2$。现在我们来说明如何设计这两个协议。

- 要计算 $\mathrm{SYM}_0 \circ \text{与}_2$，我们只需使用第一个结果。由于 $O(\sqrt{n l_0(D)})$ 成立，因此这需要 $Q(\mathrm{SYM}_0) = O(\sqrt{n l_0(D)})$ 个通信量子比特。 [26, 27]。
- 要计算 $\mathrm{SYM}_1 \circ \mathrm{AND2}$，Alice 和 Bob 直接计算集合 $\{i \le n \mid \mathrm{AND2}(x_i, y_i) = 1\}$ 中元素的数量，条件是[2] $\min\{|x|, |y|\} \ge n - l_0(D)$。对输入取反后，这个问题可化简为计算集合 $\{i \le n \mid x_i = 0 \text{ or } y_i = 0\}$ 中元素的数量，条件是 $\min\{|x|, |y|\} \le l_0(D)$。事实上，已有多项研究分析了这个问题及相关问题 [28, 29, 30, 31]，并且研究 [29] 表明，当允许使用共享随机性时，$O(l_0(D))$ 经典通信就足够了（此外，还需要 $O(\log\log n)$ 位通信[3]，才能将共享随机性转换为私有随机性）。

结合上述协议，我们构造出所需的 $\mathrm{SYM} \circ \text{与}_2$ 协议，其通信量为 $O(\sqrt{n l_0(D_f)} + l_1(D_f))$。值得注意的是，正如上述协议所示，Alice 和 Bob 事先需要共享的是共享随机性，而非共享纠缠。这意味着，我们实际上在一种较弱的通信模型中证明~~了~~了上界 $O(\sqrt{n l_0(D_f)} + l_1(D_f))$：该模型允许共享随机性，但不允许共享纠缠。

[2]如果该条件不成立，$\mathrm{SYM}_1 \circ \text{与}_2(x, y)$ 必须为零。Alice 和 Bob 只需通过两比特通信即可检查该条件。[3]在这种情况下，$\min\{|x|, |y|\} \ge n - l_0(D)$ 成立，因此纽曼定理告诉我们，$O(\log\log \#\{x \mid |x| \ge n - l_0(D)\})$ 比特即可模拟共享随机性。如第5节所示，实际所需的额外比特数有界于 $O(\log\log n)$。

1.4 论文组织结构

第 2 节列出了本文中使用的若干记号和事实。第 3 节将集合不相交问题的协议推广 [11] 并构造了一个用于证明主要结果的有效协议。第 4 节讨论第一个结果，并证明定理 1。第 5 节讨论第二个结果，并证明定理2 和定理 3。

2 预备知识

对于任意函数 f，我们分别用 $\mathrm{QCC}_{\mathrm{E}}(f)$、$\mathrm{QCC}(f)$ 和 $\mathrm{QCC}^*(f)$ 表示函数 f 的零错误协议的量子通信复杂度、无共享纠缠且错误率为 $\leq 1/3$ 的有界错误量子通信复杂度，以及有共享纠缠且错误率为 $\leq 1/3$ 的有界错误量子通信复杂度。显然，有 $\mathrm{QCC}^*(f) \leq \mathrm{QCC}(f) \leq \mathrm{QCC}_{\mathrm{E}}(f)$。我们还用 $Q(f)$ 表示函数 f 的有界错误查询复杂度。对于一个 n 位比特串 x，我们用 $\neg x = (\neg x_1, \ldots, \neg x_n)$ 表示 x 的按位取反。

对称函数 这里列出关于对称函数的几个重要事实。对于任意对称函数 f，f 可以表示为 $f(x) = D_f(|x|)$，其中使用了某个函数 $D_f\colon \{0,1,\ldots,n\} \to \{0,1\}$。记

$$\begin{aligned} l_0(D_f) &= \max\left\{l \mid 1 \leq l \leq n/2 \text{ and } D_f(l) \neq D_f(l-1)\right\}, \\ l_1(D_f) &= \max\left\{n-l \mid n/2 \leq l < n \text{ and } D_f(l) \neq D_f(l+1)\right\}, \end{aligned}$$

先前的工作 [26, 27] 表明，对称函数的查询复杂度 $Q(f)$ 可表示为 $Q(f) = \Theta(\sqrt{n(l_0(D_f) + l_1(D_f))})$。

3 查找元素的通信成本

本节旨在证明命题 2，它是 [11, 定理 5.16] 的量子通信版本。

命题 2. 存在一个协议 FIND-MORE$_k$，使用 $O(\sqrt{\frac{n}{k}}$量子通信复杂度$_{\mathrm{E}}(G))$ 个量子比特，并使用共享随机性，满足以下条件：

- 当至少存在 k 个这样的坐标时，该协议以概率 $= 1$ (X_i, Y_i) G 输出一个坐标 $i \in [n]$。
- 若不存在这样的坐标，该协议以概率 1 回答“没有这样的坐标”。
- 该协议不使用任何共享纠缠。

证明见第 3.2 节。

3.1 一个关键引理

为了证明命题2，我们先证明以下引理：

引理 1. 对于 $\gamma \in \mathbb{N}$，存在一个协议 FIND-EXACT$_\gamma$，使用 $O(\sqrt{\frac{n}{\gamma}}$量子通信复杂度$_{\mathrm{E}}(G))$ 个量子比特和共享随机性，并满足以下条件：

- 该协议输出一个坐标 $i \in [n]$，使得当存在恰好 k 个这样的坐标时，对于某个满足 $3k/2 < \gamma < 3k$ 的 k，$G(X_i, Y_i) = 1$ 的概率为 $\geq 99/100$。
- 当不存在这样的坐标时，该协议以概率 1 回答“没有这样的坐标”。
- 该协议不使用任何共享纠缠。

在引理 1 的证明中，我们使用引理 2 ，它是对 [11, 节 7] 中给出的协议的修改版本。修改详情见附录 A 。

引理 2。 存在一个 FIND-ONE 协议，其成本为 $O(\sqrt{n}$量子通信复杂度$_{\mathrm{E}}(G))$，并满足以下条件 s:

- 当存在满足 $G(X_i, Y_i)$ 的 $i \in [n]$ 时，协议以 $\geq 99/100$ 的概率输出该坐标 $= 1$ （概率意义下）。 ts.
- 若不存在这样的坐标，协议以概率 1 回答“没有这样的坐标”。
- 该协议不使用任何共享纠缠。

引理 1 的证明。我们首先将集合 $\{1, \ldots, n\}$ 划分为 n/γ 个子集 $A_j = \{(j-1)\gamma + 1$、……、$j\gamma\}\,(1 \leq j \leq n/\gamma)$，每个子集包含 γ 个子输入。Alice 和 Bob 使用共享随机性选取坐标集合 $\{i_1, \ldots, i_{n/\gamma}\} \subset [n]$ ，其中每个 i_j 都从集合 A_j 中均匀随机选取。随后，Alice 和 Bob 执行 FIND-ONE 协议，并假定 Alice 的输入为 $(X_{i_1}$,……, $X_{i_{n/\gamma}})$，Bob 的输入为 $(Y_{i_1}$,……, $Y_{i_{n/\gamma}})$。由于 FIND-ONE 对长度为 n 的输入需要 $O(\sqrt{n}$量子通信复杂度$_{\mathrm{E}}(G))$ 个通信量子比特，因此该协议对长度为 n/γ 的输入需要 $O(\sqrt{\frac{n}{\gamma}}$量子通信复杂度$_{\mathrm{E}}(G))$ 个通信量子比特。

现在，我们遵循 [11, Lemma 5.15] 中使用的技巧，分析该协议正确执行的概率。假设恰有 k 个坐标满足 $G(X_i, Y_i) = 1$ 且 $3k/2 < \gamma < 3k$ 成立。设 i_0 满足 $G(X_{i_0}, Y_{i_0}) = 1$。那么，坐标 i_0 以 $1/\gamma$ 的概率被选作共享随机性。给定 i_0 被选中，在满足 $G(X_{i'}, Y_{i'}) = 1$ 的其他坐标 i' 中，若 i_0、 i' 属于同一个子集 $A_j (1 \leq j \leq n/\gamma)$，则该坐标被选中的概率为 0；若 i_0 和 i' 属于两个不同的子集，则该坐标被选中的概率为 $1/\gamma$ 。因此，“仅坐标 i_0 被选中”的概率至少为

$$\frac{1}{\gamma}\left(1 - \frac{k-1}{\gamma}\right) \geq \frac{1}{\gamma}\left(1 - \frac{k}{\gamma}\right).$$

考虑到“坐标 i_0 被选中”这些事件互不相交，我们看到，“恰有一个这样的坐标被选中”的概率至少为 $k/\gamma - (k/\gamma)^2$。由于 $3k/2 < \gamma < 3k$ 成立，我们注意到该概率至少为 $2/9$。这表明“至少有一个元素被选中”这一事件以 $\geq 2/9$ 的概率发生。

因此，根据 FIND-ONE 的性质，我们的新协议满足以下条件:

- 当存在恰好 k 个满足 $3k/2 < \gamma < 3k$ 的 k ，且这些坐标满足 $G(X_i, Y_i) = 1$ 时，协议以 Ω(1) 的成功概率输出坐标 $i \in [n]$ 。
- 该协 议在不存在这样的坐标时，以概率 1 回答“没有这样的坐标”。
- 该协议不使用任何共享纠缠。

为了将成功概率 Ω(1) 提高到 $99/100$，Alice 和 Bob 递归地执行上述协议，并在每次重复时检查输出 i_{out} 是否满足 $G(X_{i_{\mathrm{out}}}, Y_{i_{\mathrm{out}}}) = 1$。这样的重复仅使通信成本增加一个常数开销，因此我们得到了所需的结论。 □

命题2 的证明

使用协议 FIND-EXACT$_\gamma$，我们证明命题2 如下。

命题 2的证明。 协议 FIND-MORE$_k$ 按如下方式执行:

(1) 对于 $j = 0$ to $\log_2(n/k)$，Alice 和 Bob 执行 FIND-EXACT$_{\gamma_j}$ ，其中 $\gamma_j = 2^j k$。

(2) 作为共享随机性，Alice 和 Bob 从集合 $[n]$ 中均匀随机地选取一个坐标 i ，并检查 $G(X_i, Y_i) = 1$ 是否成立。重复执行 $O(1)$ 次。

我们首先分析该协议的通信成本。第一步需要

$$\sum_{j=0}^{\log_2(n/k)} O\left(\sqrt{\frac{n}{2^j k}}\mathrm{QCC}_{\mathrm{E}}(G)\right) = O\left(\sqrt{\frac{n}{k}}\mathrm{QCC}_{\mathrm{E}}(G)\right) \sum_{j=0}^{\log_2(n/k)} \frac{1}{2^{j/2}} = O\left(\sqrt{\frac{n}{k}}\mathrm{QCC}_{\mathrm{E}}(G)\right)$$

通信量子比特。第二步需要 $O(\mathrm{QCC_E}(G))$ 个通信量子比特。因此，该协议总共使用了$O\left(\sqrt{\frac{n}{k}}\mathrm{QCC_E}(G)\right)$ 个量子比特。

接下来我们分析该协议的正确概率。设 $k^* \geq k$ 为满足$G(X_i, Y_i) = 1$的坐标数。如果 $k^* \leq n/3$，则存在满足 $3k^*/2 < \gamma_j < 3k^*$的 j。因此，FIND-EXACT$^{\gamma_j}$ 以 $\geq 99/100$的概率找到所需坐标。另一方面，如果 $k^* > n/3$，第二步以 $1/3$的概率找到所需坐标。重复 O(1) 次即可将成功概率提高到 $99/100$。 □

4 对称函数的通信协议

在 [24, 定理 22 和定理 25], 以下定理已被证明（其表达式略有不同）：

定理（[24, 定理 22 和定理 25]）。设 FIND-MORE$_k$ 使用 m 个 EPR 对作为共享纠缠，并使用任意多的共享随机性。那么对于任意对称函数 f： $\{0,1\}^n \to \{0,1\}$，以及任意二方函数 G： $\{0,1\}^j \times \{0,1\}^k \to \{0,1\}$，存在一个使用 $O(Q(f)$量子通信复杂度$_{\mathrm{E}}(G))$ 个量子比特的协议，满足以下条件：

- 该协议以概率 $\geq 99/100$ 成功计算 $f \circ G$。
- 该协议使用 $m \cdot O(l_0(D_f) + l_1(D_f))$ 个 EPR 对作为共享纠缠。
- 该协议使用 $O(\log n)$ 位共享随机性。

如命题 2所示，我们修改后的协议 FIND-MORE$_k$ 不使用任何共享纠缠。因此，我们在上述陈述中令 $m = 0$，从而得到以下定理。（注意，$O(\log n)$ 位共享随机性计入通信的一部分，因为 $O(\log n)$ 位与$Q(f) \geq \Omega(\sqrt{n})$ 相比可以忽略，只要 f 并非平凡情形。）

定理 **1.** 对于任意对称函数 $f\colon \{0,1\}^n \to \{0,1\}$ 以及任意两方函数 $G\colon \{0,1\}^j \times \{0,1\}^k \to \{0,1\}$,

$$\mathrm{QCC}(f \circ G) \in O(Q(f)\mathrm{QCC_E}(G)).$$

5 对称函数的紧致上界

在本节中，我们证明以下两个定理：

定理 **2.** 对于任意对称函数 SYM_n： $\{0,1\}^n \to \{0,1\}$， 量子通信复杂度$^*(SYM_n \circ$与$_2) \in O(\sqrt{n l_0(D)\overline{l_1}(D)}$成立。

定理 **3.** 对于任意对称函数 SYM_n： $\{0,1\}^n \to \{0,1\}$， 量子通信复杂度$(SYM_n \circ$与$_2) \in O(\sqrt{n l_0(D)\overline{l_1}(D)} + \log \log n)$ 成立。

为了证明这些定理，我们使用以下协议，该协议是对 [29,定理 3。1]中所给协议的修改。为完整起见，我们在附录 B中描述这一修改。

命题 3. 假设输入 $x, y \in \{0,1\}^n$ 满足 $\max\{|x|, |y|\} \leq k$。存在一个公共随机经典协议[4]，其通信复杂度为 $O(k)$ 位，可以以概率 $99/100$ 计算集合 $\{i | x_i = y_i = 1\} \subset [n]$。

遵循 第 [10, 节中使用的技术 4], ，我们证明定理2 和定理3 如下：

定理*2* 和定理*3*的证明。首先根据 [10, 25]中的论证，介绍一些重要事实。对于任意对称函数 f_n，相应的函数 D_{f_n} 在区间 $[l_0(D_{f_n})\ n - l_1(D_{f_n})]$上为常数。

[4]请注意，该协议可能会使用大量共享随机性。

不失一般性，假设 D_{f_n} 在该区间上取值为 0。（若 D_{f_n} 在该区间上取值为 1，则对 D_{f_n}取反。）定义 D_0和 D_1：$\{0,\dots,n\}\to\{0,1\}$如下

$$D_0(m)=\begin{cases}D_{f_n}(m) & \text{if } m\le l_0(D_{f_n})\\ 0 & \text{otherwise}\end{cases},D_1(m)=\begin{cases}D_{f_n}(m) & \text{if } m>n-l_1(D_{f_n})\\ 0 & \text{otherwise}\end{cases},$$

$D_{f_n}=D_0\vee D_1$ 成立。因此，定义 $f_n^0(x):=D_0(|x|)$ 和 $f_n^1(x):=D_1(|x|)$，可得 $f_n\circ$与$_2=(f_n^0\circ$与$_2)\vee(f_n^1\circ$与$_2)$。这意味着，分别计算 $f_n^0\circ$与$_2$ 和 $f_n^1\circ$与$_2$，就足以计算整个函数 $f_n\circ$与$_2$。为了说明，还需要注意另一个重要事实：f_n^0的查询复杂度等于~~$O(\sqrt{nl_0}(D_{f_n}))$~~，这一点已在 [26] 中证明。

从现在起，我们介绍两个协议：一个用于计算 f_n^0，另一个用于计算 f_n^1。

- 用于 f_n^0的协议：我们只需应用定理 1 中的协议，并取 $G=$与$_2$（注意，f_n^0是一个对称函数）。该协议使用 $O(\sqrt{nl_0}(D_{f_n}))$ 个量子比特，因为 $Q(f_n^1)=\Theta(\sqrt{nl_0}(D_{f_n}))$ 成立。
- f_n^1 的协议：首先，Bob 向 Alice 发送一位：如果 $|\neg y|\le l_1(D_{f_n})$，则发送 1；否则发送 0。如果 Alice 收到 1 且 $|\neg x|\le l_1(D_{f_n})$ 成立，他们就使用输入 $\neg x$ 和 $\neg y$ 执行命题 3 的协议。否则，$\min\{|x|,|y|\}<n-l_0(D_{f_n})$ 成立，因此根据 D_1 的定义，$f_n^0\circ\mathrm{AND2}(x,y)$ 必须为零。执行完命题 3 的协议后，Alice 和 Bob 知道集合 $\{i\le n\mid x_i=y_i=0\}$。接下来，Alice 发送$|\neg x|$，Bob 使用 $\log\ l_0(D_{f_n})$ 通信发送 $|\neg y|$，最后他们计算 $\#\{i\le n\mid x_i=y_i=1\}$，使其等于 $\#\{i\le n\mid x_i=y_i=1\}=n+\#\{i\le n\mid x_i=y_i=0\}-|\neg x|-|\neg y|$。该协议使用 $O(l_1(D_{f_n}))$ 个通信比特。

  接下来，我们评估使用公共随机币时的成本。尽管执行该协议可能需要大量共享随机性，但纽曼定理[4] 保证，当输入 x,y 属于集合 S时，$O(\log\log|S|)$比特就足够了。由于执行时成立 $|\neg x|,|\neg y|\le l_1(D_{f_n})$，并利用$\#\{x\in\{0,1\}^n\mid|\neg x|\le k\}\le n^k$这一事实，我们得出，$O(\log(\log\ n^{l_1(D_{f_n})}))=O(\log\ l_1(D_{f_n})+\log\log\ n)$比特的共享随机性就足够了。此外，由于 $O(\log\ l_1(D_{f_n}))$比特的共享随机性与通信中的 $O(l_1(D_{f_n}))$比特相比可以忽略不计，因此可将其作为通信的一部分，不产生额外的通信成本；我们只需使用 $O(\log\log n)$比特的共享随机性。

结合这两个协议，我们得到所需协议，其成本为 $O(\sqrt{nl_0}(D_{f_n})+l_1(D_{f_n}))$，并使用 $O(\log\log\ n)$个公共随机币。这表明 $\mathrm{QCC}^*(f_n\circ$与$_2)\in O(\sqrt{nl_0}(D_{f_n})+l_1(D_{f_n}))$，且 $\mathrm{QCC}(f_n\circ$与$_2)\in O(\sqrt{nl_0}(D_{f_n})+l_1(D_{f_n})+\log\log\ n)$；具体而言，由 Alice 发送 $O(\log\log\ n)$个随机比特，而非使用共享随机性。 □

结合目前为止的论证，我们得到共享纠缠通信模型下紧确界 $\mathrm{QCC}^*(f_n\circ$与$_2)\in\Theta(\sqrt{nl_0}(D_{f_n})+l_1(D_{f_n}))$。在无共享纠缠的模型下，我们的界 $\mathrm{QCC}(f_n\circ$与$_2)\in O(\sqrt{nl_0}(D_{f_n})+l_1(D_{f_n})+\log\log\ n)$ 与下界之间仍相差加性项 $\log\log\ n$。接下来，我们将使用一种标准技术——欺骗集论证——证明这个上界确实是最优的。

命题**1**：对于任意非平凡对称函数 $f_n:\ \{0,1\}^n\to\{0,1\}$，

- 如果函数 f_n满足 $l_0(D_{f_n})>0$或 $l_1(D_{f_n})>1$，则 $\mathrm{QCC}(f_n\circ$与$_2)\in\Omega(\sqrt{nl_0}(D_{f_n})+l_1(D_{f_n})+\log\log\ n)$ 成立。
- 否则（即，如果 f_n满足 $l_0(D_{f_n})=0$且 $l_1(D_{f_n})\le1$），则 $\mathrm{QCC}(f_n\circ$与$_2)\in\Theta(1)$ 成立。

证明。我们先证明，当 $l_0(D_{f_n})=0$且 $l_1(D_{f_n})\le1$成立时，$\mathrm{QCC}(f_n\circ$与$_2)\in\Theta(1)$ 成立。在这种情况下，函数只有两种类型：$f_n=$与$_n$ 或 $f_n=\neg$与$_n$。无论是哪一种函数，Alice 和 Bob 只需各发送一个比特，分别表示 Alice 的 $x=(1,\dots,1)$ 和 Bob 的 $y=(1,\dots,1)$ 是否成立。因此，我们得到 $\mathrm{QCC}(f_n\circ$与$_2)\in\Theta(1)$，因为下界 $\mathrm{QCC}(f_n\circ$与$_2)\in\Omega(1)$ 是显然的。

剩下的工作是在假设 $l_0(D_{f_n})>0$或$l_1(D_{f_n})>1$成立时，证明 $\mathrm{QCC}(f_n\circ$与$_2)\in\Omega(\sqrt{nl_0}(D_{f_n})+l_1(D_{f_n})+\log\log\ n)$。首先注意，当 $\sqrt{nl_0}(D_{f_n})+l_1(D_{f_n})$ 时，$\log\log\ n$ 这一因子可以忽略，因为

$l_0(D_{f_n}) > 0$成立。这意味着，众所周知的下界 $\Omega(\sqrt{n l_0(D_{f_n})} + l_1(D_{f_n}))$ [10] 已经给出了紧的下界。因此，我们只需在假设$l_0(D_{f_n}) = 0$成立时，证明 $\mathrm{QCC}(f_n \circ 与_2) \in \Omega(l_1(D_{f_n}) + \log \log n)$。此外，[10] 中给出的下界 $\mathrm{QCC}^*(f_n \circ 与_2) \in \Omega(\sqrt{n l_0(D_{f_n})} + l_1(D_{f_n}))$ 推出 $\mathrm{QCC}(f_n \circ 与_2) \in \Omega(l_1(D_{f_n}))$。因此，只需证明当 $l_0(D_{f_n}) = 0$和 $l_1(D_{f_n}) > 1$ 成立时，$\mathrm{QCC}(f_n \circ 与_2) \in \Omega(\log \log n)$。

假设 $l_0(D_{f_n}) = 0, l_1(D_{f_n}) > 1$以及 $D_{f_n} \equiv 0$在 $[l_0(D_{f_n}) \; n - l_1(D_{f_n})]$上，不失一般性，我们证明 $\mathrm{QCC}(f_n \circ 与_2) \in \Omega(\log \log n)$。为此，我们使用欺骗集论证 [2, 3]。定义

$$\mathrm{FS}_n := \{(x, y) \in \{0,1\}^n \times \{0,1\}^n \mid x = y \text{ and } |\neg x| = l_1(D_{f_n}) - 1\}.$$

于是我们看到，对于任意 $(x, y) \in \mathrm{FS}_n$，$f_n \circ 与_2(x, y) = 1$；并且对于任意 (x, y)、$(x', y') \in \mathrm{FS}_n$，若 $(x, y) \neq (x', y')$，则$f_n \circ 与_2(x, y') = f_n \circ 与_2(x', y) = 0$。因此，确定性通信复杂度 $\mathrm{DCC}(f_n \circ 与_2)$ 满足

$$\mathrm{DCC}(f_n \circ \mathsf{AND}_2) \geq \log_2 |\mathrm{FS}_n|$$

根据欺骗集论证。正如 [32], 中所示，众所周知，对于任意函数 f，$\mathrm{QCC}(f) \geq \log \mathrm{DCC}(f)$。因此，注意到对于 $l_1(D_{f_n}) > 1$，$|\mathrm{FS}^n| = \binom{n}{l_1 \quad (D_{f_n})-1} \geq \Omega(n)$，我们得到所需结论 $\mathrm{QCC}(f_n \circ 与_2) \geq \Omega(\log \log n)$。

□

致谢

作者部分获得了日本文部科学省 Q-LEAP 项目（编号：JPMXS0120319794）的资助。作者谨借此机会感谢由名古屋大学和日本科学技术振兴机构支持的“名古屋大学跨学科前沿奖学金”，该奖学金属于旨在推动科学技术创新的大学奖学金设立项目，项目编号为 JPMJFS2120。作者还要感谢 Fran¸cois Le Gall 的友善帮助和宝贵意见，以及 Ronald de Wolf 对本文早期稿件提出的友善意见。

参考文献

[1] Andrew Chi-Chih Yao. 与分布式计算相关的一些复杂性问题（初步报告）。载于第11届ACM计算理论研讨会，页码209–213，1979年。[2] Eyal Kushilevitz 和 Noam Nisan。《通信复杂度》。剑桥大学出版社，1996年。[3] Anup Rao 和 Amir Yehudayoff。《通信复杂度：及其应用》。剑桥大学出版社，2020年。[4] Ilan Newman。通信复杂度中的私有随机比特与公共随机比特。Information Processing Letters，39(2):67–71，1991年。[5] Andrew Chi-Chih Yao。量子电路复杂度。载于第34届年度计算机科学基础会议，页码352–361，1993年。[6] Richard Cleve 和 Harry Buhrman。以量子纠缠替代通信。《物理评论A辑》，56(2):1201，1997年。[7] Harry Buhrman、Richard Cleve 和 Wim van Dam。量子纠缠与通信复杂度。SIAM计算杂志，30(6):1829–1841，2001年。[8] Gilles Brassard。量子通信复杂度。《物理学基础》，33(11):1593–1616，2003年。[9] Harry Buhrman、Richard Cleve、Serge Massar 和 Ronald de Wolf。非定域性与通信复杂度。《现代物理评论》，82:665–698，2010年。

[10] Alexander A Razborov。对称谓词的量子通信复杂度。Izvestiya: Mathematics，67(1):145，2003年。[11] Scott Aaronson 和 Andris Ambainis。空间区域的量子搜索。Theory of Computing，1(4):47–79，2005年。[12] Richard Cleve、Wim van Dam、Michael Nielsen 和 Alain Tapp。量子纠缠与内积函数的通信复杂度。载于首届NASA量子计算与量子通信国际会议精选论文集（QCQC '98），页码61–74，1998年。[13] Harry Buhrman 和 Ronald de Wolf。利用多项式得到通信复杂度下界。载于第16届年度IEEE计算复杂性会议，页码120–130。IEEE，2001年。[14] John F. Clauser、Michael A. Horne、Abner Shimony 和 Richard A. Holt。旨在检验局域隐变量理论的实验方案。Physical Review Letters，23:880–884，1969年10月。[15] N. David Mermin。主要无隐变量定理的简单统一形式。Physical Review Letters，65:3373–3376，1990年12月。[16] Dmitry Gavinsky、Julia Kempe、Oded Regev 和 Ronald de Wolf。有界误差量子态识别与通信复杂度中的指数分离。载于第38届年度ACM计算理论研讨会论文集，页码594–603，2006年。[17] Dmitry Gavinsky。论共享纠缠的作用。Quantum Information & Computation，8(1):82–95，2008年。[18] Yaoyun Shi 和 Yufan Zhu。分块复合函数的量子通信复杂度。Quantum Information & Computation，9(5):444–460，2009年。[19] Troy Lee 和 Shengyu Zhang。通信复杂度中的复合定理。载于《自动机、语言与程序设计》，页码475–489，2010年。[20] Anil Ada、Arkadev Chattopadhyay、Omar Fawzi 和 Phuong Nguyen。复合函数的编号自由多方通信复杂度。载于《自动机、语言与程序设计》，页码13–24，2012年。[21] Harry Buhrman、Richard Cleve 和 Avi Wigderson。量子通信与计算和经典通信与计算的比较。载于第30届年度ACM计算理论研讨会，页码63–68，1998年。[22] Peter Høyer 和 Ronald de Wolf。不相交性与相等性的改进量子通信复杂度界。载于理论计算机科学年度研讨会，页码299–310，2002年。[23] Sourav Chakraborty、Arkadev Chattopadhyay、Nikhil S. Mande 和 Manaswi Paraashar。量子查询到通信模拟需要对数开销。载于第35届计算复杂性会议，2020年。[24] Sourav Chakraborty、Arkadev Chattopadhyay、Peter Høyer、Nikhil S. Mande、Manaswi Paraashar 和 Ronald de Wolf。对称性与量子查询到通信模拟。载于第39届理论计算机科学国际研讨会，页码20:1–20:23，2022年。[25] Alexander A. Sherstov。模式矩阵方法。SIAM计算杂志，40(6):1969–2000，2011年。[26] Ramamohan Paturi。关于逼近对称布尔函数的多项式次数（初步版本）。载于第24届年度ACM计算理论研讨会，页码468–474，1992年。[27] Robert Beals、Harry Buhrman、Richard Cleve、Michele Mosca 和 Ronald de Wolf。利用多项式得到量子下界。Journal of the ACM（JACM），48(4):778–797，2001年。[28] Wei Huang、Yaoyun Shi、Shengyu Zhang 和 Yufan Zhu。汉明距离问题的通信复杂度。Information Processing Letters，99(4):149–153，2006年。

[29] Joshua Brody、Amit Chakrabarti、Ranganath Kondapally、David P. Woodruff 和 Grigory Yaroslavtsev。《超越集合不相交性：寻找交集的通信复杂度》。载于 ACM 分布式计算原理研讨会 PODC '14，页码 106–113，2014 年。

[30] Joshua Brody、Amit Chakrabarti、Ranganath Kondapally、David P. Woodruff 和 Grigory Yaroslavtsev。《通过有限交互验证相等性》。Algorithmica，76(3):796–845，2016 年。

[31] Dawei Huang、Seth Pettie、Yixiang Zhang 和 Zhijun Zhang。《集合交集与多重相等性测试的通信复杂度》。载于第 31 届 ACM-SIAM 离散算法年会，页码 1715–1732，2020 年。

[32] Ilan Kremer 和 Noam Nisan。《量子通信》。技术报告，1995 年。

引理2的一个修改

这里我们说明如何将 [11, 第 7] 节给出的协议修改为定理2中的协议。在 [11,第 7], 节中，作者提出了一种协议，用于找到 $i \in [n]$ 使得 $x_i \wedge y_i = 1$ 其中 Alice 获得 $x \in \{0,1\}^n$，Bob 获得 $y \in \{0,1\}^n$。在该协议中，Alice 和 Bob 执行查询

$$O_{\mathrm{AND}} : |i,z\rangle_A |i\rangle_B \mapsto |i, z \oplus (x_i \wedge y_i)\rangle_A |i\rangle_B$$

共 $O(\sqrt{n})$ 次，以及其他需要 $O(\sqrt{n})$ 通信的操作。由于查询操作使用 2 比特量子通信实现，该协议需要 $2O(\sqrt{n}) + O(\sqrt{n}) = O(\sqrt{n})$ 通信。O
我们的更多 dificati。寻找满足 $G(X_i, Y_i) = 1$ 的 i 的操作很简单。我们只需将查询 O_{AND} 替换为

$$O_G : |i,z\rangle_A |i\rangle_B \mapsto |i, z \oplus G(X_i, Y_i)\rangle_A |i\rangle_B.$$

该协议确实找到了所需的坐标 i，其正确性证明与 [11, 第 7] 节中的方式相同。下面分析该协议的通信成本。由于 $\mathrm{QCC_E}(G)$ 表示G的精确通信复杂度，因此操作 O_G 使用 $2\mathrm{QCC_E}(G)$ 个量子比特实现。（首先使用 $\mathrm{QCC_E}(G)$ 通信来计算G，然后使用第二个 $\mathrm{QCC_E}(G)$ 来反向计算并清除不需要的寄存器。）其他操作与原协议相同，因此使用 $O(\sqrt{n})$ 通信。考虑到操作 O_G 执行了 $O(\sqrt{n})$ 次，我们得出，修改后的协议使用 $O(\sqrt{n}) + \mathrm{QCC_E}(G)O(\sqrt{n}) = O(\mathrm{QCC_E}(G)\sqrt{n})$ 个通信量子比特。

命题 3的 B 修改

在 [29, 定理 3。1], 作者最初证明了以下结论。

定理 4。假设输入 $x, y \in \{0,1\}^n$ 满足 $\max\{|x|, |y|\} \le k$。存在一个 $O(\sqrt{k})$ 轮的构造性随机经典协议，以成功概率 $1 - 1/\mathrm{poly}(k)$ 输出集合 $\{i \mid x_i = y_i = 1\}$。在共享随机性的模型中，总期望通信量为 $O(k)$。

为了将此定理修改为命题 3，我们需要处理成功概率和期望通信量。为处理成功概率，我们首先取一个足够大的常数 k_0，使得对于任意 $k \ge k_0$, $1/\mathrm{poly}(k) \le 1/200$。若 $k < k_0$ 成立，各方使用常数k_0执行定理 4 中的协议。这需要 $O(k_0)$ 的期望通信量。否则（即当 $k > k_0$ 成立时），各方使用常数 k执行定理 4 中的协议，这需要 $O(k)$ 的期望通信量。由于 k_0 是常数，经此修改后的协议仍需要 $O(k)$ 的期望通信量，且错误率为 $\le 1/200$。

为了将期望通信量转换为最坏情况通信量，我们使用马尔可夫不等式。假设该协议需要 $C \cdot k$ 期望通信量。那么，根据马尔可夫不等式，“通信成本$\ge 200C \cdot k$”的概率小于或等于 $1/200$。我们让 Alice 和 Bob 在通信成本达到 $200C \cdot k$时中止通信，从而构造出所需的协议。该修改后的协议仍具有成功概率$\ge 99/100$，因为第一次修改带来的错误为 $1/200$，第二次修改对错误的影响至多为$1/200$。