# Quantum Computing (Fall 2013) Instructor: Shengyu Zhang.

# Lecture 8 Quantum communication complexity: A recent protocol

*The original plan was to talk about lower bounds on quantum communication complexity, but it may again well fall into the category of being “too difficult”. So after some reflections, I decided to change to something lighter but probably with a broader range of applications.*

## Fourier analysis over

In computer science, we often run into real-valued functions defined on . (Name some examples yourself; you’d find that actually it’s even hard to think of any common function we studied that doesn’t fall into this category.) These functions form a linear space

It is easily seen that the addition of any two real-valued functions on the same domain gives another real-valued function on the domain.

A standard set of basis of this space contains the following ones:

where .

Actually these basis functions, when scaled up by a factor of , are *orthonormal* under the inner product defined by

where all expectations in this note are over uniform distribution unless stated otherwise. Namely, we have that . There is actually another orthonormal basis defined by characters.

where

**Exercise.** Verify that these character functions form an orthonormal basis.

The new basis is usually called the Fourier basis. Any real-valued function can be written in the Fourier basis:

and the coefficients are called Fourier coefficients, computed by

One useful fact about Fourier transform is that the multiplication in one domain becomes the convolution in the other. For , their convolution is defined by

In the Fourier domain, the definition is similar except for a normalization factor.

**Fact**. ,  .

One can define the -norm for as usual:

When , the quantity is the *Fourier sparsity* of , i.e. the number of nonzero Fourier coefficients.

Similarly, we can define an -norm for but note that it’s more convenient to use the expectation instead of summation.

An elegant fact is that

In computer science, we run into Boolean functions a lot. There are two ways of writing expressing a Boolean value--- or . Note that the group , where and are the XOR and multiplication, respectively. These two ways of representing a Boolean value can be exchanged easily as follows. Suppose that we use for -valued function and for the same function but with range , then

, and .

For Boolean functions with range , we have the following fact.

**Parseval Identity**. For any function , we have .

So one can view as a distribution over all .

## -degree, discrete derivatives

For Boolean functions , we can either view them as a polynomial over or a polynomial over .

**Exercise**. For the Parity function of 2 bits, write down it as a polynomial and .

Whenever we have a polynomial, we can talk about its degree. Note from the above example that the degree of as a polynomial over or that over are different. We denote by and the degrees as a polynomial over and that over , respectively.

One interesting operator on functions is the derivative. For any and any direction vector , the discrete derivative of along the direction is another function

defined by

Note that when we talk about polynomials over , all additions in the above equation are also over .

Just as derivatives for polynomials over , the discrete derivative also decrease the degree of a polynomial. That is,

When we use as the range, then the derivative changes to .

## Quantum Fourier transform

For a function , one can define an *n*-qubit quantum state

If one applies Hadamard gates, one on each qubit, then the state becomes

Verify this!

## XOR functions

XOR functions are the class of functions for some -bit function . We sometimes denote such function by The class contains interesting functions such as Equality and Hamming Distance. It also has an intimate connection to Fourier analysis because the rank of the communication matrix is nothing but the Fourier sparsity of , i.e. the number of nonzero Fourier coefficients.

**Exercise**. .

A lower bound for the quantum communication complexity for XOR functions is the following. First, let’s define a variant of the Fourier 1-norm.

**Theorem** ([LS09]). .

It was considered to be pretty tight, but it has lacked rigorous argument. Recently, the following bound was shown, which implies that the above lower bound is tight for low degree polynomials.

**Theorem** ([Z14]) where .

Next we give a protocol for a simpler case of exact communication, namely protocols without error. The communication cost is at most . The main idea is degree reduction. You’ll see how log naturally comes into the picture when using quantum protocols.

The analysis of the protocol needs the following fact.

**Fact**. For any , .

Proof. Let’s see what the Fourier coefficients of are. Define . Then

Thus,

Therefore, if , then there isn’ t with both and being nonzero. So for those .

Notation in the protocol: , , , .

To see why the protocol works, consider the second round. If is a constant, then is known; else, repeat the above procedure for . Let , and use to encode Fourier coefficients of . Note that though Alice doesn’t know and thus the Fourier coefficients of , she can still do that because for any , the Fourier support of is within .

Complexity: Stage takes communication qubits, and there is at most stages. Thus the total complexity is .

Protocol:

Bob

Alice

A random and the corresponding

Apply Hadamard on *C*, then measure *M*

Apply FT on *M*:

On :

On :

## Note

See [LS09] for a survey of classical and quantum lower bounds using norm-based methods. The protocol is from [Z14].

## Reference

[LS09] Troy Lee and Adi Shraibman, Lower bounds on communication complexity, *Foundations and Trends in Theoretical Computer Science*, 2009.

[Z14] Shengyu Zhang, Efficient quantum protocols for XOR functions, *Proceedings of the 25th Annual ACM-SIAM Symposium on Discrete Algorithms* (SODA), 2014, to appear.