Classification of Quasigroups as Boolean Functions, their Algebraic Complexity and Application of Gröbner Bases in Solving Systems of Quasigroup Equations

V. Dimitrova[1], S. Markovski[1], D. Gligoroski[2]

[1] Institute of Informatics, Faculty of Natural Sciences and Mathematics, Ss Cyril and Methodius University, Skopje, MACEDONIA,
E-mail: smile@ii.edu.mk, vesnap@ii.edu.mk

[2] Centre for Quantifiable Quality of Service in Communication Systems – Q2S, Norwegian University of Science and Technology, Trondheim, NORWAY,
E-mail: danilog@q2s.ntnu.no

Quasigroup E-Transformation

1) A **quasigroup** $(Q, *)$ is a groupoid satisfying the law:

$(\forall\, u, v \in Q)(\exists!\, x, y \in Q)\ (x * u = v\ \&\ u * y = v)$

Example 1:

*	0	1	2	3
0	1	0	2	3
1	3	2	1	0
2	2	3	0	1
3	0	1	3	2

2) **E-transformation** $E_a^{(1)}: Q^+ \to Q^+$ on the quasigroup:

$$E_a^{(1)}(x_1 x_2 \ldots x_k) = y_1 y_2 \ldots y_k \Leftrightarrow \begin{cases} y_1 = a * x_1 \\ y_{i+1} = y_i * x_{i+1} \end{cases}$$

Example 2:

	0	3	2	2	1	2	1	1	3
0	1	0	2	0	0	2	3	0	3
2	3	0	2	2	2	0	3	0	3
1	0	1	1	1	1	3	2	2	1

1

Quasigroups as Boolean functions

$f : \{0,1\}^{2n} \to \{0,1\}^n, \quad f = (f_1, f_2, \ldots, f_n)$

$f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n) = (z_1, z_2, \ldots, z_n)$

$f_i(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n) = z_i,\ i = 1, 2, \ldots, n$

Example 3: Using **Boolean functions** for quasigroups of example 4 we have these presentations:

$f_{61}(x_1, x_2, x_3, x_4) = (x_2 + x_4, x_1 + x_3 + x_2x_4),$

$f_{241} = (x_1 + x_4 + x_2x_3 + x_2x_4, 1 + x_1 + x_2 + x_3 + x_2x_3 + x_2x_4),$

$f_{350} = (1 + x_2 + x_3 + x_4 + x_1x_3, x_1 + x_2 + x_4 + x_1x_3),$

$f_{564} = (1 + x_1 + x_2 + x_3 + x_1x_4, 1 + x_1 + x_4).$

2

Classification of quasigroups

1) We give two classes of quasigroups:
- **Linear** (if all functions f_i are linear)
- **Nonlinear** (otherwise)

2) Experimental results for quasigroups of order 4 (576 quasigroups)
- 144 linear quasigroups
- 432 nonlinear quasigroups

3) The number of quasigroups of order 2^n, $n \geq 3$ is too big. For $n = 3$ it is $108776032459082956800 \sim 2^{66.56}$.

3

Algebraic Complexity

1) Experimental results of measuring number of terms in the last element obtained after 100 *E*-transformations of a sequence *A* of 1000 pairs of same bits are:

- for linear quasigroups

{1, 1, 1, 1, 1, 1, 1, 2, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}

- for nonlinear quasigroups

{5, 6, 8, 8, 7, 8, 9, 6, 10, 12, 10, 8, 6, 8, 10, 10, 4, 6, 4, 4, 6, 12, 8, 4, 8, 6, 8, 8, 8, 8, 10, 8, 10, 9, 9, 5, 8, 9, 8, 7, 7, 9, 9, 9, 9, 5, 7, 7, 7, 8, 6, 8, 5, 10, 5, 6, 10, 6, 8, 8, 10, 8, 10, 6, 7, 6, 5, 8, 7, 6, 5, 10, 5, 6, 5, 6, 7, 8, 7, 8, 9, 11, 6, 5, 7, 7, 7, 7, 6, 7, 10, 7, 6, 7, 8, 5, 8, 5, 8, 7}

2) If the sequence *A* contains *n* different pairs of bits, then for nonlinear quasigroups the numbers are of kind *exp* (*n*).

4

Applications of quasigroups

Where we use quasigroups?

- as a part of some cryptographic primitives;
- for producing pseudo random number generators
- in design of error-correcting codes, ….

Example 4: Design of the stream cipher Edon80

$*_{61}$	0	1	2	3
0	0	2	1	3
1	2	1	3	0
2	1	3	0	2
3	3	0	2	1

$*_{241}$	0	1	2	3
0	1	3	0	2
1	0	1	2	3
2	2	0	3	1
3	3	2	1	0

$*_{350}$	0	1	2	3
0	2	1	0	3
1	1	2	3	0
2	3	0	2	1
3	0	3	1	2

$*_{564}$	0	1	2	3
0	3	2	1	0
1	1	0	3	2
2	0	1	2	3
3	2	1	0	3

5

Relationship with Gröbner Bases

Can we use Gröbner Bases for finding solutions of systems of quasigroup equations?

Initial observations:

1) If linear quasigroup is used then the system can be solved much easier by using Gröbner Bases.

2) In other case, if we have nonlinear quasigroup, it is really hard to solve effectively systems of quasigroup equations by any known method.

6