Quantum Information and Computation, Vol. 9, No. 3&4 (2009) 0255–0263

COMMUNICATION COMPLEXITIES OF SYMMETRIC XOR FUNCTIONS

ZHIQIANG ZHANG[a]
Institute for Theoretical Computer Science and Center for Advanced Study
Tsinghua University, Beijing, 100084, P.R. China

YAOYUN SHI[b]
Department of Electrical Engineering and Computer Science
University of Michigan, 2260 Hayward Street, Ann Arbor, MI 48109-2121, USA

Received Auguest 12, 2008
Revised October 5, 2008

We call $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ a symmetric XOR function if for a function $S : \{0,1,...,n\} \to \{0,1\}$, $F(x,y) = S(|x \oplus y|)$, for any $x, y \in \{0,1\}^n$, where $|x \oplus y|$ is the Hamming weight of the bit-wise XOR of x and y. We show that for any such function, (a) the deterministic communication complexity is always $\Theta(n)$ except for four simple functions that have a constant complexity, and (b) up to a polylog factor, both the error-bounded randomized complexity and quantum communication with entanglement complexity are $\Theta(r_0 + r_1)$, where r_0 and r_1 are the minimum integers such that $r_0, r_1 \leq n/2$ and $S(k) = S(k+2)$ for all $k \in [r_0, n - r_1)$.

Keywords: communication complexity, XOR functions, quantum communication.

Communicated by: R Jozsa & J Watrous

1 Introduction

The two-party interactive communication model was introduced by Yao [1] in 1979, and has been widely studied since then for its simplicity and its power in capturing many of the complexity issues of communication. Let X and Y be two sets and $F : X \times Y \to \{0,1\}$ be a Boolean function. In this model, Alice has an input $x \in X$, Bob has an input $y \in Y$, and they want to compute $F(x,y)$ by exchanging messages. If the communication protocol is deterministic, the least number of bits they need to exchange on the worst-case input is the *deterministic complexity*, denoted by $D(F)$. If they are allowed to share random bits, the least number of bits they need to exchange in order to compute F with at least $2/3$ of success probability is the *randomized complexity* of F, denoted by $R(F)$. Yao also initiated the study of quantum communication complexity [2], denoted by $Q^*(F)$, which is the least number of quantum bits that Alice and Bob need to exchange in order to compute F with at least $2/3$

[a]Email: zhang@itcs.tsinghua.edu.cn. Supported in part by the National Natural Science Foundation of China Grant 60553001, the National Basic Research Program of China Grant 2007CB807900 and 2007CB807901. Part of this research was conducted while the author was visiting University of Michigan, Ann Arbor.
[b]Email: shiyy@eecs.umich.edu. Supported in part by the National Science Foundation of the United States under Awards 0347078 and 0622033.

of success probability for any input. In this paper, we allow a quantum protocol to start with an unlimited amount of quantum entanglement. Evidently, we have $Q^*(F) \leq R(F) \leq D(F)$.

A major research theme in communication complexity is to identify the asymptotic behavior of those variants of complexities for specific and often elementary functions. A closely related focus is to identify functions on which the maximum gaps among those complexities are achieved. Despite numerous studies, both types of questions are often difficult to answer. For an overview of the field, an interested reader is referred to [3, 4, 5, 6]. In this paper, we focus on the communication complexity of a class of functions that we call *symmetric XOR* functions, and our main results are tight, or almost tight, characterizations of their deterministic, randomized and quantum complexities.

To state our main results, let us define the necessary notation. Throughout this paper, the length of the inputs to Alice and Bob is denoted by n. The Hamming weight of $z \in \{0,1\}^n$ is denoted by $|z|$. The bit-wise XOR of $x, y \in \{0,1\}^n$ is denoted by $x \oplus y$. A Boolean function $f : \{0,1\}^n \to \{0,1\}$ is *symmetric* if $f(x)$ depends only on $|x|$, for all x.

Definition 1 *A communication problem $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is a* XOR function *if for a Boolean function $f : \{0,1\}^n \to \{0,1\}$, $F(x,y) = f(x \oplus y)$, for all $x, y \in \{0,1\}^n$. It is said to be* symmetric *whenever f is symmetric. A symmetric XOR function is* trivial *if the function or its negation has $f(x) = 0$, for all x, or $f(x) = |x| \mod 2$, for all x.*

If $f \equiv 0$, evidently $D(F) = 0$. If f is the XOR function, $D(F) = 1$ since it suffices for Alice to send $b = |x| \mod 2$ and Bob then calculates $b + |y| \mod 2 = F(x,y)$. For nontrivial symmetric XOR functions, we have the following.

Theorem 1 *For any nontrivial symmetric XOR function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, $D(F) = \Theta(n)$.*

To prove the above result, we make use of the following fact that relates $D(F)$ to the rank of the matrix $M_F = [F(x,y)]_{x,y \in \{0,1\}^n}$, denoted by $\mathrm{rank}(M_F)$.

Lemma 1 ([7]) *For any $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, $D(F) = \Omega(\log rank(M_F))$.*

It turns out that for a XOR function F, $\mathrm{rank}(M_F)$ is precisely the number of non-zero Fourier coefficients of f. Recall that the Fourier coefficient $\hat{f}(w)$, where $w \in \{0,1\}^n$, is defined as

$$\hat{f}(w) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot w} f(x). \tag{1}$$

Our main technical contribution is the following lemma.

Lemma 2 *For all sufficiently large n, and any symmetric function $f : \{0,1\}^n \to \{0,1\}$ other than the constant 0 function, the parity function and their negations, there exists $w \in \{0,1\}^n$ such that $\hat{f}(w) \neq 0$ and $n/16 \leq |w| \leq 15n/16$.*

By the symmetry of f, the above lemma implies that $\hat{f}$ has $2^{\Omega(n)}$ non-zero Fourier coefficients, thus $\mathrm{rank}(M_F) = 2^{\Omega(n)}$. Theorem 1 then follows from Lemma 2. Another consequence is that $D(M_F) = \Theta(\log \mathrm{rank}(M_F))$ for all symmetric XOR functions, since both $D(F)$ and $\mathrm{rank}(M_F)$ is a constant when F is trivial. That is, symmetric XOR functions satisfy the Log-Rank Conjecture of Lovász and Saks [8], which states that for all Boolean functions F, $D(F) = \log^{\Omega(1)} \mathrm{rank}(M_F)$.

We now turn to our second main result, which is on the randomized and the quantum complexities of symmetric XOR functions. The following two parameters of F are critical to the complexities.

Definition 2 *Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a symmetric XOR function, and $F(x,y) = S(|x \oplus y|)$, where $S : \{0,1,\cdots,n\} \to \{0,1\}$. Define $r_0 = r_0(F)$ and $r_1 = r_1(F)$ to be the minimum numbers r'_0 and r'_1, respectively, such that $r'_0, r'_1 \leq n/2$, and $S(k) = S(k+2)$, for any $k \in [r'_0, n - r'_1)$. Define $r = r(F) = \max\{r_0, r_1\}$.*

Theorem 2 *For any symmetric XOR function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, $Q^*(F) = \Omega(r)$, and $R(F) = O(r \log^2 r \log\log r)$.*

A corollary of the above theorem is the confirmation of the so-called Log-Equivalence Conjecture [9], when restricted to symmetric XOR functions. The Log-Equivalence Conjecture states that quantum and randomized communication complexities of any Boolean functions are polynomially related.

Before we give the details of our proofs, we relate our results to some other closely related works. That we focus on symmetric XOR functions was inspired by Razborov's work [10] on what he called "symmetric predicates" and subsequent works. A function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is a symmetric predicate if $F(x,y) = S(|x \wedge y|)$, where $S : \{0,1,...,n\} \to \{0,1\}$ and $x \wedge y \in \{0,1\}^n$ is the bit-wise AND of x and y. Let ℓ_0 and ℓ_1 be the minimal integers such that $\ell_0, \ell_1 \leq n/2$ and that S is constant in $[\ell_0, n - \ell_1)$. Razborov showed that $Q^*(F) = \Theta^*(\sqrt{n\ell_0} + \ell_1)$. Our quantum lower bound is a technical consequence of Razborov's lower bound. Our classical upper bound follows the same strategy of Huang et al. [11] in constructing a $O(d \log d)$-bits randomized protocol to decide if $|x \oplus y| > d$.

We prove Theorem 1 by Fourier analysis of Boolean functions, which is a powerful tool for the study of Boolean functions complexity. The course notes [12] provide an excellent survey on the subject. The closest result to Lemma 2 that we are aware of is by Lipton et al. [13] on a quantity $\Delta(n)$, which is the minimum integer n' such that any symmetric f other than the parity functions and the constant 0 or 1 functions has a non-zero Fourier coefficient $\hat{f}(w)$ with $1 \leq |w| \leq n'$. They showed that $\Delta(n) = O(n/\log n)$, which has applications in computational learning theory. Their method, however, does not seem to be applicable for our question.

Finally, we note that class of XOR functions is a subset of three classes of functions studied previously.

(i) Shi and Zhu [9] studied what they called *block-composed functions*, i.e. functions $F : \{0,1\}^{kn} \times \{0,1\}^{kn} \to \{0,1\}$ that can be represented as $F(x_1, x_2, ..., x_n, y_1, y_2, ..., y_n) = f(g(x_1, y_1), g(x_2, y_2), ..., g(x_n, y_n))$, for all $x_i, y_i \in \{0,1\}^k$, and some functions $f : \{0,1\}^n \to \{0,1\}$, $g : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}$. Write such an F as $f \Box g$. An XOR function is thus $f \Box \oplus$ with $k = 1$. They showed that $Q^*(F)$ is lower-bounded by the approximate polynomial degree of f when certain conditions on k and g are satisfied. Their bound does not apply to XOR functions as they require k to be sufficiently large, and that not all XOR functions are block-composed functions with a $k \geq 2$.

(ii) Independent of [9], Sherstov[14] studied what he called *pattern matrices*. Those are block-composed functions for a fixed g, $g(x,(y,w)) = x_y \oplus w$, where $x \in \{0,1\}^k$ is Alice's block, (y,w) is Bob's block with $y \in \{1,2,...,k\}$, $w \in \{0,1\}$, and x_y is the y'th bit of x. Sherstov showed that for such functions $Q^*(F)$ is lower bounded by the

approximate polynomial degree of f, multiplied by $\log k$. A XOR function is such a function with $k = 1$. However, Sherstov's lower bound vanishes on this case.

(iii) Aaronson [15] studied what he called *subset problems*. Let G be a group and S be a subset of G. A subset problem Subset(G, S) is to decide if $x + y \in S$, where $x, y \in G$ are the inputs of Alice and Bob, respectively. A XOR function is a subset function with G being the n-fold direct sum of the 2 element finite field. Aaronson derived a general lower bound on the *one-way* quantum communication complexity of a subset problem. In contrast, we study the two-way communication complexity.

We give the proofs for our main theorems in the next two sections before concluding with a discussion on open problems.

2 Deterministic communication complexity

In this section we prove Theorem 1, which states that any nontrivial symmetric XOR function must have linear deterministic communication complexity.

Proof of Theorem 1. Let $H = [(-1)^{x \cdot y}]_{x,y \in \{0,1\}^n}$ be the $2^n \times 2^n$ Hadamard Matrix and D_F be the diagonal matrix with the diagonal entries $[\hat{f}(w)]_{w \in \{0,1\}^n}$. Then $M_F = HD_FH$. Since H is orthogonal,

$$\operatorname{rank}(M_F) = \left|\{w \in \{0,1\}^n : \hat{f}(w) \neq 0\}\right|. \tag{2}$$

By the symmetry assumption on f, $\hat{f}$ is also symmetric. That is, if $\hat{f}(w) \neq 0$, $\hat{f}(w') \neq 0$ for all w' with $|w'| = |w|$. Therefore, by Lemma 2, to be proved below, $\left|\{w : \hat{f}(w) \neq 0\}\right| = 2^{\Omega(n)}$. The theorem follows from Eqn. (2) and Lemma 1 □.

We now prove Lemma 2, which states that for any symmetric $f : \{0,1\}^n \to \{0,1\}$, there exists a $w \in \{0,1\}^n$ such that $|w| \in [n/16, 15n/16]$ and $\hat{f}(x) \neq 0$.

Proof of Lemma 2. Suppose that for a symmetric f, $\hat{f}(w) = 0$ for all $w \in \{0,1\}^n$ with $|w| \in [n/16, 15n/16]$, we shall prove that f is one of the four excluded functions.

Let $f_k = f(1^k 0^{n-k})$ and $\hat{f}_k = \hat{f}(1^k 0^{n-k})$. And for a polynomial g and an integer s, let $T_s(g)$ denote the coefficient of the monomial x^s in g and G be the polynomial $\sum_{s=0}^{n} f_s x^{n-s}$. Then by the symmetry of f and $\hat{f}$,

$$\hat{f}_k = \frac{1}{2^n} \sum_{y \in \{0,1\}^n} f(y)(-1)^{1^k 0^{n-k} \cdot y} = \frac{1}{2^n} \sum_{y} f(y)(-1)^{y_1 + \cdots + y_k}.$$

Grouping y by its Hamming weight, we have

$$\hat{f}_k = \frac{1}{2^n} \sum_{s=0}^{n} f_s \sum_{|y|=s} (-1)^{y_1 + \cdots + y_k} = \frac{1}{2^n} \sum_{s} f_s \sum_{t=0}^{k} (-1)^t \binom{k}{t} \binom{n-k}{s-t}.$$

Since $\sum_t (-1)^t \binom{k}{t} \binom{n-k}{s-t}$ is the coefficient of the monomial x^s in the polynomial $(1-x)^k(1+x)^{n-k}$ and f_s is that of x^{n-s} in the polynomial G,

$$\hat{f}_k = \frac{1}{2^n} \sum_{s} f_s T_s((1-x)^k(1+x)^{n-k}) = \frac{1}{2^n} T_n(G \cdot (1-x)^k(1+x)^{n-k}).$$

Thus the assumption that $\hat{f}_k = 0$ for all $t \leq k \leq n-t$ is equivalent to

$$T_n(G \cdot (1-x)^k (1+x)^{n-k}) = 0, \quad \text{for all } k,\ t \leq k \leq n-t.$$

It follows that for any $t \leq i, j \leq n-t$ with $i+j \leq n$,

$$\begin{aligned} 0 &= \sum_{s=i}^{n-j} T_n\left(G \cdot (1-x)^s (1+x)^{n-s} \binom{n-i-j}{s-i}\right) \\ &= T_n\left(G \cdot (1-x)^i (1+x)^j \sum_{s=i}^{n-j} \binom{n-i-j}{s-i} (1-x)^{s-i} (1+x)^{n-i-j-(s-i)}\right) \\ &= T_n(G \cdot (1-x)^i (1+x)^j \cdot 2^{n-i-j}). \end{aligned}$$

Therefore, for any i, j with $t \leq i, j \leq n-t$ and $i+j \leq n$, we have

$$T_n(G \cdot (1-x)^i (1+x)^j) = 0. \tag{3}$$

Let u be an integer with $t \leq u \leq n/2$. We set $i = u$. Setting $j = u$, and $j = u+1$, respectively, Eqn. (3) becomes

$$T_n(G \cdot (1-x^2)^u) = 0,$$

and

$$0 = T_n(G \cdot (1-x^2)^u (1+x)) = T_n(G \cdot (1-x^2)^u) + T_{n-1}(G \cdot (1-x^2)^u).$$

Thus

$$T_{n-1}(G \cdot (1-x^2)^u) = 0.$$

Setting $j = u+2$ in Eqn. (3), we have

$$\begin{aligned} 0 &= T_n(G \cdot (1-x^2)^u (1+x)^2) \\ &= T_n(G \cdot (1-x^2)^u) + 2T_{n-1}(G \cdot (1-x^2)^u) + T_{n-2}(G \cdot (1-x^2)^u). \end{aligned}$$

Therefore

$$T_{n-2}(G \cdot (1-x^2)^u) = 0.$$

Continuing this process till $i = u, j = n-u$, we have

$$T_s(G \cdot (1-x^2)^u) = 0, \quad \text{for all } s,\ 2u \leq s \leq n.$$

Expanding $G \cdot (1-x^2)^u$, we have

$$T_s(G \cdot (1-x^2)^u) = T_s\left(\sum_k f_k x^{n-k} \sum_l \binom{u}{l} (-1)^l x^{2l}\right) = \sum_l \binom{u}{l} (-1)^l f_{n-s+2l} = 0.$$

If u is an odd prime, for all l, $1 \leq l \leq u-1$, $u \mid \binom{u}{l}$. Thus

$$u \mid (f_{n-s} - f_{n-s+2u}),$$

since both f_{n-s} and f_{n-s+2u} are either 1 or 0. This implies that $f_{n-s} = f_{n-s+2u}$. That is, for any odd prime $u \in [t, n/2]$, it holds that for any s with $s \leq n-2u$,

$$f_s = f_{s+2u}.$$

Bertrand's Postulate[16] states that for any integer $m > 3$, there is at least one prime number between m and $2m$. So we can take two different primes $p, q \in [t, n/4]$ (recall that $t = n/16$) when $n \geq 32$, such that $f_s = f_{s+2p}$ $(0 \leq s, s+2p \leq n)$, and $f_s = f_{s-2q}$ $(0 \leq s-2q, s \leq n)$. Using Chinese Remainder Theorem, we will get two positive integers a, b such that $2ap - 2bq = 2$. Because $2p + 2q < n$, starting from arbitrary s, every time we can either add $2p$ or subtract $2q$ to keep it in the interval $[0, n]$, until we have done a additions or b subtractions. If all a additions have been done, we continue to subtract $2q$ until the b subtractions have been done. Finally we will get $s + 2$. This implies $f_s = f_{s+2}$ for arbitrary s. Then f must be one of the four functions excluded in the statement of the theorem $\Box$.

3 Randomized and quantum complexities

In this section, we prove theorem 2. The proof has two parts, a lower bound proof and a protocol. Both proofs are along the same line as those in Huang et al. [11] on the Hamming distance functions.

Proposition 3 *For any symmetric XOR function $F(x, y) = S(|x \oplus y|)$, $Q^*(F) = \Omega(r)$.*

To prove this lower bound, we restrict the problem on those pairs of inputs with an equal Hamming weight. For an integer k, where $0 \leq k \leq n$, define $X_k = Y_k = \{x \in \{0,1\}^n : |x| = k\}$. For a function $S : \{0, 1, \cdots, n\} \to \{0, 1\}$, let F_S be the function $F_S(x, y) = S(|x \oplus y|)$. The restriction of F_S on $X_k \times Y_l$, where $0 \leq k, l \leq n$, is denoted by $F_{k,l,S}$. We shall use the following key lemma of Razborov [10].

Lemma 3 (Razborov[10]) *Suppose $k \leq n/4$ and $l \leq k/4$. Let $S : \{0, 1, \cdots, k\} \to \{0, 1\}$ be any Boolean predicate such that $S(l) \neq S(l-1)$. Let $f_{n,k,S} : X_k \times Y_k \to \{0, 1\}$ be the function such that $f_{n,k,S}(x, y) = S(|x \wedge y|)$. Then $Q^*(f_{n,k,S}) = \Omega(\sqrt{kl})$.*

Proof of Proposition 3. Any XOR function $F(x, y) = S(|x \oplus y|)$ can be decomposed into two parts $F = F_{S_0} \wedge F_{S_1}$, where F_{S_0} and F_{S_1} are XOR functions with the underlying functions $S_0, S_1 : \{0, 1, \cdots, n\} \to \{0, 1\}$ defined as follows: $S_0(t) = S(t)$ when t is even, otherwise $S_0(t) = 0$; $S_1(t) = S(t)$ when t is odd, otherwise $S_1(t) = 0$. Since Alice and Bob can compute the parity of $|x \oplus y|$ through a $O(1)$-bits protocol,

$$Q^*(F_{S_0}), Q^*(F_{S_1}) \leq Q^*(F) + O(1). \tag{4}$$

Let $r_0^0 = r_0(S_0)$ and $r_1^0 = r_1(S_0)$. We have $S_0(r_0^0 - 1) \neq S_0(r_0^0 + 1)$. We want to show $Q^*(F_{S_0}) = \Omega(r_0^0)$.

If $r_0^0 \leq 3n/8$, this will be proved by constructing another predicate $S' : [k] \to \{0, 1\}$ for Lemma 3 by $S'(t) = S_0(2k - 2t)$, here k is a parameter determined later. We define a predicate $f_{n,k,S'}$ on $X_k \times Y_k$ by $f_{n,k,S'} = S'(x \wedge y)$. Because $|x \oplus y| = |x| + |y| - 2|x \wedge y|$ for any $x \in X_k$ and $y \in Y_k$, the two functions $F_{k,k,S}$ and $f_{n,k,S'}$ are identical. Therefore, $Q^*(f_{n,k,S'}) = Q^*(F_{k,k,S_0})$.

Since $S_0(r_0^0 - 1) \neq S_0(r_0^0 + 1)$, then $S'(k - (r_0^0 - 1)/2) \neq S'(k - (r_0^0 + 1)/2)$. For $r_0^0 < 3n/8$, let $k = [2r_0^0/3]$, we have $k \leq n/4$ and $l \leq k/4$. By lemma 3, we have $Q^*(F_{S_0}) \geq Q^*(F_{k,k,S_0}) = Q^*(f_{n,k,S'}) \geq \Omega(\sqrt{kl}) = \Omega(r_0^0)$.

When $r_0^0 \geq 3n/8$, we will reduce to the previous case. Let $n' = 3n/4$ and consider the function $S_0' : [n'] \to \{0, 1\}$ defined by $S_0'(x) = S_0(n - n' + x)$. Notice that the corresponding r_0^0 for S_0' is $r_0^0 - (n - n')$, which satisfies $r_0^0 - (n - n') \leq n/2 - (n - n') = n/4 \leq 9n/32 = 3n'/8$,

and that $F_{S_0'}(x,y) = S_0'(|x \oplus y|)$ is embedded to F. Therefore, $Q^*(F_{S_0}) \geq Q^*(F_{S_0'}) = \Omega(r_0^0 - (n-n')) = \Omega(n) = \Omega(r_0^0)$.

Consider the function S_1' with $S_1'(x) = S_1(1+x)$. Since $F_{S_1'}(x,y) = F_{S_1}(0x, 1y)$, $F_{S_1'}$ is embedded in F_{S_1}. Let $r_0^1 = r_0(S_1)$ and $r_1^1 = r_1(S_1)$. Then the corresponding $r_0(S_1') = r_0^1 - 1$. Similar to the case of S_0, we have $Q^*(F_{S_1}) \geq Q^*(F_{S_1'}) \geq \Omega(r_0^1 - 1) = \Omega(r_0^1)$.

Since $r_0 = \max(r_0^0, r_0^1)$, Eqn. [4] implies that $Q^*(F) = \Omega(r_0)$. Consider $\bar{S}(x) = S(n-x)$, then the corresponding r_0 of $\bar{S}$ is exactly r_1. Since $F_{\bar{S}}(x,y) = F(\bar{x}, y)$ (here $\bar{x}$ means the bit-wise flipping of x), $F_{\bar{S}}$ and F are actually equivalent so that we have $Q^*(F) = Q^*(F_{\bar{S}}) = \Omega(r_1)$. Combining the lower bounds by r_0 and r_1, we have $Q^*(F) = \Omega(\max(r_0, r_1))$ □.

We now turn to the construction of a randomized protocol for symmetric XOR functions. Recall that the Hamming distance function $\mathrm{HAM}_{n,d}$ is defined as follows: $\mathrm{HAM}_{n,d}(x,y) = 1$ iff $|x \oplus y| > d$. Huang et al. [11] constructed an efficient randomized *one-way* communication protocol for $\mathrm{HAM}_{n,d}$, where Bob is not allowed to send messages to Alice.

Lemma 4 (Huang et al. [11]) *There is a randomized one-way communication protocol for $HAM_{n,d}$ using $O(d \log d)$ bits.*

We will make use of their protocol to prove the following.

Proposition 4 *There is a $O(r \log^2 r \log\log r)$ randomized protocol for any symmetric XOR function $F(x,y) = f(x \oplus y)$.*

Proof. We construct a public-coin randomized protocol as following. By solving $\mathrm{HAM}_{n,r}$ and $\mathrm{HAM}_{n,n-r}$ using $O(r \log r)$ bits (to make the final failure probability to be small, this step will be repeated for constant times), Alice and Bob decide which of the three intervals that $|x \oplus y|$ lies: $[r, n-r]$, $[0, r)$, or $[n-r, n]$, with high probability. If $|x \oplus y| \in [r, n-r]$, by the definition of r, F only depends on the parity of $|x \oplus y|$, which can be computed in $O(1)$ bits of communication. If $|x \oplus y| \in [0, r) \cup (n-r, n]$, Alice and Bob apply a binary search for $|x \oplus y|$. Each time they check a Hamming distance instance $Ham_{n,k}$ for some $k \in [0, r) \cap (n-r, n]$. The exact value of $|x \oplus y|$ can be determined in $O(\log r)$ rounds. To output a correct answer with probability more than $2/3$, it suffices to make sure that the failure probability is $\leq 1/(4 \log r)$ in every round. This can be done by repeating the Hamming distance instance $\Theta(\log\log r)$ times in each round. By Lemma 4, each round uses at most $O(r \log r \log\log r)$ bits. The total cost of this protocol is therefore $O(r \log^2 r \log\log r)$ □.

In the above protocol, Alice and Bob interactively send messages to determine the exact $|x \oplus y|$ by binary search in $O(\log r)$ rounds. When Bob are not allowed to send information back to Alice, they need to enumerate all possible $|x \oplus y|$ in the interval $[0, r) \cap (n-r, n]$. Enumeration of $|x \oplus y| = d$ can be done by solving two Hamming distance problems $\mathrm{HAM}_{n,d-1}$ and $\mathrm{HAM}_{n,d}$. To obtain large success probability finally, each problem must be repeated $O(\log r)$ times. This leads to the following.

Proposition 5 *There is a $O(r^2 \log^2 r)$ one-way randomized protocol for any symmetric XOR function $F(x,y) = f(x \oplus y)$.*

The lower bound in Theorem 3 is still true for one-way quantum communication because one-way complexity is always larger than the corresponding two-way complexity. There remains a quadratic gap between the lower bound and upper bound for the one-way complexity.

4 Discussion

In addition to the above-mentioned question regarding one-way communication complexity, we state two other open problems. Our result implies the correctness of the Log-Rank Conjecture for the class of symmetric XOR functions. It will be interesting to extend this consequence to the asymmetric case, and to make use of the fact that $\text{rank}(M_F) = |\{w : \hat{f}(w) \neq 0\}|$ remains true for asymmetric f.

We may also consider the unbounded-error communication complexity of XOR functions. The unbound-error complexity, equivalent with logarithm of sign-rank, has applications in other areas such as circuit complexity, rigidity and PAC learning. Sherstov[17] proved that the unbounded-error complexity of $S(|x \wedge y|)$ is essentially $|\{t : S(t) \neq S(t+1)\}|$. We conjecture that the unbounded-error complexity of $S(|x \oplus y|)$ is essentially $|\{t : S(t) \neq S(t+2)\}|$. However, Sherstov's approach does not seem to work for XOR functions because the core technique used — pattern matrix cannot be embedded in a XOR function.

Acknowledgements

We would like to thank Rani Hod for pointing out a mistake in our earlier draft and the anonymous reviewers for helping us improve the presentation of this paper.

References

1. A. C. Yao (1979), *Some complexity questions related to distributive computing*, in:Proceedings of the 11th Annual ACM Symposium on Theory of Computing, pp. 209-213.
2. A. C. Yao (1993), *Quantum circuit complexity*, in:Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science, pp. 352-361.
3. E. Kushilevitz and N. Nisan (1997), *Communication complexity*, Cambridge University Press, Cambridge.
4. G. Brassard (2004), *Quantum Communication Complexity: A Survey*, ISMVL 56.
5. H. Buhrman (2001), *Quantum Computing and Communication Complexity*, Current Trends in Theoretical Computer Science, pp 664-679.
6. A. Sherstov (2008), *Communication Lower Bounds Using Dual Polynomials*, CoRR abs/0805.2135.
7. K. Mehlhorn and E. Schmidt (1982), *Las Vegas is better than determinism in VLSI and distributed computing*, in: Proceedings of the 14th annual ACM symposium on Theory of computing, pp 330-307.
8. L. Lovász and M. Saks (1988), *Lattices, Möbius functions and communication complexity*, in:Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science, 1988, pp 330-337.
9. Y. Shi and Y. Zhu (2007), *Quantum communication of block-composed function*, in:Arxiv preprint arXiv:0710.0095.
10. A. Razborov (2003), *Quantum communication complexity of symmetric predicates*, Izvestiya Math. 67(1)(2003)145-159 (English version); also in: quant-ph/0204025.
11. W. Huang, Y. Shi, S. Zhang and Y. Zhu (2006), *The communication complexity of the Hamming distance problem*, information processing letter, 99(4):149-153.
12. R. O'Donnell (2007), *lecture notes on Analysis of Boolean Functions*, available at `http://www.cs.cmu.edu/~odonnell/boolean-analysis/`.
13. R. Lipton, E. Markakis, A. Mehta and K. Vishnoi (2005), *On the Fourier Spectrum of Symmetric Boolean Functions with Applications to Learning Symmetric Juntas*, in: Proceedings of the 20th IEEE Annual Conference on Computational Complexity, pp 112- 119.

14. A. Sherstov (2008), *The pattern matrix method for lower bounds on quantum communication*, in: Proceedings of the 40th annual ACM symposium on Theory of computing, pp 85-94.
15. S. Aaronson (2004), *Limitations of Quantum Advice and One-way Communication*, in: Proceedings of the 19th IEEE Annual Conference on Computational Complexity, pp 320-332.
16. G. H. Hardy and E. M. Wright (1938), *An Introduction to the Theory of Numbers*, Oxford University Press.
17. A. Sherstov (2008), *Unbounded-Error Communication Complexity of Symmetric Functions*, in:Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science.