Quantum Network Coding

Martin Roetteler
NEC Laboratories America
Princeton, NJ

Joint work with:
Hirotada Kobayashi, Francois Le Gall and Harumichi Nishimura

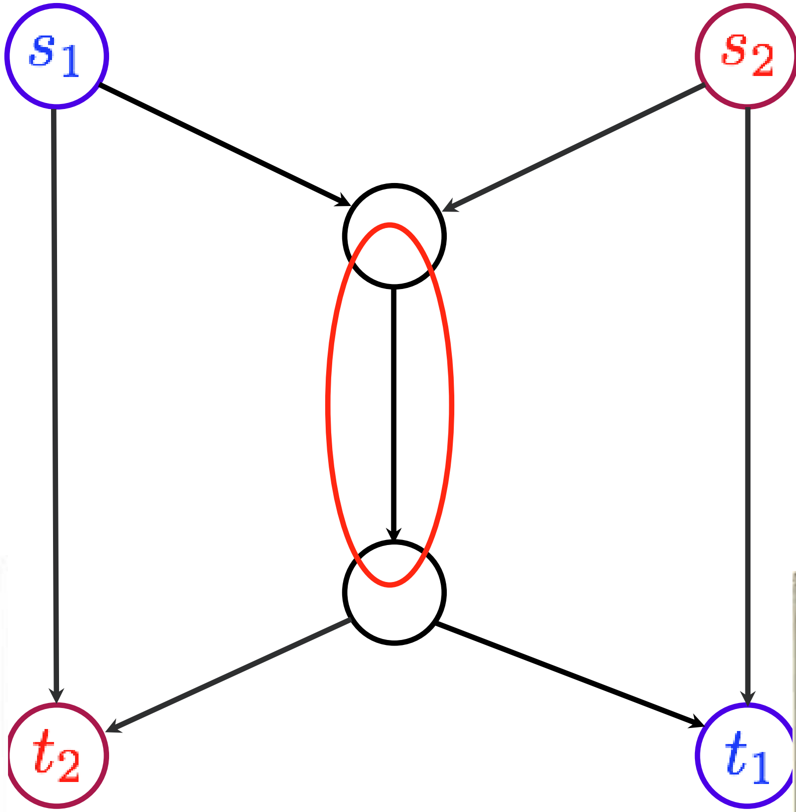
2nd Conference on Quantum Error Correction
University of Southern California
December 8, 2011

Overview

- **Communication in quantum networks**
  - Networks of quantum channels with capacity and topology constraints
  - "Quantum network coding"
    - Achieves perfect state transfer through networks
    - Allows to "switching", i.e., arbitrary permutations from the input qubits to the output qubits
    - Re-uses results from classical network coding

- **Open problems**

Network communication problems



issue: bottleneck, i.e.,
routing cannot be used

[Image credits: “Cool Hand Luke” and “The Big Lebowski”]

Network communication problems

The "Butterfly":

- two sources s_1 and s_2
- two targets t_1 and t_2
- capacity of each edge = 1 bit

Multi-cast problem:

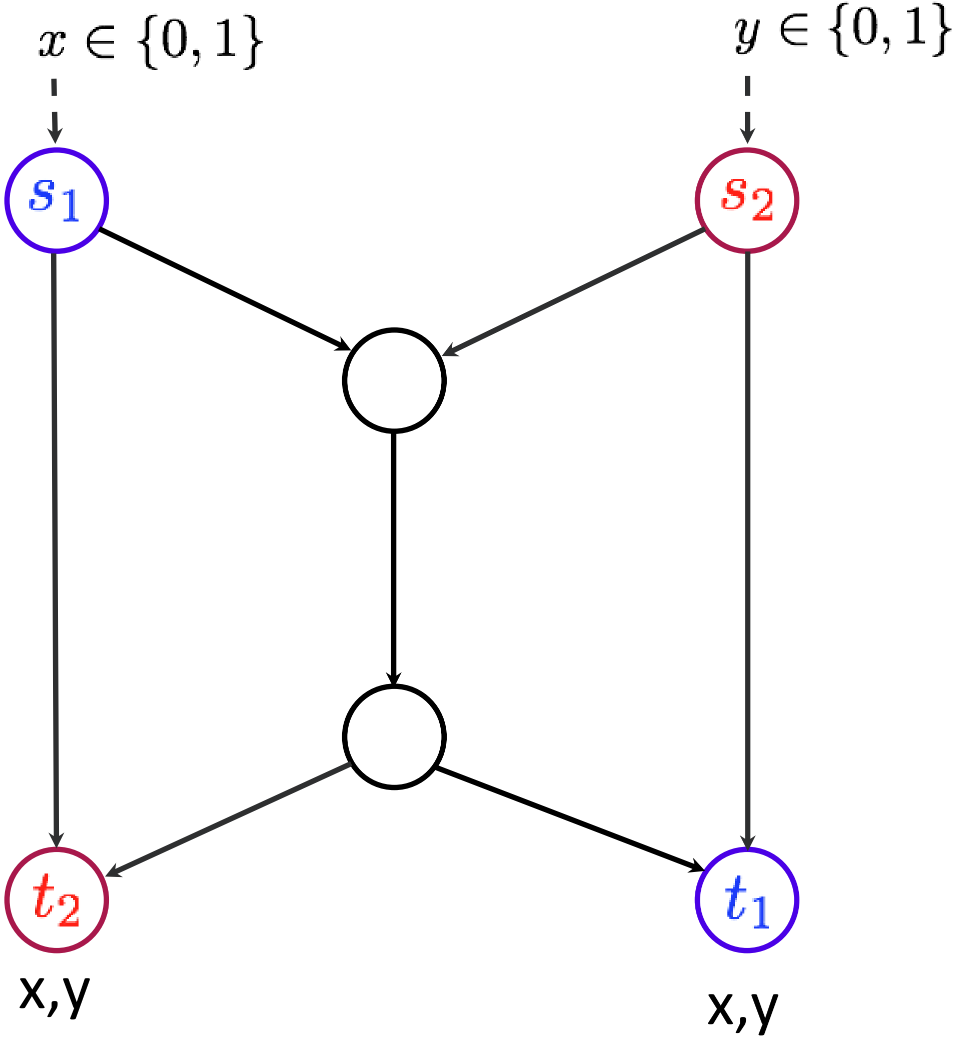
send input x to t_1

send input y to t_2

and

send input x to t_2

send input y to t_1



Classical network coding

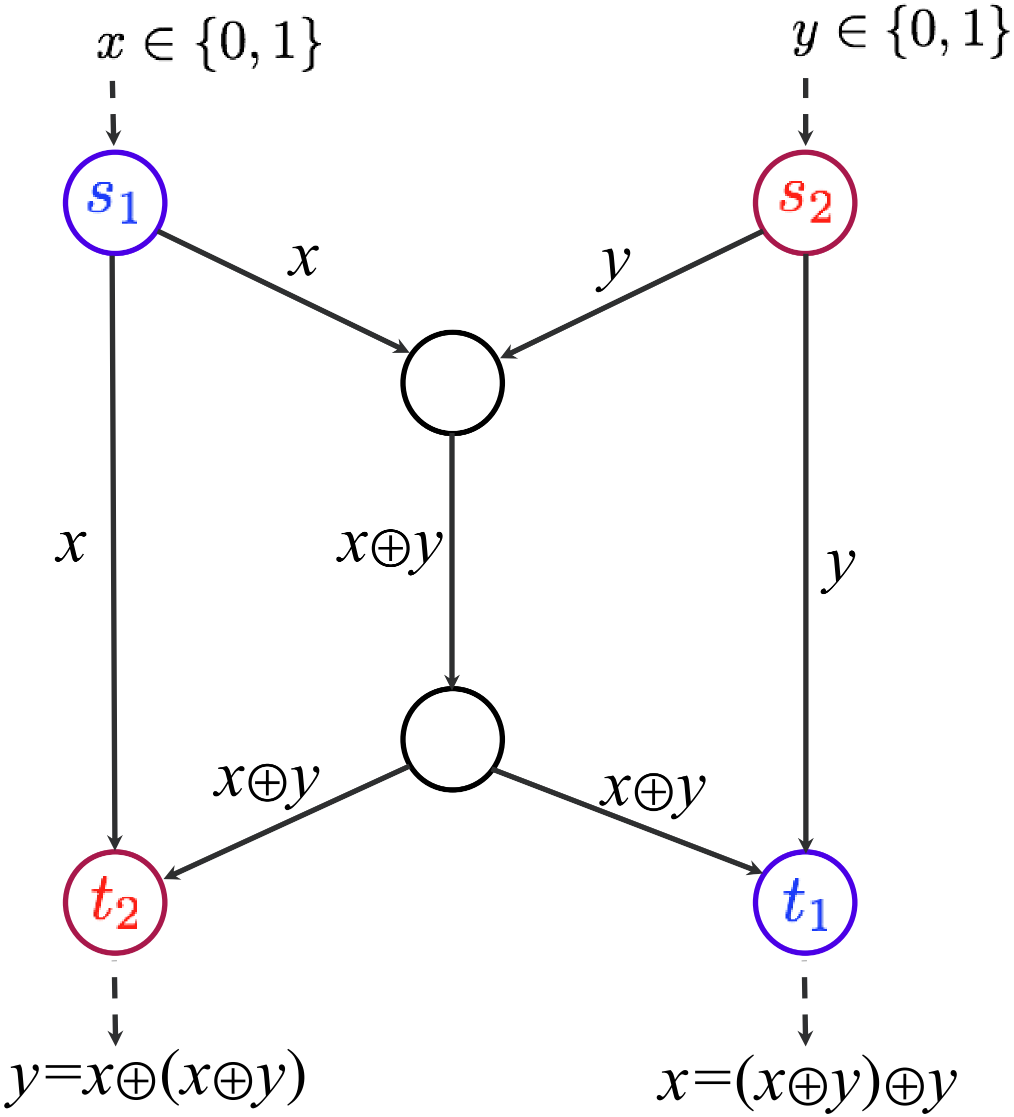
Goal:

send input x to t_1 and t_2

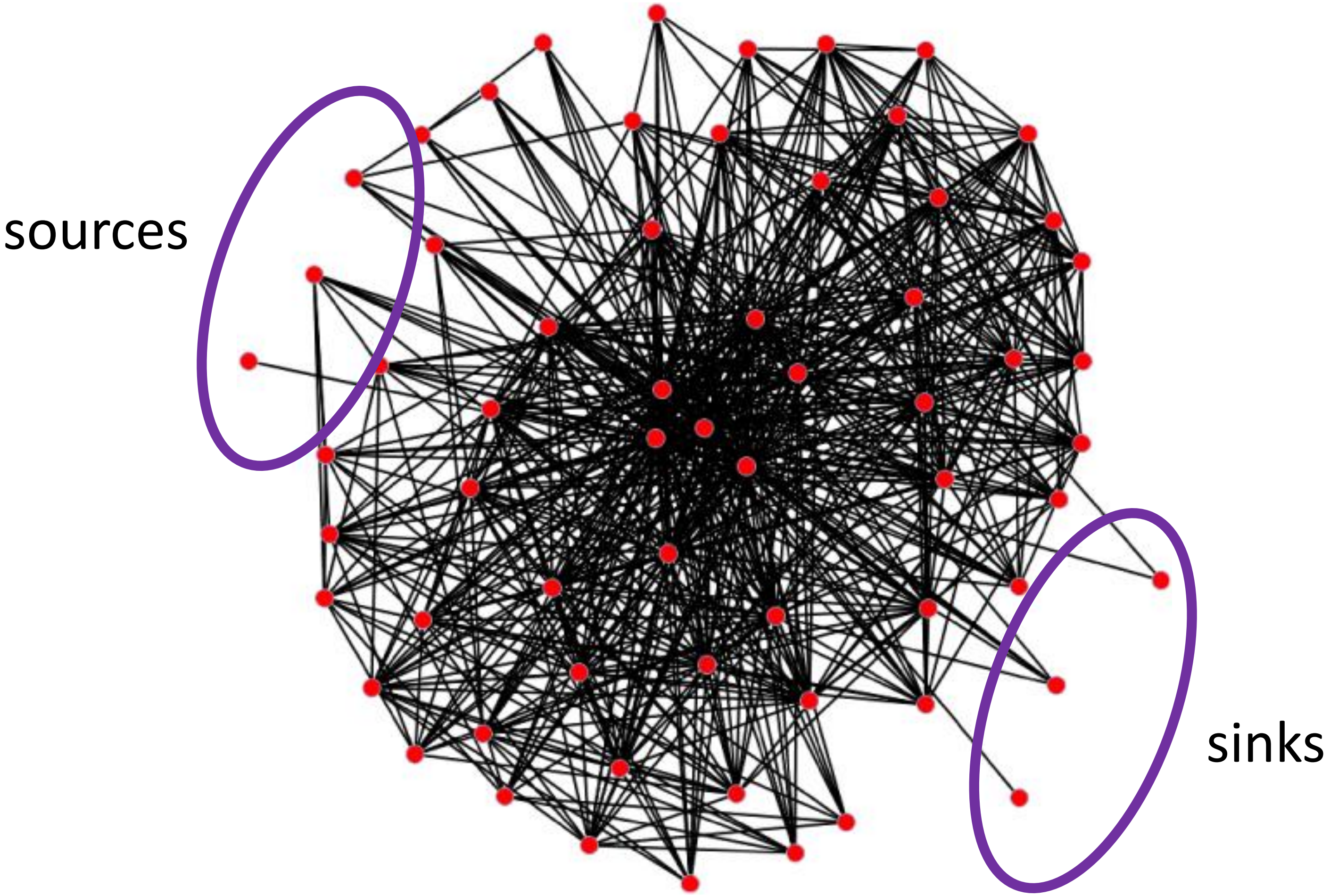
send input y to t_1 and t_2

Solution **[Ahlswede, Cai, Yi, Yeung, 2000]**:

- use “coding” operation at some of the network nodes
- then per time unit one input can be sent to one output.



The general multi-cast problem



Feasibility of the multi-cast problem is characterized by the min-cut / max flow theorem. Moreover, there is a polynomial time algorithm to find a linear network coding scheme for the multi-case problem **[Sanders, Egner, Tolhuizen, SPAA 2003].**

[Image credit: http://cneurocvs.rmki.kfki.hu/igraph/]

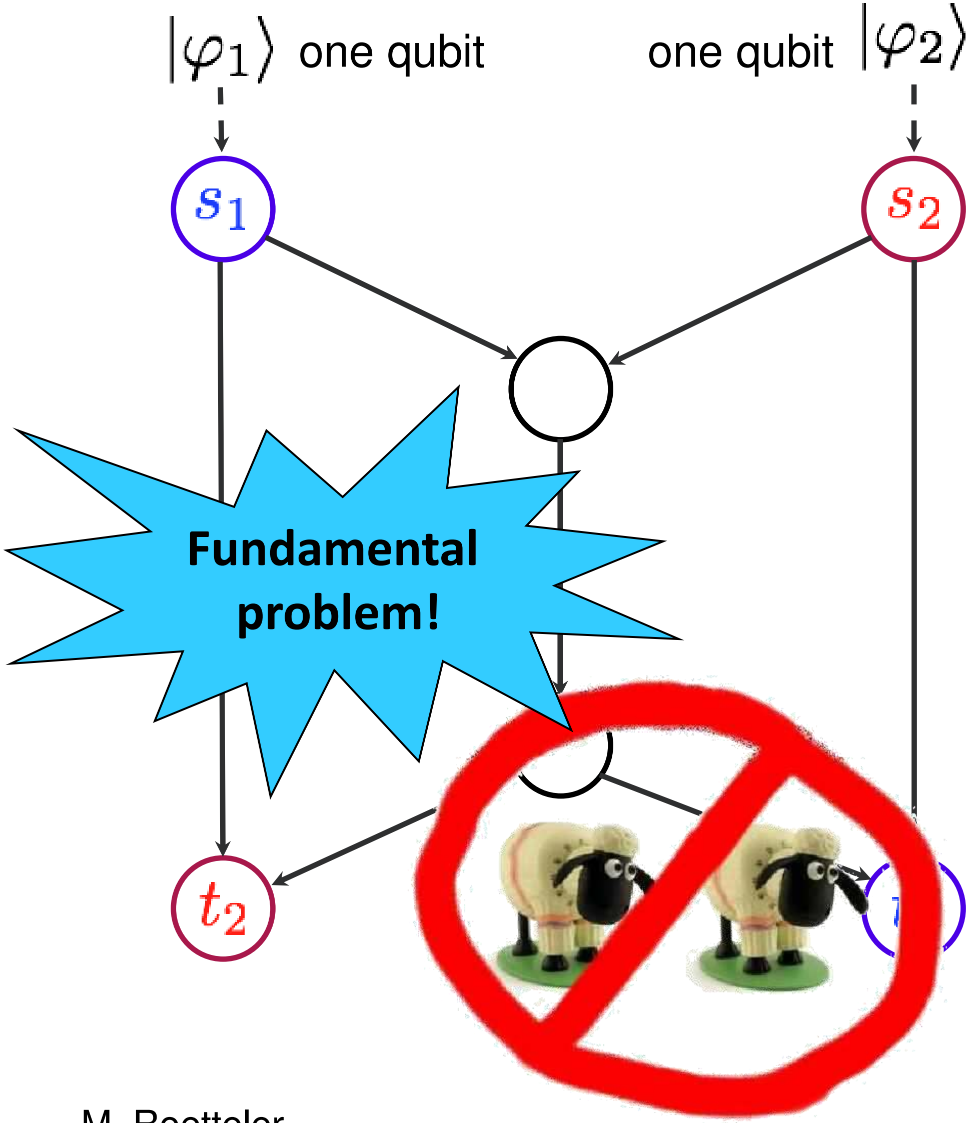
Quantum network coding?

- two sources s_1 and s_2
- two targets t_1 and t_2
- quantum capacity of each edge = 1 qubit, i.e., we assume that we have perfect quantum channels.

Goal:

send input x to t_1 and t_2

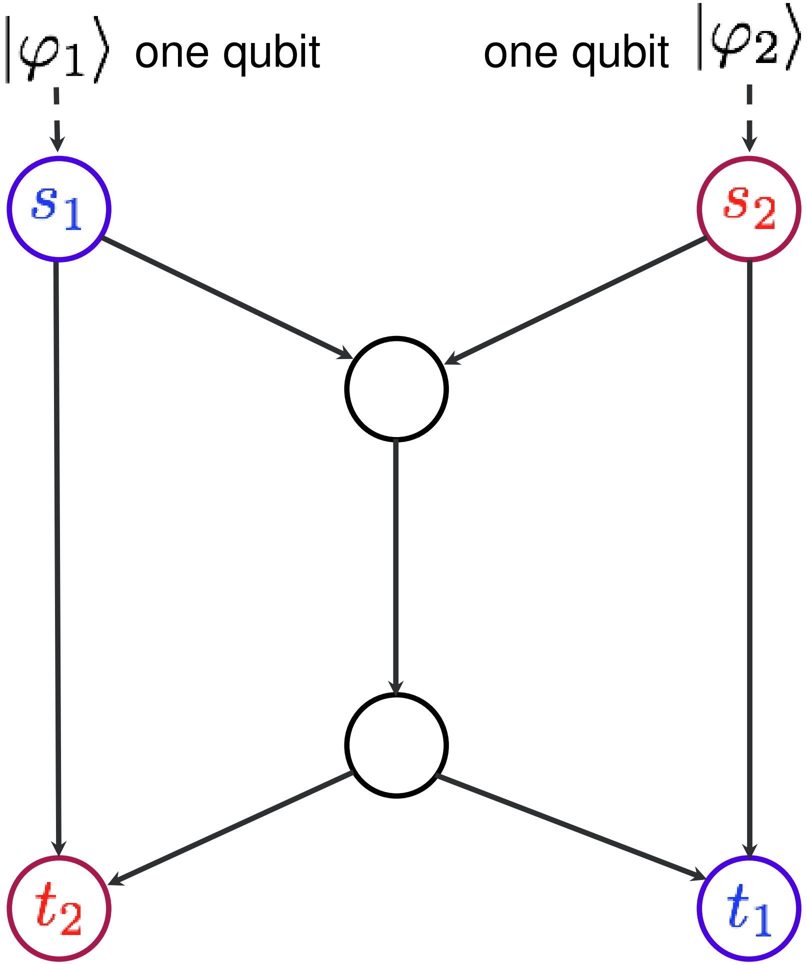
send input y to t_1 and t_2



Fundamental problem!

Quantum network coding?

- two sources s_1 and s_2
- two targets t_1 and t_2
- quantum capacity of each edge = 1 qubit, i.e., we assume that we have perfect quantum channels.

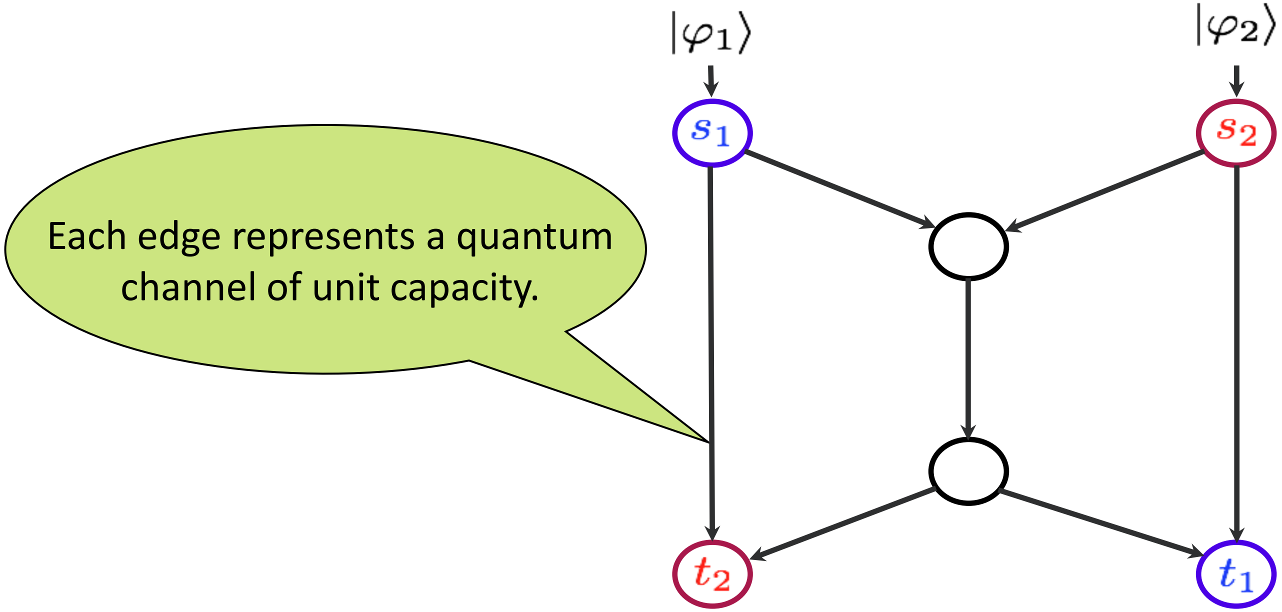


Goal:

send input $|\varphi_1\rangle$ to t_1

send input $|\varphi_2\rangle$ to t_2

Quantum network coding?



Each edge represents a quantum channel of unit capacity.

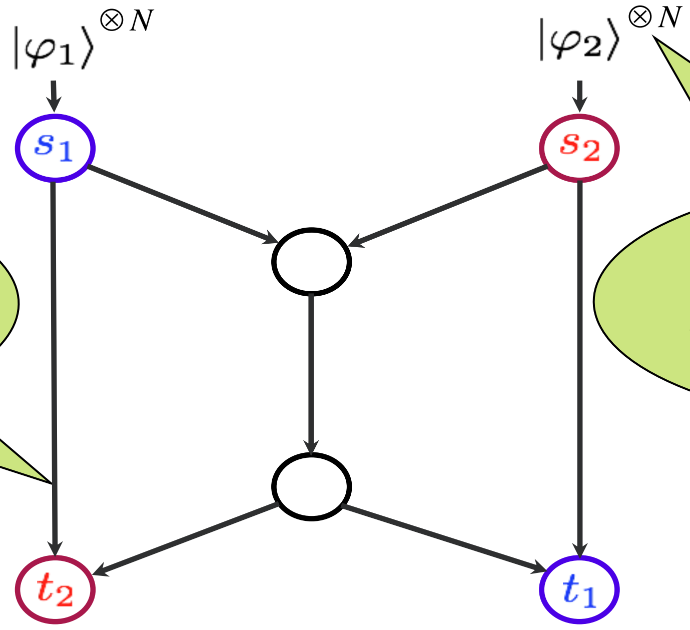
Results: [Hayashi, Iwama, Nishimura, Raymond, Yamashita'07], [Hayashi'07]

- For any protocol, there exists a quantum state $|\psi\rangle$ such that for the output state ρ the upper bound $F(\rho, |\psi\rangle) < 1$ holds.

- There exists quantum protocol with fidelities at nodes t_1 and t_2 that are > ½.

- [Winter, Leung, Oppenheim'06] consider k-pair problem and asymptotically achievable rate. Does not achieve perfect transmission.

Changing the model (first attempt)

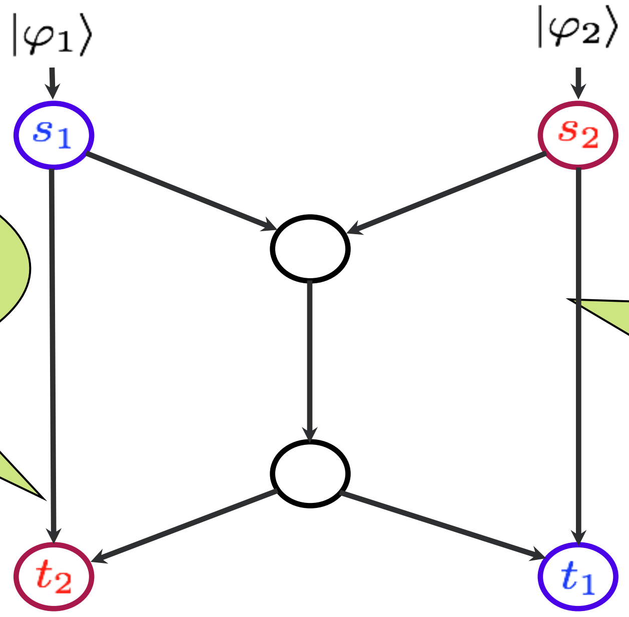

$|\varphi_1\rangle^{\otimes N}$
$|\varphi_2\rangle^{\otimes N}$
s_1
s_2
t_2
t_1

Each edge represents a Quantum channel of log(N+1) capacity.

Assume that we are given several copies of the input states.

Result: [Shi, Soljanin, ISS'06] assume h sources, N receivers, and all the source/receiver min-cuts at least h. Then the input states can be perfectly transmitted through the network, i.e., each receiver gets one copy. This is achieved by performing lossless compression and decompression operations at the network nodes and the fact the input state is in $Sym(H^{\otimes N})$ which is a very low-dimensional subspace.

Quantum network coding



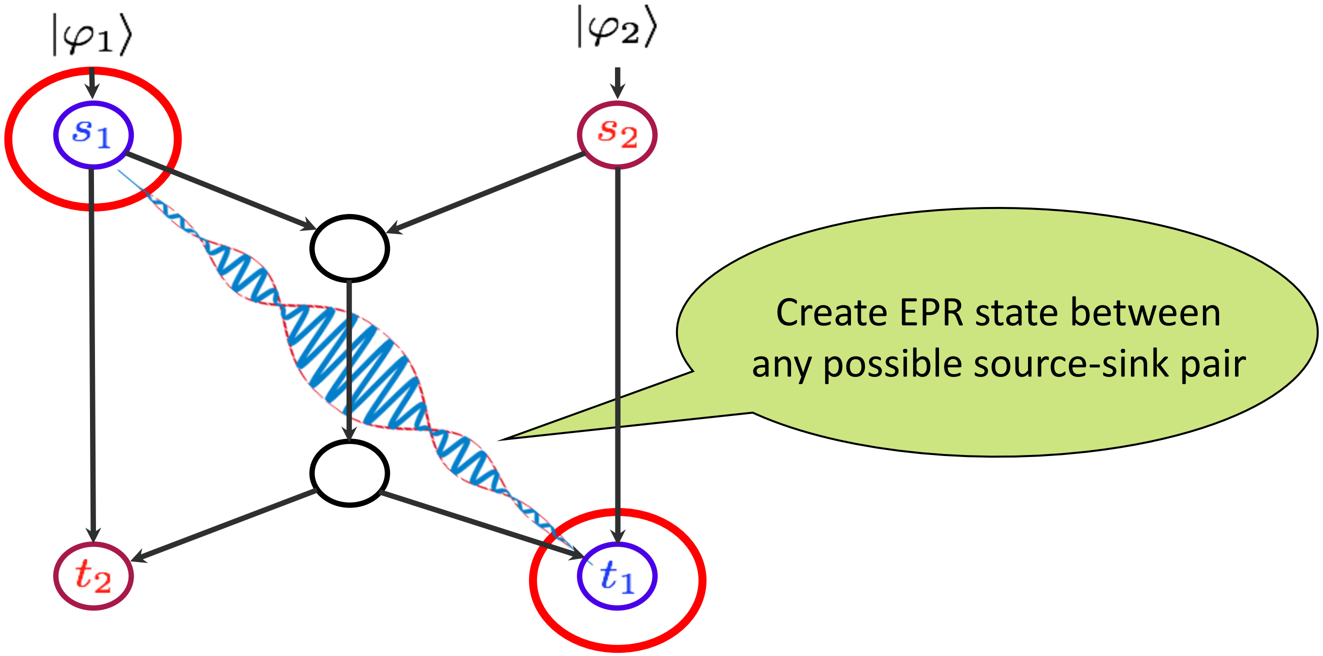
Each edge represents a quantum channel of unit capacity.

But let’s also assume that all classical communication is free!

Result: [Kobayashi, Le Gall, Nishimura, R., ISIT’10] In this model with free classical communication perfect quantum network coding is possible if a classical linear network coding scheme for the multi-cast problem exists.

Result: [Kobayashi, Le Gall, Nishimura, R., ISIT’11] Generalization to the case where a classical (linear or non-linear) network coding scheme for the k-pair problem exists.

General strategy behind the protocol



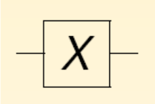
Create EPR state between any possible source-sink pair

Strategy: Use network to generate EPR pairs between sources and sinks. Then use teleportation to transfer the input states through the network.

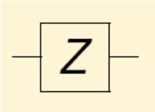
Gates used in the protocol

Clifford gates:

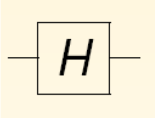
- $\sigma_X := \sum_{x \in \mathbb{F}_2} |x+1\rangle\langle x|$



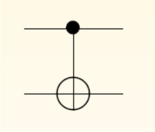
- $\sigma_Z := \sum_{z \in \mathbb{F}_2} (-1)^z |z\rangle\langle z|$



- $\mathsf{H} := \frac{1}{\sqrt{2}} \sum_{x,z \in \mathbb{F}_2} (-1)^{xz} |z\rangle\langle x|$



- $\mathsf{CNOT}^{(1,2)} := \sum_{x,y \in \mathbb{F}_2} |x\rangle_1 |x+y\rangle_2 \langle x|_1 \langle y|_2$



Hadmard basis:

$$|+\rangle = \mathsf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \mathsf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

Canceling phases

Lemma. Partition $\{1, \ldots, n\}$ into two disjoint subsets A and B:

$$|\psi_{A,B}\rangle = \sum_{x \in \mathbb{F}_2^n} \alpha_x |f(x)\rangle |g(x)\rangle,$$

$\alpha_x \in \mathbb{C}$, $f : \mathbb{F}_2^n \to \mathbb{F}_2^{|A|}$, and $g : \mathbb{F}_2^n \to \mathbb{F}_2^{|B|}$. Measuring B in $\{|+\rangle, |-\rangle\}$:

$$|\psi_A\rangle = \sum_{x \in \mathbb{F}_2^n} \alpha_x (-1)^{y_0 \cdot g(x)} |f(x)\rangle,$$

where $y_0 \in \mathbb{F}_2^{|B|}$ is a (in general random) vector.

Lemma. Let $|\psi\rangle$ be a state of the form

$$|\psi\rangle = \sum_{x \in \mathbb{F}_2^n} \alpha_x |x\rangle (-1)^{L(x)},$$

with L known linear function. Then local σ_z can map $|\psi\rangle$ to $\sum_x \alpha_x |x\rangle$.

Idea behind linear case solution

- From classical multicast property, each output can perfectly recover:

$$\sum_{a_1,\ldots,a_{|S|}} \underbrace{|a_1,\ldots,a_{|S|}\rangle}_{S} \underbrace{|a_1,\ldots,a_{|S|}\rangle}_{t_1} \cdots \underbrace{|a_1,\ldots,a_{|S|}\rangle}_{t_{|T|}} \otimes$$
$$|f_1(a_1,\ldots,a_{|S|})\rangle \cdots |f_L(a_1,\ldots,a_{|S|})\rangle,$$

  with $|S|$ qubits at source, $|T| \cdot |S|$ qubits at targets, and rest in network.

- After measuring all internal qubits in the Hadamard basis:

$$\sum_{a_1,\ldots,a_{|S|}} \underbrace{|a_1,\ldots,a_{|S|}\rangle}_{S} \underbrace{|a_1,\ldots,a_{|S|}\rangle}_{t_1} \cdots \underbrace{|a_1,\ldots,a_{|S|}\rangle}_{t_{|T|}} (-1)^{L(a_1,\ldots,a_{|S|})},$$

  where L is a linear map determined by the measurement results.

- Now, using lemma map this to

$$\sum_{a_1,\ldots,a_{|S|}} \underbrace{|a_1,\ldots,a_{|S|}\rangle}_{S} \underbrace{|a_1,\ldots,a_{|S|}\rangle}_{t_1} \cdots \underbrace{|a_1,\ldots,a_{|S|}\rangle}_{t_{|T|}}.$$

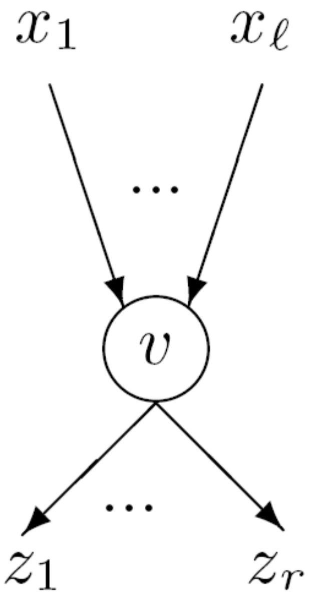
  This state is a collection of $|S|$ cat states. Can prepare EPR states from here and teleport the given state as desired.

Operations used for coding

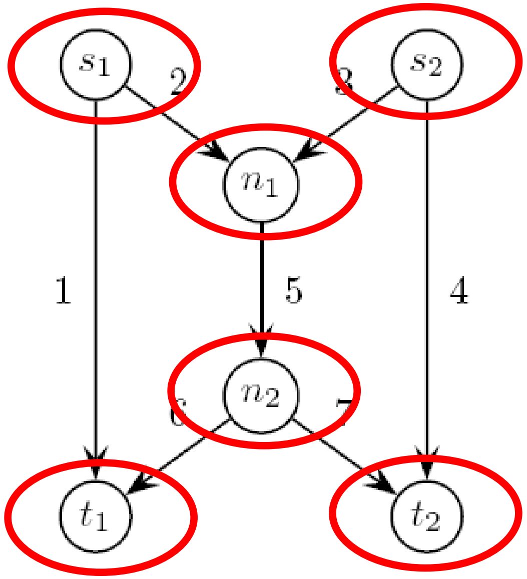
(i) **Operations at internal nodes:** Consider a node $v \in V$ with fan-in ℓ and fan-out r. Associated quantum coding operation is: attach r new ancilla qubits initialized in $|0\rangle$ and, for $j = 1, \ldots, r$, apply a controlled-NOT operation implementing an addition of γ_{ij} between all incoming qubits i as control qubits and the j-th ancilla as target qubit. This maps $|x\rangle|0\rangle^{\otimes r}$ to $|x_1, \ldots, x_\ell, z_1, \ldots, z_r\rangle$ where $z_j = \sum_{i=1}^{\ell} \gamma_{ij} x_i$. Send the r ancilla qubits along the outgoing edges, retain all incoming qubits.

(ii) **Fan-out operations:** The r-fan-out broadcast node is the special case where $\ell = 1$ and $\gamma_{1j} = 1$ for each $= 1, \ldots, r$. For a given basis vector $|x\rangle \in F_2$ on one qubit, we attach r further ancillas initialized in $|0\rangle$ and apply a controlled-NOT gate between the given qubit as control and each ancilla as target. The effect on the state is given by $|x\rangle|0\rangle^{\otimes r} \mapsto |x\rangle^{\otimes(r+1)}$.

(iii) **Measurements:** They are used to collapse the superfluous qubits (kept at each node). All qubits are measured in the Hadamard basis.



Example



s_1 t_1 n_1 s_2 t_2 n_1

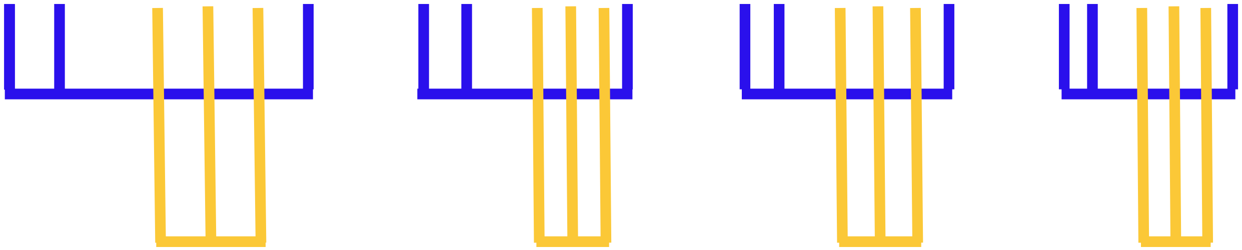
$$|0\,0\,0\,0\,0\,0\rangle + |000111\rangle + |111000\rangle + |111111\rangle$$

$$\mapsto |0\,0\,0\,0\,0\,0\rangle + |000111\rangle + |111001\rangle + |111110\rangle$$

s_1 t_1 n_1 s_2 t_2 t_1 t_2

$$\mapsto |0\,0\,0\,0\,0\,0\,0\rangle + |0001111\rangle + |1110011\rangle + |1111100\rangle$$

$$\mapsto |0\,0\,0\,0\,0\,0\,0\rangle + |0001110\rangle + |1110001\rangle + |1111111\rangle$$



🟦 GHZ state 1

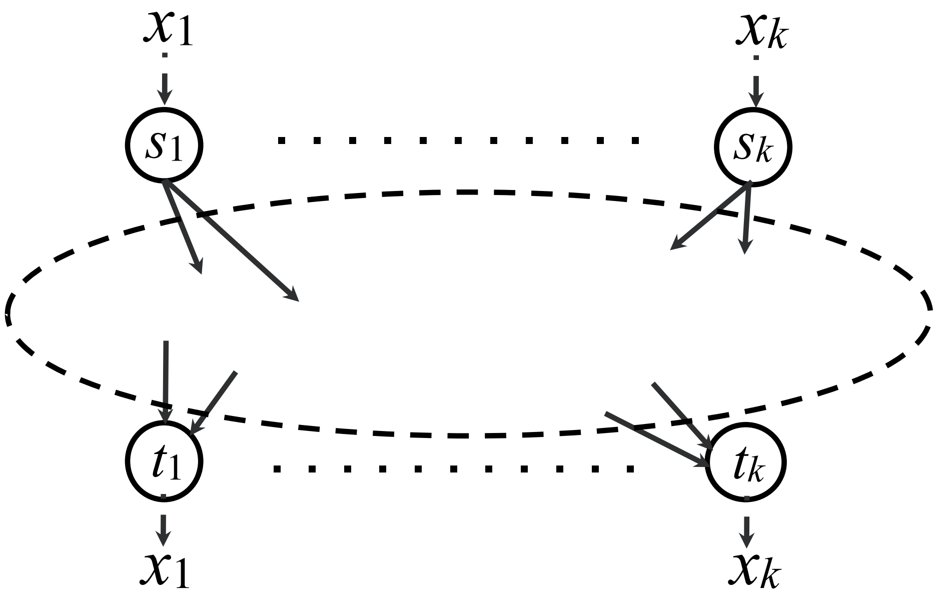
🟨 GHZ state 2

The k-pair communication problem

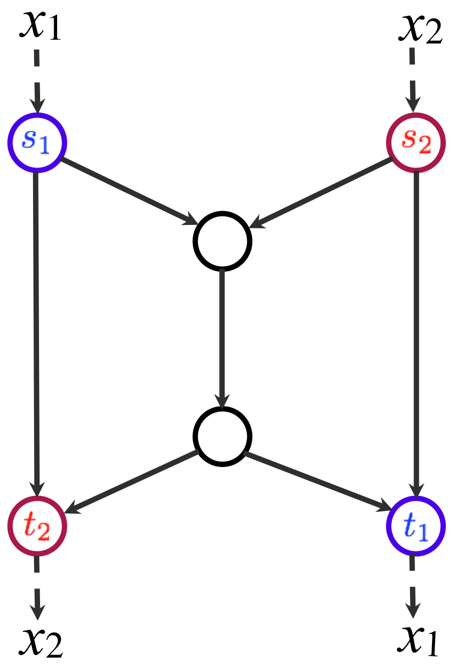
given: • a directed (acyclic) graph
• k source nodes $s_1,\ldots s_k$
• k target nodes $t_1,\ldots t_k$

goal: one bit x_i has to be sent from s_i to t_i

each edge has capacity 1



butterfly: instance of the 2-pair problem



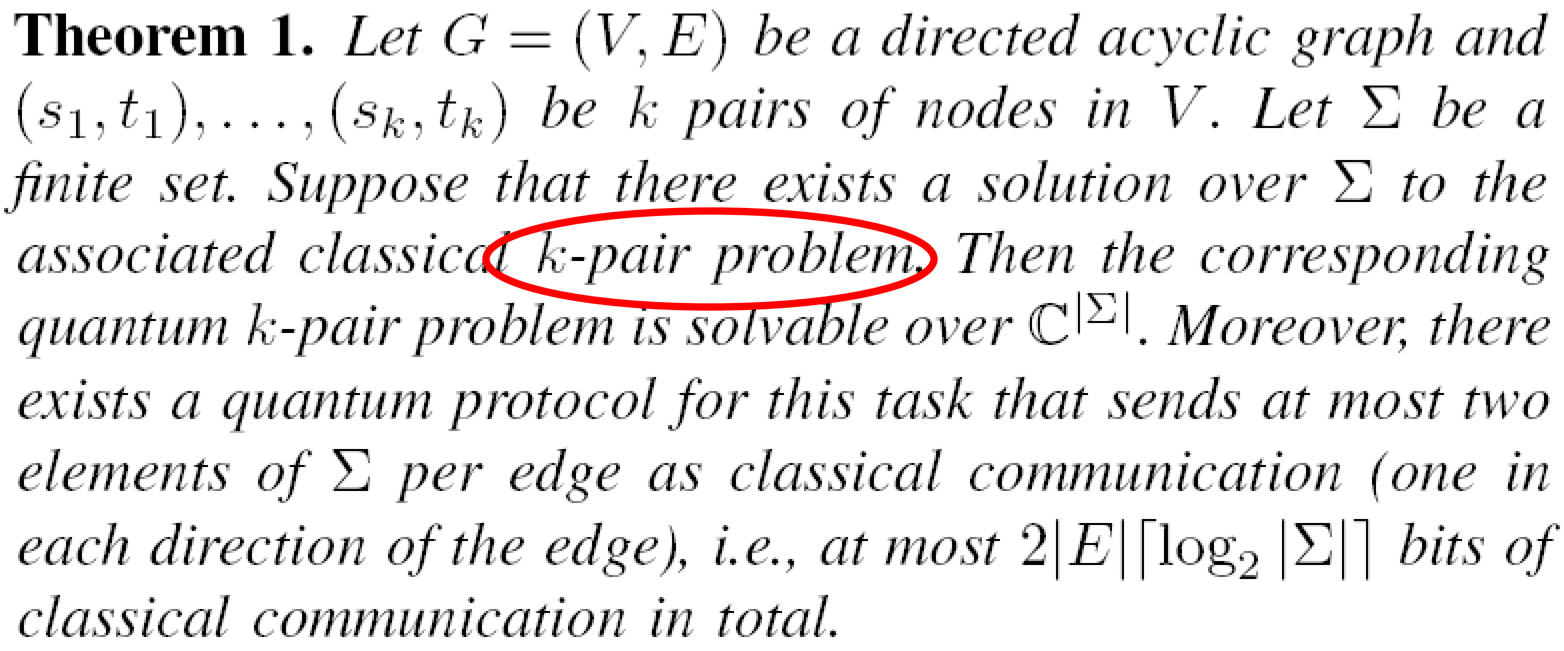
The k-pair communication problem

- Considering linear protocols is not enough in general
  - There exist examples of networks for which a non-linear protocol exists for the k-pair problem and for which it can be shown that no linear protocol can exist **[Dougherty, Freiling, Zeger 2005], [Riis 2004]**
  - There are also examples where “vector linear” protocols exist **[Koetter 2003], [Lehman, Lehman 2004]**

- For k=2 there exists a polynomial time algorithm to decide whether a protocol exists **[Wang, Shroff 2007]**

- The complexity of the case k>2 is an open problem.

Generalization: arbitrary protocols

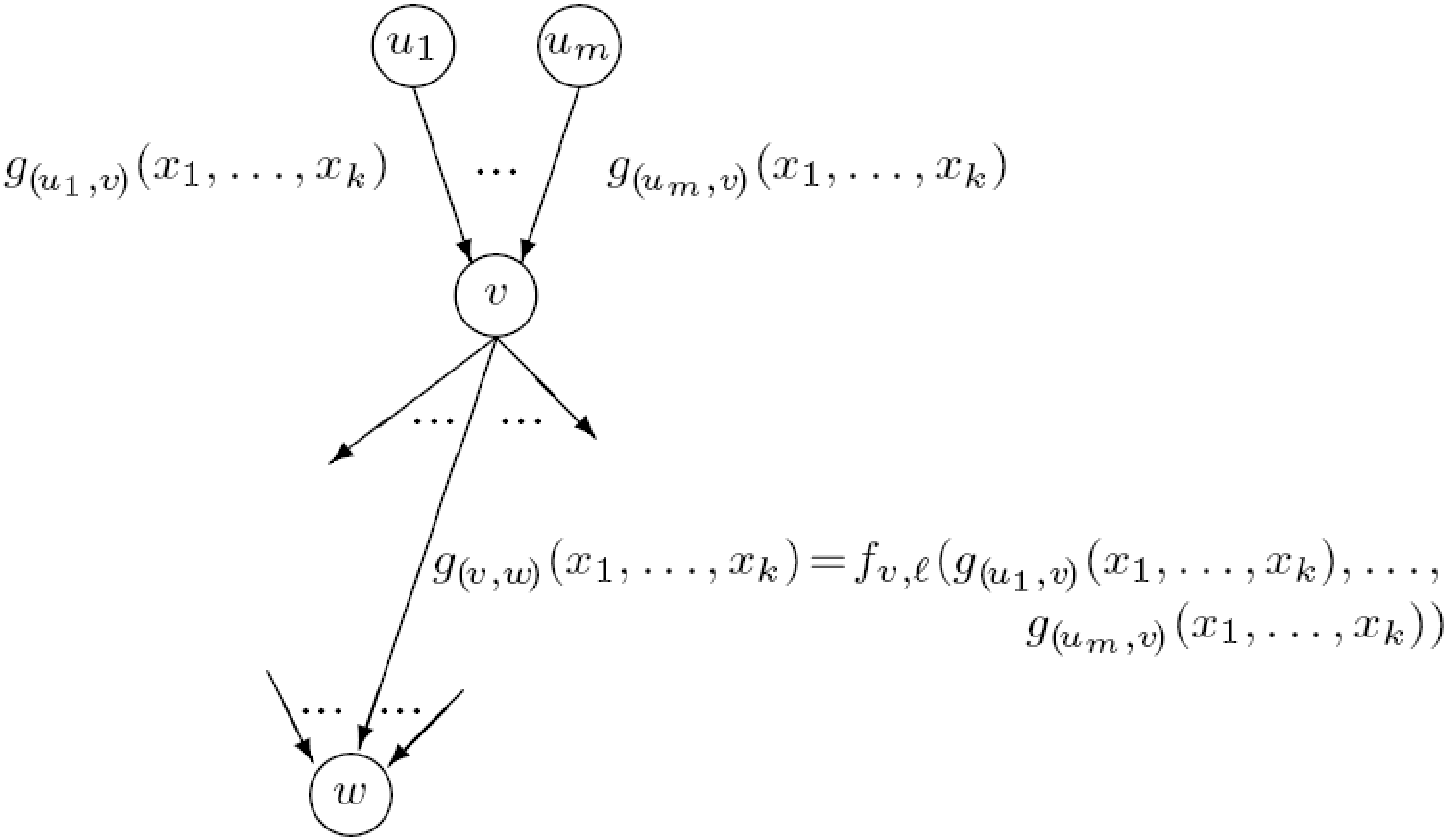


Theorem 1. *Let $G = (V, E)$ be a directed acyclic graph and $(s_1, t_1), \ldots, (s_k, t_k)$ be k pairs of nodes in V. Let Σ be a finite set. Suppose that there exists a solution over Σ to the associated classical k-pair problem. Then the corresponding quantum k-pair problem is solvable over $\mathbb{C}^{|\Sigma|}$. Moreover, there exists a quantum protocol for this task that sends at most two elements of Σ per edge as classical communication (one in each direction of the edge), i.e., at most $2|E|\lceil \log_2 |\Sigma| \rceil$ bits of classical communication in total.*

[Kobayashi, Le Gall, Nishimura, R., ISIT'11]

Proof (sketch)

Protocol removes phases “node by node”:


u_1
u_m
$g_{(u_1,v)}(x_1,\ldots,x_k)$
$\cdots$
$g_{(u_m,v)}(x_1,\ldots,x_k)$
v
$\cdots$
$\cdots$
$g_{(v,w)}(x_1,\ldots,x_k) = f_{v,\ell}(g_{(u_1,v)}(x_1,\ldots,x_k),\ldots,$
$g_{(u_m,v)}(x_1,\ldots,x_k))$
$\cdots$
$\cdots$
w

Proof (sketch)

Suppose that the input state of the quantum task is

$$|\psi_S\rangle_{(\mathsf{S}_1,\ldots,\mathsf{S}_k)} = \sum_{x_1,\ldots,x_k\in\Sigma} \alpha_{x_1,\ldots,x_k}|x_1\rangle_{\mathsf{S}_1}\otimes\cdots\otimes|x_k\rangle_{\mathsf{S}_k},$$

First, create this state:

$$\sum_{x_1,\ldots,x_k\in\Sigma} \alpha_{x_1,\ldots,x_k}|x_1\rangle_{\mathsf{S}_1}|x_1\rangle_{\mathsf{T}_1}\otimes\cdots\otimes|x_k\rangle_{\mathsf{S}_k}|x_k\rangle_{\mathsf{T}_k}\otimes\left(\bigotimes_{\vec{e}\in\overline{E}}|g_{\vec{e}}(x_1,\ldots,x_k)\rangle_{\mathsf{R}_{\vec{e}}}\right),$$

Next, apply Fourier transform at node v:

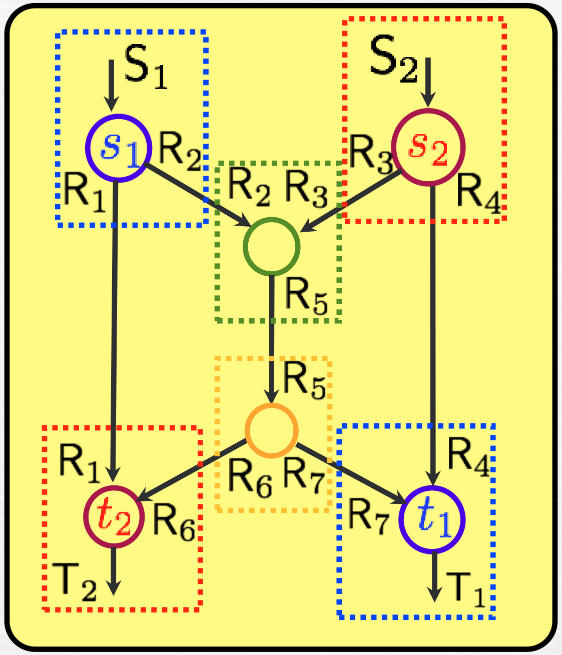
$$\sum_{x_1,\ldots,x_k\in\Sigma} \alpha_{x_1,\ldots,x_k}\exp\left(2\pi\iota\frac{\overline{a_{(v,w)}}\cdot\overline{g_{(v,w)}(x_1,\ldots,x_k)}}{|\Sigma|}\right)\times|x_1\rangle_{\mathsf{S}_1}|x_1\rangle_{\mathsf{T}_1}\otimes\cdots$$

$$\cdots\otimes|x_k\rangle_{\mathsf{S}_k}|x_k\rangle_{\mathsf{T}_k}\otimes|a_{(v,w)}\rangle_{\mathsf{R}_{(v,w)}}\otimes\left(\bigotimes_{\vec{e}\in\overline{E}\setminus\{(v,w)\}}|g_{\vec{e}}(x_1,\ldots,x_k)\rangle_{\mathsf{R}_{\vec{e}}}\right).$$

Finally, remove phase at node v:

$$\sum_{x_1,\ldots,x_k\in\Sigma} \alpha_{x_1,\ldots,x_k}|x_1\rangle_{\mathsf{S}_1}|x_1\rangle_{\mathsf{T}_1}\otimes\cdots\otimes|x_k\rangle_{\mathsf{S}_k}|x_k\rangle_{\mathsf{T}_k}\otimes\left(\bigotimes_{\substack{\vec{e}\in\overline{E}\\ \vec{e}\neq(v,w)}}|g_{\vec{e}}(x_1,\ldots,x_k)\rangle_{\mathsf{R}_{\vec{e}}}\right),$$

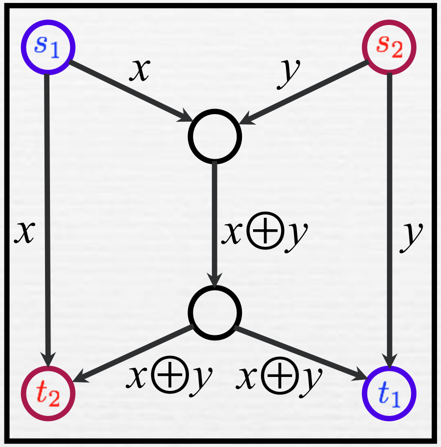
Example: node-by-node protocol

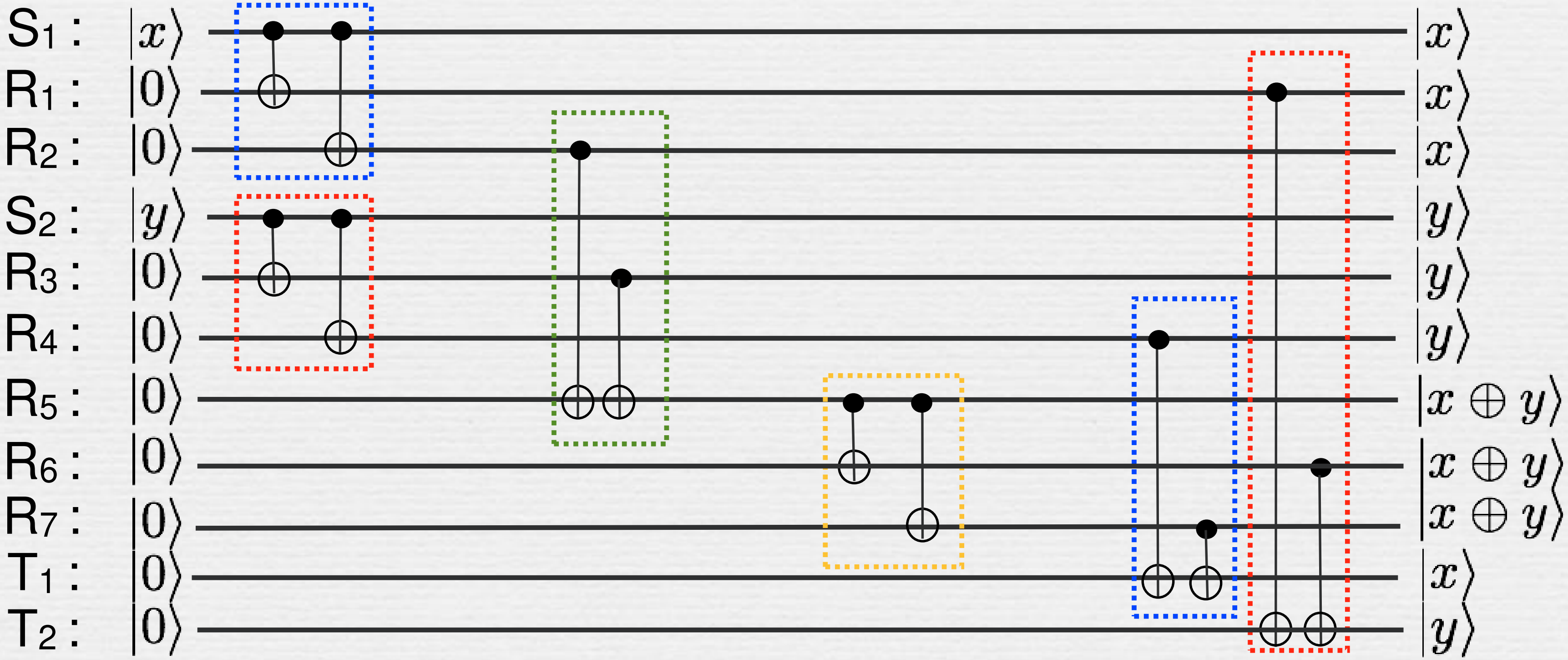


initial state: $|x\rangle_{S_1}|y\rangle_{S_2}$

basis states

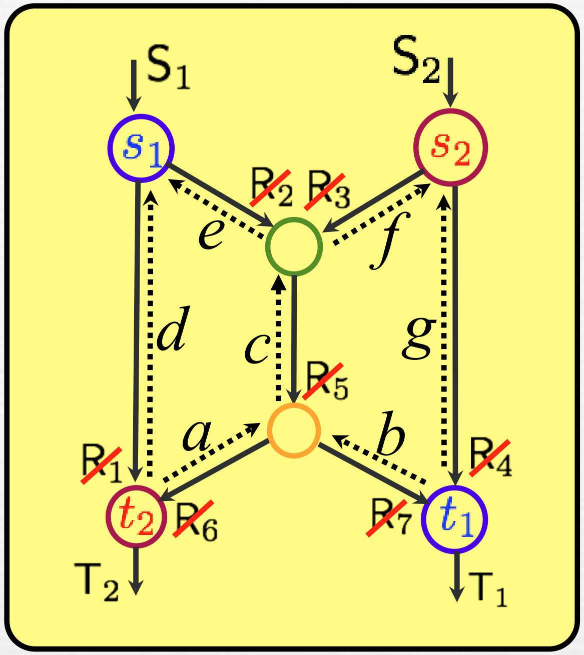
$x, y \in \{0,1\}$





Removing the internal registers

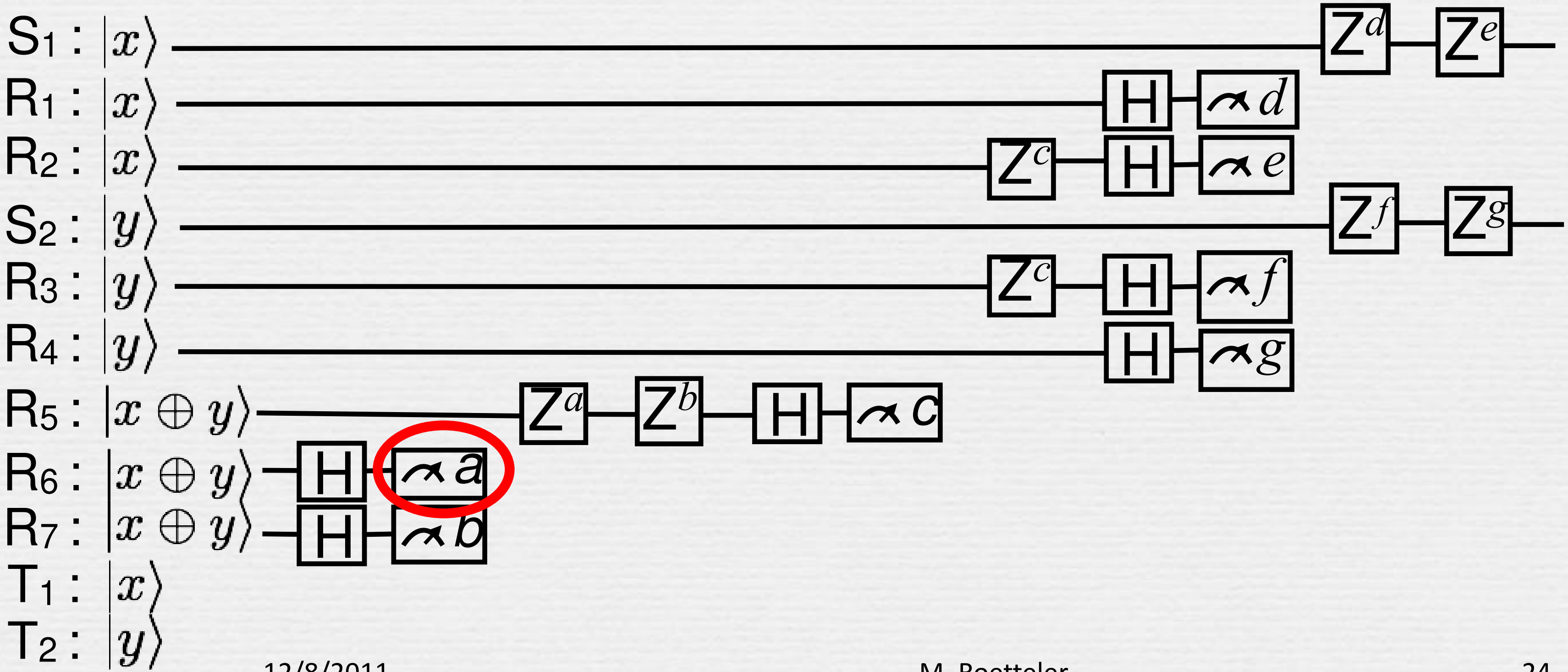
phases can always be corrected at the prior nodes



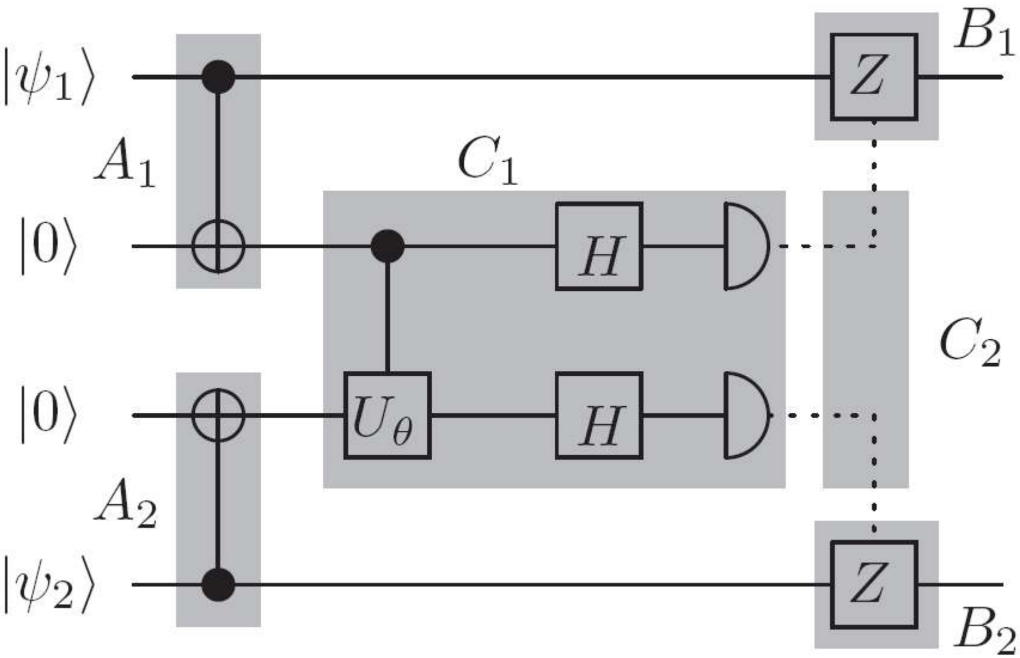
┈┈┈▸: 1 bit

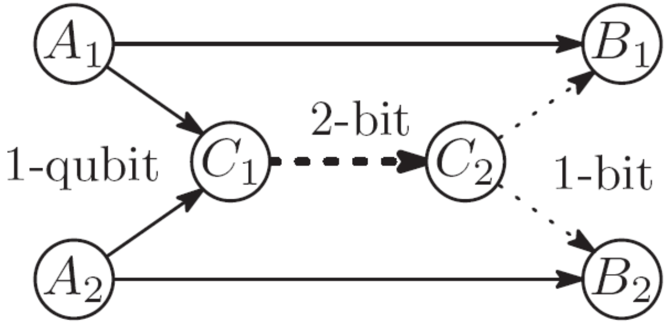
$$\sum_{x,y\in\{0,1\}} \alpha_{xy}|x\rangle_{\mathsf{S}_1}|x\rangle_{\mathsf{R}_1}|x\rangle_{\mathsf{R}_2}|y\rangle_{\mathsf{S}_2}|y\rangle_{\mathsf{R}_3}|y\rangle_{\mathsf{R}_4}\otimes$$

$$|x\oplus y\rangle_{\mathsf{R}_5}|\cancel{a}\rangle_{\mathsf{R}_6}|x\oplus y\rangle_{\mathsf{R}_7}|x\rangle_{\mathsf{T}_1}|y\rangle_{\mathsf{T}_2}$$



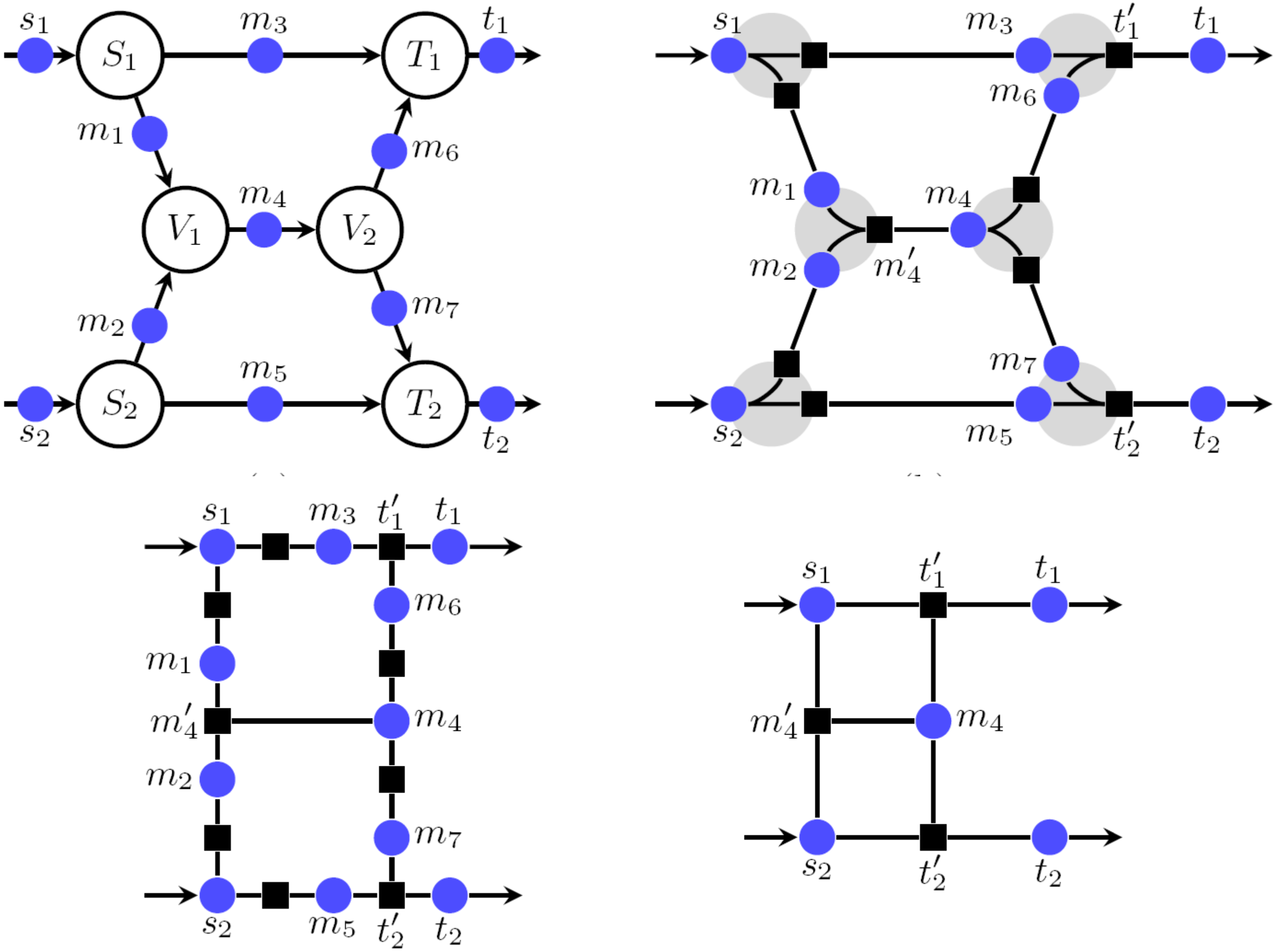
Implementing other unitaries?





Result: the butterfly network allows to implement certain unitary operations that are not permutations of basis states, e.g. controlled phase gates between the inputs (shown above), More generally any controlled-U can be realized. **[Y. Kinjo, M. Murao, A. Soeda, P.S.Turner, 2010]**

Connections to MBQC



Result: each QNC protocol is an MBQC for a graph state corresponding to the undirected graph **[N. de Beaudrap, MR, 2011, unpublished].** We conjecture that the converse is also true.

Conclusions

1. **“Quantum network coding”**

    - If classical and quantum communication are restricted, then for most networks there is no perfect communication protocol.
    - For instance for the butterfly, there is no protocol with fidelity 1, best known protocol achieves fidelity only slightly better than ½.

2. **Model with free classical communication**

    - [Kobayashi et al, ISIT’10] : whenever a classical linear network coding exists, then also perfect quantum network coding can be achieved.
      [Kobayashi et al, ISIT’11] : whenever a classical network coding protocol exists , then also perfect quantum network coding can be achieved.

    - Open: is the converse true as well? That is, does a solution for the quantum k-pairs problem imply existence of a classical solution for the k-pair problem?
    - Open: explore connections between quantum network coding and measurement-based quantum computing (MBQC)? Specifically, if a MBQC scheme exists that implements a Clifford by just local measurements in the X-Y plane, can the edges of the underlying graph be oriented to get a quantum network code?
    - Open: for a given network characterize the set of all implementable unitary transformations besides permutations of qubits.