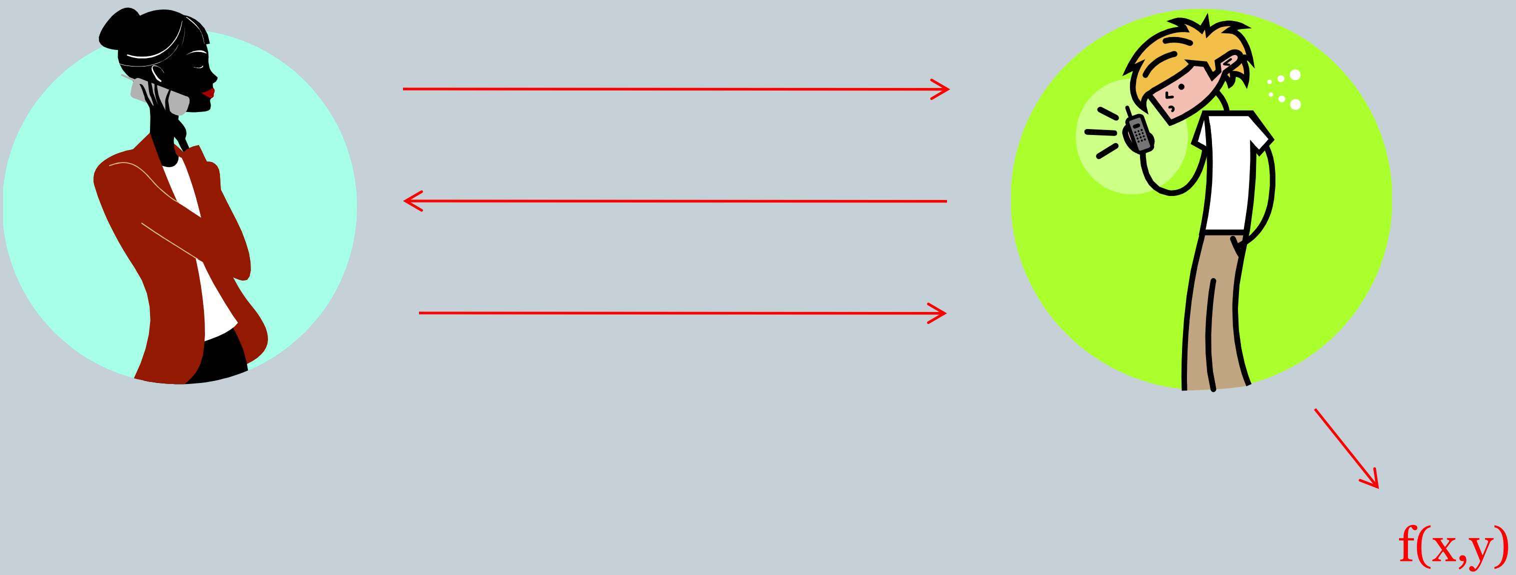
Arthur Merlin Games in Communication Complexity

HARTMUT KLAUCK
CENTRE FOR QUANTUM TECHNOLOGIES (CQT) AND NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

Communication Complexity

- A “toy” model of computation [Y79]
- One can actually prove complexity theory statements!
- Extends information theory to more complex scenarios
- Lots of applications to other models of computations

The model



- Alice and Bob communicate to compute a function f(x,y)
- Alice knows x Bob knows y

Applications

- Lower bounds in communication complexity can be used to show lower bounds for various models
  - 1-tape Turingmachines (Time)
  - (Monotone) Boolean circuits
    - Linear lower bound on circuit depth for matching problem follows from R(DISJ) bound
  - Datastream Algorithms
  - Automata
  - Data-structures/cell-probe models
  - VLSI chips (Time-Area tradeoffs)
  - Amount of entanglement needed for optimal communication
  - Limits of Proof Techniques in complexity theory
    - Algebrization [AW08]

Modes of Communication

- Different variants of the model
  - Deterministic
  - Randomized (with error)
  - Quantum (with error)
  - Unbounded error
- Notations:
  - D(f) for deterministic
  - R(f) for randomized
  - Q(f) for quantum
  - PP(f) for unbounded error

Interactive Proofs

- Interactive proofs were introduced in the 80‘s
  - Babai 85, Goldwasser Micali Rackoff 85
- Important area in TCS
- Many results:
  - PCP theorem
  - Inapproximability
  - IP=PSPACE

- Simplest Interactive proof systems: Arthur-Merlin games
- These systems define more complicated modes of computation than nondeterminism etc.

The AM Hierarchy

- Classes:
  - NP: No randomization, no interaction
  - MA: randomization, no interaction
  - AM: a random „challenge“ can be sent to the prover
  - AMAMAMAMAM many rounds of interaction between prover and verifier
- AM(k)$\subseteq$ AM for all constant k
- AM(poly(n))=IP=PSPACE (=QIP)
- On the other hand:
  - MA$\subseteq \Sigma_2^p \cap \Pi_2^p \cap$ PP
  - AM$\subseteq \Pi_2^p$

Some Problems

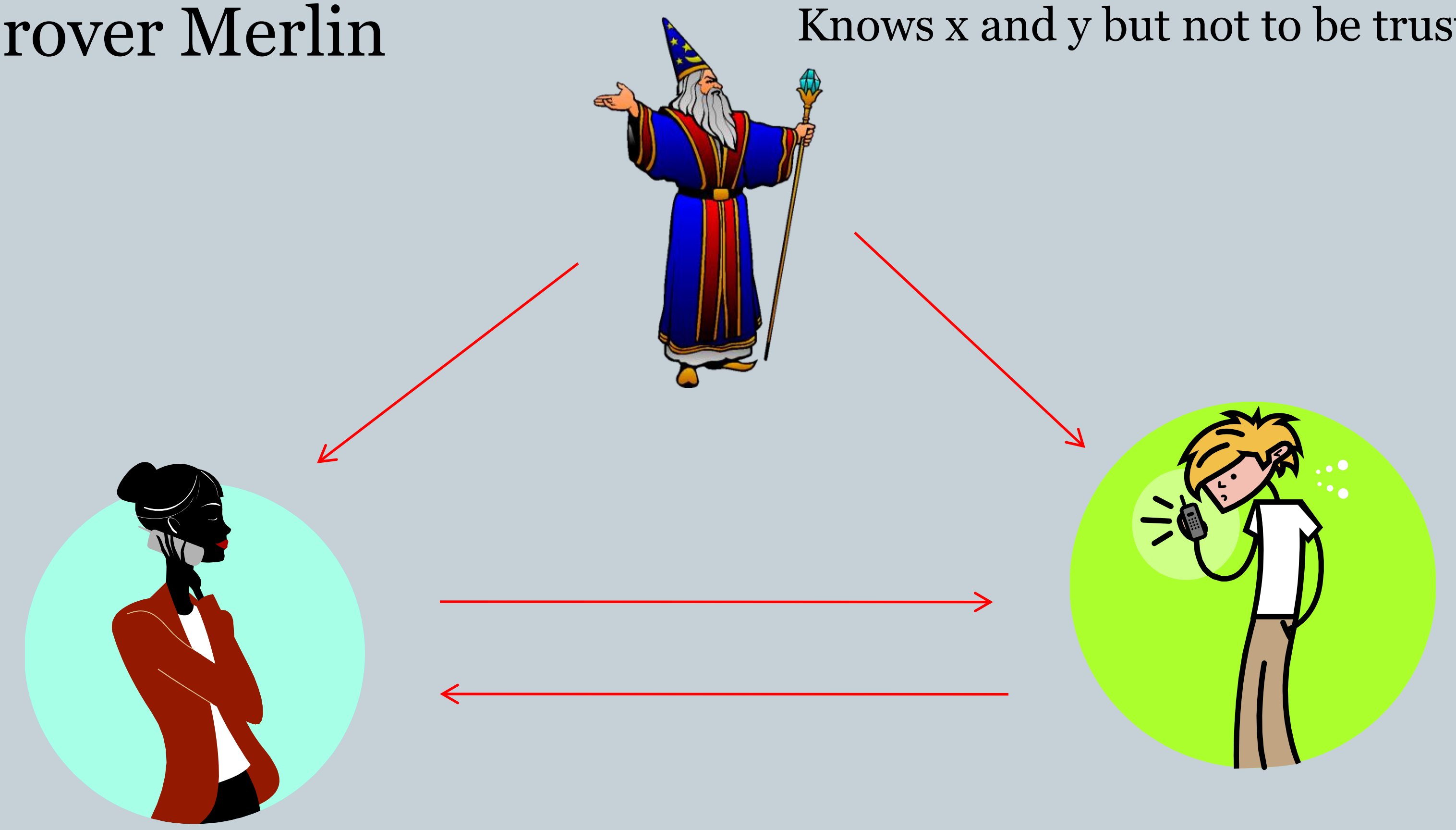
- Disjointness:
  - Alice holds a subset x of {1,…,n}
  - Bob holds a subset y of {1,…,n}
  - Accept if x and y are disjoint?
- Inner Product:
  - Alice and Bob have bit strings x,y
  - Compute $\sum_{i=1\ldots n} x_i \wedge y_i$

Complexity Bounds

- $R(DISJ)=\Theta(n)$ [KS87,R90]
- $R(IP)=\Theta(n)$ [CG85]
  - Actually $PP(IP)=\Theta(n)$ and hence $Q(IP)=\Theta(n)$
- $Q(DISJ)=\Theta(n^{1/2})$ [R02,AA03]

Interactive proofs in communication

- Extend the model
- Prover Merlin



Merlin Arthur Communication

- MA(f)
  - Classical proof verified (with error) by classical Alice and Bob
- QMA(f)
  - Quantum proof, quantum communication
- QCMA(f)
  - Classical proof, quantum communication
- AM(f)
  - (Classical) Alice and Bob “challenge” Merlin before receiving the (classical) proof, then they verify together

Merlin Arthur Communication

- Motivation:
  - The rectangle bound lies between $MA(f)^{1/2}$ and $AM(f)$
  - Separations between these complexities imply that the corresponding Turing Machine class separations are not possible with current techniques (do no “algebrize”)
  - What is the power of quantum proofs?
  - Data Stream algorithms with a “helper” … Cloud computing

Merlin Arthur

- The prover sends one classical message to Alice
- Then Alice and Bob communicate (using randomness)
- Cost: length of proof + length of communciation
- Correctness:
- $f(x,y)=1$: $\exists$ proof p: Prob(accept x,y,p) $\geq 2/3$
- $f(x,y)=0$: $\forall$ proofs p: Prob(accept x,y,p) $\leq 1/3$

- Important: include length of proof in cost!

Quantum Merlin Arthur

- The prover sends one quantum message to Alice
- Then Alice and Bob communicate (using qubits)
- Cost: length of proof + length of communciation
- Correctness:
- $f(x,y)=1$: $\exists$ proof p: Prob(accept x,y,p)$\geq 2/3$
- $f(x,y)=0$: $\forall$ proofs p: Prob(accept x,y,p)$\leq 1/3$

Arthur Merlin

- First a public coin random string r is chosen, known to Alice, Bob, Merlin
- The prover sends one classical message to Alice
- Then Alice and Bob communicate (using no further randomness)
- Cost: length of communication
- Correctness:
- $f(x,y)=1$: With prob. 2/3 there$\exists$ proof p: x,y,p,r accepted
- $f(x,y)=0$: With prob. 2/3:$\forall$ proofs p: x,y,p,r not accepted

Alternative Arthur Merlin

- Can allow Alice and Bob to use more randomness later
- Call this AMA
- We provide only upper bounds for AM, so use weaker definition

- AM definition nicer: probability distribution on nondeterministic protocols

Disjointness

- [K03] shows $MA(DISJ)=\Omega(n^{1/2})$
- Is this tight??
- Most people thought not!
- [AW09] give $O(n^{1/2} \log n)$ protocol
- Idea: view the input as $n^{1/2} \times n^{1/2}$ bits
- Input x is Boolean function $x(i,j)$
- Extend to a low degree polynomial (field size n)

Disjointness

- We want to know $\sum_{i=1 \ldots n^{1/2}} \sum_{j=1 \ldots n^{1/2}} x(i,j) \cdot y(i,j)$
- x,y are polynomials of degree $n^{1/2}$
- Merlin‘s proof: $\sum_{j=1 \ldots n^{1/2}} x(i,j) \cdot y(i,j)$
  - A polynomial p of degree $2n^{1/2}$ in i
  - Specify with $2n^{1/2}$ field elements!
- If p is correct we can compute the inner product!
- Else we can test easily: need to check for a random r in the field if
  $p(r)=\sum_{j=1 \ldots n^{1/2}} x(r,j) \cdot y(r,j)$
- Alice can send $x(r,1) \ldots x(r, n^{1/2})$ to Bob
- Error probability is at most $2n^{1/2}/n$

Merlin Arthur Communication

- Results
  - QMA(DISJ)=$\Omega(n^{1/3})$
    - Q(DISJ)=$O(n^{1/2})$, MA(DISJ)=$O(n^{1/2})$ [AW08]
    - Means: co-NP vs QMA does not algebrize
  - There is a function f such that
    - AM(f)=O(log n), AM(¬f) =O(log n),
    - PP(f)=$\Omega(n^{1/3})$
    - Hence QMA(f) also large
    - Means:
      - The rectangle bound cannot be applied to AM
      - AM can be exponentially "better" than QMA
      - QMA versus AM does not algebrize

The Problem of Rounds

- Nondeterministic Communication needs only one round
  - Alice can guess the whole conversation and send it to Bob who checks his part
  - A prover can provide the whole conversation, Alice and Bob check their parts
- ‚Realistic' modes of communication usually require round:
  - Deterministic
  - Bounded error randomized
  - Bounded error quantum

The Problem of Rounds

- An example:
  - $Ix(x,i)=x_i$
  - Alice holds x, Bob holds i
  - When Alice sends the message this is hard!
  - When Bob sends the message this is easy!
  - A prover can simply provide i

The Problem of Rounds

- What about proof system modes?
  - Arthur Merlin does not need rounds
    - AM protocols are probability distributions on nondeterministic protocols
  - What about MA and QMA?
- Interestingtingly, QMA protocols with 1 round are at most polynomially worse than those with many rounds [RS04]
  - Parallelization of the rounds with help of a quantum proof

Rounds in MA

- Theorem: There is a function MajIx, such that
  - There is a randomized protocol in which Bob sends 1 message of length O(log n)
  - For any MA protocol, when Alice sends the message the communication is $\Omega(n^{1/2})$
- Hence 1-way communication is not optimal for MA protocols
- Same result holds for QCMA protocols
  - [RS04] results truly needs quantum proofs
  - The fact that one can boost MA/QCMA one-way protocols without repeating the proof seems to be essential

Proof Ideas

QMA Lower Bounds Approach

- Proving MA/QMA lower bounds relies on the following approach:
  - If the proof has length a and the communication is c then reduce the error to $1/2^{10a}$
    - Proof length still a, communciation now O(ac)
  - This is easy for MA, but needs a special technique [MW04] for quantum
  - Now remove the proof (replace by totally mixed state)
  - Acceptance properties:
    - 1-inputs accepted with prob. $(1-1/2^{10a})/2^a$
    - 0-inputs accepted with prob. $1/2^{10a}$
    - This is still a large gap!
    - Analyze protocols with such a gap

QMA Lower Bound

- Two different proof:
  - Based on Sherstov's pattern matrix and a new method, one-sided smooth discrepancy
    - LP based general method for QMA
  - Using a result by Razborov
- Fact:
  - Given: a c-qubit protocol for a function f(x, y) with acceptance probabilities p(x,y)
  - Define p(i)=Prob(x,y with $|x \cap y|=i$ are accepted)
    - For DISJ this should approximate the NOR function
  - Then there is a degree O(c) polynomial q(i) that is $2^{-\Omega(c)}$-close to p(i)

QMA Lower Bound

- Hence we get a polynomial q(i) with the following properties:
  - $q(0) \geq 2^{-a}$
  - $q(1), \ldots, q(n) \leq 2^{-10a}$
  - Degree is O(ac)
- We can rescale the polynomial such that
  - $q(0)=1$
  - $q(1), \ldots, q(n) \leq 2^{-9a}$
  - Degree is O(ac)
- [Buhrman et al . 99] show the degree must be $(an)^{1/2}$
- Hence $ac \geq (an)^{1/2}$ and so $c \geq n^{1/3}$

QMA Lower Bounds

- The same approach shows that $(\log \text{disc})^{1/2}$ gives lower bounds for QMA protocols
- Theorem: $QMA(IP_2) \geq \Omega(n^{1/2})$
- There is also a taylor-made lower bound method:
  - one-sided smooth discrepancy
- $MA(IP)=O(n^{1/2} \log n)$
  - So the protocol for IP cannot be improved much
- But what about QMA(DISJ)?
  - $MA(DISJ)=O(n^{1/2} \log n)$
  - $Q(DISJ)=O(n^{1/2})$
  - combination of both better??

AM versus PP, QMA, MA

- Vereshchagin [92] gives a query problem that has lower AM complexity, but large PP complexity
- We do the same for communication
- Hence the problem of derandomizing AM can only be resolved by nonalgebrizing techniques
- Vereshchagin's function:
  - Defined on Boolean matrices M
  - f(M)=1 if for all i there is a j such that M(i,j)=1
  - f(M)=0 if for at least half of the i for all j M(i,j)=0

The Communication Problem

- Sherstov '08 gives a way to turn Boolean functions into communication problems: pattern matrices
- Essentially Alice receives an $n \times 2$ input matrix A
- Bob receives n bits $b_1,\ldots,b_n$
- The output is $f(A[1,b_1],\ldots,A[n, b_n])$

- We use the pattern matrix problem for Vereshchagin's function
- Function PAppMP

AM versus PP

- Clearly $AM(PAppMP)=O(\log n)$
- The pattern matrix method allows to „transfer“ discrepancy bounds from the query model to the communication model
- This means that $\log disc(PAppMP)=\Omega(N^{1/3})$
- Implies that $QMA(PAppMP)=\Omega(N^{1/6})$

Implications

- Open Problem in Communication Complexity: Separate the Polynomial Hierarchy
  - I.e., prove lower bounds for alternating modes of communication
- Related Question: What is the highest class in the hierarchy we can prove lower bounds for?
  - N(f) : easy
  - MA(f): using the rectangle bound
  - AM(f): not even discrepancy lower bounds work
- AM(f)$\leq$ k means that for all distributions μ on the inputs we can find a cover of the 1-inputs with 2^k rectangles and small error under μ
- However, it may be the case that for some μ each individual rectangle has error exponentially close to ½ or is exponentially small
- Find arguments that employ global features of covers?

Rounds

- QMA, N, AM don‘t need interaction between Alice and Bob for almost optimal protocols.
- Why would MA?
- In particular information theoretic arguments seem to fail since they probably would apply to QMA as well…
- Start with a simple lower bound idea for Index:
- $Ix(x,i)=x_i$

An Index Lower Bound

- We restrict Alice's inputs to Ix to a code with distance ¼ and size $2^{\Omega(n)}$
- Note that for Ix the rows of the communication matrix equal their labels
- Suppose two rows share the same message
- Bob cannot tell them apart, and for ¼ of all i he will make an error for one of them
- So the message has error 1/8 on those 2 rows
- Most codewords should have their own messages!
- $2^{\Omega(n)}$ Messages are needed.

The Function

- Of course $MA(Ix) \leq N(Ix) \leq \log n$

- The function MajIx:
  - Alice has n bits x_i
  - Bob has indices $i_1,\ldots,i_{n^{1/2}}$
  - Promise: Either (1-inputs) all $x(i_j)=1$, or (0-inputs) at most $0.9\ n^{1/2}$ $x(i_j)=1$
- Clearly: If Bob can send a message he can just pick and send some random i_j, communication is log n
- Easy to see that $AM(MajIx)=O(\log n)$ also
- [RS04] implies $QMA(MajIx)=\text{polylog } n$

The Lower Bound

- The QMA bound shows that the intuition „The proof must contain a lot of information about Bob‘s input“ is misleading

- Approach: Assume MA(MajIx)$\leq \gamma\, n^{1/2}$
- First we improve the error to $1/2^{10n^{1/2}}$
  - Repeat the protocol
  - The classical proof does not have to be repeated
  - Note that [MW04] boosting would introduced rounds
- Restrict Alice‘s inputs to codewords
- Fix a „large“ proof

The Lower Bound

- We are left with a randomized 1-way protocol that has the following properties:
  - A set of 1-inputs of size $2^{-\gamma\, n^{1/2}}$ are accepted with probability almost 1
  - All 0-inputs are accepted with probability $½^{-10n^{1/2}}$
  - Communication is $\gamma' n$
- Fix the remaining randomness
- Now a small set of 0-inputs is accepted, much smaller than the set of accepted 1-inputs
- Argue that a message that contains 2 codewords will have large error

Conclusions

- We show the first lower bounds for QMA communication
- Show that AM is exponentially more powerful than QMA, MA, and even PP
  - No lower bound method that applies properties of individual rectangles only (size, error) can touch AM
  - Derandomizing AM does not algebrize
- Show that MA, and QCMA protocols need interaction between Alice and Bob, while N, QMA, AM protocols do not

Open Problems

- Separate AM and MA for a total function (candidates ??)
- Show rounds for MA for a total function
- What is the right bound for QMA(DISJ)
  - Can the MA and the quantum protocol be combined?
- Tight multiplarty (number-in hand) lower bounds for MA(DISJ)
  - Applications for streaming with a helper/cloud computing
  - can improve AMS99 by a factor of k already
- Lower bounds for AM(f) for any function?
- Is $MA(f) \cdot MA(\neg f)$ an upper bound for R(f) for total Boolean f?