by Ahto Buldas

PhD Thesis

TALLINN 1999

Declaration

Herewith I declare that the thesis is my own, unaided work. It is submitted for the degree of Doctor of Philosophy in natural sciences at Tallinn Techincal University, and has not been submitted before for any degree or examination at any other university.

Signature of candidate:

Signature of supervisor:

Date:

By a *graph* we mean a pair of sets $G = (V, E)$ where E is an antireflexive (not necessarily symmetric) binary relation on V. The elements of V and E are called *vertices* and *edges* respectively. By a *graph morphism* between $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ we mean a mapping $V_1 \xrightarrow{f} V_2$ such that

$$f(v) \neq f(w) \Rightarrow [vw \in E_1 \Leftrightarrow f(v)f(w) \in E_2] \qquad (0.1)$$

for all $v, w \in V_1$. This kind of graph morphisms were explicitly defined by the author [34]. However, implicitly this type of morphisms have a long history. They arise from the work of Sabidussi [4] where the *generalized lexicographic product* operation, a generalization of the *composition* operation introduced by Harary [3], is defined. They have been re-invented later by several researchers (Hemminger [11], Spinrad [16], Möhring [18]). The main source of inspiration was the developing of fast algorithms for transitive orientation of graphs by Ghouilà-Houri [6], Gilmore and Hoffman [7], Pnueli, Lempel and Even [12], Spinrad [19] (Part VI). It turned out that the graph decomposition method, developed for the transitive orientation, works excellently for many other combinatorial problems including numerous **NP**-complete problems, such as maximum clique (Part VI) and isomorphy of two coloured graphs (Part VI). However, these techniques cannot be used if the graph studied is simple, i.e. has no nontrivial decompositions. Unfortunately, the simplicity is a property of almost all finite graphs as proved in Part II. In [24],[25] and [26] Ehrenfeucht and Rozenberg represent a structure theory of more general objects called 2-structures. The main objective of the current thesis is to study what we can do with purely algebraic techniques in the field of the structure theory of graphs.

In Part I we introduce the notation, basic definitions and results necessary to understand the thesis.

In Part II we study the basic properties of graph morphisms. We give a characterization of finite simple graphs and prove that almost all finite undirected graphs are simple.

In Part III the basic properties of the congruence lattice of a graph are discussed. The basic concept of algebraic structure theory – radical map – is defined and the characterization of semisimple graphs is given in case of the so-called $\Im$-radical defined as the intersection of all co-atoms in the congruence lattice.

In Part IV we give a complete characterization for those finite graphs whose congruence lattice satisfies a fixed lattice identity. For example, congruence distributive (corresp. modular) graphs are characterized by the requirement that all the components and their duals in the generalized lexicographic product should not have more than two (corresp. three) connected components.

In Part V we describe a certain composition operation of lattices and define it as a lexicographic product due to the fact that it exactly represents the congruence lattice of the generalized lexicographic product of graphs. We can express ourselves more poetically saying that under certain conditions the operator Con preserves the lexicographic product operation. This property gives us the complete classification of the congruence lattices of finite graphs.

In Part VI we show how the algebraic decomposition method may reduce the complexity of **NP**-hard graph-related combinatorial problems.

In Part VII we show that the structure theory developed in Parts II–V may have been significantly simplified by using the equivalence between the category of graphs and the category of quasitrivial groupoids.

Congruence relations

Let $G = (V, E)$ be a graph and ρ an equivalence relation on the vertex set V. We say that ρ is a *congruence relation* on G, if

$$x\rho x',\ y\rho y',\ \neg(x\rho y) \Rightarrow [xy \in E \Leftrightarrow x'y' \in E]$$

for arbitrary vertices $x, x', y, y' \in V$. It is easy to see, that the kernel $\operatorname{Ker} f$ of a graph morphism $G \xrightarrow{f} H$ is a congruence relation of G. And reversely, every congruence relation ρ of G is a kernel of some morphism $G \longrightarrow H$. This is true because there is a unique graph structure on the factor-set V/ρ such that the natural projection $V \xrightarrow{\pi} V/\rho$ is morphism. This graph is called a *factor graph*(*quotient graph*) of G by ρ and is denoted as G/ρ.

It turns out that a congruence relation can be defined as an equivalence relation with equivalence classes satisfying certain conditions. This has been pointed out by Hemminger [11] in the case of undirected graphs. Ehrenfeucht and Rozenberg [24] have proved similar results for directed graphs and more general objects called 2-structures.

A subset $M \subseteq V$ is called a *module* (by J.Spinrad [16]) of $G = (V, E)$ if $tu \in E \Rightarrow tw \in E$ and $ut \in E \Rightarrow wt \in E$ for arbitrary $u, w \in M$ and $t \notin M$. Modules have many different names in literature. They are called *clans* in [24],[25],[26], *externally related subsets* in [27] and *blocks* in [33]. It is easy to prove that an equivalence relation ρ on the vertex set V is a congruence relation of G if and only if all the ρ-classes are modules of G.

In Part II we prove that the morphisms of graphs behave almost in the same way as the morphisms of algebraic structures. Finally, In Part VII it turns out not to be just a coincidence.

Basic properties of $\mathrm{Con}\, G$

In Part III we prove that the set $\mathrm{Con}\, G$ of all congruence relations of a graph G is a complete lattice. We prove also that if $\rho^{\bigtriangledown}$ and $\rho^{\bigtriangleup}$ denote the principal ideal generated by ρ and its dual respectively, we have

$$\rho^{\bigtriangleup} \cong \mathrm{Con}\, G/\rho.$$

A suitable isomorphism can be defined as follows:

$$\begin{cases} \rho^{\bigtriangleup} \longrightarrow \mathrm{Con}\, G/\rho \\ \sigma \mapsto \bar{\sigma}, \end{cases}$$

where $(v/\rho, w/\rho) \in \bar{\sigma} \Leftrightarrow (v,w) \in \sigma$. We also prove that if $G/\rho = (V_0, E_0)$ and $\{G_v\}_{v \in V_0}$ is the partition corresponding to ρ then

$$\rho^{\bigtriangledown} \cong \prod_{v \in V_0} (\mathrm{Con}\, G_v, \pi_v),$$

where the corresponding projections π_v can be defined as follows:

$$\pi_v \colon \begin{cases} \rho^{\bigtriangledown} \longrightarrow \mathrm{Con}\, G_v \\ \sigma \mapsto \sigma \mid_{G_v}, \end{cases}$$

Proofs are published by the author in [38].

Radical theory

By the *radical* $\Im(G)$ of a graph G we mean the intersection of all co-atoms of its congruence lattice $\mathrm{Con}\, G$. A graph G is said to be *semisimple* if $\Im(G) = 0$. It has been proved [38] that a graph $G = (V, E)$ is semisimple if and only if G is either *simple*, *complete*, *edgeless* or *linear*, i.e. E is a linear ordering on V. Therefore, if $G = (V, E)$ is a finite semisimple graph then $\mathrm{Con}\, G$ is isomorphic either to a finite partition lattice $\mathbf{\Pi}_n$ $(n = \mid V \mid)$ or to a direct power $(\mathbf{\Pi}_2)^\ell$ $(\ell + 1 = \mid V \mid)$.

A graph G is said to be *radical*, if $\Im(G) = 1$. Only two finite graphs are radical – the empty graph $(\emptyset, \emptyset)$ and singleton. It is proved in [38], that the infinite graph $(\mathbf{N}, \{(n,m) \mid n < m, m \equiv 1 \pmod 2\})$ is radical and its congruence lattice is isomorphic to the ordinal $\omega + 1$.

The radical theory for graphs was first introduced by the author in [38]. All the proofs are presented in Part III of the thesis.

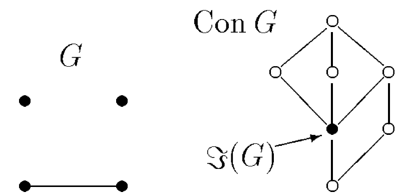


Figure 0.1: A graph G and its radical $\Im(G)$.

Lattice identities in $\operatorname{Con} G$

The congruence lattices of graphs satisfying a given lattice identity are studied in Part IV of the thesis. A complete characterization of all finite graphs with the congruence lattice laying in a given lattice variety is presented.

Let I be a lattice identity. We will find a characterization for all finite graphs G such that $\operatorname{Con} G$ satisfies I. To solve this problem, the $\Im$-*radical* defined in [38] as the meet of all co-atoms in $\operatorname{Con} G$ is useful. If $\Im(G) = 0$, then either $\operatorname{Con} G \cong \mathbf{\Pi}_n$ or $\operatorname{Con} G \cong \mathbf{\Pi}_2^n$, where $\mathbf{\Pi}_n$ is the lattice of all partitions of $n = \{0, ..., n-1\}$. For every $\Im$-semisimple graph G define a positive integer $\eta(G)$ such that $\eta(G) = n$ if G is a complete or edgeless graph with n vertices (i.e. if $\operatorname{Con} G \cong \mathbf{\Pi}_n$) and $\eta(G) = 2$ otherwise. Let $\mathcal{V}$ be a lattice variety such that $L \notin \mathcal{V}$ for at least one lattice L. There is a unique positive integer n such that $\mathbf{\Pi}_1, ..., \mathbf{\Pi}_n \in \mathcal{V}$, but $\mathbf{\Pi}_{n+1} \notin \mathcal{V}$. Denote this n as $\eta(\mathcal{V})$.

We prove that if $G/\Im(G) = \{G_1, ..., G_n\}$ and $\mathcal{V}$ is a lattice variety then $\operatorname{Con} G$ lies in $\mathcal{V}$ if and only if $\eta(G/\Im(G)) \leq \eta(\mathcal{V})$ and $\operatorname{Con} G_i \in \mathcal{V}$ for $i = 1, ..., n$. It follows that for every lattice identity I there is an $O(|V|^2)$ algorithm that determines whether I holds in $\operatorname{Con} G$, where V is the vertex set of G.

The proofs were given by the author in [39] and are presented in Part IV of the thesis.

Lexicographic product operation

For any family of graphs $G_0 = (V_0, E_0)$ and $G_v = (V_v, E_v), (v \in V_0)$ their generalized lexicographic product $G_0[(G_v)_{v \in V_0}]$ is a graph G with vertex set $V = \{(v, w) \mid v \in V_0, w \in V_v\}$ and with edge set $E = \{(v, w)(v', w') \mid vv' \in E_0$, or $v = v'$ and $ww' \in E_v\}$. The generalized lexicographic product was first introduced in the work of Sabidussi [4] it is a generalization of the *composition* operation introduced by Harary [3]. It has been re-invented later by several researchers (Hemminger [11], Spinrad [16], Möhring [18]).

It can be easily verified that the partition of the vertex set V into the components $G_v, v \in V_0$ is a congruence partition and the corresponding factor-graph is

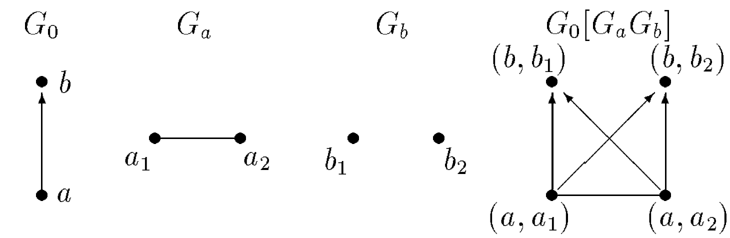


Figure 0.2: An example of the generalized lexicographic product.

isomorphic to G_0. Moreover, if ρ is a congruence relation of a graph $G = (V, E)$, $G_0 = (V_0, E_0) = G/\rho$ is the corresponding factor-graph, $G_v, (v \in V_0)$ are the ρ-classes (viewed as induced subgraphs) then $G \cong G_0[(G_v)_{v\in V_0}]$. Therefore, there is a one-to-one correspondence between the decompositions of a graph into generalized lexicographic products and the congruence relations.

Accordingly, every finite graph can be assembled from *simple* graphs (i.e. graphs that have no nontrivial congruence relations) with the help of the generalized lexicographic product operation. Such a decomposition is known as the *X-join decomposition* [9], *substitution decomposition* [17], *modular decomposition* [19] and *prime-tree decomposition* [24], [25], [26].

Lexicographic product of lattices

The radical $\Im(G)$ is a *strongly neutral* element of the lattice $\mathrm{Con}\, G$, i.e. $\Im(G) \vee \rho = \Im(G) \cup \rho$ for each $\rho \in \mathrm{Con}\, G$. Every strongly neutral element is a neutral element (proved in [39], Part IV). Therefore, the mapping

$$\varphi\colon \begin{cases} \mathrm{Con}\, G \longrightarrow \Im(G)^{\bigtriangledown} \times \Im(G)^{\bigtriangleup} \\ \rho \mapsto (\rho \wedge \Im(G), \rho \vee \Im(G)) \end{cases}$$

is a lattice embedding. Let V_0 be a set and L_0 be a sublattice of the partition lattice $\mathbf{\Pi}(V_0)$ (the lattice of all partitions of V_0). Let $L_v, (v \in V_0)$ be arbitrary lattices. By the *lexicographic product* $L_0[(L_v)_{v\in V_0}]$ we mean the following subdirect product:

$$\{(\sigma_0, (\sigma_v)_{v\in V_0}) \mid \forall v, w \in V_0 : \sigma_v \neq 1,\ (v, w) \in \sigma_0 \ \Rightarrow\ v = w\}.$$

The lexicographic product of lattices is first introduced by the author in the current thesis and is defined in Part V. All the proofs are presented in Parts IV–V.

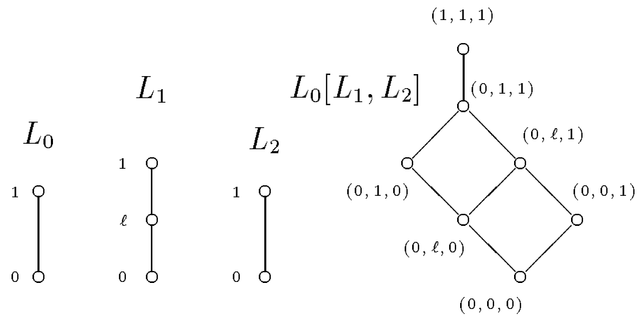


Figure 0.3: An example of the lexicographic product of lattices.

Decomposition of $\operatorname{Con} G$

Let G be a finite graph. Let ρ be a strongly neutral congruence relation of G, $G/\rho = (V_0, E_0)$ and $\{G_v\}_{v \in V_0}$ is the corresponding partition. There is a lattice embedding

$$\iota\colon \begin{cases} \operatorname{Con} G \longrightarrow \operatorname{Con} G/\rho \times \prod_{v \in V_0} \operatorname{Con} G_v \\ \sigma \mapsto (\bar{\sigma}, (\sigma\mid_{G_v})_{v \in V_0}) \end{cases}$$

It is proved in Part V that $(\sigma_0, (\sigma_v)_{v \in V_0})$ lies in $\operatorname{Im} \iota$ if and only if

$$\forall v, w \in V_0 : \sigma_v \neq 1,\ (G_w, G_v) \in \sigma_0 \ \Rightarrow\ G_w = G_v. \tag{0.2}$$

Thereby, if $G = (V, E)$ is a graph and $\{G_v\}_{v \in G/\Im(G)}$ is the partition corresponding to the radical $\Im(G)$ then the congruence lattice $\operatorname{Con} G$ is isomorphic to the lexicographic product of the lattices $\operatorname{Con} G/\Im(G)$ and $(\operatorname{Con} G_v)_{v \in G/\Im(G)}$.

In Part V we also give a proof for the proposition that a lattice L is isomorphic to the congruence lattice of a finite graph if and only if it can be assembled from the lattices $\mathbf{\Pi}_n$ and $(\mathbf{\Pi}_2)^\ell$ using the lexicographic product operation, assuming that the constructions

$$(\mathbf{\Pi}_2)^\ell[(\ldots, (\mathbf{\Pi}_2)^\ell, \ldots)],$$

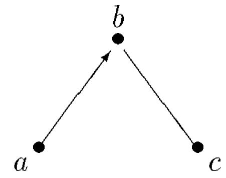
with $\ell > 1$ are not allowed.

Graphs as algebraic structures

We prove in Part VII that the notion of a graph morphism has indeed an algebraic nature. For each graph $G = (V, E)$ we can define a binary operation $V \times V \overset{\cdot}{\longrightarrow} V$ as follows:

$$v \cdot w = \begin{cases} w, & \text{if } vw \in E \\ v, & \text{if } vw \notin E. \end{cases} \tag{0.3}$$

The corresponding groupoid $(G, \cdot)$ is *quasitrivial*, i.e. $vw \in \{v, w\}, \forall v, w$. For



	a	b	c
a	a	b	a
b	b	b	c
c	c	b	c

Figure 0.4: A graph and the corresponding groupoid.

every quasitrivial groupoid $(G, \cdot)$ we can define a binary relation E such that the condition (0.3) holds. Indeed, the relation E can be defined as $E = \{(v, w) \mid v \neq w, v \cdot w = w\}$. Quasitrivial groupoids and their relations with graphs have been studied by Chech mathematicians ([14],[20],[33]).

It turns out that a mapping f between the vertex sets of two graphs is a graph morphism if and only if it is a morphism of the corresponding groupoids, i.e. iff

$$f(v \cdot w) = f(v) \cdot f(w).$$

Thereby graphs can be viewed as algebras with a single binary operation.

Discussion

The current thesis describes an algebraic framework for certain kind of graph decomposition referred to as modular decomposition having been proved to be useful in various graph-related combinatorial problems. The main objective of the thesis is to demonstrate that the ideas and methods developed during a centuries-old history of abstract algebra may be extremely fruitful for developing fast algorithms to find a solution of complex combinatorial problems, and moreover, the results of combinatorics achieved that way, re-translated to the language of algebra, are sometimes interesting for Algebra itself.

We show that the standard approach in algebraic structure theory – radical maps – may be used also in graph theory. The structure theory, based on the radical defined as the meet of all co-atoms in the congruence lattice, is shown (in the thesis) to be equivalent to the modular decomposition theory developed independently by numerous researchers. We point out also that the same decomposition theory results from a "really standard" algebraic techniques when defining graphs as quasitrivial groupoids first studied by Chech mathematicians.

The author has been studying practical applications of graphs for many years starting with digital circuit simulation [31] and ending with the recent studies in the field of digital time-stamping [40, 41] and believes that the algebraic structure theory is a method much more universal we usually imagine. While the graph theory serves as a general background for describing and formalizing complex combinatorial problems from real life, the abstract algebra is a universal method for inventing hidden symmetries that may be a key to the solution of these ugly-looking problems.

Publications

1. A.Buldas, "Comparability graphs and the structure of finite graphs." Proc. Estonian Acad. Sci. Phys. Math., 2/3, 1996, 45, 117–127.

2. A.Buldas, "Congruence lattice of a graph." Proc. Estonian Acad. Sci. Phys. Math., 1997, 46, 3, 155–170.

3. A.Buldas, "Graphs and lattice varieties," Proc. Estonian Acad. Sci. Phys. Math., 1998, 47, 2, 100–109.

4. A.Buldas, P.Laud, H.Lipmaa, J.Villemson, "Time-stamping with binary linking schemes," Advances in Cryptology – CRYPTO'98, (LNCS 1462), 486–501, 1998.

5. A.Buldas, P.Laud, "New linking schemes for digital time-stamping," Proc. ICISC'98, Seoul, Korea, 1998, 3–13.

The author expresses his thanks to the advisor prof. Leo Võhandu for stating the problem, to prof. Kalle Kaarli, to prof. Ulrich Knauer, to prof. Ellen Redi, to prof. Vello Kukk for their helpful and encouraging remarks, to dr. Ülo Jaaksoo, to prof. Jaan Penjam and dr. Uno Kaljulaid for the support.

1.1 Sets

We use the symbol $A \subseteq B$ when A is a *subset* of B, i.e. if $a \in A$ always implies $a \in B$. The symbol $A \subset B$ means the *proper inclusion*, i.e. $A \subseteq B$ but $A \neq B$. We use set theoretic operations $A \cup B$ and $A \cap B$ in the conventional sense. We use both symbols $A \backslash B$ and $A - B$ for the *set-theoretic difference*, i.e. $a \in A \backslash B$ iff $a \in A$ and $a \notin B$.

For any set $\mathcal{A}$ of sets the *union* of $\mathcal{A}$ is defined as the set

$$\cup \mathcal{A} := \{a \mid \exists A : a \in A \in \mathcal{A}\}.$$

If $\mathcal{A}$ in nonempty then the *intersection* of $\mathcal{A}$ is defined as the set

$$\cap \mathcal{A} := \{a \mid \forall A \in \mathcal{A} : a \in A\}.$$

Let V be a set. We say that V is a *direct union* of nonempty subsets $V_1, ..., V_k$ and write

$$V = V_1 \coprod V_2 \coprod ... \coprod V_k$$

if $V = V_1 \cup ... \cup V_k$ and $V_i \cap V_j = \emptyset$ for every $i \neq j$. The set $\pi = \{V_1, ..., V_k\}$ is said to be a *partition* of V. In a more general case, if π has an infinite number of elements, i.e. $\pi = \{V_\iota\}_{\iota \in I}$ we will use the notation

$$V = \coprod_{\iota \in I} V_\iota.$$

. By the *direct product* of sets V_1,...,V_k we mean the set of k-tuples

$$V_1 \times ... \times V_k := \{\langle v_1, ..., v_k \rangle \mid v_1 \in V_1, \ ..., \ v_k \in V_k\}.$$

Sometimes we need direct products with infinite sequence of sets $\langle V_\iota \rangle_{\iota \in I}$ when I may be tought about as an ordinal number. By a direct product of sets V_ι we mean the set of infinite sequences (choice functions)

$$\prod_{\iota \in I} V_\iota := \{\langle v_\iota \rangle_{\iota \in I} \mid \forall \iota \in I : v_\iota \in V_\iota\}.$$

The Axiom of Choice (see [13]) says that for every sequence $\langle V_\iota \rangle_{\iota \in I}$ of nonempty sets there exists a choice function. Therefore, direct product of nonempty sets is nonempty.

1.2 Relations

Let V be a set. By a *relation* with *arity* k on V we mean an arbitrary subset $E \subseteq V^k = \overbrace{V \times \ldots \times V}^{k}$. Relations with arity $k = 2$ are called *binary relations.* Relations with arity $k = 3$ are called *ternary relations.* If E is a binary relation then instead of $\langle u, v \rangle \in E$ we sometimes use a shorter notation $u\ E\ v$. The relation

$$1_V = \{\langle v, v \rangle \mid v \in V\}$$

is referred to as *identity relation* on V.

The relation $E^{-1} = \{\langle u, v \rangle \mid \langle v, u \rangle \in E\}$ is called the *inverse* of E. The relation $\overline{E} = (V \times V) \backslash E$ is called the *complement* of E.

A binary relation E is said to be *symmetric* if it coincides with its own inverse, i.e. if $E = E^{-1}$. A binary relation E on V is said to be *antireflexive* if $E \cap 1_V = \emptyset$ and *reflexive* if $E \cap 1_V = 1_V$.

A binary relation E on V is said to be *antisymmetric* if $E \cap E^{-1} \subseteq 1_V$, i.e. $\langle u, v \rangle, \langle v, u \rangle \in E$ always implies $u = v$.

Let E and F be two binary relations on V. By the *composition* $E \circ F$ we mean a binary relation

$$E \circ F := \{\langle u, w \rangle \mid \exists v \in V, \langle u, v \rangle \in E, \langle v, w \rangle \in F\}.$$

A binary relation E is said to be *transitive* if $E \circ E \subseteq E$, i.e. $\langle u, v \rangle, \langle v, w \rangle \in E$ always implies $\langle u, w \rangle \in E$.

By a *restriction* of a binary relation E into a subset $V' \subset V$ we mean the binary relation

$$E \mid_{V'} := E \cap (V' \times V').$$

1.3 Graphs

A pair $G = (V, E)$ is called a *graph* if E is a binary relation on V. The elements of V and E are called *vertices* and *edges* respectively. A graph G is called *undirected* if E is symmetric. Instead of $\langle x, y \rangle \in E$ we sometimes use shorter notation $xy \in E$. An edge of the form $\langle v, v \rangle$ is called a *self loop* (or *loop*). We assume that the graphs being argued about in the thesis are without self loops, i.e. we assume that the relation E is antireflexive.

A graph $G = (V, E)$ is said to be *finite* if its vertex set V is finite.

The graph $\overline{G} = (V, \overline{E})$ is said to be the *complement graph* of $G = (V, E)$.

By a *complete graph* we mean a graph $G = (V, E)$ such that $E = V \times V$. By an *edgeless graph* we mean a graph $G = (V, E)$ such that $E \subseteq 1_V$.

The set $N_{\leftarrow}(v) = \{\langle v, u\rangle \in E \mid u \in V\}$ is called a *left neighborhood* of v; and dually, the set $N_{\rightarrow}(v) = \{\langle u, v\rangle \in E \mid u \in V\}$ is called a *right neighborhood* of v. For an undirected graph the left- and right neighborhood coincide and we use the notation $N(v) := N_{\leftarrow}(v) = N_{\rightarrow}(v)$.

1.4 Subgraphs and modules

We say that $G' = (V', E')$ is a *subgraph* of $G = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E \cap (V' \times V')$. By an *induced subgraph* of G we mean a subgraph $G' = (V', E')$ such that $E' = E \cap (V' \times V')$. In most cases when speaking about the *subgraphs* we inherently assume they are induced subgraphs.

A complete induced subgraph C of a graph G is called a *clique* of G.

A pair (V_1, V_2) is called a *diclique* of G if V_1 and V_2 are subsets of V and $v_1v_2 \in E$ for every $v_1 \in V_1$, $v_2 \in V_2$ and $v_1 \neq v_2$.

Let $G = (V, E)$ be an arbitrary graph. We say that the set of vertices $M \subseteq V$ is a *module* of G (by Jeremy Spinrad) if for all $x, y \in M$ and $z \notin M$

$$(xz \in E \Rightarrow yz \in E),\ (zx \in E \Rightarrow zy \in E).$$

Let $G = (V, E)$ be an undirected graph and $v \in V$ be a vertex. By the *connected component* of v we mean a induced subgraph consisting of all vertices u such that there is a finite sequence of vertices

$$u = v_0, v_1, v_2 \ldots, v_n = v,$$

such that $v_k v_{k+1} \in E$ for every $k < n$. A graph $G = (V, E)$ is said to be *connected* if the connected component of a vertex $v \in V$ coincides with the whole graph. A graph G is said to be *complement-connected* if $\overline{G}$ is connected.

1.5 Partial orderings

Let V be a set and R be a binary relation on V. We say that R is a *partial ordering* on V, if R is antisymmetric and transitive. A partial ordering E on V is said to be *linear ordering* if $E \cup E^{-1} \supseteq (V \times V)\backslash 1_V$, i.e. if $\{\langle u, v\rangle, \langle v, u\rangle\} \notin E$ always implies $u = v$.

A pair (V, E) is said to be a *partially ordered set* (or a *poset*) if E is a partial ordering on V. If E is a linear ordering on V, the pair (V, E) is a *linearly ordered set*. A graph $G = (V, E)$ is said to be *linear* if E is a linear ordering on V.

Let $P = (V, \prec)$ be a partially ordered set and $A \subset V$ be an arbitrary subset. An element $\ell \in V$ is said to be a *lower bound* of A if $\ell \prec a$ for every $a \in A$. Dually, $u \in V$ is said to be an *upper bound* of A if $a \prec u$ for every $a \in A$. We denote by $A^{\triangledown}$ the set of all lower bounds of A and dually, by $A^{\vartriangle}$ the set of all upper bounds of A. If $A = \{a\}$ then the we omit the brackets $\{\}$ and use the notations $a^{\triangledown}$ and $a^{\vartriangle}$.

1.6 Lattices

Let $P = (V, E)$ be a poset and $A \subset V$. If there is a greatest element in $A^\triangledown$, we say that it is the *greatest lower bound* or *infimum* of A and is denoted as $\inf A$. Dually if there is a least element in $A^\vartriangle$, it is referred to as the *least upper bound* or *supremum* of A and will be denoted as $\sup A$. Therefore,

$$\begin{aligned} i = \inf A &\equiv i \in A^\triangledown,\ \forall a \in A^\triangledown : a \prec i; \\ s = \sup A &\equiv s \in A^\vartriangle,\ \forall a \in A^\vartriangle : s \prec a. \end{aligned}$$

A poset $L = (V, \prec)$ is called a *lattice* if $\inf\{a, b\}$ and $\sup\{a, b\}$ exist for all $a, b \in V$. Sometimes we use alternative symbols for supremum and infimum:

$$\begin{aligned} a \wedge b &:= \inf\{a, b\} \\ a \vee b &:= \sup\{a, b\}. \end{aligned}$$

A lattice is said to be *complete* if $\inf A$ and $\sup A$ exist for all $\emptyset \neq A \subset V$.

When speaking about lattices we assume that the corresponding partial ordering $\prec$ is reflexive. By a *chain* of a lattice $(L, \prec)$ we mean a subset $C \subseteq L$ such that the restriction $\prec|_C$ is a linear ordering on C. A chain C is said to be *maximal* if for any chain D the inclusion $C \subseteq D \subseteq L$ implies $C = D$.

We say that a finite lattice L satisfies *Jordan-Dedekind chain condition* if all the maximal chains have the same lenght.

1.7 Equivalence relations and partitions

Let V be a set. A binary relation E on V is called an *equivalence relation* if it is reflexive, symmetric and transitive. If E is an equivalence relation and $\langle u, v\rangle \in E$ then we use alternative notation $u \equiv v\,(E)$. The set $u/E = \{v \in V \mid \langle u, v\rangle \in E\}$ is called an *equivalence class* of E or simply, an *E-class* It is well known fact that equivalence relations on V are in one-to-one correspondence with partitions of V. Namely, if E is an equivalence relation on V, the set of all E-classes $\pi(E) = \{v/E \mid v \in V\}$ is a partition of V; and inversely, if $P = \{V_\iota\}_{\iota \in I}$ is a partition, the set of pairs $\epsilon(P) = \{\langle u, v\rangle \mid \exists \iota \in I : u, v \in V_\iota\}$ is an equivalence relation. Moreover, $\pi(\epsilon(P)) = P$ and $\epsilon(\pi(E)) = E$. The set of all equivalence classes of E is called a *factor set* and is denoted by V/E.

The set $\mathbf{\Pi}(V)$ of all equivalence relations on V is partially ordered by the inclusion relation $\subseteq$. Moreover, this set is a complete lattice in which $\inf \mathcal{A} = \cap\mathcal{A}$ for every subset $\mathcal{A} \subset \mathbf{\Pi}(V)$. If $V = \{1, ..., n\}$ then the partition lattice of V will be denoted as $\mathbf{\Pi}_n$. An overview about the partition lattices is given in [30].

1.8 Lattices as algebras

Let $(L, \prec)$ be a lattice. Because of the equivalences

$$u \leq v \;\equiv\; u \vee v = v \equiv u \wedge v = u$$

a lattice may be defined as an algebraic structure $(L; \vee, \wedge)$ such that:

- $\vee$ and $\wedge$ are associative, commutative and idempotent;
- $u \vee (u \wedge v) = u = u \wedge (u \vee v)$.

An equivalence relation Θ on L is called a *congruence relation* of L if $\langle u, u' \rangle, \langle v, v' \rangle \in \Theta$ implies $\langle u \vee v, u' \vee v' \rangle, \langle u \wedge v, u' \wedge v' \rangle \in \Theta$. It is well known that the set Con L of congruence relations of a lattice is itself a lattice. A lattice L is said to be *simple* if it has no nontrivial congruence relations. For example, the partition lattices $\mathbf{\Pi}(V)$ are simple (see [15]). A factor-set L/Θ be a congruence relation Θ is itself a lattice. It is called a *factor lattice* of L. Let $\langle L_\iota \rangle_{\iota \in I}$ be a sequence of lattices. By the *direct product*

$$\prod_{\iota \in I} L_\iota$$

of the lattices L_ι we mean an algebra $(L; \vee, \wedge)$ such that L is a direct product of sets L_ι and the operations $\vee$ and wedge are defined as follows:

$$\begin{aligned} \langle u_\iota \rangle_{\iota \in I} \vee \langle v_\iota \rangle_{\iota \in I} &:= \langle u_\iota \vee v_\iota \rangle_{\iota \in I} \\ \langle u_\iota \rangle_{\iota \in I} \wedge \langle v_\iota \rangle_{\iota \in I} &:= \langle u_\iota \wedge v_\iota \rangle_{\iota \in I}. \end{aligned}$$

A mapping $L \xrightarrow{\pi_\iota} L_\iota$, such that $\pi_\iota(\langle u_\iota \rangle_{\iota \in I}) = u_\iota$ is called a *natural projection*. We say that a lattice L' is a *subdirect product* of lattices $\langle L_\iota \rangle_{\iota \in I}$ if L is a subalgebra of the direct product $\prod_{\iota \in I} L_\iota$ and $\pi_\iota(L') = L_\iota$ for every $\iota \in I$. A lattice is said to be *subdirectly irreducible* if it cannot be represented in a nontrivial way as a subdirect product. For example, a simple lattice is subdirectly irreducible.

1.8.1 Lattice varieties

By a *lattice identity* we mean an identity $u(x, y, z, \ldots) = v(x, y, z, \ldots)$, where u and v are expressions formed using the variable letters $x, y, z, \ldots$ and the symbols $\vee$ and $\wedge$ of the lattice operations (i.e. the supremum and infimum respectively). A lattice L is said to be *distributive* if the following identities hold:

$$\begin{aligned} x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z) \\ x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z). \end{aligned}$$

For example, the congruence lattice of a lattice is distributive. A lattice L is said to be *modular* if it satisfies the *shearing identity*

$$x \wedge (y \vee z) = x \wedge ((y \wedge (x \vee z)) \vee z).$$

A class $\mathcal{V}$ of lattices is said to be a *lattice variety* if there is a set of identities $\mathcal{I}$ such that $L \in \mathcal{V}$ if and only if all the identities of $\mathcal{I}$ hold in L. If $\mathbf{K}$ is a class of lattices we denote by $\mathrm{Var}(\mathbf{K})$ the smallest variety containing $\mathbf{K}$.

It has been proved by B.Jónsson (consequence of Jónsson lemma [10]) that if $\mathbf{K}$ is finite set of finite lattices and L is a subdirectly irreducible lattice in $\mathrm{Var}(\mathbf{K})$ then there is a lattice $K \in L$, sublattice $S \subset K$ and a congruence relation $\Theta \in \mathrm{Con}\, S$ such that $L \cong S/\Theta$.

For example, as $\mathbf{\Pi}_n$ is simple it is also a subdirectly irreducible. It follows from the Jónsson lemma that $\mathbf{\Pi}_n \notin \mathrm{Var}(\{\mathbf{\Pi}_{n-1}\})$ because otherwise there should exist a sublattice $S \subset \mathbf{\Pi}_{n-1}$ and a congruence relation $\Theta \in \mathrm{Con}\, S$ such that $\mathbf{\Pi}_n \cong S/\Theta$ and therefore,

$$|\mathbf{\Pi}_n| = |S/\Theta| \leq |S| \leq |\mathbf{\Pi}_{n-1}| \ .$$

A contradiction, because obviously $|\mathbf{\Pi}_n| > |\mathbf{\Pi}_{n-1}|$. Hence there exists a lattice identity that holds in $\mathbf{\Pi}_{n-1}$ but not in $\mathbf{\Pi}_n$.

In 1982 J.Spinrad [16] defined modules as subgraphs with certain properties and discovered that graphs can be canonically decomposed using the structure of modules. We show that the technique he used leads us to a new concept of a graph morphism which is a generalization of strong homomorphisms. We give a characterization of simple undirected graphs and prove that almost all finite undirected graphs are simple.

2.1 Graph morphisms

Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be an arbitrary pair of graphs. We say that a mapping $V_1 \xrightarrow{f} V_2$ is a *graph morphism* if

$$f(x) \neq f(y) \Rightarrow [xy \in E_1 \Leftrightarrow f(x)f(y) \in E_2]. \tag{2.1}$$

for all $x, y \in V_1$. For emphasizing that f is a graph morphism we sometimes write $G_1 \xrightarrow{f} G_2$.

For example, consider the mappings f, g and h presented in Figure 2.5. Obviously f is not a morphism because $\langle 1', 3' \rangle \in E'$ but $\langle 1, 3 \rangle \notin E$; g is not a morphism for the same reason; h is a morphism.

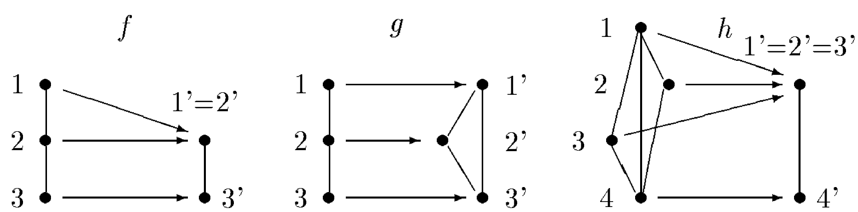


Figure 2.5: Mapping h is a morphism but f and g are not.

That kind of morphisms were introduced by the author [34]. It is easy to verify that with respect to these morphisms one gets the structure of a category. In other words, the *identity* mapping [1] $G \xrightarrow{1_G} G$ is always a morphism, the *composition* $G_1 \xrightarrow{g \circ f} G_3$ of two morphisms $G_1 \xrightarrow{f} G_2$ and $G_2 \xrightarrow{g} G_3$ is a morphism as well. We say that the morphism f is a *monomorphism* if f is injective and that f is an *epimorphism* if f is surjective. This is correct from the viewpoint of Category

[1] It coincides with the notion of *identity relation*.

Theory. It is easy to see that the category of graphs is balanced with respect to graph morphisms.

Let $G = (V, E)$ be a graph and ρ an equivalence relation on the vertex set V. We say that ρ is *congruence relation* on G, if

$$x\rho x',\ y\rho y',\ \neg(x\rho y) \Rightarrow [xy \in E \Leftrightarrow x'y' \in E]$$

for arbitrary vertices $x, x', y, y' \in V$. For example, all the equivalence relations presented in Figure 2.6 are not congruence relations. Inversely, all the relations

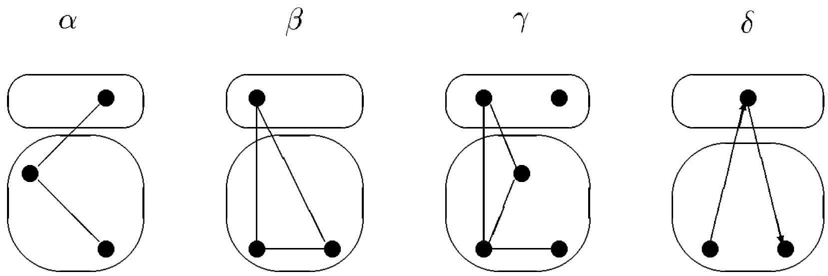


Figure 2.6: These equivalence relations are not congruence relations.

in Figure 2.7 are congruence relations.

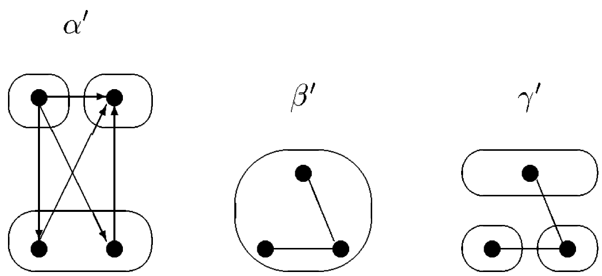


Figure 2.7: Examples of congruence relations.

It is easy to see, that the kernel $\operatorname{Ker} f$ of a graph morphism $G \xrightarrow{f} H$ is a congruence relation of G. And reversely, every congruence relation ρ of G is a kernel of some morphism $G \longrightarrow H$. This is true because there is a unique graph structure on the factor-set V/ρ such that the natural projection $V \xrightarrow{\pi} V/\rho$ is morphism. This graph is called a *factor graph*(*quotient graph*) of G by ρ and is denoted as G/ρ.

Theorem 1 *Let (A, E_A), (B, E_B) and (C, E_C) be graphs, $A \xrightarrow{f} C$ a morphism, $A \xrightarrow{g} B$ an epimorphism and $\operatorname{Ker} g \subseteq \operatorname{Ker} f$. Then there exists a unique morphism $B \xrightarrow{h} C$ which makes the following diagram commutative:*

$$\begin{array}{ccc} A & \xrightarrow{f} & C \\ {\scriptstyle g}\downarrow & & \| \\ B & \xrightarrow{h} & C. \end{array} \tag{2.2}$$

If $\operatorname{Ker} g = \operatorname{Ker} f$ then h is a monomorphism.

Proof. As g is onto there exists exactly one mapping h making the diagram (2.2) commutative. Let us show that h is a graph morphism. Let $b_1, b_2 \in B$ be vertices of B such that $h(b_1) \neq h(b_2)$. Because of the surjectivity of g there exist $a_1, a_2 \in A$ such that $g(a_1) = b_1$ and $g(a_2) = b_2$ and therefore $f(a_1) \neq f(a_2)$ and $g(a_1) \neq g(a_2)$. As f and g are morphisms, the following propositions

$$a_1a_2 \in E_A \Leftrightarrow f(a_1)f(a_2) \in E_C$$
$$a_1a_2 \in E_A \Leftrightarrow g(a_1)g(a_2) \in E_B$$

are valid and thus the proposition $b_1b_2 \in E_B \Leftrightarrow h(b_1)h(b_2) \in E_C$ is valid as well. Indeed, $h(b_1) = f(a_1)$ and $h(b_2) = f(a_2)$ because of the commutativity of the diagram (2.2). Thereby h is a graph morphism.

If $\operatorname{Ker} g = \operatorname{Ker} f$, then h is injective and therefore h is monomorphism. □

An important consequence of Theorem 1 is that if $A \xrightarrow{f} B$ is a morphism then there exists a morphism h which makes the following diagram commutative

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \pi}\downarrow & & \uparrow{\scriptstyle \iota} \\ A/\operatorname{Ker} f & \xrightarrow{h} & \operatorname{Im} f \end{array}$$

where π and ι are the natural projection and the natural injection respectively. It is easy to see that if one of the following three diagrams

$$\begin{array}{ccc} G & \xrightarrow{f} & G \\ {\scriptstyle f}\downarrow & & \| \\ G & \xrightarrow[f]{} & G \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{\pi} & G/\operatorname{Ker} f \\ {\scriptstyle f}\downarrow & & \| \\ G & \xrightarrow{\pi} & G/\operatorname{Ker} f \end{array} \qquad \begin{array}{ccc} \operatorname{Im} f & \xrightarrow{\iota} & G \\ \| & & {\scriptstyle f}\downarrow \\ \operatorname{Im} f & \xrightarrow[\iota]{} & G \end{array}$$

is commutative, then the other two diagrams are also commutative. If f is an endomorphism and makes these diagrams commutative, f is said to be an *idempotent*.

Theorem 2 *For every morphism $G \xrightarrow{g} H$ there is an idempotent $G \xrightarrow{f} G$ such that $\operatorname{Ker} f = \operatorname{Ker} g$.*

Proof. Let $G = (V, E)$ be an arbitrary graph, $V/\operatorname{Ker} g \xrightarrow{\xi} V$ a choice function and $V \xrightarrow{\pi} V/\operatorname{Ker} g$ the natural projection. Let

$$f := \xi \circ \pi.$$

Since ξ is injective, $\operatorname{Ker} f = \operatorname{Ker} g$ and it is clear that $\pi \circ \xi = 1$. Therefore we get

$$\begin{aligned} f \circ f &= (\xi \circ \pi) \circ (\xi \circ \pi) = \\ &= \xi \circ (\pi \circ \xi) \circ \pi = \\ &= \xi \circ 1 \circ \pi = \xi \circ \pi \\ &= f. \end{aligned}$$

It remains to show that f is a graph morphism. Let x and y be nodes of G such that $f(x) \neq f(y)$. Since $\operatorname{Ker} f = \operatorname{Ker} \pi$, we get also $\pi(x) \neq \pi(y)$ and $\pi(f(x)) \neq \pi(f(y))$ because of the injectivity of f. And finally

$$\begin{aligned} \langle x, y\rangle \in E &\Leftrightarrow \langle \pi(x), \pi(y)\rangle \in \tilde{E} \\ &\Leftrightarrow \langle \pi(f(x)), \pi(f(y))\rangle \in \tilde{E} \\ &\Leftrightarrow \langle f(x), f(y)\rangle \in E, \end{aligned}$$

where $\tilde{E}$ is the edge set of $G/\operatorname{Ker} f$. □

The most important consequence of Theorem 2 is that every congruence relation of G is the kernel of a suitably chosen endomorphism of G and every factor-graph of G can be embedded into G. Roughly speaking, every factor-graph is also a subgraph. Indeed, if we have an epimorphism $G \xrightarrow{g} H$ then there exists an endomorphism $G \xrightarrow{f} G$ such that $\operatorname{Ker} f = \operatorname{Ker} g$ and by Theorem 1 there exists a monomorphism $H \xrightarrow{h} G$ which makes the following diagram commutative:

$$\begin{array}{ccc} G & \xrightarrow{f} & G \\ {\scriptstyle g}\downarrow & & \| \\ H & \xrightarrow[h]{} & G. \end{array}$$

2.2 An induction principle

We give now a very powerful tool for proving propositions about all finite graphs. We say that a property $\mathcal{A}$ is *inductive* if for every graph G and congruence partition $G/\rho = \{G_1, ..., G_\ell\}$ the following implication holds

$$\mathcal{A}(G_1),\ \mathcal{A}(G_2),\ ...,\ \mathcal{A}(G_\ell),\ \mathcal{A}(G/\rho) \Rightarrow \mathcal{A}(G).$$

A property $\mathcal{A}$ is said to be *hereditary* if $\mathcal{A}(G) \Rightarrow \mathcal{A}(H)$ whenever there is a monomorphism $H \longrightarrow G$ and dually, $\mathcal{A}$ is *co-hereditary property* of graphs if

$\mathcal{A}(G) \Rightarrow \mathcal{A}(H)$ whenever there is an epimorphism $G \longrightarrow H$. It follows from Theorem 2 that every hereditary property of graphs is co-hereditary. It is clear that if every simple graph has an inductive property $\mathcal{A}$, then all (finite) graphs have this property. If $\mathcal{A}$ is both inductive and hereditary then obviously

$$\mathcal{A}(G_1),\ \mathcal{A}(G_2),\ \ldots,\ \mathcal{A}(G_\ell),\ \mathcal{A}(G/\rho) \Leftrightarrow \mathcal{A}(G)$$

and therefore we can prove the following lemma by induction on the size of G.

Lemma 1 *If properties $\mathcal{A}$,$\mathcal{B}$ are equivalent for prime graphs and are both inductive and hereditary then they are equivalent for all graphs.*

2.3 Modules and morphisms

We prove that the modules of a graph G are closely related with the morphisms from G to other graphs. It turns out that the modules of a graph G are exactly the congruence classes of G.

Theorem 3 *An induced subgraph M of $G = (V, E)$ is a module iff there exists a congruence relation ρ of G such that M is a ρ-class.*

Proof. Let M be a module. We define the following equivalence relation

$$\rho = \{\langle x, y\rangle \mid (x = y) \text{ or } (x \in M,\ y \in M)\}. \tag{2.3}$$

It is clear that M is a ρ-class. It remains to show that ρ is a congruence relation of G. Let us assume that $x\rho x'$, $y\rho y'$ and $\neg(x\rho y)$. It follows now that $\neg(x'\rho y')$ because of the transitivity of ρ.

If $x = x'$ and $y = y'$ then the statement of the theorem holds trivially. Assume now that $x \neq x'$. It follows from (2.3) that $x, x' \in M$. Since $\neg(x\rho y)$ and $\neg(x'\rho y')$, it follows that $y, y' \notin M$ and, since $y\rho y'$, we get finally $y = y'$. The following implications

$$\begin{aligned} xy \in E &\Rightarrow x'y' \in E \\ x'y' \in E &\Rightarrow xy \in E, \end{aligned}$$

are true because M is a module and this means that ρ is a congruence relation.

Let $M \subseteq V$ be a subgraph such that there exists a congruence relation ρ of G such that M is an equivalence class of ρ. Let $x, y \in M$ and $z \notin M$. Since ρ is an equivalence relation, we get $x\rho y$, $z\rho z$ and $\neg(x\rho z)$ and therefore

$$xz \in E \Rightarrow yz \in E$$

because ρ is a congruence relation. The proof of $zx \in E \Rightarrow zy \in E$ is similar and therefore M is a module. □

It is also easy to prove that an equivalence relation ρ on the vertex set V is a congruence relation of G if and only if all the ρ-classes are modules of G.

2.4 Comparison with strong homomorphisms

Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be graphs. A mapping $V_1 \xrightarrow{f} V_2$ is said to be a *homomorphism* if

$$\langle u, v\rangle \in E_1 \Rightarrow \langle f(u), f(v)\rangle \in E_2.$$

A homomorphism is called a *strong homomorphism* if also the opposite implication holds, i.e. if

$$\langle u, v\rangle \in E_1 \Leftrightarrow \langle f(u), f(v)\rangle \in E_2.$$

Strong homomorphisms were introduced in 1958 by K. Čulik [2]. The key information about strong homomorphisms are given by the following lemma

Lemma 2 *For any graph $G = (V, E)$ and a pair of vertices u, v there exists a graph H and a strong homomorphism $G \xrightarrow{f} H$ such that $f(u) = f(v)$ if and only if $N_{\leftarrow}(u) = N_{\leftarrow}(v)$ and $N_{\rightarrow}(u) = N_{\rightarrow}(v)$.*

The proof (for undirected graphs) is given in [22]. However for the morphisms in the sense of (2.1) there exist no "local" characterizations. Moreover, for each graph G there is a morphism (2.1) to the singleton graph. Thereby, in the category of graphs in the sense of (2.1) the singleton graphs are exactly the null objects [2] of the category. However, neither the category of homomorphisms nor the category of strong homomorphisms has null-objects.

The graphs G for which the semigroup SEnd(G) of strong endomorphisms is equal to the automorphism group Aut(G) are said to be S-*unretractive* [21]. Small S-unretractive graphs are classified by Ulrich Knauer [23]. However, the monoid End(G) of graph endomorhisms in the sense of 2.1 is almost never equal to Aut(G), except if G is a singleton. Indeed, for every vertex $v \in V$ the mapping $G \xrightarrow{O_v} G$ such that $O_v(u) = v$ is always an endomorphism. It is easy to see that $\text{End}(G) = \text{Aut}(G) \cup \{O_v\}_{v \in V}$ if and only if G has no nontrivial congruence relations, i.e. if G is *simple*.

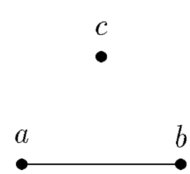


Figure 2.8: An S-unretractive graph which is not simple.

[2] An object O is said to be null-object if for every object A there is a unique morphism $A \longrightarrow O$

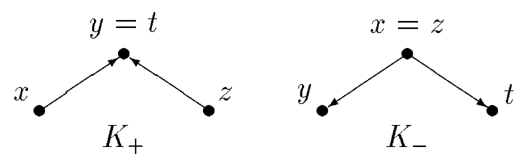
Each simple graph is S-unretractive because each strong homomorphism is a graph morphism in the sense of (2.1). The opposite is not true. For example the graph in the Figure 2.8 is S-unretractive but not simple, because the partition $\{\{a,b\},\{c\}\}$ represents a congruence relation. The mapping $f(a)=f(b)=a$ and $f(c)=c$ is a morphism in the sense of (2.1).

2.5 Strongly connected graphs

Let $G=(V,E)$ be an undirected graph. We define relations K_+ and K_- in the edge set E as follows

$$\begin{aligned} K_+ &= \{\langle xy, zy\rangle \in E\times E \mid xz \notin E\}, \\ K_- &= \{\langle xy, xt\rangle \in E\times E \mid yt \notin E\}. \end{aligned}$$

Let $\Gamma = K_+ \cup K_-$. In other words, the relation Γ consists of edge-pairs of two different types as shown in the figure below.



Relations K_+ ja K_- are both reflexive and symmetric. Therefore the transitive closure of Γ is an equivalence relation on the edge set E. The corresponding equivalence classes are called Γ-*classes*. It is clear that two edges e, e' belong to the same Γ-class iff there is a chain of edges

$$e = e_0, e_1, ..., e_\ell = e'$$

such that $\langle e_i, e_{i+1}\rangle \in \Gamma$. Edges $e_0, ..., e_\ell$ can be chosen in such a way that ℓ is odd and $\langle e_i, e_{i+1}\rangle \in K_+$ iff i is even. Roughly, we have a chain

$$e = e_0\ K_+\ e_1\ K_-\ e_2\ ...\ e_{\ell-2}\ K_-\ e_{\ell-1}\ K_+\ e_\ell = e'.$$

We write $e \equiv e'(\Gamma)$ if the edges e and e' belong to the same Γ-class. We say that the graph G is *strongly connected* if it is connected and there is a Γ-class F, such that $E = F \cup F^{-1}$. If $E' \subseteq E$ is an arbitrary subset of E then the set of vertices

$$V(E') = \{x \mid \exists y (xy \in E' \text{ or } yx \in E')\}$$

is called the *vertex part* of E'. And similarly, if $V' \subseteq V$ is an arbitrary subset of V then the set of edges

$$E(V') = \{xy \mid x, y \in V',\ xy \in E\}$$

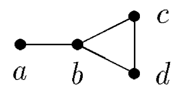


Figure 2.9: A connected graph that is not strongly connected

is called the *edge part* of V'. Graph G is called Γ-*connected* if there is a Γ-class F such that $E = V(F)$. It is obvious that for every Γ-class F the graphs $(V(F), F)$ and $(V(F), E(V(F)))$ are connected.

A connected graph may not be strongly connected. Consider the graph G in the Figure 2.9. If we divide the vertex set E of G into Γ-classes, we reach to a partition $\{E_0, E_1, E_2, E_3\}$ such that

$$\begin{aligned} E_0 &= \{ab, cb, db\} \\ E_1 &= \{ba, bc, bd\} \\ E_2 &= \{cd\} \\ E_3 &= \{dc\} \end{aligned}$$

Obviously this graph is connected but not strongly connected because there is no Γ-class F such that $F \cup F^{-1} = E$. For example the Γ-klass E_0 is not a suitable candidate for F because $E_0^{-1} = E_1$ and $E_0 \cup E_1 \neq E$. Indeed $cd \notin E_0 \cup E_1$.

All complete graphs are connected but obviously not strongly connected. A good example is also a graph (octaedron) in the Figure 6.17.

2.6 Simple graphs

A graph $G = (V, E)$ is called *simple* (or *prime*) if it has no nontrivial congruence relations. Equivalently, the graph G is simple if the only non-empty modules are G itself and the singleton subgraphs of G.

Theorem 4 *There exists no partition $E = E_r \coprod E_b$ such that the graphs $G_r = (V, E_r)$ and $G_b = (V, E_b)$ are both symmetric (non-directed), Γ-connected and $e_r \not\equiv e_b(\Gamma)$ for arbitrary $e_r \in E_r$ and $e_b \in E_b$.*

Proof. Suppose there exists such a partition. We can assume that E_r is a Γ-class. [3] From $E_r \subseteq \bar{E}_b$ and $E_b \subseteq \bar{E}_r$ it follows that the graphs G_r and G_b are complement-connected. Let us call the elements (edges) of E_r *red* and the elements of E_b *blue*.

[3] By definition of the Γ-connectivity there is a Γ-class $E_r' \subseteq E_r$ such that $V(E_r') = V$. Now taking $E_b' := V - E_r' \supseteq E_b$ we get a partition $E = E_r' \coprod E_b'$ with desired property.

For every vertex $v \in V$ there is a following partition of the vertex set V

$$V = \{v\} \coprod R_v \coprod B_v \coprod N_v,$$

where $R_v = \{w \mid vw \in E_r\}$ is the set of all red neighbours of v, $B_v = \{w \mid vw \in E_b\}$ is the set of all blue neighbours of v and $N_v = \{w \mid vw \notin E\}$ is the set of all non-neighbours of v. The sets R_v, B_v are nonempty because G_r and G_b are connected.

It is clear that the pair (B_v, R_v) is a diclique because if $x \in B_v$, $y \in R_v$ ja $xy \notin E$ then $vx \equiv vy(\Gamma)$ which is a contradiction.

Notice that if $x \in B_v$, $y \in N_v$ and $xy \in E$ then the edge xy is blue because $xv \equiv xy(\Gamma)$. Thereby, every edge between B_v and N_v is blue and similarly, every edge between R_v and N_v is red.

Now we show that there are only blue edges in the graph $(B_v, E(B_v))$. Indeed, if there is a red edge $e' \in E(B_v)$ then for every red edge e not in $E(B_v)$ (there is at least one such edge) $e \equiv e'(\Gamma)$ and therefore there exist vertices $x, y \in B_v$ and $z \notin B_v$ such that $xy \in E_r$, $zy \in E_r$ and $xz \notin E$. This is correct because E_r is a Γ-class. The vertex z is not in N_v, otherwise there would be a red edge zy between B_v and N_v. Also $z \neq v$ because $xy \notin E$ and by definition $vy \in E$. So we can conclude that $z \in R_v$ but then $xz \in E$ because (B_v, R_v) is diclique. A contradiction. So, we can draw an important conclusion:

$$\forall v \in V: \ E(B_v) \subseteq E_b.$$

Let $v, r, b \in V$ be arbitrary nodes such that $r \in R_v$ and $b \in B_v$. Then we know that $rb \in E$ because (R_v, B_v) is diclique. The edge rb is not blue, otherwise $r \in B_b$ and there is a red edge $vr \in E(B_b) \subseteq E_b$. Therefore rb is red and we can conclude that there are only red edges between R_v and B_v.

Hence, there are only red edges between R_v and $V - R_v = \{v\} \cup B_v \cup N_v$. But if $x \in R_v$ then there is at least one y such that $xy \in E_b$ (connectivity of G_b) and therefore $y \in R_v$ and $xy \in E(R_v)$. But the edge xy cannot be in the same Γ-class with any edge $e \in E(V - R_v)$, but we know that there are such edges ($B_v \neq \emptyset$). A contradiction with the Γ-connectivity of G_b. This proves the impossibility of the partition. $\square$

Theorem 5 *If $G = (V, E)$ is simple and $E \neq \emptyset$ then G is strongly connected.*

Proof. Suppose $G = (V, E)$ is prime and $F \subseteq E$ is an arbitrary Γ-class. Now we will show that $V(F)$ is module and therefore $V(F) = V$. Let $x, y \in V(F)$, $z \notin V(F)$ ja $xz \in E$. Graph $(V(F), F)$ is connected and hence there is a a sequence of vertices

$$x = x_0, x_1, ..., x_n = y$$

such that $x_i \in V(F)$ and $x_i x_{i+1} \in F$. We can prove now by induction that $yz \in E$. Indeed, $x_0 z = xz \in E$ by the assumption and if $x_i z \in E$ then $x_{i+1} z \in E$

as well because otherwise we get that $\langle x_i x_{i+1}, x_i z\rangle \in \Gamma$ which is impossible because $z \notin V(F)$. This implies $yz \in E$. The proof of the implication $zx \in E \Rightarrow zy \in E$ is similar.

Thereby, $V(F)$ is a module with at least two vertices and therefore $V(F) = V$ because of the simplicity of G. Let $E_r = F \cup F^{-1}$. Suppose $E_b = E - E_r \neq \emptyset$. Let $F' \subseteq E_b$ be a Γ-class containing an edge $xy \in F'$. It follows from the primality that $V(F') = V$ and therefore the graphs $G_r = (V, E_r)$ and $G_b = (V, E_b)$ are both symmetric, Γ-connected and $e_r \not\equiv e_b(\Gamma)$ for arbitrary $e_r \in E_r$ and $e_b \in E_b$. This is impossible by Theorem 4. Therefore, $E = F \cup F^{-1}$ and hence G is strongly connected. □

Theorem 6 *If G and its complement graph $\bar{G}$ are both strongly connected then G is simple.*

Proof. If $\emptyset \neq M \neq V$ is a module there is at least one vertex in $V - M$.

We show that the subgraph $(V - M, E(V - M))$ is not edgeless. Indeed, if it is edgeless then for every $z \in V - M$ there is an $x \in M$ such that $xy \in E$ because of the connectivity of G. But that implies for every vertex $y \in M$ there is an edge $yz \in E$ because M is a module. So, $(M, V - M)$ must be a diclique and so $\bar{G}$ is not connected. A contradiction. So, we may assume that there is at least one edge in $(V - M, E(V - M))$.

Now we can prove that $E(M) = \emptyset$. Suppose $E(M)$ is not empty. As G is strongly connected then $e \equiv e'(\Gamma)$ for every $e \in E(M)$ and $e' \in E(V - M)$. So, there must be $x, y \in M$ and $v \notin M$ such that $xy \in E$, $xv \in E$ and $yv \notin E$. But it is impossible because M is a module. Therefore M is an edgeless subgraph of G.

As M is a module of $\bar{G}$ as well, we can prove similarly that M is an edgeless subgraph of $\bar{G}$. But this implies that M is a complete subgraph of G. This means that M is complete and edgeless at the same time. It is possible only if $|M| = 1$. Therefore G is simple. □

These two theorems imply that a graph $G = (V, E)$ is simple iff either $|V| < 3$ or G and $\bar{G}$ are both strongly connected.

2.7 Almost all graphs are simple

A finite undirected graph $G = (V, E)$ is said to be *standard* if $V = \{1, 2, ..., |V|\}$. We say that *almost all finite graphs* have a property $\mathcal{A}$ if

$$\lim_{n\to\infty} \frac{|\mathcal{G}_{\mathcal{A}}(n)|}{|\mathcal{G}(n)|} = 1,$$

where $\mathcal{G}(n)$ is the set of all standard graphs with n vertices and $\mathcal{G}_{\mathcal{A}}(n)$ is the set of all graphs with n vertices having the property $\mathcal{A}$.

Theorem 7 *Almost all finite undirected graphs are simple.*

Proof. Let $\mathcal{G}_p(n)$ be the set of all simple standard graphs with n vertices and $\mathcal{G}_s(n)$ be the set of all standard graphs G with at least one module $M \subseteq G$ such that $|M|= s$. Therefore,

$$|\mathcal{G}_p(n)| \geq |\mathcal{G}(n)| - \sum_{s=2}^{n-1} |\mathcal{G}_s(n)| \; .$$

Let M be a fixed s-element subset of $n = \{0, ..., n-1\}$. It is easy to see that the number of graphs $G = (n, E)$, such that M is a module in G, is equal to

$$2^{n-s} \cdot 2^{\mathrm{C}_s^2} \cdot 2^{\mathrm{C}_{n-s}^s}, \qquad (2.4)$$

where $\mathrm{C}_n^k := \frac{n!}{k!(n-k)!}$ are the binomial coefficients. Indeed, there are $2^{\mathrm{C}_s^2}$ possibil-

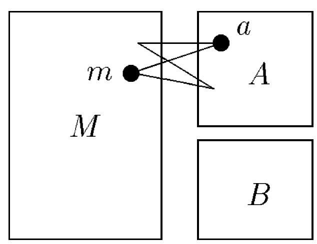


Figure 2.10: A graph with a module $|M|= s$ and set A of vertices adjacent to M.

ities to choose a subgraph M and $2^{\mathrm{C}_{n-s}^2}$ independent possibilities to choose the subgraph $V \backslash M$. If A is the subset of $V \backslash M$ consisting of all vertices $a \in V \backslash M$ such that $\langle m, a \rangle$ for some $m \in M$ (Figure 2.10). As M is a module, a should be adjacent with all vertices in M. Hence there are 2^{n-s} possible ways to choose edges between M and $V \backslash M$ assuming M is a module. Therefore the number of graphs with a module $|M|= s$ is indeed equal to (2.4). We have the following inequality

$$\begin{aligned} |\mathcal{G}_s(n)| &\leq \mathrm{C}_n^s 2^{n-s} 2^{\mathrm{C}_s^2} 2^{\mathrm{C}_{n-s}^2} = \mathrm{C}_n^s 2^{n-s} 2^{\mathrm{C}_n^2 - s(n-s)} \\ &= \mathrm{C}_n^s 2^{\mathrm{C}_n^2 - (s-1)(n-s)}. \end{aligned}$$

From the equality $|\mathcal{G}(n)|= 2^{\mathrm{C}_n^2}$ it follows that

$$\frac{|\mathcal{G}_p(n)|}{|\mathcal{G}(n)|} \geq 1 - \sum_{s=2}^{n-1} f(s),$$

where $f(s) = C_n^s 2^{-s(s-1)(n-s)}$. We will now study the properties of the function f inside the intrerval $[2, n-1]$. It turns out that f has a global maximum in 2. Indeed, the function f is decreasing in $[2, [(n-1)/2]]$ because

$$f(s+1)/f(s) = \frac{n-s}{s+1} 2^{2s-n} \leq 1, \tag{2.5}$$

whenever $2 \leq s \leq (n-1)/2$. Therefore $f(2)$ is a global maximum in $[2, [(n-1)/2]]$. But

$$f(n-s) = \frac{s+1}{n-s} f(s+1) \leq f(s+1)$$

whenever $2 \leq s \leq (n-1)/2$. Therefore, $f(2)$ is a global maximum if n is odd. If n is even, we have to compare $f(2)$ and $f(n/2)$. From the inequality (2.5) we get

$$\begin{aligned} f(n/2) &= \frac{n+2}{4n} f(n/2-1) \leq \frac{n+2}{4n} f(2) \\ &\leq f(2), \end{aligned}$$

because $2 \leq n/2 - 1 \leq (n-1)/2$. Accordingly, $f(2) = n(n-1)2^{-(n-1)}$ is a global maximum of f and therefore

$$\sum_{s=2}^{n-1} f(s) \leq n \cdot f(2) \leq \frac{n^3}{2^{n-1}}.$$

As $\lim_{n\to\infty} n^3/2^{n-1} = 0$, we have $\lim_{n\to\infty} \frac{|\mathcal{G}_p(n)|}{|\mathcal{G}(n)|} = 1$. $\square$

A radical map in the class of all graphs (not necessarily finite or undirected) is defined and a complete characterization of the corresponding semisimple graphs is given. It is proved here that the congruence lattice of finite graph satisfies the Jordan-Dedekind chain condition.

3.1 Introduction

We are studying the congruence lattice of a graph without any restrictions (finiteness or undirectedness). It is proved here that if ρ is an arbitrary congruence relation of G then the *principal ideal* $\rho^{\bigtriangledown}$ is isomorphic to the direct product of the congruence lattices of all ρ-classes and its *dual* $\rho^{\bigtriangleup}$ is always isomorphic to the congruence lattice of factor-graph G/ρ. We define a radical map as a mapping (with certain properties) from the class of all graphs to the class of all sets. We prove that taking the greatest lower bound of all co-atoms of the congruence lattice defines a radical (the $\Im$-radical). We will show that a graph G is $\Im$-semisimple ($\Im(G) = 0$) if and only if at least one of the following conditions holds.

- G is simple.
- G is edgeless.
- G is complete.
- G is linear.

Finally we prove that the congruence lattice of a finite graph satisfies the Jordan-Dedekind chain condition.

3.2 Principal ideals in the congruence lattice of a graph

Let $\operatorname{Con} G$ denote the set of all congruence relations of graph G. Note that $\operatorname{Con} G$ is partially ordered with respect to the inclusion relation $\subseteq$.

Theorem 8 *$\operatorname{Con} G$ is a complete lattice for every graph $G = (V, E)$.*

Proof. Let us prove at first that the intersection $\cap\mathcal{A}$ of every nonempty subset $\mathcal{A}$ of $\operatorname{Con} G$ is a congruence relation of G. It is obvious that $\cap\mathcal{A}$ is an equivalence relation. Let $\langle x, x'\rangle, \langle y, y'\rangle \in \cap\mathcal{A}$ and $\langle x, y\rangle \notin \cap\mathcal{A}$. Consequently there is a congruence relation $\rho \in A$ such that $\langle x, y\rangle \notin \rho$. As ρ is a congruence relation it follows from $\langle x, x'\rangle, \langle y, y'\rangle \in \cap\mathcal{A} \subseteq \rho$ that

$$\langle x, y\rangle \in E \leftrightarrow \langle x', y'\rangle \in E.$$

Therefore, $\cap\mathcal{A}$ is a congruence relation. Note that $\cap\mathcal{A}$ is also the greatest lower bound of $\mathcal{A}$. It remains to prove that there is also the least upper bound for every nonempty subset $\mathcal{A} \subseteq \mathrm{Con}\, G$. Indeed, if $\mathcal{A}$ is nonempty then the set

$$\mathcal{A}^{\triangle} = \{\sigma \mid \sigma \in \mathrm{Con}\, G,\ \forall\rho : \rho \in \mathcal{A} \Rightarrow \rho \subseteq \sigma\}$$

is nonempty because the universal congruence relation $1_G = V \times V$ belongs to $\mathcal{A}^{\triangle}$. And therefore $\cap(\mathcal{A}^{\triangle})$ is a congruence relation and it is easy to verify that it coincides with the least upper bound of $\mathcal{A}$. □

Theorem 9 *If $G = (V, E)$ is a graph and $\rho \in \mathrm{Con}\, G$ then*

$$\rho^{\triangle} \cong \mathrm{Con}\, G/\rho.$$

A suitable isomorphism can be defined as follows:

$$\begin{cases} \rho^{\triangle} \longrightarrow \mathrm{Con}\, G/\rho \\ \sigma \mapsto \bar{\sigma}, \end{cases}$$

where $(v/\rho, w/\rho) \in \bar{\sigma} \Leftrightarrow (v, w) \in \sigma$.

Proof. Before giving a proof of the theorem let us prove the following lemma.

Lemma 1 *If h is epimorphism then for every pair of morphisms g_1, g_2*

$$\mathrm{Ker}(g_1 \circ h) \subseteq \mathrm{Ker}(g_2 \circ h) \leftrightarrow \mathrm{Ker}\, g_1 \subseteq \mathrm{Ker}\, g_2.$$

Proof. If $\mathrm{Ker}(g_1 \circ h) \subseteq \mathrm{Ker}(g_2 \circ h)$ and $\langle x, y\rangle \in \mathrm{Ker}\, g_1$ then $g_1(x) = g_1(y)$. As h is onto, there are x' and y' such that $h(x') = x$ and $h(y') = y$. Consequently $g_1(h(x')) = g_1(h(x'))$ and therefore $\langle x', y'\rangle \in \mathrm{Ker}(g_1 \circ h)$. By the assumption $\langle x', y'\rangle \in \mathrm{Ker}(g_2 \circ h)$ and therefore $g_2(h(x')) = g_2(h(x'))$ which is equivalent to $\langle x, y\rangle \in \mathrm{Ker}\, g_2$.

If $\mathrm{Ker}\, g_1 \subseteq \mathrm{Ker}\, g_2$ and $\langle x', y'\rangle \in \mathrm{Ker}(g_1 \circ h)$ then $g_1(h(x')) = g_1(h(x'))$ and therefore $g_2(h(x')) = g_2(h(x'))$ which is equivalent to $\langle x', y'\rangle \in \mathrm{Ker}(g_2 \circ h)$. This completes the proof of the lemma. □

We know that every congruence relation of the quotient graph G/ρ is the kernel of some morphism $G/\rho \xrightarrow{g} H$. Let $G \xrightarrow{\pi} G/\rho$ be the natural projection. We define a mapping $\mathrm{Con}\, G/\rho \xrightarrow{f} \rho^{\triangle}$ as follows:

$$f \colon \mathrm{Ker}\, g \mapsto \mathrm{Ker}(g \circ \pi).$$

f is well-defined because if $G/\rho \xrightarrow{g_1} H_1$ and $G/\rho \xrightarrow{g_2} H_2$ are two morphisms and $\operatorname{Ker} g_1 = \operatorname{Ker} g_2$ then by lemma 1 we get $\operatorname{Ker}(g_1 \circ \pi) = \operatorname{Ker}(g_2 \circ \pi)$. And more, it follows from the lemma that f is injective and order-preserving.

It remains to prove that f is onto. Let $\delta \in \operatorname{Con} G$ and $\rho \subseteq \delta$. Then there is a graph H and a morphism $G \xrightarrow{g} H$ such that $\operatorname{Ker} g = \delta$. Therefore there is a morphism $G/\rho \xrightarrow{h} H$ such that $h \circ \pi = g$ and thus

$$\delta = \operatorname{Ker} g = \operatorname{Ker}(h \circ \pi) = f(\operatorname{Ker} h).$$

It shows that f is indeed onto and consequently f is a lattice isomorphism. □

Theorem 10 *If G is a graph, $\rho \in \operatorname{Con} G$ is an arbitrary congruence relation and $G/\rho = \{G_j\}_{j \in \mathcal{J}}$ then*

$$\rho^{\nabla} \cong \prod_{j \in \mathcal{J}} \operatorname{Con} G_j.$$

Proof. Let $G_j \xrightarrow{\iota_j} G \quad (j \in \mathcal{J})$ be the natural injections. Define a mapping $\operatorname{Con} G \xrightarrow{\phi} \prod_{j \in \mathcal{J}} \operatorname{Con} G_j$ as follows:

$$\phi\colon \operatorname{Ker} f \mapsto \{\operatorname{Ker}(f \circ \iota_j)\}_{j \in \mathcal{J}}.$$

Let $\rho^{\nabla} \xrightarrow{\iota} \operatorname{Con} G$ be a natural monomorphism.

Lemma 2 *If $\sigma_1, \sigma_2 \in \rho^{\nabla}$ then*

$$\sigma_1 \subseteq \sigma_2 \Leftrightarrow (\phi \circ \iota)(\sigma_1) \leq (\phi \circ \iota)(\sigma_2)$$

Proof. Let $\operatorname{Ker} f_1 = \iota(\sigma_1)$ and $\operatorname{Ker} f_2 = \iota(\sigma_2)$. If $\sigma_1 \subseteq \sigma_2$ then also $\operatorname{Ker} f_1 \subseteq \operatorname{Ker} f_2$ because ι is a lattice embedding. Consequently $\operatorname{Ker}(f_1 \circ \iota_j) \subseteq \operatorname{Ker}(f_2 \circ \iota_j)$ for every $j \in \mathcal{J}$ and thus $\phi\iota(\sigma_1) \leq \phi\iota(\sigma_2)$.

If $\phi\iota(\sigma_1) \leq \phi\iota(\sigma_2)$ then by definition

$$\operatorname{Ker}(f_1 \circ \iota_j) \subseteq \operatorname{Ker}(f_2 \circ \iota_j) \tag{3.1}$$

for every $j \in \mathcal{J}$. If $\langle x, y\rangle \in \iota(\sigma_1) = \operatorname{Ker} f_1$ then $\langle x, y\rangle \in \rho$ because of the inequality $\iota(\sigma_1) \subseteq \rho$. Consequently there exists $j \in \mathcal{J}$ such that $x, y \in G_j$ and therefore $\iota_j(x) = x$ and $\iota_j(y) = y$. Now we get from $f_1(x) = f_1(y)$ that $\langle x, y\rangle \in \operatorname{Ker}(f_1 \circ \iota_j)$ and by inequality (3.1) $\langle x, y\rangle \in \operatorname{Ker}(f_2 \circ \iota_j)$. Therefore $f_2(x) = f_2\iota_j(x) = f_2\iota_j(y) = f_2(y)$ and this means that $\langle x, y\rangle \in \operatorname{Ker} f_2$. Thus we have proven the inequality $\iota(\sigma_1) \subseteq \iota(\sigma_2)$. As ι is a lattice embedding it follows that $\sigma_1 \subseteq \sigma_2$. □

We now return to the proof of the theorem. It follows from the lemma that $\phi\iota$ is injective and order preserving. It remains to show that $\phi\iota$ is onto. Let $\{\sigma_j\}_{j\in\mathcal{J}}$ be an arbitrary element of $\prod_{j\in\mathcal{J}} \operatorname{Con} G_j$. Let

$$\sigma = \bigcup_{j\in\mathcal{J}} \sigma_j = \{\langle x,y\rangle \mid \exists j \in \mathcal{J} : \langle x,y\rangle \in \sigma_j\}.$$

We will show first that σ is a congruence relation and $\sigma \in (\rho]$. It is obvious that σ is an equivalence relation. Let $x, y, x', y' \in V$ be arbitrary nodes of G, $x\sigma x'$, $y\sigma y'$ and $\neg(x\sigma y)$. Consequently there are i and j in $\mathcal{J}$ such that $\langle x, x'\rangle \in \sigma_i$ and $\langle y, y'\rangle \in \sigma_j$, but $\langle x, y\rangle \notin \sigma_k$ for all $k \in \mathcal{J}$.

If $i = j$ then $\sigma_i = \sigma_j$ which implies

$$\langle x,y\rangle \in E \leftrightarrow \langle x',y'\rangle \in E \tag{3.2}$$

because σ_i is a congruence relation on G_i. If $i \neq j$ then $\neg(x\rho y)$ and therefore

$$x\rho x',\ y\rho y',\ \neg(x\rho y),$$

because $x, x' \in G_i \in G/\rho$ and $y, y' \in G_j \in G/\rho$. As ρ is a congruence relation we get (3.2). Therefore $\sigma \in \operatorname{Con} G$.

It is clear that $\sigma \subseteq \rho$ because if $\langle x,y\rangle \in \sigma$ then there exists $i \in \mathcal{J}$ such that $\langle x,y\rangle \in \operatorname{Con} G_i$. Thus $x, y \in G_i$ and therefore $\langle x,y\rangle \in \rho$.

And finally, we show that for all $\sigma \in (\rho]$ $\phi\iota(\sigma) = \{\sigma_j\}_{j\in\mathcal{J}}$. Let $\sigma = \iota(\sigma) = \operatorname{Ker} f$. Then $\phi\iota(\sigma) = \{\operatorname{Ker}(f\circ\iota_j)\}_{j\in\mathcal{J}}$ and it remains to show that $\operatorname{Ker}(f\circ\iota_j) = \sigma_j$.

Indeed, if $\langle x,y\rangle \in \operatorname{Ker}(f\circ\iota_j)$ then $x, y \in G_j$, $\iota_j(x) = x$ and $\iota_j(y) = y$. Thereby $\langle x,y\rangle \in \operatorname{Ker} f = \sigma$ and there exists $k \in \mathcal{J}$ such that $\langle x,y\rangle \in \sigma_k$ and thus $\langle x,y\rangle \in G_k$. Consequently $j = k$ and therefore $\langle x,y\rangle \in \sigma_j$.

If $\langle x,y\rangle \in \sigma_j$ then $x, y \in G_j \in G/\rho$ and $\langle x,y\rangle \in \cup_{i\in\mathcal{J}}\sigma_i = \sigma = \operatorname{Ker} f$. Therefore $\langle x,y\rangle \in \operatorname{Ker}(f\circ\iota_j)$. □

3.3 Radical maps

Let $\mathcal{S}$ and $\mathcal{G}$ be the class of all sets and the class of all graphs respectively. Let $\mathcal{H} \subseteq \mathcal{G}$ be a subclass of $\mathcal{G}$. A mapping $\mathcal{H} \stackrel{r}{\longrightarrow} \mathcal{S}$ is called a *radical map* in $\mathcal{H}$ if the following three conditions hold:

- $r(G) \in \operatorname{Con} G$
- If $G, H \in \mathcal{H}$ and $G \stackrel{f}{\longrightarrow} H$ is epimorphism then

$$\langle x,y\rangle \in r(G) \Rightarrow \langle f(x), f(y)\rangle \in r(H)$$

- $r(G/r(G)) = 0$.

A graph G is said to be *r-radical* if $r(G) = 1$ and G is said to be *r-semisimple* if $r(G) = 0$. Here 0 and 1 denote trivial congruence relations. The following theorem gives us an important example of a radical.

Theorem 11 *Let $\mathcal{H}$ be the class of all undirected graphs. Let G be an arbitrary graph in $\mathcal{H}$ and $c(G)$ is an equivalence relation corresponding to the partition of G into its maximal connected components. Then the mapping $\mathcal{H} \xrightarrow{c} \mathcal{S}$ is a radical in the class of all undirected graphs.*

Proof. Let $G = (V, E)$ and $H = (V', E')$ be undirected graphs. It is obvious that $c(G) \in \operatorname{Con} G$. Let $G \xrightarrow{f} H$ be an epimorphism and $\langle x, y\rangle \in c(G)$. Accordingly x and y lie in the same maximal connected component of G and therefore there must be a chain of vertices

$$x = v_0, ..., v_\ell = y$$

such that $v_i v_{i+1} \in E$. As f is a morphism then for every component v_i of the chain

$$f(x) = f(v_0), f(v_1), ..., f(v_\ell) = f(y)$$

either there is an edge $\langle f(v_i), f(v_{i+1})\rangle \in E'$ or $f(v_i) = f(v_{i+1})$. This means that $f(x)$ and $f(y)$ lie in the same maximal connected component of H and therefore $\langle f(x), f(y)\rangle \in c(H)$.

As $G/c(G)$ is always edgeless then all the maximal connected components of $G/c(G)$ consist of single vertex. Therefore $c(G/c(G)) = 0$. $\square$

It is easy to verify that a graph G is *r-radical* if and only if it is *connected* and G is *r-semisimple* if and only if it is *edgeless*. Let $\bar{c}(G)$ denote the partition of G into the maximal complement-connected components. It is easy to prove that $\mathcal{H} \xrightarrow{\bar{c}} \mathcal{S}$ is a radical and G is $\bar{c}$- *radical* [$\bar{c}$ − *semisimple*] iff G is *complement-connected* [*complete*].

3.4 Spinrad's congruence relation

It turns out that a congruence relation can be defined as an equivalence relation with equivalence classes satisfying a certain condition. Namely, an equivalence relation ρ on the vertex set V is a congruence relation of G if and only if all the ρ-classes are modules of G.

This has been pointed out by Hemminger [11] in the case of undirected graphs. Ehrenfeucht and Rozenberg [24] have proved similar results for directed graphs and more general objects called 2-structures.

Modules have many different names in the literature. They are called *clans* in [24],[25],[26], *externally related subsets* in [27] and *blocks* in [33].

We say that two sets *overlap* if they intersect and neither of them contains the other. A *decomposable set family* $\mathcal{F}$ on a set V is a family of subsets of V with the following properties:

- V and its singleton subsets are members of $\mathcal{F}$;
- Whenever X and Y are overlaping members of $\mathcal{F}$, then $X \cap Y$, $X \cup Y$, $X - Y$ and $X \triangle Y$ are also members of $\mathcal{F}$, where $\triangle$ is the symmetric set difference.

It is proved in [18] that

Theorem 12 *The family of all modules of an undirected graph is a decomposable set family.*

Modular decomposition of a graph has been studied by several researchers in many different areas. A nice overview is given by Möhring and Radermacher [17]. Spinrad [16] developed an $O(n^2)$ algorithm to find the modular decomposition which has been used to develop fastest known algorithms for several combinatorial problems ([19]). We prove that the modular decomposition is related with certain radical map.

As we want to avoid the finiteness assumption we need to prove a more powerful result about the union of an infinite family of overlaping modules.

Theorem 13 *If $\mathcal{M}$ is a nonempty set of modules and $\cap\mathcal{M} \neq \emptyset$ then the union $\cup\mathcal{M}$ is a module.*

Proof. Let $x, y \in \cup\mathcal{M}$ and $z \in V - \cup\mathcal{M}$. Accordingly there exists $A, B \in \mathcal{M}$ such that $x \in A$ and $y \in B$. As the intersection is not empty, there exists $t \in \cap\mathcal{M} \subseteq A \cap B$. It follows now from theorem 12 that $M = A \cup B$ is a module, $x, y \in M$ and $z \in V - M$. Statement of the theorem directly follows from the definition of module. □

For every vertex x of $G = (V, E)$ we have a set

$$\mathcal{M}(x) := \{M \mid x \in M \neq V,\ M \text{ is a module}\}$$

of all nontrivial modules containing the vertex x. Let $\mathcal{M}_x = \cup\,\mathcal{M}(x)$. It follows from theorem 13 that $\mathcal{M}_x$ is a module. Let $\mathcal{S} = \{\mathcal{M}_x \mid x \in V\}$. It is easy to verify that if there is at least two vertices in G, the following four conditions hold:

- $\mathcal{S} \subseteq \mathcal{P}(V)$,
- $\emptyset \notin \mathcal{S}$,
- $\bigcup_{x\in V} \mathcal{M}_x = V$,
- $\mathcal{M}_x \cap \mathcal{M}_y \neq \emptyset \Rightarrow \mathcal{M}_x = \mathcal{M}_y$.

Thereby we can say that $\mathcal{S}$ is a partition of the vertex set V of G. Let us denote the corresponding equivalence relation by $s(G)$. [4] As every equivalence class of $s(G)$ is a module, we can say that $s(G)$ is a congruence relation of G. Let us call it *Spinrad's congruence relation.*

Theorem 14 *If G has at least two vertices then $s(G)$ is an upper bound (in $\mathrm{Con}\, G$) of all congruence relations not equal to* 1.

Proof. Let $\rho \neq 1$ is a congruence relation of G and $\sigma = s(G)$. Let $x \in V$ be an arbitrary vertex, K is a ρ-class (module) containing the vertex x and L is a σ-class (module) containing x. By definition of $s(G)$ we have $K \subseteq L$. If $\langle x, y\rangle \in \rho$ then $x, y \in K$ and therefore $x, y \in L$ and thus $\langle x, y\rangle \in \sigma$. Accordingly $\rho \subseteq \sigma$ and thereby σ is an upper bound of all congruence relations different from 1. $\square$

Lemma 3 *If $\delta \neq 1$ is an upper bound of all congruence relations of G different from 1 then δ is a co-atom of* $\mathrm{Con}\, G$.

Proof. If $\delta \subset \sigma \subseteq 1$ then $\sigma = 1$ because otherwise $\sigma \subseteq \delta$ which leads us to the contradiction $\delta \subset \delta$. $\square$

Corollary 1 *For every graph G the Spinrad's congruence relation $s(G)$ is either equal to 1 or it is a unique co-atom of the congruence lattice* $\mathrm{Con}\, G$.

Lemma 4 *If there are no co-atoms in $\mathrm{Con}\, G$ and $G \xrightarrow{f} H$ is an epimorphism then there are no co-atoms in* $\mathrm{Con}\, H$.

Proof. If there is a co-atom ρ in $\mathrm{Con}\, H$ then there is a co-atom in the dual principal ideal $(\mathrm{Ker}\, f)^{\triangle}$ and consequently there is a co-atom in $\mathrm{Con}\, G$. Indeed, the mapping $\mathrm{Con}\, H \xrightarrow{\phi} (\mathrm{Ker}\, f)^{\triangle}$, $\mathrm{Ker}\, h \mapsto \mathrm{Ker}(h \circ f)$ is a lattice isomorphism and therefore $\phi(\rho)$ is a co-atom of $\mathrm{Con}\, G$. $\square$

Theorem 15 *The mapping $G \mapsto s(G)$ is a radical in the class of all graphs.*

Proof. We know that $s(G)$ is a congruence relation and either $s(G)$ is equal to 1 or $s(G)$ is a co-atom of $\mathrm{Con}\, G$. Accordingly there is at most two elements in $\mathrm{Con}(G/s(G))$ and therefore $s(G/s(G)) = 0$.

Let $G \xrightarrow{f} H$ be an epimorphism and $\langle x, y\rangle \in s(G)$. If $s(H) = 1$ then it is clear that $\langle f(x), f(y)\rangle \in s(H)$. If $s(G) = 1$ then by lemma 4 we have $s(H) = 1$ and therefore $\langle f(x), f(y)\rangle \in s(H)$. Consequently, we can assume that neither $s(G)$

[4] If G is a singleton graph we take $s(G) = 1$.

nor $s(H)$ is equal to 1. Therefore by the corollary 1 $s(G)$ and $s(H)$ are unique co-atoms in $\operatorname{Con} G$ and $\operatorname{Con} H$ respectively. Let $H \xrightarrow{\pi} H/s(H)$ be the natural projection. As the mapping $\phi: \operatorname{Ker} h \mapsto \operatorname{Ker}(h \circ f)$ ($H \xrightarrow{h} \cdot$ is a morphism) is an isomorphism between $\operatorname{Con} H$ and $(\operatorname{Ker} f)^{\triangle}$, the image $\operatorname{Ker}(\pi \circ f)$ of the co-atom $s(H) = \operatorname{Ker} \pi$ is a co-atom as well and therefore $\operatorname{Ker}(\pi \circ f) = s(G)$. As $\langle x, y \rangle \in s(G)$, we have $\pi(f(x)) = \pi(f(y))$ and $\langle f(x), f(y) \rangle \in \operatorname{Ker} \pi = s(H)$. □

3.5 Uniqueness of the simple quotient

Theorem 16 *If there is a co-atom ρ in $\operatorname{Con} G$ such that there is at least 3 vertices in G/ρ then ρ is a unique co-atom of $\operatorname{Con} G$ and furthermore, ρ is the least upper bound of all congruence relations different from 1.*

Proof. Let $G = (V, E)$ and $\rho \in \operatorname{Con} G$ is a co-atom such that $|G/\rho| \geq 3$. Let us assume that there is a congruence relation σ not comparable with ρ. We will obtain a contradiction. Note that there exists a σ-class M and ρ-class G_i such that $M \cap G_i \neq \emptyset$ and $G_i \not\subseteq M$. As M and G_i are intersecting modules, their union $M \cup G_i$ is a module by theorem 12. We define now the following sets of modules:

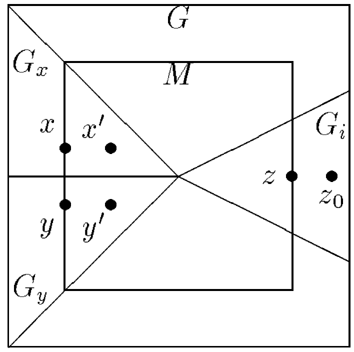
$$\begin{aligned} \mathcal{M} &= \{M \cup G_j \mid G_j \in G/\rho, \quad G_j \cap M \neq \emptyset\} \\ \mathcal{N} &= \{G_\ell \mid G_\ell \in G/\rho, \quad G_\ell \cap M = \emptyset\}. \end{aligned}$$

As $\cap \mathcal{M} \neq \emptyset$ then by theorem 13 $\cup \mathcal{M}$ is a module. The set $\mathcal{N}$ is empty because otherwise we have a partition of G into the modules

$$G = (\cup \mathcal{M}) \coprod [\coprod_{G_\ell \in \mathcal{N}} G_\ell]$$

and thus the corresponding equivalence relation ρ' is a congruence relation such that $\rho \subset \rho' \subset 1$ ($\rho \neq \rho'$). This is impossible because ρ is a co-atom. So, $M \cap G_j \neq \emptyset$ for every $G_j \in G/\rho$.

As $G_i \not\subseteq M$, there is a vertex $z_0 \in G_i - M$. Let $x, y \in G - G_i$ be arbitrary vertices not in $G - G_i$ and $z \in G_i$ is an arbitrary vertex in G_i. Let $y \in G_y \in G/\rho$, $x \in G_x \in G/\rho$, As $M \cup G_j$ is not empty for every j, there must be $y' \in M \cap G_y$ and $x' \in M \cap G_x$.



Now we get a chain of implications

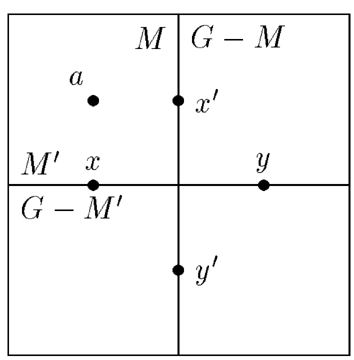
$$\begin{aligned} xz \in E &\Rightarrow xz_0 \in E \quad (G_i \text{ is a module}) \\ &\Rightarrow x'z_0 \in E \quad (G_x \text{ is a module}) \\ &\Rightarrow y'z_0 \in E \quad (M \text{ is a module}) \\ &\Rightarrow yz_0 \in E \quad (G_y \text{ is a module}) \\ &\Rightarrow yz \in E \quad (G_i \text{ is a module}) \end{aligned}$$

showing that $G - G_i$ is a module. Therefore we have a congruence partition $G/\rho'' = \{G_i, G - G_i\}$ and $\rho \subseteq \rho'' \subset 1$. Accordingly $\rho = \rho''$ but then there is olny two ρ-classes. This is impossible because of the assumption $|G/\rho| \geq 3$. □

Theorem 17 *Every two simple quotient graphs of a graph G are isomorphic.*

Proof. Let G/ρ be a simple graph. It follows from theorem 9 that ρ is a co-atom of $\operatorname{Con} G$. If $|G/\rho| \geq 3$ then by theorem 16 we have that ρ is a unique co-atom and therefore G/ρ is a unique simple quotient of G.

Let $|G/\rho| = |G/\sigma| = 2$. It is obvious that ρ and σ are co-atoms of $\operatorname{Con} G$. Let $G/\rho = \{M', M - M'\}$ and $G/\sigma = \{M, G - M\}$. Without loss of generality we may assume that $M \cap M' \neq \emptyset$. Let $a \in M \cap M'$. Let $x \in G'$, $y \in G - G'$, $x' \in M$ and $y' \in G - M$ be arbitrary vertices. We will show that $xy \in E$ iff $x'y' \in E$ (or $xy \in E$ iff $y'x' \in E$) and therefore the factor-graphs G/ρ and G/σ are isomorphic.



Let us assume first that $M' \cup M \neq G$. Consequently, $G - (M' \cap M)$ is a module because $(G - M') \cap (G - M) = G - (M' \cup M) \neq \emptyset$ and $G - (M' \cap M) = (G - M') \cup (G - M)$. But now

$$\begin{aligned} xy \in E &\Rightarrow ay \in E \quad (M' \text{ is a module}) \\ &\Rightarrow ay' \in E \quad (G - (M' \cap M) \text{ is a module}) \\ &\Rightarrow x'y' \in E \quad (M \text{ is a module}). \end{aligned}$$

If $M' \cup M = G$ then $M - M' = G - M'$ and $M' - M = G - M$. Thereby $y' \in M$, $y \in M'$ and we have a chain of implications

$$\begin{aligned} xy \in E &\Rightarrow y'y \in E \quad (M \text{ is a module}) \\ &\Rightarrow y'x' \in E \quad (M' \text{ is a module}) \end{aligned}$$

□

3.6 The $\Im$-radical

Let $\mathcal{G}$ be the class of all graphs and $\mathcal{S}$ be a class of all congruence relations of all graphs. Let $\mathcal{G} \xrightarrow{\Im} \mathcal{S}$ be a mapping such that $\Im(G) = 1$ if there are no co-atoms in $\mathrm{Con}\, G$ and otherwise $\Im(G)$ is equal to the greatest lower bound of all co-atoms in $\mathrm{Con}\, G$.

Theorem 18 *A mapping $G \mapsto \Im(G)$ is a radical in the class of all graphs.*

Proof. It is clear that $\Im(G) \in \mathrm{Con}\, G$. It follows from theorem 9 that $\Im(G/\Im(G)) = 0$.

Let $G \xrightarrow{f} H$ be an epimorphism and $\langle f(x), f(y)\rangle \notin \Im(H)$. Consequently there is a co-atom $\mathrm{Ker}\, h \in \mathrm{Con}\, H$ ($H \xrightarrow{h} \cdot$ is a morphism) such that $\langle f(x), f(y)\rangle \notin \mathrm{Ker}\, h$ and thus $\langle x, y\rangle \notin \mathrm{Ker}(h \circ f)$. We know that the mapping $\mathrm{Ker}\, h \mapsto \mathrm{Ker}(h \circ f)$ is an isomorphism between $\mathrm{Con}\, H$ and $(\mathrm{Ker}\, f)^{\triangle}$ and therefore $\mathrm{Ker}(h \circ f)$ is a co-atom in $\mathrm{Con}\, G$. Accordingly $\langle x, y\rangle \notin \Im(G)$ and thus $\Im$ is a radical. □

If $G = (V, E)$ is a linearly ordered set and $\rho \in \mathrm{Con}\, G$ is an equivalence relation. ρ is called a *cut* of G if there are subgraphs G_0, G_1 such that $G/\rho = \{G_0, G_1\}$ and there is a vertex $v \in V$ such that for arbitrary vertex $x \in V$

$$x \in G_0 \Leftrightarrow xv \in E.$$

It is clear that every cut of G is a congruence relation of G. It is obvious that if G is a linear ordering then all its cuts intersect to zero and therefore G is $\Im$-semisimple. So, we can say that a proof of the following theorem is obvious.

Theorem 19 *If G is either simple, edgeless, complete or linear then G is $\Im$-semisimple.*

Furthermore, it turns out that also the inverse statement is true.

Theorem 20 *A graph G is $\Im$-radical iff there are no co-atoms in* $\operatorname{Con} G$ *and G is $\Im$-semisimple iff it satisfies at least one of the following conditions:*

- *G is simple,*
- *G is edgeless,*
- *G is complete,*
- *G is linear.*

Proof. If there are no co-atoms in $\operatorname{Con} G$ then by definition $\Im(G) = 1$, and if $\Im(G) = 1$ then $\operatorname{Con} G$ cannot have any co-atoms.

If one of the four conditions holds then G is $\Im$-semisimple by theorem 19.

Let us assume that $\Im(G) = 0$. If there is a co-atom $\rho \in \operatorname{Con} G$ such that $|G/\rho| \geq 3$ then it follows from theorem 16 that ρ is a unique co-atom and therefore $0 = \Im(G) = \rho$. Accordingly, $|\operatorname{Con} G| = 2$ and thus G is simple.

If all the simple quotients of G have two vertices then by theorem 17 they are all isomorphic. There are 3 different graphs having exactly two vertices. Here they are. If ρ is a co-atom and $G/\rho \cong O_2$ then all the simple quotients of G are

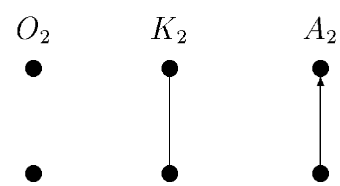


Figure 3.11: Graphs with two vertices.

isomorphic to O_2. Let $x, y \in V$ and $x \neq y$. As $\Im(G) = 0$ there is a co-atom ρ such that $\langle x, y\rangle \notin \rho$ ard therefore x and y lie in different ρ-classes. As $G/\rho \cong O_2$, we have $xy \notin E$. As the vertices x, y were chosen randomly, we can say that G is edgeless. Similarly, we can prove that if there is a co-atom $\rho \in \operatorname{Con} G$ such that $G/\rho \cong K_2$ then G is complete.

If there is a co-atom $\rho' \in \operatorname{Con} G$ such that $\operatorname{Con} G/\rho' \cong A_2$ and $x, y \in V$ are are different vertices of G then by the condition $\Im(G) = 0$ there exists a co-atom ρ such that $\langle x, y\rangle \notin \rho$. As $G/\rho \cong A_2$ then by theorem 17 either $xy \in E$ and $yx \notin E$ or $xy \notin E$ and $yx \in E$. So, we have proved that there is a directed edge between arbitrary pair of vertices. It remains to prove that there are no 3-element cycles in G. Let xyz be a cycle ($xy, yz, zx \in E$ and $xz, zy, yx \notin E$). If ρ is an arbitrary co atom then either $x \equiv y \equiv z(\rho)$ or two of the vertices are equivalent by ρ. All the free vertices cannot lie in different ρ-classes, because there are exactly two ρ-classes. If $x \equiv y(\rho)$ and $z \not\equiv x(\rho)$ then there is a ρ-class M such that $x, y \in M$ and $z \notin M$. This is impossible because M is a module. Accordingly, for every co-atom ρ and for arbitrary vertices x, y, z we have $x \equiv y \equiv z(\rho)$ which is a contradiction with the condition $\Im(G) = 0$. □

The $\Im$-radical may be used to recursively decompose a graph into a tree-like structure in the following way. Suppose we have a finite graph $G = (V, E)$ such that $\{G_1, ..., G_n\}$ is the partition corresponding to the congruence $\Im(G)$. For decomposing G we take the factor graph $G/\Im(G)$ and and add outgoing directed edges to each vertex of $G/\Im(G)$. Then we found the decompositions of the components $G_1, ..., G_n$ and "glue" them to the corresponding directed edges. Thereby, the "vertices" of the decomposition tree are $\Im$-semisimple graphs and by Theorem 20 the decomposition obtaine coincides with the modular decomposition [16, 17, 19].

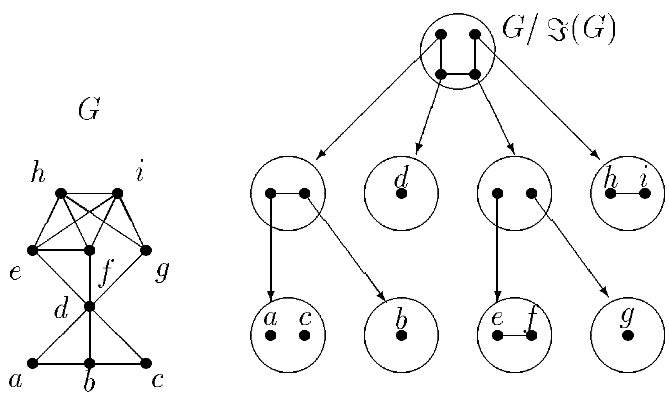


Figure 3.12: A graph and its decomposition

For example, the in the graph G in the Figure 3.12 we have $G/\Im(G) = \{\{h, i\}, \{e, f, g\}, \{d\}, \{a, b, c\}\}$. The complete decomposition is given in the right side of the figure.

3.7 An example of a $\Im$-radical graph

Let $\mathbf{N}$ be the set of natural numbers and let us define a binary relation $\propto$ on the set $\mathbf{N}$ as follows

$$n \propto m \;\equiv\; n < m \,\wedge\, \text{odd}(m),$$

where odd(m) is true iff m is odd. In this section we will prove that the corresponding infinite graph $\mathcal{N} = (\mathbf{N}, \propto)$ is $\Im$-radical.

Lemma 5 *If $M \subseteq \mathbf{N}$ is a module, $x \notin M$ and $x+1 \in M$ then $x+2 \notin M$.*

Proof. Let M be a subset of $\mathbf{N}$ such that $x \notin M$ and $x+1 \in M$. Suppose that $x+2 \in M$.

If x is odd then $x+2$ is odd and $x+1$ is even. Accordingly, $x \propto x+2$ and $x \not\propto x+1$.

If x is even then $x+1$ is odd and $x+2$ is even. Accordingly, $x \propto x+1$ and $x \not\propto x+2$. Therefore M cannot be a module. □

Lemma 6 *If $M \subseteq \mathbf{N}$ is a module, $x < y < z \in M$ and $y \notin M$ then $x \notin M$.*

Proof. If z is even then $x \propto z$ and $z \not\propto y$. Therefore x and z cannot lie in the same module M.

If z is odd then $y \propto z$ and $y \not\propto x$. Therefore $x \notin M$. □

Theorem 21 *A proper subset $M \subset \mathbf{N}$ is a module iff either $M = \{n\}$ or $M = \{0, ..., n-1\}$ for some $n \in \mathbf{N}$.*

Proof. The *if*-part is trivial. Let $M \neq \emptyset$ be a module and there is no n such that $M = \{0, ..., n-1\}$. Therefore there is $y \notin M$ such that $y+1 \in M$. Let $x \neq y$ be an arbitrary natural number.

If $x < y$ then $x \notin M$ by lemma 6. Let $x > y+1$. If $x \in M$ then $x > x+2$ by lemma 5 and therefore $y \notin M$ by lemma 6 which is a contradiction. Therefore $x \notin M$ and obviously $M = \{y+1\}$. □

Thus we have proved that there is a sequence of modules in $\mathcal{N}$

$$M_0 \subset M_1 \subset M_2 \subset ... \subset M_k \subset ...$$

such that every nontrivial module M is equal to one of the modules M_k. Accordingly, the congruence lattice $\mathrm{Con}\,\mathcal{N}$ is isomorphic to the ordinal number $\omega + 1 = \{0, 1, 2, ..., \omega\}$ which obviously has no co-atoms.

3.8 Congruence lattice of a finite $\Im$-semisimple graph

It is remarkable that the value of $\Im$-radical depends only on the congruence lattice of G but not on G itself. Thus one can define $\Im$-semisimple graphs by their congruence lattice. We know the following $\Im$-semisimple graphs.

- A trivial graph $0 = (\{\emptyset\}, \emptyset)$. Its congruence lattice is isomorphic to the trivial lattice $\mathbf{\Pi}_1$ – the partition lattice of the set $1 = \{0\}$.

- All simple graphs have the congruence lattice isomorphic to $\mathbf{\Pi}_2$ – the partition lattice of the set $2 = \{0, 1\}$.
- The edgeless graph with n-vertices O_n and the complete graph with n-vertices K_n have a congruence lattice isomorphic to $\mathbf{\Pi}_n$ – the partition lattice of the set $n = \{0, 1, ..., n-1\}$.
- n-element linear orderings have a congruence lattice isomorphic to $\mathbf{\Pi}_2^{n-1}$. This is quite obvious but we will prove it.

Theorem 22 *The congruence lattice of the n-element linear ordering is isomorphic to $\mathbf{\Pi}_2^{n-1}$*

Proof. Let $G = (V, E)$, $V = \{0, ..., n-1\}$ and E is a linear ordering such that $\langle i, j \rangle \in E$ iff $i < j$. It is obvious that there are $n-1$ atoms in $\operatorname{Con} G$. They are just the congruence relations $(01), (12), ..., (n-2, n-1)$, where $(i, i+1)$ denotes the congruence relation where i and $i+1$ are the only elements which are different and equivalent. It is obvious that every congruence relation can be uniquely represented as the least upper bound of certain set of atoms and for every set of atoms there is a unique congruence corresponding to this set of atoms. □

Corollary 2 *A graph G is $\Im$-semisimple if and only if $\operatorname{Con} G$ is either isomorphic to $\mathbf{\Pi}_n$ or to $(\mathbf{\Pi}_2)^n$ for a suitable $n > 0$.*

Therefore, all the congruence lattices of finite $\Im$-semisimple graphs are represented in the following diagram. In the Figure 3.13 is a Hasse diagram of the partially ordered set of congruence lattices of all finite $\Im$-semismple graphs. $L_1 \leq L_2$ means that there is a lattice embedding $L_1 \longrightarrow L_2$.

3.9 Jordan-Dedekind chain condition

Let L be a finite lattice. We say that L satisfies the *Jordan-Dedekind* chain condition (JD) if any two maximal chains of L have the same length.

Theorem 23 *If $\operatorname{Con} G$ is finite then it satisfies the Jordan-Dedekind chain condition (JD).*

Proof. We will prove the theorem by induction on the size of $\operatorname{Con} G$. The statement of the theorem is obvious when G is $\Im$-semisimple. Indeed, all the finite partition lattices are semimodular and therefore satisfy JD. Lattices $\mathbf{\Pi}_2^n$ satisfy JD because if $L_1, ..., L_n$ satisfy JD then also the direct product $L_1 \times ... \times L_n$ satisfies JD.

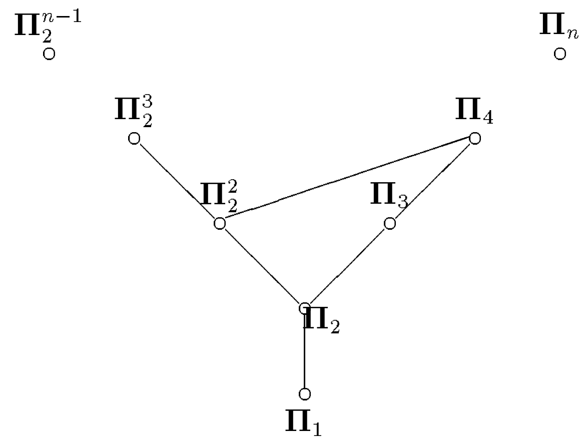
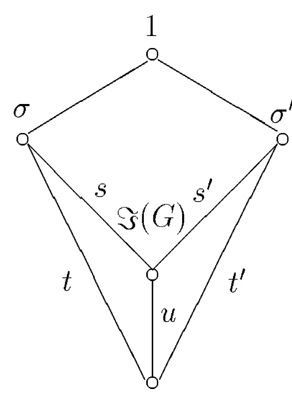


Figure 3.13: Congruence lattices of finite $\Im$-semisimple graphs.

Let $|\operatorname{Con} G| = k$ and all the smaller congruence lattices satisfy JD. We can assume that $\Im(G) \neq 0$. Let

$$c\colon\quad 0 = \sigma_0 < \sigma_1 < \ldots < \sigma_{m-1} = \sigma < \sigma_m = 1$$
$$c'\colon\quad 0 = \sigma'_0 < \sigma'_1 < \ldots < \sigma'_{n-1} = \sigma' < \sigma'_n = 1$$

two maximal chains of $\operatorname{Con} G$. Obviously σ and σ' are co-atoms of $\operatorname{Con} G$ and therefore $\Im(G) \leq \sigma$ and $\Im(G) \leq \sigma'$. Let $\ell(c)$ denote the length of c. Let s, s' and u be maximal chains of the intervals $[\Im(G), \sigma]$, $[\Im(G), \sigma']$ and $[0, \Im(G)]$ respectively. Let $t\colon \sigma_0 < \ldots < \sigma_{m-1}$ and $t'\colon \sigma'_0 < \ldots < \sigma'_{n-1}$.



It is obvious that the ideal $\Im(G)^{\triangle} \cong G/\Im(G)$ satisfies JD because $G/\Im(G)$ is $\Im$-semisimple. Therefore $\ell(s) = \ell(s')$. Also the ideal $\sigma^{\triangledown}$ satisfies JD because (by theorem 10) it is isomorphic to the direct product of smaller congruence lattices. Therefore $\ell(t) = \ell(s) + \ell(u)$. Similarly $\ell(t') = \ell(s') + \ell(u)$. Accordingly

$$\ell(c) \quad = \quad \ell(t) + 1 = \ell(s) + \ell(u) + 1$$

$$\begin{aligned} &= \ell(s') + \ell(u) + 1 = \ell(t') + 1 \\ &= \ell(c') \end{aligned}$$

and thus $\operatorname{Con} G$ satisfies JD. □

The congruence lattices of graphs satisfying a given lattice identity are studied. A complete characterization of all finite graphs with the congruence lattice laying in a given lattice variety is presented.

4.1 Introduction

It has been proved in [38] (see Theorem 8, page 43). that the set of all congruence relations of a given graph G is a complete lattice. In the current chapter the following problem is solved.

Problem. *Let I be a lattice identity. Find a characterization for all finite graphs G such that* $\operatorname{Con} G$ *satisfies I.*

To solve this problem, the $\Im$-*radical* defined in [38] as the meet of all co-atoms in $\operatorname{Con} G$ is useful. If $\Im(G) = 0$, then either $\operatorname{Con} G \cong \mathbf{\Pi}_n$ or $\operatorname{Con} G \cong \mathbf{\Pi}_2^n$, where $\mathbf{\Pi}_n$ is the lattice of all partitions of $n = \{0, ..., n-1\}$. For every $\Im$-semisimple graph G define a positive integer $\eta(G)$ such that $\eta(G) = n$ if G is a complete or edgeless graph with n vertices (i.e. if $\operatorname{Con} G \cong \mathbf{\Pi}_n$) and $\eta(G) = 2$ otherwise. Let $\mathcal{V}$ be a lattice variety such that $L \notin \mathcal{V}$ for at least one lattice L. There is a unique positive integer n such that $\mathbf{\Pi}_1, ..., \mathbf{\Pi}_n \in \mathcal{V}$, but $\mathbf{\Pi}_{n+1} \notin \mathcal{V}$. Denote this n as $\eta(\mathcal{V})$.

Theorem. *If $G/\Im(G) = \{G_1, ..., G_n\}$ and $\mathcal{V}$ is a lattice variety then* $\operatorname{Con} G$ *lies in $\mathcal{V}$ if and only if $\eta(G/\Im(G)) \leq \eta(\mathcal{V})$ and* $\operatorname{Con} G_i \in \mathcal{V}$ *for $i = 1, ..., n$.*

$G/\Im(G)$ denotes the *factor-graph* of G by $\Im(G)$ and G_i are the congruence classes viewed as subgraphs of G. It follows from the theorem that for every lattice identity I there is an $O(|V|^2)$ algorithm that determines whether I holds in $\operatorname{Con} G$, where V is the vertex set of G.

4.2 Partition lattices

Let A be an arbitrary set and $S \subseteq \mathbf{\Pi}(A)$ be a nonempty set of equivalence relations on A. A finite sequence

$$a_0, a_1, ..., a_\ell,$$

where $a_i \in A$, is called an S-*chain* if for every i there is an equivalence relation $\rho_i \in S$ such that $\langle a_i, a_{i+1} \rangle \in \rho_i$. Two S-chains $a : a_0, ..., a_\ell$ and $b : b_0, ..., b_\ell$ are *equivalent* if for every i there is $\rho_i \in S$ such that $\langle a_i, a_{i+1} \rangle \in \rho_i$ and $\langle b_i, b_{i+1} \rangle \in \rho_i$.

It is well known that $\langle x, y\rangle \in \sup S$ iff x and y can be connected with an S-chain. If $\langle x_1, y_1\rangle \in \sup S$ and $\langle x_2, y_2\rangle \in \sup S$, then the corresponding S-chains can be chosen in such a way that they are equivalent.

Theorem 24 *For all graphs $G = (V, E)$ the lattice* $\operatorname{Con} G$ *is a complete sublattice of* $\mathbf{\Pi}(V)$.

Proof. It is sufficient to show that the least upper bound (in $\mathbf{\Pi}(V)$) of every nonempty set S of congruence relations is a congruence relation. Let $\rho = \sup S$, $x\rho x'$, $y\rho y'$ and $\neg(x\rho y)$. So, there are equivalent S-chains

$$x = x_0, x_1, \ldots, x_\ell = x',$$
$$y = y_0, y_1, \ldots, y_\ell = y'$$

such that $x_i\rho_i x_{i+1}$ and $y_i\rho_i y_{i+1}$ $\forall i < \ell$.

Let $\langle x, y\rangle \in E$. We will show by induction that $\langle x_i, y_i\rangle \in E$ for all $0 \leq i \leq \ell$. Indeed, the case $i = 0$ is trivial and if $\langle x_{i-1}, y_{i-1}\rangle \in E$, then $x_{i-1}\rho_{i-1}x_i$, $y_{i-1}\rho_{i-1}y_i$. But $\neg(x_{i-1}\rho_{i-1}y_{i-1})$, because otherwise there would be an S-chain

$$x = x_0, x_1, \ldots, x_{i-1}, y_{i-1}, \ldots, y_0 = y.$$

As $\rho_{i-1} \in \operatorname{Con}(G)$, we get from the definition of congruence relation that $\langle x_i, y_i\rangle \in E$. Therefore, $\rho = \sup S$ is a congruence relation. $\Box$

4.3 Neutral and strongly neutral elements

An element α of a lattice L is said to be *neutral* ([1],[15]) if

$$(\alpha \wedge x) \vee (x \wedge y) \vee (y \wedge \alpha) = (\alpha \vee x) \wedge (x \vee y) \wedge (y \vee \alpha)$$

for all $x, y \in L$. The following theorem gives us two equivalent formulations of neutrality.

Theorem 25 *Let L be a lattice and let α be an element of L. The following conditions are equivalent:*

- *α is neutral;*
- *α is distributive, dually distributive, and $\alpha \wedge x = \alpha \wedge y$ and $\alpha \vee x = \alpha \vee y$ imply $x = y$ for any $x, y \in L$;*
- *the mapping*
$$\varphi\colon \begin{cases} L \longrightarrow \alpha^{\nabla} \times \alpha^{\triangle} \\ x \mapsto (x \wedge \alpha, x \vee \alpha) \end{cases}$$
is a lattice embedding.

A proof is given in [15].

Let V be an arbitrary set, L be a complete sublattice of $\mathbf{\Pi}(V)$ and $\rho \in L$. We say that ρ is *strongly neutral* in L if

$$\rho \vee \sigma = \sigma \cup \rho$$

for arbitrary $\sigma \in L$.

Lemma 1 *An equivalence relation $\rho \in L$ is strongly neutral iff*

$$v/\rho \subseteq v/\sigma \quad or \quad v/\sigma \subseteq v/\rho \tag{4.1}$$

for arbitrary $\sigma \in L$ and $v \in V$, where v/ρ denotes the ρ-class containing v.

Proof. Let us assume that ρ is strongly neutral, $\sigma \in L$, $v \in V$ and $v/\rho \not\subseteq v/\sigma$. We will show that $v/\sigma \subseteq v/\rho$. As v/ρ is not a subset of v/σ, there has to be an $u \in v/\rho$ such that $u \notin v/\sigma$. Let w be an arbitrary element of v/σ. As $(w, v) \in \sigma$ and $(v, u) \in \rho$, we have

$$(w, u) \in \rho \vee \sigma = \rho \cup \sigma$$

and thereby $(w, u) \in \rho$ because $(w, u) \notin \sigma$. Now we have $w \in u/\rho = v/\rho$. As w has been chosen arbitrarly, we conclude that $v/\sigma \subseteq v/\rho$.

Let us assume that the condition (4.1) holds. It is sufficient to prove that $\rho \cup \sigma$ is an equivalence relation. It is obvious that $\rho \cup \sigma$ is reflexive and symmetric. We will prove the transitivity. Let $(u, v), (v, w) \in \rho \cup \sigma$. If these pairs lie both in ρ or in σ, the transitivity is obvious. Let $(u, v) \in \sigma$ and $(v, w) \in \rho$. If $(u, w) \notin \rho$, then $u \notin w/\rho$ and therefore

$$v/\sigma = u/\sigma \not\subseteq w/\rho = v/\rho$$

and by condition (4.1) we have $w \in w/\rho = v/\rho \subseteq v/\sigma = u/\sigma$ showing that $(u, w) \in \sigma$. $\square$

Lemma 2 *Every strongly neutral element is neutral.*

Proof. Suppose $\rho \in L$ is strongly neutral. Let us prove at first that the mappings $\sigma \mapsto \sigma \cap \rho$ and $\sigma \mapsto \sigma \vee \rho$ are endomorphisms of the lattice L. The second mapping is obviously a morphism because of the distributivity of the lattice of all subsets of A. Let $\gamma = \sigma \vee \delta$. We will prove the equality

$$\gamma \cap \rho = (\sigma \cap \rho) \vee (\delta \cap \rho).$$

Indeed, as $\sigma \subseteq \gamma$ and $\delta \subseteq \gamma$, it follows that $\sigma \cap \rho \subseteq \gamma \cap \rho$ and $\delta \cap \rho \subseteq \gamma \cap \rho$. Therefore, $\gamma \cap \rho$ is an upper bound of the equivalence relations $\sigma \cap \rho$ and $\delta \cap \rho$. It remains to show that it is the least upper bound. Let

$$\sigma \cap \rho \subseteq \tau, \qquad \delta \cap \rho \subseteq \tau, \tag{4.2}$$

and $(u,v) \in \gamma \cap \rho$. Accordingly, $(u,v) \in \sigma \vee \delta$ and $(u,v) \in \rho$. Therefore there is a $\{\sigma, \delta\}$-chain

$$c: \; u = v_0, v_1, ..., v_\ell = v.$$

If $(v_i, v_{i+1}) \in \rho$ for each $i < \ell$, then obviously c is a $\{\sigma \cap \rho, \delta \cap \rho\}$-chain. Therefore, by the inclusions (4.2) and the transitivity of τ, we have $(u,v) \in \tau$.

Let i be the smallest index such that $(v_i, v_{i+1}) \notin \rho$. Then either $v_i/\sigma \nsubseteq v_i/\rho$ or $v_i/\delta \nsubseteq v_i/\rho$. Accordingly, by Lemma 1, either $v_i/\rho \subseteq v_i/\sigma$ or $v_i/\rho \subseteq v_i/\delta$, which gives that either $(u,v) \in \sigma$ or $(u,v) \in \delta$. This implies $(u,v) \in \tau$. Thus, ρ is a distributive and dually distributive element.

We assume now that $\sigma \vee \rho = \delta \vee \rho$ and $\sigma \cap \rho = \delta \cap \rho$ and show that $\sigma = \delta$. Let $(u,v) \in \sigma$. If $(u,v) \in \rho$, then $(u,v) \in \sigma \cap \rho = \delta \cap \rho \subseteq \delta$ and therefore $(u,v) \in \delta$. If $(u,v) \notin \rho$, then from $(u,v) \in \sigma \subseteq \sigma \vee \rho = \delta \vee \rho = \delta \cup \rho$ it follows that $(u,v) \in \delta$. Therefore $\sigma \subseteq \delta$. The proof of $\delta \subseteq \sigma$ is similar. Accordingly, ρ is a neutral element of L. $\Box$

Lemma 3 *If there is a co-atom ρ in* Con G *such that there are at least* 3 *vertices in G/ρ, then ρ is a unique co-atom of* Con G *and, furthermore, ρ is the least upper bound of all congruence relations different from* 1.

The proof is given in [38] (see Theorem 16, page 50).

Theorem 26 *If $G/\Im(G)$ is edgeless [complete], then every $\Im(G)$-class G_ι is connected [complement-connected].*

Proof. Let $G/\Im(G)$ be edgeless and $G_\iota \in G/\Im(G)$ be not connected. Let G'_ι be an arbitrary connected component of G_ι. It is obvious that there are no edges between G'_ι and $G - G'_\iota$ and therefore $\{G'_\iota, G - G'_\iota\}$ is a congruence partition and the corresponding congruence relation ρ is a co-atom in Con G and $\Im(G) \nleq \rho$, which is a contradiction with the definition of $\Im(G)$.

If $G/\Im(G)$ is complete, the proof is similar. $\Box$

By A_n we mean the graph $(\{0, 1, ..., n-1\}, \{(i,j) \mid 0 \leq i < j < n\})$ (a linear ordering with n elements).

Theorem 27 *If $G/\Im(G)$ is linear, then none of the $\Im(G)$-classes have a factor-graph isomorphic to A_2 (Figure 3.11, page 53).*

Proof. Let $G/\Im(G) = (V_0, E_0)$ be a linear ordering and $H \in G/\Im(G)$. Suppose there is an epimorphism $H \xrightarrow{f} A_2$ and $\{H_1, H_2\}$ is a partition corresponding to Ker f; $(f(H_1), f(H_2)) \in E(A_2)$.

We say that $H' \in V_0$ *is less than* $H \in V_0$ if $H'H \in E_0$. Let $\mathbf{G}_1 \subseteq G/\Im(G)$ be the set of elements of $G/\Im(G)$ less than H and $\mathbf{G}_2$ be the set of elements greater than H. It is obvious that the partition

$$\{(\cup \mathbf{G}_1) \cup H_1, \quad (\cup \mathbf{G}_2) \cup H_2\}$$

is a co-atom of Con G which is not comparable with $\Im(G)$. This is a contradiction. □

Theorem 28 *The radical* $\Im(G)$ *is a strongly neutral element of* Con G.

Proof. The statement is trivially true if $|G| \leq 2$. Let us assume that $|G| \geq 3$. As the graph $G/\Im(G)$ is $\Im$-semisimple, we know that $G/\Im(G)$ is either simple, complete, edgeless or linear (Theorem 20).

The cases when $G/\Im(G)$ is edgeless or complete are dual, so it is sufficient to consider only one of them. Let $G/\Im(G)$ be edgeless, $v \in V$ be an arbitrary vertex, $\sigma \in \mathrm{Con}\, G$, and $v/\sigma \not\subseteq v/\Im(G)$. Consequently there is a vertex $u \in v/\sigma - v/\Im(G)$. By Theorem 26 the induced subgraph $v/\Im(G)$ is connected. Thereby, for any vertex $w \in v/\Im(G)$ there is a chain of vertices $v = v_0, v_1, \ldots, v_\ell = w \in v/\Im(G)$ such that $v_i v_{i+1} \in E \cup E^{-1}$, $0 \leq i \leq n-1$. We will prove by induction that all the vertices v_i lie in v/σ. Obviously v lies in v/σ. Assume that $v_i \in v/\sigma$ and $v_{i+1} \notin v/\sigma$. Since there is an edge between v_i and v_{i+1} and u is contained in the module v/σ which does not contain v_{i+1}, there must be an edge between u and v_{i+1} as well. Since $G/\Im(G)$ is edgeless, this implies $u/\Im(G) = v_{i+1}/\Im(G)$, a contradiction.

Let $G/\Im(G)$ be linear. Let $H = v/\Im(G)$ and v/σ be overlapping modules. By Theorem 12 the intersection $H \cap v/\sigma$ and set difference $H - v/\sigma$ are modules of the induced subgraph H, and thereby we have a partition of H into modules. It is easy to show that the corresponding factor-graph is linear, which is a contradiction with Theorem 27.

If $G/\Im(G)$ is simple then $\Im(G)$ is the unique co-atom of Con G. If $|G/\Im(G)| = 2$, then $G/\Im(G)$ is either complete, edgeless or linear. Thus we can assume without loss of generality that $|G/\Im(G)| \geq 3$. It follows directly from Lemma 3 that every congruence relation $\rho \in \mathrm{Con}\, G$ is comparable with $\Im(G)$ and therefore $\Im(G) \vee \rho = \Im(G) \cup \rho$ for every $\rho \in \mathrm{Con}\, G$. □

4.4 Partition number of a variety

We will show in this section that the finite partition lattices $\mathbf{\Pi}_\ell$ play an important role in studying the lattice identities holding in Con G.

Let $\mathcal{L}$ be the class of all lattices, $\mathcal{V} \subseteq \mathcal{L}$ be a lattice variety, and $L_1, ..., L_n$ be arbitrary lattices. It is obvious that their direct product

$$L = L_1 \times L_2 \times ... \times L_n$$

lies in $\mathcal{V}$ if and only if every L_i lies in $\mathcal{V}$. For example L is modular [distributive] iff every L_i is modular [distributive].

As proved by Sachs in 1961 [5], every lattice identity that holds in every finite partition lattice must hold in every lattice. Thereby, for every lattice variety $\mathcal{V} \neq \mathcal{L}$, there is a unique natural number $\eta(\mathcal{V})$ such that $\mathbf{\Pi}_{\eta(\mathcal{V})} \notin \mathcal{V}$ and $\mathbf{\Pi}_m \in \mathcal{V}$ for every natural number $m < \eta(\mathcal{V})$. The natural number $\eta(\mathcal{V})$ is called a *partition number* of the variety $\mathcal{V}$.

For example, the class of all distributive lattices has the partition number 3, the class of all modular lattices has the partition number 4.

Lemma 4 *If $\mathcal{V}$ is a lattice variety and $\eta(\mathcal{V}) = 2$, then every lattice in $\mathcal{V}$ is trivial.*

Proof. If $L \in \mathcal{V}$ is a nontrivial lattice then it has a two-element sublattice isomorphic to $\mathbf{\Pi}_2$. Therefore $\eta(\mathcal{V}) > 2$. □

Let $\mathcal{L}_\ell$ denote the variety generated by the lattice $\mathbf{\Pi}_{\ell-1}$. Obviously,

$$\mathcal{L}_1 \subseteq \mathcal{L}_2 \subseteq \mathcal{L}_3 \subseteq ... \subseteq \mathcal{L}_\ell \subseteq ... \subseteq \mathcal{L}.$$

It follows from the Jonsson lemma [10],[29] that all these inclusions are proper, i.e. for every natural number $n > 0$ there is a lattice identity that holds in $\mathbf{\Pi}_n$ but not in $\mathbf{\Pi}_{n+1}$. For the case $n = 1$, the suitable identity is $x = y$, for the case $n = 2$, it is distributivity and for the case $n = 3$, modularity. It turnes out that the suitable identity for $n = 4$ is

$$\begin{aligned} x_0 \wedge (x_1 \vee x_2 \vee x_3 \vee x_4) = \quad & [x_0 \wedge (x_1 \vee x_2 \vee x_3)] \vee [x_0 \wedge (x_1 \vee x_2 \vee x_4)] \\ & \vee [x_0 \wedge (x_1 \vee x_3 \vee x_4)] \vee [x_0 \wedge (x_2 \vee x_3 \vee x_4)]. \end{aligned}$$

Obviously, the left-hand side is greater or equal than the right-hand side. To show the opposite inequality, it is sufficient to mention that for arbitrary elements $a_0, a_1, ..., a_4$ of $\mathbf{\Pi}_4$ the equivalence relation $a_0 \wedge (a_1 \vee ... \vee a_4)$ is equal to one of

$$a_0 \wedge (a_1 \vee a_2 \vee a_3), a_0 \wedge (a_1 \vee a_2 \vee a_4), a_0 \wedge (a_1 \vee a_3 \vee a_4), a_0 \wedge (a_2 \vee a_3 \vee a_4),$$

because there are no chains of length 5 in $\mathbf{\Pi}_4$ and therefore the chain

$$0 \leq a_1 \leq a_1 \vee a_2 \leq a_1 \vee a_2 \vee a_3 \leq a_1 \vee a_2 \vee a_3 \vee a_4 \leq 1$$

must have two equal elements.

But this identity does not hold in $\mathbf{\Pi}_5$. Take, for example, $x_0 = (04)$, $x_1 = (01)$, $x_2 = (12)$, $x_3 = (23)$, and $x_4 = (34)$, where (ij) denotes the minimal equivalence relation containing the pair (i, j).

A proof of the general case is similar to the proof of the case $n = 4$. Let $X = \{x_0, x_1, ..., x_n\}$ be the set of variable letters. A suitable identity that separates $\mathbf{\Pi}_n$ and $\mathbf{\Pi}_{n+1}$ is

$$x_0 \wedge (x_1 \vee ... \vee x_n) = \bigvee_{\iota}[x_0 \wedge (x_{\iota(1)} \vee ... \vee x_{\iota(n-1)})].$$

where the join in the right-hand side is calculated over all possible injections

$$\{1, ..., n-1\} \xrightarrow{\iota} \{1, ..., n\}.$$

4.5 Identities in $\operatorname{Con} G$

Let $\mathcal{L}$ be the class of all lattices, $\mathcal{L}_{\mathcal{G}}$ be the class of congruence lattices of all finite graphs. We say that two lattice varieties $\mathcal{V}_1$ and $\mathcal{V}_2$ are *equivalent* and write $\mathcal{V}_1 \sim \mathcal{V}_2$ iff $\mathcal{V}_1 \cap \mathcal{L}_{\mathcal{G}} = \mathcal{V}_2 \cap \mathcal{L}_{\mathcal{G}}$.

Lemma 5 *Let G be a graph, $\mathcal{V}$ be a lattice variety and $G/\Im(G) = \{G_i\}_{i \in \mathcal{I}}$. The congruence lattice $\operatorname{Con} G$ lies in $\mathcal{V}$ iff all the lattices $\operatorname{Con} G_i$ and the lattice $\operatorname{Con}(G/\Im(G))$ lie in $\mathcal{V}$.*

Proof. Assume $\operatorname{Con} G \in \mathcal{V}$. Now $\operatorname{Con} G_i \in \mathcal{V}$, because there are lattice embeddings $\operatorname{Con} G_i \longrightarrow \Im(G)^{\bigtriangledown} \leq G$, and $\operatorname{Con} G/\Im(G) \in \mathcal{V}$, because $\operatorname{Con} G/\Im(G) \cong \Im(G)^{\bigtriangleup} \leq \operatorname{Con} G$.

And conversely, if every $\operatorname{Con} G_i$ and $\operatorname{Con} G/\Im(G)$ lie in $\mathcal{V}$, then by Theorem 28 there is a lattice embedding

$$\operatorname{Con} G \longrightarrow \Im(G)^{\bigtriangledown} \times \Im(G)^{\bigtriangleup} \cong \operatorname{Con}(G/\Im(G)) \times \prod_{i \in \mathcal{I}} \operatorname{Con} G_i$$

and therefore $\operatorname{Con} G \in \mathcal{V}$. $\square$

Let $\mathcal{L}_J$ be the class of all congruence lattices of finite $\Im$-semisimple graphs. Let $\mathcal{V}_1$ and $\mathcal{V}_2$ be lattice varieties. We say that $\mathcal{V}_1$ and $\mathcal{V}_2$ are $\Im$-equivalent and write $\mathcal{V}_1 \sim_J \mathcal{V}_2$ iff $\mathcal{V}_1 \cap \mathcal{L}_J = \mathcal{V}_2 \cap \mathcal{L}_J$.

Lemma 6 *Two lattice varieties $\mathcal{V}_1$ and $\mathcal{V}_2$ are $\Im$-equivalent if and only if $\eta(\mathcal{V}_1) = \eta(\mathcal{V}_2)$.*

Proof. Theorem 20 gives us a complete characterization of the class $\mathcal{L}_J$. It is obvious that if any of the direct powers $\mathbf{\Pi}_2^k$ lies in $\mathcal{V}_1$ or in $\mathcal{V}_2$, then all $\mathbf{\Pi}_2^{\ell}, \ell = 1, 2, 3, ...,$ lie in $\mathcal{V}_1$ or in $\mathcal{V}_2$, respectively. Therefore, $\mathcal{V}_1$ and $\mathcal{V}_2$ are $\Im$-equivalent if and only if they contain the same partition lattices $\mathbf{\Pi}_1, \mathbf{\Pi}_2, ..., \mathbf{\Pi}_{\ell}, ...,$ i.e., iff $\eta(\mathcal{V}_1) = \eta(\mathcal{V}_2)$. $\square$

Theorem 29 *Two varieties $\mathcal{V}_1$ and $\mathcal{V}_2$ are equivalent if and only if their partition numbers coincide, i.e.,*

$$\mathcal{V}_1 \sim \mathcal{V}_2 \Leftrightarrow \eta(\mathcal{V}_1) = \eta(\mathcal{V}_2).$$

Proof. If $\mathcal{V}_1 \cap \mathcal{L}_\mathcal{G} = \mathcal{V}_2 \cap \mathcal{L}_\mathcal{G}$ then $\eta(\mathcal{V}_1) = \eta(\mathcal{V}_2)$. Indeed, if K_n is a complete graph of n vertices, then $\mathrm{Con}\, K_n \cong \mathbf{\Pi}_n$ and therefore $\{\mathbf{\Pi}_1, \mathbf{\Pi}_2, ...\} \subseteq \mathcal{L}_\mathcal{G}$.

Let us prove the opposite implication. Let G be a finite graph. Let $\eta(\mathcal{V}_1) = \eta(\mathcal{V}_2)$. Then, by Lemma 6, $\mathcal{V}_1 \cap \mathcal{L}_J = \mathcal{V}_2 \cap \mathcal{L}_J$. If G is $\Im$-semisimple, then obviously

$$\mathrm{Con}\, G \in \mathcal{V}_1 \Leftrightarrow \mathrm{Con}\, G \in \mathcal{V}_2. \tag{4.3}$$

Assume that G is not $\Im$-semisimple and (4.3) is valid for all finite graphs smaller than G. Let $G/\Im(G) = \{G_i\}_{i \in \mathcal{I}}$. By Lemma 5 $\mathrm{Con}\, G$ lies in $\mathcal{V}_1$ iff every $\mathrm{Con}\, G_i$ and $\mathrm{Con}\, G/\Im(G)$ lie in $\mathcal{V}_1$. But G_i and $G/\Im(G)$ are smaller than G and therefore by (4.3) we get that $\mathrm{Con}\, G$ is in $\mathcal{V}_1$ iff $\mathrm{Con}\, G_i, i \in \mathcal{I}$, and $\mathrm{Con}\, G/\Im(G)$ lie in $\mathcal{V}_2$, and by Lemma 5

$$\mathrm{Con}\, G \in \mathcal{V}_1 \Leftrightarrow \mathrm{Con}\, G \in \mathcal{V}_2.$$

□

Corollary 3 *If G is a finite graph and $\mathcal{V}$ is a lattice variety with partition number $\eta(\mathcal{V})$ then $\mathrm{Con}(G) \in \mathcal{V}$ if and only if the modular decomposition of G does not contain graphs O_n and K_n with $\eta(\mathcal{V}) < n$.*

We show that the graph decompositions using the lexicographic product operation arise naturally as the congruence relations of the graph. A complete characterization of the congruence lattice of a finite graph is given.

5.1 Lexicographic product of graphs

Congruence relations of a graph are closely related to the well-known *generalized lexicographic product* operation introduced by Sabidussi [4] which is a generalization of the *composition* operation introduced by Harary [3]. For any graphs $G_0 = (V_0, E_0)$ and $G_v = (V_v, E_v), (v \in V_0)$ by their *generalized lexicographic product* $G_0[(G_v)_{v \in V_0}]$ we mean a graph G with the vertex set

$$V = \{(v, w) \mid v \in V_0, w \in V_v\}$$

and with the edge set

$$E = \{(v, w)(v', w') \mid vv' \in E_0, \text{ or } v = v' \text{ and } ww' \in E_v\}.$$

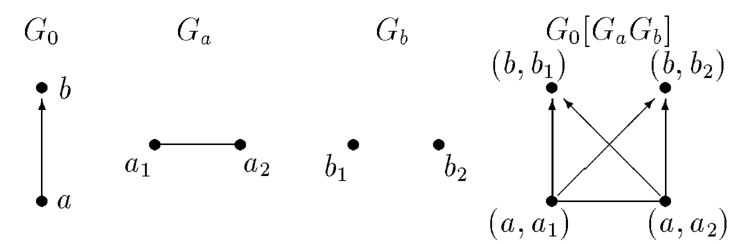


Figure 5.14: An example of the generalized lexicographic product.

It can be easily verified that the partition of the vertex set V into the components $G_v, v \in V_0$ is a congruence partition and the corresponding factor-graph is isomorphic to G_0. Moreover, if ρ is a congruence relation of a graph $G = (V, E)$, $G_0 = (V_0, E_0) = G/\rho$ is the corresponding factor-graph, $G_v, (v \in V_0)$ are the ρ-classes (viewed as induced subgraphs) then $G \cong G_0[(G_v)_{v \in V_0}]$. Therefore, there is a one-to-one correspondence between the decompositions of a graph into generalized lexicographic products and the congruence relations.

Accordingly, every finite graph can be assembled from *simple* graphs using the generalized lexicographic product operation. Such a decomposition is known as the *X-join decomposition* [9], *substitution decomposition* [17], *modular decomposition* [19] and *prime-tree decomposition* [24], [25], [26].

5.2 Lexicographic product of lattices

Let V_0 be a set and L_0 be a sublattice of the partition lattice $\mathbf{\Pi}(V_0)$ (the lattice of all partitions of V_0). Let $L_v, (v \in V_0)$ be arbitrary lattices. By the *lexicographic product* $L_0[(L_v)_{v\in V_0}]$ we mean the following subset of the direct product $L_0 \times \prod_{v\in V_0} L_v$:

$$\{(\sigma_0, (\sigma_v)_{v\in V_0}) \mid \forall v, w \in V_0 : \sigma_v \neq 1,\ (v,w) \in \sigma_0 \ \Rightarrow\ v = w\}.$$

We will prove in current chapter that this operation is sufficient for generating all

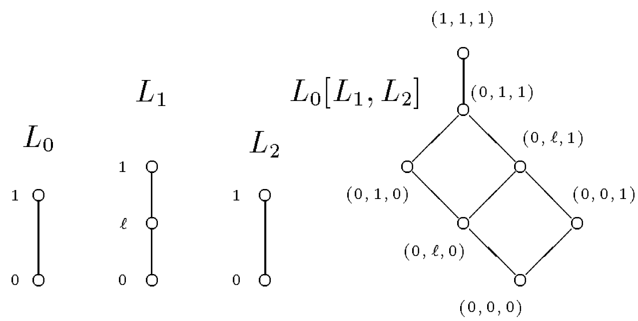


Figure 5.15: An example of the lexicographic product of lattices.

congruence lattices of finite graphs. We prove that in certain cases the mapping Con is lexicographic product preserving:

$$\mathrm{Con}(G_0[(G_v)_{v\in V_0}]) \cong (\mathrm{Con}\, G_0)[(\mathrm{Con}\, G_v)_{v\in V_0}]. \tag{5.1}$$

We prove that the congruence lattice of a finite graph G can be assembled from the lattices $\mathbf{\Pi}_n$ and $(\mathbf{\Pi}_2)^\ell$ using the lexicographic product operation.

5.3 Properties of the lexicographic product of lattices

Let L_0 be a complete sublattice of $\mathbf{\Pi}(V_0)$ such that $0, 1 \in L_0$ and $\{L_v\}_{v\in V_0}$ be arbitrary lattices with 1.

Theorem 30 *$L = L_0[(L_v)_{v\in V_0}]$ is a subdirect product of the lattices L_0 and L_v, $v \in V_0$*

Proof. We will show that L is a sublattice of the direct product of lattices L_0 and $(L_v)_{v\in V_0}$. Let $\sigma = (\sigma_0, (\sigma_v)_{v\in V_0}) \in L$ and $\delta = (\delta_0, (\delta_v)_{v\in V_0}) \in L$, that is

$$\begin{aligned} \forall v, w \in V_0 : &\quad \sigma_v \neq 1,\ (v,w) \in \sigma_0 \ \Rightarrow\ v = w \\ \forall v, w \in V_0 : &\quad \delta_v \neq 1,\ (v,w) \in \delta_0 \ \Rightarrow\ v = w. \end{aligned}$$

We have to show that $\sigma \wedge \delta = (\sigma_0 \wedge \delta_0, (\sigma_v \wedge \delta_v)_{v\in V_0}) \in L$ and $\sigma \vee \delta = (\sigma_0 \vee \delta_0, (\sigma_v \vee \delta_v)_{v\in V_0}) \in L$.

Let $\sigma_v \wedge \delta_v \neq 1$. Then either $\sigma_v \neq 1$ or $\delta_v \neq 1$. If now $(v, w) \in \sigma_0 \wedge \delta_0$ then $(v, w) \in \sigma_0$ and $(v, w) \in \delta_0$ and thus $v = w$.

Let $\sigma_v \vee \delta_v \neq 1$. Then $\sigma_v \neq 1$ and $\delta_v \neq 1$. Let $(v, w) \in \sigma_0 \vee \delta_0$. As L_0 is a complete sublattice of $\Pi(V_0)$, there has to be a chain $v_0, ..., v_\ell \in V_0$ such that

$$v = v_\ell \; \gamma_0 \; v_{\ell-1} \; \gamma_0 \; v_{\ell-2} \; \gamma_0 \; v_{\ell-3} \; \gamma_0 \; ... \; \gamma_0 \; v_0 = w,$$

where $\gamma_0 = \sigma_0 \cup \delta_0$. We can now prove the equality $v = w$ by induction. Assume $v_{j-1} = w$. Thus $(v_j, w) \in \gamma_0$ and therefore either $(v_j, w) \in \sigma_0$ or $(v_j, w) \in \delta_0$. Thereby, $v_j = w$.

For arbitrary $\sigma_0 \in L_0$ we have $(\sigma_0, (1_v)_{v\in V_0}) \in L$ and for arbitrary $v \in V_0$ and $\sigma_v \in L_v$ we have $(0, (\sigma_u)_{u\in V_0}) \in L$, where

$$\sigma_u = \begin{cases} \sigma_v, & \text{when } u = v, \\ 1_u, & \text{when } u \neq v. \end{cases}$$

Therefore we have a subdirect product. □

Theorem 31 *If* $|V_0| \geq 2$, $a = (0, (1_v)_{v\in V_0}) \in L = L_0[(L_v)_{v\in V_0}]$ *and* c *is a co-atom of* L *then* $a \leq c$.

Proof. We point out that $(1, (1_v)_{v\in V_0})$ is the unit element of L. Let $c = (c_0, (c_u)_{u\in V_0})$ be a co-atom of L such that $c_v \neq 1$. Let $c' = (c_0, (c'_u)_{u\in V_0})$, where

$$c'_u = \begin{cases} 1_v, & \text{when } u = v, \\ c_u, & \text{when } u \neq v. \end{cases}$$

Obviously, $c < c' \in L$, but $c' < 1$ because if $c'_0 = c_0 = 1$ then $c_v = 1$ which is a contradiction. Therefore, if c is a co-atom of L then $c_v = 1$ for each $v \in V_0$ and accordingly $a \leq c$. □

Theorem 32 $a = (0, (1_v)_{v\in V_0})$ *is a neutral element of* $L = L_0[(L_v)_{v\in V_0}]$, *i.e. for arbitrary* $x, y \in L$

$$(a \wedge x) \vee (x \wedge y) \vee (y \wedge a) = (a \vee x) \wedge (x \vee y) \wedge (y \vee a).$$

Proof. The proof is obvious because 0 is a neutral element of L_0 and 1_v is a neutral element of L_v for each $v \in V_0$. □

Theorem 33 *If* $a = (0, (1_v)_{v\in V_0}) \in L_0[(L_v)_{v\in V_0}]$ *then*

$$\begin{aligned} a^{\triangle} &\cong L_0 \\ a^{\triangledown} &\cong \prod_{v\in V_0} L_v. \end{aligned}$$

The proof is trivial.

5.4 Decomposition of $\operatorname{Con} G$

Let G be a finite graph. Let ρ be a strongly neutral congruence relation of G, $G/\rho = (V_0, E_0)$ and $\{G_v\}_{v\in V_0}$ is the corresponding partition. By Theorem 9 and Theorem 10 there is a lattice embedding

$$\iota : \begin{cases} \operatorname{Con} G \longrightarrow \operatorname{Con} G/\rho \times \prod_{v\in V_0} \operatorname{Con} G_v \\ \sigma \mapsto (\bar{\sigma}, (\sigma \,|_{G_v})_{v\in V_0})) \end{cases}$$

Theorem 34 *$(\sigma_0, (\sigma_v)_{v\in V_0}))$ lies in $\operatorname{Im}\iota$ if and only if*

$$\forall v, w \in V_0 : \ \sigma_v \neq 1, \ (H, G_v) \in \sigma_0 \ \Rightarrow \ G_w = G_v. \tag{5.2}$$

Proof. Let $(\sigma_0, (\sigma_v)_{v\in V_0}) \in \operatorname{Im}\iota$, i.e. there is $\sigma \in \operatorname{Con} G$ such that $\sigma_0 = \bar{\sigma}$ and $\sigma_v = \sigma \,|_{G_v}$. If $\sigma_v \neq 1$ and $(H, G_v) \in \sigma_0$ then there are $h \in H$ and $g_v \in G_v$ such that $(h, g_v) \in \sigma$. Suppose, $H \neq G_v$. Then we have $g_v/\rho \not\subseteq g_v/\sigma$ and therefore, because of the strong neutrality (Lemma 1)

$$G_v = g_v/\rho \subseteq g_v/\sigma$$

which implies $\sigma_v = \sigma \,|_{G_v} = 1$. A contradiction. Accordingly, $H = G_v$.

Assume we have an element $(\sigma_0, (\sigma_v)_{v\in V_0})$ such that (5.2) holds. It remains to show that there exists $\sigma \in \operatorname{Con} G$ such that $\iota(\sigma) = (\sigma_0, (\sigma_v)_{v\in V_0})$. Let us define σ as follows

$$\sigma := \{(u, w) \mid \exists v \in V_0 : (u, w) \in \sigma_v, \ \text{ or } \ (u/\rho, w/\rho) \in \sigma_0 \ \text{ and } \ u/\rho \neq w/\rho\}.$$

We will prove that every σ-class M is a module. Let $u, w \in M$ and $t \notin M$. Thereby $(u, w) \in \sigma$ and $(u, t) \notin \sigma$, i.e.

$$\exists v \in V_0 : (u, w) \in \sigma_v, \ \text{ or } \ (u/\rho, w/\rho) \in \sigma_0 \ \text{ and } \ u/\rho \neq w/\rho \tag{5.3}$$

$$\forall v \in V_0 : (u, t) \notin \sigma_v, \ \text{ and } \ (u/\rho, t/\rho) \notin \sigma_0 \ \text{ or } \ u/\rho = t/\rho. \tag{5.4}$$

If $(u, w) \in \sigma_v$ and $ut \in E$ [dually $tu \in E$] then $wt \in E$ [dually $tw \in E$]. Indeed, in the case if $t \in G_v$ the statement follows from the fact that u/σ_v is a module, otherwise $t \notin G_v$ we use the fact that G_v is a module. If $u/\rho \neq w/\rho$ and $(u/\rho, w/\rho) \in \sigma_0$ then $\sigma_v \neq 1$ and by (5.2) we have $w/\rho = u/\rho$, a contradiction. Therefore by (5.4) we have $(u/\rho, t/\rho) \notin \sigma_0$. If there is an edge between t and u in graph G, there has to be an edge between the corresponding ρ-classes t/ρ and u/ρ in the factor graph. As $(u/\rho)/\sigma_0 = (v/\rho)/\sigma_0$ is a module in G/ρ there has to be an edge between t and v in G/ρ. Therefore, M is a module and thereby σ is a congruence relation. It remains just to verify that $\iota(\sigma) = (\sigma_0, (\sigma_v)_{v\in V_0})$ which is obvious. □

Corollary 1 *If G is a finite graph, $G_0 = G/\Im(G) = \{G_1, ..., G_n\}$ and $L_0 = \mathrm{Con}\, G/\Im(G)$ then*

$$\mathrm{Con}\, G = \mathrm{Con}\, G_0[(G_1, ..., G_n)] = L_0[(\mathrm{Con}\, G_1, ..., \mathrm{Con}\, G_n)].$$

Corollary 2 *A lattice L is isomorphic to the congruence lattice of a finite graph if and only if it can be assembled from the lattices $\mathbf{\Pi}_n$ and $(\mathbf{\Pi}_2)^\ell$ using the lexicographic product operation, assuming that the constructions*

$$(\mathbf{\Pi}_2)^\ell[(..., (\mathbf{\Pi}_2)^\ell, ...)],$$

with $\ell > 1$ are not allowed.

The last theorem gives us a complete characterization of the congruence lattice of finite graph.

5.5 Congruence lattice of an undirected graph

Theorem 35 *If $L_0 \hookrightarrow \mathbf{\Pi}(n)$ and $L'_0 \hookrightarrow \mathbf{\Pi}(m)$ are lattices, the co-atoms of L_0 and L'_0 intersect to 0,*

$$L = L_0[(L_1, ..., L_n)] \cong L'_0[(L'_1, ..., L'_m)] = L'$$

and $L_1, ..., L_n, L'_1, ..., L'_m$ are non-trivial directly indecomposable lattices then $m = n$ and there is a suitable substitution $\mathbf{n} \xrightarrow{\alpha} \mathbf{n}$ such that $L_i \cong L'_{\alpha(i)}$ for all $i \leq n$.

Proof. Let c and c' be the intersection of all co-atoms of L and L' respectively. Therefore, by Theorem 31, we have $c = (0, 1, 1, ..., 1)$ and $c' = (0, 1, 1, ..., 1)$. If $L \xrightarrow{\phi} L'$ is an isomorphism then obviously $\phi(c) = c'$ and therefore, by Theorem 30, we have

$$L_1 \times ... \times L_n \cong L'_1 \times ... \times L'_m.$$

Accordingly, (a proof is presented in [15]) $n = m$ and there is a bijection $\mathbf{n} \xrightarrow{\alpha} \mathbf{n}$ such that $L_i \cong L'_{\alpha(i)}$ for all $i \leq n$. □

Lemma 1 *If $\mathrm{Con}\, G \cong \mathbf{\Pi}_2 \times \mathbf{\Pi}_2$ then G is not undirected.*

Proof. Assume G is undirected and $\mathrm{Con}\, G \cong \mathbf{\Pi}_2 \times \mathbf{\Pi}_2$. Let ρ_1 and ρ_2 be co-atoms of $\mathrm{Con}\, G$. G is $\Im$-semisimple because $\rho_1 \wedge \rho_2 = 0$. Therefore G must be either a complete graph or an edgeless graph and therefore $\mathrm{Con}\, G \cong \mathbf{\Pi}_n$ for some n which is a contradiction. □

Theorem 36 *The congruence lattice of a finite undirected graph G is directly indecomposable.*

Proof. We use the induction on the number of congruence relations of G. The statement is obviously true for simple graphs. Let G be a graph and the statement is true for all graphs G' such that $|\operatorname{Con} G'| \leq |\operatorname{Con} G|$. Let L_1, L_2 be nontrivial lattices and $L_1 \times L_2 \xrightarrow{\phi} \operatorname{Con} G$ be a lattice isomorphism. Let p_1 and p_2 be atoms of L_1 and L_2 respectively. Then $\rho_1 = \phi(p_1, 0)$ and $\rho_2 = \phi(0, p_2)$ are atoms of $\operatorname{Con} G$. Obviously,

$$\begin{array}{rcccl} \operatorname{Con} G/\rho_1 & \cong & {\rho_1}^{\triangle} & \cong & {p_1}^{\triangle} \times L_2 \\ \operatorname{Con} G/\rho_2 & \cong & {\rho_2}^{\triangle} & \cong & L_1 \times {p_2}^{\triangle}. \end{array}$$

As $|\operatorname{Con} G/\rho_1| \leq |\operatorname{Con} G|$ and $|\operatorname{Con} G/\rho_2| \leq |\operatorname{Con} G|$, if follows from the induction hypothesis that $\operatorname{Con} G/\rho_1$ and $\operatorname{Con} G/\rho_2$ are directly indecomposable. Therefore, at least one component is trivial in both decompositions. As L_1 and L_2 are nontrivial, we have $p_1 = 1$ and $p_2 = 1$. Accordingly, $L_1 \cong L_2 \cong \mathbf{\Pi}_2$ therefore $\operatorname{Con} G \cong \mathbf{\Pi}_2 \times \mathbf{\Pi}_2$ which is impossible by lemma 1. $\square$

In this chapter we assume that all graphs are finite.

6.1 Comparability graphs

Comparability graphs are very important objects in the field of combinatorics. They have been studied extensively by A. Ghouilà-Houri [6], P.C.Gilmore and A.J.Hoffman [7] in the sixties and independently by A.Pnueli, A.Lempel and S.Even in the seventies [12].

Let us look at the first (undirected) graph in the figure 6.16. Suppose we want

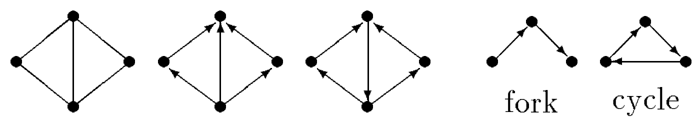


Figure 6.16: Graph and its transitive orientation

to replace undirected edges with directed edges in such a way that the last two graphs in the figure 6.16 (*fork* and *cycle*) are not induced subgraphs of the final directed graph. The second graph in the figure 6.16 shows how it can be done. Such graphs are known as *comparability graphs* or *transitively orientable (TRO)* graphs. For example, the graph in Figure 6.17. If we set a bit weaker requirement

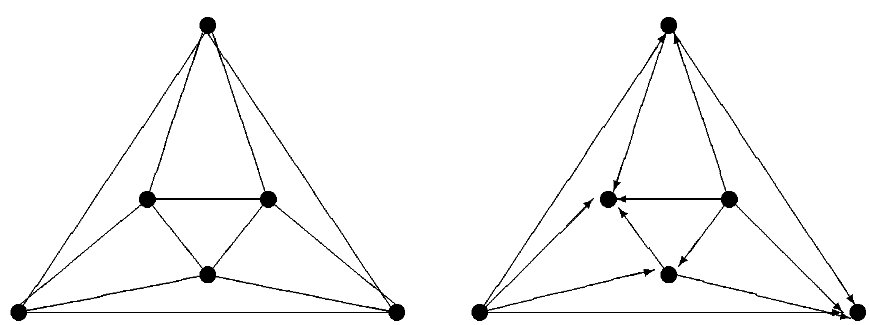


Figure 6.17: A comparability graph oriented transitively.

to the final graph by forbidding only the forks, we get a class of graphs called *pseudotransitively orientable* graphs. It is clear that every comparability graph is pseudotransitively orientable, but we also emphasize that a pseudotransitively oriented graph may contain cycles. For example, look at the graph in the figure 6.18 and also the third graph in the Figure 6.16.

It may seem surprising, but it turns out that if we can avoid forks in the final graph then we can avoid cycles as well. This is the corollary of the following theorem which is a consequence of several statements proved by A.Ghouilà-Houri, P.C.Gilmore, A.J.Hoffman.

Theorem 37 *Every pseudotransitively orientable graph is transitively orientable.*

We give a proof which is not the shortest possible, but contains some new ideas about the algebraic description of graphs. The main idea is based on the modular decomposition discovered by Jeremy Spinrad (e.g. [19]).

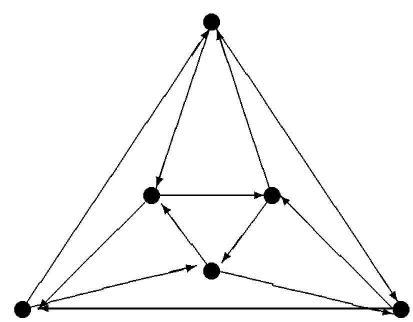


Figure 6.18: A graph oriented pseudotransitively with cycles.

6.1.1 Simple graphs and transitive relations

Binary relation S in the set V is said to be *pseudotransitive* if the condition

$$xy \in S,\ yz \in S \Rightarrow xz \in S \ \text{ or } \ zx \in S$$

holds for every $x, y, z \in V$. A graph $G = (V, E)$ is *pseudotransitively orientable* if there exists a pseudotransitive relation S such that $E = S \cup S^{-1}$. Similarily, G is *transitively orientable* if there is a partial ordering T such that $E = T \cup T^{-1}$.

Graph $G = (V, E)$ is pseudotransitively orientable iff $xy \not\equiv yx(\Gamma)$ for every edge $xy \in E$.

Theorem 38 *If $G = (V, E)$ simple, S is a pseudotransitive relation and $E = S \cup S^{-1}$ then S is transitive.*

Proof. Assume S is not transitive. It follows from the simplicity (primeness) that S and S^{-1} are the only Γ-classes of G. Indeed, if $xy \in E$ and $zt \in E$ then either $xy \equiv zt(\Gamma)$ or $xy \equiv tz(\Gamma)$. Now define a ternary relation $\mathcal{Z}$ in V such that $xyz \in \mathcal{Z}$ iff xy, yz and zx belong to S. We say that vertices x, y, z form a *cycle*.

Lemma 1 *If $xyz \in \mathcal{Z}$ then $\langle xy, ty\rangle \in K_+$ implies $tyz \in \mathcal{Z}$ and $\langle xy, xt\rangle \in K_-$ implies $xtz \in \mathcal{Z}$*

Proof. Let us prove the first claim, the proof of the second one is similar. If $xyz \in \mathcal{Z}$ and $\langle xy, ty\rangle \in K_+$ then $xy, yz, zx, ty \in S$ and $xt, tx \notin S$ by definition of K_+. As $ty \in S$ and $yz \in S$, it follows from pseudotransitivity that either $zt \in S$ or $tz \in S$. If $tz \in S$ then $zx \in S$ implies $tx \in S$ or $xt \in S$, which is impossible. Therefore $zt \in S$ and then $tyz \in \mathcal{Z}$. This proves the lemma. □

As S is not transitive there is at least one cycle xyz and therefore $xy \equiv yz(\Gamma)$. But then there should exist a chain of edges

$$xy \;\; K_+ \;\; t_1y \;\; K_- \;\; t_1t_2 \;\; K_+ \;\; ... \;\; K_+ \;\; t_\ell t_{\ell-1} \;\; K_- \;\; t_\ell z \;\; K_+ \;\; yz$$

Now we can use the previous lemma to get the following chain of implications

$$\begin{aligned}
xyz \in \mathcal{Z},\ \langle xy, t_1y\rangle \in K_+ &\;\Rightarrow\; t_1yz \in \mathcal{Z}\\
t_1yz \in \mathcal{Z},\ \langle t_1y, t_1t_2\rangle \in K_- &\;\Rightarrow\; t_1t_2z \in \mathcal{Z}\\
t_1t_2z \in \mathcal{Z},\ \langle t_1t_2, t_3t_2\rangle \in K_+ &\;\Rightarrow\; t_3t_2z \in \mathcal{Z}\\
&\ldots\\
t_\ell t_{\ell-1}z \in \mathcal{Z},\ \langle t_\ell t_{\ell-1}, t_\ell z\rangle \in K_- &\;\Rightarrow\; t_nzz \in \mathcal{Z}
\end{aligned}$$

The last sentence is obviously wrong. A contradiction. □

Thereby, we have proved the special case of Theorem 37, i.e. the case if G is simple.

Let us use the notation $\mathcal{TO}(G)$ if G is transitively orientable and the notation $\mathcal{PO}(G)$ if G is pseudotransitively orientable. It is clear that the properties $\mathcal{TO}$ and $\mathcal{PO}$ are both hereditary.

Theorem 39 *The properties $\mathcal{TO}$ and $\mathcal{PO}$ are equivalent for all graphs.*

Proof. It is sufficient to show that $\mathcal{TO}$ and $\mathcal{PO}$ are inductive. Let G be graph and $G/\rho = \{G_1, ..., G_\ell\}$ is a congruence partition and the graphs $G/\rho, G_1, ..., G_\ell$ are transitively [pseudotransitively] orientable. Let $T_1, ..., T_\ell, T_\rho$ be the corresponding transitive [pseudotransitive] and antireflexive relations. Define the relation T as follows

$$T := \{\langle x, y\rangle \mid \exists i(\langle x, y\rangle \in T_i) \text{ or } \langle \pi(x), \pi(y)\rangle \in T_\rho\}$$

where $G \xrightarrow{\pi} G/\rho$ is natural projection. It is easy to verify that T is indeed transitive [pseudotransitive]. Therefore G has property $\mathcal{TO}$ [$\mathcal{PO}$].

Thereby the properties $\mathcal{TO}$ and $\mathcal{PO}$ are equivalent for prime graphs (by Theorem 38) and they are both inductive and injective. Thus (by Lemma 1) the properties $\mathcal{TO}$ and $\mathcal{PO}$ are equivalent for all graphs. □

6.1.2 Permutation graphs

Suppose we have a permutation $\{1,...,n\} \xrightarrow{\sigma} \{1,...,n\}$. By a *permutation graph* $G(\sigma)$ we mean an undirected graph $(V, E \cup E^{-1})$ such that $V = \{1,...,n\}$ and

$$E = \{\langle i,j\rangle \mid i < j,\ \sigma(j) < \sigma(i)\}.$$

It is easy to see that an undirected graph $G = (V, E)$ is a comparability graph if and only if there exists a partial ordering T on V such that et $E = T \cup T^{-1}$, and G is a permutation graph if and only if there exist two linear orderings R, S on V such that

$$E = (R \cap S^{-1}) \cup (S \cap R^{-1}).$$

It turns out (proved by Pnueli,Lempel and Even [12]) that the permutation graphs and comparability graphs are closely related.

Theorem 40 *An undirected graph G is a permutation graph if and only if G ja $\overline{G}$ are transitively orientable.*

Proof. Let $G = (V, E)$ be a permutation graph and R, S be suitable linear orderings, i.e.

$$E = (R \cap S^{-1}) \cup (S \cap R^{-1}) = (R \cap S^{-1}) \cup (R \cap S^{-1})^{-1}.$$

As R and S^{-1} are orderings their intersection is also a partial ordering and thereby a suitable partial ordering is $T = R \cap S^{-1}$. The complement graph $\overline{G}$ is also a comparability graph because

$$\begin{aligned} \overline{E} &= \overline{R \cap S^{-1}} \cap \overline{S \cap R^{-1}} = (\overline{R} \cup S) \cap (\overline{S} \cup R) = \\ &= (R \cap S) \cup (R \cap S)^{-1} \end{aligned}$$

For proving the if-part, suppose G and $\overline{G}$ are comparability graphs and T, L are linear orderings such that $E = T \cup T^{-1}$ and $\overline{E} = L \cup L^{-1}$. The *universal relation* $U = (V \times V)\backslash 1_V$ may be represented as a direct union

$$I = T \coprod L \coprod T^{-1} \coprod L^{-1}.$$

It remains to show that $R = T \cup L$ and $S = T^{-1} \cup L$ are linear orderings. We begin with proving the transitivity of $R = T \cup L$. Suppose $\langle x, y\rangle, \langle y, z\rangle \in R$

and $\langle x,z\rangle \notin R$. We assume without loss of generality that $\langle x,y\rangle \in T$. Thereby, because of the transitivity of T we have $\langle y,z\rangle \in L$ [5] Assuming $\langle x,z\rangle \in T^{-1}$ (i.e. $\langle z,x\rangle \in T$) leads us to a contradiction with the transitivity of T [6] Assuming $\langle x,z\rangle \in L^{-1}$ leads us (in a similar manner) to a contradiction with the transitivity of L.

The linearity of R follows from $I = (T \cup L) \coprod (T \cup L)^{-1}$ which implies that $(T \cup L)^{-1} = \overline{T \cup L}$. The proof that S is a linear ordering is similar. And finally,

$$\begin{aligned} E &= T \cup T^{-1} = (T \cup \emptyset) \cup (T^{-1} \cup \emptyset) = \\ &= [T \cup (L \cap L^{-1})] \cup [T^{-1} \cup (L \cap L^{-1})] = \\ &= [(T \cup L) \cap (T \cup L^{-1})] \cup [(T^{-1} \cup L) \cap (T^{-1} \cup L^{-1})] = \\ &= (R \cap S^{-1}) \cup (S \cap R^{-1}). \end{aligned}$$

□

Each undirected graph with n vertices can be represented using $n^2/2$ bits. However, for representing a permutation graph we need only $2n \cdot \log_2 n$ bits of memory. Indeed, we need $\log_2 n$ bits for encoding a number in $\{1, ..., n\}$ and a permutation σ may be represented as a sequence of n numbers $(\sigma(1), ..., \sigma(n))$. Its size is $n \cdot \log_2 n$. For encoding a permutation graph we need another $n \cdot \log_2 n$ bits for representing an order of the vertices. For example for the edge set E of the graph in Figure 6.19 there exist no linear orderings S such that $(R \cap S^{-1}) \cup$

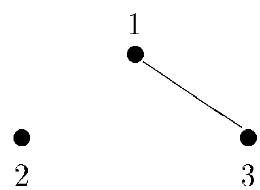


Figure 6.19: A graph that may not be represented with a single permutation.

$(R^{-1} \cap S)$, assumed that R is a natural ordering (defined by the labeling of G). The next tabel illustrates the values of the functions $n^2/2$ and $2n \cdot \log_2 n$.

	2	3	4	5	16	20	100
$n^2/2$	2	4	8	12	128	200	5000
$2n \cdot \log_2 n$	4	10	16	23	128	173	1329

Hence, large permutation graphs may be represented more efficiently by using permutations. This fact may therefore be useful in data compression.

[5]Indeed, if $\langle x,y\rangle \in T$ then by transitivity $\langle x,z\rangle \in T$ which contradicts with $\langle x,z\rangle \notin R$.
[6]Indeed, then we have $\langle z,x\rangle, \langle x,y\rangle \in T$ and $\langle z,y\rangle \notin T$.

6.2 Cliques of maximum weight

We will show that the hardness of finding the clique of maximum weight is caused by simple graphs, i.e. if there exists a polynomial algorithm to determine the maximal clique size in simple graphs, there has to be a polynomial algorithm for all graphs.

Let $G = (V, E)$ be a undirected grap and $V \xrightarrow{\mu} \mathbf{N}$ to be a positive integer valued function assigning to each vertex $v \in V$ its weight $\mu(v)$. The function μ can be extended to the power set of V by defining the weight of a subset U as the sum of the weights of its elements, i.e. $\mu(U) := \sum_{u \in U} \mu(u)$. Obviously, the problem of finding the value of

$$\mathsf{cl}[G, \mu] := \max\{\mu(C) \mid C \subseteq V \wedge \forall x, y \in C(x \neq y \Rightarrow xy \in E)\}.$$

is **NP**-complete. What we want to do is to decompose the problem into smaller subproblems using a suitable partitioning of the vertex set. It turns out that the congruence relations, if they exist, significantly simplify the problem of finding a maximum clique. It turns out that if there is a nontrivial congruence relation $\rho \in \operatorname{Con} G$ the original problem reduces to similar problems about ρ-classes. It turns out that the hardness of this problem is caused by simple graphs. Let ρ be a nontrivial congruence relation of G. And let $G_0 \cong G/\rho = \{G_1, ..., G_n\}$. We will prove prove that

$$\mathsf{cl}[G_0[(G_1, ..., G_n)], \mu] = \mathsf{cl}[G_0, \bar{\mu}]$$

where $\bar{\mu}(G_i) := \mathsf{cl}[G_i, \mu \mid_{G_i}]$.

Lemma 2 *If K is a clique of maximal weight $\mu(K)$ in $G = (V, E)$, $M \subseteq V$ is a module and $M \cap K \neq \emptyset$ then $M \cap K$ is a clique with maximal weight in M.*

Proof. Let $K' \subseteq M$ and $\mu(K') > \mu(K \cap M)$. We show that $(K - M) \cup K'$ is a clique in G. Indeed, let $x \in K - M$ and $y \in K'$. As $K \cap M \neq \emptyset$, there is $z \in K \cap M$ and as K is a clique, we have $xz \in E$. Therefore $xy \in E$ because M is a module.

Therefore, $(K - M, K')$ is a diclique and thus $(K - M) \cup K'$ is a clique because $K - M$ and K' are both cliques. Hence,

$$\mu[(K - M) \cup K'] = \mu(K - M) + \mu(K') > \mu(K - M) + \mu(K \cap M) = \mu(K).$$

A contradiction. □

Lemma 3 *If K is a clique in $G = (V, E)$ then there exists a clique $\bar{K}$ in G/ρ such that $\bar{\mu}(\bar{K}) = \mu(K)$.*

Proof. Let $V \xrightarrow{\pi} V/\rho$ be the natural projection. Define $\bar{K} := \pi(K) = \{M \mid M \in G/\rho \wedge M \cap K \neq \emptyset\}$. By lemma 2 we have

$$\bar{\mu}[\pi(K)] = \sum_{M \in \pi(K)} \bar{\mu}(M) = \sum_{M \in \pi(K)} \mu(M \cap K) = \mu(K).$$

□

Lemma 4 *If $\bar{K} \neq \emptyset$ is a clique in G/ρ then there is a clique K in G such that $\bar{\mu}(\bar{K}) \leq \mu(K)$.*

Proof. Let $\bar{K} = \{G_1, ..., G_m\}$ where $G_i \in V/\rho$. Let K_i be a clique in G_i with maximal weigth $\mu(K_i)$. Define $K := \bigcup_{i=1}^{m} K_i$ and show that K is a clique in G with desired properties. Indeed,

$$\mu(K) = \mu(\bigcup_{i=1}^{m} K_i) = \sum_{i=1}^{m} \mu(K_i) = \sum_{i=1}^{m} \bar{\mu}(G_i) = \bar{\mu}(\bar{K}).$$

□

Accordingly, if there exists a polynomial algorithm for finding a maximum clique in simple graphs then there exists a polynomial algorithm for finding a maximum clique in all graphs. The best examples demonstrating the power of using structure properties are the Moon-Moser graphs [8] $M_{i,k} = O_k[\overbrace{K_i, ..., K_i}^{k}]$ that have exponential number of maximal cliques. However, if the congruence relations are known, the time needed to determine the size of maximum clique is polynomial with respect to the number of vertices.

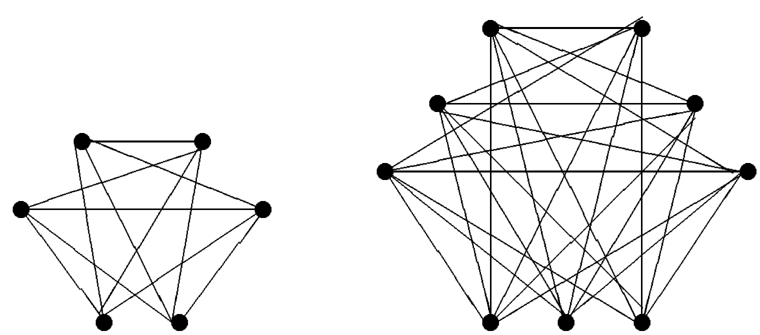


Figure 6.20: The Moon-Moser graphs $M_{3,2}$ and $M_{3,3}$.

6.3 Isomorphism of coloured graphs

By a coloured graph we mean a triple $G = (V, E, c)$, where (V, E) is a graph and $V \xrightarrow{c} \mathbf{N}$ is a function assigning to each vertex v a natural number $c(v)$ (colour of v). Let $G_1 = (V_1, E_1, c_1)$ and $G_2 = (V_2, E_2, c_2)$ be coloured graphs. A mapping $V_1 \xrightarrow{f} V_2$ is called a c-morphism if it is a graph morphism and preserves the colours, i.e. if $c_1 = c_2 \circ f$.

There is no known polynomial-time algorithms for this problem. Though, it is not proved that the problem is **NP**-complete. What we want to do is to find equivalence relations ρ_1 and ρ_2 on V_1 and V_2 such that the problem of finding an isomorphism between G_1 and G_2 reduces to find a suitable matching between the equivalence classes (viewed as induced subgraphs) of ρ_1 and of ρ_2. If we have found a mapping $G_1/\rho_1 \xrightarrow{\bar{f}} G_2/\rho_2$ such that any ρ_1-class G_{1i} is isomorphic to the ρ_2-class $\bar{f}(G_{1i})$, the isomorphism $G_1 \xrightarrow{f} G_2$ can also be built if we assume that ρ_1, ρ_2 are congruence relations and $\bar{f}$ is an isomorphism between G_1/ρ_1 and G_2/ρ_2.

However, finding such a pair of congruence relations may not be easy because when choosing arbitrary pair of congruence relations it may not be possible to find a suitable matching between the corresponding congruence classes. Thereby, the way of choosing (ρ_1, ρ_2) should be canonical, i.e. should no depend on a particular order of vertices etc. We show that a *radical maps* may be used for that purpose.

Theorem 41 *Let μ be a complete invariant, i.e. $\mu(G_1) = \mu(G_2)$ implies $G_1 \cong G_2$. Let $G_1 = (V_1, E_1, c_1)$ and $G_2 = (V_2, E_2, c_2)$ be coloured graphs, $\rho_1 \in \operatorname{Con} G_1$ and $\rho_2 \in \operatorname{Con} G_2$ be congruence relations. The isomorphity of coloured graphs $(V_1/\rho_1, E_1/\rho_1, \mu)$ and $(V_2/\rho_2, E_2/\rho_2, \mu)$ implies the isomorphity of G_1 and G_2.*

Proof. Let $V_1/\rho_1 \xrightarrow{\bar{f}} V_2/\rho_2$ be a c-isomorphism, i.e. $\mu(H) = \mu(\bar{f}(H))$ and therefore $H \cong \bar{f}(H)$ for each ρ_1-class H. Accordingly, there exists a mapping ϕ assigning to each ρ_1-class H a c-isomorphism $H \xrightarrow{\phi(H)} \bar{f}(H)$. Let $V_1 \xrightarrow{\pi_1} V_1/\rho_1$ and $V_2 \xrightarrow{\pi_2} V_2/\rho_2$ be the natural projections. Define $V_1 \xrightarrow{f} V_2$ as follows:

$$f(x) := [\phi(\pi_1(x))](x).$$

It follows immediately from the definition that the following diagram has to be commutative

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ {\scriptstyle\pi_1}\downarrow & & \downarrow{\scriptstyle\pi_2} \\ G_1/\rho_1 & \xrightarrow[\bar{f}]{} & G_2/\rho_2. \end{array} \tag{6.1}$$

f is injective, because if $f(x) = f(y)$, we have $\bar{f}(\pi_1(x)) \ni f(x) = f(y) \in \bar{f}(\pi_1(y))$ and therefore $\bar{f}(\pi_1(x)) = \bar{f}(\pi_1)(y)$ keeping in mind the fact that the intersecting equivalence classes coincide. As $\bar{f}$ is an isomorphism we have $\pi_1(x) = \pi_1(y)$ and thus

$$[\phi(\pi_1(x))](x) = [\phi(\pi_1(x))](y)$$

implying $x = y$ due to the fact that $\phi(\pi_1(x))$ is an isomorfism.

Let x' be an arbitrary vertex in V_2. As $\bar{f}$ and π_1 are onto, there exists $H \in V_1/\rho_1$ such that $\bar{f}(H) = \pi_2(x')$. Accordingly there exists an isomorphism $H \xrightarrow{\phi(H)} \pi_2(x')$. As $x' \in \pi_2(x')$ and $\phi(H)$ is onto, there exists an $x \in H$, such that $[\phi(H)](x) = x'$. As $H = \pi_1(x)$,

$$f(x) = [\phi(\pi_1(x))](x) = [\phi(H)](x) = x'$$

showing that f is onto. It remains to prove the morphism condition. Let $x, y \in V_1$ and $f(x) \neq f(y)$. If $\pi_1(x) = \pi_1(y)$, we have $xy \in E_1 \Leftrightarrow f(x)f(y) \in E_2$ because $\phi(\pi_1(x))$ is a morphism. Otherwise, if $\pi_1(x) \neq \pi_1(y)$ then $x \neq y$ and also $\bar{f}(\pi_1(x)) \neq \bar{f}(\pi_1(y))$ because of the injectivity of $\bar{f}$. From the commutativity of the Diagram (6.1) it follows that $\pi_2(f(x)) \neq \pi_2(f(y))$. As π_1, π_2 and $\bar{f}$ are morphisms, we have

$$\begin{aligned} xy \in E_1 &\Leftrightarrow \pi_1(x)\pi_1(y) \in E_1/\rho_1 \\ &\Leftrightarrow \bar{f}(\pi_1(x))\bar{f}(\pi_1(y)) \in E_2/\rho_2 \\ &\Leftrightarrow \pi_2(f(x))\pi_2(f(y)) \in E_2/\rho_2 \\ &\Leftrightarrow f(x)f(y) \in E_2 \end{aligned}$$

showing that f is a morphism. For proving that f is colour-preserving let $x \in V_1$. Thus $c_2(f(x)) = c_2[[\phi(\pi_1(x))](x)] = c_1(x)$ because $\phi(\pi_1(x))$ is a c-morphism. □

The following theorem demonstrates the importance of the concept of radical in determining the isomorphy of coloured graphs.

Theorem 42 *Let μ be a complete invariant and $\Re$ be a radical map. Two coloured graphs $G_1 = (V_1, E_1, c_1)$ and $G_2 = (V_2, E_2, c_2)$ are isomorphic if and only if the coloured graphs $(V_1/\Re(G_1), E_1/\Re(G_1), \mu)$ and $(V_2/\Re(G_2), E_2/\Re(G_2), \mu)$ are isomorphic.* [7]

Proof. The if-part is a special case of Theorem 41. Therefore it is sufficient to prove the only-if-part. Let $G_1 \xrightarrow{f} G_2$ be an isomorphism, $G_1 \xrightarrow{\pi_1} G_1/\Re(G_1)$, $G_2 \xrightarrow{\pi_2} G_2/\Re(G_2)$ be the natural projections.

If $(x, y) \in \operatorname{Ker} \pi_1 = \Re(G_1)$ then using the properties of $\Re$ we get $(f(x), f(y)) \in \Re(G_2) = \operatorname{Ker} \pi_2$, i.e. $(x, y) \in \operatorname{Ker}(\pi_2 \circ f)$. Inversely, if $(x, y) \in \operatorname{Ker}(\pi_2 \circ f)$ then $(f(x), f(y)) \in \operatorname{Ker} \pi_2 = \Re(G_2)$ by the properties of $\Re$, we get $(x, y) =$

[7] Here the notation $E_1/\Re(G_1)$ means that if $G_1 \xrightarrow{\pi_1} G_1/\Re(G_1)$ is a natural projection, then $(\pi_1(x), \pi_1(y)) \in E_1/\Re(G_1)$ if and only if $(x, y) \in E_1$.

$(f^{-1}(f(x)), f^{-1}(f(y))) \in \Re(G_1) = \operatorname{Ker}\pi_1$. Therefore $\operatorname{Ker}\pi_1 = \operatorname{Ker}(\pi_2 \circ f)$ and thus there exists an isomorphism $\bar{f}$ making the following diagram commutative:

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ G_1/\Re(G_1) & \xrightarrow[\bar{f}]{} & G_2/\Re(G_2). \end{array}$$

It remains to prove that $\bar{f}$ is colour-preserving. This follows from the assumption that f is an isomorphism and therefore the restriction of f into the arbitrary $\Re(G_1)$-class is also an isomorphism. □

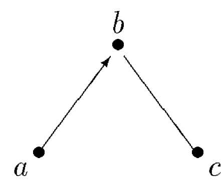
In order to determine whether the graphs G_1 and G_2 are isomorphic we should find the corresponding radicals $\Re(G_1)$ and $\Re(G_2)$. If the corresponding factor graphs have not identical number of vertices we can conclude by Theorem 42 that $G_1 \ncong G_2$. Let $G_1/\Re(G_1) = \{G_{11}, ..., G_{1\ell}\}$ and $G_2/\Re(G_2) = \{G_{21}, ..., G_{2\ell}\}$. Now we recursively compare the pairs (G_{1i}, G_{2j}) using (there are ℓ^2 of them) and assign colours to the vertices of $G_1/\Re(G_1)$ and $G_2/\Re(G_2)$ in such a way that G_{1i} and G_{2j} have the same colours if and only if $G_{1i} \cong G_{2j}$. By Theorem 42 it remains to compare the factor graphs $(V_1/\Re(G_1), E_1/\Re(G_1), \mu)$ and $(V_2/\Re(G_2), E_2/\Re(G_2), \mu)$.

Using such a technique significantly reduces the the time needed for the determination of the isomorphy of two coloured graphs in the case if the graphs are not $\Re$-semisimple. If there exists a polynomial-time algorithm capable to determine the isomorphy of simple graphs, there exist also a polynomial-time algoritm for the general case.

The name of this short chapter may as well be "Epilogue". We show that the structure theory developed in previous chapters of the thesis can be significantly simplified. The graph morphisms and congruence relations presented in the thesis seem to have similar properties with the morphisms and congruences of algebraic structures. Though, we did not use any algebraic operations. Only when the thesis was almost written, the author found a suitable binary operation on the vertex set "responsible" for such a similarity. Moreover, it turned out that the idea of representing a graph as a groupoid was already used by Czhech mathematicians ([14],[20],[33]).

The new notion of a graph morphism introduced in the thesis has indeed an algebraic nature. For each graph $G = (V, E)$ define a binary operation $V \times V \stackrel{\cdot}{\longrightarrow} V$ as follows:

$$v \cdot w = \begin{cases} w, & \text{if } vw \in E \\ v, & \text{if } vw \notin E. \end{cases} \tag{7.1}$$



	a	b	c
a	a	b	a
b	b	b	c
c	c	b	c

Figure 7.21: A graph and the corresponding groupoid.

The corresponding groupoid $(G, \cdot)$ is *quasitrivial*, i.e. $vw \in \{v, w\}, \forall v, w$. For every quasitrivial groupoid $(G, \cdot)$ we can define a binary relation E such that the condition (7.1) holds. Indeed, the relation E can be defined as $E = \{(v, w) \mid v \neq w, v \cdot w = w\}$. Quasitrivial groupoids and their relations with graphs have been studied by Czhech mathematicians ([14],[20],[33]).

Theorem 43 *A mapping f between the vertex sets of two graphs is a graph morphism if and only if it is a morphism of the corresponding groupoids, i.e. iff*

$$f(v \cdot w) = f(v) \cdot f(w).$$

The proof is straightforward and has been omitted.

Accordingly, the category of all graphs is isomorphic to the category of all quasitrivial groupoids and the graphs can be viewed as algebras with a single binary operation. We can use all the theorems about these algebras.

Several classes of graphs can be characterized by identities. For example, an *edgeless [complete]* graph can be defined by the identity $xy = x$ $[xy = y]$, a *partial* *ordering* by the identities $xy \cdot x = xy$ and $xy \cdot (x \cdot yz) = x \cdot yz$, a *linear* graph by the identities $xy = yx$ and $x \cdot yz = xy \cdot z$, a graph without 3-cycles by the identity

$$\{[(xz \cdot yz)(zy \cdot xy)][(yx \cdot yz)(zx \cdot yz)]\}(xz \cdot zy) = \\ \{(xz \cdot yz)\{[(zy \cdot xy)(yx \cdot xz)](zx \cdot yz)\}\}(xz \cdot zy).$$

Identities in graphs are studied in [14], associative identities in graph-algebras in [37].

The author should acknowledge that if this equivalence of the categories was discovered sooner, a large fraction of the claims presented in the thesis became direct corollaries of the standard results in universal algebra.

For studying decompositions of graphs we present a new structure theory essence of which is algebraic in the sense that it is based solely on the algebraic properties of the congruence lattice. The crucial point of the new structure theory is the notion of a $\Im$-radical of a graph defined as the intersection of all co-atoms in its congruence lattice. The main results of the thesis concern in the following:

- We give a characterization of the $\Im$-semisimple graphs (Theorem 20, page 53) and of the corresponding congruence lattices (Corollary 2, page 56). We point out that the recursive partition of a graph using $\Im$-radical coincides with the modular decomposition of this graph.

- We give a characterization of the finite graphs with the congruence lattice satisfying a given set of lattice identities. We prove that if G is a finite graph and $\mathcal{V}$ is a lattice variety then $\mathrm{Con}(G) \in \mathcal{V}$ if and only if the modular decomposition of G does not contain graphs O_n and K_n with $\eta(\mathcal{V}) < n$, where $\eta(\mathcal{V})$ is the largest natural number k such that $\mathbf{\Pi}_k \in \mathcal{V}$ (Corallary 3, page 68).

- We give a classification of the lattices representable as congruence lattices of finite graphs (Corollary 1, page 75, Corollary 2, page 75). This is gained by introducing a new lattice operation – the lexicographic product of lattices – such that the mapping Con behaves almost like a morphism, i.e. under certain conditions it maps the generalized lexicographic product of graphs into the lexicographic product of the corresponding congruence lattices.

Graafiks nimetatakse hulkade paari $G = (V, E)$, kus E on antirefleksiivne (mitte tingimata sümmeetriline) binaarne relatsioon hulgal V. Hulkade V ja E elemente nimetatakse vastavalt *tippudeks* ja *kaarteks*. *Morphismiks* graafide $G_1 = (V_1, E_1)$ ja $G_2 = (V_2, E_2)$ vahel nimetatakse kujutust $V_1 \xrightarrow{f} V_2$, nii et

$$f(v) \neq f(w) \Rightarrow [vw \in E_1 \Leftrightarrow f(v)f(w) \in E_2] \tag{7.2}$$

mistahes tippude $v, w \in V_1$ korral. Seesugust tüüpi morfismidel on pikk ajalugu. Nad kerkisid esmakordselt esile Sabidussi [4] töödes, kus on defineeritud ka nn. *üldistatud leksikograafilise korrutise* operatsioon, mis üldistab Harary [3] poolt defineeritud nn. *kompositsiooni* operatsiooni. Neid morfisme on hiljem taasavastatud paljude teadlaste poolt (Hemminger [11], Spinrad [16], Möhring [18]). Põhiline inspiratsiooniallikas oli graafide transitiivse suunamise ülesannet lahendavate kiirete algoritmide välja töötamine ja arendamine (Ghouilà-Houri [6], Gilmore ja Hoffman [7], Pnueli, Lempel ja Even [12], Spinrad [19]. Selgus, et transitiivse suunamise jaoks loodud graafide dekompositsioonimeetod töötab suurepäraselt ka paljude teiste kombinatoorikaprobleemide korral, muuhulgas ka paljude NP-täielike probleemide korral, nagu näiteks suurima kliki leidmine ja kahe värvitud graafi isomorfsuse tuvastamine (Osa VI). Samas aga ei ole see meetod kasutatav juhul, kui uuritav graaf on lihtne, st tal pole mittetriviaalseid lahutusi. Õnnetuseks on lihtsus peaaegu kõigi lõplike graafide omadus nagu seda on tõestatud Osas II. Töödes [24],[25] ja [26] on Ehrenfeucht ja Rozenberg esitanud struktuuriteooria graafidest üldisematele objektidele, nn 2-struktuuridele. Käesoleva dissertatsiooni põhieesmärk on uurida, mida on võimalik teha puhtalgebraliste meetoditega graafide struktuuri uurimisel.

Osas I on toodud töö sisust arusaamiseks vajalikud mõisted, nende definitsioonid ja tähistused ning ära toodud ka olulisemad tulemused, millel antud töös on oluline roll.

Osas II tuuakse sisse uus graafide morfismi mõiste ja tõestatakse morfismide ja kongruentside mõningad omadused.

Osas III arutletakse graafi kongruentside võre põhiomaduste üle. Graafide jaoks on defineeritud üks algebralise struktuuriteooria põhimõisteid – radikaal. On antud kõigi poollihtsate graafide kirjeldus nn. $\Im$-radikaali korral, mis defineeritakse kui kongruentside võre kõigi ko-aatomite alumine raja.

Osas IV antakse täielik kirjeldus neile lõplikele graafidele, mille kongruentside võres kehtib fikseeritud võresamasus. Näiteks kongruents-distributiivsed (vast. modulaarsed) graafid kirjelduvad kui graafid, mille ükski komponent ega tema duaalne üldistatud leksikograafiliseks korrutiseks lahutuses ei ole rohkem kui kahe (vast. kolme) sidususkomponendiga.

Osas V kirjeldatakse võrede teatud kompositsioonimeetodit, mis defineeritakse kui võrede leksikograafiline korrutis. Seda tänu täpsele vastavusele graafide üldistatud leksikograafilise korrutise kongruentside võrega. Võime end poeetilisemalt väljendades ütelda, et teatud tingimustel säilitab operaator Con leksikograafilise korrutise operatsiooni. See fakt annab meile lõplike graafide kongruentside võrede täieliku klassifikatsiooni.

Osas VI näidatakse, kuidas algebralise dekompositsioonimeetodi rakendamine vähendab oluliselt graafidega seotud NP-raskete kombinatoorikaülesannete lahendamise keerukust.

Osas VII näidatakse, et uut tüüpi morfismidel on algebraline loomus, st tõestatakse, et graafide kategooria on ekvivalentne teatud omadustega rühmoidide kategooriga.

Töö põhitulemused:

- Antakse kirjeldus $\Im$-poollihtsatele graafidele (Teoreem 20, lk. 53) ja vastavatele kongruentside võredele (Järeldus 2, lk. 56). Leitakse, et graafi rekursiivne tükeldamine $\Im$-radikaali abil langeb kokku tema modulaardekompositsiooniga.

- Antakse kirjeldus lõplikele graafidele, mille kongruentside võred rahuldavad etteantud hulka võresamasusi. Tõestatakse, et kui G on lõplik graaf ja $\mathcal{V}$ on mingi võrede muutkond, siis $\mathrm{Con}(G) \in \mathcal{V}$ parajasti siis, kui graafi G modulaardekompositsioon ei sisalda graafe O_n ja K_n nii et $\eta(\mathcal{V}) < n$, kus $\eta(\mathcal{V})$ on suurim naturaalarv k, mille korral $\mathbf{\Pi}_k \in \mathcal{V}$ (Järeldus 3, lk. 68).

- Antakse klassifikatsioon kõigile sellistele võredele, mis on esiatavad lõpliku graafi kõigi kongruentside võrena. (Järeldus 1, lk. 75, Järeldus 2, lk. 75). See saavutatakse uue võreoperatsiooni – võrede leksikograafilise korrutise – sissetoomisega, nii et kujutus Con käitub "peaaegu" morfismina, st. teatud tingimustel ta kujutab graafide üldistatud leksikograafilise korrutise vastavate kongruentside võrede leksikograafiliseks korrutiseks.

[1] Birkhoff, G., "Lattice theory," New York, 1948.

[2] Čulik, K., "Zur Theorie der Graphen," Casopis Pest. Mat. 83 (1958) 133–155.

[3] Harary, F., "On the group of the decomposition of two graphs," Duke Math. J. 26 (1959) 29–34.

[4] Sabidussi, G., "Graph derivatives," Math. Z., 76 (1961) 385–401.

[5] Sachs, D., "Identities in finite partition lattices," Proc. Amer. Math. Soc. 12, 944–945.

[6] Ghouilà-Houri, A., "Caractérisation des graphes nonorientés dont on peut orienter les arêtes de manière à obtenir le graphe d'une relation d'ordre," C. R. Acad. Sci. Paris I Math., 254 (1962) 1370–1371.

[7] Gilmore, P.C., Hoffman, A.J., "A characterization of comparability graphs and of interval graphs," Canad. J. Math., 16 (1964) 539–548.

[8] Moon, J., Moser, L., "On cliques in graphs," Israel J. Math., 3 (1965) 23–28.

[9] Gallai, T., "Transitiv orientierbare graphen," Acta Math. Acad. Sci. Hungar., 18 (1967) 25–66.

[10] Jónsson, B. "Algebras whose congruence lattices are distributive," *Math. Scand.* 1967, 21, 110–121.

[11] Hemminger, R.L., "The group of an X-join of graphs," J. Combin. Th., 5 (1968) 408–418.

[12] Pnueli, A., Lempel, A., Even, S., "Transitive orientation of graphs and identification of permutation graphs," Canad. J. Math., 1 (1971), 160–175.

[13] Takeuti,G., Zaring,W.M., "Introduction to Axiomatic Set Theory," Springer-Verlag, Berlin, 1971.

[14] Ježek, J., Kepka, T., "Quasitrivial and nearly quasitrivial distributive groupoids and semigroups," Acta Univ. Carolinae, Math. et Phys. 19 (1978) 25–44.

[15] Grätzer, G., "General lattice theory," Akademie-Verlag, Berlin, 1978.

[16] Spinrad,J., "Two dimensional partial orders," Ph.D. thesis, Princeton U., 1982.

[17] Möhring,R.H., Radermacher,F.J., "Substitution decomposition and connections with combinatorial optimization," Ann. Discrete Math., 19 (1984) 257–356.

[18] Möhring,R.H., "Algorithmic aspects of the substitution decomposition in optimization over relations, set systems and boolean functions," Ann. Operation Research 4 (1985/86) 195–225.

[19] Spinrad,J., "On comparability and permutation graphs," Siam J. Comput, 14(1985), 658–670.

[20] Vitek, M., "Graphs and quasitrivial groupoids," Acta Univ. Carolinae, Math. et Phys. 27 (1986) 3–15.

[21] Knauer, U., "Unretractive and S-Unretractive Joins and Lexicographic Products of Graphs," Journal of Graph Theory, 11 (1987) 429–440.

[22] Knauer, U., Nieporte, M., "Endomorphisms of graphs. I. The monoid of strong endomorphisms," Arch. Math., 52 (1989) 607–614.

[23] Knauer, U., "Endomorphisms of graphs. II. Various unretractive graphs," Arch. Math., 55 (1990) 193–203.

[24] Ehrenfeucht, H.N., Rozenberg, G., "Theory of 2-structures, part 1: Clans, Basic subclasses, and morphisms," Theor. Comp. Sci., 70 (1990) 277–303.

[25] Ehrenfeucht, H.N., Rozenberg, G., "Theory of 2-structures, part 2: Representations through labeled tree families," Theor. Comp. Sci., 70 (1990) 305–342.

[26] Ehrenfeucht, H.N., Rozenberg, G., "Primitivity is hereditary for 2-structures," Theor. Comp. Sci., 70 (1990) 343–358.

[27] Nummert, U., "Strong endomorphisms of generalized lexicographic product of graphs," Proc. of the First Estonian Conference on Graphs and Applications, Tartu-Kääriku, May 12-19, 1991.

[28] Böttcher,M., Knauer,U., "Endomorphism spectra of graphs," Discrete Mathematics 109 (1992) 45–57.

[29] Smirnov,D.M. "Varieties of Algebras," Russian Acad. of Sci. Novosibirsk, 1992.

[30] White,N., "Matroid applications," Cambridge University Press, 1992.

[31] Buldas,A., "Algebraic methods in digital circuit simulation," Master thesis (in estonian), Tallinn Technical University, 1993.

[32] Papadimitriou,C.H., "Computational Complexity," Addison-Wesley, 1994.

[33] Zelinka, B., "Representation of Undirected graphs by anticommutative conservative groupoids," Mathem. Bohemica 119 (1994) 231–237.

[34] Buldas, A. "Comparability graphs and the structure of finite graphs." *Proc. Estonian Acad. Sci. Phys. Math.*, 2/3, 1996, 45, 117–127.

[35] McConnell, R.M., Spinrad, J.P., "Linear-time transitive orientation," Proc. of the Eight Annual ACM-SIAM Symposium on Discrete Algorithms, New Orleans, Louisiana, January 5-7, 1997.

[36] Dahlhaus, E., Gustedt, J., McConnell, R.M., "Efficient and practical modular decomposition," Proc. of the Eight Annual ACM-SIAM Symposium on Discrete Algorithms, New Orleans, Louisiana, January 5-7, 1997.

[37] Leibak, A., "Associative identities in graph algebras," master thesis, Tallinn Technical University, 1997.

[38] Buldas, A. "Congruence lattice of a graph." *Proc. Estonian Acad. Sci. Phys. Math.*, 1997, 46, 3, 155–170.

[39] Buldas, A., "Graphs and lattice varieties," *Proc. Estonian Acad. Sci. Phys. Math.*, 1998, 47, 2, 100–109.

[40] A.Buldas, P.Laud, H.Lipmaa, J.Villemson, "Time-stamping with binary linking schemes," Advances in Cryptology – CRYPTO'98, (LNCS 1462), 486–501, 1998.

[41] A.Buldas, P.Laud, "New linking schemes for digital time-stamping," Proc. ICISC'98, Seoul, Korea, 1998, 3–13.