

**ACADEMIA DE ȘTIINȚE A MOLDOVEI**  
**INSTITUTUL DE MATEMATICĂ ȘI INFORMATICĂ**

Cu titlu de manuscris  
CZU: 512.548(043.3)

**ȘCERBACOV VICTOR**

**DESPRE QUASIGRUPURI LINIARE ȘI INVERSE ȘI  
APLICAREA LOR ÎN TEORIA CODURILOR**

01.01.06 - logică matematică, algebră  
și teoria numerelor

**AUTOREFERAT**  
al tezei de doctor habilitat în științe fizico-matematice

Chișinău, 2008

**Teza a fost elaborată în laboratorul *Algebră și Logică Matematică* al Institutului de Matematică și Informatică al Academiei de Științe a Moldovei**

Referenți oficiali:

**GLUKHOV Mihail**, academician, dr.hab. ș. f.-m., profesor universitar, Academia de Criptografie a Federației Ruse, Moscova, Federația Rusă.

**GVARAMIA Aleco**, academician, dr.hab. ș. f.-m., profesor universitar, Universitatea de Stat din Abhazia, Suhumi, Georgia.

**VOROBIOV Nikolai**, dr.hab. ș. f.-m., profesor universitar, Universitatea de Stat "P.M. Masherov" din Vitebsk, Republica Belarus.

Susținerea va avea loc la 17 aprilie 2008, ora 14, în ședința Consiliului Științific Specializat **DH 01.01.01.06 - 02** din cadrul Institutului de Matematică și Informatică al Academiei de Științe a Moldovei, adresa : str. Academiei, 5, MD-2028, Chișinău, Republica Moldova.

Teza de doctor habilitat și autoreferatul pot fi consultate la biblioteca Institutului de Matematică și Informatică al Academiei de Științe a Moldovei, precum și pe site-ul CNAA ([www.cnaa.acad.md](http://www.cnaa.acad.md)).

Autoreferatul a fost expediat la 16.03. 2008

Secretar științific  
al consiliului științific specializat  
dr. ș. f.-m., conf. univ.

**Sârbu Parascovia**

Autor           **Șcerbacov Victor**

## Actualitatea temei investigate și gradul de studiere al ei.

În lucrare sunt cercetate unele probleme ale teoriei quasigrupurilor  $n$ -are și binare precum și aplicațiile ei în codificarea informației.

Mulțimea nevidă  $Q$  cu operația  $n$ -ară  $f$  care posedă proprietatea: în ecuația

$$f(x_1, x_2, \dots, x_n) = x_{n+1}$$

orice  $n$  elemente din mulțimea  $\{x_1, x_2, \dots, x_n, x_{n+1}\}$  definesc în mod unic rămas element, se numește *quasigrup  $n$ -ar*  $(Q, f)$  [26, 17]. În cazul  $n = 2$  noi obținem definiția quasigrupului binar. Dacă în quasigrupul binar  $(Q, \cdot)$  există un element  $e$  cu proprietatea  $x \cdot e = e \cdot x = x$  pentru toți  $x \in Q$ , atunci quasigrupul  $(Q, \cdot)$  se numește *buclă*.

Anii 20–30 ai secolului XX sunt anii începutului dezvoltării teoriei quasigrupurilor. La sfârșitul secolului XIX David Hilbert a publicat lucrări fundamentale consacrate axiomatizării matematicii, în particular, lucrări consacrate axiomatizării geometriei. În anii următori au fost publicate multe lucrări consacrate “bazelor” geometriei. În linii mari, au fost studiate diferite sisteme de axiome ale geometriei euclidiene, proiective și hiperbolice de dimensiune doi și trei.

Deoarece geometriile sunt coordonatzate cu diferite tipuri de structuri algebrice (câmpuri, grupuri, semigrupuri, etc.), pe parcurs au fost studiate diferite sisteme de axiome ale structurilor algebrice. De exemplu, L.E. Dikson a studiat semigrupurile în anul 1905 [46].

Deci la sfârșitul secolului al XIX-lea s-a început cercetarea structurilor care apar la modificarea sistemelor de axiome ale grupului sau ale diferitor geometrii. În particular, cercetările acestea au fost “provocate” de ideea de a cerceta problemele de independență a sistemelor de axiome.

Menționăm că Wilhelm Dörnte, urmând sfatului Emmy Noether, a cercetat quasigrupurile ternare ca o generalizare a grupurilor binare [47], Anton Sușkevici [129, 130] a studiat quasigrupurile binare cu unele condiții suplimentare (cu postulate), Burstin și Mayer au studiat quasigrupurile distributive [38].

Clifford și Preston în cartea [41] scriu că dezvoltarea teoriei semigrupurilor a început după lucrările lui Sușkevici [128]. Se poate spune că A.K. Sușkevici este unul din fondatorii teoriei quasigrupurilor și teoriei semigrupurilor.

Termenul “quasigrup” a apărut în lucrarea R. Moufang [87] care este consacrată problemelor coordonatizării planelor proiective. Putem spune că termenul “quasigrup” a apărut la studierea problemei de independență a axiomelor planului proiectiv.

R. Moufang a numit cu termenul “quasigrup” obiectul care astăzi se numește bucla Moufang. De fapt R. Moufang a definit bucla Moufang  $(Q, \cdot)$  ca o *IP*-buclă cu o identitate.

R. Moufang a studiat *IP*-buclele cu identitatea  $\alpha(\gamma \cdot \alpha\beta) = (\alpha\gamma \cdot \alpha)\beta$  (“Quasi-gruppe  $Q^*$ ”) și cu identitatea  $(\alpha\beta)(\gamma\alpha) = \alpha((\beta\gamma)\alpha)$  (“Quasi-gruppe  $Q^{**}$ ”), unde  $\alpha, \beta, \gamma \in Q$  [87].

Identitatea  $\alpha(\gamma \cdot \alpha\beta) = (\alpha\gamma \cdot \alpha)\beta$  se numește astăzi identitate Moufang de stânga, identitatea  $(\alpha\beta)(\gamma\alpha) = \alpha((\beta\gamma)\alpha)$  se numește identitate Moufang medie.

Mai târziu (1937) A.K. Suškevici a definit quasigrupurile mediale (abeliene) ([130], p. 157). Vezi și articolele de pionierat ale lui A.A. Albert [1, 2], D.C. Murdoch [90, 91], K. Toyoda [135], R.H. Bruck [35], R. Baer [6, 7] și E.L. Post [99].

Amintim, că în anii 30 ai secolului XX a fost introdus un nou concept de rețea algebrică. Definirea quasigrupului în termenii teoriei rețelelor are o interpretare geometrică naturală și clară [14, 16, 19].

Pătratele latine sunt un analog combinatoric al quasigrupurilor binare finite. Menționăm că studierea pătratelor latine a început în cadrul combinatoricii și matematicii distractive mult mai devreme decât studierea quasigrupurilor în cadrul algebrei abstracte [42, 83].

Ortogonalitatea este una din cele mai populare dintre proprietățile pătratelor latine, fiindcă proprietatea aceasta, probabil, este una din cele mai “aplicate” dintre proprietățile pătratelor latine.

Quasigrupurile ca soluții de unor ecuații funcționale, apărute implicit (fără nume) în logica matematică, apar în lucrările logicianului german Ernst Schröder [59, 82].

Probabil, primul exemplu al unei bucle neasociative este bucla multiplicativă a algebrei octonionilor [20, 76]. Menționăm, că informații istorice asupra dezvoltării teoriei quasigrupurilor și buclelor se află în teza lui Hubert Kiechle [76].

În prezent, teoria quasigrupurilor, teoria pătratelor latine și teoria rețelelor algebrice sunt dezvoltate destul de intens. Chiar dacă teoriile acestea au succese, scopuri și probleme proprii, până în prezent ele se dezvoltă intersectându-se și îmbogațindu-se reciproc.

Quasigrupurile au diferite aplicații în alte domenii ale matematicii, în alte științe și în practică [83].

De exemplu, quasigrupurile (pătratele latine) sunt utilizate de mult timp în statistică (în teoria planificării experimentului [86, 80]), în teoria ecuațiilor diferențiale [39], în geometria diferențială [39], în geometria hiperbolică [137], în fizică (în mecanica relativistă [92]), în teoria codurilor [118, 88], teoria automatelor [55, 56], în criptografie [42, 45]. Din lucrările lui Schaffler [102] este clar, că quasigrupurile au aplicații directe în criptografie. Pătratele latine au fost utilizate în criptografie aproape din momentul de apariție a acestei științe.

Menționăm, că Valentin Belousov (1925–1988) a obținut rezultate fundamentale în teoria quasigrupurilor binare și  $n$ -are, în teoria rețelelor și în teoria ecuațiilor funcționale.

Pentru quasigrupuri, în mod deosebit, luând în considerație legătura lor cu combinatorica, au fost definite și activ cercetate diferite tipuri de morfisme, printre care: izomorfisme, automorfisme, izotopisme (izotopii), izostrofisme, autostrofisme, izotopisme încrucișate, izotopisme generalizate. Automorfismele și grupurile de automorfisme ale buclelor au fost studiate de A.A. Albert în primele lucrări consacrate teoriei quasigrupurilor [1, 2].

Ca și în alte domenii ale matematicii, ideea de liniaritate joacă un rol important în teoria quasigrupurilor. De exemplu, această idee se utilizează în definiția quasigrupurilor

liniare. Ideea de liniaritate relativă este ideea principală a prezentei teze. Quasigrupurile liniare sunt cercetate și/sau utilizate în toate capitolele tezei.

În prezent (a. 2007), putem numi *quasigrup liniar* un quasigrup binar cu forma  $x \cdot y = (\alpha x + \beta y) + c$ , unde  $(Q, +)$  este o buclă “bună”,  $\alpha, \beta \in \text{Aut}(Q, +)$ ,  $c$  este elementul fix al mulțimii  $Q$ . Are sens să numim *quasigrup liniar generalizat* quasigrupul, în care permutările  $\alpha, \beta$  sunt permutări “bune” ale mulțimii  $S_Q$ .

V.D. Belousov a definit quasigrupurile liniare (peste grupuri) la mijlocul anilor 60 ai secolului XX [13]. În anii 70 au fost studiate destul de intens quasigrupurile liniare peste grupuri abeliene ( $T$ -quasigrupuri) și unele clase de quasigrupuri liniare generalizate de către T. Kepka, P. Nemeč, J. Jezek, V.D. Belousov, V.I. Onoi și de alți matematicieni. Este ușor de văzut că noțiunea de quasigrup liniar generalizat poate fi extinsă pentru cazul  $n$ -ar.

Observăm că multe clase de quasigrupuri binecunoscute (clasice) se află în clasa quasigrupurilor liniare generalizate. De exemplu, quasigrupurile mediale (teorema lui Toyoda [135]), quasigrupurile distributive (teorema lui Belousov [11]), quasigrupurile distributive Steiner, quasigrupurile distributive la stânga (teorema lui Belousov-Onoi [25]),  $CH$ -quasigrupurile (teorema lui Manin [84]),  $T$ -quasigrupurile, grupurile  $n$ -are (teorema lui Gluskin-Hossu [58, 54, 126]), quasigrupurile  $n$ -are mediale (teorema lui Evans [51] și teorema lui Belousov [17]),  $F$ -quasigrupurile (teorema lui Kepka-Kinyon-Phillips [73]) sunt quasigrupuri de acest tip.

Quasigrupurile liniare pot fi prezentate destul de compact în memoria computerului. Acest fapt oferindu-ne posibilități largi de utilizare a acestor quasigrupuri în practică. Menționăm, că, în cazul general, pentru a defini un quasigrup 100-ar de ordinul 10 ne trebuie  $10^{100}$  (un Gugol) egalități.

La sfârșitul anilor 80 și începutul anilor 90 membrii școlii lui V.D. Belousov (G.B. Beliavscaia cu elevii ei P.N. Sârbu și A.H. Tabarov, W.A. Dudek, V.I. Izbaș, V.A. Șcerbacov, F.N. Sohațkii cu elevii săi O.E. Kirnasovski și P. Sivakovski) și K.K. Șciukin au început cercetarea mai activă a quasigrupurilor liniare generalizate.

Au fost efectuate studii asupra congruențelor, automorfismelor, izomorfismelor, endomorfismelor, identităților, nucleelor, centrului, asociatorilor, comutatorilor, ortogonalității quasigrupurilor liniare generalizate (inclusiv și cazul  $n$ -ar). Au fost obținute unele estimări numerice. Cercetările acestea continuă până în prezent.

Cercetări în direcția aceasta au făcut L. Beneteau, T. Kepka, P. Nemeč, J.D.H. Smith.

Ideea de cercetare, mai mult sau mai puțin completă, a quasigrupurilor liniare generalizate (inclusiv cazul  $n$ -ar) a luat naștere în timpul discuțiilor lui K.K. Șciukin cu autorul prezentei teze. Ei au popularizat activ această idee printre colegi la diferite conferințe și în timpul întâlnirilor personale. Această idee (cazul binar) este reflectată în [112, 111].

Punctul de vedere, că orice automorfism este un autotopism cu componente egale, este destul de eficient pentru studierea automorfismelor și izomorfismelor quasigrupurilor liniare generalizate. Acest mod de abordare a studierii automorfismelor quasigrupurilor  $n$ -are liniare este bazat pe faptul binecunoscut, că quasigrupurile izotopice au grupuri izomorfe de autotopii.

De aceea, dacă cunoaștem structura autotopiilor quasigrupului  $n$ -ar “bun”  $(Q, f)$  și forma izotopiei  $T$ , atunci avem posibilitatea să obținem informația despre autotopiile și automorfismele quasigrupului  $n$ -ar  $(Q, g) = (Q, f)T$ . Credem că, pentru prima dată metoda aceasta a fost utilizată la studierea grupurilor de automorfisme ale quasigrupurilor grupurilor izotopice în [108].

Astăzi este clar că această idee poate fi utilizată într-o situație mult mai generală. De exemplu, dacă cunoaștem structura autostrofiilor (endotopiilor) quasigrupului  $n$ -ar  $(Q, f)$  și forma izostrofiei  $T$  (sau altă “izoaplicație” potrivită), atunci avem posibilitatea să obținem informații despre autostrofiile, autotopiile, automorfismele (endotopismele, endomorfismele) quasigrupului  $n$ -ar  $(Q, g) = (Q, f)T$  [134].

În lucrarea [105] este introdusă o restricție potrivită, adică a fost propus să se cerceteze quasigrupuri distributive la stânga, care sunt izotopice cu un grup fix. Restricția aceasta ne dă posibilitatea să studiem izomorfismele quasigrupurilor distributive la stânga, care sunt izotopice cu grupurile. Mai târziu aceste procedee de studiere a automorfismelor și izomorfismelor quasigrupurilor liniare generalizate au fost utilizate de autorul acestei teze și unii colegi ai lui [48, 60, 61, 78, 113, 114, 125, 122].

Proape toate clasele binecunoscute (clasice) de quasigrupuri și bucle au proprietatea de “inversabilitate”. Cele mai cunoscute clase de quasigrupuri cu proprietatea de inversabilitate sunt  $IP$ -,  $LIP$ -, ( $RIP$ -),  $WIP$ - și  $CI$ -bucle și quasigrupuri.

Menționăm, că  $IP$ - și, de fapt,  $LIP$ -buclele au fost definite în lucrarea lui R. Moufang [87].  $IP$ - și  $LIP$ -quasigrupuri și bucle au fost studiate în [35, 37, 14, 52].

$WIP$ -buclele au fost definite în lucrarea lui R. Baer [7].  $WIP$ -buclele au fost studiate în [7, 98, 8].  $WIP$ -quasigrupurile au fost definite și studiate în [127].

$CI$ -buclele au fost definite în lucrarea lui R. Artzy [3],  $CI$ -buclele și  $CI$ -quasigrupurile au fost studiate în [3, 4, 27, 65, 136]; buclele  $m$ -inverse au fost definite în [64], au fost studiate în [9, 66];  $I$ -,  $PI$ -quasigrupurile și buclele au fost definite și au fost studiate în [21, 22, 53]. În [44, 45] au fost propuse unele aplicații ale quasigrupurilor inverse în criptografie.

Ideea unei generalizări a proprietăților de inversabilitate a apărut din cerințele criptografiei [44] și după citirea ultimelor lucrări ale lui V.D. Belousov [21, 22]. Această idee a fost realizată în “practică” în lucrările comune ale prof. A.D. Keedwell cu autorul.

În teză sunt studiate:

proprietățile unor clase de quasigrupuri inverse (inclusiv și clase noi:  $(\alpha, \beta, \gamma)$ -inverse și  $(r, s, t)$ -inverse); proprietățile unor clase de quasigrupuri liniare generalizate; structura quasigrupurilor  $n$ -are mediale; proprietățile quasigrupurilor cu identități Moufang; congruențele și nucleele quasigrupurilor, quasigrupurilor inverse și quasigrupurilor liniare; autotopiile, automorfismele, grupurile automorfismelor ale quasigrupurilor și quasigrupurilor liniare; codurile bazate pe quasigrupuri  $n$ -are; ortogonalitatea quasigrupurilor.

Toate cele menționate mai sus confirmă actualitatea temei alese a tezei.

Autorul exprimă sincere mulțumiri fostului conducător științific, profesorului V.D. Belousov, profesorului A.D. Keedwell și profesorului K.K. Şciukin pentru ajutorul de neprețuit.

### **Scopurile lucrării.** Scopurile tezei sunt:

de a studia unele aspecte ale quasigrupurilor, inclusiv quasigrupurile inverse și quasigrupurile  $n$ -are mediale;

de a cerceta grupurile automorfismelor quasigrupurilor  $n$ -are liniare, quasigrupurilor distributive la stânga, ortogonalitatea pătratelor;

de a construi coduri cu un simbol de control cu proprietăți mai bune decât au anumite coduri cu un simbol de control, de exemplu ca ISSN-codul, ISBN-codul, UPC-codul, EAN-codul.

### **Spport metodologic și teoretico-științific.**

În lucrare sunt utilizate metodele algebrice și combinatorice.

**Inovația științifică a lucrării.** De fapt, toate rezultatele obținute la momentul primei publicații a lor au fost noi. Au fost obținute următoarele rezultate:

Au fost introduse clase noi ale quasigrupurilor binare inverse ( $(r, s, t)$ -inverse,  $(\alpha, \beta, \gamma)$ -inverse) și cercetate proprietățile lor.

A fost demonstrată că un quasigrup cu orice identitate Moufang este o buclă.

A fost obținut un progres în rezolvarea problemei Bruck-Belousov despre normalitatea congruențelor quasigrupurilor pentru buclele de stânga (de dreapta).

A fost descrisă structura quasigrupurilor  $n$ -are mediale simple.

A fost descrisă structura quasigrupurilor  $n$ -are finite mediale.

Au fost cercetate grupurile automorfismelor  $T$ -quasigrupurilor  $n$ -are, quasigrupurilor  $n$ -are mediale și niște isotopi ai quasigrupurilor distributive la stânga.

Au fost elaborate familii noi ale codurilor, care sunt construite în mod simplu și care au caracteristici mai bune decât codurile cunoscute de același tip.

Au fost obținute condițiile necesare și suficiente despre ortogonalitatea unui quasigrup finit și orice parastrof al lui.

### **Semnificația teoretică și valoarea aplicativă a lucrării.**

În general lucrarea este consacrată aspectelor teoretice ale teoriei quasigrupurilor. Lucrarea conține unele aplicații ale quasigrupurilor  $n$ -are în teoria codurilor.

**Aprobarea rezultatelor obținute.** Rezultatele tezei au fost prezentate în forma verbală în cadrul următoarelor conferințe:

Conferința Internațională de Matematică și Informatică, Chișinău, Septembrie 19-21, 1996;

A II-a Conferință Internațională de Algebră din Ucraina, Kiev-Vinnița, 9 - 16 Mai 1999;

Conferința Internațională Loops'99, Praga, Iulie 27 - August 1, 1999;

Seminarul de Matematică Pură în Royal Holloway, Universitatea din Londra (Februarie, 2001);

Seminarul algebric în Goldsmith College, Universitatea din Londra (Februarie, 2001);

Prima Conferință a Societății Matematice din Republica Moldova, Chișinău, August 16-18, 2001;

Conferința Internațională Loops'03, Praga, August 10 - August 17, 2003;

Seminarul algebric la Charles University (Praga, Octombrie, 2003);

Second Conference of the Mathematical Society of the Republic of Moldova dedicated to the 40 anniversary of the foundation of the Institute of Mathematics and Computer Science of ASM, Chişinău, August, 17-19, 2004;

Workshop "Computational Commutative and Non-Commutative Algebraic Geometry" June 6–11, 2004, Chişinău, Moldova;

BiT+, a IV-a Conferinţă Internaţională de Tehnologii Informaţionale 2004, 3-7 Mai, 2004, Chişinău, Moldova;

A V-a Conferinţă Internaţională de Algebră din Ucraina, Odesa, Iulie, 20-27, 2005.

Rezultatele tezei au fost comunicate la Chişinău în cadrul Seminarului Orăşenesc de Algebră (de două ori pe an (2001-2006)).

**Publicaţii.** Rezultatele de bază ale tezei au fost publicate în 20 articole, 22 rezumate la conferinţe şi manifestări ştiinţifice naţionale şi internaţionale, 2 rapoarte tehnice. Printre aceste publicaţii sunt trei lucrări de sinteză.

**Volumul şi structura lucrării.** Lucrarea constă din şapte capitole (divizate în paragrafe) şi bibliografie. Toate teoremele, propoziţiile, lemele, corolarele, observaţiile şi formulele sunt numerotate cu două numere, primul din care indică numărul capitolului.

### Conţinutul pe scurt al lucrării.

Toate rezultatele icluse în teză autorul le-a obţinut de sinestător sau în cooperarea inseparabilă cu co-autorii lucrărilor publicate.

În **Capitolul 1** se expune actualitatea temei, scopul şi obiectivele tezei, aprobarea rezultatelor obţinute. În primul capitol sunt prezentate noţiunile şi rezultatele de bază, ce vor fi folosite ulterior.

În **Capitolul 2** sunt studiate noi clase ale quasigrupurilor inverse. Multe rezultate din acest capitol sunt obţinute în cooperarea inseparabilă cu prof. A.D. Keedwell. Ele au fost publicate în articole comune cu prof. A.D. Keedwell [67, 68, 69].

V.D. Belousov [21] a definit şi a început studiarea quasigrupurilor  $\lambda$ -inverse şi  $\rho$ -inverse. Un quasigrup  $(Q, \circ)$  se numeşte *quasigrup  $\lambda$ -invers sau  $\lambda$ -quasigrup* dacă există permutările  $\lambda_1, \lambda_2, \lambda_3$  ale mulţimii  $Q$  astfel, încât  $x\lambda_1 \circ (x \circ y)\lambda_2 = y\lambda_3$  pentru orice  $x, y \in Q$ .

Un quasigrup  $(Q, \circ)$  se numeşte *quasigrup  $\rho$ -invers sau  $\rho$ -quasigrup* dacă există permutările  $\rho_1, \rho_2, \rho_3$  ale mulţimii  $Q$  astfel, încât  $(x \circ y)\rho_1 \circ y\rho_2 = x\rho_3$  pentru orice  $x, y \in Q$ .

În articolele comune ale profesorului A.D. Keedwell şi ale autorului au fost introduse quasigrupurile  $(\alpha, \beta, \gamma)$ -inverse (sau  $(\alpha, \beta, \gamma)$ -quasigrupuri) : un quasigrup  $(Q, \cdot)$  se numeşte quasigrup  $(\alpha, \beta, \gamma)$ -invers dacă există permutările  $\alpha, \beta, \gamma$  ale mulţimii  $Q$  astfel, încât  $(x \circ y)\alpha \circ x\beta = y\gamma$  pentru orice  $x, y \in Q$ .

De fapt orice quasigrup invers aparţine uneia din cele trei clase ale quasigrupurilor inverse menţionate mai sus.

Vom utiliza următoarea definiţie a autostrofismului. Colecţia permutărilor  $[\sigma, (\alpha_1, \alpha_2, \alpha_3)] = [\sigma, \alpha]$ , unde  $\sigma \in S_3$  şi  $\alpha_1, \alpha_2, \alpha_3$  sunt permutări ale mulţimii  $Q$ , se numeşte un *autostrofism* al quasigrupului  $(Q, A)$  dacă şi numai dacă  $A^\sigma(x_1\alpha_1, x_2\alpha_2) = A(x_1, x_2)\alpha_3$  pentru orice  $x_1, x_2 \in Q$ .

**Teorema 2.2.** *Un quasigrup  $(Q, \otimes)$  este quasigrup  $(\alpha, \beta, \gamma)$ -invers dacă şi numai dacă  $(Q, \otimes)$  are autostrofism  $[(1\ 2\ 3), (\beta, \gamma, \alpha)]$ . Quasigrupul  $(Q, \otimes)$  este  $\lambda$ -quasigrup*

dacă și numai dacă  $(Q, \otimes)$  are autostrofism  $[(2\ 3), (\lambda_1, \lambda_3, \lambda_2)]$ . Quasigrupul  $(Q, \otimes)$  este  $\rho$ -invers dacă și numai dacă  $(Q, \otimes)$  are autostrofism  $[(1\ 3), (\rho_3, \rho_2, \rho_1)]$ .

Un quasigrup  $(Q, \circ)$  se numește *quasigrup  $(r, s, t)$ -invers sau  $(r, s, t)$ -quasigrup*, dacă există o permutare  $x \rightarrow xJ$  a mulțimii  $Q$  astfel, încât  $(x \circ y)J^r \circ xJ^s = yJ^t$  pentru orice  $x, y \in Q$ , unde  $r, s, t$  sunt numere întregi.

Quasigrupurile  $(r, s, t)$ -inverse au fost definite ca o generalizare a familiilor diferite ale quasigrupurilor cu proprietate “încrucși-inversă”: în particular, quasigrupurile  $(r, s, t)$ -inverse generalizează buclele *CI*-, *WIP*- și *m*-inverse [64]. În acest capitol atenția principală este consacrată quasigrupurilor  $(r, s, t)$ -inverse. Menționăm că quasigrupurile  $(r, s, t)$ -inverse pot avea unele aplicații în criptografie [44].

Este demonstrat că  $J^{r+s+t} \in \text{Aut}(Q, \circ)$ . Atunci orice quasigrup  $(r, s, t)$ -invers  $(Q, \cdot)$  este și  $(r + uh, s + uh, t + uh)$ -invers pentru orice  $u \in \mathbf{Z}$ , unde  $J^h \in \text{Aut}(Q, \cdot)$ .

Fie  $(Q, +)$  o buclă cu nucleu la stânga  $N_l = \{c : c + (x + y) = (c + x) + y \text{ pentru orice } x, y \in Q\}$ .

Un *quasigrup liniar la stângă* peste o buclă  $(Q, +)$  este un quasigrup  $(Q, \cdot)$  cu forma  $x \cdot y = c + x\varphi + y\psi$  pentru orice  $x, y \in Q$ , unde  $\varphi \in \text{Aut}(Q, +)$ ,  $\psi$  este o permutare a mulțimii  $Q$  cu proprietatea  $\psi 0 = 0$  (unde simbolul  $0$  denotă un element neutru al buclei  $(Q, +)$ ) și  $c \in N_l(Q, +)$ . Dacă și  $\psi \in \text{Aut}(Q, +)$ , noi obținem noțiunea unui quasigrup liniar peste bucla  $(Q, +)$ .

Dacă o buclă  $(Q, +)$  este un grup abelian și  $\varphi, \psi \in \text{Aut}(Q, +)$ , atunci quasigrupul  $(Q, \cdot)$  cu forma  $x \cdot y = c + x\varphi + y\psi$  se numește *T-quasigrup*.

Quasigrupurile  $(r, s, t)$ -inverse liniare la stânga sunt descrise în

**Teorema 2.8.** *Un quasigrup liniar la stânga  $(Q, \cdot)$  peste o buclă  $(Q, +)$  este un quasigrup  $(r, s, t)$ -invers relativ la permutarea  $J$  a mulțimii  $Q$ , unde  $J^r \in \text{Aut}(Q, +)$  și  $0J = 0$  dacă și numai dacă*

- (i)  $c + cJ^r\varphi = 0$ ,      (iii)  $x\varphi J^r\varphi + xJ^s\psi = 0$  pentru orice  $x \in Q$ ,
- (ii)  $\psi = J^t\varphi^{-1}J^{-r}$ ,      (iv)  $(Q, +)$  este o *CI*-buclă.

O descriere mai mult sau mai puțin completă a quasigrupurilor mediale  $(r, s, t)$ -inverse  $(Z_m, \cdot)$ , unde  $(Z_m, +)$  este un grup ciclic, cu condiția că permutarea  $J$  este translația la stânga a grupului  $(Z_m, +)$ , adică  $J = L_b^+$ , este dată în

**Teorema 2.12.** *Un T-quasigrup  $(Z_m, \cdot)$   $(r, s, t)$ -invers cu forma  $x \cdot y = x\phi + y\psi$  ce este definit peste un grup ciclic  $(Z_m, +)$  relativ la permutarea  $J = L_b^+$ , unde  $b$  este un element fixat al mulțimii  $b \in Z_m$  poate fi unul din următoarele tipuri de quasigrupuri:*

- (a) un quasigrup total simetric cu forma  $x \cdot y = -x - y$ ; sau
- (b) un quasigrup medial distributiv cu forma  $x \cdot y = x\phi + y\phi^{-1}$ , unde  $\phi : z \rightarrow hz$  și  $h$  este o rădăcină a ecuației  $h^2 - h + 1 = 0$ .

În orice caz,  $r, s$  și  $t$  sunt legate cu relația  $h^2r + s = ht$ .

Până la izomorfism, există numai un singur T-quasigrup  $(r, s, t)$ -invers de tipul (a) pentru orice număr pozitiv  $m$ .

T-quasigrupuri  $(r, s, t)$ -inverse de tipul (b) există dacă numărul  $m$  are una din următoarele forme: (i)  $m = p_1^{k_1} p_2^{k_2} \dots p_u^{k_u}$ , (ii)  $m = 2p_1^{k_1} p_2^{k_2} \dots p_u^{k_u}$ , (iii)  $m = 4p_1^{k_1} p_2^{k_2} \dots p_u^{k_u}$  unde, în fiecare caz,  $p_i \equiv 1 \pmod{6}$  pentru toți  $i = 1, 2, \dots, u$ .

Dacă aceste quasigrupuri există, atunci există  $2^u$   $T$ -quasigrupuri  $(r, s, t)$ -inverse de tipul (b)(i) și (b)(ii) neizomorfe două câte două și  $2^{u+1}$   $T$ -quasigrupuri  $(r, s, t)$ -inverse de tipul (b)(iii) neizomorfe două câte două.

În următoarele paragrafe se studiază unele proprietăți ale produsului direct al quasigrupurilor  $(r, s, t)$ -inverse.

Vom presupune că  $|Q_1| = n_1$  și  $|Q_2| = n_2$ ,  $h_1, h_2$  sunt cele mai mici numere pozitive pentru care  $J^{h_1} \in \text{Aut}(Q_1, \cdot)$  și  $J^{h_2} \in \text{Aut}(Q_2, \cdot)$ .

**Teorema 2.17.** *Dacă quasigrupurile  $(r, s, t)$ -inverse  $(Q_1, \cdot)$  și  $(Q_2, \circ)$  nu au coresponzător autotopisme de forma  $(J_1^{a_1}, J_1^{b_1}, J_1^{c_1})$  și  $(J_2^{a_2}, J_2^{b_2}, J_2^{c_2})$  cu excepția automorfismelor, atunci produsul direct  $(Q, *) = (Q_1, \cdot) \times (Q_2, \circ)$  va fi un quasigrup  $(r, s, t)$ -invers relativ la permutarea  $J$  a mulțimii  $Q$  pentru numerele întregi  $r, s, t$  dacă și numai dacă există două numere întregi  $u_1$  și  $u_2$  astfel, încât*

$$r - r_1 = s - s_1 = t - t_1 = u_1 h_1 \quad \text{și} \quad r - r_2 = s - s_2 = t - t_2 = u_2 h_2,$$

unde  $h_1$  și  $h_2$  sunt definite în același mod ca mai sus.

**Corolarul 2.10.** *Pentru orice numere întregi pozitive  $r, s$  și  $t$  există quasigrupuri  $(r, s, t)$ -inverse.*

Teoremele care stabilesc unele procedee pentru construirea  $WIP$ -quasigrupurilor sunt colectate în următorul paragraf.

**Teorema 2.20.** *Dacă  $(Q, \circ)$  este un quasigrup cu operația de forma  $x \circ y = x\varphi + y\psi$ , unde  $(Q, +)$  este o buclă,  $\varphi, \psi \in \text{Aut}(Q, +)$ , atunci  $(Q, \circ)$  este un  $WIP$ -quasigrup relativ la permutarea  $J$  a mulțimii  $Q$  dacă și numai dacă (i)  $J = \psi^{-1}\varphi I_0 \psi^{-1}$ ; (ii)  $[\varphi^{-1}, \psi] = \psi^{-1}\varphi^{-1}$ ; și (iii)  $(Q, +)$  este o  $WIP$ -buclă.*

Au fost studiate proprietățile  $A$ -nucleelor quasigrupurilor  $(r, s, t)$ -inverse. Reamintim, că  $A$ -nucleu la stânga al unui quasigrup  $(Q, \circ)$  se numește grupul tuturor autotopiilor de forma  $(\alpha, \varepsilon, \gamma)$ , unde  $\varepsilon$  este permutarea identică.

Prin analogie, toate autotopiile de forma  $(\alpha, \beta, \varepsilon)$  ale quasigrupului  $(Q, \circ)$  formează un  $A$ -nucleu mediu, iar autotopiile de forma  $(\varepsilon, \beta, \gamma)$  formează un  $A$ -nucleu la dreapta al quasigrupului  $(Q, \circ)$ . Notăm în mod coresponzător nucleele acestea cu  $N_l^A$ ,  $N_m^A$  și  $N_r^A$ . În [12, 70]  $A$ -nucleele se numesc respectiv grupuri de permutări regulate la stânga, la dreapta și medii ale quasigrupului  $(Q, \circ)$ .

Reamintim, că V.D. Belousov a utilizat grupul  ${}_1N_r^A$  într-o lucrare la conferința unională în anul 1958 [11].

**Teorema 2.25.** *În orice  $\lambda$ -quasigrup  $A$ -nucleul la stânga și mediu sunt izomorfe. Mai precis, se poate spune, că  $N_m^A = K^{-1}N_l^A K = KN_l^A K^{-1}$ , unde  $K = [(2\ 3), (\lambda_1, \lambda_3, \lambda_2)]$ .*

**Teorema 2.26.** *În orice  $\lambda$ -buclă nucleele la stânga și mediu coincid dacă  $\lambda_1 = \varepsilon$  sau  $\lambda_2 = \varepsilon$  sau  $\lambda_3 = \varepsilon$ .*

**Teorema 2.27.** *(i) Într-un quasigrup  $\rho$ -invers  $A$ -nucleele la stânga și mediu sunt izomorfe. Mai exact, se poate spune, că  $N_m^A = K^{-1}N_r^A K = KN_r^A K^{-1}$ , unde  $K = [(1\ 3), (\rho_3, \rho_2, \rho_1)]$ .*

(ii) Într-o buclă  $\rho$ -inversă nucleul mediu și nucleul la dreapta coincid dacă  $\rho_1 = \varepsilon$  sau  $\rho_2 = \varepsilon$  sau  $\rho_3 = \varepsilon$ .

**Corolarul 2.15.** În orice  $I$ -quasigrup  $A$ -nucleele la stânga, la dreapta și mediu sunt izomorfe. În orice  $PI$ -buclă  $A$ -nucleele la stânga, la dreapta și mediu coincid.

Din Teorema 2.26 și Teorema 2.27 putem trage concluzia cunoscută:  $N_l = N_r = N_m$  în orice  $IP$ -buclă [14].

**Teorema 2.28.** În quasigrupul  $(Q, \otimes)$   $(\alpha, \beta, \gamma)$ -invers  $A$ -nucleele la stânga, la dreapta și mediu sunt izomorfe două câte două. Mai exact, putem spune că  $N_r^A = H^{-1}N_l^A H$ ,  $N_m^A = H^{-1}N_r^A H$  și  $N_l^A = H^{-1}N_m^A H$ , unde  $H = [(1\ 2\ 3), (\beta, \gamma, \alpha)]$ .

**Teorema 2.30.** Într-o buclă  $(Q, \otimes)$   $(\alpha, \beta, \gamma)$ -inversă nucleele la stânga, la dreapta și mediu coincid dacă (i)  $\alpha$  sau  $\beta$  sau  $\gamma$  este permutarea identică, sau (ii)  $\alpha\beta$  sau  $\beta\gamma$  sau  $\gamma\alpha$  este permutarea identică.

Din Teorema 2.30 obținem binecunoscutul rezultat.

**Corolarul 2.19.** În  $CI$ -buclă și în  $WIP$ -buclă,  $N_l = N_r = N_m$  [5, 98].

În **Capitolul 3** sunt studiate două probleme din cartea lui V.D. Belousov [14].

Identitățile  $(x \cdot yz)x = xy \cdot zx$ ,  $x(yz \cdot x) = xy \cdot zx$ ,  $x(y \cdot xz) = (xy \cdot x)z$  și  $(zx \cdot y)x = z(x \cdot yx)$  se numesc identități Moufang.

În paragraful 3.1 este demonstrat că quasigrupul cu oricare din identitățile Moufang este o buclă, adică acest quasigrup are un element identic (Teorema 3.2).

Teorema aceasta rezolvă cazul particular al problemei lui Burmistrovici (Problema nr.18 din cartea lui Belousov [14]), și anume: existența cărei identități într-un quasigrup garantează, că acest quasigrup este o buclă? Rezultatele paragrafului 3.1 au fost anunțate în [62] și au fost publicate în [115]. Menționăm că rezultate similare a publicat K. Kunen în [81].

În paragraful 3.2 încercăm să rezolvăm următoarea problemă a lui Bruck-Belousov: Care buclă  $G$  are proprietatea că orice imagine omomorfă a lui  $G$  corespunzătoare unui omomorfism multiplicativ este de asemenea o buclă ([37], p. 92)?; Care sunt quasigrupurile sau buclele în care toate congruențele sunt normale ([14], Problema 20, p. 221)?

Menționăm că în acest paragraf studiem quasigrupuri în semnatura cu o operație binară. Unele rezultate din acest paragraf sunt o continuare și o dezvoltare a rezultatelor autorului din teza sa de doctor [111].

Un quasigrup  $(Q, \cdot)$  care are un element  $f$  cu proprietatea  $f \cdot x = x$  pentru orice  $x \in Q$  se numește buclă de stânga. Un quasigrup  $(Q, \cdot)$  care are un element  $e$  cu proprietatea  $x \cdot e = x$  pentru orice  $x \in Q$  se numește buclă de dreapta.

Fie  $\mathbb{T} = \{L_a, R_b \mid a, b \in Q\}$ ,  $\mathbb{T}^{-1} = \{L_a^{-1}, R_b^{-1} \mid a, b \in Q\}$ .

Cu  $\Pi(Q)$  sau cu  $\Pi$  vom nota un semigrup, care este generat de toate translațiile la stânga și la dreapta ale quasigrupului  $Q$ .

Un grup generat de toate translațiile la stânga și la dreapta ale quasigrupului  $Q$  va fi notat cu  $M(Q)$ , sau cu  $M$ , pentru simplitate.

**Definiția 3.4.** Un subgrup  $H$  al grupului  $M$  se numește  $A$ -invariant în raport cu submulțimea  $A$  a elementelor grupului  $M$ , dacă  $a^{-1}Ha \subseteq H$  pentru toți  $a \in A$ .

**Teorema 3.7.** *Toate congruențele buclei la stânga (sau la dreapta) sunt normale dacă și numai dacă subgrupurile  $\Pi$ -invariante ale grupului  $M$  sunt normale în  $M$ .*

Pentru aplicații sunt comode următoarele condiții suficiente de normalitate ale congruențelor quasigrupului.

**Propoziția 3.5.** *Dacă quasigrupul  $Q$  satisface condiția  $\mathbb{T}^{-1} \subseteq \Pi$ , atunci în  $Q$  toate congruențele sunt normale.*

Utilizând Propoziția 3.5 noi stabilim condițiile de normalitate ale tuturor congruențelor quasigrupurilor inverse.

**Definiție.** Dacă  $\theta$  este o relație binară pe mulțimea  $Q$ ,  $\alpha$  este o permutare a mulțimii  $Q$  și din  $x\theta y$  implică  $\alpha x\theta \alpha y$  pentru toți  $(x, y) \in \theta$ , atunci noi vom spune că permutarea  $\alpha$  este *semiadmisibilă* în raport cu relația  $\theta$ . O permutare semiadmisibilă  $\theta$  este o permutare *admisibilă* în raport cu relația binară  $\theta$ , dacă din  $x\theta y$  rezultă  $\alpha^{-1}x\theta\alpha^{-1}y$  pentru toți  $(x, y) \in \theta$ .

**Propoziția 3.6.** *În  $(\alpha, \beta, \gamma)$ -quasigrupul  $(Q, \cdot)$  toate congruențele sunt normale dacă permutările  $\alpha$  și  $\gamma^{-1}$  sunt semiadmisibile în raport cu orice congruență a quasigrupului  $(Q, \cdot)$ .*

**Corolarul 3.13.** *În CI-quasigrupul  $(Q, \cdot)$  toate congruențele sunt normale.*

**Corolarul 3.14.** *În WIP-quasigrupul  $(Q, \cdot)$  toate congruențele sunt normale, dacă permutarea  $J$  este admisibilă în raport cu orice congruență a lui  $(Q, \cdot)$ . În quasigrupul  $(Q, \cdot)$   $m$ -invers toate congruențele sunt normale dacă permutarea  $J^m$  este admisibilă în raport cu orice congruență a lui  $(Q, \cdot)$ .*

**Propoziția 3.8.** *Într-un I-quasigrup  $(Q, \cdot)$  toate congruențele sunt normale dacă permutările  $\lambda_2, \lambda_3^{-1}, \rho_1$  și  $\rho_3^{-1}$  sunt semiadmisibile în raport cu orice congruență a quasigrupului  $(Q, \cdot)$ .*

**Propoziția 3.12.** *Dacă  $(Q, \circ)$  este o IP-bucă,  $(Q, \cdot)$  este un izotop al său de forma  $(\alpha J^\tau, \beta J^\kappa, \varepsilon)$ , unde  $\alpha, \beta \in M(Q, \circ)$ ,  $\tau, \kappa \in \{0, 1\}$ , adică  $x \cdot y = \alpha J^\tau x \circ \beta J^\kappa y$  pentru orice  $x, y \in Q$ , atunci  $Con(Q, \circ) = nCon(Q, \cdot)$ .*

În **Capitolul 4** sunt studiate quasigrupurile  $n$ -are mediale.

Un quasigrup  $n$ -ar  $(Q, g)$  cu identitatea

$$\begin{aligned} g(g(x_{11}, x_{12}, \dots, x_{1n}), g(x_{21}, x_{22}, \dots, x_{2n}), \dots, g(x_{n1}, x_{n2}, \dots, x_{nn})) = \\ g(g(x_{11}, x_{21}, \dots, x_{n1}), g(x_{12}, x_{22}, \dots, x_{n2}), \dots, g(x_{1n}, x_{2n}, \dots, x_{nn})) \end{aligned}$$

se numește un *quasigrup medial* [17].

Un quasigrup  $(Q, f)$  care admite identitatea  $f(x, x, \dots, x) = x$  se numește *idempotent*, iar unul care admite identitatea  $f(x, x, \dots, x) = e$ , unde  $e$  este un element fix al mulțimii  $Q$ , se numește *unipotent*.

Pentru un quasigrup  $n$ -ar  $(Q, f)$  definim o aplicație  $s$  în modul următor:  $s(x) = f(x, x, \dots, x)$  pentru orice element  $x \in Q$ . A fost demonstrată că  $s$  este un omomorfism în quasigrup  $n$ -ar medial.

**Definiție.** Un quasigrup  $n$ -ar  $(Q, f)$  se numește un *quasigrup unipotent-resolubil de gradul  $m$*  dacă există un lanț finit de quasigrupuri unipotente:

$$Q/s(Q), s(Q)/s^2(Q), \dots, s^{m-1}(Q)/s^m(Q),$$

unde numărul  $m$  este numărușul minim cu proprietatea  $|s^m(Q)| = 1$ .

Următoarea teoremă este o generalizare pentru cazul  $n$ -ar a teoremei binecunoscute a lui Murdoch [91] asupra structurii quasigrupurilor binare mediale.

**Teorema 4.6.** *Orice quasigrup finit medial  $n$ -ar  $(Q, f)$  este izomorf cu produsul direct al unui quasigrup medial unipotent-resolubil  $(Q_1, f_1)$  și cu un izotop  $(Q_2, f_2)$  de forma  $(\varepsilon, \dots, \varepsilon, \gamma)$  al quasigrupului medial idempotent  $(Q_2, f_3)$ , unde  $\gamma \in \text{Aut}(Q_2, f_3)$ .*

**Definiție.** Un quasigrup  $n$ -ar  $(Q, f)$  este un *quasigrup simplu*, dacă congruențele normale ale quasigrupului  $(Q, f)$  sunt exact congruențele diagonală  $\hat{Q} = \{(q, q) \mid q \in Q\}$  și universală  $Q \times Q$ .

În paragraful 4.2 este demonstrată

**Teorema 4.12.** *Dacă un quasigrup  $n$ -ar medial  $(Q, f)$  de forma  $f(x_1, x_2, \dots, x_n) = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n + a$  peste un grup abelian  $(Q, +)$  este simplu, atunci*

1. *grupul  $(Q, +)$  este grup aditiv al unui câmp finit Galois  $GF(p^k)$ ;*
2. *grupul  $\langle \alpha_1, \dots, \alpha_n \rangle$  este grupul multiplicativ al câmpului  $GF(p^k)$  în cazul  $k > 1$  și grupul  $\langle \alpha_1, \dots, \alpha_n \rangle$  este un subgrup al grupului  $\text{Aut}(Z_p, +)$  în cazul  $k = 1$ ;*
3. *quasigrupul  $(Q, f)$  în cazul  $|Q| > 1$  poate fi un quasigrup din următoarele clase de quasigrupuri separate:*
  - (a)  $\alpha_1 + \alpha_2 + \dots + \alpha_n = \varepsilon, a = 0$ ; *în acest caz quasigrupul  $(Q, f)$  este un quasigrup idempotent;*
  - (b)  $\alpha_1 + \alpha_2 + \dots + \alpha_n = \varepsilon$  și  $a \neq 0$ ; *în acest caz quasigrupul  $(Q, f)$  nu are elemente idempotente, quasigrupul  $(Q, f)$  este izomorf cu quasigrupul  $(Q, g)$  de forma  $g(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n + 1$  peste grupul  $(Q, +)$ ;*
  - (c)  $\alpha_1 + \alpha_2 + \dots + \alpha_n \neq \varepsilon$ ; *în acest caz quasigrupul  $(Q, f)$  are exact un element idempotent, quasigrupul  $(Q, f)$  este izomorf cu un quasigrup  $(Q, g)$  de forma  $g(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$  peste grupul  $(Q, +)$ .*

În următoarele paragrafe sunt detaliate rezultatele obținute asupra structurii quasigrupurilor finite  $n$ -are mediale.

**Definiție.** Un quasigrup  $n$ -ar  $(Q, f)$  este *resolubil*, dacă există un lanț finit de quasigrupuri  $n$ -are

$$Q/Q_1, Q_1/Q_2, \dots, Q_{m-1}/Q_m,$$

unde quasigrupul  $Q_{i+1}$  este un subquasigrup maxim normal al quasigrupului  $Q_i$  și  $m$  este un număr minim cu proprietatea  $|Q_m| = 1$ .

**Propoziția 4.12.** *Orice quasigrup finit  $n$ -ar medial idempotent  $(Q, f)$  este resolubil și orice quasigrup  $Q_i/Q_{i+1}$  este un quasigrup finit  $n$ -ar medial idempotent simplu.*

**Propoziția 4.13.** *Orice quasigrup finit  $n$ -ar medial unipotent  $(Q, f)$  este un quasigrup solubil și orice quasigrup  $Q_i/Q_{i+1}$  este un quasigrup finit  $n$ -ar medial unipotent simplu.*

În subparagraful 4.4.3 este introdusă definiția  $(m, n)$ -ordinului unui element al quasigrupului binar și definiția quasigrupului  $(m, n)$ -liniar. Sunt cercetate unele quasigrupuri, în care toate elementele au  $(m, n)$ -ordine egale.

De exemplu, a fost demonstrată următoarea teoremă.

**Teorema 4.17.** *Dacă într-un  $T$ -quasigrup  $(m, n)$ -liniar  $(Q, \cdot)$  de forma  $x \cdot y = \varphi x + \psi y$  peste un grup abelian  $(Q, +)$  aplicațiile  $\varepsilon - \varphi, \varepsilon - \psi$  sunt permutări ale mulțimii  $Q$ , atunci toate elementele quasigrupului  $(Q, \cdot)$  au ordinul  $(m, n)$ .*

În **Capitolul 5** este cercetată structura grupurilor de autotopii și grupurilor de automorfisme ale quasigrupurilor  $n$ -are liniare, quasigrupurilor distributive la stânga și unii izotopi ai lor, mai ales a  $CH$ -quasigrupurilor. Formulăm câteva rezultate obținute în această direcție.

**Teorema 5.3.** *Dacă  $n$ - $T$ -quasigrupul  $(Q, g)$  de forma  $g(x_1, \dots, x_n) = \varphi_1 x_1 + \varphi_2 x_2 + \dots + \varphi_n x_n + a$  are cel puțin un element idempotent, atunci*

$$\text{Aut}(Q, g) \cong K \times C,$$

unde  $K = \{L_b^+ \mid b \in Q, \varphi_1 b + \varphi_2 b + \dots + \varphi_n b = b\}$ ,  $C = \{\omega \in \text{Aut}(Q, +) \mid \omega \varphi_i = \varphi_i \omega \forall i \in \overline{1, n}\}$ .

**Corolarul 5.7.** *Dacă  $n$ - $T$ -quasigrupul  $(Q, g)$  este un quasigrup idempotent de forma  $g(x_1, \dots, x_n) = \varphi_1 x_1 + \varphi_2 x_2 + \dots + \varphi_n x_n$  peste un grup abelian  $(Q, +)$ , atunci*

$$\text{Aut}(Q, g) \cong (Q, +) \times C,$$

$C = \{\omega \in \text{Aut}(Q, +) \mid \omega \varphi_i = \varphi_i \omega \forall i \in \overline{1, n}\}$ .

Fie  $P = \{C(a) - a\} \cap \delta Q$ ,  $C(a)$  - orbita elementului  $a$  în mulțimea  $Q$  la acțiunea grupului  $C$  și  $C$  - un centralizator al elementelor  $\varphi_1, \dots, \varphi_n$  în grupul  $\text{Aut}(Q, +)$ ,  $N$  - nucleul endomorfismului  $\delta$ ,  $\delta = \varphi_1 + \varphi_2 + \dots + \varphi_n - \varepsilon$ ,  $S$  - un stabilizator al elementului  $a$  la acțiunea grupului  $C$  pe mulțimea  $Q$ .

**Teorema 5.4.** *Dacă  $(Q, f)$  este un  $n$ - $T$ -quasigrup de forma  $f(x_1^n) = \varphi_1 x_1 + \varphi_2 x_2 + \dots + \varphi_n x_n + a$  peste un grup abelian  $(Q, +)$ , și mulțimile  $P, N, S$  au ordin finit, atunci*

$$|\text{Aut}(Q, f)| = |P| \cdot |N| \cdot |S|.$$

**Corolarul 5.8.** *Orice  $T$ -quasigrup  $(Q, f)$  finit  $n$ -ar de forma  $f(x_1^n) = \varphi_1 x_1 + \varphi_2 x_2 + \dots + \varphi_n x_n + a$  peste un grup abelian  $(Q, +)$  are grupul de automorfisme identic dacă și numai dacă*

$$(Q, +) \cong \bigoplus_{i=1}^m (Z_2)_i,$$

$(Q, f) \cong (Q, g)$ , unde  $g(x_1^n) = \sum_{i=1}^n (\varphi_i x_i)$ , endomorfismul  $\delta$  este o permutare a mulțimii  $Q$ ,  $|C| = 1$ ,  $C$  este centralizatorul elementelor  $\varphi_1, \dots, \varphi_n$  în grupul  $\text{Aut}(Q, +)$ ,  $m$  este un număr natural.

**Corolarul 5.9.** Orice quasigrup  $(Q, f)$  finit  $n$ -ar medial astfel, încât  $|Q| > 2$  are  $|\text{Aut}(Q, f)| > 1$ .

**Teorema 5.5.** Dacă  $(Q, f) = (Q, g)T_0$  este un izotop al quasigrupului  $n$ -ar idempotent  $(Q, g)$  astfel, încât izotopia  $T_0$  are forma  $(\varepsilon, \dots, \varepsilon, \beta_{i+1}, \varepsilon, \dots, \varepsilon)$  (în acest șir sunt  $(n+1)$  membri) și  $i \in \overline{0, n}$ , atunci  $\text{Aut}(Q, f) = C_{\text{Aut}(Q, g)}(\beta_{i+1})$ .

Exprimăm Teorema 5.6 sub următoarea formă.

**Teoremă 5.6.** Dacă  $(Q, f)$  este un quasigrup finit  $n$ -ar medial și  $(Q, f) \cong (A, f_1) \times (B, f_2)$ , unde quasigrupul  $(A, f_1)$  este un quasigrup medial  $n$ -ar cu un element idempotent unic, și quasigrupul  $(B, f_2)$  este un izotop al quasigrupului  $n$ -ar medial, atunci  $\text{Aut}(Q, f) \cong \text{Aut}(A, f_1) \times \text{Aut}(B, f_2)$ .

Teoremele 5.6, 5.5, 5.3 și Corolarul 5.7 dau informații mai mult sau mai puțin complete asupra grupului de automorfisme ale oricărui quasigrup finit  $n$ -ar medial.

În continuare în acest capitol (paragraful 5.2) sunt studiate grupurile de automorfisme ale quasigrupurilor distributive la stânga și unii izotopi ai lor, inclusiv grupurile de automorfisme ale  $CH$ -quasigrupurilor, quasigrupurilor distributive, quasigrupurilor distributive Steiner. Vom formula câteva din aceste rezultate.

Reamintim, că în [25] este demonstrat că orice quasigrup distributiv la stânga  $(Q, \cdot)$  are forma  $x \cdot y = \varphi x \circ \psi y$ , unde  $(Q, \circ)$  este o  $S$ -buclă,  $\psi \in \text{Aut}(Q, \circ)$ .

**Teorema 5.9.** Dacă  $(Q, \cdot)$  este un quasigrup distributiv la stânga cu forma  $x \cdot y = \varphi x \circ \psi y$ , unde  $(Q, \circ)$  este o  $S$ -buclă,  $\psi \in \text{Aut}(Q, \circ)$ , atunci

$$\text{Aut}(Q, \cdot) \cong LM(Q, \circ) \times (C/LI(Q, \circ)),$$

unde  $C = \{\alpha \in \text{Aut}(Q, \circ) \mid \alpha\psi = \psi\alpha\}$ ,  $LM(Q, \circ) = \langle L_x^\circ \mid x \in Q \rangle$ ,  $LI(Q, \circ) = \{\alpha \in LM(Q, \circ) \mid \alpha 1 = 1\}$ .

**Teorema 5.10.** Dacă  $(Q, \circ)$  este un quasigrup de forma  $x \circ y = (\varphi x + \psi y) + d$ , unde  $x \cdot y = \varphi x + \psi y$  este un quasigrup distributiv la stânga,  $d \in N_r(Q, +)$ ,  $(Q, +)$  este o  $S$ -buclă, atunci  $\text{Aut}(Q, \circ) \cong LM(Q, +) \times (H/LI(Q, +))$ , unde  $H = \{\beta \in C \mid \beta d = d\}$ .

Din Teorema lui Belousov [14] rezultă că orice quasigrup distributiv este izotopic cu o buclă Moufang comutativă (CML)  $(Q, +)$ .

**Corolarul 5.19.** Într-un quasigrup distributiv  $\text{Aut}(Q, \cdot) \cong M(Q, +) \times (C/I)$ , unde  $I$  este grupul de permutări interioare al buclei Moufang comutative.

A fost demonstrat ([84], p. 31), că orice  $CH$ -quasigrup poate fi construit în modul următor:  $x \cdot y = (-x - y) + d$ , unde elementul  $d$  este din centrul lui CML  $(Q, +)$ . O buclă Moufang comutativă  $(Q, +)$  cu identitatea  $3x = 0$  se numește 3-CML.

**Corolarul 5.20.** Dacă  $(Q, \circ)$  este un  $CH$ -quasigrup care este izotopic cu 3-CML  $(Q, +)$ , atunci  $\text{Aut}(Q, \circ) \cong M(Q, +) \times G$ , unde  $G = \{\beta \in (\text{Aut}(Q, +)/I) \mid \beta d = d\}$ .

În **Capitolul 6** sunt expuse unele aplicații ale teoriei quasigrupurilor  $n$ -are la teoria codurilor cu un simbol de control.

Cercetările statistice ale lui J. Verhoeff [138] și D.F. Beckley [10] au arătat că cele mai frecvente erorile comise de operatori în timpul transmisiei de date sunt erorile într-o singură componentă (single), erori transpoziționale (cu alte cuvinte transpoziții adiacente), adică erori de forma  $\dots ab\dots \rightarrow \dots ba\dots$ , și erori de inserție și de ștergere. Menționăm că dacă toate cuvintele codului au lungimi egale, atunci erorile de inserție și de ștergere pot fi ușor detectate.

Transpoziții cu salt  $\dots abc\dots \rightarrow \dots cba\dots$ , erori duble  $\dots aa\dots \rightarrow \dots bb\dots$ , erori fonetice ( $a \neq 0, a \neq 1$ )  $\dots a0\dots \rightarrow \dots 1a\dots$  și erori duble cu salt  $\dots aca\dots \rightarrow \dots bcb\dots$  pot apărea destul de des.

În acest capitol construim coduri destul de simple cu un simbol de control care ne permit să detectăm de fapt toate erorile indicate mai sus.

**Definiție.** [104]. Un sistem de control cu un simbol de control este un cod sistematic peste un alfabet  $Q$  care se obține prin adăugarea la dreapta a unui simbol de control  $a_{n+1}$  la orice cuvânt  $a_1a_2\dots a_n \in Q^n$ :

$$\mathfrak{C} : \begin{cases} Q^n & \longrightarrow Q^{n+1} \\ a_1a_2\dots a_n & \longmapsto a_1a_2\dots a_na_{n+1}. \end{cases}$$

Noi vom spune, că cuvintele de cod  $a_1\dots a_{n+1}$  și  $b_1\dots b_{n+1}$  sunt egale dacă și numai dacă  $a_i = b_i$  pentru toți  $i \in \{1, \dots, n+1\}$ . Uneori cuvântul de cod  $a_1\dots a_{n+1}$  îl vom nota cu  $a_1^{n+1}$ .

Printr-o eroare în cuvântul de cod  $a_1^{n+1}$  al codului  $\mathfrak{C}$  peste un alfabet  $Q$  noi înțelegem așa un cuvânt  $b_1^{n+1} \in Q^{n+1}$  astfel, încât să existe cel puțin un indice  $j \in \overline{1, n+1}$  cu proprietatea  $a_j \neq b_j$ .

Ca de obicei, un cod  $n$ -ar  $(Q, g)$  detectează o eroare într-un cuvânt  $a_1\dots a_na_{n+1}$  primit după o transmisie dacă și numai dacă  $g(a_1^n) \neq a_{n+1}$ .

**Observația principală.** Noi putem privi codul  $\mathfrak{C}$  ca o aplicație peste un alfabet (peste o mulțime  $Q$ ) astfel, încât simbolul de control  $a_{n+1}$  este obținut din simbolurile informaționale  $a_1, a_2, \dots, a_n$  în modul următor:  $g(a_1, a_2, \dots, a_n) = a_{n+1}$ , unde  $g$  este o operație  $n$ -ară pe mulțimea  $Q$ .

**Definiție.** Codul  $\mathfrak{C}$  cu un simbol de control  $a_{n+1}$  peste un alfabet  $Q$  îl notăm ca un *cod  $n$ -ar*  $(Q, g)$ . Dacă într-un cod  $n$ -ar  $(Q, g)$  operația  $g$  este o operație a unui quasigrup  $n$ -ar, atunci codul se numește  *$n$ -quasigrup cod*  $(Q, g)$ .

Următoarea teoremă permite să aplicăm aparatul teoriei quasigrupurilor  $n$ -are la teoria codurilor cu un simbol de control.

**Teorema 6.1.** *Orice cod  $n$ -ar  $(Q, g)$  detectează toate erorile single (într-o singură componentă) dacă și numai dacă codul  $(Q, g)$  este un cod  $n$ -quasigrupal, adică operația  $n$ -ară  $g$  este o operație de  $n$ -quasigrup.*

**Definiție.** Un quasigrup binar  $(Q, \cdot)$  se numește *total anticomutativ* dacă și numai dacă sunt adevărate următoarele implicații:  $x \cdot y = y \cdot x \Rightarrow x = y$ ,  $x \cdot x = y \cdot y \Rightarrow x = y$  pentru orice  $x, y \in Q$ .

**Teorema 6.3.** *Orice cod  $(Q, d)$   $n$ -quasigrupal detectează orice transpoziție și eroare dublă pe locurile de forma  $(i, i + k)$  ( $i \in \overline{1, n - k}, k \in \overline{1, n - 1}, i + k \leq n$ ) dacă și numai dacă toate  $(i, i + k)$ -retractele binare ale  $n$ -quasigrupului  $(Q, d)$  sunt quasigrupuri total anticomutative.*

A fost demonstrată următoarea teoremă care ne dă posibilitatea să construim destul de simplu coduri (sisteme de control) de orice lungime finită cu un simbol de control, care detectează toate erorile single (într-o singură componentă), transpoziționale, duble, transpoziționale cu salt, erori duble cu salt și aproape toate erorile fonetice.

**Teorema 6.8.** *Orice cod  $(n-1)$ - $T$ -quasigrupal  $(Q, g)$  cu ecuația de control (de verificare)  $d(x_1, x_2, \dots, x_n) = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n = 0$  detectează:*

a) *orice eroare transpozițională pe locuri de forma  $(i, i + 1)$ ,  $i \in \overline{1, n - 1}$ , dacă și numai dacă aplicația  $\alpha_i - \alpha_{i+1}$  este un automorfism al grupului  $(Q, +)$ ;*

b) *orice eroare transpozițională pe locuri de forma  $(i, i + 2)$  (adică transpoziții cu salt),  $i \in \overline{1, n - 2}$ , dacă și numai dacă aplicația  $\alpha_i - \alpha_{i+2}$  este un automorfism al grupului  $(Q, +)$ ;*

c) *orice eroare dublă pe locuri de forma  $(i, i + 1)$ ,  $i \in \overline{1, n - 1}$ , dacă și numai dacă aplicația  $\alpha_i + \alpha_{i+1}$  este un automorfism al grupului  $(Q, +)$ ;*

d) *orice eroare dublă pe locuri de forma  $(i, i + 2)$  (adică eroare dublă cu salt),  $i \in \overline{1, n - 2}$ , dacă și numai dacă aplicația  $\alpha_i + \alpha_{i+2}$  este un automorfism al grupului  $(Q, +)$ .*

Un cod  $n$ -quasigrupal care detectează cinci tipuri de erori (single, erorile transpoziționale și duble pe locuri de forma  $(i, i + 1)$ , unde  $i \in \overline{1, n - 1}$ , și pe locuri de forma  $(i, i + 2)$ , unde  $i \in \overline{1, n - 2}$ ), va fi numit cod 5- $n$ -quasigrupal.

**Teorema 6.9.** *Produsul direct a doua coduri 5- $n$ -quasigrupale este tot un cod 5- $n$ -quasigrupal.*

**Teorema 6.14.** *Orice cod 5- $n$ - $T$ -quasigrupal  $(Q, g)$  cu ecuația de control*

$$d(x_1^{n+1}) = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n + \alpha_{n+1} x_{n+1} = 0$$

*detectează toate erorile fonetice de pe toate locurile  $(i, i + 1)$  cu excepția a câteia unei singure erori fonetice pe fiecare loc de forma  $(i, i + 1)$ .*

În subparagraful 6.1.6 sunt construite coduri cu un caracter de control cu caracteristici mai bune decât cele ale binecunoscutelor coduri UPC (Universal Product Code), EAN (European Article Number), ISBN (International System Book Number).

**Teorema 6.15.** *Există coduri 5- $n$ - $T$ -quasigrupale pentru orice ordin prim  $p \geq 7$ ; pentru orice ordin  $m^2$  cu  $m > 1$ ; pentru orice ordin compozit  $d$  astfel încât  $d = m^2 p_1 p_2 \dots p_s$ , unde  $m \geq 1$ ,  $p_i \geq 7$ .*

Sistemul numerelor de serii ale bancnotelor germane este unul dintre cele mai vechi și cele mai renumite sisteme de control cu un simbol de control. În subparagraful 6.1.7 sunt enumerate următoarele erori : transpoziționale cu salt, erori duble, erori fonetice și erori duble cu salt, care nu detectează acest cod.

Funcția de semn (sign function) este un omomorfism  $\varphi$  al grupului simetric  $S_n$  pe grupul  $Z_2$ ,  $Z_2 = \{1, -1\}$ , astfel că  $\varphi\alpha = -1$ , dacă permutarea  $\alpha$  este egală cu produsul

unui număr impar al ciclurilor de lungimea 2,  $\varphi\alpha = 1$ , dacă permutarea  $\alpha$  este egală cu produsul unui număr par al ciclurilor de lungimea 2.

În paragraful 6.2 sunt descrise semnele translațiilor la stânga, la dreapta, medii și semnul produsului tuturor translațiilor la stânga (la dreapta, medii) ale buclei Bol finite.

Fie  $(Q, \cdot)$  un quasigrup,  $|Q| = n$ . Vom utiliza următoarele notații:  $\text{sgn } \mathbf{L} = \prod_{i=1}^n \text{sgn}(L_{a_i})$ ,  $\text{sgn } \mathbf{R} = \prod_{i=1}^n \text{sgn}(R_{a_i})$ ,  $\text{sgn } \mathbf{I} = \prod_{i=1}^n \text{sgn}(I_{a_i})$ , unde  $a_i \in Q$ ; mai departe  $\text{tsgn } Q = \langle \text{sgn } \mathbf{L}, \text{sgn } \mathbf{R}, \text{sgn } \mathbf{I} \rangle$ .

**Teorema 6.16.** *Fie  $Q$  o buclă Moufang finită. Dacă  $|Q| = 4k$ , atunci  $\text{tsgn } Q = \langle 1, 1, 1 \rangle$ ; dacă  $|Q| = 4k + 1$ , atunci  $\text{tsgn } Q = \langle 1, 1, 1 \rangle$ ; dacă  $|Q| = 4k + 2$ , atunci  $\text{tsgn } Q = \langle -1, -1, -1 \rangle$ ; dacă  $|Q| = 4k + 3$ , atunci  $\text{tsgn } Q = \langle 1, 1, -1 \rangle$ .*

În **Capitolul 7** se dezvoltă o concepție veche, binecunoscută [85], de ortogonalitate a grupoizilor binari, quasigrupurilor de stânga (dreapta) și quasigrupurilor în limbajul al  $m$ -colecțiilor de aplicații, în principal, în limbajul  $m$ -colecțiilor de permutări.

Grupoizii  $(Q, \cdot)$  și  $(Q, *)$  sunt *ortogonali* ( $(Q, \cdot) \perp (Q, *)$ ), dacă sistemul de ecuații  $x \cdot y = a$  și  $x * y = b$  are o singură soluție pentru orice  $a, b \in Q$ .

Sunt stabilite condiții necesare și suficiente ca un quasigrup să fie ortogonal pe unul dintre parastroficele lui.

**Teorema 7.9.** *Pentru un quasigrup finit  $(Q, \cdot)$  sunt îndeplinite următoarele echivalențe:*

- (i)  $(Q, \cdot) \perp (Q, \cdot)^{(12)} \iff ((x \setminus yz)x = zy \implies x = y)$ ;
- (ii)  $(Q, \cdot) \perp (Q, \cdot)^{(13)} \iff (zx \cdot x = zy \cdot y \implies x = y)$ ;
- (iii)  $(Q, \cdot) \perp (Q, \cdot)^{(23)} \iff (x \cdot xz = y \cdot yz \implies x = y)$ ;
- (iv)  $(Q, \cdot) \perp (Q, \cdot)^{(123)} \iff (x \cdot zx = y \cdot zy \implies x = y)$ ;
- (v)  $(Q, \cdot) \perp (Q, \cdot)^{(132)} \iff (xz \cdot x = yz \cdot y \implies x = y)$ .

În paragraful 7.3 sunt cercetate unele transformări ale grupoizilor și quasigrupurilor care păstrează proprietatea ortogonalității lor.

**Corolarul 7.14.** *Grupoizii  $(Q, A)$  și  $(Q, B)$  sunt ortogonali dacă și numai dacă  $(Q, A)\beta \perp (Q, B)\beta$ , unde  $\beta \in \text{ISOS}_{(12)}(Q)$ .  $\text{ISOS}_{(12)}(Q)$  este grupul tuturor izotopiilor și (12)-izostrofiilor ai mulțimii  $Q$ .*

O colecție de aplicații  $P$  are speța  $l$  dacă și numai dacă  $P$  constă din translațiile la stânga ale unui grupoid, are speța  $r$  dacă și numai dacă  $P$  constă din translațiile la dreapta ale unui grupoid, etc.

**Definiție.** Orice  $m$ -colecție de permutări  $P$  de speța  $\alpha$ ,  $\alpha \in \{l, Il, r, Ir, p, Ip\}$ , se numește *izotopie generalizată de speța  $\alpha$*  sau *gizotopie de speța  $\alpha$* .

**Propoziția 7.16.** *Acțiunea gizotopiei  $P = (p_1, p_2, \dots, p_n, \dots)$  de speța  $l$  pe un grupoid  $(Q, \cdot)$  coincide cu acțiunea colecției  $T$  a izotopiilor de forma  $T = ((\varepsilon, p_1, \varepsilon), (\varepsilon, p_2, \varepsilon), \dots, (\varepsilon, p_i, \varepsilon), \dots)$ , unde izotopia  $(\varepsilon, p_i, \varepsilon)$  acționează numai la rândul  $i$  al tabelului lui Cayley al grupoidului  $(Q, \cdot)$ .*

**Propoziția 7.21.** *Pătratele  $S_1$  și  $S_2$ , ambele de speța  $\alpha$ ,  $\alpha \in \{l, r\}$ , sunt ortogonale dacă și numai dacă imaginile gizotopice ale lor  $S_1P$  și  $S_2P$  sunt ortogonale, unde  $P$  este o gizotopie de speța  $\alpha$ .*

În paragraful 7.4 sunt formulate condițiile de ortogonalitate ale perechii  $T$ -quasigrupurilor, care sunt definite pe același grup abelian  $(Q, +)$  (nu este necesar ca ordinul mulțimii  $|Q|$  să fie finit). În același mod cercetăm ortogonalitatea  $T$ -quasigrupurilor parastrofice.

**Teorema 7.14.** *Un  $T$ -quasigrup  $(Q, \cdot)$  de forma  $x \cdot y = \alpha x + \beta y + c$  și un  $T$ -quasigrup  $(Q, \circ)$  de forma  $x \circ y = \gamma x + \delta y + d$ , ambele definite pe un grup comutativ  $(Q, +)$ , sunt ortogonale dacă și numai dacă aplicația  $\alpha^{-1}\beta - \gamma^{-1}\delta$  este un automorfism al grupului  $(Q, +)$ .*

Ortogonalitatea unui quasigrup și a (12)-parastrofului este mai clară din punct de vedere intuitiv, această ortogonalitate a fost studiată în multe lucrări [15, 100, 42, 34].

A. Sade [100, 42] a numit un quasigrup  $(Q, \cdot)$  *antiabelian* dacă  $(Q, \cdot)$  este ortogonal cu (12)-parastroful lui  $(Q, \star)$ : cu alte cuvinte, dacă  $x \cdot y = z \cdot t$  și  $y \cdot x = t \cdot z$  ( $x \star y = z \star t$ ) implică  $x = z$  și  $y = t$ .

**Teorema 7.17.** *Pentru un  $T$ -quasigrup  $(Q, \cdot)$  de forma  $x \cdot y = \varphi x + \psi y + c$  peste un grup comutativ  $(Q, +)$  sunt echivalente următoarele condiții:*

- $(x \cdot y = y \cdot x) \Rightarrow (x = y)$ ,  $(x \cdot x = y \cdot y) \Rightarrow (x = y)$  pentru toți  $x, y \in Q$ ;*
- $(x \cdot y = z \cdot t$  și  $y \cdot x = t \cdot z) \Rightarrow (x = z \text{ și } y = t)$  pentru toți  $x, y, z, t \in Q$ ;*
- aplicațiile  $\varphi - \psi$  și  $\varphi + \psi$  sunt permutări ale mulțimii  $Q$ ;*
- aplicațiile  $s\varphi^{-1} - \psi^{-1}$  și  $\varphi + \psi$  sunt permutări ale mulțimii  $Q$ ;*
- aplicația  $\varphi^{-1}\psi - \psi^{-1}\varphi$  este o permutare a mulțimii  $Q$ ;*
- $T$ -quasigrupul  $(Q, \cdot)$  și (12)-parastroful lui  $(Q, \star)$  sunt ortogonali.*

În [34] Bennett și Zhang studiază pătratele latine cu parastrofe ortogonale conjugate. Aceste pătrate corespund quasigrupurilor cu proprietatea:  $(Q, A^\sigma) \perp (Q, A^\sigma)^{(12)}$  pentru orice  $\sigma \in S_3$ . Pentru simplitate quasigrupurile cu această proprietate vom numi SOC-quasigrupuri.

Pentru SOC- $T$ -quasigrupuri putem demonstra

**Teorema 7.18.** *Un  $T$ -quasigrup  $(Q, \cdot)$  de forma  $x \cdot y = \varphi x + \psi y + c$  peste un grup abelian  $(Q, +)$  este un SOC-quasigrup dacă și numai dacă aplicațiile  $\varphi - \psi$ ,  $\varphi + \psi$ ,  $\varepsilon - \psi$ ,  $\varepsilon + \psi$ ,  $\varepsilon - \varphi$  și  $\varepsilon + \varphi$  sunt permutări ale mulțimii  $Q$ .*

S-a demonstrat ca clasa SOC-quasigrupurilor și clasa quasigrupurilor, care sunt ortogonale cu orice parastrof al lor, se intersectează dar nu coincid.

## Bibliografie

- [1] A.A. Albert, *Quasigroups. I*, Trans. Amer. Math. Soc. **54** (1943), 507–519.
- [2] A.A. Albert, *Quasigroups. II*, Trans. Amer. Math. Soc. **55** (1944), 401–419.
- [3] R. Artzy, *On loops with a special property*, Proc. Amer. Math. Soc. **6** (1955), 448–453.
- [4] R. Artzy, *Crossed-inverse and related loops*, Trans. Amer. Math. Soc. **91** (1959), 480–492.
- [5] R. Artzy, *Relation between loop identities*, Proc. Amer. Math. Soc. **11** (1960), 847–851.
- [6] R. Baer, *Nets and groups, I*, Trans. Amer. Math. Soc. **46** (1939), 110–141.
- [7] R. Baer, *Nets and groups, II*, Trans. Amer. Math. Soc. **47** (1940), 435–439.

- [8] A.S. Basarab, *Loops with weak inverse property*, Ph.D. thesis, IM AN MSSR, 1968, (in Russian).
- [9] A.S. Basarab and L.L. Kiriyak, *A class of G-loops*, Mat. Issled. **71** (1983), 3–6, (in Russian).
- [10] D.F. Beckley, *An optimum systems with modulo 11*, The Computer Bulletin **11** (1967), 213–215.
- [11] V.D. Belousov, *On the structure of distributive quasigroups*, Uspekhi Mat. Nauk **13** (1958), no. 3, 235 – 236, (in Russian).
- [12] V.D. Belousov, *Regular permutations in quasigroups*, Uchenye zapiski Bel'tskogo pedinstituta **1** (1958), 39 – 49, (in Russian).
- [13] V.D. Belousov, *Balanced identities on quasigroups*, Mat. Sbornik **70** (1966), 55 – 97, (in Russian).
- [14] V.D. Belousov, *Foundations of the theory of quasigroups and loops*, Nauka, Moscow, 1967, (in Russian).
- [15] V.D. Belousov, *Systems of orthogonal operations*, Mat. Sbornik **77 (119)** (1968), no. 1, 38 – 58, (in Russian).
- [16] V.D. Belousov, *Algebraic nets and quasigroups*, Stiintsa, Kishinev, 1971, (in Russian).
- [17] V.D. Belousov, *n-Ary quasigroups*, Stiintsa, Kishinev, 1971, (in Russian).
- [18] V.D. Belousov, *The equation of generalized mediality*, Mat. Issled. **39** (1976), 21– 31, (in Russian).
- [19] V.D. Belousov, *Configurations in algebraic nets*, Shtiinta, Kishinev, 1979, (in Russian).
- [20] V.D. Belousov, *Elements of quasigroup theory: a special course*, Kishinev State University Printing House, Kishinev, 1981, (in Russian).
- [21] V.D. Belousov, *Inverse loops*, Mat. Issled. **95** (1987), 3 – 22, (in Russian).
- [22] V.D. Belousov, *Autotopies in inverse loops*, Mat. Issled. **120** (1991), 30 – 44, (in Russian).
- [23] V.D. Belousov, *Parastrophic-orthogonal quasigroups*, Quasigroups Relat. Syst. **13** (2005), no. 1, 25 – 72.
- [24] V.D. Belousov and G.B. Belyavskaya, *Latin squares, quasigroups and their applications*, Shtiinta, Kishinev, 1989, (in Russian).
- [25] V.D. Belousov and V.I. Onoi, *On loops that are isotopic to left distributive quasigroups*, Mat. Issled. **3(25)** (1972), 135 – 152, (in Russian).
- [26] V.D. Belousov and M.D. Sandik, *n-Ary quasigroups and loops*, Siberian Math. J. **VII** (1966), 31 – 54, (in Russian).
- [27] V.D. Belousov and B.V. Tsurkan, *Crossed-inverse quasigroups (CI-quasigroups)*, Izv. Vyssh. Uchebn. Zaved. Mat. **82** (1969), no. 3, 21 – 27, (in Russian).
- [28] G.B. Belyavskaya, *Nuclei and centre of a quasigroup*, Mat. Issled. **102** (1988), 37 – 52, (in Russian).
- [29] G.B. Belyavskaya, *Abelian quasigroups are T-quasigroups*, Quasigroups Relat. Syst. **1** (1994), 1–7.
- [30] G.B. Belyavskaya, *Quasigroup theory: nuclei, centre, commutants*, Bul. Acad. Stiinte Repub. Mold., Mat. (1996), no. 2(21), 47–71, (in Russian).

- [31] G.B. Belyavskaya, W. A. Dudek, and V. A. Shcherbacov, *Valentin Danilovich Belousov – his life and work*, Quasigroups Relat. Syst. **13** (2005), 1–7.
- [32] G.B. Belyavskaya and A.Kh. Tabarov, *The nuclei and center of linear quasigroups*, Bul. Acad. Stiinte Repub. Mold., Mat. (1991), no. 3(6), 37–42, (in Russian).
- [33] G.B. Belyavskaya and A.Kh. Tabarov, *One-sided T-quasigroups and irreducible balanced identities*, Quasigroups Relat. Syst. **1** (1994), 8–21.
- [34] F.E. Bennett and H. Zhang, *Latin squares with self-orthogonal conjugates*, Discrete Math. **284** (2004), 45–55.
- [35] R.H. Bruck, *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. **55** (1944), 19 – 52.
- [36] R.H. Bruck, *Contribution to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245 – 354.
- [37] R.H. Bruck, *A survey of binary systems*, third printing, corrected ed., Springer Verlag, New York, 1971.
- [38] C. Burstin and W. Mayer, *Distributive Gruppen von endliher Ordnung*, J. Reine und Angew. Math. **160** (1929), 111–130.
- [39] O. Chein, H.O. Pflugfelder, and J.D.H. Smith, *Quasigroups and loops: Theory and applications*, Heldermann Verlag, 1990.
- [40] Dug-Hwan Choi and Jonathan D.H. Smith, *Greedy loop transversal codes for correcting error burts*, Discrete Math. **264** (2003), 37–43.
- [41] A.H. Clifford and G.B. Preston, *The algebraic theory of semigroups*, vol. I, American Mathematical Society, Rhode Island, 1961.
- [42] J. Dénes and A. D. Keedwell, *Latin squares and their applications*, Akadémiai Kiadó, Budapest, 1974.
- [43] J. Dénes and A. D. Keedwell, *Latin squares. New development in the theory and applications*, Annals of Discrete Mathematics, vol. 46, North-Holland, 1991.
- [44] J. Dénes and A. D. Keedwell, *A new authentication scheme based on latin squres*, Discrete Math. **106/107** (1992), 157–165.
- [45] J. Dénes and A. D. Keedwell, *Some applications of non-associative algebraic systems in cryptology*, P.U.M.A. **12** (2002), no. 2, 147–195.
- [46] L. E. Dickson, *On semigroups and the general isomorphism between infinite groups*, Trans. Amer. Math. Soc. **6** (1905), 205–208.
- [47] W. Dornte, *Untersuhungen über einen veralgemeinerten Gruppenbegriff*, Math. Z. **29** (1928), 1–19.
- [48] W.A. Dudek, *On number of transitive distributive quasigroups*, Mat. Issled. **120** (1991), 64–76, (in Russian).
- [49] W.A. Dudek and V.A. Shcherbacov, *Remarks to the first publications of V. D. Belousov*, Quasigroups Relat. Syst. **13** (2005), 13–24.
- [50] W.A. Dudek and P.N. Syrбу, *About self-orthogonal n-groups*, Bul. Acad. Stiinte Repub. Mold., Mat. (1992), no. 3, 37–42, (in Russian).
- [51] T. Evans, *Abstract mean values*, Duke Math. J. **30** (1963), 331–347.

- [52] I.A. Florea, *Quasigroups with inverse property*, Ph.D. thesis, IM AN MSSR, 1965, (in Russian).
- [53] M. M. Glukhov and Kh. S. Rasulov, *Special  $C$ -equivalence of finite one-side invertible quasigroups*, Diskretn. Mat. **6** (1994), no. 3, 3–16, (in Russian).
- [54] L. M. Gluskin, *Positional operatives*, Mat. Sb. **110** (1965), 444–472, (in Russian).
- [55] A. A. Gvaramiya, *Quasivarieties of automata. Relations with quasigroups*, Sibirsk. Mat. Zh. **26** (1985), no. 3, 11–30, (in Russian).
- [56] A. A. Gvaramiya, *Representations of quasigroups, and quasigroup automata*, Fundam. Prikl. Mat. **3** (1997), no. 3, 775–800, (in Russian).
- [57] D. Herbera, T. Kepka, and P. Némec, *Hamiltonian selfdistributive quasigroups*, J. Algebra **289** (2005), no. 1, 70–104.
- [58] M. Hosszu, *On the explicit form of  $n$ -group operations*, Publ. Math. Debrecen, **10**, (1963), 88–92.
- [59] S.G. Ibragimov, *About the logic-algebraic works of Ernest Schröder which have anticipated the theory of quasigroups*, Kibernetika i logika, Nauka, Moscow, 1978, (in Russian), pp. 253–313.
- [60] V.I. Izbash, *On quasigroups isotopic to groups*, 1989, Reg. in VINITI 29.06.89, No 4228-B89, Moscow (in Russian).
- [61] V.I. Izbash, *Isomorphisms of quasigroups isotopic to groups*, Quasigroups Relat. Syst. **2** (1995), 34–50.
- [62] V.I. Izbash and V.A. Shcherbacov, *On quasigroups with Moufang identity*, Abstracts of The Third International Conference in memory of M.I. Kargapolov (1928-1976) (Krasnoyarsk, Russian Federation), August 1993, (in Russian), pp. 134–135.
- [63] J. Ježek and T. Kepka, *Varieties of abelian quasigroups*, Czech. Math. J. **27** (1977), 473–503.
- [64] B. B. Karklin´š and V. B. Karklin´, *Inverse loops*, Mat. Issled. **39** (1976), 87–101, (in Russian).
- [65] A.D. Keedwell, *Crossed-inverse quasigroups with long inverse cycles and applications to cryptography*, Australas. J. Combin. **20** (1999), 241–250.
- [66] A.D. Keedwell and V.A. Shcherbacov, *On  $m$ -inverse loops and quasigroups with a long inverse cycle*, Australas. J. Combin. **26** (2002), 99–119.
- [67] A.D. Keedwell and V.A. Shcherbacov, *Construction and properties of  $(r,s,t)$ -inverse quasigroups, I*, Discrete Math. **266** (2003), no. 1-3, 275–291.
- [68] A.D. Keedwell and V.A. Shcherbacov, *Construction and properties of  $(r,s,t)$ -inverse quasigroups, II*, Discrete Math. **288** (2004), 61–71.
- [69] A.D. Keedwell and V.A. Shcherbacov, *Quasigroups with an inverse property and generalized parastrophic identities*, Quasigroups Relat. Syst. **13** (2005), 109–124.
- [70] T. Kepka, *Regular mappings of groupoids*, Acta Univ. Carolin. Math. Phys. **12** (1971), 25–37.
- [71] T. Kepka, *Structure of weakly abelian quasigroups*, Czech. Math. J. **28** (1978), 181–188.
- [72] T. Kepka,  *$F$ -quasigroups isotopic to Moufang loops*, Czech. Math. J. **29** (1979), 62–83.

- [73] T. Kepka, M.K. Kinyon, and J. D. Phillips, *The structure of  $F$ -quasigroups*, <http://arxiv.org/abs/math/0510298> (2005), 24 pages.
- [74] T. Kepka and P. Nĕmec, *T-quasigroups, II*, Acta Univ. Carolin. Math. Phys. **12** (1971), no. 2, 31–49.
- [75] T. Kepka and P. Nĕmec, *Commutative Moufang loops and distributive groupoids of small order*, Czech. Math. J. **31** (1981), 633–670.
- [76] H. Kiechle, *Theory of  $K$ -loops*, Habilitationsschrift, Fachbereich Mathematik der Universität Hamburg, Hamburg, 1998, (Habilitation Dissertation).
- [77] O.U. Kirnasovsky, *Linear isotopes of small order*, Quasigroups Relat. Syst. **2** (1995), 51–82.
- [78] O.U. Kirnasovsky, *The transitive and multitransitive automorphism group of the multi-place quasigroups*, Quasigroups Relat. Syst. **4** (1997), 23–38.
- [79] O.U. Kirnasovsky, *Binary and  $n$ -ary isotopes of groups, main algebraic notations and quantitative characteristics*, Ph.D. thesis, Taras Shevchenko Kiev State University, Kiev, 2000, (in Ukrainian).
- [80] K. Kishen, *On the construction of latin and hyper-graceo-latin cubes and hypercubes*, J. Ind. Soc. Agric. Statist. **2** (1950), 20–48.
- [81] K. Kunen, *Moufang quasigroups*, J. Algebra **183** (1996), 231–234.
- [82] A.V. Kuznetsov and E.A. Kuznetsov, *On two generated two homogeneous quasigroups*, Mat. Issled. **71** (1983), 34–53, (in Russian).
- [83] Charles F. Laywine and Gary L. Mullen, *Discrete mathematics using latin squares*, John Wiley & Sons, Inc., New York, 1998.
- [84] Yu.I. Manin, *Cubic forms*, Nauka, Moscow, 1972, (in Russian).
- [85] H.B. Mann, *The construction of orthogonal latin squares*, Ann. Math. Statist. **13** (1942), 418–423.
- [86] H.B. Mann, *Analizes and design of experiments*, Dover, New York, 1949.
- [87] R. Moufang, *Zur Structur von Alternativ Körpern*, Math. Ann. **110** (1935), 416–430.
- [88] G.L. Mullen and V.A. Shcherbacov, *Properties of codes with one check symbol from a quasigroup point of view*, Bul. Acad. Stiinte Repub. Mold., Mat. (2002), no. 3, 71–86.
- [89] G.L. Mullen and V.A. Shcherbacov,  *$n$ - $T$ -quasigroup codes with one check symbol and their error detection capabilities*, Comment. Math. Univ. Carolin. **45** (2004), no. 2, 321–340.
- [90] D.C. Murdoch, *Quasigroups which satisfy certain generalized associative laws*, Amer. J. Math. **61** (1939), 509–522.
- [91] D.C. Murdoch, *Structure of abelian quasigroups*, Trans. Amer. Math. Soc. **49** (1941), 392–409.
- [92] A.I. Nesterov and L. V. Sabinin, *Non-associative geometry and discrete structure of space-time*, Comment. Math. Univ. Carolin. **41** (2000), no. 2, 347–357.
- [93] D.A. Norton, *Group of orthogonal row-latin squares*, Pacific J. Math. **2** (1952), 335–341.
- [94] P. Nĕmec, *Arithmetical forms of quasigroups*, Comment. Math. Univ. Carolin. **29** (1988), no. 2, 295–302.

- [95] P. Němec, *Commutative Moufang loops corresponding to linear quasigroups*, Comment. Math. Univ. Carolin. **29** (1988), no. 2, 303–308.
- [96] P. Němec and T. Kepka, *T-quasigroups, I*, Acta Univ. Carolin. Math. Phys. **12** (1971), no. 1, 39–49.
- [97] V.I. Onoi, *Solution of one problem on inverse loops*, Mat. Issled. **71** (1980), 53–58, (in Russian).
- [98] M. Osborn, *Loops with the weak inverse property*, Pacific J. Math. **10** (1960), 295–304.
- [99] E. L. Post, *Polyadic groups*, Trans. Amer. Math. Soc. **48** (1940), 208–350.
- [100] A. Sade, *Produit direct-singulier de quasigroupes orthogonaux et anti-abeliens*, Ann. Soc. Sci. Bruxelles **74** (1960), 91–99.
- [101] L.V. Safonova and K.K. Shchukin, *Computation of the automorphisms and anti-automorphisms of quasigroups*, Bul. Acad. Stiinte Repub. Mold., Mat. (1990), no. 3, 49–55, (in Russian).
- [102] R. Schauffler, *Über die Bildung von Codewörter*, Arch. Elektr. Übertragung **10** (1956), 303 – 314.
- [103] R.H. Schulz, *Equivalence of check digit systems over the dicyclic groups of order 8 and 12*, Mathematikdidaktik aus Begeisterung für die Mathematik (J. Blankenagel and W. Spiegel, eds.), Klett Verlag, Stuttgart, 2000, pp. 227–237.
- [104] R.H. Schulz, *Check character systems and anti-symmetric mappings*, Computational Discrete Mathematics, LNCS, vol. 2122, Springer Verlag, 2001, pp. 136–147.
- [105] V.A. Shcherbacov, *On left distributive quasigroups isotopic to groups*, Proceedings of the XI Conference of Young Scientists of Friendship of Nations University (Moscow), no. 5305-B88, VINITI, 1988, pp. 148–149.
- [106] V.A. Shcherbacov, *About automorphism groups of quasigroups isotopic to groups*, International Conference Universal Algebra, Quasigroups and Related Systems, Abstract of Talks, May 23-28, 1989 (Jadvisin, Poland), 1989, p. 31.
- [107] V.A. Shcherbacov, *On automorphism groups of group isotopes with an idempotent*, International Algebraic Malcev conference, Novosibirsk, August 21 - 26, 1989, Abstr. of Commun. on Model Theory and Algebraic Systems (Novosibirsk), 1989, (in Russian), p. 159.
- [108] V.A. Shcherbacov, *On automorphism groups of group isotopes with an idempotent*, 1989, Reg. in VINITI 19.04.89, No 3530-B89, Moscow, 14 pages. (in Russian).
- [109] V.A. Shcherbacov, *On automorphism groups of quasigroups and linear quasigroups*, 1989, Reg. in VINITI 04.11.89, No 6710-B89, Moscow, 32 pages. (in Russian).
- [110] V.A. Shcherbacov, *On automorphism groups of linear quasigroups*, 1990, Reg. in VINITI 28.09.90, No 5185-B90, Moscow, 12 pages. (in Russian).
- [111] V.A. Shcherbacov, *On automorphism groups and congruences of quasigroups*, Ph.D. thesis, IM AN MSSR, 1991, (in Russian).
- [112] V.A. Shcherbacov, *On automorphism groups and congruences of quasigroups, synopsis of thesis*, Kishinev, 1991, (in Russian).
- [113] V.A. Shcherbacov, *On linear quasigroups and their automorphism groups*, Mat. Issled. **120** (1991), 104 – 113, (in Russian).

- [114] V.A. Shcherbacov, *On automorphism groups of left distributive quasigroups*, Bul. Acad. Stiinte Repub. Mold., Mat. (1994), no. 2, 79–86, (in Russian).
- [115] V.A. Shcherbacov and V.I. Izbash, *On quasigroups with Moufang identity*, Bul. Acad. Stiinte Repub. Mold., Mat. (1998), no. 2, 109–116.
- [116] K.K. Shchukin, *Action of a group on a quasigroup*, Kishinev State University Printing House, Kishinev, 1985, (in Russian).
- [117] K.K. Shchukin, *On simple medial quasigroups*, Mat. Issled. **120** (1991), 114 – 117.
- [118] J.D.H. Smith, *Loop transversals to linear codes*, J. Combin. Inform. System Sci. **17** (1992), 1–8.
- [119] F.N. Sokhatskii, *About isomorphism of linear quasigroups*, Abstracts of The International Algebraic Conference (Barnaul, Russian Federation), August 1991, p. 138.
- [120] F.N. Sokhatskii, *On isotopes of groups, I*, Ukraïn. Mat. Zh. **47** (1995), no. 10, 1387–1398, (in Ukrainian).
- [121] F.N. Sokhatskii, *On isotopes of groups, II*, Ukraïn. Mat. Zh. **47** (1995), no. 12, 1692–1703, (in Ukrainian).
- [122] F.N. Sokhatskii, *On isotopes of groups, III*, Ukraïn. Mat. Zh. **48** (1996), no. 2, 256–260, (in Ukrainian).
- [123] F.N. Sokhatskii, *Some linear conditions and their application to describing group isotopes*, Quasigroups Relat. Syst. **6** (1999), 43–59.
- [124] F.N. Sokhatskii and O. Kirnasovsky, *Subquasigroups and normal congruences for multiplace group isotopes*, Intern. algebraic conference dedicated to the memory of prof. L.M.Gluskin (1922-1985), 25-29 August, 1997. Abstracts of Talks (Slovyans'k, Ukraine), August 1997, pp. 40–41.
- [125] F.N. Sokhatskii and P. Syvakivskyi, *On linear isotopes of cyclic groups*, Quasigroups Relat. Syst. **1** (1994), 66–76.
- [126] E. I. Sokolov, *On the Gluskin-Hosszu theorem for Dörnte  $n$ -groups*, Mat. Issled. **39** (1976), 187–189, (in Russian).
- [127] M. Steinberger, *On loops with a general weak inverse property*, Mitt. Math. Ges. Hamburg **10** (1979), 573–586.
- [128] A.K. Suschkewitsch, *Über die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit*, Math. Ann. **99** (1928), 30–50.
- [129] A.K. Suschkewitsch, *On a generalization of the associative law*, Trans. Amer. Math. Soc. **31** (1929), 204–214.
- [130] A.K. Suschkewitsch, *The theory of generalized groups*, DNTVU, Kiev, 1937, (in Russian).
- [131] P.N. Syrbu, *On congruences on  $n$ -ary  $T$ -quasigroups*, Quasigroups Relat. Syst. **6** (1999), 71–80.
- [132] A.Kh. Tabarov, *Groups of regular permutations and nuclei of linear and close to linear quasigroups*, Bul. Acad. Stiinte Repub. Mold., Mat. (1992), no. 3, 30–36, (in Russian).
- [133] A.Kh. Tabarov, *On the variety of abelian quasigroups*, Diskretn. Mat. **10** (2000), 529–534, (in Russian).
- [134] A.Kh. Tabarov, *On endotopisms of linear and ailinear quasigroups*, The XIVth Conference on Applied and Industrial Mathematics, Communications, August 17–19, Chisinau, 2006, pp. 319–320.

- [135] K. Toyoda, *On axioms of linear functions*, Proc. Imp. Acad. Tokyo **17** (1941), 221 – 227.
- [136] B.V. Tsurkan, *CI-quasigroups with non-empty distributant*, Izv. Vyssh. Uchebn. Zaved. Mat. (1973), no. 5, 84 – 90, (in Russian).
- [137] A. Ungar, *The hyperbolic triangle centroid*, Comment. Math. Univ. Carolin. **45** (2004), no. 2, 355–370.
- [138] J. Verhoeff, *Error detecting decimal codes*, vol. 29, Math. Centrum Amsterdam, 1969.

### Publicații la tema tezei

- [1] G.B. Belyavskaya, V.I. Izbash, and V.A. Shcherbacov, *Check character systems over quasigroups and loops*, Quasigroups Relat. Syst. **10** (2003), 1–28.
- [2] A. Diordiev and V. Shcherbacov, *On the existence of rst-inverse loops of small order*, International conference Loops'03, Praha, August 10 - August 17, 2003, Submitted Abstracts (Praha, Czech Republic), 2003, p. 10.
- [3] W.A. Dudek and V.A. Shcherbacov, *Remarks to the first publications of V. D. Belousov*, Quasigroups Relat. Syst. **13** (2005), 13–24.
- [4] V.I. Izbash and V.A. Shcherbacov, *On quasigroups with Moufang identity*, Abstracts of The Third International Conference in memory of M.I. Kargapolov (1928-1976) (Krasnoyarsk, Russian Federation), August 1993, (in Russian), pp. 134–135.
- [5] A.D. Keedwell and V.A. Shcherbacov, *On m-inverse loops and quasigroups with a long inverse cycle*, Australas. J. Combin. **26** (2002), 99–119.
- [6] A.D. Keedwell and V.A. Shcherbacov, *Construction and properties of (r,s,t)-inverse quasigroups, I*, Discrete Math. **266** (2003), no. 1-3, 275–291.
- [7] A.D. Keedwell and V.A. Shcherbacov, *Construction and properties of (r,s,t)-inverse quasigroups, II*, Discrete Math. **288** (2004), 61–71.
- [8] A.D. Keedwell and V.A. Shcherbacov, *Quasigroups with an inverse property and generalized parastrophic identities*, Quasigroups Relat. Syst. **13** (2005), 109–124.
- [9] A. Marini and V.A. Shcherbacov, *About signs of Bol loop translations*, Tech. Report 97.6, IAMI, Milan, Italy, 1997, 5 pages.
- [10] A. Marini and V.A. Shcherbacov, *About signs of Bol loop translations*, Bul. Acad. Stiinte Repub. Mold., Mat. (1998), no. 3, 87–92.
- [11] A. Marini and V.A. Shcherbacov, *On autotopies and automorphisms of n-ary medial quasigroups*, International conference Loops'03, Submitted Abstracts (Prague), 2003, pp. 26–28.
- [12] A. Marini and V.A. Shcherbacov, *On autotopies and automorphisms of n-ary linear quasigroups*, Algebra and Discrete Math. (2004), no. 2, 51–75.
- [13] G.L. Mullen and V.A. Shcherbacov, *Properties of codes with one check symbol from a quasigroup point of view*, Bul. Acad. Stiinte Repub. Mold., Mat. (2002), no. 3, 71–86.
- [14] G.L. Mullen and V.A. Shcherbacov, *n-T-quasigroup codes with one check symbol and their error detection capabilities*, Comment. Math. Univ. Carolin. **45** (2004), no. 2, 321–340.
- [15] G.L. Mullen and V.A. Shcherbacov, *On orthogonality of binary operations and squares*, Bul. Acad. Stiinte Repub. Mold., Mat. (2005), no. 2 (48), 3–42.

- [16] V.A. Shcherbacov, *About one class of medial quasigroups*, Mat. Issled. 102 (1988), 111–116, (in Russian).
- [17] **V.A. Shcherbacov, *On automorphism groups of left distributive quasigroups*, Bul. Acad. Stiinte Repub. Mold., Mat. (1994), no. 2, 79–86, (in Russian).**
- [18] V.A. Shcherbacov, *Signs on loop Moufang latin squares*, The Third ROMAI Conference Applied and Industrial Mathematics, Oradea, Romania and Chishinau, Moldova Abstracts (Chisinau), August 1995, p. 21.
- [19] **V.A. Shcherbacov, *About signs of Moufang loop translations*, Bul. Acad. Stiinte Repub. Mold., Mat. (1996), no. 1, 17–19.**
- [20] V.A. Shcherbacov, *About automorphisms and isomorphisms of quasigroups*, Intern. conf. on Math. and Informatics. Abstracts (Chisinau), September 1996, p. 41.
- [21] V.A. Shcherbacov, *On signs of loop translations*, Intern. algebraic conference dedicated to the memory of prof. L.M. Gluskin (1922-1985), Abstracts (Slovyans'k), August 1997, p. 39.
- [22] V.A. Shcherbacov, *On normality of congruences of loops*, International conference Loops'99, Submitted Abstracts (Prague), August 1999, pp. 34–35.
- [23] **V.A. Shcherbacov, *On 20 Belousov's problem*, Tech. Report 99.8, IAMI, Milan, Italy, 1999.**
- [24] V.A. Shcherbacov, *On Bruck-Toyoda-Murdoch theorem and isomorphisms of some quasigroups*, First Conference of the Mathematical Society of the Republic Moldova, Abstracts (Chisinau), August 2001, pp. 138–139.
- [25] V.A. Shcherbacov, *On loops with the property  $(x^{-1})^{-1} = x$* , Third International Algebraic Conference in Ukraine, Submitted Abstracts (Sumy), July 2001, p. 104.
- [26] **V.A. Shcherbacov, *On  $n$ -ary quasigroups and their possible applications in coding theory and cryptography*, International Congress of Mathematicians. Abstracts of Short Communications and Poster Session (Beijing), August 2002, p. 30.**
- [27] V.A. Shcherbacov, *About orthogonality of a quasigroup and its parastrophes*, International Conference on Radicals (ICOR-2003), Program and Abstracts (Chisinau), August 2003, pp. 47–48.
- [28] V.A. Shcherbacov, *On automorphisms of  $n$ -ary  $T$ -quasigroups*, V international conference Algebra and Number Theory: Collection of Abstracts (Tula), May 2003, pp. 289–290.
- [29] V.A. Shcherbacov, *On autotopies and automorphisms of  $n$ -ary medial quasigroups*, 4th International Algebraic Conference in Ukraine, Abstracts (Lviv), August 2003, pp. 205–206.
- [30] V.A. Shcherbacov, *On possibilities of the system of the serial numbers of german banknotes to detect the most frequent errors and on some new systems of such kind*, The 11-th Conference Applied and Industrial Mathematics, Abstracts (Oradea), May 2003, p. 63.
- [31] V.A. Shcherbacov, *About orders of elements in quasigroups*, IX Byelorussian mathematical conference, Abstract of Talks (Grodno), November 2004, pp. 18–20.
- [32] V.A. Shcherbacov, *Error detection capabilities of codes with one check symbol and  $n$ -ary quasigroups*, IV International Conference on Information Technologies 2004, Abstracts on BiT+ (Chisinau), vol. 4, May 2004, p. 165.
- [33] **V.A. Shcherbacov, *On orders of elements in quasigroups*, Bul. Acad. Stiinte Repub. Mold., Mat. (2004), no. 2, 49–54.**
- [34] **V.A. Shcherbacov, *On Bruck-Belousov problem*, Bul. Acad. Stiinte Repub. Mold., Mat. (2005), no. 3, 123–140.**

- [35] V.A. Shcherbacov, *On simple  $n$ -ary medial quasigroups*, Proceedings of Conference Computational Commutative and Non-Commutative Algebraic Geometry, NATO Sci. Ser. F Comput. Syst. Sci., vol. 196, IOS Press, 2005, pp. 305–324.
- [36] V.A. Shcherbacov, *On structure of finite  $n$ -ary medial quasigroups and automorphism groups of these quasigroups*, Quasigroups Relat. Syst. 13 (2005), 125–156.
- [37] V.A. Shcherbacov, *On the structure of finite medial quasigroups*, Bul. Acad. Stiinte Repub. Mold., Mat. (2005), no. 1, 11–18.
- [38] V.A. Shcherbacov, *On finite simple  $n$ -ary medial quasigroups*, XIV International conference Problems of theoretical cybernetics, Penza, May 23-28, 2005, Abstracts of Talks, Moscow, 2005, p. 179, (in Russian).
- [39] V.A. Shcherbacov, *Transformations of groupoids which preserve the property of orthogonality*, Mathematics applied in biology and biophysics, Abstracts, Iasi, June 16-17, 2006, 2006, pp. 35–36.
- [40] V.A. Shcherbacov, *On parastroph orthogonality of finite binary quasigroups*, International Conference on Radicals, Abstracts. July 30 – August 5, 2006, Kyiv, Ukraine, pp. 66-67.
- [41]. V.A. Shcherbacov, *About structure of finite  $n$ -ary medial quasigroups and their automorphism groups*, The XIVth conference on applied and industrial mathematics, Communications, Chisinau, August 17–19, 2006, pp. 316-317.
- [42] V.A. Shcherbacov and V.I. Izbash, *On quasigroups with Moufang identity*, Bul. Acad. Stiinte Repub. Mold., Mat. (1998), no. 2, 109–116.
- [43]. V.A. Shcherbacov, *On automorphism groups of leftdistributive quasigroups*, Collection of Theses of the III International Conference on Algebra, Krasnojarsk, August 23-28, 1993, 1993, (in Russian), pp. 371–372.
- [44]. V.A. Shcherbacov, *On automorphisms of  $n$ - $T$ -quasigroups and structure of  $n$ -ary medial quasigroups*, 5th International Algebraic Conference in Ukraine Odessa, July, 20-27, 2005, Abstracts (Odessa), 2005, pp. 189–190.

## Adnotare

la teza de doctor habilitat a domnului V. Șcerbacov

“Despre quasigrupuri liniare și inverse și aplicarea lor în teoria codurilor”

În lucrare au fost cercetate quasigrupurile  $n$ -are și binare și unele aplicații ale lor în teoria codurilor. Au fost obținute următoarele rezultate:

- Au fost introduse clase noi ale quasigrupurilor binare inverse ( $(r, s, t)$ -inverse,  $(\alpha, \beta, \gamma)$ -inverse) și cercetate proprietățile lor.
- A fost demonstrată că un quasigrup cu orice identitate Moufang este o buclă.
- A fost obținut un progres în rezolvarea problemei Bruck-Belousov despre normalitatea congruențelor quasigrupurilor pentru bucele de stînga (de dreapta).
- A fost descrisă structura quasigrupurilor  $n$ -are mediale simple.
- A fost descrisă structura quasigrupurilor  $n$ -are finite mediale.
- Au fost cercetate grupurile automorfismelor  $T$ -quasigrupurilor  $n$ -are, quasigrupurilor  $n$ -are mediale și niște isotopi ai quasigrupurilor distributive la stînga.
- Au fost elaborate familii noi ale codurilor, care sunt construite în mod simplu și care au caracteristici mai bune decât codurile cunoscute de același tip.
- Au fost obținute condițiile necesare și suficiente despre ortogonalitatea unui quasigrup finit și orice parastrof al lui.

Teza este scrisă în limba engleză.

**Cuvinte cheie:** quasigrup, quasigrup  $n$ -ar, quasigrup liniar, quasigrup invers, quasigrup medial, patrat Latin, cod, automorfism, ortogonalitate.

## Annotation

on thesis for a Doctor's Degree of V.A. Shcherbacov

“On linear and inverse quasigroups and their applications in code theory”

This thesis is devoted to the theory of  $n$ -ary and binary quasigroups and their applications in code theory. The following results are obtained:

- New classes of binary inverse ( $(r, s, t)$ -inverse,  $(\alpha, \beta, \gamma)$ -inverse) quasigroups are introduced, their properties are researched.
- It is proved that quasigroup with any Moufang identity is a loop.
- Some progress in the solving of Bruck–Belousov problem on normality of congruences of quasigroups is achieved for left (right) loops.
- Description of structure of  $n$ -ary simple medial quasigroups is given.
- The structure of finite  $n$ -ary medial quasigroups is given.
- Automorphism groups of  $n$ -ary  $T$ -quasigroups,  $n$ -ary medial quasigroups and some isotopes of binary left distributive quasigroups are researched.
- New families of easy constructed codes with one check symbol, which have characteristics better than known codes of such kind, are discovered.
- Necessary and sufficient conditions of orthogonality of a finite quasigroup and any its parastrophe are given.

The thesis is written in English.

**Key words and phrases:** quasigroup,  $n$ -ary quasigroup, linear quasigroup, inverse quasigroup, medial quasigroup, Latin square, code, automorphism, orthogonality.

## Аннотация

на докторскую диссертацию В.А. Щербакова

”О линейных и инверсных квазигруппах и их применениях в теории кодов”

Данная диссертационная работа посвящена теории  $n$ -арных и бинарных квазигрупп и некоторым применениям квазигрупп в теории кодирования. В частности, получены следующие результаты:

- Определены новые классы бинарных инверсных квазигрупп ( $(r, s, t)$ -инверсные,  $(\alpha, \beta, \gamma)$ -инверсные) и исследованы их свойства.
- Доказано, что квазигруппа с любым из тождеств Муфанг является лупой.
- Достигнут прогресс в решении проблемы Брака–Белоусова об условиях нормальности конгруэнций квазигрупп для левых (правых) луп.
- Дано описание строения простых  $n$ -арных медиальных квазигрупп.
- Описана структура конечных  $n$ -арных медиальных квазигрупп.
- Исследованы группы автоморфизмов  $n$ -арных  $T$ -квазигрупп,  $n$ -арных медиальных квазигрупп и некоторых изотопов бинарных леводистрибутивных квазигрупп.
- Найдены семейства новых, легко конструируемых кодов с одним проверочным символом, характеристики которых лучше, чем у широко известных кодов такого рода.
- Приведены необходимые и достаточные условия ортогональности конечной квазигруппы и любого ее парастрофа.

Диссертация написана на английском языке.

**Ключевые слова и фразы:** квазигруппа,  $n$ -арная квазигруппа, линейная квазигруппа, инверсная квазигруппа, медиальная квазигруппа, латинский квадрат, код, автоморфизм, ортогональность.