Quantum algorithms for hidden nonlinear structures

Andrew Childs
Waterloo

Leonard Schulman
Caltech

Umesh Vazirani
Berkeley

Shor's algorithm finds hidden linear structures

[Shor 94]: Efficient quantum algorithms for factoring integers and calculating discrete logarithms.

Shor's algorithm finds hidden linear structures

[Shor 94]: Efficient quantum algorithms for factoring integers and calculating discrete logarithms.

Factoring $\rightarrow$ Period finding over $\mathbb{Z}$

(hidden linear structure in one dimension)

Shor's algorithm finds hidden linear structures

[Shor 94]: Efficient quantum algorithms for factoring integers and calculating discrete logarithms.

Factoring	→	Period finding over $\mathbb{Z}$ (hidden linear structure in one dimension)
Discrete log	→	Finding a hidden line in $\mathbb{Z}_p \times \mathbb{Z}_p$ (hidden linear structure in two dimensions)

Shor's algorithm finds hidden linear structures

[Shor 94]: Efficient quantum algorithms for factoring integers and calculating discrete logarithms.

Factoring	→	Period finding over $\mathbb{Z}$ (hidden linear structure in one dimension)
Discrete log	→	Finding a hidden line in $\mathbb{Z}_p \times \mathbb{Z}_p$ (hidden linear structure in two dimensions)

Key idea: The Fourier transform of a linear structure exhibits sharp constructive interference that reveals the answer.

Shor's algorithm finds hidden linear structures

[Shor 94]: Efficient quantum algorithms for factoring integers and calculating discrete logarithms.

Factoring $\rightarrow$ Period finding over $\mathbb{Z}$
(hidden linear structure in one dimension)

Discrete log $\rightarrow$ Finding a hidden line in $\mathbb{Z}_p \times \mathbb{Z}_p$
(hidden linear structure in two dimensions)

Key idea: The Fourier transform of a linear structure exhibits sharp constructive interference that reveals the answer.

Are there other ways to create sharp constructive interference over a high-dimensional space?

Beyond Shor: The hidden subgroup problem

One way to generalize: Find hidden linear structures (i.e., *subgroups* and their *cosets*) in more general (possibly non-abelian) groups.

Beyond Shor: The hidden subgroup problem

One way to generalize: Find hidden linear structures (i.e., *subgroups* and their *cosets*) in more general (possibly non-abelian) groups.

Tool for exploiting interference: Non-abelian Fourier analysis

Beyond Shor: The hidden subgroup problem

One way to generalize: Find hidden linear structures (i.e., *subgroups* and their *cosets*) in more general (possibly non-abelian) groups.

Tool for exploiting interference: Non-abelian Fourier analysis

Potential applications are exciting:

Symmetric group	Graph automorphism, graph isomorphism
Dihedral group	Finding short lattice vectors [Regev 03]

Beyond Shor: The hidden subgroup problem

One way to generalize: Find hidden linear structures (i.e., *subgroups* and their *cosets*) in more general (possibly non-abelian) groups.

Tool for exploiting interference: Non-abelian Fourier analysis

Potential applications are exciting:

Symmetric group	Graph automorphism, graph isomorphism
Dihedral group	Finding short lattice vectors [Regev 03]

... but these cases appear hard.

courtesy of the NAIC Arecibo Observatory, a facility of the NSF


$(\mathbb{F}_q)^d$
courtesy of the NAIC Arecibo Observatory, a facility of the NSF


$(\mathbb{F}_q)^d$
d fixed
degree fixed
$q \to \infty$
courtesy of the NAIC Arecibo Observatory, a facility of the NSF

Quantum computers can find hidden nonlinear structures

Shifted subset problems

Two examples:

- Hidden radius problem (partial solution, by *Fourier sampling*)
- Hidden flat of centers problem (complete solution for d odd, by *quantum walk*)

Both have:

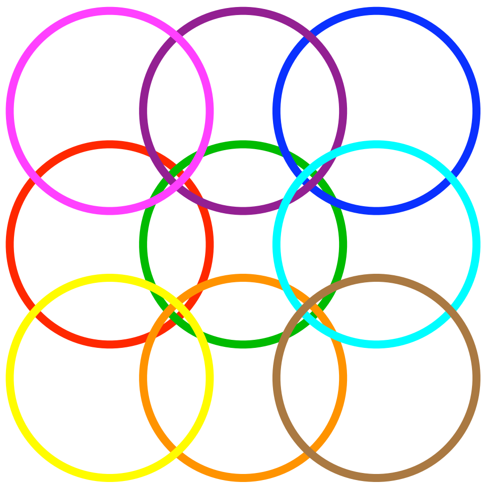
- Polynomial-time quantum algorithms
- A black-box formulation with exponential classical query complexity

Hidden polynomial problem

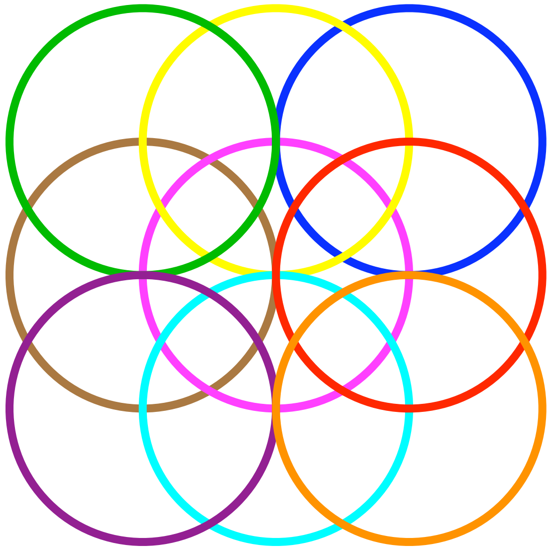
- Naturally formulated as a black-box problem with exponential classical query complexity
- Quantum query complexity is polynomial

Hidden radius problem

Quantum formulation: Suppose we can sample a quantum state that is uniform over points on a sphere of radius r, with the center chosen uniformly at random.



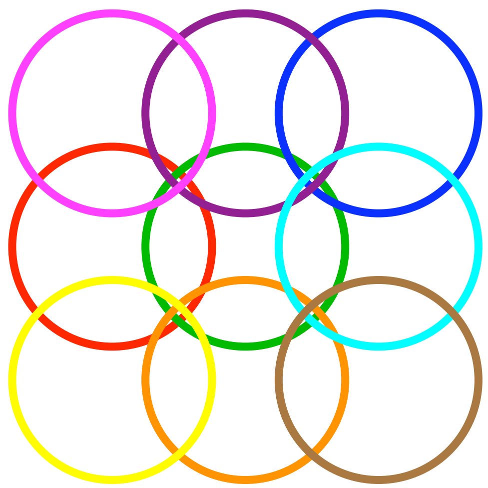
or



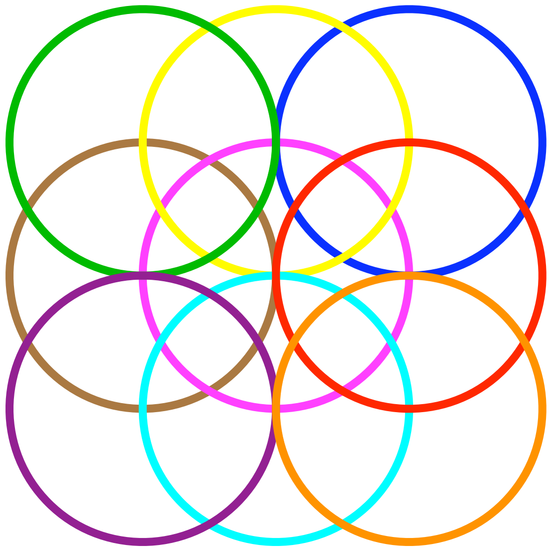
or ...

Hidden radius problem

Quantum formulation: Suppose we can sample a quantum state that is uniform over points on a sphere of radius r, with the center chosen uniformly at random.



or

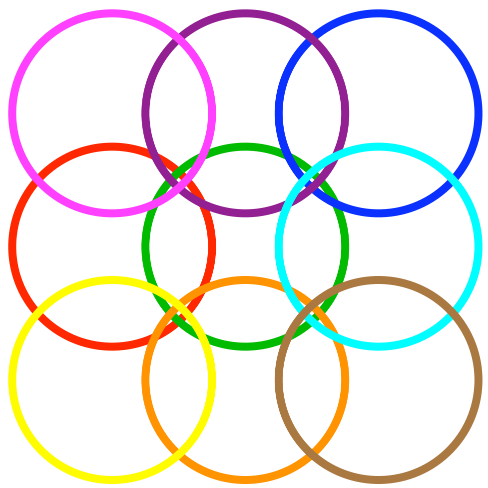


or ...

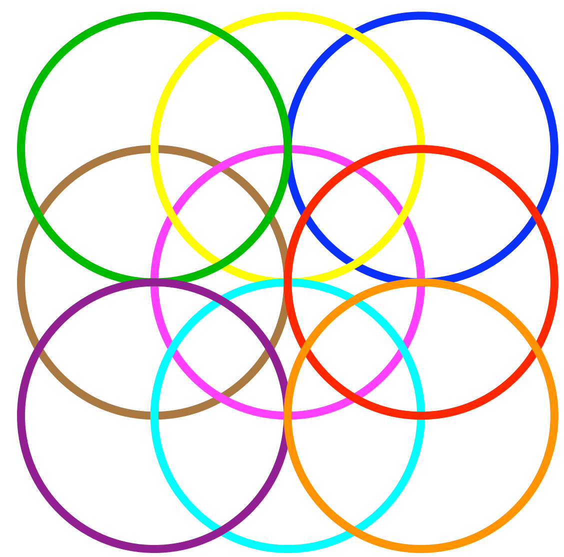
(There is a black-box version of this problem in which a quantum computer can produce these states, but a classical computer requires exponentially many queries (in $\log q$) to determine any bit of r.)

Hidden radius problem

Quantum formulation: Suppose we can sample a quantum state that is uniform over points on a sphere of radius r, with the center chosen uniformly at random.



or



or $\ldots$

(There is a black-box version of this problem in which a quantum computer can produce these states, but a classical computer requires exponentially many queries (in $\log q$) to determine any bit of r.)

Theorem. There is quantum algorithm that determines $\chi(r)$ in time $\mathrm{poly}(\log q)$, provided $d = O(1)$ is odd.

quadratic character

The Fourier transform of a sphere

From symmetry considerations, we should perform a d-dimensional Fourier transform. What does the resulting state look like?

The Fourier transform of a sphere

From symmetry considerations, we should perform a d-dimensional Fourier transform. What does the resulting state look like?

$$\sum_{\substack{x \in \mathbb{F}_q \\ x \cdot x = 1}} \omega_p^{\mathrm{tr}(k \cdot x)}$$

The Fourier transform of a sphere

From symmetry considerations, we should perform a d-dimensional Fourier transform. What does the resulting state look like?

$$\sum_{\substack{x \in \mathbb{F}_q \\ x \cdot x = 1}} \omega_p^{\mathrm{tr}(k \cdot x)} = e^{i\phi} \sqrt{q^{d-2}}\, K_{\chi^d}\left(\tfrac{k \cdot k}{4}\right)$$

where $K_\eta(a) := \sum_{x \in \mathbb{F}_q} \eta(x)\, \omega_p^{\mathrm{tr}(ax + x^{-1})}$ η-twisted Kloosterman sum

The Fourier transform of a sphere

From symmetry considerations, we should perform a d-dimensional Fourier transform. What does the resulting state look like?

$$\sum_{\substack{x\in\mathbb{F}_q \\ x\cdot x=1}} \omega_p^{\mathrm{tr}(k\cdot x)} = e^{i\phi}\sqrt{q^{d-2}}\,K_{\chi^d}\left(\tfrac{k\cdot k}{4}\right)$$

where $K_\eta(a) := \sum_{x\in\mathbb{F}_q} \eta(x)\,\omega_p^{\mathrm{tr}(ax+x^{-1})}$ η-twisted Kloosterman sum

Such sums have many interesting properties.
Theorem [Weil 48]. $|K_\eta(a)| \le 2\sqrt{q}$

The Fourier transform of a sphere

From symmetry considerations, we should perform a d-dimensional Fourier transform. What does the resulting state look like?

$$\sum_{\substack{x \in \mathbb{F}_q \\ x \cdot x = 1}} \omega_p^{\mathrm{tr}(k \cdot x)} = e^{i\phi} \sqrt{q^{d-2}}\, K_{\chi^d}\left(\tfrac{k \cdot k}{4}\right)$$

where $K_\eta(a) := \sum_{x \in \mathbb{F}_q} \eta(x)\, \omega_p^{\mathrm{tr}(ax + x^{-1})}$ η-twisted Kloosterman sum

Such sums have many interesting properties.
Theorem [Weil 48]. $|K_\eta(a)| \leq 2\sqrt{q}$

Even d: Regular Kloosterman sum ($\eta = 1$). Hard to compute?

The Fourier transform of a sphere

From symmetry considerations, we should perform a d-dimensional Fourier transform. What does the resulting state look like?

$$\sum_{\substack{x \in \mathbb{F}_q \\ x \cdot x = 1}} \omega_p^{\operatorname{tr}(k \cdot x)} = e^{i\phi} \sqrt{q^{d-2}}\, K_{\chi^d}\left(\tfrac{k \cdot k}{4}\right)$$

where $K_\eta(a) := \sum_{x \in \mathbb{F}_q} \eta(x)\, \omega_p^{\operatorname{tr}(ax + x^{-1})}$ η-twisted Kloosterman sum

Such sums have many interesting properties.
Theorem [Weil 48]. $|K_\eta(a)| \leq 2\sqrt{q}$

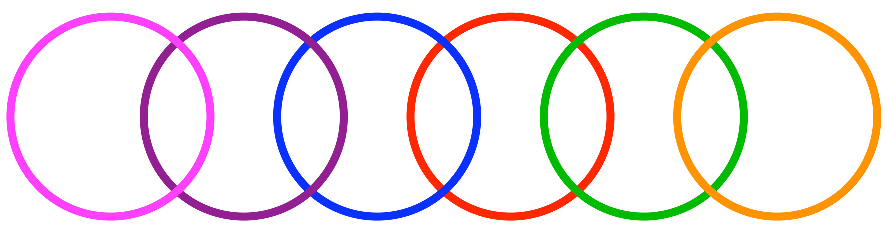
Even d: Regular Kloosterman sum ($\eta = 1$). Hard to compute?

Odd d: Salié sum ($\eta = \chi$).

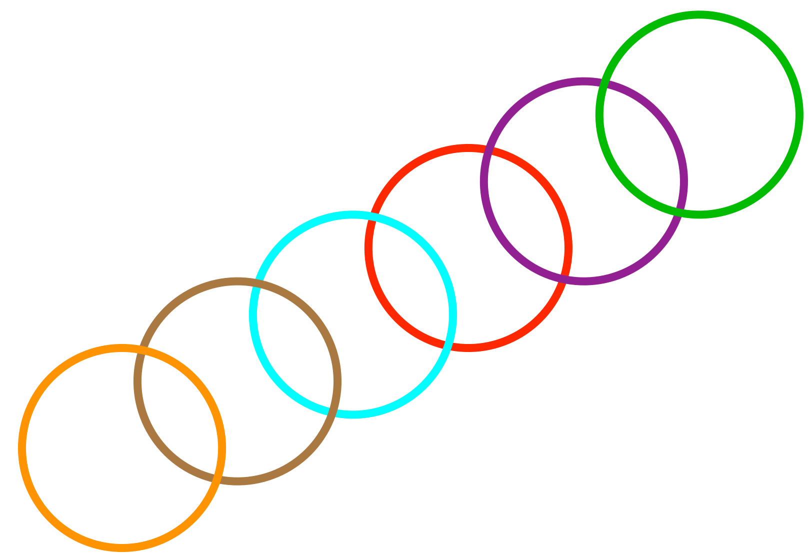
$$K_\chi(a) = e^{i\phi}\sqrt{q} \begin{cases} 1 & a = 0 \\ 2\cos \frac{4\pi \operatorname{tr}(\sqrt{a})}{p} & \chi(a) = +1 \\ 0 & \chi(a) = -1 \end{cases}$$

Hidden flat of centers problem

Quantum formulation: Suppose we can sample a quantum state that is a uniform superposition over points on a sphere of radius 1, with the center chosen uniformly at random from an unknown flat.



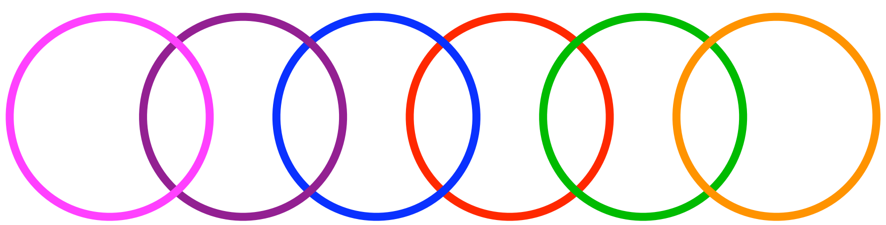
or



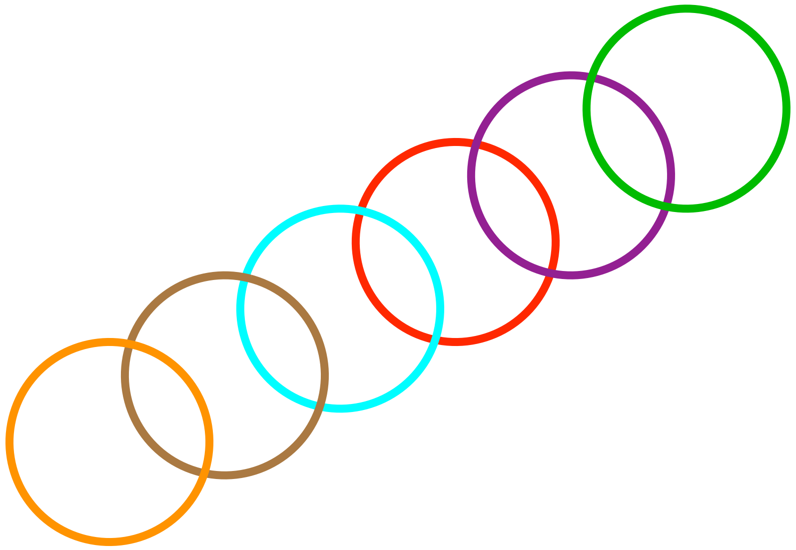
or $\ldots$

Hidden flat of centers problem

Quantum formulation: Suppose we can sample a quantum state that is a uniform superposition over points on a sphere of radius 1, with the center chosen uniformly at random from an unknown flat.



or

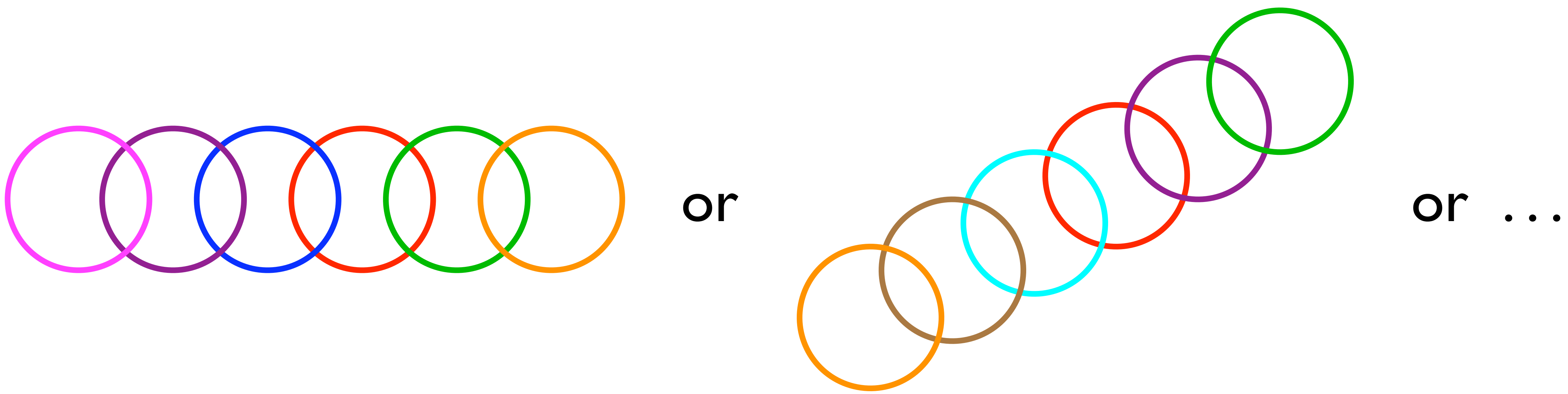


or ...

(There is a black-box version of this problem in which a quantum computer can produce these states, but a classical computer requires exponentially many queries (in $\log q$) to determine the flat.)

Hidden flat of centers problem

Quantum formulation: Suppose we can sample a quantum state that is a uniform superposition over points on a sphere of radius 1, with the center chosen uniformly at random from an unknown flat.



(There is a black-box version of this problem in which a quantum computer can produce these states, but a classical computer requires exponentially many queries (in $\log q$) to determine the flat.)

Theorem. There is quantum algorithm that finds the hidden flat in time $\mathrm{poly}(\log q)$, provided $d = O(1)$ is odd.

Quantum walk on the Winnie Li graph

Vertices: Points $x \in \mathbb{F}_q^d$

Edges: $x \sim y$ iff $(x-y)\cdot(x-y) = 1$ (y on unit sphere centered at x)

Quantum walk on the Winnie Li graph

Vertices: Points $x \in \mathbb{F}_q^d$

Edges: $x \sim y$ iff $(x-y) \cdot (x-y) = 1$ (y on unit sphere centered at x)

Continuous-time quantum walk: Unitary operator e^{-iAt}

adjacency matrix

Quantum walk on the Winnie Li graph

Vertices: Points $x \in \mathbb{F}_q^d$

Edges: $x \sim y$ iff $(x-y) \cdot (x-y) = 1$ (y on unit sphere centered at x)

Continuous-time quantum walk: Unitary operator e^{-iAt}

adjacency matrix

Eigenvalues are χ^d-twisted Kloosterman sums. Can be computed efficiently for d odd, giving an implementation of the quantum walk.

Quantum walk on the Winnie Li graph

Vertices: Points $x \in \mathbb{F}_q^d$

Edges: $x \sim y$ iff $(x-y)\cdot(x-y) = 1$ (y on unit sphere centered at x)

Continuous-time quantum walk: Unitary operator e^{-iAt}

adjacency matrix

Eigenvalues are χ^d-twisted Kloosterman sums. Can be computed efficiently for d odd, giving an implementation of the quantum walk.

Quantum walk (for an appropriately chosen, short time) moves substantial amplitude (fraction $1/\mathrm{poly}(\log q)$) from a sphere to its center.

Quantum walk on the Winnie Li graph

Vertices: Points $x \in \mathbb{F}_q^d$

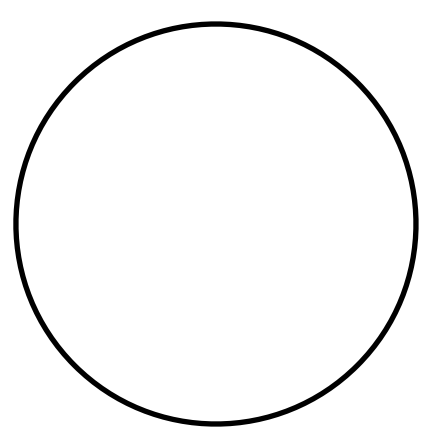
Edges: $x \sim y$ iff $(x-y)\cdot(x-y) = 1$ (y on unit sphere centered at x)

Continuous-time quantum walk: Unitary operator e^{-iAt}

adjacency matrix

Eigenvalues are χ^d-twisted Kloosterman sums. Can be computed efficiently for d odd, giving an implementation of the quantum walk.

Quantum walk (for an appropriately chosen, short time) moves substantial amplitude (fraction $1/\mathrm{poly}(\log q)$) from a sphere to its center.



Quantum walk on the Winnie Li graph

Vertices: Points $x \in \mathbb{F}_q^d$

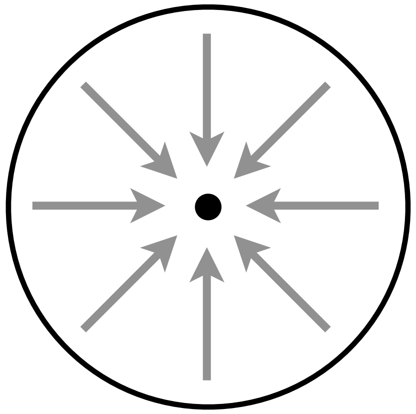
Edges: $x \sim y$ iff $(x-y)\cdot(x-y) = 1$ (y on unit sphere centered at x)

Continuous-time quantum walk: Unitary operator e^{-iAt}

adjacency matrix

Eigenvalues are χ^d-twisted Kloosterman sums. Can be computed efficiently for d odd, giving an implementation of the quantum walk.

Quantum walk (for an appropriately chosen, short time) moves substantial amplitude (fraction $1/\mathrm{poly}(\log q)$) from a sphere to its center.



Quantum walk on the Winnie Li graph

Vertices: Points $x \in \mathbb{F}_q^d$

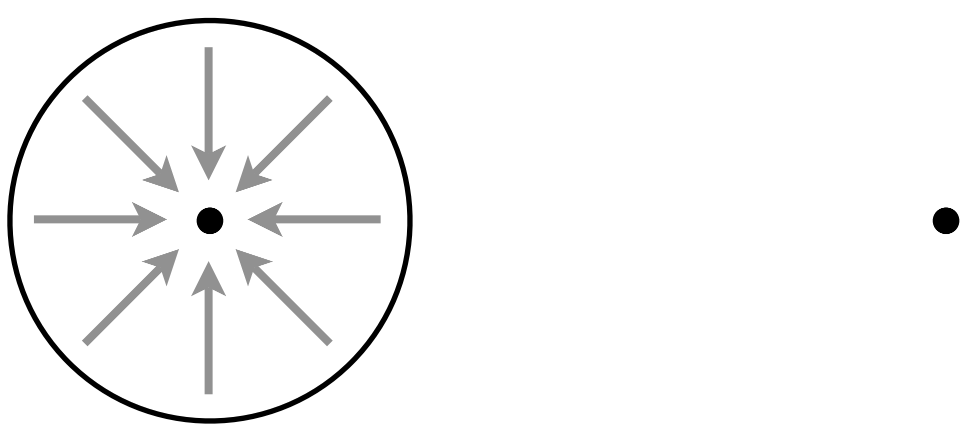
Edges: $x \sim y$ iff $(x-y)\cdot(x-y) = 1$ (y on unit sphere centered at x)

Continuous-time quantum walk: Unitary operator e^{-iAt}

adjacency matrix

Eigenvalues are χ^d-twisted Kloosterman sums. Can be computed efficiently for d odd, giving an implementation of the quantum walk.

Quantum walk (for an appropriately chosen, short time) moves substantial amplitude (fraction $1/\mathrm{poly}(\log q)$) from a sphere to its center.



Quantum walk on the Winnie Li graph

Vertices: Points $x \in \mathbb{F}_q^d$

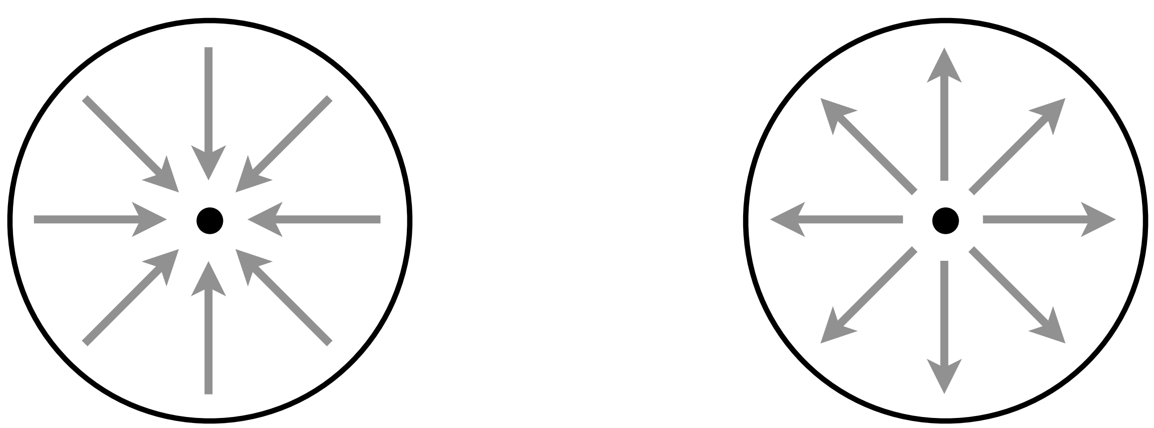
Edges: $x \sim y$ iff $(x-y)\cdot(x-y) = 1$ (y on unit sphere centered at x)

Continuous-time quantum walk: Unitary operator e^{-iAt}

adjacency matrix

Eigenvalues are χ^d-twisted Kloosterman sums. Can be computed efficiently for d odd, giving an implementation of the quantum walk.

Quantum walk (for an appropriately chosen, short time) moves substantial amplitude (fraction $1/\mathrm{poly}(\log q)$) from a sphere to its center.



Reconstructing a noisy flat

Given: Samples of points in $\mathbb{F}_q^d$ that are either

- Uniformly random in a d'-dimensional flat (probability $\frac{1}{\mathrm{poly}(\log q)}$)
- Nearly uniformly random in $\mathbb{F}_q^d$ (probability $\leq c/q^d$ for any point outside flat)

Reconstructing a noisy flat

Given: Samples of points in $\mathbb{F}_q^d$ that are either

- Uniformly random in a d'-dimensional flat (probability $\frac{1}{\mathrm{poly}(\log q)}$)
- Nearly uniformly random in $\mathbb{F}_q^d$ (probability $\leq c/q^d$ for any point outside flat)

Claim: Suppose we sample just enough points that with high probability, we see at least $4d'$ points from the hidden flat. Then the probability that there are $4d'$ or more points from any distinct d'-dimensional flat is exponentially small (in $\log q$).

Reconstructing a noisy flat

Given: Samples of points in $\mathbb{F}_q^d$ that are either

- Uniformly random in a d'-dimensional flat (probability $\frac{1}{\mathrm{poly}(\log q)}$)
- Nearly uniformly random in $\mathbb{F}_q^d$ (probability $\leq c/q^d$ for any point outside flat)

Claim: Suppose we sample just enough points that with high probability, we see at least $4d'$ points from the hidden flat. Then the probability that there are $4d'$ or more points from any distinct d'-dimensional flat is exponentially small (in $\log q$).

Thus we can find the hidden flat by sampling polynomially many points and exhaustively checking all sufficiently large (constant-size) subsets.

Reconstructing a noisy flat

Given: Samples of points in $\mathbb{F}_q^d$ that are either

- Uniformly random in a d'-dimensional flat (probability $\frac{1}{\mathrm{poly}(\log q)}$)
- Nearly uniformly random in $\mathbb{F}_q^d$ (probability $\leq c/q^d$ for any point outside flat)

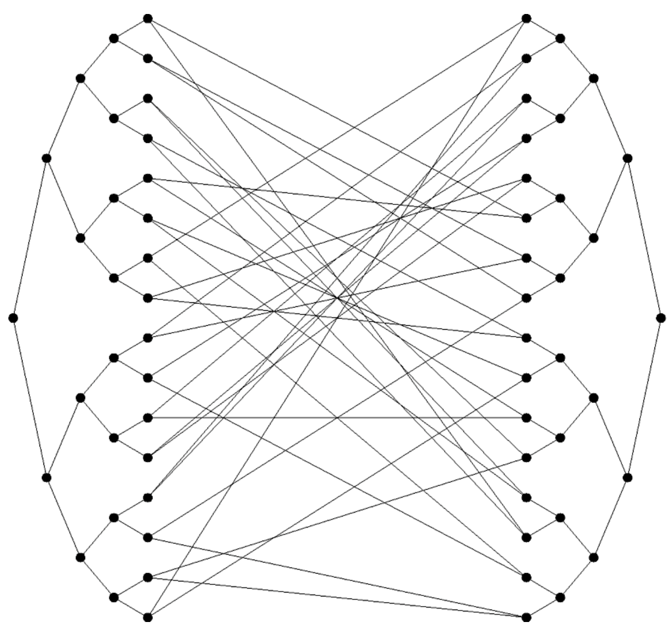
Claim: Suppose we sample just enough points that with high probability, we see at least $4d'$ points from the hidden flat. Then the probability that there are $4d'$ or more points from any distinct d'-dimensional flat is exponentially small (in $\log q$).

Thus we can find the hidden flat by sampling polynomially many points and exhaustively checking all sufficiently large (constant-size) subsets.

Note: It is crucial here that $d = O(1)$.

Exponential speedups by quantum walk

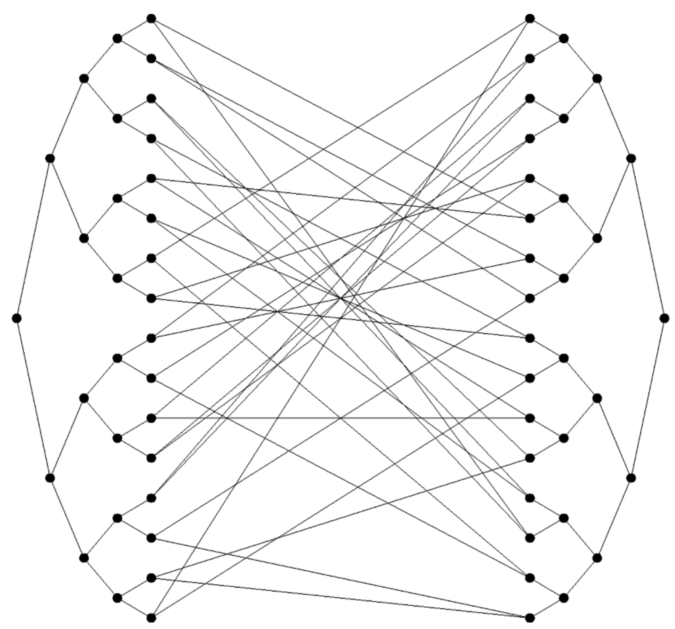
[C., Cleve, Deotto, Farhi, Gutmann, Spielman 03]:



Constructive interference takes us to a *distant* vertex

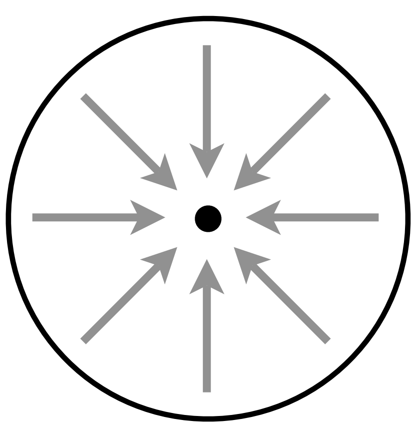
Exponential speedups by quantum walk

[C., Cleve, Deotto, Farhi, Gutmann, Spielman 03]:



Constructive interference takes us to a *distant* vertex

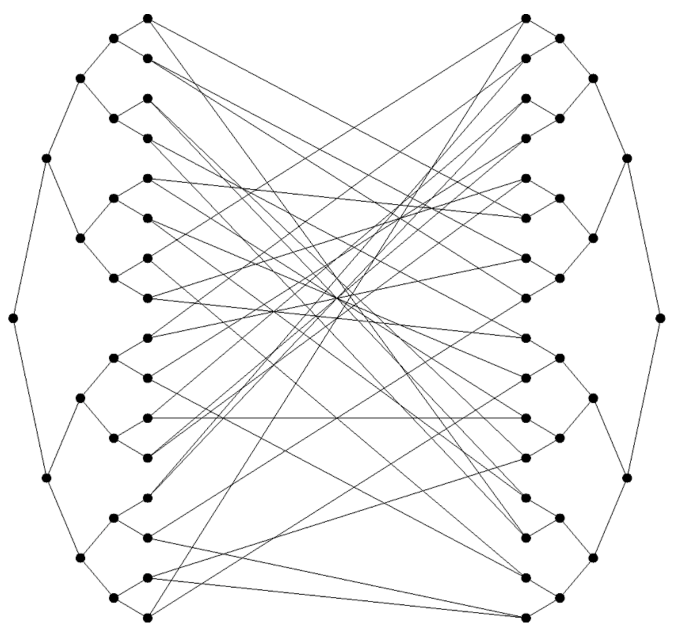
Hidden flat of centers algorithm:



Constructive interference takes us to a *nearby* vertex

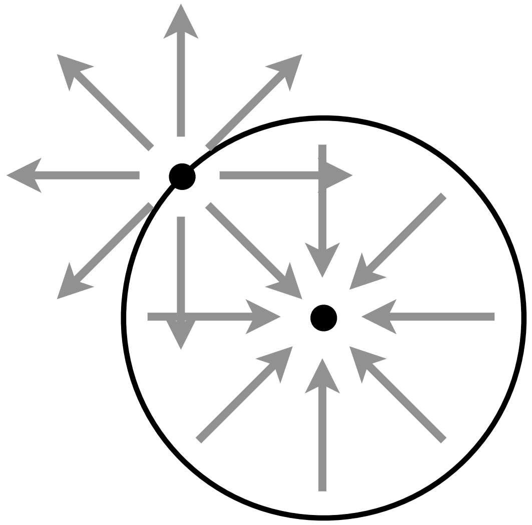
Exponential speedups by quantum walk

[C., Cleve, Deotto, Farhi, Gutmann, Spielman 03]:



Constructive interference takes us to a *distant* vertex

Hidden flat of centers algorithm:



Constructive interference takes us to a *nearby* vertex

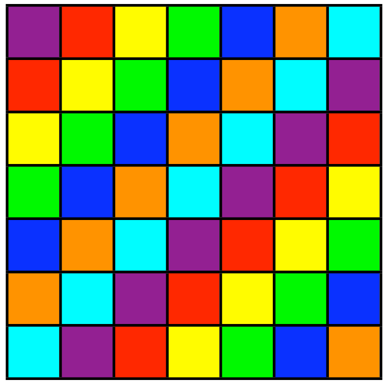
The hidden polynomial problem

Problem: Given a black-box function that is constant on the level sets of $f \in \mathbb{F}_q[x_1, \ldots, x_d]$ (of constant total degree), and distinct on different level sets, determine f (projectively).

The hidden polynomial problem

Problem: Given a black-box function that is constant on the level sets of $f \in \mathbb{F}_q[x_1, \ldots, x_d]$ (of constant total degree), and distinct on different level sets, determine f (projectively).

Linear f:

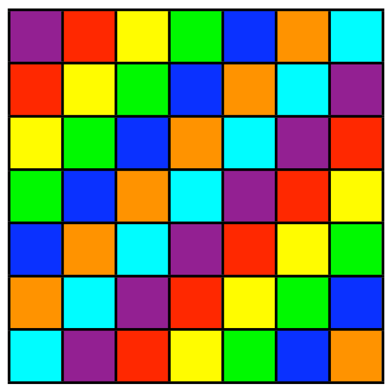


$x - y$

The hidden polynomial problem

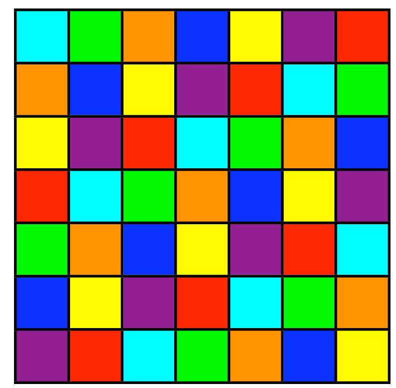
Problem: Given a black-box function that is constant on the level sets of $f \in \mathbb{F}_q[x_1, \ldots, x_d]$ (of constant total degree), and distinct on different level sets, determine f (projectively).

Linear f:



$x - y$

,



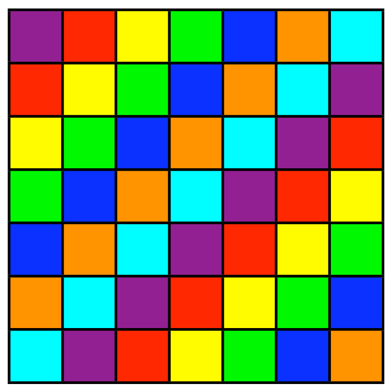
$x - 2y$

$, \quad \ldots$

The hidden polynomial problem

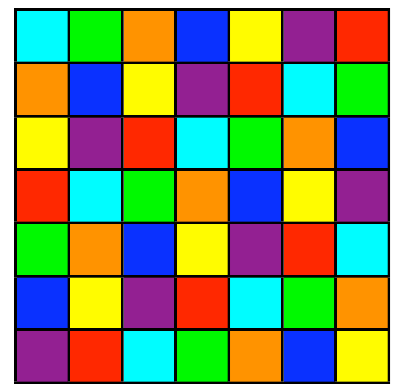
Problem: Given a black-box function that is constant on the level sets of $f \in \mathbb{F}_q[x_1, \ldots, x_d]$ (of constant total degree), and distinct on different level sets, determine f (projectively).

Linear f:



$x - y$

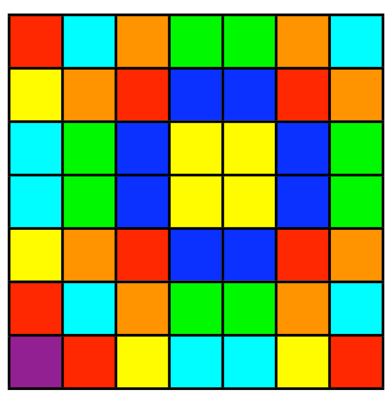
,



$x - 2y$

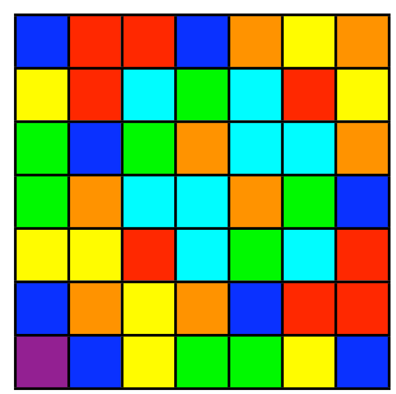
, $\ldots$

Quadratic f:



$x^2 + y^2$

,



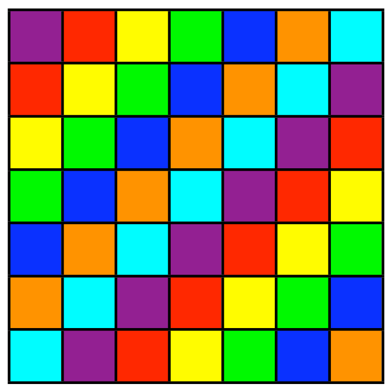
$x^2 + xy + 3y^2$

, $\ldots$

The hidden polynomial problem

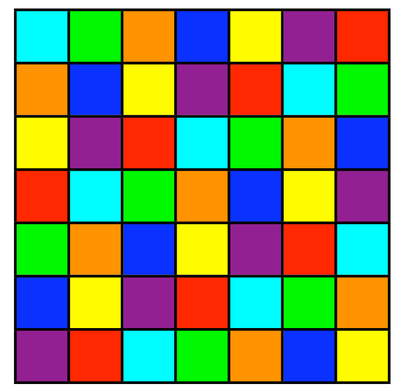
Problem: Given a black-box function that is constant on the level sets of $f \in \mathbb{F}_q[x_1, \ldots, x_d]$ (of constant total degree), and distinct on different level sets, determine f (projectively).

Linear f:



$x - y$

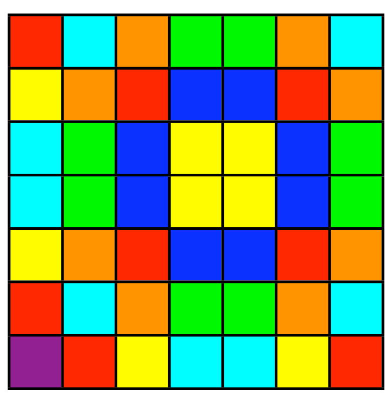
,



$x - 2y$

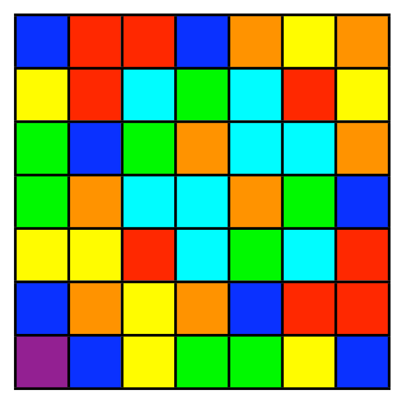
, $\ldots$

Quadratic f:



$x^2 + y^2$

,



$x^2 + xy + 3y^2$

, $\ldots$

Classical query complexity is exponential in $\log q$ (because it's hard to even find a collision).

Quantum query complexity of the HPP

Theorem. The quantum query complexity of the hidden polynomial problem is $\mathrm{poly}(\log q)$ for almost all polynomials.

Quantum query complexity of the HPP

Theorem. The quantum query complexity of the hidden polynomial problem is $\mathrm{poly}(\log q)$ for almost all polynomials.

Proof idea:

- By standard techniques, reduce to a problem of distinguishing quantum states
- States are distinguishable if the level sets of the polynomials have small intersection
- Typical size of a level set: $c\, q^{d-1}$ [Schwartz-Zippel]
- Typical size of the intersection of two level sets: $c'\, q^{d-2}$ [Weil]
- Almost all polynomials are absolutely irreducible

Open problems

Open problems

- Efficient quantum algorithms for approximating exponential sums
  - Gauss sums: [van Dam, Seroussi 02]
  - Small characteristic: Apply quantum point-counting algorithm of [Kedlaya 06] (as suggested by Shparlinski)
  - Kloosterman sums with prime characteristic?
  - General sums?

Open problems

- Efficient quantum algorithms for approximating exponential sums
  - Gauss sums: [van Dam, Seroussi 02]
  - Small characteristic: Apply quantum point-counting algorithm of [Kedlaya 06] (as suggested by Shparlinski)
  - Kloosterman sums with prime characteristic?
  - General sums?

- Efficient quantum algorithms for hidden polynomial problems
  - [Decker, Draisma, Wocjan 07]: Efficient quantum algorithm for $f(x_1, \ldots, x_{d-1}, x_d) = g(x_1, \ldots, x_{d-1}) - x_d$ (using PGM approach of [Bacon, C., van Dam 05])
  - Hidden rotation of a fixed-eccentricity ellipse?
  - General hidden polynomials?

Open problems

- Efficient quantum algorithms for approximating exponential sums
  - Gauss sums: [van Dam, Seroussi 02]
  - Small characteristic: Apply quantum point-counting algorithm of [Kedlaya 06] (as suggested by Shparlinski)
  - Kloosterman sums with prime characteristic?
  - General sums?
- Efficient quantum algorithms for hidden polynomial problems
  - [Decker, Draisma, Wocjan 07]: Efficient quantum algorithm for $f(x_1,\ldots,x_{d-1},x_d) = g(x_1,\ldots,x_{d-1}) - x_d$ (using PGM approach of [Bacon, C., van Dam 05])
  - Hidden rotation of a fixed-eccentricity ellipse?
  - General hidden polynomials?
- Applications?