Reprinted from JOURNAL OF COMPUTER AND SYSTEM SCIENCES
All Rights Reserved by Academic Press, New York and London

Vol. 18, No. 2, April 1979
Printed in Belgium

Graph Isomorphism, General Remarks*

GARY L. MILLER

Applied Mathematics Group, Department of Mathematics,
Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

Revised July 11, 1978

An open question is the computational complexity of recognizing when two graphs are isomorphic. In an attempt to answer this question we shall analyze the relative computational complexity of generalizations and restrictions of the graph isomorphism problem. We show graph isomorphism of regular undirected graphs is complete over isomorphism of explicitly given structures (say Tarski models from logic). We also show a fundamental difference between how automorphism groups can act on a graph of valence n and how they can act on graphs of valence $n + 1$ (with one exception). This group theoretic result seems to have implications on the role of valence for graph isomorphism algorithms. Finally, we introduce "certificates" for symmetric cubic graphs.

INTRODUCTION

In the late 60's and early 70's a new technique was developed to analyze the computational complexity of decision problems. Three of the many people who worked on this technique were Cobham, Cook and Karp. Cobham [64] was one of the first people to define the class of polynomial time recognizable sets. We shall denote this class by P. It is this notation of polynomial time computable which will be our notation of feasibly computable problems. Cook [70] defined the notation of nondeterministic polynomial time (NP) and NP-completeness and showed that there was a problem which was NP-complete, thus initiating a fundamental technique for classifying problems with respect to P. Following Cook, Karp [72] presented dozens of natural problems which were also NP-complete. These techniques are so widely applicable that since these papers literally hundreds of seemingly different problems have been shown to be either NP-complete or polynomial time computable.

One of the problems mentioned in both Cook [70] and Karp [72] which has not yielded to this classification technique is the problem of recognizing when two graphs are isomorphic.

The goal of this paper is to use reducibility techniques and other computational complexity notations to understand generalization and restriction of the graph iso-

* This research was supported in part by the National Research Council under Grant #NRC-A5549; in part by the Alfred P. Sloan Foundation under Grant #74-12-5; and in part by the Advanced Research Projects Agency of The Department of Defense, monitored by ONR under Contract #N00014-75-C-1091.

0022-0000/79/020128-15$02.00/0

morphism problem. The paper is divided into three sections, each quite different in both technique and goals. The first section shows that a broad class of isomorphism problems can be reduced to graph isomorphism. An example of such a reducible problem is that of isomorphism of two groups when they are given as multiplication tables.

The last two sections use considerably more group theory. In fact, the results of the second section are motivated by the question of the role of valence in graph isomorphism algorithms, but at the present time are more applicable as group theoretic results. An example of a question considered in section two is: can isomorphism of graphs of valence 4 be reduced to isomorphism of graphs of valence 3? One should point out that only positive answers to questions of this form can be given at the present time without settling the "$P - NP$" question. Thus negative results must be less than absolute. In light of the fact that negative results do not exist for these types of questions, I think the results are quite strong. We show that there is a fundamental difference between how groups act on graphs of valence n and how they can act on graphs of valence $n + 1$ (with one exception, A_4 is not a simple group).

Finally, in the last section we look more closely at solutions to the graph isomorphism problem which do not give a polynomial time algorithm but still may be of practical value. We define the notation of a succinct certificate for a graph. The basic idea is that a graph may have a short characterization and also a short proof of that characterization, but it may be hard to find such characterizations or proofs. As an example, we show that the symmetric cubic graphs have succinct certificates.

Notation. A graph throughout this paper will be a combinatorial graph. Namely, a graph G is a finite set of vertices plus a set of ordered or unordered pairs of vertices called edges. The set of vertices will be denoted by $V(G)$ while the set of edges will be denoted by $E(G)$. Graphs consisting of ordered pairs are called directed, while those consisting of unordered pairs are called undirected graphs. The graphs are undirected unless otherwise noted. The number of edges associated with a vertex is the valence of the vertex. The valence of a graph is equal to the *maximum* over the valences of the vertices. A graph is said to be regular if all vertices have the same valence. Two graphs G and G' are said to be isomorphic if there is a 1-1 map from $V(G)$ onto $V(G')$ which preserves edges. We will denote G is isomorphic to G' by $G \approx G'$.

We shall need the computational notations of Cook [70], Karp [72]:

(1) $P(NP)$ is all sets recognizable in (non)deterministic polynomial time;

(2) $A \leqslant_p B$ denote that A is polynomial time reducible to B.

I. Completeness of Graph Isomorphism over Isomorphism

The main result of this Section is Theorem 2, which states that isomorphism of undirected graphs is complete over the general isomorphism problem. We first state and prove a special case which contains most of the ideas and techniques to be used in the general case.

THEOREM 1. *Directed Graph Isomorphism* $\leqslant_p$ *Undirected Graph Isomorphism.*

Proof. Suppose that G and G' are two directed graphs on n vertices. We define a map or procedure, say α, from directed graphs to undirected graphs, such that $G \approx G'$ iff $\alpha(G) \approx \alpha(G')$. Given G we construct $\alpha(G)$ as follows:

(1) For each vertex of G construct a vertex for $\alpha(G)$.

(2) For each directed arc of G (say $(x \to y)$) construct a "gadget" using 7 new vertices and connect it to x and y as in Fig. 1.

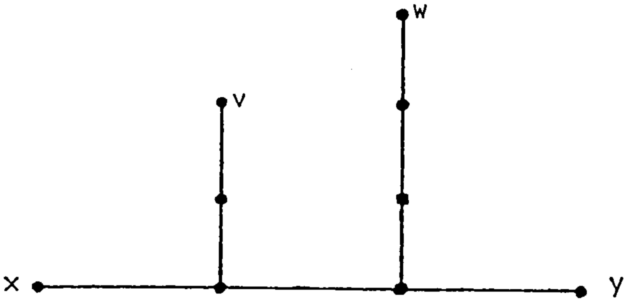

FIGURE 1

By the construction it should be clear that if g is an isomorphism of G onto G' then the natural extension of g to $\alpha(G)$ is also an isomorphism of $\alpha(G)$ onto $\alpha(G')$. Thus, to complete the proof of the theorem it suffices to prove the following lemma:

LEMMA. *If g is an isomorphism from $\alpha(G)$ onto $\alpha(G')$ then g restricted to the vertices of G is an isomorphism of G onto G'.*

Proof. The neighborhood sequence of a vertex x in a graph on n vertices is a sequence of natural numbers $S(x) = \langle a_1 ,..., a_n \rangle$ such that a_i is the number of vertices whose minimum distance to x is i. Note that the neighborhood sequence is an invariant under isomorphism. Now, neighborhood sequences of v and w of Fig. 1 have the form $\langle 1, 1, 2,... \rangle$ and $\langle 1, 1, 1, 2,... \rangle$ respectively. If $x \in V(G)$ and x is of valence l in G then the neighborhood sequence of x in $\alpha(G)$ is of the form $\langle l, 2l,... \rangle$. Thus, the vertices v (or w) from gadgets in $\alpha(G)$ are invariant under isomorphism, e.g. any isomorphism must send v vertices to v vertices. Therefore gadgets are invariants. The function g maps $V(G)$ onto $V(G')$. Finally, g restricted to $V(G)$ is an isomorphism of G onto G', since $x \to y$ iff x is connected to y by a gadget in $\alpha(G)$. This completes the proof of the lemma and hence the proof of Theorem 1.

A *structure* is a set A with relations $R_1 ,..., R_m$, where $R_i \subseteq A^A$, which we will denote by $\langle A, R_1 ,..., R_m \rangle$. We will say $\langle A, R_1 ,..., R_m \rangle$ is *isomorphic* to $\langle A', R_1' ,..., R_m' \rangle$ if there exists a one-to-one map g from A onto A' such that $\langle x_1 ,..., x_k \rangle \in R_i$ if and only if $\langle g(x_1),..., g(x_k) \rangle \in R_i'$, $1 \leqslant i \leqslant m$.

To prove that undirected graph isomorphism is complete over isomorphism of structures, using the techniques developed in the proof of the last theorem, we will need to define a general construct α.

Given a structure $\langle A, R_1, \ldots, R_m \rangle$ we defined $\alpha(\langle A, \ldots \rangle)$ as follows:

(1) For each element of A construct a vertex for $\alpha(\langle A, R_1, \ldots, R_m \rangle)$;

(2) (a) For each ordered sequence $\langle x_1, \ldots, x_k \rangle \in R_i$, $k \geqslant 3$, construct a R_i-gadget (see Fig. 2);

(b) For each $\langle x_1, x_2 \rangle \in R_i$, use the construction in Fig. 3;

(c) For each $\langle x_1 \rangle \in R_i$, use the construction in Fig. 4.

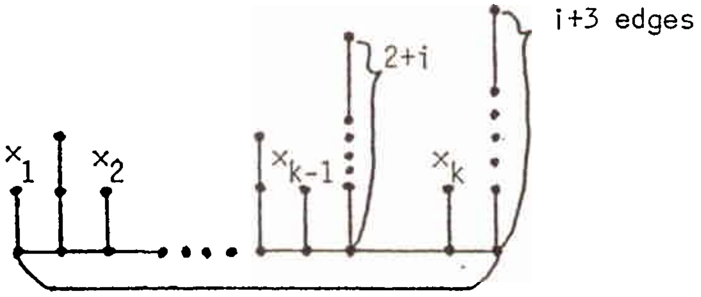

FIGURE 2

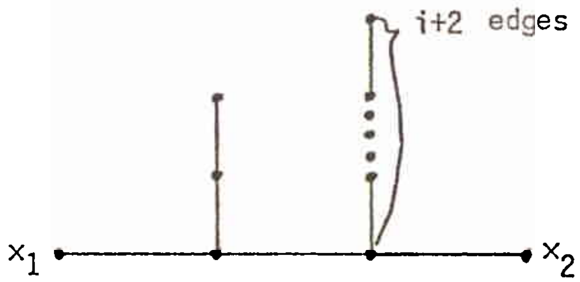

FIGURE 3

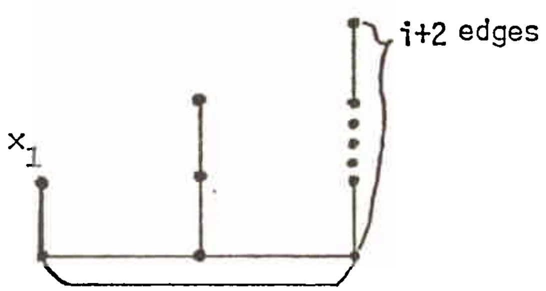

FIGURE 4

By arguments similar to those previously used, we see the neighborhood sequence of the "leaves" are unique hence invariant under isomorphism. Thus, R_i-gadgets are invariant, which implies A is an invariant. Finally, any isomorphism of $\alpha(A)$ onto $\alpha(A')$ induces an isomorphism of A onto A'. This proves the following theorem.

THEOREM 2. *Isomorphism of Structure $\leqslant_p$ Graph Isomorphism.*

By a group we shall mean a multiplication or Caley table. Since a group can be viewed as a trinary relation over a set, namely $\langle x, y, z\rangle$ iff $x \cdot y = z$, we get the following corollary:

COROLLARY (Miller, Monk). *Group Isomorphism $\leqslant_p$ Graph Isomorphism.*

The best-known upper bound for group isomorphism is $O(n^{\log n+3})$ due to Tarjan, where n is the order of the groups. For a discussion of this result and generalization to latin squares and some graphs derived from latin squares, see Miller [78]. On the other hand, isomorphism of semigroups is equivalent to graph isomorphism, see Booth [in press].

Theorem 2 seems easily strengthened in many ways. For example, let a hypergraph be a pair $\langle A, \tau\rangle$ such that $\tau \subseteq 2^A$. Then, by similar methods, hypergraph isomorphism can be easily shown polynomial time reducible to graph isomorphism.

The next result says that when we consider graphs of valence α where α is odd we need only consider the subcase of regular graphs of valence α.

THEOREM 3. *Isomorphism of graphs of valence $\alpha \leqslant_p$ isomorphism of regular graphs of valence α, when α is odd.*

Proof. Consider a $T_{\alpha,n}$ gadget, with vertices $\{x, a_{ij}, b_{ij} \mid 1 \leqslant i \leqslant \alpha - 1, 1 \leqslant j \leqslant n\}$ with connections:

$$\{\langle x, a_{i1}\rangle \mid 1 \leqslant i \leqslant \alpha - 1\}$$
$$\{\langle a_{ij}, b_{kj}\rangle \mid 1 \leqslant i, k \leqslant \alpha - 1 \text{ and } 1 \leqslant j \leqslant n\}$$
$$\{\langle b_{ij}, a_{ij+1}\rangle \mid 1 \leqslant j < n\}$$
$$\{\langle b_{in}, b_{i+1n}\rangle \mid 1 \leqslant i < \alpha - 1, i \text{ odd}\}.$$

For example, $T_{3,2}$ is given in Fig. 5.

Given a graph G of valence α, α odd, we can pick n large enough so that $T_{\alpha,n}$ never occurs in G. Now the valence of any vertex can be increased by one by simply attaching a new copy of $T_{\alpha,n}$ with an edge from the vertex to x. Thus by adding as many gadgets as necessary we can increase the value of any vertex to α. Thus Theorem 3 is proved.

This gadget has the property that all its vertices have valence α except one which has valence $\alpha - 1$. Any other gadget, it would seem, also needs to have this property.

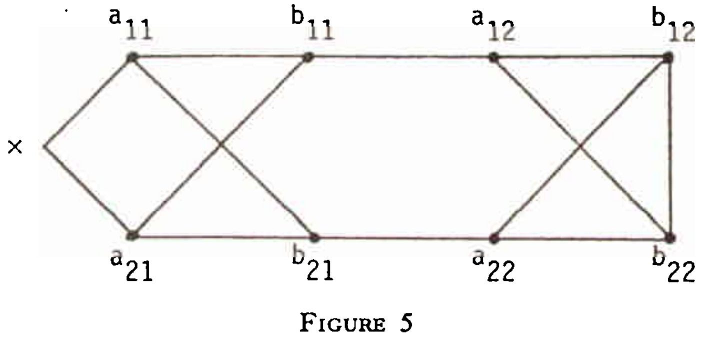

FIGURE 5

But if α is even and K is a gadget with the above property then K is a graph with an odd number of nodes of odd valence. By a simple counting argument of Euler's we see this is impossible.

Up to an increase in valence of at most one we can assume our graphs are regular.[1]

COROLLARY. *Graph Isomorphism $\leqslant_p$ Regular Graph Isomorphism.*

This corollary has been proven independently by Booth [in press].

II. BOUNDED VALENCE

All the constructions of Section I preserve valence in the sense that the valence of G equals the valence of $\alpha(G)$. Our goal in this section is to analyze the importance of valence in the isomorphism problem. A natural formalization of this problem is the following open question.

OPEN QUESTION. Graph Isomorphism $\leqslant_p$ Isomorphism over Graphs of Bounded Valence.

Let us first consider bounding the valence to 3. One way of constructing a cubic graph from an arbitrary graph is to replace vertices of valence n ($n > 3$) by an n-gon. This procedure is not well defined, as the following example shows. Consider Graph A from Fig. 6a. These are two ways to replace x by a 4-gon, giving graphs B and B' (see Figs. 6b, 6c). These two graphs are not isomorphic; in fact, B is planar while B' is not planar. Thus it seems that replacing vertices of higher valence by polygons fails because the polygons induce an orientation on the arcs attached to them. A polynomial time procedure which uniquely replaces vertices by polygons independent of how the graphs are presented would seem to have implications in both algorithms for graph isomorphism and algorithms for computing genus of a graph (see section three on surfaces (2-dimensional manifolds)).

If C is a permutation group acting on S, $S' \subseteq S$ and $c \in C$, then c is said to stabilize S' if it sends elements of S' to elements of S'. We shall denote the subgroup of C which stabilizes S' by $C(S')$. On the other hand, c fixes S' if it fixes each element of S'. The subgroup of C which fixes S' we shall denote by $C(\bigcup S')$. Using these definitions an edge of a graph is stabilized if its vertices are stabilized, and it is fixed if its vertices are fixed.

Since the n-gon is only one of an infinite number of possible graphs that might work, we now formalize the properties we seem to need of such a graph and then proceed to show that no such graph can exist (with one exception).

DEFINITION. An isomorphism (m, n)-gadget, for $m > n$, is a pair (G, A) consisting of a connected graph G with valence at most n together with m distinguished vertices Γ

[1] Corneil and Kirkpatrick [PC] have been able to prove Theorem 3 without the constraint that α is odd by using two copies of the graph.

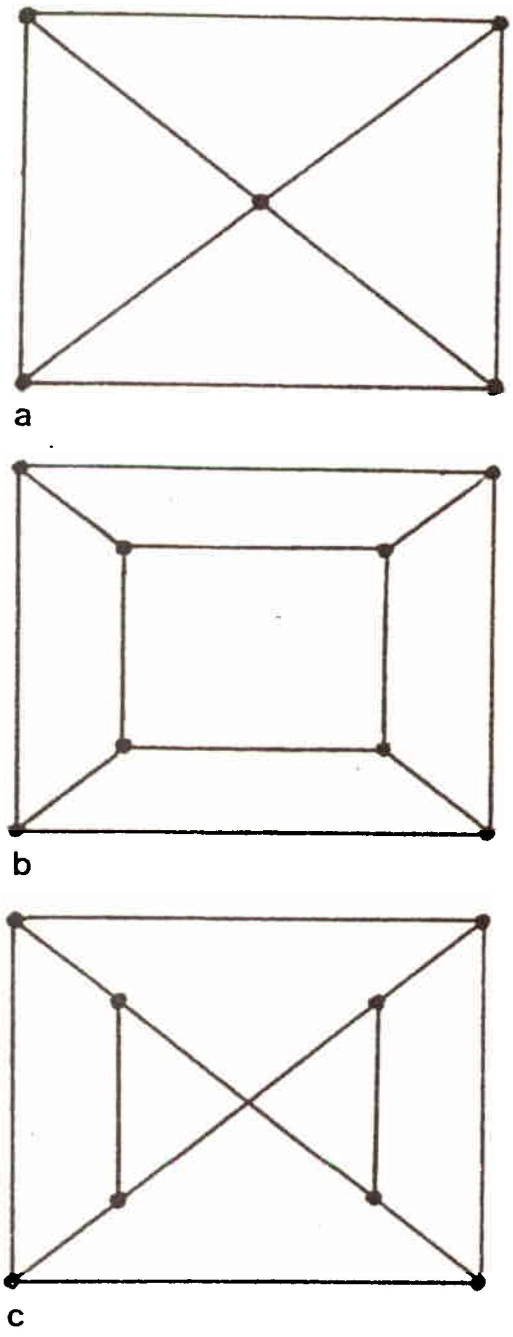

FIGURE 6

of valence at most $n - 1$, such that the group of automorphisms which stabilize Γ induces all permutations of Γ, i.e., induces symmetric group S_m on Γ. In the case that $m = n + 1$ we shall simply call them n-gadgets.

The main theorem is:

THEOREM 4. *If* (G, Γ) *is a* (m, n)*-gadget then* $m = 5$ *and* $n = 4$.

We first prove a special case. Consider the special case of a 3-gadget. In this case we use the following theorem:

Theorem 5 (Babai, Lovász) [75]. *If G is a connected graph of valence* 3 *and H is a group of automorphisms of G which leaves some edge of G fixed then H is a* 2*-group* (H *is of order* 2^m, *for some* m).

Proof. Suppose the theorem is false. Let H be as in the hypothesis of the theorem and let p divide the order of H, p an odd prime. Further, let $\langle x_0, x_1\rangle$ be the edge fixed by H and x_2 and x_3 be the other two possible neighbors of x_1. If H' is the subgroup of H which also fixes x_2 and x_3 then $[H : H'] \leqslant 2$. By our assumption that p divides $|H|$ and the fact that $[H : H'] \leqslant 2$ we have p divides $|H'|$. Using induction and the fact that G is connected, Theorem 5 is proved.

Suppose G is a 3-gadget and x_1, x_2, x_3, x_4 are distinguished nodes of G. Let H be the fixer of x_1. By attaching a new edge to x_1 (using a new vertex), H satisfies Theorem 5. But, H induces S_3 on $\{x_2, x_3, x_4\}$ by definition; therefore H is not a 2-group. This contradicts Theorem 5. Thus, 3-gadgets do not exist.

Proof of Theorem 4. We shall in fact prove something slightly stronger; namely, given a connected graph with valence n and m distinguished vertices of valence $n - 1$, say Γ, then the permutations induced on Γ cannot contain the alternating group A_{n+1}, when $n \neq 4$. The cases where $n \neq 1, 2$ are trivial; thus we can assume that $n \geqslant 3$.

Suppose the Theorem is false and (G, Γ) is a (m, n)-gadget, and $m \neq 5$ or $n \neq 4$. Since $m \neq 5$ or $n \neq 4$ we can pick an integer l such that $n \leqslant l < m$ and the alternating group A_l is a simple group (i.e. $l \neq 4$). Let $x \in \Gamma$ and $\Gamma' \subsetneq$ such that $x \notin \Gamma'$ and $|\Gamma'| = l$. Now define a subgroup H of B, the automorphism group of G, by:

$$H = \left\{\alpha \,\middle|\, \alpha \in B\left(\bigcup(\Gamma - \Gamma')\right) \text{ and } \alpha \text{ restricted to } \Gamma' \text{ is a member of } A_l\right\}.$$

We have the following two properties of H:

(1) $H(\bigcup \Gamma')$ is a normal subgroup of H;

(2) $H/H(\bigcup \Gamma') \approx A_l$.

Using only properties (1) and (2) of H, we shall construct a proper subgroup which also satisfies these properties. By induction, this is a contradiction.

Let P be a path from x to x' (some member of Γ'). Now x is fixed by H and x' is moved by H. Thus, by induction, there must exist some point y on P satisfying:

(a) the point y is fixed by H;

(b) not all neighbors of y are fixed by H;

(c) at most $n - 1$ neighbors of y are moved by H.

If Y is the set of neighbors of y then we have the following two facts:

(i) $H(\bigcup Y)$ is a proper normal subgroup of H;

(ii) $H/H(\bigcup Y) \approx K \subseteq S_{n-1}$.

We need only show that $H(\bigcup Y)$ satisfies conditions (1) and (2). The fact that $H(\bigcup Y, \bigcup \Gamma) \lhd H(\bigcup Y)$ is clear. Let $L \approx H(\bigcup Y)/H(\bigcup Y, \bigcup \Gamma)$ and consider the diagram shown in Fig. 7. The upper L follows by the second isomorphism theorem (see Rotman [65]). Now by the third isomorphism theorem (Rotman) $L \lhd A_l$. Hence $L = A_l$ or $L = I$ since A_l is simple.

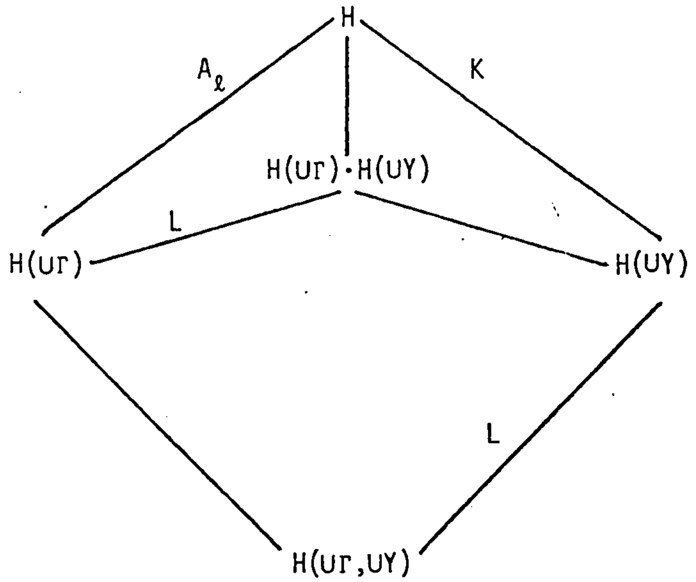

FIGURE 7

Now $|A_l| = |K| \cdot |L|$. Therefore, $(l!/2)/(n-1)! \leqslant |L|$. Since this implies $|L| > 1$ we know that $L = A_l$. Thus, $H(\bigcup Y)$ satisfies (2).

I find Theorem 4 quite surprising. What is more surprising is that 4-gadgets exist. After the presentation of this paper at the Ninth Annual ACM Symposium on the Theory of Computing, Carter found a 4-gadget. So we have:

THEOREM 6 (Carter [77]). *A 4-gadget exists.*

Using this 4-gadget and the tagging tricks developed in the previous section, we get the following corollary.

COROLLARY. *Isomorphism of graphs of valence* 5 $\leqslant_p$ *Isomorphism of graphs of valence* 4.

III. SHORT PROOFS OF NONISOMORPHISM

It is often stated that efficient graph isomorphism algorithms are useful to Chemistry since molecules can be viewed as a graph where the vertices are the atoms and edges are the bonds. A problem which arises is classifying molecules; namely, we have a very large table of molecules and we are given some new molecule and asked whether or not it is already in the list. Since the number of molecules is potentially exponential in the number of atoms per molecule, even a linear time isomorphism algorithm naively produces a potentially exponential search. We now attempt to characterize a feasible solution to the Chemist's problem.

A function f from a class of objects A to the natural numbers is called a *certificate* with respect to some equivalence relation $\equiv$ if for all G, G' in A, $G \equiv G'$ iff $f(G) = f(G')$. In the case that A is a set of incidence matrices and $\equiv$ is isomorphism, then a computable f exists since we can simply enumerate all graphs and assign a number to each graph according to when it first appeared. So the interesting question to ask of a certificate is its computational complexity. We shall say that f is a *deterministic certificate* if f is a certificate and it is computable in polynomial time.

If graph isomorphism has deterministic certificates, then graph isomorphism is in P. Thus deterministic certificates seems too strong a condition to prove existence for at the present time. If f is a certificate which is computable in nondeterministic polynomial time, then f is called a *succinct certificate.* The definition of nondeterministically computable function is given in Miller [76]. For completeness, we define it for partial functions:

DEFINITION. A function f over a domain A is said to be computable in non-deterministic polynomial time if there exists a non-deterministic machine M such that on all inputs $X \in A$ some path halts and all halting paths must output $f(X)$ in a polynomial number of steps in terms of the length of X.

The existence of a succinct certificate for graphs under isomorphism seems to formally characterize what Harary [69] calls a complete set of invariants for graphs.

OPEN QUESTION. What is the relation between the following four properties, other than (1) implies (2) implies (4) and (1) implies (3) implies (4):

(1) $\langle A, \equiv \rangle$ has deterministic certificates;

(2) equivalence of A over $\equiv$ is in P;

(3) $\langle A, \equiv \rangle$ has succinct certificates;

(4) equivalence of A over $\equiv$ is in $NP \cap \overline{NP}$?

(where $\equiv$ is an equivalence relation over a set A).

It is not known if graph isomorphism satisfies any of the above four conditions.

Since polynomial time reducibility preserves all of the conditions, a positive solution for graph isomorphism would imply a positive solution for structures. In particular, group isomorphism is not known to satisfy any of the four conditions. It seems we need to find a tractable restriction of the class of graphs so as to solve the molecular classification problem.

Before we give an example of succinct certificates we give a short discussion of certificates. Since an incidence matrix for a graph can easily be viewed as a natural number, we need only construct unique matrices, i.e., enumerations of the vertices which produce identical matrices. In general this seems difficult to find, but if we also have an embedding of the graph on some 2-dimensional orientable surface then there are enumerations dependent only on the graph and the embedding.

Suppose G is a connected graph embedded on some orientable surface. Note that an embedding can be viewed as simply a cyclic ordering of the edges incident with x, for each vertex x of G. Given an edge and a vertex x incident with it, we can induce a linear order on the remaining edges of x. Thus, given G, e and x, where G is a connected and embedded graph and e is an edge incident to vertex x, we can define an enumeration of the vertices of G starting with x, say depth first. Since the number of pairs (e, x) we need to consider is only n^2, where n is the number of vertices of G, we could compute all the incidence matrices associated with the pairs (e, x) and take the minimum where the matrices are viewed as natural numbers. Similarly, we need not assume that G is connected. Thus an embedding of a graph produces a unique incidence matrix. We have reduced the problem of finding vertex enumeration to finding unique embedding. The above arguments hold for unorientable surfaces.

Tutte [66] showed that 3-connected graphs have at most 2 embedding on the sphere. Thus many authors have noticed that isomorphism of planar 3-connected graphs is decidable in polynomial time, after finding a polynomial time planar embedding algorithms. In fact, we see that planar 3-connected graphs have deterministic certificates. In fact, Hopcroft and Tarjan [73] give an enumeration of 3-connected components. The author knows of no similar results for higher genus.

IV. Succinct Certificates for Arc Transitive Cubic Graphs

Since molecules have bounded valence and Theorem 5 gives us reason to believe graphs of bounded valence may be easier, we restrict our attention to these graphs. Valence 3 graphs are the first interesting case and by Theorem 3 we need only consider graphs of uniform valence 3, cubic graphs.

Open Question. Is cubic graph nonisomorphism in *NP*?

There are many ways of partitioning vertices of a graph into classes invariant under the automorphism group, with the goal of either finding an isomorphism or eliminating possible isomorphisms. If the automorphism group acts transitively on vertices, then the only invariance partition is the trivial one. Thus, the vertex transitive graph seems like an interesting subcase to consider. Now with one further restriction, namely that not only does the automorphism group act transitively on vertices but it also acts transitively on arcs (transitive over paths of length 1), we are able to say something interesting. Following Tutte, graphs which are arc-transitive are called symmetric.

Theorem 7. *Symmetric Cubic Graph Nonisomorphism is in NP.*

In fact, we may make a stronger statement:

Theorem 8. *Symmetric Cubic Graphs have Succinct Certificates.*

Our proofs of Theorems 7 and 8 seem to require a fair amount of group theory and algebraic graph theory. Some of Tutte's finest and least understood works [47, 59] form the basis of our argument. This general paper is not the place for a detailed proof, and we hope the diligent reader will checks the references Biggs [74], Djoković and Miller [77], Tutte [47] and Tutte [59].

It is sufficient to prove Theorems 7 and 8 for connected graphs since we can let the certificate of a graph be the order tuple of the certificates of the connected components. In general all four properties of the previous section can be reduced to the connected case. For the remainder of the proof we shall assume that the graphs are connected.

In the last section we showed that an embedding gives rise to an associated incidence matrix. Similarly we shall see that for vertex transitive graphs certain elements of the automorphism group give rise to an associated incidence matrix.

Let G be a vertex transitive graph and x be a vertex of G with adjacent vertices $x_1, \ldots, x_k$. Since G is vertex transitive there exist automorphisms $a_1, \ldots, a_k$ such that $a_1(x) = x_1, \ldots, a_k(x) = x_k$.

If H is the subgroup generated by $a_1, \ldots, a_k$ then H is vertex transitive. This statement follows by noting that if $y = f(x)$ is in the orbit of x where $f \in H$ then $fa_1(x), \ldots, fa_k(x)$ is an enumeration of the vertices adjacent to y and hence the neighbors of y are all in the orbit of x.

If H is a vertex regular group (i.e., for every pair of vertices x, y there exist a unique $f \in H$ such that $f(x) = y$) then the enumeration of the vertices with respect to $x, a_1, \ldots, a_k$ can easily be defined by the methods used for embedded graphs. Here, the ordered neighbors of y are $fa_1(x), \ldots, fa_k(x)$.

If on the other hand H is not vertex regular then we can systematically assign an automorphism to each vertex. This can be done many ways. In particular we construct a depth first search tree rooted at x which simultaneously assign an automorphism to each vertex.

Let f be an automorphism of G, x, $a_1, \ldots, a_k$ as above and let trace be a recursive procedure defined as follows:

```
Procedure trace($f, x, a_1, \ldots, a_k$)

        (1)  assign $f$ to $f(x)$ if $f(x)$ has no automorphism assigned to it; otherwise return.
        (2)  trace($fa_1, x, a_1, \ldots, a_k$)
        (3)  trace($fa_2, x, a_1, \ldots, a_k$)
          ⋮
    ($k+1$)  trace($fa_k, x, a_1, \ldots, a_k$).
```

Now, trace($I, x, a_1, \ldots, a_k$) where I is the identity automorphism defines an enumeration of the vertices of G. It is interesting to note that trace defines an ordered rooted spanning tree of G. Let $T(G, x, a_1, \ldots, a_k)$ denote the enumeration of the vertices of G induced by trace($I, x, a_1, \ldots, a_k$).

In the case when the graph is cubic and arc transitive, Tutte [47] characterized a canonical set of automorphisms which will allow us to have a canonical enumeration of these graphs. At this point we introduce the terminology to define these automorphisms.

An s-arc is a path $x_0, \ldots, x_s$ and a 1-arc is simply an arc. A graph is s-arc transitive if the automorphism group is transitive on s-arcs. A group acting on a graph is s-regular if it acts regularly on s-arcs (uniquely maps s-arcs to s-arcs). Now, Tutte proved that if a cubic graph is arc transitive then it is s-regular for some $s \leqslant 5$. Tutte also proved that there exist cubic graphs which are s-regular for $1 \leqslant s \leqslant 5$.

Suppose G is an s-regular graph and S is some s-arc, say $x_0, \ldots, x_s$, and the other two neighbors to x_s are x and y. Now, S has two unique successors, $x_1, \ldots, x_s, x$ and $x_1, \ldots, x_s, y$ which we will denote by S_1 and S_2. Let a_1 and a_2 be the unique automorphisms of S which sends S to S_1 and S_2 respectively. Automorphisms which push arcs forward are called shuntings. Tutte also proved that a_1 and a_2 in a very natural way generate the automorphism group of G.

In defining $T(G, x, a_1, \ldots, a_k)$ we used three automorphisms for cubic graphs. For arc transitive graphs we need only $k - 1$ shuntings for graphs of valence k (Tutte [66]). Thus $T(G, x_s, a_1, a_2)$ is well defined when G is cubic, s-regular and x_s, a_1, a_2 are as above.

Now if $M(G, a_1, a_2)$ is the incidence matrix induced by $T(G, x_s, a_1, a_2)$, it is independent of our choice of x_s and dependent only on the order of a_1 and a_2. That is, if $M(G, a_2, a_1)$ is the matrix induced by $T(G, x_s, a_2, a_1)$ and $M(G)$ is the minimum of $M(G, a_1, a_2)$ and $M(G, a_2, a_1)$ viewed as integers then $M(G)$ is dependent only on G. Therefore we have defined a certificate for arc transitive cubic graphs, namely, $f(G) = M(G)$. But it is not clear that f is computable in nondeterministic polynomial time. In nondeterministic polynomial time we can guess the shuntings a_1 and a_2, but we also need to recognize that G is at most s-transitive. Thus, we need to show that the set of s-regular cubic graphs is in NP for each s. A stronger fact is provable. First we formally define shuntings.

Definition. A shunting in G is an ordered pair (x, a) where x is a vertex and a is an automorphism of G such that $a(x)$ is adjacent to x and $a^2(x) \neq x$. If G is finite, then $a^i(x)$, $i \in Z$, determines a simple closed path which is rotated by a. Two shuntings (x, a), (x, b) have *overlap* s if $a^{-k}(x) = b^{-k}(x)$ for $0 \leqslant k \leqslant s$ and $a(x) \neq b(x)$, $a^{-(s+1)}(x) \neq b^{-(s+1)}(x)$. Finally, (x, a) is *conjugate* to (y, b) if there exists an automorphism α such that $(y, b) = (\alpha x, \alpha a \alpha^{-1})$. Using this notation we can show:

Theorem 9. *Given two shuntings of overlap $t \geqslant 1$ for some connected cubic graph G, then in polynomial time one can find the automorphism group of G.*

Proof. Since the automorphism group of G contains $3 \cdot 2^{s-1} \cdot n$ elements where s is the transitivity and n is the number of vertices, the size of the group is only linear in the number of vertices. Using the shuntings (x, a_1) and (x, a_2) we can construct the subgroup generated by a_1, a_2, denoted $\langle a_1, a_2 \rangle$. Now, $\langle a_1, a_2 \rangle$ is t'-regular for some $t' \leqslant 5$, by Tutte's result. If the overlap of (x, a_1) and (x, a_2), t, is strictly less than t', we can find new shuntings with overlap t' in $\langle a_1, a_2 \rangle$. Without loss of generality, we can assume that the overlap is in fact $t = t'$. Thus it is sufficient to show the following: given a t-regular subgroup of an s-regular group, for a cubic graph, we can quickly find the s-regular group. Certain of the pairs (t, s) cannot exist by the following theorem:

Theorem 10. *If a group of automorphisms for a connected cubic graph is 4- or 5-regular then it cannot contain a 2- or 3-regular subgroup.*

Proof. (See Djoković and Miller [77].)

We next consider the cases when $s = t + 1$, that is, H is the t-regular subgroup of a $t + 1$ regular group A. We show how to construct A from H. By our counting argument, the index of H in A is 2. H is a normal subgroup of A. Now there exists a unique element w in A of order 2 which fixes S. By the normality of H and the uniqueness of a_1 and a_2 in H, we have $wa_1w^{-1} = a_2$, i.e., (x, a_1) and (x, a_2) are conjugate. We can rewrite this as $wa_1 = a_2w$ and $wa_2 = a_1w$. The automorphism w is uniquely defined by

$$w(a_{i_1}, \ldots, a_{i_k}(X)) = a_{\gamma(i_1)}, \ldots, a_{\gamma(i_k)}(X)$$

where $i_j \in \{1, 2\}$ and $\gamma(1) = 2$, $\gamma(2) = 1$.

All this boils down to $M(G, a_1, a_2)$ is identical with $M(G, a_2, a_1)$.

Thus if w exists we can quickly find it; in fact, it is not hard to show that wa_1 and a_2 are two shunting functions of overlap $t + 1$.

The cases $t = 1$, $s = 3$ and $t = 1$, $s = 5$ can be handled by the following theorem:

THEOREM 11. *If H, A are 1- and 3(5)-regular groups respectively, acting on some cubic graph, then there exists a 2(4)-regular group B such that $H \leqslant B \leqslant A$.*

Proof. (See Djoković and Miller [77].)

Thus we need only deal with the case $t = 1$ and $s = 4$. The smallest 4-regular cubic graph is Heawood's graph on 14 vertices; its automorphism group contains 1-regular subgroups. We shall show that all graphs which have both a 1-regular subgroup and a 4-regular subgroup "look like" Heawood's graph. Let G be a cubic graph which is 4-transitive and let H be a 1-regular group over G. Then H contains shuntings of overlap one, say (x, a_1) and (x, a_2). Using this notation, we have the following:

THEOREM 12 (Djoković, Miller). *Given G, H, a_1 and a_2 as above, then there exists a 1-regular subgroup of Heawood's graph with shuntings (y, b_1) and (y, b_2) with overlap 1, such that the map*

$$f(a_{i_1} \cdots a_{i_k}x) = b_{i_1} \cdots b_{i_k}y$$

is a well-defined covering of G over Heawood's graph, $g(a_{i_1} \cdots a_{i_k}) = b_{i_1} \cdots b_{i_k}$ is a well-defined homomorphism from H to $\langle b_1, b_2\rangle$ and, finally, (f, g) form a covering morphism. This covering morphism allows, in a natural way, the lifting of the full automorphism group of Heawood's graph to G.

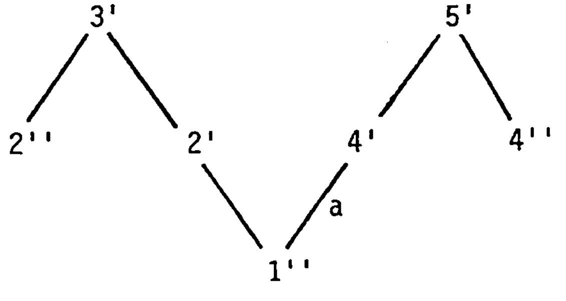

FIGURE 8

Proof. (See Djoković and Miller [77].)

Summing up, the lattice of possible regular subgroups is as shown in Fig. 8 (see Djoković and Miller [77]). Each inclusion is of index 2 except *a*. Thus we can climb up the lattice using the normality trick except for inclusion *a*. For inclusion *a* we rely on the fact that the graph is a covering of Heawood's graph.

Remark. It has been brought to the attention of the author that certain equivalent or related results appear in the literature. In particular, in Hedrlin and Pultr [66] reductions are used to prove certain algebraic reducibilities. These constructions can be used to prove Theorem 2. Using Theorems 1 and 2 of Babai and Lovász [73] and simple properties of the symmetric group one can prove Theorems 4 and 6 respectively.

Acknowledgments

It is a pleasure to thank D. Angluin, L. Carter, D. Corneil, D. Djoković, D. Kirkpatrick, L. Monk, T. Ralston, C. Thomassen, and W. Tutte for their most helpful discussions and comments.

References

1. L. Babai and L. Lovász, Permutation groups and almost regular graphs, *Studia Sci. Math. Hungar.* 8 (1973), 141–150.
2. N. Biggs, "Algebraic Graph Theory," Cambridge Univ. Press, London/New York, 1974.
3. K. S. Booth, Isomorphism testing of graphs, semisroups and finite automata are polynomially equivalent problems, *SIAM J. Comput.*, in press.
4. L. Carter, A four-gadget, *SIGACT News* 9 (1977), 36.
5. S. A. Cook, The complexity of theorem-proving procedures, *in* "Conference Record of the Third Annual ACM Symposium on the Theory of Computing, 1970, pp. 151–158.
6. A. Cobham, The intrinsic computational difficulty of functions, *in* "Proceedings of the 1964 International Congress for Logic, Methodology, and the Philosophy of Science," pp. 24–30, North–Holland, Amsterdam.
7. D. Corneil and D. Kirkpatrick, private communications.
8. D. Djoković, Automorphisms of graph and coverings, *J. Combinatorial Theory B* 16 (1974), 243–247.
9. D. Djoković, On regular graphs V, *J. Combinatorial Theory B* (1979), in press.
10. D. Djoković and G. L. Miller, "Regular Groups of Automorphisms for Cubic Graphs," Tech. Report No. 20, Computer Science Department, University of Rochester, 1977.
11. F. Harary, "Graph Theory," Addison–Wesley Reading, Mass., 1969.
12. Z. Hedrlin and A. Pultr, On full embeddings of categories of algebras, *Illinois J. Math.* 10 (1966), 392–406.
13. J. E. Hopcroft and R. E. Tarjan, Dividing a graph into triconnected components, *SIAM J. Comput.* 2 (1973), 135–158.
14. R. M. Karp, Reducibility among combinatorial problems, *in* "Complexity of Computer Computations" (R. E. Miller and J. W. Thatcher, Eds.), Plenum, New York, 1972.
15. G. L. Miller, Riemann's hypothesis and test for primality, *J. Comput. System Sci.* 13 (1976).
16. G. L. Miller, On the $n^{\log n}$ isomorphism technique, *in* "Conference Record of the 10th Annual ACM Symposium on the Theory of Computing, 1978, pp. 51–58.
17. J. J. Rotman, "The Theory of Groups: An Introduction," Allyn & Bacon, Boston, 1965.
18. W. T. Tutte, A family of cubical graphs, *Proc. Cambridge Philos. Soc.* 43 (1947), 459–474.
19. W. T. Tutte, On the symmetry of cubic graphs, *Canad. J. Math.* 11 (1959), 621–624.
20. W. T. Tutte, "Connectivity in Graphs," Univ. of Toronto Press, Toronto, 1966.

Printed by the St. Catherine Press Ltd., Tempelhof 37, Bruges, Belgium