Corollary 1. *The lattice c_∞^ω all totally ω-composition formations is $\mathfrak{G}$-separated.*

Corollary 2. *The lattice c_∞^τ all τ-closed totally composition formations is $\mathfrak{G}$-separated.*

References

1. A.N. Skiba, L.A. Shemetkov *Multiply $\mathfrak{L}$-composition formations of finite groups* Ukrainsk. math. zh. **52**, N 6, (2000), 783–797.
2. L.A. Shemetkov, A.N. Skiba *Formations of algebraic systems*, Nauka, Moscow, 1989.
3. A.N. Skiba *Algebra of formations*, Belarus. Navuka, Minsk, 1997.

Contact information

Inna P. Los
Belarusian State University, Minsk, Belarus
Email address: losip@bsu.by

Vasily G. Safonov
Belarusian State University, Minsk, Belarus
Email address: vgsafonov@bsu.by

Key words and phrases. Formation of finite groups, τ-closed formation, totally ω-composition formation, lattice of formations, $\mathfrak{G}$-separated lattice of formations

Definition of invertibility property for loops via translations

Alla Lutsenko

A *quasigroup* can be defined as a groupoid $(Q;\cdot)$ in which all *left translations* L_a ($L_a(x) := a{\cdot}x$) and all *right translations* R_a ($R_a(x) := x \cdot a$) are bijections of the carrier Q. In a quasigroup, a definition of a *middle translation* M_a ($M_a(x) = y :\Leftrightarrow xy = a$) is also possible. Therefore, an element e of a quasigroup is *neutral*, if left and right translations defined by e are identical transformations of the carrier: $L_e = R_e = \iota$. A quasigroup having a neutral element is called a *loop*.

The invertibility property also can be defined via translations of a quasigroup. Rememder that a quasigroup has [**1, 2**]:

- a *left inverse property* (briefly, a *left IP-quasigroup*), if there is a transformation λ such that for all x, y $\lambda x \cdot xy = y$;
- a *right inverse property* (briefly, a *right IP-quasigroup*), if there is a transformation ρ such that for all x, y $yx \cdot \rho x = y$;
- a *left cross inverse property* (briefly, a *left CIP-quasigroup*), if there is a transformation γ such that for all x, y $\gamma(x) \cdot yx = y$;
- a *right cross inverse property* (briefly, a *right CIP-quasigroup*), if there is a transformation δ such that for all x, y $xy \cdot \delta(x) = y$.

The defining equalities can be written as $L_{\lambda x}L_x = \iota$, $R_{\rho x}R_x = \iota$, $L_{\gamma x}R_x = \iota$, $R_{\delta x}L_x = \iota$ respectively [**1**], i.e.,

$$L_x^{-1} = L_{\lambda x}, \qquad R_x^{-1} = R_{\rho x}, \qquad R_x^{-1} = L_{\gamma x}, \qquad L_x^{-1} = R_{\delta x}.$$

Thus, the common property for all these classes of quasigroups is the following: ***each translation of a quasigroup is also a translation of the quasigroup.***

We consider the property in the variety of loops for all kinds of translations: left, right and middle. There are 9 defining relations:

$$L_x^{-1} = L_{\alpha x}, \quad L_x^{-1} = R_{\alpha x}, \quad L_x^{-1} = M_{\alpha x}, \quad R_x^{-1} = R_{\alpha x}, \quad R_x^{-1} = L_{\alpha x},$$

$$R_x^{-1} = M_{\alpha x}, \quad M_x^{-1} = M_{\alpha x}, \quad M_x^{-1} = L_{\alpha x}, \quad M_x^{-1} = R_{\alpha x}.$$

Theorem 1. *If inverses of some kind of translations of a loop $(Q; \cdot, e)$ are also translations of some fixed kind, then the loop belongs to one of the following classes of loops:*

$L_x^{-1} = L_{\alpha x}$	$x^{-1} \cdot xy = y$	*left IP-loop*
$R_x^{-1} = R_{\alpha x}$	$yx \cdot x^{-1} = y$	*right IP-loop*
$R_x^{-1} = L_{\alpha x}$	${}^{-1}x \cdot yx = y$	*left CIP-loop*
$L_x^{-1} = R_{\alpha x}$	$xy \cdot x^{-1} = y$	*right CIP-loop*
$L_x^{-1} = M_{\alpha x}$ $M_x^{-1} = L_{\alpha x}$	$xy \cdot y = x$	*right symmetric loop*
$R_x^{-1} = M_{\alpha x}$ $M_x^{-1} = R_{\alpha x}$	$xy \cdot x = y$	*semi-symmetric loop*
$M_x^{-1} = M_{\alpha x}$	$yx = xy$	*commutative loop*

where ${}^{-1}x \cdot x = e$ and $x \cdot x^{-1} = e$.

References

1. V.D. Belousov, *Foundations of the theory of quasigroups and loops*, M.: Nauka (1967), 222 (Russian).
2. N.N. Didurik and V.A. Shcherbacov, *On definition of CI-quasigroup*, ROMAI Journal (2017), Vol. 13 Issue 2, p. 55 –58.

Contact information

Alla Lutsenko
Department of mathematical analysis and differential equations, Vasyl' Stus Donetsk National University, Vinnytsia, Ukraine
Email address: lucenko.alla32@gmail.com

Key words and phrases. Quasigroup, IP-loop, invertible function, invertibility property

Models of Cryptography Transformations Based on Quasigroups

Volodymyr Luzhetskyi, Yurii Baryshev

It is intuitively obvious, that usage of unknown cryptographic transformations should be more secure against breaking, than usage of known ones. Modern cryptography approaches alters that statements reasoning, that the transformation infeasibility of breaking should be visible for customers for the verification sake. Consequently, the task of this transformation modeling to find the way out of the contradictive conditions arose.

According to the automatons definition given in [**1**] they were used to describe cryptographic transformations. An open cryptographic algorithm from the cryptanalysis point of view could be described as one performed by a deterministic automaton ADC [**2**]:

$$ADC = (PT, CT, k, IS, f(*)), \tag{1}$$

where PT – a set of all possible plaintexts; CT – a set of all possible ciphertext; k – used key; $f(*)$ – a function, which formilize known to an intruder cryptographic transformations.