Electronic Colloquium on Computational Complexity, Report No. 25 (2011)

Monotone Rank and Separations in Computational Complexity

Yang D. Li

Department of Computer Science and Engineering,
The Chinese University of Hong Kong.
Email: danielliy@gmail.com

Abstract. In the paper, we introduce the concept of monotone rank, and using it as a powerful tool, we obtain several important and strong separation results in computational complexity.

- We show a super-exponential separation between monotone and non-monotone computation in the non-commutative model, and thus give the answer to a longstanding open problem posed by Nisan [Nis91] in algebraic complexity. More specifically, we exhibit a homogeneous algebraic function f of degree d (d even) on n variables with the monotone algebraic branching program (ABP) complexity $\Omega(n^{d/2})$ and the non-monotone ABP complexity $O(d^2)$.
- We propose a relaxed version of the famous Bell's theorem [Bel64] [CHSH69]. Bell's theorem basically states that local hidden variable theory cannot predict the correlations produced by quantum mechanics, and therefore is an impossibility result. Bell's theorem heavily relies on the diversity of the measurements. We prove that even if we fix the measurement, infinite amount of local hidden variables will still be needed, though now the prediction of "quantum mechanics" becomes physically feasible. Quantitatively, at least n bits of local hidden variables are needed to simulate the correlations of size $2n$ generated from a 2-qubit Bell state. The bound is asymptotically tight.
- We generalize the log-rank conjecture [LS88] in communication complexity to the multiparty case, and prove that for super-polynomial parties, there is a super-polynomial separation between the deterministic communication complexity and the logarithm of the rank of the communication tensor. This means that the log-rank conjecture does not hold in "high" dimensions.

1 Introduction

Computational complexity focuses on studying the minimum amount of resources required for carrying out computational tasks. The resources may be time, space, randomness (public or private), communication, quantum entanglement and so on. Readers can refer to the textbook by Arora and Barak [AB09] for more knowledge on this subject.

Without any doubt, the biggest open problem in complexity theory is the **P** versus **NP** problem. Those who are optimistic and idealistic about the world often believe that $\mathbf{P} = \mathbf{NP}$, implying "hard" problems may have "easy" solutions. Some others are more pessimistic and realistic, thinking that "hard" problems have distinctions from "easy" problems. The most fundamental and natural approach for either of the two groups of people to realize their ambition is to identify an explicit **NP**-complete problem which admits an polynomial-time algorithm or an exponential-time lower bound. In fact, finding explicit functions with "high" lower bounds is crucial in numerous models of complexity theory. For example, a recent paper by Raz [Raz10] says that any explicit tensor with "high" tensor rank would have substantial impact on the lower bounds for arithmetic formulas.

In this paper, we consider explicit functions that have "high" monotone rank. Let us first define monotone rank.

Definition 1 *The* monotone rank *of a tensor* $M : \Pi_{j=1}^{d}[n_j] \to \mathbb{R}^+$ *($d \geq 2$) is the minimum r such that* $M = \sum_{i=1}^{r} v_{1,i} \otimes v_{2,i} \otimes \cdots \otimes v_{d,i}$, *where* $v_{j,i} \in (\mathbb{R}^+)^{n_j}, j \in [d], i \in [r]$. *It is denoted as* $mr(M)$.

Note that when $d = 2$, tensor becomes matrix. In this case, monotone rank is also called positive rank (or sometimes nonnegative rank). Positive rank is first introduced to complexity theory by Yannakakis [Yan91], where it is connected to the size of the linear programs to express a polytope and the

ISSN 1433-8092

nondeterministic communication complexity of a 0/1 matrix approximated from the so-called slack matrix. However, according to a recent report by Lee and Shraibman [LS09], there are no lower bounds which actually use monotone rank in practice. Consequently, to the best of our knowledge, this paper is the first to connect monotone rank to real applications in complexity theory. Also note that a similar definition appears in [AFT11]. But it is more abstract, is not for applications, and does not include the case for $d = 2$.

Admittedly, monotone rank is **NP**-hard to compute in general [Vav09] [Has90]. But for some special cases, monotone rank is known [BL09] [LC10] [AFT11]. Three separation results in complexity theory will be provided via the approach of monotone rank. The results are in various sub-areas (algebraic complexity, quantum computing and communication complexity) of complexity theory, and hence we will describe them separately.

A brief preview of the results is that we want to quantify the power of negation. In algebraic complexity, monotone computation does not allow substraction and the coefficients of the monomials are all positive; while the non-monotone model does not apply such restrictions. In quantum computing, Feynman [Fey82] points out that the only difference between the probabilistic world and the quantum world is that it happens as if the "probabilities" would have to go negative. Moreover, the split of communication complexity and the log-rank of the communication tensor is partly due to whether or not we allow negative decomposition. As a result, all we concern is a nonnegativity versus generality issue, and we will address this issue using monotone rank.

1.1 Algebraic Complexity

Valiant [Val80] shows an exponential separation between monotone and non-monotone computation in terms of algebraic circuit complexity. Nisan [Nis91] asks if the similar difference between monotone and non-monotone can be achieved in a restricted model called non-commutative model, which prohibits the commutativity of multiplication, for some complexity measure.

We answer this question in an affirmative way by showing the following theorem. The gap is more than exponential in terms of algebraic branching program (ABP) complexity, where ABP can be regarded as the analog of branching program in algebraic computation.

Theorem 1 *There exists an explicit homogeneous algebraic function f of degree d (d even) on n variables with the monotone ABP complexity $\Omega(n^{d/2})$ and the non-monotone ABP complexity $O(d^2)$.*

1.2 Quantum Computing

The charm and beauty of quantum mechanics is grounded on its counter-intuitiveness to a great extent. And one of the most ground-breaking results ever in history is Bell's theorem [Bel64] [CHSH69], implying that quantum mechanics violates either locality or counterfactual definiteness. A simple and informal restatement of Bell's theorem is that local hidden variable theory cannot reproduce all of the predictions of quantum mechanics.

Since then, lots of subsequent work is based on or related to Bell's theorem. The idea of a great deal of papers ([BCT99] [BCvD01], [BT03], [TB03], [RT09], etc.) is that local hidden variables augmented by communication could reproduce the results of quantum entanglement. Quantum entanglement also has plenty of applications in areas such as quantum teleportation [BBC$^+$93], superdense coding [BW92] and quantum cryptography [BB84].

We think about the power of entanglement and the simulation of entanglement from another prospective. In Bell's theorem, the measurements are versatile and can be chosen be with respect to various basis. Alice may choose to measure her state according to basis with an angle α relative to the standard basis; while Bob may choose another basis , which is β relative to the standard basis, for measurement. The diversity of the measurements may play a crucial role on the power of entanglement, and may make the classical simulations with local hidden variables impossible. What is the case if we fix the measurement? Is it now possible to simulate "quantum mechanics" with local hidden variables?

Next we shall make our model more formal and more concrete. The model is roughly illustrated by Figure 1.

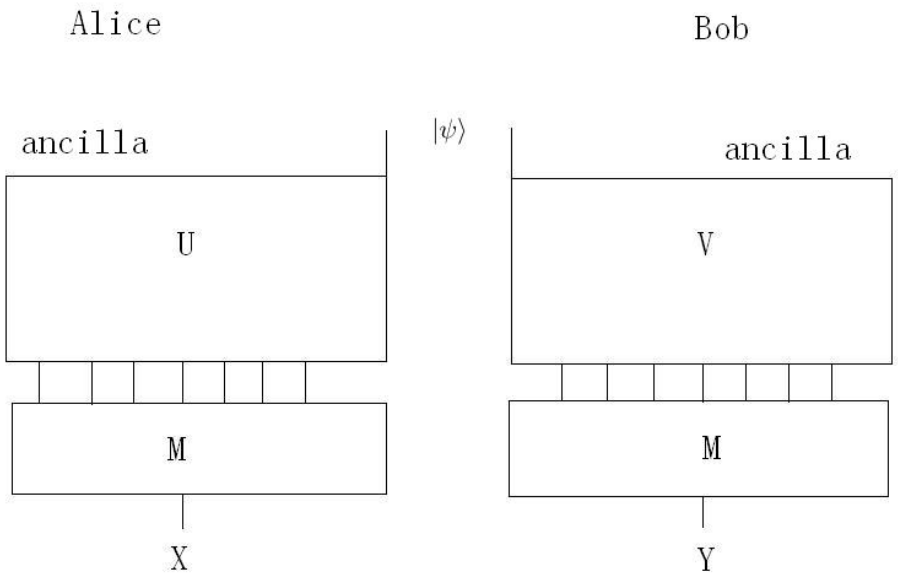

Fig. 1. Bell's Theorem with Fixed Measurement

In Figure 1, $|\psi\rangle$ represents a 2-qubit Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, where the first qubit is owned by Alice while the second belongs to Bob. We also fill some ancilla qubits. The state in the beginning is

$$\phi_0 = |0^{n-1}\rangle|\psi\rangle|0^{n-1}\rangle.$$

Then Alice applies unitary operation U and Bob applies unitary operation V, each of dimension $2^n \times 2^n$. The state becomes

$$\phi_1 = (U \otimes V)\phi_0.$$

Then Alice and Bob both apply the measurement M, which is fixed to be with respect to the standard basis. In the end, they output a correlation (X, Y) according to results of the measurement. X and Y are random variables taking values in $\{0,1\}^n$. So totally there are $2^n \times 2^n = 4^n$ possibilities for (X, Y).

Based on the model above, we have the following result.

Theorem 2 *At least n bits of local hidden variables are needed to simulate the correlations of size $2n$ generated from a 2-qubit Bell state. The bound is asymptotically tight.*

So local hidden variable theory is able to predict the correlations produced by "quantum mechanics" with fixed measurement. But n can be arbitrarily large, and therefore we actually need infinite amount of shared randomness to simulate just 2-qubit quantum entanglement, which means that quantum entanglement is still much more powerful even if we fix the measurement.

1.3 Communication Complexity

Arguably the most well-known open problem in communication complexity is the log-rank conjecture [LS88], which is stated as follows:

Conjecture 1 *There exists a constant c, such that for every function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$,*

$$D(f) = O(\log^c rk(M(f))),$$

where $D(f)$ is the deterministic communication complexity of f and $M(f)$ is the communication matrix of f.

Although a number of people aspire to resolve this conjecture, very little progress has been made in the last two decades [NW95] [RS95]. In fact, the conjecture can be easily generalized to the number-in-hand multiparty communication complexity model. Suppose there are d parties in the communication.

Conjecture 2 *There exists a constant c, such that for every function $f : (\{0,1\}^n)^d \to \{0,1\}$,*

$$D(f) = O(\log^c rk(M(f))),$$

where $M(f)$ is the communication tensor of f.

We have the following theorem for the generalized log-rank conjecture.

Theorem 3 *For every $d = \omega(n^{c'}), \forall c' > 0$, there exists a function $f : (\{0,1\}^n)^d \to \{0,1\}$, such that for every constant $c > 0$,*

$$D(f) = \omega(\log^c rk(M(f))).$$

Thus, we provide a super-polynomial separation between the deterministic communication complexity and the logarithm of the rank of the communication tensor when there are super-polynomial parties. This means that the log-rank conjecture does not hold in "high" dimensions.

2 Preliminaries

2.1 ABP Complexity

We recall some necessary definitions, notations, and results from Nisan's paper [Nis91].

Definition 2 *An* algebraic branching program (ABP) *is a directed acyclic graph with one source and one sink. The vertices of the graph are partitioned into levels numbered from 0 to d, where edges may only go from level i to level $i+1$. d is called the degree of the ABP. The source is the only vertex at level 0 and the sink is the only vertex at level d. Each edge is labeled with a homogeneous linear function of $x_1 x_2 \dots x_n$. The size of an ABP is the number of vertices. We denote (non-monotone) ABP complexity of a function f by $B(f)$.*

Definition 3 *An ABP is called monotone if all constants used as coefficients in the linear forms are positive. The monotone ABP complexity of f are denoted as $B^+(f)$.*

Definition 4 *For a function f of degree d, and $0 \le k \le d$, the k-monotone-ABP complexity of f, $B_k^+(f)$ is the minimum, over all monotone ABPs that compute f, of the size of the k'th level of the ABP.*

We use $rk(M)$ to denote the rank of a matrix M. Let f be a homogeneous function of degree d on n variables. For each $0 \le k \le d$, we define a real matrix $M_k(f)$ of dimensions n^k by n^{d-k} as follows: there is a row for each sequence of k variables (k-term), and a column for each $d-k$-term. The entry at $(x_{i_1} \cdots x_{i_k}, x_{j_1} \cdots x_{j_{d-k}})$ is defined to be the real coefficient of the monomial $x_{i_1} \cdots x_{i_k} x_{j_1} \cdots x_{j_{d-k}}$ in f.

Lemma 4 *For any homogeneous function f of degree d, $B(f) = \sum_{k=0}^{d} rk(M_k(f))$.*

Lemma 5 *For every homogeneous function f of degree d and all $0 \le k \le d$, $B_k^+(f) = mr(M_k(f))$. Also, $B^+(f) \ge \sum_{k=0}^{d} B_k^+(f)$.*

2.2 Monotone Rank

We review some of the known results on monotone rank.

Given n distinct real numbers $a_1, a_2, \ldots, a_n$, a $n \times n$ matrix M can be defined by $M_{ij} = (a_j - a_i)^2$, $i, j \in [n]$. Such matrix has the following properties, due to [BL09] and [LC10].

Lemma 6 *$rk(M) = 3$.*

Lemma 7 *$mr(M) = n$.*

A tensor $M : [n]^d \to \{0, 1\}$, which satisfies $M(i_1, i_2, i_3, \ldots, i_d) = 1$ if and only if $\sum_{j=1}^{d} i_j$ is divisible by n, has the following properties [AFT11].

Lemma 8 *$rk(M) \leq dn$.*

Lemma 9 *$mr(M) = n^{d-1}$.*

2.3 Hadamard Product

Definition 5 *Let A and B be $m \times n$ matrices with entries in $\mathbb{R}$. The* Hadamard product *of A and B is defined by $[A \circ B]_{ij} = [A]_{ij}[B]_{ij}$, for all $1 \leq i \leq m, 1 \leq j \leq n$.*

We need a folklore property of Hadamard product; see, for example, [AJS09].

Proposition 10 *Let A and B be $m \times n$ real matrices, then $rk(A \circ B) \leq rk(A)rk(B)$.*

3 Monotone vs. Non-monotone Computation

In this section, we prove Theorem 1.

A typical homogeneous function f of degree d (d even) on n variables is in the form of

$$f(x_1, x_2, \ldots, x_n) = \sum_{i_1, i_2, \ldots, i_d \in [n]} c_{i_1 i_2 \cdots i_d} x_{i_1} x_{i_2} \cdots x_{i_d}.$$

There are totally n^d monomials and n^d corresponding coefficients.

We define a function $g : \{i_1, i_2, \ldots, i_{d/2} : i_1, i_2, \ldots, i_{d/2} \in [n]\} \to [n^{d/2}]$ as follows.

$$g(i_1, i_2, \ldots, i_{d/2}) = \sum_{k=1}^{d/2} (i_k - 1) n^{d/2-k} + 1$$

It is easy to verify that g is a bijective function.

Then we define f by specifying all its coefficients.

$$c_{i_1 i_2 \cdots i_d} = (g(i_1, i_2, \ldots, i_{d/2}) - g(i_{d/2+1}, i_{d/2+2}, \ldots, i_d))^2$$

It is clear that all the coefficients are nonnegative. In a word, f is the following.

$$f(x_1, x_2, \ldots, x_n) = \sum_{i_1, i_2, \ldots, i_d \in [n]} (g(i_1, i_2, \ldots, i_{d/2}) - g(i_{d/2+1}, i_{d/2+2}, \ldots, i_d))^2 x_{i_1} x_{i_2} \cdots x_{i_d}$$

We arrange $M_{d/2}(f)$ in a way such that k-term is in the ascending order of its corresponding $g(i_1, i_2, \ldots, i_{d/2})$, and $d - k$-term is in the ascending order of its corresponding $g(i_{d/2+1}, i_{d/2+2}, \ldots, i_d)$. Then for $M_{d/2}(f)$, it is not hard to verify that $[M_{d/2}(f)]_{ij} = (j - i)^2, \forall i, j \in [n^{d/2}]$. More explicitly,

$$M_{d/2}(f) = \begin{bmatrix} 0^2 & 1^2 & 2^2 & \cdots & (n^{d/2}-1)^2 \\ 1^2 & 0^2 & 1^2 & \cdots & (n^{d/2}-2)^2 \\ 2^2 & 1^2 & 0^2 & \cdots & (n^{d/2}-3)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (n^{d/2}-1)^2 & (n^{d/2}-2)^2 & (n^{d/2}-3)^2 & \cdots & 0 \end{bmatrix}.$$

If we use M_i to represent the i-th row of $M_{d/2}(f)$, $M_{d/2}(f)$ could be written into another way.

$$M_{d/2}(f) = \begin{bmatrix} M_1 \\ M_2 \\ M_3 \\ \vdots \\ M_{n^{d/2}} \end{bmatrix}$$

More generally, $\forall k \in [d/2]$,

$$M_{d/2-k}(f) = \begin{bmatrix} M_1 & M_2 & M_3 & \cdots & M_{n^k} \\ M_{n^k+1} & M_{n^k+2} & M_{n^k+3} & \cdots & M_{2n^k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ M_{n^{d/2}-n^k+1} & M_{n^{d/2}-n^k+2} & M_{n^{d/2}-n^k+3} & \cdots & M_{n^{d/2}} \end{bmatrix}$$

Next we will show the following two lemmas, the combination of which will immediately yield the result in Theorem 1.

Lemma 11 *$B(f) = O(d^2)$.*

Lemma 12 *$B^+(f) = \Omega(n^{d/2})$.*

□

3.1 Proof of Lemma 11

By Lemma 6,

$$rk(M_{d/2}(f)) = 3.$$

We define the following subsidiary matrix S of dimension $n^{d/2-1} \times (n-1)$.

$$S = \begin{bmatrix} 1^2 & 2^2 & 3^2 & \cdots & (n-1)^2 \\ (1+n)^2 & (2+n)^2 & (3+n)^2 & \cdots & (2n-1)^2 \\ (1+2n)^2 & (2+2n)^2 & (3+2n)^2 & \cdots & (3n-1)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (n^{d/2}-n+1)^2 & (n^{d/2}-n+2)^2 & (n^{d/2}-n+3)^2 & \cdots & (n^{d/2}-1)^2 \end{bmatrix}$$

A careful comparison of $M_{d/2}(f)$ and $M_{d/2-1}(f)$ would reveal the following observation,

Observation 1 *$rk(M_{d/2-1}(f)) \leq rk(M_{d/2}(f)) + rk(S)$.*

We define another auxiliary matrix S_1.

$$S_1 = \begin{bmatrix} 1 & 2 & 3 & \cdots & (n-1) \\ (1+n) & (2+n) & (3+n) & \cdots & (2n-1) \\ (1+2n) & (2+2n) & (3+2n) & \cdots & (3n-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (n^{d/2}-n+1) & (n^{d/2}-n+2) & (n^{d/2}-n+3) & \cdots & (n^{d/2}-1) \end{bmatrix}$$

It is easy to see that

$$rk(S_1) = 2,$$

and that

$$S = S_1 \circ S_1.$$

According to Proposition 10,

$$rk(S) \leq (rk(S_1))^2 = 4.$$

Now we have

$$rk(M_{d/2-1})(f) \leq rk(M_{d/2}(f)) + 4.$$

In a similar way, we can obtain that $\forall k \in [d/2]$,

$$rk(M_{d/2-k}(f)) \leq rk(M_{d/2-k+1}(f)) + 4.$$

So we know that $\forall k \in [d/2]$,

$$rk(M_{d/2-k}(f)) \leq 3 + 4k.$$

By symmetry, $\forall k \in [d/2]$,

$$rk(M_{d/2+k}(f)) \leq 3 + 4k.$$

Therefore, according to Lemma 4,

$$B(f) = \sum_{k=0}^{d} rk(M_k(f)) = O(d^2).$$

□

3.2 Proof of Lemma 12

By Lemma 7,

$$mr(M_{d/2}(f)) = n^{d/2}.$$

For $M_{d/2-1}(f)$, it is not hard to see that after some permutation of the columns, we can obtain a sub-matrix with dimension $n^{d/2-1} \times n^{d/2-1}$ from $M_{d/2-1}(f)$ as follows:

$$\begin{bmatrix} 0^2 & n^2 & (2n)^2 & \cdots & (n^{d/2}-n)^2 \\ n^2 & 0^2 & n^2 & \cdots & (n^{d/2}-2n)^2 \\ (2n)^2 & n^2 & 0^2 & \cdots & (n^{d/2}-3n)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (n^{d/2}-n)^2 & (n^{d/2}-2n)^2 & (n^{d/2}-3n)^2 & \cdots & 0^2 \end{bmatrix}.$$

So $mr(M_{d/2-1}(f)) = n^{d/2-1}$.

Similarly, we can show that $\forall k \in [d/2]$, $mr(M_{d/2-k}(f)) = n^{d/2-k}$. By symmetry, $\forall k \in [d/2]$, $mr(M_{d/2+k}(f)) = n^{d/2-k}$.

By Lemma 5,

$$B^+(f) = \Omega(\sum_{k=0}^{d} B_k^+(f)) = \Omega(n^{d/2}).$$

□

4 Shared Randomness vs. Quantum Entanglement

In this part, we shall prove Theorem 2.

First we calculate ϕ_0 and ϕ_1.

$$\begin{aligned}\phi_0 &= |0^{n-1}\rangle|\psi\rangle|0^{n-1}\rangle \\ &= \frac{1}{\sqrt{2}}(|0^{2n}\rangle + |0^{n-1}\rangle|11\rangle|0^{n-1}\rangle).\end{aligned}$$

$$\begin{aligned}\phi_1 &= (U \otimes V)\phi_0 \\ &= \frac{1}{\sqrt{2}}((U \otimes V)|0^{2n}\rangle + (U \otimes V)|0^{n-1}\rangle|11\rangle|0^{n-1}\rangle) \\ &= \frac{1}{\sqrt{2}}(U|0^n\rangle \otimes V|0^n\rangle + U|0^{n-1}\rangle|1\rangle \otimes V|1\rangle|0^{n-1}\rangle) \\ &= \frac{1}{\sqrt{2}}(u_0 \otimes v_0 + u_1 \otimes v_1),\end{aligned}$$

where u_0 is the first column of U, v_0 is the first column of V, u_1 is the second column of U, and v_1 is the $(2^{n-1}+1)$-th column of V.

After the measurement M, there are 4^n possibilities. And

$$Prob\{X = x, Y = y\} = \frac{1}{2}|u_0(x)v_0(y) + u_1(x)v_1(y)|^2,$$

for all $x, y \in \{0,1\}^n$. Here we use x and y as the index for vector or matrix.

Suppose $N = 2^n$. We use a nonnegative matrix P of dimension $N \times N$ to demonstrate the distribution of (X, Y).

$$P = [Prob\{X = x, Y = y\}]_{xy}.$$

Suppose we want to use shared randomness to simulate this distribution generated from quantum entanglement. In the beginning Alice and Bob share a random variable Z, whose sample space is Ω. We would prove three lemmas.

Lemma 13 $|\Omega| \geq mr(P)$.

Lemma 14 *There exists a P generated from the process above, such that $mr(P) = N$.*

Lemma 15 $\log|\Omega| \leq 2n$.

From these three lemmas, it is clear that

$$n \leq \log|\Omega| \leq 2n,$$

implying that we need at least n bits of shared randomness and at most $2n$ bits of shared randomness to simulate a $2n$-bit correlation generated from a 2-qubit Bell state.

□

4.1 Proof of Lemma 13

We observe that conditional on Z, X and Y are independent. That is to say,

$$\begin{aligned} Prob\{X = x, Y = y\} &= \sum_{z\in\Omega} Prob\{Z = z\} \times Prob\{X = x, Y = y|Z = z\} \\ &= \sum_{z\in\Omega} Prob\{Z = z\} \times Prob\{X = x|Z = z\} \times Prob\{Y = y|Z = z\} \end{aligned}$$

For a fixed z, let v_z be the vector of size 2^n, such that $v_z(x) = Prob\{X = x|Z = z\}$, and v'_z be the vector of size 2^n, such that $v'_z(y) = Prob\{Y = y|Z = z\}$.

So,

$$P = \sum_{z\in\Omega} Prob\{Z = z\}(v_z)(v'_z)^T,$$

which means that P can be decomposed into $|\Omega|$ nonnegative rank-1 matrices. By the definition of $mr(P)$,

$$|\Omega| \geq mr(P).$$

□

4.2 Proof of Lemma 14

Let $\{c_x : x \in \{0,1\}^n\}$ be a set of $N = 2^n$ distinct elements of $\mathbb{R}^+$. and define matrix C to be

$$C_{xy} = c_y - c_x, x, y \in \{0,1\}^n.$$

Thus the Hadamard product of C and its conjugate matrix is

$$C \circ \bar{C} = [(c_y - c_x)^2]_{xy}.$$

Using Guassian elimination, we know that

$$rk(C) = 2.$$

Since C is an antisymmetric matrix, the eigenvalues of C are λ, $-\lambda$ and $N - 2$ 0's.
The characteristic polynomial of C is

$$\sum_{k\in\{0,1\ldots,N\}} e_k\lambda^k,$$

where e_k is the coefficient of λ^k.
It is easy to see that $e_N = 1, e_{N-1} = 0$ and

$$e_{N-2} = \sum_{1\leq x<y\leq N} (c_y - c_x)^2.$$

For $k \leq N - 3$,

$$e_k = \sum_{I\subseteq\{0,1\}^n:|I|=N-k} |C_I|,$$

where C_I is the submatrix obtained by restricting C on those rows and columns in I.
Since $rk(C) = 2$, $rk(C_I) \leq rk(C) = 2$, so

$$|C_I| = 0.$$

Consequently,

$$e_k = 0, \forall k \leq N-3.$$

Hence, the characteristic polynomial of C is

$$\lambda^N + \sum_{1 \leq x < y \leq N} (c_y - c_x)^2 \lambda^{N-2},$$

and

$$\lambda = i\sqrt{\sum_{1 \leq x < y \leq N} (c_y - c_x)^2}.$$

Since C is antisymmetric, C is normal. Using spectral decomposition, we know that

$$C = \lambda |u_0\rangle\langle u_0| - \lambda |u_1\rangle\langle u_1|,$$

where $|u_0\rangle$ is the eigenvector of λ and $|u_1\rangle$ is the eigenvector of $-\lambda$.

It is easy to take proper distinct values of $\{c_x : x \in \{0,1\}^n\}$ to satisfy $\sqrt{\sum_{1 \leq x < y \leq n} (c_y - c_x)^2} = \sqrt{1/2}$, which implies

$$\lambda = i\sqrt{1/2}.$$

Let $v_0 = \bar{u}_0$ and $v_1 = -\bar{u}_1$ and we get

$$\begin{aligned} P_{xy} &= \frac{1}{2}|u_0(x)v_0(y) + u_1(x)v_1(y)|^2 \\ &= \frac{1}{2}|u_0(x)\bar{u}_0(y) - u_1(x)\bar{u}_1(y)|^2. \end{aligned}$$

Also, we have

$$\begin{aligned} (C \circ \bar{C})_{xy} &= (\lambda u_0(x)\overline{u_0(y)} - \lambda u_1(x)\overline{u_1(y)})\overline{(\lambda u_0(x)\overline{u_0(y)} - \lambda u_1(x)\overline{u_1(y)})} \\ &= \frac{1}{2}|u_0(x)\bar{u}_0(y) - u_1(x)\bar{u}_1(y)|^2. \end{aligned}$$

Therefore,

$$P = C \circ \bar{C},$$

which means that we are able to construct P by selecting proper values for entries of C.

By Lemma 7,

$$mr(P) = mr(C \circ \bar{C}) = N.$$

□

4.3 Proof of Lemma 15

We can simply use (X, Y) as the original shared randomness by Alice and Bob. The size of (X, Y) is $2n$. So

$$\log |\Omega| \leq 2n.$$

□

5 Generalized Log-Rank Conjecture

In the section, we will prove Theorem 3.

A function $f : \{0,1\}^n \to \{0,1\}$ could be written into an equivalent form $f : [N] \to \{0,1\}$ with $N = 2^n$. For convenience, we will use the latter representation.

We define a function $f : [N]^d \to \{0,1\}$ by requiring $f(i_1, i_2, \ldots, i_d) = 1$ if and only if $\sum_{j=1}^{d} i_j$ is divisible by N.

By Lemma 8, $rk(M(f)) \leq dN$. By Lemma 9, $mr(M(f)) = N^{d-1}$.

Therefore,

$$\log rk(M(f)) \leq \log d + n,$$

and

$$\log mr(M(f)) = (d-1)n.$$

Suppose $d = \omega(n^{c'}), \forall c' > 0$. Now it is easy to see that for any constant $c > 0$,

$$\log mr(M(f)) = \omega(\log^c rk(M(f))),$$

and because of an obvious relation

$$\log(rk(M(f))) \leq \log(mr(M(f))) \leq D(f),$$

we know that for any constant $c > 0$,

$$D(f) = \omega(\log^c rk(M(f))).$$

□

6 Acknowledgements

Thanks to Shengyu Zhang for discussions at an early stage of this work, Boris Alexeev for helping me better understand his paper [AFT11] and anonymous reviewers for their comments.

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[AFT11] Boris Alexeev, Michael Forbes, and Jacob Tsimerman. Tensor rank: Some lower and upper bounds. *Electronic Colloquium on Computational Complexity*, TR11-010, 2011.

[AJS09] Vikraman Arvind, Pushkar Joglekar, and Srikanth Srinivasan. Arithmetic circuits and the Hadamard product of polynomials. *Proceedings of the 29th Annual IARCS Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 25–36, 2009.

[BB84] Charles Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.

[BBC+93] Charles Bennett, Gilles Brassard, Claude Crepeau, Richard Jozsa, Ashes Peres, and William Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[BCT99] Gilles Brassard, Richard Cleve, and Alain Tapp. The cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letters*, 83(9):1874–1877, 1999.

[BCvD01] Harry Buhrman, Richard Cleve, and Wim van Dam. Quantum engtanglement and communication complexity. *SIAM Journal on Computing*, 30(6):1829–1841, 2001.

[Bel64] John Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[BL09] Leroy Beasley and Thomas Laffey. Real rank versus nonnegative rank. *Linear Algebra and its Applications*, 431(12):2330–2335, 2009.

[BT03] Dave Bacon and Ben Tonor. Bell inequalities with auxiliary communication. *Physical Review Letters*, 90:157904, 2003.

[BW92] Charles Bennett and Stephen Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992.

[CHSH69] John Clauser, Michael Horne, Abner Shimony, and Richard Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[Fey82] Richard Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1982.

[Has90] Johan Hastad. Tensor rank is NP-complete. *Journal of Algorithms*, 11(4):644–654, 1990.

[LC10] Matthew Lin and Moody Chu. On the nonnegative rank of Euclidean distance matrices. *Linear Algebra and its Applications*, 433(3):681–689, 2010.

[LS88] Laszlo Lovasz and Michael Saks. Lattices, mobius functions and communications complexity. *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science*, pages 81–90, 1988.

[LS09] Troy Lee and Adi Shraibman. Lower bounds in communication complexity. *Foundations and Trends in Theoretical Computer Science*, 3(4):263–399, 2009.

[Nis91] Noam Nisan. Lower bounds for non-commutative computation. *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pages 410–418, 1991.

[NW95] Noam Nisan and Avi Wigderson. On rank vs. communication complexity. *Combinatorica*, 15(4):557–565, 1995.

[Raz10] Ran Raz. Tensor-rank and lower bounds for arithmetic formulas. *Proceedings of the 42th Annual ACM Symposium on Theory of Computing*, pages 659–666, 2010.

[RS95] Ran Raz and Boris Spieker. On the 'log-rank' conjecture in communication complexity. *Combinatorica*, 15(4):567–588, 1995.

[RT09] Oded Regev and Ben Tonor. Simulating quantum correlations with finite communication. *SIAM Journal on Computing*, 39(4):1562–1580, 2009.

[TB03] Ben Tonor and Dave Bacon. Communication cost of simulating Bell correlations. *Physical Review Letters*, 91:187904, 2003.

[Val80] Leslie Valiant. Negation can be exponentially powerful. *Theoretical Computer Science*, 12:303–314, 1980.

[Vav09] Stephen Vavasis. On the complexity of nonnegative matrix factorization. *SIAM Journal on Optimization*, 20(3):1364–1377, 2009.

[Yan91] Mihalis Yannakakis. Expressing combinatorial optimization problems by linear programs. *Journal of Computer and System Sciences*, 43(3):441–466, 1991.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de