A Lifting Theorem with Applications to Symmetric Functions*

Arkadev Chattopadhyay†[1] **and Nikhil S. Mande**‡[2]

1 **School of Technology and Computer Science, TIFR, Mumbai, India**
arkadev.c@tifr.res.in

2 **School of Technology and Computer Science, TIFR, Mumbai, India**
nikhil.mande@tifr.res.in

Abstract

We use a technique of "lifting" functions introduced by Krause and Pudlák [13], to amplify degree-hardness measures of a function to corresponding monomial-hardness properties of the lifted function. We then show that any symmetric function F projects onto a "lift" of another suitable symmetric function f. These two key results enable us to prove several results on the complexity of symmetric functions in various models, as given below:

1. We provide a characterization of the *approximate spectral norm* of symmetric functions in terms of the spectrum of the underlying predicate, affirming a conjecture of Ada et al. [1] which has several consequences[1] (cf. [1]).
2. We also characterize symmetric functions computable by quasi-polynomial sized Threshold of Parity circuits, resolving a conjecture of Zhang [24].
3. We show that the approximate spectral norm of a symmetric function f characterizes the (quantum and classical) bounded error communication complexity of $f \circ \mathsf{XOR}$.
4. Finally, we characterize the weakly-unbounded error communication complexity of symmetric XOR functions, resolving a weak form of a conjecture by Shi and Zhang [25].[2]

1998 ACM Subject Classification F.1.1 Models of Computation

Keywords and phrases Symmetric functions, lifting, circuit complexity, communication complexity

Digital Object Identifier 10.4230/LIPIcs.FSTTCS.2017.23

1 Introduction

For any domain $\mathcal{A}$ and range $\mathcal{R}$, an n-variate function $f : \mathcal{A}^n \to \mathcal{R}$ is called *symmetric* if for all $x_1, \ldots, x_n \in \mathcal{A}$ and every permutation $\sigma \in S_n$, one has $f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Symmetric functions are a very natural and basic class of functions, denoted by SYMM. There are several works about symmetric functions in different contexts in complexity theory that reveal their beautiful structure. As it is too numerous to list all of them out, we

* A full version of the paper is available at [6], https://arxiv.org/abs/1704.02537.
† Arkadev Chattopadhyay is partially supported by a Ramanujan fellowship of the DST.
‡ Nikhil S. Mande is partially supported by a TCS fellowship.
1 This has also been recently reported, after an early version of our manuscript was put up in the public domain, by Ada, Fawzi and Kulkarni [2] using a matrix theoretic result of Razborov [19], and other results.
2 The conjecture has been reported to be recently solved by independent works of Hatami and Qian [10] and Ada et al. [2]. Our techniques vary from theirs, a detailed comparison to related work can be found in Section 1.3.

very briefly recall a few here, some of which is relevant for this work: Paturi's famous theorem [17] characterizing the approximate degree of symmetric functions, Szegedy's [21] theorem characterizing functions that have bounded symmetric communication complexity making crucial use of symmetric functions, strong correlation bounds against low degree symmetric functions (polynomials) by Cai, Green and Thierauf [5], Razborov's theorem [19] characterizing the quantum bounded error communication complexity of $\mathsf{SYMM} \circ \mathsf{AND}$ and Sherstov's [20] theorem characterizing the unbounded error communication complexity of the same class of functions. More recently, and of particular relevance to this work, Shi and Zhang [25] characterized the (quantum) bounded-error complexity of $\mathsf{SYMM} \circ \mathsf{XOR}$ and Ada, Fawzi and Hatami [1] characterized the spectral norm of all symmetric functions. Shi and Zhang conjectured a certain characterization of the *unbounded-error* complexity of $\mathsf{SYMM} \circ \mathsf{XOR}$. Ada et al. conjectured a characterization of the *approximate* spectral norm of symmetric functions that in a way would extend Paturi's [17] characterization of the approximate degree of symmetric functions. Though these conjectures do not seem related on first glance, our work is motivated by them. In addition to proving the conjecture of Ada et al., we provide, among other things, the first characterization of the *weakly unbounded-error* communication complexity of $\mathsf{SYMM} \circ \mathsf{XOR}$. Both our results make use of a simple but somewhat surprising closure-like property of symmetric functions. The discovery of this property is one of our main technical contributions.

Krause and Pudlák [13] introduced a notion of 'lifting' functions to increase their hardness. Using this, they derived a technique to lower bound the sign monomial complexity (equivalently $\mathsf{THR} \circ \mathsf{XOR}$ circuit size) of a lifted function, f^{op}, in terms of the sign degree of f. As the lift of an AC^0 function can easily be seen to remain in AC^0, they were able to prove exponential lower bounds on the signed monomial complexity of a function in AC^0 using known sign degree lower bounds of AC^0 functions [15]. However, it is not clear how to use this lifting technique to prove lower bounds against other classes of functions. This lift is now more widely known as composition with the *indexing* gadget on two bits. The lift of f is denoted by $f \circ \mathsf{IND}_2$. Various notions of hardness amplification on composing with the indexing gadget have been studied to give breakthrough results in communication complexity [18, 8, 9].

In this work, we use the same notion of lifting to prove lower bounds of different monomial complexity measures of *symmetric* functions. In doing so, we demonstrate the robustness of the lifting technique to prove monomial complexity lower bounds on classes of functions other than AC^0. A technical hurdle that we overcome is to show that any symmetric function can 'project' onto the lift of a suitably defined symmetric function.

1.1 Our results

In this section, we provide a detailed summary of our results.

▶ **Definition 1** (Monomial projection)**.** We call a function $g : \{-1,1\}^m \to \{-1,1\}$ a *monomial projection* of a function $f : \{-1,1\}^n \to \{-1,1\}$ if $g(x_1,\ldots,x_m) = f(M_1,\ldots,M_n)$, where each M_i is a monomial in the variables $x_1,\ldots,x_m$.

We denote the *Hamming weight* of a string $x \in \{-1,1\}^n$ to be $|x| = |\{i \in [n] : x_i = -1\}|$ (this is a natural definition since we view -1 as true, and 1 as false). For a symmetric function $f : \{-1,1\}^n \to \{-1,1\}$, define its *spectrum* or *predicate* $D_f : \{0,1,\ldots,n\} \to \{-1,1\}$ by $D_f(i) = f(x)$ where $x \in \{-1,1\}^n$ is such that $|x| = i$. Note that the spectrum (predicate) of a symmetric function is well defined. For any $f : \{-1,1\}^n \to \{-1,1\}$, define the function $f^{op} : \{-1,1\}^{3n} \to \{-1,1\}$ as follows.

$$f^{op}(x_1,\ldots,x_n,y_1,\ldots,y_n,z_1,\ldots,z_n) = f(u_1,\ldots,u_n). \tag{1}$$

where for all i, $u_i = (x_i \wedge z_i) \vee (y_i \wedge \bar{z}_i)$. Intuitively speaking, the value of z_i decides whether to feed x_i or y_i as the ith input to f. This method of lifting f was introduced by Krause and Pudlák [13].

The following lemma shows how f^{op} is a monomial projection of a symmetric function, if f was symmetric itself.

▶ **Lemma 2** (Projection Lemma). *Given a symmetric function $F : \{-1,1\}^{4n} \to \{-1,1\}$, defined by the predicate $D_F : [4n] \to \{-1,1\}$, consider the symmetric function $f : \{-1,1\}^n \to \{-1,1\}$ defined by the predicate $D_f(b) = D_F(2b+n)$ for all $b \in \{0,1,\ldots,n\}$. Then, f^{op} is a monomial projection of F.*

For any function $f : \{-1,1\}^n \to \{-1,1\}$, let $f = \sum_{S\subseteq[n]} c_S \prod_{i\in S} x_i$ be the unique multilinear expansion of f. Define the *weight* of f, denoted by $wt(f)$ to be $\sum_{S\subseteq[n]} |c_S|$.[3] The sign degree of a function f, denoted $\deg_{\pm}(f)$, is defined to be the minimum degree required by a polynomial to sign represent f on all inputs.

▶ **Definition 3** (Polynomial margin). For a polynomial of weight 1, say p, which sign represents a function f, we say that p represents f with a margin of value $\min_{x\in\{-1,1\}^n} f(x)p(x)$. Define the *polynomial margin* of f, denoted $m(f)$, as follows.

$$m(f) = \max_{p:wt(p)=1} \min_{x\in\{-1,1\}^n} f(x)p(x). \tag{2}$$

To the best of our knowledge, such a definition of the polynomial margin of a function does not appear in the past literature, although very similar notions have been studied. As we note in Theorem 24, this is a useful quantity in characterizing the weakly-unbounded error communication complexity of XOR functions.

▶ **Definition 4** (Approximate weight). Define the ϵ-approximate weight of a function $f : \{-1,1\}^n \to \{-1,1\}$, denoted by $wt_\epsilon(f)$ to be the weight of a minimum weight polynomial such that for all $x \in \{-1,1\}^n$, $|p(x) - f(x)| < \epsilon$.[4]

▶ **Definition 5** (Signed monomial complexity). The *signed monomial complexity* of a function $f : \{-1,1\}^n \to \{-1,1\}$, denoted by $\mathrm{mon}_{\pm}(f)$, is the minimum number of monomials required by a polynomial p to sign represent f on all inputs.

Note that the signed monomial complexity of a function f exactly corresponds to the minimum size Threshold of Parity circuit computing it.

Let us define a notion of error in a pointwise approximation of a function by low degree polynomials. This notion is studied widely in classical approximation theory.

Note that we do not restrict the weight of the approximating polynomial in this case.

$$\varepsilon_d(f) \triangleq \min_{p:deg(p)\leq d} \left(\max_{x\in\{-1,1\}^n} |p(x) - f(x)| \right). \tag{3}$$

▶ **Definition 6** (Approximate degree). For any function $f : \{-1,1\}^n \to \{-1,1\}$ and polynomial $p : \{-1,1\}^n \to \mathbb{R}$, we say that p approximates f uniformly to error ϵ if for all $x \in \{-1,1\}^n$, $|p(x) - f(x)| \leq \epsilon$. The ϵ-approximate degree of f, denoted $\widetilde{\deg}_\epsilon(f)$ is the minimum degree of a polynomial p which approximates f uniformly to error ϵ.

[3] Note that this notion coincides with $||\hat{f}||_1$, the spectral norm of f. However, for the purposes of this paper, we shall use the former notation.

[4] This notion coincides with the notion of the *ϵ-approximate spectral norm* of f, denoted by $||\hat{f}||_{1,\epsilon}$.

The following lemma, translates degree-hardness properties of f to monomial-hardness properties of f^{op}. The proof of this lemma is based on ideas from [13].

▶ **Lemma 7** (Lifting Lemma). *Let $f : \{-1,1\}^n \to \{-1,1\}$ be any function.*
1. *If $\varepsilon_d(f) > 1 - 2^{-d}$ for some $d \geq 2$, then $m(f^{op}) \leq 2^{-c'd}$ for any constant $0 < c' < 1 - \frac{1}{d}$.*
2. $\mathrm{mon}_{\pm}(f^{op}) \geq 2^{\deg_{\pm}(f)}$. *(This part was proved in [13].)*
3. $wt_{1/3}(f^{op}) \geq 2^{c \cdot \widetilde{\deg}_{2/3}(f)}$ *for any constant $c < 1 - 3/\widetilde{\deg}_{2/3}(f)$.*

1.1.1 Applications to boolean function analysis

▶ **Definition 8.** Let $F : \{-1,1\}^n \to \{-1,1\}$ be a symmetric function. Define $r_0 = r_0(F), r_1 = r_1(F)$ to be the minimum integers such that $r_0, r_1 \leq n/2$ and $D_F(i) = D_F(i+2)$ for all $i \in [r_0, n - r_1)$. Define $r = r(F) = \max\{r_0, r_1\}$.

Using Projection Lemma, Lifting Lemma, and Paturi's theorem [17], we resolve the following conjecture by Ada et al. [1].

▶ **Theorem 9** (Conjecture 1 in [1]). *Let $F : \{-1,1\}^{4n} \to \{-1,1\}$ be any symmetric function such that $r(F) \geq 5$. Then, there exists a universal constant $c_1 > 0$ such that*

$$\log(wt_{1/3}(F)) \geq c_1 \cdot r(F).$$

One consequence of Theorem 9 is an analog of Paturi's theorem [17]. Paturi characterized the approximate degree of all symmetric functions, and we obtain a characterization of the approximate monomial complexity of symmetric functions F, in terms of $r(F)$. Let $\mathrm{mon}_{1/3}(F)$ denote the minimum number of monomials required by a polynomial to sign represent F at all points.

▶ **Theorem 10** (Approximate monomial complexity of symmetric functions). *For a symmetric function $F : \{-1,1\}^{4n} \to \{-1,1\}$,*

$$\log\left(\mathrm{mon}_{1/3}(F)\right) = \Theta^*(r(F)).$$

Theorem 10 was proved by Ada et al. [1] assuming Theorem 9. We refer the reader to [1] for a proof.

Define the *odd-even* degree of a symmetric function f, which we denote by $\deg_{oe}(f)$, to be $|i \in \{0, 1, \ldots, n-2\} : D_f(i) \neq D_f(i+2)|$.

Using Projection Lemma and Lifting Lemma, we resolve the following conjecture by Zhang [24].

▶ **Theorem 11** (Conjecture 1 in [24]). *A symmetric function $f : \{-1,1\}^n \to \{-1,1\}$ is computable by a quasi-polynomial size Threshold of Parity circuit if and only if $\deg_{oe}(f) = \log^{O(1)} n$.*

1.1.2 Applications to communication complexity of symmetric XOR functions

We consider two models of randomized communication. The first was introduced by Yao [22]. Two players, say Alice and Bob, receive a pair of inputs $x \in X$ and $y \in Y$ respectively. They want to jointly evaluate a function $F : X \times Y \to \{-1,1\}$ on the pair (x,y) by using a communication protocol that minimizes the total number of bits communicated in the worst case. The protocol is probabilistic with the requirement that $\Pr[\Pi(x,y) = F(x,y)] \geq$

$1/2 + 1/3$. The goal of the players is to design an *efficient* protocol meeting this requirement that minimizes the cost. The cost of the best protocol for computing F in this model is called its *bounded error* complexity, denoted by $R_{1/3}(F)$. We consider the bounded error complexity of XOR functions. Namely, Alice and Bob are given inputs $x, y \in \{-1,1\}^n$ and wish to compute $f(x \oplus y)$ for some given function f, where $x \oplus y$ denotes the bitwise xor of x and y.

Lee and Shraibman [14] showed that the log of the approximate weight of f is roughly a lower bound on the (quantum) bounded-error complexity of $f \circ \mathsf{XOR}$, for every f. Using our Projection Lemma and Lifting Lemma, along with this result of Lee and Shraibman [14], and an upper bound from [25] on the communication complexity of symmetric XOR functions, we obtain a characterization of the bounded error communication complexity in terms of the approximate weight of the base function.

▶ **Theorem 12.** *For any symmetric function* $f : \{-1,1\}^n \to \{-1,1\}$,

$$R_{1/3}(f \circ \mathsf{XOR}) = \Theta^*(\log wt_{1/3}(f)).$$

▶ Remark. As the method of [14] applies to even quantum communication, Theorem 12 gives even a characterization of the quantum bounded-error complexity. Recently, Zhang [23] gave upper bounds on the quantum bounded-error communication complexity of $f \circ XOR$ in terms of the log of the approximate weight of f, *provided* f has low $\mathbb{F}_2$ degree. Theorem 12 shows that when f is symmetric, then the dependence on $\mathbb{F}_2$ degree is redundant even for classical complexity.

We consider another model of randomized communication, namely the *weakly-unbounded error* model, introduced by Babai et al. [3]. A probabilistic protocol Π computes F with advantage ϵ if the probability that F and Π agree is at least $1/2 + \epsilon$ for all inputs. Denote the cost of such a protocol to be $R_\epsilon(F)$. We add a penalty term to the cost depending on the advantage, and refer to this new cost as the weakly-unbounded error complexity, or PP complexity, of F.

▶ **Definition 13.**

$$\mathsf{PP}(F) = \inf_{\epsilon} \left(R_\epsilon(F) + \log\left(\frac{1}{\epsilon}\right)\right).$$

Klauck [11] showed that the PP complexity is characterized by the well studied notion of discrepancy. Using LP duality in the full version of this paper [6], we show a general tight relationship between discrepancy of $f \circ \mathsf{XOR}$ and the margin complexity of f. Using these facts along with our Projection and Lifting Lemmas, we are able to completely characterize the PP complexity of symmetric XOR functions.

▶ **Theorem 14.** *Let* $F : \{-1,1\}^{4n} \to \{-1,1\}$ *be any symmetric function, and let* $\deg_{oe}(f) = r \geq 4$. *Then, there exists universal constants* $c, c' > 0$ *such that* $cr/\log(n/r) \leq \mathsf{PP}(F \circ \mathsf{XOR}) \leq c' r \log(n)$.

The Log Approximation Rank Conjecture [14] is the analogous version of the well-known Log Rank Conjecture, for the randomized communication complexity model. Let $\mathrm{rank}_\epsilon(M)$ denote the minimum rank of a matrix that ϵ-approximates M entry-wise. It is known that $R_{1/2-\epsilon}(F) \geq \log \mathrm{rank}_{\epsilon'}(M_F)$, where ϵ' is a constant depending on ϵ, and M_F denotes the communication matrix of F. The Log Approximation Rank Conjecture states that the lower bound is tight upto a polynomial factor.

We resolve this conjecture for symmetric XOR functions.

▶ **Theorem 15** (Log Approximation Rank Conjecture for symmetric XOR functions)**.** *Let f be any symmetric function, and $F = f \circ \mathsf{XOR}$. Then, there is a universal constant c such that*

$$\log \operatorname{rank}_{\epsilon'}(M(F)) \leq R_{1/2-\epsilon}(F) \leq \log^c \operatorname{rank}_{\epsilon'}(M(F)).$$

Ada et al. [1] prove Theorem 15 assuming Theorem 9. For a proof, and additional learning theoretic implications of Theorem 9, we refer the reader to [1].

1.2 Proof outline

First, we use an idea due to Krause and Pudlák [13], who showed that if a function f has high sign degree, f^{op} has high signed monomial complexity. We observe that their argument can be easily adapted to show a more general result. In particular, our Lemma 7 shows that the hardness of f for *low degree* polynomials, with respect to natural notions like uniform approximation and sign representation, gets amplified to corresponding hardness of f^{op} for *sparse (low weight)* polynomials. The main problem at this point is to understand the structure of f^{op}. In particular, our interest is when f^{op} suitably embeds in a symmetric function. As a first glance, symmetric functions do not seem to have the structure of a lifted function f^{op}.

At this point, inspired by the work of Krause [12], we make a simple but somewhat counter-intuitve observation that turns out to be crucial. A function g is called a monomial projection of h, if g can be obtained by substituting each input variable of h with a monomial in variables of g. What is nice about such projections is that for the polynomial sparsity measures that are relevant for us (Observation 25), the complexity of g is upper bounded by that of h. We observe (Lemma 2) that if f is a symmetric function, then there exists a symmetric function F, on a larger domain, such that f^{op} is a monomial projection of F. Moreover, the combinatorial parameters of f that caused its hardness against low-degree polynomials, nicely translate to combinatorial parameters of F that have been conjectured to cause hardness of F against sparse (low weight) polynomials.

We then find a suitable symmetric f such that f^{op} has large approximate weight and is a monomial projection of F. Lemma 2 provides such a monomial projection in which the combinatorial quantity $r(F)$ corresponds to another combinatorial quantity $\Gamma(f)$, which is defined in Section 2. Paturi's Theorem 17 shows that $\Gamma(f)$ characterizes the approximate degree of f. Our polynomial hardness amplification via Lemma 7, implies that f^{op}, and therefore F, has large approximate weight. This proves Theorem 9 which was conjectured by Ada et al. [1].

Moreover, the odd-even degree of F corresponds to the sign degree of f. Our polynomial hardness amplification via Lemma 7, implies that f^{op}, and therefore F, has large signed monomial complexity. This resolves an old conjecture of Zhang [24].

Finally, we note that F having large odd-even degree also implies that f is uniformly inapproximable by low degree polynomials. Our lifting lemma, Lemma 7 implies that f^{op}, and thus F has small polynomial margin. We then invoke a theorem, Theorem 24, proving a tight equivalence between the polynomial margin of F and the PP complexity of $F \circ \mathsf{XOR}$.

1.3 Comparison with related work

In this section, we compare our results and techniques with those of recent related works.

Shortly after our paper was put out in the public domain [6], Ada et al. [2] reported a proof of Theorem 9. However, their methods seem completely different from ours. In order to prove a lower bound on the approximate spectral norm of f, they take recourse

to the communication matrix of $f \circ \mathsf{XOR}$. Via a result of Bruck and Smolensky [4] they then show that it is enough to bound the approximate rank of this matrix. They do this by appropriately invoking a matrix theoretic lemma of Razborov [19]. This is essentially opposite to our approach. We directly prove lower bounds on the approximate spectral norm of f, using our Projection Lemma and Lifting Lemma along with Paturi's Theorem [17], without bringing communication into the picture at all. We then use the bound on the approximate spectral norm of f to prove lower bounds on the bounded error communication complexity of $f \circ \mathsf{XOR}$. It is interesting to note that, although [2] do not directly use Paturi's Theorem, the matrix theoretic lemma of Razborov that they invoke does require usage of Paturi's Theorem.

Two very recent independent works by Hatami and Qian [10] and Ada et al. [2] characterized the unbounded error communication complexity of symmetric XOR functions, strengthening our weakly-unbounded error characterization. Both the proofs involve a reduction to analyzing the unbounded error complexity of a symmetric AND function, and an invocation of a theorem of Sherstov [20] which requires heavy approximation theoretic tools. On the other hand, in order to prove our weakly-unbounded error complexity lower bound, we invoke a result of the authors [6] (a full version of this paper) relating the discrepancy of $f \circ \mathsf{XOR}$ tightly to the polynomial margin of f. Our method of lower bounding the polynomial margin of f is from first principles, and is self-contained. Although we prove a lower bound on a weaker complexity model, we shave off significant logarithmic factors from the bounds obtained by [10, 2].

In conclusion, the techniques of [10, 2] seem very specific, and use non-trivial results from [19] and [20]. Our Lifting Lemma, Lemma 7, on the other hand, applies for general functions. In particular, while the work of [10, 2] take recourse to analyzing AND functions for all their results, we build techniques that can be used directly, and in turn yield bounds on communication complexity of XOR functions. We believe our techniques will also find more use for analyzing methodically non-symmetric XOR functions, an area of active interest today. Indeed, the authors use this technique [6] to provide a simple new proof of the known separation between functions efficiently computable with weakly-unbounded error, and those efficiently computable with unbounded error, via a non-symmetric XOR function that was introduced by Goldmann et al. [7].

2 Preliminaries

We provide the necessary preliminaries in this section.

All logarithms in this paper are taken base 2.

The following result by Zhang [24] provides an upper bound on the Threshold of Parity circuit size required to compute symmetric functions.

▶ **Theorem 16** ([24]). *Let $f : \{-1,1\}^n \to \{-1,1\}$ be a symmetric boolean function such that $\deg_{oe}(f) = \log^{O(1)} n$. Then, f can be computed by a quasi-polynomial size Threshold of Parity circuit.*

The following is a result by Paturi [17] which gives us tight bounds on the approximate degree of symmetric functions.

▶ **Theorem 17** ([17]). *For any symmetric function $f : \{-1,1\}^n \to \{-1,1\}$, define the quantity $\Gamma(f) = \min\{|2k-n+1| : D_f(k) \neq D_f(k+1)$ and $0 \leq k \leq n-1\}$. Then,*

$$\widetilde{\deg}_{2/3}(f) = \Theta(\sqrt{n(n-\Gamma(f))}).$$

The following theorem was proved by Ada et al. [1], which characterizes the weight of a symmetric function.

▶ **Theorem 18** ([1]). *For any symmetric function* $f : \{-1,1\}^n \to \{-1,1\}$,

$$\log(wt(f)) = \Theta\left(r(f)\log\left(\frac{n}{r(f)}\right)\right).$$

Lee and Shraibman [14] showed that $wt_{1/3}(f)$ is a lower bound on $R_{1/3}(f \circ \mathsf{XOR})$.

▶ **Theorem 19** ([14]). *For any function* $f : \{-1,1\}^n \to \{-1,1\}$,

$$R_{1/3}(f \circ \mathsf{XOR}) = \Omega(\log wt_{1/3}(f)).$$

Shi and Zhang [25] proved that the bounded error communication complexity of symmetric XOR functions is characterized by $r(f)$.

▶ **Theorem 20** ([25]). *For any symmetric function* $f : \{-1,1\}^n \to \{-1,1\}$,

$$R_{1/3}(f \circ \mathsf{XOR}) = \Theta^*(r(f)).$$

where Θ^* *hides logarithmic factors.*

Let $\mathsf{Q}_{1/3}(F)$ denote the quantum bounded error communication complexity of F. Zhang [23] proved the following upper bound on the communication complexity of XOR functions.

▶ **Theorem 21** ([23]). *Let* $f \to \{-1,1\}^n \to \{-1,1\}$ *be any function. Suppose the* $\mathbb{F}_2$*-degree of* f *is* d*. Then,*

$$\mathsf{Q}_{1/3}(f \circ \mathsf{XOR}) = O\left(2^d\left(\log\left(wt_{1/3}(f)\right) + \log n\right)\right).$$

Define the discrepancy of a rectangle $S \times T$ under a distribution λ on $\{-1,1\}^n \times \{-1,1\}^n$ as follows.

▶ **Definition 22** (Discrepancy).

$$\mathrm{disc}_\lambda(S \times T, F) = \sum_{(x,y)\in S\times T} F(x,y)\lambda(x,y).$$

The discrepancy of F under a distribution λ is defined as

$$\mathrm{disc}_\lambda(F) = \max_{S\subseteq[n],T\subseteq[n]} \mathrm{disc}_\lambda(S \times T, F)$$

and the discrepancy of F is defined to be

$$\mathrm{disc}(F) = \min_\lambda \mathrm{disc}_\lambda(F).$$

Klauck [11] proved that the PP complexity of F is equivalent to the *discrepancy* of F.

▶ **Theorem 23** ([11]). *For any function* $F : \{-1,1\}^n \times \{-1,1\}^n \to \{-1,1\}$,

$$\mathsf{PP}(F) = \Theta\left(\log\left(\frac{1}{\mathrm{disc}(F)}\right)\right).$$

In a full version of this paper [6], the authors showed that the polynomial margin of f and the discrepancy of $f \circ \mathsf{XOR}$ are equivalent up to a constant factor.

▶ **Theorem 24** ([6]). *For any function* $f : \{-1,1\}^n \to \{-1,1\}$,

$$m(f) \le 4\mathrm{disc}(f \circ \mathsf{XOR}) \le 4m(f).$$

3 Lifting functions

In this section we first prove the Lifting Lemma, Lemma 7, which shows how certain degree-hardness properties of any function $f : \{-1,1\}^n \to \{-1,1\}$ translates to related monomial-hardness properties of f^{op}.

We then prove the Projection Lemma, Lemma 2, which shows how a symmetric function F projects onto f^{op}, for a suitably defined symmetric function f.

Finally, we list the consequences we obtain for lifting symmetric functions, which include resolving conjectures posed by Ada et al. [1], Zhang [24], and the resolution of a weak form of a conjecture by Shi and Zhang [25].

3.1 Lifting functions by the Krause-Pudlák selector

In this section, we prove the Lifting Lemma.

Proof of Lemma 7. We first prove Part 3. Suppose, to the contrary, that $wt_{1/3}(f^{op}) \leq 2^{cd}$, where c is an absolute constant, to be fixed later, and $d = \widetilde{\deg}_{2/3}(f)$. This means there exists a polynomial $p : \{-1,1\}^{3n} \to \{-1,1\}$ such that $wt(p) \leq 2^{cd}$ and $p(x)f^{op}(x) \geq 2/3$ for all $x \in \{-1,1\}^{3n}$. Say $p = \sum_{S\subseteq[3n]} w_S\chi_S$. The proof idea is to manufacture a polynomial p_2, based on p, of low *degree*, which uniformly approximates f to error $2/3$.

For this proof, we view the input variables as $\{x_{j,1}, x_{j,2}, z_j | j \in \{1,\ldots,n\}\}$, where z_j's are the 'selector' variables.

For any fixing of the z variables, define a relevant variable to be one that is 'selected' by z. Thus, for each $j \in \{1,\ldots,n\}$, exactly one of $\{x_{j,1}, x_{j,2}\}$ is relevant. Analogously, define a relevant monomial to be one that does not contain any unselected variable. For any set $S \subseteq [3n]$, define S_x to be the subset of S which contains the all the indices corresponding to the x variables.

For a uniformly random fixing of z and any subset $S \subseteq [3n]$ such that $|S_x| \geq d$,

$$\Pr_z[\chi_S \text{ is relevant}] \leq \frac{1}{2^d}.$$

$$\begin{aligned}\mathbb{E}_z[\text{wt of relevant monomials in } p\big|_z \text{ of degree } \geq d] &= \sum_{S:|S_x|\geq d} |w_S| \cdot \Pr_z[\chi_S \text{ is relevant}] \\ &\leq \frac{1}{2^d} \sum_{S:|S_x|\geq d} |w_S| \leq \frac{1}{2^d} \cdot 2^{cd}.\end{aligned}$$

Thus, there exists a fixing of the z variables such that the weight of the relevant monomials of degree at least d in $p\big|_z$ is at most $\frac{1}{2^d} \cdot 2^{cd}$. Select this fixing of z.

- Note that $p\big|_z$ is a polynomial on only the variables $\{x_{i,1}, x_{i,2} | i \in \{1,\ldots,n\}\}$. Drop the relevant monomials of degree at least d from $p\big|_z$ to obtain a polynomial p_1.
- Observe that p_1 sign represents $f^{op}\big|_z$ with error at most $\frac{1}{3} + \frac{2^{cd}}{2^d}$.
- For each $j \in \{1,\ldots,n\}$, denote the irrelevant variable by x_{j,i_j}. Consider the polynomial p_2 on n variables defined by $p_2 = \mathbb{E}_{x_{1,i_1},\ldots,x_{n,i_n}}[p_1]$, where the expectation is over each irrelevant variable being sampled uniformly and independently from $\{-1,1\}$.
- It is easy to see that any monomial containing an irrelevant variable in p_1 vanishes in p_2. Also note that p_2 is a polynomial of degree less than d, and it must sign represent f with error at most $\frac{1}{3} + \frac{2^{cd}}{2^d}$. This quantity is less than $2/3$ when $c < 1 - \frac{3}{d}$. This leads to a contradiction since we assumed that $\widetilde{\deg}_{2/3}(f) = d$.

We omit the proof of Part 1 as it follows along extremely similar lines as the proof above. ◀

3.2 Lifts as projections of symmetric functions

In this section, we prove the Projection Lemma.

The following observation is an easy consequence of definitions.

▶ **Observation 25.** *For any functions $f : \{-1,1\}^n \to \{-1,1\}$ and $g : \{-1,1\}^m \to \{-1,1\}$ such that g is a monomial projection of f, and any $\epsilon > 0$, we have*

$$\begin{aligned} \mathrm{mon}_{\pm}(g) &\leq \mathrm{mon}_{\pm}(f), \\ wt(g) &\leq wt(f), \\ wt_{\epsilon}(g) &\leq wt_{\epsilon}(f), \\ m(f) &\leq m(g). \end{aligned}$$

Proof of Lemma 2. Let $g : \{-1,1\}^{3n} \to \{-1,1\}$ be defined as follows.

$$g(x_1, \ldots x_n, y_1, \ldots, y_n, z_1, \ldots, z_n) = \\ F(x_1, \ldots, x_n, y_1, \ldots, y_n, -x_1z_1, \ldots, -x_nz_n, y_1z_1, \ldots, y_nz_n).$$

Clearly, g is a monomial projection of F. We show now that $g = f^{op}$.

For every input to g and each $i \in [n]$, define the i'th *relevant* variable to be x_i if $z_i = -1$ (define y_i to be the *irrelevant* variable in this case), and y_i if $z_1 = 1$ (x_i is irrelevant in this case). For a fixed input $x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n$, let b denote the number of relevant variables with value -1. Thus, there are $n - b$ irrelevant variables with value 1. Let a denote the Hamming weight of $(x_1, \ldots, x_n, y_1, \ldots, y_n, -x_1z_1, \ldots, -x_nz_n, y_1z_1, \ldots, y_nz_n)$ Then,

$$4n - 2a = \sum_{i=1}^{n} x_i + y_i - x_iz_i + y_iz_i = \sum_{i=1}^{n} x_i(1 - z_i) + y_i(1 + z_i) = 2n - 4b$$

(which is twice the sum of the values of the relevant variables)

$$\implies a = 2b + n.$$

Thus,

$$g(x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n) = D_F(2b + n) = D_f(b) \\ = f^{op}(x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n).$$

The last equality follows from Equation 1. ◀

▶ Remark. In fact, the proof of Lemma 2 implies the following.

Given a symmetric function $f : \{-1,1\}^n \to \{-1,1\}$ defined by the predicate $D_f(b)$, define a function $F : \{-1,1\}^{4n} \to \{-1,1\}$ (not necessarily symmetric) such that on inputs of Hamming weight $2b + n$, F takes the value $D_f(b)$ for all $b \in \{0, 1, \ldots, n\}$, and F takes arbitrary values on inputs of Hamming weight not in $\{2b + n : b \in \{0, 1, \ldots, n\}\}$. Then, f^{op} is a monomial projection of F.

3.3 Consequences for symmetric functions

In this section, we show consequences of hardness amplification of lifted symmetric functions.

We first prove Theorem 9.

Proof of Theorem 9. Assume that n is even and that $r-1$ is a multiple of 4. (If not, we can fix a constant number of input bits to suitable values).

Suppose $r_1(F) \geq r_0(F)$. Consider $\bar{F}$ defined by $\bar{F}(x_1,\ldots,x_n) = F(-x_1,\ldots,-x_n)$. Observe that $\log(wt_{1/3}(F)) = \log(wt_{1/3}(\bar{F}))$, and $r_0(\bar{F}) > r_1(\bar{F})$. Thus, we may assume, without loss of generality, that $r_0(F) > r_1(F)$.

Note that $D_F(r-1) \neq D_F(r+1)$. Define $F' : \{-1,1\}^{2r} \to \{-1,1\}$ by $D_{F'}(i) = D_F(i)$ for $i \in \{0,1,\ldots,2r\}$. It suffices to show $\log wt_{1/3}(F') \geq c'r$ for some universal constant $c' > 0$. Define $f : \{-1,1\}^{(r-1)/2} \to \{-1,1\}$ by $D_f(i) = D_{F'}(2i + (r-1)/2)$. By Lemma 2, f^{op} is a monomial projection of F'. Note that $D_f\left(\frac{r-1}{4}\right) \neq D_f\left(\frac{r-1}{4}+1\right)$, and thus $\Gamma(f) \leq 1$. By Theorem 17, $\widetilde{\deg}_{2/3}(f) = \Theta(r)$.

Using Part 3 of Lemma 7 and Observation 25, we obtain that there exists a universal constant $c_1 > 0$ such that

$$\log(wt_{1/3}(F)) \geq \log(wt_{1/3}(F')) \geq \log(wt_{1/3}(f^{op})) \geq c_1 r. \tag{4}$$

◀

We now prove Theorem 11, settling a conjecture of Zhang [24].

Proof of Theorem 11. Proof Idea: We define a (not too large) family of symmetric functions $\{f_i : i \in I\}$ such that f_i^{op} is a monomial projection of F for each $i \in I$. The sign degree of f_i will correspond to the number of $(k, k+2)$ sign changes in a corresponding interval of the spectrum of F. Moreover, the family $\{f_i : i \in I\}$ 'captures' all of the $(k, k+2)$ sign changes of D_F. Thus, we conclude the existence of an $i \in I$ such that the sign degree of f_i is large, and f_i^{op} is a monomial projection of F. Lemma 2, Part 2 of Lemma 7, and Observation 25 will then yield the desired result.

Assume without loss of generality, that n is a power of 3. Consider any symmetric function $F : \{-1,1\}^{4n} \to \{-1,1\}$ such that $\deg_{oe}(F) \geq 8j$ where $j \geq 2$. Suppose there were less than $4j$ many $(i, i+2)$ sign changes of D_F in $[0, 3n]$. Then, consider $\bar{F}$ defined by $\bar{F}(x_1,\ldots,x_n) = F(-x_1,\ldots,-x_n)$. Observe that $\mathrm{mon}_{\pm}(F) = \mathrm{mon}_{\pm}(\bar{F})$, and $D(\bar{F})$ has at least $4j$ many $(i, i+2)$ sign changes in $[0, 3n]$ (in particular, in $[0, n]$). Thus, we may assume, without loss of generality, that there are at least $4j$ many $(i, i+2)$ sign changes of D_F in $[0, 3n]$. Further assume that at least $2j$ of them occur when i's are even integers (if not, set one variable to -1).

Define a family $\{f_i : \{-1,1\}^{\frac{n}{3^i}} \to \{-1,1\} : i \in \{0,1,\ldots,\lceil \frac{1}{\log 3}\log(n/j)\rceil\}\}$ of symmetric functions as follows.

$$\forall b \in \left[\frac{n}{3^i}\right],\ D_{f_i}(b) = D_F\left(2b + \frac{n}{3^i}\right).$$

Note that the sign degree of f_i equals the number of $(k, k+2)$ sign changes in the spectrum of F in the interval $[\frac{n}{3^i}, \frac{n}{3^{i-1}}]$. Since D_F has at least $2j$ many $(i, i+2)$ sign changes in $[0, 3n]$, it has at least j many $(k, k+2)$ sign changes in the interval $[j, 3n]$. Thus, the spectrum of at least one of the f_i's (say f_ℓ) has at least $\frac{j}{\lceil \frac{1}{\log 3}\log(\frac{n}{j})\rceil}$ many $(k, k+1)$ sign changes (sign degree). The Projection Lemma (Lemma 2) tells us that f_ℓ^{op} is a monomial projection of F. Using Observation 25 and Part 2 of Lemma 7, we obtain that there exists a constant $c_2 > 0$ such that

$$\mathrm{mon}_{\pm}(F) \geq \mathrm{mon}_{\pm}(f_\ell^{op}) \geq 2^{\frac{c_2 j}{\log(n/j)}}.$$

The upper bound follows from Theorem 16. ◀

Next, we prove Theorem 12, providing a characterization of the bounded error communication complexity of symmetric XOR functions in terms of $wt_{1/3}(f)$.

Proof of Theorem 12. The upper bound follows from Theorem 20 and Theorem 18. The lower bound follows from Theorem 9, and Theorem 19. ◀

The proof of Theorem 14 can be found in the Appendix.

4 Conclusions

We provide a general lifting theorem, and list several applications to symmetric functions, via our Projection Lemma, including characterizations of bounded error and weakly-unbounded error communication complexity of symmetric XOR functions, characterization of the approximate weight of symmetric functions, and Threshold of Parity circuit size of symmetric functions.

Our lifting theorem applies to arbitrary functions, and we feel that it should be usable to prove lower bounds against classes of non-symmetric functions.

Zhang [23] (Theorem 21) showed an upper bound on the quantum bounded error communication complexity of $f \circ \mathsf{XOR}$ in terms of the approximate weight and the $\mathbb{F}_2$-degree of f. Theorem 12 shows that the dependence on the $\mathbb{F}_2$-degree is not required when f is symmetric, even for classical bounded error complexity. This shows the tightness of Theorem 19 for symmetric XOR functions.

We leave the reader with two open questions. Is the lower bound of Theorem 19 tight for *all* XOR functions? In particular, a positive answer would verify the Log Approximate Rank Conjecture for all XOR functions. It is well-known [16] that the real degree of a boolean function is polynomially related to its approximate degree. Does a similar relationship carry over to the spectral norm? Theorem 9 gives a positive answer for symmetric functions.

References

1 Anil Ada, Omar Fawzi, and Hamed Hatami. Spectral norm of symmetric functions. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 15th International Workshop, APPROX 2012, and 16th International Workshop, RANDOM 2012, Cambridge, MA, USA, August 15-17, 2012. Proceedings*, pages 338–349, 2012.

2 Anil Ada, Omar Fawzi, and Raghav Kulkarni. On the spectral properties of symmetric functions. *Arxiv*, 2017.

3 László Babai, Peter Frankl, and Janos Simon. Complexity classes in communication complexity theory (preliminary version). In *27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 27-29 October 1986*, pages 337–347, 1986.

4 Jehoshua Bruck and Roman Smolensky. Polynomial threshold functions, AC^0 functions, and spectral norms. *SIAM J. Comput.*, 21(1):33–42, 1992.

5 Jin-yi Cai, Frederic Green, and Thomas Thierauf. On the correlation of symmetric functions. *Mathematical Systems Theory*, 29(3):245–258, 1996.

6 Arkadev Chattopadhyay and Nikhil S. Mande. Dual polynomials and communication complexity of XOR functions. *CoRR*, abs/1704.02537, 2017. `arXiv:1704.02537`.

7 Mikael Goldmann, Johan Håstad, and Alexander A. Razborov. Majority gates VS. general weighted threshold gates. *Computational Complexity*, 2:277–300, 1992.

8 Mika Göös, Toniann Pitassi, and Thomas Watson. Deterministic communication vs. partition number. In *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, Berkeley, CA, USA, 17-20 October, 2015*, pages 1077–1088, 2015.

9 Mika Göös, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for BPP. *CoRR*, abs/1703.07666, 2017.

10 Hamed Hatami and Yingjie Qian. The unbounded-error communication complexity of symmetric xor functions. *Arxiv*, 2017.

11 Hartmut Klauck. Lower bounds for quantum communication complexity. *SIAM J. Comput.*, 37(1):20–46, 2007.

12 Matthias Krause. On the computational power of boolean decision lists. *Computational Complexity*, 14(4):362–375, 2006.

13 Matthias Krause and Pavel Pudlák. On the computational power of depth-2 circuits with threshold and modulo gates. *Theor. Comput. Sci.*, 174(1-2):137–156, 1997.

14 Troy Lee and Adi Shraibman. Lower bounds in communication complexity. *Foundations and Trends in Theoretical Computer Science*, 3(4):263–398, 2009.

15 Marvin Minsky and Seymour Papert. *Perceptrons - an introduction to computational geometry*. MIT Press, 1987.

16 Noam Nisan and Mario Szegedy. On the degree of boolean functions as real polynomials. *Computational Complexity*, 4:301–313, 1994.

17 Ramamohan Paturi. On the degree of polynomials that approximate symmetric boolean functions (preliminary version). In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing, May 4-6, 1992, Victoria, British Columbia, Canada*, pages 468–474, 1992.

18 Ran Raz and Pierre McKenzie. Separation of the monotone NC hierarchy. *Combinatorica*, 19(3):403–435, 1999.

19 Alexander A. Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya: Mathematics*, 67(1):145, 2003.

20 Alexander A. Sherstov. The unbounded-error communication complexity of symmetric functions. *Combinatorica*, 31(5):583–614, 2011.

21 Mario Szegedy. Functions with bounded symmetric communication complexity, programs over commutative monoids, and ACC. *J. Comput. Syst. Sci.*, 47(3):405–423, 1993.

22 Andrew Chi-Chih Yao. Some complexity questions related to distributive computing (preliminary report). In *Proceedings of the 11h Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1979, Atlanta, Georgia, USA*, pages 209–213, 1979.

23 Shengyu Zhang. Efficient quantum protocols for XOR functions. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014*, pages 1878–1885, 2014.

24 Zhi-Li Zhang. Complexity of symmetric functions in perceptron-like models. Master's thesis, University of Massachusetts at Amherst, 1992.

25 Zhiqiang Zhang and Yaoyun Shi. Communication complexities of symmetric XOR functions. *Quantum Information & Computation*, 9(3):255–263, 2009.

A Appendix

Proof of Theorem 14. By an extremely similar proof to that of Theorem 11 (using Part 1 of Lemma 7 instead of Part 2 of Lemma 7), it can be seen that there exists a constant $c' > 0$ such that

$$m(F) \leq \frac{1}{2^{c'r/\log(n/r)}}.$$

Thus, using Theorem 24, there exists a constant $c_1 > 0$ such that $\mathrm{disc}(F \circ \mathsf{XOR}) \leq \frac{1}{2^{c_1 r/\log(n/r)}}$. Along with Theorem 23, this proves that there exists a constant $c > 0$ such that $\mathsf{PP}(F \circ \mathsf{XOR}) \geq cr/\log(n/r)$.

We now prove the upper bound on $\mathsf{PP}(F \circ \mathsf{XOR})$. Define $S_{even} = \{i \in \{0, 2, \ldots, 4n-2\} : D_f(i) \neq D_F(i+2)\}$, and define $S_{odd} = \{i \in \{1, 3, \ldots, 4n-3\} : D_F(i) \neq D_F(i+2)\}$. By our assumption, $|S_{even}|, |S_{odd}| \leq r$.

Consider the polynomials $p_{even}, p_{odd} : \{-1, 1\}^{4n} \to \mathbb{R}$ defined by

$$p_{even}(x) = D_F(0) \cdot \prod_{i \in S_{even}} \left(4n - 2i + 1 - \left(\sum_{j=1}^{4n} x_j\right)\right)$$

and

$$p_{odd}(x) = D_F(1) \cdot \prod_{i \in S_{odd}} \left(4n - 2i + 1 - \left(\sum_{j=1}^{4n} x_j\right)\right)$$

The polynomial $p : \{-1, 1\}^{4n} \to \mathbb{R}$ defined by

$$p(x) = (1 + \chi_{[4n]}(x))p_{even}(x) + (1 - \chi_{[4n]}(x))p_{odd}(x)$$

sign represents F on $\{-1, 1\}^{4n}$.

We now use the simple observations that $wt(q_1 \cdot q_2) \leq wt(q_1) \cdot wt(q_2)$ and $wt(q_1 + q_2) \leq wt(q_1) + wt(q_2)$. Thus,

$$\begin{aligned} wt(p) &\leq 2wt(p_{even}) + 2wt(p_{odd}) \\ &\leq 2(8n)^r + 2(8n)^r \\ &\leq 4(8n)^r \end{aligned}$$

Note that all the coefficients of p are integer valued. Thus, the polynomial $p' = \frac{p}{wt(p)}$ is a polynomial of weight 1, which sign represents F with margin at least $\frac{1}{wt(p)}$. By Theorem 24 and Theorem 23,

$$\mathsf{PP}(F \circ \mathsf{XOR}) \leq O(\log(wt(p))) \leq O(r \log n).$$ ◀