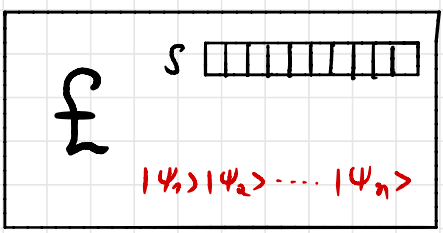
Quantum Money

Classical problems

Idea: quantum states cannot be cloned. Use this to prevent counterfeiting of money!

Tell the CRAZY Wiesner story...

Wiesner's scheme



No-cloning prevents duplication

But we also need verification

Bank prints bills consisting of:

(I) A (classical) serial number $s \in \{0,1\}^n$.

(II) n-qubit state $|\psi_1\rangle \cdots |\psi_n\rangle$.

- The qubits are unentangled.

- $\forall_{i \in [n]} \; |\psi_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

Bank maintains a database of $(s, |\psi\rangle)$ pairs.

By BBBW'82 this is not necessary: can pick secret key $k \in \{0,1\}^n$, and use $|\psi\rangle = PRG_k(s)$.

Verification

- Bank determines $|\psi\rangle$ from s.
- Bank measures each qubit in the right basis and checks it matches.

Security (Hacking the scheme)

Note that if we learn $|\psi\rangle$, we can make copies of it ∇

Observation: If we guess the basis, we learn the value.

If the guess is incorrect - we destroy it.

- Naive: guess the basis of each qubit at random;

works w.p. $1/2^n$. Each failure caught w.p. $\frac{1}{2}$

Attack

- Measure everything in the comp. basis

get $m \in \{0,1\}^n$.

- Duplicate (s, m).

- $\forall i \in [n]$ $\Pr[\text{both } (s,m) \text{ are verified}] =$

$$= \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{4} = \frac{5}{8}$$

$|\psi_i\rangle \in \{|0\rangle, |1\rangle\}$ $\quad$ $|\psi_i\rangle \in \{|+\rangle, |-\rangle\}$

A more clever attack succeeds w.p. $\left(\frac{3}{4}\right)^n$.

Wiesner claimed a matching $\left(\frac{3}{4}\right)^n$ bound.

Wrong argument, remained unquestioned for 25 years.

A Aronson asked about it on Stack Exchange

=> Molina, Vidick, Watrous prove it in '11.

Active research:

- Verification requires sending state to bank over a quantum channel [Gavinsky '11] showed classical comm. is enough
- 3rd party (i.e., Bank) verification

  [Aaronson '09]: public-key quantum money
- Interactive attacks and much more ▽

Ask me about projects...

Quantum Supremacy & Error-Correction

Important idea [John Preskill '12], with a problematic name...

Goal: Prove that a QC can perform a task that classical computers cannot.

Somewhat inherently problematic...

Question: Why not implement Shor's alg.?

Problems: - decoherence (can last several hours though)

- 2-qubit gates (CNOT) are hard to build

(But... doable!

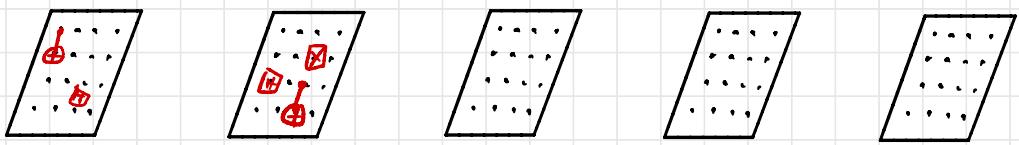
- grids  and adjacent CNOTs

(This we actually know how to do!)

Key problem: getting qubits to last through

Sequential applications of gates is hard.

(Parallelism is very important in practice)



Getting qubits that can last is more important than their number!

The ambitious solution: Error correcting codes

Classically we have this figured out...

[Chat about coding theory]

Quantumly, we can't even implement the simple repetition code (No-cloning thm...)

Still, remarkably, quantum codes are possible!

- The bit-flip code
- The sign-flip code
- The Shor code
- CSS codes, topological codes, stabiliser codes, ...

Furthermore, we need to compute over codes.

Luckily, we have the quantum fault tolerance theorem: For sufficiently small noise rate η, any m-gate quantum circuit can be implemented by an $m \cdot \text{polylog} m$ gate fault-tolerant circuit.

Why aren't we done? Several hundreds physical qubits for every single logical qubit...

So how do we prove quantum supremacy?

The Martinis (Google, UCSB) experiment:

1) Classically choose a random quantum circuit B

2) Set p_B to be the prob. dist. of $B|0\rangle^{\otimes n} \to$  .

3) Task: create a machine that draws from p_B.

4) Solve the problem by building a QC Q.

5) Show that $p_B \approx p_Q$.

6) Show that no classical comp C has $p_C \approx p_Q$.

7) Win a Nobel prize!

p_B is a Porter-Thomas distribution.

Idea: Rand. circuit $\approx$ random unitary U

Idea: $U|0\rangle$ = first column of $U \sim N(0, 1/N)$