# On the communication complexity of XOR functions

Ashley Montanaro

Department of Computer Science
University of Bristol
Bristol, UK

NUS, October 2009

Talk based on joint work with Tobias Osborne

arXiv:0909.3392

University of Bristol

Royal Holloway University of London

QICS

# Introduction

The setting of communication complexity (CC) studies the amount of communication between some parties required to complete some task.

# Introduction

The setting of communication complexity (CC) studies the amount of communication between some parties required to complete some task.

Here, we consider a traditional model of CC:

- There are two parties, Alice and Bob, each of whom gets an $n$-bit string $x$, $y$.

# Introduction

The setting of communication complexity (CC) studies the amount of communication between some parties required to complete some task.

Here, we consider a traditional model of CC:

- There are two parties, Alice and Bob, each of whom gets an $n$-bit string $x$, $y$.
- They want to compute some boolean function $f(x, y) : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}$ of their joint inputs.

# Introduction

The setting of communication complexity (CC) studies the amount of communication between some parties required to complete some task.

Here, we consider a traditional model of CC:

- There are two parties, Alice and Bob, each of whom gets an $n$-bit string $x$, $y$.
- They want to compute some boolean function $f(x, y) : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ of their joint inputs.
- They want to minimise the total number of (qu)bits transmitted.

# Introduction

The setting of communication complexity (CC) studies the amount of communication between some parties required to complete some task.

Here, we consider a traditional model of CC:

- There are two parties, Alice and Bob, each of whom gets an $n$-bit string $x$, $y$.
- They want to compute some boolean function $f(x, y) : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ of their joint inputs.
- They want to minimise the total number of (qu)bits transmitted.
- The minimum amount of communication they need is the communication complexity of $f$.

# Introduction

Variations of the model:

- Alice and Bob may have to succeed with certainty (the exact model) or with some constant probability $> 1/2$ (the bounded-error model).

# Introduction

Variations of the model:

- Alice and Bob may have to succeed with certainty (the exact model) or with some constant probability $> 1/2$ (the bounded-error model).
- They may be forced to only communicate in one direction (the one-way model), or may be allowed to communicate in both directions (the two-way model).

# Introduction

Variations of the model:

- Alice and Bob may have to succeed with certainty (the exact model) or with some constant probability $> 1/2$ (the bounded-error model).
- They may be forced to only communicate in one direction (the one-way model), or may be allowed to communicate in both directions (the two-way model).
- They may be allowed quantum communication, or just classical communication.

# Introduction

Variations of the model:

- Alice and Bob may have to succeed with certainty (the exact model) or with some constant probability $> 1/2$ (the bounded-error model).
- They may be forced to only communicate in one direction (the one-way model), or may be allowed to communicate in both directions (the two-way model).
- They may be allowed quantum communication, or just classical communication.
- They may be allowed to share public randomness.

# A zoo of communication complexity measures

For a function $f(x, y) : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}$, we define

| Quantity | Physics | Success prob. | Communication |
|---|---|---|---|
| $D^{cc}(f)$ | Classical | Exact | Two-way |
| $D^1(f)$ | Classical | Exact | One-way |
| $R_2^{cc}(f)$ | Classical | Bounded-error | Two-way |
| $R_2^1(f)$ | Classical | Bounded-error | One-way |
| $Q_E^{cc}(f)$ | Quantum | Exact | Two-way |
| $Q_E^1(f)$ | Quantum | Exact | One-way |
| $Q_2^{cc}(f)$ | Quantum | Bounded-error | Two-way |
| $Q_2^1(f)$ | Quantum | Bounded-error | One-way |

We will always allow Alice and Bob to share randomness, but not prior entanglement.

# Quantum vs. classical CC

We are interested in whether Alice and Bob can reduce the amount of communication they need by using quantum communication.

# Quantum vs. classical CC

We are interested in whether Alice and Bob can reduce the amount of communication they need by using quantum communication.

- Known that for partial functions (where there is a promise on the input) there can be an exponential separation between quantum and classical bounded-error CC, in both the one-way and two-way models [Raz '99, Gavinsky et al '07].

# Quantum vs. classical CC

We are interested in whether Alice and Bob can reduce the amount of communication they need by using quantum communication.

- Known that for partial functions (where there is a promise on the input) there can be an exponential separation between quantum and classical bounded-error CC, in both the one-way and two-way models [Raz '99, Gavinsky et al '07].
- Conjecture: For total functions, there can only be a polynomial separation between quantum and classical CC, in each of these models.

# Quantum vs. classical CC

We are interested in whether Alice and Bob can reduce the amount of communication they need by using quantum communication.

- Known that for partial functions (where there is a promise on the input) there can be an exponential separation between quantum and classical bounded-error CC, in both the one-way and two-way models [Raz '99, Gavinsky et al '07].
- Conjecture: For total functions, there can only be a polynomial separation between quantum and classical CC, in each of these models.
- We aim to study this by looking at a particular class of total functions: XOR functions.

# XOR functions

$g(x,y)$ is an XOR function if $g(x,y) = f(x \oplus y)$ for some boolean function $f : \{0,1\}^n \to \{0,1\}$.

# XOR functions

$g(x, y)$ is an XOR function if $g(x, y) = f(x \oplus y)$ for some boolean function $f : \{0, 1\}^n \to \{0, 1\}$.

The case where $f$ is symmetric ($f(x) = h(|x|)$) was recently studied by [Shi and Zhang '09]:

- Exact quantum CC is always $\Omega(n)$.
- Bounded-error two-way quantum CC is no better than classical CC (up to log factors).
- Proof uses a reduction to a previous result of [Razborov '03].

# New results for general functions

We have various partial results on XOR functions:

- A complete characterisation of exact one-way CC.

# New results for general functions

We have various partial results on XOR functions:

- A complete characterisation of exact one-way CC.
- A conjecture which would imply that exact quantum and deterministic CC are asymptotically equivalent.

# New results for general functions

We have various partial results on XOR functions:

- A complete characterisation of exact one-way CC.
- A conjecture which would imply that exact quantum and deterministic CC are asymptotically equivalent.
- Two general one-way randomised protocols, but...

# New results for general functions

We have various partial results on XOR functions:

- A complete characterisation of exact one-way CC.
- A conjecture which would imply that exact quantum and deterministic CC are asymptotically equivalent.
- Two general one-way randomised protocols, but...
- An exponential separation between one-way quantum and two-way deterministic CC.

# Specific types of function

We also consider two restricted types of function $f$:

- Monotone functions: $f(x \vee y) \geqslant \max\{f(x), f(y)\}$.

# Specific types of function

We also consider two restricted types of function $f$:

- Monotone functions: $f(x \vee y) \geqslant \max\{f(x), f(y)\}$.
- Linear threshold functions (LTFs):

$$f(x) = \begin{cases} 0 & \text{if } \sum_{i=1}^{n} w_i x_i \leqslant \theta \\ 1 & \text{if } \sum_{i=1}^{n} w_i x_i > \theta \end{cases}$$

for some $\theta$, the threshold of $f$, and some $\{w_i\}$, the weights of $f$.

# Specific types of function

We also consider two restricted types of function $f$:

- Monotone functions: $f(x \vee y) \geqslant \max\{f(x), f(y)\}$.
- Linear threshold functions (LTFs):

$$f(x) = \begin{cases} 0 & \text{if } \sum_{i=1}^{n} w_i x_i \leqslant \theta \\ 1 & \text{if } \sum_{i=1}^{n} w_i x_i > \theta \end{cases}$$

  for some $\theta$, the threshold of $f$, and some $\{w_i\}$, the weights of $f$.

- Can assume the weights are all strictly positive, implying that LTFs are monotone.

# Specific types of function

We also consider two restricted types of function $f$:

- Monotone functions: $f(x \vee y) \geqslant \max\{f(x), f(y)\}$.
- Linear threshold functions (LTFs):

$$f(x) = \begin{cases} 0 & \text{if } \sum_{i=1}^{n} w_i x_i \leqslant \theta \\ 1 & \text{if } \sum_{i=1}^{n} w_i x_i > \theta \end{cases}$$

  for some $\theta$, the threshold of $f$, and some $\{w_i\}$, the weights of $f$.

- Can assume the weights are all strictly positive, implying that LTFs are monotone.
- LTFs correspond to taking a weighted sum of differences between Alice and Bob's inputs.

## New results for specific types of function

We show that:

- For monotone functions, the separation between exact quantum and classical CC is at most quadratic.

# New results for specific types of function

We show that:

- For monotone functions, the separation between exact quantum and classical CC is at most quadratic.
- For LTFs, exact quantum CC is always $\Omega(n)$.

# New results for specific types of function

We show that:

- For monotone functions, the separation between exact quantum and classical CC is at most quadratic.
- For LTFs, exact quantum CC is always $\Omega(n)$.
- There is an efficient one-way randomised protocol for LTFs with high margin, where the margin

$$m = \min_x \left| \sum_i w_i x_i - \theta \right| .$$

# Fourier analysis

XOR functions can be studied using Fourier analysis on the boolean cube, i.e. the group $\mathbb{Z}_2^n$.

# Fourier analysis

XOR functions can be studied using Fourier analysis on the boolean cube, i.e. the group $\mathbb{Z}_2^n$.

Let $\chi_S : \{0,1\}^n \to \{\pm 1\}$ be the parity function $\chi_S(x) = (-1)^{\sum_{i \in S} x_i}$.

Then any function $f : \{0,1\}^n \to \mathbb{R}$ can be expanded as

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S)\, \chi_S(x),$$

for some $\{\hat{f}(S)\}$ – the Fourier coefficients of $f$.

# Fourier analysis

XOR functions can be studied using Fourier analysis on the boolean cube, i.e. the group $\mathbb{Z}_2^n$.

Let $\chi_S : \{0,1\}^n \to \{\pm 1\}$ be the parity function $\chi_S(x) = (-1)^{\sum_{i \in S} x_i}$.

Then any function $f : \{0,1\}^n \to \mathbb{R}$ can be expanded as

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S)\, \chi_S(x),$$

for some $\{\hat{f}(S)\}$ – the Fourier coefficients of $f$.

Define $\|\hat{f}\|_p := \left(\sum_{S \subseteq [n]} |\hat{f}(S)|^p\right)^{1/p}$, and the special case $\|\hat{f}\|_0 := |\operatorname{supp} \hat{f}| = |\{S : \hat{f}(S) \neq 0\}|$.

# Fourier analysis and XOR functions

One reason why Fourier analysis should help us study XOR functions:

Let $g(x, y) = f(x \oplus y)$ be an XOR function, and define the communication matrix $M_{xy} = g(x, y)$. Then, up to a constant factor, the eigenvalues of $M$ are the Fourier coefficients of $f$.

# Fourier analysis and XOR functions

One reason why Fourier analysis should help us study XOR functions:

Let $g(x, y) = f(x \oplus y)$ be an XOR function, and define the communication matrix $M_{xy} = g(x, y)$. Then, up to a constant factor, the eigenvalues of $M$ are the Fourier coefficients of $f$.

For example, this implies the following result for exact two-way quantum CC:

$$Q_E^{cc}(g) = \Omega(\log \|\hat{f}\|_0),$$

using the "log rank" lower bound of [Buhrman and de Wolf '01].

# Exact one-way CC

- In this model, Alice sends a message to Bob, who must compute $f(x \oplus y)$ with certainty.
- Recall that $D^1(f)$, $Q_E^1(f)$ denote the exact one-way classical/quantum CC's of $f$.

# Exact one-way CC

- In this model, Alice sends a message to Bob, who must compute $f(x \oplus y)$ with certainty.
- Recall that $D^1(f)$, $Q^1_E(f)$ denote the exact one-way classical/quantum CC's of $f$.
- Let supp $\hat{f}$ denote the support of the Fourier transform of $f$, i.e. $\{S : \hat{f}(S) \neq 0\}$, and think of this as a subset of $\{0,1\}^n$.
- Let dim $f$ be the minimum $k$ such that supp $\hat{f} \subseteq \{0,1\}^n$ lies in a $k$-dimensional subspace of $\{0,1\}^n$.

# Exact one-way CC

- In this model, Alice sends a message to Bob, who must compute $f(x \oplus y)$ with certainty.
- Recall that $D^1(f)$, $Q_E^1(f)$ denote the exact one-way classical/quantum CC's of $f$.
- Let $\operatorname{supp} \hat{f}$ denote the support of the Fourier transform of $f$, i.e. $\{S : \hat{f}(S) \neq 0\}$, and think of this as a subset of $\{0,1\}^n$.
- Let $\dim f$ be the minimum $k$ such that $\operatorname{supp} \hat{f} \subseteq \{0,1\}^n$ lies in a $k$-dimensional subspace of $\{0,1\}^n$.
- Then we have

$$D^1(f) = Q_E^1(f) = \dim f.$$

# Exact one-way CC

- $Q_E^1(f) = D^1(g) = \lceil \log_2 \mathrm{nrows}(g) \rceil$ [Klauck '00], where nrows$(g)$ denotes the number of distinct rows in the communication matrix $M_{xy} = g(x, y)$.

# Exact one-way CC

- $Q_E^1(f) = D^1(g) = \lceil \log_2 \mathrm{nrows}(g) \rceil$ [Klauck '00], where nrows$(g)$ denotes the number of distinct rows in the communication matrix $M_{xy} = g(x,y)$.

$$\mathrm{nrows}(g) \quad = \quad \sum_{x \in \{0,1\}^n} \frac{1}{|\{y : f^{\oplus x} = f^{\oplus y}\}|}$$

# Exact one-way CC

- $Q_E^1(f) = D^1(g) = \lceil \log_2 \mathrm{nrows}(g) \rceil$ [Klauck '00], where $\mathrm{nrows}(g)$ denotes the number of distinct rows in the communication matrix $M_{xy} = g(x, y)$.

$$\mathrm{nrows}(g) \quad = \quad \sum_{x \in \{0,1\}^n} \frac{1}{|\{y : f^{\oplus x} = f^{\oplus y}\}|} = \sum_{x \in \{0,1\}^n} \frac{1}{|\{y : f^{\oplus (x \oplus y)} = f\}|}$$

# Exact one-way CC

- $Q_E^1(f) = D^1(g) = \lceil \log_2 \mathrm{nrows}(g) \rceil$ [Klauck '00], where $\mathrm{nrows}(g)$ denotes the number of distinct rows in the communication matrix $M_{xy} = g(x,y)$.

$$\begin{aligned}
\mathrm{nrows}(g) &= \sum_{x \in \{0,1\}^n} \frac{1}{|\{y : f^{\oplus x} = f^{\oplus y}\}|} = \sum_{x \in \{0,1\}^n} \frac{1}{|\{y : f^{\oplus (x \oplus y)} = f\}|} \\
&= \frac{2^n}{|\{y : f^{\oplus y} = f\}|}
\end{aligned}$$

# Exact one-way CC

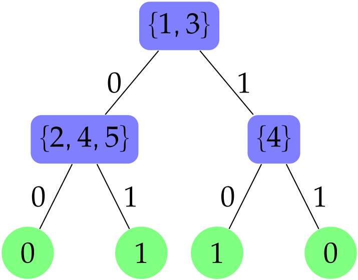
- $Q_E^1(f) = D^1(g) = \lceil \log_2 \mathrm{nrows}(g) \rceil$ [Klauck '00], where nrows$(g)$ denotes the number of distinct rows in the communication matrix $M_{xy} = g(x, y)$.

$$\begin{aligned} \mathrm{nrows}(g) &= \sum_{x \in \{0,1\}^n} \frac{1}{|\{y : f^{\oplus x} = f^{\oplus y}\}|} = \sum_{x \in \{0,1\}^n} \frac{1}{|\{y : f^{\oplus(x \oplus y)} = f\}|} \\ &= \frac{2^n}{|\{y : f^{\oplus y} = f\}|} = \frac{2^n}{|\{y : \langle y, s\rangle = 0 \ \forall s \in \mathrm{supp}\,\hat{f}\}|} \\ &= 2^{\dim f}. \end{aligned}$$

- We use the fact that $f = f^{\oplus y}$ if and only if $\chi_y \hat{f} = \hat{f}$.
- This implies that there is no $s \in \mathrm{supp}\,\hat{f}$ such that $\langle y, s \rangle = 1$, where the inner product is taken over $\mathbb{F}_2^n$.

# Parity decision trees

A parity decision tree for some function $f(x)$ is a decision tree whose nodes are queries to the parity of some subset of bits of the input $x$.




The parity decision tree complexity $D^{\oplus}(f)$ is the minimum depth of a parity decision tree for $f$.

# Exact two-way CC and parity decision trees

Let $D^{cc}(g)$ denote the exact classical CC of $g$.

**Observation**

Let $g(x,y) = f(x \oplus y)$ be an XOR fn. Then $D^{cc}(g) \leqslant 2D^{\oplus}(f)$.

# Exact two-way CC and parity decision trees

Let $D^{cc}(g)$ denote the exact classical CC of $g$.

**Observation**

Let $g(x, y) = f(x \oplus y)$ be an XOR fn. Then $D^{cc}(g) \leqslant 2D^{\oplus}(f)$.

Why? Any parity decision tree for $f$ that uses at most $D^{\oplus}(f)$ queries on any input gives a communication protocol for $g$:

- Each query to a subset $S$ of the bits of the string $x \oplus y$ can be simulated by Alice sending the parity $\bigoplus_{i \in S} x_i$ to Bob, and Bob sending Alice $\bigoplus_{i \in S} y_i$.
- This enables each of them to compute $\bigoplus_{i \in S}(x_i \oplus y_i)$.

# A conjecture about parity decision trees

**Conjecture**

Let $f : \{0,1\}^n \to \{1,-1\}$ be a boolean function. Then

$$D^{\oplus}(f) = O(\mathrm{polylog}(\|\hat{f}\|_0)).$$

# A conjecture about parity decision trees

**Conjecture**

Let $f : \{0,1\}^n \to \{1,-1\}$ be a boolean function. Then

$$D^{\oplus}(f) = O(\mathrm{polylog}(\|\hat{f}\|_0)).$$

Seems hard to prove, but in fact would follow from

**Conjecture**

Let $f : \{0,1\}^n \to \{1,-1\}$ be a boolean function. Then, for large enough $\|\hat{f}\|_0$, there exists a subset $T \subseteq [n]$ such that $|\,\mathrm{supp}(\hat{f}) \cap \mathrm{supp}(\hat{f}^{\Delta T})| \geqslant K\|\hat{f}\|_0$, for some constant $0 < K < 1$.

# One-way randomised protocols for XOR functions (1)

If $g(x,y) = f(x \oplus y)$, $f : \{0,1\}^n \to \{1,-1\}$ is an XOR function, then

$$R_2^1(g) = O(\|\hat{f}\|_1^2).$$

# One-way randomised protocols for XOR functions (1)

If $g(x,y) = f(x \oplus y)$, $f : \{0,1\}^n \to \{1,-1\}$ is an XOR function, then

$$R^1_2(g) = O(\|\hat{f}\|_1^2).$$

Protocol sketch:

- Alice and Bob pick $k = O(\|\hat{f}\|_1^2)$ subsets $\{S_i\}$ from the family of subsets of $[n]$, where the set $S$ is picked with probability $|\hat{f}(S)|/\|\hat{f}\|_1$.

# One-way randomised protocols for XOR functions (1)

If $g(x,y) = f(x \oplus y)$, $f : \{0,1\}^n \to \{1,-1\}$ is an XOR function, then

$$R_2^1(g) = O(\|\hat{f}\|_1^2).$$

Protocol sketch:

- Alice and Bob pick $k = O(\|\hat{f}\|_1^2)$ subsets $\{S_i\}$ from the family of subsets of $[n]$, where the set $S$ is picked with probability $|\hat{f}(S)|/\|\hat{f}\|_1$.
- Alice sends the Bob the $k$ bits $\chi_{S_i}(x)$, who uses these bits to compute

$$\sum_{i=1}^{k} \chi_{S_i}(x)\chi_{S_i}(y)\,\mathrm{sgn}(\hat{f}(S_i)) = \sum_{i=1}^{k} \chi_{S_i}(x \oplus y)\,\mathrm{sgn}(\hat{f}(S_i)),$$

and outputs 1 if the result is positive, and $-1$ if negative.

# One-way randomised protocols for XOR functions (1)

Proof sketch:

- For each $i$, $\chi_{S_i}(x \oplus y)\,\mathrm{sgn}(\hat{f}(S_i))$ is a sample from a random variable whose expectation is

$$\frac{1}{\|\hat{f}\|_1} \sum_{S \subseteq [n]} \chi_S(x \oplus y) \hat{f}(S) = \frac{f(x \oplus y)}{\|\hat{f}\|_1}.$$

# One-way randomised protocols for XOR functions (1)

Proof sketch:

- For each $i$, $\chi_{S_i}(x \oplus y)\,\mathrm{sgn}(\hat{f}(S_i))$ is a sample from a random variable whose expectation is

$$\frac{1}{\|\hat{f}\|_1} \sum_{S \subseteq [n]} \chi_S(x \oplus y) \hat{f}(S) = \frac{f(x \oplus y)}{\|\hat{f}\|_1}.$$

- The proof follows by a Chernoff bound.

This protocol is a variant of a protocol of [Kremer, Nisan and Ron '99].

# One-way randomised protocols for XOR functions (2)

If $g(x, y) = f(x \oplus y)$ is an XOR function where $f$ differs from a parity function on $k$ inputs, then

$$R_2^1(g) = O(\log k).$$

Special case: if $f$ takes the value 0 on $k$ inputs, $R_2^1(g) = O(\log k)$.

# One-way randomised protocols for XOR functions (2)

If $g(x, y) = f(x \oplus y)$ is an XOR function where $f$ differs from a parity function on $k$ inputs, then

$$R_2^1(g) = O(\log k).$$

Special case: if $f$ takes the value 0 on $k$ inputs, $R_2^1(g) = O(\log k)$.

Proof idea:

- Parity functions can be computed using $O(1)$ communication.
- Can check whether the input is in the "bad" set that differs from a parity function using $O(\log k)$ communication.

# One-way protocols are not the whole story

For any integer $m$, there is an XOR function $g = f(x \oplus y)$ such that $D^{cc}(g) = O(m)$, but $Q_2^1(g) = \Omega(2^m)$.

# One-way protocols are not the whole story

For any integer $m$, there is an XOR function $g = f(x \oplus y)$ such that $D^{cc}(g) = O(m)$, but $Q_2^1(g) = \Omega(2^m)$.

- The function $f$ is the addressing function on $m$ bits.
  - Divide the input into an $m$-bit address register $a$ and a $2^m$-bit data register $d$, then set $f(a, d) = d_a$.

# One-way protocols are not the whole story

For any integer $m$, there is an XOR function $g = f(x \oplus y)$ such that $D^{cc}(g) = O(m)$, but $Q_2^1(g) = \Omega(2^m)$.

- The function $f$ is the addressing function on $m$ bits.
  - Divide the input into an $m$-bit address register $a$ and a $2^m$-bit data register $d$, then set $f(a, d) = d_a$.

**Theorem**

If the matrix $M_{xy} = g(x, y)$ has a $2^k \times k$ submatrix whose rows are all distinct, then $Q_2^1(g) = \Omega(k)$ [Klauck '00].

# One-way protocols are not the whole story

For any integer $m$, there is an XOR function $g = f(x \oplus y)$ such that $D^{cc}(g) = O(m)$, but $Q_2^1(g) = \Omega(2^m)$.

- The function $f$ is the addressing function on $m$ bits.
  - Divide the input into an $m$-bit address register $a$ and a $2^m$-bit data register $d$, then set $f(a, d) = d_a$.

**Theorem**

If the matrix $M_{xy} = g(x, y)$ has a $2^k \times k$ submatrix whose rows are all distinct, then $Q_2^1(g) = \Omega(k)$ [Klauck '00].

- Take the submatrix whose rows are of the form $(0, d)$, and columns of the form $(a, 0)$.
- For all pairs $d \neq d'$, there exists an $a$ such that $d_a \neq d'_a$.

# Monotone functions

If $g(x,y) = f(x \oplus y)$ is an XOR function with $f$ monotone, we have

$$D^{cc}(g) \leqslant 2D(f) \leqslant 4s(f)^2 \leqslant 4\deg_2(f)^2 \leqslant 4(\log_2 \|\hat{f}\|_0)^2.$$

# Monotone functions

If $g(x,y) = f(x \oplus y)$ is an XOR function with $f$ monotone, we have

$$D^{cc}(g) \leqslant 2D(f) \leqslant 4s(f)^2 \leqslant 4\deg_2(f)^2 \leqslant 4(\log_2 \|\hat{f}\|_0)^2.$$

where:

- $D^{cc}(g)$ is the exact classical CC of $g$.
- $D(f)$ is the classical decision tree complexity of $f$.
- $s(f)$ is the sensitivity of $f$, i.e. the max over $x$ of the # of neighbours $y$ of $x$ such that $f(x) \neq f(y)$.
- $\deg_2(f)$ is the degree of $f$ as a polynomial over $\mathbb{F}_2$.

Only the third inequality is new.

# Linear threshold functions (1)

Finally, we have some lower and upper bounds on the CC of LTFs.

# Linear threshold functions (1)

Finally, we have some lower and upper bounds on the CC of LTFs.

Let $g(x, y) = f(x \oplus y)$, where $f$ is an LTF. Then

$$Q_E^{cc}(g) = \Omega(n).$$

Proof idea: show that $s(f) = \Omega(n)$, and use previous argument.

# Linear threshold functions (2)

$$R_2^1(g) = O((\theta/m)^2)$$

- Recall the margin $m = \min_x |\sum_i w_i x_i - \theta|$.
- Protocol idea: Alice and Bob estimate $\sum_i w_i(x_i \oplus y_i)$ to within tolerance $m$.
- This can be done by looking at parities of subsets of the input.
- Can be seen as a generalisation of a protocol of [Huang et al '06] for computing the Hamming distance.

# Conclusions

- XOR functions are an elegant setting in which to study communication complexity.

- We have various partial results, but have still not answered the original question: are the quantum and classical CC's of these functions polynomially related?

# Conclusions

- XOR functions are an elegant setting in which to study communication complexity.

- We have various partial results, but have still not answered the original question: are the quantum and classical CC's of these functions polynomially related?

Further reading:

- Our paper: `arXiv:0909.3392`
- Survey paper on Fourier analysis by Ronald de Wolf: `theoryofcomputing.org/articles/gs001/gs001.pdf`
- Lecture course on Fourier analysis by Ryan O'Donnell: `www.cs.cmu.edu/~odonnell/boolean-analysis/`

# The end

Thanks for your time!