Quantum rejection sampling

Martin Roetteler

NEC Laboratories America
4 Independence Way
Princeton, NJ, U.S.A.

Joint work with Maris Ozols and Jérémie Roland
arxiv:1103.2774

2nd Heilbronn Quantum Algorithms Day
University of Bristol
February 1, 2012
Overview

• Motivation: hidden shift problems (20 min)
  – Sampling approach
  – Correlation approach

• Quantum rejection sampling (20 min)
  – Idea: “massage” a given state into target state
  – Algorithm + analysis via SDP
  – Further applications

• Q&A (10 min)
The hidden shift problem

Problem definition:

Input: Maps $f, g: G \rightarrow R$ from finite group $G$ to set $R$
Promise: There is an $s \in G$ with $g(x) = f(x + s)$ for all $x \in G$
Task: Find $s$

Why is this interesting?

Legendre symbol [van Dam et al., 2003]

Hidden shift problem

Hidden subgroup problem

New algorithms

Attacks to cryptosystems

Symmetric group

Dihedral group

Graph isomorphism

Factorizing [Shor, 1994]

Discrete logarithm [Shor, 1994]

Pell’s equation [Hallgren, 2002]

Lattice problems [Regev, 2002]
# The hidden shift problem

## Problem definition

**Given:** Finite group $G$, finite set $R$, maps $f, g : G \rightarrow R$

**Promise:** There is $s \in G$ such that $g(x) = f(x + s)$ for all $x$

**Task:** Find $s$.

## Examples

- If $f$ is a delta function, then finding $s$ is the same as searching a list of $2^n$ items. This needs $\Theta(\sqrt{2^n})$ operations.

- There are functions $f, g$ which lead to a better speedup, e.g., the Legendre symbol [van Dam, Hallgren, Ip’02]

$$f(x) = \left( \frac{x}{p} \right) = \begin{cases} 
1 & : \ x \text{ is a square in } \mathbb{F}_p^x, \\
-1 & : \ x \text{ is a nonsquare in } \mathbb{F}_p^x, \\
0 & : \text{ if } x = 0.
\end{cases}$$

- For Legendre symbol, $s$ can be found efficiently by a quantum computer. However, no separation known.
Using the quantum Fourier transform

Shift invariance of the power spectrum:

How is this used? “Forget” information about coset. Used in factoring/order finding, dlog, [Shor’94], HSP [Kitaev’95], Pell’s equation [Hallgren’02], hidden radius problem [Childs, Schulman, Vazirani’07], ...

Convolution property:

How is this used? “Correlate” two functions. Used in hidden shift problem [van Dam, Hallgren, Ip ‘03] for shifted Legendre symbol. Works for functions g with special properties only.

Issue: in general not unitary
Boolean Fourier analysis

The Hadamard transform

Let \( f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2 \) be Boolean function. We associate with \( f \) the real valued function \( F(x) = (-1)^{f(x)} \). Its Fourier transform is

\[
\hat{F}(w) = \frac{1}{2^n} \sum_{x \in \mathbb{Z}_2^n} (-1)^{wx + f(x)}. 
\]

• Boolean Fourier analysis has many applications
  – KKL theorem, learning of DNF under uniform distribution
  – Characterization of \( \text{AC}^0 \) circuits, Bourgain’s junta theorem
  – etc.

• Finite dimensional analogue of white Gaussian noise?
  – Functions with many non-zero Fourier coefficients
  – Interesting from cryptographic point of view
Highly non-linear functions

Bent functions

- A Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is called bent [Rothaus76] if the Fourier coefficients satisfy $|\hat{F}(w)| = 2^{-n/2}$ for all $w \in \mathbb{Z}_2^n$. Such functions are studied in cryptography.
- Necessary for existence is that $n$ is even [Dillon75].
- If $f$ is bent, then we obtain another bent function $f^*$ via

$$(-1)^{f^*(w)} := 2^{n/2} \hat{F}(w).$$

By taking the dual twice we obtain $f$ back: $(f^*)^* = f$.

Example: (here $f$ is so-called Majorana-McFarland function)
Where are bent functions used?

Symmetric cryptography

For instance in DES:

\[ \text{DES}_{K_1}(m) \rightarrow 64 \text{ bit} \]

\[ K_1 \rightarrow 56 \text{ bit} \]

\[ \text{DES}(K_1, m) \rightarrow 64 \text{ bit} \]

\[ c \]

Coordinate functions are chosen to be very close to being bent.

Stream ciphers

- Here the output of two or more linear feedback shift registers (LFSRs) are combined using a bent function.

- This provides maximal resilience against correlation attacks that seek to identify the initial state of the LFSRs.
Further properties and examples

Facts

- Why the name “bent”? Since these functions are maximally far from the set of linear functions.
- Several ad-hoc constructions of classes of bent functions are known. But a complete classification is unknown.
- Total number is at least \( \Omega \left( \left( \frac{2^{n/2}+1}{e} \right)^{2^{n/2}} \sqrt{2\pi 2^{n/2}} \right). \)

Maiorana-McFarland class of bent functions

- Let \( \pi : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n \) be a permutation of strings of length \( n \) and \( g \) any function. Let \( x = (x_1, \ldots, x_n) \), \( y = (y_1, \ldots, y_n) \). Then
  \[
  f(x, y) = x\pi(y) + g(y)
  \]
is a bent function on \( 2n \) variables.
- Special case: \( \pi \) identity permutation. We get the inner product function \( ip_n(x_1, \ldots, x_n) = \sum_{i=1}^{n/2} x_{2i-1} x_{2i} \).
Sampling approach – Hidden subgroup reductions
The Hidden Subgroup Problem

Definition of the problem

**Given:** Group $G$, set $S$, map $f : G \to S$ given as black box

**Promise:** There exists subgroup $H \leq G$ with
- $f$ constant on each coset of $H$
- $g_1 H \neq g_2 H$ implies $f(g_1) \neq f(g_2)$

**Problem:** Find generators for $H$ (input size: $\log |G|$)

Visualization of the cosets of $H$ in $G$

Caveat

Difficulty of HSP depends crucially on the structure of the group $G$. 
Quantum upper bound:

- In general for $f$, $g$ injective, hidden shift can be reduced to a HSP.
- Not applicable here directly, since $f$, $g$ are not injective. But reduction is possible using quantum functions $F : x \mapsto \sum_{y \in \mathbb{Z}_2^n} (-1)^{f(x+y)} |y\rangle$
- Resulting quantum circuit:

$$
\begin{align*}
|0\rangle & \quad H \\
|0\rangle \otimes n & \quad H \otimes n \\
|0\rangle \otimes n & \quad H \otimes n \\
& \quad U_g \\
& \quad U_f \\
& \quad H \otimes n \\
\end{align*}
$$

- Note that this does not require to know $f^*$ in order to compute the shift!
- This can be used to show an exponential separation in query complexity to find the hidden shift $s$, provided $f$ and $g$ are given as oracles. [R., SODA’10]
Simplifying the circuit

\[ |0\rangle \rightarrow H \rightarrow U_g \rightarrow U_f \rightarrow H \]

\[ |0\rangle \otimes n \rightarrow H \otimes n \rightarrow U_g \rightarrow U_f \rightarrow H \otimes n \]
Sampling

\[
\sum_u \left(1 + (-1)^{-us}\right) \hat{F}(u) |u\rangle
\]

- **Sampling Subroutine**: Measure this state in the computational basis. This will give us results only those \( u_i \) with \( u_i s = 0 \).

- Let \( D \) be the distribution \( D_i := \Pr(\text{observe } u_i) = |\hat{F}(u_i)|^2 \).

- In general \( D \) is not uniform. E.g., in case of unstructured search, most of the amplitude is on the all-zero vector.

- Intuition: For random functions the spectrum is “almost flat”.

![Typical coefficients](image-url)
Sampling based algorithm

Quantum algorithm:

1. Set $i = 0$ and $V_0 = \{0\}$.

2. Run the **Sampling Subroutine**. Denote by $u_i$ the output of the measurement.

3. If $\dim(\text{Span}\{u_k | k \in [i]\}) > \dim(V_i)$ then set $i \leftarrow i+1$ and set $V_i = \langle V_{i-1}, u_{i-1} \rangle$. If $\dim(V_i) = n - 1$ then continue to next step. Otherwise go back to Step 2.

4. Output “$s$”, where $s$ is the unique solution of

\[
\begin{align*}
\langle u_1, s \rangle &= 0 \\
&\vdots \\
\langle u_t, s \rangle &= 0.
\end{align*}
\]
Analyzing the algorithm

Lemma [Influence]: For any Boolean function $f$ over $\mathbb{Z}_2^n$ and $n$-bit string $v$, we call $\gamma_{f,v} = \Pr[f(x) \neq f(x + v)]$ the influence of $v$ for $f$, and $\gamma_f = \min_v(\gamma_v)$ the minimum influence of $f$. Then

$$\gamma_{f,v} = \sum_{u: \langle v,u \rangle = 1} |\hat{F}(u)|^2$$

and $E($queries$) \leq \frac{n}{\gamma_f}$ for the expected time until $s$ is characterized.

Theorem: There exists a quantum algorithm that solves the Boolean Hidden Shift Problem for $f$ using expected $O(n/\sqrt{\gamma_f})$ oracle queries.

Theorem [Average case exponential separation]: Let $(O_f, O_g)$ be an instance of a Boolean Hidden Shift Problem where $g(x) = f(x + v)$ and $f$ and $v$ are chosen uniformly at random. Then there exists a quantum algorithm which finds $v$ with bounded error using $O(n)$ queries and in $O(\text{poly}(n))$ time whereas any classical algorithm needs $\Omega(2^{n/2})$ queries to achieve the same task.
Exponential query complexity separation

- **Quantum upper bound**

  **Theorem:** Let $\mathcal{O}_f$ be an oracle that hides an instance of a shifted bent function problem for a function $f$ and hidden shift $s$. Then there exists a polynomial time quantum algorithm that computes $s$ with constant probability of success and makes $O(n)$ queries to $\mathcal{O}_f$.

- **Classical lower bound**

  **Theorem:** Let $\mathcal{O}_f$ be an oracle that hides a hidden shift $s$ for an instance $(f, g)$ of a hidden shift problem for a bent function $f$ from Maiorana-McFarland class. Then classically $\Theta(2^{n/2})$ queries are necessary and sufficient to identify the hidden shift $s$. 

Classical lower bound

**Intuition:** Suppose classical algorithm made \( k = n^{O(1)} \) queries. Show that there exist many functions consistent with these queries but leading to different shift \( s \).

**Functions:** Chosen uniformly at random from the set of all Boolean functions \( f : \{0, 1\}^n \rightarrow \{0, 1\} \).

**Queries:** \( x_i \in \{0, 1\}^n \)

- Set \( S \) such that difference between any 2 elements in \( S \) is different from \( s \).
- Any shift \( s' \in S \), can be made consistent with sampled data (for suitable \( \pi' \)).
- Since \( |S| \geq 2^n - n^{O(1)} \), the l.b. follows.
Correlation approach – Quantum rejection sampling
Correlation algorithm

Quantum algorithm:

1.) Initialize quantum register: $|0\rangle$

2.) Equal distribution on register: $\sum_{x \in \mathbb{Z}_2^n} |x\rangle$

3.) Compute $g$ in superposition: $\sum_{x \in \mathbb{Z}_2^n} (-1)^{g(x)} |x\rangle$

4.) Compute DFT of this state: $\sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \hat{F}(w) |w\rangle$

5.) “Uncompute $\hat{F}(w)$”: $\sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} |w\rangle$

6.) Compute DFT of this state: $|s\rangle$

7.) Measure register: obtain $s$

Problem: “uncomputing” in step 5.) only works if diagonal elements are on the unit circle, i.e., only if the Fourier spectrum is flat in absolute value. One of the challenges is to generalize this to functions with non-flat spectrum.
Finding hidden shifts via correlations

Quantum algorithm for finding $s$:

$$|0\rangle \otimes n \xrightarrow{H \otimes n} U_g \xrightarrow{H \otimes n} U_{f^*} \xrightarrow{H \otimes n} |s\rangle$$

Remarks:

• The algorithm is deterministic, i.e., no error occurs, provided that initial state preparation, gates, and the measurement are perfect.

• The operators $U_g$ and $U_{f^*}$ compute $g$ and $f^*$ into the phase. For several classes of bent functions, it is known how to compute $f^*$, so this algorithm can be used. This includes (i) Majorana-McFarland bent functions, (ii) quadratics, and (iii) functions close to quadratics, as measured by the $U_3$ norm. [R., MFCS’09].

• Issues with this approach:
  - If Fourier spectrum is not flat, this method is not applicable.
  - The algorithm uses knowledge about the Fourier coefficients ($f$ is known).
Other ways to renormalize?

An idea from diffractive optics ("4f setup"): 

Methods to design diffractive phase elements:

- Gerchberg-Saxton algorithm, Iterative Fourier Transform Algorithm (IFTA)
- Characterize signal loss due to renormalization.
- Use phase freedom in the design of the diffractive element and the use of a signal windows.
In our context, $\mathcal{F}$ is the Hadamard transform. We plan to use constraints $L$ to enforce that $f$ is Boolean and constraints $R$ to enforce that $F$ is flat. Several strategies for possible $L/R$ and phase freedom might be exist. We plan to investigate this further.
Hidden shifts: two extremal cases

Bent function

\[ H_2^\otimes n \ U_f \ H_2^\otimes n \ U_g \ H_2^\otimes n \ |0\rangle = |s\rangle \]

Delta function

\[ (H_2^\otimes n \ U_f \ H_2^\otimes n \ U_g)^k \ H_2^\otimes n \ |0\rangle = |s\rangle \]

Q: how about general functions?

Complexity = 1

[R., SODA’10]

Complexity = \( N^{1/2} \)

[Grover, FOCS’96]
Target state reveals the shift

The *spiky* state (Fourier spectrum)

\[ \sum_w (-1)^{w \cdot s} \hat{f}(w) |w\rangle \]

- Simple to prepare (only 1 query to \( f_s \))
- Almost no info on \( s \)

The *flat* state

\[ \sum_w (-1)^{w \cdot s} \frac{1}{\sqrt{2^n}} |w\rangle \]

- Hard to prepare (more queries to \( f_s \))
- Complete info on \( s \)
Resampling

Classical $p \rightarrow s$ resampling problem

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

- **Task:** Sample from distribution $s$

- **Question:** How many samples from $p$ we need to prepare one sample from $s$?

- **Note:** Samples are pairs $(k, \xi(k))$ where $\xi(k)$ is not accessible
Classical rejection sampling

\[ \text{Prob(accept } x) = \frac{\gamma s(x)}{p(x)} \]

[von Neumann, 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 $\pi \rightarrow \sigma$ resampling problem

- **Given:** $\pi, \sigma \in \mathbb{R}_+^n$ with $\|\pi\|_2 = \|\sigma\|_2 = 1$
  
  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 $\pi \rightarrow \sigma$ quantum resampling problem is $\Theta(1/\gamma)$ where $\gamma = \min_k |\pi_k/\sigma_k|$.

Approximate preparation

**Task:** Prepare $\sqrt{1 - \varepsilon} |\sigma\rangle + \sqrt{\varepsilon} |\text{error}\rangle$
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 \( \delta \in \mathbb{R}_+^n \) and rotate the state in the first register:

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

3. Measure the first register:

- w.p. \( \|\delta\|_2^2 \) the state collapses to

\[
\sum_{k=1}^{n} \hat{\delta}_k |k\rangle |\xi(k)\rangle
\]

where \( \hat{\delta}_k = \delta_k / \|\delta\|_2 \)
How to choose the rotations

Optimization

Problem

\[ \min_\delta \frac{1}{\|\delta\|_2} \text{ s.t. } \sigma \cdot \hat{\delta} \geq \sqrt{1 - \varepsilon} \text{ and } 0 \leq \delta_k \leq \pi_k \]

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

- This can be stated as an SDP

Optimal solution

- Let \( \delta_k(\gamma) = \min\{\pi_k, \gamma \sigma_k\} \)
Application to hidden shifts

Main idea

- Aim for \textit{approximately flat} state
- Optimal choice is given by the “water filling” state
- Requires less iterations
- Success probability $p$

Filling the Walsh-Hadamard spectrum of $f$ with water:

Result:

**Theorem.** $\text{BHSP}_f^p = O(1/\|\varepsilon\|_2)$ where $\varepsilon$ is the largest vector such that $\|\varepsilon\|_1 = \sqrt{2^n p} \|\varepsilon\|_2$ and $\varepsilon_{\hat{w}} = \min\{|\hat{f}_{\hat{w}}|, \gamma/\sqrt{2^n}\}$ for some $\gamma > 0$, where $\hat{f}$ is the Fourier transform of $f$. [Ozols, R., Roland, arxiv:1103.2774]
Further 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...
Open problems:

• “Coherent” version of previous algorithm?

\[
\sum_{u} \left(1 + (-1)^{-us}\right) \hat{F}(u) |u\rangle
\]

• Can we uncompute the Fourier spectrum \(\hat{F}(u)\)? In other words, when given an oracle for \(f\), can we implement the Fourier transform \(\hat{F}\)? Or even just approximate it? If not, then why not? Explore relation to “forrelated” functions [Aaronson’09] and the sampling/searching problem [Aaronson’10].

• Apply PGM approach to hidden shift problem.

• Applications of hidden shift for Boolean functions?
  – Can we find initial seed of LFSR pseudorandom generator?
  – Quantum cryptanalysis?

• Can highly non-linear Boolean functions and diagonalization similar to [Watrous ’00] show oracle separation between BQP and MA?
Conclusions

• **Hidden shift problems**
  – Bent functions; connection to hidden subgroup problem
  – Special case: random functions
  – Exponential q/c query complexity separation
  – Solution via a quantum analogue of the accept/reject method

• **Quantum rejection sampling**
  – Formulation of state resampling problem
  – Algorithm using controlled rotations
  – Optimal rotation vector determined by SDP
  – Further applications

• **Acknowledgment of support:**

February 1, 2012

M. Roetteler