Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE

Bc. Adam Christov

Kryptografie založená na teorii kvazigrup

Katedra algebry

Vedoucí diplomové práce: RNDr. David Stanovský, Ph.D.
Studijní program: Matematika, obor Matematické metody informační bezpečnosti

2009

Rád bych poděkoval profesoru A. Drápalovi za jeho ochotu, trpělivost a cenné připomínky.

Také bych chtěl poděkovat svým rodičům a přítelkyni Táně Pokorné za jejich neustálou podporu, lásku a pevné nervy.

Prohlašuji, že jsem svoji diplomovou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce.

V Praze dne 17. dubna 2009 Bc. Adam Christov

Contents

Název práce: *Kryptografie založená na teorii kvazigrup*
Autor: *Bc. Adam Christov*
Katedra (ústav): *Katedra algebry*
Vedoucí diplomové práce: *RNDr. David Stanovský, Ph.D.*
e-mail vedoucího: *David.Stanovsky@mff.cuni.cz*

Abstrakt: *Možnou alternativou k bežně používaným kryptografickým schémaům s veřejným klíčem, jejichž složitost je založena na problému faktorizace nebo diskrétním logaritmu, jsou schémata využívající složitost řešení systému kvadratických rovnic o více proměnných nad konečným tělesem. Jedno takové schéma bylo navrhnuto v práci D.Gligoroskiho a spol. [8]. V tomto schématu jsou klíče konstruovány ze speciálních kvazigrup, které jsou nazývány kvadratické. V této práci jsou kvadratické kvazigrupy popsány a klasifikovány podle jejich vlastností. Nakonec je představena teorie, kterou je možné využít k jejich konstrukci.*

Klíčová slova: *kryptografie s veřejným klíčem, kvadratické rovnice o více proměnných, kvadratické kvazigrupy*

Title: *Quasigroup Based Cryptography*
Author: *Bc. Adam Christov*
Department: *Department of Algebra*
Supervisor: *RNDr. David Stanovský, Ph.D.*
Supervisor's e-mail address: *David.Stanovsky@mff.cuni.cz*

Abstract: *Public-key cryptographic schemes based on the complexity of solving multivariate quadratic equations over a finite field represent an alternative to widely used schemes relying on the complexity of factorization or on the discrete logarithm. Such a scheme was proposed by D. Gligoroski et al. [8]. Keys in this scheme are constructed using a special kind of quasigroups, the so-called quadratic quasigroups. In this paper we try and describe the quadratic quasigroups and classify them according to their properties. Finally, we present a theory which can be used to generate such quasigroups.*

Keywords: *public-key cryptography, multivariate quadratic equations, quadratic quasigroups*

Introduction

Nowadays, cryptology became a part of our daily life even though most people do not realize it. One of the important categories of cryptology is the public-key cryptography (or asymmetric cryptography), which was devised by Diffie and Hellman [3]. In the public-key cryptosystem, we use a couple of different keys – a public key and a private key. The secret encrypted by the public key can be decrypted only by the corresponding private key. It provides us with the potential of establishing an encrypted connection without having to share the secret, moreover, it enables us to sign data digitally. The security of the public-key schemes, which are currently used in practice, relies on just a small number of problems. Mostly, it involves either the problem of factorization (e.g., RSA [10]), or the discrete logarithm (e.g., ECC [9]). Therefore, the research on new cryptography schemes, particularly based on other classes of problems, is of utmost importance.

In this thesis we will focus on an innovative structure of a public-key scheme based on multivariate quadratic quasigroups (MQQ, [8]). It represents a special type of an MQ-scheme. In general, the MQ-schemes rely on the problem of finding a solution of a system of multivariate quadratic equations (MQ-problem, [13]). The private key in the MQ-scheme is a soluble system of n quadratic equations $\mathcal{P}(x)$ in n variables over the field $\mathbb{F}_2$, and two automorphisms of vector space $\mathbb{F}_2^n$, denoted by $\mathcal{L}_1$ and $\mathcal{L}_2$. The public key is the system of equations

$$\mathcal{P}'(x) = \mathcal{L}_2\Big(\mathcal{P}\big(\mathcal{L}_1(x)\big)\Big).$$

Therefore, finding the private key based on knowledge of the public key in the MQ-scheme relies on the complexity of decomposition of $\mathcal{P}'(x)$ into $\mathcal{L}_1$, $\mathcal{L}_2$, and $\mathcal{P}$ [13]. MQQ is based on an algorithm generating the system $\mathcal{P}(x)$ from a special kind of quasigroups, the so-called quadratic quasigroups. The authors of MQQ use a heuristic algorithm for generating quadratic quasigroups that can discover only some of them and that might be not quick enough. They do not provide any theoretical background that would describe the structure of quadratic quasigroups in general. Such a theory is presented in this thesis.

In Theorem 2.40 we show that every quadratic quasigroup can be described by means of four parameters. Two of which depend upon permutations of $\mathbb{F}_2^n$ that can be described by quadratic forms (we call them quadratic permutations). The further two parameters are a translation vector and a bilinear map. Our ability to generate quadratic quasigroups depends, to a large extent, upon the ability to find quadratic permutations efficiently. Chapter 3 is devoted to this topic and we give two possible ways how quadratic permutations can be constructed. In Theorem 3.8 we show that each quadratic form which is a part of a quadratic permutation is determined up to equivalence only by the dimension of its kernel. Using this fact, it is possible to find all such quadratic forms. Composition of these forms provides the first possible nondeterministic way. The second one is fully deterministic and uses a Matsumoto-Imai scheme [13].

The property of being a quadratic quasigroup is not isotopically invariant. However, if the permutations used by an isotopy are linear and one of the quasigroups is quadratic, then the other quasigroup is quadratic as well. Under certain additional conditions this is true also in the case when the isotopy permutations are quadratic. A large part of Chapter 2 is hence devoted to the study of isotopies. The achieved results can be used to derive quickly many further quadratic quasigroups that are isotopic to a known quadratic quasigroup.

Quadratic loops have only two structural invariants (cf. Theorem 2.48), i.e., a unit and a bilinear map. In Theorem 2.50 we present necessary conditions for bilinear map to represent a quadratic loop. It provides a heuristic algorithm for generating these loops. They can be used for generating further quadratic quasigroups, but they are also interesting as an algebraic object. One can ask questions about the laws (associative, Moufang etc.) that such a loop can fulfil. While these questions are certainly interesting, they are out of the scope of this thesis and I have deferred them to future studies.

The mentioned results except for basic and known facts about quasigroups, boolean functions, bilinear and quadratic forms are achieved newly in this thesis.

Preliminaries

We will use just basic knowledge of linear algebra [1], groups [4], commutative rings [5], and finite fields [12], conforming to the notation commonly used in those areas of mathematics. The Galois field of characteristic 2 will be denoted by $\mathbb{F}_2$. I_n would denote an $n \times n$ matrix, having 1's on the main diagonal and 0's elsewhere. $\delta_{i,j}$ denotes the Kronecker delta. It is a function of two variables which is 1 if they are equal, and 0 otherwise, i.e.,

$$\delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

Chapter 1

Basic Quasigroup Theory

In this chapter we introduce a definition of a general quasigroup and its basic properties [6, 11].

Definition 1.1. A *quasigroup* $(Q, *)$ or just Q is a set Q with a binary operation $*$, such that for each u and v in Q there exist unique elements x and y in Q which satisfy

$$\begin{aligned} u * x &= v, \\ y * u &= v. \end{aligned}$$

A quasigroup is called *finite* if it has a finite number of elements. The number of elements is called the *order* of the quasigroup.

The unique solution x is denoted by $u\backslash v$ where $\backslash$ is a binary operation in Q (called the *left division*) and the unique solution y by v/u where $/$ is also a binary operation in Q (called the *right division*).

Lemma 1.2. *The quasigroup $(Q, *)$ with the left and right divisions satisfies the identities*

$$\begin{aligned} u * (u\backslash v) &= v, \\ (v/u) * u &= v, \\ u\backslash(u * v) &= v, \ \textit{and} \\ (v * u)/u &= v \end{aligned}$$

for all $u, v \in Q$.

Proof. The first two identities follow directly from the definition of the divisions. From the definition of $\backslash$ we know that $u\backslash(u*v)$ is a solution of $u*x = u*v$

for every $u, v \in Q$. On the other hand, we also know that v solves this equation. From the uniqueness of the solution we obtain $u \backslash (u * v) = v$. Similarly, the equation $y * u = v * u$ is solved by both v and $(v * u)/u$. Thus $v = (v * u)/u$ for every $u, v \in Q$. $\square$

Observation 1.3. *Let $(Q, *)$ be a quasigroup and operations $\backslash$ and $/$ be left and right divisions. Then $(Q, \backslash)$ and $(Q, /)$ are also quasigroups.*

Definition 1.4. Let $(Q, *)$ be a quasigroup. An element $e_r \in Q$ is called a *right unit* if $u * e_r = u$ for all $u \in Q$. Similarly, an element $e_l \in Q$ is called a *left unit* if $e_l * u = u$ for all $u \in Q$. If $e \in Q$ is both a left unit, and a right unit, then it is called simply a *unit.* A quasigroup with a unit is called a *loop.*

Observation 1.5. *If the quasigroup $(Q, *)$ contains a right unit e_r and also a left unit e_l, then $e_r = e_l * e_r = e_l$.*

Example 1.6. A *Latin square* is an $n \times n$ square containing n copies of each of n symbols, arranged in such a way that no symbol is repeated in any row or column. Exactly the same rules have to be satisfied by the Cayley table of a finite quasigroup. It means every finite quasigroup corresponds to some Latin square. In Figure 1.1 we can see an example of a Latin square 3×3 on the left and the corresponding finite quasigroup of order 3 on the right.

1	0	2
0	2	1
2	1	0

$*$	0	1	2
0	1	0	2
1	0	2	1
2	2	1	0

Figure 1.1: The Latin square and the corresponding finite quasigroup

Example 1.7. The cyclic group $\mathbb{Z}$ with a nonassociative binary operation "minus" is an example of an infinite quasigroup. We can easily observe that the element $0 \in \mathbb{Z}$ is a right unit of $(\mathbb{Z}, -)$ because $k - 0 = k$, but $0 - k = -k$ for every $k \in \mathbb{Z}$.

Definition 1.8. A map

$$\alpha : (Q_1, *_1) \to (Q_2, *_2)$$

between quasigroups $(Q_1, *_1)$ and $(Q_2, *_2)$ is a *homomorphism* if

$$\alpha(u *_1 v) = \alpha(u) *_2 \alpha(v)$$

for all $u, v \in Q_1$. A bijective homomorphism is an *isomorphism.* If there exists an isomorphism between Q_1 and Q_2, we call quasigroups *isomorphic*, denoted by $Q_1 \cong Q_2$.

A triple of maps

$$\alpha, \beta, \gamma : (Q_1, *_1) \to (Q_2, *_2)$$

between quasigroups $(Q_1, *_1)$ and $(Q_2, *_2)$ is called a *homotopy* if

$$\alpha(u) *_2 \beta(v) = \gamma(u *_1 v)$$

for all u, v in Q_1. We call the triple an *isotopy* if the maps α, β, γ are bijective. If there exists an isotopy between Q_1 and Q_2, we call the quasigroups *isotopic*, notation $Q_1 \sim Q_2$.

Observation 1.9. *Let $(Q_1, *_1)$ be a quasigroup, and let Q_2 be a set, such that $|Q_1| = |Q_2|$. Let α, β, γ be a bijective maps $Q_2 \to Q_1$. Then $(Q_2, *_2)$, where*

$$u *_2 v = \gamma^{-1}\big(\alpha(u) *_1 \beta(v)\big),$$

for all u, v in Q_2, is a quasigroup, and (α, β, γ) is an isotopy between $(Q_2, *_2)$ and $(Q_1, *_1)$.

The isotopy (α, β, γ) between $(Q_1, *_1)$ and $(Q_2, *_2)$ can be transformed into the isotopy $(\gamma^{-1}\alpha, \gamma^{-1}\beta, \mathrm{Id}_{Q_1})$ between $(Q_1, *_1)$ and $(Q_1, *_3)$, where $*_3$ is defined as $u *_3 v = \gamma^{-1}(\gamma(u) *_2 \gamma(v))$ for all $u, v \in Q_1$. We can see that γ becomes an isomorphism between $(Q_1, *_3)$ and $(Q_2, *_2)$.

It follows that to find all quasigroups which are isotopic to $(Q, *)$ up to isomorphism we have to go through all quasigroups $(Q, \circ)$ such that

$$u \circ v = \alpha(u) * \beta(v) \qquad \text{for all } u, v \in Q,$$

where α and β permute Q. Such a quasigroup will be denoted by $Q[\alpha, \beta]$.

Definition 1.10. Let $(Q, *)$ be a quasigroup. For each $a \in Q$ define the *left translation* L_a as a map $L_a : x \mapsto a*x$ and similarly the *right translation* R_a as a map $R_a : x \mapsto x*a$ for all $x \in Q$. Both maps are bijections and $L_a^{-1} : x \mapsto a\backslash x$ and $R_a^{-1} : x \mapsto x/a$.

Lemma 1.11. *Let $(Q, *)$ be a quasigroup. $Q[\alpha, \beta]$ is a loop if and only if there exist $a, b \in Q$ such that $\alpha = {R_b}^{-1}$ and $\beta = {L_a}^{-1}$.*

Proof. Suppose $(Q[\alpha, \beta], \circ)$ is a loop with unit $e \in Q$. Then $u = u \circ e = \alpha(u) * \beta(e)$ and $\alpha(u) = u/\beta(e)$ for all $u \in Q$. Similarly $v = e \circ v = \alpha(e) * \beta(v)$ and $\beta(v) = \alpha(e)\backslash v$ for all $v \in Q$. So $b = \beta(e)$ and $a = \alpha(e)$.

Now, consider that $\alpha = {R_b}^{-1}$ and $\beta = {L_a}^{-1}$. We will show that $a * b$ is a unit.

$$u \circ (a * b) = \alpha(u) * \beta(a * b) = (u/b) * (a\backslash(a * b)) = (u/b) * b = u,$$
$$(a * b) \circ v = \alpha(a * b) * \beta(v) = ((a * b)/b) * (a\backslash v) = a * (a\backslash v) = v,$$

for all $u, v \in Q$. □

We call the loop $(Q[{R_b}^{-1}, {L_a}^{-1}], \circ)$ a *principal isotope* of $(Q, *)$.

Corollary 1.12. *Every quasigroup is isotopic to a principal isotope.*

Chapter 2

Quadratic Quasigroups

2.1 Boolean Maps

In this section we show that every map

$$\overbrace{\mathbb{F}_2^n \times \cdots \times \mathbb{F}_2^n}^{m} \to \mathbb{F}_2^n$$

can be represented by a vector of Boolean polynomials [7]. The quasigroup upon $\mathbb{F}_2^n$ can be understood as such a kind of map. Restriction to quadratic polynomials provides the definition of a quadratic quasigroup [8].

Definition 2.1. Let $\mathbb{F}_2[x_1, x_2, \ldots, x_n]$ be a ring of polynomials in variables $x_1, x_2, \ldots, x_n$ over the field $\mathbb{F}_2$. We call the elements of the quotient ring

$$\mathbb{F}_2[x_1, x_2, \ldots, x_n]/\langle x_1^2 - x_1, \ldots, x_n^2 - x_n\rangle$$

Boolean polynomials.

Each Boolean polynomial can be expressed as

$$f = \sum_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i,$$

where the coefficients $a_I \in \mathbb{F}_2$ (suppose that $\prod_{i\in I} x_i = 1$ for $I = \emptyset$). The maximal cardinality of I such that $a_I = 1$ is called a *degree* of the polynomial f and is denoted by $\deg(f)$. As a degree of a zero polynomial we set $-\infty$. For every subset $I = \{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\}$ we call the Boolean polynomial $x_{i_1} \cdots x_{i_m}$ a *monomial* and denote it shortly by x_I.

Definition 2.2. A map $\alpha : \mathbb{F}_2^n \to \mathbb{F}_2$ is called a *Boolean function of the arity n* (or an *n-ary Boolean function*).

We can assign a Boolean function $\bar{f}$ of the arity n to each Boolean polynomial $f \in \mathbb{F}_2[x_1, \ldots, x_n]$, where $\bar{f}$ is defined as an evaluation of the polynomial f:

$$\bar{f} : (u_1, \ldots, u_n) \mapsto f(u_1, \ldots, u_n).$$

Theorem 2.3. *Every n-ary Boolean function can be uniquely represented as a Boolean polynomial from $\mathbb{F}_2[x_1, \ldots, x_n]$.*

Proof. We will show that a map $\varphi : f \mapsto \bar{f}$ is an isomorphism between the ring of Boolean polynomials and the ring of Boolean functions. Let f and g be Boolean polynomials from $\mathbb{F}_2[x_1, \ldots, x_n]$. Then, we can easily observe that $(fg)(u_1, \ldots, u_n) = f(u_1, \ldots, u_n) \cdot g(u_1, \ldots, u_n)$ and $(f + g)(u_1, \ldots, u_n) = f(u_1, \ldots, u_n) + g(u_1, \ldots, u_n)$, so $\overline{fg} = \bar{f} \cdot \bar{g}$ and $\overline{f + g} = \bar{f} + \bar{g}$, and φ is a homomorphism of the rings. Let $f = \sum_{I \subseteq \{1,\ldots,n\}} a_I x_I$ be a nonzero Boolean polynomial. We pick such an $I \subseteq \{1, \ldots, n\}$ which satisfies $a_I = 1$ and the cardinality of I is minimal. Suppose the vector $u = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$ obeys $u_j = 1$ for $j \in I$, and $u_j = 0$ otherwise. If $J \subsetneq I$, then $a_J = 0$. If $J \setminus I \neq \emptyset$, then $x_J(u_1, \ldots, u_n) = 0$. Hence $f(u_1, \ldots, u_n) = x_I(u_1, \ldots, u_n) = 1$ and $\bar{f}$ is also nontrivial. It means that φ is injective. There exist exactly 2^n Boolean monomials in $\mathbb{F}_2[x_1, \ldots, x_n]$, therefore, the cardinality of the ring of Boolean polynomials is 2^{2^n}. The ring of Boolean functions has also 2^{2^n} elements because $|\mathbb{F}_2^n| = 2^n$. An injective map between two rings of the same finite cardinality is surjective, as well. □

Let α be a map

$$\alpha : \overbrace{\mathbb{F}_2^n \times \cdots \times \mathbb{F}_2^n}^{m} \to \mathbb{F}_2^n$$

and $E = \{e_1, e_2, \ldots e_n\}$ be a base of the vector space $\mathbb{F}_2^n$. $\{v\}_E$ will denote coordinates of a vector $v \in \mathbb{F}_2^n$ relative to the basis E. Note that $v \mapsto \{v\}_E$ is an automorphism of the vector space $\mathbb{F}_2^n$. There exists exactly one map α_E such that

$$\begin{aligned} \alpha_E :\ & \overbrace{\mathbb{F}_2^n \times \cdots \times \mathbb{F}_2^n}^{m} \to \mathbb{F}_2^n, \\ \alpha_E :\ & (x_1^1, \ldots, x_n^1), \ldots, (x_1^m, \ldots, x_n^m) \mapsto (y_1, \ldots, y_n), \end{aligned}$$

where $(x_1^j, \ldots, x_n^j) = \{u^j\}_E, (y_1, \ldots, y_n) = \{v\}_E$ and vectors $u^j, v \in \mathbb{F}_2^n$ for $j = 1, \ldots, m$ satisfy $\alpha(u^1, \ldots, u^m) = v$. Each $y_i, i = 1, \ldots, n$ is uniquely determined by the bit values $\{x_i^j; i = 1, \ldots, n, j = 1, \ldots, m\}$. Thus, we can represent y_i as a mn-ary Boolean function

$$\begin{aligned} \bar{f}_i :\ & \overbrace{\mathbb{F}_2^n \times \cdots \times \mathbb{F}_2^n}^{m} \to \mathbb{F}_2, \\ \bar{f}_i :\ & (x_1^1, \ldots, x_n^1), \ldots, (x_1^n, \ldots, x_n^m) \mapsto y_i, \quad i = 1, 2, \ldots, n. \end{aligned}$$

Using Theorem 2.3 we obtain a Boolean polynomial f_i for all such Boolean functions $\bar{f}_i$. We can thus state

Theorem 2.4. *Let α be a map*

$$\alpha : \overbrace{\mathbb{F}_2^n \times \cdots \times \mathbb{F}_2^n}^{m} \to \mathbb{F}_2^n.$$

For each base E of $\mathbb{F}_2^n$ there exists exactly one vector of Boolean polynomials $(f_1, f_2, \ldots, f_n) \in \big(\mathbb{F}_2[x_i^j; i = 1, \ldots, n, j = 1, \ldots, m]\big)^n$, such that

$$\{\alpha(u^1, \ldots, u^m)\}_E = \Big(f_1(\{u^1\}_E, \ldots, \{u^m\}_E), \ldots, f_n(\{u^1\}_E, \ldots, \{u^m\}_E)\Big)$$

for all $u^1, \ldots, u^m \in \mathbb{F}_2$.

We call the vector of the Boolean polynomials $(f_1, f_2, \ldots, f_n)$ a *Boolean polynomial representation* (or just *representation*) of the map α *in the base E*, denoted by $\alpha_E = (f_1, f_2, \ldots, f_n)$.

Definition 2.5. Let α be a map

$$\alpha : \overbrace{\mathbb{F}_2^n \times \cdots \times \mathbb{F}_2^n}^{m} \to \mathbb{F}_2^n$$

and E be a base of the vector space $\mathbb{F}_2^n$. Then we call α a *Boolean map of degree d in the base E* if $d = \max\{\deg(f_i), i = 1, \ldots, n\}$, where $\alpha_E = (f_1, f_2, \ldots, f_n)$.

Proposition 2.6. *The degree of a Boolean map is independent of the selected base of $\mathbb{F}_2^n$.*

Proof. Let E, E' be two bases of the vector space $\mathbb{F}_2^n$ and let R be a transformation matrix from base E to base E', i.e., $\{u\}_E = \{u\}_{E'}R$ for $u \in \mathbb{F}_2^n$. Recall that the matrix R is regular. Let $f \in \mathbb{F}_2[x_i^j; i = 1, \ldots, n, j = 1, \ldots, m]$ be a Boolean polynomial. Then $g = f\big((x_1^1, \ldots, x_n^1)R, \ldots, (x_1^m, \ldots, x_n^m)R\big)$ is also Boolean polynomial and satisfies $\deg(g) \leq \deg(f)$. Using the transformation matrix R^{-1} for g in the same way, we get $\deg(f) = \deg(g)$. Now let $(g_1, \ldots, g_n)$ be a vector of Boolean polynomials from $\mathbb{F}_2[x_i^j; i = 1, \ldots, n, j = 1, \ldots, m]^n$. Then $(h_1, \ldots, h_n) = (g_1, \ldots, g_n)R^{-1}$ is also a vector of Boolean polynomials and satisfies

$$\max\{\deg(h_i), i = 1, \ldots, n\} \leq \max\{\deg(g_i), i = 1, \ldots, n\}.$$

Using the transformation matrix R for $(h_1, \ldots, h_n)$ in the same way, we obtain

$$\max\{\deg(h_i), i = 1, \ldots, n\} = \max\{\deg(g_i), i = 1, \ldots, n\}.$$

Let α be a map

$$\alpha : \overbrace{\mathbb{F}_2^n \times \cdots \times \mathbb{F}_2^n}^{m} \to \mathbb{F}_2^n.$$

with a Boolean polynomial representation $(f_1, f_2, \ldots, f_n)$ in the base E. Then

$$\begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{pmatrix} = (R^T)^{-1} \begin{pmatrix} f_1\big((x_1^1, \ldots, x_n^1)R, \ldots, (x_1^m, \ldots, x_n^m)R\big) \\ f_2\big((x_1^1, \ldots, x_n^1)R, \ldots, (x_1^m, \ldots, x_n^m)R\big) \\ \vdots \\ f_n\big((x_1^1, \ldots, x_n^1)R, \ldots, (x_1^m, \ldots, x_n^m)R\big) \end{pmatrix}$$

is a Boolean polynomial representation of α in E' and from the calculations above we get $\max\{\deg(f_i), i = 1, \ldots, n\} = \max\{\deg(g_i), i = 1, \ldots, n\}$. □

2.2 Bilinear and Quadratic Forms

In this section we present definitions of quadratic and bilinear forms over a finite field, particularly, $\mathbb{F}_2$ [2], which is used in the next section.

Definition 2.7. Let V be a vector space upon a field F. A *bilinear form* on V is a map $\mathbf{b} : V \times V \to F$ which is linear in each argument separately, i.e., satisfies:

(i) $\mathbf{b}(u + w, v) = \mathbf{b}(u, v) + \mathbf{b}(w, v)$

(ii) $\mathbf{b}(u, v + w) = \mathbf{b}(u, v) + \mathbf{b}(u, w)$

(iii) $\mathbf{b}(\lambda u, v) = \mathbf{b}(u, \lambda v) = \lambda \mathbf{b}(u, v)$

for every $u, v, w \in V$ and $\lambda \in F$.

We say that a bilinear form $\mathbf{b}$ is *symmetric* if $\mathbf{b}(u, v) = \mathbf{b}(v, u)$ for every $u, v \in V$. The bilinear form is called *alternating* if $\mathbf{b}(u, u) = 0$ for every $u \in V$. In this paper we suppose that the vector space V is always finite.

Lemma 2.8. *Let $\mathbf{b}$ be a bilinear form on a vector space V upon a field F and let $E = \{e_1, e_2, \ldots, e_n\}$ be a base of V. Then the value of $\mathbf{b}(u, v)$, where $u, v \in V$ and $\{u\}_E = (x_1, x_2, \ldots, x_n)$, $\{v\}_E = (y_1, y_2, \ldots, y_n)$, can be expressed as*

$$\mathbf{b}(u, v) = \sum_{i,j=1,\ldots,n} x_i y_j \mathbf{b}(e_i, e_j). \tag{2.1}$$

Proof. We just use the properties of a bilinear form repeatedly.

$$\begin{aligned}\mathbf{b}(u,v) = \mathbf{b}\left(\sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j\right) &= \sum_{i=1}^{n} \mathbf{b}\left(x_i e_i, \sum_{j=1}^{n} y_j e_j\right) \\ &= \sum_{i,j=1}^{n} \mathbf{b}(x_i e_i, y_j e_j) = \sum_{i,j=1}^{n} x_i y_j \mathbf{b}(e_i, e_j).\end{aligned}$$

□

We call the expression (2.1) a *coordinate representation* of the bilinear form in the base E.

Lemma 2.9. *Let $A = [a_{i,j}]$ be a matrix from $F^{n\times n}$ and $E = \{e_1, e_2, \ldots, e_n\}$ be a base of the vector space V. Define a map $\mathbf{b} : V \times V \to F$ by*

$$\mathbf{b}(u,v) = \sum_{i,j=1,\ldots,n} x_i y_j a_{i,j},$$

where $u, v \in V$ and $\{u\}_E = (x_1, x_2, \ldots, x_n), \{v\}_E = (y_1, y_2, \ldots, y_n)$. Then $\mathbf{b}$ is a bilinear form.

Proof. It is easy to observe that $\mathbf{b}(\lambda u, v) = \mathbf{b}(u, \lambda v) = \lambda \mathbf{b}(u,v)$ for all $\lambda \in F$ and $u, v \in V$. Now let $u, v, w \in V$ and $\{u\}_E = (x_1, \ldots, x_n)$, $\{v\}_E = (y_1, \ldots, y_n)$, $\{w\}_E = (z_1, \ldots, z_n)$. Then

$$\begin{aligned}\mathbf{b}(u+w,v) = \mathbf{b}\left(\sum_{i=1}^{n}(x_i + z_i)e_i, \sum_{i=1}^{n} y_i e_i\right) &= \sum_{i,j=1,\ldots,n} (x_i + z_i) y_j a_{i,j} \\ = \sum_{i,j=1,\ldots,n} x_i y_j a_{i,j} + \sum_{i,j=1,\ldots,n} z_i y_j a_{i,j} &= \mathbf{b}(u,v) + \mathbf{b}(w,v).\end{aligned}$$

Using the same method we will get $\mathbf{b}(u, v + w) = \mathbf{b}(u,v) + \mathbf{b}(u,w)$, thus $\mathbf{b}$ is a bilinear form. □

In other words, each bilinear form can be fully described by a matrix and also each matrix defines a bilinear form. We can formulate these facts in a corollary:

Corollary 2.10. *Let V be a vector space upon a field F and $E = \{e_1, \ldots, e_n\}$ be a base of V. Let $\mathbf{b}$ be a map $V \times V \to F$. Then $\mathbf{b}$ is a bilinear form if and only if there exists a matrix $A \in F^{n\times n}$ such that*

$$\mathbf{b}(u,v) = (x_1, \ldots, x_n) A (y_1, \ldots, y_n)^T$$

for every $u, v \in V$, where $\{u\}_E = (x_1, x_2, \ldots, x_n), \{v\}_E = (y_1, y_2, \ldots, y_n)$.

Definition 2.11. Let $\mathbf{b}$ be a bilinear form on the vector space V. We define the *left* and *right radical* as follows:

$$\operatorname{Rad}_L \mathbf{b} = \{u \in V; \mathbf{b}(u,w) = 0, \forall w \in V\},$$
$$\operatorname{Rad}_R \mathbf{b} = \{u \in V; \mathbf{b}(w,u) = 0, \forall w \in V\}.$$

It is easy to observe that $\operatorname{Rad}_L \mathbf{b}$, and $\operatorname{Rad}_R \mathbf{b}$ are vector subspaces of V. Since the rank of the matrix is the same as the rank of its transpose, hance $\dim \operatorname{Rad}_L \mathbf{b} = \dim \operatorname{Rad}_R \mathbf{b}$.

A bilinear form $\mathbf{b}$ is said to be *non-degenerate* if $\operatorname{Rad}_L \mathbf{b} = \operatorname{Rad}_R \mathbf{b} = \{0\}$.

Definition 2.12. Let V be a vector space upon a field F. A *quadratic form* on V is a map $\mathbf{q} : V \to F$ which satisfies the conditions

(i) $\mathbf{q}(\lambda v) = \lambda^2 \mathbf{q}(v)$ for all $\lambda \in F, v \in V$.

(ii) The map $\mathbf{b} : V \times V \to F$ defined by

$$\mathbf{q}(v+w) = \mathbf{q}(v) + \mathbf{q}(w) + \mathbf{b}(v,w)$$

is a bilinear form.

We say that the bilinear form $\mathbf{b}$ is *associated* with the quadratic form $\mathbf{q}$. Directly from the definition follows that $\mathbf{b}(v,w) = \mathbf{b}(w,v)$, thus the associated bilinear form is always symmetric. The properties of quadratic forms are different in the case the characteristic of the field F is 2 or different. We will focus only on the case the characteristic is 2. So from now on, assume that $F = \mathbb{F}_2$. We can see that in this case $\mathbf{b}(v,v) = 0$ for every $v \in V$ which means that $\mathbf{b}$ is alternating. Also, because $\lambda^2 = \lambda$ for all $\lambda \in \mathbb{F}_2$, we have

$$\mathbf{q}(\lambda v) = \lambda \mathbf{q}(v) \text{ for all } v \in V.$$

Definition 2.13. Let $\mathbf{q}$ be a quadratic form on $\mathbb{F}_2^n$ and $\mathbf{b}$ be its associated bilinear form. Then the set

$$\operatorname{Rad} \mathbf{q} = \{u \in \mathbb{F}_2^n; \mathbf{b}(u,w) = \mathbf{b}(w,u) = 0, \forall w \in \mathbb{F}_2^n\}$$

is called the *radical* of the quadratic form $\mathbf{q}$. We can see that $\operatorname{Rad} \mathbf{q} = \operatorname{Rad}_L \mathbf{b} = \operatorname{Rad}_R \mathbf{b}$. Therefore, $\operatorname{Rad} \mathbf{q}$ is a vector subspace of $\mathbb{F}_2^n$.

Lemma 2.14. *Let $\mathbf{q}$ be a quadratic form on a vector space $\mathbb{F}_2^n$ with a base $E = \{e_1, e_2, \dots, e_n\}$ and let $\mathbf{b}$ be its associated bilinear form. Then the image of $v \in \mathbb{F}_2^n$, where $\{v\}_E = (x_1, x_2, \dots, x_n)$, can be expressed as*

$$\mathbf{q}(v) = \sum_{i=1}^{n} x_i \mathbf{q}(e_i) + \sum_{\substack{i,j=1,\dots,n \\ i<j}} x_i x_j \mathbf{b}(e_i, e_j). \tag{2.2}$$

Proof. We will use an induction on n. For $n = 1$ the statement holds. Suppose that the assertion holds for $n = k-1$. Then, using the definition of a quadratic form, we have

$$\begin{aligned}\mathbf{q}\left(\sum_{i=1}^{k} x_i e_i\right) &= \mathbf{q}\left(\sum_{i=1}^{k-1} x_i e_i\right) + \mathbf{q}(x_k e_k) + \mathbf{b}\left(\sum_{i=1}^{k-1} x_i e_i, x_k e_k\right) \\ &= \sum_{i=1}^{k-1} x_i \mathbf{q}(e_i) + \sum_{\substack{i,j=1,\dots,k-1\\ i<j}} x_i x_j \mathbf{b}(e_i, e_j) + x_k \mathbf{q}(e_k) + \sum_{i=1}^{k-1} x_i x_k \mathbf{b}(e_i, e_k) \\ &= \sum_{i=1}^{k} x_i \mathbf{q}(e_i) + \sum_{\substack{i,j=1,\dots,k\\ i<j}} x_i x_j \mathbf{b}(e_i, e_j).\end{aligned}$$

□

We call the expression (2.2) a *coordinate representation* of the quadratic form in the base E.

Lemma 2.15. *Let $A = [a_{i,j}]$ be a symmetric matrix in $\mathbb{F}_2^{n\times n}$ such that $a_{i,i} = 0$ for every $i = 1, \dots, n$ and let $(b_1, b_2, \dots, b_n)$ be a vector in $\mathbb{F}_2^n$. Let $E = \{e_1, e_2, \dots, e_n\}$ be a base of the vector space $\mathbb{F}_2^n$. Now define a map $\mathbf{q} : \mathbb{F}_2^n \to \mathbb{F}_2$ by*

$$\mathbf{q}(v) = \sum_{i=1}^{n} x_i b_i + \sum_{\substack{i,j=1,\dots,n\\ i<j}} x_i x_j a_{i,j},$$

where $v \in \mathbb{F}_2^n$ and $\{v\}_E = (x_1, x_2, \dots, x_n)$. Then $\mathbf{q}$ is a quadratic form and $\mathbf{q}(e_i) = b_i$ for every $i = 1, 2, \dots, n$.

Proof. It can be easily observed that $\mathbf{q}(\lambda v) = \lambda \mathbf{q}(v)$ for all $\lambda \in \mathbb{F}_2, v \in \mathbb{F}_2^n$. Now let $u, v \in \mathbb{F}_2^n$ and $\{u\}_E = (x_1, \dots, x_n), \{v\}_E = (y_1, \dots, y_n)$. Then

$$\begin{aligned}&\mathbf{q}(u+v) = \\ &= \mathbf{q}\left(\sum_{i=1}^{n}(x_i + y_i)e_i\right) = \sum_{i=1}^{n}(x_i + y_i)b_i + \sum_{\substack{i,j=1,\dots,n\\ i<j}} (x_i + y_i)(x_j + y_j)a_{i,j} \\ &= \sum_{i=1}^{n} x_i b_i + \sum_{\substack{i,j=1,\dots,n\\ i<j}} x_i x_j a_{i,j} + \sum_{i=1}^{n} y_i b_i + \sum_{\substack{i,j=1,\dots,n\\ i<j}} y_i y_j a_{i,j} \\ &\quad + \sum_{\substack{i,j=1,\dots,n\\ i<j}} x_i y_j a_{i,j} + \sum_{\substack{i,j=1,\dots,n\\ i<j}} x_j y_i a_{i,j} \\ &= \mathbf{q}(u) + \mathbf{q}(v) + \sum_{i,j=1,\dots,n} x_i y_j a_{i,j}.\end{aligned}$$

It follows from Lemma 2.9 that $\mathbf{b} = \sum_{i,j=1,\dots,n} x_i y_j a_{i,j}$ represents a bilinear form associated with $\mathbf{q}$. The fact that $\mathbf{q}(e_i) = b_i$ follows directly from the definition of $\mathbf{q}$. □

The lemmas above also yield that every quadratic form is fully determined by an alternating symmetric bilinear form and a vector $(b_1, b_2, \dots, b_n) \in \mathbb{F}_2^n$ which defines values of the form on the elements of the base.

Corollary 2.16. *Let $\mathbf{q}$ be an n-ary Boolean function and $E = \{e_1, e_2, \dots, e_n\}$ be a base of the vector space $\mathbb{F}_2^n$. Then $\mathbf{q}$ is a quadratic form if and only if there exist values $a_{i,j}, i, j = 1, \dots, n, i < j, b_k, k = 1, \dots, n$ such that*

$$\mathbf{q}(v) = \sum_{i=1}^{n} x_i b_i + \sum_{\substack{i,j=1,\dots,n \\ i<j}} x_i x_j a_{i,j}$$

for every $v \in \mathbb{F}_2^n$ where $\{v\}_E = (x_1, x_2, \dots, x_n)$.

It will come in handy to use the quadratic form $\mathbf{q}$ directly as its representation in a previously given base. It means that for $u \in \mathbb{F}_2^n, \{u\}_E = (x_1, \dots, x_n)$ we will write just $\mathbf{q}(x_1, \dots, x_n)$ instead of $\mathbf{q}(u)$ and we will work with $\mathbf{q}$ as if it were a polynomial $\mathbf{q}(x_1, \dots, x_n) \in \mathbb{F}_2^n[x_1, \dots, x_n]$. The same convention will be used for bilinear forms.

Corollary 2.17. *Let $p \in \mathbb{F}_2^n[x_1, \dots, x_n]$ be a Boolean polynomial of degree 2 and let $E = \{e_1, e_2, \dots, e_n\}$ be a base of the vector space $\mathbb{F}_2^n$. Then there exists exactly one quadratic form $\mathbf{q}$ and a vector $c \in \mathbb{F}_2$ such that*

$$p(x_1, \dots, x_n) = \mathbf{q}(x_1, \dots, x_n) + c.$$

2.3 Bilinear Maps and Quadratic Permutations

Now, we define bilinear maps and quadratic permutations which can be used to describe a quadratic quasigroup. We show that bilinear maps consist of bilinear forms, whereas quadratic permutations of quadratic forms.

Definition 2.18. Let γ be a Boolean map

$$\gamma : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n.$$

Then we say that γ is *bilinear* if it satisfies conditions

(i) $\gamma(u + w, v) = \gamma(u, v) + \gamma(w, v)$

(ii) $\gamma(u, v + w) = \gamma(u, v) + \gamma(u, w)$

(iii) $\gamma(\lambda u, v) = \gamma(u, \lambda v) = \lambda\gamma(u, v)$

for every $u, v, w \in V$ and $\lambda \in \mathbb{F}_2$. The last condition follows from the first two conditions, i.e., $\gamma(0u, v) = \gamma(u + u, v) = \gamma(u, v) + \gamma(u, v) = o = \gamma(u, v) + \gamma(u, v) = \gamma(u, v + v) = \gamma(u, 0v)$.

Consider a representation $\gamma_E = (f_1, \ldots, f_n)$ in some base E. Then for $u, v, w \in V$ where $\{u\}_E = x, \{v\}_E = y, \{w\}_E = z$ is $\gamma_E(x + z, y) = \gamma_E(\{u\}_E + \{w\}_E, \{v\}_E) = \gamma_E(\{u+w\}_E, \{v\}_E) = \{\gamma(u+w, v)\}_E = \{\gamma(u, v)+\gamma(w, v)\}_E = \{\gamma(u, v)\}_E + \{\gamma(w, v)\}_E = \gamma_E(x, y) + \gamma_E(z, y)$. The other two conditions for bilinearity are similarly satisfied, thus, γ_E is also bilinear. Then, each f_i as a component of γ_E has to satisfy the same conditions, therefore, f_i is a representation of a bilinear form.

On the other hand, if we construct a Boolean map γ' from a representation $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ where $\mathbf{b}_1, \ldots, \mathbf{b}_n$ are bilinear forms on the vector space $\mathbb{F}_2^n$ in a representation form, then the Boolean map γ' surely satisfies all conditions to be bilinear. We can claim

Lemma 2.19. *Let γ be a Boolean map*

$$\gamma : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$$

and E be a base of the vector space $\mathbb{F}_2^n$. Then γ is bilinear *if and only if there exist bilinear forms $\mathbb{F}_2^n$ $\mathbf{b}_1, \ldots, \mathbf{b}_n$ on the vector space such that $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is a representation of γ in the base E.*

Note that for each base there exists different vector of bilinear forms. Let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a representation of γ in the base E and $(\mathbf{b}'_1, \ldots, \mathbf{b}'_n)$ be a representation of γ in the base E'. If R is a transformation matrix from E to E' then $(\mathbf{b}_1, \ldots, \mathbf{b}_n) = (\mathbf{b}'_1, \ldots, \mathbf{b}'_n)R$.

Let $o = (0, \ldots, 0) \in \mathbb{F}_2^n$ denote a vector of zeros. Then $\{o\}_E = (0, \ldots, 0)$ for every base E of $\mathbb{F}_2^n$.

Definition 2.20. Let γ be a bilinear map on the vector space $\mathbb{F}_2^n$. We define the *left* and *right radical* as follows:

$$\operatorname{Rad}_L \gamma = \{u \in V; \gamma(u, w) = o, \forall w \in V\},$$
$$\operatorname{Rad}_R \gamma = \{u \in V; \gamma(w, u) = o, \forall w \in V\}.$$

It is easy to observe that $\operatorname{Rad}_L \gamma$, and $\operatorname{Rad}_R \gamma$ are vector subspaces of $\mathbb{F}_2^n$.

Let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a representation of the bilinear map γ in the base E. Then, we can equivalently set

$$\operatorname{Rad}_L \gamma = \bigcap_{i=1}^{n} \operatorname{Rad}_L \mathbf{b}_i,$$

and

$$\mathrm{Rad}_R\,\gamma = \bigcap_{i=1}^{n} \mathrm{Rad}_R\,\mathbf{b}_i.$$

Definition 2.21. Let α be a permutation of the vector space $\mathbb{F}_2^n$. We call α a *quadratic permutation* if it has degree 2 in the sense of Definition 2.5 and we call α a *linear permutation* if it has degree 1.

Lemma 2.22. *Let α be a linear permutation of the vector space $\mathbb{F}_2^n$ with a representation $(f_1, \ldots, f_n)$ in a base E. Then the representation can be expressed as*

$$\begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix} = Ax^T + c^T, \tag{2.3}$$

where the matrix $A \in \mathbb{F}_2^{n\times n}$ and the vector $c \in \mathbb{F}_2^n$ are uniquely determined and A is regular.

Also for each regular matrix A' and a vector $c' \in \mathbb{F}_2^n$, $A'x^T + c'^T$ is a representation of a linear permutation.

Proof. The polynomial f_i is linear for every $i = 1, \ldots, n$, thus, $f_i = a_0^i + \sum_{j=1}^n a_j^i x_j$ for some $a_j^i \in \mathbb{F}_2, j = 1, \ldots, n$. Then, we can define the matrix A as

$$A = \begin{pmatrix} a_1^1 & a_2^1 & \ldots & a_n^1 \\ a_1^2 & a_2^2 & \ldots & a_n^2 \\ \vdots & & & \\ a_1^n & a_2^n & \ldots & a_n^n \end{pmatrix},$$

and the vector c as

$$c = (a_0^1, a_0^2, \ldots, a_0^n),$$

which satisfy (2.3). Since the permutation α is invertible, the equation

$$y^T = Ax^T + c^T$$

has to have a unique solution x for every $y \in \mathbb{F}_2^n$. That's possible if and only if the matrix A is invertible and so

$$x^T = A^{-1}(y^T - c^T).$$

As we have just rewritten the expression in a matrix form, the uniqueness is clear.

The rest follows by direct verification. □

Corollary 2.23. *Let α be a linear permutation of the vector space $\mathbb{F}_2^n$. Then α^{-1} is also a linear permutation.*

Lemma 2.24. *Let β be a quadratic permutation of the vector space $\mathbb{F}_2^n$ with a representation $(f_1, \ldots, f_n)$ in a base E. Then there exists exactly one vector of quadratic forms $(\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_n)$ on the vector space $\mathbb{F}_2^n$ and exactly one vector $c \in \mathbb{F}_2^n$ such that the representation $(f_1, \ldots, f_n)$ can be expressed as*

$$\begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} \mathbf{q}_1(x_1, \ldots, x_n) \\ \mathbf{q}_2(x_1, \ldots, x_n) \\ \vdots \\ \mathbf{q}_n(x_1, \ldots, x_n) \end{pmatrix} + c^T. \tag{2.4}$$

Proof. The polynomial f_i is quadratic for every $i = 1, \ldots, n$, therefore, we can use Corollary 2.17 to find a quadratic form $\mathbf{q}_i$ and a constant $c_i \in \mathbb{F}_2$ such that the claim holds. □

Lemma 2.25. *Let α be a Boolean map*

$$\alpha : \overbrace{\mathbb{F}_2^n \times \cdots \times \mathbb{F}_2^n}^{m} \to \mathbb{F}_2^n$$

of degree $d, d > 0$ and $\mathcal{L}$ be a linear permutation of $\mathbb{F}_2^n$. Then maps

$$\alpha' : u_1, \ldots, u_m \mapsto \alpha(u_1, \ldots, \mathcal{L}(u_r), \ldots, u_m)$$

where $1 \leq r \leq m$, and

$$\alpha'' : u_1, \ldots, u_m \mapsto \mathcal{L}\big(\alpha(u_1, \ldots, u_m)\big)$$

are also of degree d.

Proof. Let $(f_1, \ldots, f_n)$, where $f_i \in \mathbb{F}_2[x_j; j = 1, \ldots, mn], i = 1, \ldots, n$, be a representation of α in a base E. Let $xL + c$, where $L = [l_{i,j}]$ is a regular matrix $n \times n$ and $c = (c_1, \ldots, c_n) \in \mathbb{F}_2^n$, be a representation of $\mathcal{L}$ in the base E. We will choose some monomial x_I from f_i. Now we divide the set I to $I_1 = I \cap \{(r-1)n + 1, \ldots, rn\}$ and $I_2 = I \setminus \{(r-1)n + 1, \ldots, rn\}$. We will denote $x^k = (x_{(k-1)n+1}, x_{(k-1)n+2}, \ldots, x_{kn})$. Then

$$\begin{aligned} & x_I\big(x^1, \ldots, x^{r-1}, x^r L + c, x^{r+1}, \ldots, x^m\big) \\ &\quad = x_I\big(x_1, \ldots, \sum_{i=1}^{n} l_{1,i} x_{r(n-1)+i} + c_1, \ldots, \sum_{i=1}^{n} l_{n,i} x_{r(n-1)+i} + c_n, \ldots, x_{mn}\big) \\ &\qquad = \prod_{j \in I_1} \left(\sum_{i=1}^{n} l_{j,i} x_{r(n-1)+i} + c_j \right) \cdot x_{I_2} = \sum_{J \subseteq I_1} a_J x_J \cdot x_{I_2} = \sum_{J \subseteq I_1} a_J x_{J \cup I_2}, \end{aligned}$$

where $a_J \in \mathbb{F}_2$, thus, the degree of monomial x_I after the composition with $\mathcal{L}$ is not greater than $|I|$. Note that $\deg(x_{J_1} + x_{J_2}) \leq \max\{|J_1|, |J_2|\}$ for sets $J_1, J_2 \subseteq \{1, 2, \ldots, mn\}$ (the degree is equal to $-\infty$ if $J_1 = J_2$), consequently, the polynomial $g_i = f_i\big(x^1, \ldots, x^{r-1}, x^r L + c, x^{r+1}, \ldots, x^m\big)$ satisfies $\deg(g_i) \leq \deg(f_i)$. The same procedure works for the polynomial g_i and the linear permutation $\mathcal{L}^{-1}$, providing $\deg(f_i) \leq \deg(g_i)$, thus $\deg(f_i) = \deg(g_i)$. All polynomials $f_i, g_i, i = 1, \ldots, n$ fulfil this identity. It is clear that the maps α and α' have the same degree since $(g_1, \ldots, g_n)$ represents the map α' .

Now, suppose that $(h_1, \ldots, h_n)$ represents the map $\alpha'' = \mathcal{L}(\alpha)$ in the base E. For each $k = 1, \ldots, n$ we can express the polynomial h_k as $h_k = \sum_{i=1}^{n} l_{k,i} f_i + c_k$. Then $\deg(h_k) \leq \max\{f_i, i = 1, \ldots, n\}$, and that's why degree of α'' is less or equal to degree of α. Using the same procedure for $\alpha = \mathcal{L}^{-1}(\alpha'')$ we will obtain equality of the degrees. □

Lemma 2.26. *Let α be a permutation of $\mathbb{F}_2^n$. Then there exists a permutation β of the same degree and a vector $c \in \mathbb{F}_2^n$ such that $\beta(o) = o$ and*

$$\alpha(u) = \beta(u) + c,$$

for every $u \in \mathbb{F}_2^n$.

Proof. We set $c = \alpha(o)$ and $\beta(u) = \alpha(u) + c$ for every $u \in \mathbb{F}_2^n$ □

Lemma 2.27. *Let β be a quadratic permutation of $\mathbb{F}_2^n$, which satisfies $\beta(o) = o$. Then the map $\widetilde{\beta} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ defined by*

$$\beta(u + v) = \beta(u) + \beta(v) + \widetilde{\beta}(u, v) \tag{2.5}$$

is bilinear.

Proof. Suppose β has a representation in a base E in the form $(\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_n) + c$, where $\mathbf{q}_i, i = 1, \ldots, n$ are quadratic forms as in Lemma 2.24. Then, since $\beta(o) = o$, hence $c = o$. The rest is clear using the definition of a quadratic form and Lemma 2.19. □

We say that the bilinear map $\widetilde{\beta}$ is *associated* with the quadratic permutation β. It is clear that the bilinear map $\widetilde{\beta}$ is symmetric and alternating, i.e., $\widetilde{\beta}(u, v) = \widetilde{\beta}(v, u)$ and $\widetilde{\beta}(u, u) = o$ for all $u, v \in \mathbb{F}_2^n$. Furthermore, the map β is linear if and only if $\widetilde{\beta}$ is trivial.

Lemma 2.28. *Let β be a permutation of $\mathbb{F}_2^n$ such that $\beta(o) = o$. Then β is quadratic permutation if and only if $\widetilde{\beta}$, defined by* (2.5)*, is a nontrivial bilinear map.*

Proof. It follows directly from Lemmas 2.24 and 2.19, and the definition of a quadratic form.

□

Definition 2.29. Let β be quadratic permutation of $\mathbb{F}_2^n$ such that $\beta(o) = o$. Then the set

$$\operatorname{Rad}\beta = \{u \in \mathbb{F}_2^n; \widetilde{\beta}(v,u) = \widetilde{\beta}(u,v) = 0, \forall v \in \mathbb{F}_2^n\}$$

is called the *radical* of the quadratic permutation β. We can see that $\operatorname{Rad}\beta = \operatorname{Rad}_L \widetilde{\beta} = \operatorname{Rad}_R \widetilde{\beta}$. Therefore, $\operatorname{Rad}\beta$ is a vector subspace of $\mathbb{F}_2^n$.

Let E be a base of $\mathbb{F}_2^n$ and let $(\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_n)$ be a representation of the quadratic permutation β in the base E. We see that

$$\operatorname{Rad}\beta = \bigcap_{i=1}^{n} \operatorname{Rad}\mathbf{q}_i.$$

Lemma 2.30. *Let β be a quadratic permutation of $\mathbb{F}_2^n$ such that $\beta(o) = o$. Then, for every $u, v \in \operatorname{Rad}\beta$, is*

$$\beta(u+v) = \beta(u) + \beta(v),$$

i.e., the restriction of β to $\operatorname{Rad}\beta$ is linear.

Proof. The claim follows directly from the definition of a radical. For every $u, v \in \operatorname{Rad}\beta$ is $\widetilde{\beta}(u,v) = o$, thus

$$\beta(u+v) = \beta(u) + \beta(v) + \widetilde{\beta}(u,v) = \beta(u) + \beta(v).$$

□

Lemma 2.31. *Let β be a quadratic permutation of $\mathbb{F}_2^n$ such that $\beta(o) = o$, and let $c \in \mathbb{F}_2^n$. We define a quadratic permutation α by $\alpha(u) = \beta(u) + \widetilde{\beta}(u,c)$. Then, α is a quadratic permutation of $\mathbb{F}_2^n$.*

Proof. Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be linear permutations $\mathcal{L}_1 : u \mapsto u + c$ and $\mathcal{L}_2 : u \mapsto u + \beta(c)$. Then the composition $\mathcal{L}_2 \circ \beta \circ \mathcal{L}_1$ is a quadratic permutation and satisfies

$$\begin{aligned}\mathcal{L}_2(\beta(\mathcal{L}_1(u))) &= \beta(u+c) + \beta(c)\\ &= \beta(u) + \widetilde{\beta}(u,c) + \beta(c) + \beta(c) = \beta(u) + \widetilde{\beta}(u,c) = \alpha(u).\end{aligned}$$

□

Lemma 2.32. *Consider a bilinear Boolean map α on the vector space $\mathbb{F}_2^n$. Then, for every fixed $c \in \mathbb{F}_2^n$, the maps defined by $u \mapsto \alpha(u, c)$ and $v \mapsto \alpha(c, v)$ are linear.*

Proof. Let E be base of $\mathbb{F}_2^n$. Then, using Lemma 2.19, we can find a vector of bilinear forms $(\mathbf{b}_1, \dots, \mathbf{b}_n)$ such that it represents the bilinear map α. Then for each $\mathbf{b}_k, k = 1, \dots, n$ there exist $a_{i,j}^k, i, j = 1, \dots, n$ such that $\sum_{i,j=1}^n a_{i,j}^k x_i y_j$ represents the bilinear form $\mathbf{b}_k$. Put $(c_1, \dots, c_n) = \{c\}_E$. Then,

$$\left(\sum_{i=1}^n \Big(\sum_{j=1}^n a_{i,j}^1 c_j\Big) x_i, \dots, \sum_{i=1}^n \Big(\sum_{j=1}^n a_{i,j}^n c_j\Big) x_i\right)$$

is representation of the map $u \mapsto \alpha(u, c)$ and

$$\left(\sum_{j=1}^n \Big(\sum_{i=1}^n a_{i,j}^1 c_i\Big) y_j, \dots, \sum_{j=1}^n \Big(\sum_{i=1}^n a_{i,j}^n c_i\Big) y_j\right)$$

is representation of the map $v \mapsto \alpha(c, v)$, where $\{u\}_E = (x_1, \dots, x_n)$ and $\{v\}_E = (y_1, \dots, y_n)$. It follows directly from the form of the representations that the both maps are linear. □

2.4 Boolean Quasigroups

In this section we finally define quadratic quasigroups ([8]). Then, we use the theory presented in the previous sections to represent a quadratic quasigroup as a sum of two quadratic permutations, a bilinear map, and a vector in the vector space $\mathbb{F}_2^n$. This representation is unique and provides a classification of quadratic quasigroups.

Suppose that $(Q, *)$ is a finite quasigroup of order 2^n upon the vector space $Q = \mathbb{F}_2^n$. Let $E = \{e_1, e_2, \dots e_n\}$ be a base of $\mathbb{F}_2^n$. Now, the binary operation $*$ can be seen as a Boolean map $* : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ defined as

$$* : (u, v) \mapsto w,$$

where $u, v, w \in \mathbb{F}_2^n$ satisfy $u * v = w$. Using Theorem 2.4 we can state

Lemma 2.33. *Let $(Q, *)$ be a quasigroup upon $\mathbb{F}_2^n$. For each base E of $\mathbb{F}_2^n$ there exists exactly one vector of Boolean polynomials $(f_1, f_2, \dots, f_n) \in \big(\mathbb{F}_2[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n]\big)^n$, such that*

$$\{u * v\}_E = \Big(f_1(\{u\}_E, \{v\}_E), \dots, f_n(\{u\}_E, \{v\}_E)\Big)$$

for all $u, v \in \mathbb{F}_2^n$.

Observation 2.34. *Let $(f_1, f_2, \ldots, f_n) \in \mathbb{F}_2[x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n]^n$ be a vector of Boolean polynomials. Then the system of equations with the variables $y_1, y_2, \ldots, y_n$*

$$\begin{array}{rcl} f_1(a_1, a_2, \ldots, a_n, y_1, y_2, \ldots, y_n) & = & b_1, \\ f_2(a_1, a_2, \ldots, a_n, y_1, y_2, \ldots, y_n) & = & b_2, \\ & \vdots & \\ f_n(a_1, a_2, \ldots, a_n, y_1, y_2, \ldots, y_n) & = & b_n, \end{array}$$

and the system of equations with the variables $x_1, x_2, \ldots, x_n$

$$\begin{array}{rcl} f_1(x_1, x_2, \ldots, x_n, c_1, c_2, \ldots, c_n) & = & d_1, \\ f_2(x_1, x_2, \ldots, x_n, c_1, c_2, \ldots, c_n) & = & d_2, \\ & \vdots & \\ f_n(x_1, x_2, \ldots, x_n, c_1, c_2, \ldots, c_n) & = & d_n, \end{array}$$

have for every $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{F}_2^n$ and every $(c_1, \ldots, c_n), (d_1, \ldots, d_n) \in \mathbb{F}_2^n$ exactly one solution if and only if $(f_1, f_2, \ldots, f_n)$ is a representation of a quasigroup in some base E.

Definition 2.35. Let $(Q, *)$ be a quasigroup upon $\mathbb{F}_2^n$. We call $(Q, *)$ a *Boolean quasigroup of degree d* if the Boolean map $* : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ is of degree d.

Definition 2.36. Let Q_1 and Q_2 be quasigroups upon $\mathbb{F}_2^n$. We say that Q_1 and Q_2 are *linearly isotopic* if there exist three linear permutations $\mathcal{L}_1, \mathcal{L}_2$ and $\mathcal{L}_3$ which form an isotopy $(\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3)$ such that

$$(\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3) : Q_1 \to Q_2.$$

We say that Q_1 and Q_2 are *linearly isomorphic* if $\mathcal{L}_1 = \mathcal{L}_2 = \mathcal{L}_3$.

We observe that the relation of being linearly isotopic represents an equivalence on the set of quasigroups. We show in the following proposition that all quasigroups in one class of equivalence have the same degree.

Proposition 2.37. *Linearly isotopic Boolean quasigroup have the same degree.*

Proof. The assertion follows directly from Lemma 2.25. □

We shall call the Boolean quasigroup of degree 2 shortly a *quadratic quasigroup* and Boolean quasigroups of degree 1 a *linear quasigroup.*

Let $(\mathbb{F}_2^n, *)$ be a quadratic quasigroup and $(f_1, f_2, \dots, f_n)$ be its representation in a base E. In a general case the form of the polynomial f_i is as follows:

$$\begin{aligned} & f_i(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n) \\ & \quad = \sum_{k,l \in \{1,\dots,n\}} m^i_{k,l}\ x_k y_l + \sum_{\substack{k,l \in \{1,\dots,n\} \\ k<l}} a^i_{k,l}\ x_k x_l + \sum_{\substack{k,l \in \{1,\dots,n\} \\ k<l}} b^i_{k,l}\ y_k y_l \\ & \qquad\qquad + \sum_{k \in \{1,\dots,n\}} c^i_k x_k + \sum_{k \in \{1,\dots,n\}} d^i_k y_k + e^i, \qquad (2.6) \end{aligned}$$

where the coefficients $m^i_{k,l}, a^i_{k,l}, b^i_{k,l}, c^i_k, d^i_k, e^i \in \mathbb{F}_2$. Using Corollary 2.10 and Corollary 2.16, we can express this polynomial as

$$\begin{aligned} & f_i(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n) \\ & \quad = \mathbf{p}_i(x_1, \dots, x_n) + \mathbf{b}_i\big((x_1, \dots, x_n), (y_1, \dots, y_n)\big) + \mathbf{q}_i(y_1, \dots, y_n) + d_i, \end{aligned}$$

where $\mathbf{p}_i, \mathbf{q}_i$ are quadratic and $\mathbf{b}_i$ bilinear forms in their coordinate representation in the base $E, (x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n)$ are the coordinates in the base E and $d_i \in \mathbb{F}_2$. We have just showed following

Lemma 2.38. *Let $(\mathbb{F}_2^n, *)$ be a quadratic quasigroup. Then, for every base E of $\mathbb{F}_2^n$ there exist quadratic forms $\mathbf{p}_i, \mathbf{q}_i, i = 1, \dots, n$, bilinear forms $\mathbf{b}_i, i = 1, \dots, n$ on the vector space $\mathbb{F}_2^n$ and a vector of constants $d \in \mathbb{F}_2^n$ such that*

$$\{u * v\}_E = \begin{pmatrix} \mathbf{p}_1(x) \\ \mathbf{p}_2(x) \\ \vdots \\ \mathbf{p}_n(x) \end{pmatrix} + \begin{pmatrix} \mathbf{b}_1(x,y) \\ \mathbf{b}_2(x,y) \\ \vdots \\ \mathbf{b}_n(x,y) \end{pmatrix} + \begin{pmatrix} \mathbf{q}_1(y) \\ \mathbf{q}_2(y) \\ \vdots \\ \mathbf{q}_n(y) \end{pmatrix} + d^T \qquad (2.7)$$

is a representation of $(\mathbb{F}_2^n, *)$ in the base E where $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$, while $\{u\}_E = x, \{v\}_E = y$.

Lemma 2.39. *Let E be a base of the vector space $\mathbb{F}_2^n$ and $(\mathbb{F}_2^n, *)$ be a quadratic quasigroup with a representation in the form (2.7). Then each of vectors $(\mathbf{p}_1, \dots, \mathbf{p}_n)$ and $(\mathbf{q}_1, \dots, \mathbf{q}_n)$ represents a quadratic or linear permutation.*

Proof. Recall that every quadratic form $\mathbf{q}$ and bilinear form $\mathbf{b}$ satisfy $\mathbf{q}(o) = 0$ and $\mathbf{b}(x, o) = \mathbf{b}(o, y) = 0$. Now we can easily derive representations of the translations L_o and R_o.

$$\begin{aligned} & \{L_o(v)\}_E = \{o * v\}_E \\ & \quad = \begin{pmatrix} \mathbf{p}_1(o) \\ \mathbf{p}_2(o) \\ \vdots \\ \mathbf{p}_n(o) \end{pmatrix} + \begin{pmatrix} \mathbf{b}_1(o,y) \\ \mathbf{b}_2(o,y) \\ \vdots \\ \mathbf{b}_n(o,y) \end{pmatrix} + \begin{pmatrix} \mathbf{q}_1(y) \\ \mathbf{q}_2(y) \\ \vdots \\ \mathbf{q}_n(y) \end{pmatrix} + d^T = \begin{pmatrix} \mathbf{q}_1(y) \\ \mathbf{q}_2(y) \\ \vdots \\ \mathbf{q}_n(y) \end{pmatrix} + d^T, \end{aligned}$$

$$\begin{aligned}\{R_o(u)\}_E &= \{u * o\}_E \\ &= \begin{pmatrix} \mathbf{p}_1(x) \\ \mathbf{p}_2(x) \\ \vdots \\ \mathbf{p}_n(x) \end{pmatrix} + \begin{pmatrix} \mathbf{b}_1(x,o) \\ \mathbf{b}_2(x,o) \\ \vdots \\ \mathbf{b}_n(x,o) \end{pmatrix} + \begin{pmatrix} \mathbf{q}_1(o) \\ \mathbf{q}_2(o) \\ \vdots \\ \mathbf{q}_n(o) \end{pmatrix} + d^T = \begin{pmatrix} \mathbf{p}_1(x) \\ \mathbf{p}_2(x) \\ \vdots \\ \mathbf{p}_n(x) \end{pmatrix} + d^T,\end{aligned}$$

where $u, v \in \mathbb{F}_2^n$ and $\{u\}_E = x, \{v\}_E = y$. Let $c \in \mathbb{F}_2^n$ satisfy $\{c\}_E = d$. Because L_o and R_o are permutations of $\mathbb{F}_2^n$, $L_o - c$ and $R_o - c$ are permutations too and their representations are exactly $(\mathbf{q}_1, \dots, \mathbf{q}_n)$ and $(\mathbf{p}_1, \dots, \mathbf{p}_n)$, respectively. If at least one of the quadratic forms $\mathbf{q}_1, \dots, \mathbf{q}_n$, or $\mathbf{p}_1, \dots, \mathbf{p}_n$ is associated with a nontrivial bilinear form, then $L_o - c$, or $R_o - c$, respectively, is a quadratic permutation. Otherwise, it's a linear permutation. □

Theorem 2.40. *Let $(\mathbb{F}_2^n, *)$ be a quadratic quasigroup. Then there exist Boolean permutations α and β of $\mathbb{F}_2^n$ that are of degrees at most 2 and satisfy $\alpha(o) = \beta(o) = o$, a bilinear Boolean map γ on $\mathbb{F}_2^n$ and a vector $c \in \mathbb{F}_2^n$ such that*

$$u * v = \alpha(u) + \gamma(u, v) + \beta(v) + c$$

for every $u, v \in \mathbb{F}_2^n$. The maps α, β, γ and the vector c are uniquely determined.

Proof. Suppose the quasigroup $(\mathbb{F}_2^n, *)$ is represented in the base E as in Lemma 2.38, i.e.,

$$\{u * v\}_E = \begin{pmatrix} \mathbf{p}_1(x) \\ \mathbf{p}_2(x) \\ \vdots \\ \mathbf{p}_n(x) \end{pmatrix} + \begin{pmatrix} \mathbf{b}_1(x,y) \\ \mathbf{b}_2(x,y) \\ \vdots \\ \mathbf{b}_n(x,y) \end{pmatrix} + \begin{pmatrix} \mathbf{q}_1(y) \\ \mathbf{q}_2(y) \\ \vdots \\ \mathbf{q}_n(y) \end{pmatrix} + d^T,$$

whenever $u, v \in \mathbb{F}_2^n, \{u\}_E = x$, and $\{v\}_E = y$. It follows from Lemma 2.39 that $(\mathbf{p}_1, \dots, \mathbf{p}_n)$ and $(\mathbf{q}_1, \dots, \mathbf{q}_n)$ are representations of Boolean permutations which are linear or quadratic. Let α and β denote these permutations. The representations of α and β imply that $\alpha(o) = \beta(o) = o$. Lemma 2.19 yields that $(\mathbf{b}_1, \dots, \mathbf{b}_n)$ is a representation of a bilinear Boolean map. Let γ denote this bilinear map. Next, define a vector $c \in \mathbb{F}_2^n$ by $\{c\}_E = d$. Suppose that $u, v \in \mathbb{F}_2^n$ and $\{u\}_E = x, \{v\}_E = y$. Then, using the fact that $u \mapsto \{u\}_E$ is an isomorphism of the vector space $\mathbb{F}_2^n$ and the vector space of coordinates

$\mathbb{F}_2^n$, we see that

$$\begin{aligned}\{u*v\}_E &= \begin{pmatrix}\mathbf{p}_1(x)\\ \mathbf{p}_2(x)\\ \vdots \\ \mathbf{p}_n(x)\end{pmatrix} + \begin{pmatrix}\mathbf{b}_1(x,y)\\ \mathbf{b}_2(x,y)\\ \vdots \\ \mathbf{b}_n(x,y)\end{pmatrix} + \begin{pmatrix}\mathbf{q}_1(y)\\ \mathbf{q}_2(y)\\ \vdots \\ \mathbf{q}_n(y)\end{pmatrix} + d^T\\ &= \{\alpha(u)\}_E + \{\gamma(u,v)\}_E + \{\beta(v)\}_E + \{c\}_E\\ &= \{\alpha(u)+\gamma(u,v)+\beta(v)+c\}_E\end{aligned}$$

which implies $u*v = \alpha(u)+\gamma(u,v)+\beta(v)+c$.

Consider maps α', β', γ' and a vector c' which satisfy the claim, too. Then

$$\begin{aligned}\alpha(o)+\gamma(o,o)+\beta(o)+c = o*o = \alpha'(o)+\gamma'(o,o)+\beta'(o)+c' &\Rightarrow \quad c=c',\\ \alpha(u)+\gamma(u,o)+\beta(o)+c = u*o = \alpha'(u)+\gamma'(u,o)+\beta'(o)+c &\Rightarrow \quad \alpha=\alpha',\\ \alpha(o)+\gamma(o,v)+\beta(v)+c = o*v = \alpha(o)+\gamma'(o,v)+\beta'(v)+c &\Rightarrow \quad \beta=\beta',\\ \alpha(u)+\gamma(u,v)+\beta(v)+c = u*v = \alpha(u)+\gamma'(u,v)+\beta(v)+c &\Rightarrow \quad \gamma=\gamma'.\end{aligned}$$

Thus the maps α, β, γ and the vector c are uniquely determined. □

A linear quasigroup is just a special case of a quadratic quasigroup, therefore, we can state the following definition for both linear, and quadratic quasigroups.

Definition 2.41. Let $(Q,*)$ be a linear or quadratic quasigroup. The expression of $*$ as

$$u*v = \alpha(u)+\gamma(u,v)+\beta(v)+c,$$

from Theorem 2.40, will be called a *canonical decomposition.* In such a case we shall say that the quasigroup $(Q,*)$ decomposes as $(\alpha,\gamma,\beta)_c$. We shall call α the *left component* of $(Q,*)$, β the *right component*, γ the *bilinear component* and c the (*translation*) *factor.*

We can now state an interesting property of a quadratic quasigroup.

Corollary 2.42. *Let $(\mathbb{F}_2^n,*)$ be a quadratic quasigroup. Then the Boolean map $\gamma : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ defined as*

$$\gamma : (u,v) \mapsto (u*v) + R_o(u) + L_o(v) + (o*o)$$

is bilinear.

Definition 2.43. Let $(Q,*)$ be a quadratic quasigroup and $(\alpha,\gamma,\beta)_c$ be its canonical decomposition. We associate the quasigroup $(Q,*)$ with a *type* (i,j,k), where $i,j,k \in \{0,1\}$ such that $i=0$ iff α is linear, $k=0$ iff β is linear and $j=0$ iff γ is trivial.

We show in the following proposition that each equivalence class of linearly isotopic quadratic quasigroups has an invariant type.

Proposition 2.44. *Linearly isotopic quadratic quasigroup are of the same type.*

Proof. Let $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$ be linear permutations of $\mathbb{F}_2^n$ which forms an isotopy between quadratic quasigroups $(Q_1, *)$ and $(Q_2, \circ)$ upon the vector space $\mathbb{F}_2^n$. Each permutation $\mathcal{L}_i, i = 1, 2, 3$ can be expressed as $\mathcal{L}'_i + c_i$, where $\mathcal{L}'_i$ is linear permutation such that $\mathcal{L}'_i(o) = o$, and $c_i \in \mathbb{F}_2^n$ (we used Lemma 2.26). Let $(\alpha, \gamma, \beta)_c$ be a canonical decomposition of $(Q_1, *)$. Then

$$\begin{aligned}\mathcal{L}_3(u \circ v) = {} & \alpha(\mathcal{L}'_1(u) + c_1) + \gamma(\mathcal{L}'_1(u) + c_1, \mathcal{L}'_2(v) + c_2) + \beta(\mathcal{L}'_2(v) + c_2) \\ = {} & \underbrace{\alpha(\mathcal{L}'_1(u)) + \widetilde{\alpha}(\mathcal{L}'_1(u), c_1) + \gamma(\mathcal{L}'_1(u), c_2)}_{=\alpha'(u)} \\ & + \underbrace{\gamma(\mathcal{L}'_1(u), \mathcal{L}'_2(v))}_{=\gamma'(u,v)} \\ & + \underbrace{\beta(\mathcal{L}'_2(v)) + \widetilde{\beta}(\mathcal{L}'_2(v), c_2) + \gamma(c_1, \mathcal{L}'_2(v))}_{=\beta'(v)} \\ & + \underbrace{\alpha(c_1) + \gamma(c_1, c_2) + \beta(c_2) + c}_{=c'}.\end{aligned}$$

It follows from Lemmas 2.32 and 2.25 that the maps $u \mapsto \widetilde{\alpha}(\mathcal{L}'_1(u), c_1)$, $u \mapsto \gamma(\mathcal{L}'_1(u), c_2)$,$v \mapsto \widetilde{\alpha}(\mathcal{L}'_2(v), c_2)$, and $v \mapsto \gamma(c_1, \mathcal{L}'_2(v))$ are linear. Lemma 2.25 implies the map $u \mapsto \alpha(\mathcal{L}'_1(u))$ is of the same degree as α and $v \mapsto \beta(\mathcal{L}'_2(v))$ is of the same degree as β. If the map α is quadratic then α' is quadratic too. In the case that the map α is linear, the map α' is either linear, or constant. Suppose that $\alpha' = b$ for some $b \in \mathbb{F}_2^n$. Then, $\mathcal{L}_3(u \circ o) = \alpha'(u) + \gamma'(u, o) + \beta'(o) = b$ for every $u \in \mathbb{F}_2^n$, which is contradiction. That means the degree of α' is the same as the degree of α and symmetrically the degree of β' is same as the degree of β. It can be easily observed that $\alpha'(o) = \beta'(o) = o$. It follows from Lemma 2.25 that the degree of the map γ' is the same as the degree of γ (i.e., 2, or both γ' and γ are trivial), and by direct verification we can see that γ' is a bilinear map. Now, define maps

$$\begin{aligned}\alpha''(u) &= \mathcal{L}'^{-1}_3(\alpha'(u)), \\ \gamma''(u, v) &= \mathcal{L}'^{-1}_3(\gamma'(u, v)), \text{ and} \\ \beta''(v) &= \mathcal{L}'^{-1}_3(\beta'(v)),\end{aligned}$$

and the vector $c'' = \mathcal{L}'^{-1}_3(c') + \mathcal{L}'^{-1}_3 c_3$. Lemma 2.25 implies that the degree of map α'' is same as the degree of α', β'' as β' and γ'' as γ'. By direct verification we can see that γ'' is a bilinear map and $\alpha''(o) = \beta''(o) = o$. The maps satisfy $u \circ v = \alpha''(u) + \gamma''(u, v) + \beta''(v) + c''$. Suppose L_o and R_o is the left and right translation of $(Q_2, \circ)$. Then,

$$\begin{aligned} R_o(u) &= u \circ o = \alpha''(u) + \gamma''(u, o) + \beta''(o) + c'' = \alpha''(u) + c'', \text{ and} \\ L_o(u) &= o \circ u = \alpha''(o) + \gamma''(o, u) + \beta''(u) + c'' = \beta''(u) + c'', \end{aligned}$$

thus, α'' and β'' are permutations and $(\alpha'', \gamma'', \beta'')_{c''}$ is canonical decomposition of $(Q_2, \circ)$, therefore, $(Q_2, \circ)$ is of the same type as $(Q_1, *)$. □

Proposition 2.45. *Linear quasigroups are necessarily of the type* $(0, 0, 0)$.

Proof. Consider the canonical decomposition $(\alpha, \gamma, \beta)_c$ of a linear quasigroup $(Q, *)$, i.e.,

$$u * v = \alpha(u) + \gamma(u, v) + \beta(v) + c.$$

Then $(Q, *)$ is linear if and only if at least one of the maps α, β or γ is linear and the others are constant. Because the maps α, and β cannot be constant, they have to be linear. Each representation of the map γ is composed from bilinear forms, which are always quadratic, therefore, γ is trivial. □

Example 2.46. Let the finite quasigroup $(Q, *)$ of order $2^3 = 8$ be given by the Cayley table 2.1.

$*$	0	1	2	3	4	5	6	7
0	1	5	4	7	3	6	2	0
1	0	2	6	3	7	4	5	1
2	2	0	3	6	4	7	1	5
3	5	1	7	4	6	3	0	2
4	6	3	0	2	5	1	7	4
5	4	7	1	5	2	0	3	6
6	7	4	5	1	0	2	6	3
7	3	6	2	0	1	5	4	7

Table 2.1: Cayley table of $(Q, *)$ of order 8

Using an inverse of the bijection $\varphi : \mathbb{F}_2^3 \to \mathbb{Z}_8$, $\varphi(x_1, x_2, x_3) = 4x_1 + 2x_2 + x_3$ we can represent each element of Q as a binary vector from $\mathbb{F}_2^3$. Then the representation of $(Q,*)$ in the canonic base is as follows

$$\begin{aligned}
f_1(x_1,x_2,x_3,y_1,y_2,y_3) &= x_2y_1+x_2y_2+x_2y_3+x_3y_1+x_3y_3+x_2x_3+y_1y_2\\
&\quad + y_2y_3+x_1+y_2+y_3,\\
f_2(x_1,x_2,x_3,y_1,y_2,y_3) &= x_1y_2+x_2y_3+x_3y_2+x_3y_3+x_1x_2+x_1x_3+x_2x_3\\
&\quad + y_2y_3+x_1+x_2+y_1,\\
f_3(x_1,x_2,x_3,y_1,y_2,y_3) &= x_1y_1+x_1y_2+x_1y_3+x_3y_1+x_3y_2+x_1x_3+y_1y_3\\
&\quad + y_2y_3+x_1+x_2+x_3+y_2+1.
\end{aligned}$$

Now, consider a canonical decomposition $(\alpha,\gamma,\beta)_c$ of $(Q,*)$. Then,

$$\begin{pmatrix} x_2x_3+x_1\\ x_1x_2+x_1x_3+x_2x_3+x_1+x_2\\ x_1x_3+x_1+x_2+x_3 \end{pmatrix}$$

is a representation of α,

$$\begin{pmatrix} y_2y_3+y_2+y_3\\ y_2y_3+y_1\\ y_1y_3+y_2y_3+y_2 \end{pmatrix}$$

is a representation of β,

$$\begin{pmatrix} x_2y_1+x_2y_2+x_2y_3+x_3y_1+x_3y_3\\ x_1y_2+x_2y_3+x_3y_2+x_3y_3\\ x_1y_1+x_1y_2+x_1y_3+x_3y_1+x_3y_2 \end{pmatrix}$$

is a representation of γ, and $c=(0,0,1)$. It can be easily seen that $(Q,*)$ is a quadratic quasigroup of the type $(1,1,1)$.

2.5 Quadratic Loops

In this section we describe properties of quadratic loops using the classification from the previous section. Then, we show that each quadratic loop can be represented by n matrices $n\times n$ and we present a necessary condition so that the matrices could represent a quadratic loop.

Lemma 2.47. *Let $(Q,*)$ be a quadratic loop and let $e\in\mathbb{F}_2^n$ be its unit. Then there exists a quadratic loop $(Q,\circ)$ with the unit $o=(0,0,\dots,0)\in\mathbb{F}_2^n$ which is linearly isomorphic to $(Q,*)$.*

Proof. Define a binary operation $\circ$ by $x \circ y = \mathcal{L}^{-1}\big(\mathcal{L}(x) * \mathcal{L}(y)\big)$, where $\mathcal{L}$ is a bijection

$$\begin{aligned} \mathcal{L} &: \mathbb{F}_2^n \to \mathbb{F}_2^n, \\ \mathcal{L} &: x \mapsto x + e. \end{aligned}$$

Then

$$\begin{aligned} x \circ o = \mathcal{L}^{-1}\big(\mathcal{L}(x) * \mathcal{L}(o)\big) = (x+e) * e + e = x + e + e = x, \\ o \circ x = \mathcal{L}^{-1}\big(\mathcal{L}(o) * \mathcal{L}(x)\big) = e * (x+e) + e = x + e + e = x, \end{aligned}$$

for every $x \in Q$ so o is the unit. Since $\mathcal{L}(x \circ y) = \mathcal{L}(x) * \mathcal{L}(y)$, hence $\mathcal{L}$ is an isomorphism between $(Q, *)$ and $(Q, \circ)$. Using Proposition 2.37 we can see that $(Q, \circ)$ is also a quadratic quasigroup. □

Theorem 2.48. *Let $(Q, *)$ be a linear or a quadratic loop with the unit $o = (0, 0, \ldots, 0) \in \mathbb{F}_2^n$. Suppose that the quasigroup $(Q, *)$ is canonically decomposed as $(\alpha, \gamma, \beta)_c$. Then $\alpha = \beta = \mathrm{Id}$ and $c = o$, i.e., for every $u, v \in Q$, we have*

$$u * v = u + \gamma(u, v) + v.$$

Proof. We know that

$$u * v = \alpha(u) + \gamma(u, v) + \beta(v) + c.$$

The vector o is both left, and right unit, and thus, for every $u \in Q$

$$\begin{aligned} o = o * o = \alpha(o) + \gamma(o, o) + \beta(o) + c = c \quad &\Rightarrow \quad c = o, \\ \mathrm{Id}(u) = R_o(u) = u * o = \alpha(u) + \gamma(u, o) + \beta(o) = \alpha(u) \quad &\Rightarrow \quad \alpha = \mathrm{Id}, \text{ and} \\ \mathrm{Id}(u) = L_o(u) = o * u = \alpha(o) + \gamma(o, u) + \beta(u) = \beta(u) \quad &\Rightarrow \quad \beta = \mathrm{Id}\,. \end{aligned}$$

□

The previous theorem also yields that if the loop $(Q, *)$ is linear, then it is of the type $(0, 0, 0)$. If the loop $(Q, *)$ is quadratic, then it is of the type $(0, 1, 0)$.

Proposition 2.49. *The only linear loop with a unit $o = (0, 0, \ldots, 0)$ is the group $(\mathbb{F}_2^n, +)$.*

Proof. Directly by Theorem 2.48 and Proposition 2.45 we have

$$u * v = u + v$$

for every $u, v \in \mathbb{F}_2^n$. □

Consider a base E of $\mathbb{F}_2^n$. The representation in the base E of the identity is simply $(f_1, \ldots, f_n) = (x_1, \ldots, x_n)$. The representation of the bilinear component γ in the base E is $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, where $\mathbf{b}_i, i = 1, \ldots, n$ are bilinear forms on $\mathbb{F}_2^n$. Each bilinear form $\mathbf{b}_i$ has a form xM_iy^T where M_i is matrix in $\mathbb{F}_2^{n\times n}$. Then, we can express the representation of the quadratic loop Q in base E as follows

$$\begin{pmatrix} xM_1y^T \\ xM_2y^T \\ \vdots \\ xM_ny^T \end{pmatrix} + x^T + y^T. \tag{2.8}$$

Now let $M_i = [m^i_{k,l}] \in \mathbb{F}_2^{n\times n}, i = 1, \ldots, n$ be arbitrary matrices. We shall try to derive necessary conditions for $M_1, M_2, \ldots, M_n$ so that a loop with the unit $o = (0, 0, \ldots, 0) \in \mathbb{F}_2^n$ can be represented in the form (2.8). Note that $xM_iy^T = (xM_iy^T)^T = yM_i^Tx^T$. Using Observation 2.34, we can see that each of equations (2.9) and (2.10)

$$\begin{pmatrix} aM_1y^T \\ aM_2y^T \\ \vdots \\ aM_ny^T \end{pmatrix} + a^T + y^T = b^T$$

$$\underbrace{\left(\begin{pmatrix} aM_1 \\ aM_2 \\ \vdots \\ aM_n \end{pmatrix} + I_n\right)}_{\mathbf{\Lambda}(a)} y^T = b^T + a^T, \tag{2.9}$$

$$\begin{pmatrix} cM_1^Tx^T \\ cM_2^Tx^T \\ \vdots \\ cM_n^Tx^T \end{pmatrix} + x^T + c^T = d^T$$

$$\underbrace{\left(\begin{pmatrix} cM_1^T \\ cM_2^T \\ \vdots \\ cM_n^T \end{pmatrix} + I_n\right)}_{\mathbf{\Omega}(c)} x^T = d^T + c^T, \tag{2.10}$$

has to have a unique solution for every $a, b \in \mathbb{F}_2^n$, and every $c, d \in \mathbb{F}_2^n$, respectively. It means that the matrices $\mathbf{\Lambda}(a)$ and $\mathbf{\Omega}(c)$ have to be regular for every

$a, c \in \mathbb{F}_2^n$. Then we can easily express the solution as

$$y^T = \mathbf{\Lambda}(a)^{-1}(b^T + a^T)$$

and

$$x^T = \mathbf{\Omega}(c)^{-1}(d^T + c^T).$$

Recall that the matrices $\mathbf{\Lambda}(a)$ and $\mathbf{\Omega}(c)$ are regular if and only if $\det \mathbf{\Lambda}(a) = 1$ and $\det \mathbf{\Omega}(c) = 1$ in $\mathbb{F}_2$. We have just proved

Theorem 2.50. *Let $M_i = [m_{k,l}^i] \in \mathbb{F}_2^{n \times n}, i = 1, \ldots, n$ be arbitrary matrices. Then the vector of polynomials*

$$\begin{pmatrix} xM_1y^T \\ xM_2y^T \\ \vdots \\ xM_ny^T \end{pmatrix} + x^T + y^T$$

represents a quadratic loop with the unit $o = (0, 0, \ldots, 0)$ if and only if $\det \mathbf{\Lambda}(a) = 1$ and $\det \mathbf{\Omega}(c) = 1$ for every $a, c \in \mathbb{F}_2^n$, where $\mathbf{\Lambda}(a), \mathbf{\Omega}(c)$ are the matrices defined in (2.9) and (2.10).

Expanding the determinants $\det \mathbf{\Lambda}(a)$ and $\det \mathbf{\Omega}(c)$ we obtain

$$\det \mathbf{\Lambda}(a) = \lambda_\emptyset + \sum_{i_1 \in \{1,\ldots,n\}} \lambda_{i_1} a_{i_1} + \sum_{\substack{i_1,i_2 \in \{1,\ldots,n\} \\ i_1 < i_2}} \lambda_{i_1,i_2}\, a_{i_1} a_{i_2} + \sum_{\substack{i_1,i_2,i_3 \in \{1,\ldots,n\} \\ i_1 < i_2 < i_3}} \lambda_{i_1,i_2,i_3}\, a_{i_1} a_{i_2} a_{i_3} + \cdots + \lambda_{1,2,\ldots,n}\, a_1 a_2 \ldots a_n, \quad (2.11)$$

and

$$\det \mathbf{\Omega}(c) = \omega_\emptyset + \sum_{i_1 \in \{1,\ldots,n\}} \omega_{i_1} c_{i_1} + \sum_{\substack{i_1,i_2 \in \{1,\ldots,n\} \\ i_1 < i_2}} \omega_{i_1,i_2}\, c_{i_1} c_{i_2} + \sum_{\substack{i_1,i_2,i_3 \in \{1,\ldots,n\} \\ i_1 < i_2 < i_3}} \omega_{i_1,i_2,i_3}\, c_{i_1} c_{i_2} c_{i_3} + \cdots + \omega_{1,2,\ldots,n}\, c_1 c_2 \ldots c_n, \quad (2.12)$$

where the elements λ_I, ω_I depend only on $\{m_{k,l}^i; i, k, l = 1, 2, \ldots, n\}$ for every $I \subseteq \{1, 2, \ldots, n\}$.

Proposition 2.51. *Let $\mathbf{\Lambda}(a), \mathbf{\Omega}(c)$ be the matrices defined in (2.9) and (2.10) and let λ_I, ω_I be the elements defined in (2.11) and (2.12) for every $I \subseteq \{1, 2, \ldots, n\}$. Then the conditions $\det \mathbf{\Lambda}(a) = 1$ and $\det \mathbf{\Omega}(c) = 1$ are satisfied for every chosen $a, c \in \mathbb{F}_2^n$ if and only if*

$$\lambda_\emptyset = \omega_\emptyset = 1 \text{ and } \lambda_I = \omega_I = 0 \text{ for every nonempty } I \subseteq \{1, 2, \ldots, n\}. \quad (2.13)$$

Proof. We consider a Boolean polynomial $f = \det \mathbf{\Lambda}(x_1, \ldots, x_n)$. Its corresponding Boolean function $\bar{f}$ has to satisfy $\bar{f}(a) = 1$ for every $a \in \mathbb{F}_2^n$. We can observe that $\bar{f} = \bar{g}$ holds for the Boolean polynomial $g = 1$. Theorem 2.3 implies that $f = g$, i.e., the coefficients λ_I of polynomial f have to fulfil the conditions (2.13). The proof regarding $\det \mathbf{\Omega}(c)$ can be led in the same way. □

Proposition 2.52. *Let $\lambda_\emptyset, \omega_\emptyset$ be the elements defined in* (2.11) *and* (2.12). *Then, $\lambda_\emptyset = \omega_\emptyset = 1$ necessarily.*

Proof. The value in the cell of the matrix $\mathbf{\Lambda}(a)$ on the position (i, j) is as follows

$$\mathbf{\Lambda}(a)_{i,j} = \left(\sum_{k=1}^{n} m^i_{k,j} a_k\right) + \delta_{i,j}.$$

Hence,

$$\det \mathbf{\Lambda}(a) = \sum_{\pi \in S_n} \prod_{i=1}^{n} \left(\sum_{k=1}^{n} m^i_{k,\pi(i)} a_k\right) + \delta_{i,\pi(i)}.$$

Using the equation (2.11) it be easily observed that $\det \mathbf{\Lambda}(0, 0, \ldots, 0) = \lambda_\emptyset$. So $\lambda_\emptyset = \sum_{\pi \in S_n} \prod_{i=1}^n \delta_{i,\pi(i)} = \prod_{i=1}^n \delta_{i,\mathrm{Id}(i)} = 1$. An analogous proof will work for $\omega_\emptyset$. □

Proposition 2.53. *Let $\lambda_{1,\ldots,n}, \omega_{1,\ldots,n}$ be the elements defined in* (2.11) *and* (2.12). *Then,*

$$\lambda_{1,\ldots,n} = \omega_{1,\ldots,n} = \sum_{\pi,\rho \in S_n} \prod_{i=1}^{n} m^i_{\rho(i),\pi(i)}.$$

Proof. We know that

$$\det \mathbf{\Lambda}(a) = \sum_{\pi \in S_n} \prod_{i=1}^{n} \left(\sum_{k=1}^{n} m^i_{k,\pi(i)} a_k\right) + \delta_{i,\pi(i)}.$$

For fixed $\pi \in S_n$ we can rewrite $\prod_{i=1}^n (\sum_{k=1}^n m^i_{k,\pi(i)} a_k) + \delta_{i,\pi(i)}$ as

$$\begin{aligned}
&(m^1_{1,\pi(1)} a_1 + m^1_{2,\pi(1)} a_2 + \cdots + m^1_{n,\pi(1)} a_n + \delta_{1,\pi(1)}) \\
&\cdot(m^2_{1,\pi(2)} a_1 + m^2_{2,\pi(2)} a_2 + \cdots + m^2_{n,\pi(2)} a_n + \delta_{2,\pi(2)}) \\
&\vdots \\
&\cdot(m^n_{1,\pi(n)} a_1 + m^n_{2,\pi(n)} a_2 + \cdots + m^n_{n,\pi(n)} a_n + \delta_{n,\pi(n)}).
\end{aligned} \tag{2.14}$$

If we choose the term $m^i_{k_i,\pi(i)} a_{k_i}$ in i-th row in such a way, that $k_i \neq k_j$ whenever $i \neq j, i, j \in \{1, 2, \ldots, n\}$, and multiple these terms, we will have $\prod_{i=1}^n m^i_{k_i,\pi(i)} a_{k_i} = (\prod_{i=1}^n m^i_{k_i,\pi(i)}) a_1 a_2 \cdots a_n$. That's obviously the only way how to obtain an element which contains $a_1a_2\cdots a_n$. We can see that each combination $(k_1,\dots,k_n)$ corresponds to a permutation $\rho\in S_n$. It means that every summand in the expansion of (2.14), which contains $a_1a_2\cdots a_n$, has to be in the form $(\prod_{i=1}^n m^i_{\rho(i),\pi(i)})a_1a_2\cdots a_n$ for some permutation $\rho\in S_n$. This fact implies

$$\lambda_{1,\dots,n}=\sum_{\pi,\rho\in S_n}\prod_{i=1}^n m^i_{\rho(i),\pi(i)}.$$

We use the same method for $\mathbf{\Omega}(c)$. Since M_i^T (instead of M_i) is used in each row to define the matrix $\mathbf{\Omega}(c)$ we may simply substitute $m_{i,j}$ by $m_{j,i}$. We get

$$\det\mathbf{\Omega}(c)=\sum_{\pi\in S_n}\prod_{i=1}^n\sum_{k=1}^n(m^i_{\pi(i),k}c_k+\delta_{i,\pi(i)})$$

and

$$\omega_{1,\dots,n}=\sum_{\pi,\rho\in S_n}\prod_{i=1}^n m^i_{\pi(i),\rho(i)}.$$

Therefore, $\lambda_{1,\dots,n}=\omega_{1,\dots,n}$. □

In the paper from D. Gligoroski et al. [8], there are presented sufficient conditions for two matrices and two vectors of linear polynomials to represent a quadratic quasigroup. In Theorem 2.50, we provide both sufficient, and necessary conditions for a bilinear map to represent a quadratic loop. Furthermore, we showed that some of them are neither always satisfied or dependent. The conditions are in the form of a system of equations which verification is very fast.

2.6 Isotopes of Linear and Quadratic Loops

Corollary 1.12 implies that every quasigroup is isotopic to a loop. We shall try and find linear and quadratic quasigroups which are isotopic to a linear or a quadratic loop. It follows from Lemma 2.47 that we need to deal only with quasigroups isotopic to a linear or quadratic loop with the unit o.

Let $(\mathbb{F}_2^n,*)$ be a linear or a quadratic quasigroup. Suppose $(\mathbb{F}_2^n,*)$ is canonically decomposed as $(\alpha,\gamma,\beta)_c$. Then, the translations R_o, and L_o satisfy

$$\begin{aligned}R_o(u)&=\alpha(u)+c,\text{ and}\\ L_o(v)&=\beta(v)+c,\end{aligned}$$

whenever $u,v\in\mathbb{F}_2^n$. It means that the degree of map R_o is the same as the degree of α, and the degree of map L_o is the same as the degree of β. Let

$\big(\mathbb{F}_2^n[R_o^{-1}, L_o^{-1}], \circ\big)$ be a principal isotope of $(\mathbb{F}_2^n, *)$. Then, for every $u, v \in \mathbb{F}_2^n$, we have

$$u \circ v = u + \gamma\big(R_o^{-1}(u), L_o^{-1}(v)\big) + v + c.$$

Therefore, the principal isotope is linear or quadratic if γ is trivial, or α and β are linear. If α (or β) is quadratic, then the degree of R_o^{-1} (or L_o^{-1}) is greater than or equal to 2. Furthermore, if γ is nontrivial then the degree of $\gamma\big(R_o^{-1}(u), L_o^{-1}(v)\big)$ is greater than 2 in most cases.

We discuss the case where α and β are linear or γ is trivial in the following two theorems.

Theorem 2.54. *Let $(\mathbb{F}_2^n, *)$ be a linear or a quadratic quasigroup of the type $(i, 0, j)$, where $i, j \in \{0, 1\}$. Suppose $(\mathbb{F}_2^n, *)$ is canonically decomposed as $(\alpha, o, \beta)_c$. Then $(\alpha, \beta, \mathrm{Id} + c)$ is an isotopy between the group $(\mathbb{F}_2^n, +)$ and $(\mathbb{F}_2^n, *)$.*

Proof. It follows directly from the definition of the isotopy. □

Theorem 2.55. *Let $(\mathbb{F}_2^n, *)$ be a quadratic quasigroup of the type $(0, 1, 0)$. Then there exists a quadratic loop with the unit o which is linearly isotopic to $(\mathbb{F}_2^n, *)$.*

Proof. Suppose $(\mathbb{F}_2^n, *)$ is canonically decomposed as $(\alpha, \gamma, \beta)_c$, i.e.,

$$u * v = \alpha(u) + \gamma(u, v) + \beta(v) + c,$$

where α and β are linear. We can now define linear permutations $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3 : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ as

$$\begin{aligned} \mathcal{L}_1 &: x \mapsto \alpha^{-1}(x), \\ \mathcal{L}_2 &: y \mapsto \beta^{-1}(y), \text{ and} \\ \mathcal{L}_3 &: z \mapsto z + c. \end{aligned}$$

Let $(\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3)$ be an isotopy between $(\mathbb{F}_2^n, *)$ and the quasigroup $(\mathbb{F}_2^n, \circ)$. Then, for every $u, v \in \mathbb{F}_2^n$, we have

$$\begin{aligned} u \circ v = \mathcal{L}_3^{-1}\big(\mathcal{L}_1(u) * \mathcal{L}_2(v)\big) &= \\ = \Big(\alpha\big(\alpha^{-1}(u)\big) + \gamma\big(\mathcal{L}_1(u), \mathcal{L}_2(v)\big) + \beta\big(\beta^{-1}(v)\big) + c\Big) - c &= \\ = u + \gamma\big(\mathcal{L}_1(u), \mathcal{L}_2(v)\big) + v&. \end{aligned}$$

We can easily verify that $\gamma\big(\mathcal{L}_1(u), \mathcal{L}_2(v)\big)$ is a bilinear map. Note that $\mathcal{L}_1(o) = \mathcal{L}_2(o) = o$, and thus for every $u \in \mathbb{F}_2^n$ is

$$\begin{aligned} u \circ o &= u + \gamma\big(\mathcal{L}_1(u), o\big) + o = u, \text{ and} \\ o \circ u &= o + \gamma\big(o, \mathcal{L}_2(u)\big) + u = u, \end{aligned}$$

consequently, $(\mathbb{F}_2^n, \circ)$ is a quadratic loop with the unit o. □

Now, we can express all quasigroups of types $(0,0,0)$, $(0,0,1)$, $(1,0,0)$, $(1,0,1)$, $(0,1,0)$ as an isotopy of a linear or quadratic loop with the unit o.

Let $(\mathbb{F}_2^n, *)$ be a linear or quadratic loop with the unit o, and let $\mathcal{B}_1, \mathcal{B}_2$, and $\mathcal{B}_3$ be linear or quadratic permutations of $\mathbb{F}_2^n$. Suppose that $(\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3^{-1})$ is an isotopy between $(\mathbb{F}_2^n, *)$ and the quasigroup $(\mathbb{F}_2^n, \circ)$. We shall try to derive conditions for $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$, so that $(\mathbb{F}_2^n, \circ)$ is a linear or quadratic quasigroup. Linearly isotopic linear or quadratic quasigroups are of the same degree and of the same type, therefore, we can use an isotopy in the form $(\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3^{-1})$, where $\mathcal{B}_i(o) = o$, and $\mathcal{B}_i$ is either quadratic, or $\mathcal{B}_i = \mathrm{Id}, i = 1,2,3$.

Lemma 2.56. *Let $\mathcal{B}_1$, and $\mathcal{B}_2$ be linear or quadratic permutations of $\mathbb{F}_2^n$ such that $\mathcal{B}_1(o) = \mathcal{B}_2(o) = o$. Suppose that $\operatorname{Img}\widetilde{\mathcal{B}_2} \subseteq \operatorname{Rad}\mathcal{B}_1$. Then the permutation $\mathcal{B}_1\mathcal{B}_2$ is linear if $\mathcal{B}_1\widetilde{\mathcal{B}_2}(u,v) = \widetilde{\mathcal{B}_1}\big(\mathcal{B}_2(u), \mathcal{B}_2(v)\big)$, for every $u, v \in \mathbb{F}_2^n$. Otherwise, $\mathcal{B}_1\mathcal{B}_2$ is a quadratic permutation.*

Proof. By Lemma 2.28, the map $\mathcal{B}_1\mathcal{B}_2$ is quadratic if the map $\widetilde{\mathcal{B}_1\mathcal{B}_2}$, defined as $\widetilde{\mathcal{B}_1\mathcal{B}_2}(u,v) = \mathcal{B}_1\mathcal{B}_2(u) + \mathcal{B}_1\mathcal{B}_2(v) + \mathcal{B}_1\mathcal{B}_2(u+v)$, is bilinear ($\mathcal{B}_1\mathcal{B}_2$ is linear if $\widetilde{\mathcal{B}_1\mathcal{B}_2}$ is trivial). We have, for every $u, v \in \mathbb{F}_2^n$,

$$\begin{aligned}
\mathcal{B}_1\mathcal{B}_2(u+v) &= \mathcal{B}_1\big(\mathcal{B}_2(u) + \widetilde{\mathcal{B}_2}(u,v) + \mathcal{B}_2(u)\big) \\
&= \mathcal{B}_1\mathcal{B}_2(u) + \mathcal{B}_1\widetilde{\mathcal{B}_2}(u,v) + \mathcal{B}_1\mathcal{B}_2(v) + \widetilde{\mathcal{B}_1}\big(\mathcal{B}_2(u), \mathcal{B}_2(v)\big) \\
&\quad + \underbrace{\widetilde{\mathcal{B}_1}\big(\mathcal{B}_2(u) + \mathcal{B}_2(v), \widetilde{\mathcal{B}_2}(u,v)\big)}_{=o},
\end{aligned}$$

thus, $\widetilde{\mathcal{B}_1\mathcal{B}_2} = \mathcal{B}_1\widetilde{\mathcal{B}_2}(u,v) + \widetilde{\mathcal{B}_1}\big(\mathcal{B}_2(u), \mathcal{B}_2(v)\big)$. $\mathcal{B}_1\widetilde{\mathcal{B}_2}(u,v) = \widetilde{\mathcal{B}_1}\big(\mathcal{B}_2(u), \mathcal{B}_2(v)\big)$ implies $\widetilde{\mathcal{B}_1\mathcal{B}_2} = o$, therefore, $\mathcal{B}_1\mathcal{B}_2$ is linear. Otherwise, we will show that $\widetilde{\mathcal{B}_1\mathcal{B}_2}$ is a bilinear map. Let $u, v, w \in \mathbb{F}_2^n$. Then

$$\begin{aligned}
\widetilde{\mathcal{B}_1\mathcal{B}_2}(u+w, v) &= \mathcal{B}_1\widetilde{\mathcal{B}_2}(u+w, v) + \widetilde{\mathcal{B}_1}\big(\mathcal{B}_2(u+w), \mathcal{B}_2(v)\big) \\
&= \mathcal{B}_1\big(\widetilde{\mathcal{B}_2}(u,v) + \widetilde{\mathcal{B}_2}(w,v)\big) \\
&\quad + \widetilde{\mathcal{B}_1}\big(\mathcal{B}_2(u) + \widetilde{\mathcal{B}_2}(u,w) + \mathcal{B}_2(w), \mathcal{B}_2(v)\big) \\
&= \mathcal{B}_1\big(\widetilde{\mathcal{B}_2}(u,v)\big) + \mathcal{B}_1\big(\widetilde{\mathcal{B}_2}(w,v)\big) + \underbrace{\widetilde{\mathcal{B}_1}\big(\widetilde{\mathcal{B}_2}(u,v), \widetilde{\mathcal{B}_2}(w,v)\big)}_{=o} \\
&\quad + \widetilde{\mathcal{B}_1}\big(\mathcal{B}_2(u), \mathcal{B}_2(v)\big) + \widetilde{\mathcal{B}_1}\big(\mathcal{B}_2(w), \mathcal{B}_2(v)\big) \\
&\quad + \underbrace{\widetilde{\mathcal{B}_1}\big(\widetilde{\mathcal{B}_2}(u,w), \mathcal{B}_2(v)\big)}_{=o} = \widetilde{\mathcal{B}_1\mathcal{B}_2}(u,v) + \widetilde{\mathcal{B}_1\mathcal{B}_2}(w,v),
\end{aligned}$$

and symmetrically $\widetilde{\mathcal{B}_1\mathcal{B}_2}(u, v+w) = \widetilde{\mathcal{B}_1\mathcal{B}_2}(u,v) + \widetilde{\mathcal{B}_1\mathcal{B}_2}(u,w)$. Thus, $\mathcal{B}_1\mathcal{B}_2$ is a quadratic permutation. □

Theorem 2.57. *Let each of $\mathcal{B}_1, \mathcal{B}_2$, and $\mathcal{B}_3$ be either a quadratic permutation of $\mathbb{F}_2^n$ such that $\mathcal{B}_i(o) = o$, or an identity on $\mathbb{F}_2^n$. Let $(\mathbb{F}_2^n, *)$ be a linear or a quadratic loop with the unit o, and the bilinear component γ. Suppose that $(\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3^{-1})$ is an isotopy between $(\mathbb{F}_2^n, *)$ and quasigroup $(\mathbb{F}_2^n, \circ)$. Then, $(\mathbb{F}_2^n, \circ)$ is a quadratic quasigroup if the following conditions are fulfilled*

(i) $\operatorname{Img}\gamma \subseteq \operatorname{Rad}\mathcal{B}_3$,

(ii) $\operatorname{Img}\widetilde{\mathcal{B}_1} \subseteq \operatorname{Rad}_L\gamma \cap \operatorname{Rad}\mathcal{B}_3$,

(iii) $\operatorname{Img}\widetilde{\mathcal{B}_2} \subseteq \operatorname{Rad}_R\gamma \cap \operatorname{Rad}\mathcal{B}_3$.

Furthermore, let (i, j, k) be the type of $(\mathbb{F}_2^n, \circ)$. Then,

(i) *$i = 1$ if and only if $\mathcal{B}_3\mathcal{B}_1$ is quadratic,*

(ii) *$k = 1$ if and only if $\mathcal{B}_3\mathcal{B}_2$ is quadratic,*

(iii) *$j = 1$ if and only if $\mathcal{B}_3\gamma \neq \widetilde{\mathcal{B}_3}$.*

Proof. Using the fact that $\operatorname{Img}\gamma \subseteq \operatorname{Rad}\mathcal{B}_3$, we have for every $u, v \in \mathbb{F}_2^n$,

$$\begin{aligned} u \circ v &= \mathcal{B}_3\big(\mathcal{B}_1(u) * \mathcal{B}_2(v)\big) \\ &= \mathcal{B}_3\Big(\mathcal{B}_1(u) + \gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(v)\big) + \mathcal{B}_2(v)\Big) \\ &= \underbrace{\mathcal{B}_3\mathcal{B}_1(u)}_{=\alpha(u)} + \underbrace{\mathcal{B}_3\gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(v)\big)}_{=\gamma_1'(u,v)} + \underbrace{\widetilde{\mathcal{B}_3}\big(\mathcal{B}_1(u), \mathcal{B}_2(v)\big)}_{=\gamma_2'(u,v)} + \underbrace{\mathcal{B}_3\mathcal{B}_2(v)}_{=\beta(v)} \\ &\quad + \underbrace{\widetilde{\mathcal{B}_3}\Big(\mathcal{B}_1(u), \gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(v)\big)\Big)}_{=o} + \underbrace{\widetilde{\mathcal{B}_3}\Big(\gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(v)\big), \mathcal{B}_2(v)\Big)}_{=o}. \end{aligned}$$

Lemma 2.56 implies that α and β are linear or quadratic permutations of $\mathbb{F}_2^n$ (we used the second and the third condition). Now, we will show that γ_1' and γ_2' are bilinear maps. We have, for every $u, v, w \in \mathbb{F}_2^n$,

$$\begin{aligned} \gamma_1'(u, v + w) &= \mathcal{B}_3\gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(v + w)\big) \\ &= \mathcal{B}_3\gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(v) + \widetilde{\mathcal{B}_2}(v, w) + \mathcal{B}_2(w)\big) \\ &= \mathcal{B}_3\Big(\gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(v)\big) + \gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(w)\big) + \underbrace{\gamma\big(\mathcal{B}_1(u), \widetilde{\mathcal{B}_2}(v, w)\big)}_{=o}\Big) \\ &= \mathcal{B}_3\gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(v)\big) + \mathcal{B}_3\gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(w)\big) \\ &\quad + \underbrace{\widetilde{\mathcal{B}_3}\Big(\gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(v)\big), \gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(w)\big)\Big)}_{=o} = \gamma_1'(u, v) + \gamma_1'(u, w), \end{aligned}$$

and

$$\begin{aligned}
\gamma_1'(u+w,v) &= \mathcal{B}_3\gamma\big(\mathcal{B}_1(u+w),\mathcal{B}_2(v)\big)\\
&= \mathcal{B}_3\gamma\big(\mathcal{B}_1(u)+\widetilde{\mathcal{B}_1}(u,w)+\mathcal{B}_1(w),\mathcal{B}_2(v)\big)\\
&= \mathcal{B}_3\Big(\gamma\big(\mathcal{B}_1(u),\mathcal{B}_2(v)\big)+\gamma\big(\mathcal{B}_1(w),\mathcal{B}_2(v)\big)+\underbrace{\gamma\big(\widetilde{\mathcal{B}_1}(u,w),\mathcal{B}_2(v)\big)}_{=o}\Big)\\
&= \mathcal{B}_3\gamma\big(\mathcal{B}_1(u),\mathcal{B}_2(v)\big)+\mathcal{B}_3\gamma\big(\mathcal{B}_1(w),\mathcal{B}_2(v)\big)\\
&\quad+\underbrace{\widetilde{\mathcal{B}_3}\Big(\gamma\big(\mathcal{B}_1(u),\mathcal{B}_2(v)\big),\gamma\big(\mathcal{B}_1(w),\mathcal{B}_2(v)\big)\Big)}_{=o}=\gamma_1'(u,v)+\gamma_1'(w,v),
\end{aligned}$$

thus, γ_1' is a bilinear map. Next, for every $u,v,w\in\mathbb{F}_2^n$, γ_2' fulfils

$$\begin{aligned}
\gamma_2'(u+w,v) &= \widetilde{\mathcal{B}_3}\big(\mathcal{B}_1(u+w),\mathcal{B}_2(v)\big)\\
&= \widetilde{\mathcal{B}_3}\big(\mathcal{B}_1(u)+\widetilde{\mathcal{B}_1}(u,w)+\mathcal{B}_1(w),\mathcal{B}_2(v)\big)\\
&= \widetilde{\mathcal{B}_3}\big(\mathcal{B}_1(u),\mathcal{B}_2(v)\big)+\widetilde{\mathcal{B}_3}\big(\mathcal{B}_1(w),\mathcal{B}_2(v)\big)+\underbrace{\widetilde{\mathcal{B}_3}\big(\widetilde{\mathcal{B}_1}(u,w),\mathcal{B}_2(v)\big)}_{=o}\\
&= \gamma_2'(u,v)+\gamma_2'(w,v),
\end{aligned}$$

and symmetrically $\gamma_2'(u,v+w)=\gamma_2'(u,v)+\gamma_2'(v,w)$. Thus, γ_2' is a bilinear map. It is clear that the map $\gamma'=\gamma_1'+\gamma_2'$ is bilinear, too. Therefore, the quasigroup $(\mathbb{F}_2^n,\circ)$ canonically decomposes as $(\alpha,\gamma',\beta)_o$. The rest is clear. □

Corollary 2.58. *Let $\mathcal{B}$ be a quadratic permutation of $\mathbb{F}_2^n$ such that $\mathcal{B}(o)=o$. Let $(\mathbb{F}_2^n,+)$ be a group. Suppose that $(\mathrm{Id},\mathrm{Id},\mathcal{B}^{-1})$ is an isotopy between $(\mathbb{F}_2^n,+)$ and the quasigroup $(\mathbb{F}_2^n,\circ)$. Then $(\mathbb{F}_2^n,\circ)$ is a quadratic quasigroup of type $(1,1,1)$.*

The condition presented in Theorem 2.57 are sufficient but not necessary. In the following theorem we show that if we consider an isotopy $(\mathcal{B}_1,\mathcal{B}_2,\mathrm{Id})$, the conditions are both necessary, and sufficient.

Theorem 2.59. *Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be quadratic permutations of $\mathbb{F}_2^n$ such that $\mathcal{B}_1(o)=\mathcal{B}_2(o)=o$. Let $(\mathbb{F}_2^n,*)$ be a quadratic loop with the unit o, and the bilinear component γ. Suppose that $(\mathcal{B}_1,\mathcal{B}_2,\mathrm{Id})$ is an isotopy between $(\mathbb{F}_2^n,*)$ and the quasigroup $(\mathbb{F}_2^n,\circ)$. Then, $(\mathbb{F}_2^n,\circ)$ is a quadratic quasigroup if and only if $\operatorname{Img}\widetilde{\mathcal{B}_1}\subseteq\operatorname{Rad}_L\gamma$ and $\operatorname{Img}\widetilde{\mathcal{B}_2}\subseteq\operatorname{Rad}_R\gamma$. The type of the quasigroup is $(1,1,1)$.*

Proof. The backward implication, as well as the type of $(\mathbb{F}_2^n,\circ)$ follows directly from Theorem 2.57 (recall that $\operatorname{Rad}\mathrm{Id}=\mathbb{F}_2^n$).

Now, consider that there exist $u_1,u_2\in\mathbb{F}_2^n$ such that $\widetilde{\mathcal{B}_1}(u_1,u_2)\notin\operatorname{Rad}_L\gamma$, i.e., there exits nonzero $u_3\in\mathbb{F}_2^n$ such that $\gamma\big(\widetilde{\mathcal{B}_1}(u_1,u_2),u_3\big)\neq o$. Suppose that

$(\mathbb{F}_2^n, \circ)$ is a quadratic quasigroup. Then, it follows form Corollary 2.42 that the map

$$\zeta : (u, v) \mapsto u \circ v + o \circ v + o \circ v + o \circ o$$

is bilinear. We can see that $\zeta(u, v) = \gamma\big(\mathcal{B}_1(u), \mathcal{B}_2(v)\big)$, where $u, v \in \mathbb{F}_2^n$. We have,

$$\begin{aligned}\zeta(u_1 + u_2, u_3) &= \gamma\big(\mathcal{B}_1(u_1 + u_2), \mathcal{B}_2(u_3)\big)\\ &= \gamma\big(\mathcal{B}_1(u_1), \mathcal{B}_2(u_3)\big) + \gamma\big(\mathcal{B}_1(u_2), \mathcal{B}_2(u_3)\big) + \gamma \underbrace{\big(\widetilde{\mathcal{B}_1}(u_1, u_2), \mathcal{B}_2(u_3)\big)}_{\neq o}\\ &\neq \zeta(u_1, u_3) + \zeta(u_2, u_3),\end{aligned}$$

therefore, ζ is not bilinear. The existence of $u_1, u_2 \in \mathbb{F}_2^n$ such that $\widetilde{\mathcal{B}_2}(u_1, u_2) \notin \operatorname{Rad}_R \gamma$, results in the same result. Thus, the degree of $(\mathbb{F}_2^n, \circ)$ is greater than 2. □

We summarize the results of this section in Table 2.2. In each row we present the type of the class of linearly isotopic quadratic quasigroups which can be obtained from a loop using an isotopy if we fulfil the conditions. $\mathcal{B}$ and $\mathcal{B}_i$ denote a quadratic permutation. γ denotes the bilinear component of a quadratic loop (with the unit o). If all quasigroups (or all classes of quasigroups) can be yielded in this way, we note it in the last column. We also do not include cases that can be yielded by a simpler construction or which have too complex conditions.

These results provide a way how to generate the quadratic quasigroup of desired type using quadratic permutations from a known quadratic loop.

	Isotopy	Loop	Conditions	Type	Note
1.	$(\mathrm{Id}, \mathrm{Id}, \mathrm{Id})$	$\gamma = 0$		$(0, 0, 0)$	All quasigroups
2.	$(\mathrm{Id}, \mathrm{Id}, \mathrm{Id})$	$\gamma \neq 0$		$(0, 1, 0)$	All quasigroups
3.	$(\mathcal{B}, \mathrm{Id}, \mathrm{Id})$	$\gamma = 0$		$(1, 0, 0)$	All quasigroups
4.	$(\mathrm{Id}, \mathcal{B}, \mathrm{Id})$	$\gamma = 0$		$(0, 0, 1)$	All quasigroups
5.	$(\mathcal{B}_1, \mathcal{B}_2, \mathrm{Id})$	$\gamma = 0$		$(1, 0, 1)$	All quasigroups
6.	$(\mathrm{Id}, \mathrm{Id}, \mathcal{B}^{-1})$	$\gamma = 0$		$(1, 1, 1)$	
7.	$(\mathrm{Id}, \mathrm{Id}, \mathcal{B}^{-1})$	$\gamma \neq 0$	$\operatorname{Img} \gamma \subseteq \operatorname{Rad} \mathcal{B}$, $\mathcal{B}\gamma \neq \widetilde{\mathcal{B}}$	$(1, 1, 1)$	
8.	$(\mathcal{B}, \mathrm{Id}, \mathrm{Id})$	$\gamma \neq 0$	$\operatorname{Img} \widetilde{\mathcal{B}} \subseteq \operatorname{Rad}_L \gamma$	$(1, 1, 0)$	Necessary cond.
9.	$(\mathrm{Id}, \mathcal{B}, \mathrm{Id})$	$\gamma \neq 0$	$\operatorname{Img} \widetilde{\mathcal{B}} \subseteq \operatorname{Rad}_R \gamma$	$(0, 1, 1)$	Necessary cond.
10.	$(\mathcal{B}_1, \mathcal{B}_2, \mathrm{Id})$	$\gamma \neq 0$	$\operatorname{Img} \widetilde{\mathcal{B}_1} \subseteq \operatorname{Rad}_L \gamma$, $\operatorname{Img} \widetilde{\mathcal{B}_2} \subseteq \operatorname{Rad}_R \gamma$	$(1, 1, 1)$	Necessary cond.

Table 2.2: The isotopes of linear or quadratic loops

Chapter 3

Construction of Quadratic Permutations

In the previous chapter we have shown that it is possible to generate quadratic quasigroups from linear or quadratic loops using isotopies composed from linear or quadratic permutations. Linear permutations can be easily constructed from a regular matrix and a vector, by Lemma 2.22. We will introduce two different ways how to construct quadratic permutations.

3.1 Nondeterministic

Let α be a quadratic permutation of $\mathbb{F}_2^n$, and let E be a base of $\mathbb{F}_2^n$. Then, by Lemma 2.24, α can be represented as $(\mathbf{q}_1, \ldots, \mathbf{q}_n) + c$ in the base E where $\mathbf{q}_1, \ldots, \mathbf{q}_n$ are quadratic forms and $c \in \mathbb{F}_2^n$. We shall try and derive conditions for arbitrary quadratic form, so that it can be used as a part of representation of a quadratic permutation. We will use the theory from [2].

Definition 3.1. Let V be a vector space over the field $\mathbb{F}_2$. Suppose $\mathbf{q}$ is a quadratic form and $\mathbf{b}$ is its associated bilinear form.

The set

$$\operatorname{Ker} \mathbf{q} = \{u \in V; \mathbf{q}(u) = 0 \wedge \mathbf{b}(u, w) = \mathbf{b}(w, u) = 0, \forall w \in \mathbb{F}_2^n\}$$

is called a *kernel* of the quadratic form $\mathbf{q}$. We can observe that $\operatorname{Ker} \mathbf{q}$ is a subspace of $\mathbb{F}_2^n$.

A quadratic form $\mathbf{q}$ is said to be *regular* if $\operatorname{Ker} \mathbf{q}$ is the zero subspace. It follows directly from the definition that the quadratic form $\mathbf{q}$ is regular if the associated bilinear form $\mathbf{b}$ is non-degenerate.

Two elements $u, w \in V$ are called *orthogonal* if $\mathbf{b}(u, w) = 0$. Two subspaces $U, W \leq V$ are called *orthogonal* if $\mathbf{b}(u, w) = 0$ for all $u \in U$ and all $w \in W$.

The subspace U is said to be *anisotropic* if $\mathbf{q}(u) = 1$ for all $u \in U$, $u \neq o$.

We call the subspace U a *hyperbolic plane* if $U = \langle e, f \rangle$ where $\mathbf{q}(e) = \mathbf{q}(f) = 0$ and $\mathbf{b}(e, f) = 1$.

Two quadratic forms $\mathbf{q}_1$ on V_1 and $\mathbf{q}_2$ on V_2 are *equivalent* if there exists an invertible linear map $\mathcal{L} : V \to V'$ such that $\mathbf{q}_2\big(\mathcal{L}(u)\big) = \mathbf{q}_1(u)$ for all $u \in V$.

Theorem 3.2. *Let* $\mathbf{q}$ *be a regular quadratic form on* V *(over* $\mathbb{F}_2$*).*

(i) *An anisotropic space has dimension at most 2.*

(ii) *There exists an anisotropic space* W *and hyperbolic planes* $U_1, \ldots, U_r$ *such that*

$$V = W \oplus U_1 \oplus \cdots \oplus U_r$$

and the summands are pairwise orthogonal.

(iii) *Let* $\mathbf{q}'$ *be a regular quadratic form on* V' *(over* $\mathbb{F}_2$*) and let*

$$V' = W' \oplus U_1' \oplus \cdots \oplus U_s'$$

be a decomposition as in (ii) *according to* $\mathbf{q}'$*. Then* $\mathbf{q}$ *and* $\mathbf{q}'$ *are equivalent if and only if* $r = s$ *and* $\dim W = \dim W'$*.*

Proof. The proof can be found in [2]. □

The previous theorem yields that all quadratic forms over $\mathbb{F}_2$ are determined up to equivalence by two invariants, the number r of hyperbolic planes, and the dimension of the anisotropic part.

Definition 3.3. Let $\mathbf{q}$ be a quadratic form on the vector space V (over $\mathbb{F}_2$). Suppose that

$$V = W \oplus U_1 \oplus \cdots \oplus U_r$$

as in Theorem 3.2. The number r of hyperbolic planes is called *Witt index.* We say that the form is of *type* $+1, 0$, or -1 according to $\dim W = 0, 1$, or 2, respectively.

Definition 3.4. Let $\mathbf{q}$ be a quadratic form on the vector space V over $\mathbb{F}_2$. We set

$$\operatorname{Null} \mathbf{q} = \{u \in V; \mathbf{q}(u) = 0\}.$$

Lemma 3.5. *For* $\varepsilon = \pm 1$*, let* $\mathbf{q}$ *be a regular quadratic form of type* ε *on a vector space* V *of even dimension* $2k$ *over* $\mathbb{F}_2$*. Then* $|\operatorname{Null} \mathbf{q}| = 2^{k-1}(2^k + \varepsilon)$*.*

Proof. The proof can be found in [2]. □

Lemma 3.6. *Let* $\mathbf{q}$ *be a regular quadratic form on the vector space* V *of odd dimension* $2k+1$ *over* $\mathbb{F}_2$*. Then* $|\operatorname{Null}\mathbf{q}| = 2^{2k}$.

Proof. Consider a decomposition of V, by Theorem 3.2, as follows

$$V = W \oplus U_1 \oplus \cdots \oplus U_r.$$

$\dim V = 2k+1$ implies $\dim W = 1$, and $r = k$. We set $U = U_1 \oplus \cdots \oplus U_k$. Then $\dim U = 2k$. Put $s = |\{u \in U; \mathbf{q}(u) = 0\}|$. Every $v \in V$ can be uniquely expressed as $v = w + u$, where $w \in W$ and $u \in U$. Then $\mathbf{q}(w+u) = \mathbf{q}(w) + \mathbf{q}(u) + \mathbf{b}(w,u) = \mathbf{q}(w) + \mathbf{q}(u)$, therefore, $\mathbf{q}(w+u) = 0$ if and only if $\mathbf{q}(w) = \mathbf{q}(u)$. We obtain

$$|\operatorname{Null}\mathbf{q}| = s + \big(|U| - s\big) = |U| = 2^{2k}.$$

□

We generalize the Lemma 3.5 for all quadratic forms.

Theorem 3.7. *Let* $\mathbf{q}$ *be a nontrivial quadratic form on the vector space* V *of dimension* n *over* $\mathbb{F}_2$*. Put* $d = \dim\operatorname{Ker}\mathbf{q}$*. Then* $|\operatorname{Null}\mathbf{q}| = 2^{n-1}$ *if and only if* $n-d$ *is odd.*

Proof. Let V' be a subspace of V such that $V = \operatorname{Ker}\mathbf{q} \oplus V'$. Put $s = |\{v' \in V'; \mathbf{q}(v') = 0\}|$. Every $v \in V$ can be uniquely expressed as $v = v' + u$, where $v' \in V'$ and $u \in \operatorname{Ker}\mathbf{q}$. Then $\mathbf{q}(v'+u) = \mathbf{q}(v') + \mathbf{q}(u) + \mathbf{b}(v',u) = \mathbf{q}(v')$, therefore, $\mathbf{q}(v'+u) = 0$ if and only if $\mathbf{q}(v') = 0$. We obtain

$$|\operatorname{Null}\mathbf{q}| = 2^d s.$$

The restriction of $\mathbf{q}$ to V', denoted by $\mathbf{q}|_{V'}$, is regular and we can use Lemmas 3.5 and 3.6.

Consider $n-d = 2k$. Then $\big|\operatorname{Null}\mathbf{q}|_{V'}\big| = 2^{k-1}(2^k + \varepsilon)$, where ε is the type of $\mathbf{q}|_{V'}$ which satisfy $\varepsilon \neq 0$. Then

$$|\operatorname{Null}\mathbf{q}| = 2^d 2^{k-1}(2^k + \varepsilon) = 2^{d+2k-1} + \varepsilon 2^{d+k+1} = 2^{n-1} + \varepsilon 2^{d+k+1} \neq 2^{n-1}.$$

Now, consider $n-d = 2k+1$. Then $\big|\operatorname{Null}\mathbf{q}|_{V'}\big| = 2^{2k}$ and

$$|\operatorname{Null}\mathbf{q}| = 2^d 2^{2k} = 2^{d+2k} = 2^{n-1}.$$

□

Theorem 3.8. *Let* $\mathbf{q}$ *and* $\mathbf{q}'$ *be quadratic forms on the vector space* V *of dimension* n *over* $\mathbb{F}_2$*. Suppose the numbers* $(n - \dim\operatorname{Ker}\mathbf{q})$ *and* $(n - \dim\operatorname{Ker}\mathbf{q}')$ *are odd. Then* $\mathbf{q}$ *and* $\mathbf{q}'$ *are equivalent if and only if* $\dim\operatorname{Ker}\mathbf{q} = \dim\operatorname{Ker}\mathbf{q}'$.

Proof. The left-to-right implication is clear.

Now, consider $\dim \operatorname{Ker} \mathbf{q} = \dim \operatorname{Ker} \mathbf{q}'$. Suppose the subspaces $U, U' \leq V$ such that $V = \operatorname{Ker} \mathbf{q} \oplus U$ and $V = \operatorname{Ker} \mathbf{q}' \oplus U'$. Then $\dim U = \dim U'$ is odd. Thus, by Theorem 3.2, there exists an invertible linear map $\mathcal{L}_1 : U \to U'$ such that $\mathbf{q}'\big(\mathcal{L}_1(u)\big) = \mathbf{q}(u)$ for all $u \in U$. Let $\mathcal{L}_2$ be a arbitrary invertible linear map $\mathcal{L}_2 : \operatorname{Ker} \mathbf{q} \to \operatorname{Ker} \mathbf{q}'$ (i.e., an isomorphism between $\operatorname{Ker} \mathbf{q}$ and $\operatorname{Ker} \mathbf{q}'$). Since every $v \in V$ can be uniquely decomposed as $v = w + u = w' + u'$, where $w \in \operatorname{Ker} \mathbf{q}$, $w' \in \operatorname{Ker} \mathbf{q}'$, $u \in U$, and $u' \in U'$, hence the map $\mathcal{L} : V \to V$, defined as $\mathcal{L}(w + u) = \mathcal{L}_2(w) + \mathcal{L}_1(u)$, is linear and invertible and $\mathbf{q}'\big(\mathcal{L}(v)\big) = \mathbf{q}(v)$ for all $v \in V$. □

Proposition 3.9. *Let $\mathbf{q}_1, \ldots, \mathbf{q}_n$ be quadratic forms on $\mathbb{F}_2^n$. Then $(\mathbf{q}_1, \ldots, \mathbf{q}_n)$ represents a quadratic permutation if and only if for every subset $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ is*

$$\left|\Big\{v \in \mathbb{F}_2^n;\, \big(\mathbf{q}_{i_1}(v), \ldots, \mathbf{q}_{i_k}(v)\big) = u\Big\}\right| = 2^{n-k}, \text{ for every } u \in \mathbb{F}_2^k.$$

Proof. The right-to-left implication follows from choosing the set $\{1, \ldots, n\}$.

Suppose that $(\mathbf{q}_1, \ldots, \mathbf{q}_n)$ represents a quadratic permutation of $\mathbb{F}_2^n$. Let $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ and let $(u_1, \ldots, u_k) \in \mathbb{F}_2^k$. Then the number of vectors $(v_1, v_2, \ldots, v_n) \in \mathbb{F}_2^n$ such that $v_{i_j} = u_j$, for $j = 1, \ldots, k$, is 2^{n-k}. The second implication follows from the fact that $(\mathbf{q}_1, \ldots, \mathbf{q}_n)$ is surjective. □

Therefore, by the previous lemma, every quadratic form $\mathbf{q}$, as a part of representation of a quadratic permutation of $\mathbb{F}_2^n$, has to satisfy $|\operatorname{Null} \mathbf{q}| = 2^{n-1}$. Theorems 3.7 and 3.8 imply that every such a quadratic form is determined up to equivalence by the odd number $i \in \{1, \ldots, n\}$, $i = n - \dim \operatorname{Ker} \mathbf{q}$.

Thus, we need to find just $\lceil \frac{n}{2} \rceil$ non-equivalent quadratic forms to obtain all suitable quadratic forms for a construction of a quadratic permutation of $\mathbb{F}_2^n$. Now, we can construct a quadratic permutation from these quadratic forms by stepwise verification of the conditions from Proposition 3.9. Unfortunately, this nondeterministic algorithm is effective just for small n.

3.2 Deterministic

There is also a deterministic way how to construct a quadratic permutation. We will introduce the Matsumoto-Imai scheme [13].

Let $p(x) \in \mathbb{F}_2[x]$ be an irreducible polynomial of degree n. Then $\mathbb{F}_2[x]/p(x)$ is a field with invertible operations addition "+" and multiplication "·" between polynomials modulo $p(x)$ [12]. Since every element of $\mathbb{F}_2[x]/p(x)$ have a form

$a_{n-1}x^{n-1} + \cdots a_1x + a_0$, where $a_i \in \mathbb{F}_2, i = 1, \ldots, n$, hence we can define a bijection

$$\begin{aligned} \Phi :&\ \mathbb{F}_2[x]/p(x) \to \mathbb{F}_2^n, \\ \Phi :&\ a_{n-1}x^{n-1} + \cdots a_1x + a_0 \mapsto (a_0, a_1, \ldots, a_{n-1}). \end{aligned}$$

It can be easily observed that $\Phi\big(f(x) + g(x)\big) = \Phi\big(f(x)\big) + \Phi\big(g(x)\big)$ for every $f, g \in \mathbb{F}_2[x]/p(x)$.

Theorem 3.10. *Let $\mathbb{E} = \mathbb{F}_2[x]/p(x)$ be a field, where $p(x)$ is an irreducible polynomial with degree n, and let $\lambda \in \mathbb{N}$ be an integer with $\gcd(2^n - 1, 2^\lambda + 1) = 1$. Let's define a map $F : \mathbb{E} \to \mathbb{E}$ by*

$$F : g \mapsto g^{2^\lambda+1}, \text{ for every } g \in \mathbb{E}.$$

Then the map $\alpha : u \mapsto \Phi\Big(F\big(\Phi^{-1}(u)\big)\Big), u \in \mathbb{F}_2^n$ is a quadratic permutation of $\mathbb{F}_2^n$.

Proof. Since $\gcd(2^n - 1, 2^\lambda + 1) = 1$, hence there exists $k < 2^n - 1$ such that $k(2^\lambda + 1) = 1 \mod 2^n - 1$. Suppose that $g \in \mathbb{E}$. Then $F(g^k) = g^{k(2^\lambda+1)} = g$. Thus, the map F is a permutation of $\mathbb{E}$ and α is a permutation of $\mathbb{F}_2^n$, too.

Suppose that $\sum_{i=0}^{n-1} a_i x^i = g \in \mathbb{E}$. Then

$$\begin{aligned} F(g) = g^{2^\lambda+1} = g^{2^\lambda} g = \left(\sum_{i=0}^{n-1} a_i x^i\right)^{2^\lambda} & \left(\sum_{i=0}^{n-1} a_i x^i\right) \\ &= \left(\sum_{i=0}^{n-1} a_i x^{i2^\lambda}\right)\left(\sum_{i=0}^{n-1} a_i x^i\right). \end{aligned}$$

We have, for every $g, h \in \mathbb{E}$, $\sum_{i=0}^{n-1} a_i x^i = g$, $\sum_{i=0}^{n-1} b_i x^i = h$,

$$\begin{aligned} \widetilde{F}(g,h) &= F(g+h) + F(g) + F(h) \\ &= \left(\sum_{i=0}^{n-1} a_i x^{i2^\lambda}\right)\left(\sum_{i=0}^{n-1} b_i x^i\right) + \left(\sum_{i=0}^{n-1} b_i x^{i2^\lambda}\right)\left(\sum_{i=0}^{n-1} a_i x^i\right). \end{aligned}$$

Furthermore, we have, for $e \in \mathbb{E}$, $\sum_{i=0}^{n-1} c_i x^i = e$,

$$\begin{aligned}
\widetilde{F}(g+e,h) = & \left(\sum_{i=0}^{n-1}(a_i+c_i)x^{i2^\lambda}\right)\left(\sum_{i=0}^{n-1} b_i x^i\right) \\
& + \left(\sum_{i=0}^{n-1} b_i x^{i2^\lambda}\right)\left(\sum_{i=0}^{n-1}(a_i+c_i)x^i\right) \\
= & \left(\sum_{i=0}^{n-1} a_i x^{i2^\lambda}\right)\left(\sum_{i=0}^{n-1} b_i x^i\right) + \left(\sum_{i=0}^{n-1} c_i x^{i2^\lambda}\right)\left(\sum_{i=0}^{n-1} b_i x^i\right) \\
& + \left(\sum_{i=0}^{n-1} b_i x^{i2^\lambda}\right)\left(\sum_{i=0}^{n-1} a_i x^i\right) + \left(\sum_{i=0}^{n-1} b_i x^{i2^\lambda}\right)\left(\sum_{i=0}^{n-1} c_i x^i\right) \\
= & \widetilde{F}(g,h) + \widetilde{F}(e,h),
\end{aligned}$$

and symmetrically $\widetilde{F}(g,h+e) = \widetilde{F}(g,h) + \widetilde{F}(g,e)$. Thus, by Lemma 2.28, α is a quadratic permutation.

□

Bibliography

[1] Bican L., *Lineární algebra a geometrie*, Academia, ISBN **88-200-0843-8**, (2000)

[2] Cameron P.J.: *Finite Geometry and Coding Theory,* Socrates Intensive Programme Finite Geometies and Their Automorphisms, Potenza, Italy (1999)

[3] Diffie W., Hellman M., *New Directions in Cryptography*, IEEE Trans. Information Theory, Vol. IT-**22**,No **6**, (1976), 644–654

[4] Drápal A.: *Teorie grup - základní aspekty,* Karolinum, ISBN **80-246-0162-1** (2000)

[5] Drápal A.: *Komutativní okruhy,* Lecture Notes, Charles University in Prague, Faculty of Mathematics and Physics, (2006)

[6] Drápal A.: *Group Isotopes and a Holomorphic Action,* Charles University in Prague, (2008)

[7] Drápal A.: *Samoopravné kódy,* Lecture Notes, Charles University in Prague, Faculty of Mathematics and Physics, (2009)

[8] Gligoroski D., Markovski S., Knapskog S.J.: *A Public Key Block Cipher Based on Multivariate Quadratic Quasigroups,* arXiv:**0808.0247v1** (2008)

[9] Koblitz N., *Elliptic curve cryptosystems*, Mathematics of Computation **48**, (1987), 203–209

[10] Rivest R. , Shamir A., Adleman L., *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Comm. ACM, Vol. **21**, No. **2**, (1978), 120–126

[11] Smith J.D.H.: *Four Lectures on Quasigroup Representation,* Quasigroup and Related Systems **15** (2007), 109-140

[12] Tůma J.: *Konečná tělesa,* Lecture Notes, Charles University in Prague, Faculty of Mathematics and Physics, (2006)

[13] Wolf C., Preneel B.: *Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations,* K.U.Leuvenm ESAT-COSIC, Belgium, Cryptology ePrint Archive, Report **2005**/**077** (2005)