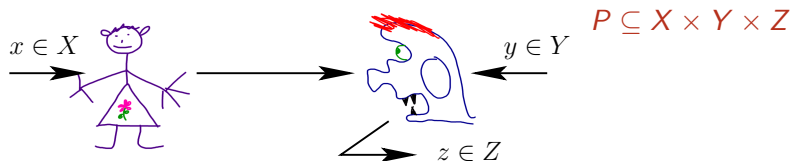


On the Role of Shared Entanglement

Dmitry Gavinsky

University of Calgary

Communication Complexity: the One-Way Model (R^1)



One-Way Message Passing:

- ▶ Alice receives x and Bob receives y ;
- ▶ Alice sends a message to Bob;
- ▶ Bob produces an answer (based on the message and y).

Communication Complexity: the One-Way Model (R^1)



One-Way Message Passing:

- ▶ Alice receives x and Bob receives y ;
- ▶ Alice sends a message to Bob;
- ▶ Bob produces an answer (based on the message and y).

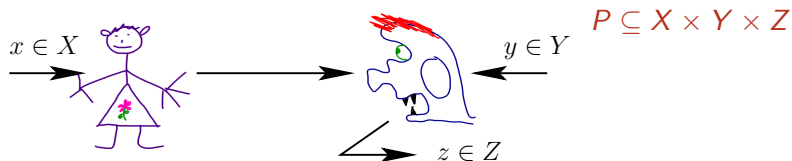
Communication Complexity: the One-Way Model (R^1)



One-Way Message Passing:

- ▶ Alice receives x and Bob receives y ;
- ▶ Alice sends a message to Bob;
- ▶ Bob produces an answer (based on the message and y).

Communication Complexity: the One-Way Model (R^1)



One-Way Message Passing:

- ▶ Alice receives x and Bob receives y ;
- ▶ Alice sends a message to Bob;
- ▶ Bob produces an answer (based on the message and y).

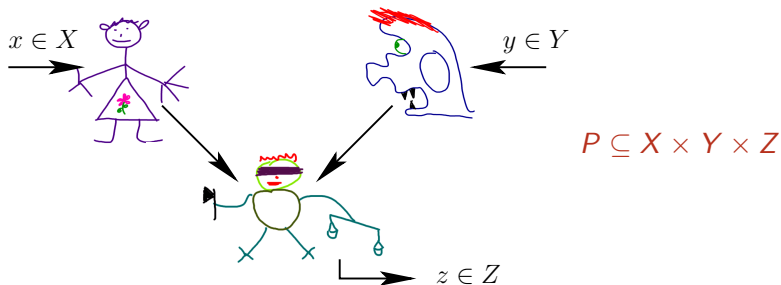
Communication Complexity: the One-Way Model (R^1)



One-Way Message Passing:

- ▶ Alice receives x and Bob receives y ;
- ▶ Alice sends a message to Bob;
- ▶ Bob produces an answer (based on the message and y).

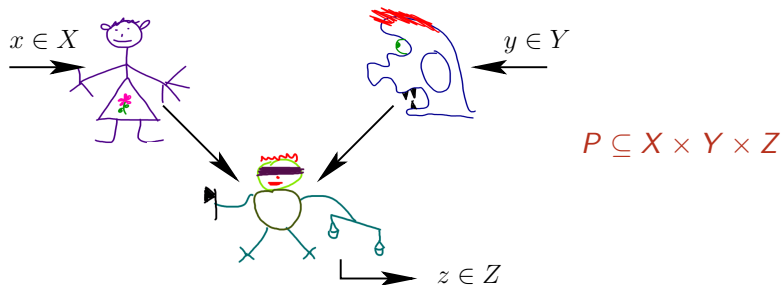
Communication complexity: the SMP model (R^{\parallel})



Simultaneous Message Passing:

- ▶ Alice receives x and sends a message to the referee;
- ▶ (at the same time) Bob receives y and sends a message to the referee;
- ▶ the referee reads the messages and produces an answer.

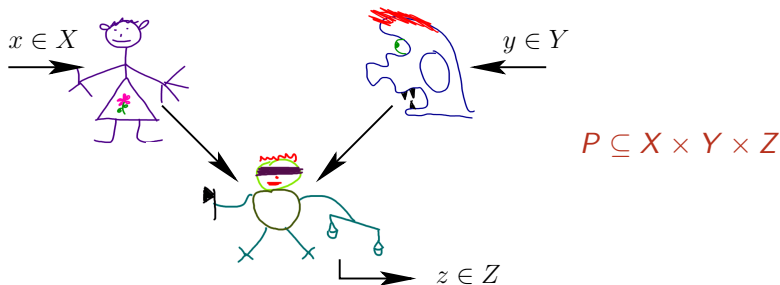
Communication complexity: the SMP model (R^{\parallel})



Simultaneous Message Passing:

- ▶ Alice receives x and sends a message to the referee;
- ▶ (at the same time) Bob receives y and sends a message to the referee;
- ▶ the referee reads the messages and produces an answer.

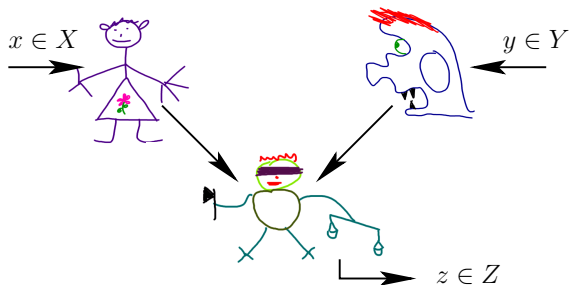
Communication complexity: the SMP model (R^{\parallel})



Simultaneous Message Passing:

- ▶ Alice receives x and sends a message to the referee;
- ▶ (at the same time) Bob receives y and sends a message to the referee;
- ▶ the referee reads the messages and produces an answer.

Communication complexity: the SMP model (R^{\parallel})



$$P \subseteq X \times Y \times Z$$

Is $(x, y, z) \in P$?

Simultaneous Message Passing:

- ▶ Alice receives x and sends a message to the referee;
- ▶ (at the same time) Bob receives y and sends a message to the referee;
- ▶ the referee reads the messages and produces an answer.

Shared Entanglement

- ▶ We may allow Alice and Bob to share *entangled qubits*, denote the corresponding models by $R^{\perp,ent}$, $R^{\parallel,ent}$.

Shared Randomness vs. Shared Entanglement

- ▶ The “classical analogue” of shared entanglement is **shared randomness**.
- ▶ Newman has shown in 1991 that no communication problem requires more than $O(\log n)$ shared random bits.
- ▶ *What about shared entanglement?*

Shared Entanglement

- ▶ We may allow Alice and Bob to share *entangled qubits*, denote the corresponding models by $R^{\perp,ent}$, $R^{\parallel,ent}$.

Shared Randomness vs. Shared Entanglement

- ▶ The “classical analogue” of shared entanglement is **shared randomness**.
- ▶ Newman has shown in 1991 that **no communication problem requires more than $O(\log n)$ shared random bits**.
- ▶ *What about shared entanglement?*

Shared Entanglement

- ▶ We may allow Alice and Bob to share *entangled qubits*, denote the corresponding models by $R^{\perp,ent}$, $R^{\parallel,ent}$.

Shared Randomness vs. Shared Entanglement

- ▶ The “classical analogue” of shared entanglement is **shared randomness**.
- ▶ Newman has shown in 1991 that **no communication problem requires more than $O(\log n)$ shared random bits**.
- ▶ *What about shared entanglement?*

Shared Entanglement

- ▶ We may allow Alice and Bob to share *entangled qubits*, denote the corresponding models by $R^{\perp,ent}$, $R^{\parallel,ent}$.

Shared Randomness vs. Shared Entanglement

- ▶ The “classical analogue” of shared entanglement is **shared randomness**.
- ▶ Newman has shown in 1991 that **no communication problem requires more than $O(\log n)$ shared random bits**.
- ▶ *What about shared entanglement?*

Shared Entanglement

- ▶ We may allow Alice and Bob to share *entangled qubits*, denote the corresponding models by $R^{\perp,ent}$, $R^{\parallel,ent}$.

Shared Randomness vs. Shared Entanglement

- ▶ The “classical analogue” of shared entanglement is **shared randomness**.
- ▶ Newman has shown in 1991 that **no communication problem requires more than $O(\log n)$ shared random bits**.
- ▶ *What about shared entanglement?*

Our Result: *the “entanglement analogue” of Newman’s theorem does not hold*

- ▶ *Low-end:* For any $t > 2$, there exists a problem which can be solved in $O(\log^t n)$ communication using $\log^t n$ qubits of entanglement in the SMP model.
The same problem requires $\Omega(\sqrt{n})$ communication if shared entanglement is limited to $o(\log^{t-2} n)$, even in the model of one-way communication.
- ▶ *High-end:* For any $\varepsilon > 0$, there exists a problem which can be solved in $O(n^{1-\varepsilon} \log n)$ communication using $n^{1-\varepsilon} \log n$ qubits of entanglement in the SMP model.
The same problem requires $\Omega(n^{1-\varepsilon/2} / \log n)$ communication if shared entanglement is limited to $o(n^{1-\varepsilon} / \log n)$, even in the model of one-way communication.

Our Result: *the “entanglement analogue” of Newman’s theorem does not hold*

- ▶ *Low-end:* For any $t > 2$, there exists a problem which can be solved in $O(\log^t n)$ communication using $\log^t n$ qubits of entanglement in the SMP model.
The same problem requires $\Omega(\sqrt{n})$ communication if shared entanglement is limited to $o(\log^{t-2} n)$, even in the model of one-way communication.
- ▶ *High-end:* For any $\varepsilon > 0$, there exists a problem which can be solved in $O(n^{1-\varepsilon} \log n)$ communication using $n^{1-\varepsilon} \log n$ qubits of entanglement in the SMP model.
The same problem requires $\Omega(n^{1-\varepsilon/2} / \log n)$ communication if shared entanglement is limited to $o(n^{1-\varepsilon} / \log n)$, even in the model of one-way communication.

Communication problem

- ▶ The following problem is defined and analyzed in BJK'04.

$$HMP_m$$

- Alice gets $x \in \{0, 1\}^m$;
- Bob gets y , a perfect matching on m nodes.
- **Output:** Any $(i, j, x_i \oplus x_j)$, s.t. $(i, j) \in y$.

- ▶ Define k -wise direct product:

$$HMP_m^{(k)}$$

$HMP_m^{(k)} = \{((x_1, \dots, x_k), (y_1, \dots, y_k), (z_1, \dots, z_k))\}$, where for all $i \in \{1, \dots, k\}$ it holds that $(x_i, y_i, z_i) \in HMP_m$.

Communication problem

- ▶ The following problem is defined and analyzed in BJK'04.

$$HMP_m$$

- Alice gets $x \in \{0, 1\}^m$;
- Bob gets y , a perfect matching on m nodes.
- **Output:** Any $(i, j, x_i \oplus x_j)$, s.t. $(i, j) \in y$.

- ▶ Define k -wise direct product:

$$HMP_m^{(k)}$$

$HMP_m^{(k)} = \{((x_1, \dots, x_k), (y_1, \dots, y_k), (z_1, \dots, z_k))\}$, where for all $i \in \{1, \dots, k\}$ it holds that $(x_i, y_i, z_i) \in HMP_m$.

Our proof

- ▶ The communication cost of HMP_m is $O(\log m)$ with entanglement but $\Omega(\sqrt{m})$ without it (BJK'04).
- ▶ We prove a *strong direct product theorem* for R^1 and conclude that any R^1 -protocol of cost $o\left(\frac{k\sqrt{m}}{\log m}\right)$ solves $HMP_m^{(k)}$ with probability at most $1/2^{\Omega\left(\frac{k}{\log m}\right)}$.
- ▶ We show that *adding prior entanglement over e qubits can increase the success probability at most by a multiplicative factor of 2^e* .
- ▶ Therefore the communication cost of solving $HMP_m^{(k)}$ using $o\left(\frac{k}{\log m}\right)$ qubits of entanglement is $\Omega\left(\frac{k\sqrt{m}}{\log m}\right)$.
- ▶ Our entanglement vs. communication tradeoffs follow.

Our proof

- ▶ The communication cost of HMP_m is $O(\log m)$ with entanglement but $\Omega(\sqrt{m})$ without it (BJK'04).
- ▶ We prove a *strong direct product theorem* for R^1 and conclude that any R^1 -protocol of cost $o\left(\frac{k\sqrt{m}}{\log m}\right)$ solves $HMP_m^{(k)}$ with probability at most $1/2^{\Omega\left(\frac{k}{\log m}\right)}$.
- ▶ We show that *adding prior entanglement over e qubits can increase the success probability at most by a multiplicative factor of 2^e* .
- ▶ Therefore the communication cost of solving $HMP_m^{(k)}$ using $o\left(\frac{k}{\log m}\right)$ qubits of entanglement is $\Omega\left(\frac{k\sqrt{m}}{\log m}\right)$.
- ▶ Our entanglement vs. communication tradeoffs follow.

Our proof

- ▶ The communication cost of HMP_m is $O(\log m)$ with entanglement but $\Omega(\sqrt{m})$ without it (BJK'04).
- ▶ We prove a *strong direct product theorem* for R^1 and conclude that any R^1 -protocol of cost $o\left(\frac{k\sqrt{m}}{\log m}\right)$ solves $HMP_m^{(k)}$ with probability at most $1/2^{\Omega\left(\frac{k}{\log m}\right)}$.
- ▶ We show that *adding prior entanglement over e qubits can increase the success probability at most by a multiplicative factor of 2^e* .
- ▶ Therefore the communication cost of solving $HMP_m^{(k)}$ using $o\left(\frac{k}{\log m}\right)$ qubits of entanglement is $\Omega\left(\frac{k\sqrt{m}}{\log m}\right)$.
- ▶ Our entanglement vs. communication tradeoffs follow.

Our proof

- ▶ The communication cost of HMP_m is $O(\log m)$ with entanglement but $\Omega(\sqrt{m})$ without it (BJK'04).
- ▶ We prove a *strong direct product theorem* for R^1 and conclude that any R^1 -protocol of cost $o\left(\frac{k\sqrt{m}}{\log m}\right)$ solves $HMP_m^{(k)}$ with probability at most $1/2^{\Omega\left(\frac{k}{\log m}\right)}$.
- ▶ We show that *adding prior entanglement over e qubits can increase the success probability at most by a multiplicative factor of 2^e* .
- ▶ Therefore the communication cost of solving $HMP_m^{(k)}$ using $o\left(\frac{k}{\log m}\right)$ qubits of entanglement is $\Omega\left(\frac{k\sqrt{m}}{\log m}\right)$.
- ▶ Our entanglement vs. communication tradeoffs follow.

Our proof

- ▶ The communication cost of HMP_m is $O(\log m)$ with entanglement but $\Omega(\sqrt{m})$ without it (BJK'04).
- ▶ We prove a *strong direct product theorem* for R^1 and conclude that any R^1 -protocol of cost $o\left(\frac{k\sqrt{m}}{\log m}\right)$ solves $HMP_m^{(k)}$ with probability at most $1/2^{\Omega\left(\frac{k}{\log m}\right)}$.
- ▶ We show that *adding prior entanglement over e qubits can increase the success probability at most by a multiplicative factor of 2^e* .
- ▶ Therefore the communication cost of solving $HMP_m^{(k)}$ using $o\left(\frac{k}{\log m}\right)$ qubits of entanglement is $\Omega\left(\frac{k\sqrt{m}}{\log m}\right)$.
- ▶ Our entanglement vs. communication tradeoffs follow.

Preliminaries

- ▶ Assume that a communication problem P over $X \times Y = \{0, 1\}^m \times \{0, 1\}^m$ is solvable by a protocol of cost $c(m)$.
- ▶ There exists $A \subseteq X$ of size almost $2^{m-c(m)}$, such that it is possible to solve P for most of $x \in A$ and $y \in Y$ by giving an answer **which depends on y only**.
- ▶ If there exists $z(y)$, such that $\Pr_{x \in A} [(x, y, z(y)) \in P] \geq p_0$, we say that y is **p_0 -successful over A w.r.t. P** .

Preliminaries

- ▶ Assume that a communication problem P over $X \times Y = \{0, 1\}^m \times \{0, 1\}^m$ is solvable by a protocol of cost $c(m)$.
- ▶ There exists $A \subseteq X$ of size almost $2^{m-c(m)}$, such that it is possible to solve P for most of $x \in A$ and $y \in Y$ by giving an answer **which depends on y only**.
- ▶ If there exists $z(y)$, such that $\Pr_{x \in A} [(x, y, z(y)) \in P] \geq p_0$, we say that y is p_0 -successful over A w.r.t. P .

Preliminaries

- ▶ Assume that a communication problem P over $X \times Y = \{0, 1\}^m \times \{0, 1\}^m$ is solvable by a protocol of cost $c(m)$.
- ▶ There exists $A \subseteq X$ of size almost $2^{m-c(m)}$, such that it is possible to solve P for most of $x \in A$ and $y \in Y$ by giving an answer **which depends on y only**.
- ▶ If there exists $z(y)$, such that $\Pr_{x \in A} [(x, y, z(y)) \in P] \geq p_0$, we say that **y is p_0 -successful over A w.r.t. P** .

Direct product theorem

- ▶ Assume that for any set $A \subseteq X$ which is sufficiently large, a random $y_0 \in Y$ is $2/3$ -successful over A w.r.t. P with probability **at most** $1/2^{10}$.

Moreover, we require that a random $z_0 \in Z$ satisfy that $\Pr_{x \in A} [(x, y_0, z_0) \in P] \geq 2/3$ with probability at most $\frac{1}{|Z| \cdot 2^{10}}$.

- ▶ We prove a **quantifier-free version** of the strong direct product theorem. Informally, the theorem gives an upper bound of $\left(\frac{\delta}{|Z|}\right)^k$ (for sufficiently small δ) on the probability that a **random $z \in Z^k$ is a valid answer to P^k** .
- ▶ The probability that **there exists a valid answer** is at most $|Z|^k$ times the probability that a random answer is valid, which is equal to δ^k .

Direct product theorem

- ▶ Assume that for any set $A \subseteq X$ which is sufficiently large, a random $y_0 \in Y$ is $2/3$ -successful over A w.r.t. P with probability **at most** $1/2^{10}$.

Moreover, we require that a random $z_0 \in Z$ satisfy that $\Pr_{x \in A} [(x, y_0, z_0) \in P] \geq 2/3$ with probability at most $\frac{1}{|Z| \cdot 2^{10}}$.

- ▶ We prove a **quantifier-free version** of the strong direct product theorem. Informally, the theorem gives an upper bound of $\left(\frac{\delta}{|Z|}\right)^k$ (for sufficiently small δ) on the probability that a **random $z \in Z^k$ is a valid answer to P^k** .
- ▶ The probability that **there exists a valid answer** is at most $|Z|^k$ times the probability that **a random answer is valid**, which is equal to δ^k .

Direct product theorem

- ▶ Assume that for any set $A \subseteq X$ which is sufficiently large, a random $y_0 \in Y$ is $2/3$ -successful over A w.r.t. P with probability **at most** $1/2^{10}$.

Moreover, we require that a random $z_0 \in Z$ satisfy that $\Pr_{x \in A} [(x, y_0, z_0) \in P] \geq 2/3$ with probability at most $\frac{1}{|Z| \cdot 2^{10}}$.

- ▶ We prove a **quantifier-free version** of the strong direct product theorem. Informally, the theorem gives an upper bound of $\left(\frac{\delta}{|Z|}\right)^k$ (for sufficiently small δ) on the probability that a **random $z \in Z^k$ is a valid answer to P^k** .
- ▶ The probability that **there exists a valid answer** is at most $|Z|^k$ times the probability that **a random answer is valid**, which is equal to δ^k .

Direct product theorem

- ▶ Assume that for any set $A \subseteq X$ which is sufficiently large, a random $y_0 \in Y$ is $2/3$ -successful over A w.r.t. P with probability **at most** $1/2^{10}$.

Moreover, we require that a random $z_0 \in Z$ satisfy that $\Pr_{x \in A} [(x, y_0, z_0) \in P] \geq 2/3$ with probability at most $\frac{1}{|Z| \cdot 2^{10}}$.

- ▶ We prove a **quantifier-free version** of the strong direct product theorem. Informally, the theorem gives an upper bound of $\left(\frac{\delta}{|Z|}\right)^k$ (for sufficiently small δ) on the probability that a **random** $z \in Z^k$ is a valid answer to P^k .
- ▶ The probability that **there exists a valid answer** is at most $|Z|^k$ times the probability that **a random answer is valid**, which is equal to δ^k .

Conclusions

- ▶ $HMP_m^{(k)}$ can be solved *exactly in the SMP model* using $k \log(m)$ EPR pairs by a protocol of cost $O(k \log(m))$.
- ▶ Solving the problem *with an error bounded by a constant in the one-way model*, given only $o\left(\frac{k}{\log m}\right)$ qubits of shared entanglement requires $\Omega\left(\frac{k\sqrt{m}}{\log m}\right)$ bits of communication.
- ▶ Our protocols use *shared EPR pairs*, while the lower bounds apply to *any sort of shared entanglement*.

Conclusions

- ▶ $HMP_m^{(k)}$ can be solved *exactly in the SMP model* using $k \log(m)$ EPR pairs by a protocol of cost $O(k \log(m))$.
- ▶ Solving the problem *with an error bounded by a constant in the one-way model*, given only $o\left(\frac{k}{\log m}\right)$ qubits of shared entanglement requires $\Omega\left(\frac{k\sqrt{m}}{\log m}\right)$ bits of communication.
- ▶ Our protocols use *shared EPR pairs*, while the lower bounds apply to *any sort of shared entanglement*.

Conclusions

- ▶ $HMP_m^{(k)}$ can be solved *exactly in the SMP model* using $k \log(m)$ EPR pairs by a protocol of cost $O(k \log(m))$.
- ▶ Solving the problem *with an error bounded by a constant in the one-way model*, given only $o\left(\frac{k}{\log m}\right)$ qubits of shared entanglement requires $\Omega\left(\frac{k\sqrt{m}}{\log m}\right)$ bits of communication.
- ▶ Our protocols use *shared EPR pairs*, while the lower bounds apply to *any sort of shared entanglement*.

Open problems

- ▶ Can similar results be obtained for a functional communication problem?
- ▶ More communication vs. entanglement trade-offs?

Open problems

- ▶ Can similar results be obtained for a functional communication problem?
- ▶ More communication vs. entanglement trade-offs?

