Title: Quantum Algorithms Using Clebsch-Gordan Transforms

Date: May 16, 2007 04:00 PM

URL: http://pirsa.org/07050006

Abstract: In nearly every quantum algorithm which exponentially outperforms the best classical algorithm the quantum Fourier transform plays a central role. Recently, however, cracks in the quantum Fourier transform paradigm have begun to emerge. In this talk I will discuss one such development which arises in a new efficient quantum algorithm for the Heisenberg hidden subgroup problem. In particular I will show how considerations of symmetry for this hidden subgroup problem lead naturally to a different transform than the quantum Fourier transform, the Clebsch-Gordan transform over the Heisenberg group. Clebsch-Gordan transforms over finite groups thus appear to be an important new tool for those attempting to find new quantum algorithms. [Part of this work was done in collaboration with Andrew Childs (Caltech) and Wim van Dam (UCSB)]

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩
group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩
group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA
NSF
SCIENCE TO SHAPE THE FUTURE OF THE ARMY ARMY RESEARCH OFFICE 1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA
NSF
SCIENCE TO SHAPE THE FUTURE OF THE ARMY ARMY RESEARCH OFFICE 1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

$|QW\rangle$ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

$|QW\rangle$ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩
group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

$|QW\rangle$ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩ group

"Que Dubayah"

Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

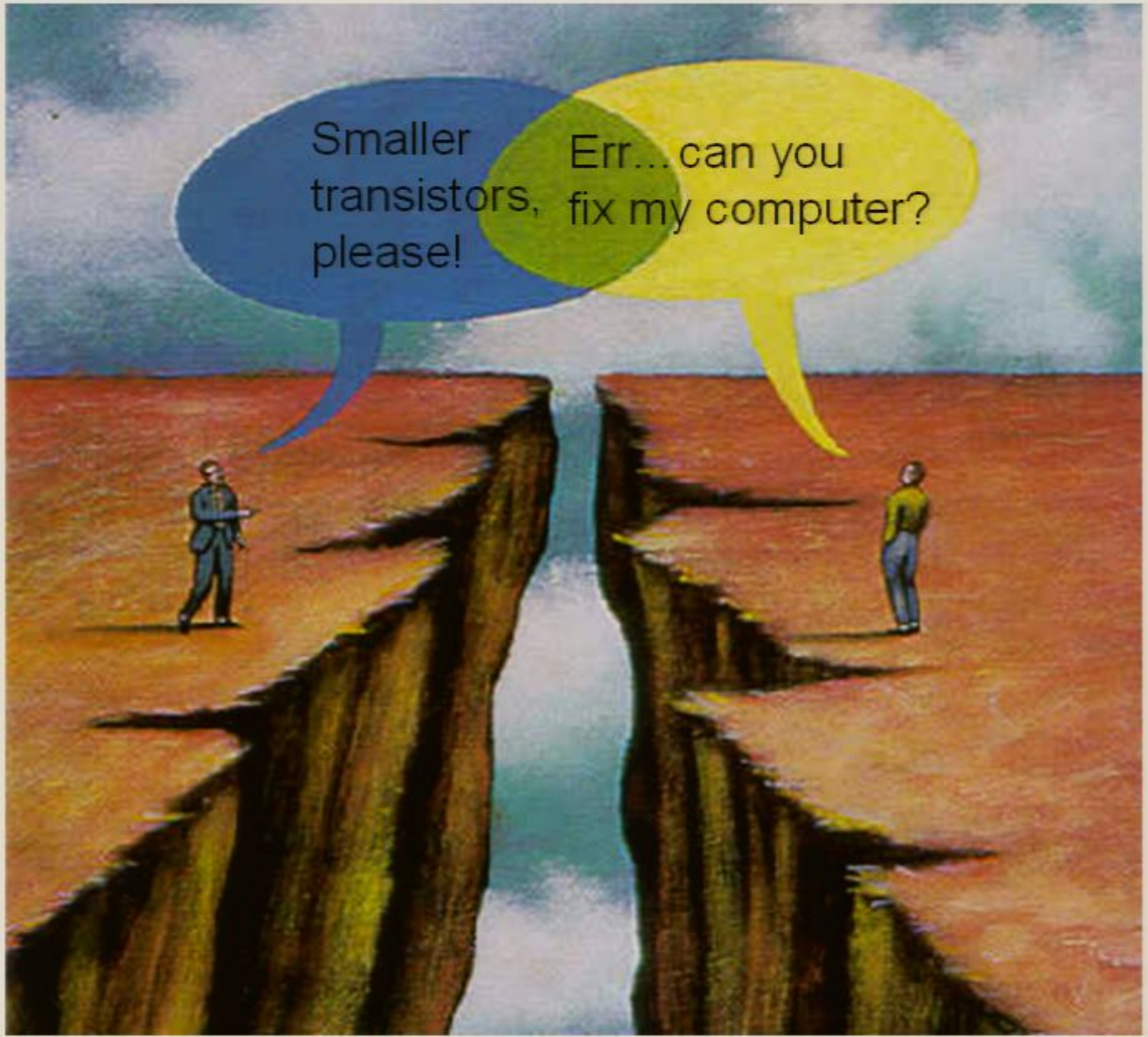
|QW⟩
group

"Que Dubayah"

A Brief History of Hiring in Quantum Computing

Physics and Computer Science

Physics and Computer Science



They're Scared?

Email I received from Wim van Dam about FOCS 2006:

Leslie Valiant in his great talk on 'accidental algorithms': "We have all these complexity classes, and we don't know at all if they are different... It would be a nightmare if they turn out to be all the same, such that NC2=P=P^#P and so on." <comment from the audience about if this would really be so bad> "Yes it would be a nightmare, but the *worst* possible nightmare would be if NC=P=P^#P and if it was a *physicist* who proved it."

They're Not Scared?

Aaronson

Q: Does quantum computing really belong in CS departments, as opposed to physics departments?

A: It belongs if we want it to belong! In my experience, the *physicists* have a bigger hurdle than the computer scientists in getting started with quantum computing research. All we need to do is ask themselves: "what happens if we generalize probability theory to allow minus signs, and base it on the L2 norm instead of the L1 norm?" From then on it's just the concepts we know and love: states, transformations, recursion, reductions, universality, asymptotic efficiency, and so on. Physicists, by contrast, have to learn most of this stuff for the first time. It's been a great personal pleasure to watch physicists who once suspected that CS was devoid of intellectual content, struggle with that content while trying to learn quantum computing!

Shor's Algorithm

Factor N:

Find $x^2 = 1 \mod N \quad x^2 \neq \pm 1$

$$\Rightarrow (x+1)(x-1) = 0 \mod N$$

Either: $(x+1)$ or $(x-1)$ must share a common divisor with N

Shor's Algorithm

Factor N:

Find $x^2 = 1 \mod N \quad x^2 \neq \pm 1$

$$\Rightarrow (x+1)(x-1) = 0 \mod N$$

Either: $(x+1)$ or $(x-1)$ must share a common divisor with N

Shor's Algorithm

Factor N:

Find $x^2 = 1 \mod N \quad x^2 \neq \pm 1$

$$\Rightarrow (x+1)(x-1) = 0 \mod N$$

Either: $(x+1)$ or $(x-1)$ must share a common divisor with N

How to do **Find**:

Pick random r coprime to N

Define: $f(s) = r^s \mod N$

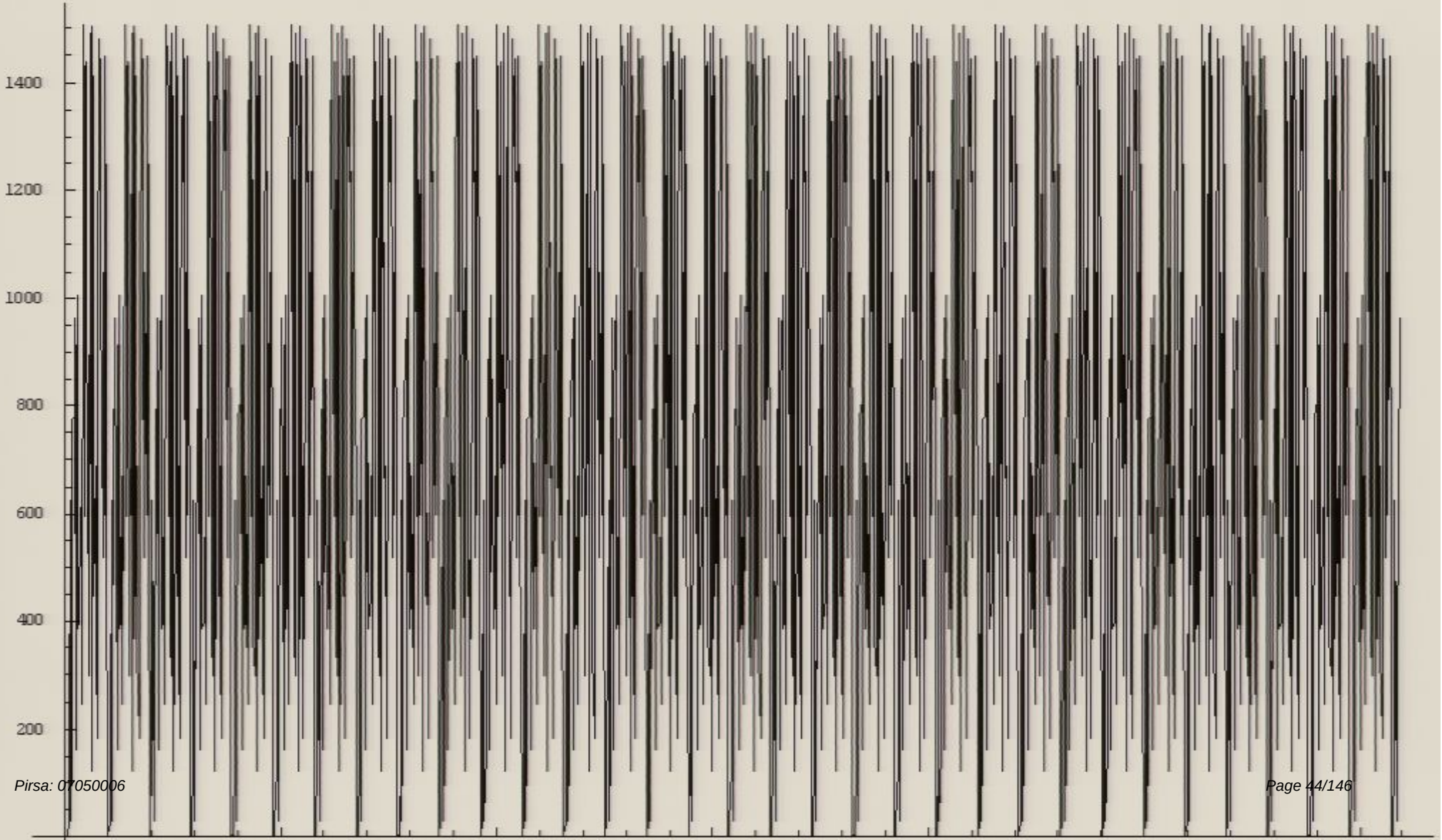
Period of $f(s)$ is smallest k such that $r^k = 1 \mod N$

If k is even, then $x = r^{\frac{k}{2}}$ (about 50% of time)

Periodicity Finding $\Rightarrow$ Factoring

Shor's Algorithm

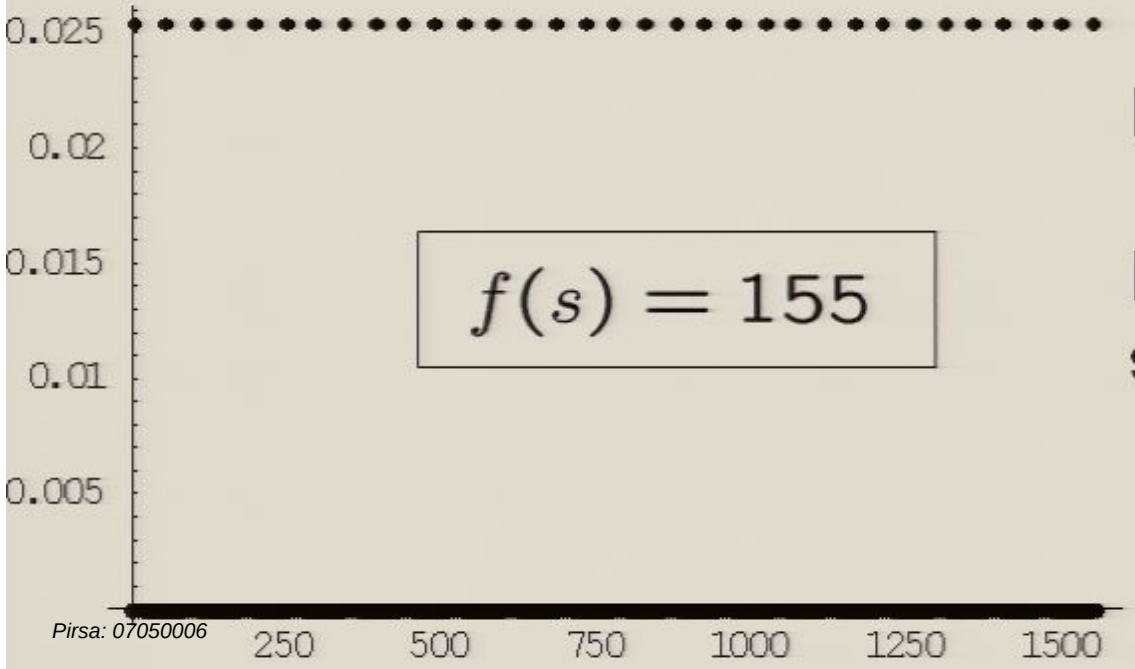
N=1547, r=5, Period = 48. 48+1=49 GCD(1547,49)=7



Period Finding

Why hard? $f(s) = r^s \bmod N$

$$\frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} |s\rangle \otimes |f(s)\rangle$$



$f(s) = 155$

Measure second register

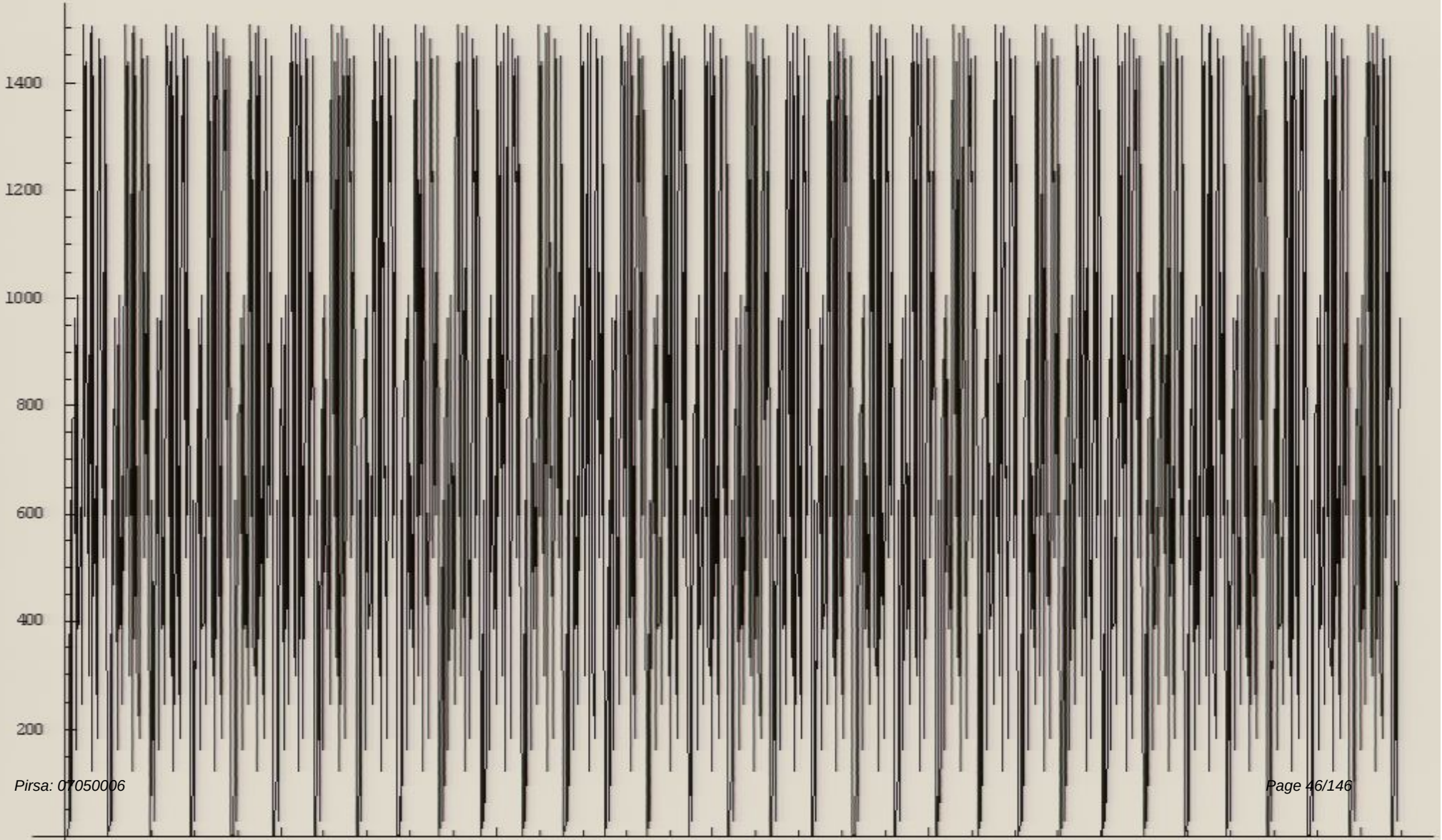
First register is (nearly) symmetric under translation

$$T|x\rangle = |x+1\rangle$$

$$T\rho T^\dagger \approx \rho$$

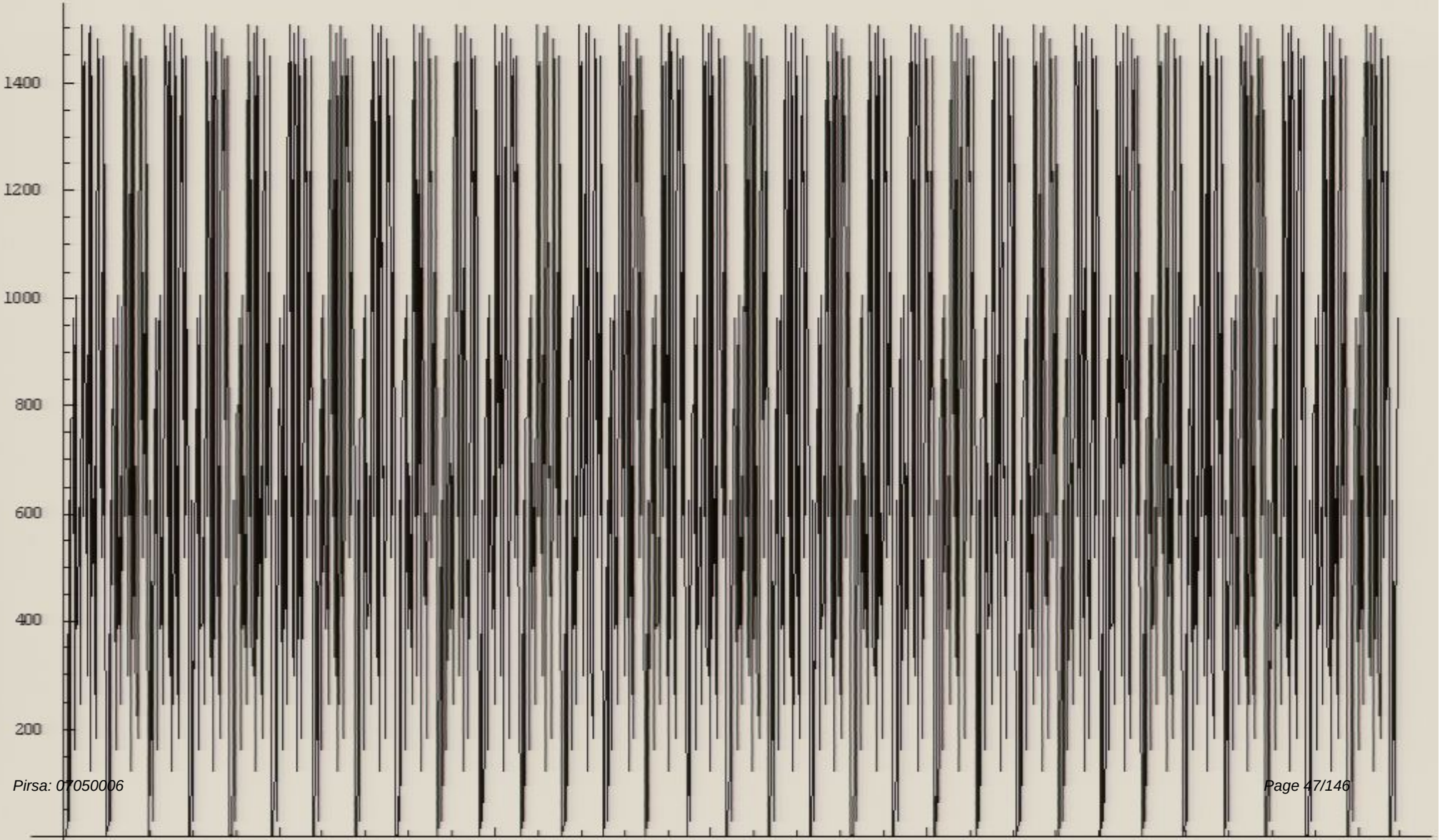
Shor's Algorithm

N=1547, r=5, Period = 48. 48+1=49 GCD(1547,49)=7



Shor's Algorithm

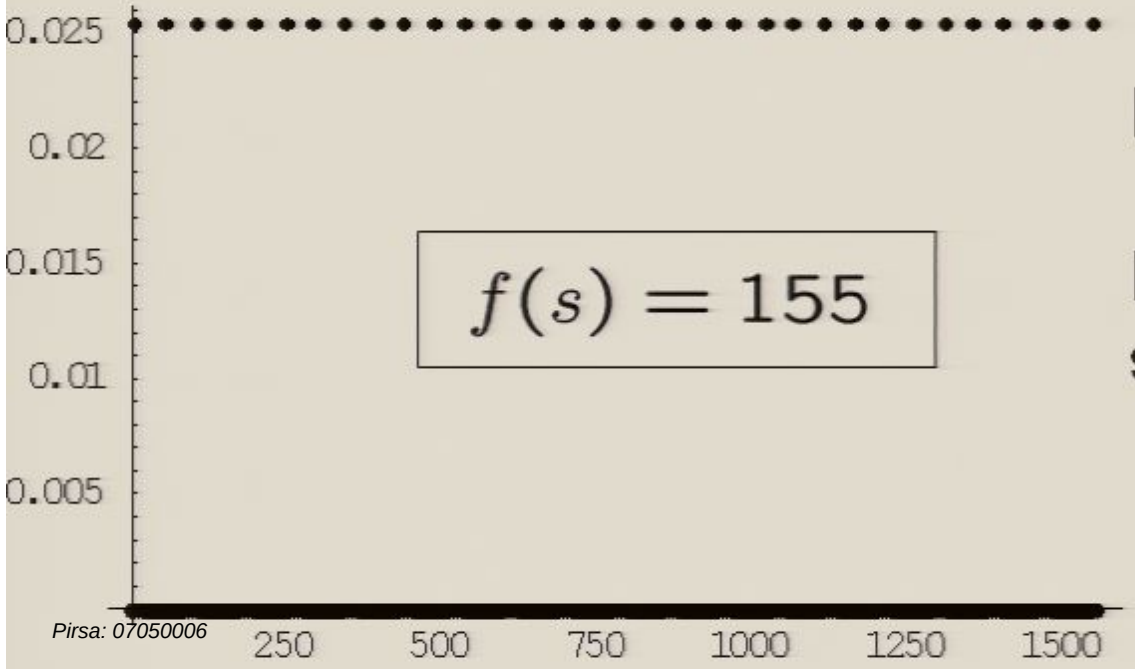
N=1547, r=5, Period = 48. 48+1=49 GCD(1547,49)=7



Period Finding

Why hard? $f(s) = r^s \bmod N$

$$\frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} |s\rangle \otimes |f(s)\rangle$$



$f(s) = 155$

Measure second register

First register is (nearly) symmetric under translation

$$T|x\rangle = |x+1\rangle$$

$$T\rho T^\dagger \approx \rho$$

The First Basis Change We Learn In Quantum Mechanics

$$\frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} |s\rangle \otimes |f(s)\rangle$$

symmetry under translation

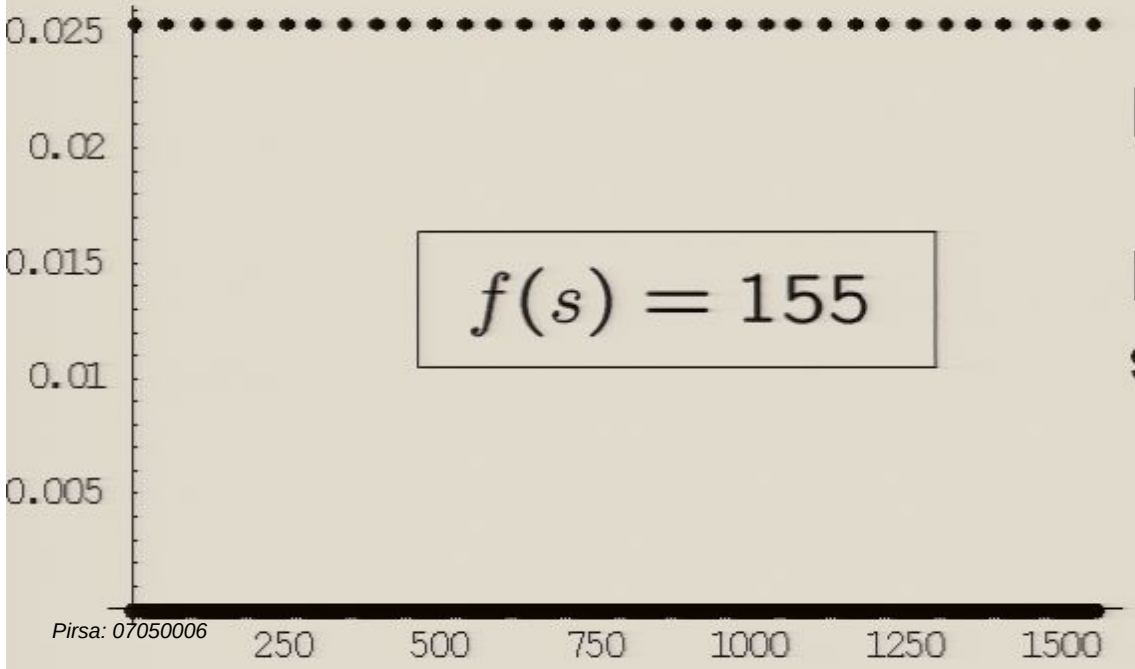
$$T|x\rangle = |x+1\rangle$$

$$T\rho T^\dagger = \rho$$

Period Finding

Why hard? $f(s) = r^s \bmod N$

$$\frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} |s\rangle \otimes |f(s)\rangle$$



$f(s) = 155$

Measure second register

First register is (nearly) symmetric under translation

$$T|x\rangle = |x+1\rangle$$

$$T\rho T^\dagger \approx \rho$$

The First Basis Change We Learn In Quantum Mechanics

$$\frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} |s\rangle \otimes |f(s)\rangle$$

symmetry under translation

$$T|x\rangle = |x+1\rangle$$

$$T\rho T^\dagger = \rho$$

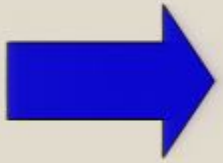
The First Basis Change We Learn In Quantum Mechanics

$$\frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} |s\rangle \otimes |f(s)\rangle$$

symmetry under translation

$$T|x\rangle = |x+1\rangle$$

$$T\rho T^\dagger = \rho$$



change to momentum basis!

$$|p\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \omega_N^{ixp} |x\rangle$$

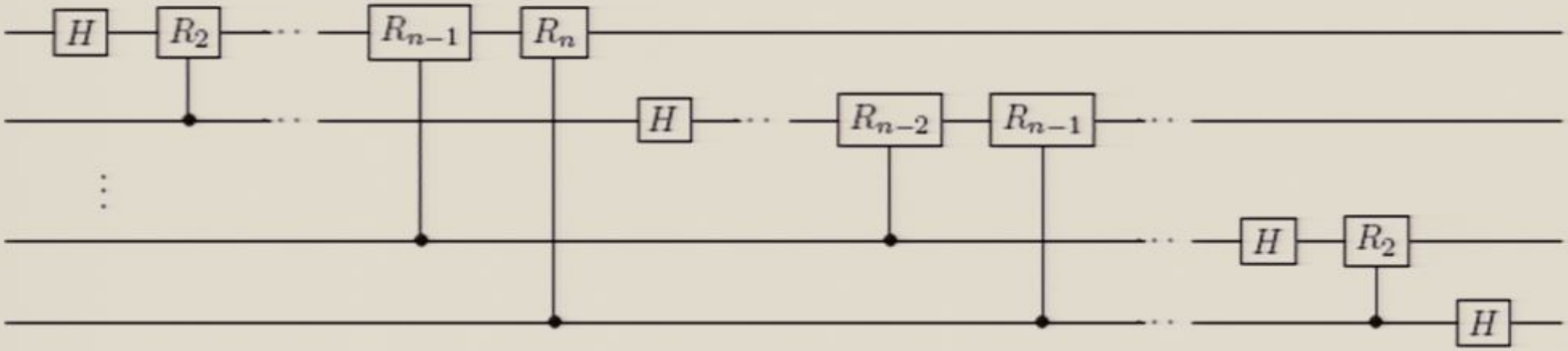
$$\omega_N = \exp\left(\frac{2\pi i}{N}\right)$$

Perform a Fourier Transform!

Quantum Fourier Transform

Efficient quantum circuit for quantum Fourier transform:

[Efficient = O(poly[# qubits])



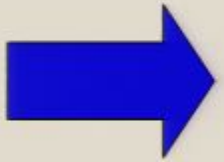
The First Basis Change We Learn In Quantum Mechanics

$$\frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} |s\rangle \otimes |f(s)\rangle$$

symmetry under translation

$$T|x\rangle = |x+1\rangle$$

$$T\rho T^\dagger = \rho$$



change to momentum basis!

$$|p\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \omega_N^{ixp} |x\rangle$$

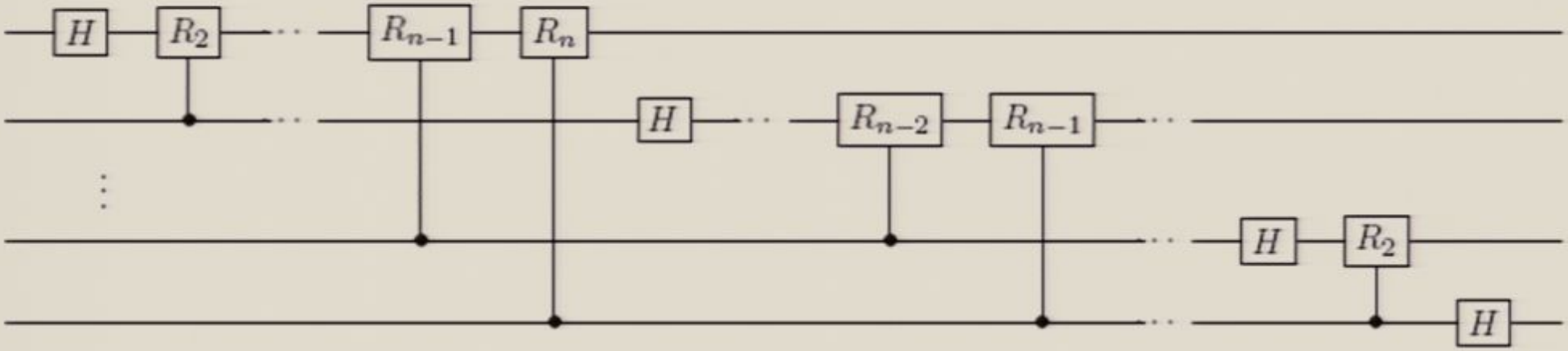
$$\omega_N = \exp\left(\frac{2\pi i}{N}\right)$$

Perform a Fourier Transform!

Quantum Fourier Transform

Efficient quantum circuit for quantum Fourier transform:

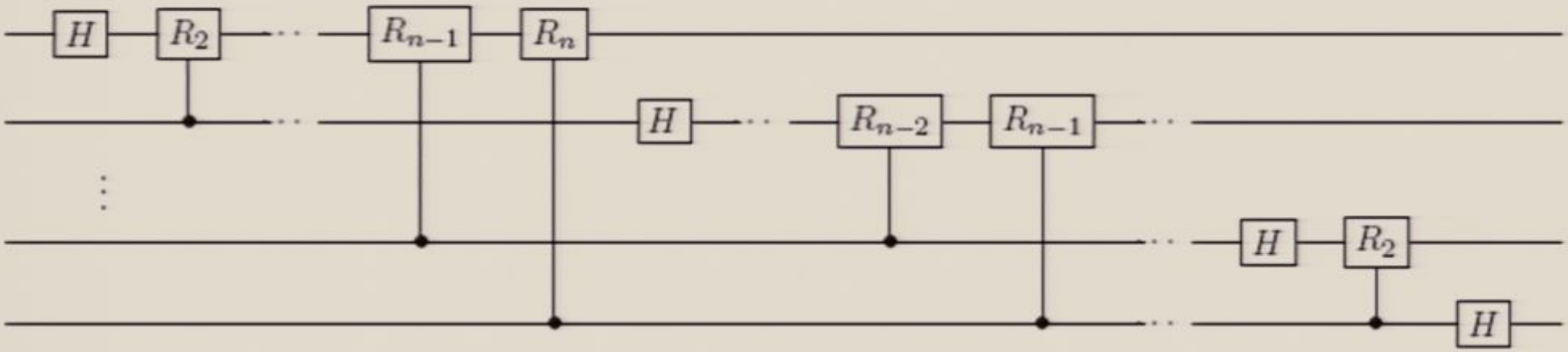
[Efficient = O(poly[# qubits])



Quantum Fourier Transform

Efficient quantum circuit for quantum Fourier transform:

[Efficient = O(poly[# qubits])



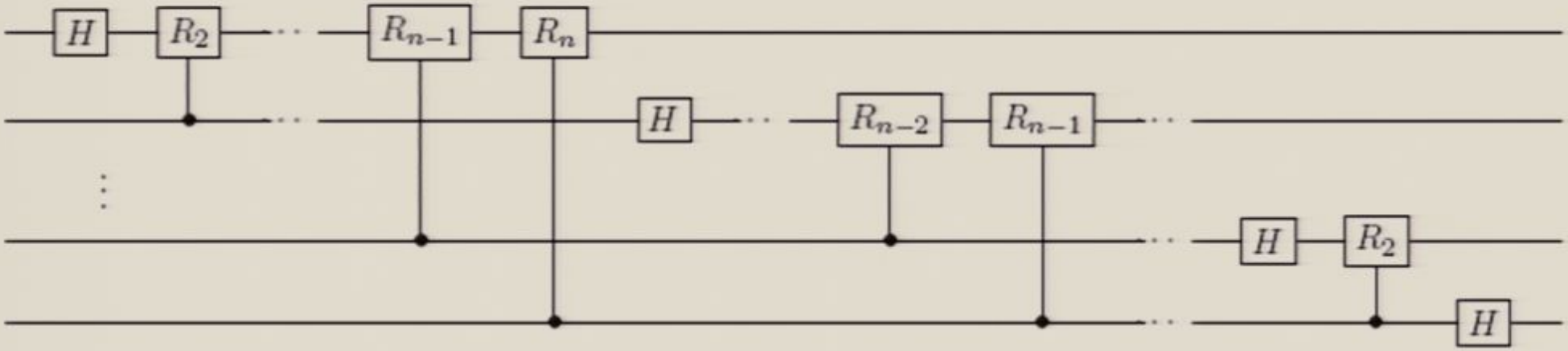
Factoring

Period Finding

Quantum Fourier Transform

Efficient quantum circuit for quantum Fourier transform:

[Efficient = O(poly[# qubits])



Factoring

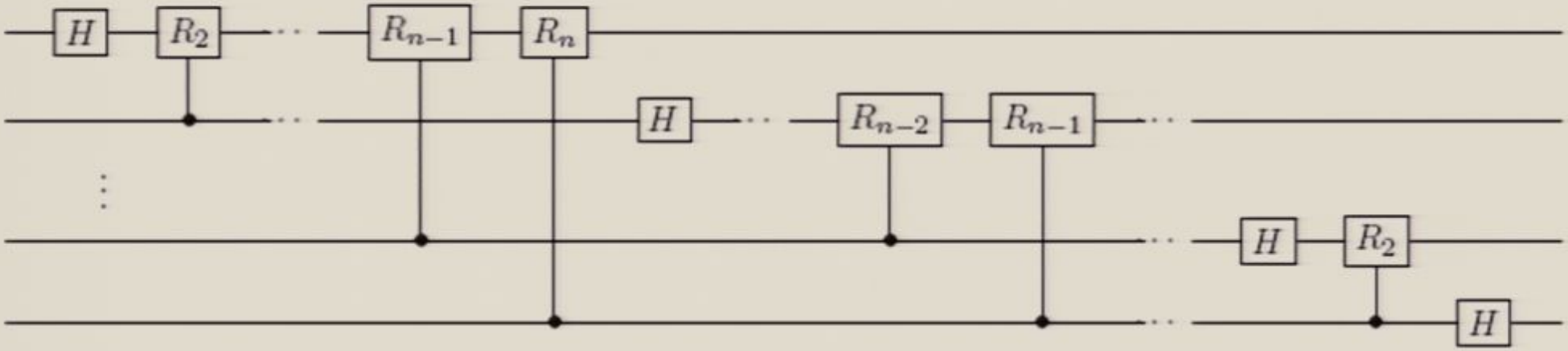
Symmetry

Period Finding

Quantum Fourier Transform

Efficient quantum circuit for quantum Fourier transform:

[Efficient = O(poly[# qubits])



Factoring

Period Finding

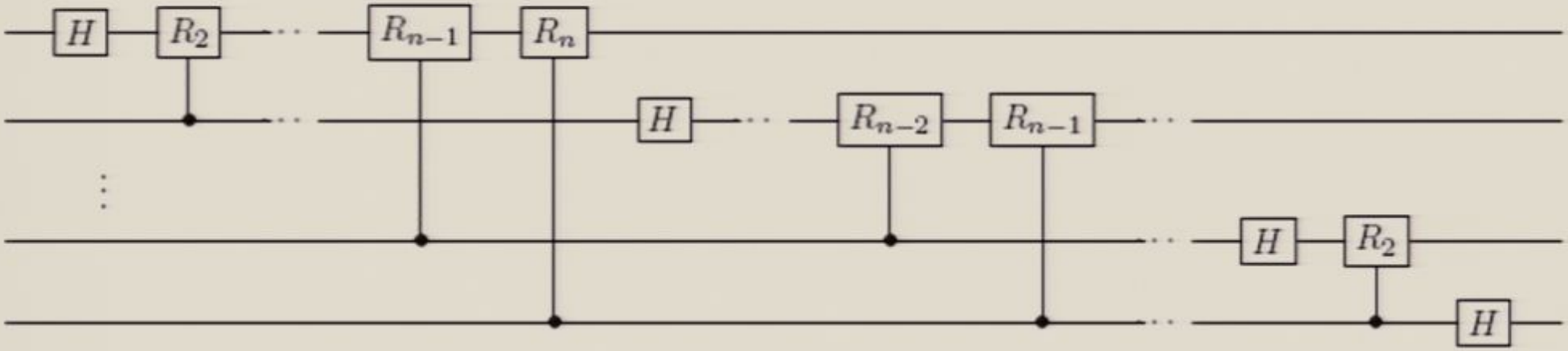
Symmetry

Change Basis

Quantum Fourier Transform

Efficient quantum circuit for quantum Fourier transform:

[Efficient = O(poly[# qubits])



Factoring

Period Finding

Symmetry

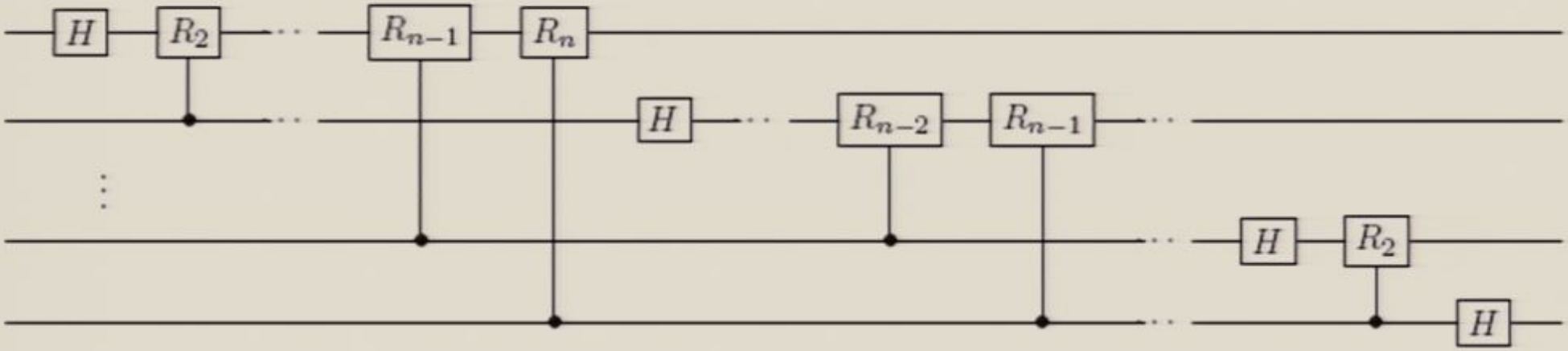
Change Basis

Efficient Circuit

Quantum Fourier Transform

Efficient quantum circuit for quantum Fourier transform:

[Efficient = O(poly[# qubits])



Factoring

Period Finding

Symmetry

Change Basis

Efficient Circuit

Shor's Algorithm

Moral

Symmetries

Quantum algorithms

Moral

Symmetries

Quantum algorithms

The Second Basis Change We Learn In Quantum Mechanics?

The Second Basis Change We Learn In Quantum Mechanics:

Clebsch-Gordan Transform

Singlet:

$$|S=0,m=0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle \otimes |\downarrow\rangle - |\downarrow\rangle \otimes |\uparrow\rangle)$$

Triplet:

$$|S=1,m=1\rangle = |\uparrow\rangle \otimes |\uparrow\rangle$$

$$|S=1,m=0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle \otimes |\downarrow\rangle + |\downarrow\rangle \otimes |\uparrow\rangle)$$

$$|S=1,m=-1\rangle = |\downarrow\rangle \otimes |\downarrow\rangle$$

What Use?

Collective Unitaries

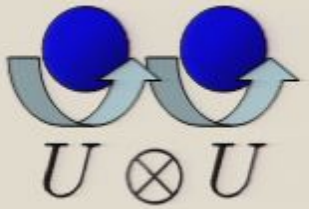
$$|S=0,m=0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle\otimes|\downarrow\rangle - |\downarrow\rangle\otimes|\uparrow\rangle)$$

$$|S=1,m=1\rangle = |\uparrow\rangle\otimes|\uparrow\rangle$$

$$|S=1,m=0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle\otimes|\downarrow\rangle + |\downarrow\rangle\otimes|\uparrow\rangle)$$

$$|S=1,m=-1\rangle = |\downarrow\rangle\otimes|\downarrow\rangle$$

$$\left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & U \end{array}\right]$$



Collective Unitaries

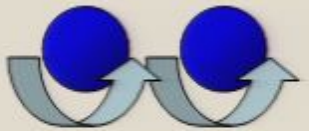
$$|S=0,m=0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle\otimes|\downarrow\rangle - |\downarrow\rangle\otimes|\uparrow\rangle)$$

$$|S=1,m=1\rangle = |\uparrow\rangle\otimes|\uparrow\rangle$$

$$|S=1,m=0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle\otimes|\downarrow\rangle + |\downarrow\rangle\otimes|\uparrow\rangle)$$

$$|S=1,m=-1\rangle = |\downarrow\rangle\otimes|\downarrow\rangle$$

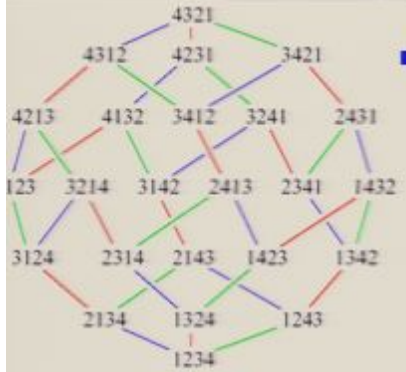
$$\left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & U \end{array}\right]$$



$U \otimes U$

Symmetry Under n Collective Unitary Rotations

$U^{\otimes n}$



The Symmetric Group

Transform Under SWAP

Singlet:

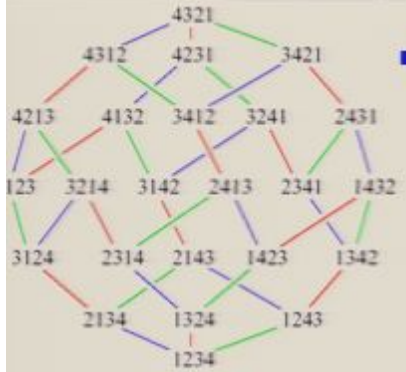
$$|S=0,m=0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle\otimes|\downarrow\rangle - |\downarrow\rangle\otimes|\uparrow\rangle) \quad \Big\} \quad -1$$

Triplet:

$$|S=1,m=1\rangle = |\uparrow\rangle\otimes|\uparrow\rangle$$

$$|S=1,m=0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle\otimes|\downarrow\rangle + |\downarrow\rangle\otimes|\uparrow\rangle) \quad \Big\} \quad +1$$

$$|S=1,m=-1\rangle = |\downarrow\rangle\otimes|\downarrow\rangle$$



The Symmetric Group

Transform Under SWAP

Singlet:

$$|S=0,m=0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle\otimes|\downarrow\rangle - |\downarrow\rangle\otimes|\uparrow\rangle) \quad \Big\} \quad -1$$

Triplet:

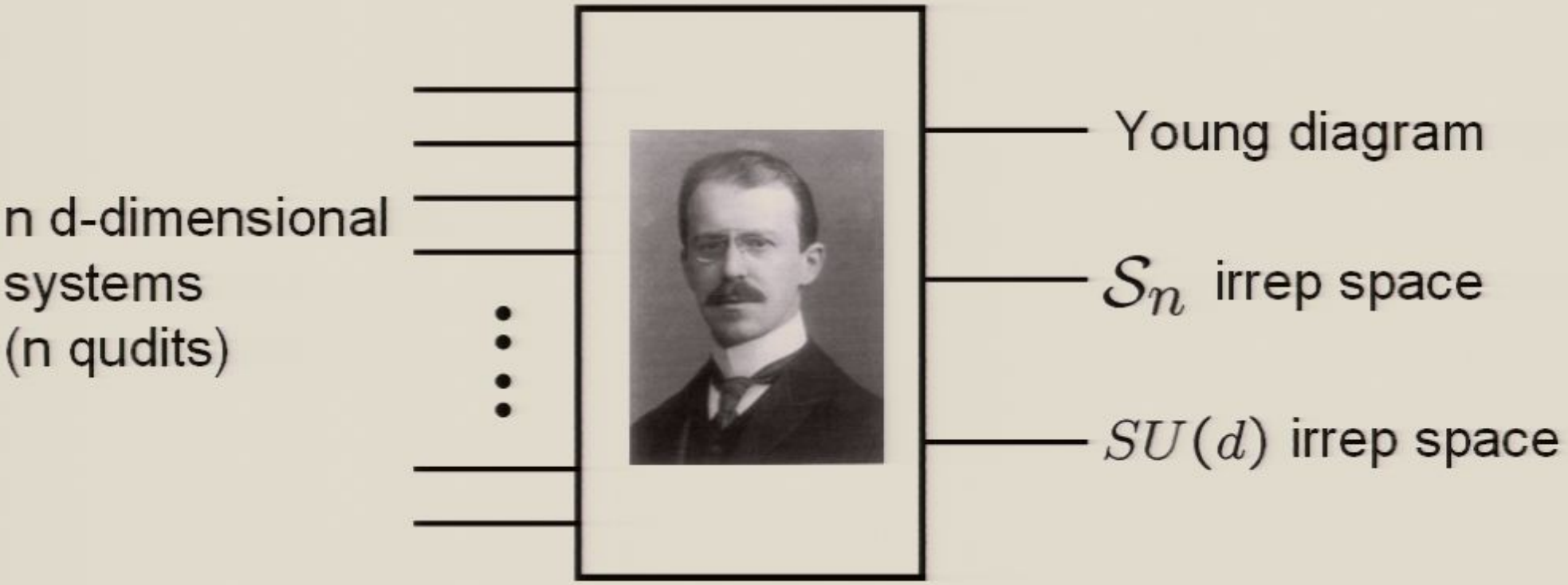
$$|S=1,m=1\rangle = |\uparrow\rangle\otimes|\uparrow\rangle$$

$$|S=1,m=0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle\otimes|\downarrow\rangle + |\downarrow\rangle\otimes|\uparrow\rangle) \quad \Big\} \quad +1$$

$$|S=1,m=-1\rangle = |\downarrow\rangle\otimes|\downarrow\rangle$$

Symmetry Under Permutation of n Subsystems

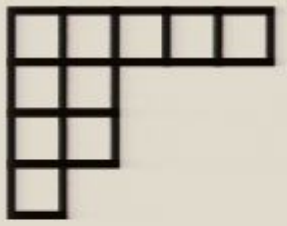
Quantum Schur Transform



Schur duality

$$[\mathbb{C}^d]^{\otimes n} \overset{\text{Schur}}{\cong} \bigoplus_{\mathcal{Y}} S_{\mathcal{Y}} \otimes U_{\mathcal{Y}}$$

Young diagram

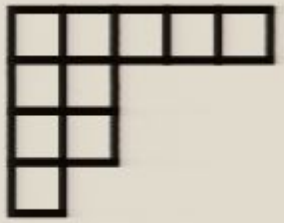


$$k_1 \geq k_2 \geq \cdots \geq k_d$$

$$\sum_{i=1}^{d} k_i = n$$

Uses of Schur

Young diagram

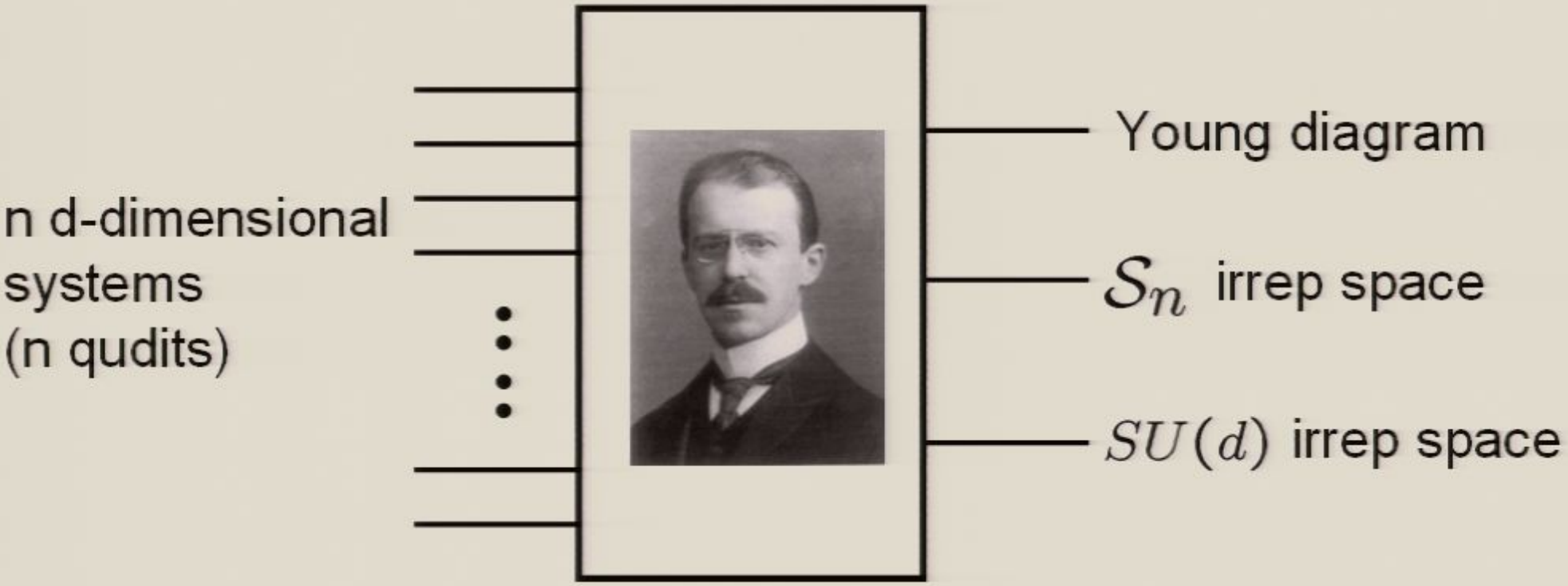


$$k_1 \geq k_2 \geq \cdots \geq k_d$$

$$\sum_{i=1}^{d} k_i = n$$

What does this remind you of?

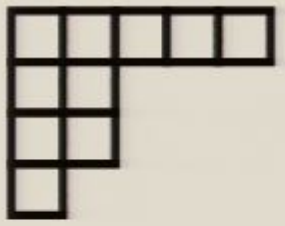
Quantum Schur Transform



Schur duality

$$[\mathbb{C}^d]^{\otimes n} \overset{\text{Schur}}{\cong} \bigoplus_{\mathcal{Y}} S_{\mathcal{Y}} \otimes U_{\mathcal{Y}}$$

Young diagram

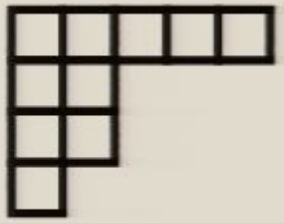


$$k_1 \geq k_2 \geq \cdots \geq k_d$$

$$\sum_{i=1}^{d} k_i = n$$

Uses of Schur

Young diagram



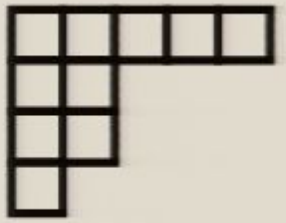
$$k_1 \geq k_2 \geq \cdots \geq k_d$$

$$\sum_{i=1}^{d} k_i = n$$

What does this remind you of?

Uses of Schur

Young diagram



$$k_1 \geq k_2 \geq \cdots \geq k_d$$

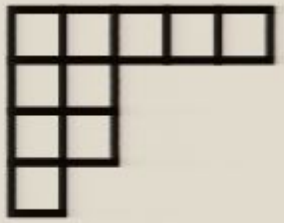
$$\sum_{i=1}^{d} k_i = n$$

What does this remind you of?

$\frac{k_i}{n}$ like probabilities like the spectrum of a density operator

Uses of Schur

Young diagram



$$k_1 \geq k_2 \geq \cdots \geq k_d$$

$$\sum_{i=1}^{d} k_i = n$$

What does this remind you of?

$\frac{k_i}{n}$ like probabilities like the spectrum of a density operator

Young diagram ← Optimal spectrum estimate
[Keyl and Werner. PRA, 2001]

$\mathcal{S}_n$ irrep space

$SU(d)$ irrep space

The Plethora of Uses of Schur

Optimal spectrum estimation

[M. Keyl and R. F. Werner. Phys. Rev. A, 2001]

Universal distortion-free entanglement concentration

[M. Hayashi and K. Matsumoto. Information Theory, 2004]

Universal compression with optimal overflow exponent

[M. Hayashi and K. Matsumoto. Phys. Rev. A, 2002]

Optimal quantum hypothesis testing

[M. Hayashi, J. Phys. A, 2002]

Communicating without a shared reference frame

[S. Bartlett, T. Rudolph, and R. Spekkens, Phys. Rev. Lett., 2003]

Encoding into decoherence-free (noiseless) subsystems

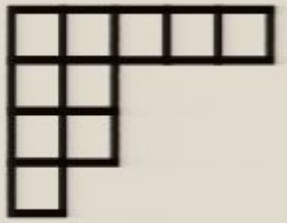
[J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A, 2001]

Simulating lattice gauge theories on a quantum computer

[T. Byrnes and Y. Yoshihisa, Phys. Rev. A 2006]

Uses of Schur

Young diagram



$$k_1 \geq k_2 \geq \cdots \geq k_d$$

$$\sum_{i=1}^{d} k_i = n$$

What does this remind you of?

$\frac{k_i}{n}$ like probabilities like the spectrum of a density operator

Young diagram ← Optimal spectrum estimate

[Keyl and Werner. PRA, 2001]

$\mathcal{S}_n$ irrep space

$SU(d)$ irrep space

The Plethora of Uses of Schur

Optimal spectrum estimation

[M. Keyl and R. F. Werner. Phys. Rev. A, 2001]

Universal distortion-free entanglement concentration

[M. Hayashi and K. Matsumoto. Information Theory, 2004]

Universal compression with optimal overflow exponent

[M. Hayashi and K. Matsumoto. Phys. Rev. A, 2002]

Optimal quantum hypothesis testing

[M. Hayashi, J. Phys. A, 2002]

Communicating without a shared reference frame

[S. Bartlett, T. Rudolph, and R. Spekkens, Phys. Rev. Lett., 2003]

Encoding into decoherence-free (noiseless) subsystems

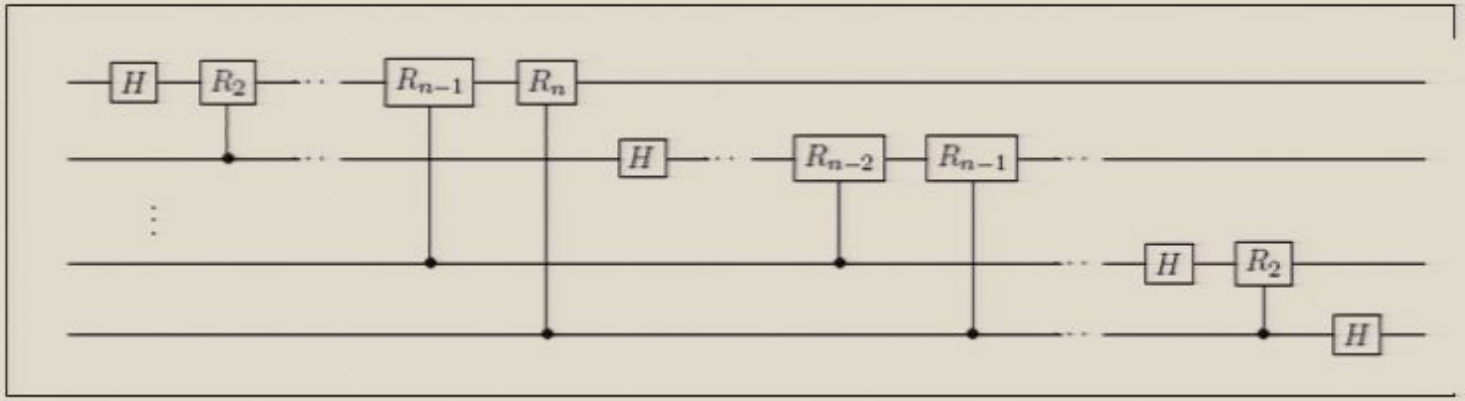
[J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A, 2001]

Simulating lattice gauge theories on a quantum computer

[T. Byrnes and Y. Yoshihisa, Phys. Rev. A 2006]

But Efficient?

QFT

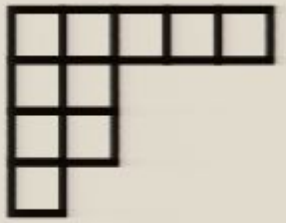


Schur

?

Uses of Schur

Young diagram



$$k_1 \geq k_2 \geq \cdots \geq k_d$$

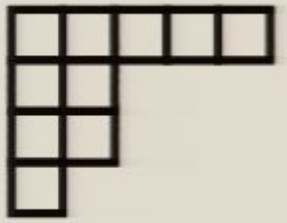
$$\sum_{i=1}^{d} k_i = n$$

What does this remind you of?

$\frac{k_i}{n}$ like probabilities like the spectrum of a density operator

Uses of Schur

Young diagram



$$k_1 \geq k_2 \geq \cdots \geq k_d$$

$$\sum_{i=1}^{d} k_i = n$$

What does this remind you of?

$\frac{k_i}{n}$ like probabilities like the spectrum of a density operator

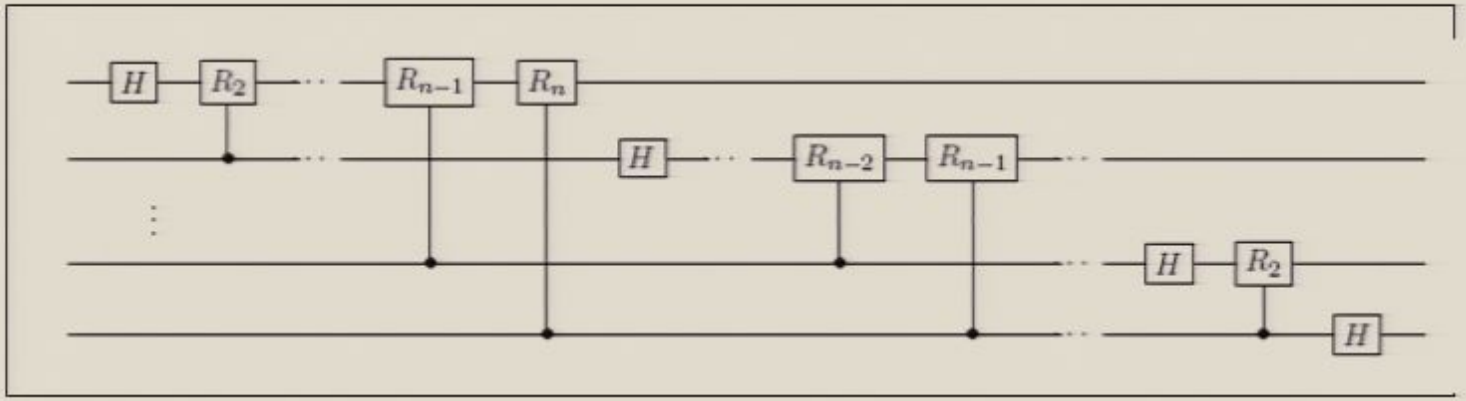
Young diagram ← Optimal spectrum estimate
[Keyl and Werner. PRA, 2001]

$\mathcal{S}_n$ irrep space

$SU(d)$ irrep space

But Efficient?

QFT

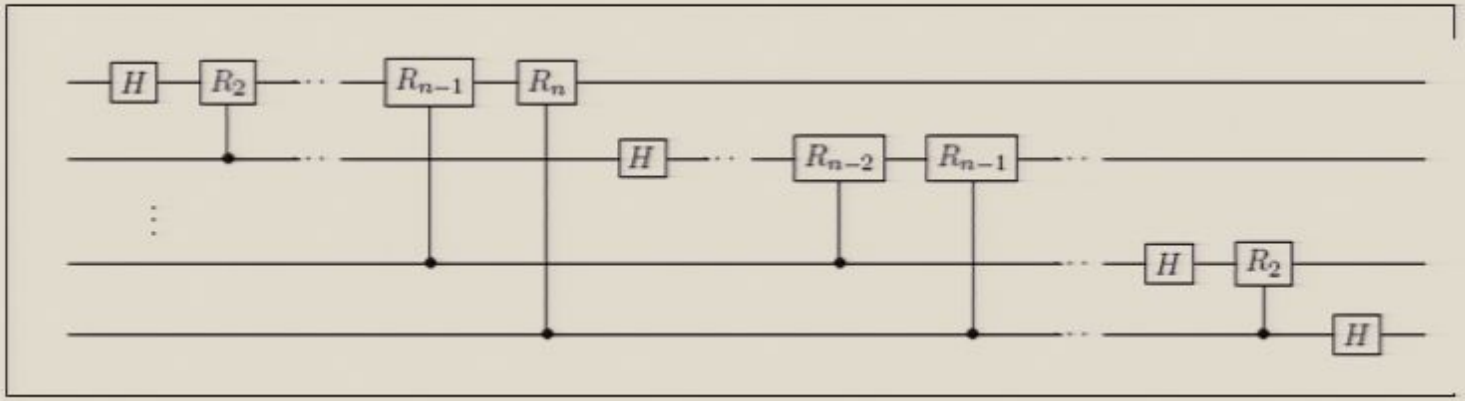


Schur

?

But Efficient?

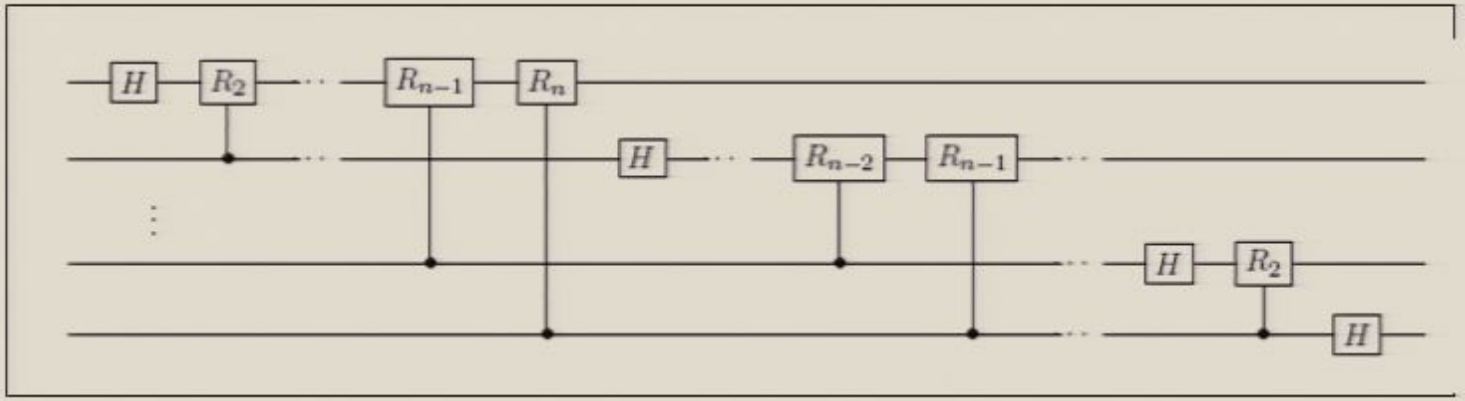
QFT



Schur

But Efficient?

QFT

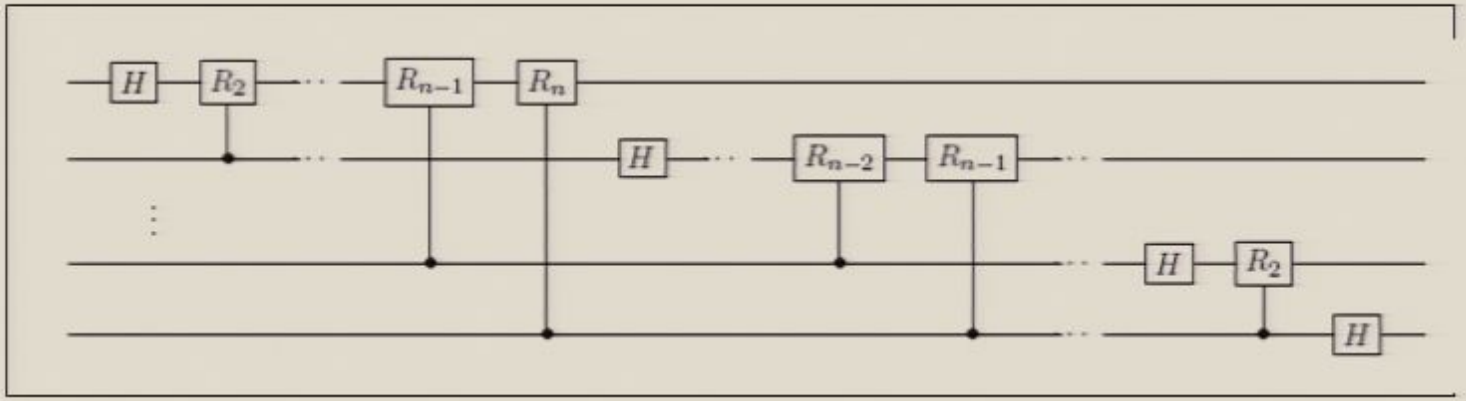


Schur

Who would need to efficiently calculate Clebsch-Gordan coefficients for SU(d)?

But Efficient?

QFT



Schur

Who would need to efficiently calculate Clebsch-Gordan coefficients for SU(d)?

[L. C. Biedenharn and J. D. Louck, Commun. Math. Phys. 1968]

Efficient Schur

[D. Bacon, I.L. Chuang, A. Harrow, Phys. Rev. Lett. 2006]
[D. Bacon, I.L. Chuang, A. Harrow, SODA 2007]

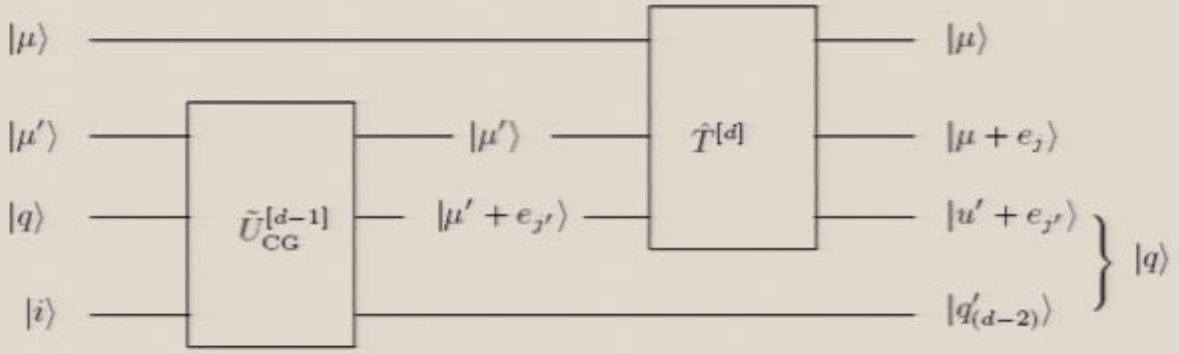


FIG. 4: The $\mathcal{U}_d$ CG transform, $\mathbf{U}_{\mathrm{CG}}^{[d]}$, is decomposed into a $\mathcal{U}_{d-1}$ CG transform $\tilde{U}_{\mathrm{CG}}^{[d-1]}$ (see Eq. (54)) and a reduced Wigner operator $\hat{T}^{[d]}$. In Fig. 5 we show how to reduce the reduced Wigner operator to a $d \times d$ matrix conditioned on μ and $\mu' + e_{j'}$.

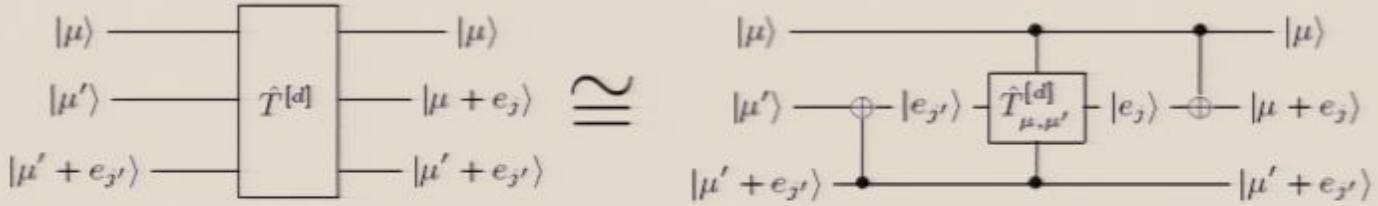
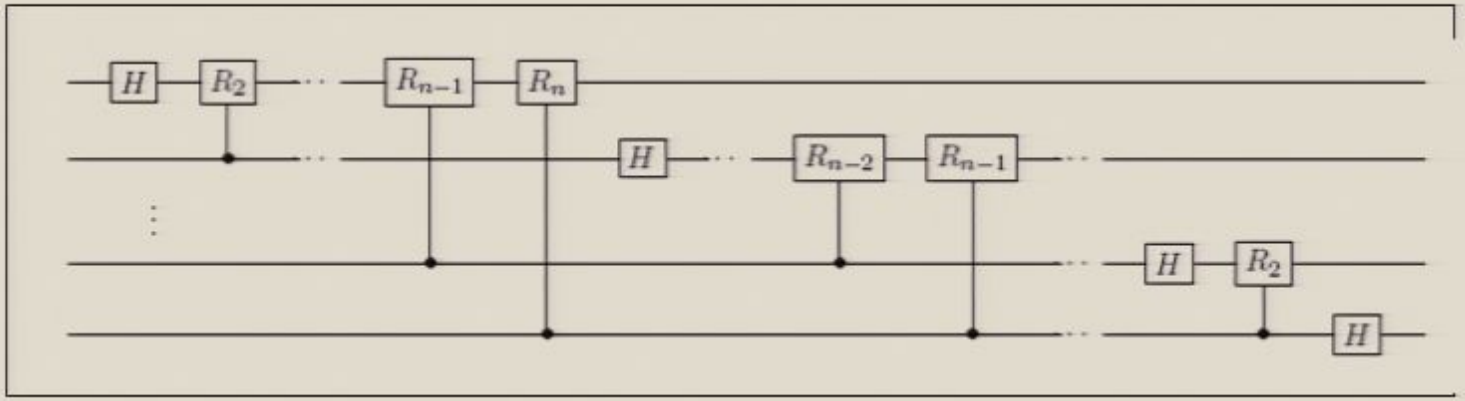


FIG. 5: The reduced Wigner transform $\hat{T}^{[d]}$ can be expressed as a $d \times d$ rotation whose coefficients are controlled by μ and $\mu' + e_{j'}$.

Schur transform to accuracy ϵ : $poly\left(log\frac{1}{\epsilon}, n, d\right)$ time

But Efficient?

QFT



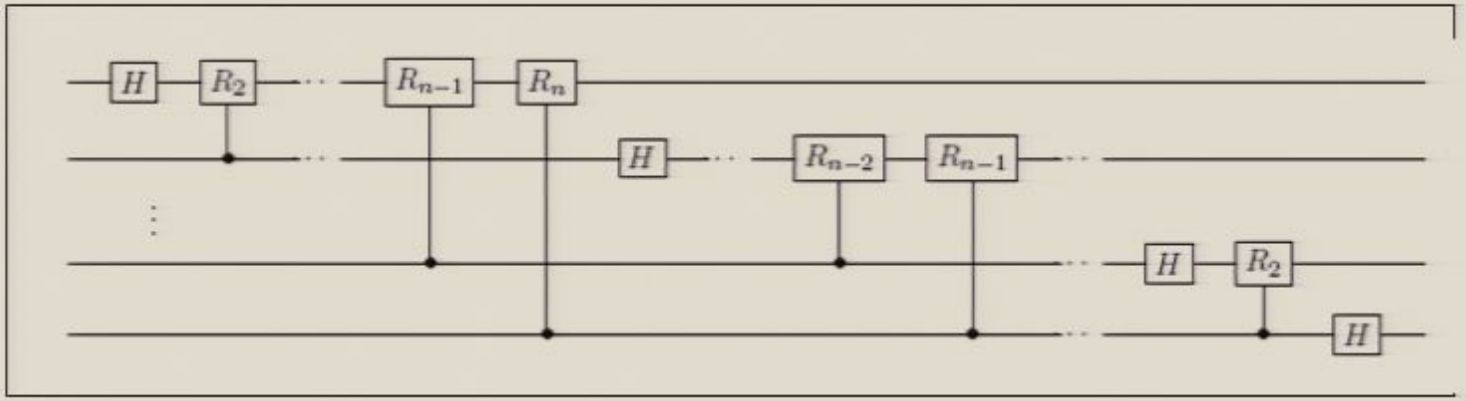
Schur

Who would need to efficiently calculate Clebsch-Gordan coefficients for SU(d)?

[L. C. Biedenharn and J. D. Louck, Commun. Math. Phys. 1968]

But Efficient?

QFT



Schur

Who would need to efficiently calculate Clebsch-Gordan coefficients for SU(d)?

[L. C. Biedenharn and J. D. Louck, Commun. Math. Phys. 1968]

Efficient Schur

[D. Bacon, I.L. Chuang, A. Harrow, Phys. Rev. Lett. 2006]
[D. Bacon, I.L. Chuang, A. Harrow, SODA 2007]

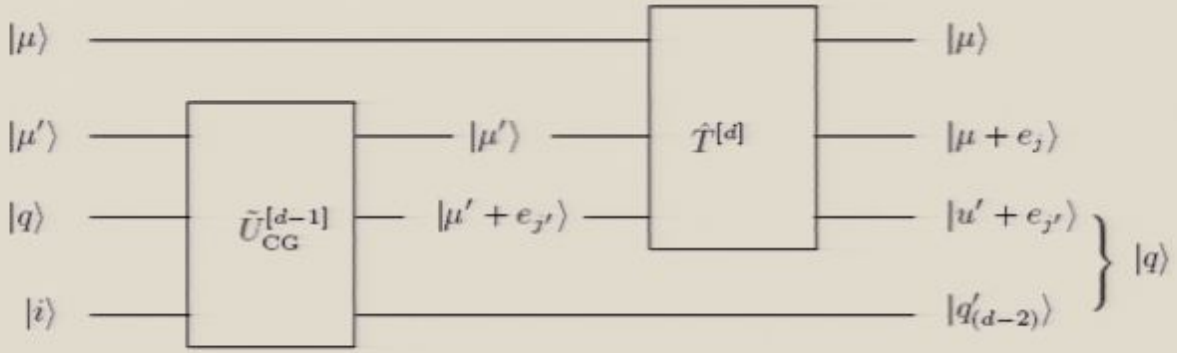


FIG. 4: The $\mathcal{U}_d$ CG transform, $\mathbf{U}_{\mathrm{CG}}^{[d]}$, is decomposed into a $\mathcal{U}_{d-1}$ CG transform $\tilde{U}_{\mathrm{CG}}^{[d-1]}$ (see Eq. (54)) and a reduced Wigner operator $\hat{T}^{[d]}$. In Fig. 5 we show how to reduce the reduced Wigner operator to a $d \times d$ matrix conditioned on μ and $\mu' + e_{j'}$.

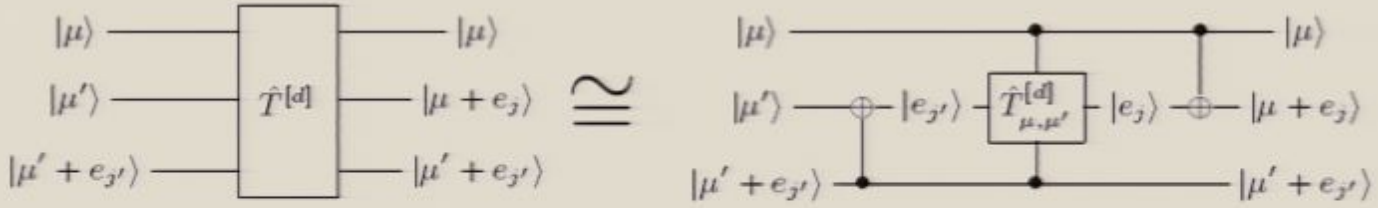


FIG. 5: The reduced Wigner transform $\hat{T}^{[d]}$ can be expressed as a $d \times d$ rotation whose coefficients are controlled by μ and $\mu' + e_{j'}$.

Schur transform to accuracy ϵ : $poly\left(log\frac{1}{\epsilon}, n, d\right)$ time

The Plethora of Uses of Schur

Optimal spectrum estimation

[M. Keyl and R. F. Werner. Phys. Rev. A, 200[illegible]]

Universal distortion-free entanglement concentration

[M. Hayashi and K. Matsumoto. Information Theory, 2004]

Universal compression with optimal overflow exponent

[M. Hayashi and K. Matsumoto. Phys. Rev. A, 2002]

Optimal quantum hypothesis testing

[M. Hayashi, J. Phys. A, 2002]

Communicating without a shared reference frame

[S. Bartlett, T. Rudolph, and R. Spekkens, Phys. Rev. Lett., 2003]

Encoding into decoherence-free (noiseless) subsystems

[J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A, 2001]

Simulating lattice gauge theories on a quantum computer

[T. Byrnes and Y. Yoshihisa, Phys. Rev. A 2006]

Tractable

Efficient Schur

[D. Bacon, I.L. Chuang, A. Harrow, Phys. Rev. Lett. 2006]
[D. Bacon, I.L. Chuang, A. Harrow, SODA 2007]

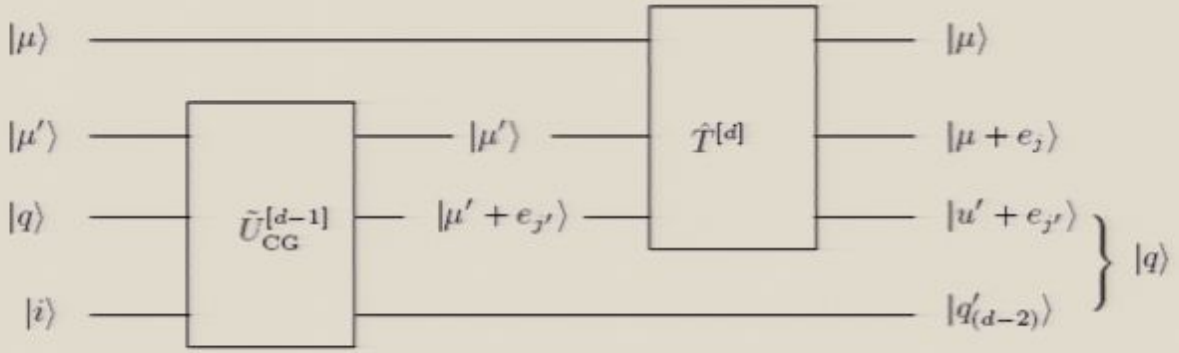


FIG. 4: The $\mathcal{U}_d$ CG transform, $\mathbf{U}_{\mathrm{CG}}^{[d]}$, is decomposed into a $\mathcal{U}_{d-1}$ CG transform $\tilde{U}_{\mathrm{CG}}^{[d-1]}$ (see Eq. (54)) and a reduced Wigner operator $\hat{T}^{[d]}$. In Fig. 5 we show how to reduce the reduced Wigner operator to a $d \times d$ matrix conditioned on μ and $\mu' + e_{j'}$.

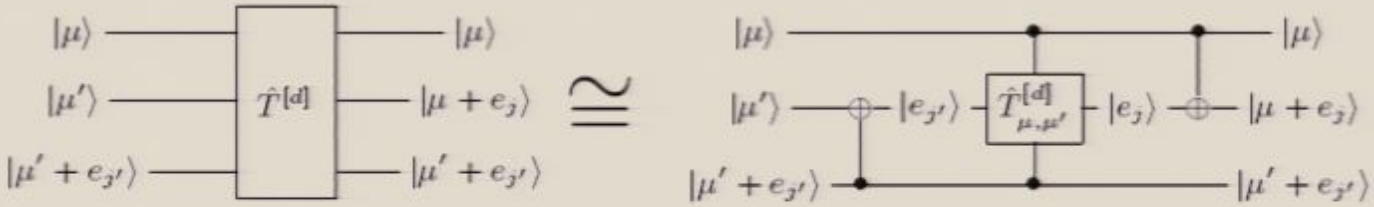


FIG. 5: The reduced Wigner transform $\hat{T}^{[d]}$ can be expressed as a $d \times d$ rotation whose coefficients are controlled by μ and $\mu' + e_{j'}$.

Schur transform to accuracy ϵ : $poly\left(log\frac{1}{\epsilon}, n, d\right)$ time

The Plethora of Uses of Schur

Optimal spectrum estimation

[M. Keyl and R. F. Werner. Phys. Rev. A, 200]

Universal distortion-free entanglement concentration

[M. Hayashi and K. Matsumoto. Information Theory, 2004]

Universal compression with optimal overflow exponent

[M. Hayashi and K. Matsumoto. Phys. Rev. A, 2002]

Optimal quantum hypothesis testing

[M. Hayashi, J. Phys. A, 2002]

Communicating without a shared reference frame

[S. Bartlett, T. Rudolph, and R. Spekkens, Phys. Rev. Lett., 2003]

Encoding into decoherence-free (noiseless) subsystems

[J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A, 2001]

Simulating lattice gauge theories on a quantum computer

[T. Byrnes and Y. Yoshihisa, Phys. Rev. A 2006]

Tractable

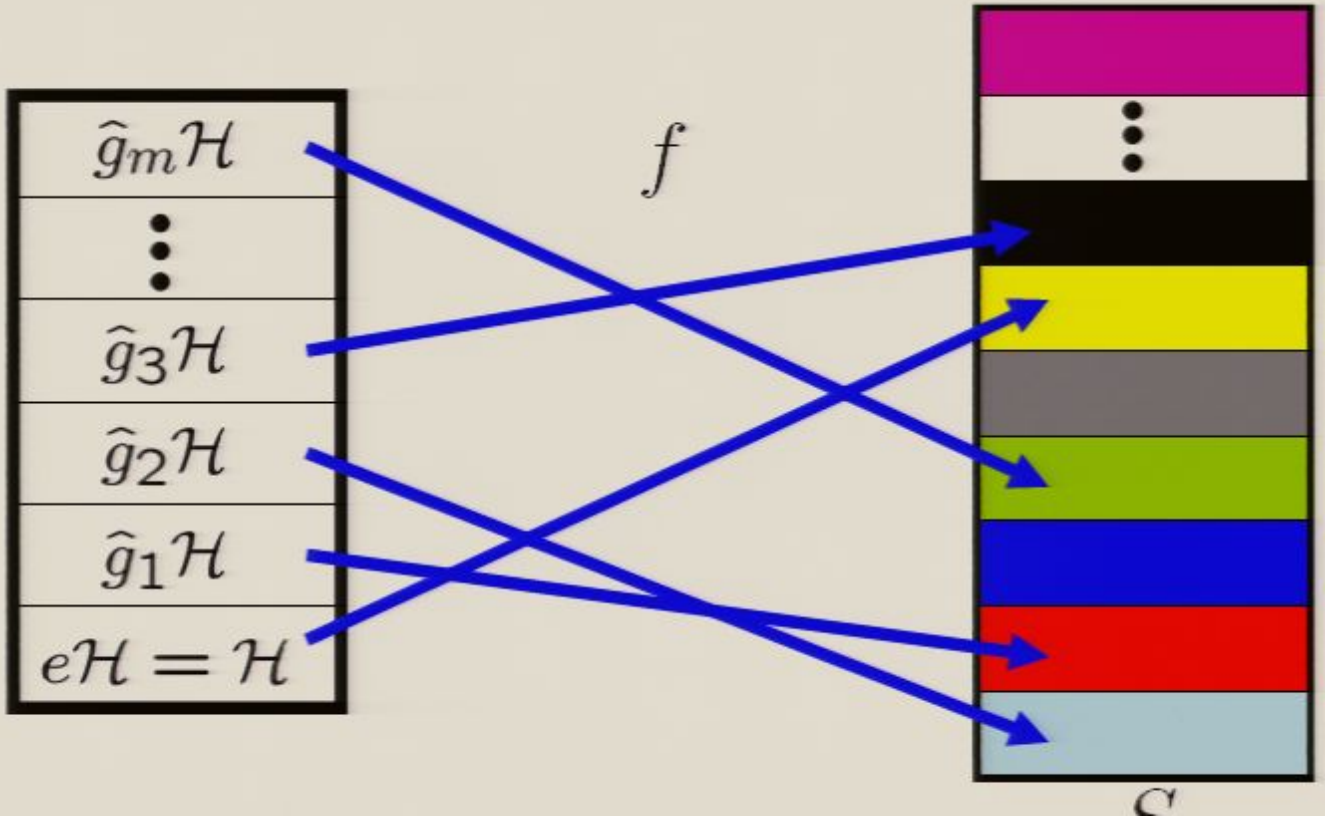
But Algorithms?

The Hidden Subgroup Problem

Setup: Fix a group $\mathcal{G}$ (known) and a subgroup $\mathcal{H} \subset \mathcal{G}$ (unknown). Given query access to a function $f: \mathcal{G} \to S$ that is constant and distinct on left (right) cosets of $\mathcal{H}$ in $\mathcal{G}$. We say that f hides $\mathcal{H}$.

Problem: Find a generating set for $\mathcal{H}$ ("identify $\mathcal{H}$").

Efficient: If runs in time polylog($|\mathcal{G}|$)



Hidden Subgroup Disease

"The quantum measurement problem refers to a set of people."

- Hideo Mabuchi

"The hidden subgroup problem refers to a subgroup of people."

Why the Fuss?

Solved Problems (Shor 1994)

efficient algorithm for HSP over $\mathbb{Z}_N$ → efficient algorithm for factoring whole numbers

efficient algorithm for HSP over $\mathbb{Z}_N \times \mathbb{Z}_N$ → efficient algorithm for the discrete logarithm problem

Why the Fuss?

Solved Problems (Shor 1994)

efficient algorithm for HSP over $\mathbb{Z}_N$ → efficient algorithm for factoring whole numbers

efficient algorithm for HSP over $\mathbb{Z}_N \times \mathbb{Z}_N$ → efficient algorithm for the discrete logarithm problem

Open Problems

efficient algorithm for HSP over $\mathcal{S}_n \wr \mathbb{Z}_2$ (or $\mathcal{S}_{2n}$) → efficient algorithm for the graph isomorphism problem

efficient "standard" quantum algorithm for HSP over dihedral group $\mathcal{D}_N$ → efficient algorithm for the poly(n) unique shortest vector in a lattice problem

Graph Isomorphism

adjacency matrix A_1

$G_1 = (V_1, E_1)$

adjacency matrix A_2

$G_2 = (V_2, E_2)$

Problem: Is there a 1-to-1 mapping p from the vertices V_1 to the vertices V_2 such that the edges are respected, $p(E_1) = E_2$?

Mapping to the HSP:

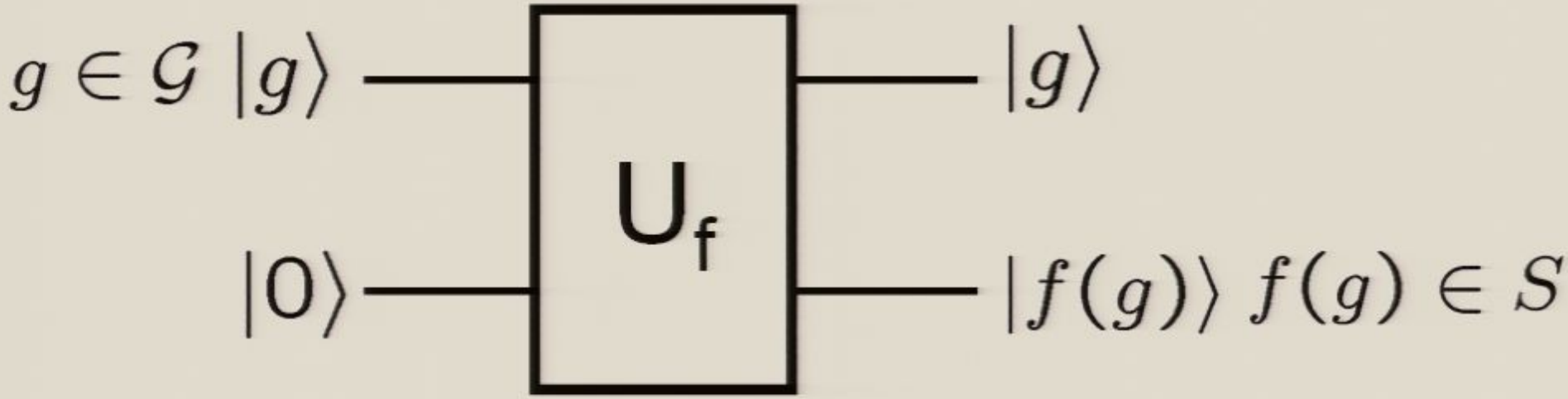
$$f : \mathcal{S}_{2n} \to \mathbb{Z}_{n(2n-1)}$$

$$f(\pi) = \pi(A_1 \oplus A_2)$$

If graphs are not isomorphic, hidden subgroup will not mix the graphs. If they are isomorphic, they will mix the graphs.

Standard Query Model

Oracle:



Query in equal superposition over group elements

$$\frac{1}{\sqrt{|\mathcal{G}|}} \sum_{g \in \mathcal{G}} |g\rangle|0\rangle \rightarrow \sum_{g \in \mathcal{G}} \frac{1}{\sqrt{|\mathcal{G}|}} |g\rangle|f(g)\rangle$$

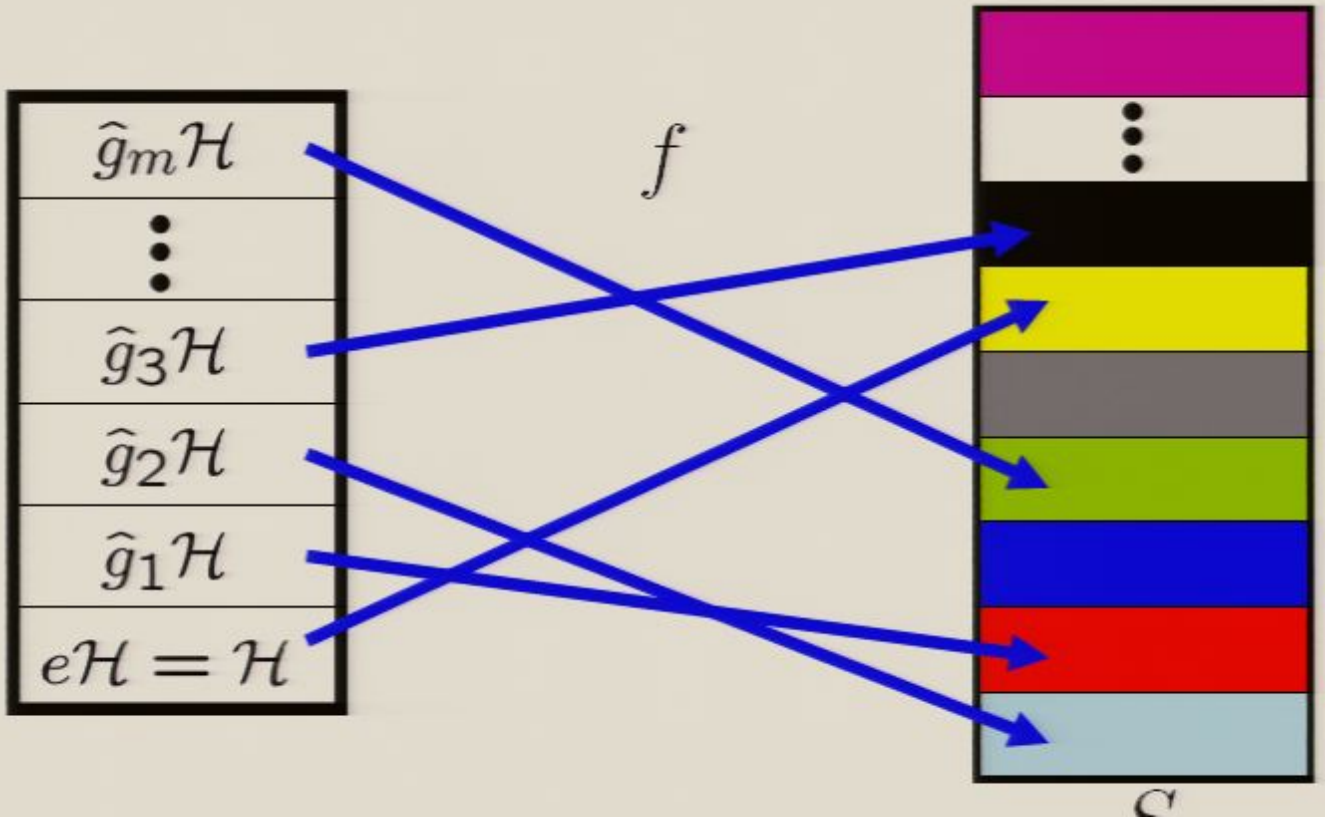
$$\rho_{\mathcal{H}} = \frac{|\mathcal{H}|}{|\mathcal{G}|} \sum_{g \in \hat{\mathcal{G}}} |g\mathcal{H}\rangle\langle g\mathcal{H}|$$ hidden subgroup state

The Hidden Subgroup Problem

Setup: Fix a group $\mathcal{G}$ (known) and a subgroup $\mathcal{H} \subset \mathcal{G}$ (unknown). Given query access to a function $f: \mathcal{G} \to S$ that is constant and distinct on left (right) cosets of $\mathcal{H}$ in $\mathcal{G}$. We say that f hides $\mathcal{H}$.

Problem: Find a generating set for $\mathcal{H}$ ("identify $\mathcal{H}$").

Efficient: If runs in time polylog($|\mathcal{G}|$)



Graph Isomorphism

adjacency matrix A_1

$G_1 = (V_1, E_1)$

adjacency matrix A_2

$G_2 = (V_2, E_2)$

Problem: Is there a 1-to-1 mapping p from the vertices V_1 to the vertices V_2 such that the edges are respected, $p(E_1) = E_2$?

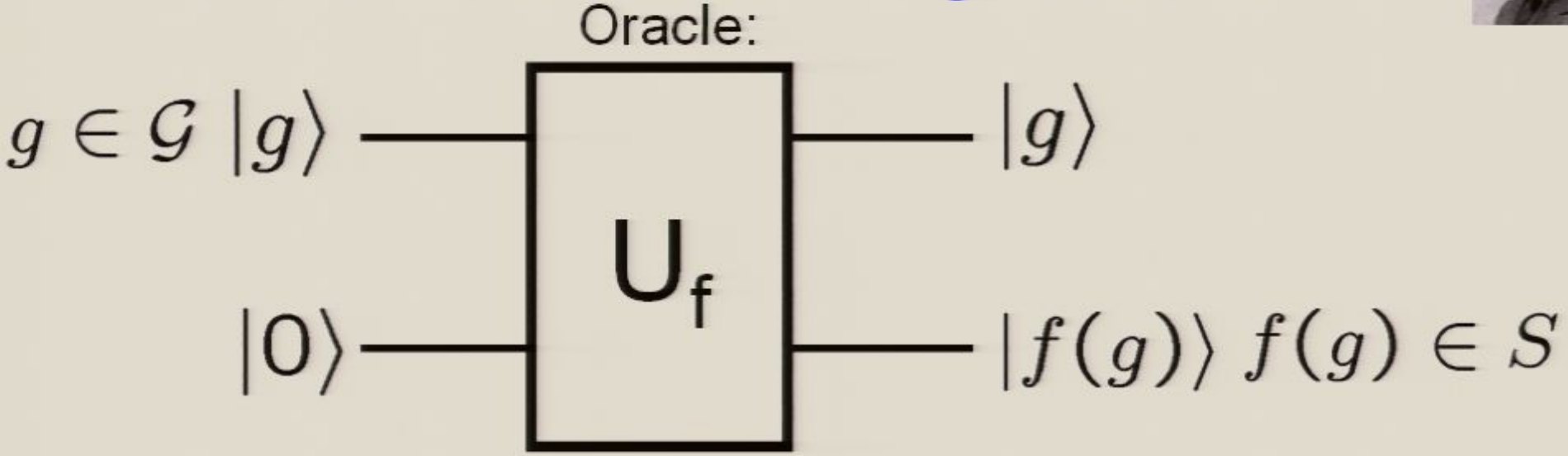
Mapping to the HSP:

$$f : \mathcal{S}_{2n} \rightarrow \mathbb{Z}_{n(2n-1)}$$

$$f(\pi) = \pi(A_1 \oplus A_2)$$

If graphs are not isomorphic, hidden subgroup will not mix the graphs. If they are isomorphic, they will mix the graphs.

Standard Query Model



Query in equal superposition over group elements

$$\frac{1}{\sqrt{|\mathcal{G}|}} \sum_{g \in \mathcal{G}} |g\rangle|0\rangle \rightarrow \sum_{g \in \mathcal{G}} \frac{1}{\sqrt{|\mathcal{G}|}} |g\rangle|f(g)\rangle$$

$$\rho_{\mathcal{H}} = \frac{|\mathcal{H}|}{|\mathcal{G}|} \sum_{g \in \hat{\mathcal{G}}} |g\mathcal{H}\rangle\langle g\mathcal{H}|$$ hidden subgroup state

You Down With Symmetry?

$$\rho_{\mathcal{H}} = \frac{|\mathcal{H}|}{|\mathcal{G}|} \sum_{g \in \hat{\mathcal{G}}} |g\mathcal{H}\rangle\langle g\mathcal{H}| \quad \text{hidden subgroup state}$$

Symmetry under left regular representation:

$$D_L(g)|g'\rangle = |gg'\rangle \qquad D_L(g)\rho_{\mathcal{H}} D_L(g^{-1}) = \rho_{\mathcal{H}}$$

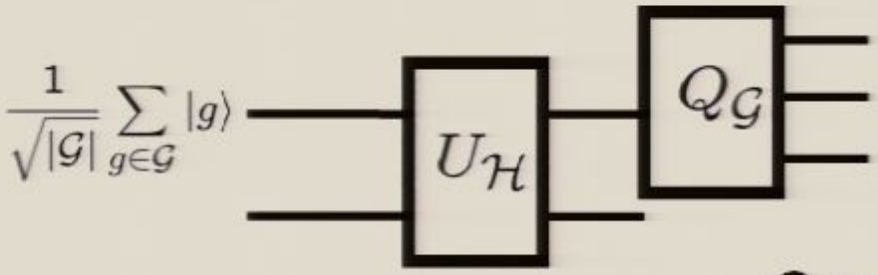
You Down With Symmetry?

$$\rho_{\mathcal{H}} = \frac{|\mathcal{H}|}{|\mathcal{G}|} \sum_{g \in \hat{\mathcal{G}}} |g\mathcal{H}\rangle\langle g\mathcal{H}| \quad \text{hidden subgroup state}$$

Symmetry under left regular representation:

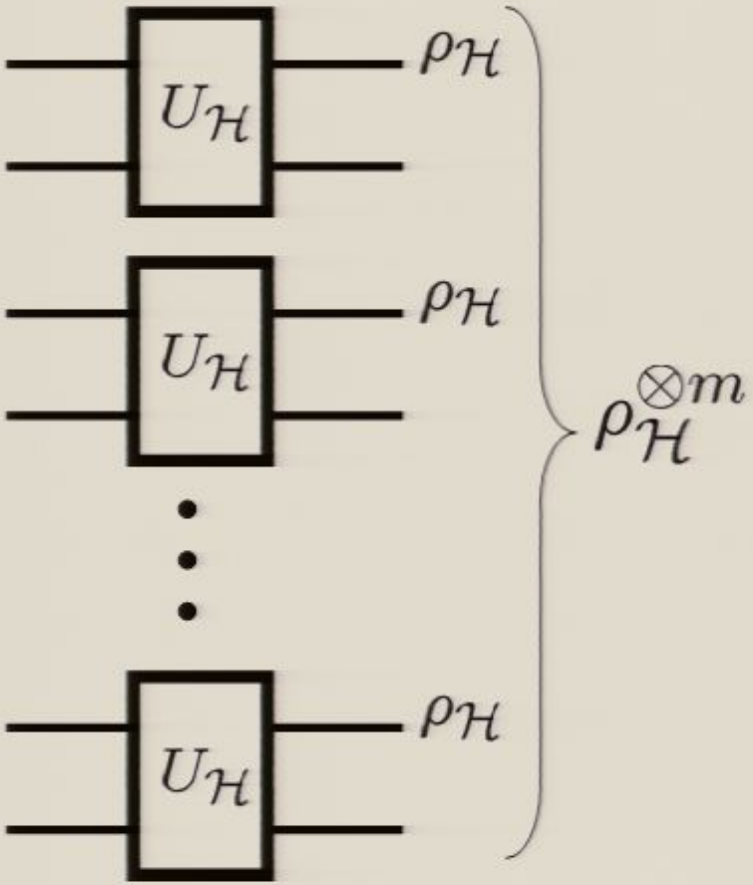
$$D_L(g)|g'\rangle = |gg'\rangle \qquad D_L(g)\rho_{\mathcal{H}} D_L(g^{-1}) = \rho_{\mathcal{H}}$$

Fourier transform over finite group $\mathcal{G}$



Can we solve HSP this way?

Multicopy

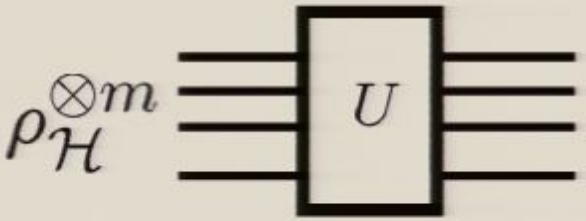


Can we make a measurement on $m < O(\log |\mathcal{G}|)$ copies and learn the subgroup?

In general (and for important case of symmetric group) **NO**

[Moore, Russell, Hallgren, Roetteler, Sen 05]

Required:



You Down With Symmetry?

$$\rho_{\mathcal{H}} = \frac{|\mathcal{H}|}{|\mathcal{G}|} \sum_{g \in \hat{\mathcal{G}}} |g\mathcal{H}\rangle\langle g\mathcal{H}| \quad \text{hidden subgroup state}$$

Symmetry under left regular representation:

$$D_L(g)|g'\rangle = |gg'\rangle \qquad D_L(g)\rho_{\mathcal{H}} D_L(g^{-1}) = \rho_{\mathcal{H}}$$

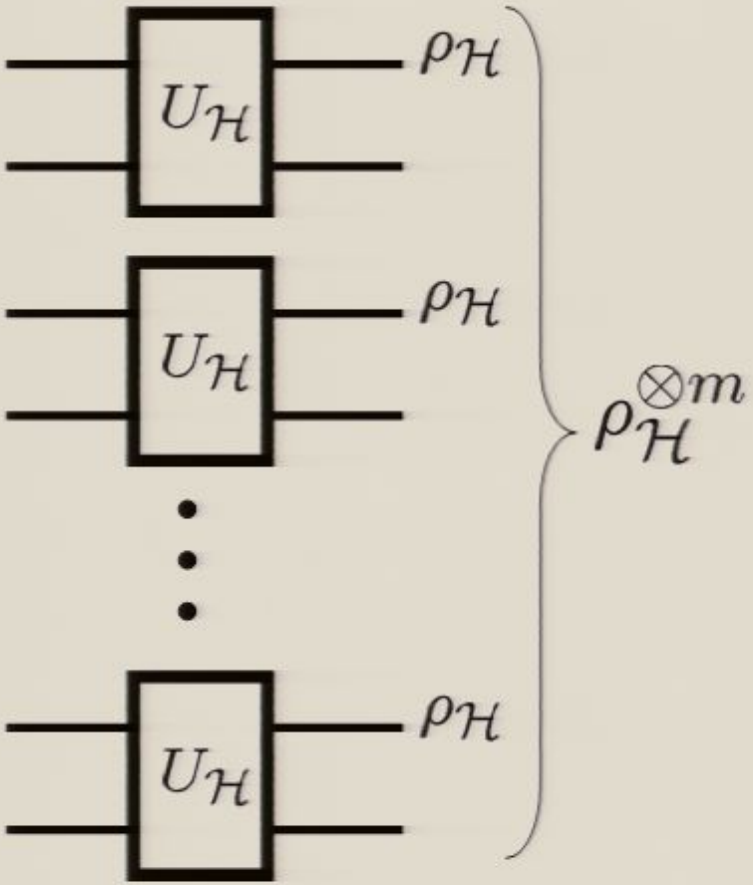
Symmetry of two copies?

$$\rho_{\mathcal{H}} \otimes \rho_{\mathcal{H}}$$

Permutation symmetry….measure the Young Diagram?

Nope [Childs, Harrow, Wocjan 06]

Multicopy

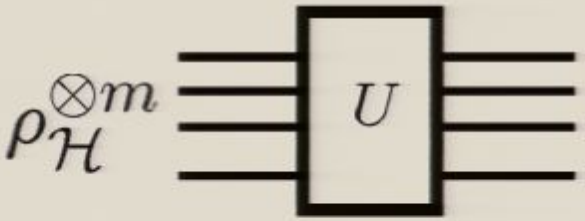


Can we make a measurement on $m < O(\log |\mathcal{G}|)$ copies and learn the subgroup?

In general (and for important case of symmetric group) **NO**

[Moore, Russell, Hallgren, Roetteler, Sen 05]

Required:



You Down With Symmetry?

$$\rho_{\mathcal{H}} = \frac{|\mathcal{H}|}{|\mathcal{G}|} \sum_{g \in \hat{\mathcal{G}}} |g\mathcal{H}\rangle\langle g\mathcal{H}| \quad \text{hidden subgroup state}$$

Symmetry under left regular representation:

$$D_L(g)|g'\rangle = |gg'\rangle \qquad D_L(g)\rho_{\mathcal{H}} D_L(g^{-1}) = \rho_{\mathcal{H}}$$

Symmetry of two copies?

$$\rho_{\mathcal{H}} \otimes \rho_{\mathcal{H}}$$

Permutation symmetry….measure the Young Diagram?

Nope [Childs, Harrow, Wocjan 06]

Heisenberg Group

Semidirect product group $\mathbb{Z}_p^2 \rtimes \mathbb{Z}_p$

Elements of the group:

$$\left(\begin{pmatrix} x \\ y \end{pmatrix}, b\right) \quad x, y, b \in \mathbb{Z}_p$$

Multiplication rule:

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, b_1\right)\left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, b_2\right) =$$

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{b_1} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, b_1 + b_2\right)$$

From the play "Copenhagen" Margrethe Bohr to Heisenberg:

"Your talent is for ski-ing too fast for anyone to see where you are. For always being in more than one position at a time, like one of your particles."

You Down With Symmetry?

$$\rho_{\mathcal{H}} = \frac{|\mathcal{H}|}{|\mathcal{G}|} \sum_{g \in \hat{\mathcal{G}}} |g\mathcal{H}\rangle\langle g\mathcal{H}| \quad \text{hidden subgroup state}$$

Symmetry under left regular representation:

$$D_L(g)|g'\rangle = |gg'\rangle \qquad D_L(g)\rho_{\mathcal{H}} D_L(g^{-1}) = \rho_{\mathcal{H}}$$

Symmetry of two copies?

$$\rho_{\mathcal{H}} \otimes \rho_{\mathcal{H}}$$

Permutation symmetry….measure the Young Diagram?

Nope [Childs, Harrow, Wocjan 06]

Heisenberg Group

Semidirect product group $\mathbb{Z}_p^2 \rtimes \mathbb{Z}_p$

Elements of the group:

$$\left(\begin{pmatrix} x \\ y \end{pmatrix}, b\right) \quad x, y, b \in \mathbb{Z}_p$$

Multiplication rule:

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, b_1\right)\left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, b_2\right) =$$

$$\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{b_1} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, b_1 + b_2\right)$$

From the play "Copenhagen" Margrethe Bohr to Heisenberg:

"Your talent is for ski-ing too fast for anyone to see where you are. For always being in more than one position at a time, like one of your particles."

Multicopy Success!

Efficient algorithm for the Heisenberg HSP: $\mathbb{Z}_p^2 \rtimes \mathbb{Z}_p$

[D. Bacon, A.M. Childs, and W. van Dam FOCS 2005]

PGM/optimal measurement approach:

$$\rho_{\mathcal{H}} \qquad Pr(succ) = O\left(\frac{1}{p}\right)$$

$$\rho_{\mathcal{H}} \otimes \rho_{\mathcal{H}} \qquad Pr(succ) = O(1)$$

Efficient algorithm for the Heisenberg HSP:

1. PGM is optimal and succeed w.h.p.
2. How to efficiently implement the PGM?

But Why Does It Work?

Clebsch-Gordan Transform To The Rescue?

Problem:

$\rho_{\mathcal{H}} \otimes \rho_{\mathcal{H}}$ does not have a Clebsch-Gordan related symmetry

Graph Isomorphism

adjacency matrix A_1

$G_1 = (V_1, E_1)$

adjacency matrix A_2

$G_2 = (V_2, E_2)$

Problem: Is there a 1-to-1 mapping p from the vertices V_1 to the vertices V_2 such that the edges are respected, $p(E_1) = E_2$?

Mapping to the HSP:

$$f : \mathcal{S}_n \wr \mathcal{S}_2 \to \mathbb{Z}_{n(2n-1)}$$

$$f((\pi_1, \pi_2, \tau)) = \tau(\pi_1(A_1) \oplus \pi_2(A_2))$$

Notice now we are only worried if hidden subgroup has a nontrivial τ

Conjugate Subgroups

Two subgroups, $\mathcal{H}_1$ and $\mathcal{H}_2$, are conjugate if there exists an element of the group $g \in \mathcal{G}$ such that

$$\mathcal{H}_1 = \{ghg^{-1}, h \in \mathcal{H}_2\}$$

This is an equivalence relation among the subgroups of $\mathcal{G}$

$$\mathcal{H}_i \equiv_{\mathcal{G}} \mathcal{H}_j$$

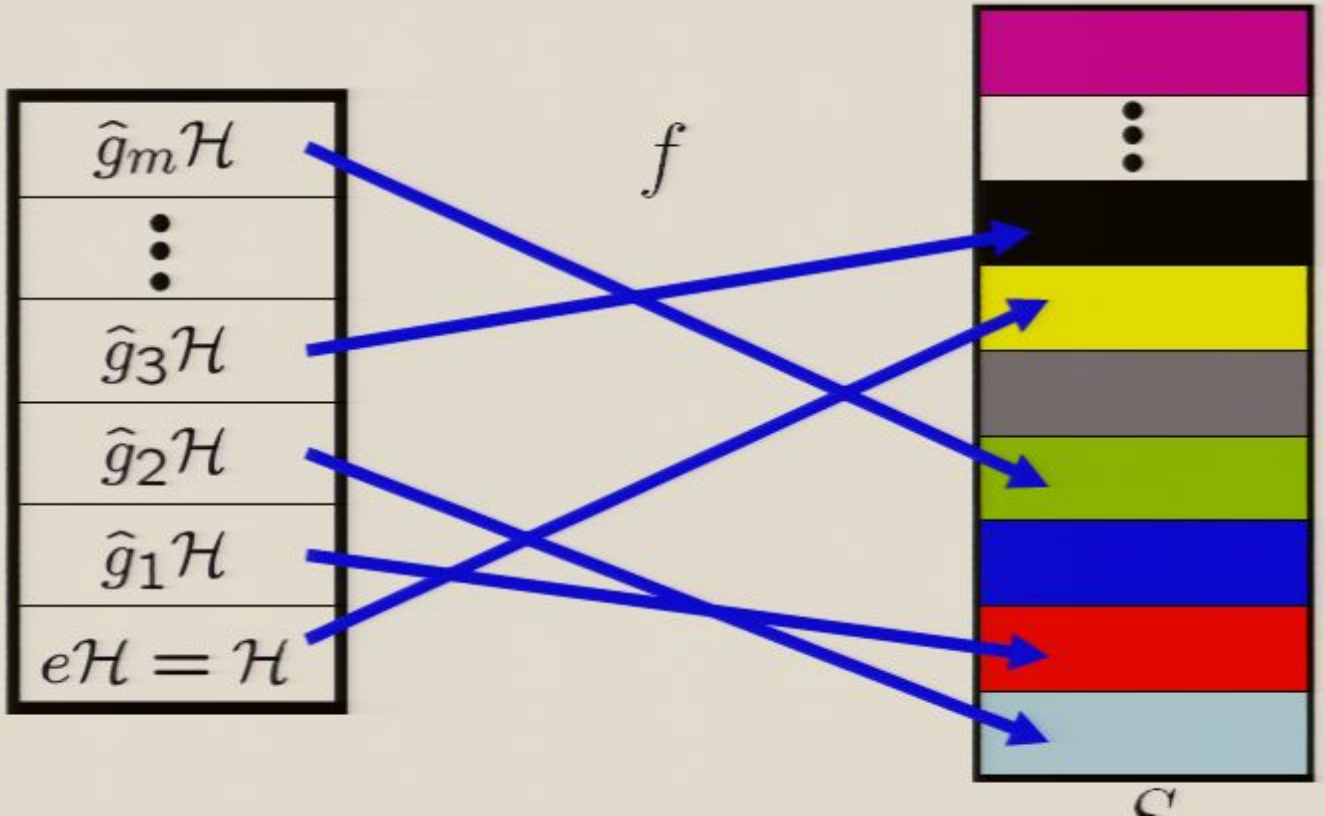
ir: voy, vas, va, vamos, van

Hidden Subgroup Conjugacy Problem

Setup: Fix a group $\mathcal{G}$ (known) and a subgroup $\mathcal{H} \subset \mathcal{G}$ (unknown). Given query access to a function $f: \mathcal{G} \to S$ that is constant and distinct on left (right) cosets of $\mathcal{H}$ in $\mathcal{G}$. We say that f hides $\mathcal{H}$.

Problem: identify the conjugate subgroup class of $\mathcal{H}$.

Efficient: If runs in time polylog($|\mathcal{G}|$)



Relationships

How do the hidden subgroup problem (HSP) and the hidden subgroup conjugacy problem (HSCP) differ?

1. If group is abelian, HSCP=HSP

All subgroups are only conjugate to themselves

$$g\mathcal{H}g^{-1} = \mathcal{H}$$

2. If subgroups are normal, HSCP=HSP

All subgroups are only conjugate to themselves

$$g\mathcal{H}g^{-1} = \mathcal{H}$$

These are two cases where we know quantum computers can efficiently solve the HSP. Coincidence?

Symmetries of HSCP States

Hidden subgroup conjugate state

$$\rho_{[\mathcal{H}]} = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} \rho_{g\mathcal{H}g^{-1}}$$

Hidden subgroup conjugate states

$$\rho_{[\mathcal{H}]}^{\otimes m} = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} (\rho_{g\mathcal{H}g^{-1}})^{\otimes m}$$

In context of optimal measurement method (PGM)

[e.g. Ip 03, Bacon, Childs, and van Dam 05]

this translates into extra symmetry of the optimal measurement

$$\rho_{[\mathcal{H}]}^{\otimes m} = \bigoplus_{\mu_1,\ldots,\mu_m} \left(I_D \otimes \bigoplus_{\mu} \left(R_{[\mathcal{H}]} \otimes I_{d_\mu} \right) \right)$$

Symmetries of HSCP States

What is the extra symmetry of the multiple HSCP states?

Clebsch-Gordan transform for the regular representation of finite groups:

$$D_R(g)^{\otimes m} = \left[\bigoplus_{\mu}(I_{d_\mu} \otimes D_\mu(g))\right]^{\otimes m} \quad D_R(g)|g'\rangle = |g'g^{-1}\rangle$$

$$D_{\mu_1}(g) \otimes \cdots \otimes D_{\mu_m}(g) = \bigoplus_{\mu} \left(I_{n_\mu(\mu_1,\ldots,\mu_m)} \otimes D_\mu(g)\right)$$

Symmetries of HSCP States

Hidden subgroup conjugate state

$$\rho_{[\mathcal{H}]} = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} \rho_{g\mathcal{H}g^{-1}}$$

Hidden subgroup conjugate states

$$\rho_{[\mathcal{H}]}^{\otimes m} = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} (\rho_{g\mathcal{H}g^{-1}})^{\otimes m}$$

In context of optimal measurement method (PGM)

[e.g. Ip 03, Bacon, Childs, and van Dam 05]

this translates into extra symmetry of the optimal measurement

$$\rho_{[\mathcal{H}]}^{\otimes m} = \bigoplus_{\mu_1,\ldots,\mu_m} \left(I_D \otimes \bigoplus_{\mu} \left(R_{[\mathcal{H}]} \otimes I_{d_\mu} \right) \right)$$

Symmetries of HSCP States

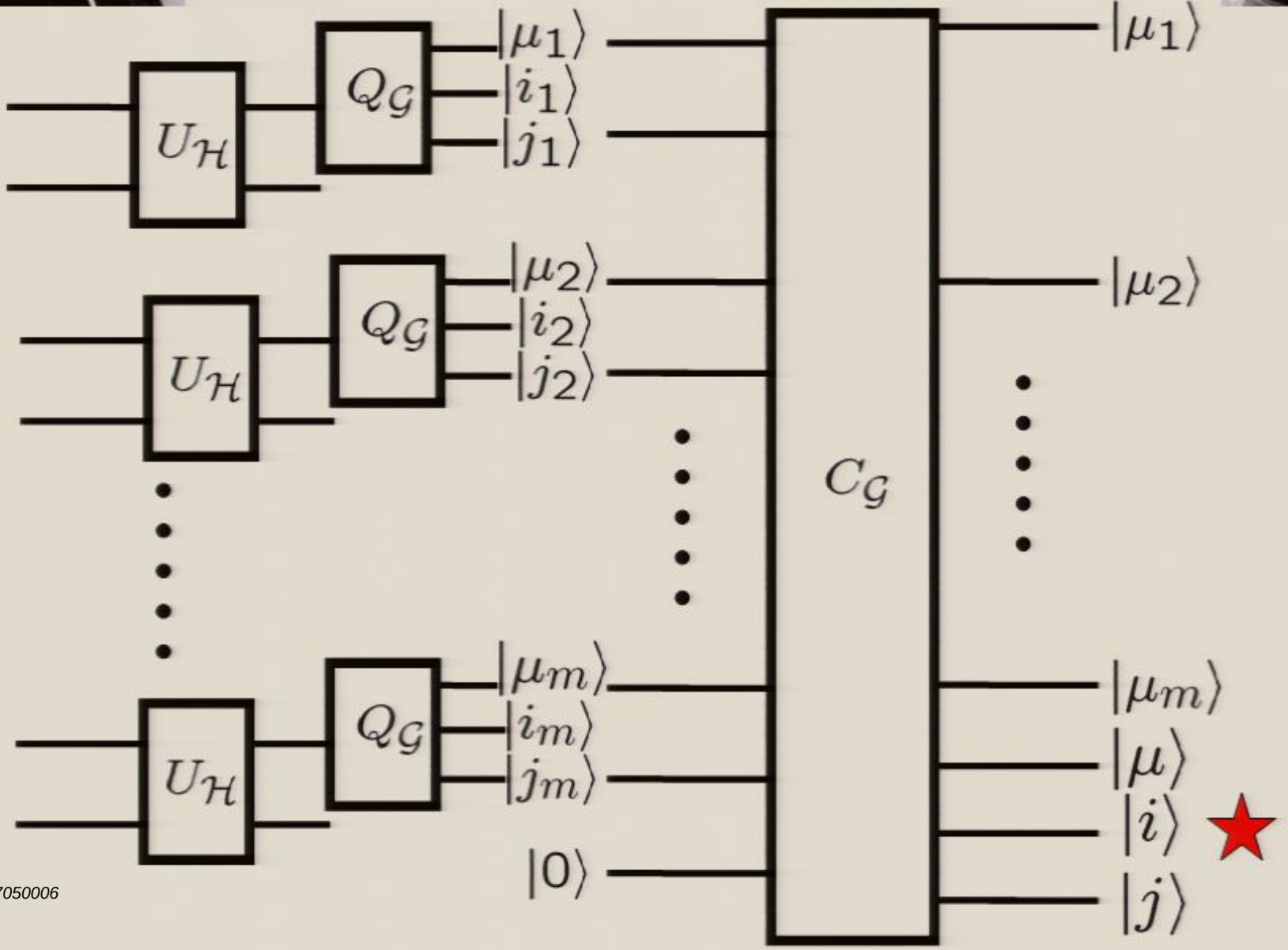
What is the extra symmetry of the multiple HSCP states?

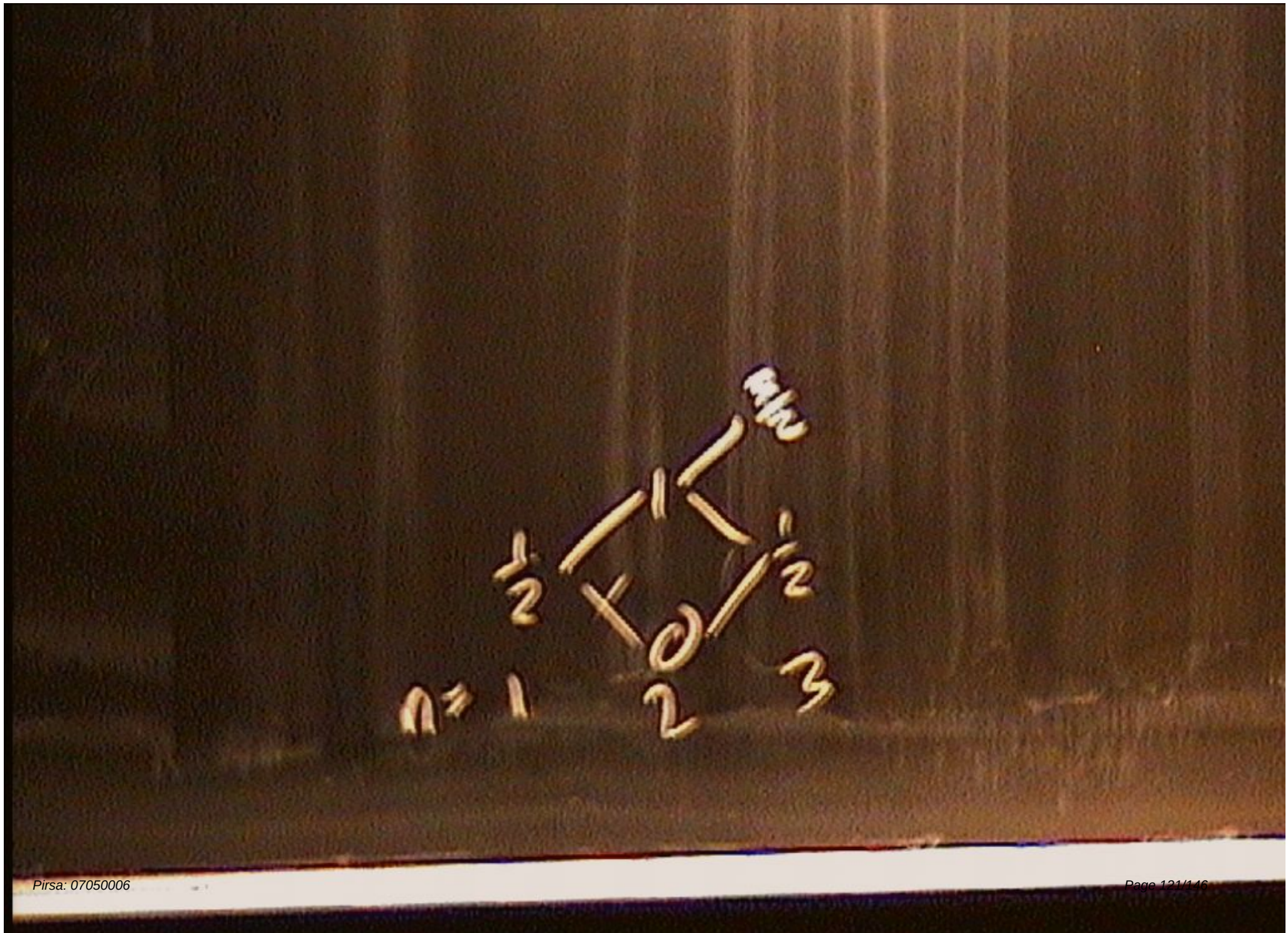
Clebsch-Gordan transform for the regular representation of finite groups:

$$D_R(g)^{\otimes m} = \left[\bigoplus_{\mu}(I_{d_\mu} \otimes D_\mu(g))\right]^{\otimes m} \quad D_R(g)|g'\rangle = |g'g^{-1}\rangle$$

$$D_{\mu_1}(g) \otimes \cdots \otimes D_{\mu_m}(g) = \bigoplus_{\mu} \left(I_{n_\mu(\mu_1,\ldots,\mu_m)} \otimes D_\mu(g)\right)$$

General Circuit

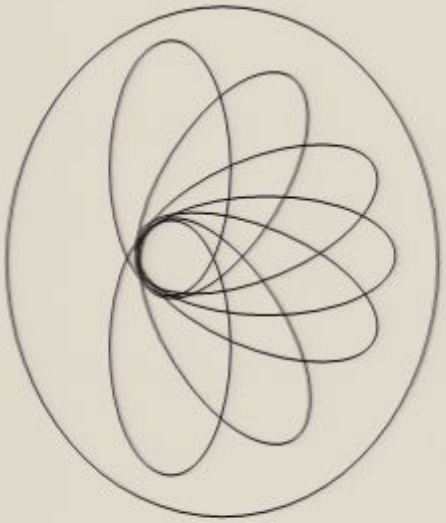



n=1
2
3

Heisenberg HSCP and HSP

[Bacon, arXiv:quant-ph/0612107]

Heisenberg HSCP $\Rightarrow$ Heisenberg HSP



Conjugate subgroups are all normal subgroups of a subgroup of Heisenberg group

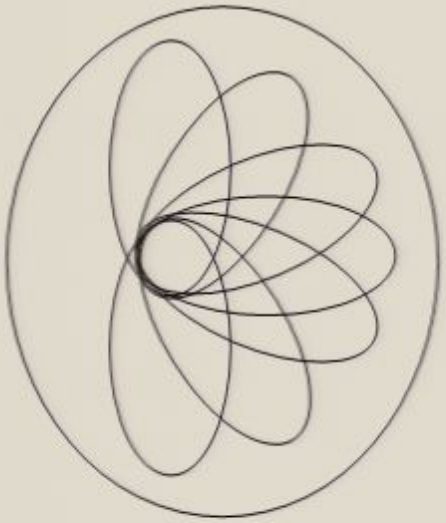
Identifying which conjugate subgroup identifies this subgroup

Thus solving HSCP implies solving HSP (use normal subgroup algorithm)

Heisenberg HSCP and HSP

[Bacon, arXiv:quant-ph/0612107]

Heisenberg HSCP $\Rightarrow$ Heisenberg HSP



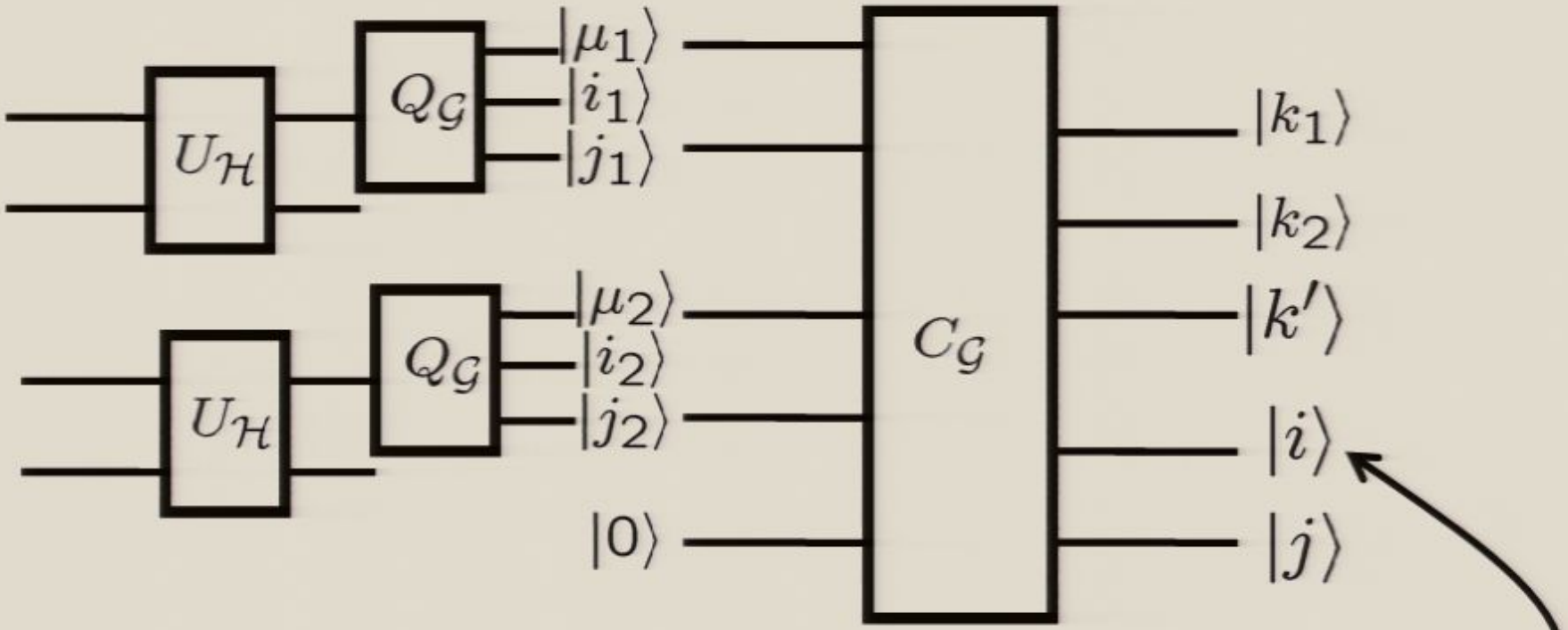
Conjugate subgroups are all normal subgroups of a subgroup of Heisenberg group

Identifying which conjugate subgroup identifies this subgroup

Thus solving HSCP implies solving HSP (use normal subgroup algorithm)

Heisenberg HSCP, CG Way

[Bacon, arXiv:quant-ph/0612107]



$$\frac{1}{\sqrt{p}} \sum_{s \in \mathbb{Z}_p} \omega^{i 2^{-1} \frac{k_1 k_2}{k_1 + k_2} s^2} |s\rangle$$

j labels set of conjugate subgroups

Heisenberg HSCP, CG Way

[Bacon, arXiv:quant-ph/0612107]

$$\frac{1}{\sqrt{p}} \sum_{s \in \mathbb{Z}_p} \omega^{i 2^{-1} \frac{k_1 k_2}{k_1 + k_2} s^2} |s\rangle$$

i can be found by performing

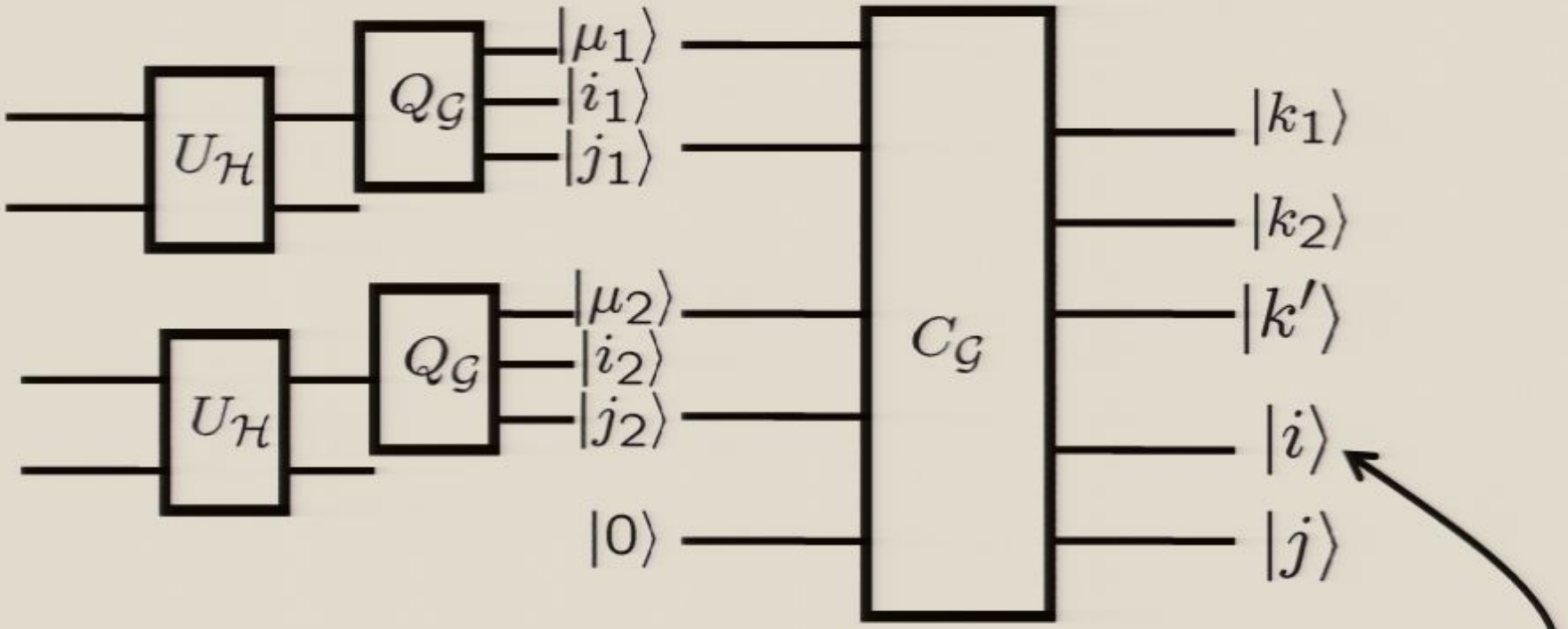
$$|t^2\rangle \rightarrow \frac{1}{\sqrt{2}}(|t\rangle + |-t\rangle)$$

and performing a QFT

Clebsch-Gordan transform over Heisenberg group is related to "symmetry" which allows for efficient quantum algorithm for the Heisenberg HSP.

Heisenberg HSCP, CG Way

[Bacon, arXiv:quant-ph/0612107]



$$\frac{1}{\sqrt{p}} \sum_{s \in \mathbb{Z}_p} \omega^{i 2^{-1} \frac{k_1 k_2}{k_1 + k_2} s^2} |s\rangle$$

j labels set of conjugate subgroups

Heisenberg HSCP, CG Way

[Bacon, arXiv:quant-ph/0612107]

$$\frac{1}{\sqrt{p}} \sum_{s \in \mathbb{Z}_p} \omega^{i 2^{-1} \frac{k_1 k_2}{k_1 + k_2} s^2} |s\rangle$$

i can be found by performing

$$|t^2\rangle \rightarrow \frac{1}{\sqrt{2}}(|t\rangle + |-t\rangle)$$

and performing a QFT

Clebsch-Gordan transform over Heisenberg group is related to "symmetry" which allows for efficient quantum algorithm for the Heisenberg HSP.

Heisenberg HS State

Restricted subgroups:

$$\mathcal{H}_{d_1,d_2} = \left\{ \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, 0 \right), \left(\begin{pmatrix} d_1 \\ d_2 \end{pmatrix}, 1 \right), \left(\begin{pmatrix} 2d_1 + d_2 \\ 2d_2 \end{pmatrix}, 2 \right), \ldots \right\}$$

Random coset states:

$$|l_1, l_2, d_1, d_2\rangle = \frac{1}{\sqrt{p}} \sum_{b \in \mathbb{Z}_p} \left| \left(\left(\begin{pmatrix} l_1 \\ l_2 \end{pmatrix} + M^{(b)} \begin{pmatrix} d_1 \\ d_2 \end{pmatrix} \right), b \right) \right\rangle$$

$$M^{(b)} = \sum_{i=0}^{b-1} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^i = \begin{bmatrix} b & \frac{b(b-1)}{2} \\ 0 & b \end{bmatrix}$$

Coset labels:

$l_1, l_2 \in_U \mathbb{Z}_p$

Hidden Subgroup states:

$$\rho_{d_1,d_2} = \frac{1}{p^2} \sum_{l_1,l_2 \in \mathbb{Z}_p} |l_1, l_2, d_1, d_2\rangle\langle l_1, l_2, d_1, d_2|$$

HS States

$$|l_1, l_2, d_1, d_2\rangle = \frac{1}{\sqrt{p}} \sum_{b \in \mathbb{Z}_p} \left| \left(\left(\begin{pmatrix} l_1 \\ l_2 \end{pmatrix} + M^{(b)} \begin{pmatrix} d_1 \\ d_2 \end{pmatrix} \right), b \right) \right\rangle$$

$$|l_1, l_2, d_1, d_2\rangle = \frac{1}{\sqrt{p}} \sum_{b \in \mathbb{Z}_p} \left| l_1 + bd_1 + \frac{b(1-b)}{2} d_2, l_2 + bd_2; b \right\rangle$$

Perform the QFT over $(\mathbb{Z}_p)^2$ to the first two registers:

$$|l_1, l_2, d_1, d_2\rangle = \frac{1}{\sqrt{p^3}} \sum_{b, x_1, y_1 \in \mathbb{Z}_p} \omega_p^{(l_1 + bd_1 + \frac{b(1-b)}{2} d_2) x_1 + (l_2 + bd_2) y_1} |x_1, y_1, b\rangle$$

Measure these two registers: $x_1, y_1 \in_U \mathbb{Z}_p$

$$|x_1, y_1, d_1, d_2\rangle = \frac{1}{\sqrt{p}} \sum_{b \in \mathbb{Z}_p} \omega_p^{(bd_1 + \frac{b(1-b)}{2} d_2) x_1 + bd_2 y_1} |b\rangle$$

HS States

Two copies: $x_1, y_1, x_2, y_2 \in_U \mathbb{Z}_p$

$$\frac{1}{p} \sum_{b_1, b_2 \in \mathbb{Z}_p} \omega_p^{(b_1 x_1 + b_2 x_2) d_1 + \left(\frac{b_1(1-b_1)}{2} x_1 + b_1 y_1 + \frac{b_2(1-b_2)}{2} x_2 + b_2 y_2 \right) d_2} |b_1, b_2\rangle$$

$$v = b_1 x_1 + b_2 x_2$$

$$w = \frac{b_1(1-b_1)}{2} x_1 + b_1 y_1 + \frac{b_2(1-b_2)}{2} x_2 + b_2 y_2$$

$$\frac{1}{p} \sum_{b_1, b_2 \in \mathbb{Z}_p} \omega_p^{v d_1 + w d_2} |b_1, b_2\rangle$$

Compute v and w:

$$\frac{1}{p} \sum_{b_1, b_2 \in \mathbb{Z}_p} \omega_p^{v d_1 + w d_2} |b_1, b_2\rangle |v, w\rangle$$

Uncompute

If we could erase the b_1,b_2 values:

$$\frac{1}{p} \sum_{b_1,b_2 \in \mathbb{Z}_p} \omega_p^{vd_1+wd_2} |b_1, b_2\rangle |v, w\rangle \rightarrow \frac{1}{p} |0, 0\rangle \sum_{v,w} \omega_p^{vd_1+wd_2} |v, w\rangle$$

Then a QFT over $(\mathbb{Z}_p)^2$ would find d_1 and d_2.

Remember v and w are a function of b_1 and b_2.

Solving Equations

Compute v and w:

$$\frac{1}{p} \sum_{b_1,b_2 \in \mathbb{Z}_p} \omega_p^{vd_1+wd_2} |b_1, b_2\rangle |v, w\rangle$$

$$v = b_1 x_1 + b_2 x_2$$

$$w = \frac{b_1(1-b_1)}{2} x_1 + b_1 y_1 + \frac{b_2(1-b_2)}{2} x_2 + b_2 y_2$$

For fixed x_1, x_2, y_1, y_2 let $S_{v,w}$ be the set of b_1, b_2 solutions to these equations.

$$\frac{1}{p} \sum_{v,w \in \mathbb{Z}_p} \omega_p^{vd_1+wd_2} \left(\sum_{b_1,b_2 \in S_{v,w}} |b_1, b_2\rangle \right) |v, w\rangle$$

We want to implement $\frac{1}{\sqrt{|S_{v,w}|}} \sum_{b_1,b_2 \in S_{v,w}} |b_1, b_2\rangle |v, w\rangle \rightarrow |0, 0\rangle |v, w\rangle$

Solving Equations

$$\frac{1}{\sqrt{|S_{v,w}|}} \sum_{b_1,b_2 \in S_{v,w}} |b_1, b_2\rangle |v, w\rangle \rightarrow |0,0\rangle |v, w\rangle$$

Easier to think about the inverse (do it unitarily):

$$|0,0\rangle |v, w\rangle \rightarrow \frac{1}{\sqrt{|S_{v,w}|}} \sum_{b_1,b_2 \in S_{v,w}} |b_1, b_2\rangle |v, w\rangle$$

i.e. given v and w, transform to superposition over solutions to the equations

$$v = b_1 x_1 + b_2 x_2$$

$$w = \frac{b_1(1-b_1)}{2} x_1 + b_1 y_1 + \frac{b_2(1-b_2)}{2} x_2 + b_2 y_2$$

Solving Equations

$$v = b_1 x_1 + b_2 x_2$$

$$w = \frac{b_1(1-b_1)}{2} x_1 + b_1 y_1 + \frac{b_2(1-b_2)}{2} x_2 + b_2 y_2$$

Assuming y_1, y_2, y_1+y_2 do not equal 0 (prob O(1/p)), then

$$\frac{p(p-1)}{2} \text{ solutions have } |S_{v,w}| = 0$$

$$p \text{ solutions have } |S_{v,w}| = 1$$

$$\frac{p(p-1)}{2} \text{ solutions have } |S_{v,w}| = 2$$

Solving Equations

$$v = b_1 x_1 + b_2 x_2$$

$$w = \frac{b_1(1-b_1)}{2} x_1 + b_1 y_1 + \frac{b_2(1-b_2)}{2} x_2 + b_2 y_2$$

Focus on when there are two solutions.

We can use standard finite arithmetic to find these solutions. Use to create labeled superposition of solutions:

$$\frac{1}{\sqrt{2}} \sum_{j=0,1} |j, (b_1)_j, (b_2)_j\rangle$$

Hadamard first qubit, measure. If 0, you have

$$\frac{1}{\sqrt{2}} \sum_{j=0,1} |(b_1)_j, (b_2)_j\rangle$$

Heisenberg HSP Solved

This allows us to perform:

$$\frac{1}{p}\sum_{b_1,b_2\in\mathbb{Z}_p}\omega_p^{vd_1+wd_2}|b_1,b_2\rangle|v,w\rangle \rightarrow \frac{1}{p}|0,0\rangle\sqrt{|S_{v,w}|}\sum_{v,w}\omega_p^{vd_1+wd_2}|v,w\rangle$$

Which has a O(1/2) fidelity squared with the state we desire.

QFTing the second register will let us find d_1 and d_2

Efficient algorithm for the Heisenberg HSP!

Solving Equations

$$v = b_1 x_1 + b_2 x_2$$

$$w = \frac{b_1(1-b_1)}{2} x_1 + b_1 y_1 + \frac{b_2(1-b_2)}{2} x_2 + b_2 y_2$$

Focus on when there are two solutions.

We can use standard finite arithmetic to find these solutions. Use to create labeled superposition of solutions:

$$\frac{1}{\sqrt{2}} \sum_{j=0,1} |j, (b_1)_j, (b_2)_j\rangle$$

Hadamard first qubit, measure. If 0, you have

$$\frac{1}{\sqrt{2}} \sum_{j=0,1} |(b_1)_j, (b_2)_j\rangle$$

Solving Equations

Compute v and w:

$$\frac{1}{p}\sum_{b_1,b_2\in\mathbb{Z}_p}\omega_p^{vd_1+wd_2}|b_1,b_2\rangle|v,w\rangle$$

$$v = b_1x_1 + b_2x_2$$

$$w = \frac{b_1(1-b_1)}{2}x_1 + b_1y_1 + \frac{b_2(1-b_2)}{2}x_2 + b_2y_2$$

For fixed x_1,x_2,y_1,y_2 let $S_{v,w}$ be the set of b_1,b_2 solutions to these equations.

$$\frac{1}{p}\sum_{v,w\in\mathbb{Z}_p}\omega_p^{vd_1+wd_2}\left(\sum_{b_1,b_2\in S_{v,w}}|b_1,b_2\rangle\right)|v,w\rangle$$

We want to implement $\frac{1}{\sqrt{|S_{v,w}|}}\sum_{b_1,b_2\in S_{v,w}}|b_1,b_2\rangle|v,w\rangle \to |0,0\rangle|v,w\rangle$

Solving Equations

$$\frac{1}{\sqrt{|S_{v,w}|}} \sum_{b_1,b_2 \in S_{v,w}} |b_1, b_2\rangle |v, w\rangle \rightarrow |0, 0\rangle |v, w\rangle$$

Easier to think about the inverse (do it unitarily):

$$|0, 0\rangle |v, w\rangle \rightarrow \frac{1}{\sqrt{|S_{v,w}|}} \sum_{b_1,b_2 \in S_{v,w}} |b_1, b_2\rangle |v, w\rangle$$

i.e. given v and w, transform to superposition over solutions to the equations

$$v = b_1 x_1 + b_2 x_2$$

$$w = \frac{b_1(1-b_1)}{2} x_1 + b_1 y_1 + \frac{b_2(1-b_2)}{2} x_2 + b_2 y_2$$

Heisenberg HSP Solved

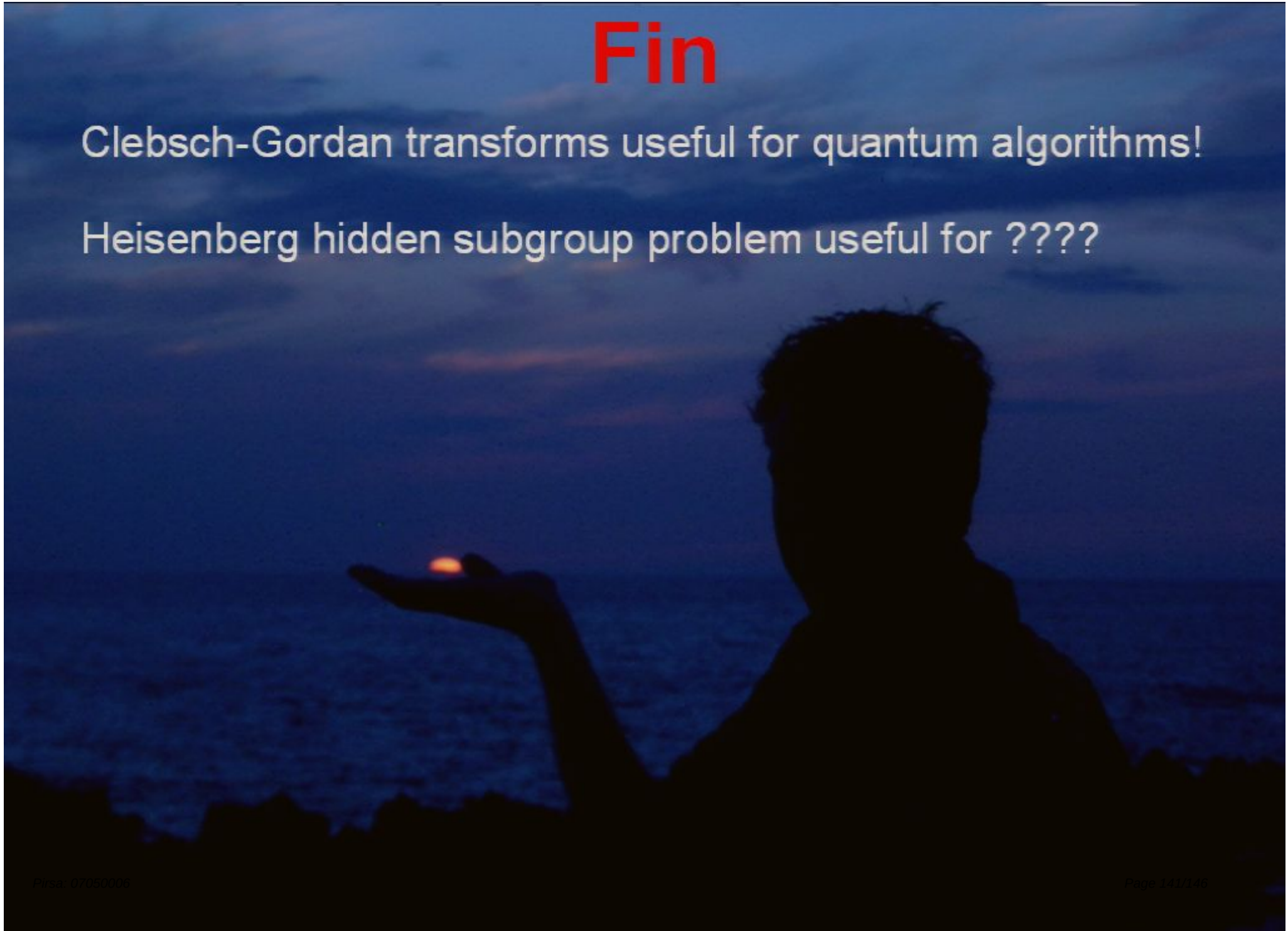
This allows us to perform:

$$\frac{1}{p}\sum_{b_1,b_2\in\mathbb{Z}_p}\omega_p^{vd_1+wd_2}|b_1,b_2\rangle|v,w\rangle \rightarrow \frac{1}{p}|0,0\rangle\sqrt{|S_{v,w}|}\sum_{v,w}\omega_p^{vd_1+wd_2}|v,w\rangle$$

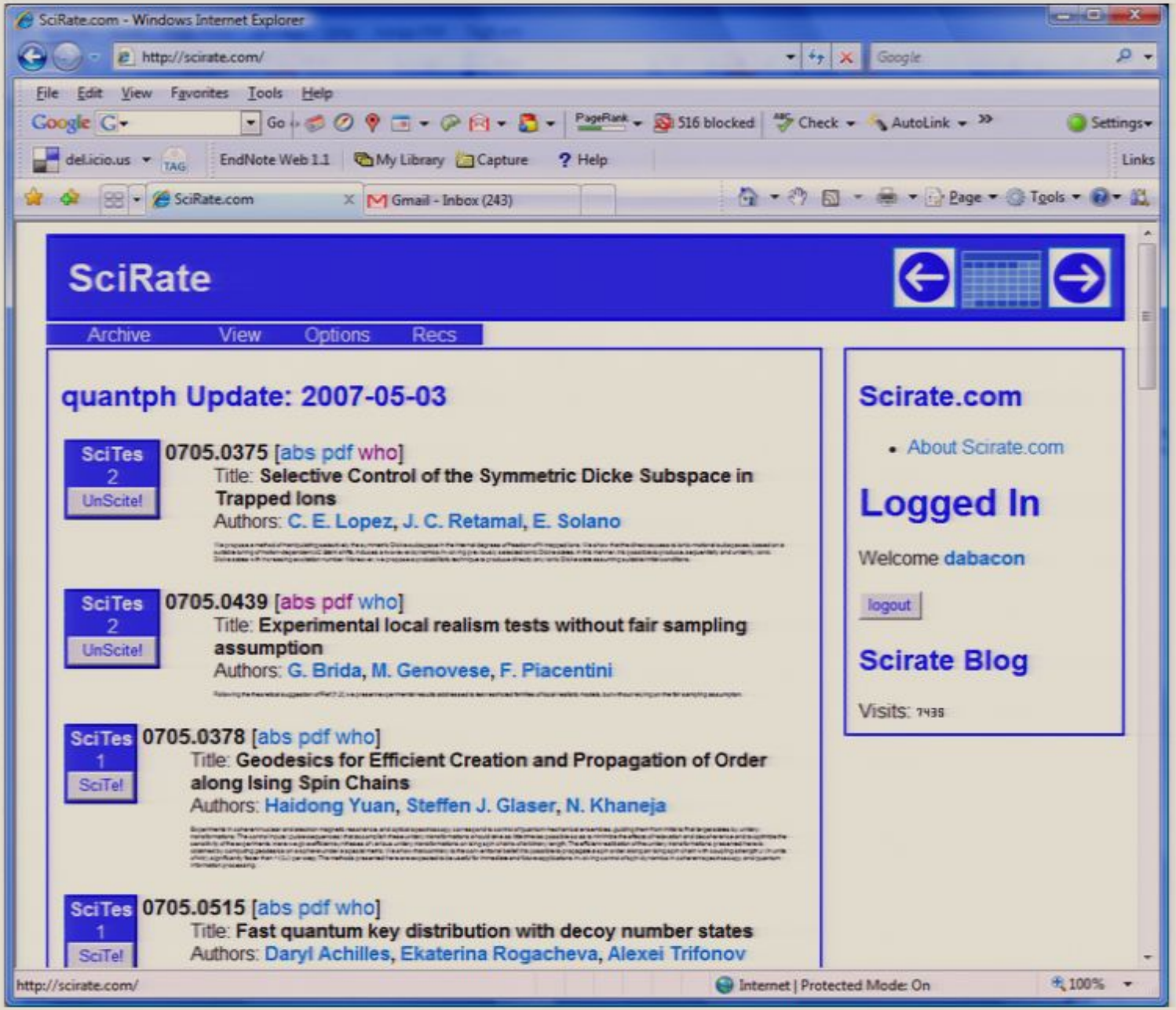
Which has a O(1/2) fidelity squared with the state we desire.

QFTing the second register will let us find d_1 and d_2

Efficient algorithm for the Heisenberg HSP!


Fin
Clebsch-Gordan transforms useful for quantum algorithms!
Heisenberg hidden subgroup problem useful for ????

Quick Promo: scirate.com



Quantum Algorithms Using Clebsch-Gordan Transforms

Dave Bacon
Department of Computer Science & Engineering
University of Washington

funded by

DTO

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

SCIENCE TO SHAPE THE FUTURE OF THE ARMY
ARMY RESEARCH OFFICE
1951

|QW⟩
group

"Que Dubayah"

Collaborators: Childs [Caltech], van Dam [UCSB], Chuang [MIT], Harrow [Bristol]

Heisenberg HSP Solved

This allows us to perform:

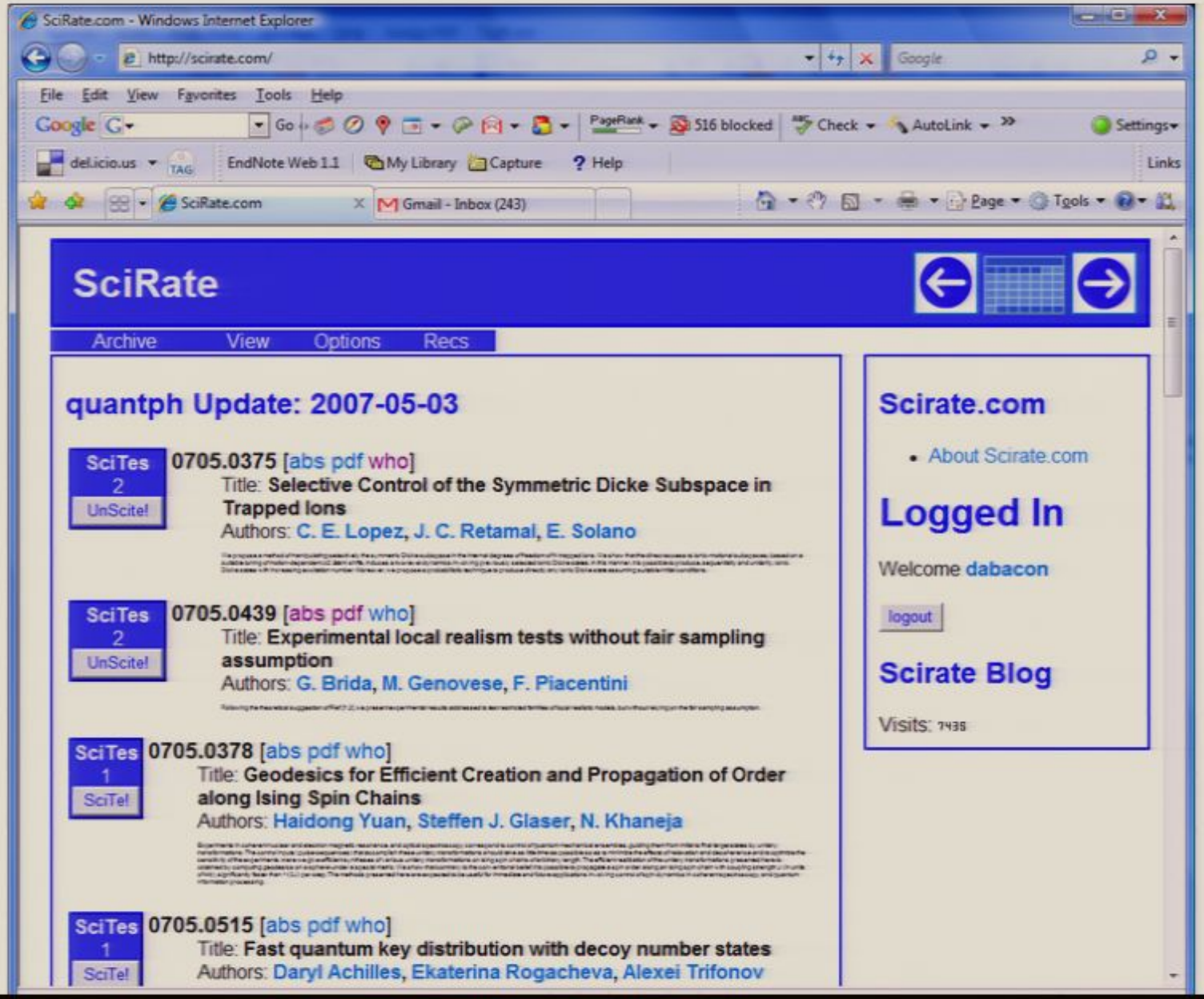
$$\frac{1}{p}\sum_{b_1,b_2\in\mathbb{Z}_p}\omega_p^{vd_1+wd_2}|b_1,b_2\rangle|v,w\rangle \rightarrow \frac{1}{p}|0,0\rangle\sqrt{|S_{v,w}|}\sum_{v,w}\omega_p^{vd_1+wd_2}|v,w\rangle$$

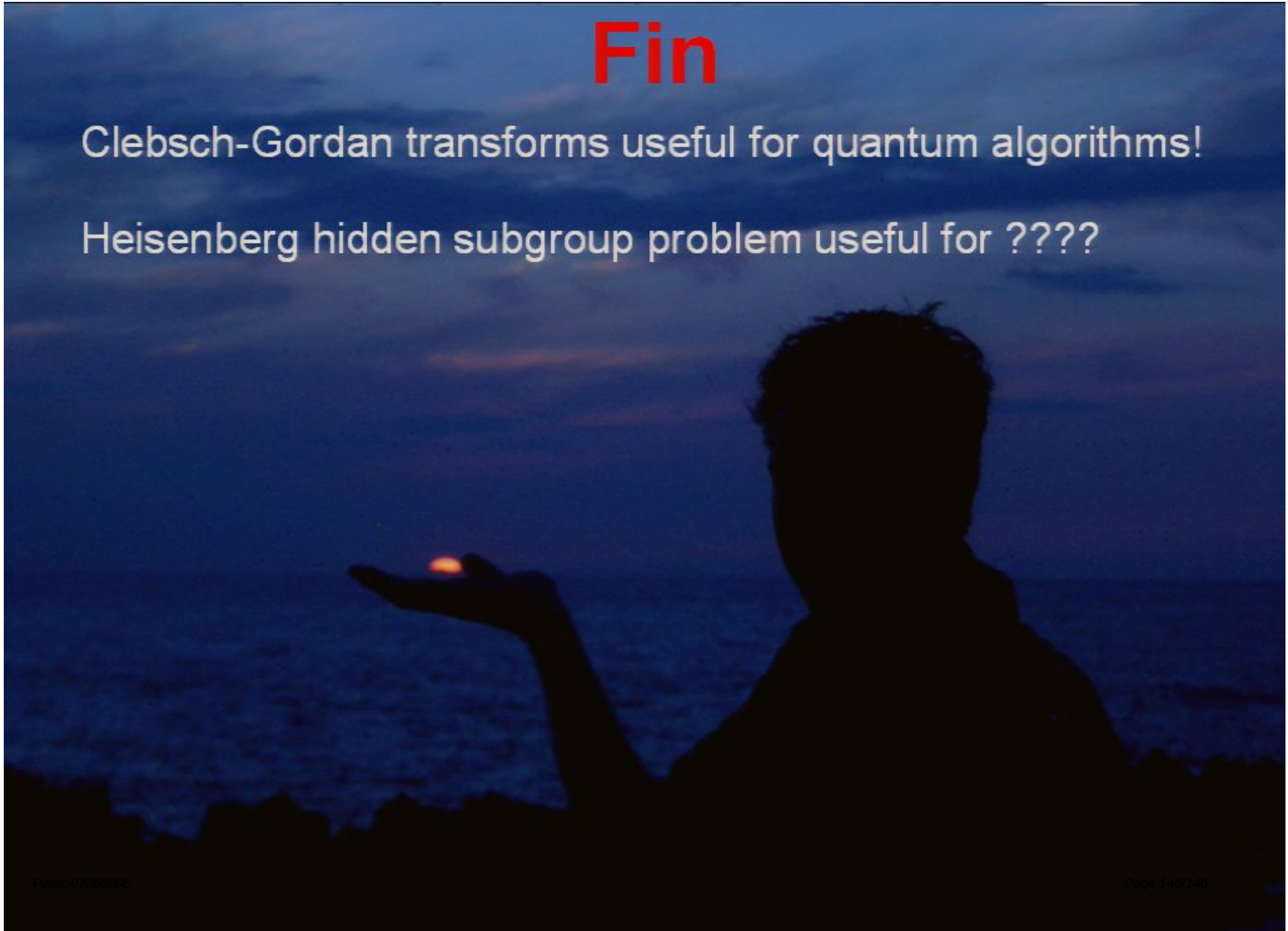
Which has a O(1/2) fidelity squared with the state we desire.

QFTing the second register will let us find d_1 and d_2

Efficient algorithm for the Heisenberg HSP!

Quick Promo: scirate.com




Fin
Clebsch-Gordan transforms useful for quantum algorithms!
Heisenberg hidden subgroup problem useful for ????