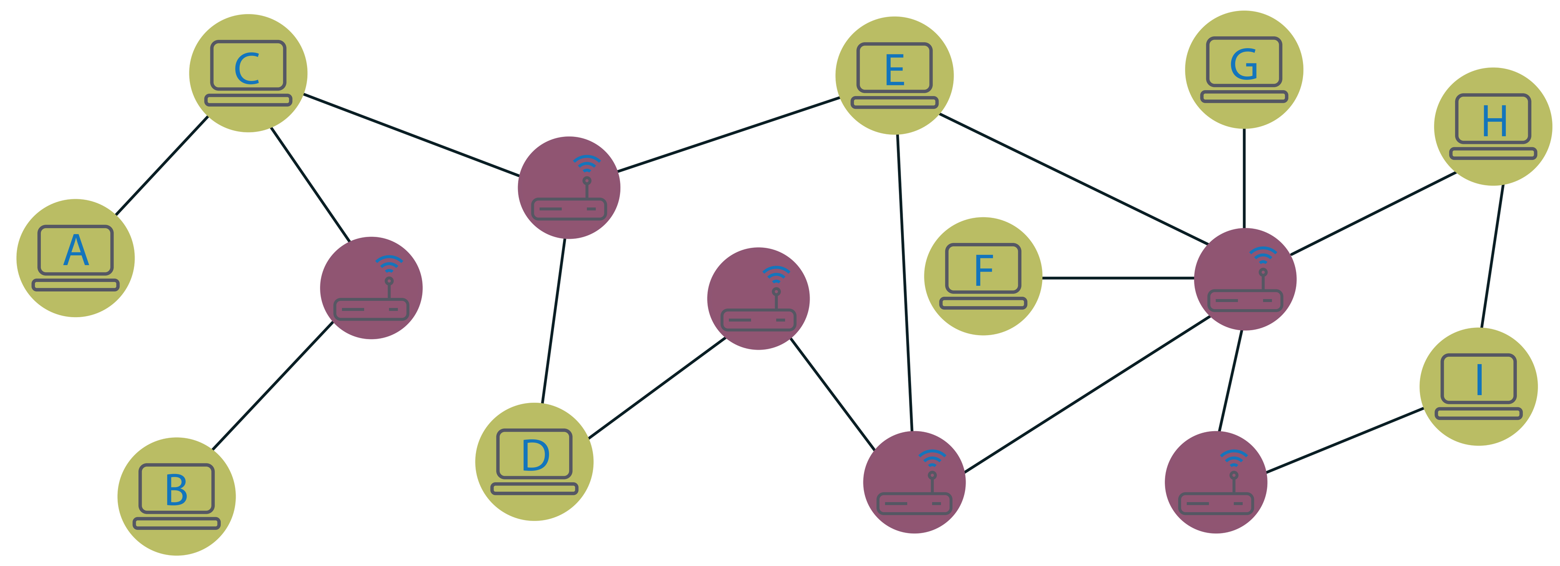
Linear programs for entanglement and key distribution in the quantum internet

Stefan Bäuml, Koji Azuma, Go Kato, David Elkouss

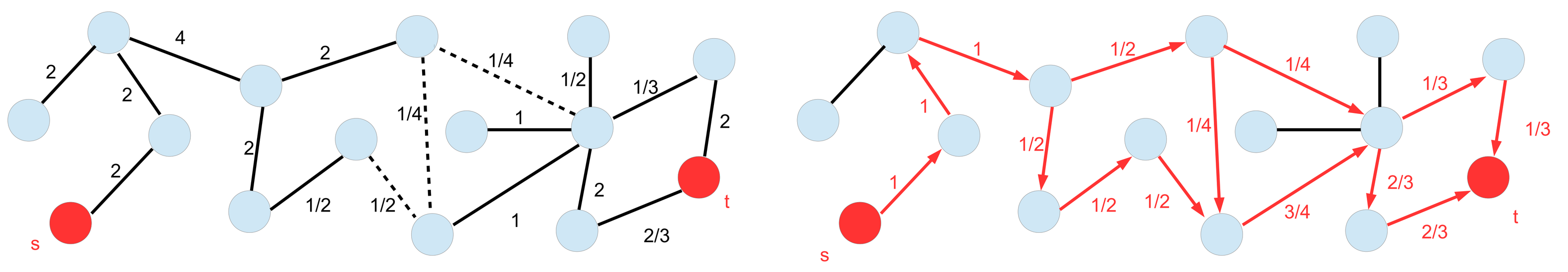
Communications Physics 3.1 (2020): 1-12, arXiv:1809.03120

Quantum Internet



- Quantum network consisting of channels, repeater stations and end users. Goal: distribution of entanglement by **adaptive** LOCC protocol. Possible target target states:
- Bell states $|\Phi^d\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^d |ii\rangle$.
- Private states $\gamma^d = U^{\text{twist}}|\Phi^d\rangle\langle\Phi^d| \otimes \sigma U^{\text{twist}\dagger}$.
- GHZ states $|\Phi^{\text{GHZ},d}\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1} |i\rangle \otimes \cdots \otimes |i\rangle$.
- Multipartite pdits $\gamma^d = U^{\text{twist}}|\Phi^{\text{GHZ},d}\rangle\langle\Phi^{\text{GHZ},d}| \otimes \sigma U^{\text{twist}\dagger}$.

Bipartite User Scenarios



- *Quantum* and *private network capacities*:

$$\mathcal{Q}, \mathcal{P}_{\text{network}} = \lim_{\epsilon\to 0}\lim_{m\to\infty}\sup_{\Lambda}\left\{\frac{\log d}{m} : \left\|\rho_{AB}^{(m)} - \theta_{target}^d\right\|_1 \le \epsilon\right\}.$$

- Upper bound[a]:

$$\mathcal{P}_{\text{network}} \le \max_{\{p_{uv}\}}\min_{S\leftrightarrow T}\sum_{uv\in E:\{uv\}\in S\leftrightarrow T} p_{uv}\mathcal{E}(\mathcal{N}^{uv}),$$

  for $\mathcal{E} = E_{sq}, E_{max}$ or E_R for teleportation stretchable channels

- Apply max-flow min-cut Theorem: Flow optimization in network with edge capacities $p_{uv}\mathcal{E}(\mathcal{N}^{uv})$.
- Lower bound on $\mathcal{Q}_{\text{network}}$: Aggregated repeater protocol[b]: Distill Bell pairs across each edge with asymptotic rate $p_{uv}\mathcal{Q}^{\leftrightarrow}(\mathcal{N}^{uv})$ and swap along paths: Flow optimization in network with edge capacities $p_{uv}\mathcal{Q}^{\leftrightarrow}(\mathcal{N}^{uv})$.
- **Efficiently computable** bounds:

$$f_{\mathcal{Q}^{\leftrightarrow}}^{a\to b} \le \mathcal{Q}_{\text{network}} \le \mathcal{P}_{\text{network}} \le f_{\mathcal{E}}^{a\to b},$$

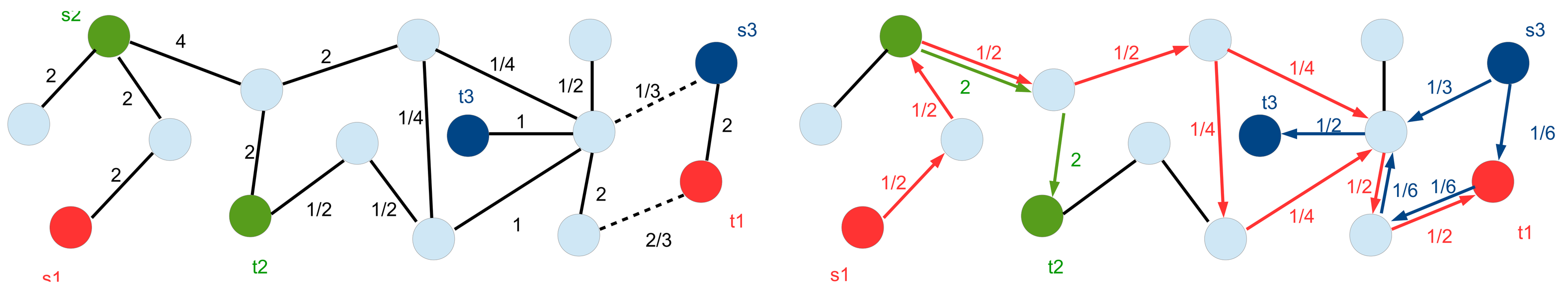
  with the **linear program**

$$\begin{aligned} f_c^{a\to b} &= \max \sum_{v:\{av\}\in E'} (f_{av} - f_{va}) \\ &\forall \{vw\}\in E' :\ f_{wv} + f_{vw} \le p_{wv}c_{wv} + p_{vw}c_{vw} \\ &\forall w \in V : w \neq a, b, \quad \sum_{v:\{vw\}\in E'} (f_{vw} - f_{wv}) = 0, \end{aligned}$$

  where the maximization is over edge flows $f_{vw} \ge 0$ and usage frequencies $0 \le p_e \le 1$, $\sum_e p_e = 1$.

[a] Azuma et al. 2016, Pirandola 2016, Rigovacca et al. 2017.
[b] Azuma, Kato 2016

Multiple pairs of users: Worst Case

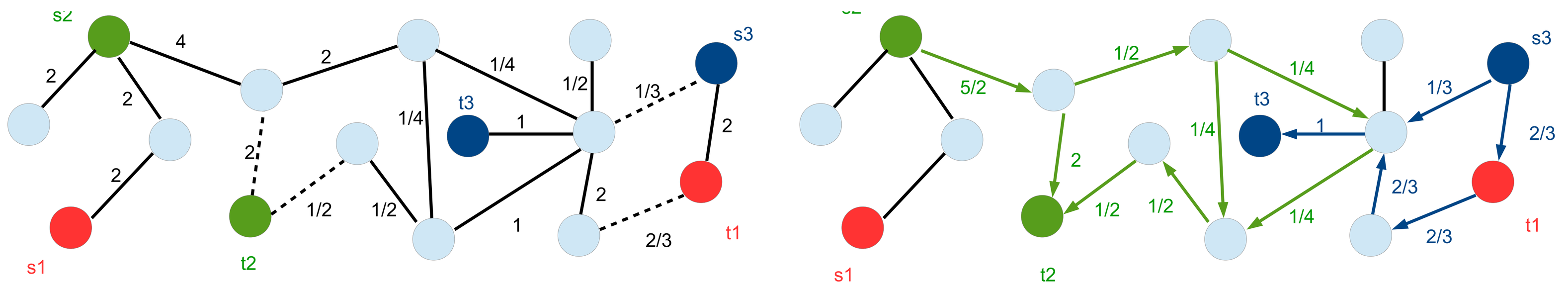


- $\mathcal{Q}, \mathcal{P}_{\text{network}}^{\text{worst case}}$: Smallest rate that can be achieved by all user pairs concurrently.
- $\mathcal{P}_{\text{network}}^{\text{worst case}} \le \max_{\{p_{uv}\}}\min_{V_1\leftrightarrow V_2} \frac{\sum_{V_1\leftrightarrow V_2} p_{uv}\mathcal{E}(\mathcal{N}^{uv})}{\#\text{ pairs divided by } V_1\leftrightarrow V_2}$.
- Relax to **concurrent multicommodity flow** optimization LP[a]. Gap of $\mathcal{O}(\log k)$.
- Lower bounds by concurrent aggregated repeater protocol.
- **Efficiently computable** bounds:

$$f_{\mathcal{Q}^{\leftrightarrow}}^{\text{worst case}} \le \mathcal{Q}_{\text{network}}^{\text{worst case}} \le \mathcal{P}_{\text{network}}^{\text{worst case}} \le \mathcal{O}(\log k) f_{\mathcal{E}}^{\text{worst case}}.$$

[a] Aumann, Rabani 1998

Total Throughput

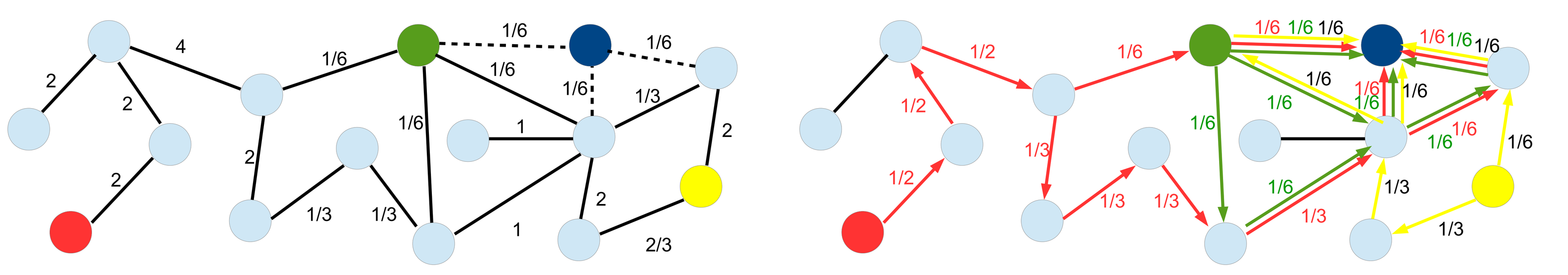


- $\mathcal{Q}, \mathcal{P}_{\text{network}}^{\text{total}}$: Maximize sum of concurrent rates.
- $\mathcal{P}_{\text{network}}^{\text{total}} \le \max_{\{p_{uv}\}}\min_{\{S\}\leftrightarrow\{T\}}\sum_{\{S\}\leftrightarrow\{T\}} p_{uv}E_{sq}(\mathcal{N}^{uv})$.
- Relax to **max total flow** optimization LP[a]. Gap of $\mathcal{O}(\log k)$.
- Lower bounds by concurrent aggregated repeater protocol.
- **Efficiently computable** bounds:

$$f_{\mathcal{Q}^{\leftrightarrow}}^{\text{total}} \le \mathcal{Q}_{\text{network}}^{\text{total}} \le \mathcal{P}_{\text{network}}^{\text{total}} \le \mathcal{O}(\log k) f_{E_{sq}}^{\text{total}}.$$

[a] Garg et al. 1993

Multipartite User Scenario



- $\mathcal{Q}, \mathcal{P}_{\text{network}}^{S}$: Maximum rate for distribution of GHZ or multipartite private states among set S of users.
- $\mathcal{P}_{\text{network}}^{S} \le \max_{\{p_{uv}\}}\min_{S\text{-cut } S_i\leftrightarrow S_j}\sum_{S_i\leftrightarrow S_j} p_{uv}E_{sq}(\mathcal{N}^{uv})$.
- S-connectivity can be transformed into flow LP using max-flow min-cut Theorem.
- Lower bounds: Entanglement swapping → 'GHZ-swapping', paths → Steiner trees.
- Steiner tree packing problem NP hard, but can be relaxed to S-connectivity[a], which can be transformed into flow LP.
- **Efficiently computable** bounds:

$$\frac{1}{2} f_{\mathcal{Q}^{\leftrightarrow}}^{S} \le \mathcal{Q}_{\text{network}}^{S} \le \mathcal{P}_{\text{network}}^{S} \le f_{E_{sq}}^{S}.$$

[a] Günlük 2007