LATTICES AND INVARIANTS
Ph.D. DISSERTATION

Eszter K. Horváth

Supervisors:
Prof. Dr. Béla Csákány
Doctor of mathematical science
Prof. Dr. Gábor Czédli
Doctor of mathematical science

SZTE Bolyai Institute
UNIVERSITY OF SZEGED
2004.

CHAPTER 1

Introduction

Lattices and groups are important algebraic structures and they are the most important related algebraic structures. They often appear in many branches of algebra, they are clear enough to consider easily, and rich enough to characterize many types of algebraic properties.

In this dissertation lattices play more important role than groups, this is why we put *lattices* in the title.

The reason why we put *invariants* in the title is more complex. Traditionally in mathematics, cf. Wikipedia [Inv1]: " An **invariant** is something that does not change under a set of transformations. The property of being an invariant is **invariance.** For the laymen, let us say an *invariant* is some kind of correspondence between two types of mathematical objects, so that two 'similar' things correspond to one and the same object. Invariants are useful in discriminating complicated objects.

Mathematicians say that a quantity is invariant "under" a transformation; some economists say it is invariant "to" a transformation.

Some examples, ...

- The degree of a polynomial, under linear change of variables
- The dimension of a topological object, under homeomorphism
- The number of fixed points of a dynamical system is invariant under many mathematical operations.
- Euclidean distance is invariant under orthogonal transformations and under translations.
- The cross-ratio is invariant under projective transformations.
- The determinant and trace of a square matrix are invariant under changes of basis.
- The singular values of a matrix are invariant under orthogonal transformations.
- Lebesgue measure is invariant under translations.

• The variance of a probability distribution is invariant under translations of the real line; hence the variance of a random variable is unchanged by the addition of a constant to it."

See also [Inv 2]. Invariants have frequently been in the centre of mathematical investigations. For example "Klein's synthesis of geometry as the study of the properties of a space that are invariant under a given group of transformations, known as the Erlanger Programme (1872), profoundly influenced mathematical development.

...The Erlanger Programme gave a unified approach to geometry which is now the standard accepted view." (Quotation is from [Inv3].) See also [Inv4].

However, beside its strict meaning outlined above, the word 'invariant' has also a more general meaning in universal algebra. We obtain this meaning by replacing transformation, which is a selfmap $A \to A$ of a set A by the notion of algebraic operations. Thus we arrive at the notion of an invariant relation ρ with respect to an operation $f : A^n \to A$. In other words, ρ is one of the invariants of f, cf. e.g. [PK].

The present dissertation uses the word 'invariant' in both meanings. The reader will find invariance groups as well as invariant (preserved) relations, namely: congruences and tolerances.

Lattices and invariants proceed along the whole dissertation, but their ratio is varying chapter by chapter.

In Chapter 2 we start with the invariance groups of threshold functions which are a special kind of Boolean functions.

In Chapter 3 we extend our investigation to functions on a finite set. In order to give entirely new proofs for primality theorems, we make use of the operation-relation duality which is established by the preservation of relations by functions. Here not only invariant relations, but also lattices (i.e. the lattice of clones) come into picture, although they play no essential role in the investigation.

All the other chapters are much more connected with lattices consisting of invariants, which will be congruences (= preserved equivalences) and tolerances (= preserved symmetric and reflexive relations). In Chapter 4 we analyze diagrammatic statements concerning congruences and tolerances. Motivated by these diagrammatic statements, in Chapter 5 we carry out lattice theoretic investigation on the shift of a lattice identity. In Chapter 6 tolerances are in the centre, and some lattice theoretic points of interest appear. Finally, Chapter 7 brings an essential contribution to the 34 year old open problem: which congruence lattice identities can be characterized by Maltsev condition?

CHAPTER 2

Invariance groups of threshold functions

There are many parts of informatics where Boolean functions, i.e.

$$\{0,1\}^n \to \{0,1\}$$

mappings are important. The main questions practice raised are the following:

1) How can we represent a Boolean function in the simplest or in the most economical way?

2) Which Boolean functions can be given as superposition of a given set of Boolean functions?

A *threshold function* is a Boolean function, i.e. a mapping $\{0,1\}^n \to \{0,1\}$, with the following property: There exist real numbers $w_1, ..., w_n$, t such that

$$f(x_1, \ldots, x_n) = 1 \text{ iff } \sum_{i=1}^{n} w_i x_i \geq t,$$

where w_i is called the *weight* of x_i for $i = 1, 2, \ldots, n$, and t is a constant called the *threshold value.*

There is a geometrical interpretation of threshold functions. The set $\{0,1\}^n$ can be considered to span a hypercube in the Euclidean space $\mathbf{R}^n$. A Boolean function is defined by assigning either 0 or 1 to the 2^n vertices of the hypercube $\{0,1\}^n$. In the n-dimensional space $\mathbf{R}^n$ the set of vertices where the value of the function is 1 can be separated by a hyperplane from those vertices where the value is 0. This is why threshold functions are also called linearly separable functions ([Sh]).

Threshold functions are useful to study because they are not only models of neurons for example, but also it is easy and relatively cheap to realize them by electrical network ([Sh], [Mu]).

From algebraic point of view, up to now, the main result is the characterization of threshold functions by fundamental ideals of group rings ([ABGG]). However, new investigations in the direction of constraints and taking minors are very promising ([Pip], [CF]).

Surprisingly enough, the number of the n-variable threshold functions is still not known ([Sh], [Mu]).

In many branches of mathematics, symmetry properties of the investigated objects are useful if discovered. Permutations of variables leaving a given Boolean function $f(x_1, \ldots, x_n)$ invariant form a group, which we call the *invariance group* G of the function. Barbara Wnuk has published in a paper ([Wn]) written in Polish that every permutation group is representable as the invariance group of a Boolean function.

In this chapter we are going to prove that the invariance group of threshold functions is isomorphic to a direct product of symmetric groups.

We can suppose without loss of generality (see [ABGG] and [YI]) that

$$w_1 < w_2 < \ldots < w_n.$$

We use the notation: $(X) = (x_1, \ldots, x_n)$; $W = (w_1, \ldots, w_n)$; $W(X) = \sum_{i=1}^{n} w_i x_i$.

If $\sigma \in S_n$, then let $\sigma(X) = ((x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, and for $P = (p_1, p_2, \ldots, p_n) \in \{0,1\}^n$ let $\sigma(P) = (p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(n)}) \in \{0,1\}^n$.

Consider a partition C on the set $\mathbf{n} = \{1, 2, \ldots, \mathrm{n}\}$. As usual, we shall denote the class of C that contains $i \in \mathbf{n}$ by $\bar{i}$. We call C *convex* if $i < j < k$ and $\bar{i} = \bar{k}$ together imply $\bar{i} = \bar{j}$. For any convex partition C of $\mathbf{n}$, the ordering $<$ of $\mathbf{n}$ induces an ordering of the set of blocks of $\mathbf{n}$ in a natural way: $\bar{i} < \bar{j}$ iff $i < j$.

We say that a permutation $\pi \in S_n$ preserves a subset $\mathbf{n}'$ of $\mathbf{n}$ if for each $i \in \mathbf{n}'$, $\pi(i) \in \mathbf{n}'$ holds. We say that a permutation $\sigma \in S_n$ leaves a Boolean function invariant, if $f(\sigma(P)) = f(P)$ for all $P \in \{0,1\}^n$. Permutations leaving f invariant constitute the *invariance group* of the Boolean function.

THEOREM 2.1 ([Ho1]). *For every n-ary threshold function f there exists a partition C_f of $\mathbf{n}$ such that the invariance group G of f consists exactly of those permutations of S_n which preserve each block of C_f. Conversely, for every partition C of $\mathbf{n}$ there exists a threshold function f_C such that the invariance group G of f_C consists exactly of those permutations of S_n that preserve each block of C.*

Proof. The proof of Theorem 2.1 requires several subsidiary statements. First, consider an arbitrary n-ary threshold function f. Let us define the relation $\sim$ on the set $\mathbf{n}$ as follows: $i \sim j$ iff $i = j$ or the transposition $(i\ j)$ leaves f invariant. Clearly, this relation is reflexive, and symmetric. Moreover, it is transitive because

$$(i\ j)(j\ k)(i\ j) = (i\ k).$$

Hence $\sim$ is an equivalence relation.

Claim 2.1. The partition C_f defined by $\sim$ is convex.

Proof. If it is not so, then there exist $i < j < k$, $i \sim k$, $i \not\sim j$, hence there exists a Boolean vector $(d_1, \ldots, d_n) \in \{0,1\}^n$ such that

$$d + w_i d_j + w_j d_i + w_k d_k < t, \tag{1}$$

$$d + w_i d_i + w_j d_j + w_k d_k \geq t, \tag{2}$$

where $d = \sum_{q \neq i,j,k} c_q d_q$. Now (1) and (2) together with $w_i < w_j$ imply $d_i = 0$ and $d_j = 1$ because $0 < (2) - (1) = (w_j - w_i)(d_j - d_i)$. Since $i \sim k$, from (1) and (2) we infer:

$$d + w_i d_k + w_k = d + w_i d_k + w_j d_i + w_k d_j < t, \tag{3}$$

$$d + w_i d_k + w_j = d + w_i d_k + w_j d_j + w_k d_i \geq t. \tag{4}$$

Now $w_j \geq t - d - w_i d_k > w_k$, a contradiction.
Claim 2.1 is proved.

$\square$

For the reason of convexity, the blocks of $\sim$ can be given this way:

$$\begin{aligned} C_1 &= \{1, \ldots, i_1\}, \\ C_2 &= \{i_1 + 1, \ldots, i_1 + i_2\} \\ &\vdots \\ C_l &= \{i_1 + i_2 + \ldots + i_{l-1} + 1, \ldots, i_1 + \ldots + i_l\}. \end{aligned}$$

Every permutation that is a product of some "permitted" transpositions preserves the blocks of C_f, and belongs to G. We show that if a permutation does not preserve each blocks of C_f defined by $\sim$, then it cannot belong to G.

Claim 2.2. Let $\gamma = (j_1\ j_2 \ldots j_{k-1}\ l j_k \ldots j_m) \in S_n$ be a cycle of length $m+1$ with $j_s \in C_p$, $1 \leq s \leq m$, $l \in C_q$, $p \neq q$. Then $\gamma \notin G$.

Proof. Let us confine our attention to the following:

$$(l\ j_{k-1})(j_1\ j_2 \ldots j_{k-1}\ l\ j_k \ldots j_m) = (j_1\ j_2 \ldots j_m)(l),$$

so

$$(l\ j_{k-1}) = (j_1\ j_2 \ldots j_m)(j_1\ j_2 \ldots j_{k-1} l j_k \ldots j_m)^{-1}.$$

If γ were an element of G, then $(l\ j_{k-1})$ would be also an element of G which contradicts the definition of $\sim$.
Claim 2.2. is proved.

$\square$

Lemma 2.1 ([Ho1]). *If a cycle $\beta \in S_n$ has entries from at least two blocks of C_f, then $\beta \notin G$.*

Proof. Given the convex partition C_f of $(\mathbf{n}; \leq)$, for any cycle β of length k we construct a sequence of cycles of increasing length, called the *downward sequence* of β (the reason of this name is that the new entry of each member of the sequence will always correspond to the smallest weight), as follows: Let p be the greatest entry of β and let q be the greatest entry of β which is not in $\bar{p}$. We cancel some entries of β in such a way that we keep *all* entries in $\bar{p}$, and we keep q, and we delete all the remaining entries of β.

This results in the initial cycle of the downward sequence $\beta^{(r)}$ of length r; $r \geq 2$. We do not need to define members of the downward sequence with superscripts less then r. If we have constructed $\beta^{(i)}$, we obtain the next member $\beta^{(i+1)}$ of the downward sequence by taking back the greatest cancelled (and not yet restored) entry of β to its original place. Thus, the final member of the downward sequence is $\beta^{(k)} = \beta$. Let us denote by $m(i)$ $(i > r)$, the "new" entry of $\beta^{(i)}$. If $i \leq r$, then we do not have to define $m(i)$. As an illustration take the following (let $n = 8$):

$$\begin{aligned} C_1 =& \{1, 2\}, \\ C_2 =& \{3, 4\}, \\ C_3 =& \{5, 6, 7\}, \\ C_4 =& \{8\}, \end{aligned}$$

and

$$\beta = (4\ 5\ 1\ 7\ 3) = (1\ 7\ 3\ 4\ 5).$$

The downward sequence is:

$$\beta^{(3)} = (7\ 4\ 5),$$

$$\beta^{(4)} = (7\ 3\ 4\ 5), \qquad m(4) = 3,$$

$$\beta^{(5)}(= \beta) = (1\ 7\ 3\ 4\ 5), \qquad m(5) = 1.$$

It is obvious from the construction of the downward sequence that the weight corresponding to an arbitrary entry of $\beta^{(i)}$ is greater than the weight corresponding to $m(i+1)$. By Claim 2.2, the initial cycle of the downward sequence (in our example $\beta^{(3)}$) is not in G. Hence there exist $A^{(r)} = (a_1^{(r)}, \ldots, a_n^{(r)})$ and $B^{(r)} = (b_1^{(r)}, \ldots, b_n^{(r)})$ with $A^{(r)}, B^{(r)} \in \{0,1\}^n$ and $f(A^{(r)}) \neq f(B^{(r)})$. We can assume without loss of generality that $f(A^{(r)}) = 0$ and $f(B^{(r)}) = 1$, for otherwise we can work with β^{-1} instead of β.

In order to prove that $\beta \notin G$ it suffices to construct $A^{(i)}$ and $B^{(i)}$ for $i = r+1, r+2, \ldots, k$ such that $f(A^{(i)}) = 0$ and $f(B^{(i)}) = 1$ and $\beta^{(i)}(A^{(i)}) = B^{(i)}$.

It is enough to (and we are able to) show that if for $i \geq r$ there exist $A^{(i)} = (a_1^{(i)}, \ldots, a_n^{(i)})$ and $B^{(i)} = (b_1^{(i)}, \ldots, b_n^{(i)})$ with $A^{(i)}, B^{(i)} \in \{0,1\}^n$ such that $f(A^{(i)}) = 0$ and $f(B^{(i)}) = 1$ and $\beta^{(i)}(A^{(i)}) = B^{(i)}$, then we are able to construct $A^{(i+1)} = (a_1^{(i+1)}, \ldots, a_n^{(i+1)})$ and $B^{(i+1)} = (b_1^{(i+1)}, \ldots, b_n^{(i+1)})$ with $A^{(i+1)}$, $B^{(i+1)} \in \{0,1\}^n$ satisfying $f(A^{(i+1)}) = 0$ and $f(B^{(i+1)}) = 1$ and $\beta^{(i+1)}(A^{(i+1)}) = B^{(i+1)}$. Let us denote by $l(j)$ and $r(j)$ the left and the right neighbour of $m(j)$ in the cycle $\beta^{(j)}$, respectively. (For the sake of clarity: $l(5) = 5$ and $r(5) = 7$. We shall use this notation for the corresponding components of a concrete Boolean vector as well: $a_{l(j)}^{(i)}$, $a_{m(j)}^{(i)}$ and $a_{r(j)}^{(i)}$, e.g.: if $A^{(i)} = (1,0,0,1,0,1,0,1)$, then $a_{l(5)}^{(i)} = 0$, $a_{m(5)}^{(i)} = 1$, $a_{r(5)}^{(i)} = 0$.

We have three possibilities for $A^{(i)}$:

Case 1. $a_{m(i+1)}^{(i)} = a_{r(i+1)}^{(i)}$.

Case 2. $a_{m(i+1)}^{(i)} = 1$, $a_{r(i+1)}^{(i)} = 0$.

Case 3. $a_{m(i+1)}^{(i)} = 0$, $a_{r(i+1)}^{(i)} = 1$.

We show that in the first two cases $A^{(i)}$ is appropriate for $A^{(i+1)}$. In Case 3 the only thing we have to do is to transpose two components of $A^{(i)}$ in order to get a suitable $A^{(i+1)}$.

Case 1. Let $a^{(i)}_{m(i+1)} = a^{(i)}_{r(i+1)} = y$. Put $A^{(i+1)} = A^{(i)}$.

Remember that

$$\beta_{(i)} = (\ldots l(i+1)\ r(i+1)\ldots)$$

and

$$\beta_{(i+1)} = (\ldots l(i+1)\ m(i+1)\ r(i+1)\ldots).$$

Even though $\beta^{(i)}$ does not contain $m(i+1)$, $\beta^{(i+1)}(A^{(i)}) = \beta^{(i)}(A^{(i)})$ holds because $a^{(i)}_{(i+1)} = a^{(i)}_{r(i+1)}$. If $A^{(i+1)} = A^{(i)}$, then $\beta^{(i+1)}(A^{(i+1)}) = \beta^{(i)}(A^{(i)}) = B^{(i)}$. So let us choose $B^{(i+1)} = B^{(i)}$. Thus $f(A^{(i+1)}) = 0$, $f(B^{(i+1)}) = 1$ and $\beta^{(i+1)}(A^{(i+1)}) = B^{(i+1)}$ are satisfied. We present this here in a tabular form as well:

	$x_{l(i+1)}$	$x_{m(i+1)}$	$x_{r(i+1)}$
$A^{(i)}$	y	y	$a^{(i)}_{r(i+1)}$
$B^{(i)}$	$b^{(i)}_{l(i+1)}$	y	y
$A^{(i+1)}$	y	y	$a^{(i)}_{r(i+1)}$
$B^{(i+1)}$	$b^{(i+1)}_{l(i+1)}$	y	y

Case 2. $a^{(i)}_{m(i+1)} = 1$, $a^{(i)}_{r(i+1)} = 0$.

Now, $A^{(i)}$ is appropriate for $A^{(i+1)}$ but that is not the case for $B^{(i)}$ and $B^{(i+1)}$. Let $A^{(i+1)} = A^{(i)}$, and $B^{(i+1)} = \beta^{(i+1)}(A^{(i+1)})$. We can get the Boolean vector $B^{(i+1)}$ from $B^{(i)}$ if we transpose $b^{(i)}_{l(i+1)}$ and $b^{(i)}_{m(i+1)}$, i.e.:

$$b^{(i+1)}_{l(i+1)} = 1, \text{ and } b^{(i+1)}_{m(i+1)} = 0,$$

while

$$b^{(i)}_{l(i+1)} = 0, \text{ and } b^{(i)}_{m(i+1)} = 1;$$

furthermore, all the other components of $B^{(i+1)}$ and $B^{(i)}$ are identical. Since $m(i+1)$ corresponds to the smallest weight in $\beta^{(i+1)}$, we get

$$\sum_{j=1}^{n} w_j b^{(i)}_j \leq \sum_{j=1}^{n} w_j b^{(i+1)}_j,$$

which means that $f(B^{(i+1)}) = 1$. Moreover, $f(A^{(i+1)}) = 0$ and $\beta^{(i+1)}(A^{(i+1)}) = B^{(i+1)}$ are satisfied. We again display this in a tabular form:

	$x_{l(i+1)}$	$x_{m(i+1)}$	$x_{r(i+1)}$
$A^{(i)}$	0	1	$a^{(i)}_{r(i+1]}$
$B^{(i)}$	$a^{(i)}_{l(i+1]}$	1	0
$A^{(i+1)}$	0	1	$a^{(i+1)}_{r(i+1)}$
$B^{(i+1)}$	$b^{[r(i+1)]}_{(i+1)}$	0	1

Case 3. $a^{(i)}_{m(i+1)} = 0$, $a^{(i)}_{r(i+1)} = 1$.
Let us construct $A^{(i+1)}$ from $A^{(i)}$ as follows: Put

$$a^{(i+1)}_{m(i+1)} = 1, \qquad a^{(i+1)}_{r(i+1)} = 0,$$

$$a^{(i+1)}_{j} = a^{(i)}_{j} \quad \text{if} \quad a^{(i+1)}_{j} \neq a^{(i+1)}_{m(i+1)} \quad \text{or} \quad a^{(i+1)}_{j} \neq a^{(i+1)}_{r(i+1)}.$$

(Transpose $a^{(i)}_{m(i+1)}$ and $a^{(i)}_{r(i+1)}$ in the Boolean vector $A^{(i)}$ (and keep all of its other components unchanged) to get $A^{(i+1)}$.) Since $m(i+1)$ corresponds to the smallest weight in $\beta^{(i+1)}$, we get

$$\sum_{j=1}^{n} w_j a^{(i+1)}_{j} \leq \sum_{j=1}^{n} w_j a^{(i)}_{j};$$

hence $f(A^{(i+1)}) = 0$. Let $B^{(i+1)} = \beta^{(i+1)}(A^{(i+1)})$. With this choice $B^{(i+1)} = B^{(i)}$, hence $f(B^{(i+1)}) = 1$. In the tabular form:

	$x_{l(i+1)}$	$x_{m(i+1)}$	$x_{r(i+1)}$
$A^{(i)}$	1	0	$a^{(i)}_{r(i+1)}$
$B^{(i)}$	$b^{(i)}_{l(i+1)}$	0	1
$A^{(i+1)}$	0	1	$a^{(i+1)}_{r(i+1)}$
$B^{(i+1)}$	$b^{(i+1)}_{r(i+1)}$	0	1

Lemma 2.1. is proved.

$\square$

Every permutation that is a product of disjoint cycles each one of which preserves every block of C_f belongs to the invariance group G of f. We have to show that if not all of the factors have this property, then the permutation does not leave the threshold function f invariant.

For any permutation π of X, the *moving set* of π, denoted by $M(\pi)$, consists of all elements x of X satisfying $\pi(x) \neq x$.

Lemma 2.2 ([Ho1]). *Let $\pi \in S_X$ be of the form $\pi = \pi_2\pi_1$, where $\pi_1, \pi_2 \in S_X$, with $M(\pi_1) \cap M(\pi_2) = \emptyset$ and $\pi_1 \notin G$. Then $\pi \notin G$.*

Proof. Suppose that it is not so, i.e. $\pi \in G$. Now $\pi_1 \notin G$ means that there exist $X_0, X_1 \in \{0,1\}^n$ with $f(X_0) \neq f(X_1)$. First we assume that $f(X_0) = 0, f(X_1) = 1$ and $\pi_1(X_0) = X_1$. Let $X_2 = \pi_2(X_1)$, i.e. $X_2 = \pi(X_0)$. Since $\pi \in G$, we infer $f(X_2) = 0$. Let $X_3 = \pi_1(X_2)$. As $M(\pi_1) \cap M(\pi_2) = \emptyset$, we have $\pi_1\pi_2 = \pi_2\pi_1$. Therefore $X_3 = \pi(X_1)$. The assumption $\pi \in G$ implies $f(X_3) = 1$. Looking at the infinite series of Boolean vectors

$$X_0, X_1, \ldots, X_n, \ldots$$

we can establish in the same way that $f(X_i) = 0$ if i is even and $f(X_i) = 1$ if i is odd. On the other hand,

$$W(X) = S(X)^{[1]} + S(X)^{[2]} + S(X)^{[3]},$$

where

$$S(X)^{[1]} = \sum_{x_j \in M(\pi_1)} w_j x_j,$$

$$S(X)^{[2]} = \sum_{x_j \in M(\pi_2)} w_j x_j,$$

$$S(X)^{[3]} = \sum_{x_j \notin M(\pi)} w_j x_j.$$

With this notation: $S(X_0)^{[1]} < S(X_1)^{[1]}$, $S(X_0)^{[2]} = S(X_1)^{[2]}$, $S(X_0)^{[3]} = S(X_1)^{[3]}$. For the series of $S(X_i)^{[1]}$:

$$(5) \qquad S(X_0)^{[1]} < S(X_1)^{[1]} = S(X_2)^{[1]} < S(X_3)^{[1]} = S(X_4)^{[1]} < \ldots.$$

Indeed, applying π_2 changes only $S(X_i)^{[2]}$; moreover, $f(X_{2k}) = 0$ and $f(X_{2k+1}) = 1$ imply $W(X_{2k}) < W(X_{2k+1})$, hence $S(X_{2k})^{[1]} < S(X_{2k+1})^{[1]}$. On the other hand, if z is the order of π_1, then $S(X_0)^{[1]} = S(X_{2z})^{[1]}$, which contradicts (5).

The case $f(X_0) = 1, f(X_1) = 0$ is quite similar, for X_{i+1} will play the role of X_i.
Lemma 2.2. is proved.

□

Claim 2.3. For $\pi \in S_X$, let $\pi = \gamma_1 \dots \gamma_r$ where the γ_i are disjoint cycles. If there exists a γ_j with $1 \le j \le r$ and $\gamma_j \notin G$, then $\pi \notin G$.

Proof. Since disjoint cycles commute, we can assume that $\gamma \notin G$. Then $\pi = \gamma_1(\gamma_2 \dots \gamma_r) \in G$ follows from Lemma 2.2.
Claim 2.3 is proved.

□

Now we are in the position to prove the first part of Theorem 2.1. Suppose π is a permutation that preserves each block of C_f. Decompose π to a product of disjoint cycles: $\pi = \gamma_1 \dots \gamma_r$. Then all the γ_i $(1 \le i \le r)$ preserve each block of C_f. For a fixed i $(1 \le i \le r)$, γ_i is of the form $(k_1, k_2, \dots, k_s)$. Clearly, $k_1 \sim k_2 \sim \dots \sim k_s$, whence all the transpositions $(k_1\ k_2)$, $(k_1\ k_3), \dots, (k_1\ k_s)$ preserve f. Therefore so does $\gamma_i = (k_1\ k_2\ \dots k_s) = (k_1\ k_2)(k_1\ k_3) \dots (k_1\ k_s)$, implying $\pi \in G$.

Now suppose that π fails to preserve the blocks of C_f. Then so does at least one of the γ_i $(1 \le i \le r)$, and $\pi \notin G$ comes from Claim 2.3.

In order to prove the converse statement, i.e., the second part of Theorem 2.1, we show first that for any n there exist an n-ary threshold function which is *rigid* in the sense that its invariance group has only one element (the identity permutation).

Suppose n is odd. With $n = 2k + 1$, consider the following weights:

w_1	w_2	$\dots$	w_k	w_{k+1}	w_{k+2}	$\dots$	w_{2k}	w_{2k+1}
$-k$	$-k+1$	$\dots$	-1	0	1	$\dots$	$k-1$	k

(6)

Let $t = 0$. We prove that for any transposition τ of form $(x_j x_{j-1})$ where $2 \le j \le n$ there exists a Boolean vector $U = (u_1, \dots, u_n) \in \{0,1\}^n$ such that $f(U) = 1$ and $f(\tau(U)) = 0$. For a fixed j let $u_j = 1$, $u_{n+1-j} = 1$, $u_i = 0$ if $i \ne j$, $i \ne n+1-j$. It is obvious that $f(U) = 1$; however, $f(\tau(U)) = 0$. Hence C_f is the trivial partition. By the first part of Theorem 1.1, f is rigid.

Now let n be even. With $n = 2k$, consider the following weights:

w_1	w_2	$\dots$	w_{k-1}	w_k	w_{k+1}	w_{k+2}	$\dots$	w_{2k-1}	w_{2k}
$-k$	$-k+1$	$\dots$	-2	-1	1	2	$\dots$	$k-1$	k

(7)

Let $t = 0$. The method is almost the same as before, i.e. consider the following $U = (u_1, \ldots, u_n)$: If $j \neq k+1$ then let $u_j = 1$, $u_{n+1-j} = 1$, $u_i = 0$ if $i \neq j, -j$. If $j = k+1$ then let $u_{k+1} = 1$ and $u_i = 0$ if $i \neq k+1$. If $\tau = (x_j x_{j-1})$, where $2 \leq j \leq n$, then $f(U) = 1$ while $f(\tau(U)) = 0$.

Now, we construct a threshold function g_C for an arbitrary partition C of an arbitrary ordered set X of variables. Denote now by $\sim^*$ the equivalence relation on X defined by C. First, suppose that C is convex. Let $i_1, \ldots, i_l$ denote the number of elements of the blocks of C, respectively. Consider the rigid function f of l variables that is defined by (6) or (7), depending on the parity of l. Take the weight w_1 i_1 times, the weight w_2 i_2 times and so on in order to define a threshold function g of $n = i_1 + i_2 + \ldots + i_l$ variables. Variables of g with the same weight are permutable. However, transpositions σ of form $(x_j x_{j-1})$, where $2 \leq j \leq n$ and $j \not\sim^* j-1$, are "forbidden" for g because if we consider the corresponding U and construct a Boolean vector V of dimension n from U by rewriting it in the following way: instead of u_m $(m = 1, \ldots, l)$, write 0 i_m times, whenever $u_m = 0$; and write 1 (once) then 0 $i_m - 1$ times otherwise; then we shall get a Boolean vector V of dimension n, for which $g(V) = 1$ while $g(\sigma(V)) = 0$. If C is not convex, the only thing we have to do is to reindex the variables in order to get a convex partition. After constructing a threshold function for the rearranged variables with the procedure described above, put the original indexes back and the desired threshold function is ready.
Theorem 2.1 is proved.

□

Corollary 2.1 ([Ho1]). *The invariance group of any threshold function is isomorphic to a direct product of symmetric groups.*

Proof. Let the blocks of C_f be the following (see the first part of Theorem 2.1):

$$\begin{aligned}
C_1 &= \{1, \ldots, i_1\}, \\
C_2 &= \{i_1 + 1, \ldots, i_1 + i_2\} \\
&\vdots \\
C_l &= \{i_1 + i_2 + \ldots + i_{l-1} + 1, \ldots, i_1 + \ldots + i_l\}
\end{aligned}$$

If π preserves C_f, then $\pi = \pi_1 \pi_2 \ldots \pi_l$ where $M(\pi_i) \subseteq C_i$. So the map

$$\pi_1 \pi_2 \ldots \pi_l \rightarrow (\pi_1, \pi_2, \ldots, \pi_l)$$

is clearly an isomorphism.
Corollary 2.1 is proved.

□

The invariance group G_B of an arbitrary Boolean function is not necessarily of the form

$$G \cong S_{i_1} \times \ldots \times S_{i_l}. \tag{8}$$

For example, let h be the following: $h(x_1, \ldots, x_n) = 1$ iff there exists i such that $x_i = 1$, $x_{i\oplus 1} = 1$, $x_j = 0$ if $j \neq i, i+1$ where $\oplus$ means addition *mod* n. The invariance group of h contains the cycle $(1\ 2 \ldots,\ n)$ and its powers but it does not contain transposition at all. If φ were an isomorphism into a direct product of symmetric groups, then the order of $\varphi(1\ 2 \ldots,\ n)$ is also n, but such direct products contain permutation of order two, which should be the image of some transposition under φ, a contradiction.

However, there exist Boolean functions with invariance groups of the form (8) which are not threshold functions. Probably the simplest example:

$$f(x_1, x_2, x_3) = x_1 x_2 \overline{x_3} \vee x_1 \overline{x_2} x_3.$$

Permutable variables of a threshold function do not necessarily mean equal weights. Here is an example: $h(x) = x_1 x_2 x_4 \vee x_3 x_4$. This is a threshold function with the following weights, and threshold value:

w_1	w_2	w_3	w_4	t
1	2	3	4	7

The transposition $(x_1 x_2)$ is "permitted", but the others are not.

But the weights can always be chosen to be identical for variables belonging to the same equivalence class. If the j-th class

$$C_j = \{i_1 + i_2 + \ldots + i_{j-1} + 1, \ldots, i_1 + \ldots + i_j\},$$

then let

$$w_{[j]} = \frac{w_{i_1+i_2+\ldots+i_{j-1}+1} + \ldots + w_{i_1+\ldots+i_j}}{i_j}.$$

Replace

$$w_{i_1+i_2+\ldots+i_{j-1}+1}, \ldots, w_{i_1+\ldots+i_j}$$

by $w_{[j]}$. Since

$$x_{i_1+i_2+\ldots+i_{j-1}+1}, \ldots, x_{i_1+\ldots+i_j}$$

are from the same equivalence class, for fixed

$$x_1, \ldots, x_{i_1+\ldots i_{j-1}}$$

and

$$x_{i_1+\ldots i_j+1}, \ldots x_{i_1+\ldots i_l},$$

the fact that $W(X)$ exceeds t (or not) depends only on the number r of 1-s among the coordinates

$$x_{i_1+i_2+\ldots+i_{j-1}+1}, \ldots, x_{i_1+\ldots+i_j};$$

moreover, $W(X)$ has a maximum (minimum) if we put all our 1-s to places with the greatest (smallest) weights possible. Obviously

$$\frac{w_{i_1+\ldots i_{r-1}+1} + \ldots + w_{i_1+\ldots i_{j-1}+1+r}}{r} \leq w_{[j]};$$

moreover,

$$w_{[j]} \leq \frac{w_{i_1+\ldots i_j-r} + \ldots + w_{i_1+\ldots i_j}}{r}.$$

Hence

$$w_{i_1+\ldots i_{r-1}+1} + \ldots + w_{i_1+\ldots i_{j-1}+1+r} \leq rw_{[j]} \leq w_{i_1+\ldots i_j-r} + \ldots + w_{i_1+\ldots i_j}.$$

Consequently, after replacing $w_{i_1+i_2+\ldots+i_{j-1}+1}, \ldots, w_{i_1+\ldots+i_j}$ by $w_{[j]}$, we still have the same threshold function.

There are many natural areas for algebraists to investigate concerning threshold functions.

1) It would be interesting and useful to survey, which clones of the Post diagram are generated by threshold functions (or more generally, which threshold functions preserve a given relation, and which threshold functions do not.)([Cz1], [Sz]).

2) Boolean functions are very closely related to lattices ([Cz]); we expect, that many interesting lattice theoretic results can be obtained by investigating threshold functions, since many partially ordered sets can be discovered while dealing with some practical questions about threshold functions. (In the literature I could only read about the lattice of threshold functions of at most 5 variables [Mu]). Lattice theoretic results might take us closer to the number of threshold functions.

3) What can be said about the behaviour of cellular automata where the local rule is a threshold function ([Ka], [Wo])?

CHAPTER 3

Proving primality by the operation-relation duality

In this chapter a method is presented for proving primality and functional completeness theorems. This method makes use of the operation–relation duality, or in other words, the invariant relations of an algebra. By a theorem of Sierpiński we have to investigate relations generated by the two-element subsets of A^k only. We show how the method applies for proving Słupecki's classical theorem by generating diagonal relations from each pair of k-tuples.

An algebra $\mathbf{A} = (A, F)$, with a finite support A, is called *primal* if all possible operations on A are term operations of $\mathbf{A}$. Establishing primality is often facilitated by theorems asserting that if F contains operations with some properties, then $\mathbf{A}$ is primal. A natural way to prove such theorems is to construct all operations on A as compositions of those in F. Another way is provided by the operation–relation duality exhibited by Bodnarčuk, Kalužnin, Kotov, Romov ([BKKR]), and Geiger ([Gei]). First, we outline their theory in a few sentences.

Let A be a set and B a subset of A^k. We say that an operation f *preserves* a relation $R \subseteq A^k$ if R is a subuniverse of the algebra $(A, f)^k$. We say that F preserves $R \subseteq A^k$, or in other words R is invariant with respect to F if every $f \in F$ preserves R ([Cs2]). The set of all relations preserved by F is called the set of *invariant relations* of $\mathbf{A} = (A, F)$. A set of operations on a fixed base set is called a *clone* if it contains all projections and is closed under superposition. A non-empty set of relations is called a *closed class of relations,* or in other words a *relational clone* if it is closed under direct products, projections onto arbitrary sets of its variables and diagonalizations.

It is well known (cf. [Cs2]) that preservation establishes a Galois connection between the set of operations and the set of relations on A. On one side, the Galois-closed subsets of the set of all operations are exactly the clones of operations. On the other side, the relational clones are exactly the Galois closed subsets of the set of all relations on A. More precisely, if F is a set of operations, then

$$Inv(F) := \{\rho : \rho \text{ is a relation on } A \text{ that is preserved by all } f \in F\}$$

is a relational clone on A. If R is a set of relations, then

$$Pol(R) := \{f : f \text{ is an operation on } A \text{ that preserves all } \rho \in R\}$$

is a clone on A. Moreover, $F \to Inv(F)$ is a dual lattice isomorphism from the complete (in fact, algebraic and dually algebraic) lattice of all operation clones on A to the lattice of all relational clones on A. The inverse dual lattice isomorphism is given by $R \to Pol(R)$. To summarize, operation clones and relational clones mutually determine each other.

If we apply this result only for the clone of all operations, we conclude that (A, F) is primal iff F preserves exactly the relations on A constituting the least closed class of relations; this is also a consequence of another more general fact on quasiprimal algebras due to P. H. Krauss ([Kr1], [Kr2]). More and detailed information concerning this topic can be found in [I], [PK], [Sz], [We1]. Related ideas were used, e. g., in [BP].

First, we need some definitions. We consider a k-ary relation as a set of unary functions r: $\mathbf{k} \to A$, $\mathbf{k} = \{1, 2, \ldots, k\}$. We say that a k-ary relation D is *diagonal,* if there exists an equivalence relation ρ_D on $\mathbf{k}$ such that

$$D = \{r\colon \mathbf{k} \to A \mid r(u) = r(v) \text{ if } u\rho_D v,\ u, v \in \mathbf{k}\}.$$

All the diagonal relations on A form the minimal closed class of relations on A. Notice that a diagonal relation and the corresponding equivalence relation mutually define each other, so we may use the denotation D_ρ for the diagonal relation determined by an equivalence relation ρ on $\mathbf{k}$. Moreover, to each $r \in A^k$, we assign an equivalence relation ρ_r on the set $\mathbf{k}$ as follows:

$$u\rho_r v \qquad \text{iff} \qquad r(u) = r(v).$$

Evidently, for any diagonal relation D, we have $\rho_D = \bigcap_{r\in D} \rho_r$. Now let $R \subseteq A^k$. By $[R]$ we mean the underlying set of the subalgebra of $\mathbf{A}^k$ generated by R.

The following statement comes straight from definitions.

Proposition 3.1 (Bodnarčuk–Kalužnin–Kotov–Romov [BKKR], Geiger [Gei], Krauss [Kr1],[Kr2]). *A finite algebra* $\mathbf{A} = (A, F)$ *is primal, iff every relation preserved by all operations in* F *is diagonal.*

The following Lemma 3.1 is a reformulation of the well known fact that the clone O_A of all operations defined on a finite set A can be generated by binary operations (Sierpiński [Si]).

Lemma 3.1 ([Ho2]). *Given an algebra* $\mathbf{A} = (A, F)$*, the following two conditions are equivalent:*

(i) For each $R \subseteq A^k$, the relation $[R]$ is diagonal.

(ii) For each $x, y \in A^k$, the relation $[x, y]$ is diagonal.

Proof. By virtue of Sierpiński's result and Proposition 3.1 it suffices to show that (ii) implies that $[F]$, the clone generated by F, contains all binary operations. Let $g : A^2 \to A$ be a binary operation, and let $(x_1, y_1), (x_2, y_2), \ldots (x_k, y_k)$ be an enumeration of A^2. Here $k = |A|^2$ and$(x_i, y_i) \neq (x_j, y_j)$ for $1 \leq i < j \leq k$. Take $x = (x_1, \ldots, x_k)$ and $y = (y_1, \ldots, y_k)$, and let $R_2 = \{x, y\} \subseteq A^k$. Then $\rho_{[x,y]} = \rho_x \cap \rho_y = \rho_\omega$, the smallest equivalence on $\mathbf{k}$. This and (ii) yield $[x, y] = A^k$. Take $z = (g(x_1, y_1), \ldots, g(x_k, y_k)) \in A^k$. Since $z = [x, y]$, there is a binary term h, i.e. a binary $h \in [F]$, such that $z = h(x, y)$. This means $g(x_i, y_i) = z_i = h(x_i, y_i)$ for $i = 1, \ldots, k$, whence $g = h \in [F]$.
Lemma 3.1. is proved.

□

For equivalences μ and ρ on $\mathbf{k}$ if $\mu \subseteq \rho$ then $D_\rho \subseteq D_\mu$. Hence the smallest diagonal relation containing $x, y \in A^k$ is D_η where $\eta = \rho_x \cap \rho_y$. (The particular case when $\rho = \omega$ has already occured in the above proof.) Since $[x, y] \subseteq D_\eta$, $[x, y] = D_\eta$ is clearly equivalent to the condition

$$\rho \supseteq \eta \ \to D_\rho \subseteq [x, y].$$

This allows us to extract the following statement from the previous ones, (ii) of which avoids the use of the notion of diagonal relation.

Lemma 3.1′ ([Ho2]). *The following three conditions are equivalent:*

(i) The algebra $\mathbf{A} = (A, F)$ is primal.

(ii) For each $x, y, z \in A^k$, we have $z \in [x, y]$ whenever

$$((\forall u, v \in \mathbf{k}\ )(x(u) = x(v) \wedge y(u) = y(v) \to z(u) = z(v))).$$

(iii) For each $k \geq 1$ $x, y \in A^k$, and for any equivalence ρ on $\mathbf{k}$ if $\rho \supseteq \rho_x \cap \rho_y$, then $D_\rho \subseteq [x, y]$.

By Lemma 3.1 the problem of proving a primality theorem simplifies to the investigation of some suitably chosen matrices. We demonstrate our method on the Słupecki Criterion in detail. We cannot avoid using the Yablonski Lemma.

Lemma 3.2 (Yablonski [JL]). *Let $f = f(x_1, \ldots, x_n)$ be an at least binary operation on A depending on x_1 and x_2 such that the range of f contains at least* *three elements. Then there exist $a, b, a_2, \ldots, a_n, b_2, \ldots b_n \in A$ such that the elements $c_1 = f(a, a_2, \ldots a_n)$, $c_2 = f(b, a_2, \ldots, a_n)$, and $c_3 = f(a, b_2, \ldots, b_n)$ are pairwise different.*

We call an operation *essential,* if it is surjective and at least binary.

THEOREM 3.1 (Słupecki [Sl]). *Let A be a finite set with $|A| > 2$. If F contains an essential operation f and all the unary operations, then the algebra $\mathbf{A} = (A, F)$ is primal.*

Proof. We shall show that (iii) of Lemma 3.1' holds. This will be done via induction on the number t of the blocks of ρ. However, first we summarize some early observations for later reference.

(a) If $\rho_1 \subseteq \rho_2$ then $D_{\rho_2} \subseteq D_{\rho_1}$;

(b) For any $z \in A^k$, $D_{\rho_z} = [z]$.

(c) The inclusion $\rho \supseteq \rho_z$ implies $D_\rho \subseteq [z]$.

(d) If $x, y \in A^k$ such that, for all $i, j \in \mathbf{k}$, $x(i) = x(j)$ implies $y(i) = y(j)$, then $y \in [x]$.

Here (a) is obvious by definition, (b) follows easily by using unary functions, and (c) is evident by (a) and (b). Finally, the premise of (d) means $\rho_x \subseteq \rho_y$, so $y \in [y] = D_{\rho_y} \subseteq D_{\rho_x} = [x]$ follows by (b) and (a).

Now, if $t = 1$, then $\rho \supseteq \rho_x$ implies $D_\rho \subseteq [x] \subseteq [x, y]$ by (c). Hence the first step of the induction is trivial.

The case $t = 2$ ramifies.

The first subcase is when ρ and $\rho_x \cap \rho_y$ have a common block C. To simplify the notations (i.e., to avoid double subscripts) we may assume that $C = \{1, 2, ..., s\}$. (The general case, $C = \{i_1, i_2, \ldots, i_s\}$, would be similar.) So ρ has two blocks: C and $\{s+1, \ldots, k\}$. If $\rho \supseteq \rho_x$ then $D_\rho \subseteq [x] \subseteq [x, y]$ by (c) and there is nothing to prove. Hence we assume that $\rho \not\supseteq \rho_x$ and, similarly, $\rho \not\supseteq \rho_y$. Hence there are $u, v \in \mathbf{k}$ with $(u, v) \in \rho_x$ and $(u, v) \notin \rho$. Since ρ has only two blocks, $u = 1$ and $v > s$ can be assumed. Similarly, there is a $w > s$ with $(1, w) \in \rho_y$. Since $C = \{1, 2, ..., s\}$ is also a block of $\rho_x \cap \rho_y$, v is necessarily distinct from w. Hence, without loss of generality, we may assume that the ρ_x -block resp. ρ_y-block of 1 is $\{1, \ldots, s, s+1, \ldots, s+l\}$ resp. $\{1, \ldots, s, s+l+1, \ldots, s+l+m\}$ where $l, m \geq 1$.

Now choose elements $a, b, a_2, \dots, a_n, b_2, \dots, b_n \in A$ according to the Yablonski Lemma. Here n is the arity of f, and $c_1 = f(a, a_2, \dots, a_n)$, $c_2 = f(b, a_2, \dots, a_n)$ and $c_3 = f(a, b_2, \dots, b_n)$ are three distinct elements of A. Let $c_4 = f(b, b_2, \dots, b_n)$.

If $c_4 \neq c_1$ then consider the $(n \times k)$ size matrix

$$\begin{array}{cccccccccccc}
a & \dots & a & a & \dots & a & b & \dots & b & b & \dots & b \\
a_2 & \dots & a_2 & b_2 & \dots & b_2 & a_2 & \dots & a_2 & b_2 & \dots & b_2 \\
\vdots & & & & & & & & & & & \\
a_n & \dots & a_n & b_n & \dots & b_n & a_n & \dots & a_n & b_n & \dots & b_n
\end{array}$$

where there are $s+l$ a-s and $k-(s+l)$ b-s in the first row, $s+m$ a_i-s and $k-(s+m)$ b_i-s in the others $(2 \leq i \leq n)$, and this defines the set of rows. Now (d) yields that the first row of this matrix is in $[x]$ while the rest of its rows are in [y]. So all the rows belong to $[x, y]$. Applying f to these rows componentwise, we obtain that

$$z = (c_1, \dots, c_1, c_3, \dots c_3, c_2 \dots c_2, c_4, \dots, c_4) \in [x, y].$$

Since $c_1 \neq c_4$, $\rho_z \subseteq \rho$. Hence, because of (a) and (b), we conclude that

$$D_\rho \subseteq \ D\rho_z = [z] \subseteq [x, y],$$

indeed.

If $c_1 = c_4$ then we consider another $(n \times k)$ matrix:

$$\begin{array}{cccccccccccc}
a & \dots & a & a & \dots & a & b & \dots & b & b & \dots & b \\
b_2 & \dots & b_2 & a_2 & \dots & a_2 & b_2 & \dots & b_2 & a_2 & \dots & a_2 \\
\vdots & & & & & & & & & & & \\
b_n & \dots & b_n & a_n & \dots & a_n & b_n & \dots & b_n & a_n & \dots & a_n
\end{array}$$

where the first row is the same as before. Now, with the same argument, we arrive at

$$z' = (c_3, \dots, c_3, c_1, \dots, c_1, c_4, \dots, c_4, c_2, \dots, c_2) \in [x, y].$$

Since $\rho_{z'} \subseteq \rho$ again, $D_\rho \subseteq [x, y]$ follows the same way as before.

The second subcase is when the blocks of ρ are unions of j_1 resp. j_2 blocks of $\rho_x \cap \rho_y$. We handle this situation via induction on $j = \min\{j_1, j_2\}$. Notice that $j = 1$ is just the previous subcase.

To perform the induction step, assume that $j > 1$. Let

$$\{C_1, C_2, \dots, C_j, C_{j+1}, \dots, C_s\}$$

be the set of $(\rho_x \cap \rho_y)$-blocks such that $C = C_1 \cup \ldots \cup C_j$ and $\overline{C} = C_{j+1} \cup \ldots \cup C_s$ are the two blocks of ρ. We define two new equivalences ρ' and ρ'' that correspond to the respective partitions

$$\{C_1 \cup \ldots \cup C_{j-1},\ C_j \cup C_{j+1} \cup C_{j+2} \cup \ldots \cup C_s\}$$

and

$$\{C_2 \cup \ldots \cup C_j,\ C_1 \cup C_{j+1} \cup C_{j+2} \cup \ldots \cup C_s\}.$$

This makes sense, for $2 \leq j$.

By the induction hypothesis on j, $D_{\rho'} \subseteq [x, y]$ and $D_{\rho''} \subseteq [x, y]$. Since ρ' has only two blocks and $|A| \geq 2$ (in fact $|A| \geq 3$), there exists an $x' \in A^k$ such that $\rho' = \rho_{x'}$. Similarly, there exists an $y' \in A^k$ with and $\rho'' = \rho_{y'}$. Using (b) we obtain

$$[x'] = D_{\rho_{x'}} = D_{\rho'} \subseteq [x, y],$$

and

$$[y'] = D_{\rho_{y'}} = D_{\rho''} \subseteq [x, y],$$

whence $[x', y'] \subseteq [x, y]$.

Now ρ has only two blocks, $\rho \supseteq \rho' \cap \rho''$, $C_{j+1} \cup \ldots \cup C_s$ is a common block of ρ and

$$\rho_{x'} \cap \rho_{y'} = \rho' \cap \rho''.$$

Therefore the previously settled case (i.e. our first subcase) gives $D_\rho \subseteq [x', y']$. Combining the previous displayed formulas, we conclude $D_\rho \subseteq [x, y]$, as requested.

Now we handle the case $3 \leq t \leq |A|$. For simplicity, to avoid complicated subscripts, we assume without loss of generality that 1, 2 and 3 are pairwise incongruent modulo ρ. As in a previous stage of our proof, we will use the elements $a, b, a_2, \ldots, a_n, b_2, \ldots, b_n, c_1, c_2, c_3$ supplied by the Yablonski Lemma. Choose additional elements $c_4, \ldots, c_k \in A$ such that, for $1 \leq i < j \leq k$, $c_i = c_j$ iff $(i, j) \in \rho$. This is possible, for ρ has t blocks and $t \leq |A|$. Notice that for $z = (c_1, c_2, \ldots, c_k)$ we have

$$\rho = \rho_z.$$

The surjectivity of f allows us to find appropriate elements $d_{i,j}$, $1 \leq i \leq n$ and $4 \leq j \leq k$, such that $c_j = f(d_{1j}, \ldots, d_{nj})$ for $4 \leq j \leq k$. Moreover, we assume that the new elements, the d_{ij}, are different from any previous arguments of f only if this is necessary; this further condition on the d_{ij} will be specified later. Now consider the matrix

$$\begin{array}{cccccc} a & b & a & d_{14} & \dots & d_{1k} \\ a_2 & a_2 & b_2 & d_{24} & \dots & d_{2k} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_n & a_n & b_n & d_{n4} & \dots & d_{n,k}, \end{array}$$

the rows of which belong to A^k. If we apply f to the rows of this matrix, then we obtain $z = (c_1, \dots, c_k)$. So, to conclude $z \in [x, y]$, it suffices to show that each row of this matrix is in $[x, y]$.

Now the extra condition on the d_{ij}-s we promised reads as follows: for any $1 \leq i \leq j \leq k$ if $c_i = c_j$ (or equivalently, if $(i, j) \in \rho$) then the i-th and the j-th columns of the matrix coincide. Now let $u = (u_1, u_2, \dots, u_k)$ be an arbitrary row of the matrix. The condition above gives $\rho \subseteq \rho_u$. Since ρ_u collapses at least two of 1, 2 and 3, we have $\rho \subset \rho_u$, and therefore ρ_u has less blocks then ρ, i.e. less than t blocks. By the induction hypothesis and (b) we have $u \in [u] = D_{\rho_u} \subseteq [x, y]$. Hence all rows of the matrix and z belong to $[x, y]$. Hence, making use of (b) and $\rho = \rho_z$, we conclude $D_\rho = D_{\rho_z} = [z] \subseteq [x, y]$. This settles the induction step to $3 \leq t \leq |A|$.

Now let $t > |A|$, and take an arbitraty $z \in D_\rho$. Since $\rho_z \supseteq \rho$ by definitions and $\rho \supseteq \rho_x \cap \rho_y$ by the assumption, $\rho_z \supseteq \rho_x \cap \rho_y$. Since z has at most $|A|$ components, ρ_z has at most $|A|$ blocks. Now the induction hypothesis yields $D_{\rho_z} \subseteq [x, y]$. This and (b) imply $z \in [z] = D_{\rho_z} \subseteq [x, y]$. Thus $D_\rho \subseteq [x, y]$.
Theorem 3.2. is proved.

□

There is an improvement of the Słupecki Criterion by Yablonskii ([JL]): if we omit the injective unary operations from F, then (A, F) is still primal. Even though every one of the previous steps needs some reconsideration, this case can also be completed by the method facilitated by Proposition 3.1 and Lemma 3.1.

An algebra $\mathbf{A} = (A, F)$ is called *functionally complete* if all possible operations on the base set A are polynomials of $\mathbf{A}$. Proving functional completeness for (A, F) is the same as proving primality for the algebra $(A, F \cup F_0)$ where F_0 is the set of all constant operations on A. The above type matrices can be analyzed easily not only in the case of the Słupecki Criterion, but also in cases of other primality and functional completeness results. We proved e.g. the functional completeness of the ternary discriminator ([Sz]), the dual discriminator (for $|A| \geq 3$) ([FP]), the n-ary ($n \geq 3$) near-projections ([Cs1]) as well as the primality theorem of Foster ([F]) this way.

CHAPTER 4

Diagrammatic schemes

4.1. From triangular schemes to Maltsev conditions, a short overview

Motivated by Gumm's Shifting Lemma ([Gu1]), which asserts that congruence modular varieties satisfy a nice rectangular congruence scheme, Chajda ([ChH1], Subdivision 4.2) investigated a triangular scheme, which is a consequence of congruence distributivity. Congruence distributive varieties satisfy this scheme not only for arbitrary three congruences, but also for one tolerance and two congruences; i.e., the analogue of Gumm's Shifting Principle is valid.

The investigations went on in different directions. First, while the triangular scheme is not known to characterize congruence distributivity, an appropriate generalization called trapezoid scheme does ([CCH2], Subdivision 4.3). Secondly, the underlying reason for congruence schemes is that certain lattice indentities are equivalent with appropriate Horn sentences, called the shift of the lattice identity; however, not every lattice identity has a shift ([CCH1], Chapter 5). The third and surely the most important direction that grew out from the topic is the question if it is possible to put tolerances (reflexive, symmetric, compatible binary relations) in place of all three congruences. The answer is yes ([CzH2], Subdivision 6.1). As a special case, we obtain that in a congruence modular variety,

$$\Gamma \cap \Phi^* \subseteq (\Gamma \cap \Phi)^*$$

holds for any two tolerances R and S. As Radeleczki and Kearnes pointed out, this can easily be turned into a much more useful property, the so-called Tolerance Intersection Property, TIP for short, of congruence modular varieties:

$$\Gamma^* \cap \Phi^* = (\Gamma \cap \Phi)^*.$$

TIP has some applications. It is known that **Tol L**, the lattice of tolerances of a lattice **L**, has several nice properties discovered by Bandelt ([B]). Using TIP, these properties (some of them in a weaker form) can be extended to congruence distributive or congruence modular varieties, or varieties with a majority term ([CHR], Subdivision 6.2). For example, if an algebra **A** has a majority term, then **Tol L** is 0-modular, i.e. $\mathbf{Tol\,A} \setminus \{0\}$ contains no pentagon; the proof now is even simpler than Bandelt's original one for lattices. Another application of TIP is about Maltsev conditions. Using TIP we could prove that if $p \le q$ is a lattice identity strong enough to imply modularity, then $p \le q$ has a Maltsev condition ([CzH3], Chapter 7). This Maltsev condition is simply the conjunction of Day's condition and the Wille–Pixley's characterization of $p_3 \subseteq q$. Here p_3 is the $\{\wedge, \circ\}$ term which we obtain from p by replacing joins by three-fold relation product throughout. In case $p \le q$ has a previously known Maltsev condition, the Maltsev conditon extracted form $p_3 \subseteq q$ is not as good as the known one, because it contains terms with too many variables. Much better Maltsev condition would come from $p_2 \subseteq q$ instead of $p_3 \subseteq q$; the latest development is that this is possible ([CHL], Chapter 7).

4.2. Triangular schemes for congruence distributivity

The story started with the book of H. Peter Gumm entitled "Geometrical methods in congruence modular algebras". In this book he introduced the so called *Shifting Lemma,* and *Shifting Principle.*

An algebra **A** is said to satisfy the *Shifting Lemma* (in other words *Rectangular Lemma*) if for any $\alpha, \beta, \gamma \in \mathbf{Con\,A}$ if $\alpha \cap \beta \subseteq \gamma$, $(x, u), (y, v) \in \alpha$, $(x, y), (u, v) \in \beta$ and $(u, v) \in \gamma$, then $(x, y) \in \gamma$, cf. [Gu1]. Pictorially, the Rectangular Lemma is the condition given by Figure 1.

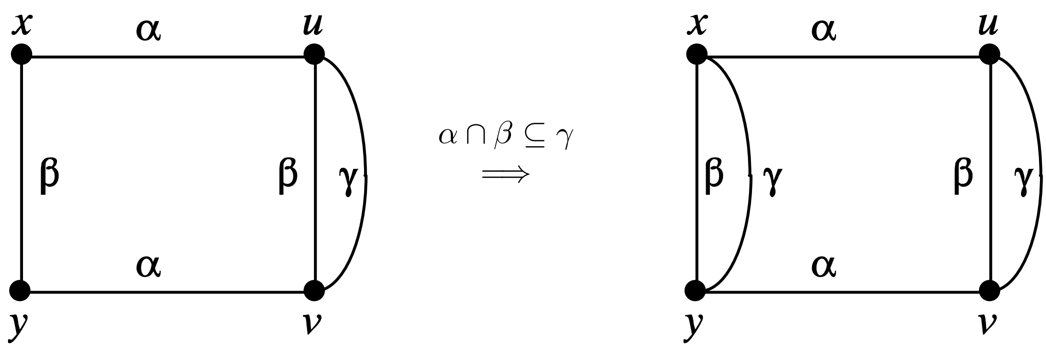


Figure 1

The corresponding condition called *Shifting* (or *Rectangular*) *Principle* (cf. [Gu1]), is defined similarly, the only difference is that α should be replaced by Φ, which stands for an arbitrary *tolerance* (i.e. compatible, reflexive and symmetric binary relation) of $\mathbf{A}$. Gumm shows that for congruence modular algebras the Shifting Lemma holds (the converse of this implication is not true). Moreover, for whole varieties, rather than a single algebra, both Shifting Lemma and Shifting Principle are equivalent to modularity. These innocuous looking diagrammatic schemes lead to a simple geometric development of commutator theory for arbitrary congruences, as one can follow through Gumm's previously mentioned book.

We report here how the story continues for congruence distributivity. Following Gumm's style of [Gu1; Corollary 4.6], schemes for congruences will be called *lemmas* although they are just conditions, and we keep the word *principle* for schemes where tolerances also occur. The schemes defined by triangles (and in the following subdivision trapezes) are in the centre of interest now.

Definition 4.1. An algebra $\mathbf{A} = (A, F)$ satisfies the *Triangular Lemma* if for any $x, y, z \in \mathbf{A}$ and every $\alpha, \beta, \gamma \in \mathbf{Con\,A}$ with $\alpha \cap \beta \subseteq \gamma$ the following implication holds:

$$\text{if } \langle x, y\rangle \in \gamma,\ \langle x, z\rangle \in \alpha, \langle z, y\rangle \in \beta \text{ then } \langle y, z\rangle \in \gamma.$$

The Triangular Lemma can be visualized as shown in Figure 2.

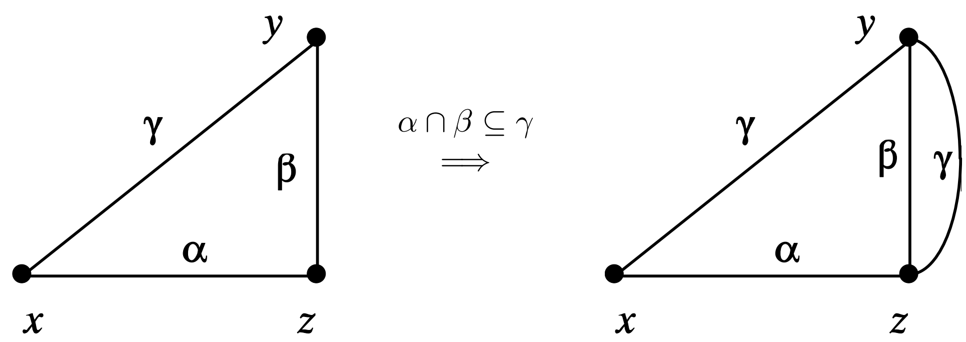


Figure 2

We quote here Chajda's theorems (Theorem 4.1, Theorem 4.2) without their proofs:

THEOREM 4.1 (Chajda [ChH1]). *Every congruence distributive algebra satisfies the Triangular Lemma.*

For $\mathbf{A}$ congruence permutable the converse assertion also holds, cf. Corollary 4.2 later.

Now let us introduce the following concept:

Definition 4.2. Given $n \in \mathbf{N}$ and an algebra $\mathbf{A} = (A, F)$, we say that $\mathbf{A}$ satisfies the *Weak Triangular Principle* for n if for any $x, y, z \in \mathbf{A}$ and every $\alpha, \beta, \gamma \in \mathbf{Con\,A}$ with $\alpha \cap \beta \subseteq \gamma$ and $\Lambda_n = \gamma \circ \alpha \circ \gamma \circ \ldots$ (n factors) the following implication holds:

$$\text{if } \langle x, y\rangle \in \alpha,\ \langle z, y\rangle \in \beta,\ \langle x, y\rangle \in \Lambda_n \text{ then } \langle z, y\rangle \in \gamma.$$

If $\mathbf{A}$ satisfies the Weak Triangular principle for all $n \in \mathbf{N}$, then we simply say that $\mathbf{A}$ satisfies the Weak Triangular Principle.

The Weak Triangular Principle can be visualized as shown in Figure 3.

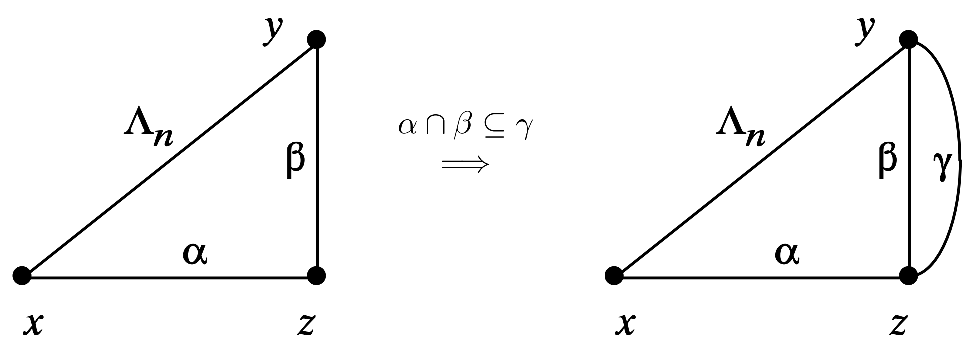


Figure 3

THEOREM 4.2 (Chajda [ChH1]). *An algebra* $\mathbf{A}$ *satisfies the Weak Triangular Principle if and only if* $\mathbf{Con\,A}$ *is distributive.*

The distributivity of $\mathbf{Con\,A}$ is (by Theorem 4.2) equivalent to the implication depicted in Figure 4.

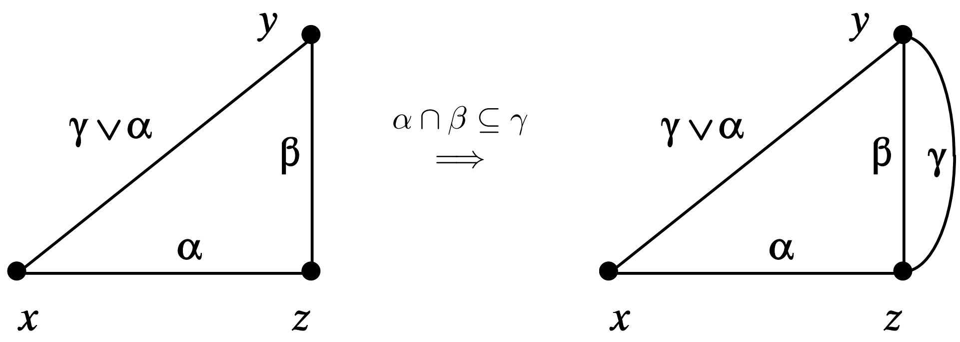


Figure 4

In the case of k-permutable algebra $\mathbf{A}$ we need not require the satisfaction of the Weak Triangular Principle for each $n \in \mathbf{N}$, but Theorem 4.2 yields almost immediately the following:

Corollary 4.1 ([ChH1]). *Let* $\mathbf{A}$ *be a* k*- permutable algebra. Then* **Con A** *is distributive if and only if* $\mathbf{A}$ *satisfies the Weak Triangular Principle for* $n = k - 1$*.*

When $k = 2$, Corollary 4.1 yields the following assertion.

Corollary 4.2 ([ChH1]). *Let* $\mathbf{A}$ *be a congruence permutable algebra. Then* $\mathbf{A}$ *is congruence distributive if and only if* $\mathbf{A}$ *satisfies the Triangular Lemma.*

Remark 4.1. Ivan Chajda in ([ChH1]) gave an example of algebra $\mathbf{A}$ satisfying the Triangular Scheme, but not the Weak Triangular Principle, i.e. whose congruence lattice is not distributive.

Under the name *Shifting Principle* Gumm ([Gu1]) considers a condition in which not only congruences but tolerances also occur. Now we introduce the "congruence distributive counterpart" of this condition.

Definition 4.3. An algebra $\mathbf{A} = (A, F)$ satisfies the *Triangular Principle* if for each tolerance Φ and congruences β, γ the implication depicted in Figure 5 holds.

THEOREM 4.3 ([ChH1]). *In congruence distributive varieties (i. e. in the algebras of such varieties) the Triangular Principle holds.*

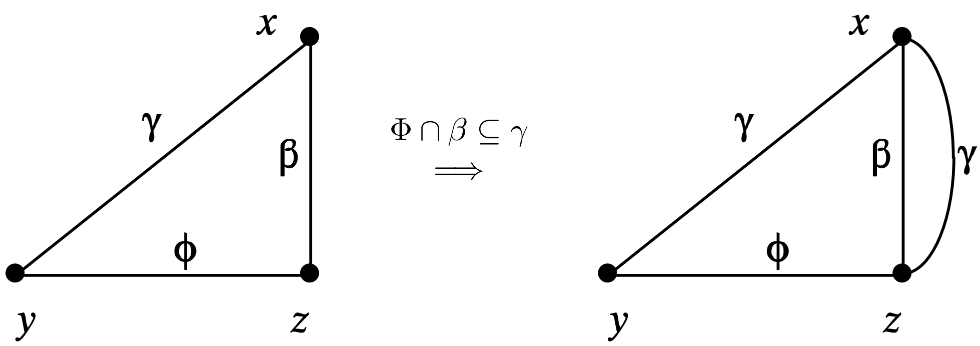


Figure 5

Proof. Let $\mathcal{V}$ be a congruence distributive variety. Then we have Jónsson terms $t_0(x, y, z) \ldots t_n(x, y, z)$ such that

$$t_0(x, y, z) = x, \quad t_n(x, y, z) = z,$$
$$t_i(x, y, x) = x \text{ for all i},$$
$$t_i(x, x, y) = t_{i+1}(x, x, y) \text{ for } i \text{ even, and}$$
$$t_i(x, y, y) = t_{i+1}(x, y, y) \text{ for } i \text{ odd.}$$

Let $\beta, \gamma \in \mathbf{Con\,A}$ and $\Phi \in \mathbf{Tol\,A}$, $\mathbf{A} \in \mathcal{V}$, $a, b, c \in A$ and suppose that $\Phi \cap \beta \subseteq \gamma$, and we have the situation according to Figure 6.

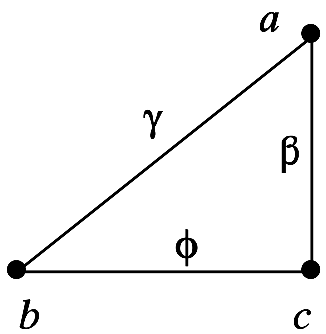


Figure 6

Consider the elements $d_i := t_i(a, b, c)$, $(i = 0, 1, \ldots, n)$. Now $d_0 = a$, $d_n = c$. If i is even, then $d_i = t_i(a, b, c)\gamma t_i(a, a, c) = t_{i+1}(a, a, c)\gamma t_{i+1}(a, b, c) = d_{i+1}$, consequently, for i even, $d_i \gamma d_{i+1}$. If i is odd, then we have to work a little bit more: first of all $d_i = t_i(a, b, c)\Phi t_i(a, c, c)$, and on the other hand, since $d_i = t_i(a, b, c)\beta t_i(a, b, a) = a = t_i(a, a, a)\beta t_i(a, c, c)$, we have $(d_i, t_i(a, c, c)) \in \Phi \cap \beta \subseteq \gamma$. If we put $i+1$ instead of i, then in the same way we have $(d_{i+1}, t_{i+1}(a, c, c)) \in \Phi \cap \beta \subseteq \gamma$.

But in this case $d_i \gamma t_i(a,c,c) = t_{i+1}(a,c,c)\gamma d_{i+1}$, and by the transitivity of γ, we get that $d_i \gamma d_{i+1}$ holds. Hence, for all i, $d_i \; \gamma \; d_{i+1}$, so $(a,c) = (d_0, d_n) \in \gamma$, i. e. the Triangular Principle holds.
Theorem 4.3 is proved.

$\square$

4.3. Trapezoid schemes for congruence distributivity

While the previous schemes seem to be just technical conditions, the Trapezoid Principle is an essential step towards

1) proving that the distributive resp. modular law holds in congruence distributive resp. congruence modular varieties even for tolerance relations;

2) showing that for an arbitrary lattice identity implying modularity (or at least congruence modularity) a Maltsev condition can be given such that the identity holds in congruence lattices of algebras of a variety if and only if the variety satisfies the corresponding Maltsev condition.

Now we introduce a new condition under the name *Trapezoid Lemma* as follows: for any $\alpha, \beta, \gamma \in \mathbf{Con\,A}$ (where $\mathbf{A} = (A, F)$ is an algebra) if $\alpha \cap \beta \subseteq \gamma$, $(x,u), (y,v) \in \alpha$, $(x,y) \in \beta$ and $(u,v) \in \gamma$, then $(x,y) \in \gamma$. The Trapezoid Lemma is depicted in Figure 7.

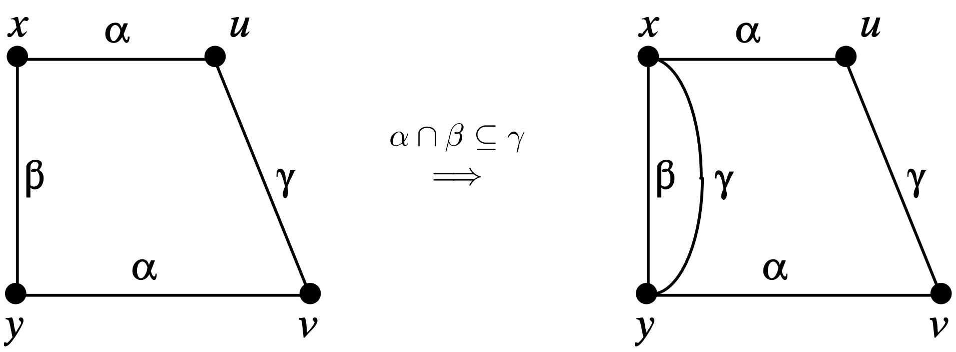


Figure 7

The corresponding condition called *Trapezoid Principle* is defined similarly, the only difference is that α should be replaced by Φ, which stands for an arbitrary *tolerance* (i.e., compatible, reflexive and symmetric binary relation) of $\mathbf{A}$.

Our figures follow the tradition that parallel edges have the same label. Sometimes we do not require the above-defined conditions for all triplets (α, β, γ) just for a single triplet $(\alpha_0, \beta_0, \gamma_0)$; in this case we will say so.

Given a direct product $\mathbf{A} = \mathbf{A_1} \times \mathbf{A_2}$, a congruence $\gamma \in \mathbf{Con\,A}$ is called *directly decomposable* if $\gamma = \gamma_1 \times \gamma_2$ for appropriate $\gamma_1 \in \mathbf{Con\,A_1}$ and $\gamma_2 \in \mathbf{Con\,A_2}$. One of the motivations for introducing the Trapezoid Lemma is revealed by the following statement.

Proposition 4.1 ([CCH1]). *Let $\gamma \in \mathbf{Con}\,(\mathbf{A_1} \times \mathbf{A_2})$ and let π_i denote the kernel of the projection $A_1 \times A_2 \to A_i$, $(x_1, x_2) \mapsto x_i$, $i = 1, 2$. Then the following three conditions are equivalent:*

(a) γ is directly decomposable;

(b) the Trapezoid Lemma holds for (π_1, π_2, γ) and (π_2, π_1, γ);

(c) both the Rectangular Lemma and the Triangular Lemma hold for (π_1, π_2, γ) and (π_2, π_1, γ).

Proof. The equivalence of (a) and (b), in a slightly different formulation, is proved by Fraser and Horn ([FH1 Thm. 1 (1),(3)], cf. also the trapezes in [CG, Figure 31, page 128]). The implication (b) $\Longrightarrow$ (c) is evident; this will also be clear from the forthcoming Proposition 4.2. Proving (c) $\Longrightarrow$ (b) is obvious, too: if $(x, u), (y, v) \in \pi_1$, $(x, y) \in \pi_2$ and $(u, v) \in \gamma$ then with $w := (y_1, u_2) = (v_1, u_2)$ the Triangular Lemma gives $(u, w) \in \gamma$, whence the Rectangular Lemma yields $(x, y) \in \gamma$.
Proposition 4.1 is proved.

□

The following statement presents some connections among our conditions in case of a single algebra; for varieties of algebras we will soon state more.

Proposition 4.2 ([CCH1]). *Let $\mathbf{A}$ be an algebra.*

(1) If $\mathbf{A}$ satisfies the Trapezoid Lemma resp. the Trapezoid Principle, then it satisfies the Rectangular Lemma and the Triangular Lemma resp. the Rectangular Principle and the Triangular Principle. Moreover, each of the three principles implies the corresponding lemma.

(2) If $\mathbf{Con\,A}$ is distributive, then $\mathbf{A}$ satisfies the Trapezoid Lemma (and therefore the other two lemmas as well).

(3) If **A** *satisfies the Trapezoid Principle, then* **Con A** *is distributive.*

(4) If **A** *satisfies the Rectangular Principle, then* **Con A** *is modular (cf. [Gu2], Lemma 4.2).*

(5) If **A** *is congruence permutable, then* **Con A** *is distributive if and only if* **A** *satisfies the Triangular Lemma (cf.* [CzH1], *Cor. 2).*

Proof. (1) is trivial. (2) comes easily from the fact that a lattice is distributive iff it satisfies the Horn sentence

$$\alpha \wedge \beta \leq \gamma \Longrightarrow \beta \wedge (\alpha \vee \gamma) \leq \gamma, \tag{$*$}$$

which we prove in the next chapter. Hence only (3) needs a proof. Suppose **A** is an algebra satisfying the Trapezoid Principle and $\alpha, \beta, \gamma \in \mathbf{Con\,A}$ with $\alpha \wedge \beta \leq \gamma$. According to $(*)$ it suffices to show $\beta \wedge (\alpha \vee \gamma) \leq \gamma$. Borrowing the idea from the proof of Lemma 4.2 in Gumm ([Gu1]), define tolerances $\Phi_0 = \alpha$ and $\Phi_{n+1} = \Phi_n \circ \gamma \circ \alpha, \ \ n \in \mathbf{N}$. Via induction on n we want to show that $\beta \cap \Phi_n \subseteq \gamma$. For $n = 0$ this is clear. Now suppose $\beta \cap \Phi_n \subseteq \gamma$ and let (x, y) be an arbitrary pair in $\beta \cap \Phi_{n+1}$. Then $(x, y) \in \beta \cap \Phi_{n+1} = \beta \cap (\Phi_n \circ \gamma \circ \alpha) \subseteq \beta \cap (\Phi_n \circ \gamma \circ \Phi_n)$, so there are $u, v \in A$ such that $(x, u), (y, v) \in \Phi_n$, $(x, y) \in \beta$ and $(u, v) \in \gamma$. Hence the induction hypothesis $\beta \cap \Phi_n \subseteq \gamma$ and the Trapezoid Principle gives $(x, y) \in \gamma$. This shows $\beta \cap \Phi_{n+1} \subseteq \gamma$, completing the induction. Finally,

$$\beta \wedge (\alpha \vee \gamma) = \beta \cap \bigcup_{n=0}^{\infty} \Phi_n = \bigcup_{n=0}^{\infty} (\beta \cap \Phi_n) \subseteq \gamma,$$

proving $(*)$ and (3).
Proposition 4.2 is proved.

□

We do not know if the implication in (1), (2), (3) and (4) of Proposition 4.2 can be reversed, but we guess the answer is negative in each case. However, for varieties rather than single algebras much more can be said. Of course, a condition is said to hold in a variety if it holds in all algebras of the variety. Part (a) $\Longleftrightarrow$ (c) of the following theorem was announced by Duda ([Du1]).

THEOREM 4.4 ([CCH1]). *Let $\mathcal{V}$ be a variety of algebras. Then the following five conditions are equivalent.*

(a) $\mathcal{V}$ is congruence distributive;

(b) the Trapezoid Principle holds in $\mathcal{V}$;

(c) the Trapezoid Lemma holds in $\mathcal{V}$;

(d) the Rectangular Lemma and the Triangular Lemma hold in $\mathcal{V}$;

(e) there is a positive integer n and there are quaternary terms $d_0, d_1, \ldots, d_n$ such that the identities

(e1) $d_0(x, y, u, v) = x, \quad d_n(x, y, u, v) = y$,

(e2) $d_i(x, y, x, y) = d_{i+1}(x, y, x, y)$ for i even,

(e3) $d_i(x, y, z, z) = d_{i+1}(x, y, z, z)$ for i odd, and

(e4) $d_i(x, x, y, z) = x$ for all i

hold in $\mathcal{V}$.

Remark 4.2. Congruence distributivity and congruence modularity of varieties are characterized by classical Maltsev conditions, namely by the Jónsson terms, cf. [J1], and the Day terms, cf. [Da1]. Since distributivity implies modularity, one would expect that Jónsson terms trivially produce Day terms, but this is not the case. To fulfil this wish (and also to reduce the number of variables) Gumm ([Gu1], [Gu2]) characterizes congruence modularity with another Maltsev condition, the Gumm terms, and he points out that Jónsson terms trivially produce Gumm terms. Now (e) of Theorem 4.4 gives an alternative way to meet the mentioned expectation. Namely, Day terms are quaternary terms satisfying (e1), (e2), (e3) and

(e4') $d_i(x, x, y, y) = x$ for all i,

so our terms in (e) clearly produce (and in fact, constitute) Day terms. Notice that (e) is a byproduct of studying the Trapezoid Lemma; indeed, the proof of Theorem 4.4. is easier with (e) than with Jónsson terms. To reveal the connection between (e) and Jónsson terms we mention that the $p_i(x, y, z) = d_i(x, z, y, z)$ are Jónsson terms provided the d_i are (e) terms.

Remark 4.3. Theorem 4.4 and Proposition 4.2 clearly imply Theorem 4.3, which says that congruence distributive varieties satisfy the Triangular Principle.

Proof of Theorem 4.4. (a) $\Longrightarrow$ (e) follows in the standard way of deriving Maltsev conditions if we consider the the principal congruences $\beta = \mathrm{con}(u, v)$ and $\gamma = \mathrm{con}(x, y)$, and the congruence $\alpha = \mathrm{con}(x, u) \vee \mathrm{con}(y, v)$ of the free algebra $F_{\mathcal{V}}(x, y, u, v)$.

(e) $\Longrightarrow$ (b): Assuming that (e) holds in $\mathcal{V}$, let $\mathbf{A} \in \mathcal{V}$, let Φ be a tolerance relation of $\mathbf{A}$, let $\beta, \gamma \in \mathbf{Con}\,\mathbf{A}$ with $\Phi \cap \beta \subseteq \gamma$, let $x, y, u, v \in \mathbf{A}$ and suppose $(x,u),(y,v) \in \Phi$, $(x,y) \in \beta$ and $(u,v) \in \gamma$. We have to show that $(x,y) \in \gamma$. Consider the elements $h_i = d_i(x,y,u,v)$, $i = 0,\dots,n$, where the terms d_i are provided by (e). Then for i odd, $h_i = d_i(x,y,u,v)\,\gamma\,d_i(x,y,u,u) = d_{i+1}(x,y,u,u)\,\gamma\,d_{i+1}(x,y,u,v) = h_{i+1}$, i.e., $(h_i,h_{i+1}) \in \gamma$ for i odd. For i even we have to work a bit more. We start with $h_i = d_i(x,y,u,v)\,\Phi\,d_i(x,y,x,y)$ and $h_i = d_i(x,y,u,v)\,\beta\,d_i(x,x,u,v) = x = d_i(x,x,x,x)\,\beta\,d_i(x,y,x,y)$. Hence $\big(h_i, d_i(x,y,x,y)\big) \in \Phi \cap \beta \subseteq \gamma$. We obtain $\big(h_{i+1}, d_{i+1}(x,y,x,y)\big) \in \gamma$ similarly. But $d_i(x,y,x,y) = d_{i+1}(x,y,x,y)$, whence the transitivity of γ gives $(h_i,h_{i+1}) \in \gamma$ for i even. Now $(h_i,h_{i+1}) \in \gamma$ for all i, and we conclude $(x,y) = (h_0,h_n) \in \gamma$. I.e., $\mathcal{V}$ satisfies (b).

Observe that (b) $\Longrightarrow$ (c) and (c) $\Longrightarrow$ (d) are evident (or follow from Proposition 4.2).

(d) $\Longrightarrow$ (a): Let $\mathcal{V}$ be a variety satisfying the Rectangular Lemma and the Triangular Lemma. The Rectangular Lemma in itself implies that $\mathcal{V}$ is congruence modular according to Gumm ([Gu1 Cor. 4.6]). Now, by way of contradiction, assume that $\mathcal{V}$ is not congruence distributive. Then there is an algebra $\mathbf{A} \in \mathcal{V}$ and there are congruences $\alpha,\beta,\gamma \in \mathbf{Con\,A}$ generating a five-element nondistributive sublattice $\mathbf{M_3} = \{\alpha,\beta,\gamma,\omega,\iota\}$ of $\mathbf{Con\,A}$ with $\omega < \alpha < \iota$, $\omega < \beta < \iota$ and $\omega < \gamma < \iota$. The theory of modular commutator says, cf. [Gu1, Cor. 8.9] or Freese and McKenzie,[FM Lemma 13.1], that any two elements of this $\mathbf{M_3}$ permute. Since $\beta \not\subseteq \gamma$, we can pick a pair $(y,z) \in \beta \setminus \gamma$. Since $(y,z) \in \beta \subseteq \iota = \gamma \vee \alpha = \gamma \circ \alpha$, there is an element x with $(y,x) \in \gamma$ and $(x,z) \in \alpha$, cf. the left hand side of Figure 2. Now $\alpha \cap \beta = \omega \subseteq \gamma$, so the Triangular Lemma yields $(y,z) \in \gamma$, a contradiction. This proves that $\mathcal{V}$ is congruence distributive.
Theorem 4.4 is proved.

$\square$

Several parts of this subdivision are in close connection with former results of J. Duda. He also introduced the Trapezoid Lemma (under the name Upright Principle) and announced that conditions (a) and (c) of Theorem 4.4 are equivalent, cf. [Du1], and they are equivalent to the conjunction of congruence modularity and the Triangular Lemma, cf. [Du2]. (In virtue of Gumm's classical result, this conjunction is clearly equivalent to (d) of Theorem 4.4.) Duda ([Du1]) also gave a Maltsev condition to characterize the Trapezoid Lemma; his Maltsev condition consists of 6-ary terms.

4.4. Schemes for congruence semidistributivity

The previous subdivisions (and [CR], [CTS]) show that instead of identities in congruence lattices, certain diagrammatic statements are reasonable to consider. The aim of the present subdivision is to show that this phenomenon can be extended to lattice Horn sentences as well. We emphasize that the subsequent statements do not yet have any continuation, so they seem to be much less important (and they are definitely much less elegant, although not trivial) then the previous ones.

Definition 4.4. A lattice $\mathbf{L}$ is $\wedge$-*semidistributive* if it satisfies the following implication for all $\alpha, \beta, \gamma \in \mathbf{L}$:

$$\alpha \wedge \beta = \alpha \wedge \gamma \quad \Rightarrow \quad \alpha \wedge (\beta \vee \gamma) = \alpha \wedge \beta.$$

The $\wedge$-semidistributive law above is often denoted by $SD_\wedge$. More general (in fact, weaker) Horn sentences have been investigated by Geyer ([Gey]) and Czédli ([Cz3]). For $n \geq 2$ put $\mathbf{n} = \{0, 1, \ldots, n-1\}$ and let $P_2(\mathbf{n})$ denote the set $\{S : S \subseteq \mathbf{n} \text{ and } |S| \geq 2\}$.

Definition 4.5. For $\emptyset \neq H \subseteq P_2(\mathbf{n})$ we define the *generalized meet semidistributive law* $SD_\wedge(n, H)$ for lattices as follows: for all $\alpha, \beta_0, \ldots, \beta_{n-1}$

$$\alpha \wedge \beta_0 = \alpha \wedge \beta_1 = \ldots = \alpha \wedge \beta_{n-1} \quad \Rightarrow \quad \alpha \wedge \beta_0 = \alpha \wedge \bigwedge_{I \in H} \bigvee_{i \in I} \beta_i.$$

As a particular case, when $H = \{S : S \subseteq \mathbf{n} \text{ and } |S| = 2\}$, $SD_\wedge(n, H)$ is denoted by $SD_\wedge(n, 2)$. Notice that $SD_\wedge(n, 2)$ is the following lattice Horn sentence:

$$\alpha \wedge \beta_0 = \alpha \wedge \beta_1 = \cdots = \alpha \wedge \beta_{n-1} \quad \Rightarrow \quad \alpha \wedge \bigwedge_{0 \leq i < j < n} (\beta_i \vee \beta_j) = \alpha \wedge \beta_0,$$

which was originally studied by Geyer ([Gey]), and $SD_\wedge(2, 2)$ is the $\wedge$-semidistributivity law defined in Definition 4.4. Czédli ([Cz3]) noticed that $SD_\wedge(n, 2)$ is strictly weakening in n, i. e. $SD_\wedge(n, 2)$ implies $SD_\wedge(n+1, 2)$, but not conversely.

Our goal is to study $SD_\wedge(n, H)$ in congruence lattices of *single* algebras. Although it is usual to consider lattice identities and Horn sentences in congruence lattices of all algebras of a variety, this is not our case. The reason is that, for an arbitrary variety $\mathcal{V}$, if $SD_\wedge(n,H)$ holds in $\{\mathbf{Con\,A} \ : \ \mathbf{A} \in \mathcal{V}\}$ then so does $SD_\wedge$. (This was proved by Czédli ([Cz3]) and an anonymous referee of [Cz3] who pointed out that both Kearnes and Szendrei ([KSz]) and Lipparini ([L1]) contain implicitly the statement that if a lattice Horn sentence λ can be characterized by a weak Maltsev condition and, for each nontrivial module variety $\mathcal{M}$, λ fails in $\mathbf{Con\,M}$ for some $\mathbf{M} \in \mathcal{M}$, then for an arbitrary variety $\mathcal{V}$ if λ holds in $\{\mathbf{Con\,A} \ : \ \mathbf{A} \in \mathcal{V}\}$, then so does $SD_\wedge$, cf. the last paragraph in [Cz3].) In particular, for any variety $\mathcal{V}$ and any $n \geq 2$, $SD_\wedge(n,2)$ and $SD_\wedge$ are equivalent for the class $\{\mathbf{Con\,A} \ : \ \mathbf{A} \in \mathcal{V}\}$. Hence $SD_\wedge(n,2)$ does not deserve a separate study for *varieties*.

First, we consider congruence permutable algebras.

THEOREM 4.5 ([ChH2]). *Let* $\mathbf{A}$ *be a congruence permutable algebra. Then* $\mathbf{Con\,A}$ *satisfies* $SD_\wedge(n,2)$ *if and only if* $\mathbf{A}$ *satisfies the scheme depicted in Figure 8 for* $\alpha, \beta_0, \ldots, \beta_{n-1} \in \mathbf{Con\,A}$ *and* $x_0, \ldots, x_k, y, z \in A$ *where* $k = \frac{n(n-1)}{2} - 1$ *and* δ *stands for* $\beta_0 \cap \beta_1 \cap \cdots \cap \beta_{n-1}$.

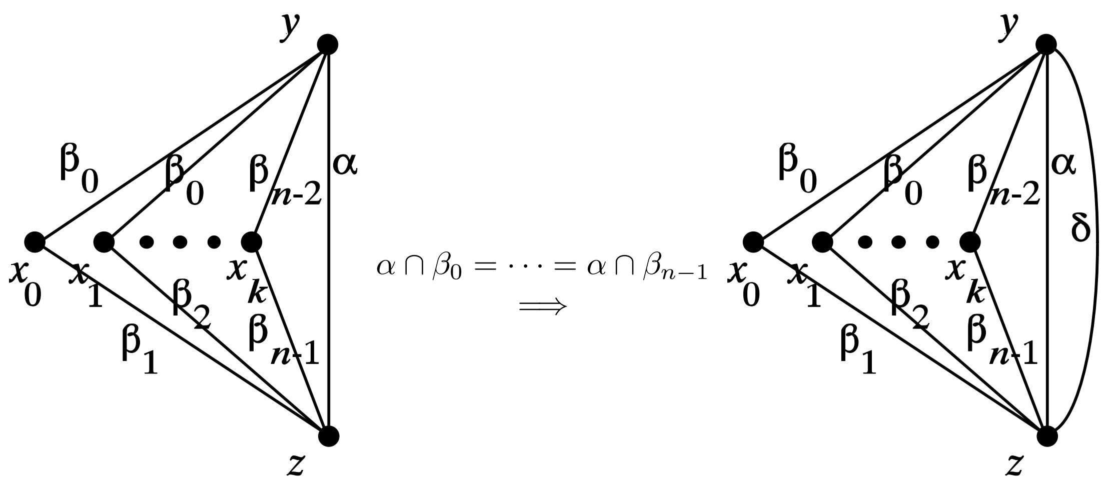


Figure 8

Proof. Suppose $SD_\wedge(n,2)$ holds. Using the premise of $SD_\wedge(n,2)$ we obtain

$$\alpha \cap \beta_0 = (\alpha \cap \beta_0) \cap \cdots \cap (\alpha \cap \beta_{n-1}) = \alpha \cap (\beta_0 \cap \cdots \cap \beta_{n-1}) \subseteq \delta,$$

whence Con A satisfies the Horn sentence

$$\alpha \cap \beta_0 = \cdots = \alpha \cap \beta_{n-1} \quad \Rightarrow \quad \alpha \cap \bigcap_{0 \leq i < j < n} (\beta_i \vee \beta_j) \leq \delta.$$

This implies the scheme, for the situation on the left hand side in Figure 8 then gives

$$(y,z) \in \alpha \cap \bigcap_{0 \le i < j < n} (\beta_i \circ \beta_j) \subseteq \alpha \cap \bigcap_{0 \le i < j < n} (\beta_i \vee \beta_j) \subseteq \delta.$$

To show the converse suppose that the scheme given by Figure 8 holds, $\alpha, \beta_0, \ldots, \beta_{n-1} \in$ **Con A** with $\alpha \cap \beta_0 = \cdots = \alpha \cap \beta_{n-1}$, and suppose that $(y,z) \in \alpha \cap \bigcap_{0 \le i < j < n} (\beta_i \vee \beta_j)$. Since $\beta_i \vee \beta_j = \beta_i \circ \beta_j$ by congruence permutability, there exist $x_0, x_1, \ldots, x_k$ of **A** such that for each j $(1 \le j \le k)$ there exist u, v such that $(z, x_j) \in \beta_u$ and $(x_j, y) \in \beta_v$ (according to the left hand side of Figure 8). Then the scheme applies and we conclude $(y,z) \in \delta$. Since $\delta \subseteq \beta_0$, $(y,z) \in \beta_0$. Hence $(y,z) \in \alpha \cap \beta_0$. This proves the "$\le$" part of $SD_\wedge(n,2)$. The reverse part is simpler and does not need the scheme: $\alpha \supseteq \alpha \cap \beta_0$ and $\beta_i \vee \beta_j \supseteq \beta_i \supseteq \alpha \cap \beta_i = \alpha \cap \beta_0$ clearly give

$$\alpha \cap \bigcap_{0 \le i < j < n} (\beta_i \vee \beta_j) \supseteq \alpha \cap \beta_0,$$

proving the theorem.
Theorem 4.5 is proved.

□

In the particular case when $n = 2$ we trivially conclude the following assertion:

THEOREM 4.6 ([ChH2]). *Let* **A** *be a congruence permutable algebra. Then* **Con A** *is $\wedge$-semidistributive if and only if* **A** *satisfies the scheme in Figure 9 for any $\alpha, \beta, \gamma \in$* **Con A** *and $x, y, z \in$* **A**.

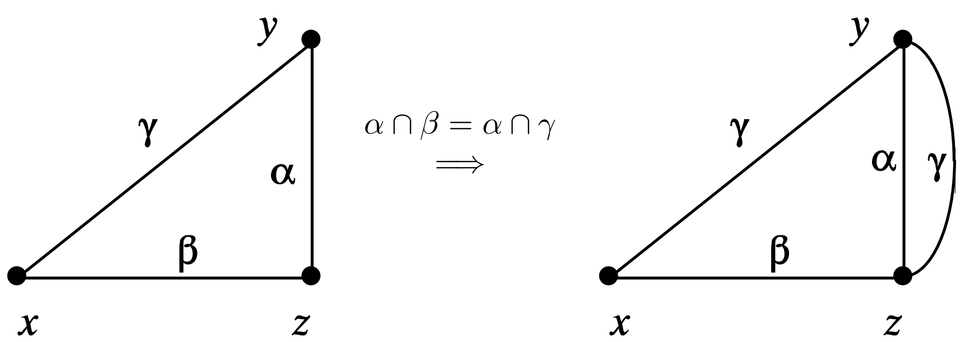


Figure 9

Proof. If **Con A** is $\wedge$-semidistributive, then the premise of the scheme gives $(y, z) \in \ \beta \cap \gamma \subseteq \gamma$ by Theorem 4.5. Conversely, if the scheme holds for **A** then its premise, after interchanging the role of β and γ, implies $(y, z) \in \beta \cap \gamma$, so $SD_\wedge(2, 2)$, which is the usual $\wedge$-semidistributivity, holds in **Con A** according to Theorem 4.5.

Theorem 4.6. is proved.

$\square$

One may observe that this scheme in Theorem 4.6. implies Corollary 4.2 characterizing congruence distributivity in the congruence permutable case. This implies that: *in presence of congruence permutability congruence $\wedge$-semidistributivity is equivalent to congruence distributivity.*

This follows also from another direction. Let **A** be congruence permutable and satisfying $SD_\wedge$. In this case **A** is congruence distributive since otherwise its congruence lattice, being modular due to congruence permutability, contains M_3 but with the choice α, β, γ on Figure 10 we see that $SD_\wedge$ fails.

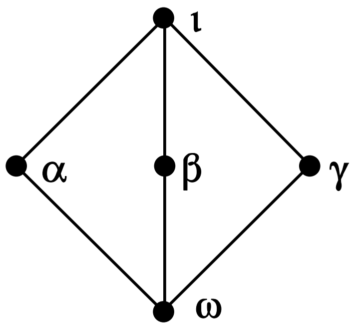


Figure 10

Remark 4.4. For $SD_\wedge(n, H)$, a similar scheme can be derived as in Theorem 4.5.

Without congruence permutability, for the case $SD_\wedge(2, 2) = SD_\wedge$, the following theorem can be stated:

THEOREM 4.7 ([ChH2]). *Let* **A** *be an algebra. The congruence lattice* **Con A** *is $\wedge$-semidistributive if and only if for each n,* **A** *satisfies the scheme in Figure 11 for $\alpha, \beta, \gamma \in$* **Con A** *and $x, y, z \in A$, where $\Lambda_0 = \beta$ and $\Lambda_{m+1} = \Lambda_m \circ \gamma \circ \beta$.*

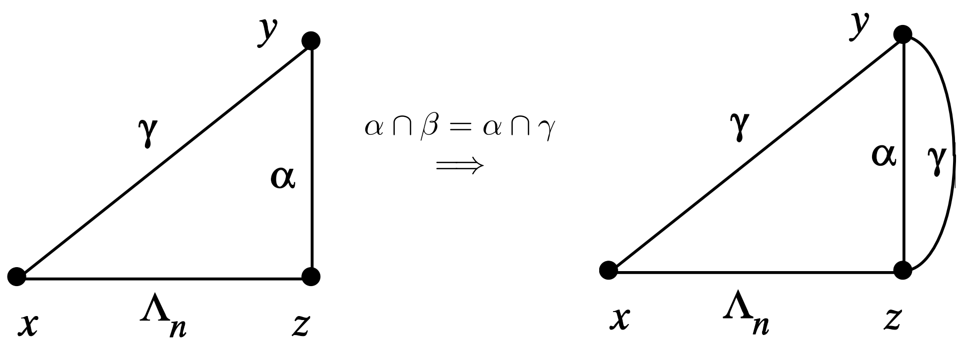


Figure 11

Proof. Suppose that **Con A** is $\wedge$-semidistributive and $\alpha, \beta, \gamma \in$ **Con A** with $\alpha \cap \beta = \alpha \cap \gamma$. Let $x, y, z \in A$ and let $(x, y) \in \gamma$, $(y, z) \in \alpha$ and $(x, z) \in \Lambda_n$. Then

$$(y, z) \in \alpha \cap (\Lambda_n \circ \gamma) \subseteq \alpha \cap (\beta \vee \gamma) = \alpha \cap \beta = \alpha \cap \gamma$$

due to the $\wedge$-semidistributivity. Thus $(y, z) \in \gamma$, proving the validity of the scheme.

Conversely, let **A** satisfy the scheme for each $n \in \alpha N_0$, let $\alpha, \beta, \gamma \in$ **Con A** with $\alpha \cap \beta = \ \alpha \cap \gamma$. Suppose $(z, y) \in \alpha \cap (\beta \vee \gamma)$. Then there exists $n \in \alpha N_0$ such that $(z, y) \in \alpha \cap (\Lambda_n \circ \gamma)$ and hence $(x, y) \in \gamma$ and $(y, z) \in \alpha$ and $(x, z) \in \Lambda_n$ for some $x \in$ **A**. Due to the scheme, we conclude $(x, y) \in \alpha \cap \gamma$, i.e. $\alpha \cap (\beta \vee \gamma) \subseteq \alpha \cap \gamma \subseteq \alpha \cap \beta$. The converse inclusion is trivial, thus **Con A** is $\wedge$-semidistibutive.
Theorem 4.7. is proved.

$\square$

CHAPTER 5

Shifting lattice identities

The motivation for this chapter is the following question: what is the purely lattice theoretic connection between the Shifting Lemma resp. the Triangular Lemma and modularity resp. distributivity?

Let

$$\lambda : \quad p(x_1, \ldots, x_n) \leq q(x_1, \ldots, x_n)$$

be a lattice identity. (Notice that by a lattice identity we always mean an inequality, i.e. we use $\leq$ but never $=$.) If y is a variable, then let $S(\lambda, y)$ denote the Horn sentence

$$q(x_1, \ldots, x_n) \leq y \Longrightarrow p(x_1, \ldots, x_n) \leq y.$$

If $y \notin \{x_1, \ldots, x_n\}$, then λ is clearly equivalent to $S(\lambda, y)$. However, we are interested in the case when $y \in \{x_1, \ldots, x_n\}$, say $y = x_i$ $(1 \leq i \leq n)$. Then $S(\lambda, x_i)$ is a consequence of λ. When $S(\lambda, x_i)$ happens to be equivalent to λ, then $S(\lambda, x_i)$ will be called *a shift of* λ. If $S(\lambda, x_i)$ is equivalent to λ only within a lattice variety $\mathcal{V}$, then we say that $S(\lambda, x_i)$ *is a shift of* λ *in* $\mathcal{V}$.

As it will soon become clear, not every lattice identity has a shift. If an identity λ can be characterized by excluded (partial) sublattices, then it is usually much easier to decide whether λ has a shift, but we also handle identities, n-distributivity and Fano identity, without such characterization.

First consider the distributive law

$$\text{dist:} \quad \beta(\alpha + \gamma) \leq \beta\alpha + \beta\gamma.$$

In this chapter there are some lattice terms with high complexity; hence the lattice operations are denoted by sum and product instead of $\vee$ and $\wedge$. Then $S(\text{dist:}, \gamma)$ is $\beta\alpha + \beta\gamma \leq \gamma \Longrightarrow \beta(\alpha + \gamma) \leq \gamma$, which is clearly equivalent to saying that

$$\alpha\beta \leq \gamma \Longrightarrow \beta(\alpha + \gamma) \leq \gamma \tag{1}$$

is a shift of dist. Indeed, replacing γ with $\alpha\beta + \gamma$, (1) implies the identity $\beta(\alpha + \gamma) \leq \alpha\beta + \gamma$, whence $\beta(\alpha + \gamma) \leq \beta(\alpha\beta + \gamma)$. Using this second identity twice we obtain

$$\beta(\alpha + \gamma) \leq \beta(\alpha\beta + \gamma) \leq \beta\alpha + \beta\gamma,$$

the distributive law.

Although $S(\mathrm{dist}, \gamma)$ and, rather, (1) are not lattice identities, they have two conspicuous advantages over distributivity. Firstly, if we want to test the distributivity of an n-element lattice in the most straightforward way, then we have to evaluate both sides of $\beta(\alpha + \gamma) \le \beta\alpha + \beta\gamma$ for n^3 triplets. But to test $S(\mathrm{dist}, \gamma)$ resp. (1) we have to evaluate $\beta(\alpha+\gamma)$ for those triplets for which $\beta\alpha+\beta\gamma$ resp. $\alpha\beta$ is below γ. Secondly, $S(\mathrm{dist}, \gamma)$ or (1) makes it clear that the Triangular Scheme holds when the congruence lattice is distributive. (In fact, the Triangular Scheme is equivalent to congruence distributivity provided the algebra in question has permutable congruences.)

Practically the same is true for the modular law

$$\mathrm{mod}: \quad \alpha(\beta + \alpha\gamma) \le \alpha\beta + \alpha\gamma.$$

Now $S(\mathrm{mod}, \gamma)$: $\alpha\beta + \alpha\gamma \le \gamma \Longrightarrow \alpha(\beta + \alpha\gamma) \le \gamma$, which is clearly equivalent to

$$\alpha\beta \le \gamma \Longrightarrow \alpha(\beta + \alpha\gamma) \le \gamma. \tag{2}$$

To show that (2) implies modularity it suffices to observe that (2) fails in the pentagon (five element nonmodular lattice) when $\beta \parallel \gamma < \alpha \parallel \beta$. Again, $S(\mathrm{mod}, \gamma)$ and (2) are easier to test from a computational point of view, they evidently imply the Shifting Lemma, and, in fact, the satisfaction of (2) is equivalent to the Shifting Lemma provided the algebra has 3-permutable congruences.

The examples above show the advantage of shifts of lattice identities: they are easier to test and they give rise to congruence diagrammatic-statements which could be quite useful. In the rest of the chapter we consider some concrete lattice identities, and we give their shifts or show that no shift exists.

Following Huhn ([Hu1]) and ([Hu2]), a lattice $\mathbf{L}$ is said to be n-distributive ($n \ge 1$) if the identity

$$\mathrm{dist}_n: \quad \beta \sum_{i=0}^{n} \alpha_i \le \sum_{j=0}^{n} \left(\beta \sum_{i \in \{0,\dots,n\} \setminus \{j\}} \alpha_i \right)$$

holds in $\mathbf{L}$. (Notice that in his earlier papers Huhn assumed modularity in the definition but later he dropped this assumption.) Clearly, dist_1 is the usual distributivity.

THEOREM 5.1 ([CCH2]). *$S(dist_n, \alpha_0)$ is a shift of $dist_n$ in the variety of modular lattices. However, if $n \geq 2$, then $dist_n$ has no shift (in the variety of all lattices).*

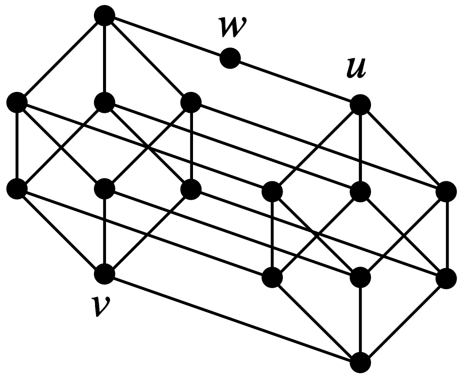


Figure 12

Proof. Let **L** be a modular lattice such that dist_n fails in **L**. Then, by Huhn ([Hu1]) and ([Hu2]), **L** contains an n-diamond (This is the current terminology. Huhn called an equivalent notion an $(n-1)$-diamond.), i.e. there are pairwise distinct elements $u, v, a_0, \ldots, a_{n+1}$ in **L** such that for any n-element subset $H \subseteq \{0, 1, \ldots, n+1\}$ and $k \in \{0, \ldots, n+1\} \setminus H$ we have

$$a_k \sum_{i \in H} a_i = u \quad \text{and} \quad a_k + \sum_{i \in H} a_i = v.$$

Notice that these equations mean that any $n+1$ elements of $\{a_0, \ldots, a_{n+1}\}$ are the atoms of a Boolean sublattice with bottom u and top v. Now the substitution $\alpha_i = a_i$, $i = 0, \ldots, n$, and $\beta = a_{n+1}$ shows that $S(\mathrm{dist}_n, \alpha_0)$ fails in **L**.

Now let $n \geq 2$. We define a lattice **L** such that dist_n fails, but all the "shift candidates" $S(\mathrm{dist}_n, \beta)$, $S(\mathrm{dist}_n, \alpha_0)$, ..., $S(\mathrm{dist}_n, \alpha_n)$ hold in **L**. Take the finite Boolean lattice with $n+2$ atoms, pick an atom v, let u be the complement of v and insert a new element w in the prime interval $[u, 1]$. This way we obtain **L**, which is depicted in Figure 12 when $n = 2$. Letting $\{\alpha_0, \ldots, \alpha_n\}$ be the set of covers of v and $\beta = w$ we see that dist_n fails in **L**. Clearly, $S(\mathrm{dist}_n, \beta)$ holds in any lattice. Now, by way of contradiction, assume that $S(\mathrm{dist}_n, \alpha_0)$ fails for some $\beta, \alpha_0, \ldots, \alpha_n \in$ **L**. Then we have

$$p \not\leq q, \quad q \leq \alpha_0, \quad p \not\leq \alpha_0, \tag{3}$$

$$(\forall i)\ \beta \not\leq \alpha_i, \tag{4}$$

$$(\forall j)\ \alpha_j \not\leq \sum_{i\in\{0,\dots,n\}\setminus\{j\}} \alpha_i, \tag{5}$$

$$w \in \{\beta, \alpha_0, \dots, \alpha_n\}. \tag{6}$$

Indeed, (5) follows from (3), and (6) follows from (3) and the fact that $p \leq q$ in the Boolean lattice $\mathbf{L} \setminus\{w\}$. If $w = \alpha_k$, $0 \leq k \leq n$, then either the interval $[v, 1]$ contains some α_i and $1 = \alpha_k + \alpha_i$ contradicts (5) (this is where $n \geq 2$ is used) or all the α_i belong to $[0, w] = [0, \alpha_k]$, which contradicts (5) again. Hence (6) yields $\beta = w$. In what follows, $=_d$ will refer to distributivity applied for elements of the sublattice $\mathbf{L} \setminus\{w\}$. If $\sum_{i\in\{0,\dots,n\}} \alpha_i \neq 1$ then, for any $H \subseteq \{0, \dots, n\}$, $\beta \sum_{i\in H} \alpha_i = u \sum_{i\in H} \alpha_i$, and using the above-mentioned distributivity clearly gives $p = q$, contradicting (3). Hence $\sum_{i\in\{0,\dots,n\}} \alpha_i = 1$ and $p = \beta = w$. Since

$$q = \sum_{j\in\{0,\dots,n\}} \beta \sum_{i\in\{0,\dots,n\}\setminus\{j\}} \alpha_i \geq$$
$$\sum_{j\in\{0,\dots,n\}} u \sum_{i\in\{0,\dots,n\}\setminus\{j\}} \alpha_i =_d \quad u \sum_{j\in\{0,\dots,n\}} \alpha_j = \quad u$$

and $q \leq p \not\leq q$, we have $q = u$. Then (3) gives $\alpha_0 = u$ and (5) gives a contradiction again, either because $[v, 1]$ contains some α_i and $\alpha_0 + \alpha_i = 1$ or because $[0, \alpha_0]$ contains all the α_i.
Theorem 5.1. is proved.

□

Now, to show once again how a shift leads to a diagrammatic statement, we visualize dist_2. The following statement clearly follows from the preceding part of the chapter. It is worth mentioning that when congruence lattices of all algebras of a given variety are considered then each of dist_n is equivalent to the usual distributivity by Nation ([N]); hence the following statement is totally uninteresting for varieties instead of single algebras.

Corollary 5.1 ([CCH2]). *(A) Let* $\mathbf{A}$ *be an algebra with modular congruence lattice* $\mathbf{Con\,A}$. *If* $\mathbf{Con\,A}$ *is 2-distributive then the diagrammatic statement depicted in Figure 13 holds in* $\mathbf{A}$.

(B) If $\mathbf{A}$ *is congruence permutable, then* $\mathbf{Con\,A}$ *is 2-distributive if and only if the diagrammatic statement depicted in Figure 13 holds in* $\mathbf{A}$.

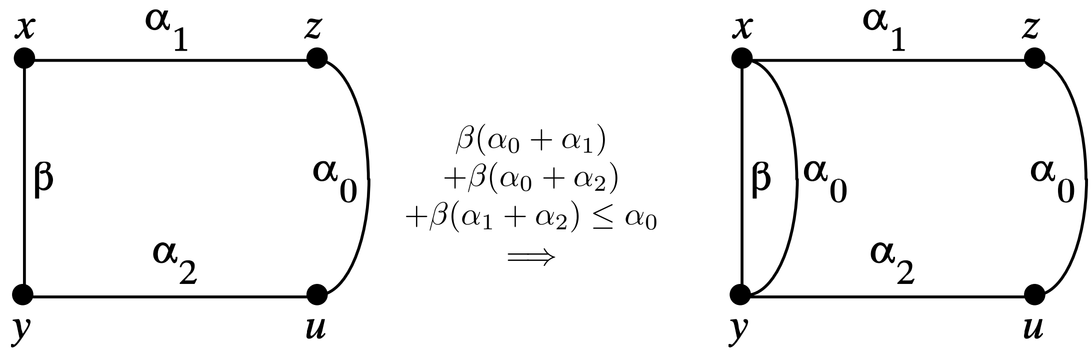


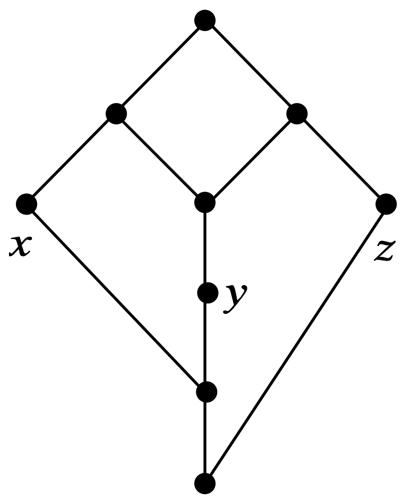
Figure 13

The next group of lattice identities we consider is taken from McKenzie [Mc]. These identities are as follows:

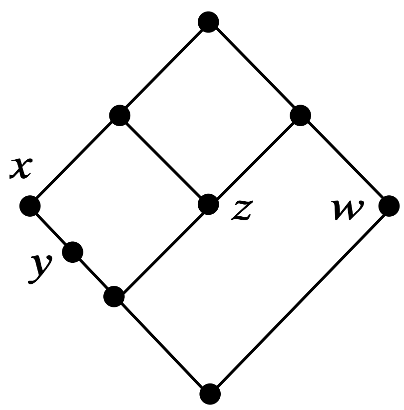
$$\begin{aligned}
\zeta_0:&\quad (x+y(z+xy))(z+xy)\le y+(x+z(x+y))(y+z),\\
\zeta_1:&\quad x(xy+z(w+xyz))\le xy+(z+w)(x+w(x+z)),\\
\zeta_2:&\quad (x+y)(x+z)\le x+(x+y)(x+z)(y+z),\\
\zeta_3:&\quad (x+yz)(z+xy)\le z(x+yz)+x(z+xy),\text{ and}\\
\zeta_4:&\quad y(z+y(x+yz))\le x+(x+y)(z+x(y+z)).
\end{aligned}$$

Notice that ζ_3 is Gedeonová's p-modularity ([Ged1]).

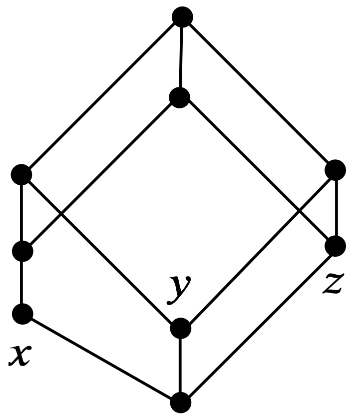
THEOREM 5.2 ([CCH2]). *$S(\zeta_0, y)$, $S(\zeta_1, y)$, $S(\zeta_2, x)$, and $S(\zeta_3, y)$ are shifts of ζ_0, ζ_1, ζ_2 and ζ_3, respectively. On the other hand, ζ_4 has no shift.*



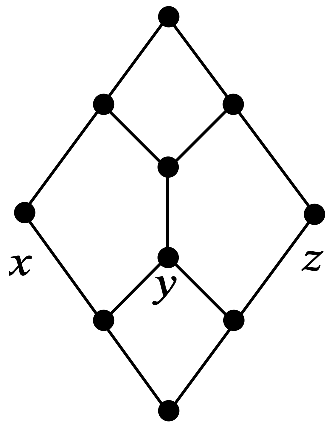
Q_0



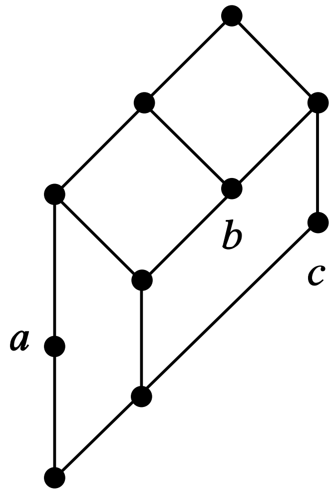
Q_1



Q_2



Q_3



Q_4

Proof. Consider the lattices $Q_0, \ldots, Q_4$ given by their Hasse diagram. For $i = 0, \ldots, 4$ McKenzie ([Mc]) proved that Q_i is a projective splitting lattice with conjugate identity ζ_i. As a consequence, for an arbitrary lattice $\mathbf{L}$, ζ_i holds in $\mathbf{L}$ if and only if Q_i is not (isomorphic to) a sublattice of $\mathbf{L}$; for $i = 3$ this was previously proved by Gedeonová ([Ged1]).

(Since it is not so easy to extract this well-known consequence from [Mc], perhaps a short hint is helpful. By definitions, for any lattice variety $\mathcal{V}$ either ζ_i holds in $\mathcal{V}$ or $Q_i \in \mathcal{V}$. Now suppose that ζ_i fails in a lattice $\mathbf{L}$. Then $Q_i \in \mathbf{HSP}\{\mathbf{L}\} = \mathbf{P_s HSP_u}\{\mathbf{L}\}$. Splitting lattices are subdirectly irreducible, so $Q_i \in \mathbf{HSP_u}\{\mathbf{L}\}$. Since Q_i is projective, $Q_i \in \mathbf{SP_u}\{\mathbf{L}\}$, i.e. Q_i can be embedded into an ultrapower of $\mathbf{L}$. But Q_i is finite, its embeddability can be expressed by a first order formula, so applying Loś' theorem we conclude that Q_i is embeddable into $\mathbf{L}$.)

Now if the shift of ζ_i, $0 \le i \le 3$, (i.e. $S(\zeta_2, x)$ for $i = 2$ and $S(\zeta_i, y)$ for $2 \ne i \le 3$) held, but ζ_i failed in a lattice L then Q_i would be a sublattice of L and the elements $x, y, \ldots$ indicated in the diagram of Q_i would refute the satisfaction of the shift of ζ_i in L.

It follows from definitions (or by substituting $(x, y, z) = (a, b, c)$) that ζ_4 fails in Q_4. So, to prove that $\zeta_4 : p_4 \le q_4$ has no shift, it suffices to show that all the "shift candidates" $S(\zeta_4, x)$, $S(\zeta_4, y)$ and $S(\zeta_4, z)$ hold in Q_4. If $x, y, z \in Q_4$ with $\{x, y, z\} \ne \{a, b, c\}$ then the sublattice $[x, y, z]$ is distinct from Q_4, so it has no sublattice isomorphic to Q_4, hence ζ_4 and therefore the shift candidates hold in $[x, y, z]$. Hence it suffices to test substitutions with $\{x, y, z\} = \{a, b, c\}$; six cases. It turns out that $(x, y, z) = (a, b, c)$ is the only case when $p_4 \not\le q_4$, so it is quite easy to see that all the shift candidates hold in Q_4.
Theorem 5.2 is proved.

$\square$

Theorem 5.2 raises the problem of characterizing splitting lattices whose conjugate identities have shifts.

All the previous lattice identities have known characterizations by excluded (partial) sublattices (at least in the variety of modular lattices) and, except for distributivity, our proofs were based on these characterizations. (Even in the second half of the proof of Theorem 5.1 the construction was motivated by Huhn' characterization for the modular case.) It would be interesting but probably difficult to avoid the use of excluded sublattices. The Fano identity (cf. e.g. Herrmann and Huhn ([HH])):

$$\chi_2 : \quad (x + y)(z + t) \le (x + z)(y + t) + (x + t)(y + z)$$

has no similar known characterization; yet, we have the following statement.

THEOREM 5.3 ([CCH2]). *The Fano identity has no shift — not even in the variety of modular lattices.*

Proof. Suppose that χ_2 has a shift in the variety of modular lattices. Since the role of its variables is symmetric, we can assume that this shift is

$$S(\chi_2, x) : \quad (x + z)(y + t) + (x + t)(y + z) \le x \Longrightarrow (x + y)(z + t) \le x.$$

Let $\mathbf{L}$ be the subspace lattice of the real projective plane. Then $\mathbf{L}$ is a modular lattice with length 3. It contains $0 = 0_L = \emptyset$, the atoms are the projective points

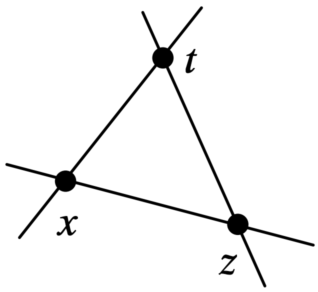


Figure 14

(as singleton subspaces), the coatoms are the projective lines, and the full plane is $1 = 1_L$. It follows from Herrmann and Huhn ([HH]) that χ_2 fails in $\mathbf{L}$. We intend to show that $S(\chi_2, x)$ holds in $\mathbf{L}$ and this will imply our theorem. We will use the modular law in its classical form

$$x \le z \Longrightarrow (\underline{x} + y)\underline{\underline{z}} = x + yz$$

and also in the form of shearing identity

$$x(y+z) =_s x(y(x+z)+z) = x(y(x+z)+z(x+y)).$$

First we show that χ_2 and therefore $S(\chi_2, x)$ hold for $x, y, z, t \in \mathbf{L}$ when $\{x, y, z, t\}$ is not an antichain. By symmetry, it is enough to treat two cases.

Case 1: $x \le y$, then

$$(x+y)(z+t) = y(z+t) =_s y(z(y+t)+t(y+z)) \le z(y+t)+t(y+z) \le$$
$$(\underline{x} + z\underline{\underline{(y+t)}}) + (\underline{x} + t\underline{\underline{(y+z)}}) = (x+z)(y+t)+(x+t)(y+z).$$

Case 2: $x \le z$, then

$$(\underline{x}+y)\underline{\underline{(z+t)}} = x + y(z+t) =_s x + y(z(y+t)+t(y+z)) \le$$
$$z(y+t) + \underline{x} + t\underline{\underline{(y+z)}} = (x+z)(y+t)+(x+t)(y+z).$$

Let $\{x, y, z, t\}$ be an antichain in $\mathbf{L}$. Thus each of x, y, z and t is a point or a line.

If x is a line then we infer $x + z = 1$ from $z \not\le x$ and the premise of $S(\chi_2, x)$ gives $x \ge (x+z)(y+t) = y+t \ge y$, a contradiction. Therefore x is a point. If z is a line then $x + z = 1$ again and we can derive the same contradiction. Hence z is a point and, by z–t symmetry, so is t. Similarly, if y is a line then $x \ge (x+z)(y+t) = x+z \ge z$, therefore y is a point.

We have seen that x, y, z and t are pairwise distinct points. Let us consider the "triangle" xzt, cf. Figure 14. The premise of $S(\chi_2, x)$ says $(x+z)(y+t) \leq x$, which is possible only when $y \leq x + t$ (i.e., y is on the line through x and t). Similarly, $(x+t)(y+z) \leq x$ forces $y \leq x + z$. Hence $y \leq (x+t)(x+z) = x$, a contradiction. Theorem 5.3 is proved.

$\square$

CHAPTER 6

Tolerances and tolerance lattices

6.1. The inequalities mod(tol,tol,tol) and dist(tol,tol,tol) in case of congruence modularity and distributivity

Let dist(x, y, z) resp. mod(x, y, z) denote the distributive law

$$x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z)$$

resp. the modular law

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

For an algebra **A**, the *set* of tolerances and the *lattice* of congruences of **A** will be denoted by **Tol A** and **Con A**, respectively. We say that dist(tol,tol,tol) holds in **A** if $\Gamma \wedge (\Phi \vee \Psi) \subseteq (\Gamma \wedge \Phi) \vee (\Gamma \wedge \Psi)$ is valid for any $\Gamma, \Phi, \Psi \in$ **Tol A**, where the meet resp. the join is the intersection resp. the transitive closure of the union. Denoting the transitive closure by *, $\Phi \vee \Psi = (\Phi \cup \Psi)^* = \Phi^* \vee \Psi^*$ (the second join is from **Con A**) for any tolerances Φ and Ψ *in the present subdivision throughout.* The meaning of mod(tol,tol,tol) is analogous. We should emphasize here that $\Phi \vee \Psi$ is **not** the join in **Tol A**, the lattice of tolerance relations of **A**.

THEOREM 6.1 ([CzH2]). *If $\mathcal{V}$ is a congruence distributive resp. congruence modular variety, then dist(tol,tol,tol) resp. mod(tol,tol,tol) holds in all algebras of $\mathcal{V}$.*

Proof. Suppose $\mathcal{V}$ is congruence distributive. Then we have Jónsson terms, cf. Jónsson ([J1]), i.e. ternary $\mathcal{V}$-terms $t_0, \ldots, t_n$ for some even $n \in \mathbf{N}_0 = \{0, 1, 2, \ldots\}$ such that $\mathcal{V}$ satisfies the identities $t_0(x, y, z) = x$, $t_n(x, y, z) = z$, $t_i(x, x, y) = t_{i+1}(x, x, y)$ for i even, $t_i(x, y, y) = t_{i+1}(x, y, y)$ for i odd, and $t_i(x, y, x) = x$ for all i. Now let $A \in \mathcal{V}$, $\Gamma, \Phi, \Psi \in$ **Tol A** and $(a, b) \in \Gamma \wedge (\Phi \vee \Psi)$. Then there is an even

k, and there are elements $c_0 = a, c_1, \ldots, c_{k-1}, c_k = b$ such that $(c_i, c_{i+1}) \in \Phi$ for i even, $(c_i, c_{i+1}) \in \Psi$ for i odd and $(a, b) = (c_0, c_k) \in \Gamma$. Since

$$t_i(a, u, b) = t_i(t_i(a, v, a), u, t_i(b, v, b)) \;\Gamma\; t_i(t_i(a, v, b), u, t_i(a, v, b)) = t_i(a, v, b),$$

for all i and any $u, v \in \mathbf{A}$ we have

$$(t_i(a, u, b), t_i(a, v, b)) \in \Gamma. \tag{1}$$

Now we define a sequence from a to b as follows:

$$\begin{gathered}
a = t_0(a, c_0, b) = t_1(a, c_0, b) \;\Phi\; t_1(a, c_1, b) \;\Psi\; t_1(a, c_2, b) \;\Phi\; t_1(a, c_3, b) \\
\Psi\; \ldots \Phi\; t_1(a, c_{k-1}, b) \;\Psi\; t_1(a, c_k, b) = t_1(a, b, b) = t_2(a, b, b) = \\
t_2(a, c_k, b) \;\Psi\; t_2(a, c_{k-1}, b) \;\Phi\; t_2(a, c_{k-2}, b) \;\Psi\; \ldots \;\Phi\; t_2(a, c_0, b) = \\
t_2(a, a, b) = t_3(a, a, b) \;\Phi\; t_3(a, c_1, b) \Psi t_3(a, c_2, b) \;\Phi\; \ldots \;\Psi \\
t_3(a, c_k, b) = t_4(a, c_k, b) \;\Psi\; t_4(a, c_{k-1}, b) \;\Phi \quad \ldots \quad \Phi \\
t_{n-1}(a, c_{k-1}, b) \;\Psi\; t_{n-1}(a, c_k, b) = t_{n-1}(a, b, b) = t_n(a, b, b) = b.
\end{gathered}$$

It follows from (1) that any two consecutive members of this series are in

$$(\Gamma \cap \Phi) \cup (\Gamma \cap \Psi) \subseteq (\Gamma \wedge \Phi) \vee (\Gamma \vee \Psi).$$

Thus $(a, b) \in (\Gamma \wedge \Phi) \vee (\Gamma \cap \Psi)$, whence dist(tol,tol,tol) holds in $\mathcal{V}$.

Now let $\mathcal{V}$ be congruence modular. Then we have Day terms, i.e. quaternary $\mathcal{V}$-terms $m_0, m_1, \ldots, m_k$ for some $0 < k \in \mathbf{N}_0$ such that $\mathcal{V}$ satisfies the identities

$$\begin{gathered}
m_0(x, y, u, v) = x, \quad m_k(x, y, u, v) = y \\
m_i(x, y, x, y) = m_{i+1}(x, y, x, y) \text{ for } i \text{ even}, \\
m_i(x, y, z, z) = m_{i+1}(x, y, z, z) \text{ for } i \text{ odd, and} \\
m_i(x, x, y, y) = x \text{ for all } i,
\end{gathered}$$

cf. Day ([Da1]). First we show that, for any $\mathbf{A} \in \mathcal{V}$ and $\Gamma, \Phi, \Psi \in \mathbf{Tol}\,\mathbf{A}$,

$$\Gamma \cap (\Phi \circ (\Gamma \cap \Psi) \circ \Phi) \subseteq (\Gamma \cap \Phi) \vee (\Gamma \cap \Psi). \tag{2}$$

Let $(a, b) \in \Gamma \cap (\Phi \circ (\Gamma \cap \Psi) \circ \Phi)$. Then there are $c, d \in \mathbf{A}$ with $(a, c), (d, b) \in \Phi$, $(c, d) \in \Gamma \cap \Psi$ and, of course, $(a, b) \in \Gamma$. Consider the elements $d_i = m_i(a, b, c, d)$ for

$i = 0, 1, \ldots, k$, $e_i = m_i(a, b, c, c) = m_{i+1}(a, b, c, c)$ for i odd, and $e_i = m_i(a, b, a, b) = m_{i+1}(a, b, a, b)$ for i even. Then $d_0 = a$, $d_k = b$, and $(d_i, e_i), (e_i, d_{i+1}) \in \Gamma \cap \Psi$ for i odd.

For i even we have $(d_i, e_i), (e_i, d_{i+1}) \in \Phi$,

$$d_i = m_i(a, b, c, d) = m_i(m_i(a, b, c, d), m_i(a, b, c, d), a, a)\ \Gamma$$
$$m_i(m_i(a, a, c, c), m_i(b, b, d, d), a, b) = m_i(a, b, a, b) = e_i,$$

i.e. $(d_i, e_i) \in \Gamma \cap \Phi$. Similarly, $(e_i, d_{i+1}) \in \Gamma \cap \Phi$.

Now $(a, b) \in (\Gamma \wedge \Phi) \vee (\Gamma \wedge \Psi)$ follows from transitivity and from the fact that all the (d_i, e_i) and (e_i, d_{i+1}) belong to $(\Gamma \wedge \Phi) \vee (\Gamma \wedge \Psi)$. This shows (2).

Now define $\Phi_0 = \Phi$ and $\Phi_{n+1} = \Phi_n \circ (\Gamma \cap \Psi) \circ \Phi_n$ for $n \geq 1$. Notice that all the Φ_n belong to **Tol A**. We claim that for all $n \in \mathbf{N}_0$,

$$\Gamma \cap \Phi_n \subseteq (\Gamma \cap \Phi) \vee (\Gamma \cap \Psi). \tag{3}$$

This is evident for $n = 0$. Assuming (3) for an arbitrary n and applying (2) we obtain $\Gamma \cap \Phi_{n+1} = \Gamma \cap (\Phi_n \circ (\Gamma \cap \Psi) \circ \Phi_n) \subseteq (\Gamma \cap \Phi_n) \vee (\Gamma \cap \Psi) \subseteq (\Gamma \cap \Phi) \vee (\Gamma \cap \Psi) \vee (\Gamma \cap \Psi) = (\Gamma \cap \Phi) \vee (\Gamma \cap \Psi)$, i.e. (3) holds for $n + 1$. Thus (3) holds for all n and we obtain $\Gamma \wedge (\Phi \vee (\Gamma \wedge \Psi)) = \Gamma \cap \bigcup\{\Phi_n : n \in \mathbf{N}_0\} = \bigcup\{\Gamma \cap \Phi_n : n \in \mathbf{N}_0\} \subseteq (\Gamma \cap \Phi) \vee (\Gamma \cap \Psi)$. Theorem 6.1 is proved.

□

Corollary 6.1 (Gumm [Gu1]). *If $\mathcal{V}$ is a congruence modular variety, then it satisfies Gumm's Shifting Principle, i.e. for any* $\mathbf{A} \in \mathcal{V}$, $\alpha, \gamma \in$ **Con A** *and* $\Phi \in$ **Tol A** *if* $(x, y), (u, v) \in \alpha$, $(x, u), (y, v) \in \Phi$, $(u, v) \in \gamma$ *and* $\alpha \cap \Phi \subseteq \gamma$, *then* $(x, y) \in \gamma$.

Proof. $(x, y) \in \alpha \cap (\Phi \vee (\alpha \wedge \gamma)) \subseteq (\alpha \wedge \Phi) \vee (\alpha \wedge \gamma) \subseteq \gamma \vee \gamma = \gamma$. Corollary 6.1 is proved.

□

Notice that Theorem 6.1 also implies the Triangular Principle and the Trapezoid Principle for congruence distributive varieties, cf. [ChH1] and [CCH2].

Now we give an example. Consider the monounary algebra $\mathbf{B} = (\{0, 1, 2\}, -)$ where $-0 = 0$, $-1 = 2$ and $-2 = 1$. Then α with the associated partition $\{\{0\}, \{1, 2\}\}$ is the only nontrivial congruence of $\mathbf{B}$, so **Con A** is distributive. Notice that

$$\Phi = \{(0, 1), (1, 0), (0, 2), (2, 0), (0, 0), (1, 1), (2, 2)\}$$

is a tolerance and $\alpha \cap \Phi^* \not\subseteq (\alpha \cap \Phi)^*$. Hence the following statement indicates that Theorem 6.1 cannot be extended for single algebras.

Proposition 6.1 ([CzH2]). *If mod(tol,tol,tol) or dist(tol,tol,tol) holds in an algebra* $\mathbf{A}$, *then* $\Gamma \cap \Phi^* \subseteq (\Gamma \cap \Phi)^*$ *for any* $\Gamma, \Phi \in \mathbf{Tol\,A}$.

Proof. Apply mod$(\Gamma, \Phi, 0)$ or dist$(\Gamma, \Phi, 0)$.
Proposition 6.1 is proved.

□

6.2. Tolerance lattices of algebras in congruence modular varieties

The tolerances and the congruences of an algebra $\mathbf{A}$ form algebraic lattices denoted by $\mathbf{Tol\,A} = ($ Tol $A, \wedge, \sqcup)$ and $\mathbf{Con\,A} = ($ Con $A, \wedge, \vee)$, respectively. The congrence lattice $\mathbf{Con\,A}$ of an algebra $\mathbf{A}$ is an algebraic lattice, but (according to the Grätzer–Schmidt theorem, cf. [GS]) it has no further special properties. The same is true for the tolerance lattice $\mathbf{Tol\,A}$ by [CC] (for an alternative proof cf. also Theorem 2 with ρ being the identical map plus checking the construction for reflexivity in Grätzer and Lampe ([GL]). As a contrast to the general case, the tolarence lattice $\mathbf{Tol\,L}$ of an arbitrary lattice $\mathbf{L}$ has many nice properties by [RS] and Bandelt ([B]). Bandelt [B] is also a good source to convince the reader about the importance of tolerances of lattices.

The purpose of the present subdivision is to extend known results on tolerance lattices of lattices to tolerance lattices of more general algebras. Some results will be extended "only" for algebras with a majority term while some others for algebras in a congruence modular variety. Surprisingly enough, the proof of our generalized statement on 0-modularity, to be stated in the last theorem here, is considerably simpler than Bandelt's original approach and seems to be the right way to reveal what is behind the scene in [B]. In spite of the present achievments, we are not able to generalize all properties of lattice tolerances, for example, there is still no generalization of [Cz4].

For $\Phi \in \mathbf{Tol\,A}$, the transitive closure of Φ will be denoted by Φ^*. Clearly, Φ^* is a congruence of $\mathbf{A}$. For any $\Phi, \Psi \in \mathbf{Tol\,A}$ the least congruence containing both

Φ and Ψ will be denoted here by $\Phi \vee \Psi$. Obviously, we have $\Phi \vee \Psi = (\Phi \sqcup \Psi)^* = \Phi^* \vee \Psi^*$. We recall from the previous subdivision that we say that dist(tol,tol,tol) respectively mod(tol,tol,tol) holds in $\mathbf{A}$, if $\Gamma \wedge (\Phi \vee \Psi) \leq (\Gamma \wedge \Phi) \vee (\Gamma \wedge \Psi)$ respectively $\Gamma \wedge (\Phi \vee (\Gamma \wedge \Psi)) \leq (\Gamma \wedge \Phi) \vee (\Gamma \wedge \Psi)$ is valid for all $\Gamma, \Phi, \Psi \in \mathbf{Tol\,A}$.

In the previous subdivision we proved that if $\mathcal{V}$ is a congruence modular resp. congruence distributive variety, then for each algebra $\mathbf{A} \in \mathcal{V}$, mod(tol,tol,tol) resp. dist(tol,tol,tol) holds in $\mathbf{A}$. We also proved that $\Phi \wedge \Psi^* \leq (\Phi \wedge \Psi)^*$ for all $\Phi, \Psi \in \mathbf{Tol\,A}$ and $\mathbf{A} \in \mathcal{V}$, and pointed out that it is essential to consider a whole variety, not just a single algebra.

It is known that the variety of all lattices is congruence distributive. The afore-mentioned results of Bandelt ([B]) state that for any lattice $\mathbf{L}$, $\mathbf{Tol\,L}$ is a pseudocomplemented and 0-modular lattice. The pseudocomplement $\Phi^{\#}$ of any $\Phi \in \mathbf{Tol\,A}$ is a congruence by [RS]. Now the above-mentioned results of [CzH2] provide us with the main tool to prove, for instance, that if $\mathbf{A}$ belongs to a congruence modular variety, then $\mathbf{Con\,A}$ is a homomorphic image of $\mathbf{Tol\,A}$; if $\mathbf{A}$ belongs to a congruence distributive variety, then $\mathbf{Tol\,A}$ is 0-1 modular and pseudocomplemented lattice and for any $\Phi \in \mathbf{Tol\,A}$ $\Phi^{\#}$ is a congruence.

A lattice $\mathbf{L}$ with 0 is called *0-modular,* cf. Stern ([St]), if there is no N_5 sublattice of $\mathbf{L}$ including 0. A bounded lattice L is called 0-1 *modular* if no N_5 of $\mathbf{L}$ includes both 0 and 1. Clearly, this is equivalent to the condition that none of the elements of $\mathbf{L}$ has comparable complements. A complete lattice $\mathbf{L}$ is called *upper continuous,* cf. Schmidt ([Sch]), if any directed family of elements $\{a_\delta \mid \delta \in D\} \subseteq \mathbf{L}$ and any $a \in \mathbf{L}$ satisfies $a \wedge (\bigvee \{a_\delta \mid \delta \in D\}) = \bigvee \{a \wedge a_\delta \mid \delta \in D\}$. It is well-known that any algebraic lattice is upper continuous.

For $a, b \in L$ set SC $(a/b) = \{x \in L \mid a \wedge x \leq b\}$. If $\mathbf{L}$ is an upper continuous lattice, then the set SC (a/b) contains at least one maximal element [CrD], which is called a *weak pseudocomplement* of a *relative to* b and it is denoted by $a_w b$. It is easy to see that $a_w b$ is not necessarily unique and for any $x \in$ SC (a/b) there exists at least one $a_w b$ such that $x \leq a_w b$. If $0 \in \mathbf{L}$, then $a_w 0$ is called a *weak pseudocomplement* of a and it is denoted by a^w. If a^w is unique, i.e. if a^w is the greatest element of SC $(a/0)$, then it is called the *pseudocomplement* of a and usually it is denoted by $a^{\#}$. $\mathbf{L}$ is called a *pseudocomplemented lattice* if for each $a \in \mathbf{L}$ there exists $a^{\#} \in \mathbf{L}$. In other words, $\mathbf{L}$ is pseudocomplemented if for any $a \in \mathbf{L}$ there exists an $a^{\#} \in \mathbf{L}$ such that for any $x \in L$, $x \wedge a = 0 \Leftrightarrow x \leq a^{\#}$. It is known that any algebraic distributive lattice is pseudocomplemented. If $\mathbf{L}$ is a pseudocomplemented lattice, then $(L, \wedge, \vee, ^{\#}, 0, 1)$ is called a *p-algebra* . We will use $\triangle$ and ∇ for the equality relation and the total relation on $\mathbf{A}$, respectively. The algebra $\mathbf{A}$ is called *tolerance-simple,* cf. e.g. Chajda [Ch], if $\mathbf{Tol\,A} = \{\triangle, \nabla\}$.

The following lemma will be useful in our proofs:

Lemma 6.1 ([CHR]). *Let* $\mathbf{A}$ *be an arbitrary algebra and* $\Phi_1, \Phi_2 \in \mathbf{Tol\,A}$. *Then* $\Phi_1 \sqcup \Phi_2 = \nabla$ *implies* $\Phi_1 \circ \Phi_2 = \Phi_2 \circ \Phi_1 = \nabla$.

Proof. Since $(\Phi_1 \circ \Phi_2) \cap (\Phi_2 \circ \Phi_1)$ is clearly a tolerance of $\mathbf{A}$, cf. e.g. [RRS], and it includes Φ_1 and Φ_2, we obtain $\nabla = \Phi_1 \sqcup \Phi_2 \subseteq (\Phi_1 \circ \Phi_2) \cap (\Phi_2 \circ \Phi_1)$. Hence $\Phi_1 \circ \Phi_2 = \Phi_2 \circ \Phi_1 = \nabla$.
Lemma 6.1 is proved.

$\square$

Lemma 6.2 ([CHR]). *Let* $\mathbf{A}$ *be a congruence modular (congruence distributive) algebra. Then the following statements are equivalent:*

(i) For any $\theta \in \mathbf{Con\,A}$ *and any* $\Phi \in \mathbf{Tol\,A}$ *we have* $\Phi_w\theta \in \mathbf{Con\,A}$.

(ii) $\Phi^* \wedge \Psi^* = (\Phi \wedge \Psi)^*$, *for all* $\Phi, \Psi \in \mathbf{Tol\,A}$.

(iii) The map h: $\mathbf{Tol\,A} \to \mathbf{Con\,A}$, $\Phi \mapsto \Phi^*$, *is a surjective lattice homomorphism.*

(iv) mod(tol,tol,tol) (dist(tol,tol,tol)) holds in $\mathbf{A}$.

Proof. (i) $\Rightarrow$(ii). Let $\Phi, \Psi \in \mathbf{Tol\,A}$ and consider $\theta = (\Phi \wedge \Psi)^* \in \mathbf{Con\,A}$. Then $\Phi \wedge \Psi \leq \theta$. As $\mathbf{Tol\,A}$ is an algebraic lattice, there exists a $\Phi_w\theta$ such that $\Psi \leq \Phi_w\theta$. Since by the assumption of (i) $\Phi_w\theta \in \mathbf{Con\,A}$, we obtain $\Psi^* \leq \Phi_w\theta$, and this implies $\Phi \wedge \Psi^* \leq (\Phi \wedge \Psi)^*$. As this relation is valid for any pair of tolerances, we obtain

$$\Phi^* \wedge \Psi^* \leq (\Phi^* \wedge \Psi)^* \leq ((\Phi \wedge \Psi)^*)^* = (\Phi \wedge \Psi)^*.$$

Since $(\Phi \wedge \Psi)^* \leq \Phi^* \wedge \Psi^*$, we obtain $\Phi^* \wedge \Psi^* = (\Phi \wedge \Psi)^*$.

(ii)$\Rightarrow$(iii). Since for any $\theta \in \mathbf{Con\,A}$ we have $h(\theta) = \theta$, the map

$$h : \mathbf{Tol\,A} \to \mathbf{Con\,A}$$

is surjective. Take $\Phi, \Psi \in \mathbf{Tol\,A}$. Then $h(\Phi \sqcup \Psi) = (\Phi \sqcup \Psi)^* = \Phi^* \vee \Psi^* = h(\Phi) \vee h(\Psi)$, moreover (ii) implies $h(\Phi \wedge \Psi) = (\Phi \wedge \Psi)^* = (\Phi \wedge \Psi)^* = h(\Phi) \wedge h(\Psi)$. Thus h is a homomorphism.

(iii)⇒(iv). Take $\Gamma, \Phi, \Psi \in \mathbf{Tol\,A}$. Then we have

$$\Gamma \wedge (\Phi \vee (\Gamma \wedge \Psi)) \leq \Gamma^* \wedge (\Phi^* \vee (\Gamma \wedge \Psi)^*) \leq \Gamma^* \wedge (\Phi^* \vee (\Gamma^* \wedge \Psi^*)).$$

If $\mathbf{Con\,A}$ is a modular lattice, then we obtain $\Gamma^* \wedge (\Phi^* \vee (\Gamma^* \vee \Psi^*)) \leq (\Gamma^* \wedge \Phi^*) \vee (\Gamma^* \wedge \Psi^*)$. Since $h(\Phi) = \Phi^*$ is a homomorphism, we have $(\Gamma \wedge \Phi)^* = \Gamma^* \wedge \Phi^*$ and $(\Gamma \wedge \Psi)^* = \Gamma^* \wedge \Psi^*$. Thus we obtain $\Gamma \wedge (\Phi \vee (\Gamma \wedge \Psi)) \leq (\Gamma^* \wedge \Phi^*) \vee (\Gamma^* \wedge \Psi^*) = (\Gamma \wedge \Phi)^* \vee (\Gamma \wedge \Psi)^* = (\Gamma \wedge \Phi) \vee (\Gamma \wedge \Psi)$, and so mod(tol,tol,tol) holds in $\mathbf{A}$.

The case when $\mathbf{Con\,A}$ is distributive is similar:

$$\Gamma \wedge (\Phi \vee \Psi) \leq \Gamma^* \wedge (\Phi^* \vee \Psi^*) = (\Gamma^* \wedge \Phi^*) \vee (\Gamma^* \wedge \Psi^*) =$$
$$(\Gamma \wedge \Phi)^* \vee (\Gamma \wedge \Psi)^* = (\Gamma \wedge \Phi) \vee (\Gamma \wedge \Psi),$$

and this proves that dist(tol,tol,tol) holds in $\mathbf{A}$.

(iv)⇒(i). Clearly, dist(tol,tol,tol) implies mod(tol,tol,tol) and the latter, according to [CzeHor2] or substituting 0 for the "third tol", implies $\Gamma \wedge \Phi^* \leq (\Gamma \wedge \Phi)^*$ for all $\Gamma, \Phi \in \mathbf{Tol\,A}$. Take any $\theta \in \mathbf{Con\,A}$ and $\Phi \in \mathbf{Tol\,A}$. Then $\Phi \wedge \Phi_w\theta \leq \theta$ implies $\Phi \wedge (\Phi_w\theta)^* \leq (\Phi \wedge \Phi_w\theta)^* \leq \theta^* = \theta$, i.e. $(\Phi_w\theta)^* \in$ SC (Φ/θ). As $\Phi_w\theta$ is a maximal element of SC (Φ/θ) and since $\Phi_w\theta \leq (\Phi_w\theta)^*$, we obtain $\Phi_w\theta = (\Phi_w\theta)^* \in \mathbf{Con\,A}$.
Lemma 6.2 is proved.

□

Proposition 6.2 ([CHR]). *Let* $\mathbf{A}$ *be an algebra in a congruence modular variety* $\mathcal{V}$. *Then the following two statements hold:*

(i) For any $\Phi \in \mathbf{Tol\,A}$ *each* $\Phi^w \in \mathbf{Con\,A}$.

(ii) If Φ *and* Ψ *are complements of each other in* $\mathbf{Tol\,A}$, *then they are weak pseudocomplements of each other and form a factor congruence pair of* $\mathbf{A}$.

Proof. (i) Since $\mathcal{V}$ is congruence modular, mod(tol,tol,tol) holds in $\mathbf{A}$ according to [CzH2]. As $\Phi^w = \Phi_w 0$, applying Lemma 6.2 we infer (i).

(ii) Let Φ and Ψ be complements of each other in $\mathbf{Tol\,A}$. Then, by Lemma 6.1, $\Phi \sqcup \Psi = \nabla$ implies $\Phi \circ \Psi = \Psi \circ \Phi = \nabla$. As $\Phi \wedge \Psi = \triangle$, there is a Φ^w such that $\Psi \leq \Phi^w$. We have to prove $\Psi = \Phi^w$, i.e. $\Phi^w \leq \Psi$.

Take any $(x, y) \in \Phi^w$. Since $(x, y) \in \Phi \circ \Psi$, there exists a $z \in A$ such that $(x, z) \in \Phi$ and $(z, y) \in \Psi$. However $\Psi \leq \Phi^w$ implies $(z, y) \in \Phi^w$. As $\Phi^w \in \mathbf{Con\,A}$, we obtain $(x, z) \in \Phi^w \wedge \Phi = \triangle$, i.e. $x = z$. Therefore we obtain $(x, y) \in \Psi$ proving $\Phi^w \leq \Psi$. Thus, we conclude that $\Psi = \Phi^w \in \mathbf{Con\,A}$. Interchanging the role of Φ

and Ψ we obtain $\Phi = \Psi^w \in \mathbf{Con\,A}$. As $\Phi \wedge \Psi = \triangle$ and $\Phi \circ \Psi = \Psi \circ \Phi = \nabla$, Φ and Ψ are factor congruences of $\mathbf{A}$.
Proposition 6.2 is proved.

$\square$

Definition 6.1. The lattice $\mathbf{L}$ with 0 satisfies the *general disjointness property* (GD) if $a \wedge b = 0$ and $(a \vee b) \wedge c = 0$ imply $a \wedge (b \vee c) = 0$. (See [S] or [St].)

It is easy to check that any pseudocomplemented lattice has the (GD) property. It was proved in [S] that any 0-modular lattice satisfies the (GD) property, too.

THEOREM 6.2 [(CHR)]. *Let* $\mathbf{A}$ *be an algebra in a congruence modular variety* $\mathcal{V}$. *Then the following statements hold:*

(i) The map h: $\mathbf{Tol\,A} \to \mathbf{Con\,A}$, $\Phi \mapsto \Phi^*$, *is a surjective lattice homomorphism and* $\mathbf{Tol\,A}$ *is a* 0-1 *modular lattice having the (GD) property.*

(ii) $\mathbf{Tol\,A}$ *is pseudocomplemented if and only if* $\mathbf{Con\,A}$ *is pseudocomplemented.*

Proof. (i) Since $\mathcal{V}$ is a congruence modular variety and $\mathbf{A} \in \mathcal{V}$, by [CzH1] mod(tol,tol,tol) holds in $\mathbf{A}$. Therefore by applying Lemma 6.2 we obtain the required homomorphism.

Now, by way of contradiction, suppose that $\mathbf{Tol\,A}$ is not 0-1 modular. Then an N_5 sublattice of $\mathbf{Tol\,A}$ includes Δ and ∇. Hence each element of this N_5 has a complement in $\mathbf{Tol\,A}$. Since complements are weak pseudocomplements as well, we conclude from Proposition 6.2(ii) that $N_5 \subseteq \mathbf{Con\,A}$. Hence the homorphism h acts identically on N_5 and we infer that N_5, as a homomorphic image, is a sublattice of $\mathbf{Tol\,A}$, contradicting congruence modularity.

Finally, take $\Gamma, \Phi, \Psi \in \mathbf{Tol\,A}$ and assume that $\Gamma \wedge \Phi = \triangle$ and $(\Gamma \sqcup \Phi) \wedge \Psi = \triangle$. Applying the homomorphism h to these two equations we obtain $h(\Gamma) \wedge h(\Phi) = h(\triangle) = \triangle$ and $(h(\Gamma) \vee h(\Phi)) \wedge h(\Psi) = \triangle$. Since $\mathbf{Con\,A}$ is a modular lattice, it has the (GD) property as well, and this gives $\Gamma \wedge (\Phi \sqcup \Psi) \leq h(\Gamma \wedge (\Phi \sqcup \Psi)) = h(\Gamma) \wedge (h(\Phi) \vee h(\Psi)) = \triangle$. Thus $\mathbf{Tol\,A}$ has the (GD) property.

(ii) Assume that $\mathbf{Tol\,A}$ is a pseudocomplemented lattice. Since now for any $\theta \in \mathbf{Con\,A}$, $\theta^{\#}$ is its (unique) weak pseudocomplement in $\mathbf{Tol\,A}$, Proposition 6.2(i) gives $\theta^{\#} \in \mathbf{Con\,A}$. As any $\zeta \in \mathbf{Con\,A}$ is also a tolerance, we have $\theta \wedge \zeta = \triangle \Leftrightarrow \zeta \leq \theta^{\#}$. Hence $\theta^{\#}$ is the pseudocomplement of θ in the lattice $\mathbf{Con\,A}$ as well. Thus $\mathbf{Con\,A}$ is pseudocomplemented.

Conversely, assume that **Con A** is pseudocomplemented and denote by $\theta^{\#}$ the pseudocomplement of a $\theta \in$ **Tol A**. We prove that for each $\Phi \in$ **Tol A** the congruence $((\Phi)^*)^{\#}$ is the pseudocomplement of Φ in **Tol A**.

Let $\Psi \in$ **Tol A**, $\Psi \leq (\Phi^*)^{\#}$. Then $\Phi \wedge \Psi \leq \Phi^* \wedge (\Phi^*)^{\#} = \triangle$. Take a $\Psi \in$ **Tol A** with $\Phi \wedge \Psi = \triangle$. Then, in view of Lemma 6.2(ii), we have $\Phi^* \wedge \Psi^* = (\Phi \wedge \Psi)^* = \triangle$. Thus we obtain $\Psi^* \leq (\Phi^*)^{\#}$ and so $\Psi \leq (\Phi^*)^{\#}$. Hence $\Phi \wedge \Psi = 0 \Leftrightarrow \Psi \leq (\Phi^*)^{\#}$ and this proves that **Tol A** is pseudocomplemented and the pseudocomplement $\Phi^{\#}$ of Φ in **Tol A** is the same as $(\Phi^*)^{\#}$.
Theorem 6.2 is proved.

□

Remark 6.1. Observe that the following is implicit in the proof of Theorem 6.2(ii): The pseudocomplement in **Con A** of a $\Theta \in$ **Con A** is the same as its pseudocomplement in **Tol A**. As a consequence, the pseudocomplementation operation will be denoted by the same symbol "$\#$" in both of the lattices **Tol A** and **Con A**. It is also clear that in this case $(\mathbf{Con\,A}, \wedge, ^{\#})$ is a subalgebra of $(\mathbf{Tol\,A}, \wedge, ^{\#})$. Notice that in the proof of the Theorem 6.2(ii) it was also deduced that $\Phi^{\#} = (\Phi^*)^{\#}$.

Proposition 6.3 ([CHR]). *Let $\mathcal{V}$ be a congruence distributive variety and let $\mathbf{A} \in \mathcal{V}$. Then the following statements hold:*

(i) **Tol A** *is a pseudocomplemented* 0-1 *modular lattice and for any* $\Phi \in$ **Tol A** *we have* $\Phi^{\#} \in$ **Con A**.

(ii) The map $h : \mathbf{Tol\,A} \to \mathbf{Con\,A}$, $\Phi \mapsto \Phi^*$, *is a homomorphism of the p-algebra* $(\mathbf{Tol\,A}, \wedge, \sqcup, ^{\#}, \triangle, \nabla)$ *onto the p-algebra* $(\mathbf{Con\,A}, \wedge, \vee, ^{\#}, \triangle, \nabla)$.

Proof. Now **Con A**, as an algebraic distributive lattice, is pseudocomplemented as well. Therefore (i) is an obvious consequence of Theorem 6.2 and Proposition 6.2(i).

(ii) In view of Theorem 6.2(i) h is a lattice homomorphism and h is surjective. We have also $h(\triangle) = \triangle$ and $h(\nabla) = \nabla$. Since $\Phi^{\#} \in$ **Con A**, $h(\Phi^{\#}) = \Phi^{\#}$. On the other hand, we have $(h(\Phi))^{\#} = (\Phi^*)^{\#} = \Phi^{\#}$, according to Remark 6.1. Thus we obtain $h(\Phi^{\#}) = (h(\Phi))^{\#}$, and hence h is a homomorphism of p-algebras.
Proposition 6.3 is proved.

□

Corollary 6.2 ([CHR]). *Let* **A** *be an algebra of a variety $\mathcal{V}$.*

(i) If $\mathcal{V}$ is congruence modular and **Tol A** *is a simple or complemented lattice, then* **Tol A** $=$ **Con A**.

(ii) If $\mathcal{V}$ is congruence distributive and the lattice **Tol A** *is simple, then the algebra* **A** *itself is tolerance-simple.*

Proof. We may assume that $|A| \geq 2$.

(i) If **Tol A** is complemented, then Proposition 6.2(ii) gives **Tol A** $=$ **Con A**. If **Tol A** is simple, then the congruence $\Theta \subseteq$ **Tol A** $\times$ **Tol A** defined by

$$(\Phi_1, \Phi_2) \in \Theta \Leftrightarrow \Phi_1^* = \Phi_2^*$$

is either the identity relation or the total relation on **Tol A**. The latter case can be excluded, as $\triangle^* = \triangle \neq \nabla = \nabla^*$. Since we have $(\Phi, \Phi^*) \in \Theta$, we obtain $\Phi = \Phi^*$ for all $\Phi \in$**Tol A**, i.e. **Tol A** $=$ **Con A**.

(ii) We have **Tol A** $=$ **Con A**, according to the above (i). As now **Con A** is a simple distributive lattice, it is a two-element chain. Hence **Tol A** is also a two-element chain, i.e. **A** is tolerance-simple.

Corollary 6.2 is proved.

□

A term function $m(x, y, z)$ of an algebra **A** is called a *majority term* if $m(x, x, y) = m(x, y, x) = m(y, x, x) = x$ holds for all $x, y \in A$. For instance, any lattice $(\mathbf{L}, \wedge, \vee)$ admits a majority term; namely:

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

It is well-known that the variety $\mathcal{V}(\mathcal{A})$ generated by an algebra **A** with a majority term is congruence distributive.

Now let **A** be an arbitrary algebra and $\Gamma, \Phi \in$ **Tol A**. By an (Γ, Φ)-*circle* we mean a quadruplet $(a, b, c, d) \in A^4$ such that $(a, b), (c, d) \in \Gamma$ and $(b, c), (d, a) \in \Phi$.

Lemma 6.3 ([CHR]). *Let* **A** *be an algebra with a majority term m, and let $\Gamma, \Phi \in$* **Tol A** *with $\Gamma \wedge \Phi = \triangle$.*

(i) If $(a, b, c, d) \in A^4$ is an (Γ, Φ)-circle, then

$$m(a, b, c) = b, \ m(b, c, d) = c, \ m(c, d, a) = d, \ m(d, a, b) = a. \tag{1}$$

(ii) We have $\Gamma \sqcup \Phi = (\Gamma \circ \Phi) \cap (\Phi \circ \Gamma)$.

Proof. (i) Because of symmetry, it suffices to prove the first equality. Since we have $(m(a, b, c), m(b, b, c)) \in \Gamma$, $((m(a, b, c), m(a, b, b)) \in \Phi$ and $m(b, b, c) = m(a, b, b) = b$, the first equality comes from $\Gamma \wedge \Phi = \triangle$.

(ii) As it was pointed out in the argument of Lemma 6.1, we have $(\Gamma \circ \Phi) \cap (\Phi \circ \Gamma) \in$ **Tol A** and $\Gamma \sqcup \Phi \subseteq (\Gamma \circ \Phi) \cap (\Phi \circ \Gamma)$. Now let Ψ be a tolerance with $\Gamma \leq \Psi$ and $\Phi \leq \Psi$ and take any $a, c \in A$ with $(a, c) \in (\Gamma \circ \Phi) \cap (\Phi \circ \Gamma)$. Then there exist $b, d \in A$ such that $(a, b) \in \Gamma$, $(b, c) \in \Phi$ and $(a, d) \in \Phi$, $(d, c) \in \Gamma$. Then (a, b, c, d) is an (Γ, Φ)-circle. Therefore (1) gives $m(d, a, b) = a$. On the other hand, $(d, c), (b, c) \in \Psi$ implies $(m(d, a, b), m(c, a, c)) \in \Psi$. As $m(c, a, c) = c$, we obtain $(a, c) \in \Psi$. Thus we conclude $(\Gamma \circ \Phi) \cap (\Phi \circ \Gamma) \leq \Psi$ and this proves $(\Gamma \circ \Phi) \cap (\Phi \circ \Gamma) = \Gamma \sqcup \Phi$.
Lemma 6.3 is proved.

□

THEOREM 6.3 ([CHR]). *Let* **A** *be an algebra. If* **A** *has a majority term, then:*

(i) **Tol A** *is a 0-modular pseudocomplemented lattice.*

(ii) The tolerances Γ, Φ are complements of each other in **Tol A** *if and only if they form a factor congruence pair of A.*

Proof. (i) Since the variety $\mathcal{V}(\mathcal{A})$ is congruence distributive, in view of Proposition 6.3, **Tol A** is pseudocomplemented.

In order to prove that **Tol A** is 0-modular, by way of contradiction let us assume that $\{\triangle, \Gamma, \Phi, \Sigma, \Omega\}$ is an N_5 sublattice in Tol$A$ with $\triangle < \Gamma < \Sigma < \Omega$, $\triangle < \Phi < \Omega$ and $\Gamma \sqcup \Phi = \Sigma \sqcup \Phi = \Omega$, $\Gamma \wedge \Phi = \Sigma \wedge \Phi = \triangle$. Take any $a, c \in A$ with $(a, c) \in \Sigma$. As by Lemma 6.3(ii) we have $\Omega = \Gamma \sqcup \Phi = (\Gamma \circ \Phi) \cap (\Phi \circ \Gamma)$ and since $\Sigma < \Omega$, we obtain $(a, c) \in (\Gamma \circ \Phi) \cap (\Phi \circ \Gamma)$. Then there exist $c, d \in A$ such that $(a, b) \in \Gamma$, $(b, c) \in \Phi$ and $(a, d) \in \Phi$, $(d, c) \in \Gamma$, i.e. such that (a, b, c, d) is an (Γ, Φ)-circle.

¿From $(a, c) \in \Sigma$ and (1) we obtain $b = m(a, b, c) \ \Sigma \ m(c, b, c) = c$. Thus we obtain $(b, c) \in \Sigma \wedge \Phi = \triangle$, i.e. $b = c$. Hence we conclude $(a, c) = (a, b) \in \Gamma$. We have shown $\Sigma \leq \Gamma$, a contradiction. Therefore **Tol A** is 0-modular.

(ii) If Γ and Φ are complements of each other, then they form a factor congruence pair in virtue of Proposition 6.2(ii). Conversely, suppose that $\Gamma, \Phi \in$ **Con A** form a factor congruence pair. Then $\Gamma \circ \Phi = \Phi \circ \Gamma = \nabla$ and $\Gamma \wedge \Phi = \triangle$, whence we conclude from Lemma 6.3 (ii) that $\Gamma \sqcup \Phi = (\Gamma \circ \Phi) \cap (\Phi \circ \Gamma) = \nabla$. Thus Γ and Φ are complements of each other in **Tol A**.
Theorem 6.3 is proved.

□

CHAPTER 7

Maltsev conditions for congruence lattice identities in modular varieties

It is an old problem if all congruence lattice identities are equivalent to Maltsev conditions. In other words, we say that a lattice identity λ can be characterized by a Maltsev condition if there exists a Maltsev condition M such that, for any variety $\mathcal{V}$, λ holds in congruence lattices of all algebras in $\mathcal{V}$ if and only if M holds in $\mathcal{V}$; and the problem is if all lattice identities can be characterized this way. This problem was raised first in Grätzer ([Gr1]), where the notion of a Maltsev condition was defined. A *strong Maltsev condition* for varieties is a condition of the form "there exist terms $h_0, \ldots, h_k$ satisfying a set Σ of identities" where k is fixed and the form of Σ is independent of the type of algebras considered. By a *Maltsev condition* we mean a condition of the form "there exists a natural number n such that P_n holds" where the P_n are strong Maltsev conditions and P_n implies P_{n+1} for every n. The condition "P_n implies P_{n+1}" is usually expressed by saying that a Maltsev condition must be weakening in its parameter. (For a more precise definition of Maltsev conditions cf. [T].) The problem was repeatedly asked by several authors, including Taylor ([T]), Jónsson ([J2]) and Freese and McKenzie ([FM]).

Certain lattice identities have known characterizations by Maltsev conditions. The first two results of this kind are Jónsson's characterization of (congruence) distributivity by the existence of Jónsson terms, cf. Jónsson ([J1]), and Day's characterization of (congruence) modularity by the existence of Day terms, cf. Day ([D1]). Since Day's result will be needed in the sequel, we formulate it now. For $n \geq 2$ let $(\mathbf{D}_n)$ denote the strong Maltsev condition "there are quaternary terms $m_0, \ldots, m_n$ satisfying the identities

$$m_0(x,y,z,u) = x, \qquad m_n(x,y,z,u) = u,$$
$$m_i(x,y,y,x) = x \quad \text{for } i = 0,1,\ldots,n,$$
$$m_i(x,x,y,y) = m_{i+1}(x,x,y,y) \quad \text{for } i = 0,1,\ldots,n, \quad i \text{ even},$$
$$m_i(x,y,y,z) = m_{i+1}(x,y,y,z) \quad \text{for } i = 0,1,\ldots,n, \quad i \text{ odd}".$$

Now Day's celebrated result says that a variety $\mathcal{V}$ is congruence modular iff the Maltsev condition "$(\exists n)(\mathbf{D}_n)$" holds in $\mathcal{V}$.

Jónsson terms and Day terms were soon followed by some similar characterizations for other lattice identities, given for example by Gedeonová ([Ge2]) and Mederly ([Me]), but Nation ([N]) and Day ([Da2]) showed that these Maltsev conditions are equivalent to the existence of Day terms or Jónsson terms; the reader is referred to Jónsson ([Jo2]) and Freese and McKenzie ([FM]) for more details.

The next milestone is Chapter XIII in Freese and McKenzie's book ([FM]). Let us call a lattice identity λ in n^2 variables a *frame identity* if λ implies modularity and λ holds in a modular lattice iff it holds for the elements of every (von Neumann) n-frame of the lattice. Freese and McKenzie showed that frame identities can be characterized by Maltsev conditions. Although that time there was a hope that their method combined with [HC] gives a Maltsev condition for each λ that implies modularity, cf. [FM], Pálfy and Szabó ([PSz]) destroyed this expectation.

The goal of the present chapter is to prove that each lattice identity implying modularity is equivalent to a Maltsev condition. Moreover, this Maltsev condition is very easy to construct. In order to formulate a slightly stronger statement, some definitions come first.

A lattice identity λ is said to imply modularity in congruence varieties, in notation $\lambda \models_c \text{mod}$ if for any variety $\mathcal{V}$ if all the congruence lattices $\mathbf{Con\,A}$, $\mathbf{A} \in \mathcal{V}$, satisfy λ, then all these lattices are modular. If λ implies modularity in the usual lattice theoretic sense, then of course $\lambda \models_c \text{mod}$ as well. However, it was a great surprise by Nation ([N]) that $\lambda \models_c \text{mod}$ is possible even when λ does not imply modularity in the usual sense. Jónsson ([J2]) gives an overview of similar results. We mention that there is an algorithm to test if $\lambda \models_c \text{mod}$, cf. [CzF], which is based on Day and Freese ([DF]).

Given a lattice term p and $k \geq 2$, we define p_k via induction as follows. If p is a variable, then let $p_k = p$. If $p = r \wedge s$, then let $p_k = r_k \cap s_k$. Finally, if $p = r \vee s$, then let $p_k = r_k \circ s_k \circ r_k \circ s_k \circ \ldots$ with k factors on the right. When congruences or, more generally, reflexive compatible relations are substituted for the variables of p_k, then the operations $\cap$ and $\circ$ will be interpreted as intersection and relational product, respectively. By a *lattice identity* λ we mean an *inequality* $p \leq q$ where p and q are lattice terms. This does not hurt generality because $p \leq q$ is equivalent to an appropriate identity $r = s$ modulo lattice theory and vice versa. If $\lambda : p \leq q$ is a lattice identity and $m, n \geq 2$, then we can consider the *inclusion* $p_m \subseteq q_n$. If $\mathbf{A}$ is an algebra, then p_m and q_n do not give congruences in general when their variables are substituted by congruences of $\mathbf{A}$. However, it makes sense to say that $p_m \subseteq q_n$ holds or fails for congruences of $\mathbf{A}$. Now Wille ([Wi]) and Pixley ([Pix]) give an easy algorithm to construct a strong Maltsev condition $M(p_m \subseteq q_n)$ such that, for any variety $\mathcal{V}$, $p_m \subseteq q_n$ holds for congruences of all algebras in $\mathcal{V}$ if and only if $M(p_m \subseteq q_n)$ holds in $\mathcal{V}$. (Notice that the construction of $M(p_m \subseteq q_n)$ is outlined in Freese and McKenzie ([FM]), and, with the notation $U(G_m(p) \leq G_n(q))$, it is detailed in [CzD].) Wille and Pixley showed also that $p_m \subseteq q$ holds for congruences of algebras in $\mathcal{V}$ if and only if $\mathcal{V}$ satisfies the Maltsev condition "there is an n such that $M(p_m \subseteq q_n)$ holds"; this will be needed in our proof. Now we can formulate the main result.

THEOREM 7.1 ([CzH3]). *Let $\lambda : p \leq q$ be a lattice identity such that $\lambda \models_c$ modularity. Then for any variety $\mathcal{V}$ the following two conditions are equivalent.*

(a) For all $\mathbf{A} \in \mathcal{V}$, λ holds in the congruence lattice of $\mathbf{A}$.

(b) $\mathcal{V}$ satisfies the Maltsev condition "there is an $n \geq 2$ such that $M(p_3 \subseteq q_n)$ and ($\mathbf{D}_n$) hold".

This chapter will not detail the construction of $M(p_3 \subseteq q_n)$, but we mention that if we consider $\lambda : (x \wedge (y \vee (x \wedge z)) \leq (x \wedge y) \vee (x \wedge z)$, the modular law, then Day's characterization of congruence modularity becomes a particular case of Theorem 1.

Before proving Theorem 7.1 we give some definitions and remarks. The set of tolerances of $\mathbf{A}$ will be denoted by $\mathbf{Tol\,A}$. The *transitive closure* of a tolerance $\Phi \in \mathbf{Tol\,A}$ will be denoted by

$$\Phi^{\,*} = \bigcup_{n=1}^{\infty} (\Phi \circ \Phi \circ \Phi \circ \ldots) \quad (n \text{ factors}).$$

Note that $\Phi^{\,*}$ always belongs to $\mathbf{Con\,A}$, the congruence lattice of $\mathbf{A}$, and

$$\alpha \vee \beta = (\alpha \cup \beta)^{\,*} \tag{1}$$

holds for any $\alpha, \beta \in \mathbf{Con\,A}$. Our interest in tolerances started with generalizing the Shifting Principle from Gumm ([Gu1]) for congruence distributive varieties, cf. [ChH1] and [CCH1], see also Chapter 4. It appeared soon that formulas give stronger generalizations than diagrams both for the congruence distributive and for the congruence modular case, and we proved in [CzH2] (and in Chapter 6) that if $\mathcal{V}$ is a congruence modular variety, $\mathbf{A} \in \mathcal{V}$ and $\Gamma, \Phi, \Psi \in \mathbf{Tol\,A}$, then

$$\Gamma \cap (\Phi \cup (\Gamma \cap \Psi))^{\,*} \subseteq ((\Gamma \cap \Phi) \cup (\Gamma \cap \Psi))^{\,*}. \tag{2}$$

Notice that formally, according to (1), (2) is a variant of the modular law. Substituting 0 for Ψ in (2) we obtained, cf. Proposition 1 in [CzH2] (Proposition 6.1 in Chapter 6), that

$$\Gamma \cap \Phi^{\,*} \subseteq (\Gamma \cap \Phi)^{\,*}. \tag{3}$$

Notice that it is essential to consider varieties here, for [CzH2] presents a single algebra with modular congruence lattice, a tolerance Φ and a congruence Γ of this algebra such that $\Gamma \cap \Phi^{\,*} \subseteq (\Gamma \cap \Phi)^{\,*}$ fails. As the next step towards Theorem 7.1 , Radeleczki ([CHR]) and later, independently, Kearnes [Ke1] noticed that (3) trivially implies a more useful statement: if $\mathbf{A}$ belongs to a congruence modular variety and $\Gamma, \Phi \in \mathbf{Tol\,A}$, then

$$\Gamma^{\,*} \cap \Phi^{\,*} = (\Gamma \cap \Phi)^{\,*}. \tag{4}$$

Indeed, applying (3) for $\Gamma^{\,*}$ and Φ, and then for Φ and Γ we obtain the nontrivial inclusion part of (4). Here we will give a direct proof of (3), which is of course a special (and therefore a bit shorter) case of the proof of (2).

Proof of Theorem 7.1. First we prove (3). Let $\mathcal{V}$ be a congruence modular variety with Day-terms $m_0, \ldots, m_n$. Let Γ and Φ be tolerances of an algebra $\mathbf{A}$ in $\mathcal{V}$. First we show that

$$\Gamma \cap (\Phi \circ \Phi) \subseteq (\Gamma \cap \Phi)^{\,*}. \tag{5}$$

Suppose $(a, b) \in \Gamma \cap (\Phi \circ \Phi)$. Then there is an element $c \in A$ with $(a, c), (c, b) \in \Phi$, and of course, $(a, b) \in \Gamma$. Now we define further elements. Let $d_i = m_i(a, c, c, b)$ for $i = 0, \ldots, n$ and let $e_i = m_i(a, a, b, b)$ for i even, $i = 0, \ldots, n$. Notice that $d_i = d_{i+1}$ for i odd. Let j denote an arbitrary even index. Then $(d_j, e_j) \in \Phi$ is clear. Since

$$\begin{aligned} d_j =& m_j(m_j(a, c, c, b), a, a, m_j(a, c, c, b)) \;\Gamma\; m_j(m_j(a, c, c, a), a, b, m_j(b, c, c, b)) \\ =& m_j(a, a, b, b) = e_j, \end{aligned}$$

we obtain $(d_j, e_j) \in \Gamma \cap \Phi$. Since $e_j = m_j(a, a, b, b) = m_{j+1}(a, a, b, b)$, we conclude $(d_{j+1}, e_j) \in \Gamma \cap \Phi$ exactly the same way. Since any two neighbouring members of the sequence

$$a = d_0,\ e_0,\ d_1 = d_2,\ e_2,\ d_3 = d_4,\ e_4,\ d_5 = d_6,\ \ldots,\ d_n = b$$

are in the relation $\Gamma \cap \Phi$, we infer $(a, b) \in (\Gamma \cap \Phi)^{\,*}$. This proves (5).

Now let $\Phi_0 = \Phi$ and $\Phi_{n+1} = \Phi_n \circ \Phi_n$, these are tolerances again. We claim that, for all n,

$$\Gamma \cap \Phi_n \subseteq (\Gamma \cap \Phi)^{\,*}. \tag{6}$$

This is evident for $n = 0$. If (6) holds for some n, then applying (5) for Γ and Φ_n and using the induction hypothesis, we have

$$\Gamma \cap \Phi_{n+1} = \Gamma \cap (\Phi_n \circ \Phi_n) \subseteq (\Gamma \cap \Phi_n)^{\,*} \subseteq ((\Gamma \cap \Phi)^{\,*})^{\,*} = (\Gamma \cap \Phi)^{\,*}.$$

Hence (6) holds for all n. Therefore we obtain

$$\Gamma \cap \Phi^{\,*} = \Gamma \cap \bigcup_{n=0}^{\infty} \Phi_n = \bigcup_{n=0}^{\infty} (\Gamma \cap \Phi_n) \subseteq \bigcup_{n=0}^{\infty} (\Gamma \cap \Phi)^{\,*} = (\Gamma \cap \Phi)^{\,*}$$

This proves (3) for any tolerances Γ and Φ.

Applying (3) first for $\Gamma^{\,*}$ and Φ and then for Φ and Γ we obtain

$$\Gamma^{\,*} \cap \Phi^{\,*} \subseteq (\Gamma^{\,*} \cap \Phi)^{\,*} = (\Phi \cap \Gamma^{\,*})^{\,*} \subseteq ((\Phi \cap \Gamma)^{\,*})^{\,*} = (\Gamma \cap \Phi)^{\,*},$$

i.e. $\Gamma^{\,*} \cap \Phi^{\,*} \subseteq (\Gamma \cap \Phi)^{\,*}$. Since forming transitive closure is a monotone operation, the reverse inclusion is evident. This proves (4).

For tolerances Φ and Ψ it is easy to see that $\Phi \circ \Psi \circ \Phi$ is again a tolerance. It follows from reflexivity that

$$(\Phi \circ \Psi \circ \Phi)^{\,*} = \Phi^{\,*} \vee \Psi^{\,*}, \tag{7}$$

where the join is taken in **Con A**. An easy induction shows that if $r = r(x_1, \dots, x_k)$ is a lattice term and $\Phi_1, \dots, \Phi_k$ are tolerances or, as a particular case, congruences of an algebra $\mathbf{A}$, then $r_3(\Phi_1, \dots, \Phi_k)$ is a tolerance again.

Now let $\mathcal{V}$ be a variety and assume (a). Let p and q be, say, k-ary lattice terms. Since an easy induction shows that, for any $\mathbf{A} \in \mathcal{V}$ and any congruences $\alpha_1, \dots, \alpha_k$ of $\mathbf{A}$ we have $p_3(\alpha_1, \dots, \alpha_k) \subseteq p(\alpha_1, \dots, \alpha_k)$, we conclude that $p_3 \subseteq q$ holds for congruences of any $\mathbf{A} \in \mathcal{V}$. Hence the afore-mentioned result of Wille and Pixley yields that $M(p_3 \subseteq q_{n_1})$ holds in $\mathcal{V}$ for some n_1. Since $\lambda \models_c \text{mod}$, there is an n_2 such that $\mathbf{D}_{n_2}$ holds in $\mathcal{V}$. Now let n be the maximum of n_1 and n_2. Since Maltsev conditions are weakening in their parameter, we obtain that $\mathcal{V}$ satisfies (b).

Now, to show the reverse implication, assume that (b) holds. By Day's result, $\mathcal{V}$ is congruence modular, whence (4) holds as well. The afore-mentioned result of Wille and Pixley gives that $p_3 \subseteq q$ holds for congruences in $\mathcal{V}$. So for any congruences $\alpha_1, \dots, \alpha_k$ of $\mathbf{A} \in \mathcal{V}$, we have $p_3(\alpha_1, \dots, \alpha_k) \subseteq q(\alpha_1, \dots, \alpha_k)$. Hence

$$p_3(\alpha_1, \dots, \alpha_k)^{\,*} \subseteq q(\alpha_1, \dots, \alpha_k)^{\,*}. \tag{8}$$

Since $q(\alpha_1, \ldots, \alpha_k)$ is a congruence, it equals its transitive closure. On the other hand, a trivial induction based on (4) and (7) gives that $p_3(\alpha_1, \ldots, \alpha_k)^* = p(\alpha_1{}^*, \ldots, \alpha_k{}^*) = p(\alpha_1, \ldots, \alpha_k)$. This way (8) turns into

$$p(\alpha_1, \ldots, \alpha_k) \subseteq q(\alpha_1, \ldots, \alpha_k),$$

proving that λ holds in **Con A** for all $A \in \mathcal{V}$. Thus (a) holds.
Theorem 7.1 is proved.

□

Now it was proved in theorem 7.1 that if $\lambda \models_c$ modularity, then λ can be characterized by a Maltsev condition. The proof of this fact is relatively elementary and easy, but the Maltsev conditions obtained are far from being optimal in most of those cases where Maltsev conditions were previously known.

Next we improve Theorem 7.1 by giving the simplest (and in this sense hopefully the best) Maltsev condition associated with λ when $\lambda \models_c$ modularity.

We recall now that a very important condition appeared in (4). From now on we will call this condition *tolerance intersection property*, TIP for short. More precisely, an algebra **A** is said to satisfy the tolerance intersection property if for any two tolerances (i.e. reflexive symmetric compatible relations) Γ and Φ of **A** we have

$$\Gamma^* \cap \Phi^* = (\Gamma \cap \Phi)^*$$

where * stands for transitive closure. In the proof of Theorem 7.1 we already proved the following statement:

THEOREM 7.2 ([CHL]). *Every algebra in a congruence modular variety satisfies TIP.*

Given an algebra **A**, the set $\mathrm{Rel}_r(A)$ of all reflexive and compatible relations on **A** (in other words, all subalgebras of $\mathbf{A^2}$ including the diagonal subalgebra) has the operations intersection $\cap$, inverse $^{-1}$, composition $\circ$, transitive closure * and join $\vee$ as usual: for α and β in $\mathrm{Rel}_r(\mathbf{A})$, $(x, y) \in \alpha^{-1}$ iff $(y, x) \in \alpha$, $(x, y) \in \alpha \circ \beta$ iff there exists a $z \in A$ with $(x, z) \in \alpha$ and $(z, y) \in \beta$, and $\alpha \vee \beta$ is the transitive closure of $\alpha \cup \beta$. Notice that for *tolerances* $\alpha, \beta \in \mathrm{Rel}_r(\mathbf{A})$ we have

$$\alpha \vee \beta = (\alpha \vee \beta)^* = \alpha^* \vee \beta^* = (\alpha \circ \beta)^* = (\alpha^* \vee \beta^*)^*.$$

Sometimes we write $\wedge$ instead of $\cap$. When we speak of terms in these operations, the motivating idea is substituting the variables by reflexive compatible relations later.

For a term $p = p(x_1, \ldots, x_k)$ in the binary operations $\cap, \vee, \circ$, in short for a $\{\cap, \vee, \circ\}$-term, and for $n \geq 2$ we define two kinds of derived $\{\cap, \circ\}$-terms, p_n and $p_{2,2}$ via induction as follows. (When p happens to be a lattice term then p_n will be the same as before.) If p is a variable, then let $p_n = p_{2,2} = p$. If $p = r \cap s$, then let $p_n = r_n \cap s_n$ and $p_{2,2} = r_{2,2} \cap s_{2,2}$. Similarly, if $p = r \circ s$, then let $p_n = r_n \circ s_n$ and $p_{2,2} = (r_{2,2} \circ s_{2,2}) \cap (s_{2,2} \circ r_{2,2})$. Finally, if $p = r \vee s$, then let $p_n = r_n \circ s_n \circ \cdots$ with n factors on the right and $p_{2,2} = (r_{2,2} \circ s_{2,2}) \cap (s_{2,2} \circ r_{2,2})$. The tool to exploit TIP is provided by the following lemma; notice that part (D) was previously proved by Kearnes ([Ke2]) in a different way.

Lemma 7.1 ([CHL]). *Let* $\mathbf{A}$ *be an algebra satisfying TIP, let* $p = p(x_1, \ldots, x_k)$ *be a* $\{\cap, \vee, \circ\}$*-term, let* $q = q(x_1, \ldots, x_k)$ *be a lattice term (i.e. a* $\{\cap, \vee\}$*-term), and let* $\alpha_1, \ldots, \alpha_k \in \mathbf{Con\, A}$*. Then*

(A) $p_{2,2}(\alpha_1, \ldots, \alpha_k) \subseteq p_2(\alpha_1, \ldots, \alpha_k) \subseteq p(\alpha_1, \ldots, \alpha_k)$ *(even without assuming TIP);*

(B) $p_{2,2}(\alpha_1, \ldots, \alpha_k)^* = p_2(\alpha_1, \ldots, \alpha_k)^* = p(\alpha_1, \ldots, \alpha_k)^*$*;*

(C) $q_2(\alpha_1, \ldots, \alpha_k)^* = q_{2,2}(\alpha_1, \ldots, \alpha_k)^* = q(\alpha_1, \ldots, \alpha_k)$*; and*

(D) $\mathbf{Con\, A}$ *is modular.*

Proof. Since the operations $\cap$, $\vee$, and $\circ$ are monotone, an easy induction on the length of p shows part (A). Since * is isotone, $p_{2,2}(\alpha_1, \ldots, \alpha_k)^* \subseteq p_2(\alpha_1, \ldots, \alpha_k)^* \subseteq p(\alpha_1, \ldots, \alpha_k)^*$ follows from (A). Hence, to prove (B), it suffices to show that

$$p_{2,2}(\alpha_1, \ldots, \alpha_k)^* \supseteq p(\alpha_1, \ldots, \alpha_k)^*. \tag{1}$$

This will be done via induction on the length of p.

First of all notice that $p_{2,2}(\alpha_1, \ldots, \alpha_k)$ is always a tolerance of $\mathbf{A}$; this follows via induction on the length of p. Now (1) is evident when p is a variable. Suppose that $p = r \cap s$ (and (1) holds for r and s). Then, with the notation $\vec{\alpha} = (\alpha_1, \ldots, \alpha_k)$ and using TIP (indicated by $\overset{\text{TIP}}{=}$) and the induction hypothesis (indicated by $\supseteq_{ind}$) we have

$$p_{2,2}(\vec{\alpha})^* = \big(r_{2,2}(\vec{\alpha}) \cap s_{2,2}(\vec{\alpha})\big)^* = \big(r_{2,2}(\vec{\alpha}) \cap s_{2,2}(\vec{\alpha})\big)^{**} \overset{\text{TIP}}{=}$$
$$\big(r_{2,2}(\vec{\alpha})^* \cap s_{2,2}(\vec{\alpha})^*\big)^* \supseteq_{ind} \big(r(\vec{\alpha})^* \cap s(\vec{\alpha})^*\big)^* \supseteq$$
$$\big(r(\vec{\alpha}) \cap s(\vec{\alpha})\big)^* = p(\vec{\alpha})^*,$$

indeed. Now suppose that $p = r \circ s$. Then

$$p_{2,2}(\vec{\alpha})^{\,*} = \Big(\big(r_{2,2}(\vec{\alpha}) \circ s_{2,2}(\vec{\alpha})\big) \cap \big(s_{2,2}(\vec{\alpha}) \circ r_{2,2}(\vec{\alpha})\big)\Big)^{\,*} \supseteq$$
$$\big(r_{2,2}(\vec{\alpha}) \cup s_{2,2}(\vec{\alpha})\big)^{\,*} = r_{2,2}(\vec{\alpha})^{\,*} \vee s_{2,2}(\vec{\alpha})^{\,*} \supseteq_{ind}$$
$$r(\vec{\alpha})^{\,*} \vee s(\vec{\alpha})^{\,*} = \big(r(\vec{\alpha}) \circ s(\vec{\alpha})\big)^{\,*} = p(\vec{\alpha})^{\,*},$$

indeed. Finally, if $p = r \vee s$, then

$$p_{2,2}(\vec{\alpha})^{\,*} = \Big(\big(r_{2,2}(\vec{\alpha}) \circ s_{2,2}(\vec{\alpha})\big) \cap \big(s_{2,2}(\vec{\alpha}) \circ r_{2,2}(\vec{\alpha})\big)\Big)^{\,*} \supseteq$$
$$\big(r_{2,2}(\vec{\alpha}) \cup s_{2,2}(\vec{\alpha})\big)^{\,*} = r_{2,2}(\vec{\alpha})^{\,*} \vee s_{2,2}(\vec{\alpha})^{\,*} \supseteq_{ind}$$
$$r(\vec{\alpha})^{\,*} \vee s(\vec{\alpha})^{\,*} = \big(r(\vec{\alpha}) \vee s(\vec{\alpha})\big)^{\,*} = p(\vec{\alpha})^{\,*}.$$

This proves (1) and part (B) of the lemma.

Since $q(\alpha_1, \ldots, \alpha_k)$ is a congruence, it equals its transitive closure and (C) becomes a particular case of (B).

Now, to prove (D), let $\alpha, \beta, \gamma \in \mathbf{Con\,A}$ with $\alpha \subseteq \gamma$ and consider the lattice terms $p(\alpha_1, \alpha_2, \alpha_3) = (\alpha_1 \vee \alpha_2) \wedge \alpha_3$ and $q(\alpha_1, \alpha_2, \alpha_3) = \alpha_1 \vee (\alpha_2 \wedge \alpha_3)$. We have to show that $p(\alpha, \beta, \gamma) \subseteq q(\alpha, \beta, \gamma)$. Let $(x, y) \in p_2(\alpha, \beta, \gamma) = (\alpha \circ \beta) \cap \gamma$. Then $(x, y) \in \gamma$ and there is a $z \in A$ such that $(x, z) \in \alpha$, $(z, y) \in \beta$. Since $\alpha \subseteq \gamma$, $(x, z) \in \gamma$ and $(z, y) \in \gamma$ by transitivity. So $(z, y) \in \beta \cap \gamma$ and we obtain $(x, y) \in \alpha \circ (\beta \cap \gamma) = q_2(\alpha, \beta, \gamma)$. This shows that $p_2(\alpha, \beta, \gamma) \subseteq q_2(\alpha, \beta, \gamma)$. Hence (C) applies and we conclude $p(\alpha, \beta, \gamma) = p_2(\alpha, \beta, \gamma)^{\,*} \subseteq q_2(\alpha, \beta, \gamma)^{\,*} = q(\alpha, \beta, \gamma)$, the modular law.
Lemma 7.1 is proved.

□

Part (D) of Lemma 7.1, first proved by Kearnes [Ke2], says that TIP is a stronger property than congruence modularity. It is properly stronger, for [CzH2], right before Proposition 1, gives an example of a three element (therefore congruence modular) monounary algebra which fails TIP. However, part (D) of Lemma 7.1 together with Theorem 7.2 imply the following statement, which is worth separate formulating even if it has been known for a while.

THEOREM 7.3 ([CHR], [CzH3], [Ke2], [CHL]). *Let $\mathcal{V}$ be a variety of algebras. Then $\mathcal{V}$ satisfies the tolerance intersection property if and only if $\mathcal{V}$ is congruence modular.*

The way we proved part (D) of Lemma 7.1 leads to the following more general statement, which we formulate for later reference.

Corollary 7.1 ([CHL]). *Let* $\mathbf{A}$ *be an algebra satisfying TIP, let* $p = p(x_1, \ldots, x_k)$ *be a* $\{\cap, \vee, \circ\}$*-term and let* $q = q(x_1, \ldots, x_k)$ *be a lattice term. Then the following conditions are equivalent.*

(a) $p \subseteq q$ *holds for congruences of* $\mathbf{A}$*,*

(b) $p_2 \subseteq q$ *holds for congruences of* $\mathbf{A}$*,*

(c) $p_{2,2} \subseteq q$ *holds for congruences of* $\mathbf{A}$*.*

Proof. According to Lemma 7.1 (A), (a) implies (b) and (b) implies (c). Now suppose (c). Then, in virtue of Lemma 7.1(B) we obtain

$$q(\vec{\alpha}) = q(\vec{\alpha})^* \supseteq p_{2,2}(\vec{\alpha})^* = p(\vec{\alpha})^* \supseteq p(\vec{\alpha}).$$

This shows that (c) implies (a).
Corollary 7.1 is proved.

□

Given two $\{\cap, \vee, \circ\}$-terms, $p = p(x_1, \ldots, x_k)$ and $q = q(x_1, \ldots, x_k)$, we say that the *congruence inclusion formula* $p \subseteq q$ holds in a variety $\mathcal{V}$ (or, in other words, $p \subseteq q$ *holds for congruences* of $\mathcal{V}$) if for any algebra $\mathbf{A} \in \mathcal{V}$ and for any congruences $\alpha_1, \ldots, \alpha_k$ of $\mathbf{A}$ we have $p(\alpha_1, \ldots, \alpha_k) \subseteq q(\alpha_1, \ldots, \alpha_k)$ in $\mathrm{Rel}\,_r(\mathbf{A})$. When both p and q are join-free, i.e. they are $\{\cap, \circ\}$-terms, then Wille ([Wi]) and Pixley ([Pix]) gives an algorithm to construct a strong Maltsev condition $M(p \subseteq q)$ such that, for any variety $\mathcal{V}$, the congruence inclusion formula $p \subseteq q$ holds in $\mathcal{V}$ if and only if $M(p \subseteq q)$ holds in $\mathcal{V}$. We do not give the details of the Wille–Pixley algorithm here, for it is also available from several secondary sources; for example from [HC] or from Chapter XIII of Freese and McKenzie ([FM]). Notice that for an arbitrary lattice identity $p \leq q$ Wille and Pixley show that this identity holds in all congruence lattices of $\mathcal{V}$ iff $\mathcal{V}$ satisfies the weak Maltsev condition $(\forall m \geq 2)\,(\exists n \geq n)\,\big(M(p_m \subseteq q_n)\big)$.

Now we formulate one of our main results.

THEOREM 7.4 ([CHL]). *Let* $p \subseteq q$ *be a congruence inclusion formula with* q *being* $\circ$*-free. (I.e.* p *is a* $\{\cap, \vee, \circ\}$*-term and* q *is a lattice term.) Then for any congruence modular variety* $\mathcal{V}$ *the following conditions are equivalent.*

(i) $p \subseteq q$ *holds for congruences of* $\mathcal{V}$*,*

(ii) $p_2 \subseteq q$ *holds for congruences of* $\mathcal{V}$*,*

(iii) $p_{2,2} \subseteq q$ *holds for congruences of* $\mathcal{V}$*,*

(iv) the Maltsev condition

$$(\exists n \geq 2)\,\big(M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)\big)$$

(where $q_2 \circ q_2 \circ \cdots \circ q_2$ *denotes a product of* n *factors) holds in* $\mathcal{V}$*.*

Proof. In virtue of Theorem 7.3 the algebras in $\mathcal{V}$ satisfy TIP. Hence the equivalence of (i), (ii) and (iii) follows from Corollary 7.1.

If (iv) holds, then applying Wille and Pixley's result to the strong Maltsev condition $M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)$ we obtain that $p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2$ (with n factors) holds for congruences of $\mathcal{V}$ for some n. But, using Lemma 7.1 (C), $q_2 \circ q_2 \circ \cdots \circ q_2 \subseteq {q_2}^* = q$, so the congruence inclusion formula $p_2 \subseteq q$ holds in $\mathcal{V}$. This shows that (iv) implies (ii).

Now let (ii) hold and suppose the reader has some basic idea how Wille and Pixley's proof works for lattice identities. What we have to know from their proof is the following. Associated with p_2 we construct a finitely generated free algebra $\mathbf{F}$ in $\mathcal{V}$ with distinguished free generators x_0 and x_1. Also, we construct finitely generated congruences $\alpha_1, \ldots, \alpha_k$ of $\mathbf{F}$ such that $(x_0, x_1) \in p_2(\alpha_1, \ldots, \alpha_k)$. Let $\vec{\alpha}$ stand for $(\alpha_1, \ldots, \alpha_k)$. Since $p_2(\vec{\alpha}) \subseteq q(\vec{\alpha})$, $(x_0, x_1) \in q(\vec{\alpha})$. Now $q(\vec{\alpha}) = q_2(\vec{\alpha})^*$ by Lemma 7.1 (C), so there is an integer $n \geq 2$ such that $(x_0, x_1) \in q_2(\vec{\alpha}) \circ \cdots \circ q_2(\vec{\alpha})$ (with n factors). And this is the formula from which Wille and Pixley conclude that $M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)$ holds in $\mathcal{V}$. We have shown that (ii) implies (iv). Theorem 7.4 is proved.

□

The following corollary is worth formulating:

Corollary 7.2 ([CHL]). *Let* $p \leq q$ *be a lattice identity which implies modularity in congruence varieties. Then, for an arbitrary variety* $\mathcal{V}$*,* $p \leq q$ *holds for congruences of* $\mathcal{V}$ *iff* $M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)$ *holds in* $\mathcal{V}$ *for some* $n \geq 2$ *and* $\mathcal{V}$ *has Day terms.*

Now we recall a nice result from Lipparini ([CHL]). Given a lattice term q, let $q_{[d]}$ stand for its "disjunctive normal form", which is computed by distributing meets over joins everywhere as if we were in a distributive lattice, so $q_{[d]}$ is a join of meets of variables. The precise formal definition and the simultaneous proof that $q_{[d]}$ is a join of meets of variables go via induction on the length of q as follows.

Let $q_{[d]} = q$ when q is a variable. If $q = r \vee s$, then let $q_{[d]} = r_{[d]} \vee s_{[d]}$. Finally, if $q = r \wedge s$, then $r_{[d]} = \bigvee_{i \in I} a_i$ and $s_{[d]} = \bigvee_{j \in J} b_j$ with the a_i and b_j being meets of variables, and we let $q_{[d]} = \bigvee_{i \in I,\ j \in J} (a_i \wedge b_j)$. Now Lipparini ([CHL]) proved that (i) of Theorem 7.4 is equivalent to

(v) the Maltsev condition

$$(\exists n \geq 2) \left(M(p_2 \subseteq q_{[d]2} \circ \cdots \circ q_{[d]2} \circ q_2)\right)$$

(where $q_{[d]2} \circ \cdots \circ q_{[d]2}$ denotes a product of $n-1$ factors) holds in $\mathcal{V}$.

We conclude this chapter and the dissertation with the following remarks. The spirit of Wille and Pixley's theorem says that part (iv) of Theorem 7.4 can be replaced with the Maltsev condition $(\exists n \geq 2) \left(M(p_2 \subseteq q_n)\right)$. However, (iv) and (v) are simpler conditions. In fact, no known Maltsev conditions for lattice identities are simpler than those supplied by (iv) and/or (v). Sometimes (iii) is the best to use: indeed, $p_{2,2} \subseteq p_2$ indicates that, for a given variety $\mathcal{V}$, it is easier to show (iii) than (ii).

REFERENCES

[ABGG] N. N. Aizenberg, A. A. Bovdi, E. I. Gergo, F. E. Geche: Algebraic aspects of threshold logic, *Kibernetica (Kiev)*, **2** (1980), 26–30.

[B] H. -J. Bandelt: Tolerance relations on lattices, *Bull. Austral Math Soc.,*, **23** (1981), 367–381.

[BP] K. A. Baker, A. F. Pixley: Polynomial interpolation and the Chinese Remainder theorem for Algebraic Systems, *Matematische Zeitscrift*, **143** (1975), 165–174.

[BKKR] V. G. Bodnarčuk, L. A. Kalužnin, V. N. Kotov, B. A. Romov: Galois theory for Post algebras, I–II (Russian), *Kibernetika*, **5** (1969), 1–10; 1–9..

[Ch] I. Chajda: *Algebraic theory of tolerance relations*, Univerzita Palackého Olomouc, Olomouc, 1991.

[CC] I. Chajda, G. Czédli: A note on representation of lattices by tolerances, *J. Algebra*, **148** (1992), 274–275.

[CCH1] I. Chajda, G. Czédli, E. K. Horváth.: Trapezoid lemma and congruence distributivity, *Math Slovaca*, **53** (2003), No.3, 247–253.

[CCH2] I. Chajda, G. Czédli, E. K. Horváth: The shifting lemma and shifting lattice identities, *Algebra Universalis*, **50** (2003), 51–60.

[CEL] I. Chajda, G. Eigenthaler and H. Länger: *Congruence classes in universal algebra*, Memoirs of the Amer. Math. Soc.. **286** (1983)

[CG] I. Chajda, K. Glazek: *A Basic Course on Algebra*, Technical University Press, Zielona Góra, Poland. (2000)

[ChH1] I. Chajda, E. K. Horváth: A triangular scheme for congeruence distributivity, *Acta Sci. Math. (Szeged)*, **68** (2002), 29–35.

[ChH2] I. Chajda, E. K. Horváth: A scheme for congruence semidistributivity, *Discussiones Mathematicae, General Algebra and Applications*, **23** (2003), 13–18.

[CST] I. Chajda, B. Šešelja, A. Tepavčevič: A Note on Triangular schemes for Weak Congruences, *preprint*, 2004..

[CR] I. Chajda, S. Radeleczki: 0-conditions and tolerance schemes, *Acta Math. Univ. Comenianae*, **XXII, 2** (2003), 177–184.

[CF] M. Couceiro, S. Földes: On closed sets of relational constraints and classes of functions closed under variable substitutions, *Rutcor Research Report*, March, 2004.

[CrD] P. Crawley, R. P. Dilworth: *Algebraic theory of lattices*, Prentice-Hall Inc., New Jersey, 1973.

[Cs1] B. Csákány: Homogeneous algebras are functionally complete, *Algebra Universalis*, **11** (1980), 149–158.

[Cs2] Csákány B.: *Függelék Burris-Sankappanavar Bevezetés az univerzális algebrába c. könyv magyar nyelvű kiadásához*, Tankönyvkiadó, Budapest, 1988.

[Cz1] Czédli G.: *Boole függvények*, Polygon, Szeged, 1995.

[Cz2] Czédli G.: *Hálóelmélet*, JATEPress, Szeged, 1999.

[Cz3] G. Czédli: Weak congruence semidistributivity laws and their conjugates, *Acta Math Univ. Comenian.*, **68** (1999), 153–170.

[Cz4] G. Czédli: Factor lattices by tolerances, *Acta Sci. Math. (Szeged)*, **44** (1982), 35–42.

[CzD] G. Czédli, A. Day: Horn sentences with (W) and weak Mal'cev conditions, *Algebra Universalis*, **19** (1984), 217–253.

[CzFr] G. Czédli, R. Freese: On congruence distributivity and modularity, *Algebra Universalis*, **17** (1983), 216–219.

[CzH1] G. Czédli, E. K. Horváth: Reflexive relations and Mal'tsev conditions for congruence lattice identities in modular varieties, *Acta Univ. Palacki Olomouc., Fac. rer. nat., Mathematica*, **41** (2002), 43–53.

[CzH2] G. Czédli, E. K. Horváth: Congruence distributivity and modularity permit tolerances, *Acta Univ. Palacki. Olomouc., Fac.rer.nat., Mathematica*, **41** (2002), 39–42.

[CzH3] G. Czedli, E. K. Horváth: All congruence lattice identities implying modularity have Malt'sev conditions, *Algebra Universalis*, **50** (2003), 69–74.

[CHR] G. Czédli, E. K. Horváth, S. Radeleczki: On tolerance lattices of algebras in congruence mudular varieties, *Acta Math. Hungar.*, **100 (1–2)** (2003), 9–17.

[CHL] G. Czédli, E. K. Horváth, P. Lipparini: Optimal Mal'tsev conditions for congruence modular varieties, *Algebra Universalis*, to appear.

[Da1] A. Day: A characterization of modularity for congruence lattices of algebras, *Canad. Math. Bull.*, **12** (1969), 167–173.

[Da2] A. Day: p-modularity implies modularity in equational classes, *Algebra Universalis*, **3** (1973), 398–399.

[DF] A. Day, R. Freese: A characterization of identities implying congruence modularity I., *Canad. J. Math.*, **32** (1980), 1140–1167.

[Du1] J. Duda: The Upright Principle for congrunce distributive varieties., *Abstract of seminar lecture presented in Brno*, (2000), March.

[Du2] J. Duda: The Triangular Principle for congruence distributive varieties, *Unpublished abstract*, (2000), March.

[Fo] A. L. Foster: An existence theorem for functionally complete universal algebras, *Math Z.*, **71** (1959), 69–82.

[FH] G. Fraser, A. Horn: Congruence relations in direct products, *Proc. Amer. Math. Soc.*, **26** (1970), 390–394.

[Fr] R. Freese: Finitely based modular congruence varieties are distributive, *Algebra Universalis*, **32** (1994), 104–114.

[FJ] R. Freese, B. Jónsson: Congruence modularity implies the Arguesian identity, *Algebra Universalis*, **6** (1976), 225–228.

[FM] R. Freese, R. McKenzie: *Commutator theory for congruence modular varieties*, Cambridge Univ. Press, Cambridge, 1987.

[FP] E. Fried, A. F. Pixley: The dual discriminator function in universal algebra, *Acta Sci. Math. (Szeged)*, **41.** (1979), 83–100

[Ged1] E. Gedeonova: Jordan-Hölder theorem for lines, *Mat. Časopis Sloven. Akad. Vied.*, **22.** (1972), 177–198

[Ged2] E. Gedeonová: A characterization of p-modularity for congruence lattices of algebras, *Acta Fac. Rerum Natur. Univ Comenian. Math Publ.*, **28** (1972), 99–106.

[Gei] D. Geiger: Closed systems of functions and predicates, *Pacific J. Math.*, **27** (1968), 95–100.

[Gey] W. Geyer: Generalizing semidistributivity, *Order*, **10** (1993), 77–92.

[Gu1] H.-P. Gumm: *Geometrical methods in congruence modular algebras*, Memoirs of the Amer. Math. Soc.. **45** (1983)

[Gu2] H.-P. Gumm: Congruence modularity is permutability composed with distributivity, *Arch. Math. (Basel)*, **36** (1981), 569–576.

[Gr1] G. Gratzer: Two Mal'cev-type theorems in universal algebra , *J. Combinatorial Theory* , **8** (1970), 334–342.

[Gr2] G. Grätzer: *Universal algebra*, Springer-Verlag, New York–Heidelberg, 1979.

[GL] G. Grätzer, W. A. Lampe: Characterisations of congruence lattices of abstract algebras, *J. Algebra*, **7** (1967), 263–270.

[GS] G. Grätzer, E. T. Schmidt: Characterisations of congruence lattices of abstract algebras, *Acta Sci. Math.*, **24** (1963), 34–59.

[H] M. Haiman: Arguesian lattices which are not type-1., *Algebra Universalis*, **28** (1991), 128–137.

[Ho1] E. K. Horváth: Invariance groups of threshold functions, *Acta Cybernetica.*, **11** (1994), 325–332.

[Ho2] E. K. Horváth: The Słupecki criterion by duality, *Discussiones Mathematicae (General Algebra and Applications.*, **21** (2001), 5–10.

[Hu1] A. P. Huhn: Schwach distributive Verbände I, *Acta Sci. Math. (Szeged)*, **33** (1972), 297–305.

[Hu2] A. P. Huhn: On Grätzer's problem concerning automorphisms of a finitely presented lattice, *Algebra Universalis.*, **5** (1975), 65–71.

[HC] G. Hutchinson, G. Czedli: A test for identities satisfied in lattices of submodules, *Algebra Universalis* , **8** (1978), 269–309.

[I] Th. Ihringer: *Allgemeine Algebra*, Teubner-Verlag, Stuttgart, 1993.

[JL] S. W. Jablonski, O. B. Lupanow: *Diskrete Mathematik und mathematische Fragen*, Akademie–Verlag Berlin, 1980.

[J1] B. Jónsson: Algebras whose congruence lattices are distributive, *Math. Scand.*, Polygon. **21** (1967), 110–121

[J2] B. Jónsson: Congruence varieties, *Algebra Universalis*, **10** (1980), 355–394.

[Ka] Kalmárné Németh Márta: Volt-e választási lehetősége Conwaynak?, *Polygon*, **2** (1972), 62–67.

[Ke1] K. A. Kearnes: Personal communication, , .

[Ke2] K. A. Kearnes: Communication via e-mails, *(2001)*, .

[KSz] K. A. Kearnes, Á. Szendrei: The relationship between two commutators, *Internat. J. Algebra Comput.*, **8** (1998), 497–53.

[Kra1] P. H. Krauss: On primal algebras, *Algebra Universalis*, **I.X.** (1999), 37–46.

[Kra2] P. H. Krauss: On quasi primal algebras, *Math Z.*, **134** (1973), 85–89.

[L1] P. Lipparini: Characterization of varieties with a difference term, II.: neutral=meet semidistributive, *Canadian Math Bull.*, **41** (1988), 318–327.

[L2] P. Lipparini: Commutator theory without join-distributivity, *Trans. Amer. Math. Soc.*, **346** (1994), 177–202.

[L3] P. Lipparini: congruence modularity implies the Arguesian law for single algebras with a difference term, *J. Algebra*, **219** (1999), 658–681.

[Ma] A. I. Mal'tsev: On the general theory of algebraic systems (Russian), *Mat. Sb. (N. S.)*, **35 (77)** (1954), 3–20.

[Mc] R. McKenzie: Equational bases and non-modular lattice varieties, *Trans. Amer. Math. Soc.*, **174** (1972), 1–43.

[Me] P. Mederly: Three Mal'cev type theorems and their application, *Mat. Casopis Sloven. Akad. Vied* , **25** (1975), 83–95.

[Mu] S. Muroga: *Threshold logic and its applications*, WILEY-INTERSCIENCE, a Division of John Wiley & sons, Inc. New York * London * Sydney * Toronto, 1971.

[Na] G. B. Nation: Varieties whose congruences satisfy certain lattice identities, *Algebra Universalis*, **4** (1974), 78–88.

[Ne] W. D. Neumann: On Malcev conditions, *J. Austral. Math. Soc.*, **17** (1974), 376–384.

[PSz] P. P. Pálfy, Cs. Szabó: An identity for subgroup lattices of abelian group, *Algebra Universalis*, **33.** (1995), 191–195

[Pip] N. Pippenger: Galois theory for minors of finite functions, *Discrete Mathematics*, **254** (2002), 405–419.

[Pix] A. F. Pixley: Local Malcev conditions, *Canad. Math. Bull.*, **15** (1972), 559–568.

[PK] R. Pöschel, L. A. Kalushnin: *Funktionen- und Relationenalgebren*, Verlag der Wissenschaften, Berlin, 1979.

[RS] S. Radeleczki, D. Schweigert: Lattices with complemented tolerance lattice, *Czech.Math.J.*, in print..

[RRS] J. G. Raftery, I. G. Rosenberg, T. Sturm: Tolerance relations and BCK-algebras, *Math. Japon.*, **36** (1991), 399–410.

[S] M. Saarimäki: Disjointness of lattice elements, *Math. Nachr.*,, **159** (1992), 169–174.

[Sch] E. T. Schmidt: *A survey of congruence lattice representation*, Teubner Texts in Mathematics 42, B. G. Teubner (Leipzig, 1982)..

[Sh] Ching Lai Sheng: *Threshold logic (H. G. Booker and N. DeClaris, eds.*, Academic Press, London and New York, 1969..

[Si] W. Sierpiński: Sur les fonctions de plusieurs variables, *Fund. Math.*, **33** (1945), 169–173.

[Sl] J. Słupecki: Completeness criterion for systems of many-valued propositional calculus (in Polish), *C. R. des Séances de la Societé des Sciences et des Lettres de Varsovie Cl. II*, **32** (1939), 102–109.

[Sn] J. W. Snow: Mal'tsev conditions and relations on algebras, *Algebra Universalis*, **42** (1999), 299–309.

[St] M. Stern: *Semimodular lattices, Theory and applications*, Cambridge-New York-Melbourne, 1999.

[Sz] Á. Szendrei: *Clones in Universal Algebra*, Université de Montréal, 1986.

[T] W. Taylor: Characterizing Mal'cev conditions, *Algebra Universalis*, **3** (1973), 351–397.

[Wer1] H. Werner: *Discriminator–Algebras*, Akademie–Verlag, Berlin, 1978.

[Wer2] H. Werner: Eine Characterisierung funktional vollstandiger Algebren, *Arch. Math. (Basel)*, **21** (1970), 381–385.

[Wi] R. Wille: *Kongruenzklassengeometrien*, Springer–Verlag, Berlin-New York, 1970.

[Wo] S. Wolfram: *Theory and applications of cellular automata*, World Scientific, Singapore, 1986.

[Wn] B. Wnuk: On symmetry groups of algebraic operations. (Polish. English summary.), *Zeszty Nauk. Wyz. Szkoly. Ped. w Opolu Mat.*, **21** (1980).

[YI] S. Yajima and T. Ibaraki,: A lower bound of the number of threshold functions, *Trans. IEE, EC-14*, **6** (1965), 926-929..

[Inv1] http://en.wikipedia.org/wiki/Invariants

[Inv2] http://en.wikipedia.org/wiki/Invariant_theory

[Inv3] http://www-gap.dcs.st-and.ac.uk/ history/Mathematicians/Klein.html

[Inv4] http://www-gap.dcs.st-and.ac.uk/ history/HistTop

SUMMARY

1. Introduction

Lattices are very important related algebraic structures. They often appear in many branches of algebra, they are clear enough to consider easily, and rich enough to characterize many types of algebraic properties. Here lattices occur in connection with diagrammatic schemes and Maltsev conditions. Moreover, we carry out lattice theoretic investigations on the shift of a lattice identity.

Traditionally in mathematics: " An **invariant** is something that does not change under a set of transformations. The property of being an invariant is **invariance.** "(Wikipedia [Inv1].)

However, beside its strict meaning outlined above, the word 'invariant' has also a more general meaning in universal algebra. We obtain this meaning by replacing transformation, which is a selfmap $A \to A$ of a set A by the notion of algebraic operations. Thus we arrive at the notion of an **invariant relation** ([PK]).

2. Invariance groups of threshold functions

A *threshold function* is a Boolean function, i.e. a mapping $\{0,1\}^n \to \{0,1\}$ with the following property: There exist real numbers $w_1, ..., w_n$, t such that

$$f(x_1, \ldots, x_n) = 1 \text{ iff } \sum_{i=1}^{n} w_i x_i \geq t,$$

where w_i is called the *weight* of x_i for $i = 1, 2, \ldots, n$, and t is a constant called the *threshold value.*

THEOREM 2.1 ([Ho1]). *For every n-ary threshold function f there exists a partition C_f of $\mathbf{n}$ such that the invariance group G of f consists exactly of those permutations of S_n which preserve each block of C_f. Conversely, for every partition C of $\mathbf{n}$ there exists a threshold function f_C such that the invariance group G of f_C consists exactly of those permutations of S_n that preserve each block of C.*

The proof contains only elementary considerations.

Corollary 2.1([Ho1]). *The invariance group of any threshold function is isomorphic to a direct product of symmetric groups.*

3. Proving primality by the operation-relation duality

We consider a k-ary relation as a set of unary functions $r\colon \mathbf{k} \to A$, $\mathbf{k} = \{1, 2, \ldots, k\}$. We say that a k-ary relation D is *diagonal,* if there exists an equivalence relation ρ_D on $\mathbf{k}$ such that

$$D = \{r\colon \mathbf{k} \to A \mid r(u) = r(v) \text{ if } u \rho_D v,\ u, v \in \mathbf{k}\}.$$

The collection of all diagonal relations on A forms the minimal closed class of relations on A.

The following Proposition 3.1 and Lemma 3.1 and Lemma 3.1' enable us to new proofs for primality theorems. This will be demonstrated in case of Słupecki's theorem.

Proposition 3.1 (Bodnarčuk–Kalužnin–Kotov–Romov [BKKR], Geiger [Gei], Krauss [Kr1],[Kr2]). *A finite algebra* $\mathbf{A} = (A, F)$ *is primal, iff every relation preserved by all operations in* F *is diagonal.*

Lemma 3.1 ([Ho2]). *Given an algebra* $\mathbf{A} = (A, F)$*, the following two conditions are equivalent:*

(i) For each $R \subseteq A^k$*, the relation* $[R]$ *is diagonal.*

(ii) For each $x, y \in A^k$*, the relation* $[x, y]$ *is diagonal.*

Lemma 3.1′ ([Ho2]). *The following three conditions are equivalent:*

(i) The algebra $\mathbf{A} = (A, F)$ *is primal.*

(ii) For each $x, y, z \in A^k$*, we have* $z \in [x, y]$ *whenever*

$$((\forall u, v \in \mathbf{k})(x(u) = x(v) \wedge y(u) = y(v) \rightarrow z(u) = z(v))).$$

(iii) For each $k \geq 1$ $x, y, z \in A^k$*, and for any equivalence* ρ *on* $\mathbf{k}$ *if* $\rho \supseteq \rho_x \cap \rho_y$*, then* $D_\rho \subseteq [x, y]$.

4. Diagrammatic schemes

Motivated by Gumm's Shifting Lemma ([Gu1]), which asserts that congruence modular varieties satisfy a nice rectangular congruence scheme, Chajda ([ChH1], Subdivision 4.2) investigated a triangular scheme, which is a consequence of congruence distributivity. Congruence distributive varieties satisfy this scheme not only for arbitrary three congruences, but also for one tolerance and two congruences; i.e., the analogue of Gumm's Shifting Principle is valid. While the triangular scheme is not known to characterize congruence distributivity, an appropriate generalization called trapezoid scheme does ([CCH2], Subdivision 4.3). These examples show that instead of identities in congruence lattices, diagrammatic statements are reasonable to consider. This phenomenon can be extended to lattice Horn sentences as well.

5. Shifting lattice identities

Let

$$\lambda : \quad p(x_1, \ldots, x_n) \leq q(x_1, \ldots, x_n)$$

be a lattice identity. (Notice that by a lattice identity we always mean an inequality, i.e. we use $\leq$ but never $=$.) If y is a variable, then let $S(\lambda, y)$ denote the Horn sentence

$$q(x_1,\dots,x_n) \le y \Longrightarrow p(x_1,\dots,x_n) \le y.$$

If $y \notin \{x_1,\dots,x_n\}$, then λ is clearly equivalent to $S(\lambda, y)$. However, we are interested in the case when $y \in \{x_1,\dots,x_n\}$, say $y = x_i$ $(1 \le i \le n)$. Then $S(\lambda, x_i)$ is a consequence of λ. When $S(\lambda, x_i)$ happens to be equivalent to λ, then $S(\lambda, x_i)$ will be called *a shift of* λ. If $S(\lambda, x_i)$ is equivalent to λ only within a lattice variety $\mathcal{V}$, then we say that $S(\lambda, x_i)$ *is a shift of* λ *in* $\mathcal{V}$. In this chapter some known lattice identities will be shown to have a shift while some others have no shift.

6. Tolerances and tolerance lattices

Let dist(x, y, z) resp. mod(x, y, z) denote the distributive law $x \wedge (y \vee z) \le (x \wedge y) \vee (x \wedge z)$ resp. the modular law $x \wedge (y \vee (x \wedge z)) \le (x \wedge y) \vee (x \wedge z)$. For an algebra $\mathbf{A}$, the *set* of tolerances and the *lattice* of congruences of $\mathbf{A}$ will be denoted by $\mathbf{Tol\,A}$ and $\mathbf{Con\,A}$, respectively. We say that dist(tol,tol,tol) holds in $\mathbf{A}$ if $\Gamma \wedge (\Phi \vee \Psi) \subseteq (\Gamma \wedge \Phi) \vee (\Gamma \wedge \Psi)$ is valid for any $\Gamma, \Phi, \Psi \in \mathbf{Tol\,A}$, where the meet resp. the join is the intersection resp. the transitive closure of the union. The meaning of mod(tol,tol,tol) is analogous. We should emphasize here that $\Phi \vee \Psi$ is **not** the join in $\mathbf{Tol\,A}$, the lattice of tolerance relations of $\mathbf{A}$. With the help of Jónsson terms ([J1]) we proved the next theorem:

THEOREM 6.1 ([CzH2]). *If $\mathcal{V}$ is a congruence distributive resp. congruence modular variety, then dist(tol,tol,tol) resp. mod(tol,tol,tol) holds in all algebras of $\mathcal{V}$.*

Two important consequences are formulated in Corollary 6.1 and Proposition 6.1.

Corollary 6.1 (Gumm [Gu1]). *If $\mathcal{V}$ is a congruence modular variety, then it satisfies Gumm's Shifting Principle, i.e. for any $\mathbf{A} \in \mathcal{V}$, $\alpha, \gamma \in \mathbf{Con\,A}$ and $\Phi \in \mathbf{Tol\,A}$ if $(x, y), (u, v) \in \alpha$, $(x, u), (y, v) \in \Phi$, $(u, v) \in \gamma$ and $\alpha \cap \Phi \subseteq \gamma$, then $(x, y) \in \gamma$.*

Denoting the transitive closure by *, the following proposition is an essential step towards the Maltsev conditions in Chapter 7:

Proposition 6.1 ([CzH2]). *If mod(tol,tol,tol) or dist(tol,tol,tol) holds in an algebra $\mathbf{A}$, then $\Gamma \cap \Phi^* \subseteq (\Gamma \cap \Phi)^*$ for any $\Gamma, \Phi \in \mathbf{Tol\,A}$.*

A lattice $\mathbf{L}$ with 0 is called *0-modular,* cf. Stern ([St]), if there is no N_5 sublattice of $\mathbf{L}$ including 0. The lattice $\mathbf{L}$ with 0 satisfies the *general disjointness property* (GD) if $a \wedge b = 0$ and $(a \vee b) \wedge c = 0$ imply $a \wedge (b \vee c) = 0$. If for each $a \in \mathbf{L}$ the set $\{x \in \mathbf{L} : \mathrm{a} \wedge \mathrm{x} = 0\}$ has greatest element, then $\mathbf{L}$ is called a *pseudocomplemented* lattice.

The following Theorem 6.2 and 6.3 are the main results about tolerance lattices in congruence modular varieties.

THEOREM 6.2 ([CHR]). *Let* $\mathbf{A}$ *be an algebra in a congruence modular variety* $\mathcal{V}$*. Then the following statements hold:*

(i) The map h*:* $\mathbf{Tol\,A} \to \mathbf{Con\,A}$, $\Phi \mapsto \Phi^*$, *is a surjective lattice homomorphism and* $\mathbf{Tol\,A}$ *is a* 0-1 *modular lattice having the (GD) property.*

(ii) $\mathbf{Tol\,A}$ *is pseudocomplemented if and only if* $\mathbf{Con\,A}$ *is pseudocomplemented.*

THEOREM 6.3 ([CHR]). *Let* $\mathbf{A}$ *be an algebra. If* $\mathbf{A}$ *has a majority term, then:*

(i) $\mathbf{Tol\,A}$ *is a 0-modular pseudocomplemented lattice.*

(ii) The tolerances Γ, Φ *are complements of each other in* $\mathbf{Tol\,A}$ *if and only if they form a factor congruence pair of* A*.*

7. Maltsev conditions for congruence lattice identities in modular varieties

A *strong Maltsev condition* for varieties is a condition of the form "there exist terms $h_0, \ldots, h_k$ satisfying a set Σ of identities" where k is fixed and the form of Σ is independent of the type of algebras considered. By a *Maltsev condition* we mean a condition of the form "there exists a natural number n such that P_n holds" where the P_n are strong Maltsev conditions and P_n implies P_{n+1} for every n.

A celebrated result says that a variety $\mathcal{V}$ is congruence modular iff the Maltsev condition due to Day ([Da1]) "$(\exists n)(\mathbf{D}_n)$" holds in $\mathcal{V}$.

A lattice identity λ *is said to imply modularity in congruence varieties,* in notation $\lambda \models_c$ mod if for any variety $\mathcal{V}$ if all the congruence lattices $\mathbf{Con\,A}$, $\mathbf{A} \in \mathcal{V}$, satisfy λ, then all these lattices are modular. For example this is always the case when λ implies modularity in the usual lattice theoretic sense.

Given a lattice term p and $k \geq 2$, we define p_k via induction as follows. If p is a variable, then let $p_k = p$. If $p = r \wedge s$, then let $p_k = r_k \cap s_k$. Finally, if $p = r \vee s$, then let $p_k = r_k \circ s_k \circ r_k \circ s_k \circ \ldots$ with k factors on the right. When congruences or, more generally, reflexive compatible relations are substituted for the variables of p_k, then the operations $\cap$ and $\circ$ will be interpreted as intersection and relational product, respectively.

Our first result about Maltsev conditions is Theorem 7.1.

THEOREM 7.1 ([CzH3]). *Let* $\lambda : p \leq q$ *be a lattice identity such that* $\lambda \models_c$ *modularity. Then for any variety* $\mathcal{V}$ *the following two conditions are equivalent.*

(a) For all $\mathbf{A} \in \mathcal{V}$, *$\lambda$ holds in the congruence lattice of* $\mathbf{A}$.

(b) $\mathcal{V}$ *satisfies the Maltsev condition "there is an* $n \geq 2$ *such that* $M(p_3 \subseteq q_n)$ *and* $(\mathbf{D}_n)$ *hold".*

Next we improve Theorem 7.1 by giving the simplest (and in this sense hopefully the best) Maltsev condition associated with λ when $\lambda \models_c$ modularity.

For a term $p = p(x_1, \ldots, x_k)$ in the binary operations $\cap, \vee, \circ$, in short for a $\{\cap, \vee, \circ\}$-term, and for $n \geq 2$ we define two kinds of derived $\{\cap, \circ\}$-terms, p_n and $p_{2,2}$ via induction as follows. (When p happens to be a lattice term then p_n will be the same as before.) If p is a variable, then let $p_n = p_{2,2} = p$. If $p = r \cap s$, then let $p_n = r_n \cap s_n$ and $p_{2,2} = r_{2,2} \cap s_{2,2}$. Similarly, if $p = r \circ s$, then let $p_n = r_n \circ s_n$ and $p_{2,2} = (r_{2,2} \circ s_{2,2}) \cap (s_{2,2} \circ r_{2,2})$. Finally, if $p = r \vee s$, then let $p_n = r_n \circ s_n \circ r_n \circ s_n \circ \cdots$ with n factors on the right and $p_{2,2} = (r_{2,2} \circ s_{2,2}) \cap (s_{2,2} \circ r_{2,2})$.

THEOREM 7.4 ([CHL]). *Let* $p \subseteq q$ *be a congruence inclusion formula with* q *being* $\circ$*-free. (I.e.* p *is a* $\{\cap, \vee, \circ\}$*-term and* q *is a lattice term.) Then for any congruence modular variety* $\mathcal{V}$ *the following conditions are equivalent.*

(i) $p \subseteq q$ *holds for congruences of* $\mathcal{V}$,

(ii) $p_2 \subseteq q$ *holds for congruences of* $\mathcal{V}$,

(iii) $p_{2,2} \subseteq q$ *holds for congruences of* $\mathcal{V}$,

(iv) the Maltsev condition

$$(\exists n \geq 2) \left(M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2) \right)$$

(where $q_2 \circ q_2 \circ \cdots \circ q_2$ *denotes a product of* n *factors) holds in* $\mathcal{V}$.

As a corollary, we obtain the desired improvement of Theorem 7.1:

Corollary 7.2 ([CHL]). *Let* $\lambda : p \leq q$ *be a lattice identity such that* $\lambda \models_c$ *modularity. Then for any variety* $\mathcal{V}$ *the following three conditions are equivalent.*

(a) For all $\mathbf{A} \in \mathcal{V}$, *$\lambda$ holds in the congruence lattice of* $\mathbf{A}$.

(b') $\mathcal{V}$ *satisfies the Maltsev condition "there is an* $n \geq 2$ *such that* $M(p_2 \subseteq q_n)$ *and* $(\mathbf{D}_n)$ *hold".*

(c) $\mathcal{V}$ *satisfies the Maltsev condition "there is an* $n \geq 2$ *such that* $M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)$ *(with* n *factors) and and* $(\mathbf{D}_n)$ *hold".*

ÖSSZEFOGLALÓ

1. Bevezetés

A hálók nagyon fontos kísérőstruktúrák. Gyakran bukkannak fel az algebra különböző ágaiban. Egyszerűen áttekinthetők, de elég gazdagok ahhoz, hogy sokféle algebrai tulajdonságot jellemezzenek. Itt a hálók diagrammsémákkal és Malcev-feltételekkel kapcsolatban lépnek fel. Emellett hálóelméleti vizsgálatokat folytatunk a hálóazonosságok shiftjével kapcsolatban.

A matematikában hagyományosan az "**invariáns** valami olyan, ami változatlan marad transzformációk bizonyos halmazára nézve. Az 'invariánsnak lenni' tulajdonságot *invarianciának* nevezzük."(Wikipedia [Inv1].)

Az univerzális algebrában ezen szoros értelemben vett jelentésen túlmenően az 'invariáns' szó általánosabb jelentéssel is bír. Helyettesítsük a fent említett transzformációt (amely egy $A \to A$ leképezés, ahol A tetszőleges halmaz) az algebrai művelet fogalmával. Ily módon az **invariáns reláció** fogalmához érkezhetünk ([PK]).

2. Küszöbfüggvények invarianciacsoportja

Egy Boole-függvényt *küszöbfüggvénynek* nevezünk, ha alkalmas $w_1, ..., w_n$, t valós számokra

$$f(x_1, \ldots, x_n) = 1 \text{ akkor és csak akkor, ha} \sum_{i=1}^{n} w_i x_i \geq t.$$

Itt w_i-t az x_i változó *súlyának* ($i = 1, 2, \ldots, n$), a t-t pedig *küszöbértéknek* nevezzük.

2.1. TÉTEL ([Ho1]). *Bármely n változós f küszöbfüggvényhez létezik* $\mathbf{n}=\{1, 2, \ldots, n\}$*-nek olyan C_f osztályozása, hogy f invarianciacsoportja pontosan S_n azon permutációiból áll, amely C_f minden blokkját megőrzi. Megfordítva:* $\mathbf{n}$ *bármely C osztályozásához létezik olyan f_C küszöbfüggvény, hogy $C = C_{f_C}$.*

A bizonyítás csak elemi megfontolásokat tartalmaz.

2.1. Korollárium ([Ho1]). *Bármely küszöbfüggvény invarianciacsoportja szimmetrikus csoportok direkt szorzatával izomorf.*

3. Teljességi tételek bizonyítása függvény-reláció dualitás segítségével

Tekintsük a k változós relációkat egyváltozós r: $\mathbf{k} \to A$ ($\mathbf{k} = \{1, 2, \ldots, k\}$) függvények halmazának. Azt mondjuk, hogy egy k változós D reláció *diagonális,* ha létezik egy olyan ρ_D ekvivalenciareláció $\mathbf{k}$-n, hogy

$$D = \{r \colon \mathbf{k} \to A \mid r(u) = r(v), \text{ ha } u \rho_D v, \ u, v \in \mathbf{k}\}.$$

Az A-n definiálható diagonális relációk összessége alkotja a minimális relációklónt.

A következő 3.1 Állítás, valamint a 3.1 és a 3.1' Lemmák segítségével új bizonyítások adhatók ismert teljességi tételekre. Ezt Słupecki tételének új bizonyításával szemléltetjük.

3.1. Állítás (Bodnarčuk–Kalužnin–Kotov–Romov [BKKR], Geiger [Gei], Krauss [Kr1],[Kr2]). *Egy* $\mathbf{A} = (A, F)$ *algebra pontosan akkor primál, ha minden olyan reláció diagonális, amelyet minden* F*-beli reláció megőriz.*

3.1. Lemma ([Ho2]). *Adott* $\mathbf{A} = (A, F)$ *algebra esetén a következő két feltétel ekvivalens:*

(i) Bármely $R \subseteq A^k$ *esetén az* $[R]$ *reláció diagonális.*

(ii) Bármely $x, y \in A^k$ *esetén az* $[x, y]$ *reláció diagonális.*

3.1$'$. Lemma ([Ho2]). *A következő három állítás ekvivalens:*

(i) Az $\mathbf{A} = (A, F)$ *algebra primál.*

(ii) Bármely $x, y, z \in A^k$ *esetén* $z \in [x, y]$*, ha*

$$((\forall u, v \in \mathbf{k}\ )(x(u) = x(v) \wedge y(u) = y(v) \to z(u) = z(v))).$$

(iii) Bármely $k \geq 1$ $x, y, z \in A^k$*, és a* $\mathbf{k}$*-n definiált bármely* ρ *ekvivalenciareláció esetén ha* $\rho \supseteq \rho_x \cap \rho_y$*, akkor* $D_\rho \subseteq [x, y]$*.*

4. Diagrammsémák

Gumm Shifting Lemmája ([Gu1]) azt állítja, hogy kongruenciamoduláris varietások szép, téglalap alakban felrajzolható diagrammsémát elégítenek ki. Ennek hatására Chajda ([ChH1], 4.2. Alfejezet) egy olyan háromszögsémát vizsgált, amely a kongruenciadisztributivitás következménye. A kongruenciadisztributív varietások nemcsak három tetszőleges kongruenciára, hanem egy toleranciára és két kongruenciára is kielégítik ezt a sémát, azaz Gumm Shifting Elvének analógiája érvényes. Míg a háromszögsémáról nem ismert, hogy jellemzi-e a kongruenciadisztributivitást, egy trapézsémának nevezett megfelelő általánosításról megmutattuk, hogy igen ([CCH2], 4.3. Alfejezet). Ezek a példák mutatják, hogy kongruenciahálóbeli azonosságok, sőt Horn formulák helyett időnként érdemes diagrammsémákban gondolkodni.

5. Hálóazonosságok shiftje

Legyen

$$\lambda : \quad p(x_1, \ldots, x_n) \leq q(x_1, \ldots, x_n)$$

hálóazonosság. (Megjegyezzük, hogy hálóazonosságon mindig egyenlőtlenséget értünk, azaz $\leq$-t használunk $=$ helyett.) Ha y változó, akkor jelölje $S(\lambda, y)$ a

$$q(x_1, \ldots, x_n) \leq y \Longrightarrow p(x_1, \ldots, x_n) \leq y$$

formulát. Ha $y \notin \{x_1, \ldots, x_n\}$, akkor λ nyilvánvalóan ekvivalens $S(\lambda, y)$-nal. Számunkra az az eset a legfontosabb, amikor $y \in \{x_1, \ldots, x_n\}$, azaz $y = x_i$ $(1 \leq i \leq n)$. Ekkor $S(\lambda, x_i)$ következménye λ-nak. Ha $S(\lambda, x_i)$ ekvivalens λ-val, akkor $S(\lambda, x_i)$-t λ *shiftjének* nevezzük. Ha $S(\lambda, x_i)$ ekvivalens λ-val egy $\mathcal{V}$ varietáson belül, akkor azt mondjuk, hogy $S(\lambda, x_i)$ egy *shiftje* λ*-nak* $\mathcal{V}$*-ben.* Ebben a fejezetben néhány ismert hálóazonosságról megmutatjuk, hogy van shiftje, néhány továbbiról pedig azt, hogy nincs.

6. Toleranciák és toleranciahálók

Jelölje $\operatorname{dist}(x, y, z)$ a disztributív azonosságot: $x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z)$, $\operatorname{mod}(x, y, z)$ pedig a moduláris azonosságot: $x \wedge (y \vee (x \wedge z)) \leq (x \wedge y) \vee (x \wedge z)$. Jelölje $\mathbf{Tol\,A}$ az $\mathbf{A}$ algebra toleranciáinak *halmazát,* $\mathbf{Con\,A}$ pedig az $\mathbf{A}$ algebra kongruenciáinak *hálóját.* Azt mondjuk, hogy dist(tol,tol,tol) teljesül $\mathbf{A}$-ban, ha

$$\Gamma \wedge (\Phi \vee \Psi) \subseteq (\Gamma \wedge \Phi) \vee (\Gamma \wedge \Psi)$$

fennáll bármely $\Gamma, \Phi, \Psi \in \mathbf{Tol\,A}$ esetén, ahol a $\wedge$ közös rész képzést, $\vee$ pedig az unió tranzitív lezártját jelöli. Analóg módon értelmezzük mod(tol,tol,tol)-t. Hangsúlyozzuk, hogy $\Phi \vee \Psi$ **nem** a $\mathbf{Tol\,A}$ hálóbeli egyesítést jelenti. Jónsson kifejezések ([J1]) segítségével bizonyítottuk a következő tételt:

6.1. TÉTEL ([CzH2]). *Ha $\mathcal{V}$ kongruenciadisztributív (kongruenciamoduláris) varietás, akkor $\mathcal{V}$ minden algebrájában teljesül dist(tol,tol,tol) (mod(tol,tol,tol)).*

Két fontos következmény:

6.1. Korollárium (Gumm [Gu1]). *Ha $\mathcal{V}$ kongruenciamoduláris varietás, akkor teljesül a Gummtól származó Shifting Elv, azaz bármely $\mathbf{A} \in \mathcal{V}$-re, $\alpha, \gamma \in$ $\mathbf{Con\,A}$ and $\Phi \in \mathbf{Tol\,A}$ ha $(x, y), (u, v) \in \alpha$, $(x, u), (y, v) \in \Phi$, $(u, v) \in \gamma$ és $\alpha \cap \Phi \subseteq \gamma$, akkor $(x, y) \in \gamma$.*

Jelöljük *-gal a tranzitív lezártat. A következő állítás lényeges lépés a 7. Fejezetben található Malcev-feltételek felé:

6.1. Állítás ([CzH2]). *Ha mod(tol,tol,tol) vagy dist(tol,tol,tol) teljesül egy* $\mathbf{A}$ *algebrában, akkor $\Gamma \cap \Phi^* \subseteq (\Gamma \cap \Phi)^*$ bármely $\Gamma, \Phi \in$* $\mathbf{Tol\,A}$ *esetén.*

Egy 0-elemes $\mathbf{L}$ hálót *0-modulárisnak* nevezünk ([St]), ha nincs N_5-tel izomorf, 0_L-et tartalmazó részhálója. Egy 0-val rendelkező $\mathbf{L}$ háló teljesíti az *általános diszjunktsági tulajdonságot* (GD), ha az $a \wedge b = 0$ és az $(a \vee b) \wedge c = 0$ egyenlőségekből következik az $a \wedge (b \vee c) = 0$. Ha bármely $a \in \mathbf{L}$ esetén $\{x \in \mathbf{L}\colon a \wedge x = 0\}$-nak van legnagyobb eleme, akkor L-et *pszeudokomplementumos hálónak* nevezzük.

A most következő 6.2. és 6.3. Tételek tartalmazzák legfontosabb eredményeinket a kongruenciamoduláris varietásbeli toleranciahálókról.

6.2. TÉTEL ([CHR]). *Legyen* $\mathbf{A}$ *a* $\mathcal{V}$ *kongruenciamoduláris varietás egy algebrája. Ekkor fennállnak a következők:*

(i) A h*:* $\mathbf{Tol\,A} \to \mathbf{Con\,A}$, $\Phi \mapsto \Phi^*$ *leképezés szürjektív hálóhomomorfizmus, és* $\mathbf{Tol\,A}$ 0-1 *moduláris háló, amely rendelkezik a (GD) tulajdonsággal.*

(ii) $\mathbf{Tol\,A}$ *pontosan akkor pszeudokomplementumos, ha* $\mathbf{Con\,A}$ *pszeudokomplementumos.*

6.3. TÉTEL ([CHR]). *Legyen* $\mathbf{A}$ *tetszőleges algebra. Ha* $\mathbf{A}$*-n van többségi függvény, akkor:*

(i) $\mathbf{Tol\,A}$ 0*-moduláris pszeudokomplementumos háló.*

(ii) A Γ *és a* Φ *pontosan akkor komplementumai egymásnak* $\mathbf{Tol\,A}$*-ban, ha faktorkongruencia párt alkotnak* A*-ban.*

7. Kongruenciaháló azonosságok Malcev-feltételei moduláris varietásokban

Varietásra vonatkozó *erős Malcev-feltételnek* a következő alakú feltételt nevezzük: "léteznek $h_0, \ldots, h_k$ olyan kifejezések, amelyek kielégítik azonosságok egy Σ halmazát", ahol k rögzített, és Σ független a tekintett algebrák típusától. *Malcev-feltétel* alatt "létezik olyan n természetes szám, hogy P_n teljesül" alakú feltételt értünk, ahol a P_n-ek erős Malcev-feltételek és P_n-ből következik P_{n+1} bármely n-re. Day ismert eredménye szerint $\mathcal{V}$ pontosan akkor kongruenciamoduláris, ha " $(\exists n)(\mathbf{D}_n)$" teljesül $\mathcal{V}$-ben.

Azt mondjuk, hogy a λ *hálóazonosságból következik a modularitás kongruenciavarietásokban,*azaz $\lambda \models_c$ mod, ha bármely $\mathcal{V}$ varietás esetén ha minden $\mathbf{Con\,A}$ kongruenciahálóban ($\mathbf{A} \in \mathcal{V}$) teljesül λ, akkor minden ilyen kongruenciaháló moduláris. Például mindig ez a helyzet, ha λ-ból következik a modularitás hálóelméleti értelemben.

Legyen adott a p hálókifejezés és legyen $k \geq 2$. Definiáljuk a p_k kifejezéseket indukcióval a következőképpen. H p változó, akkor legyen $p_k = p$. Ha $p = r \wedge s$, akkor legyen $p_k = r_k \cap s_k$. Végül ha $p = r \vee s$, akkor legyen $p_k = r_k \circ s_k \circ r_k \circ s_k \circ \ldots$, amely k-tényezős szorzat. Ha kongruenciákat, vagy még általánosabban, reflexív kompatibilis relációkat helyettesítünk p_k változói helyére, akkor a $\cap$ közös rész képzésként és a $\circ$ relációszorzásként interpretálandó.

A Malcev-feltételekkel kapcsolatos első eredményünk a 7.1. Tétel.

7.1. TÉTEL ([CzH3]). *Legyen $\lambda : p \leq q$ olyan hálóazonosság, hogy $\lambda \models_c$ modularitás. Ekkor bármely $\mathcal{V}$ varietásra a következő két feltétel ekvivalens:*

(a) Bármely $\mathbf{A} \in \mathcal{V}$ algebra esetén λ teljesül $\mathbf{A}$ kongruenciahálójában.

(b) $\mathcal{V}$ kielégíti a következő Malcev-feltételt: "létezik $n \geq 2$ úgy, hogy $M(p_3 \subseteq q_n$ és $(\mathbf{D}_n)$ teljesül".

A következőekben javítjuk a 7.1. Tételt oly módon, hogy megadjuk a λ-t jellemző legegyszerűbb (és ebben az értelemben remélhetőleg a legjobb) Malcev-feltételt, amennyiben $\lambda \models_c$ modularitás.

Tetszőleges, a $\cap, \vee, \circ$ műveleti jelekből és változókból felépülő $p = p(x_1, \ldots, x_k)$, kifejezésre, röviden $\{\cap, \vee, \circ\}$-kifejezésre, és $n \geq 2$-re definiáljuk a p_n és a $p_{2,2}$ $\{\cap, \circ\}$-kifejezéseket indukció segítségével a következő módon. Ha p változó, akkor legyen $p_n = p_{2,2} = p$. Ha $p = r \cap s$, akkor legyen $p_n = r_n \cap s_n$ és $p_{2,2} = r_{2,2} \cap s_{2,2}$. Hasonlóan, ha $p = r \circ s$, akkor legyen $p_n = r_n \circ s_n$ és $p_{2,2} = (r_{2,2} \circ s_{2,2}) \cap (s_{2,2} \circ r_{2,2})$. Végül, ha $p = r \vee s$, akkor legyen $p_n = r_n \circ s_n \circ r_n \circ s_n \circ \cdots$ amely n szorzótényezőt tartalmaz a jobb oldalon, és legyen $p_{2,2} = (r_{2,2} \circ s_{2,2}) \cap (s_{2,2} \circ r_{2,2})$.

7.4. TÉTEL ([CHL]). *Legyen $p \subseteq q$ egy (kongruenciákra vonatkozó) tartalmazási formula, ahol q $\circ$-mentes. (Azaz a p egy $\{\cap, \vee, \circ\}$-kifejezés és q pedig háló-kifejezés.) Ekkor bármely $\mathcal{V}$ kongruenciamoduláris varietásra a következő feltételek ekvivalensek:*

(i) $p \subseteq q$ teljesül $\mathcal{V}$ kongruenciáira,

(ii) $p_2 \subseteq q$ teljesül $\mathcal{V}$ kongruenciáira,

(iii) $p_{2,2} \subseteq q$ teljesül $\mathcal{V}$ kongruenciáira,

(iv) A

$$(\exists n \geq 2)\big(M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)\big)$$

Malcev-feltétel (ahol $q_2 \circ q_2 \circ \cdots \circ q_2$ egy n-tényezős szorzatot jelöl) teljesül $\mathcal{V}$-ben.

Korolláriumként mondjuk ki a 7.1. Tétel javítását:

7.2. Korollárium ([CHL]). *Legyen $\lambda : p \leq q$ olyan hálóazonosság, hogy $\lambda \models_c$ modularitás. Ekkor bármely $\mathcal{V}$ varietásra a következő három feltétel ekvivalens:*

(a) Bármely $\mathbf{A} \in \mathcal{V}$ algebra esetén λ teljesül $\mathbf{A}$ kongruenciahálójában.

(b') $\mathcal{V}$ kielégíti a következő Malcev-feltételt: "létezik $n \geq 2$ úgy, hogy $M(p_2 \subseteq q_n)$ és $(\mathbf{D}_n)$ teljesül".

(c) $\mathcal{V}$ kielégíti a következő Malcev-feltételt: "létezik $n \geq 2$ úgy, hogy $M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)$ (n szorzótényező) és $(\mathbf{D}_n)$ teljesül".

7.4. TÉTEL ([CHL]). *Legyen $p \subseteq q$ egy (kongruenciákra vonatkozó) tartalmazási formula, ahol q $\circ$-mentes. (Azaz a p egy $\{\cap, \vee, \circ\}$-kifejezés és q pedig háló-*

kifejezés.) Ekkor bármely $\mathcal{V}$ kongruenciamoduláris varietásra a következő feltételek ekvivalensek:

(i) $p \subseteq q$ teljesül $\mathcal{V}$ kongruenciáira,

(ii) $p_2 \subseteq q$ teljesül $\mathcal{V}$ kongruenciáira,

(iii) $p_{2,2} \subseteq q$ teljesül $\mathcal{V}$ kongruenciáira,

(iv) A

$$(\exists n \geq 2)\big(M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)\big)$$

Malcev-feltétel (ahol $q_2 \circ q_2 \circ \cdots \circ q_2$ egy n-tényezős szorzatot jelöl) teljesül $\mathcal{V}$-ben.

Korolláriumként mondjuk ki a 7.1. Tétel javítását:

7.2. Korollárium ([CHL]). *Legyen $\lambda : p \leq q$ olyan hálóazonosság, hogy $\lambda \models_c$ modularitás. Ekkor bármely $\mathcal{V}$ varietásra a következő három feltétel ekvivalens:*

(a) Bármely $\mathbf{A} \in \mathcal{V}$ algebra esetén λ teljesül $\mathbf{A}$ kongruenciahálójában.

(b') $\mathcal{V}$ kielégíti a következő Malcev-feltételt: "létezik $n \geq 2$ úgy, hogy $M(p_2 \subseteq q_n)$ és $(\mathbf{D}_n)$ teljesül".

(c) $\mathcal{V}$ kielégíti a következő Malcev-feltételt: "létezik $n \geq 2$ úgy, hogy $M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)$ (n szorzótényező) és $(\mathbf{D}_n)$ teljesül".