Title: Quantum Algorithms for Hidden Shift Problems

Date: Apr 12, 2012 04:30 PM

URL: http://pirsa.org/12040115

Abstract: TBA

On quantum algorithms for hidden shift problems

Martin Roetteler

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

Recent Progress in Quantum Algorithms
IQC and Perimeter Institute
Waterloo, April 12, 2012

Quantum Fourier Transform: use cases (!?)

Shift invariance of the power spectrum:

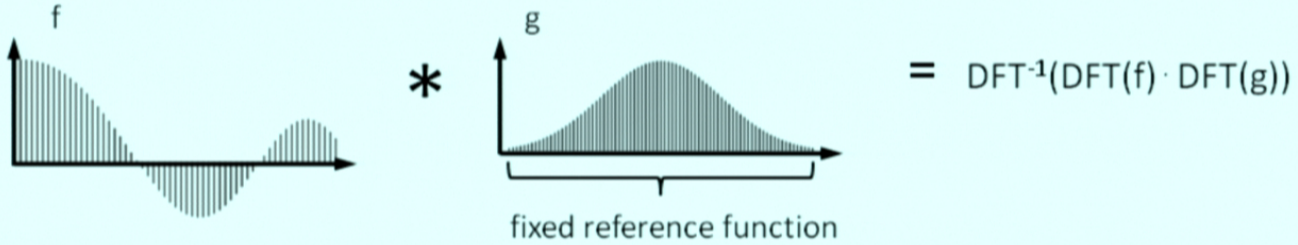
How is this used? "Forget" information about coset. Used in factoring/order finding, dlog, [Shor'94], HSP [Kitaev'95], Pell's equation [Hallgren'02], hidden radius problem [Childs, Schulman, Vazirani'07], ...

Quantum Fourier Transform: use cases (!?)

Shift invariance of the power spectrum:

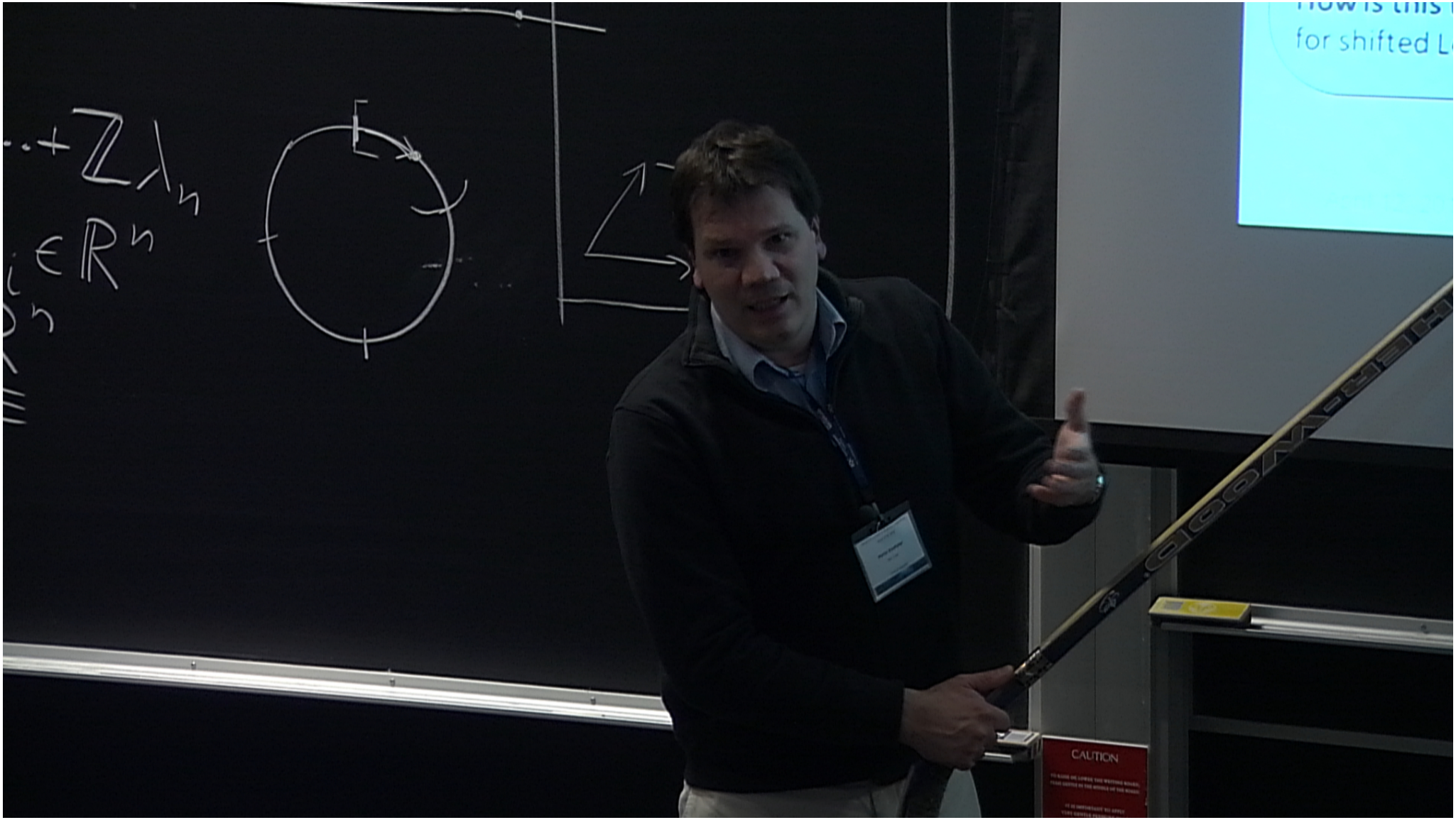
How is this used? "Forget" information about coset. Used in factoring/order finding, dlog, [Shor'94], HSP [Kitaev'95], Pell's equation [Hallgren'02], hidden radius problem [Childs, Schulman, Vazirani'07], ...

Convolution property:



$= \mathrm{DFT}^{-1}(\mathrm{DFT}(f) \cdot \mathrm{DFT}(g))$

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.

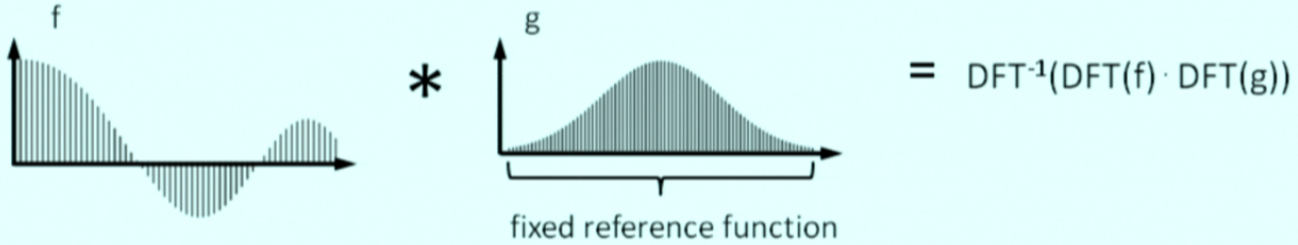

for shifted
CAUTION

Quantum Fourier Transform: use cases (!?)

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:



$= \mathrm{DFT}^{-1}(\mathrm{DFT}(f) \cdot \mathrm{DFT}(g))$

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.

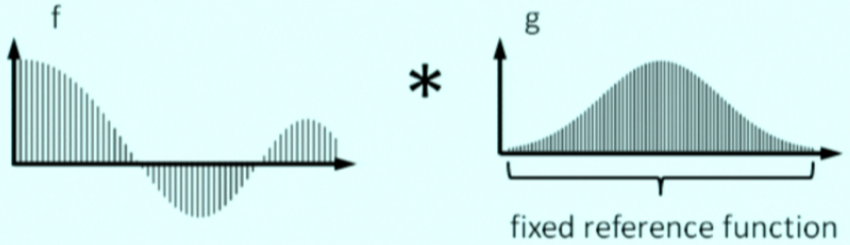
Quantum Fourier Transform: use cases (!?)

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:

Issue: in general not unitary



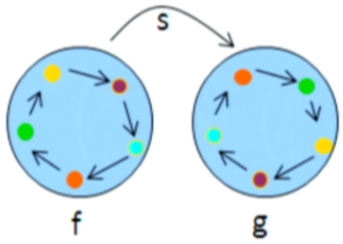
$$= \mathrm{DFT}^{-1}(\mathrm{DFT}(f) \cdot \mathrm{DFT}(g))$$

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.

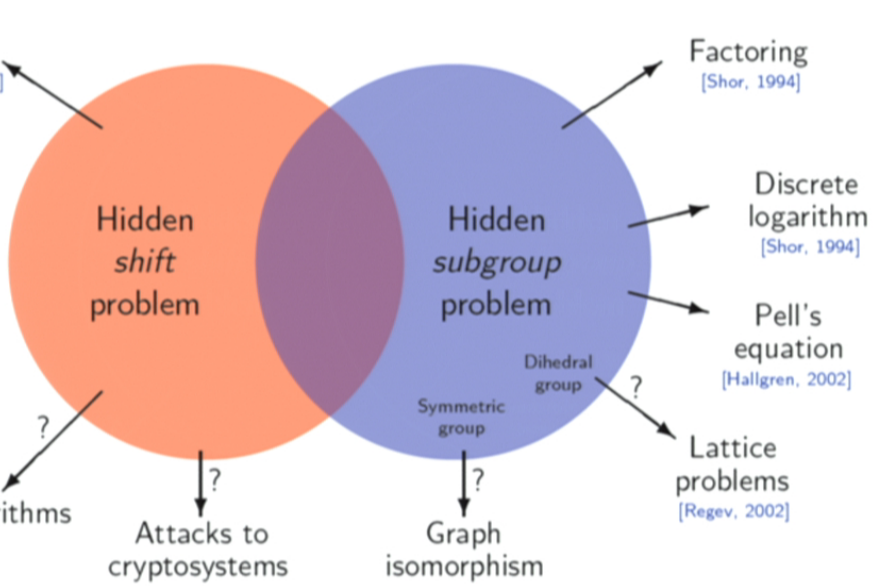
Hidden shift problem

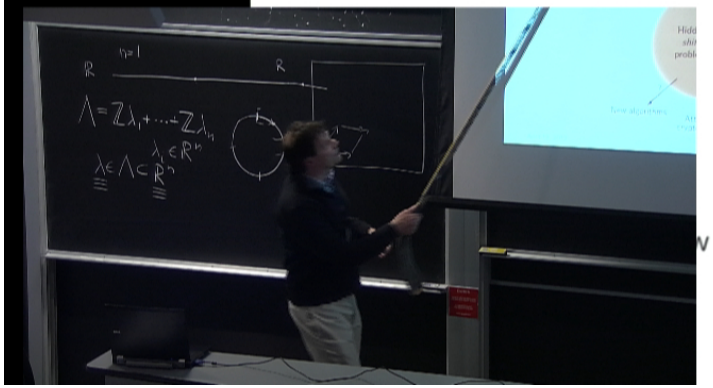
Problem definition:

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



Why is this interesting?





Correlation algorithm

Quantum algorithm: [van Dam, Hallgren, Ip, SODA'03]

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:	$\sum_{w\in\mathbb{Z}_2^n} (-1)^{s\cdot w} \widehat{F}(w) \|w\rangle$
5.)	"Uncompute $\widehat{F}(w)$":	$\sum_{w\in\mathbb{Z}_2^n} (-1)^{s\cdot w} \|w\rangle$
6.)	Compute DFT of this state:	$\|s\rangle$
7.)	Measure register:	obtain s

Correlation algorithm

Quantum algorithm: [van Dam, Hallgren, Ip, SODA'03]

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:	$\sum_{w\in\mathbb{Z}_2^n} (-1)^{s\cdot w} \widehat{F}(w) \|w\rangle$
5.)	"Uncompute $\widehat{F}(w)$":	$\sum_{w\in\mathbb{Z}_2^n} (-1)^{s\cdot w} \|w\rangle$
6.)	Compute DFT of this state:	$\|s\rangle$
7.)	Measure register:	obtain s

Correlation algorithm

Quantum algorithm: [van Dam, Hallgren, Ip, SODA'03]

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

Boolean hidden shift problems

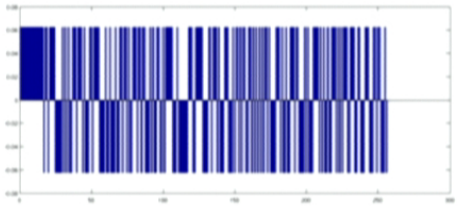
Bent functions

- A Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is called *bent* [Rothaus76] if the Fourier coefficients satisfy $|\widehat{F}(w)| = 2^{-n/2}$ 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 $f^\star$ via

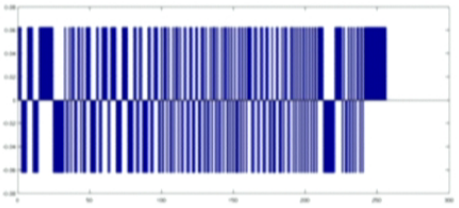
$$(-1)^{f^\star(w)} := 2^{n/2}\widehat{F}(w).$$

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

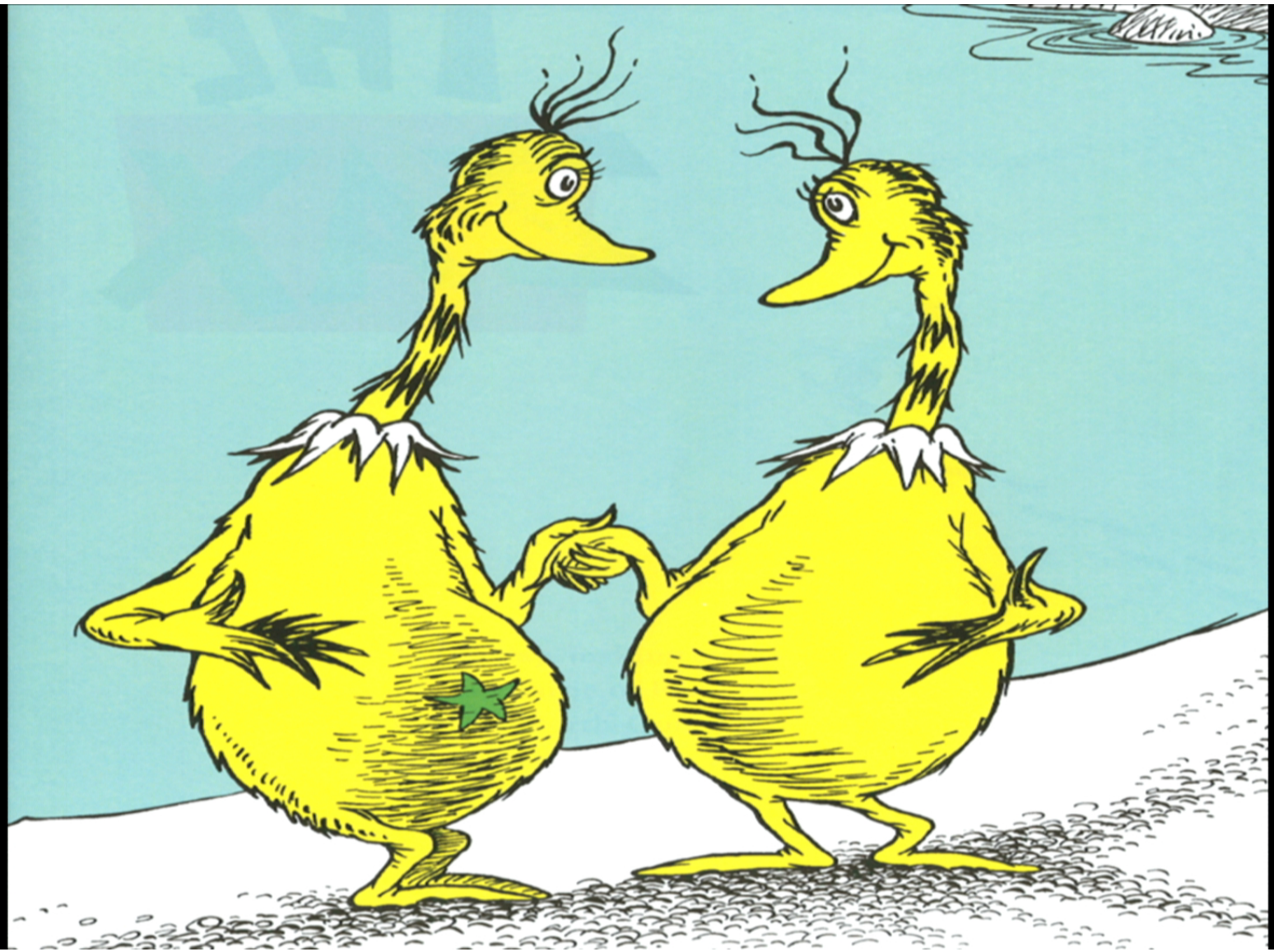
Example: (here f is so-called Maiorana-McFarland function)



F



$\widehat{F}$

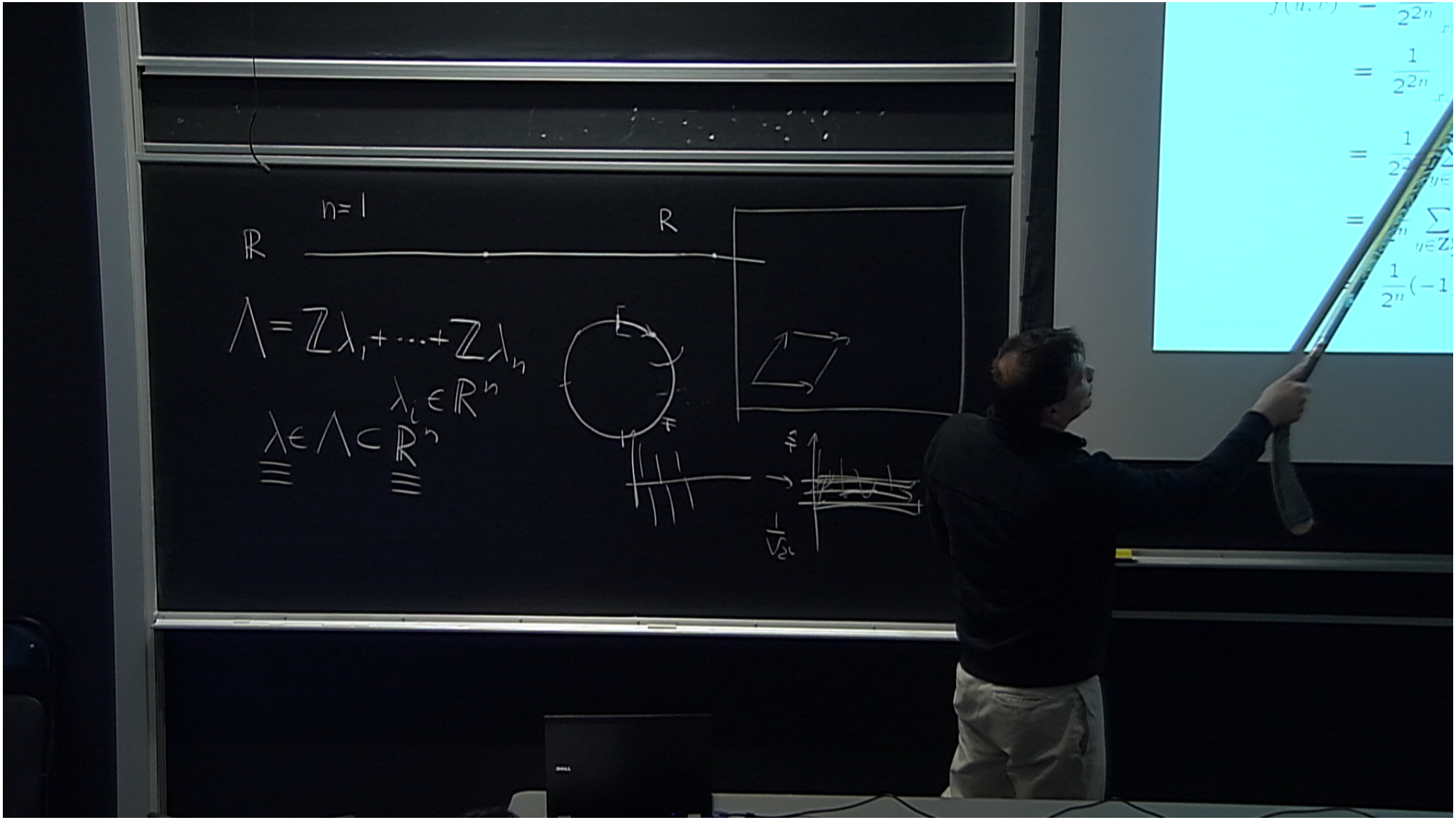


Maiorana-McFarland functions

Theorem: Let $f(x,y) := x\pi(y)^t + g(y)$. Then the dual bent function is given by $f^\star(x,y) = \pi^{-1}(x)y^t + g(\pi^{-1}(x))$.

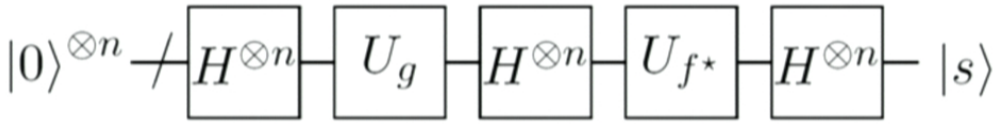
Proof: Let $\widehat{f}(u,v)$ be the Fourier transform of f at (u,v).

$$\begin{aligned}
\widehat{f}(u,v) &= \frac{1}{2^{2n}} \sum_{x,y \in \mathbf{Z}_2^n} (-1)^{f(x,y)+(u,v)(x,y)^t} \\
&= \frac{1}{2^{2n}} \sum_{x,y \in \mathbf{Z}_2^n} (-1)^{x\pi(y)^t+g(y)+(u,v)(x,y)^t} \\
&= \frac{1}{2^{2n}} \sum_{y \in \mathbf{Z}_2^n} (-1)^{vy^t+g(y)} \left(\sum_{x \in \mathbf{Z}_2^n} (-1)^{(u+\pi(y))x^t} \right) \\
&= \frac{1}{2^n} \sum_{y \in \mathbf{Z}_2^n} (-1)^{vy^t+g(y)} \delta_{u,\pi(y)} \\
&= \frac{1}{2^n} (-1)^{v\pi^{-1}(u)^t+g(\pi^{-1}(u))}.
\end{aligned}$$


n=1
R
R
$\Lambda = \mathbb{Z}\lambda_1 + \cdots + \mathbb{Z}\lambda_n$
$\lambda_i \in \mathbb{R}^n$
$\lambda \in \Lambda \subset \mathbb{R}^n$

Finding hidden shifts via correlations

Quantum algorithm for finding s:



Remarks:

- The algorithm is deterministic, i.e., no error occurs, provided that initial state preparation, gates, and the measurement are perfect.
- U_g and U_{f^*} compute g and f* into the phase. For several classes of bent functions, it is know how to compute f*, so this algorithm can be used.
- If Fourier transform *F(w)* is not flat, [Curtis/Meyer'02] proposed to renormalize

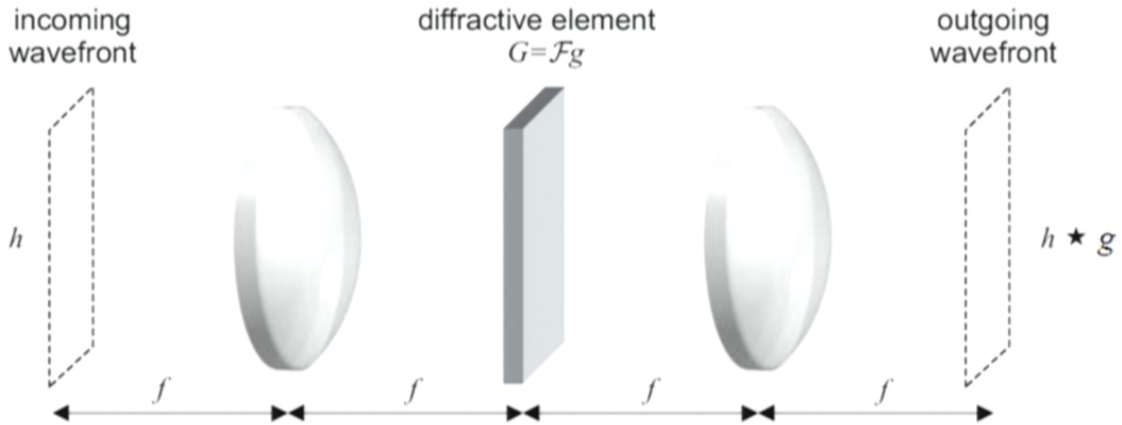
$$\widehat{F}'(w) := \frac{1}{\sqrt{2^n}} \frac{\widehat{F}(w)}{|\widehat{F}(w)|}$$

and to correlate with respect to $\widehat{F}'$. But there are some issues with this approach.

- Issues:
  - Potentially leads to very high "distortion" of spectrum.
  - The algorithm uses knowledge about Fourier coefficients (i.e., f* must be known).

Other ways to renormalize?

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



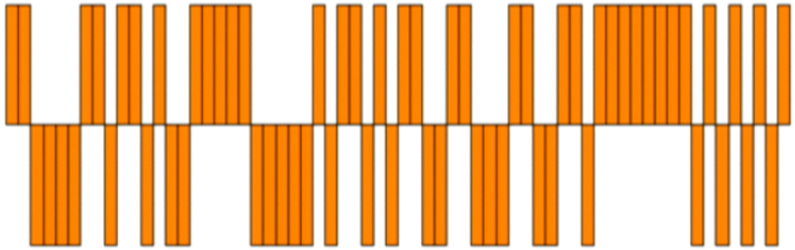
Methods to design diffractive phase elements:

- Gerchberg-Saxton algorithm, Iterative Fourier Transform Algorithm (IFTA)
- Characterize signal loss due to renormalization.
- Use phase freedom in the design of the diffractive element.

→ but: it seems difficult to prove rigorous statements about such methods.

Hidden shifts: two extremal cases

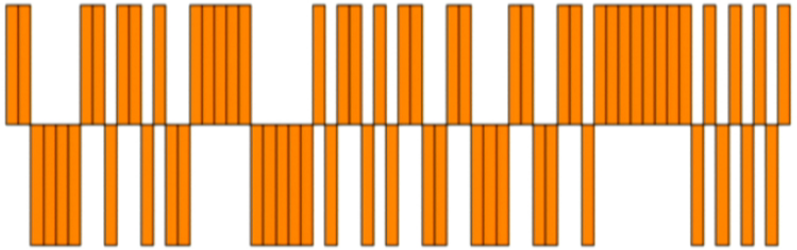
Bent function



Delta function

Hidden shifts: two extremal cases

Bent function

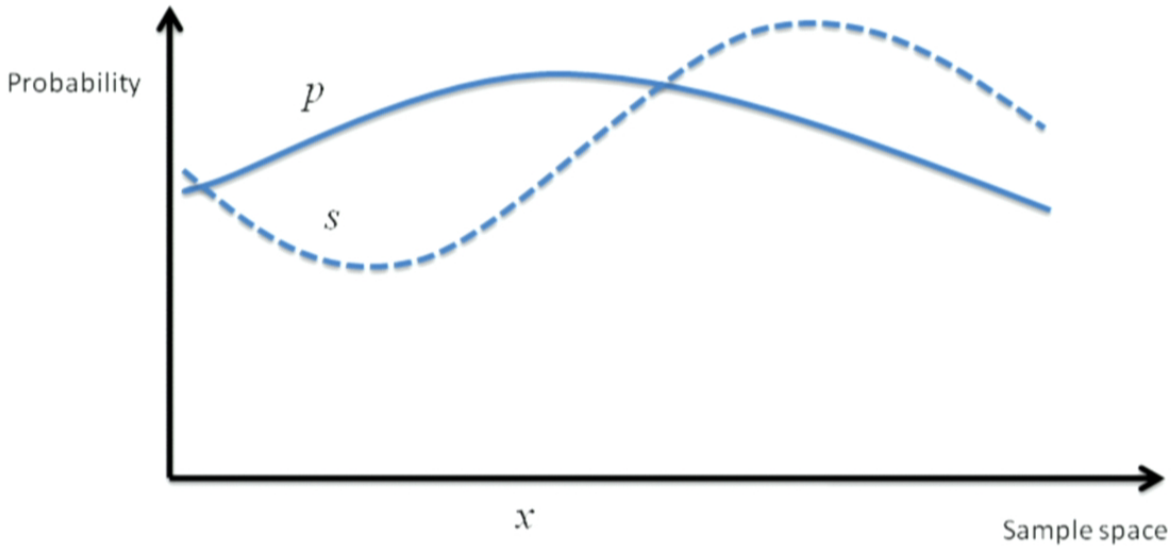


Complexity = 1

Delta function

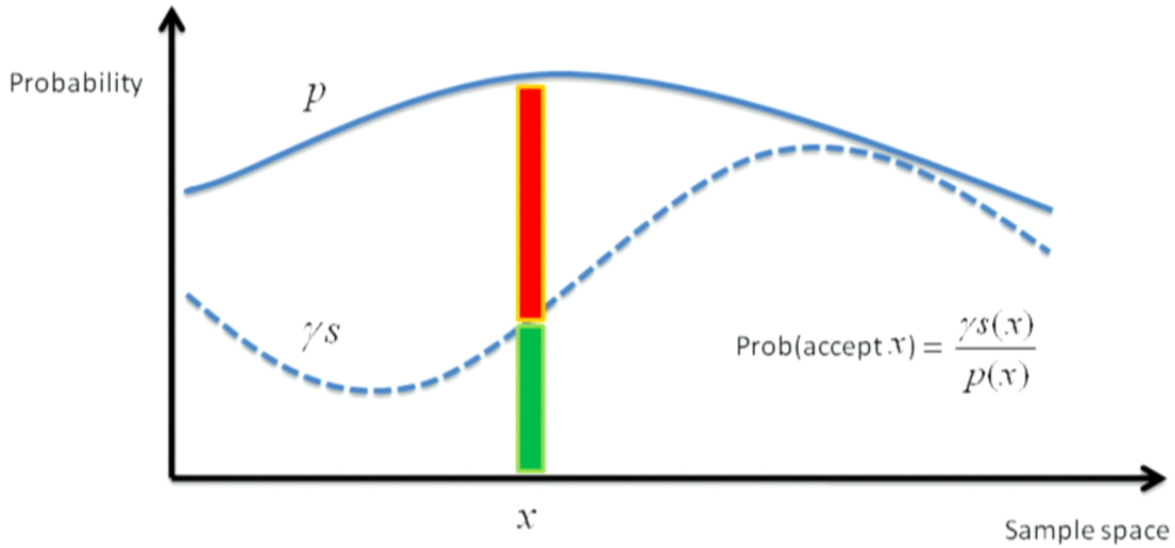
Complexity = $N^{1/2}$

Classical rejection sampling



[von Neumann, 1951]

Classical rejection sampling



[von Neumann, 1951]

Quantum resampling problem

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 $\sqrt{1-\varepsilon}|\sigma\rangle + \sqrt{\varepsilon}|\text{error}\rangle$

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

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

3. Measure the first register:
   - w.p. $\|\boldsymbol{\delta}\|_2^2$ the state collapses to

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

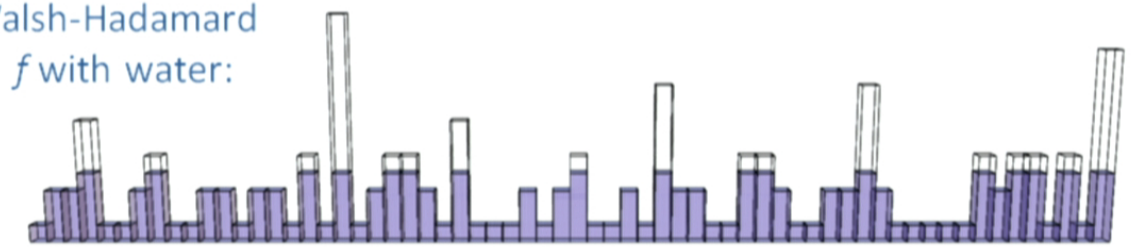
   where $\hat{\delta}_k = \delta_k / \|\boldsymbol{\delta}\|_2$ → Further details: Maris' talk tomorrow

Application to hidden shifts

Main idea

- Aim for *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:



Special case: hidden shift target state

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

- Pick $\varepsilon \in \mathbb{R}^{2^n}$ such that $\forall w : 0 \leq \varepsilon_w \leq |\hat{F}(w)|$
- Apply $R_\varepsilon : |w\rangle|0\rangle \mapsto |w\rangle\frac{1}{\hat{F}(w)}\Big(\sqrt{\hat{F}(w)^2-\varepsilon_w^2}|0\rangle + \varepsilon_w|1\rangle\Big)$
- If we would measure the last qubit, we would get outcome "1" w.p. $\|\varepsilon\|_2^2$ and the post-measurement state would be

$$\frac{1}{\|\varepsilon\|_2}\sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}\varepsilon_w|w\rangle$$

- Instead of measuring, amplify the amplitude on $|1\rangle$
- Complexity: $O(1/\|\varepsilon\|_2)$
- Take $\varepsilon_w = \hat{F}_{\min}$ to get s with certainty in $O\Big(\frac{1}{\sqrt{2^n}\hat{F}_{\min}}\Big)$ queries

Sampling approach – Hidden subgroup reductions

The Hidden Subgroup Problem

Definition of the problem

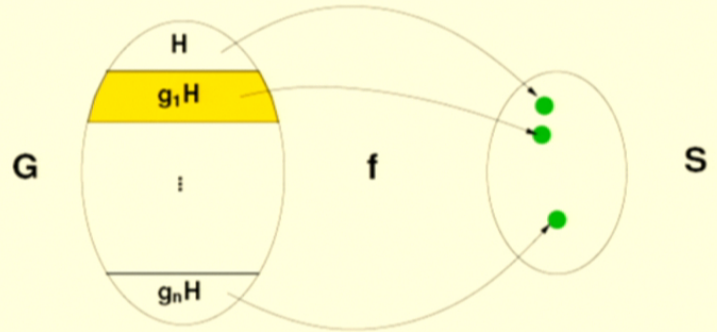
Given: Group G, set S, map $f : G \to S$ given as black box

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



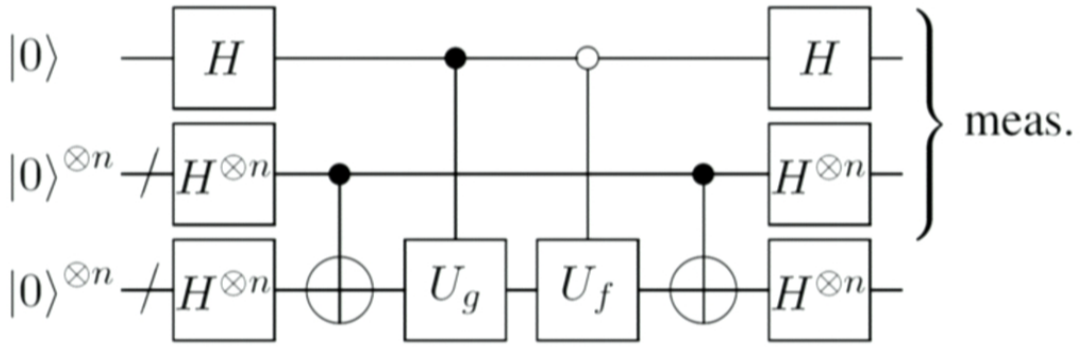
Caveat

Difficulty of HSP depends crucially on the structure of the group G.

Hidden shifts via hidden subgroups

Quantum upper bound:

- In general for f, g injective, hidden shift can be reduced to a HSP.
- Not applicable here directly, since f, g might not be 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:



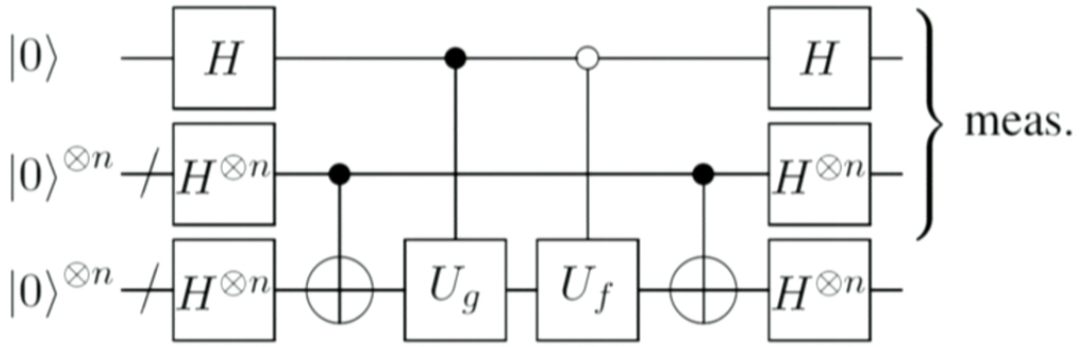
- Note that this does not require to know f* in order to compute the shift!
- This can be used to show an exponential separation in query complexity to find the hidden shift s, provided f and g are given as oracles.

[R., SODA'10, arxiv:0811.3208]

Hidden shifts via hidden subgroups

Quantum upper bound:

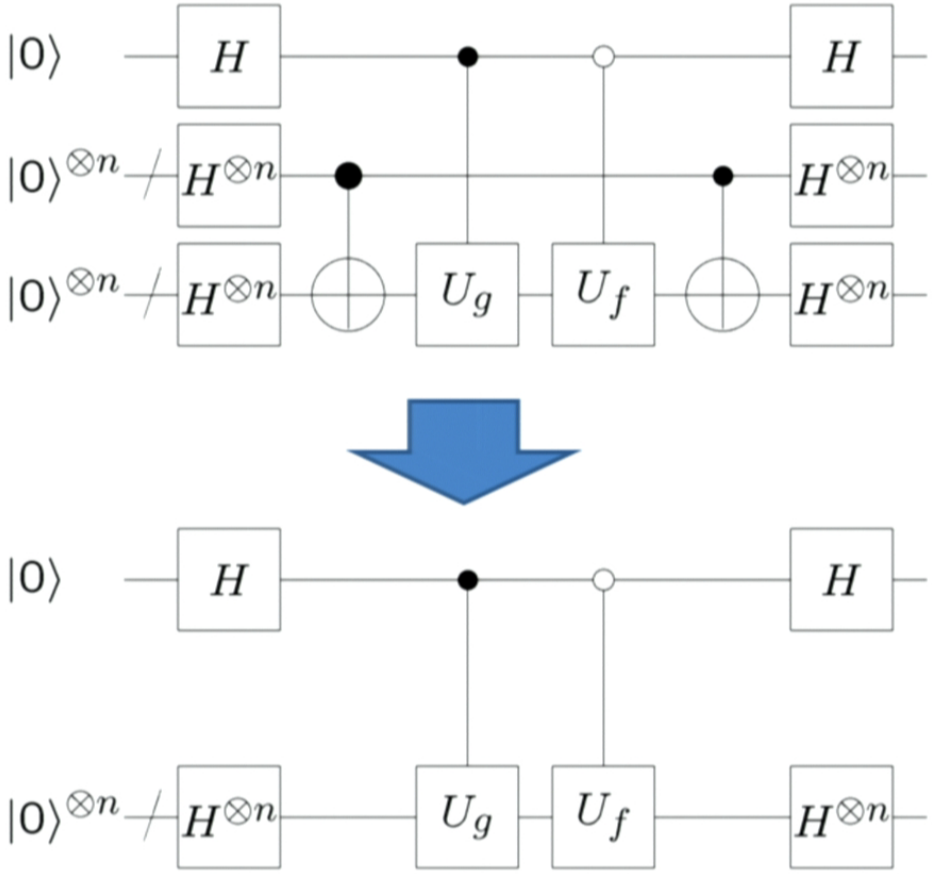
- In general for f, g injective, hidden shift can be reduced to a HSP.
- Not applicable here directly, since f, g might not be injective. But reduction is possible using quantum functions $F : x \mapsto \sum_{y \in \mathbb{Z}_2^n} (-1)^{f(x+y)} |y\rangle$
- Resulting quantum circuit:



- 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, arxiv:0811.3208]

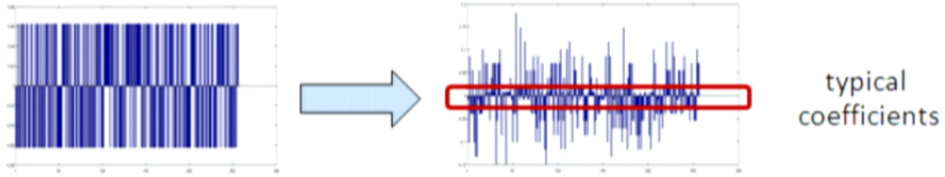
Simplifying the circuit



Sampling approach

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

- **Sampling Subroutine:** Measure this state in the computational basis. This will give as 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".



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 $\dim(\mathrm{Span}\{u_k | k \in [i]\}) > \dim(V_i)$ 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

$$\begin{cases} \langle u_1, s \rangle = 0 \\ \quad \cdots \\ \langle u_t, s \rangle = 0. \end{cases}$$

Analyzing the algorithm

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

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

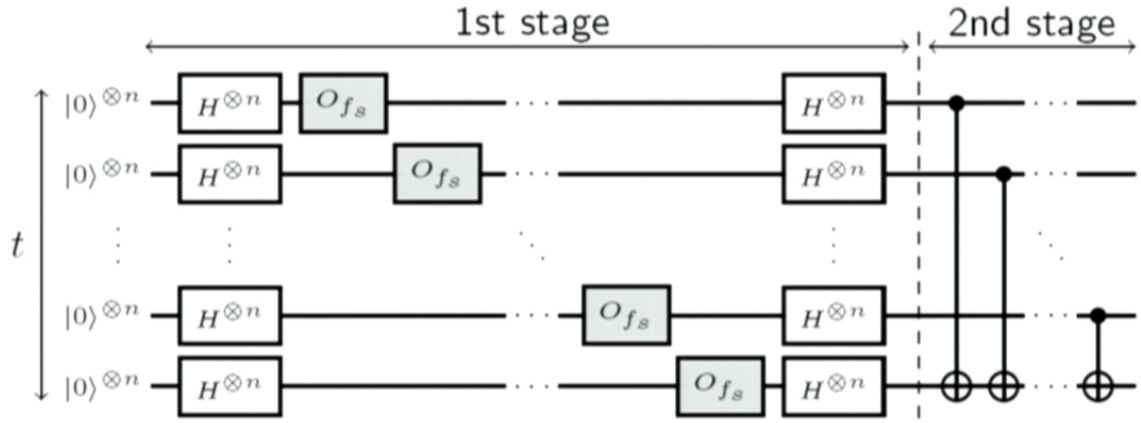
and $\mathbf{E}(\#queries) \leq \frac{n}{\gamma_f}$ for the expected time until s is characterized.

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 $(\mathcal{O}_f, \mathcal{O}_g)$ 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.

[Gavinsky, R., Roland, COCOON'11, arxiv:1103.3017]

PGM approach



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

After stage 2: $|\Phi^t(s)\rangle := \sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}|\mathcal{F}_w^t\rangle|w\rangle$

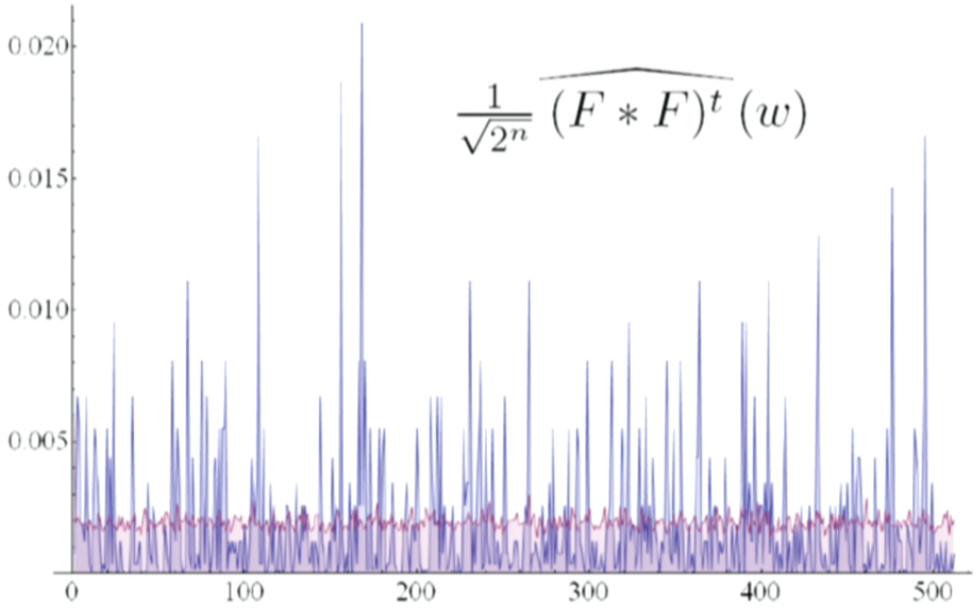
PGM: $|E_s^t\rangle := \frac{1}{\sqrt{2^n}}\sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}\frac{|\mathcal{F}_w^t\rangle}{\||\mathcal{F}_w^t\rangle\|_2}|w\rangle$

E.g., for $t=1$: $|E_s^1\rangle := \frac{1}{\sqrt{2^n}}\sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}\frac{\hat{F}(w)}{|\hat{F}(w)|}|w\rangle$

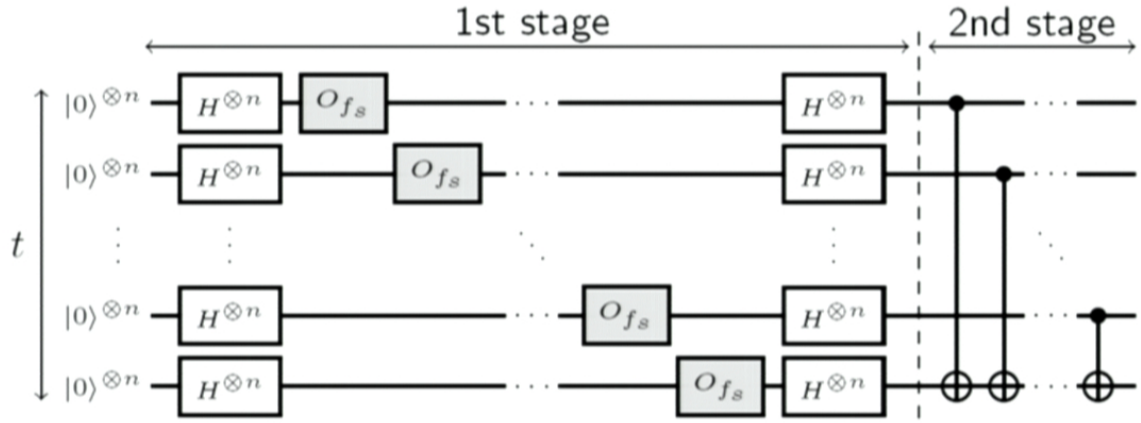
Work in progress with A. Childs and M. Ozols and J. Roland

The effect of increasing *t*

- States: $|\Phi^t(s)\rangle := \sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}|\mathcal{F}_w^t\rangle|w\rangle$
  where $\||\mathcal{F}_w^t\rangle\|_2^2 = \left[\hat{F}^2\right]^{*t}(w) = \frac{1}{\sqrt{2^n}}\widehat{(F*F)^t}(w)$
- Convolution: $(F*F)(w) = \sum_{x\in\mathbb{Z}_2^n} F(x)F(w-x)$



PGM approach



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

After stage 2: $|\Phi^t(s)\rangle := \sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}|\mathcal{F}_w^t\rangle|w\rangle$

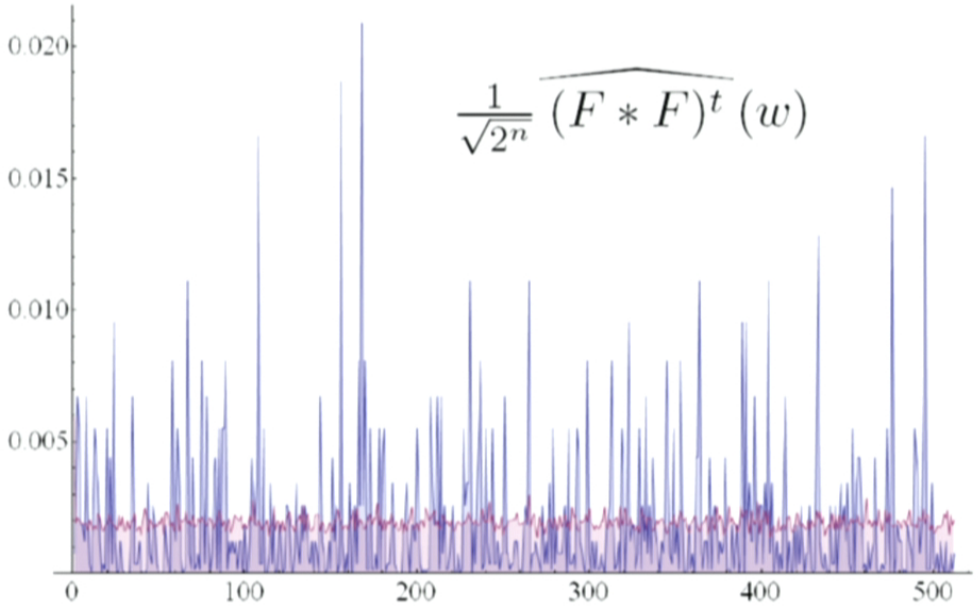
PGM: $|E_s^t\rangle := \frac{1}{\sqrt{2^n}}\sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}\frac{|\mathcal{F}_w^t\rangle}{\||\mathcal{F}_w^t\rangle\|_2}|w\rangle$

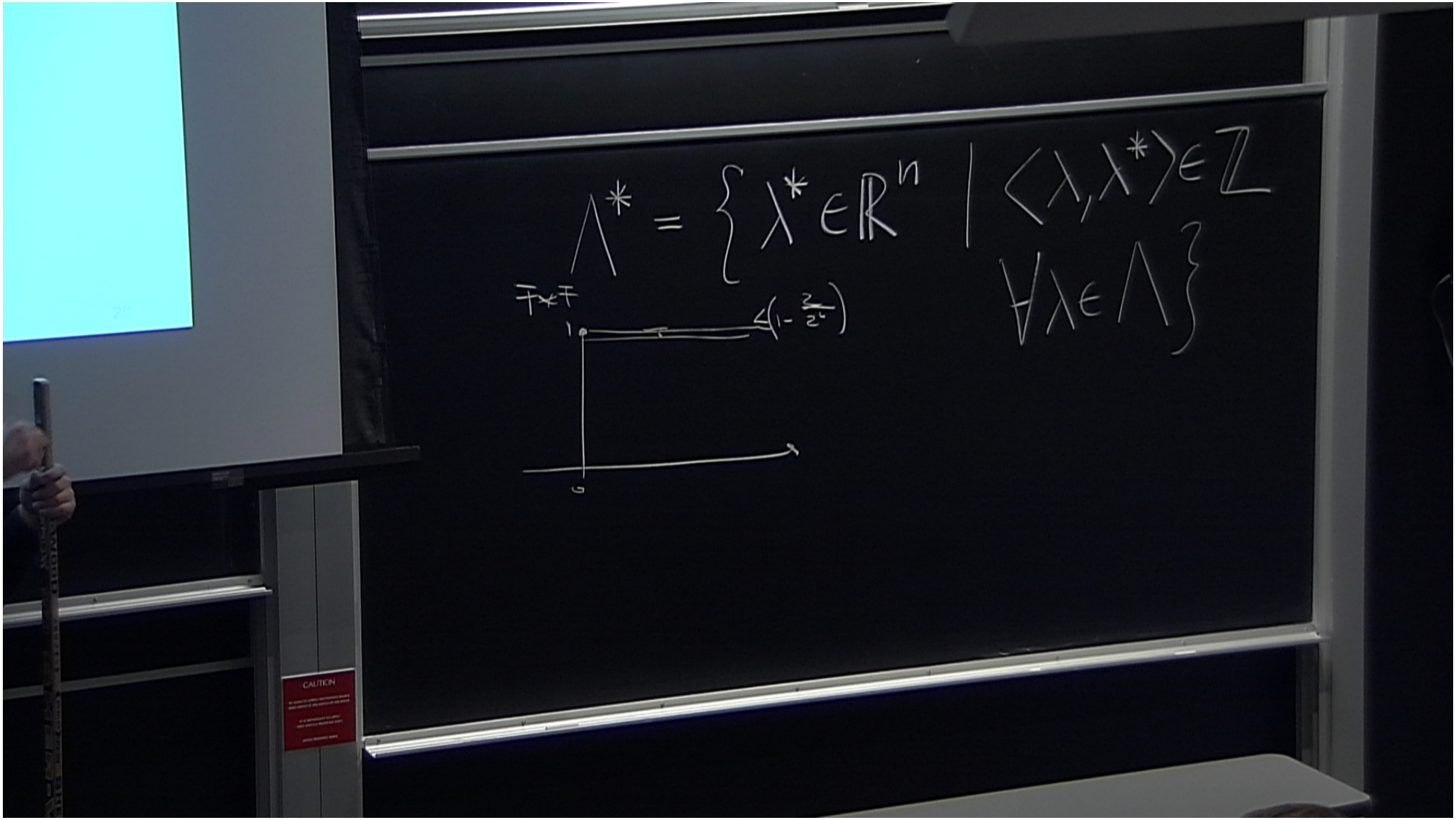
E.g., for $t=1$: $|E_s^1\rangle := \frac{1}{\sqrt{2^n}}\sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}\frac{\hat{F}(w)}{|\hat{F}(w)|}|w\rangle$

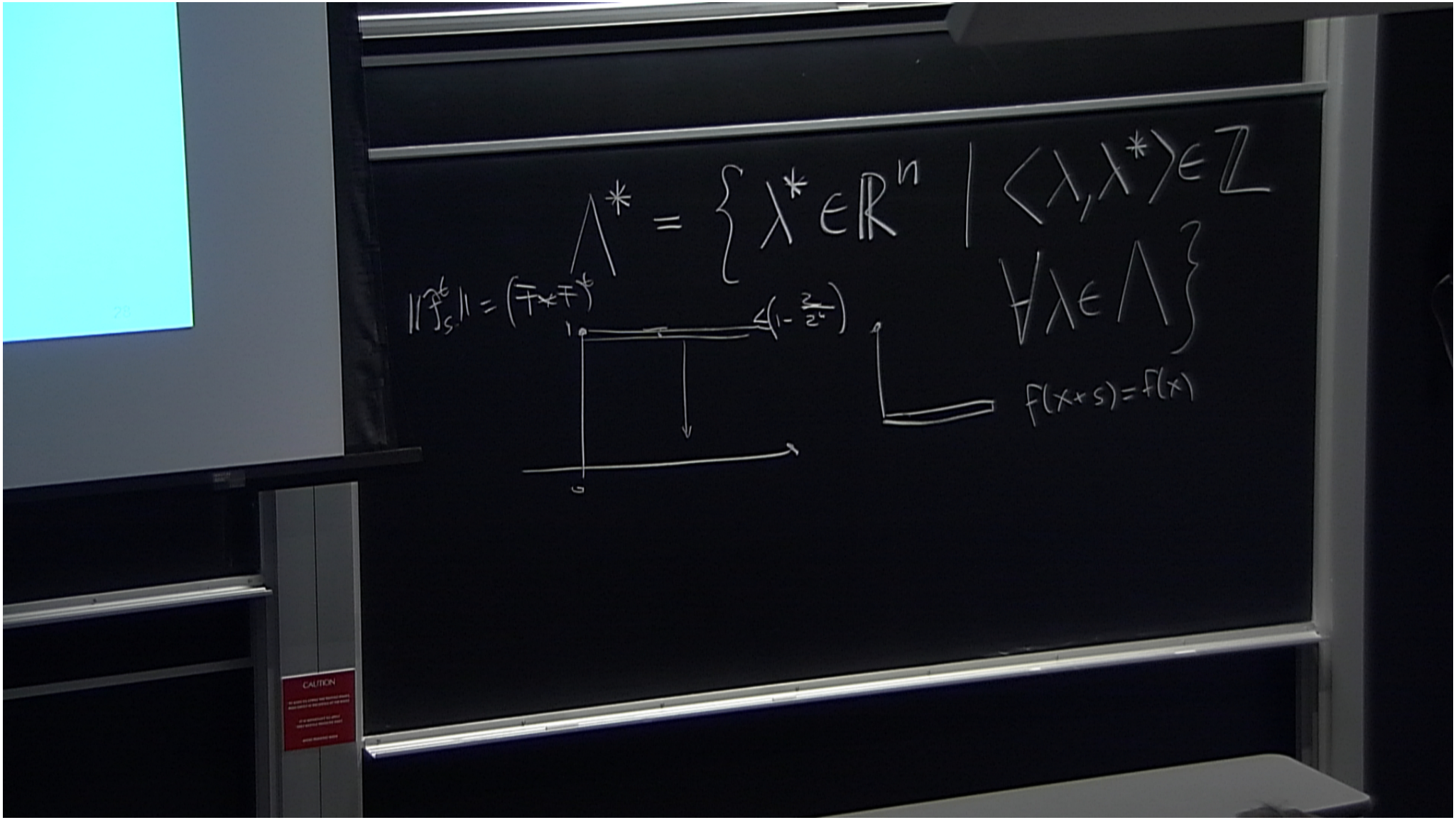
Work in progress with A. Childs and M. Ozols and J. Roland

The effect of increasing *t*

- States: $|\Phi^t(s)\rangle := \sum_{w\in\mathbb{Z}_2^n}(-1)^{s\cdot w}|\mathcal{F}_w^t\rangle|w\rangle$
  where $\||\mathcal{F}_w^t\rangle\|_2^2 = \left[\hat{F}^2\right]^{*t}(w) = \frac{1}{\sqrt{2^n}}\widehat{(F*F)^t}(w)$
- Convolution: $(F*F)(w) = \sum_{x\in\mathbb{Z}_2^n} F(x)F(w-x)$




$\Lambda^* = \{\lambda^* \in \mathbb{R}^n \mid \langle \lambda, \lambda^* \rangle \in \mathbb{Z}$
$\forall \lambda \in \Lambda\}$
$\frac{1}{2} \times \frac{1}{2}$
$< (1 - \frac{2}{2^n})$
1
0
CAUTION


$\Lambda^* = \{\lambda^* \in \mathbb{R}^n \mid \langle \lambda, \lambda^* \rangle \in \mathbb{Z} \; \forall \lambda \in \Lambda\}$
$\|f_s^{\otimes k}\| = (f * f^{\vee})^{\otimes k}$
$\leq (1 - \frac{3}{2^k})$
$f(x+s) = f(x)$
CAUTION

Open problems

- "Coherent" version of previous algorithm?

$$\sum_u \left(1 + (-1)^{-us}\right) \widehat{F}(u) \, |u\rangle$$

  - Can we uncompute the Fourier spectrum $\widehat{F}(u)$? In other words, for a function given by an oracle, can we implement its Fourier transform?
  - If not, can we approximately implement $\widehat{F}$? If not, then why not?
  - Explore relation to the problem of deciding "forrelated" functions [Aaronson'09] and the sampling/searching problem [Aaronson'10].

- Show advantage of applying PGM approach to hidden shift problem.
  - Combine with rejection sampling? (while bounding query complexity)
  - Improvement by considering several registers?

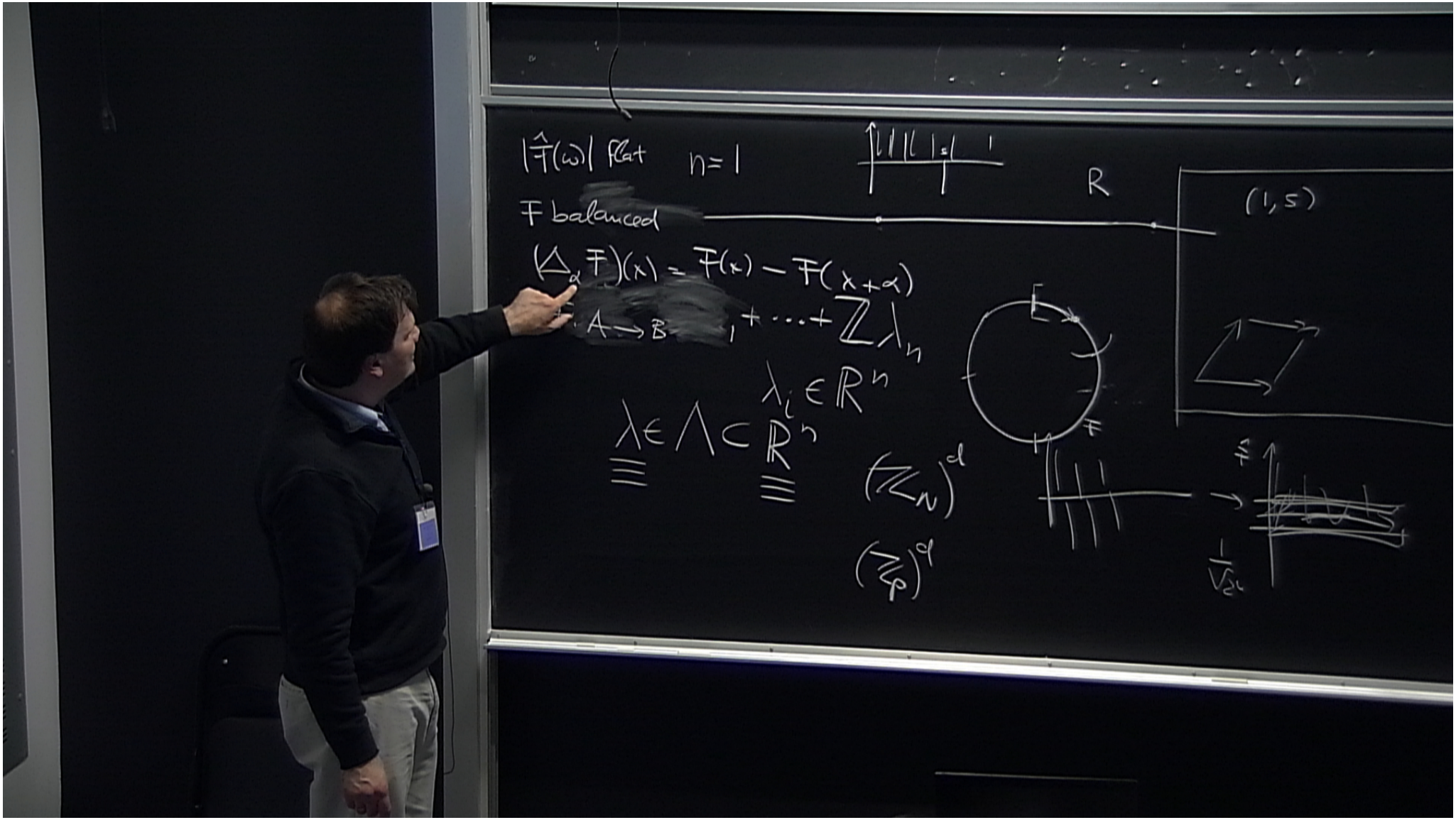
- Applications of hidden shift for Boolean functions?
  - Quantum cryptanalysis?

Conclusions

- **Hidden shift problems**
  - Motivation: Legendre function, bent functions
  - Connection to hidden subgroup problem
  - Special case: random functions
  - Exponential q/c query complexity separation

- **Some approaches to hidden shift problems**
  - Sampling based approach
  - Correlation based approach; quantum state resampling problem
    - Amplitude amplification ("quantum rejection sampling")
    - Optimal rotation vector determined by SDP
  - Multi-register (PGM) approach

- **Acknowledgment of support:**


$|\hat{F}(\omega)|$ flat
$n=1$
R
F balanced
$(\Delta_\alpha F)(x) = F(x) - F(x+\alpha)$
$F: A \to B$
$\lambda_1 + \cdots + \mathbb{Z}\lambda_n$
$\lambda_i \in R^n$
$\lambda \in \Lambda \subset R^n$
$(\mathbb{Z}_N)^d$
$(\mathbb{Z}_p)^d$
(1, 5)