The Abdus Salam
International Centre for Theoretical Physics

United Nations
Educational, Scientific and
Cultural Organization

IAEA
International Atomic Energy Agency

2254-8

Workshop on Sphere Packing and Amorphous Materials

25 - 29 July 2011

Quantum Random Walks of Interacting Particles and the Graph Isomorphism Problem

Susan N. COPPERSMITH

University of Wisconsin, Madison, 1150 University Avenue
Madison, WI 53706
U.S.A.

Quantum random walks of interacting particles and the graph isomorphism problem

Susan N. Coppersmith
University of Wisconsin, Madison

collaborators: Eric Bach, Mark Friesen, John Gamble, Robert Joynt, Mark Wellons, Kenneth Rudinger, Shiue-Yuan Shiau, Dong Zhou

S.-Y. Shiau et al., Quantum Information and Computation 5, 492-506 (2005)
J. Gamble et al., Phys. Rev. A **81**, 052313 (2010), arxiv 1002.3003
K. Rudinger, et al., in preparation

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.

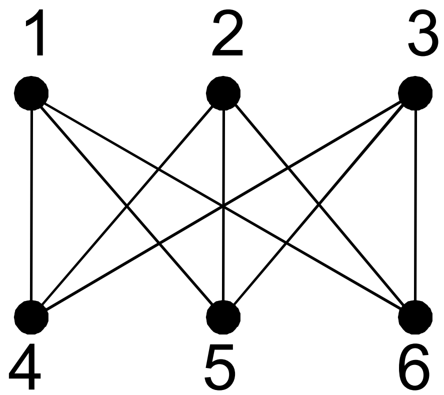
Outline

- The graph isomorphism problem
  - What is it?
  - Why are people interested? (Detour into complexity theory)
  - Why are physicists interested? (Detour into quantum computing)
  - What good can we do?
- Single-particle walks
  - Tantalizing successes
  - Instructive iailures
- Multi-particle walks
  - Even more tantalizing successes
  - Possibly instructive failures
- Status and outlook

The graph isomorphism problem

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

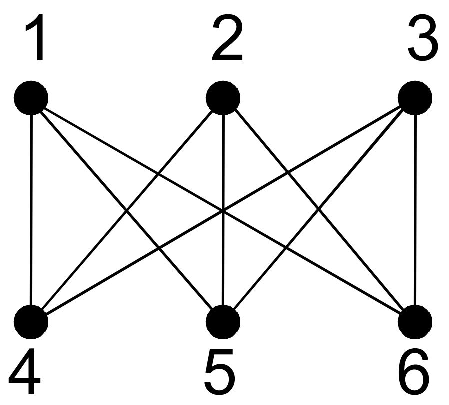
G



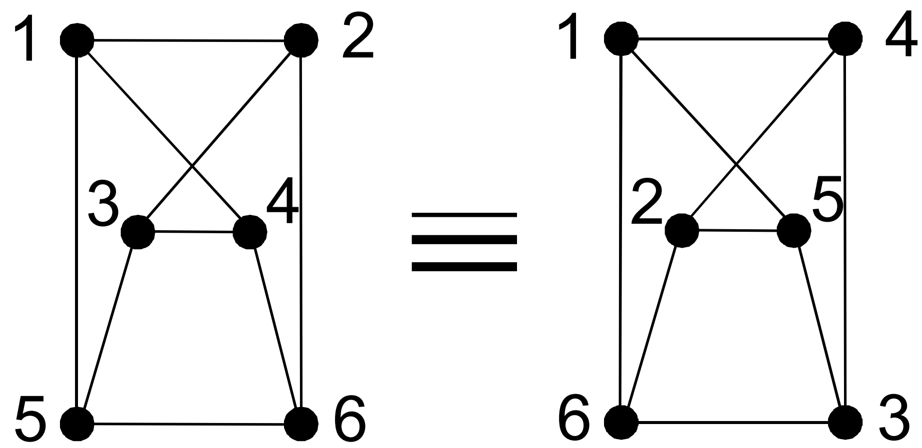
edges between 1 and 4, 1 and 5, 1 and 6, etc.

Graph isomorphism (GI)

G



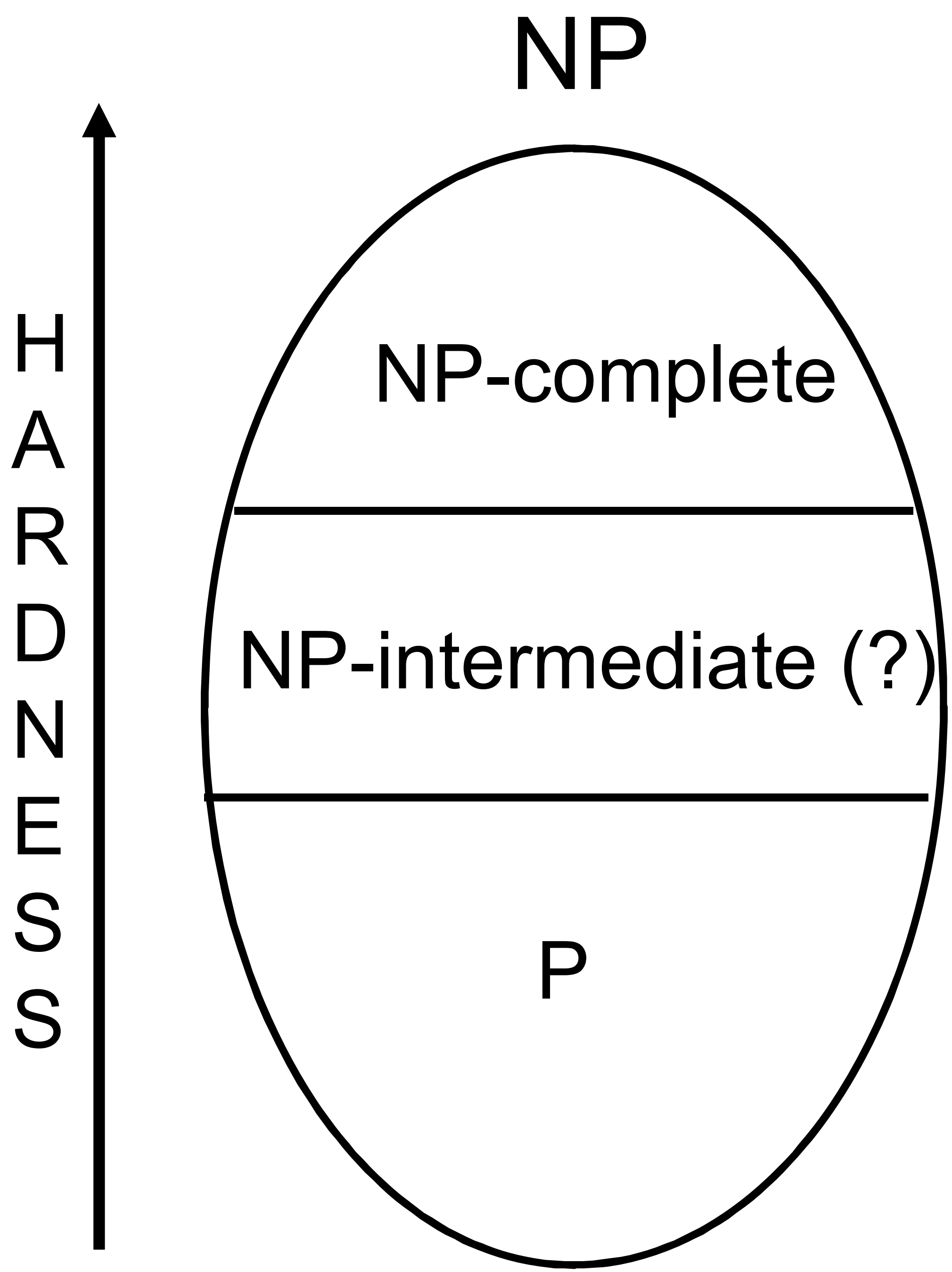
G′



G' goes into G if we relabel the vertices of G' by:
1→ 1, 2 → 4, 3 → 2, 4 → 5, 5 → 6, 6 → 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.



- NP problems have solutions that can be checked in polynomial time.
- If an NP-complete problem has an efficient solution method, you could solve all the other NP problems efficiently.
- P problems have solutions that can be found in polynomial time.
- NP-intermediate problems (if there are any) are neither P nor NP-complete.

Computational Complexity of GI is Similar to Factoring!

- Naively, GI is difficult (i.e., not in P) – 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.

- Suggests we should look for a quantum algorithm to solve GI

- Our approach is to simulate quantum systems to see if the results can distinguish graphs

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 quantum computers to efficiently simulate quantum systems can be exploited for attacking GI.

Our Approach: Quantum Random Walks on Graphs

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,
$U \rightarrow \infty$ for hard-core bosons.

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.

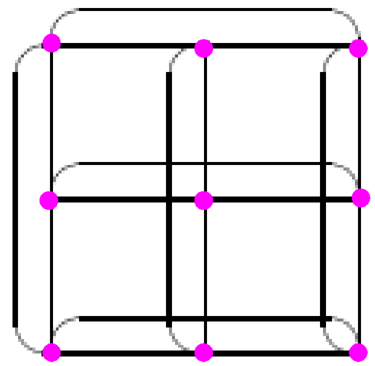
‘Quantum walk’ algorithms for graph isomorphism

- 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.
- Three-particle quantum random walks of both Fermions or Bosons (both non-interacting and hard-core).

[previous work: T. Rudolph, quant-ph/0206068, S.-Y. Shiau et al., Quantum Information and Computation **5**, 492-506 (2005)].

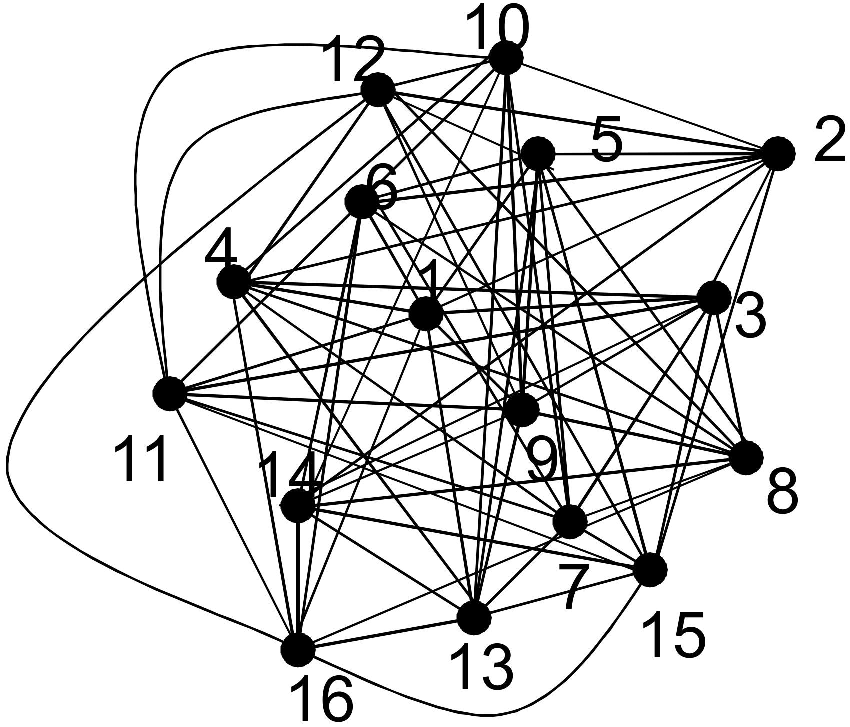
Strongly Regular Graphs (SRGs)

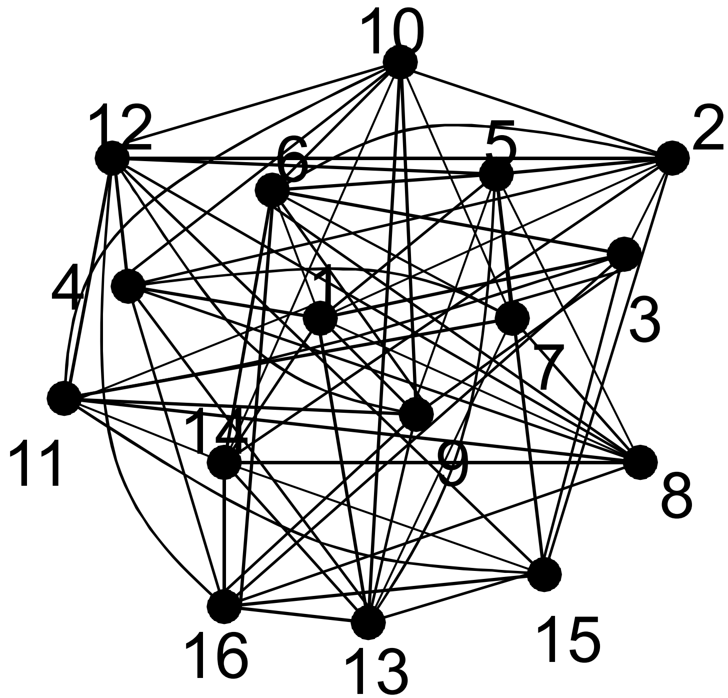
- A SRG with family parameters (N, k, λ, μ) is a graph with N vertices in which each vertex has k neighbors, each pair of adjacent vertices has λ neighbors in common, and each pair of non-adjacent vertices has μ neighbors in common.
- The one at right has N = 9, k = 4, λ = 1, μ= 2.
- Non-isomorphic pairs 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.





Numerical test of the quantum walks

One-particle case:

Compute

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

One-particle Green's function

Amplitude that particle starting at vertex j at time 0 is at vertex i at time t.

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

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

tilde (amplitudes are sorted

R and I are "distances" between 2 graphs.

0 if the graphs are isomorphic

???? Are they nonzero if the graphs are not isomorphic ????

Numerical test of the quantum walks

Two-particle case:

Compute

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

Two-particle Green's function

Amplitude that particles starting at vertices i and j at time 0 are at vertices k and l at time t.

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

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

tilde ⎝ amplitudes are sorted

R and I are "distances" between 2 graphs.

0 if the graphs are isomorphic

???? Are they nonzero if the graphs are not isomorphic ????

(Similar procedure for more particles)

One-particle walks don't work!

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

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:
    $A^2 = kI + \lambda A + \mu(J - I - A)$.

.

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

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

One-particle walks don't work! (2)

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

where a, b, and c depend only on N, k, λ, and μ,
I is the identity matrix and J is the matrix consisting entirely of 1's.

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 family 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.

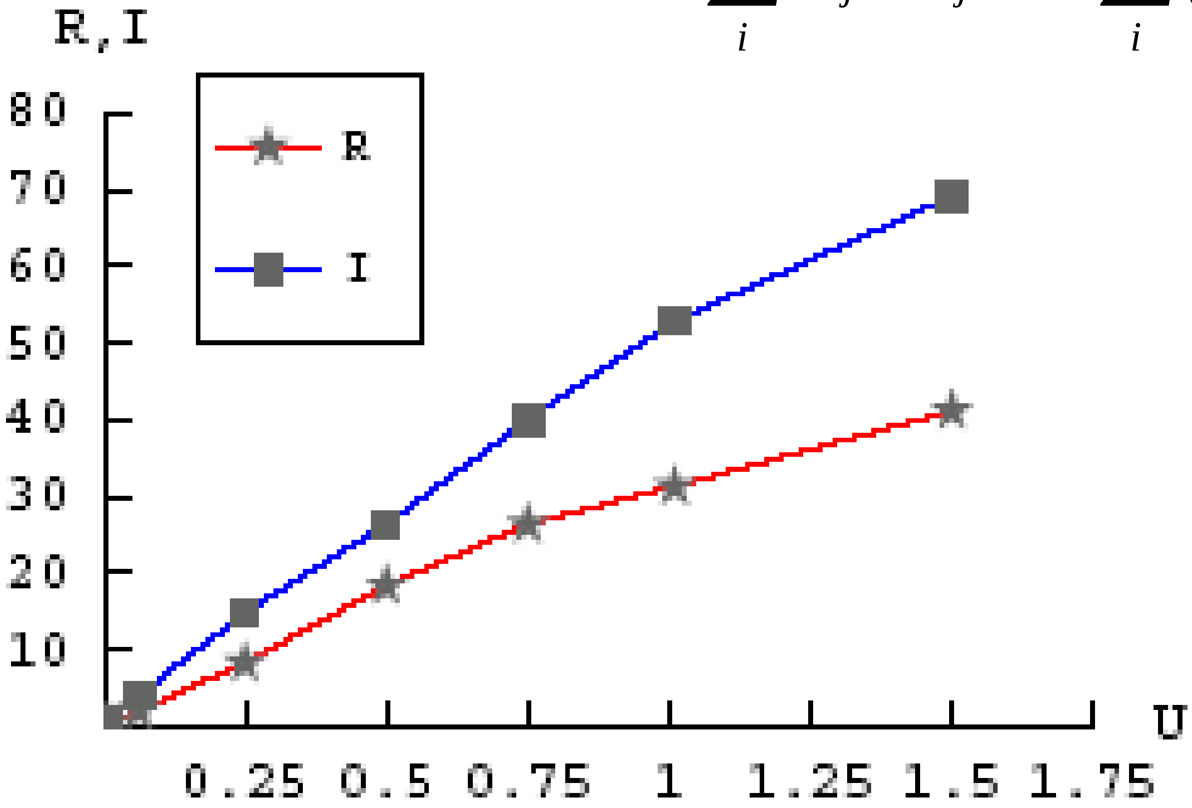
More results for two-particle quantum walks on strongly regular graphs (SRGs)

1) Quantum walks of two noninteracting particles (Bosons or Fermions) do not distinguish SRGs from the same family (analytic proof)

2) Quantum walks of two hard-core Bosons distinguish all nonisomorphic SRGs with up to 64 vertices. This required serious computing: For example, for the (36,15,6,6) family, one needs to perform 529,669,878 comparisons to check all pairs. (Thanks to the Center for High-Throughput Computing at UW-Madison.)

Soft-core bosons work, too

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



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

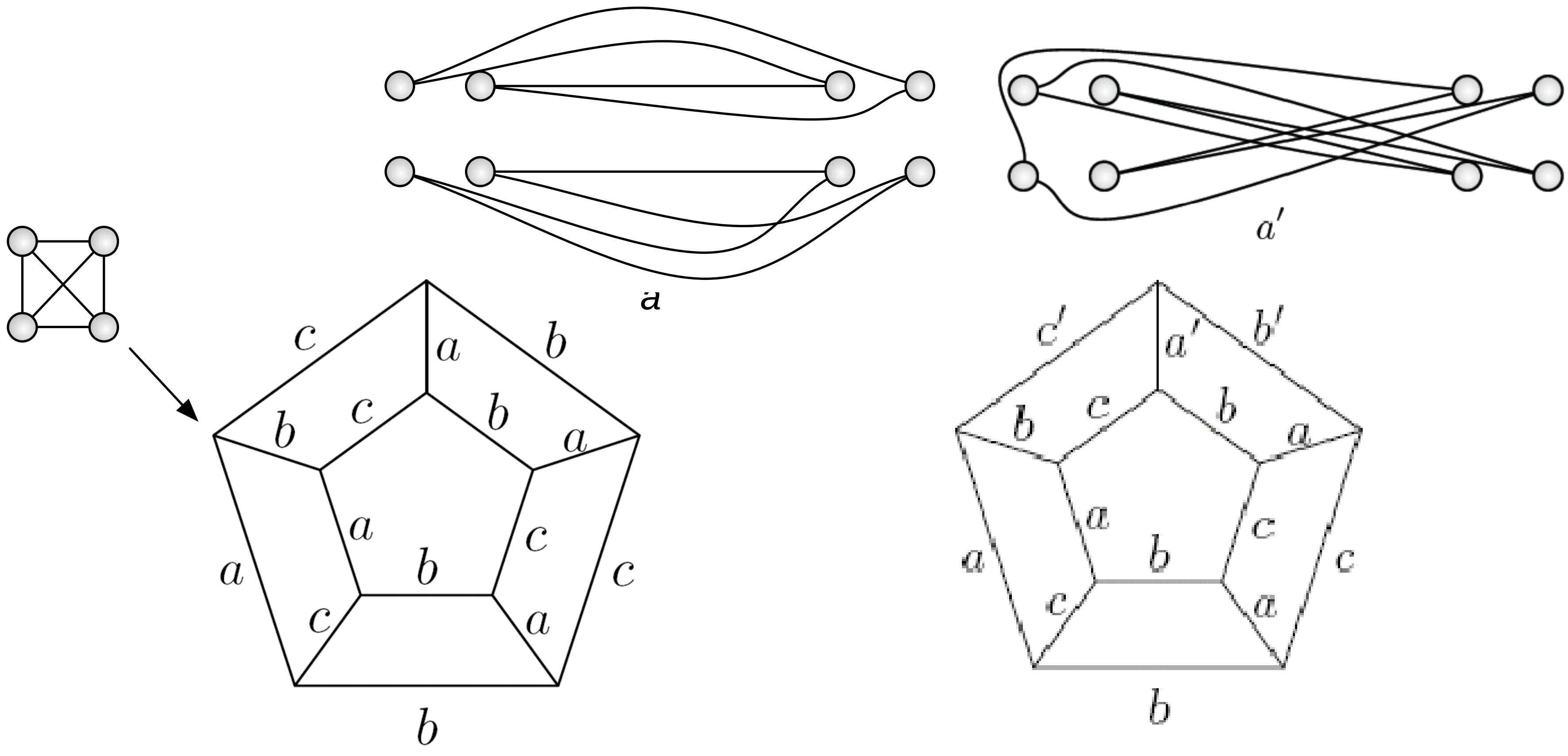
QRWs with two hard-core Bosons distinguish all pairs of nonisomorphic SRGS that we tested.

But they do not distinguish all pairs of nonisomorphic graphs.

- “Counterexample” pairs that we have identified have a number of vertices that scales as square of the number of Bosons (so efficient quantum algorithm is not ruled out).

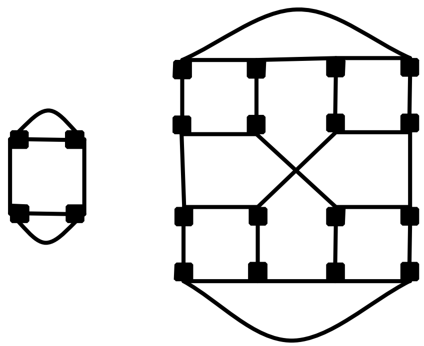
Hard core bosons fail to distinguish some pairs of nonisomorphic graphs

Ponomarenko construction: 4 orbitals per site
G and G' are not isomorphic but have zero 'distance'
[A. R. Barghi and I. Ponomarenko, The Electronic Journal of Combinatorics **16** (2009), J. Smith, arxiv:1004.0206]

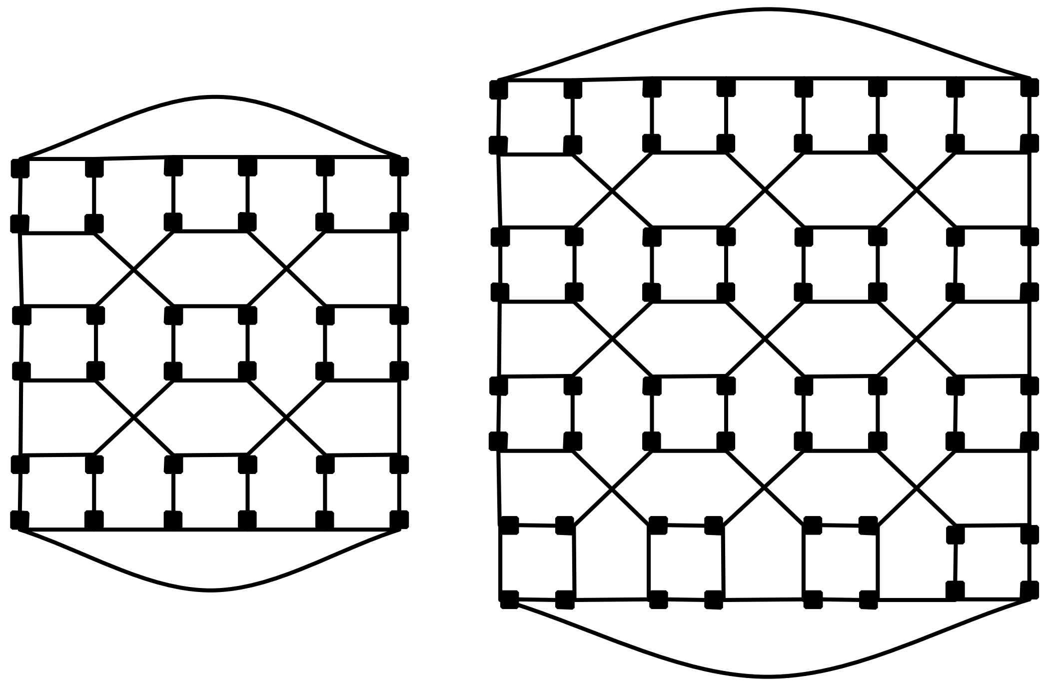


G   G'

“Counterexample” pairs have number of vertices that scales as square of the number of Bosons



2-particle
counterexample graph



3-particle
counterexample graph

Possible conjectures

- Two interacting bosons can distinguish nonisomorphic graphs
  - ➔ GI is in P
- 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 algorithm (current technique is exponentially large for O(N) particles)

Possible conjectures

- ~~Two interacting bosons can distinguish nonisomorphic graphs~~
  - ~~➔ GI is in P~~

progress!

- 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 algorithm (current technique is exponentially large for O(N) particles)

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.

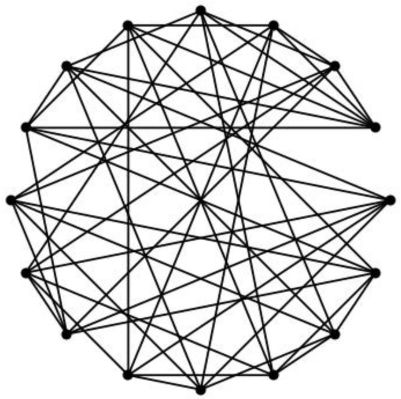
  Generalizing this, we find that noninteracting bosons have 6 independent operators, while interacting bosons have 16, acting in the two-particle space of the SRG.
- Only a small subset of the operators actually distinguish between graphs, in the sense that their matrix representations can be distinguished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

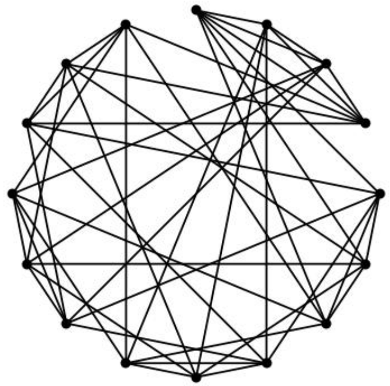
Quantum walks with more particles

- Adding more particles increases distinguishing power of quantum walks of hard core Bosons on counterexample graphs.
- Quantum walks of 3 or more noninteracting particles (both Fermions and Bosons) can distinguish some (but not all) nonisomorphic pairs of SRGs from the same family.

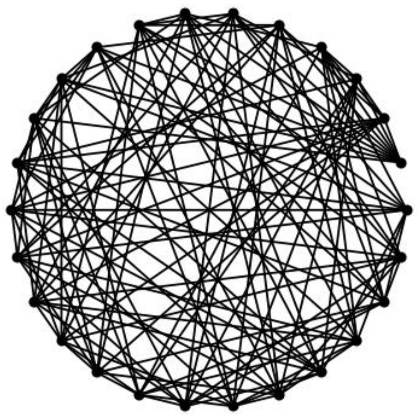
Three noninteracting Bosons distinguish some but not all pairs of nonisomorphic SRGs from the same family

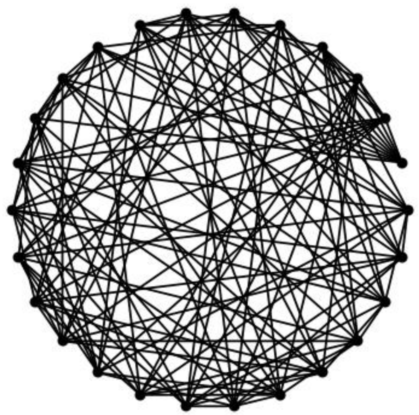
- These two graphs, in the SRG family (16,6,2,2), are distinguished by walks of three noninteracting Bosons





- These two graphs, in the SRG family (26,10,3,4), are NOT distinguished by walks of three noninteracting Bosons

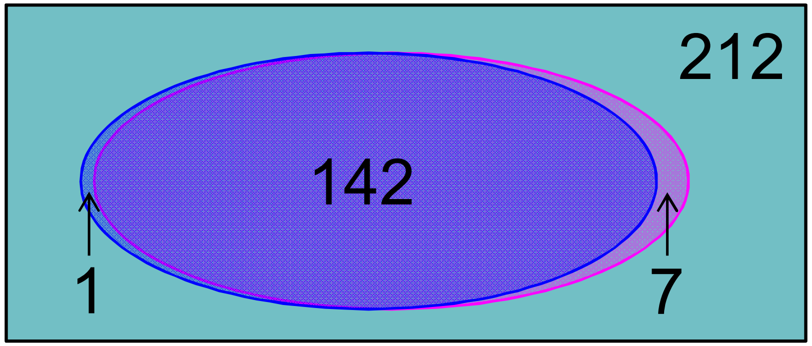




Noninteracting Fermions behave similarly.

Analytic studies of evolution matrix U_{3B} for 3 noninteracting Bosons

- All U_{3B} element values can be calculated analytically for any SRG.
- The maximum number of distinct U_{3B} element values for a given SRG is 212. (For 2 noninteracting bosons, this number was 22.)
- Graphs are distinguished when multiplicities of values are different (some multiplicities are zero).



We have been able to obtain bounds on the multiplicities that imply that a fixed number of noninteracting Bosons cannot distinguish all nonisomorphic pairs of SRGs.

The upshot: possible conjectures consistent with results known so far

- Conjecture #1: Quantum walks with two interacting bosons can distinguish *all* pairs of non-isomorphic strongly regular graphs.

- Conjecture #2: Quantum walks on N sites with O(N) interacting bosons can distinguish *all* pairs of non-isomorphic graphs.
  - If yes, the GI *may* be in QP
  - Still need to develop efficient protocol that requires polynomially large number of initializations and measurements.

Summary

- Quantum random walks with multiple particles have computational power that single-particle walks do not have (at least for distinguishing non-isomorphic strongly regular graphs).
- Quantum walks of interacting particles have more computational power than those of noninteracting particles.
- Understanding the computational power of interacting quantum random walks may yield new insight into how to distinguish non-isomorphic graphs.
- Via algebraic characterization of the evolutions, this may lead back to deeper understanding of many-body systems