Quantum Information and Computation, Vol. 5, No. 6 (2005) 492–506

PHYSICALLY-MOTIVATED DYNAMICAL ALGORITHMS FOR THE GRAPH ISOMORPHISM PROBLEM

SHIUE-YUAN SHIAU ROBERT JOYNT S.N. COPPERSMITH
Department of Physics, University of Wisconsin, Madison, Wisconsin 53706, United States

Received November 1, 2004
Revised June 14, 2005

The graph isomorphism problem (GI) plays a central role in the theory of computational complexity and has importance in physics and chemistry as well [1, 2]. No polynomial-time algorithm for solving GI is known. We investigate classical and quantum physics-based polynomial-time algorithms for solving the graph isomorphism problem in which the graph structure is reflected in the behavior of a dynamical system. We show that a classical dynamical algorithm proposed by Gudkov and Nussinov [25] as well as its simplest quantum generalization fail to distinguish pairs of non-isomorphic strongly regular graphs. However, by combining the algorithm of Gudkov and Nussinov with a construction proposed by Rudolph [26] in which one examines a graph describing the dynamics of two particles on the original graph, we find an algorithm that successfully distinguishes all pairs of non-isomorphic strongly regular graphs that we tested with up to 29 vertices.

Keywords: Graph isomorphism, quantum computing
Communicated by: R Jozsa & J Watrous

1 Introduction

A graph is a set of N points, or vertices, and a set of edges, or unordered pairs of those points. If two graphs differ only in the labelling of their points, then we say they are isomorphic, otherwise they are non-isomorphic. The graph isomorphism 'meta-problem' is to determine whether or not there is an algorithm that runs in polynomial time ($t \sim N^x$, with x independent of N) that distinguishes non-isomorphic pairs with certainty. The problem of distinguishing distinct atomic clusters of size N, in which a cluster is defined by the bonds between its atoms, is the same problem in another guise [3].

Typical instances of graph isomorphism (GI) can be solved in polynomial time because two randomly chosen graphs with identical numbers of vertices and edges typically have different degree and eigenvalue distributions. Moreover, GI can be solved efficiently for restricted classes of graphs, such as trees [4], planar graphs [5], graphs with bounded degree [6, 7], bounded eigenvalue multiplicity [8], and bounded average genus [9]. However, no algorithm for solving GI for all graphs is presently known; the best existing upper bound is $\exp\sqrt{cN\log N}$ [10]. There is evidence that indicates that GI is not NP-complete: first, counting the number of isomorphisms is reducible to the decisional version of the problem [11], unlike what is believed to be the case for NP-complete problems, and second, if GI were NP-complete then certain complexity classes that are believed to be different would be identical [12, 13]. GI is in NP, so it is believed that either GI is in P or else it is in the class of problems that are

neither in P nor are NP-complete [14].

One way to solve GI is to solve the hidden subgroup problem for the permutation group. Unfortunately, though the hidden subgroup problem for abelian groups can be solved efficiently [15], no efficient algorithm for solving the hidden subgroup problem for the permutation group is known [16, 17]. Indeed, some recent results [18], [19] have given rise to pessimism that this is possible.

Recent results of Aaronson, while not ruling out a generic algorithm for finding a non-abelian hidden subgroup, do show that any efficient quantum algorithm for GI would have to exploit structural information about the problem [20].

In this paper we investigate classical and quantum approaches to solving the graph isomorphism problem that are motivated by physical processes [21]. Our work combines and extends ideas of Gudkov and Nussinov [25] and of Rudolph [26] for attacking the GI problem using algorithms based on physical intuition. We show that the interesting classical dynamical algorithm proposed by Gudkov and Nussinov fails to distinguish an infinite set of pairs of non-isomorphic graphs, and thus does not solve the GI problem in polynomial time. We trace this failure to certain algebraic properties of these particular pairs of graphs and show that the simplest quantum generalizations of the Gudkov and Nussinov algorithm also fails to distinguish these pairs of graphs. However, an algorithm obtained by combining the basic idea of the Gudkov and Nussinov algorithm with a construction proposed by Rudolph [26] does distinguish all pairs of graphs that we have examined, including many with the same eigenvalue spectra.

The detailed statement of the GI problem is that we are given two graphs, each with N vertices. The first has vertices $\{v_1, v_2, ...v_N\}$, together with a set of edges, or unordered pairs $\{e_1, e_2, ...\}$ connecting pairs of these vertices, while the second graph is a set of vertices $\{v'_1, v'_2, ...v'_N\}$, and a set of edges $\{e'_1, e'_2, ...\}$. Each e_i is associated with a pair $\{v_a, v_b\}$, and each e'_i is associated with a pair $\{v'_a, v'_b\}$. We wish to determine whether there exists a permutation $\mathcal{P}$ of the v_i such that the set of pairs $\{\mathcal{P}v_a, \mathcal{P}v_b\}$ is identical with the set of pairs $\{v'_a, v'_b\}$.

An equivalent but more useful formulation for our purposes is to represent each graph by its adjacency matrix A. A_{ab} is an $N \times N$ matrix such that $A_{ab} = 1$ if there is a pair $e = \{v_a, v_b\}$ and $A_{ab} = 0$ otherwise. Two graphs are isomorphic if and only if there exists a permutation matrix P such that $A' = PAP^{-1}$.

2 Dynamical Algorithms

2.1 Classical algorithm

In the Gudkov and Nussinov approach to this problem [25], each vertex of the graph is mapped into a point in an $N-$dimensional Hilbert space. These points move in time. The vertex v_1 sits initially at the point $\vec{r}_1 = (1, 0, 0, ..., 0)$, v_2 at $\vec{r}_2 = (0, 1, 0, ...0)$, and so on. These are the vertices of an $(N-1)-$dimensional simplex. We now view these as mass-points with forces acting pairwise among them. There is one force law if two particles are connected by an edge and a different force law if they are not. The forces are derived from potentials U_1 and U_2 that depend only on the distances between the points in the pair. From the initial

configuration, the particles move in time according to the relaxational equations of motion

$$\mu \frac{d\vec{r}_a(t)}{dt} = \vec{F}_a,$$

where

$$\vec{F}_a = -\nabla_{\vec{r}_a} U(\vec{r}_1, \vec{r}_2, ...)$$

and

$$U = \sum_{a>b} A_{ab} U_1(|\vec{r}_a - \vec{r}_b|) + \sum_{a>b} (1 - A_{ab}) U_2(|\vec{r}_a - \vec{r}_b|). \tag{1}$$

The motion may be computed by any convenient algorithm. After a time T the positions are given by $\vec{r}_a(T)$ for $a = 1, 2, ...N$. We now compute the set of $N(N-1)/2$ distances $d_{ab} = |\vec{r}_a(T) - \vec{r}_b(T)|$. Given a second graph, we compute $d'_{ab} = |\vec{r}'_a(T) - \vec{r}'_b(T)|$ using the same prescription. The sets $\{d_{ab}\}$ and $\{d'_{ab}\}$, being non-negative real numbers, may be arranged in increasing order.

This suggests the following conjecture.

Conjecture 1 (Gudkov and Nussinov [25]): If the ordered distance sets $\{d_{ab}\}$ and $\{d'_{ab}\}$ for the graphs G and G' are identical, then G and G' are isomorphic.

Note that as long as T itself is of polynomial size, this is a polynomial-time algorithm. In fact, in the algorithm as it stands, T is a constant. This would appear to be sufficient, since the time evolution is unitary, which means that no chaotic (exponential sensitivity to initial conditions) motion is possible. The sets d_{ab} and d'_{ab} can be computed, ordered, and compared efficiently. We now wish to examine the validity of Conjecture 1.

For purposes of clarity, we shall consider a slightly simpler model than the one defined by Eq. 1, one in which a harmonic force acts only between particles connected by edges:

$$\widetilde{U} = -\mu \sum_{a>b} A_{ab} |\vec{r}_a - \vec{r}_b|^2/2.$$

We shall call this the $\widetilde{U}-$model. We then define an $N \times N$ matrix X, where the i-th coordinate of the a-th "particle" is denoted by X_{ai}. Thus the above initial condition can be rewritten as

$$X_{ai}(t=0) = \delta_{ai},$$

where δ_{ai} is the Kronecker symbol: $\delta_{ai} = 1$ if $a = i$ and $\delta_{ai} = 0$ otherwise. The equations of motion for the $\widetilde{U}-$model are

$$\frac{dX_{ai}}{dt} = \sum_b F^{(i)}_{ab} = \sum_b A_{ab}(X_{ai} - X_{bi}) = -\sum_b A_{ab} X_{bi} + \sum_b \sum_c A_{ac} \delta_{ab} X_{bi} = \sum_b L_{ab} X_{bi},$$

where

$$L_{ab} = \delta_{ab} \sum_c A_{ac} - A_{ab} = D_{ab} - A_{ab},$$

is the Laplacian matrix. The diagonal matrix D is the degree sequence matrix: D_{aa} is the number of edges incident to the vertex a. Note that L is symmetric: $L = L^T$. The algebraic

isomorphism criterion mentioned in the introduction may also be put in terms of L : two graphs defined by the Laplacian matrices L and L' are isomorphic if and only if there exists a permutation matrix P such that

$$L' = PLP^T.$$

The $\widetilde{U}-$model possesses an explicit solution to the differential equation of motion :

$$X_{ai}(t) = \left(e^{Lt}\right)_{ab} X_{bi}(t=0) = \left(e^{Lt}\right)_{ai}$$

so the final positions are

$$X(T) = e^{LT},$$

in the matrix notation.
Definition: The dot product matrix S is defined as:

$$S_{ab} = \sum_i X_{ai} X_{bi}$$

S_{ab} is the dot product of the vectors associated with the vertices a and b.

The precise form of S depends on the potential function. In the example defined by $\widetilde{U}$, S is given by

$$S = XX^{Transpose} = X^2 = e^{2Lt} = 1 + 2tL + \frac{(2t)^2}{2!}L^2 + ...$$

Another graph would be characterized by a different dot product matrix

$$S' = e^{2L't}.$$

Since the N^2 squared distances $d_{ab}^2 = |\vec{r}_a'(T) - \vec{r}_b'(T)|^2$ satisfy $d_{ab}^2 = S_{aa} + S_{bb} - 2S_{ab}$, comparing the set of numbers in the matrices S and S' is essentially the same as comparing the distances. (We shall consider the relationship more carefully below.)

If the graphs are isomorphic, then clearly S' is a rearrangement of S :

$$S' = e^{2L'T} = e^{2PLP^{-1}T} = Pe^{2Lt}P^{-1} = PSP^{-1}.$$

Conjecture 1 is the converse statement.

In fact there do exist many interesting graph pairs for which the classical algorithm works. Because S is most easily computed in the $\widetilde{U}-$model by diagonalizing the real symmetric matrix L, it is natural to ask whether pairs of non-isomorphic but isospectral graphs can be distinguished by the method. Isospectral graphs are those for which the eigenvalues of A and A' are the same. We have investigated this question for some small graphs that are isospectral but not isomorphic. A simple illustrative pair is shown in Fig. 1

We take the total time interval as $T = 1$ and compute numerically the dynamics of the simple harmonic model for 10 steps of length 0.1 using the first-order Euler algorithm and finally obtain a normalized $X(T)$. The sorted d_{ab}^2 and $d_{ab}^{2\prime}$ for two graphs G and G' in Fig. 1 are respectively

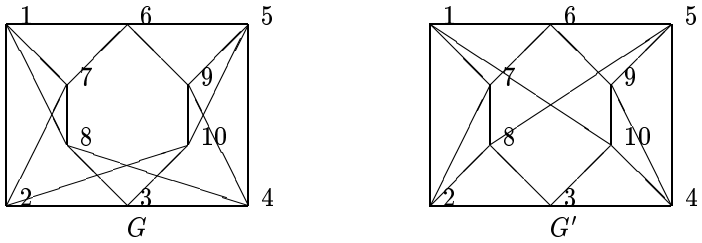

Fig. 1. Two isospectral graphs

$$d^2_{ab} = \{[0]^{10}, [0.6092]^4, [1.0261]^8, [1.1168]^8, [1.4014]^4, [1.6484]^8,$$
$$[1.9936]^{16}, [2.0661]^4, [2.6094]^4, [3.1010]^2, [3.1107]^8, [3.2248]^{16}, [3.3762]^{16}\}.$$
$$d^{2\prime}_{ab} = \{[0]^{10}, [0.8778]^8, [1.0261]^8, [1.1168]^8, [1.6210]^4, [1.6484]^4, [1.9936]^8,$$
$$[2.0660]^4, [2.2605]^8, [2.6318]^4, [2.8788]^4, [3.1010]^2, [3.1107]^8, [3.2248]^8,$$
$$[3.3762]^8, [3.6212]^4\}.$$

In these expressions the superscripts denote the multiplicity of the number in square brackets.

Thus the algorithm of Ref. [25] works for this non-isomorphic isospectral pair. The dynamical algorithm also distinguishes successfully some pairs of graphs that have both identical degree distributions and identical Laplacian spectra [a].

It has been known for decades, however, that certain classes of graphs are difficult to distinguish by elementary methods. An important intransigent class is the so-called "strongly regular graphs" [27, 28].

Definition: A strongly regular graph (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.

An example known as $L_2(3)$ with parameters $(9, 4, 1, 2)$ is shown in Fig. 2. Many pairs of nonisomorphic SRGs with the same parameter set are known. [b]

The adjacency matrix A of a SRG has some interesting algebraic 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 $\left(A^2\right)_{ab} = k$ if $a = b$, $\left(A^2\right)_{ab} = \lambda$ if a is adjacent to b, and $\left(A^2\right)_{ab} = \mu$ 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

$$AJ = JA = kJ.$$

[a] For example, the two graphs of example 2.7 of Russell Merris, Laplacian Graph Eigenvectors, Linear Algebra and its Applications, v. 278, 1998, pp. 221-236, are distinguished successfully.

[b] A list of all known SRGs with fewer than 100 vertices is given at the web site http://www.cs.uwa.edu.au/~gordon/remote/srgs/.

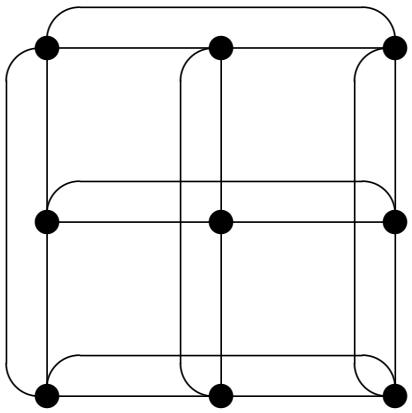

Fig. 2. $L_2(3)$ $(9,4,1,2)$

This follows from the fact that multiplication of a matrix by J has the effect of adding the rows or columns of the matrix. For A, this sum is just the number of neighbors. The Laplacian matrix for a SRG is

$$L = kI - A$$

These equations show that the three matrices $\{I, J, L\}$ form a commutative, associative algebra, which is called the adjacency algebra. The elements of the adjacency algebra have the form $R = fI + gJ + hL$, where f, g and h are real numbers. The multiplication rule is:

$$\begin{aligned} RR' = R'R &= (fI + gJ + hL)\,(f'I + g'J + h'L) \\ &= \left\{ff' - [k^2 - k(\lambda - \mu + 1) + \mu]hh'\right\} I + (fg' + gf' + Ngg' + \mu hh')J \\ &+ [fh' + hf' + (2k + \mu - \lambda)hh']\, L \end{aligned}$$

The three-dimensional character of the adjacency algebra reflects the fact that A has only three distinct eigenvalues.

The main point for our purposes is that the structure of the algebra is independent of the precise form of the L matrix: it depends only on the (N, k, λ, μ) parameters.

With this background we may prove the following result.

Theorem: Any two non-isomorphic strongly regular graphs G and G' characterized by identical parameter sets (N, k, λ, μ) have identical sorted distance matrices: $\{d_{ab}(T)\}$ and $\{d'_{ab}(T)\}$.

Proof

Let G and G' have Laplacian and adjacency matrices L, A and L', A', respectively. The corresponding dot product matrices S and S' are then computed by any desired approximation to the solution of the differential equation of motion. Any such approximation has the form of a finite polynomial in I, J, L :

$$S = \sum a_{rst} I^r J^s L^t, \tag{2}$$

while

$$S = \sum a_{rst} I^r J^s \left(L'\right)^t. \tag{3}$$

The coefficients a_{rst} depend on the model and the approximation, but they are the same for the two graphs. Using the multiplication rules of the adjacency algebra, *which are the same for both graphs*, these expression become

$$S = b_I I + b_J J + b_L L = \left(b_I + k\right) I + b_J J - b_L A, \tag{4}$$

and

$$S' = b_I I + b_J J + b_L L' = \left(b_I + k\right) I + b_J J - b_L A'. \tag{5}$$

The diagonal elements of S and S' are all equal to $b_I + k + b_J$. The off-diagonal elements are equal to b_j or $b_J - b_L$. Now, in any row or column of A or A', precisely k entries are equal to 1 and $N - k$ entries are equal to 0. It follows that, considered as a set of numbers, S has N entries equal to $b_I + k + b_J$, Nk entries equal to $b_J - b_L$, and $N(N - k - 1)$ entries equal to b_J. The same holds true for S'.

The N^2 squared distances satisfy $d^2_{ab} = S_{aa} + S_{bb} - 2S_{ab} = 2\left(b_I + k\right) + 2b_L A_{ab}$, and $\left(d^2\right)'_{ab} = S'_{aa} + S'_{bb} - 2S'_{ab} = 2\left(b_I + k\right) + 2b_L A_{ab}$ when $a \neq b$. For $a = b$, $d^2_{ab} = d^{2\prime}_{ab} = 0$. There are Nk nonzero entries of A_{ab} and A'_{ab} with $a \neq b$. Hence, for both graphs there will be Nk squared distances $2\left(b_I + k + b_L\right)$, $N(N - k - 1)$ squared distances equal to $2\left(b_I + k\right)$, and N squared distances equal to 0. Hence the ordered sets of distances obtained by taking square roots are identical. This completes the proof □.

Corollary 1a: The theorem immediately implies that any pair of non-isomorphic SRG's with the same parameter set furnishes a counterexample to Conjecture 1. It is believed that there is an infinite number of such pairs; if so, then the algorithm fails on an infinite set.

To illustrate the breakdown of the algorithm, we shall apply it to the smallest pair of non-isomorphic SRGs. These are the "Latin square" graphs with $N = 16$ vertices. Latin squares are two-dimensional $M \times M$ arrays of the numbers 1 to M, arranged so that in each row and column no number is repeated. Two examples are shown in Fig. 3. Latin square graphs are constructed from Latin squares as follows: Given a Latin square of order M, the vertices are the $N = M^2$ cells. Two vertices are adjacent if they lie in the same row or column or if they share the same integer label.

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

Fig. 3. Latin squares $L_3(4)$ $(16, 9, 4, 6)$[29]

We use the following non-harmonic potential U_1 to calculate normalized $X(T)$ and d_{ab}^2 again using the first-order Euler algorithm for the two non-isomorphic Latin square graphs drawn from Fig. 3.

$$U_1 = -A\sum(r_a - r_b)^2 + B\sum(r_a - r_b)^4 \,,$$

where the sum is over pairs of connected vertices. Again taking time interval $T = 1$ with step of length 0.1, we obtain the distances d_{ab}^2 for $A = 1,\ B = 1$

$$d_{ab}^2 = \left\{[0]^{16}, [1.8641]^{96}, [2.3129]^{144}\right\}.$$
$$d_{ab}^{2\prime} = \left\{[0]^{16}, [1.8641]^{96}, [2.3129]^{144}\right\}.$$

$f^{(\prime)},\ h^{(\prime)}$ are computed from $d_{ab}^{2(\prime)}$

$$f = f' = -1.0876$$
$$h = h' = 0.2244$$

$g = g'$, but these quantities do not affect the distances. We have also verified that the two sets are identical at each of the discrete time steps. As one would expect, the multiplicity of each distinct distance depends only on N and k and are independent of time.

For completeness we tried a different non-harmonic attractive(repulsive) potential $U_1(\vec{r}_a - \vec{r}_b)(U_2(\vec{r}_a - \vec{r}_b))$ whose force is expressed as

$$\vec{F}_{1a} = -\nabla_{\vec{r}_a} U_1(\vec{r}_a - \vec{r}_b) = \frac{\vec{r}_a - \vec{r}_b}{1 + |\vec{r}_a - \vec{r}_b|^3}.$$
$$\vec{F}_{1a} = -\vec{F}_{2a}.$$

Using this potential and still taking $T = 1$, we obtain the distances

$$d_{ab}^2 = \left\{[0]^{16}, [1.4991]^{96}, [2.4486]^{144}\right\}.$$
$$d_{ab}^{2\prime} = \left\{[0]^{16}, [1.4991]^{96}, [2.4486]^{144}\right\}.$$

with $f^{(\prime)},\ h^{(\prime)}$

$$f = f' = -3.5482$$
$$h = h' = 0.4748$$

Thus, using a non-harmonic potential does not enable the dynamical algorithm to distinguish these graphs.

2.2 Quantum algorithms

The classical algorithm depends on an embedding of the graph in a Hilbert space. This suggests a simple quantum modification of the classical algorithm, a kind of single-particle quantum random walk. Consider the vertices of the graph as states $|j\rangle$ in a Hilbert space. The Hamiltonian for the walk is

$$H = -\sum_{ab} A_{ab} c_a^\dagger c_b,$$

where the operator $c_a^\dagger c_b$ is defined by $\langle i \left| c_a^\dagger c_b \right| j \rangle = \delta_{ia}\delta_{bj}$. In physics terms, this is simply a tight-binding model with bonds on the vertices of the graph. We now consider N possible starting wavefunctions

$$|\psi_1(t=0)\rangle = |1\rangle\,, \;\; |\psi_2(t=0)\rangle = |2\rangle\,, \;\; ...$$

and we evolve these forward in time according to the usual time-dependent Schrödinger equation

$$i\frac{d\,|\psi\rangle}{dt} = H\,|\psi\rangle \tag{6}$$

for a time T. We then compute the $N \times N$ matrix of overlaps

$$O_{ij} = \langle \psi_i(0) | \psi_j(T) \rangle\,.$$

This is an analog of the distance matrix for the classical algorithm. The O_{ij} can be sorted by any convenient method. For example, one may first sort the real parts, then use the imaginary parts to break ties. Let the sorted set so obtained be denoted by $\left\{\widetilde{O}_{ij}\right\}$. This leads to

Conjecture 2. If the sorted overlap sets $\left\{\widetilde{O}_{ij}\right\}$ and $\left\{\widetilde{O}'_{ij}\right\}$ obtained by the single-particle quantum random walks for the graphs G and G' are identical, then G and G' are isomorphic.

It is certainly the case that $\left\{\widetilde{O}_{ij}\right\}$can distinguish certain isospectral graphs, since it uses information about the eigenvectors of H, not just information about the spectrum. Nonetheless, conjecture 2 is false.

Corollary 1b: By following the proof of theorem 1, we find that pairs of non-isomorphic SRG's with identical parameter sets have identical sorted overlap sets $\left\{\widetilde{O}_{ij}\right\}$ and $\left\{\widetilde{O}'_{ij}\right\}$. The algebra over I, J, L is complex in the quantum case, but there are no other differences, so we omit the details of the proof.

Hence Conjecture 2 is false.

Though the two strongly regular Latin square graphs of Fig. 3 are not distinguished by the classical or the one-particle quantum random walk algorithms, they can be distinguished in polynomial time by using a construction proposed by Rudolph [26]. Now we use the same Hamiltonian but consider the quantum-mechanical motion of three particles. Rudolph uses symmetric wavefunctions (to be defined below) but forbids double occupancy of any site, corresponding in physics terms to a hard-core boson model. Rudolph showed that the spectra of the 3-particle matrices obtained from two non-isomorphic regular graphs with identical

single-particle spectra are different, demonstrating that the multiparticle construction does increase the power of the algorithm to distinguish similar graphs.

Here we combine Rudolph's multiparticle construction with the dynamical algorithm for wavefunction overlaps; this hybrid algorithm has the advantage that it can distinguish non-isomorphic strongly regular graphs using the 2-particle matrices, as opposed to 3-particle matrices needed if the matrix eigenvalues are examined. In addition to Rudolph's original case of hard-core bosons, we also examine non-hard-core bosons and noninteracting spinless fermions.

For bosons (which have wavefunctions that are symmetric under particle interchange) we consider a simple Hubbard Hamiltonian [30], in which each boson can hop between two vertices if and only if the vertices are connected by an edge, and in addition there is an energy cost U if two bosons are on the same site. Using as a basis the states $|ij\rangle$ with particles at vertices i and j, the matrix K for the level 2 (i.e. two-particle) graph for bosons is specified by the Hamiltonian matrix elements

$$\begin{aligned} K^B_{ij,\ kl} &\equiv -\langle ij\,|H|\,kl\rangle \\ &= \delta_{il}A_{kj} + \delta_{jk}A_{il} + \delta_{ik}A_{jl} + \delta_{jl}A_{ik} \qquad \text{if } i \neq j \text{ and } k \neq l \\ &= U\delta_{ik} \qquad \text{if } i = j \text{ and } k = l \\ &= \frac{1}{\sqrt{2}}(\delta_{il}A_{kj} + \delta_{jk}A_{il} + \delta_{ik}A_{jl} + \delta_{jl}A_{ik}) \qquad \text{if } i = j \text{ or } k = l. \end{aligned}$$

There are $N(N+1)/2$ initial two-particle states

$$|ij\rangle = |11\rangle\,, |12\rangle\,, |13\rangle\,, \ldots |1N\rangle\,, |22\rangle\,, |23\rangle\,, |24\rangle \ldots, |NN\rangle\,.$$

In the hard core limit $U \to \infty$ the basis states with doubly-occupied sites can be ignored, so that the Hilbert space has $N(N-1)/2$ dimensions, and the Hamiltonian matrix elements are

$$\begin{aligned} K^{HCB}_{ij,\ kl} &\equiv -\langle ij\,|H|\,kl\rangle \\ &= \delta_{il}A_{kj} + \delta_{jk}A_{il} + \delta_{ik}A_{jl} + \delta_{jl}A_{ik}\ , \end{aligned}$$

where now we require $i \neq j$ and $k \neq l$.

For fermions, (which have wavefunctions that are antisymmetric under particle interchange), the Hilbert space has $N(N-1)/2$ dimensions, since only at most one fermion is allowed on a site. We can choose the basis states $|ij\rangle$, $i \neq j$. The Hamiltonian matrix elements are

$$K^F_{ij,\ kl} = \delta_{il}A_{kj} + \delta_{jk}A_{il} - \delta_{ik}A_{jl} - \delta_{jl}A_{ik}.$$

Thus we extend an adjacency matrix of rank N to a matrix K of higher rank, either $N(N+1)/2$ (for non-hard-core bosons) or $N(N-1)/2$ (for hard-core bosons and for fermions). Technically, except for hard core bosons, the matrix K is not an adjacency matrix since it has elements other than 0 and 1. For fermionic statistics, some entries of K are equal to -1, while for soft-core bosons some entries are equal to $\sqrt{2}$ and others to U. K can be pictured basically as a matrix in which every off-diagonal element represents the probability amplitude for two particles to hop from one state to another state. Accordingly, the information of the adjacency matrix A is embedded in the corresponding K.

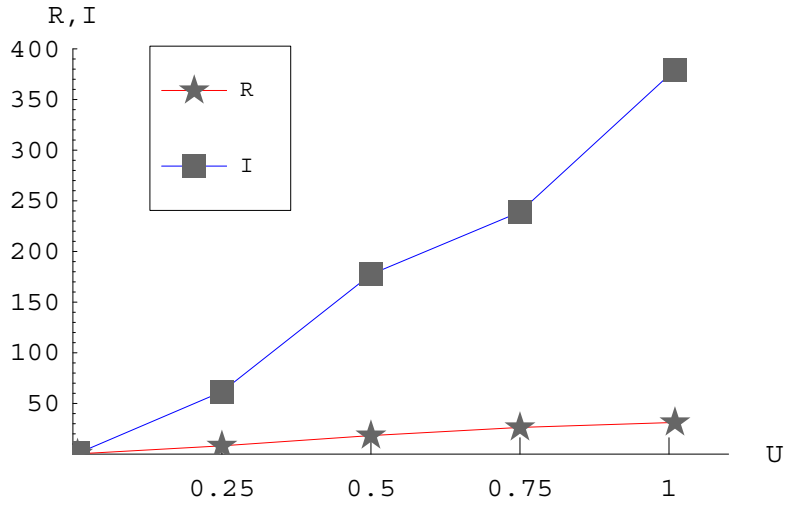

Fig. 4. Variation of the numbers R and I (defined in Eqs. 7 and 8) as a function U (potential) for the two non-isomorphic Latin square graphs with N=16. As U goes to zero, R and I vanish.

Again we evolve forward the initial two-particle states in time according to the quantum mechanical evolution Eq. (6) and ask whether any pair of nonisomorphic graphs has two distinct sets of $\left\{\widetilde{O}_{ij'kl}(T)\right\}$. We order these sets dictionary-style, first by their real parts and then use the imaginary parts to break ties, and make the following set of conjectures:

Conjectures 2a,2b,2c: If the sorted overlap sets $\left\{\widetilde{O}_{ij,kl}\right\}$ and $\left\{\widetilde{O}'_{ij,kl}\right\}$ obtained by two-particle quantum random walks of (a) non-interacting bosons, (b) non-interacting fermions, (c) interacting bosons, for the graphs G and G' are identical, then G and G' are isomorphic.

We do not at present have analytical arguments to support or confute these conjectures, and give only numerical evidence. The test of isomorphism is whether the sets $\left\{\widetilde{O}_{ij,kl}\right\}$ and $\left\{\widetilde{O}'_{ij,kl}\right\}$are the same after rearranging. A simple way to compare the ordered sets is to compute the numbers R and I defined as

$$R(T) = \sum_{i,j} |\mathrm{Re}\widetilde{\mathrm{O}}_{\mathrm{ij,kl}}(\mathrm{T}) - \mathrm{Re}\widetilde{\mathrm{O}}'_{\mathrm{ij,kl}}(\mathrm{T})| \tag{7}$$

$$I(T) = \sum_{i,j} |\mathrm{Im}\widetilde{\mathrm{O}}_{\mathrm{ij,kl}}(\mathrm{T}) - \mathrm{Im}\widetilde{\mathrm{O}}'_{\mathrm{ij,kl}}(\mathrm{T})|, \tag{8}$$

where in both cases the differences are taken between the entries in the ordered sets of overlaps. We compute R and I for pairs of non-isomorphic SRG's with the same parameter sets. If either $R(T)$ or $I(T)$ is nonzero, it follows immediately that the graphs are not isomorphic. Conjectures 2a, 2b, and 2c are the converse of this statement.

For each graph in a given pair, we find numerically the eigenvectors and eigenvalues of K and use them to calculate the $\{O_{ij,kl}\}$, $\{\ O_{ij,kl}\}$then $R(T)$ and $I(T)$ for $T = 1$. The qualitative behavior does not depend on the choice of T. Table 1 shows that for all these pairs of graphs

graph specification	fermions	noninteracting bosons	hard-core bosons
(16,9,4,6)	R=1.37 I=11.11	R=0 I=0	R=110.66 I=886.05
(25,12,5,6)	R=1.24 I=5.96	R=0 I=0	R=129.66 I=2160.86
(26,10,3,4)	R=1.91 I=3.50	R=0 I=0	R=14.88 I=896.75
(28,12,6,4)	R=1.82 I=6.88	R=0 I=0	R=87.27 I=1384.86
(29,14,6,7)	R=3.50 I=6.08	R=0 I=0	R=28.69 I=2672.23
(35,18,9,9)	R=0 I=0	R=0 I=0	R=300.63 I=3970.15

Table 1. Table of results for hybrid dynamical algorithm for pairs of nonisomorphic strongly regular graphs for non-interacting fermions, non-interacting bosons, and hard-core bosons. Each pair of graphs has the same parameters (N, k, λ, μ), where N is the number of vertices, 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. Noninteracting bosons do not distinguish any of the pairs of nonisomorphic graphs, noninteracting fermions distinguish most but not all pairs of nonisomorphic graphs tested, and hard-core bosons distinguish all pairs of nonisomorphic graphs examined.

both R and I vanish for noninteracting bosons, but both R and I are nonzero for hard core bosons and for noninteracting fermions for $N \leq 29$. $R = I = 0$ for the noninteracting fermion algorithm for a specific pair of non-isomorphic graphs with $N = 35$. Hence Conjectures 2a and 2b are false, but conjecture 2c remains open. However, the non-interacting fermion algorithm is much more powerful than the non-interacting boson algorithm, for reasons that we do not at present understand. We find also that R and I are nonzero for graphs with nonzero but finite U. An illustration of this is shown in Fig. 4 the pair with $N = 16$. Note that the linear term in U is sufficient to distinguish these graphs.

We remark that it is necessary examine all matrix elements of K, not just the spectrum of K. The K matrices of the two non-isomorphic graphs still share the same set of eigenvalues for all non-interacting two-particle systems. In physical terms, this is due to the additivity

	graph 1	graph 2	graph 3	graph 4	graph 5
graph 2	No				
graph 3	Yes	Yes			
graph 4	No	No	Yes		
graph5	No	No	Yes	No	
graph6	No	No	Yes	No	No

Table 2. Table of distinguishability by fermions for six (35,18,9,9) nonisomorphic SRGs. Yes entries denote graph pairs that are distinguished by the two-fermion algorithm. Note that only graph 3 is distinguished from the other five graphs. Thus, it appears that there may be some distinct properties among these graphs that allow fermions to tell some but not all of them apart.

of energies for non-interacting particles.

1	2	3	4	5
2	3	4	5	1
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4

1	2	3	4	5
2	1	4	5	3
3	5	1	2	4
4	3	5	1	2
5	4	2	3	1

Fig. 5. Latin squares $L_3(5)$ $(25, 12, 5, 6)$[29]

2.3 Summary

We have examined several dynamical algorithms for the GI problem, both classical and quantum. Our work shows that the classical algorithm, the one-particle quantum algorithm, and the two-particle non-interacting boson algorithm, all fail on the class of strongly regular graphs (falsity of conjectures 1, 2, and 3a). Intriguingly, the two particle non-interacting fermion algorithm also fails to distinguish at least one non-isomorphic pair of strongly regular graphs, (falsity of conjecture 3b), but does appear to distinguish most such pairs, at least when the number of vertices is reasonably small. Conjecture 3c, that the two-particle non-interacting boson algorithm solves GI, has stood all tests so far.

3 Discussion

From the standpoint of efficiency, we must distinguish whether the algorithms are run on a classical or a quantum computer. The two-particle algorithms already run in polynomial time on a classical computer. The $\{O_{ij,kl}\}$ matrix contains $O(N^4)$ entries, each of which is computed in a time of $O(N^4)$. If conjecture 3c holds, then GI is in P. If conjecture 3c does not hold, then we may consider an extension of the algorithm to an N_p- particle quantum random walk, where $N_p \sim O(N)$. Then the running time on a classical computer is roughly $\binom{N}{N_p} \sim \binom{N}{N/2}$, which is exponential. The question of efficiency on a quantum computer is more interesting. The motion of $N_p \sim N$ particles can be mapped onto the Heisenberg model of a spin system at a fixed magnetization, which is nothing more than the dynamics of N qubits with a constraint. Thus the evolution takes place in polynomial time on a quantum computer. On the other hand, the simplest extension of the quantum algorithm requires an exponential number of measurements. However, since all we need to do is ask whether the evolution of the two systems is in some sense similar, there may exist a preparation that entangles the graphs and a single measurement, or perhaps a set of measurements of polynomial size, that captures the needed information. In this connection, the work of Aharonov and Ta-Shma, who showed that GI is reducible to estimating the inner product of two quantum states, is perhaps relevant [31].

In conclusion, we have shown that strongly regular graphs provide a useful testbed for both classical and quantum dynamical algorithms that aim to solve the graph isomorphism problem. Pairs of graphs in this class cannot be distinguished by the classical algorithm of Gudkov and

Nussinov [25], but quantum algorithms combining the dynamical evolution of the algorithm of Gudkov and Nussinov with a construction of Rudolph [26] using interacting bosons as well as noninteracting fermions can distinguish pairs of SRGs of order ≤ 29, while a two-boson noninteracting algorithm fails [32]. An algorithm employing non-interacting fermions fails at $N = 35$. Interesting open questions include whether there exists a counterexample for the two-particle hard-core-boson algorithm, whether an N_p-hard-core-boson algorithm solves GI, and if so, what value of N_p suffices, and whether an algorithm with $N_p \sim N$ can be implemented efficiently on a quantum computer.

Acknowledgements

We thank Eric Bach and Dieter van Melkebeek for extremely useful conversations. This research was supported by the NSF QuBIC program under Grant No. NSF-ITR-0130400.

References

1. J. Köbler, U. Schöning, and J. Toràn. *The Graph Isomorphism Problem — Its Structural Complexity.* Progress in Theoretical Computer Science. Birkhäuser, Boston, 1993.
2. S. Fortin, *The graph isomorphism problem*, Tech. Report TR 96-20, Dept. of Computing Science, University of Alberta, 1996.
3. X. Liu and D.J. Klein, *The graph isomorphism problem*, *J. Comput. Chem.* **12**, 1243-1251 (1991).
4. Hopcroft, J.E. and Tarjan, R.E., *A V^2 algorithm for determining isomorphism of planar graphs*, *Information Processing Letters* **1**, 32-34 (1971).
5. Hopcroft, J.E. and Wong, J.K., *Linear time algorithm for isomorphism of planar graphs*, *Proc. 6th ACM Symposium on Theory of Comput.*, 1974, 172-184.
6. Luks, E.M., *Isomorphism of graphs of bounded valence can be tested in polynomial time*, *J. Comput. Sys. Sci.* **25**, 42-65 (1982)
7. Hoffmann, C.M., *Group-theoretic algorithms and graph isomorphism.* Springer-Verlag, Berlin, 1982.
8. L. Babai, D. Grigoryev, and D. Mount, *Isomorphism of graphs with bounded eigenvalue multiplicity.* In *Proc. 14th ACM Symp. on Theory of Computing*, pp. 310-324, 1982.
9. J. Chen, *A linear-time algorithm for isomorphism of graphs of bounded average genus*, *SIAM J. Disc. Math.* **7**, 614-631 (1994).
10. L. Babai and E. Luks, *Canonical labeling of graphs*, in *Proc. 15th ACM Symp. on Theory of Computing*, 171-183 (1983).
11. R. Mathon, *A note on the graph isomorphism counting problem*, *Information Processing Letters*, **8**, 131-132 (1979).
12. R. Boppana, J. Hastad, and S. Zachos, *Does co-NP have short interactive proofs?* In *Information Processing Letters* **25**, pp. 27-32, 1987.
13. U. Schöning, *Graph isomorphism is in the low hierarchy*, *J. Computer and System Sciences* **37**, 312-323 (1988).
14. Perhaps the best-known example of a problem believed to be neither in P nor NP-complete is factorization, for which no classical polynomial algorithm is known but which can be solved in polynomial time on a quantum computer [15].
15. P.W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Sci. Statis. Comput. **26**, 1484 (1997).
16. M. Grigni, L. J. Schulman, M. Vazirani, and U. Vazirani, *Quantum mechanical algorithms for the non-abelian hidden subgroup problem*, in *Proc. 33rd Annual ACM symposium on theory of computing*, pp. 68-74 (2001).
17. S. Hallgren, A. Russell, and A. Ta-Shma, *The hidden subgroup problem and quantum computation using group representations*, SIAM J. Comput. **32**, 916-934 (2003).

18. C. Moore, A. Russell, and L.J. Schulman, *The symmetric group defies strong Fourier sampling, Part I.* quant-phys 0501056.
19. C. Moore and A. Russell, *The symmetric group defies strong Fourier sampling, Part II.* quant-phys 0501066.
20. Aaronson *Quantum Lower Bound for the Collision Problem* in *Proc. ACM Symp. on Theory of Computing,* 635-642 (2002).
21. A well-known quantum algorithm motivated by physical processes is the adiabatic algorithm proposed by Farhi and collaborators [22, 23, 24]. The algorithms we examine are clearly different than the adiabatic algorithm, but the philosophy underlying the scheme is analogous.
22. E. Farhi et al., *A quantum adiabatic algorithm applied to random instances of an NP-complete problem*, Science **292**, 472-475 (2001).
23. A.M. Childs, E. Farhi, and J. Preskill, *Robustness of adiabatic quantum computation*, Phys. Rev. A **65**, 012322 (2002).
24. J. Roland and N.J. Cerf, *Quantum search by local adiabatic evolution*, Phys. Rev. A **65**, 042308 (2002).
25. V. Gudkov and S. Nussinov, *Graph equivalence and characterization via a continuous evolution of a physical analog*, cond-mat/0209112.
26. T. Rudolph, *Constructing physically intuitive graph invariants*, quant-ph/0206068.
27. D.B. West, *Introduction to Graph Theory, 2nd ed.* Prentice-Hall, Englewood Cliffs, NJ (2000).
28. A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs,* SpringerVerlag, Berlin, 1989.
29. Denes, J.; Keedwell, A. D.: *Latin Squares and Their Application.* Academic Press, New York, London, 1974.
30. J. Hubbard, Proc. R. Soc. London Sr. A **276**, 238 (1963); M. Gutzwiller, Phys. Rev. Lett. **10**, 159 (1963); J. Kanamori, Prog. Theor. Phys. **30**, 275 (1963).
31. Aharonov and Ta-Shma, *Adiabatic Quantum State Generation and Statistical Zero Knowledge*, in *Proc. ACM Symp. on Theory of Computing*, 20-29 (2003).
32. We do not know whether the noninteracting N_p-boson algorithm distinguishes SRGs when $N_p > 2$.