Tradeoffs between Quantum Memory and Communication

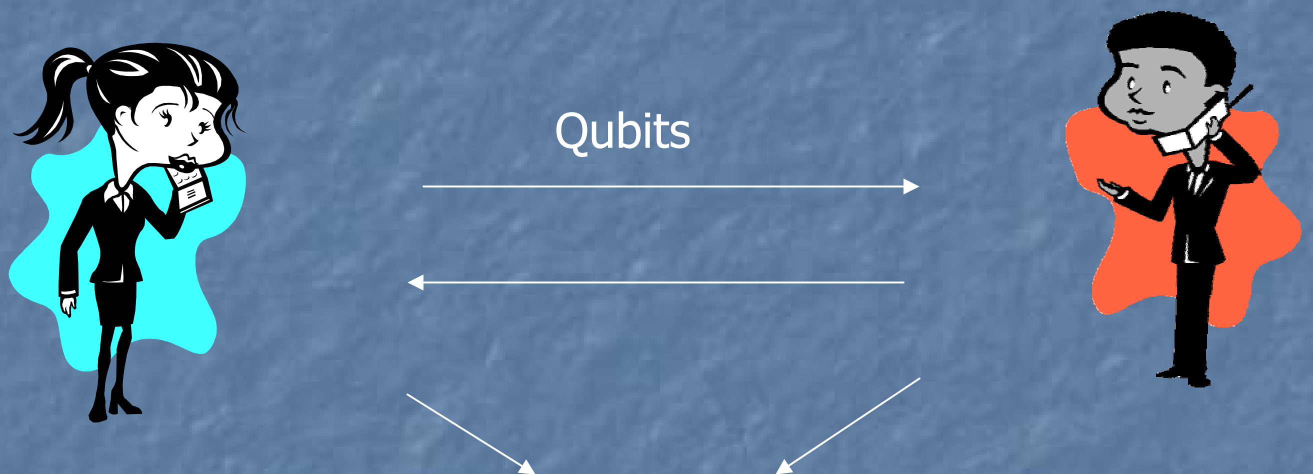
Hartmut Klauck
University of Calgary

I.

Communication complexity with bounded memory

Motivation: What is the computational power of quantum computation with a limited number of qubits?

Model A): Quantum communication complexity



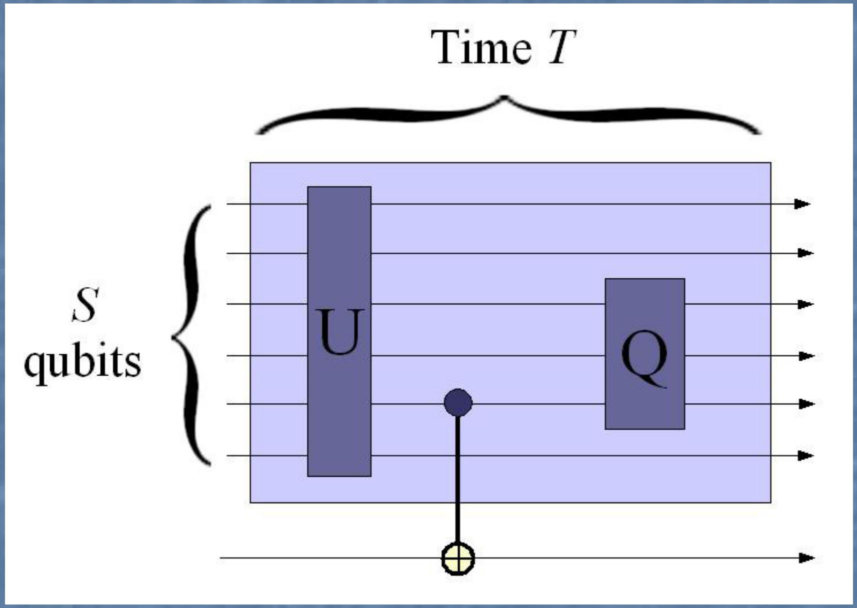
$x \in \{0,1\}^n$ Outputs $y \in \{0,1\}^n$

Cost of a protocol: number of qubits sent

Complexity $Q(f)$: cost of best protocol

Model B): Memory bounded quantum circuits

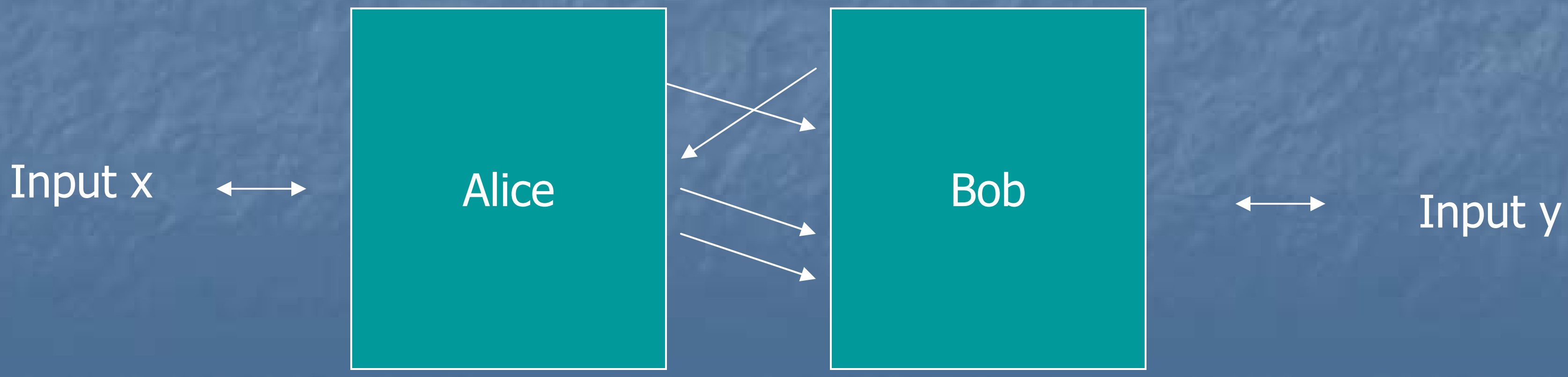
- Circuits on S qubits, accessing input as oracle
- U: unitary op
- output gate: *controlled not* to extra qubit
- Q: query gate:



$$|i\rangle|a\rangle \mapsto |i\rangle|a \oplus q(i)\rangle$$

Model C): Communicating quantum circuits, bounded memory

- Quantum circuit in two parts
- Separate input oracles
- Circuit with C qubit wires crossing uses communication C
- Work on S qubits



Conventions

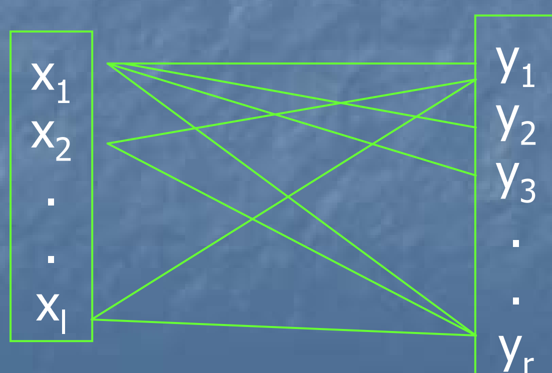
- Outputs are sent to the other circuit
- Circuits may “drop” qubits and use fresh qubits

An Example

- DISJ(x,y)=1 iff $\sum_{i=1..n} x_i$ Æ $y_i > 0$
- Grover-like Protocol [BCW98] searches for i with $x_i=y_i=1$
- Uses $O(\log n)$ qubits and $O(n^{1/2} \log n)$ communication
- No classical protocol is better than $\Omega(n)$ [KS87] (independent of space)
  $O(n)$ with space $O(\log n)$ possible
- So does more memory ever help?

Functions

- Let $f:\{0,1\}^n \pounds \{0,1\}^n \alpha \{0,1\}$
- Then $f_{l,r}$ computes on $\{0,1\}^{n \text{¢} l} \pounds \{0,1\}^{n \text{¢} r}$ $f(x,y)$ for all $l \text{¢} r$ pairs of inputs (lr outputs)



Functions

- Examples:
- IP(x,y) = ©$_{i=1..n}$ x_i Æ y_i (inner product)
- DISJ(x,y) = 1 iff $\sum_{i=1..n} x_i$ Æ $y_i > 0$

- $\mathrm{DISJ}_{n,n}$ Boolean matrix product
- $\mathrm{IP}_{n,n}$ Matrix product GF(2)
- $\mathrm{IP}_{n,1}$ Matrix vector product

Complexity Notation

- Always allow error 1/3
- $C_S(f)$ denotes classical communication with space S
- $Q_S(f)$ denotes quantum communication with space S

Results

- Inner Product:

$C_S(IP_{l,r}) < O\ (l\ r\ n\ /\ \min\{S,l\}\ )$

$Q_S(IP_{l,r}) > \Omega(l\ r\ n\ /\ S)$

$C_S(IP_{n,n}\ ) = \Theta(n^3/S)=\Theta(Q_S(IP_{n,n}))$

$C_S(IP_{n,1}\ ) = \Theta(n^2/S)=\Theta(Q_S(IP_{n,1}))$

Results

- More general, f with discrepancy bound d have $Q_S(f_{l,r}) > \Omega(l\ r\ d\ /\ S)$.
- Classically: Beame et al. prove lower bounds for universal hash functions

What about DISJ?

- Disjointness:

  $Q_S(DISJ_{l,r}) < \tilde{O}\,(l\ r\ n^{1/2} / S^{1/2})$

  $Q_S(DISJ_{n,n}) < \tilde{O}(n^{2.5} / S^{1/2})$

  $Q_S(DISJ_{n,1}) < \tilde{O}(n^{1.5} / S^{1/2})$

- Even classical lower bound for $DISJ_{n,n}$ unknown!, probably $\Theta(n^3 / S)$

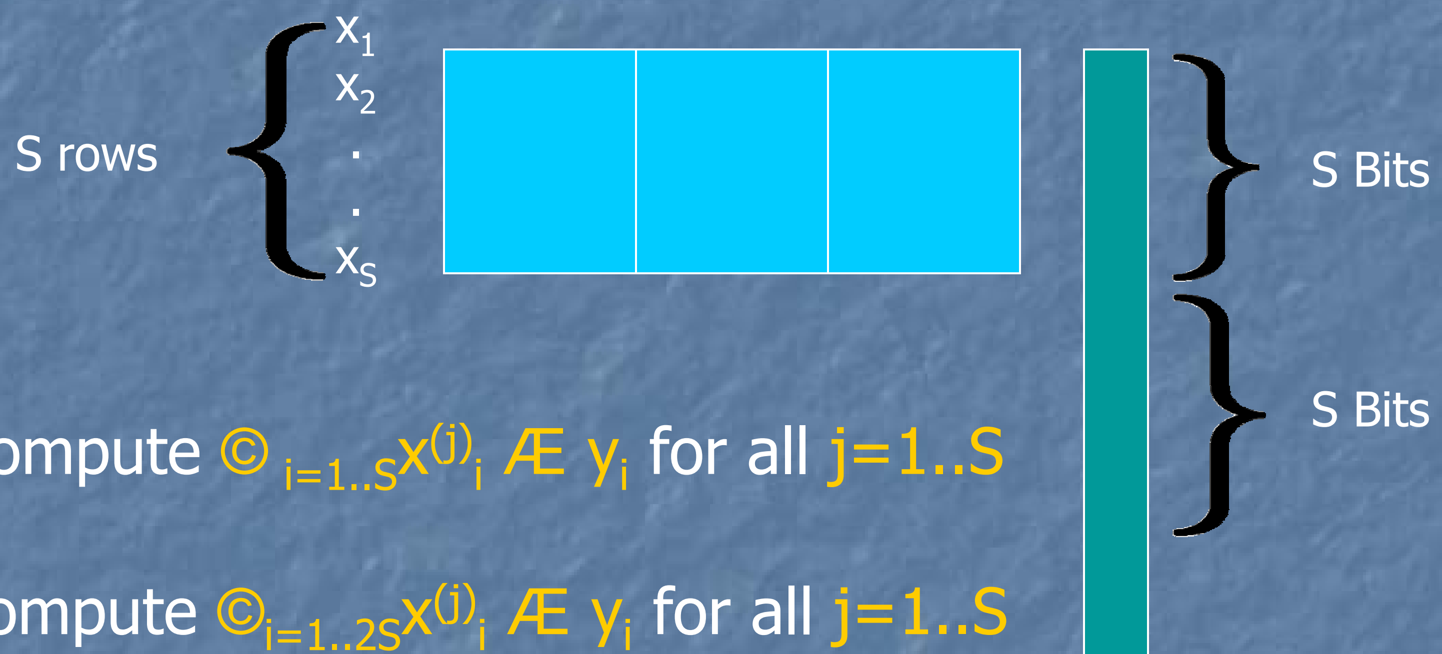
II.

Inner product modulo 2

Inner product, upper bound

- Asume l,r > S
- Solve $IP_{S,1}$ and iterate l/S ¢ r times
- To solve $IP_{S,1}$ Bob sends S bits of his input, Alice computes partial sums for all S function values
- Iterate n/S times
- Overall complexity l/S ¢ r ¢ S¢ n/S=l r n / S
- Storage S

Inner product, upper bound



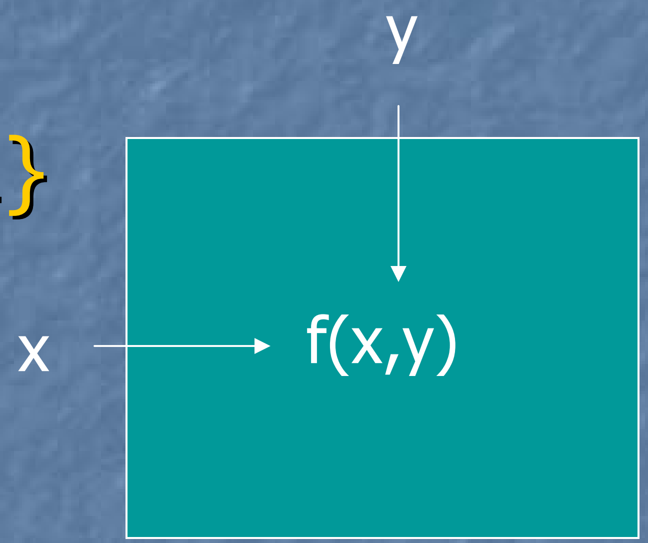
Compute © $_{i=1..S}x^{(j)}_i$ Æ y_i for all j=1..S

Compute ©$_{i=1..2S}x^{(j)}_i$ Æ y_i for all j=1..S

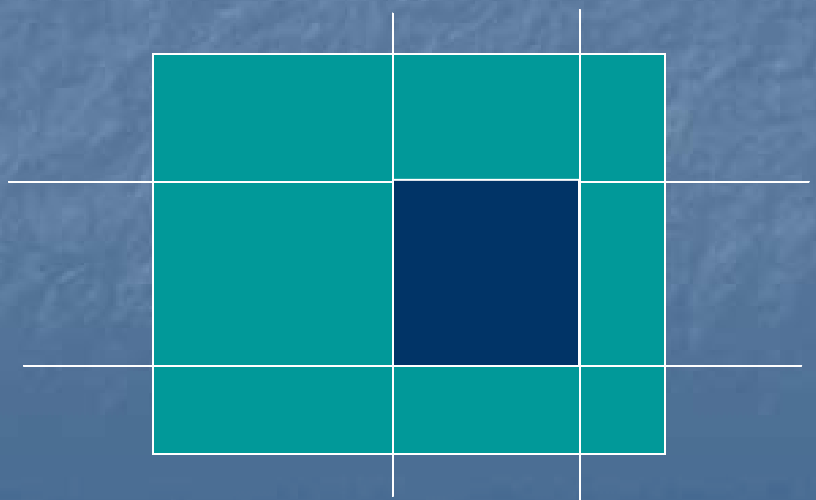
etc.

The lower bound

- $f:\{0,1\}^n$ £ $\{0,1\}^n$ α $\{0,1\}$
- M_f is the communication matrix:



- Rectangle: product set in the matrix



The discrepancy bound

- disc(f)=max$_R$ |μ(R Å f^{-1}(1))-μ(R Å f^{-1}(0))| over rectangles R (uniform distribution μ)
- [KY]: Q(f)> Ω(-log disc(f))

- Here: $Q_S(f_{l,r})$ > Ω(lr ¢ -log(disc(f))/S)

Application

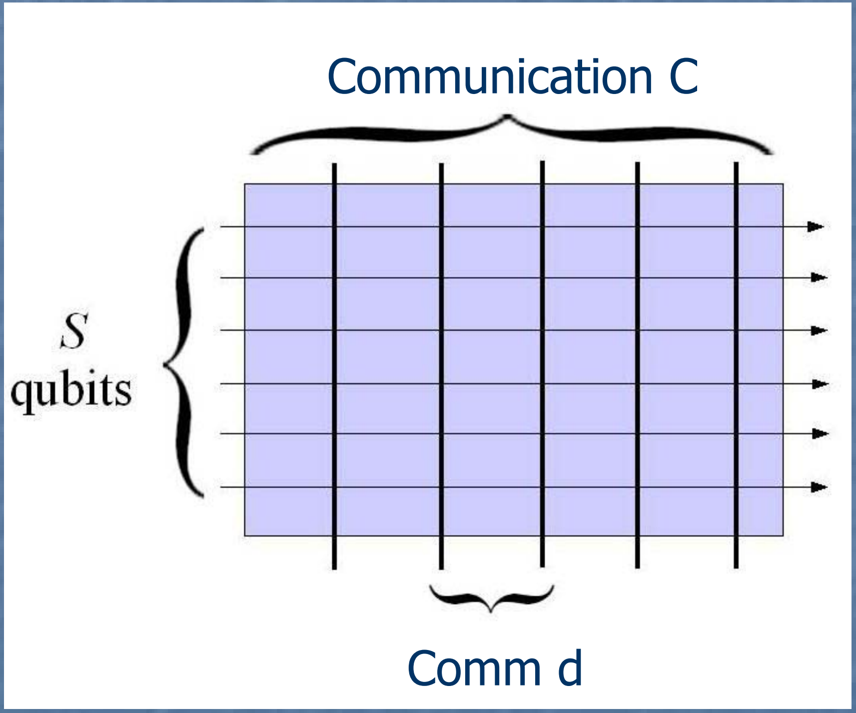
- [Chor et al.] $disc(IP) < 1/2^{n/2}$
- Hence $Q_S(IP_{l,r}) > \Omega(lrn/S)$
- Matrix Product over GF(2) needs communication n^3/S,
  Matrix Vector Product needs n^2/S

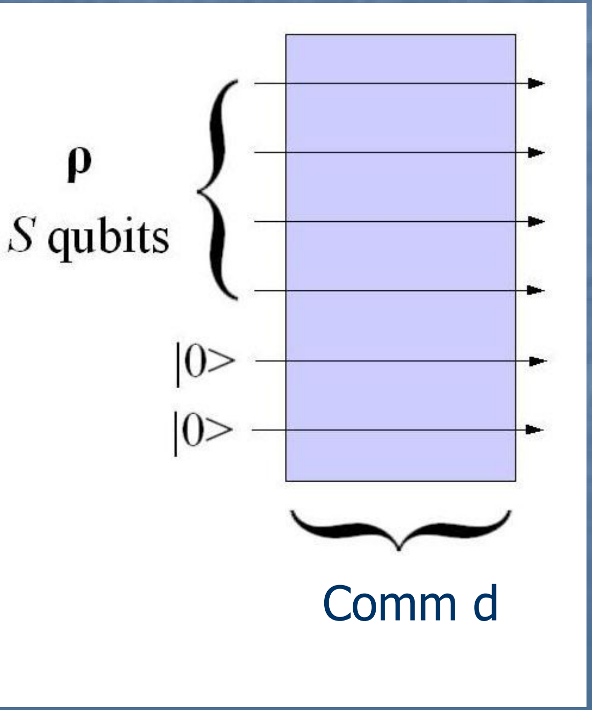
How to prove it

- Given circuit pair with communication C and space S
- Slice the circuit into segments containing communication d, if disc(f) ¼ $1/2^d$
- Intuitively not enough communication to compute f even once
- Show that each slice can make few outputs, namely $O(S)$
- Then C/d ¢ $S > \Omega($ l r $)$

Slicing the circuit

Show: <O(S) outputs





How to prove it

- If each slice has $O(S)$ outputs, then: C/d ¢ $O(S) > lr$
- Furthermore can assume that $S < o(d)$, since else with $C>lr$ we get $C>\Omega(lrd/S)$

The initial information

- Suppose a circuit produces some output with probability p, given some initial state ρ on S qubits.
- Idea: replace ρ by the totally mixed state.
- Claim: circuit succeeds with probability $p/2^S$
- Reason: every quantum state "sits" in the totally mixed state with "size" $1/2^S$

Why that?

- Totally mixed state is $M=\mathrm{diag}(1/2^S,\ldots,1/2^S)$
- For all density matrices ρ there is a density matrix σ so that $M=1/2^S\rho+(1-1/2^S)\sigma$

Direct Products

- Given communicating quantum circuits with communication d
- Produce L outputs with success probability 2/3 ¢ $1/2^{S}$.
- Show that all such circuits have success probability at most $1/2^{\Omega(L)}$
- Then $L=O(S)$
- Need to show this only for $L<o(d)$

Direct Products

- $f_{l,r}$ with $disc(f)<1/2^d$.
- Select L=const ¢ $S = o(d)$ and $L<lr$ and L outputs for $f(x_i,y_j)$
- Show that success probability of a quantum protocol w/ communication d is $1/2^{\Omega(L)}$
- Hardest case: $L=lr$ (most dependencies)

Direct Products

- Know that each rectangle in $\{0,1\}^n$£$\{0,1\}^n$ contains ½§ $1/2^d$ zero-inputs and ½§$1/2^d$ one-inputs or has size < $1/2^d$

A) Show that rectangles in $\{0,1\}^{nl}$£$\{0,1\}^{nr}$ contain each of $L=2^{lr}$ function values with probability $1/2^L + 1/2^{d/2}$ for $L<o(d)$

B) Show that each quantum protocol with communication d and correctness $2^{-o(L)}$ induces better rectangles

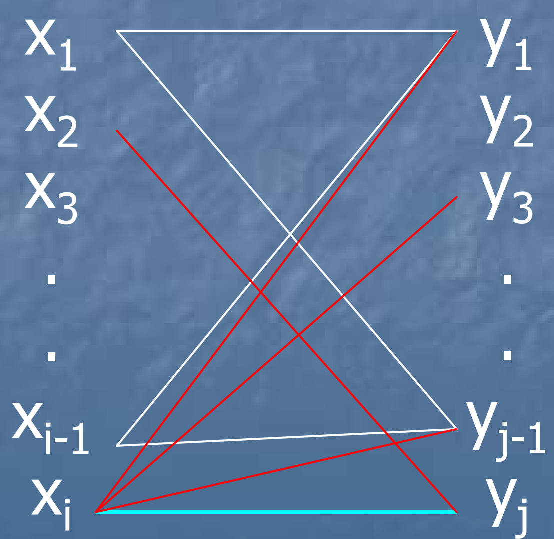
A)

- Rectangle in $\{0,1\}^{nl}£\{0,1\}^{nr}$
- What is probability of $f(x_i,y_i)=c_{ij}$ for all i,j and some fixed c_{ij}?

Product of conditional probabilities that $f(x_i,y_j)=c_{ij}$ given previous $f(x_u,y_v)=c_{uv}$.

A)

- Current input pair: x_i, y_j
- Conditions not involving x_i or y_j , white
- Conditions involving x_i or y_j , red



A)

- Fix all x_u, y_v other than x_i, y_j
- Obtain rectangle R in $\{0,1\}^n$£ $\{0,1\}^n$
- Case 1: R is smaller than $½^d$
  All such rectangles can have combined size $½^d$ at most
  (in uniform distribution on $\{0,1\}^{ln}$£$\{0,1\}^{rn}$)

A)

- Other case: R is "large"
- Further conditions: $f(x_i,y_v)=c_{iv}$ (row conditions)
- $f(x_u,y_j)=c_{uj}$ (column conditions)
- Lead to $<2^L$ disjoint subrectangles
- Each contains $1/2$§ $1/2^d$ zeroes/ones
- Overall R contains $1/2$§ $2^L/2^d$ zeroes/ones

A) fin.

- Hence
  $Prob(f(x_i,y_j)=c_{ij})<1/2+2^L/2^d < 1/2+2^{d/2}$
  for all conditions
- $Prob(f(x_i,y_j)=c_{ij}$ for all i,j)
  $< (1/2 +1/2^{d/2})^L$
  $< 1/2^L + 2/2^{d/2}$

B)

- Given is a quantum protocol with L outputs, communication C and success probability $1/2^L + p$
- Find a rectangle that contains inputs with $f(x_i, y_j) = c_{ij}$ in proportion $1/2^L + p/2^C$
- Proof by decomposing protocols into weighted rectangles

II.

Disjointness

Disjointness upper bound

- DISJ(x,y)=1 iff $\sum_{i=1..n} x_i$ Æ $y_i > 0$

- $Q_S(\mathrm{DISJ}_{l,r}) < \tilde{O}\ (l\ r\ n^{1/2} / S^{1/2})$

  $Q_S(\mathrm{DISJ}_{n,n}) < \tilde{O}(n^{2.5} / S^{1/2})$

  $Q_S(\mathrm{DISJ}_{n,1}) < \tilde{O}(n^{1.5} / S^{1/2})$

Upper bound

- Solve $\mathrm{DISJ}_{S,1}$ with communication $\tilde{O}(\ (nS)^{1/2}\ )$ and space S
- Iterate lr/S times, communication $\tilde{O}(lr/S\text{¢}\ (nS)^{1/2}) = \tilde{O}(lr\ n^{1/2}/S^{1/2})$

Protocol for $\text{DISJ}_{S,1}$

- Alice has sets $x_1,\ldots,x_S$; Bob has set y
- Alice and Bob run a Grover-like protocol on $z=[\ x_i$ and y
- Find $j\ 2\ z$ Å y
- Determine all x_i with $j2\ x_i$, call their union z'
- Set $z=z-z'$ and iterate.

Protocol

- Problem: cannot store z explicitly (size n)
- Can store array of inputs x_i for which output is already computed
- Construct superposition $\sum_{j: j \in z} |j\rangle$ from oracle and array
- During the protocol use the oracle to implement each Grover iteration

Analysis

- Assume that $|z$ Å $y|=K_l$ in step l.
- Then one element in the intersection can be found with $\tilde{O}(n^{1/2} / K_l^{\ 1/2})$ Grover iterations
- All elements can be found with $\tilde{O}(n^{1/2}$ ¢ $K_l^{\ 1/2})$ iterations
- If $K_l < S$ then find all with $(nS)^{1/2}$ at most
- If $K_l > S$, then find one element with $n^{1/2} / S^{1/2}$ at most , at most S iterations
- Cost always $(nS)^{1/2}$

Conclusion

- Have analyzed the effect of a limited number of qubits on the quantum communication complexity
- If the discrepancy bound is good, then quantum does not seem to help
- Matrix product over GF(2): no speedup by quantum
- For Boolean matrix vector product: given upper bound

Open Problems

- Lower bounds for $DISJ_{l,r}$, i.e., for Boolean matrix products (even open classically)
- Communication-space tradeoffs for decision problemss