INFORMATIQUE THÉORIQUE ET APPLICATIONS

P. GORALČÍK
A. GORALČÍKOVÁ
V. KOUBEK

How much semigroup structure is needed to encode graphs ?

Informatique théorique et applications, tome 20, n° 2 (1986), p. 191-206

<http://www.numdam.org/item?id=ITA_1986__20_2_191_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 20, n° 2, 1986, p. 191 à 206)

HOW MUCH SEMIGROUP STRUCTURE IS NEEDED TO ENCODE GRAPHS? (*)

by P. GORALČÍK (1), A. GORALČÍKOVÁ (1), V. KOUBEK (1)

Communicated by J.-E. PIN

Abstract. – *A class of finite semigroups is called a variety if it is closed under taking finite cartesian products, subsemigroups, and homomorphic images. Ordered by inclusion, the varieties of finite semigroups form a complete lattice. The problem of testing graph isomorphism can be polynomially reduced to the problem of testing for isomorphism of two semigroups belonging to a rather small variety, e.g., the variety of all finite semilattices. A variety $\mathcal{V}$ is called critical if it is isomorphism complete and every variety $\mathcal{W}$ properly contained in $\mathcal{V}$ has a polynomial time isomorphism algorithm. Under the conjecture that the finite groups do not form an isomorphism complete variety, we enumerate all critical varieties of finite semigroups and show that if a variety $\mathcal{V}$ includes no critical one then it has a subexponential, i.e., $O(n^{c_1 \log n + c_2})$ time isomorphism algorithm.*

Résumé. – *On appelle ici variété une classe de semigroupes finis, fermée par produits finis, sous-semigroupes et images homomorphes. Ordonnées par l'inclusion, les variétés de semigroupes finis forment un treillis complet. Le test d'isomorphisme pour les graphes admet une réduction polynômiale au test d'isomorphisme pour les semigroupes appartenant à des variétés relativement petites, par exemple les demitreillis. Appelons critique une variété $\mathcal{V}$ dont le problème d'isomorphisme est polynômialement équivalent au problème d'isomorphisme pour les graphes, tandis que chaque sous-variété $\mathcal{W}$ propre de $\mathcal{V}$ admet un algorithme décidant l'isomorphisme dans un temps polynômial. Sous l'hypothèse que le problème d'isomorphisme pour les groupes finis n'est pas polynômialement equivalent à celui pour les graphes, nous donnons la liste de toutes les variétés critiques de semigroupes finis. Quant aux variétés ne contenant aucune variété critique, nous démontrons qu'elles admettent un algorithme d'isomorphisme sous-expenentiel, c'est-à-dire en temps $O(n^{c_1 \log n + c_2})$.*

0. INTRODUCTION

Among various classes listed in [3] as isomorphism complete we find the class of all finite semigroups. This means that every graph (V, E) can be encoded, in time polynomial in $|V|$, as a semigroup $S(V, E)$ uniquely determi-

(*) Received in February 1985, revised in October 1985.
(1) Faculty of Mathematics and Physics, Charles University, Sokolovska 83, 18600 Praha 8, Czechoslovakia.

informatique théorique et Applications/Theoretical Informatics and Applications
0296-1598/ 86/02 191 16/$3.60/

ning (V, E) up to isomorphism. The first such encoding due to Booth [2] defines $S(V, E)$ as a semigroup on $V \cup E \cup \{0\}$ with the multplication

$$xy = yx = \begin{cases} x & \text{if } x = y, \\ y & \text{if } x \in y \in E, \\ \{x, y\} & \text{if } \{x, y\} \in E, \\ 0 & \text{otherwise} \end{cases}$$

We see that $S(V, E)$ is commutative and idempotent, that is to say, a semilattice. Booth's encoding actually shows that the class of all finite semilattices is isomorphism complete.

Let $\mathscr{S}$ denote throughout the class of all finite semigroups. In a very definite sense, the semilattices in $\mathscr{S}$ represent a rather limited amount of semigroup structure. Let us agree that we represent the "structural richness" of a class $\mathscr{X} \subseteq \mathscr{S}$ by the class $\mathrm{Str}(\mathscr{X}) \subseteq \mathscr{S}$ of all semigroups constructible from those in $\mathscr{X}$ in a finite sequence of steps, each step consisting in taking a finite cartesian product, a subsemigroup, or a homomorphic image of either some semigroups in $\mathscr{X}$ or those constructed on previous steps. Then we are in a position to compare the "amounts of structure' carried by any two classes $\mathscr{X}$, $\mathscr{Y}$ of finite semigroups: $\mathscr{X}$ carries less or at most as much structure as $\mathscr{Y}$ iff $\mathrm{Str}(\mathscr{X}) \subseteq \mathrm{Str}(\mathscr{Y})$.

For every $\mathscr{X} \subseteq \mathscr{S}$, $\mathrm{Str}(\mathscr{X})$ is what S. Eilenberg [5] calls a *variety:* a class $\mathscr{V} \subseteq \mathscr{S}$ closed under taking finite products, subsemigroups, and homomorphic images.

Typical examples of varieties are the so called equational classes of finite semigroups. To describe them, recall that a semigroup identity (or equation) is any pair (u, v) of words in a free semigroup X^+ over a fixed countably inifnite set X of variables. A semigroup S is said to satisfy an identity (u, v), written $S \models u = v$, if for every homomorphism $f: X^+ \to S$ we have $f(u) = f(v)$. Likewise, given a set Σ of semigroup identities, a semigroup S satisfies Σ, $S \models \Sigma$, if $S \models u = v$ for every $(u, v) \in \Sigma$. We denote $\mathrm{Mod}(\Sigma) = \{S \in \mathscr{S} \mid S \models \Sigma\}$. Now, a class $\mathscr{X} \subseteq \mathscr{S}$ is an equational class if there exists a set Σ of semigroup identities such that $\mathscr{X} = \mathrm{Mod}(\Sigma)$. The class of all finite semilattices is equational, determined by the identities $xy = yx$, $x^2 = x$. Not all varieties are, however, equational. For example, the variety $\mathscr{G}$ of all finite groups or the variety $\mathscr{N}$ of all finite nil semigroups (a semigroup is nil if it has a zero 0 and for every $x \in S$ there exists an integer $k > 0$ such that $x^k = 0$) does not satisfy any equation which is not satisfied by all semigroups.

It is routine to see that varieties of finite semigroups form a closure system, thus a complete lattice under inclusion: the intersection of an arbitrary collection of varieties is again a variety, the infimum of the collection. Every class $\mathscr{X} \subseteq \mathscr{S}$ is represented by the least variety $\mathrm{Str}(\mathscr{X})$ including it, as an element in the lattice of varieties, the latter playing a role of a structural hierarchy.

Let us ask how far down along this structural hiearchy one can go without loosing the isomorphism completeness. We may ask, in particular, if it is possible to determine the minimal isomorphism complete varieties, that is to say, the minimum "amounts of semigroup structure" needed for a polynomial time encoding of graphs into semigroups.

The complexity of graph isomorphism being unresolved, we are in a position only to mark out, among semigroup varieties, the potential candidates for minimal isomorphism complete varieties. Let us call a variety $\mathscr{V}$ *critical* if $\mathscr{V}$ itself is isomorphism complete but any variety $\mathscr{W}$ properly included in $\mathscr{V}$ has a polynomial time isomorphism algorithm. This notion is implicit in and has been taken by us from Kučera and Trnková [6, 7] who have described the critical members in the lattice of equational classes of finite unary algebras.

We conjecture that the finite groups do not form an isomorphism complete class, on the basis of a simple observation that the testing of isomorphism for groups requires a subexponential time (since a group of order n has a set of $\log n$ generators) while there is nothing yet to promise subexponential time for graph isomorphism. Under this conjecture, we enumerate all critical semigroup varieties and show that if a variety $\mathscr{V}$ includes no critical one then the isomorphism testing in $\mathscr{V}$ can be done by a subexponential, i.e. $O(n^{c_1 \log n + c_2})$ time algorithm. The gap between the subexponential time and the best known estimates for graph isomorphism due to Babai [1] leaves a margin for the conjecture that our critical varieties coincide with the minimal isomorphism complete varieties of finite semigroups.

The results of this paper were presented at the ICALP'82.

We want to thank the referees for valuable remarks.

1. VARIETIES OF FINITE SEMIGROUPS

In this paper we deal only with finite semigroups. For the reader's convenience, we start with a brief survey of some basic facts about finite semigroups needed in the sequel. For proofs and additional information see [4].

Let S be a finite semigroup. Given two subsets A, $B \subseteq S$, we denote $AB = \{ s \in S \mid s = ab$ for some $a \in A$ and $b \in B \}$. In particular, S^2 will always denote the subset SS of S and is not to be confused with the cartesian product $S \times S$. The index of an element $s \in S$ is the smallest positive integer i such that $s^{i+k} = s^i$, for some $k > 0$. The cyclic subsemigroup generated by $s \in S$ will be denoted by $\langle s \rangle$. By $E(S) = \{ e \in S \mid e^2 = e \}$ we denote the set of idempotents of S. The cartesian product $X \times Y$ of two sets is called a rectangular band whenever we think of it as a semigroup with the multiplication $(x, y)(u, v) = (x, v)$. An idempotent $e \in E(S)$ is an identity of S if $es = se = s$ for all $s \in S$, a zero of S if $es = se = e$ for all $s \in S$. S is a group if it has a unique idempotent $1 \in S$ and the idempotent is an identity of S. S is a nil semigroup if it has a unique idempotent $0 \in S$ and the idempotent is a zero of S. A subset $A \subseteq S$ is an ideal of S if both $SA \subseteq A$ and $AS \subseteq A$. For a non-void ideal A of S, the Rees quotient S/A is the quotient of S by the congruence on S generated by $A \times A$. The corresponding canonical homomorphism $S \to S/A : s \mapsto s/A$ is injective on $S - A$ and takes A to the zero of S/A. The intersection of all non-void ideals of S, called the kernel of S, will be denoted by $K(S)$. $K(S)$ is a union of mutually isomorphic groups of the form eSe, $e \in K(S) \cap E(S)$. We denote by $G(S)$ and call the Suškevič group of S any group isomorphic with them. If $G(S)$ is not trivial then the Suškevič groups contained in $K(S)$ are the non-trivial blocks of a congruence on S, which we call the Suškevič congruence and denote by σ_S. S is a simple semigroup, or a kernel, if $S = K(S)$, or equivalently, if $SsS = S$ for every $s \in S$.

Let be given a group G, two finite sets X and Y, and a mapping $P : Y \times X \to G : (y, x) \mapsto p_{yx}$. Defining a multiplication on $G \times X \times Y$ by $(a, x, y)(b, u, v) = (ap_{yu}b, x, v)$ we get a simple semigroup, the so called Rees matrix semigroup $\mathcal{M}(G, X, Y, P)$ with the structure group G and the sandwich matrix P. The quotient of $\mathcal{M}(G, X, Y, P)$ by the Suškevič congruence is isomorphic to the rectangular band $X \times Y$. Every simple semigroup K is isomorphic to some Rees matrix semigroup and the latter can be computed from K in time polynomial in $|K|$. Two Rees matrix semigroups $\mathcal{M}(G, X, Y, P)$ and $\mathcal{M}(G, X, Y, P')$, differing at most by their sandwich matrices, are isomorphic iff there exist bijections $f : X \to X$, $g : Y \to Y$, mappings $c : X \to G$, $r : Y \to G$, and an automorphism $h : G \to G$ such that $p'_{g(y)\, f(x)} = r(y)\, h(p_{yx})\, c(x)$. We then say that the sandwich matrices P and P' are equivalent. In case $X = \{1, \ldots, m\}$ and $Y = \{1, \ldots, n\}$ we write $\mathcal{M}(G, m, n, P)$ instead of $\mathcal{M}(G, X, Y, P)$ and present P as an array of n rows and m columns.

We now focus our attention on semigroup varieties.

The class $\mathscr{S}$ of all finite semigroups is our largest variety. Given $\mathscr{X} \subseteqq \mathscr{S}$, we can form every semigroup S in $\mathrm{Str}(\mathscr{X})$ in three steps:

STATEMENT 1 : We have $S \in \mathrm{Str}(\mathscr{X})$, for $\mathscr{X} \subseteqq \mathscr{S}$, iff S is a homomorphic image of a subsemigroup T of a product $S_1 \times \ldots \times S_m$ of a finite family $S_1, \ldots, S_m$ in $\mathscr{X}$, written

$$S \twoheadleftarrow T \subsetneq S_1 \times \ldots \times S_m.$$

Proof: Straightforward.

We say that a semigroup S is separated by homomorphisms to $\mathscr{X} \subseteqq \mathscr{S}$ if for any two distinct $x, y \in S$ there exists a homomorphism $h: S \to T$ with $T \in \mathscr{X}$ and $h(x) \neq h(y)$.

STATEMENT 2: Let $\mathscr{X} \subseteqq \mathscr{S}$. If a semigroup S is separated by homomorphisms to $\mathscr{X}$ then $S \in \mathrm{Str}(\mathscr{X})$.

Proof: The separation can be done by a finite family of homomorphisms $h_i: S \to T_i \in \mathscr{X}$, $i = 1, \ldots, m$. The family defines an embedding

$$S \subsetneq T_1 \times \ldots \times T_m : S \mapsto (h_1(s), \ldots, h_m(s))$$

For $\mathscr{X} \subseteqq \mathscr{S}$, let $\sqrt{\mathscr{X}}$ denote the class of all semigroups S with $S^2 \in \mathscr{X}$.

STATEMENT 3: For any variety $\mathscr{V}$, $\sqrt{\mathscr{V}}$ is again a variety and $\mathscr{V} \subseteqq \sqrt{\mathscr{V}}$.

Proof: Let $S \twoheadleftarrow T \subsetneq S_1 \times \ldots \times S_m$ for $S_1, \ldots, S_m \in \sqrt{\mathscr{V}}$. Then $S^2 \twoheadleftarrow T^2 \subsetneq (S_1 \times \ldots \times S_m)^2 = S_1^2 \times \ldots S_m^2$.

Given two varieties $\mathscr{V}$, $\mathscr{W} \subseteqq \mathscr{S}$, we denote by $\mathscr{V}\mathscr{W}$ their intersection and by $\mathscr{V} \vee \mathscr{W}$ their join, $\mathscr{V} \vee \mathscr{W} = \mathrm{Str}(\mathscr{V} \cup \mathscr{W})$.

STATEMENT 4: For any two varieties $\mathscr{V}$, $\mathscr{W} \subseteqq \mathscr{S}$, we have $S \in \mathscr{V} \vee \mathscr{W}$ iff S is a quotient of a subsemigroup T of a product $V \times W$ of a semigroup $V \in \mathscr{V}$ and a semigroup $W \in \mathscr{W}$, $S \twoheadleftarrow T \subsetneq V \times W$.

Proof: By Statement 1.

A variety $\mathscr{V}$ is covered by a variety $\mathscr{W}$ if $\mathscr{V} \subseteqq \mathscr{W}$ and there is no variety properly included between $\mathscr{V}$ and $\mathscr{W}$, that is to say, for every variety $\mathscr{U}$, if $\mathscr{V} \subseteqq \mathscr{U} \subseteqq \mathscr{W}$ then either $\mathscr{U} = \mathscr{V}$ or $\mathscr{U} = \mathscr{W}$. We then also say that $\mathscr{W}$ is a cover of $\mathscr{V}$. We call a $\mathscr{V}$-variety every subvariety of a variety $\mathscr{V}$.

Let us now briefly describe some varieties closely related to our subject.

$\mathscr{T} = \mathrm{Mod}(x = y)$, the trivial variety; it contains only one-point and empty semigroups, it is the least variety, its covers are called atomic varieties;

$\mathscr{K}$, the variety of kernels or simple semigroups;

$\mathscr{G}$, the variety of groups;

$\mathscr{N}$, the variety of nil semigroups;

$\mathscr{B} = \mathrm{Mod}(x^2 = x)$, the variety of bands or idempotent semigroups;

$\mathscr{C} = \mathrm{Mod}(xy = yx)$, the variety of commutative semigroups;

$\mathscr{CB} = \mathrm{Mod}(x^2 = x,\ xy = yx)$, the variety of commutative bands or semilattices;

$\mathscr{L} = \mathrm{Mod}(xy = x)$, the variety of left zero semigroups; it is atomic;

$\mathscr{R} = \mathrm{Mod}(xy = y)$, the variety of right zero semigroups; it is atomic;

$\mathscr{L} \vee \mathscr{R}$, the variety of rectangular bands;

$\mathscr{G} \vee \mathscr{L}$, the variety of left groups;

$\mathscr{G} \vee \mathscr{R}$, the variety of right groups;

$\mathscr{G} \vee \mathscr{L} \vee \mathscr{R}$, the variety of rectangular groups;

$\mathscr{I} = \mathrm{Mod}(xy = zt)$, the inflationary variety; it is atomic;

$\mathscr{I} \vee \mathscr{L} \vee \mathscr{G}$, the variety of inflations of left groups;

$\mathscr{I} \vee \mathscr{R} \vee \mathscr{G}$, the variety of inflations of right groups.

For every prime p, let C_p denote a cyclic group of order p. Let 1 denote the identity of C_p, let $a \in C_p$ be an arbitrary element distinct from 1, and let

$$K_p = \mathscr{M}\left(C_p,\ 2,2,\ \begin{pmatrix} a1 \\ 11 \end{pmatrix}\right).$$

Let M denote the semigroup given by the multiplication table

	a	b	c	0
a	0	c	0	0
b	c	0	0	0
c	0	0	0	0
0	0	0	0	0

$\mathscr{E}_p = \mathrm{Str}(C_p)$, the variety of abelian groups of exponent p;

$\mathscr{K}_p = \mathrm{Str}(K_p)$;

$\mathscr{M} = \mathrm{Str}(\mathrm{M})$. (Note that $\mathscr{M} = \mathrm{Mod}(xy = yx,\ xyz = x^2 = x^2 u)$.)

STATEMENT 5: $\mathscr{CB} = \mathrm{Str}(D)$, where $D = \{0, 1\}$ is a two-point semilattice with identity 1 and zero 0. $\mathscr{CB}$ is atomic.

Proof: We have $D \in \mathscr{CB}$, thus $\mathrm{Str}(D) \subseteqq \mathscr{CB}$. Conversely, if $S \in \mathscr{CB} - \mathscr{I}$ then define for every $a \in S$ a mapping $h_a : S \to D$ by

$$h_a(s) = \begin{cases} 1 & \text{if } as = a, \\ 0 & \text{if } as \neq a. \end{cases}$$

This mapping is a homomorphism since we have $h_a(st)=1$ iff $ast=a$, which is equivalent to $as=a=at$ and this to $h_a(s)h_a(t)=1$. Homomorphisms h_a, $a\in S$, separate S. Indeed, let $x, y\in S$ and assume that $h_a(x)=h_a(y)$ for all $a\in S$. Then $h_x(y)=h_x(x)=1$ and $h_y(x)=h_y(y)=1$, thus $x=xy=yx=y$. By Statement 2, $S\in \mathrm{Str}(D)$, thus we have $\mathscr{CB}\subseteq \mathrm{Str}(\mathrm{D})$. Any non-trivial variety included in $\mathscr{CB}$ contains D thus $\mathscr{CB}$ is atomic.

STATEMENT 6: $\mathscr{M}$ is the unique nil cover of $\mathscr{I}$.

Proof: We assume that $S\in\mathscr{N}-\mathscr{I}$ and show that $\mathrm{M}\in\mathrm{Str}(S)$. If there is some $s\in S$ with $s^2\neq 0$ then $T=\langle s\rangle/\{s^k \mid k\geq 3\}$ is in $\mathrm{Str}(S)$, $T=\{s, s^2, 0\}$. The power $T\times T\times T$ contains the subsemigroup

$$\{(s, s^2, s), (s, s, s^2), (s^2, 0, 0), (s^2, 0, s^2), (s^2, s^2, 0), (0, 0, 0)\}$$

whose quotient obtained by the identification of $(s^2, 0, s^2)$ and $(s^2, s^2, 0)$ with $(0, 0, 0)$ is isomorphic to M, thus $M\in\mathrm{Str}(S)$.

Assume that $s^2=0$ for all $s\in S$. Since $S\notin\mathscr{I}$, there exist distinct $s, t\in S$ with $st\neq 0$. If $st=ts$ then S contains the subsemigroup $\{s, t, st, 0\}$ isomorphic to M. If $st\neq ts$ then we have in S the subsemigroup $\{s, t, st, ts, sts, tst, 0\}$. Identifying ts, sts, and tst with 0 we obtain P whose square $P\times P$ contains the subsemigroup $\{(s, t), (t, s), (st, 0), (0, st), (0, 0)\}$ and this can be made into a copy of M by identifying $(0, st)$ with $(st, 0)$. We have again $M\in\mathrm{Str}(S)$.

STATEMENT 7: Let $\mathscr{V}\subseteq\mathscr{S}$ be an arbitrary variety. If $\mathscr{I}$ is not included in $\mathscr{V}$ then $\mathscr{I}\vee\mathscr{V}$ covers only $\mathscr{V}$ and $\mathscr{I}\vee\mathscr{U}$ for the varieties $\mathscr{U}$ covered by $\mathscr{V}$.

Proof: Note first that if $\mathscr{I}\not\subseteq\mathscr{V}$ then the cyclic subsemigroups of any $V\in\mathscr{V}$ must be cyclic groups. Consequently, for every such $V\in\mathscr{V}$, we can find an integer $r\geq 2$ such that $v^r=v$ for all $v\in V$. If now $S\in\mathscr{I}\vee\mathscr{V}$, say $S\leftarrow T\hookrightarrow I\times V$, $I\in\mathscr{I}$, then S has an inflation endomorphism f onto S^2 defined by $f(s)=s^r$. This shows that every $S\in\mathscr{I}\vee\mathscr{V}$ is an inflation of S^2, and clearly, $S^2\in\mathscr{V}$. Put otherwise, for every subvariety $\mathscr{U}$ of $\mathscr{I}\vee\mathscr{V}$, the class $\mathscr{U}^2=\{S^2 \mid S\in\mathscr{U}\}$ is a subvariety of $\mathscr{V}$ and we have either $\mathscr{U}=\mathscr{U}^2$ or $\mathscr{U}=\mathscr{I}\vee\mathscr{U}^2$. It follows that if $\mathscr{U}$ is covered by $\mathscr{I}\vee\mathscr{V}$ then $\mathscr{U}=\mathscr{V}$ or $\mathscr{U}=\mathscr{I}\vee\mathscr{U}^2$ where $\mathscr{U}^2$ is covered by $\mathscr{V}$.

STATEMENT 8: Let $S\in\sqrt{\mathscr{L}\vee\mathscr{G}}-\mathscr{I}\vee\mathscr{L}\vee\mathscr{G}$. Then the Suškevič quotient $S/\sigma_S\in\sqrt{\mathscr{L}}-\mathscr{I}\vee\mathscr{L}$.

Proof: It is easily verified that $I\times L\models xy=x^2$ for any $I\in\mathscr{I}$ and $L\in\mathscr{L}$, therefore $\mathscr{I}\vee\mathscr{L}\models xy=x^2$. Assume that $S/\sigma_S\in\mathscr{I}\vee\mathscr{L}$. Then $st/\sigma_S=s^2/\sigma_S$ for every $s, t\in S$. Let $m=|G(S)|$. Then $s^m\in E(S)$ and $s^{m+1}=s$ for every $s\in K(S)=S^2$. Therefore, $(s, t)\in\sigma_S$ iff $s, t\in K(S)$ and $s^m=t^m$. The equality

$st/\sigma_S = s^2/\sigma_S$ for any $s, t \in S$ then means that $S \models (xy)^m = x^{2m}$. Since $E(S) \in \mathscr{L}$, we have $s^{2m} t^{2m} = (s^{2m})^2$ for any $s, t \in S$. It follows that $(st)^{2m+1} = s^{2m} s^{2m} st = ss^{2m} t^{2m} t = s^{2m+1} t^{2m+1}$. The assignment $s \mapsto (s/S^2, s^{2m+1})$ defines an injective homomorphism of S into $S/S^2 \times K(S) \in \mathscr{I} \vee \mathscr{L} \vee \mathscr{G}$, a contradiction. Clearly, if $S \in \sqrt{\mathscr{L} \vee \mathscr{G}}$ then $S/\sigma_S \in \sqrt{\mathscr{L}}$.

STATEMENT 9: $\sqrt{\mathscr{L}}$ covers only $\mathscr{I} \vee \mathscr{L}$ and $\sqrt{\mathscr{L}} = \mathrm{Mod}(xyz = xy)$.

Proof: If $S \in \sqrt{\mathscr{L}}$, that is to say, $S^2 \in \mathscr{L}$, then for any $s, t, u \in S$ we have $st \in E(S)$, $stu \in E(S)$, therefore $stu = ststu = st$, which means that $S \models xyz = xy$. On the other hand, if $S \models xyz = xy$ then clearly $S^2 \in \mathscr{L}$.

We show that $\sqrt{\mathscr{L}}$ covers only $\mathscr{I} \vee \mathscr{L}$. Let $S \in \sqrt{\mathscr{L}} - \mathscr{I} \vee \mathscr{L}$. Then by Statement 8, $S \not\models xy = x^2$, thus we can find $a, u \in S$ such that $au \neq a^2$. Denote $b = a^2$, $c = au$, $d = u^2$. We show that a, b, c, d are pairwise distinct, by showing that any assumption of equality contradicts to $au \neq a^2$:

$$
\begin{aligned}
a = b &\Rightarrow a = a^2 \Rightarrow au = a^2 u = a^2, \\
a = c &\Rightarrow a = au \Rightarrow au = aua = a^2, \\
a = d &\Rightarrow a = u^2 \Rightarrow a^2 = au^2 = au, \\
b = c &\Rightarrow a^2 = au, \\
b = d &\Rightarrow a^2 = u^2 \Rightarrow a^2 = a^3 = au^2 = au, \\
c = d &\Rightarrow au = u^2 \Rightarrow a^2 = a^2 u = au^2 = au.
\end{aligned}
$$

The four elements form a subsemigroup Q of S, given by the table

	a	b	c	d
a	b	b	b	c
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

It remains to show that $\sqrt{\mathscr{L}} = \mathrm{Str}(Q)$. Let $S \in \sqrt{\mathscr{L}}$, $|S| = n \geqq 2$. Take an alphabet X with $|X| = n$ and define a semigroup F_X on the set $X \cup X \times X$ of words over X of length one and two, in such a way that elements in $X \times X$ are left zeros of F_X. An arbitrary bijection $f: X \to S$ can be extended to a homomorphism $\bar{f}: F_X \to S$ by setting $\bar{f}(xy) = f(x) f(y)$ for any $xy \in X^2$, thus $S \in \mathrm{Str}(F_X)$. We prove that $F_X \in \mathrm{Str}(Q)$ by showing that F_X is separated by homomorphisms to $Q \times Q$.

For $(x, y) \in X \times X$, $x \neq y$, let $\bar{h}_{xy}: F_X \to Q \times Q$ be a homomorphism such that for every $z \in X$

$$h_{xy}(z) = \begin{cases} (a, d) & \text{if } z = x, \\ (d, a) & \text{if } z = y, \\ (b, b) & \text{if } x \neq z \neq y. \end{cases}$$

This homomorphism takes injectively the subsemigroup F_{xy} of F_X generated by x, y, $F_{xy} = \{x, y, xy, yx, x^2, y^2\}$ to the subsemigroup $\{(a, d), (d, a), (c, d), (d, c), (b, d), (d, b)\}$ of $Q \times Q$. Each word of the form z, z^2, zx, zy with $z \in X - \{x, y\}$ is separated by $\bar{h}_{xy}$ from all other words in F_{xy}. Only xz is collapsed with x^2 and yz with y^2. However, these can be separated by $\bar{g}_{xy}: F_X \to Q \times Q$ defined by

$$g_{xy}(z) = \begin{cases} (a, d) & \text{if } z = x, \\ (d, a) & \text{if } z = y, \\ (d, d) & \text{if } x \neq z \neq y \end{cases}$$

for $z \in X$.

STATEMENT 10. — $S \in \mathscr{K} - \mathscr{G} \vee \mathscr{L} \vee \mathscr{R}$ iff $K_p \in \mathrm{Str}(S)$ for a prime p.

Proof: Let $S = \mathscr{M}(G, X, Y, P)$. It is easy to obtain, by a suitable choice of $r(y)$ and $c(x)$, an equivalent sandwich matrix P' with all entries in the last row and the last column equal to 1, the identity of G. Now, $S \notin \mathscr{G} \vee \mathscr{L} \vee \mathscr{R}$ is equivalent to the existence of an entry $b \neq 1$ in P'. Therefore, we have

$$\mathscr{M}\left(C_p, 2,2, \begin{pmatrix} a & 1 \\ 1 & 1 \end{pmatrix}\right) \twoheadleftarrow \mathscr{M}\left(\langle b \rangle, 2,2, \begin{pmatrix} b & 1 \\ 1 & 1 \end{pmatrix}\right) \subsetneq \mathscr{M}(G, X, Y, P) \text{ for any}$$

prime p dividing the period of b.

STATEMENT 11: $S \in (\mathscr{I} \vee \mathscr{L} \vee \mathscr{G}) \cup (\mathscr{I} \vee \mathscr{R} \vee \mathscr{G}) \cup (\mathscr{L} \vee \mathscr{R} \vee \mathscr{G})$ iff $\mathrm{Str}(S)$ does not include any of the varieties $\mathscr{CB}$, $\mathscr{M}$, $\sqrt{\mathscr{L}}$, $\sqrt{\mathscr{R}}$, $\mathscr{I} \vee \mathscr{L} \vee \mathscr{R}$, and $\mathscr{K}_p$ for p prime.

Proof: It is clear that none of the varieties listed is included in $\mathscr{I} \vee \mathscr{L} \vee \mathscr{G}$ or $\mathscr{I} \vee \mathscr{R} \vee \mathscr{G}$ or $\mathscr{L} \vee \mathscr{R} \vee \mathscr{G}$, thus neither in $\mathrm{Str}(S)$ for any

$$S \in (\mathscr{I} \vee \mathscr{L} \vee \mathscr{G}) \cup (\mathscr{I} \vee \mathscr{R} \vee \mathscr{G}) \cup (\mathscr{L} \vee \mathscr{R} \vee \mathscr{G}).$$

Let $S \notin (\mathscr{I} \vee \mathscr{L} \vee \mathscr{G}) \cup (\mathscr{I} \vee \mathscr{R} \vee \mathscr{G}) \cup (\mathscr{L} \vee \mathscr{R} \vee \mathscr{G})$.

If $S^2 \neq K(S)$ then either $S/K(S)$ contains an idempotent distinct from 0 and by Statement 5, $\mathscr{CB}\,\mathrm{Str}(S)$, or $S/K(S) \in \mathscr{N} - \mathscr{I}$ and by Statement 6, $\mathscr{M} \subseteq \mathrm{Str}(S)$.

If $S \neq S^2 = K(S)$ then either $\mathscr{I} \vee \mathscr{L} \vee \mathscr{R} \subseteq \mathrm{Str}(S)$ or $K(S) \in (\mathscr{L} \vee \mathscr{G}) \cup (\mathscr{R} \vee \mathscr{G})$. Let, say, $K(S) \in \mathscr{L} \vee \mathscr{G}$. Then we have

$S \in \sqrt{\mathscr{L} \vee \mathscr{G}} - \mathscr{I} \vee \mathscr{L} \vee \mathscr{G}$, therefore by Statement 8, the Suškevič quotient $S/\sigma_S \in \sqrt{\mathscr{L}} - \mathscr{I} \vee \mathscr{L}$, hence by Statement 9, $\sqrt{\mathscr{L}} \subseteq \mathrm{Str}(S)$.

If $S = S^2 = K(S)$, then $S \in \mathscr{K} - (\mathscr{L} \vee \mathscr{R} \vee \mathscr{G})$, therefore by Statement 10, $\mathscr{K}_p \subseteq \mathrm{Str}(S)$ for some prime p.

2. CRITICAL VARIETIES AND THE SUBEXPONENTIAL CLASS

When we want to prove that a variety $\mathscr{V}$ is critical, we must:

– find a polynomial-time encoding of some isomorphism complete class of graphs or directed graphs into $\mathscr{V}$;

– prove that any variety $\mathscr{W}$ properly included in $\mathscr{V}$ has a polynomial-time isomorphism algorithm.

Recall that an assignment $(V, E) \mapsto S(V, E) \in \mathscr{V}$ is an encoding of some class $\mathbb{G}$ of graphs into $\mathscr{V}$ if for every (V, E), $(V', E') \in \mathbb{G}$ we have $(V, E) \simeq (V', E')$ iff $S(V, E) \simeq S(V', E')$, or equivalently, iff we are able to recover an isomorphic copy of (V, E) from a semigroup S isomorphic to $S(V, E)$. The encoding is a polynomial-time encoding if we can compute the multiplication table of $S(V, E)$ from (V, E) in time polynomial in $|V|$. For each encoding in this section it will be clear from its description that it can be done in polynomial time.

DEFINITION Let $D(5, 2)$ denote the class of all directed graphs (X, R) with the following properties:

(i) X can be partitioned into two parts X_1 and X_2 in such a way that $R \subseteq X_1 \times X_2$;

(ii) for some integer d such that $5 < d < (1/3)|X|$, the outdegrees of all points in X_1 and the indegrees of all points in X_2 are equal to d;

(iii) for every $x \in X_i$, $i = 1, 2$, there exists $y \in X_i$ such that

$$|\{z \mid (x, z), (y, z) \in R \text{ or } (z, x), (z, y) \in R\}| \leqq 2,$$

i. e. there are at most two points adjacent with both x and y.

STATEMENT 12: $D(5,2)$ is isomorphism complete.

Proof: Let (V, E) be a connected d-regular graph with $|V| = n$, $n - 1 > d > 5$, $V = \{v_1, \ldots, v_n\}$. Construct a directed graph (X, R) with points x_{ij}, x'_{ij} for $i, j = 1, \ldots, n$, and arcs (x_{ij}, x'_{ik}) for all $i, j, k = 1, \ldots, n$ and (x_{ik}, x'_{jk}), (x_{jk}, x'_{ik}) for all $k = 1, \ldots, n$ and $\{v_i, v_j\} \in E$. The graph is bipartite, the outdegree of x_{ij} is equal to the indegree of x'_{kl} for all $i, j, k, l = 1, \ldots, n$,

their common value being $n+d$. Since $5<d<n-1$, we have $5<n+d<(2/3)n^2=(1/3)|X|$. Moreover, points x_{ij} and x_{kl} with $k\neq i$ and $l\neq j$ can both be adjacent only to x'_{kj} and x'_{il} and this only if $\{v_i, v_k\}\in E$. Likewise, there are at most two points adjacent to both x'_{ij} and x'_{kl}. We have proved that (X, R) is in $D(5,2)$. The construction $(V, E)\mapsto(X, R)$ is obviously polynomial-time, and it is an encoding since we can recover a copy of (V, E) by factorizing (X, R) by its unique decomposition into complete bipartite n, n-graphs. It has been established in [2] that the class of all regular graphs, and thereby also the class of all regular graphs of degree >5, is isomorphism complete.

STATEMENT 13: $\mathscr{CB}$ is critical.

Proof: The isomorphism completeness of $\mathscr{CB}$ was established by Booth [2]. By Statement 5, $\mathscr{T}$ is the only variety properly included in $\mathscr{CB}$, and $\mathscr{T}$-isomorphism is trivial.

STATEMENT 14: $\mathscr{M}$ is critical.

Proof: To every graph (V, E) without loops and isolated vertices assign a semigroup $S(V, E)=V\cup E\cup\{0\}$ with a multiplication given by

$$xy=\begin{cases}\{x, y\} & \text{if } \{x, y\}\in E,\\ 0 & \text{otherwise.}\end{cases}$$

The multiplication is associative since $x(yz)=0=(xy)z$ is satisfied. The semigroup $S(V, E)$ is easily seen to belong to $\mathscr{M}$ by virtue of satisfying the equations for $\mathscr{M}$, namely, $xy=yx$ and $xyz=x^2=x^2u$.

Given a semigroup S isomorphic to $S(V, E)$, we can recover an isomorphic copy (V', E') of (V, E) by taking

$$V'=S-S^2 \qquad \text{and} \qquad E'=\{\{s, t\}\,|\,s, t\in V', st\neq 0\}.$$

The assignment $(V, E)\mapsto S(V, E)$ is a polynomial-time encoding of an isomorphism complete class of graphs into $\mathscr{M}$. $\mathscr{M}$ covers only $\mathscr{S}$ and $\mathscr{S}$-isomorphism is polynomial-time.

STATEMENT 15: $\sqrt{\mathscr{L}}$ and $\sqrt{\mathscr{R}}$ are critical.

Proof: Let (X, R) be an arbitrary directed graph. Take pairwise distinct elements a, b, c, u, v not belonging to $X\cup R$ and define a multiplication on $\{a, b, c, u, v\}\cup X\cup R$ by

$$\begin{aligned} &a.(x, y)=b.(x, y)=x, \quad c.(x, y)=y && \text{for } (x, y)\in R,\\ &az=bz=u, \quad cz=v && \text{for } z\in\{a, b, c, u, v\}\cup X,\\ &st=s && \text{for } s\in\{u, v\}\cup X\cup R.\end{aligned}$$

We show that the multiplication is associative:

$$a.(st)=as=(as)t, \qquad b(st)=bs=(bs)t,$$
$$c(st)=cs=(cs)t \quad \text{for} \quad s\in\{u, v\}\cup X\cup R,$$
$$a(st)=u=(as)t, \qquad b(st)=u=(bs)t,$$
$$c(st)=v=(cs)t \quad \text{for} \quad s\in\{a, b, c,\}.$$

Denote by $S(X, R)$ the semigroup obtained. $S(X, R)\models xyz=xy$, therefore by Statement 9, $S(X, R)\in\sqrt{\mathscr{L}}$. Given $S\simeq S(X, R)$, we recover an isomorphic copy (X', R') of (X, R) as follows: There is a three-element set $\{a', b', c'\}=S-S^2$. Two of the elements, say a' and b', have the same square u', distinct from the square v' of c'. Take

$$X'=\{s\in S^2-\{u', v'\}\mid a's=u'\},$$
$$R'=\{(a's, c's)\mid s\in S, a's\neq u'\}.$$

The semigroup opposite to $S(X, R)$ encodes (X, R) into $\sqrt{\mathscr{R}}.\sqrt{\mathscr{L}}$ covers only $\mathscr{I}\vee\mathscr{L}$. To decide about isomorphism of S, T in $\mathscr{I}\vee\mathscr{L}$, of size $n=|S|=|T|$, we form in $O(n^2)$ time a relation $R\subseteq S^2\times T^2$ such that $(s, t)\in R$ iff s and t have the same number of square roots, i. e.

$$\forall\,|\{u\in S\mid u^2=s\}|=|\{v\in T\mid v^2=t\}|.$$

Then $S\simeq T$ iff a bijection can be extracted from R; this can be decided in $O(n^{2,5})$ time (*cf.* [8]).

STATEMENT 16: $\mathscr{I}\vee\mathscr{L}\vee\mathscr{R}$ is critical.

Proof: Let $I=\{a, b, 0\}\in\mathscr{I}$. We encode every directed graph without loops (X, R) as a subsemigroup $S(X, R)$ of $I\times(X\times X)$ (here $X\times X$ is considered as a rectangular band) generated by the set of triples

$$\{(i, x, y)\mid (i\in\{a, b\} \text{ and } x=y) \text{ or } (i=a \text{ and } (x, y)\in R)\}.$$

An isomorphic copy (X', R') is recovered from $S\simeq S(X, R)$ by taking

$$X'=\{s\in S\mid \text{there are two distinct } u, v\in S-S^2 \text{ with } u^2=v^2=s\},$$
$$R'=\{(s, t)\in X'\times X'\mid \text{there is exactly one } w\in S-S^2 \text{ with } w^2=st\}.$$

$\mathscr{I}\vee\mathscr{L}\vee\mathscr{R}$ covers only $\mathscr{L}\vee\mathscr{R}$, $\mathscr{I}\vee\mathscr{L}$, $\mathscr{I}\vee\mathscr{R}$, and the latter clearly have a polynomial-time isomorphism test.

STATEMENT 17: For every prime integer p, $\mathscr{K}_p$ is critical.

Proof: Let (X, R) be a directed graph. Let 1 denote the identity of C_p, let $a \in C_p$ be a fixed element distinct from 1. For every $(x, y) \in X \times X$ define a 2×2-matrix $P(x, y) = (p_{i,j}^{(x,y)})$ by $P(x, y) = \begin{pmatrix} a & 1 \\ 1 & 1 \end{pmatrix}$ if $x = y$ or $(x, y) \in R$, $P(x, y) = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ otherwise, and form the cartesian product

$$\prod_{(x, y) \in X \times X} \mathscr{M}(C_p, 2, 2, P(x, y)) = \mathscr{M}(C_p^{X \times X}, 2^{X \times X}, 2^{X \times X}, P)$$

where the sandwich matrix P has for entries families

$$p_{f, g} = \{p_{f(x, y), g(x, y)}^{(x, y)};\ (x, y) \in X \times X\}$$

for $f, g: X \times X \to 2$. Factorize this product by the homomorphism

$$h: C_p^{X \times X} \to C_p : f \mapsto \prod_{(x, y) \in X \times X} f(x, y)$$

onto $\mathscr{M}(C_p, 2^{X \times X}, 2^{X \times X}, h(P))$ and select in the latter a subsemigroup $\mathscr{M}(C_p, X, X, P(X, R))$, where $P(X, R)$ is a submatrix of $h(P) = (h(p_{f, g}))$ with entries $p_{u, v}^{(X, R)} = h(p_{f_u, g_v})$, where

$$f_u(x, y) = \begin{cases} 1 & \text{for } u = x \\ 2 & \text{for } u \neq x \end{cases}, \qquad g_v(x, y) = \begin{cases} 1 & \text{for } v = y \\ 2 & \text{for } v \neq y \end{cases}, \qquad u, v \in X.$$

Clearly, the semigroup thus obtained is in $\mathscr{K}_p$ and we have

$$p_{u, v}^{(X, R)} = \begin{cases} a & \text{if } u = v \text{ or } (u, v) \in R, \\ 1 & \text{otherwise } \forall. \end{cases}$$

We show that the assignment $(X, R) \mapsto \mathscr{M}(C_p, X, X, P(X, R))$ is an encoding of $D(5,2)$ into $\mathscr{K}_p$. Let (X, R), $(X', R') \in D(5,2)$. We have to show that $(X, R) \simeq (X', R')$ iff the corresponding sandwich matrices

$$P = P(X, R) = (p_{x, y}) \qquad \text{and} \qquad P' = P(X', R') = (p'_{x', y'})$$

are equivalent.

If $f: X \to X'$ is an isomorphism of (X, R) onto (X', R') then $p'_{f(x), f(y)} = p_{x, y}$, hence the sandwich matrices are equivalent.

Assume now that they are equivalent. We have then

$$p'_{f(x), g(y)} = r(x)\, h(p_{x, y})\, c(y)$$

for some bijections $f, g: X \to X'$, functions $r, c: X \to C_p$, and $h \in \mathrm{Aut}(C_p)$. We

easily recognize from P the partition of X into X_1 and X_2 such that $R \subseteq X_1 \times X_2$. Indeed, $x \in X_1$ if there is more than one occurrence of a in the x-th row of P, and $x \in X_2$ if there is only one. We show that $f(X_2) \subseteq X_2'$. Assume to the contrary that $f(x) \in X_1'$ for some $x \in X_2$. Then the $f(x)-$th row in P' has $d+1$ entries a and $n-d-1$ entries 1. Denote

$$A = \{y \in X - \{x\} \mid p'_{f(x),\, g(y)} = a\},$$
$$B = \{y \in X - \{x\} \mid p'_{f(x),\, g(y)} = 1\}.$$

The function $c: X \to C_p$ must be constant on both A and B. Further, $|A| \geqq d$, $|B| \geqq n-d-2$. For an arbitrary $z \in X_2$, $z \neq x$, there must be distinct $b_1, b_2 \in C_p$ such that

$$p'_{f(z),\, g(y)} = \begin{cases} b_1 & \text{for } y \in A - \{z\}, \\ b_2 & \text{for } y \in B - \{z\}. \end{cases}$$

It follows that $b_1 = a$, $b_2 = 1$, and $f(z) \in X_1'$, thus $f(X_2) = X_1'$. But then for any two rows in P' indexed by two distinct elements of X_1' there are at least four $a's$ in the same places, a contradiction with the properties of (X', R'). We have proved so far that $f(X_i) = X_i'$ for $i = 1, 2$, and that $c(x)$ is constant, say, $c(x) = c$ for all $x \in X$. In a similar way, we prove that $g(X_i) = X_i'$, $i = 1, 2$, and $r(y) = r$ for all $y \in X$. It remains to show that $f = g$. For $x \in X_2$, $y \in X$;

$$p'_{f(x),\, g(y)} = \begin{cases} rc & \text{for } y \neq x, \\ rh(a)c & \text{for } y = x, \end{cases}$$

whence $f(x) = g(x)$. Similarly for $x \in X_1$. Moreover, $rc = 1$, $rh(a)c = a$, thus $h(a) = a$, $p'_{f(x),\, f(y)} = p_{x,\, y}$, hence f is an isomorphism of the graphs.

$\mathscr{K}_p$ covers only $\mathscr{L} \vee \mathscr{R} \vee \mathscr{E}_p$ and the latter has a polynomial time isomorphism test.

Denote $\mathrm{Sub} = (\mathscr{I} \vee \mathscr{L} \vee \mathscr{G}) \cup (\mathscr{I} \vee \mathscr{R} \vee \mathscr{G}) \cup (\mathscr{L} \vee \mathscr{R} \vee \mathscr{G})$.

STATEMENT 18: There is a subexponential, i.e. $O(n^{c_1 \log n + c_2})$ time isomorphism algorithm for Sub.

Proof: Clearly, S, $T \in \mathrm{Sub}$ can be isomorphic only if they belong to the same one of the three varieties whose union is Sub.

If S, $T \in \mathscr{L} \vee \mathscr{R} \vee \mathscr{G}$, then $S \simeq T$ iff $G(S) \simeq G(T)$ and $E(S) \simeq E(T)$, subexponential and polynomial, respectively.

Let S, $T \in \mathscr{I} \vee \mathscr{L} \vee \mathscr{G}$. Define the multiplicity function μ_S on $K(S)$ by

$$\mu_S(u) = |\{s \in S - S^2 \mid s^{m+1} = u\}| \qquad \text{where} \quad m = |G(S)|$$

Every isomorphism $h: S \to T$ restricts to a multiplicity preserving isomorphism, or a μ-isomorphism, $g: K(S) \to K(T)$, $\mu_T(g(u)) = \mu_S(u)$, and, every μ-isomorphism $g: K(S) \to K(T)$ can be extended to an isomorphism $h: S \to T$.

Choose fixed idempotents $a \in E(S)$ and $b \in E(T)$. Every isomorphism $f: K(S) \to K(T)$ determines a $\mathcal{G}$-isomorphism $\varphi: aS \to bT$ and $\mathcal{L}$-isomorphism $\psi: E(S) \to E(T)$, by $\varphi(as) = bf(s)$ and $\psi(e) = f(e)$, and is determined by them by

$$f(s) = \psi(e)\varphi(as) \qquad \text{for} \quad e \in E(S) \quad \text{such that } es = s.$$

Moreover, this formula defines an isomorphism f for any pair of isomorphisms $\varphi: aS \to bT$ and $\psi: E(S) \to E(T)$. The isomorphism will be denoted by $f = \varphi \times \psi$.

Given a fixed isomorphism $\varphi: aS \to bT$, define a relation $R_\varphi \subseteq E(S) \times E(T)$ by

$$(e, i) \in R_\varphi \qquad \text{iff} \quad \mu_S(es) = \mu_T(i\varphi(as)) \quad \text{for all } s \in S.$$

Then for an arbitrary bijection $\psi: E(S) \to E(T)$, $\varphi \times \psi$ is a μ-isomorphism iff $\psi \subseteq R_\varphi$. Consequently, $K(S)$ and $K(T)$ are μ-isomorphic iff a bijection can be extracted from R_φ for some isomorphism $\varphi: aS \to bT$. All isomorphisms $\varphi: aS \to bT$ can be computed in time subexponential in $|S|$, the formation of R_φ and extraction of a maximal bijection from R_φ is for each particular φ a polynomial-time matter [8].

In the light of the above statement, we may call Sub the subexponential class. Statements 11-18 can now be summarized into the final result of this paper.

THEOREM *Under the conjecture that $\mathcal{G}$ is not isomorphism complete, the varieties $\mathcal{CB}$, $\mathcal{M}$, $\sqrt{\mathcal{L}}$, $\sqrt{\mathcal{R}}$, $\mathcal{J} \vee \mathcal{L} \vee \mathcal{R}$, and $\mathcal{K}_p$ for prime p are all critical semigroup varieties. Every variety $\mathcal{V}$ either includes one of the critical varieties and then is isomorphism complete, or is included in the subexponential class*

$$\text{Sub} = (\mathcal{J} \vee \mathcal{L} \vee \mathcal{G}) \cup (\mathcal{J} \vee \mathcal{R} \vee \mathcal{G}) \cup (\mathcal{L} \vee \mathcal{R} \vee \mathcal{G})$$

and then it has a subexponential time isomorphism algorithm.

Let us remark in closing that in case of varieties of finite monoids the situation is much simpler: every monoid variety which is not a group variety contains the variety of commutative idempotent monoids – the only critical monoid variety.

BIBLIOGRAPHIE

1. L. BABAI, *Moderately exponential bound for graph isomorphism*, FCT'81, Lecture Notes in Comp. Sci, n. 117, Springer, 1981, pp. 34-50.
2. K. S. BOOTH, *Isomorphism testing for graphs, semigroups, and finite automata are polynomially equivalent problems*, SIAM J. Comput. Vol. 7, 1976, pp. 273-279.
3. K. S. BOOTH and Ch. J. COLBOURN, *Problems polynomially equivalent to graph isomorphism*, Tech. Rep. CS-77-04, Univ. of Waterloo, 1979.
4. A. H. CLIFFORD and G. B. PRESTON, *The algebraic theory of semigroups*, A.M.S., Providence, Rhode Island, 1967.
5. S. EILENBERG, *Automata, Languages, and Machines*, Vol. B, Academic Press, 1976.
6. L. KUČERA and V. TRNKOVÁ, *Isomorphism completeness for some algebraic structures*, FCT'81, Lecture Notes in Comp. Sci, n. 117, Springer, 1981, pp. 218-225.
7. L. KUČERA and V. TRNKOVÁ, *Isomorphism testing in unary algebras* [to appear in SIAM J. Comput].
8. S. MICALI and V. V. VAZIRANI, *An* $O(\sqrt{|V|}.|E|)$ *algorithm for finding maximum matching in general graphs*, Proc. FOCS'80, pp. 17-27.