Quantum rejection sampling

Maris Ozols
University of Waterloo
Institute for Quantum Computing

Martin Rötteler
NEC Laboratories America

Jérémie Roland
Université Libre de Bruxelles

arXiv:1103.2774

Motivation

We started with...

Boolean hidden shift problem

- Could be useful for breaking cryptosystems (LFSRs)
- Potential insights into the dihedral hidden subgroup problem

Motivation

We started with...

Boolean hidden shift problem

- Could be useful for breaking cryptosystems (LFSRs)
- Potential insights into the dihedral hidden subgroup problem

...but ended up with

A useful primitive for constructing quantum algorithms:

- Quantum algorithm for linear systems of equations [HHL09]
- Quantum Metropolis algorithm [TOVPV11]
- Preparing PEPS [STV11]
- more...

Resampling

Classical $\boldsymbol{p} \to \boldsymbol{s}$ resampling problem

- **Given:** $\boldsymbol{p}, \boldsymbol{s} \in \mathbb{R}^n_+$ with $\|\boldsymbol{p}\|_1 = \|\boldsymbol{s}\|_1 = 1$
  Ability to sample from distribution $\boldsymbol{p}$
- **Task:** Sample from distribution $\boldsymbol{s}$

Resampling

Classical $\boldsymbol{p} \to \boldsymbol{s}$ resampling problem

- **Given:** $\boldsymbol{p}, \boldsymbol{s} \in \mathbb{R}_+^n$ with $\|\boldsymbol{p}\|_1 = \|\boldsymbol{s}\|_1 = 1$
  Ability to sample from distribution $\boldsymbol{p}$
- **Task:** Sample from distribution $\boldsymbol{s}$
- **Question:** How many samples from $\boldsymbol{p}$ we need to prepare one sample from $\boldsymbol{s}$?

Resampling

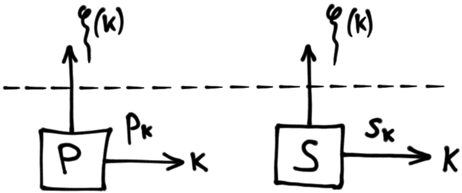
Classical $\boldsymbol{p} \to \boldsymbol{s}$ resampling problem

- **Given:** $\boldsymbol{p}, \boldsymbol{s} \in \mathbb{R}_+^n$ with $\|\boldsymbol{p}\|_1 = \|\boldsymbol{s}\|_1 = 1$
  Ability to sample from distribution $\boldsymbol{p}$
- **Task:** Sample from distribution $\boldsymbol{s}$
- **Question:** How many samples from $\boldsymbol{p}$ we need to prepare one sample from $\boldsymbol{s}$?

Resampling

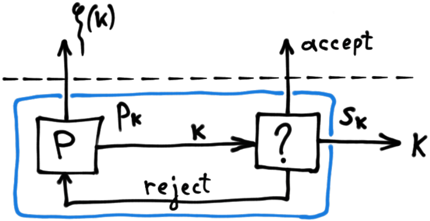
Classical $\boldsymbol{p} \to \boldsymbol{s}$ resampling problem

- **Given:** $\boldsymbol{p}, \boldsymbol{s} \in \mathbb{R}_+^n$ with $\|\boldsymbol{p}\|_1 = \|\boldsymbol{s}\|_1 = 1$
  Ability to sample from distribution $\boldsymbol{p}$
- **Task:** Sample from distribution $\boldsymbol{s}$
- **Question:** How many samples from $\boldsymbol{p}$ we need to prepare one sample from $\boldsymbol{s}$?
- **Note:** Samples are pairs $(k, \xi(k))$ where $\xi(k)$ is not accessible



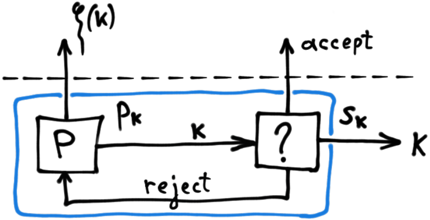
Classical rejection sampling

Algorithm



Classical rejection sampling

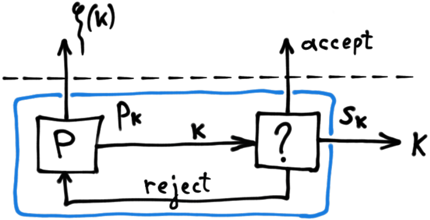
Algorithm



- Accept k with probability $\gamma s_k / p_k$

Classical rejection sampling

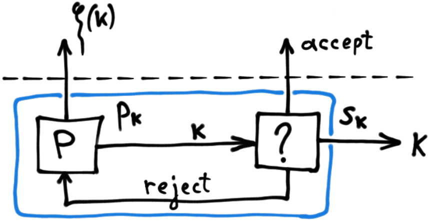
Algorithm

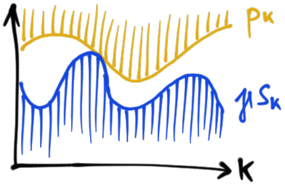


- Accept k with probability $\gamma s_k / p_k$
- Avg. prob. to accept: $\sum_k p_k \cdot \gamma s_k / p_k = \gamma$

Classical rejection sampling

Algorithm

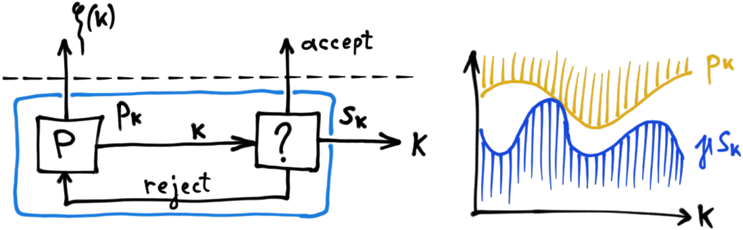




- Accept k with probability $\gamma s_k / p_k \ \leq 1$
- Avg. prob. to accept: $\sum_k p_k \cdot \gamma s_k / p_k = \gamma$

Classical rejection sampling

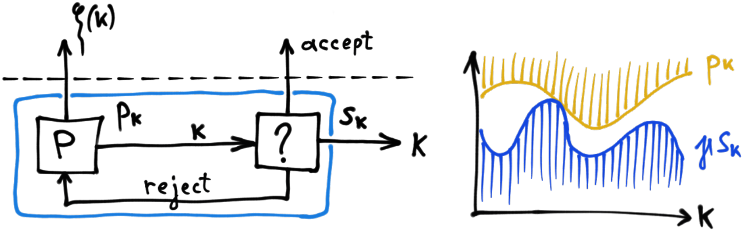
Algorithm



- Accept k with probability $\gamma s_k/p_k \ \leq 1$, so $\gamma = \min_k p_k/s_k$
- Avg. prob. to accept: $\sum_k p_k \cdot \gamma s_k/p_k = \gamma$

Classical rejection sampling

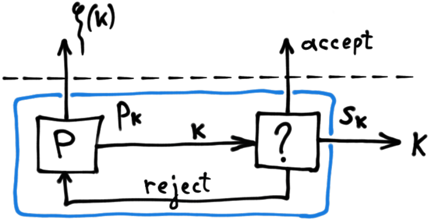
Algorithm

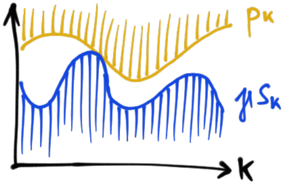


- Accept k with probability $\gamma s_k / p_k \; \leq 1$, so $\gamma = \min_k p_k / s_k$
- Avg. prob. to accept: $\sum_k p_k \cdot \gamma s_k / p_k = \gamma$
- Query complexity: $\Theta(1/\gamma)$

Classical rejection sampling

Algorithm

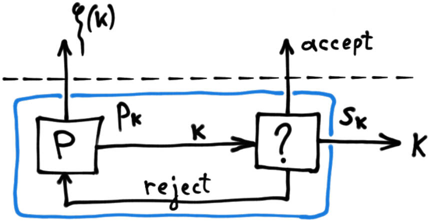


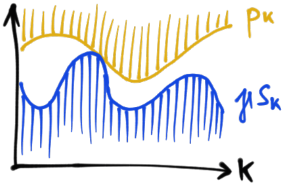


- Accept k with probability $\gamma s_k/p_k \leq 1$, so $\gamma = \min_k p_k/s_k$
- Avg. prob. to accept: $\sum_k p_k \cdot \gamma s_k/p_k = \gamma$
- Query complexity: $\Theta(1/\gamma)$
- Introduced by von Neumann in 1951

Classical rejection sampling

Algorithm





- Accept k with probability $\gamma s_k / p_k \ \leq 1$, so $\gamma = \min_k p_k / s_k$
- Avg. prob. to accept: $\sum_k p_k \cdot \gamma s_k / p_k = \gamma$
- Query complexity: $\Theta(1/\gamma)$
- Introduced by von Neumann in 1951
- Has numerous applications:
  - Metropolis algorithm [MRRTT53]
  - Monte-Carlo simulations
  - optimization (simulated annealing), etc.

Quantum resampling

Quantum $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ resampling problem

- **Given:** $\boldsymbol{\pi}, \boldsymbol{\sigma} \in \mathbb{R}_+^n$ with $\|\boldsymbol{\pi}\|_2 = \|\boldsymbol{\sigma}\|_2 = 1$
  Oracle for preparing $|\pi\rangle = \sum_{k=1}^n \pi_k |k\rangle |\xi(k)\rangle$

Quantum resampling

Quantum $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ resampling problem

- **Given:** $\boldsymbol{\pi}, \boldsymbol{\sigma} \in \mathbb{R}_+^n$ with $\|\boldsymbol{\pi}\|_2 = \|\boldsymbol{\sigma}\|_2 = 1$
  Oracle for preparing $|\pi\rangle = \sum_{k=1}^n \pi_k |k\rangle|\xi(k)\rangle$
- **Task:** Prepare $|\sigma\rangle = \sum_{k=1}^n \sigma_k |k\rangle|\xi(k)\rangle$

Quantum resampling

Quantum $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ resampling problem

- **Given:** $\boldsymbol{\pi}, \boldsymbol{\sigma} \in \mathbb{R}_+^n$ with $\|\boldsymbol{\pi}\|_2 = \|\boldsymbol{\sigma}\|_2 = 1$
  Oracle for preparing $|\pi\rangle = \sum_{k=1}^n \pi_k |k\rangle|\xi(k)\rangle$
- **Task:** Prepare $|\sigma\rangle = \sum_{k=1}^n \sigma_k |k\rangle|\xi(k)\rangle$
- **Question:** How many $|\pi\rangle$s we need to produce one $|\sigma\rangle$?

Quantum resampling

Quantum $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ resampling problem

- **Given:** $\boldsymbol{\pi}, \boldsymbol{\sigma} \in \mathbb{R}_+^n$ with $\|\boldsymbol{\pi}\|_2 = \|\boldsymbol{\sigma}\|_2 = 1$
  Oracle for preparing $|\pi\rangle = \sum_{k=1}^n \pi_k |k\rangle|\xi(k)\rangle$
- **Task:** Prepare $|\sigma\rangle = \sum_{k=1}^n \sigma_k |k\rangle|\xi(k)\rangle$
- **Question:** How many $|\pi\rangle$s we need to produce one $|\sigma\rangle$?
- **Note:** States $|\xi(k)\rangle$ are not known

Quantum resampling

Quantum $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ resampling problem

- **Given:** $\boldsymbol{\pi}, \boldsymbol{\sigma} \in \mathbb{R}_+^n$ with $\|\boldsymbol{\pi}\|_2 = \|\boldsymbol{\sigma}\|_2 = 1$
  Oracle for preparing $|\pi\rangle = \sum_{k=1}^n \pi_k |k\rangle |\xi(k)\rangle$
- **Task:** Prepare $|\sigma\rangle = \sum_{k=1}^n \sigma_k |k\rangle |\xi(k)\rangle$
- **Question:** How many $|\pi\rangle$s we need to produce one $|\sigma\rangle$?
- **Note:** States $|\xi(k)\rangle$ are not known

Main theorem (exact case)

The quantum query complexity of the exact $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ quantum resampling problem is $\Theta(1/\gamma)$ where $\gamma = \min_k |\pi_k/\sigma_k|$

Quantum resampling

Quantum $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ resampling problem

- **Given:** $\boldsymbol{\pi}, \boldsymbol{\sigma} \in \mathbb{R}_+^n$ with $\|\boldsymbol{\pi}\|_2 = \|\boldsymbol{\sigma}\|_2 = 1$
  Oracle for preparing $|\pi\rangle = \sum_{k=1}^n \pi_k |k\rangle|\xi(k)\rangle$
- **Task:** Prepare $|\sigma\rangle = \sum_{k=1}^n \sigma_k |k\rangle|\xi(k)\rangle$
- **Question:** How many $|\pi\rangle$s we need to produce one $|\sigma\rangle$?
- **Note:** States $|\xi(k)\rangle$ are not known

Main theorem (exact case)

The quantum query complexity of the exact $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ quantum resampling problem is $\Theta(1/\gamma)$ where $\gamma = \min_k |\pi_k/\sigma_k|$

Approximate preparation

Task: Prepare $\sqrt{1-\varepsilon}|\sigma\rangle + \sqrt{\varepsilon}|\mathrm{error}\rangle$

Quantum resampling

Quantum $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ resampling problem

- **Given:** $\boldsymbol{\pi}, \boldsymbol{\sigma} \in \mathbb{R}_+^n$ with $\|\boldsymbol{\pi}\|_2 = \|\boldsymbol{\sigma}\|_2 = 1$
  Oracle for preparing $|\pi\rangle = \sum_{k=1}^n \pi_k |k\rangle |\xi(k)\rangle$
- **Task:** Prepare $|\sigma\rangle = \sum_{k=1}^n \sigma_k |k\rangle |\xi(k)\rangle$
- **Question:** How many $|\pi\rangle$s we need to produce one $|\sigma\rangle$?
- **Note:** States $|\xi(k)\rangle$ are not known

Main theorem (exact case)

The quantum query complexity of the exact $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ quantum resampling problem is $\Theta(1/\gamma)$ where $\gamma = \min_k |\pi_k/\sigma_k|$

Approximate preparation

Task: Prepare $\sqrt{1-\varepsilon}|\sigma\rangle + \sqrt{\varepsilon}|\mathrm{error}\rangle$
$\iff$ Prepare $|\delta\rangle$ with $\boldsymbol{\sigma} \cdot \boldsymbol{\delta} \geq \sqrt{1-\varepsilon}$

Quantum rejection sampling algorithm

1. Use the oracle to prepare
$$|0\rangle|\pi\rangle = |0\rangle \sum_{k=1}^{n} \pi_k |k\rangle |\xi(k)\rangle$$

Quantum rejection sampling algorithm

1. Use the oracle to prepare
$$|0\rangle|\pi\rangle = |0\rangle \sum_{k=1}^{n} \pi_k |k\rangle|\xi(k)\rangle$$
2. Pick some $\boldsymbol{\delta} \in \mathbb{R}_+^n$ and rotate the state in the first register:
$$\sum_{k=1}^{n} \big(\sqrt{|\pi_k|^2 - |\delta_k|^2}\,|0\rangle + \delta_k\,|1\rangle\big)|k\rangle|\xi(k)\rangle$$

Quantum rejection sampling algorithm

1. Use the oracle to prepare

$$|0\rangle|\pi\rangle = |0\rangle \sum_{k=1}^{n} \pi_k |k\rangle|\xi(k)\rangle$$

2. Pick some $\boldsymbol{\delta} \in \mathbb{R}_+^n$ and rotate the state in the first register:

$$\sum_{k=1}^{n} \big(\sqrt{|\pi_k|^2 - |\delta_k|^2}\, |0\rangle + \delta_k\, |1\rangle \big) |k\rangle|\xi(k)\rangle$$

3. Measure the first register:

Quantum rejection sampling algorithm

1. Use the oracle to prepare
$$|0\rangle|\pi\rangle = |0\rangle \sum_{k=1}^{n} \pi_k |k\rangle|\xi(k)\rangle$$
2. Pick some $\boldsymbol{\delta} \in \mathbb{R}_+^n$ and rotate the state in the first register:
$$\sum_{k=1}^{n} \Big(\sqrt{|\pi_k|^2 - |\delta_k|^2}\,|0\rangle + \delta_k\,|1\rangle \Big) |k\rangle|\xi(k)\rangle$$
3. Measure the first register:
   - w.p. $\|\boldsymbol{\delta}\|_2^2$ the state collapses to
   $$\sum_{k=1}^{n} \hat{\delta}_k |k\rangle|\xi(k)\rangle$$
   where $\hat{\delta}_k = \delta_k / \|\boldsymbol{\delta}\|_2$

Quantum rejection sampling algorithm

Subroutine

$$\text{one copy of } |\pi\rangle \quad \mapsto \quad \sum_{k=1}^{n} \hat{\delta}_k |k\rangle|\xi(k)\rangle \quad \text{w.p.} \quad \|\boldsymbol{\delta}\|_2^2$$

Quantum rejection sampling algorithm

Subroutine

$$\text{one copy of } |\pi\rangle \quad \mapsto \quad \sum_{k=1}^{n} \hat{\delta}_k |k\rangle|\xi(k)\rangle \quad \text{w.p.} \quad \|\boldsymbol{\delta}\|_2^2$$

Amplification

- **Naïve:** repeat $1/\|\boldsymbol{\delta}\|_2^2$ times to succeed w.p. ≈ 1

Quantum rejection sampling algorithm

Subroutine

$$\text{one copy of } |\pi\rangle \quad \mapsto \quad \sum_{k=1}^{n} \hat{\delta}_k |k\rangle |\xi(k)\rangle \quad \text{w.p.} \quad \|\boldsymbol{\delta}\|_2^2$$

Amplification

- **Naïve:** repeat $1/\|\boldsymbol{\delta}\|_2^2$ times to succeed w.p. ≈ 1
- **Quantum:** $1/\|\boldsymbol{\delta}\|_2$ repetitions of amplitude amplification suffice [BHMT00]

Quantum rejection sampling algorithm

Subroutine

$$\text{one copy of } |\pi\rangle \quad \mapsto \quad \sum_{k=1}^{n} \hat{\delta}_k |k\rangle|\xi(k)\rangle \quad \text{w.p.} \quad \|\boldsymbol{\delta}\|_2^2$$

Amplification

- **Naïve:** repeat $1/\|\boldsymbol{\delta}\|_2^2$ times to succeed w.p. ≈ 1
- **Quantum:** $1/\|\boldsymbol{\delta}\|_2$ repetitions of amplitude amplification suffice [BHMT00]

Summary

We can prepare $\sum_{k=1}^{n} \hat{\delta}_k |k\rangle|\xi(k)\rangle$ with $O(1/\|\boldsymbol{\delta}\|_2)$ quantum queries

Quantum rejection sampling algorithm

Subroutine

$$\text{one copy of } |\pi\rangle \quad \mapsto \quad \sum_{k=1}^{n} \hat{\delta}_k |k\rangle |\xi(k)\rangle \quad \text{w.p.} \quad \|\boldsymbol{\delta}\|_2^2$$

Amplification

- **Naïve:** repeat $1/\|\boldsymbol{\delta}\|_2^2$ times to succeed w.p. ≈ 1
- **Quantum:** $1/\|\boldsymbol{\delta}\|_2$ repetitions of amplitude amplification suffice [BHMT00]

Summary

We can prepare $\sum_{k=1}^{n} \hat{\delta}_k |k\rangle |\xi(k)\rangle$ with $O(1/\|\boldsymbol{\delta}\|_2)$ quantum queries

Goal: preparing $|\sigma\rangle$

- What $\boldsymbol{\delta}$ should we choose?
- We are done if $\boldsymbol{\sigma} \cdot \hat{\boldsymbol{\delta}} \geq \sqrt{1-\varepsilon}$ where $\hat{\boldsymbol{\delta}} = \boldsymbol{\delta}/\|\boldsymbol{\delta}\|_2$

Optimization

Problem

- $\min_{\boldsymbol{\delta}} 1/\|\boldsymbol{\delta}\|_2$ s.t. $\boldsymbol{\sigma} \cdot \hat{\boldsymbol{\delta}} \geq \sqrt{1-\varepsilon}$

Optimization

$$\sum_{k=1}^{n} \left(\sqrt{|\pi_k|^2 - |\delta_k|^2}\, |0\rangle + \delta_k\, |1\rangle \right) |k\rangle |\xi(k)\rangle$$

Problem

- $\min_{\boldsymbol{\delta}} 1/\|\boldsymbol{\delta}\|_2$ s.t. $\boldsymbol{\sigma} \cdot \hat{\boldsymbol{\delta}} \geq \sqrt{1-\varepsilon}$ and $0 \leq \delta_k \leq \pi_k$

Optimization

$$\sum_{k=1}^{n} \left(\sqrt{|\pi_k|^2 - |\delta_k|^2}\,|0\rangle + \delta_k\,|1\rangle\right)|k\rangle|\xi(k)\rangle$$

Problem

- $\min_{\boldsymbol{\delta}} 1/\|\boldsymbol{\delta}\|_2$ s.t. $\boldsymbol{\sigma} \cdot \hat{\boldsymbol{\delta}} \geq \sqrt{1-\varepsilon}$ and $0 \leq \delta_k \leq \pi_k$
- This can be stated as an SDP

Optimization

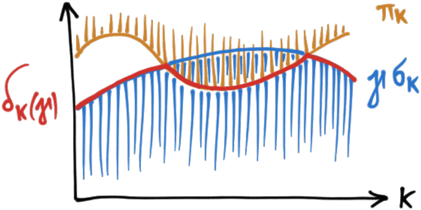
$$\sum_{k=1}^{n} \left(\sqrt{|\pi_k|^2 - |\delta_k|^2}\,|0\rangle + \delta_k\,|1\rangle\right)|k\rangle|\xi(k)\rangle$$

Problem

- $\min_{\boldsymbol{\delta}} 1/\|\boldsymbol{\delta}\|_2$ s.t. $\boldsymbol{\sigma} \cdot \hat{\boldsymbol{\delta}} \geq \sqrt{1-\varepsilon}$ and $0 \leq \delta_k \leq \pi_k$
- This can be stated as an SDP

Optimal solution

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



Optimization

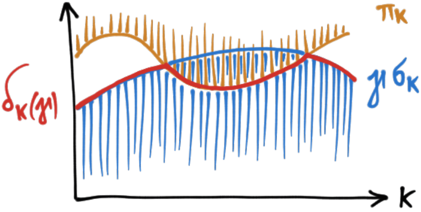
$$\sum_{k=1}^{n} \left(\sqrt{|\pi_k|^2 - |\delta_k|^2}\,|0\rangle + \delta_k\,|1\rangle\right)|k\rangle|\xi(k)\rangle$$

Problem

- $\min_{\boldsymbol{\delta}} 1/\|\boldsymbol{\delta}\|_2$ s.t. $\boldsymbol{\sigma} \cdot \hat{\boldsymbol{\delta}} \geq \sqrt{1-\varepsilon}$ and $0 \leq \delta_k \leq \pi_k$
- This can be stated as an SDP

Optimal solution

- Let $\delta_k(\gamma) = \min\{\pi_k, \gamma\sigma_k\}$
- Choose $\bar{\gamma} = \max \gamma$ s.t. $\boldsymbol{\sigma} \cdot \hat{\boldsymbol{\delta}}(\gamma) \geq \sqrt{1-\varepsilon}$



Optimization

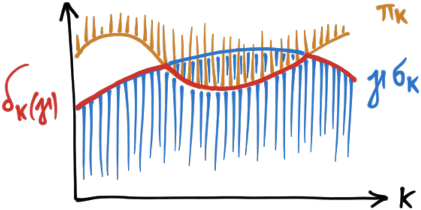
$$\sum_{k=1}^{n}\left(\sqrt{|\pi_k|^2 - |\delta_k|^2}\,|0\rangle + \delta_k\,|1\rangle\right)|k\rangle|\xi(k)\rangle$$

Problem

- $\min_{\boldsymbol{\delta}} 1/\|\boldsymbol{\delta}\|_2$ s.t. $\boldsymbol{\sigma} \cdot \hat{\boldsymbol{\delta}} \geq \sqrt{1-\varepsilon}$ and $0 \leq \delta_k \leq \pi_k$
- This can be stated as an SDP

Optimal solution

- Let $\delta_k(\gamma) = \min\{\pi_k, \gamma\sigma_k\}$
- Choose $\bar{\gamma} = \max \gamma$ s.t. $\boldsymbol{\sigma} \cdot \hat{\boldsymbol{\delta}}(\gamma) \geq \sqrt{1-\varepsilon}$



Main theorem

The quantum query complexity of the ε-approximate $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ quantum resampling problem is $\Theta(1/\|\boldsymbol{\delta}(\bar{\gamma})\|_2)$

Applications

Implicit use

- Synthesis of quantum states [Grover, 2000]
- Linear systems of equations [Harrow, Hassidim and Lloyd 2009]
- Fast amplification of QMA [Nagaj, Wocjan, Zhang, 2009]

Applications

Implicit use

- Synthesis of quantum states [Grover, 2000]
- Linear systems of equations [Harrow, Hassidim and Lloyd 2009]
- Fast amplification of QMA [Nagaj, Wocjan, Zhang, 2009]

New applications

- Speed up quantum Metropolis sampling algorithm by [Temme, Osborne, Vollbrecht, Poulin, Verstraete, 2011]
- New quantum algorithm for the hidden shift problem of any Boolean function

Applications

Implicit use

- Synthesis of quantum states [Grover, 2000]
- Linear systems of equations [Harrow, Hassidim and Lloyd 2009]
- Fast amplification of QMA [Nagaj, Wocjan, Zhang, 2009]

New applications

- Speed up quantum Metropolis sampling algorithm by [Temme, Osborne, Vollbrecht, Poulin, Verstraete, 2011]
- New quantum algorithm for the hidden shift problem of any Boolean function

Future applications

- Preparing PEPS [Schwarz, Temme, Verstraete, 2011]
- More...

Applications

Implicit use

- Synthesis of quantum states [Grover, 2000]
- Linear systems of equations [Harrow, Hassidim and Lloyd 2009]
- Fast amplification of QMA [Nagaj, Wocjan, Zhang, 2009]

New applications

- Speed up quantum Metropolis sampling algorithm by [Temme, Osborne, Vollbrecht, Poulin, Verstraete, 2011]
- New quantum algorithm for the hidden shift problem of any Boolean function

Future applications

- Preparing PEPS [Schwarz, Temme, Verstraete, 2011]
- More...

Boolean hidden shift problem (BHSP)

Problem

- **Given:** Complete knowledge of $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ and access to a black-box oracle for $f_s(x) := f(x + s)$

$$x \Rightarrow \blacksquare \Rightarrow f_s(x)$$

- **Determine:** The hidden shift s

Boolean hidden shift problem (BHSP)

Problem

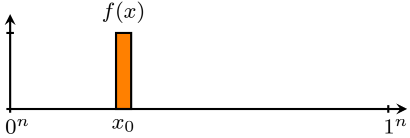
- **Given:** Complete knowledge of $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ and access to a black-box oracle for $f_s(x) := f(x+s)$

$$x \Rightarrow \blacksquare \Rightarrow f_s(x)$$

- **Determine:** The hidden shift s

Delta functions are hard

- $f(x) := \delta_{x,x_0}$



Boolean hidden shift problem (BHSP)

Problem

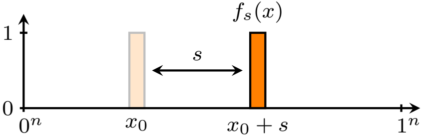
- **Given:** Complete knowledge of $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ and access to a black-box oracle for $f_s(x) := f(x+s)$

$$x \Rightarrow \blacksquare \Rightarrow f_s(x)$$

- **Determine:** The hidden shift s

Delta functions are hard

- $f(x) := \delta_{x,x_0}$



Boolean hidden shift problem (BHSP)

Problem

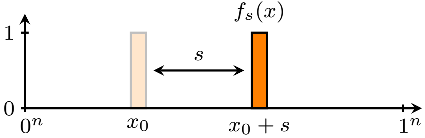
- **Given:** Complete knowledge of $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ and access to a black-box oracle for $f_s(x) := f(x+s)$

$$x \Rightarrow \blacksquare \Rightarrow f_s(x)$$

- **Determine:** The hidden shift s

Delta functions are hard

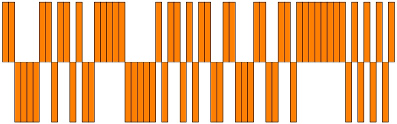
- $f(x) := \delta_{x,x_0}$
- Equivalent to Grover's search: $\Theta(\sqrt{2^n})$



Fourier transform of Boolean functions

The ± 1-function (normalized)

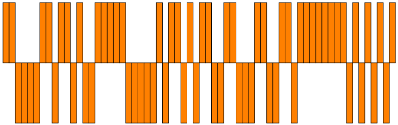
- $F(x) := \frac{1}{\sqrt{2^n}}(-1)^{f(x)}$



Fourier transform of Boolean functions

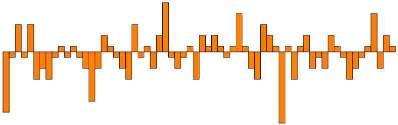
The ± 1-function (normalized)

- $F(x) := \frac{1}{\sqrt{2^n}}(-1)^{f(x)}$



Fourier transform

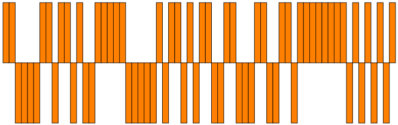
- $\hat{F}(w) := \langle w|H^{\otimes n}|F\rangle$



Fourier transform of Boolean functions

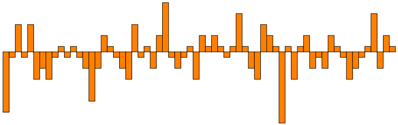
The ± 1-function (normalized)

- $F(x) := \frac{1}{\sqrt{2^n}}(-1)^{f(x)}$



Fourier transform

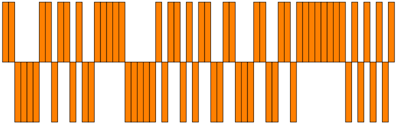
- $\hat{F}(w) := \langle w | H^{\otimes n} | F \rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{Z}_2^n} (-1)^{w \cdot x} F(x)$



Fourier transform of Boolean functions

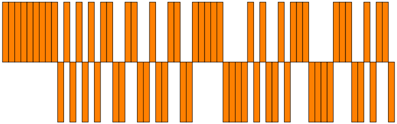
The ± 1-function (normalized)

- $F(x) := \frac{1}{\sqrt{2^n}}(-1)^{f(x)}$



Fourier transform

- $\hat{F}(w) := \langle w|H^{\otimes n}|F\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{Z}_2^n} (-1)^{w \cdot x} F(x)$



Function f is **bent** if $\forall w : |\hat{F}(w)| = \frac{1}{\sqrt{2^n}}$

Bent functions are easy

Preparing the "phase state"

- Phase oracle $O_{f_s} : |x\rangle \mapsto (-1)^{f_s(x)}|x\rangle$

Bent functions are easy

Preparing the "phase state"

- Phase oracle $O_{f_s} : |x\rangle \mapsto (-1)^{f_s(x)}|x\rangle$

$$|0\rangle^{\otimes n} \;-\!\!\boxed{H^{\otimes n}}\!\!-\!\!\boxed{O_{f_s}}\!\!-\!\!\boxed{H^{\otimes n}}\!\!-\; |\Phi(s)\rangle$$

- $|\Phi(s)\rangle := \sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}\hat{F}(w)|w\rangle$

Bent functions are easy

Preparing the "phase state"

- Phase oracle $O_{f_s} : |x\rangle \mapsto (-1)^{f_s(x)}|x\rangle$

$$|0\rangle^{\otimes n} \;-\!\boxed{H^{\otimes n}}\!-\!\boxed{O_{f_s}}\!-\!\boxed{H^{\otimes n}}\!-\; |\Phi(s)\rangle$$

- $|\Phi(s)\rangle := \sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}\hat{F}(w)|w\rangle$

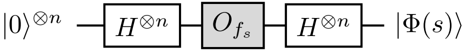
Algorithm [Rötteler'10]

- Prepare $|\Phi(s)\rangle$

Bent functions are easy

Preparing the "phase state"

- Phase oracle $O_{f_s} : |x\rangle \mapsto (-1)^{f_s(x)}|x\rangle$



- $|\Phi(s)\rangle := \sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \hat{F}(w) |w\rangle$

Algorithm [Rötteler'10]

- Prepare $|\Phi(s)\rangle$
- Apply $D := \mathrm{diag}\left(\frac{|\hat{F}(w)|}{\hat{F}(w)}\right)$ [Curtis & Meyer'04] and get $D|\Phi(s)\rangle = \sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} |\hat{F}(w)| |w\rangle$

Bent functions are easy

Preparing the "phase state"

- Phase oracle $O_{f_s} : |x\rangle \mapsto (-1)^{f_s(x)}|x\rangle$

$$|0\rangle^{\otimes n} \; - \boxed{H^{\otimes n}} - \boxed{O_{f_s}} - \boxed{H^{\otimes n}} - \; |\Phi(s)\rangle$$

- $|\Phi(s)\rangle := \sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}\hat{F}(w)|w\rangle$

Algorithm [Rötteler'10]

- Prepare $|\Phi(s)\rangle$
- Apply $D := \mathrm{diag}\left(\frac{|\hat{F}(w)|}{\hat{F}(w)}\right)$ [Curtis & Meyer'04] and get $D|\Phi(s)\rangle = \sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}|\hat{F}(w)||w\rangle$
- If f is bent then $H^{\otimes n}D|\Phi(s)\rangle = |s\rangle$

Bent functions are easy

Preparing the "phase state"

- Phase oracle $O_{f_s} : |x\rangle \mapsto (-1)^{f_s(x)}|x\rangle$

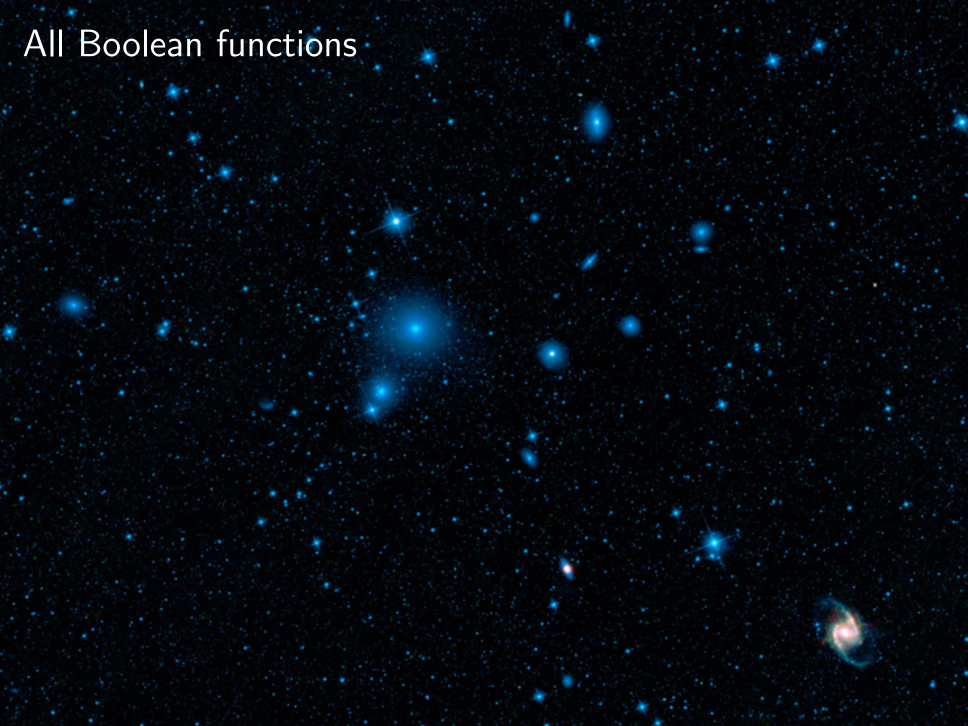
$$|0\rangle^{\otimes n} \; — \boxed{H^{\otimes n}} — \boxed{O_{f_s}} — \boxed{H^{\otimes n}} — \; |\Phi(s)\rangle$$

- $|\Phi(s)\rangle := \sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \hat{F}(w) |w\rangle$

Algorithm [Rötteler'10]

- Prepare $|\Phi(s)\rangle$
- Apply $D := \mathrm{diag}\left(\frac{|\hat{F}(w)|}{\hat{F}(w)}\right)$ [Curtis & Meyer'04] and get $D|\Phi(s)\rangle = \sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} |\hat{F}(w)| |w\rangle$
- If f is bent then $H^{\otimes n} D |\Phi(s)\rangle = |s\rangle$
- Complexity: $\Theta(1)$

All Boolean functions

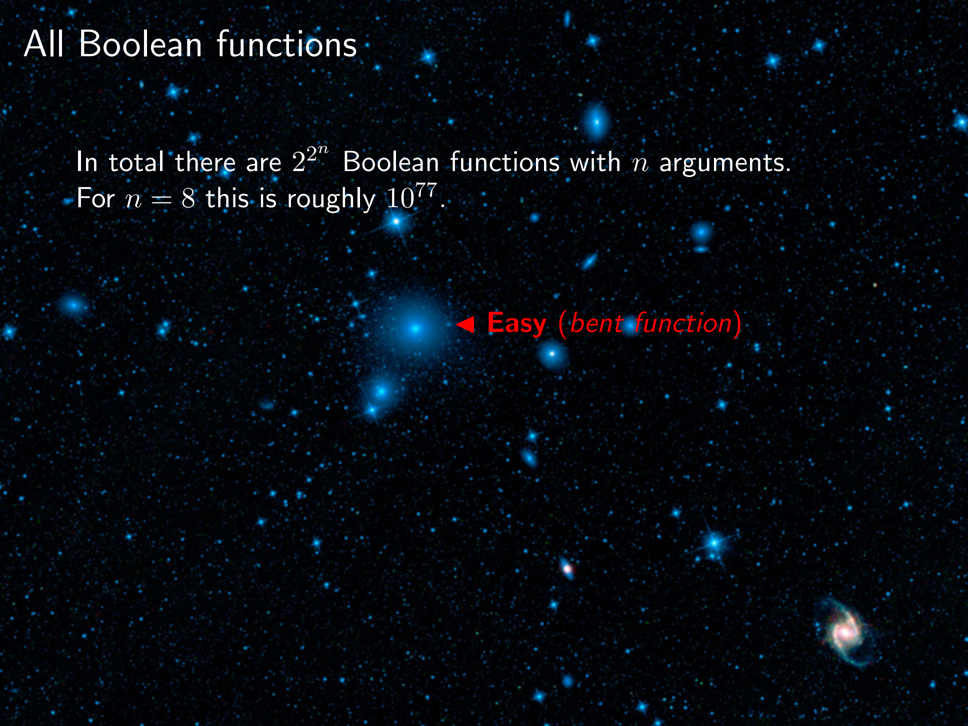


All Boolean functions

In total there are 2^{2^n} Boolean functions with n arguments.
For $n = 8$ this is roughly 10^{77}.

All Boolean functions

In total there are 2^{2^n} Boolean functions with n arguments.
For $n = 8$ this is roughly 10^{77}.



All Boolean functions

In total there are 2^{2^n} Boolean functions with n arguments.
For $n = 8$ this is roughly 10^{77}.

All Boolean functions

In total there are 2^{2^n} Boolean functions with n arguments.
For $n = 8$ this is roughly 10^{77}.

◄ **Easy** (*bent function*)

What about the rest?

Hard (*delta function*) ►

Algorithm for any Boolean function

Resampling approach

$$\sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \hat{F}(w) |w\rangle \mapsto \sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \frac{1}{\sqrt{2^n}} |w\rangle$$

Algorithm for any Boolean function

Resampling approach

$$\sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \hat{F}(w) |w\rangle \mapsto \sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \frac{1}{\sqrt{2^n}} |w\rangle$$

This is a quantum $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ resampling problem with

$$\pi_w = \hat{F}(w) \qquad \sigma_w = \frac{1}{\sqrt{2^n}} \qquad |\xi(w)\rangle = (-1)^{s \cdot w}$$

Algorithm for any Boolean function

Resampling approach

$$\sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \hat{F}(w) |w\rangle \mapsto \sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \frac{1}{\sqrt{2^n}} |w\rangle$$

This is a quantum $\boldsymbol{\pi} \to \boldsymbol{\sigma}$ resampling problem with

$$\pi_w = \hat{F}(w) \qquad \sigma_w = \frac{1}{\sqrt{2^n}} \qquad |\xi(w)\rangle = (-1)^{s \cdot w}$$

Quantum query complexity

Recall that this can be solved using quantum rejection sampling in $O(1/\gamma)$ queries where $\gamma = \min_w \pi_w / \sigma_w$. In our case this is:

$$O\left(\frac{1}{\sqrt{2^n} \hat{F}_{\min}}\right)$$

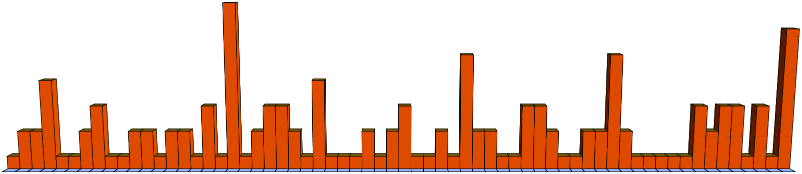
“Demo”

Algorithm

“Demo”

Algorithm

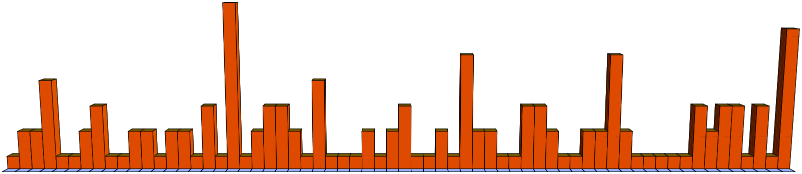
1. Prepare $|\Phi(s)\rangle = H^{\otimes n} O_{f_s} H^{\otimes n} |0\rangle^{\otimes n} = \sum_w (-1)^{s \cdot w} \hat{F}(w) |w\rangle$



"Demo"

Algorithm

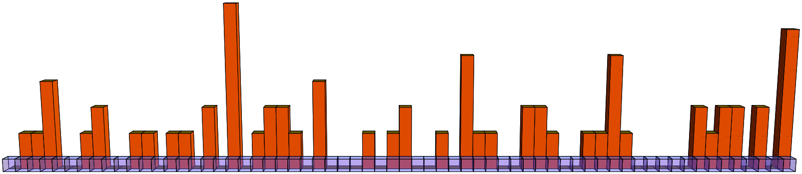
1. Prepare $|\Phi(s)\rangle = H^{\otimes n} O_{f_s} H^{\otimes n} |0\rangle^{\otimes n} = \sum_w (-1)^{s \cdot w} \hat{F}(w) |w\rangle$
2. Perform a $\boldsymbol{\delta}$-rotation where $\delta_w = \hat{F}_{\min}$ for all $w \in \mathbb{Z}_2^n$



“Demo”

Algorithm

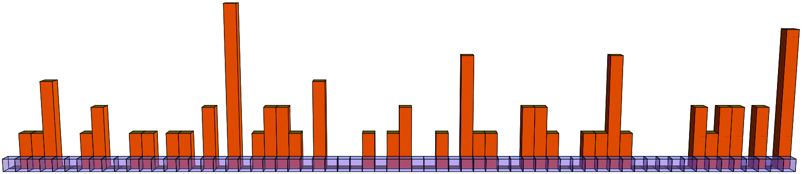
1. Prepare $|\Phi(s)\rangle = H^{\otimes n} O_{f_s} H^{\otimes n} |0\rangle^{\otimes n} = \sum_w (-1)^{s \cdot w} \hat{F}(w) |w\rangle$
2. Perform a $\boldsymbol{\delta}$-rotation where $\delta_w = \hat{F}_{\min}$ for all $w \in \mathbb{Z}_2^n$



"Demo"

Algorithm

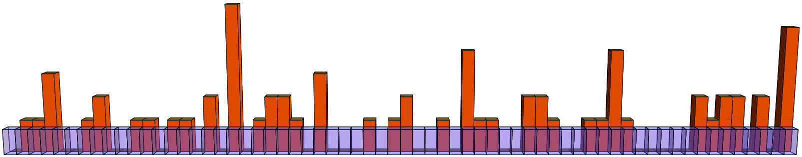
1. Prepare $|\Phi(s)\rangle = H^{\otimes n} O_{f_s} H^{\otimes n} |0\rangle^{\otimes n} = \sum_w (-1)^{s \cdot w} \hat{F}(w) |w\rangle$
2. Perform a $\boldsymbol{\delta}$-rotation where $\delta_w = \hat{F}_{\min}$ for all $w \in \mathbb{Z}_2^n$
3. Do amplitude amplification



“Demo”

Algorithm

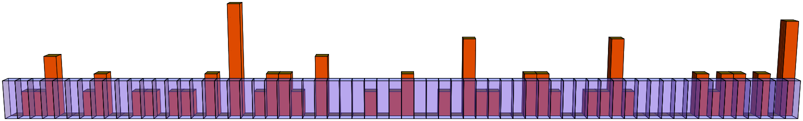
1. Prepare $|\Phi(s)\rangle = H^{\otimes n} O_{f_s} H^{\otimes n} |0\rangle^{\otimes n} = \sum_w (-1)^{s \cdot w} \hat{F}(w) |w\rangle$
2. Perform a $\boldsymbol{\delta}$-rotation where $\delta_w = \hat{F}_{\min}$ for all $w \in \mathbb{Z}_2^n$
3. Do amplitude amplification



"Demo"

Algorithm

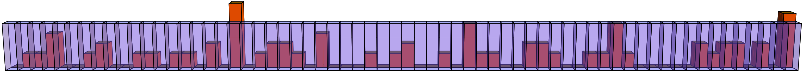
1. Prepare $|\Phi(s)\rangle = H^{\otimes n} O_{f_s} H^{\otimes n} |0\rangle^{\otimes n} = \sum_w (-1)^{s \cdot w} \hat{F}(w) |w\rangle$
2. Perform a $\boldsymbol{\delta}$-rotation where $\delta_w = \hat{F}_{\min}$ for all $w \in \mathbb{Z}_2^n$
3. Do amplitude amplification



“Demo”

Algorithm

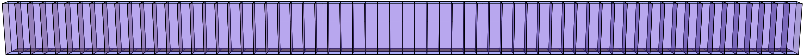
1. Prepare $|\Phi(s)\rangle = H^{\otimes n} O_{f_s} H^{\otimes n} |0\rangle^{\otimes n} = \sum_w (-1)^{s \cdot w} \hat{F}(w) |w\rangle$
2. Perform a $\boldsymbol{\delta}$-rotation where $\delta_w = \hat{F}_{\min}$ for all $w \in \mathbb{Z}_2^n$
3. Do amplitude amplification



"Demo"

Algorithm

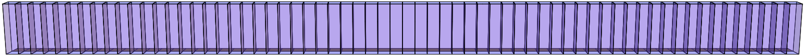
1. Prepare $|\Phi(s)\rangle = H^{\otimes n} O_{f_s} H^{\otimes n} |0\rangle^{\otimes n} = \sum_w (-1)^{s \cdot w} \hat{F}(w) |w\rangle$
2. Perform a $\boldsymbol{\delta}$-rotation where $\delta_w = \hat{F}_{\min}$ for all $w \in \mathbb{Z}_2^n$
3. Do amplitude amplification



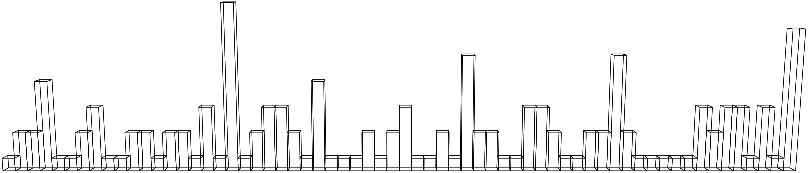
“Demo”

Algorithm

1. Prepare $|\Phi(s)\rangle = H^{\otimes n} O_{f_s} H^{\otimes n} |0\rangle^{\otimes n} = \sum_w (-1)^{s \cdot w} \hat{F}(w) |w\rangle$
2. Perform a $\boldsymbol{\delta}$-rotation where $\delta_w = \hat{F}_{\min}$ for all $w \in \mathbb{Z}_2^n$
3. Do amplitude amplification
4. Measure the resulting state in Fourier basis

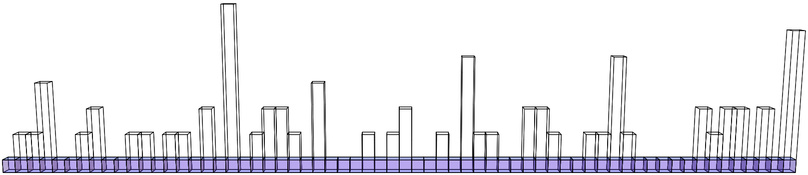


“Demo” (approximate version)



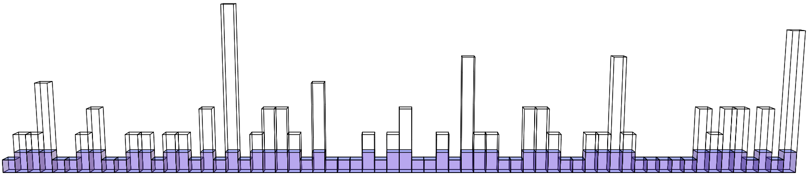
“Demo” (approximate version)

- Instead of the “flat” state



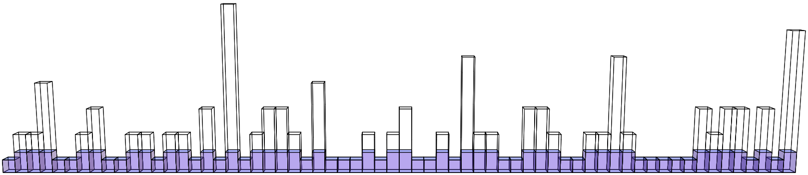
"Demo" (approximate version)

- Instead of the "flat" state aim for "*approximately* flat" state



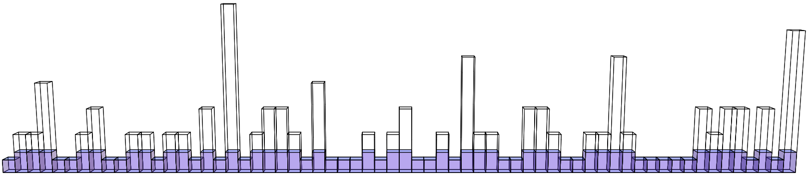
“Demo” (approximate version)

- Instead of the “flat” state aim for “*approximately* flat” state
- Fix the desired success probability p



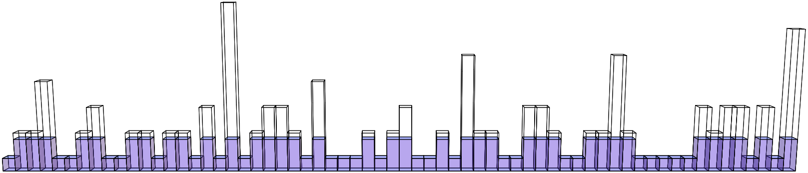
“Demo” (approximate version)

- Instead of the “flat” state aim for “*approximately* flat” state
- Fix the desired success probability p
- Optimal choice of $\boldsymbol{\delta}$ is given by the “water filling” vector $\boldsymbol{\delta}_p$ such that $\boldsymbol{\sigma}^{\mathsf{T}} \cdot \boldsymbol{\delta}_p / \|\boldsymbol{\delta}_p\|_2 \geq \sqrt{p}$ where $\sigma_w = \frac{1}{\sqrt{2^n}}$



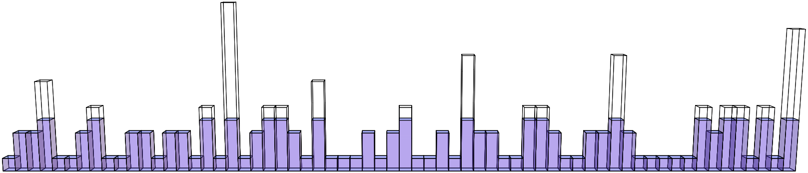
“Demo” (approximate version)

- Instead of the “flat” state aim for “*approximately* flat” state
- Fix the desired success probability p
- Optimal choice of $\boldsymbol{\delta}$ is given by the “water filling” vector $\boldsymbol{\delta}_p$ such that $\boldsymbol{\sigma}^{\mathsf{T}} \cdot \boldsymbol{\delta}_p / \|\boldsymbol{\delta}_p\|_2 \geq \sqrt{p}$ where $\sigma_w = \frac{1}{\sqrt{2^n}}$



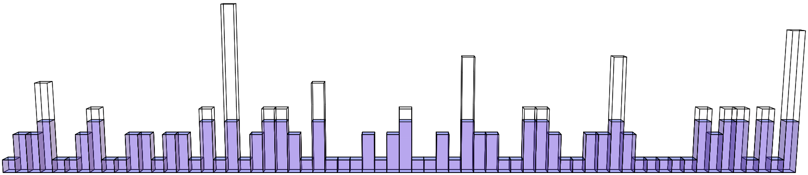
"Demo" (approximate version)

- Instead of the "flat" state aim for "*approximately* flat" state
- Fix the desired success probability p
- Optimal choice of $\boldsymbol{\delta}$ is given by the "water filling" vector $\boldsymbol{\delta}_p$ such that $\boldsymbol{\sigma}^{\mathsf{T}} \cdot \boldsymbol{\delta}_p / \|\boldsymbol{\delta}_p\|_2 \geq \sqrt{p}$ where $\sigma_w = \frac{1}{\sqrt{2^n}}$



“Demo” (approximate version)

- Instead of the “flat” state aim for “*approximately* flat” state
- Fix the desired success probability p
- Optimal choice of $\boldsymbol{\delta}$ is given by the “water filling” vector $\boldsymbol{\delta}_p$ such that $\boldsymbol{\sigma}^{\mathsf{T}} \cdot \boldsymbol{\delta}_p / \|\boldsymbol{\delta}_p\|_2 \geq \sqrt{p}$ where $\sigma_w = \frac{1}{\sqrt{2^n}}$
- Query complexity: $O(1/\|\boldsymbol{\delta}_p\|_2)$



Thank you!

Funding: