New Limits on Fault-Tolerant Quantum Computation

Falk Unger[1]

Joint work with: Harry Buhrman[1,2], Richard Cleve[3], Monique Laurent[1], Noah Linden[4], Alexander Schrijver[1,2]

[1] CWI Amsterdam, [2] UvA Amsterdam, [3] University of Calgary, [4] University of Bristol

Fault-tolerant Quantum Computation

- Problem in QC: physical devices cannot be made perfect (noise-free)
- Fault-tolerant computing helps
  - There is a threshold $\hat{\theta} > 0$, s.t. for noise less than $\hat{\theta}$ quantum circuits can be made fault-tolerant
  - There are various lower bounds on this noise rate: $10^{-4} \ldots 10^{-6} \leq \hat{\theta}$
    - And even $3\% \leq \hat{\theta}$ [Knill, 2005] for circuits with a restricted class of gates (using a heuristic simulation argument)
- We prove an upper bound on $\hat{\theta}$

$$\hat{\theta} < \frac{6 - 2\sqrt{2}}{7} \approx 45\%$$

Depolarizing Noise

Applying depolarizing noise p to 1-qubit unitary U yields operation

$$U_p(\rho) = (1-p)U\rho U^\dagger + pI/2$$

Related results

1. Too much depolarizing noise implies efficient classical simulation
   - $p_\epsilon > 97\%$ for gates with fan-in ≤ 2 [Aharonov, Ben-Or '96]
   - $p_\epsilon > 74\%$ (2-qubit gates can not create entanglement) [Harrow, Nielsen '03]
2. Other results
   - For $p_\epsilon > 50\%$ circuits of super-logarithmic depth using gates of fan-in ≤ 2 are "useless" [Razborov '03].
     (but there are log-depth circuits doing useful things)

Main result

Arbitrary 1-qubit gates with depolarizing error greater than $\frac{6-2\sqrt{2}}{7} \approx 45\%$ together with all (noise-free) gates from the Clifford group (generated by CNOT, H and S) are not universal.

Relation to former results

- no constraints on circuit depth
- prove not only classical simulability
- some (very common) gates are even noise-free
- However, we don't, allow arbitrary 2-qubit gates

Overview

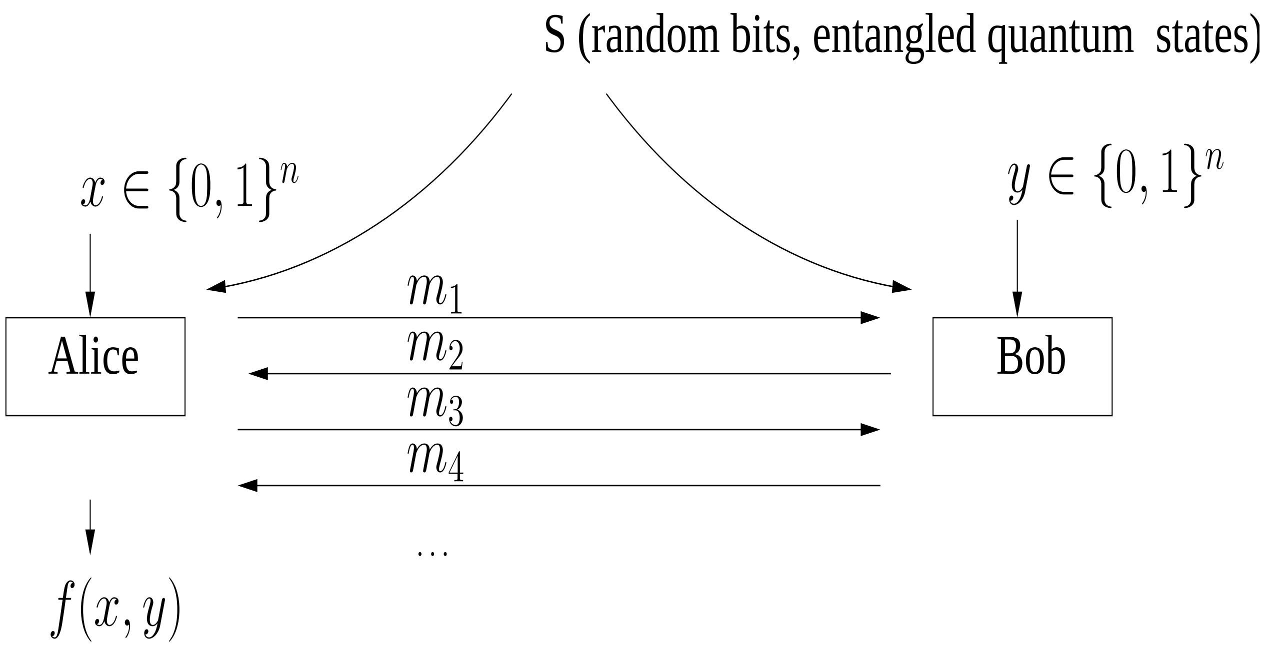
1. Communication complexity
2. Clifford gates
3. 2-party simulation of Clifford circuits with one bit of communication
4. Simulation of 1-qubit unitary gates with depolarizing noise 45% by probabilistic mixture of Cliffords
5. Threshold for fault-tolerant quantum computing

Overview

1. $\boxed{\text{Communication complexity}}$
2. Clifford gates
3. 2-party simulation of Clifford circuits with one bit of communication
4. Simulation of 1-qubit unitary gates with depolarizing noise 45% by probabilistic mixture of Cliffords
5. Threshold for fault-tolerant quantum computing

Communication Complexity

- Two separated parties want to compute $f : \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}$



- How many bits need to be communicated such that for each input one party outputs the correct result (with error probability at most $\epsilon < 1/2$)?

Communication Complexity bounds

Inner product function :

$$IP_n(x,y) = \sum_{i=1}^{n} x_i \cdot y_i \mod 2$$

Deterministic protocols $C_0(IP_n) = n$

Probabilistic protocols $C_\epsilon(IP_n) \in \Omega(n)$ for any $\epsilon < 1/2$

Entanglement assisted $C^*_\epsilon(IP_n) \in \Omega(n)$ for any $\epsilon < 1/2$

(actually, most functions f have $C_{0/\epsilon/\epsilon^*}(f) \in \Omega(n)$)

Overview

1. Communication complexity
2. $\boxed{\text{Clifford gates}}$
3. 2-party simulation of Clifford circuits with one bit of communication
4. Simulation of 1-qubit unitary gates with depolarizing noise 45% by probabilistic mixture of Cliffords
5. Threshold for fault-tolerant quantum computing

Clifford gates

- Gate C is in the Clifford group if for any tensor product of Pauli-operators P_1 there is a tensor product of Pauli-operators P_2 with

$$CP_1C^\dagger = \alpha P_2 \longleftrightarrow CP_1 = P_2C$$

Gates generating the Clifford-group are

$$\text{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

- Clifford-group gates together with one other 1-qubit-gate are universal

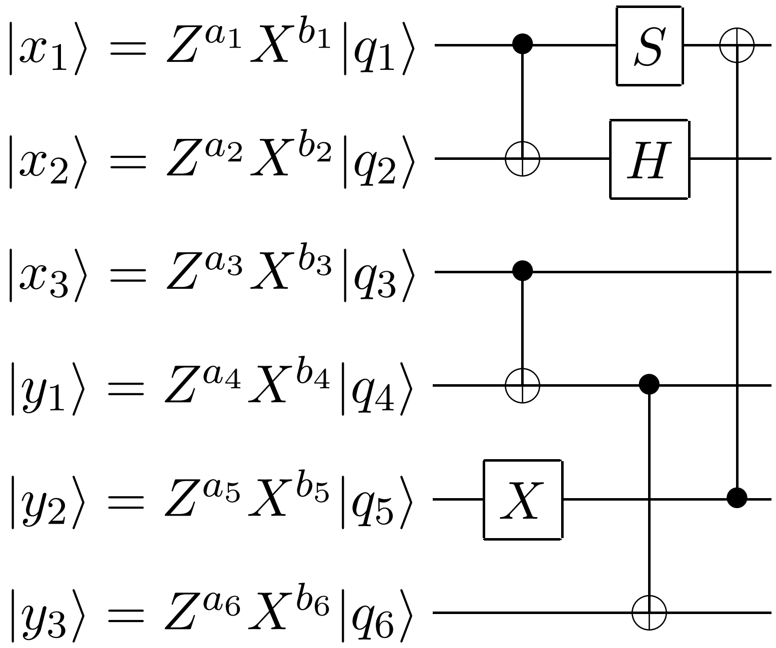
Overview

1. Communication complexity
2. Clifford gates
3. 2-party simulation of Clifford circuits with one bit of communication
4. Simulation of 1-qubit unitary gates with depolarizing noise 45% by probabilistic mixture of Cliffords
5. Threshold for fault-tolerant quantum computing

Any CC has CC $=1$

Let C be any Clifford circuit. Alice, given x, and Bob, given y, want to compute $C(x, y)$. They can do so using only one bit of communication, by simulating C ...

Simulating Clifford-circuits



Logical representation of i-th qubit

$$Z^{a_i}X^{b_i}|q_i\rangle$$

where a_i, b_i belong to Alice and $|q_i\rangle$ to Bob.

Initialization can be done without communication

$$\begin{aligned} |x_i\rangle &= Z^0X^{x_i}|0\rangle \\ |y_j\rangle &= Z^0X^0|y_j\rangle \end{aligned}$$

Simulating Clifford operations

- 1-qubit Clifford-gate C
  (Remember: $CP_1 = P_2C$)

$$CX^aZ^b|q_i\rangle = P_1CZ^b|q_i\rangle = P_1P_2C|q_i\rangle = X^{a'}Z^{b'}|q_i'\rangle$$

- Similar for CNOT-gates

$$\text{Example:} \quad \begin{aligned} SXZ|\psi\rangle &= YSZ|\psi\rangle \\ &= YZS|\psi\rangle \\ &= iXS|\psi\rangle \end{aligned}$$

$\rightarrow$ Distributed simulation of Clifford-gates without communication

Measurement

Bob can measure i-th qubit

$$Z^{a_i} X^{b_i} |q_i\rangle$$

in the computational basis, if he knows b_i.
$\rightarrow$ 1 bit of communication

Any function $f : \{0,1\}^{m_A} \times \{0,1\}^{m_B} \rightarrow \{0,1\}$ which can be computed by a Clifford-circuit, has deterministic communication complexity 1.

$\rightarrow$ Clifford circuits are not universal

Overview

1. Communication complexity
2. Clifford gates
3. 2-party simulation of Clifford circuits with one bit of communication
4. $\boxed{\text{Simulation of 1-qubit unitary gates with depolarizing noise } 45\% \text{ by probabilistic mixture of Cliffords}}$
5. Threshold for fault-tolerant quantum computing

Noisy simulation of 1-qubit gates

- For any 1-qubit unitary U let U_p be the faulty version with depolarizing error p

$$U_p : \rho \mapsto (1-p)U\rho U^\dagger + pI_2$$

- We prove: If

$$p \geq \frac{6-2\sqrt{2}}{7} \approx 45\%$$

then any U_p can be simulated by a probabilistic mixture of Clifford-gates

$$U_p(\rho) = \sum_i p_i C_i \rho C_i^\dagger$$

(Use Bloch representation)

Bloch-representation

- 1-qubit state ρ can be written as

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}, ||\vec{r}|| \leq 1$$

$(\vec{r} \cdot \vec{\sigma} = r_1\sigma_1 + r_2\sigma_2 + r_3\sigma_3)$

- For any unitary $U \in \mathbb{C}^{2\times 2}$ there is a 3×3 rotation matrix $R \in SO(3)$ with

$$U\left(\frac{I + \vec{r} \cdot \vec{\sigma}}{2}\right) = \frac{I + \vec{r}' \cdot \vec{\sigma}}{2} \leftrightarrow R\vec{r} = \vec{r}'$$

- If U_p is U with dep. error p, and U has Bloch representation $R \in SO(3)$, then U_p has Bloch representation

$$R_p = (1 - p)R$$

Our problem in Bloch representation

- Let $R_i^C \in SO(3)$ be the 24 Cliffords in Bloch representation
- Find the smallest p such that for all rotation matrices $R \in SO(3)$ we can write

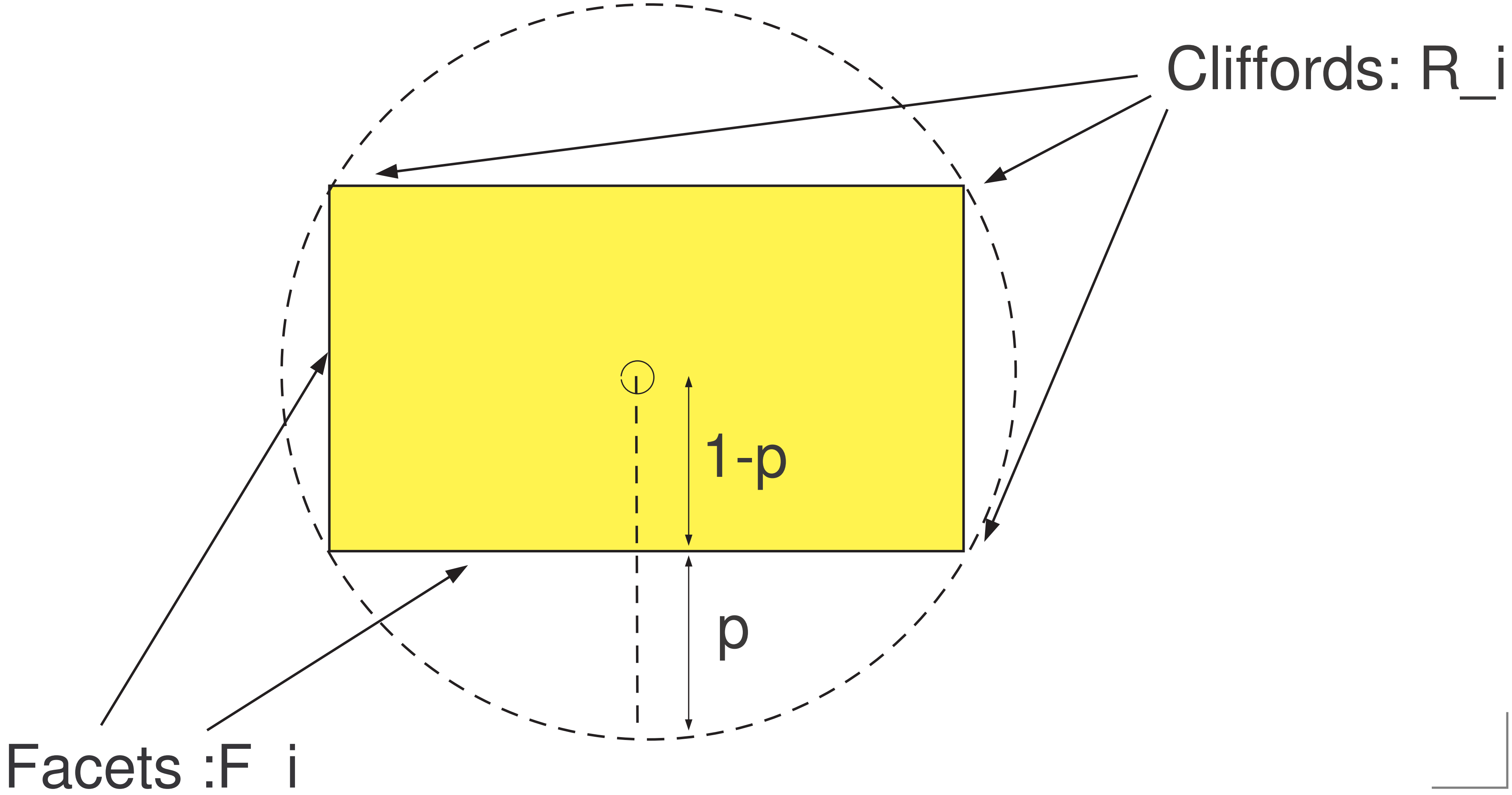
$$(1-p)R = \sum_i p_i R_i^C$$

$$\leftrightarrow (1-p)R \in \text{ConvHull}(R_1^C, \ldots, R_{24}^C) = \mathcal{P}$$

$\rightarrow$ optimization problem in 9 dimensions

From vertex description to facet description

ConvHull$(R_1^C, \ldots, R_{24}^C) = \mathcal{P}$, Want $\forall R : (1-p)R \in \mathcal{P}$



Use facet description

- Our polytope $\mathcal{P}$ has 120 facets $F_1, \ldots F_{120}$, i.e. for any point $x \in R^{3\times 3}$

$$x \in \mathcal{P} \leftrightarrow \forall_{i=1,\ldots,120} : x \bullet F_i \leq 1,$$

where $A \bullet B = \sum_{ij} a_{ij} b_{ij}$.

- Our problem becomes

$$\begin{aligned} & \min_p \{p : \forall_{R \in SO(3), i=1,\ldots,120} : (1-p)R \bullet F_i \leq 1\} \\ = \max_{i=1,\ldots,120} \quad & \min_p \{p : \forall_{R \in SO(3)} : (1-p)R \bullet F_i \leq 1\} \end{aligned}$$

But this is easy!

Rewriting and we are done

The following optimizations are equivalent

$$\min_p\{p : \quad \forall_{R\in SO(3)} : (1-p)R\bullet F_i \le 1\}$$
$$\max_p\{1-p : \quad \forall_{R\in SO(3)} : (1-p)R\bullet F_i \le 1\}$$
$$\max_{R\in SO(3)}\{R\bullet F_i\}$$

This last problem is easy to solve using Lagrange multipliers (KKT-conditions)

- We get $p = 45\%$!
- The optimal gate is the $\pi/8$-gate

Overview

1. Communication complexity
2. Clifford gates
3. 2-party simulation of Clifford circuits with one bit of communication
4. Simulation of 1-qubit unitary gates with depolarizing noise 45% by probabilistic mixture of Cliffords
5. Threshold for fault-tolerant quantum computing

Fault-tolerance threshold

1. Any function $f : \{0,1\}^{m_A} \times \{0,1\}^{m_B} \to \{0,1\}$ which can be computed by
   - perfect CNOT- and Clifford gates
   - 1-qubit-gates with depolarizing error $p \geq 45\%$

   has randomized communication complexity 1 bit
2. But communication complexity of IP is

$$C_\epsilon(IP_n) \in \Omega(n)$$

> Arbitrary 1-qubit gates with depolarizing error $\geq 45\%$ and (noise-free) Cliffords are not universal for fault-tolerant quantum computation.

In fact, only probabilistic parity functions can be computed.

What was the overall concept?

Distributed simulations of (quantum) circuits using little communication, and communication complexity lower bounds give upper bounds on thresholds for fault-tolerance.

Remarks and Open problems

- Generalization for quantum inputs possible
- How well can 2-qubit unitaries be simulated by Cliffords?
- Narrow and close the gap between upper bounds and lower bounds on $\hat{\theta}$.