Title: Quantum random walks of interacting particles and the graph isomorphism problem.

Date: Jan 20, 2010 02:00 PM

URL: http://pirsa.org/10010001

Abstract: The graph isomorphism (GI) problem plays a central role in the theory of computational complexity and has importance in physics and chemistry as well. While no general efficient algorithm for solving GI is known, it is unlikely to be NP-complete; in this regard it is similar to the factoring problem, for which Shor has developed an efficient quantum algorithm.

In this talk I will discuss our investigations of quantum particles walking on graphs and their implications for possible algorithms for GI. We find that single-particle quantum random walks fail to distinguish some nonequivalent graphs that can be distinguished by random walks with two interacting particles. The implications of these observations for classical and quantum algorithms for GI will be discussed.

Quantum random walks of interacting particles and the graph isomorphism problem

Susan N. Coppersmith
University of Wisconsin, Madison

collaborators: Mark Friesen, John Gamble, Robert Joynt, Shiue-Yuan Shiau

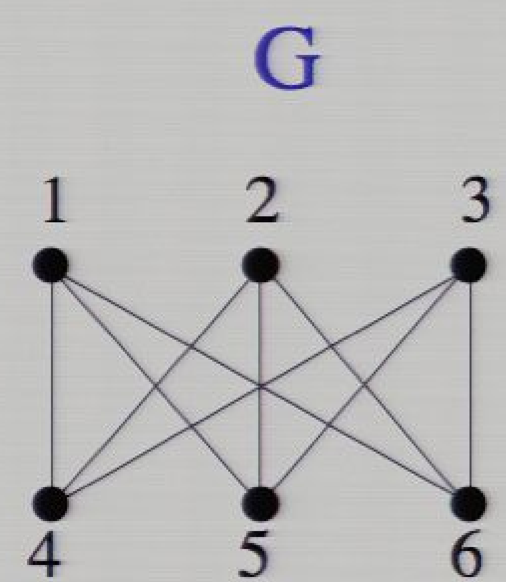
S.-Y. Shiau et al., Quantum Information and Computation 5, 492-506 (2005)
(+ unpublished work)
Funding: NSF, ARO/NSA

Overall goal of work:

- Our goal is to understand how quantum dynamics of physical systems can be exploited to create new, more efficient algorithms (on either classical or quantum computers).
- Here we compare multi-particle quantum random walks as opposed to single-particle quantum random walks in one specific context.
  - Our work provides indications that multi-particle random walks have more computational power for the graph isomorphism problem.

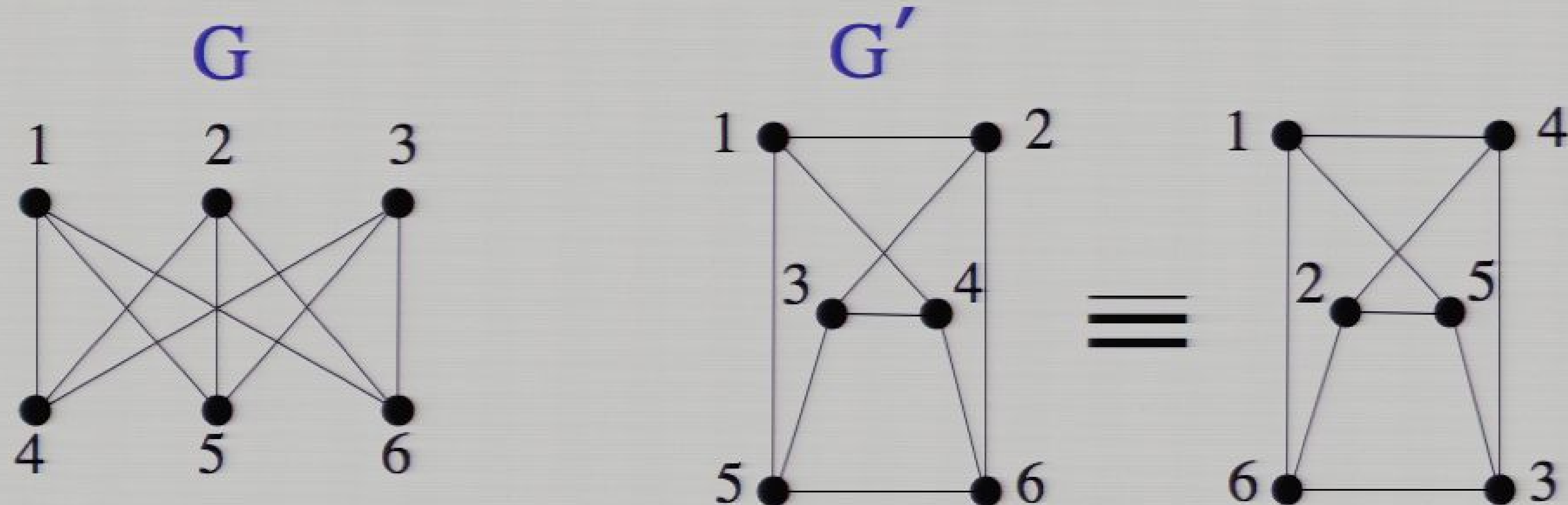
The graph isomorphism problem

A **graph** is a set of N vertices, some pairs of which are connected by edges:



edges between 1 and 4, 1 and 5, 1 and 6, etc.

Graph isomorphism



G’ goes into G if we relabel the vertices of G’ by:
$1 \to 1, 2 \to 4,\ 3 \to 2, 4 \to 5, 5 \to 6, 6 \to 3.$
If such a transformation exists, then we say that G and G’ are **isomorphic**.

The problem of determining whether two graphs are isomorphic is called the graph isomorphism (GI) problem and it is a classic problem of computer science, *a pattern recognition problem in a decisional form*.

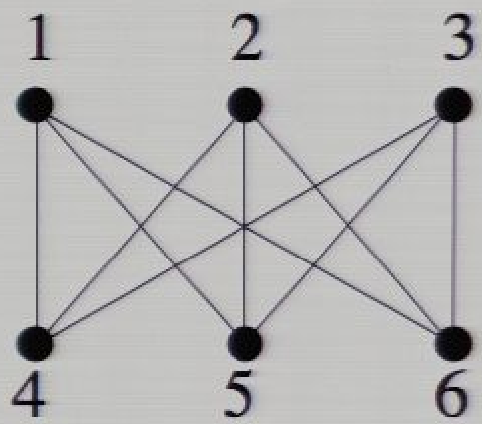
GI has applications to optimization, communications, enumeration of compounds and atomic clusters, fingerprint matching, etc.

Computational complexity

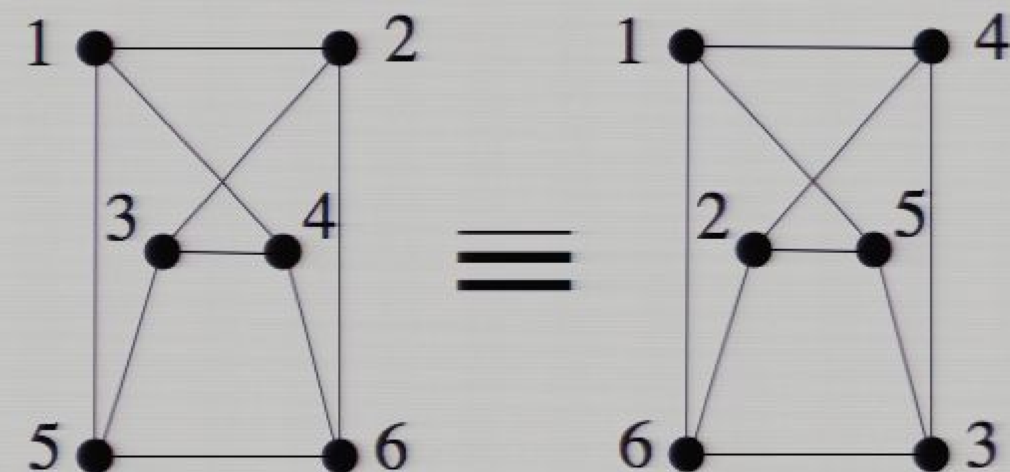
- P is the set of problems that are soluble in polynomial time
- NP is the set of problems whose solutions are checkable in polynomial time – it has never been shown that P $\neq$ NP
- NP-complete problems are the hardest ones in NP: those whose solution would guarantee, via a polynomial mapping, the solution of all NP problems in polynomial time. Many well-known problems in NP have been shown to be NP-complete, but GI is an exception (as is factoring).

Graph isomorphism

G



G′



G' goes into G if we relabel the vertices of G' by:

$1 \rightarrow 1, 2 \rightarrow 4,\ 3 \rightarrow 2, 4 \rightarrow 5, 5 \rightarrow 6, 6 \rightarrow 3.$

If such a transformation exists, then we say that G and G' are **isomorphic**.

The problem of determining whether two graphs are isomorphic is called the graph isomorphism (GI) problem and it is a classic problem of computer science, *a pattern recognition problem in a decisional form*.

GI has applications to optimization, communications, enumeration of compounds and atomic clusters, fingerprint matching, etc.

Computational complexity

- P is the set of problems that are soluble in polynomial time
- NP is the set of problems whose solutions are checkable in polynomial time – it has never been shown that P $\neq$ NP
- NP-complete problems are the hardest ones in NP: those whose solution would guarantee, via a polynomial mapping, the solution of all NP problems in polynomial time. Many well-known problems in NP have been shown to be NP-complete, but GI is an exception (as is factoring).

WHAT IS THE COMPUTATIONAL COMPLEXITY OF THE GI PROBLEM?

- Naively, GI is difficult – to search the set of all permutations would take N! operations!
- It is not presently known whether GI can be solved in polynomial time: the best existing algorithm takes a time of order exp $[(cN \log N)^{1/2}]$, with c = constant.
- GI is certainly in NP but is thought to be not NP-complete. It therefore occupies a somewhat unusual intermediate position (NP-intermediate?) among the unsolved problems in classical complexity theory, as does factoring.

Why investigate quantum algorithms for graph isomorphism (GI)?

- GI has similarities to factoring, so success of Shor's quantum algorithm for factoring has motivated investigations of quantum algorithms for GI.
- Quantum approaches using "hidden subgroup" approach do not appear promising.

  S. Hallgren, C. Moore, M. Rötteler, A. Russell, and P. Sen, in *Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC'06)*, 604–617 (2006).

  C. Moore, A. Russell, L.J. Schulman, quant–ph/0501056.
- Here, we investigate whether the ability of QCs to efficiently simulate quantum systems can be exploited for attacking GI.

Single-particle versus multi-particle quantum random walks

- Many useful (classical) algorithms are based on Markov chains (classical random walks)
- Single-particle quantum random walks are useful algorithmically (searching hypercube, element distinctness)

  (see A. Ambainis, quant-ph/0403120)

- Our work: multi-particle quantum walks (MPQWs) may be more powerful than single-particle quantum walks for the graph isomorphism problem.

‘Quantum walk’ algorithms for graph isomorphism

- One-particle quantum random walk on the graph
- Two-particle quantum random walk on the graph, with the particles being either non-interacting or hard-core bosons.

[related to T. Rudolph, quant-ph/0206068].

Quantum Random Walk on a Graph

The Hamiltonian is

$$H = -\sum_i A_{ij} c_i^+ c_j + U \sum_i \left(c_i^+ c_i\right)\left(c_i^+ c_i - 1\right),$$

where $A_{ij} = 1$, if i and j are connected by an edge, and 0 otherwise. (A is the *adjacency matrix* of the graph.)

The c_i^+ and c_i are operators that create and annihilate a boson at site i:

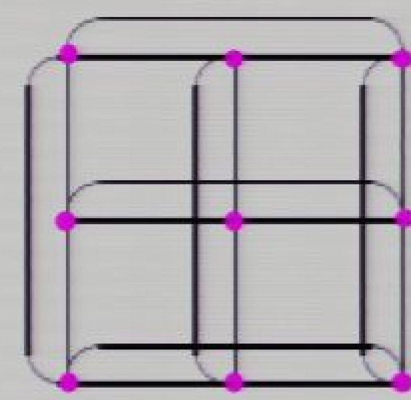
$$c_i c_j^+ - c_j c_i^+ = \delta_{ij}$$

$U = 0$ for the noninteracting particles,

$U \to \infty$ for the hard-core bosons.

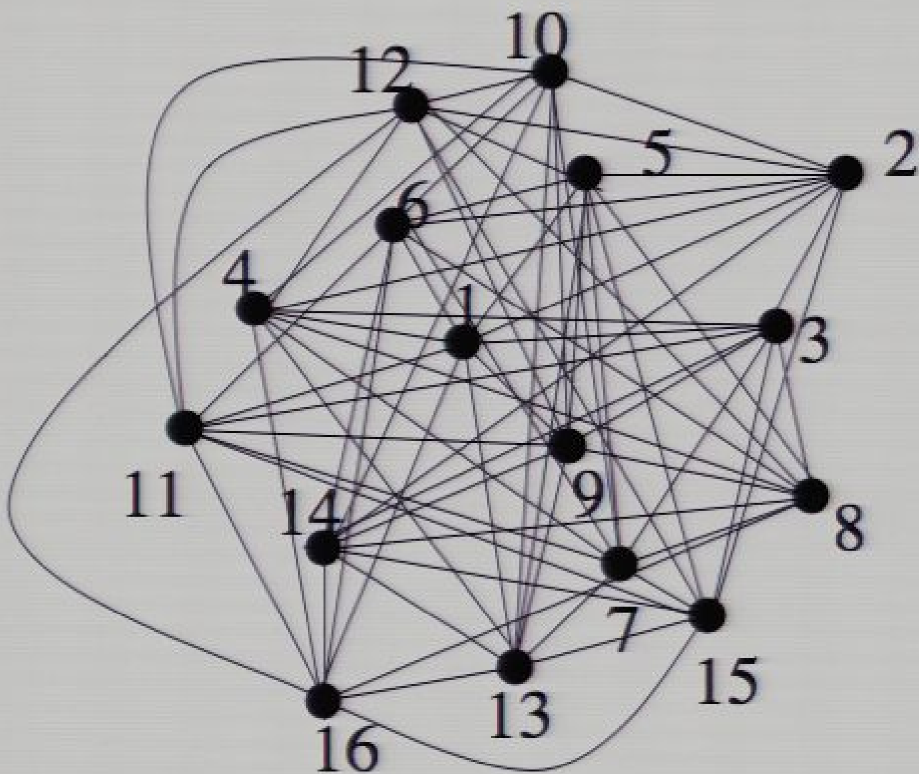
Strongly Regular Graphs (SRGs)

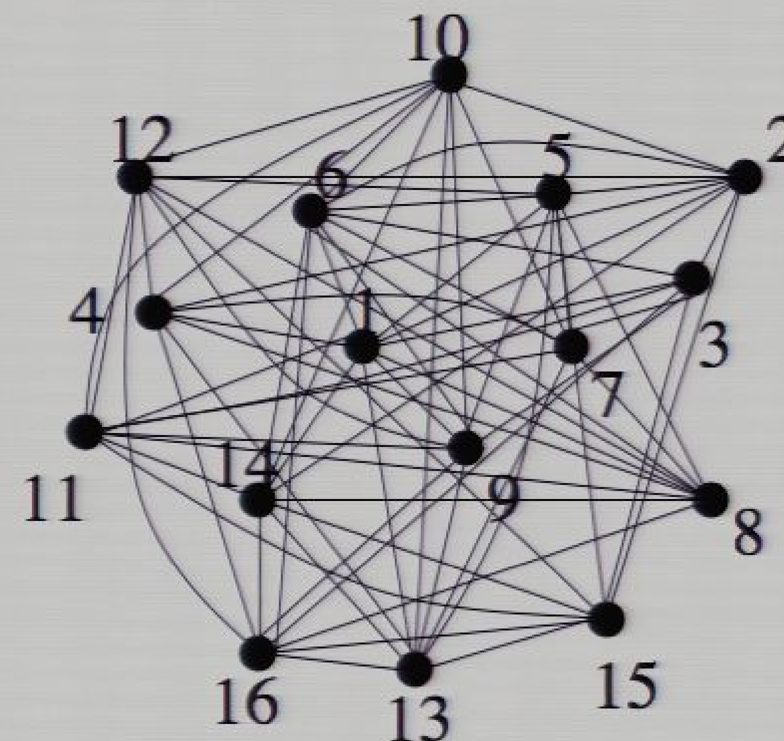
- A SRG with parameters (N, k, λ, μ) is a graph with N vertices in which each vertex has k neighbors, each pair of adjacent vertices has λ neighbors in common, and each pair of non-adjacent vertices has μ neighbors in common.
- The one at right has $N = 9$, $k = 4$, $\lambda = 1$, $\mu = 2$.
- Non-isomorphic pairs of SRGs with the same parameter sets are known to be very difficult to distinguish: many simple algorithms fail – so they are useful for testing proposed algorithms.



Two non-isomorphic strongly regular graphs

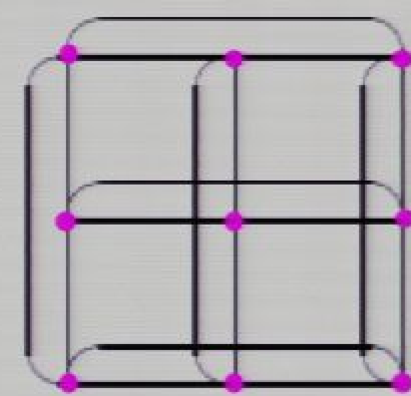
(16,9,4,6) – the smallest known such pair.





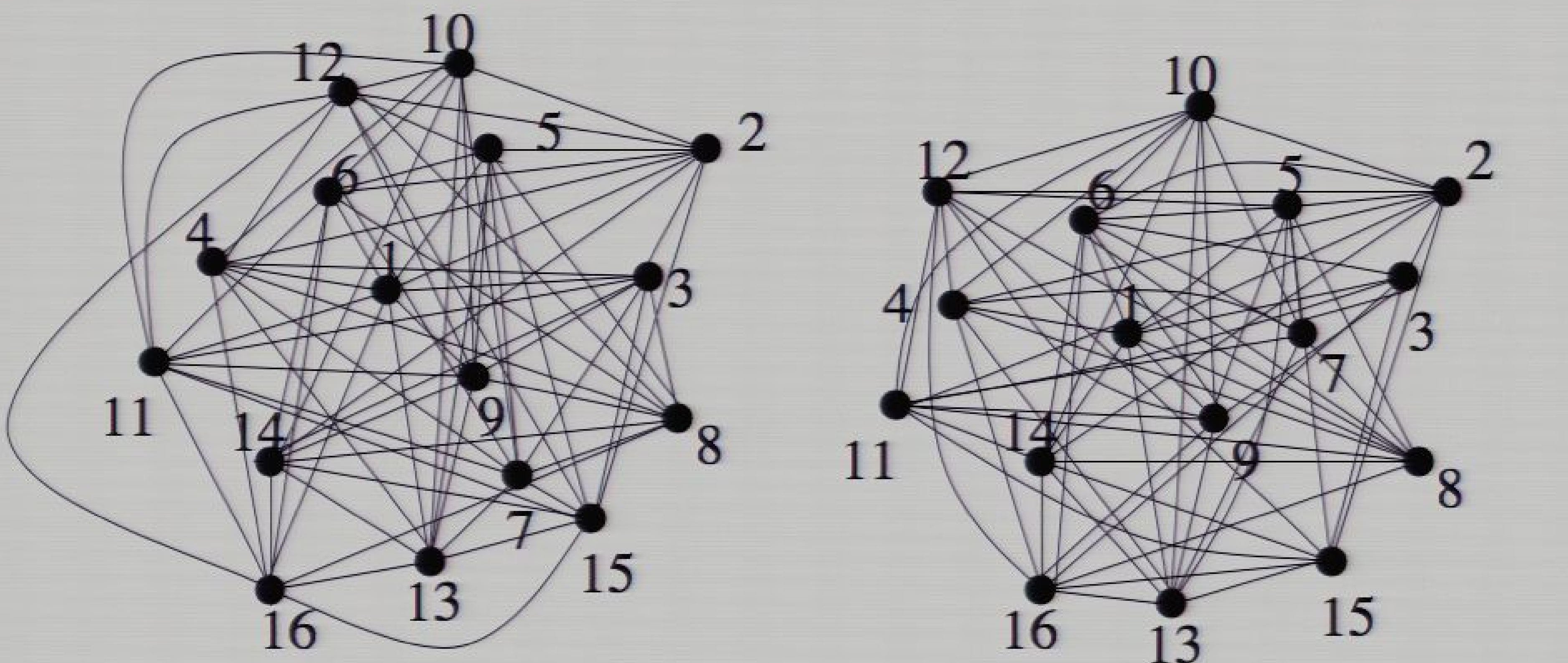
Strongly Regular Graphs (SRGs)

- A SRG with parameters (N, k, λ, μ) is a graph with N vertices in which each vertex has k neighbors, each pair of adjacent vertices has λ neighbors in common, and each pair of non-adjacent vertices has μ neighbors in common.
- The one at right has N = 9, k = 4, λ = 1, μ= 2.
- Non-isomorphic pairs of SRGs with the same parameter sets are known to be very difficult to distinguish: many simple algorithms fail – so they are useful for testing proposed algorithms.



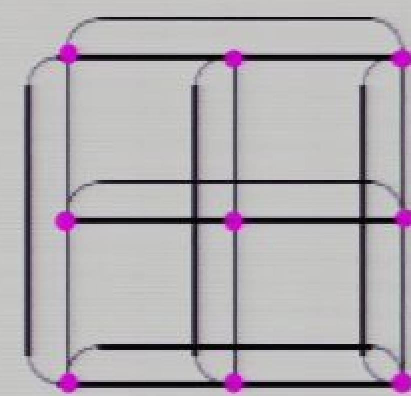
Two non-isomorphic strongly regular graphs

(16,9,4,6) – the smallest known such pair.



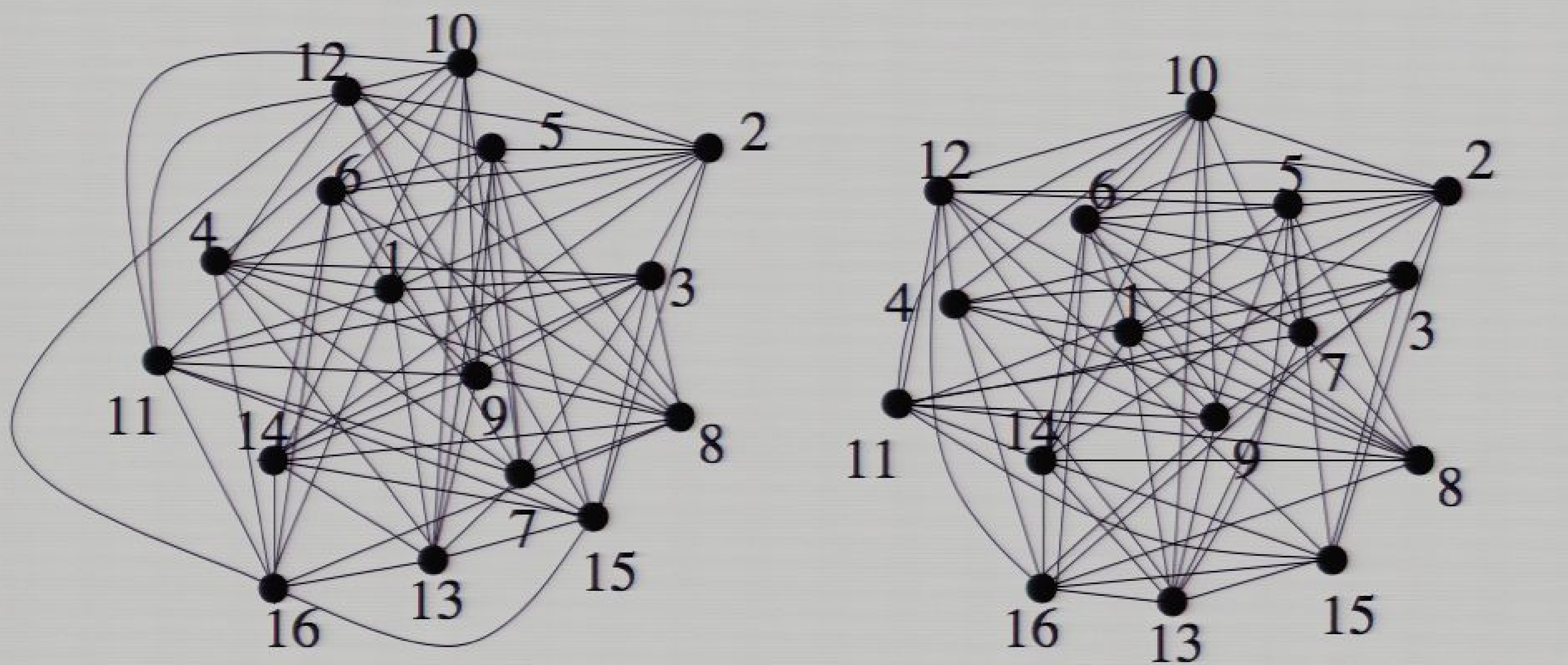
Strongly Regular Graphs (SRGs)

- A SRG with parameters (N, k, λ, μ) is a graph with N vertices in which each vertex has k neighbors, each pair of adjacent vertices has λ neighbors in common, and each pair of non-adjacent vertices has μ neighbors in common.
- The one at right has $N = 9$, $k = 4$, $\lambda = 1$, $\mu = 2$.
- Non-isomorphic pairs of SRGs with the same parameter sets are known to be very difficult to distinguish: many simple algorithms fail – so they are useful for testing proposed algorithms.



Two non-isomorphic strongly regular graphs

(16,9,4,6) – the smallest known such pair.



Numerical test of the quantum walks

Compute

$$O_{i,j} = \langle i | \exp(iHt) | j \rangle$$

One-particle
Green's function
(doesn't work!)

$$O_{ij,kl} = \langle ij | \exp(iHt) | kl \rangle$$

Two-particle
Green's function

$$R(T) = \sum_{i,j} \left| \mathrm{Re}\,\tilde{O}_{ij}(T) - \mathrm{Re}\,\tilde{O}'_{ij}(T) \right|$$

$$I(T) = \sum_{i,j} \left| \mathrm{Im}\,\tilde{O}_{ij}(T) - \mathrm{Im}\,\tilde{O}'_{ij}(T) \right|$$

tilde ⇒ amplitudes are sorted

R and I are the distances between the *sorted* amplitudes for two-non-isomorphic SRG's

(Similar procedure for the two-particle case)

Single-particle amplitudes don't work!

Can prove this using the algebraic properties of adjacency matrices of strongly regular graphs.

The adjacency matrix of a SRG has the following properties:

- For a general graph, the (a, b) entry of A^2 is the number of vertices adjacent to both a and b. For SRGs, this number is $(A^2)_{ab} = k$ if $a = b$, $(A^2)_{ab} = \lambda$ if a is adjacent to b, and $(A^2)_{ab} = \mu$ if a is not adjacent to b.
- Hence $A^2 = kI + \lambda A + \mu(J - I - A)$, where I is the identity matrix and J is the matrix consisting entirely of 1's.
- $J^2 = NJ$
- A and J also have the properties that $AJ = JA = kJ$.
  - ➢ The matrices, A, I, and J form a closed algebra.

$$\Rightarrow \exp(iA) = aI + bJ + cA,$$

where a, b, and c depend only on N, k, λ, and μ

Single-particle amplitudes don't work! (2

$A^2 = kI + \lambda A + \mu(J - I - A)$, where I is the identity matrix and J is the matrix consisting entirely of 1's.

$$\Rightarrow \exp(iA) = aI + bJ + cA,$$

where a, b, and c depend only on N, k, λ, and μ

Since the vertices of the two graphs all have the same degree, the adjacency matrices for the different graphs have the same number of 1's. So the numerical values of all the matrix elements of $\exp(iAt)$ must be identical for graphs with the same N, k, λ, and μ.

The matrices A, I, and J form a closed algebra whose properties depend only on the set (N, k, λ, μ), and the dynamical process can be mapped into an orbit in this algebra. Non-isomorphic SRGs with the same parameters follow the same orbit and this implies *that the sorted walk amplitudes are the same.*

Quantum walks of two interacting particles can distinguish strongly regular graphs.

graph specification	noninteracting bosons	hard core bosons
(16,9,4,6)	R=0 I=0	R=110.66 I=886.05
(25,12,5,6)	R=0 I=0	R=129.66 I=2160.86
(26,10,3,4)	R=0 I=0	R=14.88 I=896.75
(28,12,6,4)	R=0 I=0	R=87.27 I=1384.86
(29,14,6,7)	R=0 I=0	R=28.69 I=2672.23
(35,18,9,9)	R=0 I=0	R=300.63 I=3970.15

$R = \Sigma\, |\mathrm{Re}\, O_{ij} - \mathrm{Re}\, O_{ij}'|$ and $I = \Sigma\, |\mathrm{Im}\, O_{ij} - \mathrm{Im}\, O_{ij}'|$

R = I = 0 means that the algorithm has failed!

Algorithm works for hard-core but not noninteracting bosons.

Single-particle amplitudes don't work! (2

$A^2 = kI + \lambda A + \mu(J - I - A)$, where I is the identity matrix and J is the matrix consisting entirely of 1's.

$$\Rightarrow \exp(iA) = aI + bJ + cA,$$

where a, b, and c depend only on N, k, λ, and μ

Since the vertices of the two graphs all have the same degree, the adjacency matrices for the different graphs have the same number of 1's. So the numerical values of all the matrix elements of $\exp(iAt)$ must be identical for graphs with the same N, k, λ, and μ.

The matrices A, I, and J form a closed algebra whose properties depend only on the set (N, k, λ, μ), and the dynamical process can be mapped into an orbit in this algebra. Non-isomorphic SRGs with the same parameters follow the same orbit and this implies *that the sorted walk amplitudes are the same.*

Single-particle amplitudes don't work!

Can prove this using the algebraic properties of adjacency matrices of strongly regular graphs.

The adjacency matrix of a SRG has the following properties:

- For a general graph, the (a, b) entry of A^2 is the number of vertices adjacent to both a and b. For SRGs, this number is $(A^2)_{ab} = k$ if $a = b$, $(A^2)_{ab} = \lambda$ if a is adjacent to b, and $(A^2)_{ab} = \mu$ if a is not adjacent to b.
- Hence $A^2 = kI + \lambda A + \mu(J - I - A)$, where I is the identity matrix and J is the matrix consisting entirely of 1's.
- $J^2 = NJ$
- A and J also have the properties that $AJ = JA = kJ$.
  - ➢ The matrices, A, I, and J form a closed algebra.

$$\Rightarrow \exp(iA) = aI + bJ + cA,$$

where a, b, and c depend only on N, k, λ, and μ

Single-particle amplitudes don't work! (2

$A^2 = kI + \lambda A + \mu(J - I - A)$, where I is the identity matrix and J is the matrix consisting entirely of 1's.

$$\Rightarrow \exp(iA) = aI + bJ + cA,$$

where a, b, and c depend only on N, k, λ, and μ

Since the vertices of the two graphs all have the same degree, the adjacency matrices for the different graphs have the same number of 1's. So the numerical values of all the matrix elements of $\exp(iAt)$ must be identical for graphs with the same N, k, λ, and μ.

The matrices A, I, and J form a closed algebra whose properties depend only on the set (N, k, λ, μ), and the dynamical process can be mapped into an orbit in this algebra. Non-isomorphic SRGs with the same parameters follow the same orbit and this implies *that the sorted walk amplitudes are the same.*

Quantum walks of two interacting particles can distinguish strongly regular graphs.

graph specification	noninteracting bosons	hard core bosons
(16,9,4,6)	R=0 I=0	R=110.66 I=886.05
(25,12,5,6)	R=0 I=0	R=129.66 I=2160.86
(26,10,3,4)	R=0 I=0	R=14.88 I=896.75
(28,12,6,4)	R=0 I=0	R=87.27 I=1384.86
(29,14,6,7)	R=0 I=0	R=28.69 I=2672.23
(35,18,9,9)	R=0 I=0	R=300.63 I=3970.15

$R = \Sigma\, |\mathrm{Re}\, O_{ij} - \mathrm{Re}\, O_{ij}'|$ and $I = \Sigma\, |\mathrm{Im}\, O_{ij} - \mathrm{Im}\, O_{ij}'|$

R = I = 0 means that the algorithm has failed!

Algorithm works for hard-core but not noninteracting bosons.

Numerical results

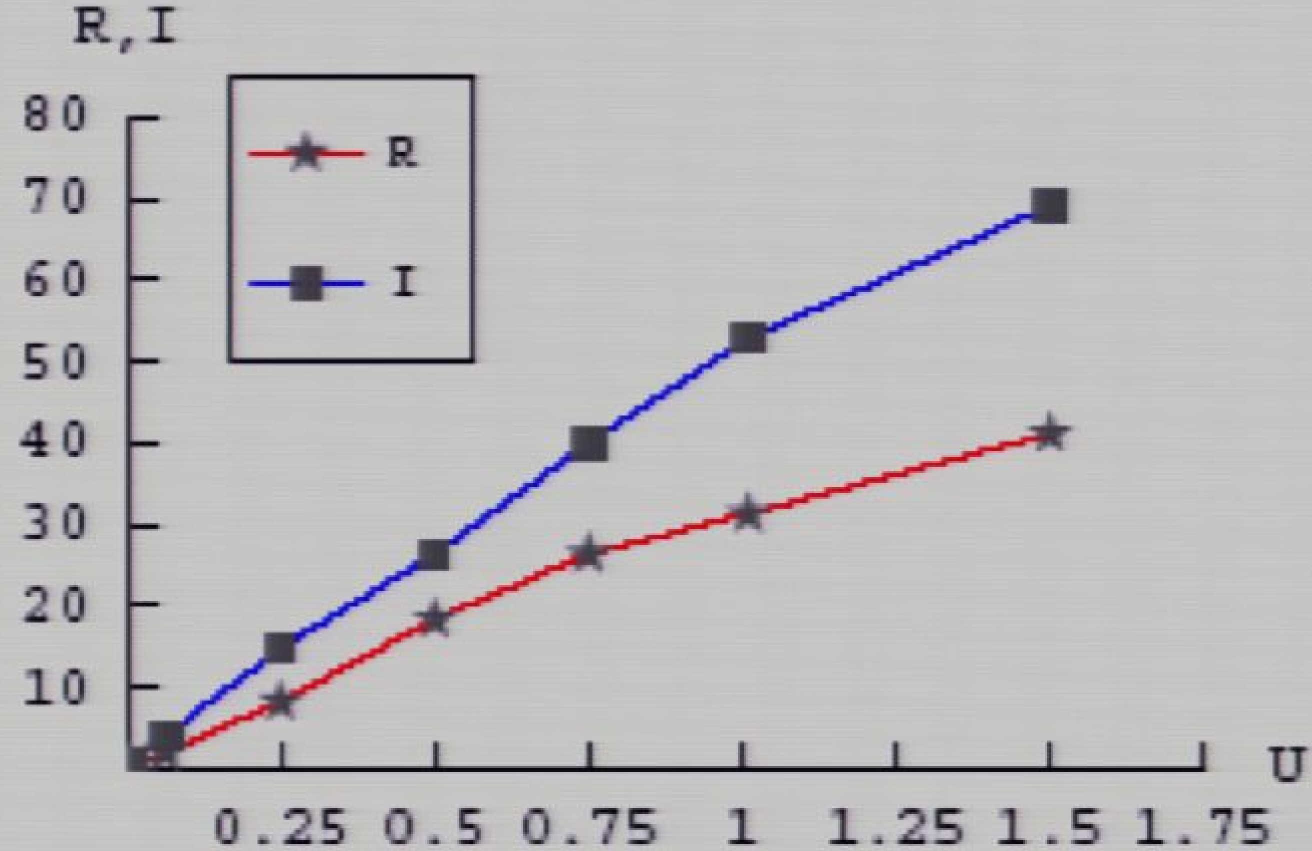
- Algorithm with two hard-core bosons successfully distinguishes all nonisomorphic pairs of strongly regular graphs that we tested (including all pairs of the ~32,000 nonisomorphic graphs with 36 vertices).

Noninteracting bosons and noninteracting fermions do not distinguish nonisomorphic pairs of strongly regular graphs.

- We have proven that noninteracting fermions fail to distinguish non-isomorphic SRGs with the same parameters (using method similar method to that for single particles, but messier).

- We have found numerically that noninteracting bosons fail to distinguish non-isomorphic SRGs with the same parameters. We are still working to try to prove that they fail.

Soft-core bosons work, too

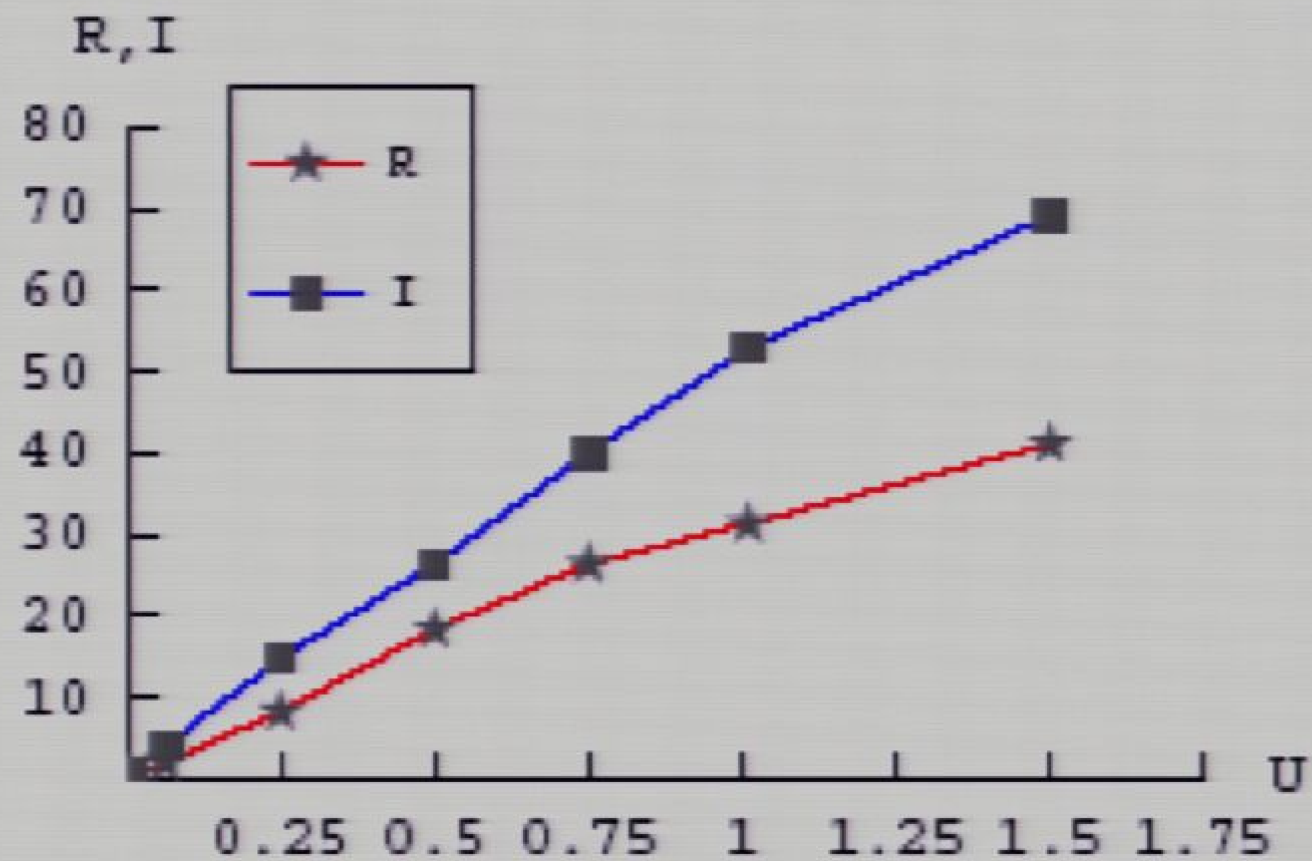


R and I for the two non-isomorphic SRGs with N = 16.

Noninteracting bosons and noninteracting fermions do not distinguish nonisomorphic pairs of strongly regular graphs.

- We have proven that noninteracting fermions fail to distinguish non-isomorphic SRGs with the same parameters (using method similar method to that for single particles, but messier).
- We have found numerically that noninteracting bosons fail to distinguish non-isomorphic SRGs with the same parameters. We are still working to try to prove that they fail.

Soft-core bosons work, too



R and I for the two non-isomorphic SRGs with N = 16.

Can quantum walks with two interacting bosons distinguish all pairs of nonisomorphic graphs?

- If yes, then GI is in P

  (two-particle quantum walk can be implemented on classical computer in polynomial time)

- We conjecture no – will investigate using numerics as well as with algebraic approach (can now investigate all pairs of strongly regular graphs with up to 64 vertices)

Algebraic Approach for Finding Limitations of Two-Particle Quantum Walks: Distinguishing Operators

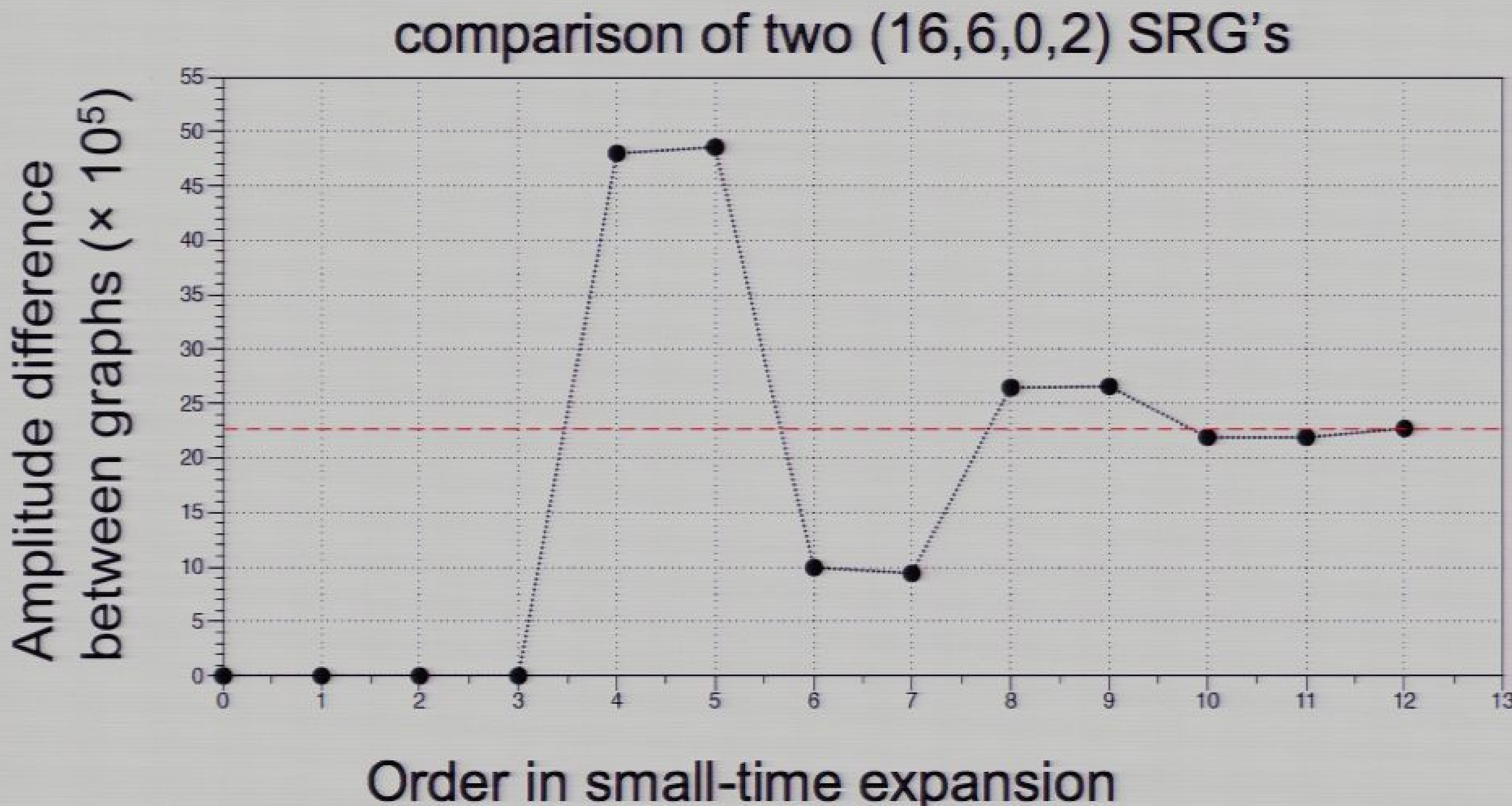
- The adjacency matrix A for an SRG has only three distinct eigenvalues, implying that A satisfies a cubic equation:

  $$(A-\lambda_1 I)\,(A-\lambda_2 I)\,(A-\lambda_3 I)=0,$$

  so that $\exp(iHt) = aA^2+bA+c$ for some a,b,c.

  Generalizing this, we find that noninteracting bosons have 6 independent operators, while interacting bosons have 16, acting in the two-particle space.
- Only a small subset of the operators actually distinguish between graphs, in the sense that their matrix representations can be distinguished in polynomial time by our procedures.
- We are now focusing on the construction and diagnosis of two-particle operators.

Short-time expansion: distinguishing power arises in 4th order of expansion:



A “more likely” conjecture:

- N/2 interacting bosons can distinguish nonisomorphic graphs

  ➔ Hilbert space is exponentially large, but can be explored with polynomially many qubits

    - But need to develop specific algorithm
      - current technique is exponentially large for $\theta(N)$ particles, both because of the size of the Hilbert space and because of number of possible initial conditions

Summary

- Quantum random walks with interacting particles have computational power that single-particle walks do not have (at least for distinguishing non-isomorphic strongly regular graphs).
- Understanding the computational power of interacting quantum random walks may yield new insight into how to distinguish non-isomorphic graphs.

Quantum random walks of interacting particles and the graph isomorphism problem

Susan N. Coppersmith
University of Wisconsin, Madison

collaborators: Mark Friesen, John Gamble, Robert Joynt, Shiue-Yuan Shiau

S.-Y. Shiau et al., Quantum Information and Computation 5, 492-506 (2005)
(+ unpublished work)