Quantum rejection sampling

Maris Ozols
University of Waterloo

Martin Rötteler
NEC Laboratories America

Jérémie Roland
Université Libre de Bruxelles

[ITCS’12, arXiv:1103.2774]
Introduction

- (Classical) rejection sampling
  - Algorithmic tool introduced by von Neumann (1951)
  - Can be used to sample from arbitrary distributions
  - Numerous applications: * Metropolis algorithm [MRRTT53]
    - Monte-Carlo simulations
    - optimization (simulated annealing)
    - etc...

- Quantum rejection sampling
  - Natural quantum analogue: probabilities $\rightarrow$ amplitudes
  - New algorithmic tool
  - Applications: * Linear system of equations [HHL09]
    - Quantum Metropolis algorithm
    - Boolean hidden shift problem
Classical resampling problem

Setup:

- $P$ and $S$: two probability distributions

Resampling problem

Given the ability to sample according to $P$, produce a sample distributed according to $S$. 

\[ k \sim p_k \rightarrow \text{Accept/reject?} \rightarrow k \sim s_k \]
Rejection sampling

\[ P \xrightarrow{k \sim p_k} \text{Accept/reject?} \xrightarrow{\text{accept}} k \sim s_k \]

- \( \Pr[\text{accept } k] = \gamma \frac{s_k}{p_k} \)
- \( \gamma = \min_k \frac{p_k}{s_k} \)

Expected number of required samples: \( T = \frac{1}{\gamma} \)

- This is optimal [Letac75]
- Many applications in randomized algorithms
Quantum resampling problem

- Given access to a black box $O_\xi$ preparing a state
  \[ |\pi^\xi\rangle = \sum_k \pi_k |\xi_k\rangle |k\rangle \]
  known amplitudes unknown states

- Prepare the state
  \[ |\sigma^\xi\rangle = \sum_k \sigma_k |\xi_k\rangle |k\rangle \]
  different amplitudes same states

- Question: How many calls to $O_\xi$ are necessary?

- Tool: Query complexity
Classical query complexity

- Function $f(x)$, where $x = (x_1, \ldots, x_n)$
- Oracle $O_x : i \rightarrow x_i$
- Goal: Compute $f(x)$ given black-box access to $O_x$

Randomized query complexity $R_\varepsilon(f)$

Minimum $\#$ calls to $O_x$ necessary to compute $f(x)$ with success probability $(1 - \varepsilon)$
Quantum query complexity

Different quantum extensions:

1. Can query $O_x$ in superposition $\Rightarrow Q_\varepsilon(f) \leq R_\varepsilon(f)$

2. Instead of computing a function $f(x)$, generate a quantum state $|\psi_x\rangle$

3. Oracle $O_\xi$ is a unitary that hides the label $\xi$ in a non-explicit way

Example: Quantum resampling
Quantum state generation

- Set of quantum states $\Psi = \{ |\psi_\xi\rangle : \xi \in X \}$
- Set of oracles $\mathcal{O} = \{ O_\xi : \xi \in X \}$
- Quantum state generation problem $\mathcal{P}$ defined by $(\Psi, \mathcal{O})$
- Goal: Generate $|\psi_\xi\rangle$ given black-box access to $O_\xi$

Quantum query complexity $Q_\varepsilon(\mathcal{P})$

Minimum # calls to $O_\xi$ necessary to generate a state $\sqrt{1-\varepsilon}|\psi_\xi\rangle|0\rangle + \sqrt{\varepsilon}|\text{error}_\xi\rangle$

work space
Quantum rejection sampling

- Use oracle $O_\xi$ to create the original state
  \[ O_\xi |0\rangle = \sum_k \pi_k |\xi_k\rangle |k\rangle \]

- Use control-rotation on an ancilla qubit
  \[ |0\rangle \rightarrow \sum_k |\xi_k\rangle |k\rangle \left( \sqrt{\pi_k^2 - |\alpha_k|^2} |0\rangle + \alpha_k |1\rangle \right) \]

- If we measure the ancilla and obtain $|1\rangle$ (“accept”):
  \[ \frac{1}{||\vec{\alpha}||} \sum_k \alpha_k |\xi_k\rangle |k\rangle \]

- OK if $\vec{\alpha}$ is close to $\vec{\sigma}$, more precisely:
  \[ \frac{\vec{\sigma} \cdot \vec{\alpha}}{||\vec{\alpha}||} \geq \sqrt{1 - \varepsilon} \]
Optimization

\[ \sum_{k} |\xi_k\rangle |k\rangle \left( \sqrt{|\pi_k|^2 - |\alpha_k|^2} |0\rangle + \alpha_k |1\rangle \right) \]

- We measure \(|1\rangle\) ("accept") with probability \(\|\vec{\alpha}\|^2\)
- Naive approach: repeat \(O(1/\|\vec{\alpha}\|^2)\) times
- Using amplitude amplification: reduce to \(O(1/\|\vec{\alpha}\|)\)
- Optimizing \(\vec{\alpha}\) : Semidefinite program

Maximize \(\|\vec{\alpha}\|\) subject to \(0 \leq \alpha_k \leq \pi_k \quad \forall \, k\)
\[
\frac{\vec{\sigma} \cdot \vec{\alpha}}{\|\vec{\alpha}\|} \geq \sqrt{1 - \varepsilon}
\]

[BrassardHøyerMoscaTapp00]
Optimal solution

Let $\alpha_k(\gamma) = \min\{\pi_k, \gamma\sigma_k\}$

We take $\tilde{\gamma} = \max \gamma$ such that $\frac{\tilde{\sigma} \cdot \tilde{\alpha}(\gamma)}{\|\tilde{\alpha}(\gamma)\|} \geq \sqrt{1 - \varepsilon}$

We can prove that this leads to an optimal algorithm

Matching lower bound uses automorphism principle with $G = \mathbb{Z}_2^n \times U(N - 1)$

Theorem

$Q_\varepsilon(Q\text{Sampling}_{\tilde{\pi} \rightarrow \tilde{\sigma}}) = \Theta(1/\|\tilde{\alpha}(\tilde{\gamma})\|)$
Applications

- **Linear system of equations** [HHL09]
  - QRS was used implicitly

- **Quantum Metropolis algorithm**
  - Improvement on the original algorithm [TOVPV11]

- **Boolean hidden shift problem**
  - New algorithm!
Linear system of equations

Setup:

- Invertible \( d \times d \) matrix \( A \)
- Vector \( |b\rangle \in \mathbb{C}^d \)

Quantum linear equations problem

Prepare the state \( |x\rangle \) such that

\[
A|x\rangle = |b\rangle
\]

Main idea: use quantum phase estimation (QPE) [Kitaev95,CEMM97] + quantum rejection sampling (QRS)
Algorithm

Let $|b\rangle = \sum_k b_k |\psi_k\rangle$, where

- $|\psi_k\rangle$ are the eigenstates of $A$
- $\lambda_k$ are the corresponding eigenvalues

Use QPE to prepare

$$|b\rangle = \sum_k b_k |\psi_k\rangle |\lambda_k\rangle$$

Use QRS to get

$$\sum_k b_k \lambda_k^{-1} |\psi_k\rangle |\lambda_k\rangle$$

- Known amplitude (ratios): $\lambda_k^{-1}$
- Unknown states: $|\psi_k\rangle$

Undo phase estimation to obtain

$$|x\rangle = \sum_k b_k \lambda_k^{-1} |\psi_k\rangle = A^{-1} |b\rangle$$
Quantum Metropolis algorithm

Setup:

- Hamiltonian $H$
  - Eigenstates $|\psi_k\rangle$
  - Eigenenergies $E_k$
- Inverse temperature $\beta$

Metropolis sampling problem
Prepare the thermal state $\sum_k p_k |\psi_k\rangle \langle \psi_k|$, where $p_k \sim \exp(-\beta E_k)$ is the Gibbs distribution
Classical solution

- If $H$ is diagonal (= classical)
  - Eigenstates $|\psi_k\rangle$ are known
  - Eigenenergy $E_k$ can be efficiently computed from $|\psi_k\rangle$

- Start from a random $|\psi_k\rangle$

- Apply a “kick” to get another $|\psi_l\rangle$

- Compute the energies $E_k$ and $E_l$
  - If $E_l \leq E_k$, accept the move
  - If $E_l > E_k$, accept only with probability $\exp(\beta(E_k - E_l))$

- Repeat
Quantum Metropolis algorithm

- If $H$ is not diagonal (=quantum)
  - Eigenstates $|\psi_k\rangle$ and eigenergies $E_k$ are not known to start with
  - But: we can project onto the $|\psi_k\rangle$-basis and get the corresponding $E_k$ by using quantum phase estimation (QPE).

- Prepare a random $|\psi_k\rangle$ using QPE (and record $E_k$)
- Apply a “kick” (random unitary gate)
- Use QPE to project on another $|\psi_l\rangle$ (and record $E_l$)
- Compare the energies $E_k$ and $E_l$
  - If $E_l \leq E_k$, accept the move
  - If $E_l > E_k$, accept only with probability $\exp(-\beta(E_l - E_k))$
Quantum Metropolis algorithm

Problem:

- Rejected moves require to revert the state from $|\psi_i\rangle$ to $|\psi_k\rangle$
- We cannot keep a copy of $|\psi_k\rangle$ (requires to clone an unknown state!)

Two solutions:

- Temme et al. [TOVPV11] propose a “rewinding” technique to revert to $|\psi_k\rangle$, based on a series of projective measurements.
- Use quantum rejection sampling! Equivalent to amplifying accepted moves, therefore avoiding having to revert moves at all.
Boolean hidden shift

Setup:

- \( f(x) \): (known) Boolean function
- \( f_s(x) = f(x + s) \), with an (unknown) shift \( s \in \{0, 1\}^n \)

Boolean hidden shift problem

Given black-box access to \( f_s(x) \), find the hidden shift \( s \)
Special cases

- Delta function $f(x) = \delta_{x x_0}$
  - $\square$ = Grover’s search problem
  - $\square$ Requires $\Theta(\sqrt{2^n})$ queries [Grover96]

- Bent functions
  - $\square$ = Functions with flat Fourier spectrum
  - $\square$ Can be solved with 1 query! [Rötteler10]

- What about other functions???
New algorithm based on QRS

- Use the following circuit, where
  - $H$ is the Hadamard transform
  - $O_{f_s}$ is the black box for $f_s$, acting as $O_{f_s} |x\rangle = (-1)^{f_s(x)} |x\rangle$

$$
\begin{align*}
|0\rangle &\quad H \quad H \\
|0\rangle &\quad H \quad O_{f_s} \quad H \\
\vdots &\quad \vdots \quad \vdots \\
|0\rangle &\quad H \quad H \\
\end{align*}

\begin{align*}
\sum_w (-1)^{w\cdot s} \hat{f}(w) |w\rangle
\end{align*}
$$

- Use QRS to produce the state $\frac{1}{\sqrt{2^n}} \sum_w (-1)^{w\cdot s} |w\rangle$
  - Known amplitudes = Fourier coefficients $\hat{f}(w)$
  - Unknown “states” = phases $(-1)^{w\cdot s}$

- Use a final Fourier transform $H^\otimes n$ to get $|s\rangle$
Wrap-up

☐ Rejection sampling has found many applications in classical computing

☐ Quantum rejection sampling could be as useful for quantum computing!

☐ Example: 3 diverse applications
  ☐ Linear system of equations [HarrowHassidimLloyd09]
  ☐ Quantum Metropolis algorithm
  ☐ Boolean hidden shift problem
Outlook

- Other applications
  - Amplifying QMA witnesses [MarriottWatrous05,NagajWocjanZhang09]
  - Preparing PEPS states [SchwarzTemmeVerstraete11]
  - ???
  
- Adversary method for this extended model of quantum query complexity?
  - Non-trivial error dependence
  - Infinite-size adversary matrices

Support: