Grover's algorithm

- Given quantum circuit Q_F implementing $F\colon \{0,1\}^n \to \{0,1\}$, want to find $x \in \{0,1\}^n$ such that $F(x) = 1$ or become confident none exists
- Key difference from Bernstein–Vazirani / Simon / Shor
  - F is not promised to have any special structure / pattern
- Assume hardest case $F(x) = 1$ for exactly one string $x^* \in \{0,1\}^n$
  - Quantum algorithm uses $\sqrt{N}$ queries

Extension

- What if $k = 2$?
  - After $\sqrt{N}/4$ iterations, find x_1^* or x_2^* with probability 5%
- Use different strategies if we know
  - 10% when $1 \leq K < 2$.
  - 5% when $2 \leq K < 4$.
  - …
  - $10\,\%/\log(N/16)$, when $N/32 \leq k < N/16$.
  - Random algorithm, when $k \geq N/16$.

Extension

- What if we don't know k?
  - Pretend $1 \leq k < 2$, and find x^*
  - Or pretend $2 \leq k < 4$, and find x^*
  - …
  - Or pretend $N/32 \leq k < N/16$, and find x^*
  - Or pretend $k \geq N/16$, and find x^* via random algorithm
- If found no x^*, conclude $F = 0$

Quantum query complexity and lower bounds

- Black-box query model
  - Given $F\colon \{0,1\}^n \to \{\text{labels}\}$ and quantum circuit Q_F (or $Q_F^{\pm}$) for F
  - Solve some problem about F
- Example: Grover's problem, labels are {0, 1}. Find x^* s.t. $F(x^*) = 1$ or determine no such x^* exists
- Query complexity model
  - Treat Q_F (or $Q_F^{\pm}$) as a black box
  - Cost of an algorithm is the number of applications of Q_F (queries)
  - All other computation is free

Why study this model?

- Usually the freee computation is cheap, say poly(n) gates per query, where $n = \log N$
- You can prove lower bounds (no-go / impossibility results)
- Example: Any quantum algorithm that solvers Grover's problem requires at least $c\sqrt{N}$ queries of Q_F

New notation for query complexity

- Given $F\colon \{0,1\}^n \to \{\text{labels}\}$, think of F as a string of length $N = 2^n$
  - $w = w_1 w_2 \dots w_N$, where
    $w_1 = F(00\dots00), w_2 = F(00\dots01), \dots, w_N = F(11\dots11)$
  - Classically, you query $i \in \{1,\dots,N\}$, get w_i
  - Quantumly, you can query superposition

Decision problems

- Focus on decision (yes or no) tasks, that is, {labels} = {0,1}
- Example: “Decision Grover”
  - Given $w \in \{0,1\}^N$ (unknown)
  - Can query superposition of $i \in \{1,2,\ldots,N\}$
  - Decide whether $w_i = 1$ for some i
  - Output YES / NO, that is, OR($w_1, \ldots, w_N$)
- Thank of a decision problem as $\varphi =$ (YES, NO)
  - YES = {w : output for w is YES} and NO = {w : output for w is NO}

Decision problems

- Example: Decision Grover
- Decision problems might be
  - Total: $YES \cup NO = \{\text{all strings}\}$
  - Partial: $YES \cup NO \subset \{\text{all strings}\}$ (i.e., have some promise on strings)

Lower bounds on quantum query complexity

- [Bennet–Berstein–Brassard–Vazirani ’96] Cost for “decision Grover” is at least $c\sqrt{N}$ queries
- [Ambrainis ’00] The basic adversary method
- [Høyer–Lee–Špálek ’07] General adversary method
- Special case of Basic adversary method
  - For φ = (YES, NO). Suppose $Y \subseteq$ YES and $Z \subseteq$ NO s.t.
    - For each $y \in Y$, there exist m strings $z \in Z$ s.t. $\mathrm{dist}(y, z) = 1$
    - For each $z \in Z$, there exist m' strings $y \in Y$ s.t. $\mathrm{dist}(y, z) = 1$
  - Then cost of quantum query algorithm to solve φ is at least $c\sqrt{mm'}$

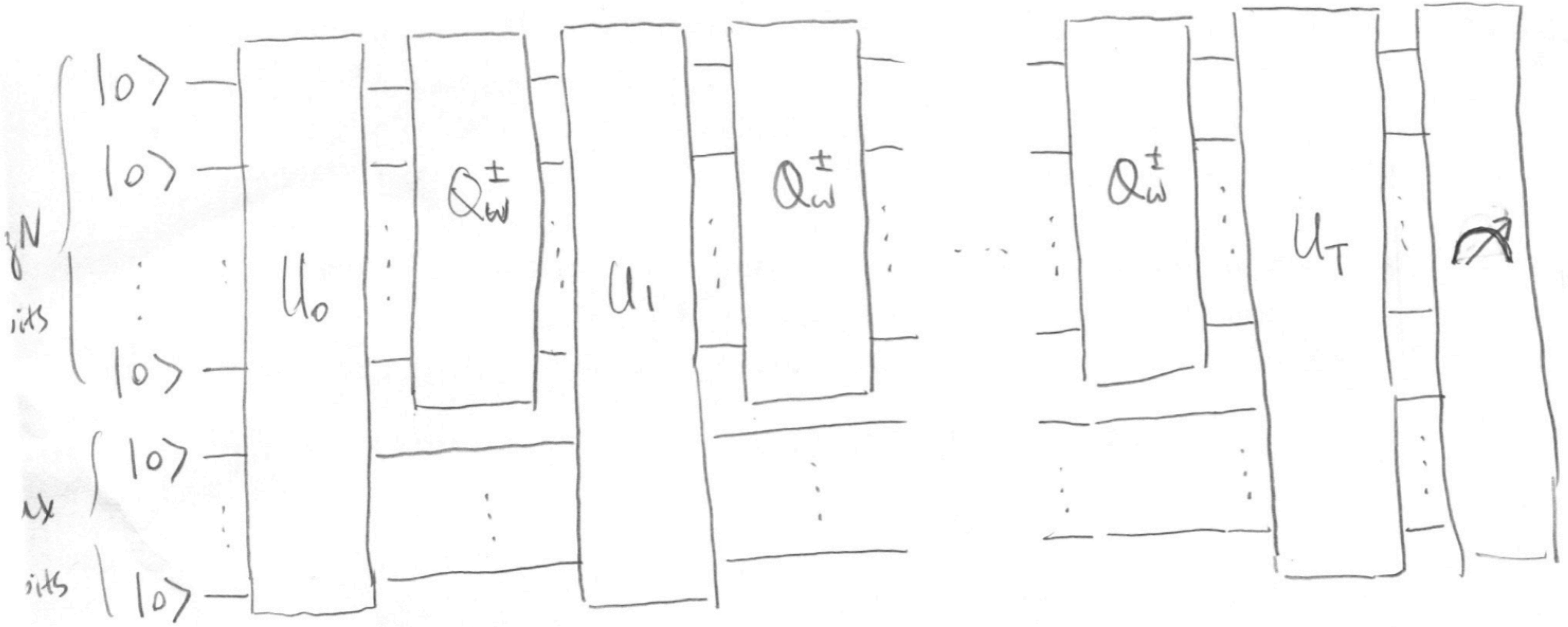
Applications

- Decision Grover
- Decide if w has $\geq k$ ones or $< k$ ones
- Partition w into $\sqrt{N}$ blocks of size $\sqrt{N}$. Decide if there is a one in each block.

Proof of special case

- Generic quantum query algorithm looks like:

- Here $Q_w^{\pm}$: $|i\rangle \mapsto (-1)^{w_i}|i\rangle$



- What does it imply when we say quantum query algorithm solves φ?
- Imagine an "adversary" picks $y \in$ YES and $z \in$ NO and runs the quantum query algorithm with $w = y$ and $w = z$ respectively
- The final joint states are respectively $|\Psi_y^{\text{final}}\rangle$ and $|\Psi_z^{\text{final}}\rangle$
- Goal: Discriminate the above two joint states
- In fact, we want $|\langle \Psi_y^{\text{final}} \mid \Psi_z^{\text{final}} \rangle| \leq 0.99$