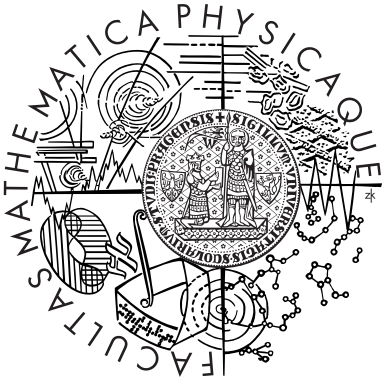
KARLOVA UNIVERZITA V PRAZE
MATEMATICKO-FYZIKÁLNÍ FAKULTA

DIPLOMOVÁ PRÁCE



Andrea Frisová

Kryptografie založená na teorii kvazigrup

KATEDRA ALGEBRY

Vedoucí diplomové práce:
RNDr. David Stanovský, Ph.D.

Studijní program:
Matematika
Matematické metody informační bezpečnosti

2009

Chtěla bych poděkovat prof. Aleši Drápalovi, DSc. a RNDr. Davidovi Stanovskému, Ph.D. za konzultace a rady, kterými mi pomohli tuto práci napsat. Také bych velmi ráda poděkovala Michalovi Johanisovi za korektury textu a trpělivost.

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

V Praze dne 14.4.2009 Andrea Frisová

Název práce: Kryptografie založená na teorii kvazigrup
Autor: Andrea Frisová
Katedra (ústav): Katedra algebry
Vedoucí diplomové práce: RNDr. David Stanovský, Ph.D.
e-mail vedoucího: stanovsk@karlin.mff.cuni.cz

Abstrakt: Předložená práce se zabývá vlastnostmi určité nekonečné matice, jejíž prvky jsou prvky kvazigrupy. Tato matice je vygenerovaná z určeného nekonečného vektoru pomocí levých iterovaných translací. Z předpokladu, že vstupní vektor je periodický, zkoumáme, jaké periody můžou mít jednotlivé řádky matice pro dané typy kvazigrup. Cílem této práce je ukázat, že pro centrální kvazigrupy periody rostou nejvýše lineárně, a snažit se tento fakt aplikovat na proudovou šifru Edon-80.

Klíčová slova: kvazigrupy, periody, proudová šifra, Edon-80

Title: Quasigroup based cryptography
Author: Andrea Frisová
Department: Department of Algebra
Supervisor: RNDr. David Stanovský, Ph.D.
Supervisor's e-mail address: stanovsk@karlin.mff.cuni.cz

Abstract: In this work, we study some properties of an infinite matrix, which consists of quasigroup elements. This matrix is generated from a certain sequence X using left iterated translations. We suppose that the sequence X is periodic and we examine how the periods of the rows of our matrix behave for various types of quasigroups. We show that for central quasigroups the periods increase at most linearly. Further, we try to apply our result to the stream cipher Edon-80.

Keywords: quasigroups, periods, stream cipher, Edon-80

Contents

CHAPTER 1

Introduction

An *alphabet* is a finite set of symbols. A *keystream* is a sequence $(k_i)_{i=1}^{\infty}$, $k_i \in \mathcal{K}$, where $\mathcal{K}$ is a finite set. Let $\mathcal{A}$ be an alphabet and for each $e \in \mathcal{K}$ let E_e and D_e be permutations on $\mathcal{A}$ such that $D_e \circ E_e = \mathrm{id}_{\mathcal{A}}$. Let $(m_i)_{i=1}^{\infty}$ be a string of symbols from $\mathcal{A}$ (plaintext) and $(k_i)_{i=1}^{\infty}$ be a keystream. A *stream cipher* encrypts the plaintext to a ciphertext $(c_i)_{i=1}^{\infty}$ by the formula $c_i = E_{k_i}(m_i)$ for each $i \in \mathbb{N}$, while the formula $m_i = D_{k_i}(c_i)$ is used for decryption. A *binary additive cipher* is a stream cipher such that $\mathcal{A} = \mathcal{K} = \{0, 1\}$ and for each $k \in \mathcal{K}$, $D_k(m) = E_k(m) = k \oplus m$ for each $m \in \mathcal{A}$.

The keystream could be generated at random, or by an algorithm which generates the keystream from an initial value (called a *seed*), or from a seed and previous ciphertext symbols. Such an algorithm is called a *keystream generator*. For every new plaintext the keystream generator uses a new seed. The seed is usually sent along with the ciphertext.

The keystream generator should produce a pseudo-random sequence as long as the plaintext. This means that the keystream should have no periods or at least very large periods (possibly longer than the length of all admissible plaintexts). If this condition is not satisfied, two parts of plaintext will be encrypted by the same keystream, which opens ways to attack the cipher. For example, suppose $c_1c_2 \dots c_t$ and $c'_1c'_2 \dots c'_t$ are two ciphertext strings produced by the same keystream $k_1k_2 \dots k_t$ from plaintexts $m = m_1m_2 \dots m_t$ and $m' = m'_1m'_2 \dots m'_t$, respectively. Then $c_i = m_i \oplus k_i$, $c'_i = m'_i \oplus k_i$ and $c_i \oplus c'_i = m_i \oplus m'_i$. Therefore, if we know m then it easy to find m'. However, most plaintexts contain enough redundancy so that the knowledge of m is not necessary to recover both m and m' from $m \oplus m'$.

Edon-80 is a binary stream cipher. Its description can be found in Chapter 6. The keystream in Edon-80 is generated as a row of a certain matrix whose elements are defined iteratively using quasigroup operations.

The main problem of Edon-80 keystream generator is the question whether there exist weak keys, i.e. keys which induce a short period of keystream. There are some indications that such keys exist, but their existence is based upon heuristic arguments [**H**] and statistical models [**G**] that do not seem to be completely substantiated. However, no weak key seems to have been explicitly described and its existence is thus still hypothetical.

The task to decide the existence of weak keys fully formally seems to be quite complicated. In this thesis, we shall be solving a related problem for which we have developed a formalism that might be useful in the future.

We do not compute the distribution of keystream period lengths, but we compute the lengths of periods of formal expressions that can be regarded as elements of a certain group ring. The keystream periods are then obtained by substituting into these expression variables that reflect the input data (in particular, the key) of the cipher.

Unfortunately, up to now we were able to perform calculations only for some classes of the quasigroups - the medial quasigroups and the central quasigroups. This covers 19 of the 35 quasigroups of order four. The four quasigroups of order four that are used in Edon-80 are not among those 19 quasigroups. However, the other quasigroups can be obtained by a modification of the central quasigroups and that gives hope that we shall

be able to extend the results in the future. Our results can also justify why the central quasigroups are not actually used in Edon-80.

First, we summarise basic facts about quasigroups. We will describe properties, equivalent definitions and relationships between various types of quasigroups. We will also classify all quasigroups of order 4 to 35 isomorphism classes.

Next, we define the infinite matrix $T_{X,Y,(Q,*)}$ using left iterated translations and study its properties for periodic sequence X.

Further, we define the matrix $A_{\alpha,\beta}$ over a group ring $\mathbb{Z}_{e_G}[\mathrm{Aut}(G)]$ for some finite Abelian group G. For central quasigroup $(Q,*)$, we transform the problem of the finding periods of the row of the matrix $T_{X,Y,(Q,*)}$ to the problem of the finding the periods of the row of the matrix $A_{\alpha,\beta}$.

Then we will try to compute the periods of the rows of the matrix $A_{\alpha,\beta}$ for medial quasigroups and certain central quasigroups. After that we will use our results for central quasigroups of order 4 and we will determine the periods of the rows of the matrix $A_{\alpha,\beta}$ for some isomorphism classes of quasigroups of order 4.

CHAPTER 2

Elements of quasigroup theory

In this chapter we summarise some known fact about quasigroups, which we will use in this thesis. If the proofs are taken from literature, we indicate the source.

1. Definitions and basic facts

DEFINITION 2.1. A *quasigroup* is a set Q with a binary operation $\cdot\colon Q\times Q\to Q$, such that for each $u,v\in Q$ there exist unique $x,y\in Q$ which satisfy $u\cdot x=v$ and $y\cdot u=v$. A quasigroup will be denoted by Q or $(Q,\cdot)$.

LEMMA 2.2. *(The cancellation property) Let $(Q,\cdot)$ be a quasigroup. Then for all $u,v,w\in Q$ the following holds:*

(i) $u\cdot v=u\cdot w$ *implies* $v=w$.
(ii) $v\cdot u=w\cdot u$ *implies* $v=w$.

PROOF. Put $x=u\cdot v=u\cdot w$. By the definition of the quasigroup there exists a unique $y\in Q$ such that $u\cdot y=x$. The uniqueness of y implies $v=w$ and we have (i). (ii) follows similarly.

□

LEMMA 2.3. *$(Q,\cdot)$ is a quasigroup if and only if Q is a set with binary operations $\cdot$, $/$, and $\backslash$, such that the following conditions are satisfied:*

(i) (left division identities) for all $u,v\in Q$, $u\backslash(u\cdot v)=v$ and $u\cdot(u\backslash v)=v$,
(ii) (right division identities) for all $u,v\in Q$, $(v\cdot u)/u=v$ and $(v/u)\cdot u=v$.

PROOF. First, suppose that $(Q,\cdot)$ is a quasigroup. For any $u,v\in Q$, put $u\backslash v=x$ and $v/u=y$, where x,y are the unique solutions of equations $u\cdot x=v$ and $y\cdot u=v$, respectively. Then, using the cancellation property, the left and right division identities are clearly satisfied.

On the other hand, assume that Q is a set with binary operations $\cdot$, $/$, and $\backslash$, and the left and right division identities hold. The identities $u\cdot(u\backslash v)=v$ and $(v/u)\cdot u=v$ give us that the equations $u\cdot x=v$ and $y\cdot u=v$ have solutions $u\backslash v$ and v/u, respectively. It remains to prove the uniqueness of these solutions. Suppose that $x_1,x_2\in Q$ are two solutions of the equation $u\cdot x=v$ for some $u,v\in Q$. Then $v=u\cdot x_1=u\cdot x_2$ and

$$x_1=u\backslash(u\cdot x_1)=u\backslash(u\cdot x_2)=x_2.$$

Similarly we obtain that $y\cdot u=v$ has a unique solution $y\in Q$.

□

The operation $\cdot$ is sometimes called *quasigroup multiplication* and operations $\backslash$ and $/$ are called *left division* and *right division*, respectively.

A quasigroup will be also denoted by $(Q,\cdot,/,\backslash)$.

From Lemma 2.3 we immediately obtain the following rule for compound fractions:

FACT 2.4. *Let $(Q,\cdot)$ be a quasigroup. For each $u,v\in Q$,*

$$u/(v\backslash u)=v\quad\text{and}\quad(u/v)\backslash u=v.$$

DEFINITION 2.5. Let $(Q, \cdot, /, \backslash)$ be a quasigroup. If a subset P of Q is closed under operations $\cdot, /, \backslash$, then $P = (P, \cdot, /, \backslash)$ is called a *subquasigroup* of $Q = (Q, \cdot, /, \backslash)$.

DEFINITION 2.6. A *Latin square of order* n is an $n \times n$ table filled with n copies of each of n different symbols in which no symbol is repeated in any row or column.

OBSERVATION 2.7. *Let $(Q, \cdot)$ be a quasigroup. If Q is a finite set, then the multiplication table of $(Q, \cdot)$ corresponds to a Latin square of order $|Q|$. Conversely, each Latin square determines a multiplication table of a finite quasigroup.*

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

$\cdot$	0	1	2	3
0	1	0	3	2
1	0	3	2	1
2	2	1	0	3
3	3	2	1	0

FIGURE 1. Example of a Latin square and the corresponding multiplication table of a finite quasigroup

DEFINITION 2.8. A *symmetric group* on a set X, denoted by $S(X)$, is a group whose underlying set is the set of all bijections from X to X and the group operation is a composition of bijections, denoted by $\circ$. The unit in $S(X)$ is the identity map and the inverse element to ϕ is the inverse map to the map ϕ, denoted by ϕ^{-1}.

DEFINITION 2.9. Let $(Q, \cdot)$ and $(P, *)$ be quasigroups.

A map $f\colon Q \to P$ is called a *homomorphism* between quasigroups Q and P if $f(x) * f(y) = f(x \cdot y)$ for all x, y in Q.

An *isomorphism* is a bijective homomorphism. If there is an isomorphism between quasigroups P and Q we say that P and Q are *isomorphic*, notation $P \cong Q$.

An isomorphism from Q to Q is called an *automorphism* of Q. The set of all automorphisms of a quasigroup Q forms a group called the *automorphism group* of Q, notation $\mathrm{Aut}(Q)$.

A quasigroup *homotopy* from $(Q, \cdot)$ to $(P, *)$ is a triple (α, β, γ) of maps from Q to P such that

$$\alpha(x) * \beta(y) = \gamma(x \cdot y) \quad \text{for all } x, y \text{ in } Q.$$

An *isotopy* is a homotopy for which each of the three maps (α, β, γ) is a bijection of Q onto P. Then $(\alpha^{-1}, \beta^{-1}, \gamma^{-1})$ is clearly also an isotopy. If there is an isotopy from Q to P then we say that P and Q are *isotopic*. In terms of Latin squares, the map α corresponds to a permutation of rows, the map β corresponds to a permutation of columns, and the map γ corresponds to a permutation of the set of symbols.

LEMMA 2.10. *Let $(Q, \cdot, /, \backslash)$ be a quasigroup, (α, β, γ) be a triple of bijections from Q to P, and $x * y = \gamma(\alpha^{-1}(x) \cdot \beta^{-1}(y))$ for all $x, y \in P$. Then $(P, *)$ is a quasigroup.*

PROOF. [**HV**] Put $a \backslash\backslash b = \beta(\alpha^{-1}(a) \backslash \gamma^{-1}(b))$ and $b /\!/ a = \alpha(\gamma^{-1}(b) / \beta^{-1}(a))$ for each $a, b \in P$. Then

$$\begin{aligned} a \backslash\backslash (a * b) &= \beta\Big(\alpha^{-1}(a) \backslash \gamma^{-1}\left(\gamma(\alpha^{-1}(a) \cdot \beta^{-1}(b))\right)\Big) \\ &= \beta\left(\alpha^{-1}(a) \backslash (\alpha^{-1}(a) \cdot \beta^{-1}(b))\right) \\ &= \beta(\beta^{-1}(b)) = b, \end{aligned}$$

and

$$\begin{aligned} a * (a\backslash\!\backslash b) &= \gamma\Big(\alpha^{-1}(a) \cdot \beta^{-1}\left(\beta(\alpha^{-1}(a)\backslash\gamma^{-1}(b))\right)\Big) \\ &= \gamma\left(\alpha^{-1}(a) \cdot (\alpha^{-1}(a)\backslash\gamma^{-1}(b))\right) \\ &= \gamma(\gamma^{-1}(b)) = b. \end{aligned}$$

This means that the left division identities are satisfied. Similarly we can prove the right division identities and hence $(P, *, /\!/, \backslash\!\backslash)$ is a quasigroup.

□

LEMMA 2.11. *The isotopy (α, β, γ) from a quasigroup $(Q, \cdot)$ to a quasigroup $(P, *)$ induces an isotopy $(\gamma^{-1}\alpha, \gamma^{-1}\beta, \mathrm{id}_Q)$ from $(Q, \cdot)$ to a quasigroup $(Q, \diamond)$, where $\diamond$ is defined by $x \diamond y = \gamma^{-1}(\gamma(x) * \gamma(y))$ for all $x, y \in Q$. The mapping $\gamma\colon (Q, \diamond) \to (P, *)$ is an isomorphism.*

PROOF. We have

$$\gamma^{-1}(\alpha(x)) \diamond \gamma^{-1}(\beta(y)) = \gamma^{-1}\Big(\gamma\big(\gamma^{-1}(\alpha(x))\big) * \gamma\big(\gamma^{-1}(\beta(y))\big)\Big) = \gamma^{-1}(\alpha(x) * \beta(y)) = x \cdot y.$$

□

Let $(Q, \cdot)$ be a quasigroup, $\alpha, \beta \in S(Q)$. Define $x * y = \alpha(x) \cdot \beta(y)$ for all $x, y \in Q$. By Lemma 2.10, $(Q, *)$ is a quasigroup isotopic to $(Q, \cdot)$. This quasigroup is called a *principal isotope* of $(Q, \cdot)$ and denoted by $Q[\alpha, \beta]$.

REMARK 2.12. As a consequence of Lemma 2.11 it follows that instead of studying all isotopes of $(Q, \cdot)$, it suffices to study all principal isotopes of $(Q, \cdot)$.

DEFINITION 2.13. Let $(Q, \cdot)$ be a quasigroup. For every $a \in Q$ we define the *left translation* and *right translation*, denoted by L_a and R_a, as $L_a\colon x \mapsto a \cdot x$ and $R_a\colon x \mapsto x \cdot a$ for all $x \in Q$.

REMARK 2.14. It is clear that left translations and right translations are bijections and that $L_a^{-1}\colon y \mapsto a\backslash y$ and $R_a^{-1}\colon y \mapsto y/a$ for all $a, y \in Q$.

DEFINITION 2.15. A *loop* is a quasigroup $(Q, \cdot)$ with a unit e, i.e. $e \cdot a = a = a \cdot e$ for each $a \in Q$. A loop is usually denoted by $(Q, \cdot, e)$.

Notice that the unit e is uniquely determined and each element a of a loop $(Q, \cdot, e)$ has a unique left and right inverse given by e/a and $a\backslash e$, respectively.

LEMMA 2.16. *Let $(Q, \cdot)$ be a quasigroup. The quasigroup $(Q, *) = Q[\alpha, \beta]$ is a loop, if and only if $\alpha = R_b^{-1}$ and $\beta = L_a^{-1}$ for some $a, b \in Q$. Then*

$$x * y = (x/b) \cdot (a\backslash y)$$

and $a \cdot b$ is the unit of $(Q, *)$.

PROOF. Assume that $\alpha = R_b^{-1}$ and $\beta = L_a^{-1}$. Using Lemma 2.3 we have

$$(a \cdot b) * y = ((a \cdot b)/b) \cdot (a\backslash y) = a \cdot (a\backslash y) = y \quad \text{for all } y \in Q.$$

Similarly, for all $x \in Q$

$$x * (a \cdot b) = (x/b) \cdot (a\backslash(a \cdot b)) = (x/b) \cdot b = x.$$

This implies that $a \cdot b$ is the unit of $(Q, *)$ and $(Q, *, a \cdot b)$ is a loop.

On the other hand, if $(Q, *) = Q[\alpha, \beta]$ is a loop then there exists $e \in Q$ such that $e * x = x * e = x$ for all $x \in Q$. Thus $\alpha(e) \cdot \beta(x) = \alpha(x) \cdot \beta(e) = x$. Put $\bar{a} = \alpha(e)$ and $\bar{b} = \beta(e)$. Then $\beta(x) = \bar{a}\backslash x = L_{\bar{a}}^{-1}(x)$, $\alpha(x) = x/\bar{b} = R_{\bar{b}}^{-1}(x)$ and $e = e * e = \alpha(e) \cdot \beta(e) = \bar{a} \cdot \bar{b}$.

□

COROLLARY 2.17. *Each quasigroup is isotopic to a loop.*

LEMMA 2.18. *Each loop isotopic to a group is isomorphic to this group.*

PROOF. [**S**] Let Q be a loop isotopic to a group $(G, \cdot, ^{-1}, 1)$. By Remark 2.12, there is a quasigroup isomorphism between Q and a principal isotope $G[\alpha, \beta]$. Because this isomorphism preserves the unit, $G[\alpha, \beta] = (G, *, e)$ is also a loop. We have $x*y = \alpha(x)\cdot\beta(y)$ for all $x, y \in G$. Since $\alpha(e) \cdot \beta(y) = e * y = y$ and $\alpha(x) \cdot \beta(e) = x * e = x$, it follows that $\beta(y) = (\alpha(e))^{-1} \cdot y$ and $\alpha(x) = x \cdot (\beta(e))^{-1}$ for any $x, y \in G$. Then

$$\begin{aligned}(\alpha(e) \cdot x \cdot \beta(e)) * (\alpha(e) \cdot y \cdot \beta(e)) &= \alpha\left(\alpha(e) \cdot x \cdot \beta(e)\right) \cdot \beta\left(\alpha(e) \cdot y \cdot \beta(e)\right) \\ &= \left(\alpha(e) \cdot x \cdot \beta(e) \cdot (\beta(e))^{-1}\right) \cdot \left((\alpha(e))^{-1} \cdot \alpha(e) \cdot y \cdot \beta(e)\right) = \alpha(e) \cdot x \cdot y \cdot \beta(e).\end{aligned}$$

This means that $\varphi\colon (G, \cdot, ^{-1}, 1) \to (G, *, e)$, $\varphi(x) = \alpha(e) \cdot x \cdot \beta(e)$ is a homomorphism. Because both left and right translations are bijections, $\varphi = L_{\alpha(e)} \circ R_{\beta(e)}$ is an isomorphism. □

COROLLARY 2.19. *Isotopic groups are isomorphic.*

The following lemma shows that a key property of a quasigroup is that its operation is generally not associative.

LEMMA 2.20. *Let $(Q, \cdot)$ be a quasigroup such that the operation $\cdot$ is associative. Then $(Q, \cdot)$ is a group.*

PROOF. Because $\cdot$ is associative,

$$a \cdot ((a\backslash a) \cdot b) = (a \cdot (a\backslash a)) \cdot b = a \cdot b \quad \text{for each } a, b \in Q.$$

Using the cancellation property we obtain that

$$(a\backslash a) \cdot b = b \quad \text{for each } a, b \in Q$$

or equivalently

$$a\backslash a = b/b \quad \text{for each } a, b \in Q.$$

For $b = a$ we have that $a\backslash a = a/a$ for each $a \in Q$, which means that

$$a/a = a\backslash a = b/b = b\backslash b \quad \text{for any } a, b \in Q.$$

Choose an $x \in Q$ and put $e = x/x$. Then, using the identity above,

$$a \cdot e = a \cdot (a\backslash a) = a \quad \text{and} \quad e \cdot a = (a/a) \cdot a = a,$$

which shows that e is a unit. For each $a \in Q$ we define a^{-1} as e/a. Then

$$a^{-1} \cdot a = (e/a) \cdot a = e.$$

Further,

$$(a \cdot a^{-1}) \cdot a = a \cdot (a^{-1} \cdot a) = a \cdot e = a = e \cdot a.$$

This together with the cancellation property gives that

$$a \cdot a^{-1} = e.$$

□

LEMMA 2.21. *Let $(R, +, \cdot)$ be a ring and a, b be some invertible elements of R. For all $x, y \in R$ define a binary operation*

$$x \diamond y = a \cdot x + b \cdot y.$$

Then $(R, \diamond)$ is a quasigroup.

PROOF. Put

$$x\backslash y = b^{-1} \cdot (y - a \cdot x),$$
$$y/x = a^{-1} \cdot (y - b \cdot x) \quad \text{for any } x, y \in R.$$

For any $x, y \in R$, we have

$$x \diamond (x\backslash y) = x \diamond (b^{-1} \cdot (y - a \cdot x)) = a \cdot x + b \cdot b^{-1} \cdot (y - a \cdot x) = a \cdot x + y - a \cdot x = y,$$
$$x\backslash(x \diamond y) = b^{-1} \cdot (x \diamond y - a \cdot x) = b^{-1} \cdot (a \cdot x + b \cdot y - a \cdot x) = b^{-1} \cdot (b \cdot y) = y.$$

Similarly,

$$(y/x) \diamond x = (a^{-1} \cdot (y - b \cdot x)) \diamond x = a \cdot (a^{-1} \cdot (y - b \cdot x)) + b \cdot x = y - b \cdot x + b \cdot x = y,$$
$$(x \diamond y)/y = a^{-1} \cdot ((x \diamond y) - b \cdot y) = a^{-1} \cdot ((a \cdot x + b \cdot y) - b \cdot y) = a^{-1} \cdot (a \cdot x) = x.$$

Using Lemma 2.3, we obtain that $(R, \diamond)$ is a quasigroup.

□

2. Special types of quasigroups

2.1. Central quasigroups.

DEFINITION 2.22. A *direct product* of quasigroups P and Q is the product set $P \times Q$ considered with componentwise multiplication and divisions. It is clearly a quasigroup. The direct product $Q \times Q$ will be denoted by Q^2.

DEFINITION 2.23. Let Q be a quasigroup.

The *multiplication group* of Q, notation $\mathrm{Mlt}(Q)$, is the subgroup of $S(Q)$ which is generated by all left and right translations.

The *diagonal* of Q is the set $\hat{Q} = \{(x, x);\ x \in Q\}$. It is clearly a subquasigroup of Q^2, which is isomorphic to Q.

A *congruence* on Q is an equivalence relation on Q which, as a subset Q^2, is a subquasigroup of Q^2.

LEMMA 2.24. *Let V be a subquasigroup of Q^2. If V contains the diagonal $\hat{Q}$ then V is a congruence.*

A proof can be found in [**S**, p. 62].

LEMMA 2.25. *Let V be an equivalence relation on a quasigroup $(Q, \cdot)$. The relation V is a congruence if and only if it is invariant under* $\mathrm{Mlt}(Q)$.

PROOF. First, assume that V is a congruence. To prove an invariance under $\mathrm{Mlt}(Q)$, we have to prove only invariance under all left translations, right translations, and their inverses. Because V is an equivalence relation, $(a, a) \in V$ for all $a \in Q$. Let $(x, y) \in V$. Then

$$(R_a(x), R_a(y)) = (x \cdot a, y \cdot a) = (x, y) \cdot (a, a) \in V,$$
$$(L_a(x), L_a(y)) = (a \cdot x, a \cdot y) = (a, a) \cdot (x, y) \in V,$$
$$(R_a^{-1}(x), R_a^{-1}(y)) = (x/a, y/a) = (x, y)/(a, a) \in V,$$
$$(L_a^{-1}(x), L_a^{-1}(y)) = (a\backslash x, a\backslash y) = (a, a)\backslash(x, y) \in V \quad \text{for each } a \in Q.$$

Suppose that V is invariant under $\mathrm{Mlt}(Q)$. Let $(x_1, y_1), (x_2, y_2) \in V$. We obtain that $(R_{x_2}(x_1), R_{x_2}(y_1)) = (x_1 \cdot x_2, y_1 \cdot x_2) \in V$, $(L_{y_1}(x_2), L_{y_1}(y_2)) = (y_1 \cdot x_2, y_1 \cdot y_2) \in V$ and the transitivity gives us $(x_1 \cdot x_2, y_1 \cdot y_2) \in V$. Further, $(x_2/y_1, y_2/y_1) = (R_{y_1}^{-1}(x_2), R_{y_1}^{-1}(y_2)) \in V$ and $(y_1, x_1) \in V$ by the symmetry. Using the closedness under multiplication, we have $(x_2/y_1, y_2/y_1) \cdot (y_1, x_1) = (x_2, (y_2/y_1) \cdot x_1) \in V$ which in turn yields $(x_2/x_1, y_2/y_1) =$

$(R_{x_1}^{-1}(x_2), R_{x_1}^{-1}((y_2/y_1)\cdot x_1)) \in V$. The fact that V is closed under the left division $\backslash$ can be shown similarly.

□

DEFINITION 2.26. Let P be a subquasigroup of a quasigroup Q. If there exists a congruence V on Q having P as a congruence class then P is called a *normal* subquasigroup of Q, written $P \lhd Q$.

DEFINITION 2.27. A quasigroup Q is called *central* if the diagonal $\hat{Q}$ is a normal subquasigroup of Q^2.

LEMMA 2.28. *Let $(Q,\cdot)$ be a quasigroup and $v \in Q$. If $((x\cdot y)/v)\cdot z = ((x\cdot z)/v)\cdot y$ for all $x,y,z \in Q$, then Q is isotopic to an Abelian group.*

PROOF. [**D1**] We define a binary operation $x \diamond y = (x/v)\cdot(v\backslash y)$. Notice that $(Q,\diamond) = Q[R_v^{-1}, L_v^{-1}]$. Lemma 2.16 says that $(Q,\diamond)$ is a loop with the unit $v\cdot v$. For all $x,y,z \in Q$,

$$((x\cdot v)\diamond(v\cdot y))\diamond(v\cdot z) = ((x\cdot y)/v)\cdot z = ((x\cdot z)/v)\cdot y = ((x\cdot v)\diamond(v\cdot z))\diamond(v\cdot y).$$

This implies that

$$(a\diamond b)\diamond c = (a\diamond c)\diamond b \quad \text{for all } a,b,c \in Q. \tag{1}$$

If $a = v\cdot v$ then $b\diamond c = c\diamond b$ for all $b,c \in Q$, which shows the commutativity. Using (1) and the commutativity we obtain

$$(a\diamond b)\diamond c = (b\diamond a)\diamond c = (b\diamond c)\diamond a = a\diamond(b\diamond c)$$

and thus $(Q,\diamond)$ is an Abelian group by Lemma 2.20.

□

PROPOSITION 2.29. *A central quasigroup is isotopic to an Abelian group.*

PROOF. [**D1**] Let $(Q,\cdot)$ be a central quasigroup. Then $\hat{Q}$ is a congruence class of V, where V is a congruence on Q^2. It means that $((v,v),(u_1,u_2)) \in V$ if and only if $u_1 = u_2$ for each $u_1,u_2,v \in Q$.

Fix any $x,y,v \in Q$. Put $\varphi = R^{-1}_{(v,v)\backslash(y,y)} \circ L_{(v,x)} \circ L^{-1}_{(v,v)} \circ R_{(v,x)\backslash(y,y)}$. Then $(R^{-1}_{v\backslash y} \circ L_v \circ L_v^{-1} \circ R_{v\backslash y})(z) = z$, and hence

$$\varphi(z,z) = (z,\psi(z)) \text{ for } z \in Q, \text{ where } \psi = R^{-1}_{v\backslash y} \circ L_x \circ L_v^{-1} \circ R_{x\backslash y}.$$

Using this further on $z = v$ together with Fact 2.4, we obtain

$$\varphi(v,v) = \Big(v, \big(x\cdot(v\backslash(v\cdot(x\backslash y)))\big)/(v\backslash y)\Big) = (v,v).$$

By Lemma 2.25 the congruence V is invariant under $\mathrm{Mlt}(Q^2)$. Because $((v,v),(z,z)) \in V$ and $\varphi \in \mathrm{Mlt}(Q^2)$, $(\varphi(v,v),\varphi(z,z)) = ((v,v),(z,\psi(z))) \in V$. This fact gives us that ψ has to be the identity on Q, which means that $R^{-1}_{v\backslash y} \circ L_x = R^{-1}_{x\backslash y} \circ L_v$.

Therefore

$$(x\cdot z)/(v\backslash y) = (v\cdot z)/(x\backslash y) \quad \text{for all } x,y,v,z \in Q.$$

Substituting $x\cdot y$ for y gives

$$(x\cdot z)/(v\backslash(x\cdot y)) = (v\cdot z)/y \quad \text{for all } x,y,v,z \in Q.$$

Equivalently

$$x\cdot z = ((v\cdot z)/y)\cdot(v\backslash(x\cdot y)) \quad \text{for all } x,y,v,z \in Q.$$

Put $w = v\backslash(x\cdot y)$. Then $x = (v\cdot w)/y$ and

$$((v\cdot w)/y)\cdot z = ((v\cdot z)/y)\cdot w \quad \text{for all } v,w,y,z \in Q.$$

Using Lemma 2.28 we obtain the desired statement.

□

COROLLARY 2.30. *Every central loop is an Abelian group.*

PROOF. Combine Proposition 2.29 with Lemma 2.18.

□

PROPOSITION 2.31. *Let $(Q,\cdot)$ be a quasigroup isotopic to an Abelian group and $y \in Q$. The following conditions are equivalent:*

(i) Q is a central quasigroup

(ii) For all $x, z \in Q$,

$$(y \cdot (x \cdot z))/(x \cdot y) = (y \cdot (y \cdot z))/(y \cdot y),$$
$$(y \cdot x)\backslash((z \cdot x) \cdot y) = (y \cdot y)\backslash((z \cdot y) \cdot y).$$

(iii) The maps $R_{x\cdot y}^{-1} \circ L_y \circ L_x$ and $L_{y\cdot x}^{-1} \circ R_y \circ R_x$ are independent on the choice of $x \in Q$.

A proof can be found in [**D1**].

THEOREM 2.32. *Let $(Q,\cdot)$ be a quasigroup. The following are equivalent:*

(i) $(Q,\cdot)$ is a central quasigroup.

(ii) For all $x, y, z, v \in Q$ the following identities hold:

$$((x \cdot y)/v) \cdot z = ((x \cdot z)/v) \cdot y,$$
$$(y \cdot (x \cdot z))/(x \cdot y) = (y \cdot (y \cdot z))/(y \cdot y),$$
$$(y \cdot x)\backslash((z \cdot x) \cdot y) = (y \cdot y)\backslash((z \cdot y) \cdot y).$$

(iii) There exists an Abelian group $(Q,+)$, $\alpha, \beta \in \mathrm{Aut}((Q,+))$, and $c \in Q$ such that

$$x \cdot y = \alpha(x) + \beta(y) + c \quad \text{for all } x, y \in Q.$$

A proof of this theorem can be also found in [**D1**].

2.2. Medial quasigroups.

DEFINITION 2.33. A quasigroup $(Q,\cdot)$ is called *medial* if $(x \cdot y) \cdot (u \cdot v) = (x \cdot u) \cdot (y \cdot v)$ for all $x, y, u, v \in Q$. This identity is sometimes called a *medial* or *entropic law.*

THEOREM 2.34. *Each medial quasigroup is central.*

To prove this theorem, we need several auxiliary results.

PROPOSITION 2.35. *Each medial quasigroup which is isotopic to an Abelian group is central.*

PROOF. [**HV**] Let $(Q,\cdot)$ be a medial quasigroup and $(G,+,e)$ be an Abelian group to which $(Q,\cdot)$ is isotopic. Using Remark 2.12 we can suppose that Q is a principal isotope of G. It means that $x \cdot y = \alpha(x) + \beta(y)$ for some $\alpha, \beta \in S(G)$ and all $x, y \in G$. Thus the medial law has a form

$$\alpha(\alpha(a) + \beta(b)) + \beta(\alpha(c) + \beta(d)) = \alpha(\alpha(a) + \beta(c)) + \beta(\alpha(b) + \beta(d)) \quad \text{for all } a, b, c, d \in G.$$

Put $\bar{a} = \alpha(a)$, $c = e$, and $\bar{d} = \beta(d)$. Then

$$\alpha(\bar{a} + \beta(b)) + \beta(\alpha(e) + \bar{d}) = \alpha(\bar{a} + \beta(e)) + \beta(\alpha(b) + \bar{d}) \quad \text{for all } \bar{a}, b, \bar{d} \in G.$$

Equivalently,

$$\alpha(\bar{a} + \beta(b)) - \alpha(\bar{a} + \beta(e)) = \beta(\alpha(b) + \bar{d}) - \beta(\alpha(e) + \bar{d}) \quad \text{for all } \bar{a}, b, \bar{d} \in G. \tag{2}$$

The formula holds for each $\bar{a} \in G$, hence also for $\bar{a} = e$:

$$\alpha(\beta(b)) - \alpha(\beta(e)) = \beta(\alpha(b) + \bar{d}) - \beta(\alpha(e) + \bar{d}) \quad \text{for all } b, \bar{d} \in G. \tag{3}$$

Denote $\bar{b} = \beta(b)$. Equations (2) and (3) give

$$\alpha(\bar{a} + \bar{b}) = \alpha(\bar{a} + \beta(e)) + \alpha(\bar{b}) - \alpha(\beta(e)) \quad \text{for all } \bar{a}, \bar{b} \in G. \tag{4}$$

Because the operation $+$ is commutative, for all $\bar{a}, \bar{b} \in G$ we have

$$\alpha(\bar{a} + \beta(e)) + \alpha(\bar{b}) - \alpha(\beta(e)) = \alpha(\bar{a} + \bar{b}) = \alpha(\bar{b} + \bar{a}) = \alpha(\bar{b} + \beta(e)) + \alpha(\bar{a}) - \alpha(\beta(e)).$$

This implies that

$$\alpha(\bar{a} + \beta(e)) = \alpha(\bar{b} + \beta(e)) + \alpha(\bar{a}) - \alpha(\bar{b}) \quad \text{for all } \bar{a}, \bar{b} \in G.$$

For $\bar{b} = e$,

$$\alpha(\bar{a} + \beta(e)) = \alpha(\beta(e)) + \alpha(\bar{a}) - \alpha(e) \quad \text{for all } \bar{a} \in G. \tag{5}$$

Equation (4) together with (5) says that

$$\alpha(\bar{a} + \bar{b}) = \alpha(\bar{a}) + \alpha(\bar{b}) - \alpha(e) \quad \text{for all } \bar{a}, \bar{b} \in G. \tag{6}$$

Similarly, we can prove that

$$\beta(\bar{a} + \bar{b}) = \beta(\bar{a}) + \beta(\bar{b}) - \beta(e) \quad \text{for all } \bar{a}, \bar{b} \in G. \tag{7}$$

Put

$$\varphi(x) = \alpha(x) - \alpha(e),$$
$$\psi(x) = \beta(x) - \beta(e) \quad \text{for every } x \in G.$$

Using (6) and (7) we obtain that $\varphi, \psi \in \mathrm{Aut}((G, +))$ and

$$x \cdot y = \alpha(x) + \beta(y) = \varphi(x) + \psi(y) + (\alpha(e) + \beta(e)).$$

By Theorem 2.32 this means that $(Q, \cdot)$ is a central quasigroup.

□

LEMMA 2.36. *Every medial loop is an Abelian group.*

PROOF. [**HV**] Let $(Q, \cdot, 1)$ be a medial loop. Then $(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d)$ for all $a, b, c, d \in Q$. For $a = 1$ and $d = 1$ we have $b \cdot c = c \cdot b$ for all $b, c \in Q$. For $c = 1$, $(a \cdot b) \cdot d = a \cdot (b \cdot d)$ for all $a, b, d \in Q$ and Lemma 2.20 says that $(Q, \cdot, 1)$ is an Abelian group.

□

LEMMA 2.37. *Let $(Q, \cdot)$ be a medial quasigroup and $(Q, *)$ be a principal isotope of $(Q, \cdot)$. If $(Q, *)$ is a loop then it is also medial.*

PROOF. [**HV**] By Lemma 2.16 there exist $a, b \in Q$ such that $(Q, *) = Q[R_a^{-1}, L_b^{-1}]$. For all $x, y \in Q$, put

$$x *_1 y = R_a^{-1}(x) \cdot y.$$

Then $x *_1 a = R_a^{-1}(x) \cdot a = (x/a) \cdot a = x$. Thus, using Lemma 2.10, $(Q, *_1)$ is a quasigroup with a right unit a. Using the medial law, we have

$$(\bar{x} \cdot \bar{y}) \cdot a = (\bar{x} \cdot \bar{y}) \cdot ((a/a) \cdot a) = (\bar{x} \cdot (a/a)) \cdot (\bar{y} \cdot a) \quad \text{for all } \bar{x}, \bar{y} \in Q.$$

Equivalently,

$$\bar{x} \cdot \bar{y} = R_a^{-1}(R_{a/a}(\bar{x}) \cdot R_a(\bar{y})) \quad \text{for all } \bar{x}, \bar{y} \in Q.$$

Put $x = R_a(R_{a/a}(\bar{x}))$ and $y = R_a(\bar{y})$. Then

$$R_{a/a}^{-1}(R_a^{-1}(x)) \cdot R_a^{-1}(y) = R_a^{-1}(R_a^{-1}(x) \cdot y) \quad \text{for all } x, y \in Q.$$

This identity together with the medial law give us

$$\begin{aligned}(x *_1 y) *_1 (z *_1 v) &= R_a^{-1}(R_a^{-1}(x)\cdot y)\cdot(R_a^{-1}(z)\cdot v)\\ &= (R_{a/a}^{-1}(R_a^{-1}(x))\cdot R_a^{-1}(y))\cdot(R_a^{-1}(z)\cdot v)\\ &= (R_{a/a}^{-1}(R_a^{-1}(x))\cdot R_a^{-1}(z))\cdot(R_a^{-1}(y)\cdot v)\\ &= R_a^{-1}(R_a^{-1}(x)\cdot z)\cdot(R_a^{-1}(y)\cdot v)\\ &= (x *_1 z) *_1 (y *_1 v) \quad \text{for all } x,y,z,v\in Q,\end{aligned}$$

which means that $(Q, *_1)$ is medial.

Next, notice that

$$x * y = R_a^{-1}(x)\cdot L_b^{-1}(y) = x *_1 L_b^{-1}(y) \quad \text{for all } x,y\in Q.$$

Therefore, using the mediality of $(Q, *_1)$ we can prove the mediality of $(Q, *)$ analogously as above.

□

Proof of Theorem 2.34. [**HV**] Let $(Q,\cdot)$ be a medial quasigroup. Choose $a, b \in Q$. Lemma 2.16 together with Remark 2.12 gives that $(Q, *) = Q[R_a^{-1}, L_b^{-1}]$ is a loop isotopic to $(Q,\cdot)$. Lemma 2.37 says that $(Q, *)$ is medial. Because $(Q, *)$ is a medial loop, it is also an Abelian group by Lemma 2.36. Therefore, $(Q,\cdot)$ is a medial quasigroup isotopic to an Abelian group and using Proposition 2.35 we obtain that $(Q,\cdot)$ is central.

□

Suppose that Q is medial. By Theorem 2.34 and Theorem 2.32 there is an Abelian group $(Q,+)$, $\alpha,\beta\in\mathrm{Aut}((Q,+))$, and $c\in Q$ such that $x\cdot y=\alpha(x)+\beta(y)+c$ for all $x,y\in Q$. Using this formula on the medial law of the quasigroup $(Q,\cdot)$ we obtain for any $x,y,u,v\in Q$

$$\begin{aligned}(x\cdot y)\cdot(u\cdot v) &= (x\cdot u)\cdot(y\cdot v)\\ \alpha^2(x)+\alpha\beta(y)+\beta\alpha(u)+\beta^2(v) &= \alpha^2(x)+\alpha\beta(u)+\beta\alpha(y)+\beta^2(v)\\ \alpha\beta(y)+\beta\alpha(u) &= \alpha\beta(u)+\beta\alpha(y)\\ \alpha\beta(y-u) &= \beta\alpha(y-u).\end{aligned}$$

Since these four identities are equivalent, we have proven the following theorem:

Theorem 2.38. *A quasigroup is medial if and only if there exists an Abelian group $(Q,+)$, $\alpha,\beta\in\mathrm{Aut}((Q,+))$, and $c\in Q$ such that $x\cdot y=\alpha(x)+\beta(y)+c$ for all $x,y\in Q$ and the automorphisms α and β commute.*

2.3. Holomorphic quasigroups.

Definition 2.39. Let $G=(G,\cdot)$ be a group. The *holomorph* of G, denoted by $\mathrm{Hol}(G)$, is defined as a semidirect product

$$\mathrm{Hol}(G) = G\rtimes\mathrm{Aut}(G) = (G\times\mathrm{Aut}(G), *),$$

in which

$$(a,\alpha)*(b,\beta) = (a\cdot\alpha(b),\alpha\circ\beta) \text{ for all } a,b\in G \text{ and all } \alpha,\beta\in\mathrm{Aut}(G).$$

Define a map $\varphi\colon G\mapsto S(G)$, $\varphi(g)=L_g$. It is clear that $\mathrm{Ker}\,\varphi$ is trivial and using the First Isomorphism Theorem we obtain that $G\cong\mathrm{Im}\,\varphi=\{L_g;\ g\in G\}\subset S(G)$. The homomorphism φ is called the *left regular representation.*

Now consider the map $\phi\colon (g,\alpha)\mapsto L_g\circ\alpha$. Because $(L_g\circ\alpha)\circ(L_h\circ\beta)=L_{g\cdot\alpha(h)}\circ(\alpha\circ\beta)$ for all $g,h\in G$ and all $\alpha,\beta\in\mathrm{Aut}(G)$, ϕ is a homomorphism from $\mathrm{Hol}(G)$ into $S(G)$. Thus $\mathrm{Im}\,\phi=\{L_g\circ\alpha; g\in G,\alpha\in\mathrm{Aut}(G)\}$ is a subgroup of $S(G)$. The homomorphism ϕ is

clearly injective and hence $\{L_g \circ \alpha; g \in G, \alpha \in \mathrm{Aut}(G)\}$ as the subgroup of $S(G)$ presents a faithful permutation representation of $\mathrm{Hol}(G)$. It is common to identify $\mathrm{Hol}(G)$ with this faithful representation and we will use this convention.

Since $R_g^{-1} \circ L_g, L_g^{-1} \circ R_g \in \mathrm{Aut}(G)$ for all $g \in G$, $\{L_g \circ \varphi; g \in G, \varphi \in \mathrm{Aut}(G)\} = \{R_g \circ \varphi; g \in G, \varphi \in \mathrm{Aut}(G)\}$.

DEFINITION 2.40. Let $G = (G, \cdot)$ be a group. If $\gamma \in \{L_g \circ \varphi; g \in G, \varphi \in \mathrm{Aut}(G)\} = \{R_g \circ \varphi; g \in G, \varphi \in \mathrm{Aut}(G)\}$, then γ is called a *holomorphic permutation*.

A quasigroup is called *left (right) holomorphic* if it can be expressed as a principal isotope $G[\alpha, \beta]$ of group G, where α is a holomorphic permutation (respectively β is holomorphic).

A quasigroup is called *holomorphic* if it can be expressed as a principal isotope $G[\alpha, \beta]$ of group G, where G is a group and α, β are holomorphic permutations.

THEOREM 2.41. *Let $(Q, \cdot)$ be a quasigroup and e be an element of Q. The following conditions are equivalent:*

(i) Q is a left holomorphic quasigroup.

(ii) For all $x, y, z \in Q$,

$$(y/x) \cdot ((x/e) \cdot z) = (y/e) \cdot ((e/e) \cdot z).$$

(iii) The map $L_{y/x} \circ L_{x/e}$ is independent on the choice of $x \in Q$.

A proof can be found in [**D2**].

Compare this theorem with Proposition 2.31.

PROPOSITION 2.42. *Let $(G, \cdot, e)$, $(H, *, 1)$ be groups and $G[\alpha_1, \beta_1]$ be isomorphic to $H[\alpha_2, \beta_2]$. Then α_1 is holomorphic if and only if α_2 is holomorphic and β_1 is holomorphic if and only if β_2 is holomorphic.*

PROOF. [**D2**] Let $\varphi\colon G[\alpha_1, \beta_1] \to H[\alpha_2, \beta_2]$ be an isomorphism. Then

$$\varphi(\alpha_1(x) \cdot \beta_1(y)) = \alpha_2(\varphi(x)) * \beta_2(\varphi(y)) \quad \text{for all } x, y \in G. \tag{8}$$

Put $a = (\alpha_1 \circ \varphi^{-1} \circ \alpha_2^{-1})(1)$ and $b = (\beta_1 \circ \varphi^{-1} \circ \beta_2^{-1})(1)$. Then

$$\varphi(\alpha_1(x) \cdot b) = \varphi\left(\alpha_1(x) \cdot \beta_1(\varphi^{-1}(\beta_2^{-1}(1)))\right) = \alpha_2(\varphi(x)) * \beta_2\left(\varphi(\varphi^{-1}(\beta_2^{-1}(1)))\right) = \alpha_2(\varphi(x))$$

and

$$\varphi(a \cdot \beta_1(y)) = \alpha_2\left(\varphi(\varphi^{-1}(\alpha_2^{-1}(1)))\right) * \beta_2(\varphi(y)) = \beta_2(\varphi(y)) \quad \text{for all } x, y \in G.$$

This means that $\varphi \circ R_b \circ \alpha_1 = \alpha_2 \circ \varphi$ and $\varphi \circ L_a \circ \beta_1 = \beta_2 \circ \varphi$, hence

$$\alpha_2 = \varphi \circ R_b \circ \alpha_1 \circ \varphi^{-1} \quad \text{and} \quad \beta_2 = \varphi \circ L_a \circ \beta_1 \circ \varphi^{-1}. \tag{9}$$

Using this, (8) has a form

$$\varphi(\alpha_1(x) \cdot \beta_1(y)) = \varphi(R_b(\alpha_1(x))) * \varphi(L_a(\beta_1(y))) = \varphi(\alpha_1(x) \cdot b) * \varphi(a \cdot \beta_1(y)) \quad \text{for all } x, y \in G.$$

Equivalently,

$$\varphi(x \cdot y) = \varphi(x \cdot b) * \varphi(a \cdot y) \quad \text{for all } x, y \in G.$$

Therefore,

$$\varphi((x \cdot b^{-1}) \cdot (a^{-1} \cdot y)) = \varphi(x) * \varphi(y) \quad \text{for all } x, y \in G.$$

It can be rewritten as

$$\varphi(x \cdot c^{-1} \cdot y) = \varphi(x) * \varphi(y) \quad \text{for all } x, y \in G,$$

where $c = a \cdot b$. This implies that

$$\varphi(c \cdot x) * \varphi(c \cdot y) = \varphi(c \cdot x \cdot c^{-1} \cdot c \cdot y) = \varphi(c \cdot x \cdot y) \quad \text{for all } x, y \in G,$$

which means that $(\varphi \circ L_c)(x \cdot y) = (\varphi \circ L_c)(x) * (\varphi \circ L_c)(y)$ for every $x, y \in G$. We have just shown that $\nu = \varphi \circ L_c$ is an isomorphism. Applying $\varphi = \nu \circ L_c^{-1}$ to (9) we obtain

$$\alpha_2 = \nu \circ L_c^{-1} \circ R_b \circ \alpha_1 \circ L_c \circ \nu^{-1} = \nu \circ L_c^{-1} \circ L_b \circ L_b^{-1} \circ R_b \circ \alpha_1 \circ L_c \circ \nu^{-1} \text{ and}$$
$$\beta_2 = \nu \circ L_c^{-1} \circ L_a \circ \beta_1 \circ L_c \circ \nu^{-1} = \nu \circ L_b^{-1} \circ \beta_1 \circ L_c \circ \nu^{-1}.$$

Suppose that α_1 is a holomorphic permutation. Since $L_g \circ \alpha = \alpha \circ L_{\alpha^{-1}(g)}$ for each $g \in G$ and $\alpha \in \mathrm{Aut}(G)$, and $L_b^{-1} \circ R_b \in \mathrm{Aut}(G)$, we have $\alpha_2 = \nu \circ L_g \circ \psi \circ \nu^{-1}$ for some $g \in G$ and $\psi \in \mathrm{Aut}(G)$. This means that

$$\alpha_2(x) = \nu(g \cdot \psi(\nu^{-1}(x))) = \nu(g) * \nu(\psi(\nu^{-1}(x))) = \left(L_{\nu(g)} \circ (\nu \circ \psi \circ \nu^{-1})\right)(x).$$

Because $\nu \circ \psi \circ \nu^{-1} \in \mathrm{Aut}(H)$, α_2 is holomorphic. Similarly we obtain that β_2 is holomorphic whenever β_1 is holomorphic.

The converse implication follows by passing to φ^{-1}.

□

Corollary 2.43. *A quasigroup is holomorphic if and only if it is both left holomorphic and right holomorphic.*

Proposition 2.44. *Let $(G, \cdot)$ be a group.*

(i) A quasigroup $(G, *)$ is left (right) holomorphic if and only if it can be expressed as $G[\rho, \sigma]$, where $\rho \in \mathrm{Aut}(G)$, $\sigma \in S(G)$ (respectively $\rho \in S(G)$, $\sigma \in \mathrm{Aut}(G)$).

(ii) A quasigroup $(G, *)$ is holomorphic if and only if there exists $\rho, \sigma \in \mathrm{Aut}(G)$ and $c \in G$ such that $x * y = \rho(x) \cdot c \cdot \sigma(y)$ for all $x, y \in G$. Then $(G, *)$ is isotopic to $(G, \cdot)$.

Proof. (i): Suppose that $(G, *) = G[\alpha, \beta]$, where α is holomorphic. Then there exist $\rho \in \mathrm{Aut}(G)$ and $g \in G$ such that $\alpha = R_g \circ \rho$. Then, for any $x, y \in G$,

$$x * y = \alpha(x) \cdot \beta(y) = R_g(\rho(x)) \cdot \beta(y) = \rho(x) \cdot g \cdot \beta(y) = \rho(x) \cdot \underbrace{(L_g \circ \beta)}_{\sigma}(y).$$

Conversely, if $(G, *) = G[\rho, \sigma]$, $\rho \in \mathrm{Aut}(G)$, then ρ is also holomorphic and the proof is complete.

The proof for right holomorphic quasigroup is analogous.

(ii): Suppose that $(G, *) = G[\alpha, \beta]$ and α, β are holomorphic permutations. Then there exist $\rho, \sigma \in \mathrm{Aut}(G)$ and $g, h \in G$ such that $\alpha = R_g \circ \rho$ and $\beta = L_h \circ \sigma$. Then, for any $x, y \in G$,

$$x * y = \alpha(x) \cdot \beta(y) = R_g(\rho(x)) \cdot L_h(\sigma(y)) = \rho(x) \cdot g \cdot h \cdot \sigma(y) = \rho(x) \cdot \underbrace{(g \cdot h)}_{c} \cdot \sigma(y).$$

On the other hand,

$$x * y = \rho(x) \cdot c \cdot \sigma(y) = \rho(x) \cdot (L_c \circ \sigma)(y) \quad \text{for all } x, y \in G.$$

Since $\rho, \sigma \in \mathrm{Aut}(G)$ and $c \in G$, we obtain that $(G, *) = G[\rho, L_c \circ \sigma]$ is holomorphic.

□

Comparing Theorem 2.32 with Proposition 2.44 reveals that the central quasigroups are related to Abelian groups in the same way as the holomorphic quasigroups are related to noncommutative groups.

Corollary 2.45. *Every central quasigroup is holomorphic.*

Figure 2 summarises the relationships between different classes of quasigroups.

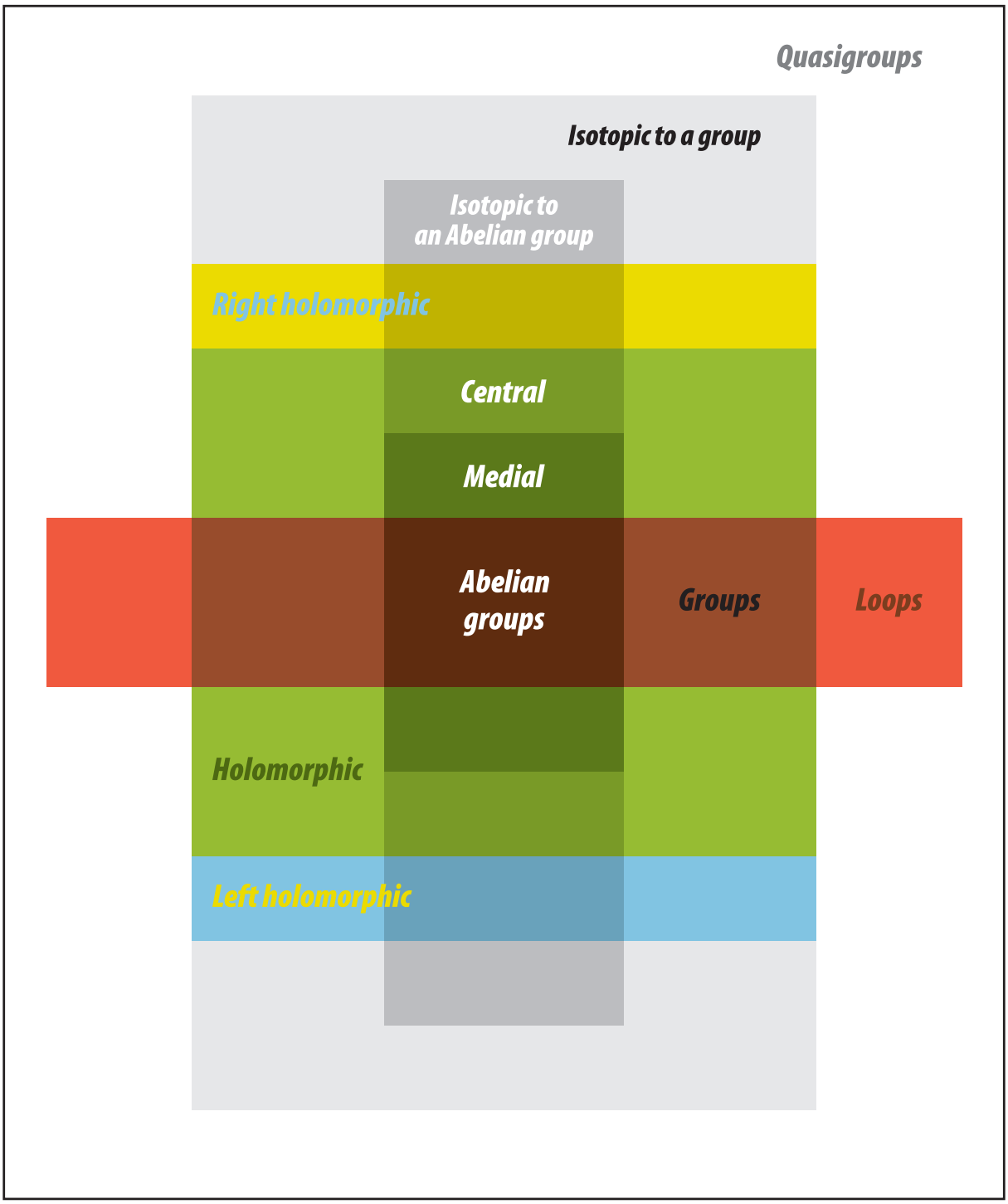


FIGURE 2. The relations between quasigroup classes

3. Classification of quasigroups of order 4

The results in this section are from [**D2**].

PROPOSITION 2.46. *There exist exactly* 20 *isomorphism classes of quasigroups isotopic to a* 4*-element cyclic group* $\mathbb{Z}_4$*. Five of these classes contain quasigroups with no idempotent.*

PROPOSITION 2.47. *There exist exactly* 15 *isomorphism classes of quasigroups isotopic to Klein group* V_4*. All of them are central and exactly four of these classes contain quasigroups with no idempotent.*

We have 35 isomorphism classes of quasigroups which are isotopic to either $\mathbb{Z}_4$ or V_4. Now we describe the representatives of these classes. Let $G = (G, +)$ be a group $\mathbb{Z}_4$ or V_4. Each of the representatives is a quasigroup which can be expressed as $G[\alpha, \beta]$. In Table 1 we summarise the representatives of the isomorphism classes and some of their characteristics and Table 2 shows the multiplication tables of the representatives.

TABLE 1.

N	G	α	β	The strongest property of $G[\alpha, \beta]$	A	I	D	E	F
1	V_4	id	id	Abelian group	6	1	1	1	1
2	V_4	id	(1 2)	medial quasigroup	2	1	2	2	1
3	V_4	(1 2)	id	medial quasigroup	2	1	2	1	2
4	V_4	id	(1 2 3)	medial quasigroup	3	1	4	4	1
5	V_4	(1 2 3)	id	medial quasigroup	3	1	4	1	4
6	V_4	(1 2)	(1 2)	medial quasigroup	2	1	1	2	2
7	V_4	(1 2 3)	(1 2 3)	medial quasigroup	3	1	1	4	4
8	V_4	(1 2 3)	(1 3 2)	medial quasigroup	12	4	4	4	4
9	V_4	(1 2 3)	(0 2 3)	medial quasigroup	4	0	4	4	4
10	V_4	(1 2)	(1 2 3)	central quasigroup	2	2	2	4	2
11	V_4	(1 2 3)	(1 2)	central quasigroup	2	2	2	2	4
12	V_4	(1 2)	(1 3)	central quasigroup	2	2	4	2	2
13	V_4	(1 2)	(0 2 1)	central quasigroup	2	0	2	4	2
14	V_4	(0 2 1)	(1 2)	central quasigroup	2	0	2	2	4
15	V_4	(1 2)	(0 2)	central quasigroup	2	0	4	2	2
16	$\mathbb{Z}_4$	id	id	Abelian group	2	1	2	1	1
17	$\mathbb{Z}_4$	id	(1 3)	medial quasigroup	2	1	1	2	1
18	$\mathbb{Z}_4$	(1 3)	id	medial quasigroup	2	1	1	1	2
19	$\mathbb{Z}_4$	(1 3)	(1 3)	medial quasigroup	2	1	2	2	2
20	$\mathbb{Z}_4$	id	(1 2)	left holomorphic quasigroup	1	1	3	3	1
21	$\mathbb{Z}_4$	(1 2)	id	right holomorphic quasigroup	1	1	3	1	3
22	$\mathbb{Z}_4$	id	(1 2 3)	left holomorphic quasigroup	1	1	3	3	1
23	$\mathbb{Z}_4$	(1 2 3)	id	right holomorphic quasigroup	1	1	3	1	3
24	$\mathbb{Z}_4$	(1 3)	(1 2)	left holomorphic quasigroup	1	2	3	3	2
25	$\mathbb{Z}_4$	(1 2)	(1 3)	right holomorphic quasigroup	1	2	3	2	3
26	$\mathbb{Z}_4$	(1 3)	(0 1)	left holomorphic quasigroup	1	0	3	3	2
27	$\mathbb{Z}_4$	(0 1)	(1 3)	right holomorphic quasigroup	1	0	3	2	3
28	$\mathbb{Z}_4$	(1 2)	(1 2)	isotopic to an Abelian group	1	2	2	3	3
29	$\mathbb{Z}_4$	(1 2)	(2 3)	isotopic to an Abelian group	1	1	3	3	3
30	$\mathbb{Z}_4$	(1 2)	(1 2 3)	isotopic to an Abelian group	1	1	1	3	3
31	$\mathbb{Z}_4$	(1 2)	(0 2 1)	isotopic to an Abelian group	1	1	1	3	3
32	$\mathbb{Z}_4$	(1 2)	(1 3 2)	isotopic to an Abelian group	1	3	3	3	3
33	$\mathbb{Z}_4$	(1 2)	(0 1)	isotopic to an Abelian group	1	0	3	3	3
34	$\mathbb{Z}_4$	(1 2)	(0 3 1)	isotopic to an Abelian group	1	0	3	3	3
35	$\mathbb{Z}_4$	(1 2)	(0 3 2)	isotopic to an Abelian group	1	0	2	3	3

N ... the reference number of the isomorphism class
A ... the order of the automorphism group
I ... the number of idempotents, i.e. $I = |\{x \in Q;\ x * x = x\}|$
D ... the number of squares, i.e $D = |\{x * x;\ x \in Q\}|$
E ... the number of local left units, i.e. $E = |\{x \in Q;\ \exists y \in Q : x * y = y\}|$
F ... the number of local right units, i.e. $F = |\{x \in Q;\ \exists y \in Q : y * x = y\}|$

TABLE 2.

$*_1$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$*_2$	0	1	2	3
0	0	2	1	3
1	1	3	0	2
2	2	0	3	1
3	3	1	2	0

$*_3$	0	1	2	3
0	0	1	2	3
1	2	3	0	1
2	1	0	3	2
3	3	2	1	0

$*_4$	0	1	2	3
0	0	2	3	1
1	1	3	2	0
2	2	0	1	3
3	3	1	0	2

$*_5$	0	1	2	3
0	0	1	2	3
1	2	3	0	1
2	3	2	1	0
3	1	0	3	2

$*_6$	0	1	2	3
0	0	2	1	3
1	2	0	3	1
2	1	3	0	2
3	3	1	2	0

$*_7$	0	1	2	3
0	0	2	3	1
1	2	0	1	3
2	3	1	0	2
3	1	3	2	0

$*_8$	0	1	2	3
0	0	3	1	2
1	2	1	3	0
2	3	0	2	1
3	1	2	0	3

$*_9$	0	1	2	3
0	2	1	3	0
1	0	3	1	2
2	1	2	0	3
3	3	0	2	1

$*_{10}$	0	1	2	3
0	0	2	3	1
1	2	0	1	3
2	1	3	2	0
3	3	1	0	2

$*_{11}$	0	1	2	3
0	0	2	1	3
1	2	0	3	1
2	3	1	2	0
3	1	3	0	2

$*_{12}$	0	1	2	3
0	0	3	2	1
1	2	1	0	3
2	1	2	3	0
3	3	0	1	2

$*_{13}$	0	1	2	3
0	2	0	1	3
1	0	2	3	1
2	3	1	0	2
3	1	3	2	0

$*_{14}$	0	1	2	3
0	2	0	3	1
1	0	2	1	3
2	1	3	0	2
3	3	1	2	0

$*_{15}$	0	1	2	3
0	2	1	0	3
1	0	3	2	1
2	3	0	1	2
3	1	2	3	0

$*_{16}$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$*_{17}$	0	1	2	3
0	0	3	2	1
1	1	0	3	2
2	2	1	0	3
3	3	2	1	0

$*_{18}$	0	1	2	3
0	0	1	2	3
1	3	0	1	2
2	2	3	0	1
3	1	2	3	0

$*_{19}$	0	1	2	3
0	0	3	2	1
1	3	2	1	0
2	2	1	0	3
3	1	0	3	2

$*_{20}$	0	1	2	3
0	0	2	1	3
1	1	3	2	0
2	2	0	3	1
3	3	1	0	2

$*_{21}$	0	1	2	3
0	0	1	2	3
1	2	3	0	1
2	1	2	3	0
3	3	0	1	2

$*_{22}$	0	1	2	3
0	0	2	3	1
1	1	3	0	2
2	2	0	1	3
3	3	1	2	0

$*_{23}$	0	1	2	3
0	0	1	2	3
1	2	3	0	1
2	3	0	1	2
3	1	2	3	0

$*_{24}$	0	1	2	3
0	0	2	1	3
1	3	1	0	2
2	2	0	3	1
3	1	3	2	0

$*_{25}$	0	1	2	3
0	0	3	2	1
1	2	1	0	3
2	1	0	3	2
3	3	2	1	0

$*_{26}$	0	1	2	3
0	1	0	2	3
1	0	3	1	2
2	3	2	0	1
3	2	1	3	0

$*_{27}$	0	1	2	3
0	1	0	3	2
1	0	3	2	1
2	2	1	0	3
3	3	2	1	0

$*_{28}$	0	1	2	3
0	0	2	1	3
1	2	0	3	1
2	1	3	2	0
3	3	1	0	2

$*_{29}$	0	1	2	3
0	0	1	3	2
1	2	3	1	0
2	1	2	0	3
3	3	0	2	1

$*_{30}$	0	1	2	3
0	0	2	3	1
1	2	0	1	3
2	1	3	0	2
3	3	1	2	0

$*_{31}$	0	1	2	3
0	2	0	1	3
1	0	2	3	1
2	3	1	2	0
3	1	3	0	2

$*_{32}$	0	1	2	3
0	0	3	1	2
1	2	1	3	0
2	1	0	2	3
3	3	2	0	1

$*_{33}$	0	1	2	3
0	1	0	2	3
1	3	2	0	1
2	2	1	3	0
3	0	3	1	2

$*_{34}$	0	1	2	3
0	3	0	2	1
1	1	2	0	3
2	0	1	3	2
3	2	3	1	0

$*_{35}$	0	1	2	3
0	3	1	0	2
1	1	3	2	0
2	0	2	1	3
3	2	0	3	1

CHAPTER 3

Binomial coefficients and divisibility

In this chapter we study the divisibility of binomial coefficients. We will need this in later chapters.

DEFINITION 3.1. Let $p, a \in \mathbb{N}$, $p > 1$. The *p-adic expansion* of a is

$$a = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_k \cdot p^k,$$

where $a_i \in \{0, 1, \ldots, p-1\}$ for $i = 1, 2, \ldots, k$. We define the *p-adic representation* of a as

$$a = (a_k a_{k-1} \ldots a_1 a_0)_p.$$

For $p = 2$ a p-adic representation is called a binary representation.

We can see that k in the previous definition is not uniquely determined, as we can add zeros to the left.

DEFINITION 3.2. Let $m, n \in \mathbb{N}$ and $m = (m_l \ldots m_0)_p$ and $n = (n_l \ldots n_0)_p$ be p-adic representations of m and n. Put $c_{-1} = 0$ and for $0 \leq i \leq l$

$$c_i = \begin{cases} 1 & \text{if } m_i + n_i + c_{i-1} \geq p, \\ 0 & \text{otherwise.} \end{cases}$$

The *number of carries* in a p-adic addition of m and n

$$C_p(m, n) = |\{i;\ c_i > 0\}| = \sum_{k=0}^{l} c_i.$$

It is clear that $C_p(m, n) = C_p(n, m)$.

LEMMA 3.3. *Let $n \in \mathbb{N}$, p be a prime, $n = (n_l \ldots n_0)_p$ be a p-adic representation of n, and $m \in \mathbb{N} \cup \{0\}$ such that $p^m \mid n!$ and $p^{m+1} \nmid n!$. Then $m = \frac{1}{p-1}(n - \sum_{k=0}^{l} n_k)$.*

PROOF. If m_i is the exponent of the greatest power of p which divides i, $1 \leq i \leq n$, then $m = \sum_{i=1}^{n} m_i$. ($p^{m+1} \nmid n!$ follows from the fact that p is a prime.)

Define

$$\varepsilon_{i,k} = \begin{cases} 1 & \text{if } p^k \mid i, \\ 0 & \text{otherwise.} \end{cases}$$

Notice that $\varepsilon_{i,k} = 0$ for all $k > l$, $1 \leq i \leq n$, because the p-adic representation of n is $(n_l \ldots n_0)_p$. Thus $m_i = \sum_{k=1}^{l} \varepsilon_{i,k}$ for $1 \leq i \leq n$. Further, among the numbers $1, 2, \ldots, n$, exactly $\lfloor \frac{n}{p^k} \rfloor$ are divisible by p^k for each $k \in \mathbb{N}$. Therefore

$$m = \sum_{i=1}^{n} m_i = \sum_{i=1}^{n} \sum_{k=1}^{l} \varepsilon_{i,k} = \sum_{k=1}^{l} \sum_{i=1}^{n} \varepsilon_{i,k} = \sum_{k=1}^{l} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

This can be expressed as

$$\begin{aligned} m = \sum_{k=1}^{l} \left\lfloor \frac{n}{p^k} \right\rfloor &= \sum_{k=1}^{l} \left\lfloor \frac{n_0 + n_1 p + n_2 p^2 + \cdots + n_l p^l}{p^k} \right\rfloor \\ &= \sum_{k=1}^{l} \left(n_k + n_{k+1} p + \cdots + n_l p^{l-k} \right) \\ &= n_1 + n_2(1+p) + n_3(1+p+p^2) + \cdots + n_l \sum_{k=0}^{l-1} p^k \\ &= \sum_{k=1}^{l} n_k \frac{p^k - 1}{p-1} = \sum_{k=0}^{l} n_k \frac{p^k - 1}{p-1} \\ &= \frac{1}{p-1} \left(\sum_{k=0}^{l} n_k p^k - \sum_{k=0}^{l} n_k \right) = \frac{1}{p-1}(n - \sum_{k=0}^{l} n_k). \end{aligned}$$

□

THEOREM 3.4 (Ernst Eduard Kummer). *Let p be a prime and $m, n \in \mathbb{N}$. The number $\binom{n+m}{m}$ is divisible by the prime power $p^{C_p(m,n)}$, but not by $p^{C_p(m,n)+1}$.*

PROOF. [**P**] Let $m, n \in \mathbb{N}$ and $m = (m_l \dots m_0)_p$, $n = (n_l \dots n_0)_p$, and $m + n = (r_l \dots r_0)_p$ be p-adic representations of m, n, and $m+n$, respectively.

Using Lemma 3.3, the exponent of the greatest power of p which divides $\binom{m+n}{n} = \frac{(m+n)!}{n!m!}$ is

$$\frac{1}{p-1} \left((m+n) - m - n + \sum_{k=1}^{l} (-(m+n)_k + n_k + m_k) \right) = \frac{1}{p-1} \sum_{k=0}^{l} (n_k + m_k - r_k). \tag{10}$$

Let c_i, $-1 \le i \le l$, be the carries in definition of $C_p(m,n)$. We can see that

$$r_k = m_k + n_k + c_{k-1} - p \cdot c_k.$$

Thus

$$\begin{aligned} \sum_{k=0}^{l} (n_k + m_k - r_k) &= \sum_{k=0}^{l} (n_k + m_k - m_k - n_k - c_{k-1} + p \cdot c_k) \\ &= \sum_{k=0}^{l} (c_k - c_{k-1} + p \cdot c_k - c_k) \\ &= \sum_{k=0}^{l} (c_k - c_{k-1}) + (p-1) \cdot \sum_{k=0}^{l} c_k \\ &= c_l - c_{-1} + (p-1) \cdot \sum_{k=0}^{l} c_k = 0 - 0 + (p-1) \cdot \sum_{k=0}^{l} c_k \\ &= (p-1) \cdot \sum_{k=0}^{l} c_k = (p-1) \cdot C_p(m,n). \end{aligned}$$

Using (10) we obtain the desired statement.

□

Now we will describe some properties of the number $C_p(m,n)$. Since $p^s = (1\underbrace{0\dots0}_{s})_p$ for any $p, s \in \mathbb{N}$, the following facts are easy to see:

FACT 3.5. *Let $b, p \in \mathbb{N}$, $s \in \mathbb{N} \cup \{0\}$, and $b = (b_k \dots b_0)_p$. Then $C_p(b, p^s) = m \geq 0$ if and only if $b_j = p-1$ for each $j = s, \dots, s+m-1$ and $b_{s+m} \neq p-1$.*

FACT 3.6. *Let $b, p \in \mathbb{N}$, $b = (b_k \dots b_0)_p$ and $s \in \mathbb{N} \cup \{0\}$ such that $C_p(b, p^s) > 0$. Then $C_p(b, p^{s+1}) = C_p(b, p^s) - 1$.*

If $b \in \mathbb{N}$ has a p-adic representation $(b_k \dots b_0)_p$ then $pb + j$, $0 \leq j \leq p-1$, has a p-adic representation $(c_{k+1} \dots c_0)_p = (b_k \dots b_0 j)_p$. Using Fact 3.5 we obtain:

FACT 3.7. *Let $b, p \in \mathbb{N}$ and $s \in \mathbb{N} \cup \{0\}$. Then $C_p(b, p^s) = C_p(pb + j, p^{s+1})$ for any $0 \leq j \leq p-1$.*

The following lemma describes how many integers from certain interval belong to the same congruent class.

LEMMA 3.8. *Let $n \in \mathbb{N}$, $a, b, j \in \mathbb{N} \cup \{0\}$, $0 \leq j < n$. Then*

$$\left|\{i;\ a \leq i < a+b,\ i \equiv j \pmod n\}\right| = \left\lceil \frac{a+b-j}{n} \right\rceil - \left\lceil \frac{a-j}{n} \right\rceil.$$

PROOF. Denote $\sigma_j(a,b) = |\{i;\ a \leq i < a+b,\ i \equiv j \pmod n\}|$. Clearly $\sigma_j(a,b) = \sigma_j(0, a+b) - \sigma_j(0,a)$. Further,

$$\begin{aligned}
\sigma_j(a,b) &= |\{i;\ a \leq i < a+b,\ i \equiv j \pmod n\}| \\
&= |\{i;\ a \leq i < a+b,\ i+n-j \equiv 0 \pmod n\}| \\
&= |\{k+j-n;\ a \leq k+j-n < a+b,\ k \equiv 0 \pmod n\}| \\
&= |\{k;\ a+n-j \leq k < a+n-j+b,\ k \equiv 0 \pmod n\}| \\
&= \sigma_0(a+n-j, b) = \sigma_0(0, a+b+n-j) - \sigma_0(0, a+n-j).
\end{aligned}$$

It follows that we only need to evaluate $\sigma_0(0,c)$, $c \in \mathbb{N}$.

Choose any $c \in \mathbb{N}$. There is $1 \leq r \leq n$ such that $c = n(\lceil \frac{c}{n} \rceil - 1) + r$. Then

$$\sigma_0(0,c) = \sigma_0\left(0, n\left(\left\lceil \frac{c}{n} \right\rceil - 1\right)\right) + \sigma_0\left(n\left(\left\lceil \frac{c}{n} \right\rceil - 1\right), r\right) = \left\lceil \frac{c}{n} \right\rceil - 1 + 1 = \left\lceil \frac{c}{n} \right\rceil.$$

(Notice that in the interval $\langle n(\lceil \frac{c}{n} \rceil - 1), n(\lceil \frac{c}{n} \rceil - 1) + r)$ there is exactly one number divisible by n.) Putting everything together we obtain

$$\sigma_j(a,b) = \left\lceil \frac{a+b+n-j}{n} \right\rceil - \left\lceil \frac{a+n-j}{n} \right\rceil = \left\lceil \frac{a+b-j}{n} \right\rceil - \left\lceil \frac{a-j}{n} \right\rceil.$$

□

Further, we study under which conditions certain products of the binomial coefficients are odd.

LEMMA 3.9. *Let $a, b, c \in \mathbb{N} \cup \{0\}$ and $b \leq 3 \cdot 2^c - 1$. Then the number*

$$\binom{b+a}{a}\binom{3\cdot 2^c - 1 - b + a}{a}$$

is odd if and only if one of the following conditions is satisfied:

(i) $a = q \cdot 2^{c+2}$ *for some* $q \in \mathbb{N} \cup \{0\}$,
(ii) $a = q \cdot 2^{c+2} + 2^c$ *for some* $q \in \mathbb{N} \cup \{0\}$, *and* $b < 2^c$ *or* $b \geq 2^{c+1}$,
(iii) $a = q \cdot 2^{c+2} + 2^{c+1}$ *for some* $q \in \mathbb{N} \cup \{0\}$, *and* $2^c \leq b < 2^{c+1}$.

PROOF. The number $\binom{b+a}{a}\binom{3\cdot 2^c-1-b+a}{a}$ is odd if and only if both $\binom{b+a}{a}$ and $\binom{3\cdot 2^c-1-b+a}{a}$ are odd. Using Theorem 3.4 we obtain that it is possible if and only if $C_2(a,b)=0$ and $C_2(a,3\cdot 2^c-1-b)=0$.

The binary representations of the numbers a, $3\cdot 2^c-1$, and b are

$$\begin{aligned} a &= (a_k\dots a_0)_2,\\ 3\cdot 2^c-1 &= (10\underbrace{1\dots 1}_{c})_2,\\ b &= (b_{c+1}b_c\dots b_0)_2, \quad \text{where } b_c=0 \text{ if } b_{c+1}=1. \end{aligned}$$

Since $(b_{c+1}b_c\dots b_0)_2+((1-b_c-b_{c+1})b_c(1-b_{c-1})\dots(1-b_0))_2=(10\underbrace{1\dots 1}_{c})_2$, the binary representation of $3\cdot 2^c-1-b$ is

$$3\cdot 2^c-1-b=((1-b_c-b_{c+1})b_c(1-b_{c-1})\dots(1-b_0))_2.$$

Suppose $m,n\in\mathbb{N}\cup\{0\}$, $m=(m_l\dots m_0)_2$ and $n=(m_l\dots m_0)_2$. Then $C_2(m,n)=0$ if and only if $m_in_i=0$ for each $0\le i\le l$. This implies that $\binom{b+a}{a}\binom{3\cdot 2^c-1-b+a}{a}$ is odd if and only if

$$\begin{aligned} a_ib_i &= 0 \quad \text{for } 0\le i\le c+1,\\ a_i(1-b_i) &= 0 \quad \text{for } 0\le i\le c-1,\\ a_{c+1}(1-b_c-b_{c+1}) &= 0. \end{aligned}$$

This system of equations can be easily transformed into

$$\begin{aligned} a_i &= 0 \quad \text{for } 0\le i\le c-1,\\ a_cb_c &= 0,\\ a_{c+1}b_{c+1} &= 0,\\ a_{c+1}(1-b_c) &= 0. \end{aligned}$$

The last three equations have the following three solutions:

(i) $a_c=a_{c+1}=0$,
(ii) $a_c=1$, $a_{c+1}=0$, $b_c=0$,
(iii) $a_c=0$, $a_{c+1}=1$, $b_c=1$, $b_{c+1}=0$.

This implies our statement. □

LEMMA 3.10. *Let $a\in\mathbb{N}$, $b,c\in\mathbb{N}\cup\{0\}$ and $b\le 3\cdot 2^c-1$. Then the number*

$$\binom{b+a-1}{a-1}\binom{3\cdot 2^c-1-b+a}{a}$$

is odd if and only if one of the following conditions is satisfied:

(i) $a=q2^{t+1}+2^t$ *for some* $q,t\in\mathbb{N}\cup\{0\}$, $t>c+1$, *and* $b=0$,
(ii) $a=q2^{c+2}+2^{c+1}$ *for some* $q\in\mathbb{N}\cup\{0\}$, *and* $b=2^{c+1}$,
(iii) $a=q2^{c+2}+2^c$ *for some* $q\in\mathbb{N}\cup\{0\}$, *and either* $b=0$ *or* $b=2^{c+1}$,
(iv) $a=q2^{c+2}+2^{c+1}+2^t$ *for some* $q,t\in\mathbb{N}\cup\{0\}$, $t<c$, $b=r2^{t+1}+2^t$ *for some* $r\in\mathbb{N}\cup\{0\}$, *and* $2^c\le b<2^{c+1}$,
(v) $a=q2^{c+2}+2^c+2^t$ *for some* $q,t\in\mathbb{N}\cup\{0\}$, $t<c$, $b=r2^{t+1}+2^t$ *for some* $r\in\mathbb{N}\cup\{0\}$, *and either* $b<2^c$ *or* $b\ge 2^{c+1}$,
(vi) $a=q2^{c+2}+2^t$ *for some* $q,t\in\mathbb{N}\cup\{0\}$, $t<c$, *and* $b=r2^{t+1}+2^t$ *for some* $r\in\mathbb{N}\cup\{0\}$.

PROOF. The number $\binom{b+a-1}{a-1}\binom{3\cdot 2^c-1-b+a}{a}$ is odd if and only if $C_2(a-1,b)=0$ and $C_2(a,3\cdot 2^c-1-b)=0$. The binary representations are:

$$\begin{aligned}
a &= (a_k \dots a_{t+1} 1 \underbrace{0 \dots 0}_{t})_2 \quad \text{for some } 0 \le t \le k,\\
a-1 &= (a_k \dots a_{t+1} 0 \underbrace{1 \dots 1}_{t})_2,\\
3\cdot 2^c - 1 &= (10 \underbrace{1 \dots 1}_{c})_2,\\
b &= (b_{c+1} b_c \dots b_0)_2, \quad \text{where } b_c = 0 \text{ if } b_{c+1} = 1,\\
3\cdot 2^c - 1 - b &= (d_{c+1} \dots d_0)_2 = ((1-b_c-b_{c+1}) b_c (1-b_{c-1}) \dots (1-b_0))_2.
\end{aligned}$$

We know that $C_2(a-1,b)=0$ and $C_2(a,3\cdot 2^c-1-b)=0$ if and only if

$$\begin{aligned}
b_i &= 0 \quad \text{for } 0 \le i \le t-1,\\
a_i b_i &= 0 \quad \text{for } t+1 \le i \le c+1,\\
d_t &= 0,\\
d_i a_i &= 0 \quad \text{for } t+1 \le i \le c+1.
\end{aligned} \tag{11}$$

Suppose that $t > c+1$. Then the system (11) reduces to

$$b_i = 0 \quad \text{for } 0 \le i \le c+1,$$

that is $b=0$ and (i) is satisfied.

For $t = c+1$ we have that

$$\begin{aligned}
b_i &= 0 \quad \text{for } 0 \le i \le c,\\
d_t &= d_{c+1} = 1 - b_c - b_{c+1} = 1 - b_{c+1} = 0,
\end{aligned}$$

that is $b = 2^{c+1}$ and (ii) holds.

For $t = c$, (11) has a form

$$\begin{aligned}
b_i &= 0 \quad \text{for } 0 \le i \le c-1,\\
a_{c+1} b_{c+1} &= 0,\\
d_c &= b_c = 0,\\
d_{c+1} a_{c+1} &= (1-b_c-b_{c+1}) a_{c+1} = (1-b_{c+1}) a_{c+1} = 0,
\end{aligned}$$

which is satisfied if and only if $b_i = 0$ for each $0 \le i \le c$ and $a_{c+1} = 0$. This means that $a = (a_k \dots a_{c+2} 01 \underbrace{0 \dots 0}_{c})_2$ and either $b=0$ or $b = 2^{c+1}$, which implies (iii).

Finally, assume that $t < c$. Thus

$$\begin{aligned}
b_i &= 0 \quad \text{for } 0 \le i \le t-1,\\
a_i b_i &= 0 \quad \text{for } t+1 \le i \le c+1,\\
d_t &= 1 - b_t = 0,\\
d_i a_i &= (1-b_i) a_i = 0 \quad \text{for } t+1 \le i \le c-1,\\
d_c a_c &= b_c a_c = 0,\\
d_{c+1} a_{c+1} &= (1-b_c-b_{c+1}) a_{c+1} = (1-b_c) a_{c+1} = 0.
\end{aligned}$$

This system of equations can be easily transformed into

$$\begin{aligned} b_i &= 0 \quad \text{for } 0 \le i \le t-1, \\ b_t &= 1, \\ a_i &= 0 \quad \text{for } t+1 \le i \le c-1, \\ a_c b_c &= 0, \\ a_{c+1} b_{c+1} &= 0, \\ a_{c+1}(1-b_c) &= 0. \end{aligned}$$

The last three equations have the following three solutions:

(iv) $a_c = 0$, $a_{c+1} = 1$, $b_c = 1$, $b_{c+1} = 0$.
(v) $a_c = 1$, $a_{c+1} = 0$, $b_c = 0$,
(vi) $a_c = a_{c+1} = 0$,

This implies our statement.

□

LEMMA 3.11. *Let $a, b, c \in \mathbb{N} \cup \{0\}$ and $b \le a$. Then*

$$\binom{b+2^c-1}{2^c-1}\binom{a-b+2^c-1}{2^c-1}$$

is odd if and only if $2^c \mid a$ and $2^c \mid b$.

PROOF. The number $\binom{b+2^c-1}{2^c-1}\binom{a-b+2^c-1}{2^c-1}$ is odd if and only if both binomial coefficients $\binom{b+2^c-1}{2^c-1}$ and $\binom{a-b+2^c-1}{2^c-1}$ are odd, which is equivalent to $C_2(2^c-1, b) = C_2(2^c-1, a-b) = 0$. The binary representation of $2^c - 1$ is $(\underbrace{1 \dots 1}_{c})_2$. Let $b = (b_k \dots b_0)_2$, $a = (a_k \dots a_0)_2$, and $a - b = (d_k \dots d_0)_2$. Then $C_2(2^c - 1, b) = 0$ if and only if $b_i = 0$ for $0 \le i \le c-1$. It implies that $a - b = (d_k \dots d_c a_{c-1} \dots a_0)_2$. Thus $C_2(2^c - 1, a - b) = 0$ if and only if $a_i = 0$ for $0 \le i \le c-1$.

□

LEMMA 3.12. *Let p be a prime, $a, b, c \in \mathbb{N} \cup \{0\}$, and $a < b < p^c$. Then the number*

$$\binom{p^c + a}{b}$$

is divisible by p.

PROOF. By Theorem 3.4, the number $\binom{p^c+a}{b}$ is divisible by p if and only if $C_p(b, p^c + a - b) > 0$, i.e. there is at least one carry in the p-adic addition of the numbers b and $q = p^c + a - b$.

From $a < b$ we obtain $q < p^c$. But $b + q = p^c + a \ge p^c$. Since the sum of two numbers which are smaller than p^c is greater than or equal to p^c, there must be at least one carry in their p-adic addition.

□

LEMMA 3.13. *Let $b \in \mathbb{N} \cup \{0\}$, $c \in \mathbb{N}$ and $b \le 2^c$. Then the number*

$$\binom{2^c + 2^{c-1} - 1}{2^c - b}\binom{2^c + 2^{c-1}}{b}$$

is odd if and only if $b = 0$ or $b = 2^c$.

PROOF. By Lemma 3.12, if $0 < b < 2^{c-1} + 1$ then $\binom{2^c+2^{c-1}-1}{2^c-b}$ is even and if $2^{c-1} < b < 2^c$ then $\binom{2^c+2^{c-1}}{b}$ is even.

For $b = 0$, $\binom{2^c+2^{c-1}}{0} = 1$ and since $C_2(2^c, 2^{c-1} - 1) = 0$, the number $\binom{2^c+2^{c-1}-1}{2^c}$ is odd by Theorem 3.4. For $b = 2^c$, $\binom{2^c+2^{c-1}-1}{0} = 1$ and because $C_2(2^c, 2^{c-1}) = 0$, the number $\binom{2^c+2^{c-1}}{2^c}$ is odd by Theorem 3.4.

□

CHAPTER 4

Periods

In this chapter we define certain infinite matrices and we will study their properties.

1. Matrices $T_{X,Y,(Q,*)}$ and $A_{\alpha,\beta}$

In this section we fix a finite quasigroup $(Q,*)$.

Let X be a set. A set of all infinite sequences $(a_i)_{i=1}^{\infty}$, where $a_i \in X$ for all $i \geq 1$, will be denoted by $X^{\mathbb{N}}$ and a set of sequences of length n will be denoted by X^n.

Definition 4.1. For each $y \in Q$ we define a map

$$\begin{aligned} \tau_y\colon \quad Q^{\mathbb{N}} &\to Q^{\mathbb{N}} \\ (a_i)_{i=1}^{\infty} &\mapsto (b_i)_{i=1}^{\infty} \end{aligned}$$

by

$$\begin{aligned} b_1 &= y * a_1, \\ b_i &= b_{i-1} * a_i \quad \text{for } i > 1. \end{aligned}$$

The map τ_y is called a *left iterated translation*. When working with Q^n, a restriction of τ_y to a canonical embedding of Q^n into $Q^{\mathbb{N}}$ will also be denoted by τ_y.

Lemma 4.2. *For each $y \in Q$, a left iterated translation τ_y is a bijection and a map $\upsilon_y\colon (b_i)_{i=1}^{\infty} \mapsto (a_i)_{i=1}^{\infty}$ defined by*

$$\begin{aligned} a_1 &= y \backslash b_1, \\ a_i &= b_{i-1} \backslash b_i \quad \textit{for } i > 1. \end{aligned}$$

is an inverse map to τ_y for all $y \in Q$.

Proof. It is clear that $\upsilon_y \circ \tau_y = \mathrm{id}_{Q^{\mathbb{N}}} = \tau_y \circ \upsilon_y$ for all $y \in Q$ and these identities imply that τ_y is a bijection.

□

Definition 4.3. Let $X = (x_i)_{i=1}^{\infty}$ and $Y = (y_i)_{i=1}^{\infty}$ belong to $Q^{\mathbb{N}}$. An infinite matrix $T_{X,Y,(Q,*)} = T = (t_{i,j})_{i,j=1}^{\infty}$ over Q is defined this way:

$$\begin{aligned} t_{1,1} &= y_1 * x_1, \\ t_{1,j} &= t_{1,j-1} * x_j \quad \text{for } j > 1, \\ t_{i,1} &= y_i * t_{i-1,1} \quad \text{for } i > 1, \\ t_{i,j} &= t_{i,j-1} * t_{i-1,j} \quad \text{for } i,j > 1. \end{aligned}$$

$*$	x_1	x_2	x_3	$\ldots$
y_1	$y_1 * x_1$	$(y_1 * x_1) * x_2$	$((y_1 * x_1) * x_2) * x_3$	
y_2	$y_2 * (y_1 * x_1)$	$(y_2 * (y_1 * x_1)) * ((y_1 * x_1) * x_2)$	$((y_2 * (y_1 * x_1)) * ((y_1 * x_1) * x_2)) * (((y_1 * x_1) * x_2) * x_3)$	
$\vdots$				

Table 3. The matrix T

The first row of the matrix T can be written as $\tau_{y_1}((x_i)_{i=1}^{\infty})$. Similarly, for $i > 1$ we can express the ith row using the $(i-1)$th row and y_i as $(t_{i,j})_{j=1}^{\infty} = \tau_{y_i}((t_{i-1,j})_{j=1}^{\infty})$.

DEFINITION 4.4. Let $(a_i)_{i=1}^{\infty} \in Q^{\mathbb{N}}$. If there exist a positive integer P such that

$$a_i = a_{i+P} \quad \text{for all } i \geq 1,$$

we say that the sequence $(a_i)_{i=1}^{\infty}$ is *periodic* and P is called a *period* of the sequence $(a_i)_{i=1}^{\infty}$. The smallest period is called the *minimal period*.

FACT 4.5. *Let $A = (a_i)_{i=1}^{\infty}$ be a periodic sequence. A number $P \in \mathbb{N}$ is a period of A if and only if P is a multiple of the minimal period of the sequence A.*

PROOF. It is clear that every multiple of the minimal period is also a period. Let P be a period of A and P_m be the minimal period of A. Clearly, $P = kP_m + l$ for some $k \in \mathbb{N}$ and $0 \leq l < P_m$. If $l > 0$ then $a_i = a_{i+P} = a_{i+kP_m+l} = a_{i+l}$ for each $i \in \mathbb{N}$. Thus $l < P_m$ is a period of A, which is a contradiction.

□

LEMMA 4.6. *Let $y \in Q$ and $(a_i)_{i=1}^{\infty} \in Q^{\mathbb{N}}$, $(b_i)_{i=1}^{\infty} = \tau_y((a_i)_{i=1}^{\infty})$ be periodic sequences. Then the minimal period of the sequence $(b_i)_{i=1}^{\infty}$ is a multiple of the minimal period of the sequence $(a_i)_{i=1}^{\infty}$.*

PROOF. Denote the minimal period of $(a_i)_{i=1}^{\infty}$ by P_1 and the minimal period of $(b_i)_{i=1}^{\infty}$ by P_2. We have

$$a_i = a_{i+P_1} \quad \text{for } i \geq 1.$$

If we apply the definition of the sequence $(b_i)_{i=1}^{\infty}$ and the fact that P_2 is the period of $(b_i)_{i=1}^{\infty}$ we obtain:

$$a_i = b_{i-1} \backslash b_i = b_{i+P_2-1} \backslash b_{i+P_2} = a_{i+P_2} \quad \text{for } i \geq 2. \tag{12}$$

Put $N = \operatorname{lcm}(P_1, P_2)$. There exist $k, l \geq 1$ such that $N = k \cdot P_1 = l \cdot P_2$. The $(N+1)$th element of the sequence $(a_i)_{i=1}^{\infty}$ can be expressed as

$$a_1 = a_{k \cdot P_1 + 1} = a_{N+1} = a_{l \cdot P_2 + 1} = a_{(l-1) \cdot P_2 + P_2 + 1} = a_{P_2+1}.$$

This identity together with (12) gives that $a_i = a_{i+P_2}$ for all $i \geq 1$ and hence P_2 is a period of the sequence $(a_i)_{i=1}^{\infty}$. Because P_1 is the minimal period, P_2 has to be a multiple of P_1 by Fact 4.5.

□

LEMMA 4.7. *Let $y \in Q$, $(a_i)_{i=1}^{\infty} \in Q^{\mathbb{N}}$ be a periodic sequence with a minimal period P, and $(b_i)_{i=1}^{\infty} = \tau_y((a_i)_{i=1}^{\infty})$. Then $(b_i)_{i=1}^{\infty}$ is periodic with the minimal period $s \cdot P$ for some $s \in \{1, 2, 3, \ldots, |Q|\}$.*

PROOF. Because P is the minimal period of $(a_i)_{i=1}^{\infty}$, we have

$$a_{i+P} = a_i \quad \text{for } i \geq 1.$$

Put $S := (a_1, a_2, \ldots, a_P) \in Q^P$. The sequence $(b_i)_{i=1}^{\infty}$ can be divided into P-tuples and we denote them by

$$B_k = (b_{(k-1) \cdot P+1}, b_{(k-1) \cdot P+2}, \ldots, b_{k \cdot P}) \quad \text{for } k = 1, 2, \ldots.$$

Using the left iterated translation $\tau_y \colon Q^P \to Q^P$ we obtain that

$$\begin{aligned} B_1 &= \tau_y(S), \\ B_k &= \tau_{b_{(k-1) \cdot P}}(S) \quad \text{for } k \geq 2. \end{aligned}$$

Since $|Q|$ is a finite number, by the pigeonhole principle we can find two same elements among $y, b_P, b_{2 \cdot P}, \ldots, b_{|Q| \cdot P}$. There are two possibilities:

First, $y = b_{r \cdot P}$ for some $1 \leq r \leq |Q|$. Then $B_1 = B_{r+1}$ and hence $B_k = B_{r+k}$ for $k \geq 1$. This implies that $r \cdot P$ is a period of $(b_i)_{i=1}^{\infty}$.

Second, $b_{r_1 \cdot P} = b_{r_2 \cdot P}$ for some $1 \leq r_1 < r_2 \leq |Q|$. Put $r = r_2 - r_1$. Then $B_{r_1+1} = B_{r_2+1} = B_{r_1+r+1}$ and hence $B_{r_1+k} = B_{r_1+r+k}$ for all $k \geq 1$. It follows that

$$b_j = b_{r \cdot P + j} \quad \text{for } j \geq r_1 \cdot P + 1. \tag{13}$$

Using the definition of the sequence $(b_i)_{i=1}^{\infty}$ and the fact that P is a period of $(a_i)_{i=1}^{\infty}$, for $0 \leq i \leq r_1 \cdot P - 1$ the following holds:

$$\begin{aligned} b_{r_1 \cdot P+1} &= (\cdots (b_{r_1 \cdot P - i} * a_{r_1 \cdot P + 1 - i}) * \cdots) * a_{r_1 \cdot P + 1}, \\ b_{r_1 \cdot P + r \cdot P + 1} &= (\cdots (b_{r_1 \cdot P + r \cdot P - i} * a_{r_1 \cdot P + r \cdot P + 1 - i}) * \cdots) * a_{r_1 \cdot P + r \cdot P + 1} \\ &= (\cdots (b_{r_1 \cdot P + r \cdot P - i} * a_{r_1 \cdot P + 1 - i}) * \cdots) * a_{r_1 \cdot P + 1}. \end{aligned}$$

Since, by (13), $b_{r_1 \cdot P+1} = b_{r_1 \cdot P + r \cdot P + 1}$, using the cancellation property (Lemma 2.2) we obtain

$$b_{r_1 \cdot P - i} = b_{r_1 \cdot P - i + r \cdot P} \quad \text{for } 0 \leq i \leq r_1 \cdot P - 1,$$

which together with (13) gives that $r \cdot P$ is a period of the sequence $(b_i)_{i=1}^{\infty}$.

Finally, by Lemma 4.6 there is $s \in \mathbb{N}$, $s \leq r$ such that $s \cdot P$ is the minimal period of $(b_i)_{i=1}^{\infty}$.

□

It is clear that the following statements hold:

COROLLARY 4.8. *Let $(a_i)_{i=1}^{\infty} \in Q^{\mathbb{N}}$ be periodic and $(b_i)_{i=1}^{\infty} = \tau_y((a_i)_{i=1}^{\infty})$ for some $y \in Q$. Denote the minimal period of $(a_i)_{i=1}^{\infty}$ by P_1. Then $(b_i)_{i=1}^{\infty}$ is periodic and the minimal period of the sequence $(b_i)_{i=1}^{\infty}$ is P_2 if and only if P_2 is the smallest multiple of P_1 such that*

$$b_{P_2} = y.$$

COROLLARY 4.9. *Suppose that the sequence $X = (x_i)_{i=1}^{\infty} \in Q^{\mathbb{N}}$ is periodic. Then each row of the matrix $T_{X,Y,(Q,*)}$ is periodic, for any sequence $Y = (y_i)_{i=1}^{\infty} \in Q^{\mathbb{N}}$.*

Moreover, denote by P_0 be the minimal period of the sequence X and by P_i be the minimal period of the ith row of the matrix $T_{X,Y,(Q,*)}$. Then

(i) For each $i \geq 1$ there exists $k_i \in \{1, 2, \ldots, |Q|\}$ such that

$$P_i = k_i \cdot P_{i-1}.$$

(ii) The minimal period of the ith row is a positive integer P if and only if P is the smallest multiple of P_{i-1} such that

$$t_{i,P} = y_i.$$

2. Central quasigroups

Suppose that $G = (G, +)$ is an Abelian group. Let $\alpha, \beta \in G^G$. We define a map $\alpha + \beta \colon G \to G$ by $(\alpha + \beta)(g) := \alpha(g) + \beta(g)$ for all $g \in G$. If moreover $\alpha, \beta \in \mathrm{End}(G)$ then $\alpha + \beta \in \mathrm{End}(G)$. Further, we define maps $0 \colon G \to G$ and $-\alpha \colon G \to G$ by $0(g) = 0$ and $(-\alpha)(g) = -(\alpha(g))$ for all $g \in G$. If $\alpha \in \mathrm{End}(G)$ then $-\alpha \in \mathrm{End}(G)$ and 0 is always an endomorphism of G. Hence $(\mathrm{End}((G, +)), +, -, 0)$ is an Abelian group and $(\mathrm{End}((G, +)), +, \circ)$ is a ring.

In what follows we use the notation $\alpha\beta$ instead of $\alpha \circ \beta$, 1_G instead of id_G, $\alpha^k = \underbrace{\alpha \circ \cdots \circ \alpha}_{k}$, $k \in \mathbb{N}$, $\alpha^0 = 1_G$, and $n\alpha = \underbrace{\alpha + \cdots + \alpha}_{n}$, $n \geq 1$, for all $\alpha, \beta \in G^G$.

DEFINITION 4.10. Let $(H, \cdot, 1)$ be a group. For each $h \in H$, the *order* of the element h is the smallest $k \in \mathbb{N}$ such that

$$h^k = 1,$$

and we denote it $\mathrm{ord}(h)$. If no such integer k exists, then an element h has an infinite order.

The *exponent* of the group H, notation e_H, is the smallest $n \in \mathbb{N}$ such that $h^n = 1$ for each $h \in H$. It is easy to see that $e_H = \mathrm{lcm}(\{\mathrm{ord}(h);\ h \in H\})$.

By the Lagrange theorem, the order of each element of the group H divides the order of H. It follows that e_H divides $|H|$. If H is a cyclic group then $e_H = |H|$.

LEMMA 4.11. *Let $(G,+)$ be an Abelian group of a finite order and $\alpha \in G^G$. Then $e_G\alpha = 0$ and if moreover $\alpha \in S(G)$ then e_G is the smallest $n \in \mathbb{N}$ such that $n\alpha = 0$.*

PROOF. Since the group G is finite, $e_G \in \mathbb{N}$. The definition of e_G gives that $e_G g = 0$ for any g in G. For all $h \in G$ the following holds:

$$(e_G\alpha)(h) = (\underbrace{\alpha + \cdots + \alpha}_{e_G})(h) = e_G(\alpha(h)) = 0.$$

Suppose that $\alpha \in S(G)$ and there exists $0 < m < e_G$ such that $m\alpha = 0$. Because $0 < m < e_G$, there exists $h \in G$ such that $mh \neq 0$. Put $f = \alpha^{-1}(h) \in G$. Then

$$(m\alpha)(f) = (\underbrace{\alpha + \cdots + \alpha}_{m})(f) = m(\alpha(f)) = mh \neq 0,$$

a contradiction.

□

We fix a finite central quasigroup $(G,*)$. There exists an Abelian group $(G,+)$, $\alpha, \beta \in \mathrm{Aut}((G,+))$, and $c \in G$ such that

$$x * y = \alpha(x) + \beta(y) + c \quad \text{for all } x, y \in G.$$

$*$	x_1	x_2	$\ldots$
y_1	$\alpha(y_1) + \beta(x_1) + c$	$\alpha^2(y_1) + \alpha\beta(x_1) + \alpha(c) + \beta(x_2) + c$	
y_2	$\alpha(y_2) + \beta\alpha(y_1) + \beta^2(x_1) + \beta(c) + c$	$\alpha^2(y_2) + \beta^2(x_2) + (\alpha\beta^2 + \beta\alpha\beta)(x_1) +$ $(\beta\alpha^2 + \alpha\beta\alpha)(y_1) + (\beta\alpha + \beta + \alpha\beta + \alpha + \mathrm{id}_G)(c)$	
$\vdots$			

TABLE 4. The matrix $T_{X,Y,(G,*)}$ for a central quasigroup

DEFINITION 4.12. We define a matrix $A_{\alpha,\beta} = (a_{i,j})_{i,j=1}^{\infty}$ over $\mathrm{End}((G,+))$ by

$$\begin{aligned} a_{1,j} &= \alpha^{j-1} \quad \text{for } j \geq 1, \\ a_{i,1} &= \beta^{i-1} \quad \text{for } i \geq 1, \\ a_{i,j} &= \alpha a_{i,j-1} + \beta a_{i-1,j} \quad \text{for } i, j > 1. \end{aligned}$$

1_G	α	α^2	$\ldots$
β	$\alpha\beta + \beta\alpha$	$\alpha^2\beta + \alpha\beta\alpha + \beta\alpha^2$	
β^2	$\alpha\beta^2 + \beta\alpha\beta + \beta^2\alpha$	$\alpha^2\beta^2 + \alpha\beta\alpha\beta + \alpha\beta^2\alpha + \beta\alpha^2\beta + \beta\alpha\beta\alpha + \beta^2\alpha^2$	
β^3	$\alpha\beta^3 + \beta\alpha\beta^2 + \beta^2\alpha\beta + \beta^3\alpha$		
β^4	$\alpha\beta^4 + \beta\alpha\beta^3 + \beta^2\alpha\beta^2 + \beta^3\alpha\beta + \beta^4\alpha$		
$\vdots$			

TABLE 5. The matrix $A_{\alpha,\beta}$

Using Lemma 4.11 and the fact that $(\mathrm{End}(G,+),+)$ is an Abelian group, notice that elements of the matrix $A_{\alpha,\beta}$ are elements of the group ring $\mathbb{Z}_{e_G}[\mathrm{Aut}(G)]$.

On the set $\mathrm{End}((G,+))$ define a binary operation $\diamond$ by $x \diamond y = \alpha \circ x + \beta \circ y$ for all $x, y \in \mathrm{End}(G)$. Because $\alpha, \beta \in \mathrm{Aut}((G,+))$ and $(\mathrm{End}((G,+)),+,\circ)$ is a ring, Lemma 2.21 says that $(\mathrm{End}((G,+)),\diamond)$ is a quasigroup.

Put $Z = (z_i)_{i=1}^{\infty} = (a_{1,i})_{i=1}^{\infty}$, $W = (w_i)_{i=1}^{\infty} = (0)_{i=1}^{\infty} = 0$. Then we can see that the matrix $\bar{A}_{\alpha,\beta} = (a_{i+1,j})_{i,j=1}^{\infty}$ is the matrix $T_{Z,W,(\mathrm{End}((G,+)),\diamond)}$. Thus all the statements about the periods of matrix rows (4.6–4.9) apply also to the rows of the matrix $\bar{A}_{\alpha,\beta}$.

Because $(G,+)$ is a finite group, $\mathrm{Aut}((G,+))$ is also a finite group. By the Lagrange theorem each element of a finite group has a finite order. Therefore, the first row of the matrix $A_{\alpha,\beta}$ is always periodic, which implies that each row of the matrix $A_{\alpha,\beta}$ is periodic by Corollary 4.9. For each $i \in \mathbb{N}$, let P_i denote the minimal period of the ith row of the matrix $A_{\alpha,\beta}$ and we will keep this notation throughout.

Thus using Corollary 4.9 we have:

COROLLARY 4.13. *For each $i \in \mathbb{N}$, let P_i denote the minimal period of the ith row of the matrix $A_{\alpha,\beta}$. Then the following holds:*

(i) $P_1 = \mathrm{ord}(\alpha)$.

(ii) For each $i > 1$ there exists $k_i \in \{1, 2, \ldots, |G|\}$ such that

$$P_i = k_i \cdot P_{i-1}.$$

(iii) P_i is the smallest multiple of P_{i-1} such that

$$a_{i,P_i} = 0.$$

The matrix $T_{X,Y,(G,*)}$ is closely related to the matrix $A_{\alpha,\beta}$, as can be seen in the next lemma. The reason for the introduction of the matrix $A_{\alpha,\beta}$ is that it is much easier to work with and the periods of T can be estimated by periods of A, see Theorem 4.15.

LEMMA 4.14. *Each element of the matrix $T_{X,Y,(G,*)} = (t_{i,j})_{i,j=1}^{\infty}$ can be expressed using the elements of the matrix $A_{\alpha,\beta} = (a_{i,j})_{i,j=1}^{\infty}$ as*

$$t_{i,j} = \sum_{k=1}^{i}\sum_{l=1}^{j} a_{k,l}(c) + \sum_{k=1}^{i} a_{i-k+1,j}(\alpha(y_k)) + \sum_{l=1}^{j} a_{i,j-l+1}(\beta(x_l)).$$

PROOF. We will use an induction on $i + j$. For $i + j = 2$ we obtain that

$$t_{1,1} = \alpha(y_1) + \beta(x_1) + c = a_{1,1}(\alpha(y_1)) + a_{1,1}(\beta(x_1)) + a_{1,1}(c).$$

Suppose that the statement holds for $t_{1,j-1}$, $j > 1$. Because $\alpha a_{1,l} = a_{1,l+1}$ for each $l \geq 1$, we have

$$\begin{aligned}
t_{1,j} &= t_{1,j-1} * x_j = \alpha(t_{1,j-1}) + \beta(x_j) + c \\
&= \alpha\left(\sum_{l=1}^{j-1} a_{1,l}(c) + a_{1,j-1}(\alpha(y_1)) + \sum_{l=1}^{j-1} a_{1,j-l}(\beta(x_l))\right) + \beta(x_j) + c \\
&= \sum_{l=1}^{j-1} a_{1,l+1}(c) + a_{1,j}(\alpha(y_1)) + \sum_{l=1}^{j-1} a_{1,j-l+1}(\beta(x_l)) + a_{1,1}\beta(x_j) + c \\
&= \sum_{l=2}^{j} a_{1,l}(c) + a_{1,j}(\alpha(y_1)) + \sum_{l=1}^{j-1} a_{1,j-l+1}(\beta(x_l)) + a_{1,j-j+1}\beta(x_j) + a_{1,1}(c) \\
&= \sum_{l=1}^{j} a_{1,l}(c) + a_{1,j}(\alpha(y_1)) + \sum_{l=1}^{j} a_{1,j-l+1}(\beta(x_l)).
\end{aligned}$$

Suppose that the statement holds for $t_{i-1,1}$, $i > 1$. Because $\beta a_{k,1} = a_{k+1,1}$ for each $k \geq 1$, we obtain that

$$\begin{aligned}
t_{i,1} &= y_i * t_{i-1,1} = \alpha(y_i) + \beta(t_{i-1,1}) + c \\
&= \alpha(y_i) + \beta\left(\sum_{k=1}^{i-1} a_{k,1}(c) + \sum_{k=1}^{i-1} a_{i-k,1}(\alpha(y_k)) + a_{i-1,1}(\beta(x_1))\right) + c \\
&= a_{1,1}(\alpha(y_i)) + \sum_{k=1}^{i-1} a_{k+1,1}(c) + \sum_{k=1}^{i-1} a_{i-k+1,1}(\alpha(y_k)) + a_{i,1}(\beta(x_1)) + c \\
&= a_{i-i+1,1}(\alpha(y_i)) + \sum_{k=2}^{i} a_{k,1}(c) + \sum_{k=1}^{i-1} a_{i-k+1,1}(\alpha(y_k)) + a_{i,1}(\beta(x_1)) + a_{1,1}(c) \\
&= \sum_{k=1}^{i} a_{k,1}(c) + \sum_{k=1}^{i} a_{i-k+1,1}(\alpha(y_k)) + a_{i,1}(\beta(x_1)).
\end{aligned}$$

Now, for $i, j > 1$,

$$\begin{aligned}
\alpha\left(\sum_{k=1}^{i}\sum_{l=1}^{j-1} a_{k,l}\right) + \beta\left(\sum_{k=1}^{i-1}\sum_{l=1}^{j} a_{k,l}\right) + 1_G &= \sum_{k=1}^{i}\sum_{l=1}^{j-1} \alpha a_{k,l} + \sum_{k=1}^{i-1}\sum_{l=1}^{j} \beta a_{k,l} + 1_G \\
&= \sum_{k=0}^{i-1}\sum_{l=1}^{j-1} \alpha a_{k+1,l} + \sum_{k=1}^{i-1}\sum_{l=0}^{j-1} \beta a_{k,l+1} + 1_G \\
&= \sum_{k=1}^{i-1}\sum_{l=1}^{j-1} (\alpha a_{k+1,l} + \beta a_{k,l+1}) + \sum_{l=1}^{j-1} \alpha a_{1,l} + \sum_{k=1}^{i-1} \beta a_{k,1} + 1_G \qquad (14) \\
&= \sum_{k=1}^{i-1}\sum_{l=1}^{j-1} a_{k+1,l+1} + \sum_{l=1}^{j-1} a_{1,l+1} + \sum_{k=1}^{i-1} a_{k+1,1} + a_{1,1} \\
&= \sum_{k=0}^{i-1}\sum_{l=0}^{j-1} a_{k+1,l+1} = \sum_{k=1}^{i}\sum_{l=1}^{j} a_{k,l}.
\end{aligned}$$

Assume that the statement holds for $t_{i,j-1}$ and $t_{i-1,j}$, where $i, j > 1$. Then

$$\begin{aligned}
t_{i,j} &= t_{i,j-1} * t_{i-1,j} = \alpha(t_{i,j-1}) + \beta(t_{i-1,j}) + c \\
&= \alpha\left(\sum_{k=1}^{i}\sum_{l=1}^{j-1} a_{k,l}(c) + \sum_{k=1}^{i} a_{i-k+1,j-1}(\alpha(y_k)) + \sum_{l=1}^{j-1} a_{i,j-l}(\beta(x_l))\right) \\
&\quad + \beta\left(\sum_{k=1}^{i-1}\sum_{l=1}^{j} a_{k,l}(c) + \sum_{k=1}^{i-1} a_{i-k,j}(\alpha(y_k)) + \sum_{l=1}^{j} a_{i-1,j-l+1}(\beta(x_l))\right) + c \\
&= \left(\alpha\left(\sum_{k=1}^{i}\sum_{l=1}^{j-1} a_{k,l}\right) + \beta\left(\sum_{k=1}^{i-1}\sum_{l=1}^{j} a_{k,l}\right) + 1_G\right)(c) \\
&\quad + \sum_{k=1}^{i-1} \left(\alpha a_{i-k+1,j-1} + \beta a_{i-k,j}\right)(\alpha(y_k)) + \alpha a_{1,j-1}(\alpha(y_i)) \\
&\quad + \sum_{l=1}^{j-1} \left(\alpha a_{i,j-l} + \beta a_{i-1,j-l+1}\right)(\beta(x_l)) + \beta a_{i-1,1}(\beta(x_j)).
\end{aligned}$$

Using the definition of the matrix $A_{\alpha,\beta}$ and (14) we obtain that:

$$\begin{aligned} t_{i,j} &= \sum_{k=1}^{i}\sum_{l=1}^{j} a_{k,l}(c) + \sum_{k=1}^{i-1} a_{i-k+1,j}(\alpha(y_k)) + \sum_{l=1}^{j-1} a_{i,j-l+1}(\beta(x_l)) + a_{1,j}(\alpha(y_i)) + a_{i,1}(\beta(x_j)) \\ &= \sum_{k=1}^{i}\sum_{l=1}^{j} a_{k,l}(c) + \sum_{k=1}^{i} a_{i-k+1,j}(\alpha(y_k)) + \sum_{l=1}^{j} a_{i,j-l+1}(\beta(x_l)). \end{aligned}$$

□

THEOREM 4.15. *Suppose that a sequence $X = (x_k)_{k=1}^{\infty} \in G^{\mathbb{N}}$ is periodic with the minimal period P_X. Then for each $i \in \mathbb{N}$,*

$$e_G \cdot \operatorname{lcm}(P_X, P_i)$$

is a period of the ith row of the matrix $T_{X,Y,(G,*)}$.

PROOF. Fix $i, j \geq 1$. Put $P = e_G \operatorname{lcm}(P_X, P_i)$. By Lemma 4.14 we have

$$t_{i,j} = \sum_{k=1}^{i}\sum_{l=1}^{j} a_{k,l}(c) + \sum_{k=1}^{i} a_{i-k+1,j}(\alpha(y_k)) + \sum_{l=1}^{j} a_{i,j-l+1}(\beta(x_l))$$

and

$$t_{i,j+P} = \sum_{k=1}^{i}\sum_{l=1}^{j+P} a_{k,l}(c) + \sum_{k=1}^{i} a_{i-k+1,j+P}(\alpha(y_k)) + \sum_{l=1}^{j+P} a_{i,j+P-l+1}(\beta(x_l)).$$

Since P is a multiple of P_i, $a_{i,l+P} = a_{i,l}$ for each $l \geq 1$. By Corollary 4.13, P_k divides P_i for each $1 \leq k \leq i$, and hence $P = e_G r P_i = e_G r_k P_k$ for some $r_k \in \mathbb{N}$. This implies that $a_{k,j+P} = a_{k,j}$ for $1 \leq k \leq i$. Therefore

$$\begin{aligned} t_{i,j+P} - t_{i,j} &= \sum_{k=1}^{i}\sum_{l=1}^{j+P} a_{k,l}(c) + \sum_{k=1}^{i} a_{i-k+1,j+P}(\alpha(y_k)) + \sum_{l=1}^{j+P} a_{i,j+P-l+1}(\beta(x_l)) \\ &\quad - \left(\sum_{k=1}^{i}\sum_{l=1}^{j} a_{k,l}(c) + \sum_{k=1}^{i} a_{i-k+1,j}(\alpha(y_k)) + \sum_{l=1}^{j} a_{i,j-l+1}(\beta(x_l)) \right) \\ &= \sum_{k=1}^{i}\sum_{l=j+1}^{j+P} a_{k,l}(c) + \sum_{l=j+1}^{j+P} a_{i,j+P-l+1}(\beta(x_l)) \\ &= \sum_{k=1}^{i}\sum_{l=1}^{P} a_{k,l+j}(c) + \sum_{l=1}^{P} a_{i,P-l+1}(\beta(x_{l+j})) \end{aligned} \tag{15}$$

and

$$\begin{aligned} \sum_{l=1}^{P} a_{k,l+j}(c) &= \sum_{l=1}^{P_k} a_{k,l+j}(c) + \sum_{l=P_k+1}^{2P_k} a_{k,l+j}(c) + \cdots + \sum_{l=P-P_k+1}^{P} a_{k,l+j}(c) \\ &= \sum_{m=0}^{e_G r_k - 1}\sum_{l=1}^{P_k} a_{k,l+j+mP_k}(c) = \sum_{m=0}^{e_G r_k - 1}\sum_{l=1}^{P_k} a_{k,l+j}(c) \\ &= e_G r_k \sum_{l=1}^{P_k} a_{k,l+j}(c) = 0. \end{aligned} \tag{16}$$

Further,

$$\begin{aligned}
\sum_{l=1}^{P} a_{i,P-l+1}\beta(x_{l+j}) &= \sum_{l=1}^{e_G \operatorname{lcm}(P_X,P_i)} a_{i,e_G \operatorname{lcm}(P_X,P_i)-l+1}\beta(x_{l+j}) \\
&= \sum_{m=0}^{e_G-1} \sum_{l=m \operatorname{lcm}(P_X,P_i)+1}^{(m+1) \operatorname{lcm}(P_X,P_i)} a_{i,e_G \operatorname{lcm}(P_X,P_i)-l+1}\beta(x_{l+j}) \\
&= \sum_{m=0}^{e_G-1} \sum_{l=1}^{\operatorname{lcm}(P_X,P_i)} a_{i,e_G \operatorname{lcm}(P_X,P_i)-l-m \operatorname{lcm}(P_X,P_i)+1}\beta(x_{l+j+m \operatorname{lcm}(P_X,P_i)}) \\
&= \sum_{m=0}^{e_G-1} \sum_{l=1}^{\operatorname{lcm}(P_X,P_i)} a_{i,(e_G-m) \operatorname{lcm}(P_X,P_i)-l+1}\beta(x_{l+j}) \\
&= \sum_{m=0}^{e_G-1} \sum_{l=1}^{\operatorname{lcm}(P_X,P_i)} a_{i,\operatorname{lcm}(P_X,P_i)-l+1}\beta(x_{l+j}) \\
&= e_G \sum_{l=1}^{\operatorname{lcm}(P_X,P_i)} a_{i,\operatorname{lcm}(P_X,P_i)-l+1}\beta(x_{l+j}) = 0.
\end{aligned} \tag{17}$$

Equations (16) and (17) together with (15) give that $t_{i,j+P} = t_{i,j}$ for each $j \geq 1$, which implies that P is a period of the ith row of the matrix T.

□

Observe that each element $a_{i,j}$ of the matrix $A_{\alpha,\beta}$, where $i > 1$ and $j \geq 1$, can be expressed using the elements in the previous (i.e. $(i-1)$th) row in the following way:

$$\begin{aligned}
a_{i,j} &= \alpha a_{i,j-1} + \beta a_{i-1,j} \\
&= \alpha^2 a_{i,j-2} + \alpha\beta a_{i-1,j-1} + \beta a_{i-1,j} \\
&= \alpha^3 a_{i,j-3} + \alpha^2\beta a_{i-1,j-2} + \alpha\beta a_{i-1,j-1} + \beta a_{i-1,j} \\
&\vdots \\
&= \alpha^{j-1} a_{i,1} + \sum_{k=2}^{j} \alpha^{j-k}\beta a_{i-1,k} \\
&= \alpha^{j-1}\beta a_{i-1,1} + \sum_{k=2}^{j} \alpha^{j-k}\beta a_{i-1,k} \\
&= \sum_{k=1}^{j} \alpha^{j-k}\beta a_{i-1,k}.
\end{aligned} \tag{18}$$

LEMMA 4.16. *For each $i > 1$, P_i divides $e_G \cdot P_{i-1}$.*

PROOF. Fix $i > 1$. By Corollary 4.13, $\mathrm{ord}(\alpha)$ divides P_{i-1}, hence $\alpha^{P_{i-1}} = 1_G$. Using (18) we obtain for any $j \geq 1$

$$\begin{aligned}
a_{i,e_G P_{i-1}+j} &= \sum_{k=1}^{e_G P_{i-1}+j} \alpha^{e_G P_{i-1}+j-k}\beta a_{i-1,k} \\
&= \sum_{k=1}^{j} \alpha^{e_G P_{i-1}}\alpha^{j-k}\beta a_{i-1,k} \\
&\quad + \sum_{m=0}^{e_G-1} \sum_{k=mP_{i-1}+j+1}^{(m+1)P_{i-1}+j} \alpha^{(e_G-m-1)P_{i-1}}\alpha^{(m+1)P_{i-1}+j-k}\beta a_{i-1,k} \\
&= \sum_{k=1}^{j} \alpha^{j-k}\beta a_{i-1,k} + \sum_{m=0}^{e_G-1} \sum_{k=mP_{i-1}+j+1}^{(m+1)P_{i-1}+j} \alpha^{(m+1)P_{i-1}+j-k}\beta a_{i-1,k} \\
&= a_{i,j} + \sum_{m=0}^{e_G-1} \sum_{k=j+1}^{P_{i-1}+j} \alpha^{P_{i-1}+j-k}\beta a_{i-1,k+mP_{i-1}} \\
&= a_{i,j} + \sum_{m=0}^{e_G-1} \sum_{k=j+1}^{P_{i-1}+j} \alpha^{P_{i-1}+j-k}\beta a_{i-1,k} \\
&= a_{i,j} + e_G \sum_{k=j+1}^{P_{i-1}+j} \alpha^{P_{i-1}+j-k}\beta a_{i-1,k} = a_{i,j},
\end{aligned}$$

where the last equality follows from Lemma 4.11. Because $e_G P_{i-1}$ is a period of the ith row, P_i divides $e_G P_{i-1}$ by Fact 4.5.

□

COROLLARY 4.17. *For each $i > 1$, $P_i = d \cdot P_{i-1}$, where d divides e_G.*

From Corollary 4.13 and Corollary 4.17 we obtain

COROLLARY 4.18. *Let p be a prime, $r \in \mathbb{N}$, and $e_G = p^r$. Then there is a non-decreasing sequence $(c_i)_{i=1}^{\infty}$, $c_i \in \mathbb{N} \cup \{0\}$, such that*

$$P_i = \mathrm{ord}(\alpha) \cdot p^{c_i} \quad \text{for each } i \geq 1,$$

where $c_1 = 0$ and $0 \leq c_{j+1} - c_j \leq r$ for each $j \geq 1$.

LEMMA 4.19. *For each $i \in \mathbb{N}$, $P_i \geq i$.*

PROOF. Suppose that $\alpha x + \beta y = 0$ for some $x, y \in (\mathrm{End}((G,+)),+,0)$. Then $x = 0$ if and only if $y = 0$. Indeed, if $y = 0$ then $\alpha x = 0$ and using the fact that $\alpha \in \mathrm{Aut}((G,+))$ we have $x = 0$. Similarly for the converse.

By Corollary 4.13, $a_{j,P_i} = a_{j,P_j} = 0$ for all $2 \leq j \leq i$. Applying repeatedly the statement from the previous paragraph we obtain that for $2 \leq j \leq i$ we have $a_{j,k} = 0$ for $P_i - j + 2 \leq k \leq P_i$ and $a_{j,P_i-j+1} \neq 0$. Since $a_{i,1} = \beta^{i-1} \neq 0$, $P_i - i + 2 \geq 2$.

□

Let p be a prime and

$$G_p = \{g \in G;\ p^n g = 0 \text{ for some } n \in \mathbb{N}\}.$$

If $p^n a = 0$ and $p^m b = 0$ then $p^n(-a) = 0$, $p^{\max(m,n)}(a+b) = 0$, and hence G_p is a subgroup of G.

Because the group G is a finite Abelian group, there exists $n \in \mathbb{N}$ and pairwise distinct primes $p_1, \ldots, p_n$ such that

$$G = \bigoplus_{k=1}^{n} G_{p_k}$$

and

$$\mathrm{Aut}(G) = \prod_{k=1}^{n} \mathrm{Aut}(G_{p_k}),$$

where $\varphi(g) = ((\varphi_k)_{k=1}^n)((g_k)_{k=1}^n) = (\varphi_k(g_k))_{k=1}^n$ for each $g = (g_p)_{k=1}^n \in G$ and $\varphi = (\varphi_p)_{k=1}^n \in \mathrm{Aut}(G)$. (This result can be found e.g. in [**D3**, p. 39 and 163].)

Thus $\alpha = (\alpha_k)_{k=1}^n$, $\beta = (\beta_k)_{k=1}^n$ and $c = (c_k)_{k=1}^n$ for some $\alpha_k, \beta_k \in \mathrm{Aut}(G_{p_k})$ and $c_k \in G_{p_k}$.

Let $A_{\alpha,\beta} = (a_{i,j})_{i,j=0}^{\infty}$, $A_{\alpha_k,\beta_k} = (a_{i,j}^k)_{i,j=0}^{\infty}$, and P_i^k denote the minimal period of the ith row of the matrix A_{α_k,β_k}. It is easy to see that $a_{i,j} = \begin{pmatrix} a_{i,j}^1 \\ \vdots \\ a_{i,j}^n \end{pmatrix}$. This implies that

$$P_i = \mathrm{lcm}(P_i^1, \ldots, P_i^n). \tag{19}$$

For each $1 \leq k \leq n$, define $(G_{p_k}, *_k)$ such that $a *_k b = \alpha_k(a) + \beta_k(b) + c_k$ for all $a, b \in G_{p_k}$. Theorem 2.32 together with the fact that G_{p_k} is an Abelian group gives that $(G_{p_k}, *_k)$ is a central quasigroup. Further, for each $x = (x_k)_{k=1}^n$ and $y = (y_k)_{k=1}^n \in G$,

$$x * y = \alpha(x) + \beta(y) + c = \begin{pmatrix} \alpha_1(x_1) + \beta_1(y_1) + c_1 \\ \vdots \\ \alpha_n(x_n) + \beta_n(y_n) + c_n \end{pmatrix} = \begin{pmatrix} x_1 *_1 y_1 \\ \vdots \\ x_n *_n y_n \end{pmatrix}.$$

Let $T_{(G,*)} = (t_{i,j})_{i,j=0}^{\infty}$, $T_{(G_{p_k},*_k)} = (t_{i,j}^k)_{i,j=0}^{\infty}$, and Q_i, Q_i^k denote the minimal periods of the ith row of the matrix $T_{(G,*)}$ and $T_{(G_{p_k},*_k)}$, respectively. Then it is easy to show that $t_{i,j} = \begin{pmatrix} t_{i,j}^1 \\ \vdots \\ t_{i,j}^n \end{pmatrix}$ and hence $Q_i = \mathrm{lcm}(Q_i^1, \ldots, Q_i^n)$.

Since for each $1 \leq k \leq n$ there exist $r_k \in \mathbb{N}$ such that $e_{G_{p_k}} = p_k^{r_k}$, it suffices to compute the periods for the central quasigroup $(G, *)$ such that e_G is a prime power.

3. Medial quasigroups

In this section the quasigroup $(G, *)$ will be a fixed medial quasigroup of finite order. Thus there exists an Abelian group $(G, +)$, $\alpha, \beta \in \mathrm{Aut}((G, +))$, and $c \in G$ such that $x * y = \alpha(x) + \beta(y) + c$ for all $x, y \in G$ and the automorphisms α and β commute.

LEMMA 4.20. *Each element of the matrix $A_{\alpha,\beta} = (a_{i,j})_{i,j=1}^{\infty}$ can be expressed as*

$$a_{i,j} = \binom{i+j-2}{i-1} \alpha^{j-1} \beta^{i-1}.$$

PROOF. We will use an induction on $i + j$. The statement is obvious for $i = 1$ or $j = 1$. Suppose that $a_{i+1,j} = \binom{i+j-1}{i} \alpha^{j-1} \beta^i$ and $a_{i,j+1} = \binom{i+j-1}{i-1} \alpha^j \beta^{i-1}$. Using the definition of

the matrix $A_{\alpha,\beta}$ and the fact that automorphisms α, β commute, we obtain:

$$\begin{aligned} a_{i+1,j+1} &= \alpha a_{i+1,j} + \beta a_{i,j+1} \\ &= \alpha\left(\binom{i+j-1}{i}\alpha^{j-1}\beta^i\right) + \beta\left(\binom{i+j-1}{i-1}\alpha^j\beta^{i-1}\right) \\ &= \binom{i+j-1}{i}\alpha^j\beta^i + \binom{i+j-1}{i-1}\alpha^j\beta^i \\ &= \binom{i+j}{i}\alpha^j\beta^i. \end{aligned}$$

□

COROLLARY 4.21. *Let $X, Y \in G^{\mathbb{N}}$. Each element of the matrix $T_{X,Y,(G,*)} = (t_{i,j})_{i,j=1}^{\infty}$ can be expressed as*

$$\begin{aligned} t_{i,j} = &\sum_{k=0}^{i-1}\sum_{l=0}^{j-1}\binom{k+l}{k}\alpha^l\beta^k(c) \\ &+ \sum_{k=1}^{i}\binom{i-k+j-1}{i-k}\alpha^j\beta^{i-k}(y_k) \\ &+ \sum_{l=1}^{j}\binom{i+j-l-1}{i-1}\alpha^{j-l}\beta^i(x_l). \end{aligned}$$

PROOF. Combine Lemma 4.14 with the previous lemma.

□

Now we will try to find the minimal period of the matrix $A_{\alpha,\beta}$, where $\alpha\beta = \beta\alpha$.
Corollary 4.13 says that P_i, $i \geq 2$, is the smallest multiple of P_{i-1} such that

$$a_{i,P_i} = \binom{P_i+i-2}{i-1}\alpha^{P_i-1}\beta^{i-1} = 0. \tag{20}$$

The last identity holds if and only if $\binom{P_i+i-2}{i-1}$ is a multiple of e_G (Lemma 4.11).

P_1 and P_2 are easily determined: Corollary 4.13 gives us that $P_1 = \mathrm{ord}(\alpha)$. If $i = 2$ then $\binom{P_i+i-2}{i-1} = P_2$. The smallest positive integer which is a multiple of $\mathrm{ord}(\alpha)$ and a multiple of e_G is $P_2 = \mathrm{lcm}(e_G, \mathrm{ord}(\alpha))$.

According to the remarks at the end of the previous section we can suppose that $e_G = p^r$, where p is a prime and $r \in \mathbb{N}$. By Theorem 3.4, $e_G = p^r$ divides $\binom{P_i+i-2}{i-1}$ if and only if $C_p(P_i - 1, i - 1) \geq r$. Using this fact and (20) we obtain:

LEMMA 4.22. *Let p be a prime, $r \in \mathbb{N}$ and $e_G = p^r$. Then P_i, $i \geq 2$, is the smallest multiple of P_{i-1} such that $C_p(P_i - 1, i - 1) \geq r$.*

We will show that the period of rows, whose indices are between certain powers of p, does not change.

LEMMA 4.23. *Let p be a prime, $r \in \mathbb{N}$ and $e_G = p^r$. Then for each $s \geq 0$,*

$$P_j = P_{p^s+1} \quad \textit{for } p^s + 1 \leq j \leq p^{s+1}.$$

PROOF. Fix $s \geq 0$. Lemma 4.22 says that $C_p(P_{p^s+1} - 1, p^s) \geq r$.
The p-adic representation of p^s is

$$p^s = (1\underbrace{0\ldots0}_{s})_p.$$

Consider a number $a \in \mathbb{N}$ with p-adic representation

$$a = (a_s a_{s-1} \dots a_0)_p, \quad a_s \neq 0. \tag{21}$$

Then $C_p(P_{p^s+1} - 1, a) \geq C_p(P_{p^s+1} - 1, p^s) \geq r$. Because each natural number between p^s and $p^{s+1} - 1$ is of the form (21), using Lemma 4.22 we obtain $P_j = P_{p^s+1}$ for $p^s + 1 \leq j \leq p^{s+1}$.

□

LEMMA 4.24. *Let p be a prime, $r \in \mathbb{N}$ and $e_G = p^r$. If $s \geq 0$ and $C_p(P_{p^s+1} - 1, p^s) = m \geq r$ then*

$$P_j = P_{p^s+1} \quad \textit{for } p^s + 1 \leq j \leq p^{s+m-r+1}$$

and

$$P_{p^{s+m-r+1}+1} \neq P_{p^s+1}.$$

PROOF. Use repeatedly Lemma 4.23, Fact 3.6 and Lemma 4.22.

□

Next we show that the periods of successive rows can increase only by a factor of p.

LEMMA 4.25. *Let p be a prime, $r \in \mathbb{N}$ and $e_G = p^r$. If $P_{p^s+1} \neq P_{p^{s+1}+1}$ for some $s \geq 0$ then $P_{p^{s+1}+1} = pP_{p^s+1}$.*

PROOF. Using Fact 3.7 together with Lemma 4.22 we obtain $C_p(pP_{p^s+1} - 1, p^{s+1}) = C_p(P_{p^s+1} - 1, p^s) \geq r$. This implies (by the analysis in the beginning of this section and Lemma 4.23) that pP_{p^s+1} is a period of the $(p^{s+1} + 1)$th row. Since $P_{p^{s+1}+1}$ is a multiple of $P_{p^{s+1}} = P_{p^s+1}$ (Corollary 4.13, Lemma 4.23), we have:

$$pP_{p^s+1} = kP_{p^{s+1}+1} = klP_{p^s+1}, \quad k, l \in \mathbb{N}.$$

As p is a prime and $k \neq p$ (because $P_{p^s+1} \neq P_{p^{s+1}+1}$), it follows that $l = p$, which proves our claim.

□

The following theorem summarises the results of this section.

THEOREM 4.26. *Let p be a prime, $r \in \mathbb{N}$, $e_G = p^r$, and $t, q \in \mathbb{N}$ be such that $\operatorname{lcm}(p^r, \operatorname{ord}(\alpha)) = p^t q$, where $t \geq r$ and $p \nmid q$. Then*

$$P_1 = \operatorname{ord}(\alpha) \quad \textit{and} \quad P_i = p^{\max\{0, r-t-1+\lceil \log_p i \rceil\}} \operatorname{lcm}(p^r, \operatorname{ord}(\alpha)) \quad \textit{for } i > 1.$$

PROOF. $P_1 = \operatorname{ord}(\alpha)$ by Corollary 4.13.

The statement of the theorem can be reformulated as

$$P_i = \operatorname{lcm}(p^r, \operatorname{ord}(\alpha)) \quad \text{for } 2 \leq i \leq p^{t-r+1}, \tag{22}$$

$$P_i = p^j \operatorname{lcm}(p^r, \operatorname{ord}(\alpha)) \quad \text{for } p^{t-r+j} + 1 \leq i \leq p^{t-r+j+1},\ j \geq 1. \tag{23}$$

Indeed, if $2 \leq i \leq p^{t-r+1}$ then $r - t - 1 + \log_p i \leq 0$ and $\max\{0, r - t - 1 + \lceil \log_p i \rceil\} = 0$. For $p^{t-r+j} + 1 \leq i \leq p^{t-r+j+1}$, where $j \geq 1$, we obtain that $j - 1 < r - t - 1 + \log_p i \leq j$ and $\max\{0, r - t - 1 + \lceil \log_p i \rceil\} = j$.

Now we will prove (22). Lemma 4.23 says that

$$P_i = P_2 = \operatorname{lcm}(p^r, \operatorname{ord}(\alpha)) \quad \text{for } i = 2, \dots, p.$$

Because $p \nmid q$, the p-adic representation of q is $q = (q_k q_{k-1} \dots q_0)_p$, $0 < q_0 < p$ and $p^t q - 1 = (q_k q_{k-1} \dots (q_0 - 1) \underbrace{(p-1) \dots (p-1)}_{t})_p$. Using this together with Fact 3.5 we get

$$C_p(P_2 - 1, 1) = C_p(\operatorname{lcm}(p^r, \operatorname{ord}(\alpha)) - 1, 1) = C_p(p^t q - 1, 1) = t.$$

Lemma 4.24 gives us that

$$P_i = P_2 \quad \text{for } 2 \le i \le p^{t-r+1} \quad \text{and} \quad P_{p^{t-r+1}+1} \neq P_2. \tag{24}$$

To prove (23) we use an induction on j. Applying Lemma 4.25 on (24) we obtain

$$P_{p^{t-r+1}+1} = pP_2,$$

which together with Lemma 4.23 gives

$$P_i = pP_2, \quad p^{t-r+1}+1 \le i \le p^{t-r+2}.$$

Suppose that for some $j > 1$

$$P_i = p^j \operatorname{lcm}(p^r, \operatorname{ord}(\alpha)) = p^{j+t}q \quad \text{for } p^{t-r+j}+1 \le i \le p^{t-r+j+1}. \tag{25}$$

We can compute

$$\begin{aligned} r &= C_p(p^{j+t-1}q-1,1) - (j+t-r-1) = C_p(p^{j+t-1}q-1, p^{j+t-r-1}) \\ &= C_p(p^{j+t}q-1, p^{j+t-r}) = C_p(P_{p^{j+t-r}+1}-1, p^{j+t-r}), \end{aligned}$$

where we used Fact 3.5, Fact 3.6, Fact 3.7 and the assumption (25). By Lemma 4.24 we have that $P_{p^{j+t-r+1}+1} \neq P_{p^{j+t-r}+1}$. Hence, using Lemma 4.25, $P_{p^{j+t-r+1}+1} = pP_{p^{j+t-r}+1} = p^{j+1}\operatorname{lcm}(p^r, \operatorname{ord}(\alpha))$. Lemma 4.23 then implies

$$P_i = P_{p^{j+t-r+1}+1} = p^{j+1}\operatorname{lcm}(p^r, \operatorname{ord}(\alpha)) \quad \text{for } p^{j+t-r+1}+1 \le i \le p^{j+t-r+2}.$$

□

Corollary 4.27. *Let p be a prime, $r \in \mathbb{N}$, $e_G = p^r$, and $t, q \in \mathbb{N}$ be such that $\operatorname{lcm}(p^r, \operatorname{ord}(\alpha)) = p^t q$, where $p \nmid q$. Then*

$$p^{r-1}qi \le P_i \le p^r q(i-1) \quad \textit{for } i \ge p^{t-r+1}.$$

Moreover these estimates are sharp in the sense that there are no better affine estimates.

Proof. Using $\log_p i \le \lceil \log_p i \rceil$ we have $p^{r-1}qi \le P_i$. For $p^s + 1 \ge p^{t-r+1}$, we have $P_{p^s+1} = p^{r-1}qp^{\lceil \log_p(p^s+1)\rceil} = p^{r-1}qp^{s+1} = p^r q p^s$. This means that $P_i = p^r q(i-1)$ for $i = p^s + 1$. Since P_i as the function of i is constant for $p^s + 1 \le i \le p^{s+1}$ and the function $p^r q(i-1)$ is an increasing function, we obtain the rest of the statement.

□

Corollary 4.28. *Let $e_G = p_1^{r_1} \cdots p_n^{r_n}$, where p_k are distinct primes. Let $\alpha = (\alpha_k)_{k=1}^n \in \operatorname{Aut}(G) = \prod_{k=1}^n \operatorname{Aut}(G_{p_k})$ and for $1 \le k \le n$ let $\operatorname{ord}(\alpha_k) = q_k p_1^{t_1^k} \cdots p_n^{t_n^k}$, where $t_j^k \in \mathbb{N} \cup \{0\}$ and $p_j \nmid q_k$ for all $1 \le j, k \le n$. Then*

$$P_i = \prod_{k=1}^n q_k p_k^{r_k - 1 + \lceil \log_{p_k} i \rceil}$$

for all i large enough such that $\lceil \log_{p_j} i \rceil \ge \max\{r_j, t_j^1, \ldots, t_j^n\} - r_j + 1$ for each $1 \le j \le n$.

Proof. The group $(G, +)$ is decomposed as $G = \bigoplus_{k=1}^n G_{p_k}$, where $e_{G_{p_k}} = p_k^{r_k}$. Further,

$$\operatorname{lcm}(p_k^{r_k}, \operatorname{ord}(\alpha_k)) = p_k^{\max\{r_k, t_k^k\}} q_k \prod_{\substack{j=1 \\ j \neq k}}^n p_j^{t_j^k}.$$

Hence by Theorem 4.26 for each $1 \le k \le n$

$$P_i^k = p_k^{r_k - 1 + \lceil \log_{p_k} i \rceil} q_k \prod_{\substack{j=1 \\ j \neq k}}^n p_j^{t_j^k} \qquad \text{for } \lceil \log_{p_k} i \rceil \ge \max\{r_k, t_k^k\} - r_k + 1.$$

By (19), $P_i = \operatorname{lcm}(P_i^1, \dots, P_i^n)$. Therefore if $\lceil \log_{p_j} i \rceil \geq \max\{r_j, t_j^1, \dots, t_j^n\} - r_j + 1$ for each $1 \leq j \leq n$ then

$$P_i = \prod_{k=1}^{n} q_k p_k^{r_k - 1 + \lceil \log_{p_k} i \rceil}.$$

□

COROLLARY 4.29. *Let $e_G = p_1^{r_1} \cdots p_n^{r_n}$, where p_k are distinct primes. Let $\alpha = (\alpha_k)_{k=1}^n \in \operatorname{Aut}(G) = \prod_{k=1}^n \operatorname{Aut}(G_{p_k})$ and for $1 \leq k \leq n$ let $\operatorname{ord}(\alpha_k) = q_k p_1^{t_1^k} \cdots p_n^{t_n^k}$, where $t_j^k \in \mathbb{N} \cup \{0\}$ and $p_j \nmid q_k$ for all $1 \leq j, k \leq n$. Then for all i large enough*

$$i^n \prod_{k=1}^{n} q_k p_k^{r_k - 1} \leq P_i < i^n \prod_{k=1}^{n} q_k p_k^{r_k}.$$

Using Theorem 4.15 we obtain

COROLLARY 4.30. *Let $e_G = p_1^{r_1} \cdots p_n^{r_n}$, where p_k are distinct primes. Denote by Q_i the minimal period of the ith row of the matrix $T_{X,Y,(G,*)}$. Then there is a constant $C > 0$ such that $Q_i < C \cdot i^n$ holds for all sufficiently large i.*

4. Central quasigroups related to the dihedral groups

In this section we will consider a quasigroup $(G, *)$ which is central but non-medial and has some additional properties. Since $(G, *)$ is central, there exists an Abelian group $(G, +)$, $\alpha, \beta \in \operatorname{Aut}((G, +))$, and $c \in G$ such that $x * y = \alpha(x) + \beta(y) + c$ for all $x, y \in G$. Further, we suppose that $\alpha\beta \neq \beta\alpha$ (as medial quasigroups were already studied in the previous section). Finally, in this section we will assume that α, β generate a dihedral group. Therefore α and β satisfy one of these conditions:

(C1) $\operatorname{ord}(\alpha) = n > 2$, $\operatorname{ord}(\beta) = 2$, and $\beta\alpha^m = \alpha^{-m}\beta$ for all $m \in \mathbb{Z}$,
(C2) $\operatorname{ord}(\alpha) = 2$, $\operatorname{ord}(\beta) = n > 2$, and $\alpha\beta^m = \beta^{-m}\alpha$ for all $m \in \mathbb{Z}$,
(C3) $\operatorname{ord}(\alpha) = \operatorname{ord}(\beta) = 2$ and $\operatorname{ord}(\alpha\beta) = \operatorname{ord}(\beta\alpha) = n > 2$.

Indeed, recall that a *dihedral group* D_{2n} is the symmetry group of an n-sided regular polygon for $n > 1$. It consists of rotations and reflections. The order of all reflections is 2 and the following rules hold: The rotations commute, a rotation composed with a reflection as well as a reflection composed with a rotation is a reflection, and a composition of two reflections is a rotation.

So if α, β generate a dihedral group, there are four possibilities:

- α and β are both rotations. This would mean that $\alpha\beta = \beta\alpha$, which is forbidden.
- α is a rotation and β is a reflection. Because $\alpha\beta$ is a reflection, $\operatorname{ord}(\alpha\beta) = 2$. Therefore $\operatorname{ord}(\beta) = 2$ and $\operatorname{ord}(\alpha) > 2$ (the case $\operatorname{ord}(\alpha) \leq 2$ implies $\alpha\beta = \beta\alpha$). It is easy to show that from $\beta^2 = 1$ and $(\alpha\beta)^2 = 1$ it follows that $\beta\alpha^m = \alpha^{-m}\beta$ for all $m \in \mathbb{Z}$ and hence (C1) holds.
- α is a reflection and β is a rotation. Then $\operatorname{ord}(\alpha) = 2$, $\operatorname{ord}(\beta) > 2$ and $\alpha\beta^m = \beta^{-m}\alpha$ for all $m \in \mathbb{Z}$ as in the previous case. Thus (C2) holds.
- α and β are both reflections. Therefore $\operatorname{ord}(\alpha) = \operatorname{ord}(\beta) = 2$ and $\alpha\beta$ is a rotation. If $\operatorname{ord}(\alpha\beta) \leq 2$ then α and β commute. Thus $\operatorname{ord}(\alpha\beta) > 2$ and (C3) is satisfied.

In the following several statements we try to express the elements of the matrix $A_{\alpha,\beta}$ using additional properties of the automorphisms α and β.

REMARK 4.31. Notice that $(A_{\alpha,\beta})^T = A_{\beta,\alpha}$. Since the conditions (C1) and (C2) are symmetric to each other, we will formulate the statements considering (C1) or (C2) only for the condition (C1). The analogous statements for (C2) can be obtained by switching i with j and α with β.

LEMMA 4.32. *Let $A_{\alpha,\beta} = (a_{i,j})_{i,j=1}^{\infty}$. Suppose that $\beta\alpha^m = \alpha^{-m}\beta$ for each $m \in \mathbb{Z}$. Then, for $j \geq 0$ and $i \geq 1$,*

$$a_{i+1,j+1} = \sum_{k=0}^{j} \binom{k + \left\lfloor \frac{i-1}{2} \right\rfloor}{\left\lfloor \frac{i-1}{2} \right\rfloor} \binom{j - k + \left\lfloor \frac{i}{2} \right\rfloor}{\left\lfloor \frac{i}{2} \right\rfloor} \alpha^{j-2k}\beta^i.$$

PROOF. We use an induction on $i + j$.
First, if $j = 0$ then for $i \geq 1$

$$a_{i+1,1} = \beta^i = \binom{0 + \left\lfloor \frac{i-1}{2} \right\rfloor}{\left\lfloor \frac{i-1}{2} \right\rfloor} \binom{0 + \left\lfloor \frac{i}{2} \right\rfloor}{\left\lfloor \frac{i}{2} \right\rfloor} \alpha^0\beta^i$$

and the statement holds. Further, for $i = 1$ using (18) and then the fact that $\beta\alpha^k = \alpha^{-k}\beta$ we obtain

$$\begin{aligned} a_{2,j+1} &= \sum_{k=1}^{j+1} \alpha^{j+1-k}\beta a_{1,k} \\ &= \sum_{k=1}^{j+1} \alpha^{j+1-k}\beta\alpha^{k-1} \\ &= \sum_{k=0}^{j} \alpha^{j-k}\beta\alpha^k \\ &= \sum_{k=0}^{j} \binom{k}{0} \binom{j-k}{0} \alpha^{j-2k}\beta^1. \end{aligned}$$

Now suppose that the statement holds for $a_{i,j+1}$ and $a_{i+1,j}$, where $i \geq 2$ and $j \geq 1$. Then

$$\begin{aligned} a_{i+1,j+1} &= \alpha a_{i+1,j} + \beta a_{i,j+1} \\ &= \alpha \left(\sum_{k=0}^{j-1} \binom{k + \left\lfloor \frac{i-1}{2} \right\rfloor}{k} \binom{j - k - 1 + \left\lfloor \frac{i}{2} \right\rfloor}{j-k-1} \alpha^{j-1-2k}\beta^i \right) \\ &\quad + \beta \left(\sum_{k=0}^{j} \binom{k + \left\lfloor \frac{i-2}{2} \right\rfloor}{k} \binom{j - k + \left\lfloor \frac{i-1}{2} \right\rfloor}{j-k} \alpha^{j-2k}\beta^{i-1} \right) \\ &= \sum_{k=0}^{j-1} \binom{k + \left\lfloor \frac{i-1}{2} \right\rfloor}{k} \binom{j - k - 1 + \left\lfloor \frac{i}{2} \right\rfloor}{j-k-1} \alpha^{j-2k}\beta^i \\ &\quad + \sum_{k=0}^{j} \binom{k + \left\lfloor \frac{i-2}{2} \right\rfloor}{k} \binom{j - k + \left\lfloor \frac{i-1}{2} \right\rfloor}{j-k} \beta\alpha^{j-2k}\beta^{i-1}. \end{aligned}$$

Applying $\beta\alpha^m = \alpha^{-m}\beta$, $m \in \mathbb{Z}$, we obtain

$$\begin{aligned}
a_{i+1,j+1} &= \sum_{k=0}^{j-1} \binom{k + \lfloor \frac{i-1}{2} \rfloor}{k} \binom{j-k-1+\lfloor \frac{i}{2} \rfloor}{j-k-1} \alpha^{j-2k}\beta^i \\
&\quad + \sum_{k=0}^{j} \binom{k + \lfloor \frac{i-2}{2} \rfloor}{k} \binom{j-k+\lfloor \frac{i-1}{2} \rfloor}{j-k} \alpha^{2k-j}\beta^i \\
&= \sum_{k=0}^{j-1} \binom{k + \lfloor \frac{i-1}{2} \rfloor}{k} \binom{j-k-1+\lfloor \frac{i}{2} \rfloor}{j-k-1} \alpha^{j-2k}\beta^i \\
&\quad + \sum_{k=0}^{j} \binom{j-k + \lfloor \frac{i-2}{2} \rfloor}{j-k} \binom{k+\lfloor \frac{i-1}{2} \rfloor}{k} \alpha^{j-2k}\beta^i \\
&= \sum_{k=0}^{j-1} \left(\binom{k + \lfloor \frac{i-1}{2} \rfloor}{k} \binom{j-k-1+\lfloor \frac{i}{2} \rfloor}{j-k-1} + \binom{j-k + \lfloor \frac{i-2}{2} \rfloor}{j-k} \binom{k+\lfloor \frac{i-1}{2} \rfloor}{k} \right) \alpha^{j-2k}\beta^i \\
&\quad + \binom{j + \lfloor \frac{i-1}{2} \rfloor}{j} \alpha^{-j}\beta^i \\
&= \sum_{k=0}^{j-1} \binom{k + \lfloor \frac{i-1}{2} \rfloor}{k} \binom{j-k+\lfloor \frac{i}{2} \rfloor}{j-k} \alpha^{j-2k}\beta^i + \binom{j + \lfloor \frac{i-1}{2} \rfloor}{j} \alpha^{-j}\beta^i \\
&= \sum_{k=0}^{j} \binom{k + \lfloor \frac{i-1}{2} \rfloor}{k} \binom{j-k+\lfloor \frac{i}{2} \rfloor}{j-k} \alpha^{j-2k}\beta^i,
\end{aligned}$$

where we used the fact that $\binom{a}{b} + \binom{a}{b+1} = \binom{a+1}{b+1}$.

□

LEMMA 4.33. *Let* $A_{\alpha,\beta} = (a_{i,j})_{i,j=1}^{\infty}$. *Suppose that* $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta) = 2$.

(i) If $j \geq i \geq 0$ *then*

$$a_{i+1,j+1} = \sum_{k=0}^{i} \binom{\lfloor \frac{i+j}{2} \rfloor}{i-k} \binom{\lfloor \frac{i+j+1}{2} \rfloor}{k} (\alpha\beta)^{i-2k}\alpha^{j-i}.$$

(ii) If $i \geq j \geq 0$ *then*

$$a_{i+1,j+1} = \sum_{k=0}^{j} \binom{\lfloor \frac{i+j}{2} \rfloor}{j-k} \binom{\lfloor \frac{i+j+1}{2} \rfloor}{k} (\beta\alpha)^{j-2k}\beta^{i-j}.$$

PROOF. We use an induction on $i + j$.
Suppose that $i = 0$. Then for $j \geq 0$ we have

$$a_{1,j+1} = \alpha^j = \binom{\lfloor \frac{j}{2} \rfloor}{0} \binom{\lfloor \frac{j+1}{2} \rfloor}{0} (\alpha\beta)^0\alpha^j.$$

Similarly the statement (ii) holds for $j = 0$.

Suppose that the statement holds for $a_{i,j+1}$ and $a_{i+1,j}$, $i,j \geq 1$. If $j > i$ then $j > i-1$ and $j-1 \geq i$. Thus we have

$$\begin{aligned}
a_{i+1,j+1} &= \alpha a_{i+1,j} + \beta a_{i,j+1} \\
&= \alpha\left(\sum_{k=0}^{i}\binom{\lfloor\frac{i+j-1}{2}\rfloor}{i-k}\binom{\lfloor\frac{i+j}{2}\rfloor}{k}(\alpha\beta)^{i-2k}\alpha^{j-1-i}\right) \\
&\quad + \beta\left(\sum_{k=0}^{i-1}\binom{\lfloor\frac{i-1+j}{2}\rfloor}{i-1-k}\binom{\lfloor\frac{i+j}{2}\rfloor}{k}(\alpha\beta)^{i-1-2k}\alpha^{j-i+1}\right) \\
&= \sum_{k=0}^{i}\binom{\lfloor\frac{i+j-1}{2}\rfloor}{i-k}\binom{\lfloor\frac{i+j}{2}\rfloor}{k}\alpha(\alpha\beta)^{i-2k}\alpha^{j-1-i} \\
&\quad + \sum_{k=0}^{i-1}\binom{\lfloor\frac{i-1+j}{2}\rfloor}{i-1-k}\binom{\lfloor\frac{i+j}{2}\rfloor}{k}\beta(\alpha\beta)^{i-1-2k}\alpha^{j-i+1}.
\end{aligned}$$

Using $\alpha^2 = \beta^2 = 1$, which implies $(\beta\alpha)^{-1} = \alpha\beta$, we can see that for any $k \in \mathbb{Z}$

$$\begin{aligned}
\alpha(\alpha\beta)^{i-2k}\alpha^{j-i-1} &= (\beta\alpha)^{i-2k}\alpha^{j-i} = (\alpha\beta)^{2k-i}\alpha^{j-i}, \\
\beta(\alpha\beta)^{i-1-2k}\alpha^{j-i+1} &= (\beta\alpha)^{i-2k}\alpha^{j-i} = (\alpha\beta)^{2k-i}\alpha^{j-i}.
\end{aligned}$$

Then

$$\begin{aligned}
a_{i+1,j+1} &= \sum_{k=0}^{i-1}\binom{\lfloor\frac{i+j-1}{2}\rfloor}{i-k}\binom{\lfloor\frac{i+j}{2}\rfloor}{k}(\alpha\beta)^{2k-i}\alpha^{j-i} + \binom{\lfloor\frac{i+j}{2}\rfloor}{i}(\alpha\beta)^{i}\alpha^{j-i} \\
&\quad + \sum_{k=0}^{i-1}\binom{\lfloor\frac{i-1+j}{2}\rfloor}{i-1-k}\binom{\lfloor\frac{i+j}{2}\rfloor}{k}(\alpha\beta)^{2k-i}\alpha^{j-i} \\
&= \sum_{k=0}^{i-1}\left(\binom{\lfloor\frac{i+j-1}{2}\rfloor}{i-k}\binom{\lfloor\frac{i+j}{2}\rfloor}{k} + \binom{\lfloor\frac{i-1+j}{2}\rfloor}{i-1-k}\binom{\lfloor\frac{i+j}{2}\rfloor}{k}\right)(\alpha\beta)^{2k-i}\alpha^{j-i} \\
&\quad + \binom{\lfloor\frac{i+j}{2}\rfloor}{i}(\alpha\beta)^{i}\alpha^{j-i}.
\end{aligned}$$

Using $\binom{a}{b+1} + \binom{a}{b} = \binom{a+1}{b+1}$ we obtain

$$a_{i+1,j+1} = \sum_{k=0}^{i}\binom{\lfloor\frac{i+j+1}{2}\rfloor}{i-k}\binom{\lfloor\frac{i+j}{2}\rfloor}{k}(\alpha\beta)^{2k-i}\alpha^{j-i} = \sum_{k=0}^{i}\binom{\lfloor\frac{i+j+1}{2}\rfloor}{k}\binom{\lfloor\frac{i+j}{2}\rfloor}{i-k}(\alpha\beta)^{i-2k}\alpha^{j-i}.$$

For $j < i$ we may use the result of the previous part together with the fact that $A_{\beta,\alpha} = (A_{\alpha,\beta})^T$.

The last case is $i = j$. Since $i > i-1$ and $i-1 < i$ we have to use the formula in (ii) for $a_{i+1,i}$ and the formula in (i) for $a_{i,i+1}$. Therefore

$$\begin{aligned}
a_{i+1,i+1} &= \alpha a_{i+1,i} + \beta a_{i,i+1} \\
&= \alpha\left(\sum_{k=0}^{i-1}\binom{\lfloor\frac{2i-1}{2}\rfloor}{i-1-k}\binom{\lfloor\frac{2i}{2}\rfloor}{k}(\beta\alpha)^{i-1-2k}\beta^{i-i+1}\right) \\
&\quad + \beta\left(\sum_{k=0}^{i-1}\binom{\lfloor\frac{2i-1}{2}\rfloor}{i-1-k}\binom{\lfloor\frac{2i}{2}\rfloor}{k}(\alpha\beta)^{i-1-2k}\alpha^{i-i+1}\right) \\
&= \sum_{k=0}^{i-1}\binom{i-1}{i-1-k}\binom{i}{k}\alpha(\beta\alpha)^{i-1-2k}\beta + \sum_{k=0}^{i-1}\binom{i-1}{i-1-k}\binom{i}{k}\beta(\alpha\beta)^{i-1-2k}\alpha.
\end{aligned}$$

Because $\alpha(\beta\alpha)^{i-1-2k}\beta = (\alpha\beta)^{i-2k}$, $\beta(\alpha\beta)^{i-1-2k}\alpha = (\beta\alpha)^{i-2k}$, and $(\beta\alpha)^{-1} = \alpha\beta$, we have

$$\begin{aligned} a_{i+1,i+1} &= \sum_{k=0}^{i-1} \binom{i-1}{i-1-k}\binom{i}{k}(\alpha\beta)^{i-2k} + \sum_{k=0}^{i-1} \binom{i-1}{i-1-k}\binom{i}{k}(\beta\alpha)^{i-2k} \\ &= \sum_{k=0}^{i-1} \binom{i-1}{i-1-k}\binom{i}{k}(\alpha\beta)^{i-2k} + \sum_{k=1}^{i} \binom{i-1}{k-1}\binom{i}{i-k}(\alpha\beta)^{i-2k}. \end{aligned}$$

Because $\binom{i-1}{i-k-1}\binom{i}{k} + \binom{i-1}{k-1}\binom{i}{i-k} = \binom{i}{k}\left(\binom{i-1}{i-k-1} + \binom{i-1}{i-k}\right) = \binom{i}{k}\binom{i}{i-k}$ holds for each $0 \le k \le i$,

$$\begin{aligned} a_{i+1,i+1} &= \sum_{k=1}^{i-1} \binom{i}{i-k}\binom{i}{k}(\alpha\beta)^{i-2k} + \binom{i-1}{i-1}\binom{i}{0}(\alpha\beta)^{i} + \binom{i-1}{i-1}\binom{i}{0}(\alpha\beta)^{-i} \\ &= \sum_{k=0}^{i} \binom{i}{i-k}\binom{i}{k}(\alpha\beta)^{i-2k}, \end{aligned}$$

which is the formula in (i) for $i = j$. The formula in (ii) for $i = j$ follows again by passing to $(A_{\alpha,\beta})^T$.

□

Next, we try to express the elements of the matrix $A_{\alpha,\beta}$ in the form $\sum_k c_k\varphi_k$, where φ_k are pairwise distinct automorphisms.

PROPOSITION 4.34. *Suppose (C1) holds and $j \ge 0$, $i \ge 1$. If n is odd then*

$$a_{i+1,j+1} = \sum_{k=0}^{n-1} \left(\sum_{l=0}^{\lceil \frac{j+1-k}{n} \rceil - 1} \binom{k+ln+\lfloor \frac{i-1}{2} \rfloor}{\lfloor \frac{i-1}{2} \rfloor} \binom{j-(k+ln)+\lfloor \frac{i}{2} \rfloor}{\lfloor \frac{i}{2} \rfloor} \right) \alpha^{j-2k}\beta^i.$$

If n is even then

$$a_{i+1,j+1} = \sum_{k=0}^{\frac{n}{2}-1} \left(\sum_{l=0}^{\lceil \frac{2(j+1-k)}{n} \rceil - 1} \binom{k+l\frac{n}{2}+\lfloor \frac{i-1}{2} \rfloor}{\lfloor \frac{i-1}{2} \rfloor} \binom{j-(k+l\frac{n}{2})+\lfloor \frac{i}{2} \rfloor}{\lfloor \frac{i}{2} \rfloor} \right) \alpha^{j-2k}\beta^i.$$

PROOF. Because $\mathrm{ord}(\alpha) = n$, $\alpha^{j-2k_1} = \alpha^{j-2k_2}$ if and only if $k_1, k_2 \in \mathbb{Z}$ are such that $j - 2k_1 \equiv j - 2k_2 \pmod{n}$. This holds if and only if $2(k_1 - k_2) \equiv 0 \pmod{n}$. For n odd this is equivalent to $k_1 - k_2 \equiv 0 \pmod{n}$ and for n even to $k_1 - k_2 \equiv 0 \pmod{\frac{n}{2}}$. Using this together with Lemma 4.32 and Lemma 3.8 we obtain:

If n is odd, then

$$\begin{aligned}
a_{i+1,j+1} &= \sum_{s=0}^{j} \binom{s+\left\lfloor\frac{i-1}{2}\right\rfloor}{\left\lfloor\frac{i-1}{2}\right\rfloor}\binom{j-s+\left\lfloor\frac{i}{2}\right\rfloor}{\left\lfloor\frac{i}{2}\right\rfloor}\alpha^{j-2s}\beta^i \\
&= \sum_{k=0}^{n-1}\sum_{\substack{0\le s\le j\\ s\equiv k \pmod n}} \binom{s+\left\lfloor\frac{i-1}{2}\right\rfloor}{\left\lfloor\frac{i-1}{2}\right\rfloor}\binom{j-s+\left\lfloor\frac{i}{2}\right\rfloor}{\left\lfloor\frac{i}{2}\right\rfloor}\alpha^{j-2s}\beta^i \\
&= \sum_{k=0}^{n-1}\sum_{\substack{s=k+ln\\ 0\le l<\left\lceil\frac{j+1-k}{n}\right\rceil}} \binom{s+\left\lfloor\frac{i-1}{2}\right\rfloor}{\left\lfloor\frac{i-1}{2}\right\rfloor}\binom{j-s+\left\lfloor\frac{i}{2}\right\rfloor}{\left\lfloor\frac{i}{2}\right\rfloor}\alpha^{j-2s}\beta^i \\
&= \sum_{k=0}^{n-1}\sum_{l=0}^{\left\lceil\frac{j+1-k}{n}\right\rceil-1} \binom{k+ln+\left\lfloor\frac{i-1}{2}\right\rfloor}{\left\lfloor\frac{i-1}{2}\right\rfloor}\binom{j-(k+ln)+\left\lfloor\frac{i}{2}\right\rfloor}{\left\lfloor\frac{i}{2}\right\rfloor}\alpha^{j-2k-2ln}\beta^i \\
&= \sum_{k=0}^{n-1}\sum_{l=0}^{\left\lceil\frac{j+1-k}{n}\right\rceil-1} \binom{k+ln+\left\lfloor\frac{i-1}{2}\right\rfloor}{\left\lfloor\frac{i-1}{2}\right\rfloor}\binom{j-(k+ln)+\left\lfloor\frac{i}{2}\right\rfloor}{\left\lfloor\frac{i}{2}\right\rfloor}\alpha^{j-2k}\beta^i.
\end{aligned}$$

Analogously for n even.

□

PROPOSITION 4.35. *Suppose (C3) holds and $j \ge i \ge 0$. If n is odd then*

$$a_{i+1,j+1} = \sum_{k=0}^{n-1}\left(\sum_{l=0}^{\left\lceil\frac{i+1-k}{n}\right\rceil-1}\binom{\left\lfloor\frac{i+j}{2}\right\rfloor}{i-(k+ln)}\binom{\left\lfloor\frac{i+j+1}{2}\right\rfloor}{k+ln}\right)(\alpha\beta)^{i-2k}\alpha^{j-i}.$$

If n is even then

$$a_{i+1,j+1} = \sum_{k=0}^{\frac{n}{2}-1}\left(\sum_{l=0}^{\left\lceil\frac{2(i+1-k)}{n}\right\rceil-1}\binom{\left\lfloor\frac{i+j}{2}\right\rfloor}{i-(k+l\frac{n}{2})}\binom{\left\lfloor\frac{i+j+1}{2}\right\rfloor}{k+l\frac{n}{2}}\right)(\alpha\beta)^{i-2k}\alpha^{j-i}.$$

PROOF. Since $\operatorname{ord}(\alpha\beta) = n$, $(\alpha\beta)^{i-2k_1} = (\alpha\beta)^{i-2k_2}$ if and only if $k_1, k_2 \in \mathbb{Z}$ are such that $i - 2k_1 \equiv i - 2k_2 \pmod n$. This holds if and only if $2(k_1 - k_2) \equiv 0 \pmod n$. For n odd this is equivalent to $k_1 - k_2 \equiv 0 \pmod n$ and for n even to $k_1 - k_2 \equiv 0 \pmod{\frac{n}{2}}$.

Using this together with Lemma 4.33 and Lemma 3.8 we obtain that in the case n is odd

$$\begin{aligned}
a_{i+1,j+1} &= \sum_{s=0}^{i} \binom{\lfloor \frac{i+j}{2} \rfloor}{i-s} \binom{\lfloor \frac{i+j+1}{2} \rfloor}{s} (\alpha\beta)^{i-2s}\alpha^{j-i} \\
&= \sum_{k=0}^{n-1} \sum_{\substack{0\le s\le i \\ s\equiv k \pmod n}} \binom{\lfloor \frac{i+j}{2} \rfloor}{i-s} \binom{\lfloor \frac{i+j+1}{2} \rfloor}{s} (\alpha\beta)^{i-2s}\alpha^{j-i} \\
&= \sum_{k=0}^{n-1} \sum_{\substack{s=k+ln \\ 0\le s\le i}} \binom{\lfloor \frac{i+j}{2} \rfloor}{i-s} \binom{\lfloor \frac{i+j+1}{2} \rfloor}{s} (\alpha\beta)^{i-2s}\alpha^{j-i} \\
&= \sum_{k=0}^{n-1} \sum_{l=0}^{\lceil \frac{i+1-k}{n} \rceil - 1} \binom{\lfloor \frac{i+j}{2} \rfloor}{i-(k+ln)} \binom{\lfloor \frac{i+j+1}{2} \rfloor}{k+ln} (\alpha\beta)^{i-2(k+ln)}\alpha^{j-i} \\
&= \sum_{k=0}^{n-1} \sum_{l=0}^{\lceil \frac{i+1-k}{n} \rceil - 1} \binom{\lfloor \frac{i+j}{2} \rfloor}{i-(k+ln)} \binom{\lfloor \frac{i+j+1}{2} \rfloor}{k+ln} (\alpha\beta)^{i-2k}\alpha^{j-i}.
\end{aligned}$$

The proof for n even is analogous.

□

Now we try to apply the explicit formulas for the elements of the matrix $A_{\alpha,\beta}$ to find some periods of its rows.

PROPOSITION 4.36. *Suppose (C1) holds and $i > 1$. If n is odd and P is a multiple of P_{i-1} such that*

$$\sum_{l=0}^{\frac{P}{n}-1} \binom{k+ln+\lfloor \frac{i-2}{2} \rfloor}{\lfloor \frac{i-2}{2} \rfloor} \binom{P-1-(k+ln)+\lfloor \frac{i-1}{2} \rfloor}{\lfloor \frac{i-1}{2} \rfloor} \equiv 0 \pmod{e_G} \text{ for each } 0 \le k < n$$

then P is a period of the ith row of the matrix $A_{\alpha,\beta}$.

If n is even and P is a multiple of P_{i-1} such that

$$\sum_{l=0}^{\frac{2P}{n}-1} \binom{k+l\frac{n}{2}+\lfloor \frac{i-2}{2} \rfloor}{\lfloor \frac{i-2}{2} \rfloor} \binom{P-1-(k+l\frac{n}{2})+\lfloor \frac{i-1}{2} \rfloor}{\lfloor \frac{i-1}{2} \rfloor} \equiv 0 \pmod{e_G} \text{ for each } 0 \le k < \frac{n}{2}$$

then P is a period of the ith row of the matrix $A_{\alpha,\beta}$.

PROOF. For n odd using Proposition 4.34 we obtain that

$$a_{i,P} = \sum_{k=0}^{n-1} \sum_{l=0}^{\lceil \frac{P-k}{n} \rceil - 1} \binom{k+ln+\lfloor \frac{i-2}{2} \rfloor}{\lfloor \frac{i-2}{2} \rfloor} \binom{P-1-(k+ln)+\lfloor \frac{i-1}{2} \rfloor}{\lfloor \frac{i-1}{2} \rfloor} \alpha^{P-1-2k}\beta^{i-1}.$$

Corollary 4.13 says that $P_1 = \mathrm{ord}(\alpha) = n$ and $P_1 = n$ divides P_{i-1}. Because P is a multiple of P_{i-1}, n divides also P. Then

$$a_{i,P} = \sum_{k=0}^{n-1} \left(\sum_{l=0}^{\frac{P}{n}-1} \binom{k+ln+\lfloor \frac{i-2}{2} \rfloor}{\lfloor \frac{i-2}{2} \rfloor} \binom{P-1-(k+ln)+\lfloor \frac{i-1}{2} \rfloor}{\lfloor \frac{i-1}{2} \rfloor} \right) \alpha^{-(2k+1)}\beta^{i-1}.$$

Since

$$\sum_{l=0}^{\frac{P}{n}-1} \binom{k+ln+\lfloor \frac{i-2}{2} \rfloor}{\lfloor \frac{i-2}{2} \rfloor} \binom{P-1-(k+ln)+\lfloor \frac{i-1}{2} \rfloor}{\lfloor \frac{i-1}{2} \rfloor} \equiv 0 \pmod{e_G} \text{ for each } 0 \le k < n,$$

$a_{i,P} = 0$ by Lemma 4.11. Then it is easy to see that P is a period of the ith row of the matrix $A_{\alpha,\beta}$.

The statement for n even can be obtained similarly.

□

PROPOSITION 4.37. *Suppose (C2) holds and $i > 1$. If n is odd and P is a multiple of P_{i-1} such that*

$$\sum_{l=0}^{\lceil \frac{i-k}{n} \rceil - 1} \binom{k+ln+\frac{P}{2}-1}{\frac{P}{2}-1} \binom{i-1-(k+ln)+\frac{P}{2}-1}{\frac{P}{2}-1} \equiv 0 \pmod{e_G} \text{ for each } 0 \leq k < n$$

then P is a period of the ith row of the matrix $A_{\alpha,\beta}$.

If n is even and P is a multiple of P_{i-1} such that

$$\sum_{l=0}^{\lceil \frac{2(i-k)}{n} \rceil - 1} \binom{k+l\frac{n}{2}+\frac{P}{2}-1}{\frac{P}{2}-1} \binom{i-1-(k+l\frac{n}{2})+\frac{P}{2}-1}{\frac{P}{2}-1} \equiv 0 \pmod{e_G} \text{ for each } 0 \leq k < \frac{n}{2}$$

then P is a period of the ith row of the matrix $A_{\alpha,\beta}$.

PROOF. Using Proposition 4.34 together with Remark 4.31, if n is odd then

$$a_{i,P} = \sum_{k=0}^{n-1} \sum_{l=0}^{\lceil \frac{i-k}{n} \rceil - 1} \binom{k+ln+\lfloor \frac{P-2}{2} \rfloor}{\lfloor \frac{P-2}{2} \rfloor} \binom{i-1-(k+ln)+\lfloor \frac{P-1}{2} \rfloor}{\lfloor \frac{P-1}{2} \rfloor} \beta^{i-1-2k} \alpha^{P-1}.$$

By Corollary 4.13, $P_1 = \mathrm{ord}(\alpha) = 2$ divides P_{i-1}. Because P is a multiple of P_{i-1}, P is even and hence

$$a_{i,P} = \sum_{k=0}^{n-1} \sum_{l=0}^{\lceil \frac{i-k}{n} \rceil - 1} \binom{k+ln+\frac{P}{2}-1}{\frac{P}{2}-1} \binom{i-1-(k+ln)+\frac{P}{2}-1}{\frac{P}{2}-1} \beta^{i-1-2k} \alpha^{P-1}.$$

Because

$$\sum_{l=0}^{\lceil \frac{i-k}{n} \rceil - 1} \binom{k+ln+\frac{P}{2}-1}{\frac{P}{2}-1} \binom{i-1-(k+ln)+\frac{P}{2}-1}{\frac{P}{2}-1} \equiv 0 \pmod{e_G} \text{ for each } 0 \leq k < n,$$

$a_{i,P} = 0$ by Lemma 4.11. Using this together with the fact that P is a multiple of P_{i-1}, it is easy to see that P is a period of the ith row of the matrix $A_{\alpha,\beta}$.

For n even similarly.

□

PROPOSITION 4.38. *Suppose that (C3) holds and $i > 1$. If n is odd and P is a multiple of P_{i-1} such that $P \geq i$ and*

$$\sum_{l=0}^{\lceil \frac{i-k}{n} \rceil - 1} \binom{\lfloor \frac{i}{2} \rfloor + \frac{P}{2} - 1}{i-1-(k+ln)} \binom{\lfloor \frac{i-1}{2} \rfloor + \frac{P}{2}}{k+ln} \equiv 0 \pmod{e_G} \text{ for each } 0 \leq k < n$$

then P is a period of the ith row of the matrix $A_{\alpha,\beta}$.

If n is even and P is a multiple of P_{i-1} such that $P \geq i$ and

$$\sum_{l=0}^{\lceil \frac{2(i-k)}{n} \rceil - 1} \binom{\lfloor \frac{i}{2} \rfloor + \frac{P}{2} - 1}{i-1-(k+l\frac{n}{2})} \binom{\lfloor \frac{i-1}{2} \rfloor + \frac{P}{2}}{k+l\frac{n}{2}} \equiv 0 \pmod{e_G} \text{ for each } 0 \leq k < \frac{n}{2}$$

then P is a period of the ith row of the matrix $A_{\alpha,\beta}$.

We note that the assumption $P \geq i$ is in fact not restrictive, as $P_i \geq i$ by Lemma 4.19.

PROOF. By Corollary 4.13 $P_1 = \mathrm{ord}(\alpha) = 2$ and $P_1 = 2$ divides P_{i-1} for each $i \geq 1$. Thus P is also even. Since $P \geq i$, using Proposition 4.35 for n odd we have

$$a_{i,P} = \sum_{k=0}^{n-1} \left(\sum_{l=0}^{\lceil \frac{i-k}{n} \rceil - 1} \binom{\lfloor \frac{i+P-2}{2} \rfloor}{i-1-(k+ln)} \binom{\lfloor \frac{i+P-1}{2} \rfloor}{k+ln} \right) (\alpha\beta)^{i-1-2k} \alpha^{P-i}$$

$$= \sum_{k=0}^{n-1} \left(\sum_{l=0}^{\lceil \frac{i-k}{n} \rceil - 1} \binom{\lfloor \frac{i}{2} \rfloor + \frac{P}{2} - 1}{i-1-(k+ln)} \binom{\lfloor \frac{i-1}{2} \rfloor + \frac{P}{2}}{k+ln} \right) (\alpha\beta)^{i-1-2k} \alpha^{i}.$$

Since

$$\sum_{l=0}^{\lceil \frac{i-k}{n} \rceil - 1} \binom{\lfloor \frac{i}{2} \rfloor + \frac{P}{2} - 1}{i-1-(k+ln)} \binom{\lfloor \frac{i-1}{2} \rfloor + \frac{P}{2}}{k+ln} \equiv 0 \pmod{e_G} \text{ for each } 0 \leq k < n,$$

$a_{i,P} = 0$ by Lemma 4.11. Using this together with the fact that P is a multiple of P_{i-1}, it is easy to see that P is a period of the ith row of the matrix $A_{\alpha,\beta}$.

For n even similarly.

□

Notice that the periods P found in the preceding propositions are not in general the minimal periods P_i. For each of the cases (C1), (C2), and (C3) we have the formula for $a_{i,P_i} = \sum_{k=0}^{m} c_k \varphi_k$, where $c_k \in \mathbb{N}$ and $\varphi_{k_1} \neq \varphi_{k_2}$ for $k_1 \neq k_2$. Moreover, either all the φ_ks are rotations or all the φ_ks are reflections. Corollary 4.13 says that P_i for $i > 1$ is the smallest multiple of P_{i-1} such that $a_{i,P_i} = \sum_{k=0}^{m} c_k \varphi_k = 0$. One possibility to satisfy this condition is that $c_k \equiv 0 \pmod{e_G}$ for each $0 \leq k \leq m$. But this may not be a necessary condition, as there may exist coefficients c_k not all divisible by e_G such that $\sum_{k=0}^{m} c_k \varphi_k = 0$. For example consider $G = V_4$. Then $e_G = 2$, $\mathrm{Aut}(G) = D_6 = \{\mathrm{id}_G, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ and $(1\ 2) + (1\ 3) + (2\ 3) = 0$ in $(\mathrm{End}(G), +, 0)$.

CHAPTER 5

Periods in central quasigroups of order 4

In this chapter we will compute the minimal periods of the rows of the matrix $A_{\alpha,\beta}$ for the concrete isomorphism classes of quasigroups of order 4. We will use our results from the previous chapter.

Fix a central quasigroup $(G,*)$ of order 4. By Theorem 2.32 there exists an Abelian group $(G,+)$, such that $x*y=\alpha(x)+\beta(y)+c$, $\alpha,\beta\in\mathrm{Aut}((G,+))$. Because $(G,*)$ has order 4, $(G,+)$ is either $\mathbb{Z}_4$ or V_4. These groups have the following properties: $e_{\mathbb{Z}_4}=4=2^2$, $e_{V_4}=2$, $\mathrm{Aut}(\mathbb{Z}_4)=\{\mathrm{id}_{\mathbb{Z}_4},(1\ 3)\}$, and $\mathrm{Aut}(V_4)=D_6=\{\mathrm{id}_{V_4},(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$. This implies that if $\alpha\in\mathrm{Aut}(\mathbb{Z}_4)$ then $\mathrm{ord}(\alpha)\in\{1,2\}$ and if $\alpha\in\mathrm{Aut}(V_4)$ then $\mathrm{ord}(\alpha)\in\{1,2,3\}$.

1. Medial quasigroups of order 4

Let $(G,*)$ be a medial quasigroup. According to Table 1, $(G,*)$ is isomorphic to one of the quasigroups 1–9 or 16–19. Because $(G,*)$ is medial, the minimal periods of the matrix $A_{\alpha,\beta}$ can be computed by Theorem 4.26.

Thus for quasigroups 1, 2, 4 ($e_G=2$, $\mathrm{ord}(\alpha)=1$) and quasigroups 3 and 6 ($e_G=2$, $\mathrm{ord}(\alpha)=2$), we have

$$P_1=\mathrm{ord}(\alpha),\quad P_i=2^{\lceil\log_2 i\rceil}\qquad\text{for } i>1.$$

The minimal periods for quasigroups 5, 7, 8, and 9 ($e_G=2$, $\mathrm{ord}(\alpha)=3$) are

$$P_1=3,\quad P_i=3\cdot 2^{\lceil\log_2 i\rceil}\qquad\text{for } i>1.$$

For the isomorphism classes 16, 17 ($e_G=4$, $\mathrm{ord}(\alpha)=1$) and 18, 19 ($e_G=4$, $\mathrm{ord}(\alpha)=2$) we obtain the following minimal periods:

$$P_1=\mathrm{ord}(\alpha),\quad P_i=2^{\lceil\log_2 i\rceil+1}\qquad\text{for } i>1.$$

2. Non-medial central quasigroups of order 4

If $(G,*)$ is a central non-medial quasigroup of order 4, then $(G,*)$ is isomorphic to a principal isotope of the group V_4 (see Table 1). By Theorem 2.32 there exists an Abelian group $(G,+)$, such that $x*y=\alpha(x)+\beta(y)+c$, $\alpha,\beta\in\mathrm{Aut}((G,+))$, $c\in G$. Using Proposition 2.44 we have that $(G,*)$ is isotopic to $(G,+)$. Since $(G,*)$ is isotopic to $(G,+)$ and also to V_4, V_4 and $(G,+)$ are isotopic and hence V_4 and $(G,+)$ are isomorphic by Corollary 2.19. Then $(G,*)=(V_4,*)$ such that $x*y=\alpha(x)+\beta(y)+c$, $\alpha,\beta\in\mathrm{Aut}(V_4)$, $\alpha\beta\neq\beta\alpha$, $c\in G$, and $e_G=e_{V_4}=2$.

Because $\mathrm{Aut}(V_4)=D_6=\{\mathrm{id}_{V_4},(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$, α,β satisfy one of these statements:

(K1) $\mathrm{ord}(\alpha)=3$, $\mathrm{ord}(\beta)=2$ and $(\alpha\beta)^2=(\beta\alpha)^2=\mathrm{id}_{V_4}$,
(K2) $\mathrm{ord}(\alpha)=2$, $\mathrm{ord}(\beta)=3$ and $(\alpha\beta)^2=(\beta\alpha)^2=\mathrm{id}_{V_4}$,
(K3) $\mathrm{ord}(\alpha)=2$, $\mathrm{ord}(\beta)=2$ and $(\alpha\beta)^3=(\beta\alpha)^3=\mathrm{id}_{V_4}$.

The conditions (K1), (K2) and (K3) correspond to conditions (C1), (C2) and (C3) from Chapter 4, Section 4, where $n=3$. Table 6 shows all the non-medial central quasigroups of order 4, where $(G,*)=V_4[\varphi,\psi]$ and $x*y=\alpha(x)+\beta(y)+c$ (see also Table 1).

Isomorphism class	φ	ψ	α	β	c	case
10	(1 2)	(1 2 3)	(1 2)	(1 2 3)	0	(K2)
11	(1 2 3)	(1 2)	(1 2 3)	(1 2)	0	(K1)
12	(1 2)	(1 3)	(1 2)	(1 3)	0	(K3)
13	(1 2)	(0 2 1)	(1 2)	(1 2 3)	2	(K2)
14	(0 2 1)	(1 2)	(1 2 3)	(1 2)	2	(K1)
15	(1 2)	(0 2)	(1 2)	(1 3)	2	(K3)

TABLE 6. Non-medial central quasigroups of order 4

In the following we will compute the minimal periods of the matrix $A_{\alpha,\beta}$ for the non-medial central quasigroups using results from Chapter 4, Section 4.

LEMMA 5.1. *Let $c_1, c_2, c_3 \in \mathbb{N} \cup \{0\}$ and $\varphi_1, \varphi_2, \varphi_3 \in \mathrm{Aut}((V_4, +))$ be pairwise distinct. Then $c_1\varphi_1 + c_2\varphi_2 + c_3\varphi_3 = 0$ if and only if*

- *c_1, c_2, c_3 are all even or*
- *c_1, c_2, c_3 are all odd and either $\varphi_1, \varphi_2, \varphi_3 \in \{(1\ 2), (1\ 3), (2\ 3)\}$ or $\varphi_1, \varphi_2, \varphi_3 \in \{\mathrm{id}_{V_4}, (1\ 2\ 3), (1\ 3\ 2)\}$.*

PROOF. Because of Lemma 4.11 and the fact that $e_{V_4} = 2$, passing to $c_i \bmod 2$ we may without loss of generality assume that $c_1, c_2, c_3 \in \{0, 1\}$.

It is easy to check that $(1\ 2) + (1\ 3) + (2\ 3) = 0$ and $\mathrm{id}_{V_4} + (1\ 2\ 3) + (1\ 3\ 2) = 0$.

Assume that $c_1 = 1$ and $c_2 = c_3 = 0$. Because φ_1 is an automorphism of V_4, $c_1\varphi_1 + c_2\varphi_2 + c_3\varphi_3 = \varphi_1 \neq 0$.

If $g, h \in V_4$ then $g + h = 0$ if and only if $g = h$. Suppose $c_1 = c_2 = 1$ and $c_3 = 0$. Since $\varphi_1 \neq \varphi_2$, there exists $g \in V_4$ such that $\varphi_1(g) \neq \varphi_2(g)$ and hence $c_1\varphi_1 + c_2\varphi_2 + c_3\varphi_3 = \varphi_1 + \varphi_2 \neq 0$.

Let $c_1 = c_2 = c_3 = 1$ and $\varphi_1, \varphi_2 \in \{(1\ 2), (1\ 3), (2\ 3)\}$. If $\varphi_1 + \varphi_2 + \varphi_3 = 0$ then using $(1\ 2) + (1\ 3) + (2\ 3) = 0$ we obtain $\varphi_3 = -(\varphi_1 + \varphi_2) \in \{(1\ 2), (1\ 3), (2\ 3)\}$. Similarly, if $\varphi_1, \varphi_2 \in \{\mathrm{id}_{V_4}, (1\ 2\ 3), (1\ 3\ 2)\}$, then also $\varphi_3 \in \{\mathrm{id}_{V_4}, (1\ 2\ 3), (1\ 3\ 2)\}$.

□

2.1. Case (K1). Proposition 4.34 says that

$$a_{i,j} = \sum_{k=0}^{2} d_k(i,j)\alpha^{j-1-2k}\beta^{i-1}$$

for $i > 1$, $j \geq 1$, where

$$d_k(i,j) = \sum_{l=0}^{\lceil \frac{j-k}{3} \rceil - 1} \binom{k + 3l + \lfloor \frac{i-2}{2} \rfloor}{\lfloor \frac{i-2}{2} \rfloor} \binom{j - 1 - (k + 3l) + \lfloor \frac{i-1}{2} \rfloor}{\lfloor \frac{i-1}{2} \rfloor}.$$

Since $\alpha^{j-1}\beta^{i-1} = \alpha^{(j+2) \bmod 3}\beta^{(i-1) \bmod 2}$, $\alpha^{j-3}\beta^{i-1} = \alpha^{j \bmod 3}\beta^{(i-1) \bmod 2}$, and $\alpha^{j-5}\beta^{i-1} = \alpha^{(j+1) \bmod 3}\beta^{(i-1) \bmod 2}$ are either three distinct rotations or three distinct reflections in D_6, by Lemma 5.1

$$a_{i,j} = 0 \text{ if and only if } d_0(i,j),\ d_1(i,j),\ d_2(i,j) \text{ have the same parity.} \tag{26}$$

By Corollary 4.18 there is a non-decreasing sequence $(c_i)_{i=1}^{\infty}$, $c_i \in \mathbb{N} \cup \{0\}$, such that

$$P_i = 3 \cdot 2^{c_i} \quad \text{for each } i \geq 1,$$

where $c_1 = 0$ and $c_{j+1} - c_j \leq 1$ for each $j \geq 1$.

LEMMA 5.2. *Let $c, s \in \mathbb{N} \cup \{0\}$. Then $a_{2^s+1,3\cdot 2^c} = 0$ if and only if $s \leq c$.*

PROOF. By (26), $a_{2^s+1,3\cdot 2^c} = 0$ if and only if the numbers $d_0(2^s+1, 3\cdot 2^c)$, $d_1(2^s+1, 3\cdot 2^c)$, and $d_2(2^s+1, 3\cdot 2^c)$ have the same parity.

First, assume that $s = 0$. Then for $k = 0, 1, 2$

$$d_k(2, 3\cdot 2^c) = \sum_{l=0}^{2^c-1} \binom{k+3l+0}{0} \binom{3\cdot 2^c - 1 - (k+3l) + 0}{0} = 2^c,$$

and hence $d_k(2, 3\cdot 2^c)$ have the same parity for each $k = 0, 1, 2$ whenever $c \geq 0$.

Now suppose that $s > 0$. For $0 \leq m \leq 3\cdot 2^c - 1$ put

$$B(c, s, m) = \binom{m + 2^{s-1} - 1}{2^{s-1} - 1} \binom{3\cdot 2^c - 1 - m + 2^{s-1}}{2^{s-1}}.$$

Then

$$d_k(2^s + 1, 3\cdot 2^c) = \sum_{l=0}^{2^c-1} B(c, s, k+3l).$$

For $k = 0, 1, 2$ denote

$$M_k = \big|\{m;\ m \equiv k \pmod 3,\ 0 \leq m \leq 3\cdot 2^c - 1,\ B(c, s, m) \text{ is odd}\}\big|.$$

Then $d_k(2^s + 1, 3\cdot 2^c)$ is even if and only if M_k is even. Hence $d_k(2^s + 1, 3\cdot 2^c)$ have the same parity for each $k = 0, 1, 2$ if and only if M_0, M_1, and M_2 have the same parity.

To find out the parity of the M_ks we need to determine under which circumstances are the numbers $B(c, s, m)$ odd. To this end we apply Lemma 3.10 with $a = 2^{s-1}$ and $b = m$. It follows that there are four possibilities:

- Case $s > c + 2$:

The number $B(c, s, m)$ is odd if and only if $m = 0$. Therefore $M_0 = 1$ and $M_1 = M_2 = 0$.

- Case $s = c + 2$:

Then $B(c, s, m)$ is odd only for $m = 2^{c+1}$. Thus $M_{2^{c+1} \bmod 3} = 1$ and $M_k = 0$ for $k \neq 2^{c+1} \bmod 3$.

- Case $s = c + 1$:

The number $B(c, s, m)$ is odd if and only if $m \in \{0, 2^{c+1}\}$. Because $2^{c+1} \not\equiv 0 \pmod 3$, $M_{2^{c+1} \bmod 3} = M_0 = 1$ and $M_{2^c \bmod 3} = 0$.

- Case $s < c + 1$:

The number $B(c, s, m)$ is odd if and only if $m \equiv 2^{s-1} \pmod{2^s}$. Thus

$$M_k = \big|\{m;\ m \equiv k \pmod 3,\ m \equiv 2^{s-1} \pmod{2^s},\ 0 \leq m \leq 3\cdot 2^c - 1\}\big|.$$

By the Chinese Remainder Theorem for each $k = 0, 1, 2$ there exists uniquely determined $x_k \in \{0, \ldots, 3\cdot 2^s - 1\}$ such that

$$M_k = \big|\{m;\ m \equiv x_k \pmod{3\cdot 2^s},\ 0 \leq m \leq 3\cdot 2^c - 1\}\big|.$$

Now applying Lemma 3.8 we obtain $M_k = \left\lceil \frac{3\cdot 2^c - x_k}{3\cdot 2^s} \right\rceil = 2^{c-s}$. Hence,

$$M_0 = M_1 = M_2 = 2^{c-s}.$$

Therefore M_0, M_1, and M_2 have the same parity if and only if $s \leq c$.

□

LEMMA 5.3. *Let $s \in \mathbb{N}$, $c \in \mathbb{N} \cup \{0\}$, and $P_{2^s+1} = 3\cdot 2^c$. Then*

$$P_i = P_{2^s+1} = 3\cdot 2^c \quad \textit{for } 2^s + 1 \leq i \leq 2^{s+1}.$$

PROOF. Notice that for i even we have

$$d_k(i, j) = \sum_{l=0}^{\lceil \frac{j-k}{3} \rceil - 1} \binom{k + 3l + \frac{i-2}{2}}{\frac{i-2}{2}} \binom{j - 1 - (k+3l) + \frac{i-2}{2}}{\frac{i-2}{2}},$$

while for i odd we have

$$d_k(i,j) = \sum_{l=0}^{\lceil \frac{j-k}{3} \rceil - 1} \binom{k+3l+\frac{i-1}{2}-1}{\frac{i-1}{2}-1} \binom{j-1-(k+3l)+\frac{i-1}{2}}{\frac{i-1}{2}}.$$

By Corollary 4.13 and the fact that $P_{2^s+1} = 3 \cdot 2^c$, $a_{2^s+1,3\cdot 2^c} = 0$ and hence $s \leq c$ by Lemma 5.2.

Suppose that $2^s + 1 < i \leq 2^{s+1}$ and i is even. Then $0 < \frac{i-2}{2} < 2^s \leq 2^c$ and using Lemma 3.9 with $a = \frac{i-2}{2}$ we obtain that

$$\binom{m+\frac{i-2}{2}}{\frac{i-2}{2}} \binom{3\cdot 2^c - 1 - m + \frac{i-2}{2}}{\frac{i-2}{2}}$$

is even for each $0 \leq m \leq 3 \cdot 2^c - 1$. Therefore $d_k(i, 3 \cdot 2^c)$ is even for each $k = 0, 1, 2$.

Similarly, if $2^s + 1 < i \leq 2^{s+1}$ and i is odd, then $2^{s-1} < \frac{i-1}{2} < 2^s \leq 2^c$ and using Lemma 3.10 with $a = \frac{i-1}{2}$ we obtain that

$$\binom{m+\frac{i-1}{2}-1}{\frac{i-1}{2}-1} \binom{3\cdot 2^c - 1 - m + \frac{i-1}{2}}{\frac{i-1}{2}}$$

is even for each $0 \leq m \leq 3 \cdot 2^c - 1$. Thus $d_k(i, 3 \cdot 2^c)$ is even for each $k = 0, 1, 2$.

Putting both cases together, we have that $d_1(i, 3 \cdot 2^c)$, $d_2(i, 3 \cdot 2^c)$, and $d_3(i, 3 \cdot 2^c)$ are even for every $2^s + 1 < i \leq 2^{s+1}$. The statement now follows using (26) and Corollary 4.13. □

THEOREM 5.4. *Suppose (K1) holds. Then*

$$P_1 = 3 \quad \textit{and} \quad P_i = 3 \cdot 2^{\lceil \log_2 i \rceil - 1} \quad \textit{for } i > 1.$$

PROOF. Obviously, $P_1 = \mathrm{ord}(\alpha) = 3$. We show that $P_i = 3 \cdot 2^s$ for $2^s + 1 \leq i \leq 2^{s+1}$, $s \geq 0$. We do that using an induction on s. For $s = 0$ we have $a_{2,3} = 0$ by Lemma 5.2 and hence $P_2 = 3$ by Corollary 4.13.

Now suppose that the statement holds for some $s > 0$. Then $P_{2^{s+1}} = 3 \cdot 2^s$. Further, $a_{2^{s+1}+1,3\cdot 2^s} \neq 0$ and $a_{2^{s+1}+1,3\cdot 2^{s+1}} = 0$ by Lemma 5.2. Hence $P_{2^{s+1}+1} = 3 \cdot 2^{s+1}$ by Corollary 4.13. An application of Lemma 5.3 now finishes the proof. □

2.2. Case (K2). By Proposition 4.34 and Remark 4.31 we have that

$$a_{i,j} = d_0(i,j)\beta^{i-1}\alpha^{j-1} + d_1(i,j)\beta^{i-3}\alpha^{j-1} + d_2(i,j)\beta^{i-5}\alpha^{j-1}$$

for $i \geq 1$, $j > 1$, where

$$d_k(i,j) = \sum_{l=0}^{\lceil \frac{i-k}{3} \rceil - 1} \binom{k+3l+\lfloor \frac{j-2}{2} \rfloor}{\lfloor \frac{j-2}{2} \rfloor} \binom{i-1-(k+3l)+\lfloor \frac{j-1}{2} \rfloor}{\lfloor \frac{j-1}{2} \rfloor}.$$

Because $\beta^{i-1}\alpha^{j-1} = \beta^{(i-1) \bmod 3}\alpha^{(j-1) \bmod 2}$, $\beta^{i-3}\alpha^{j-1} = \beta^{i \bmod 3}\alpha^{(j-1) \bmod 2}$, $\beta^{i-5}\alpha^{j-1} = \beta^{(i-2) \bmod 3}\alpha^{(j-1) \bmod 2}$ are either three distinct rotations or three distinct reflections in D_6, by Lemma 5.1

$$a_{i,j} = 0 \text{ if and only if } d_0(i,j),\ d_1(i,j),\ d_2(i,j) \text{ have the same parity.} \tag{27}$$

By Corollary 4.18 there exists a non-decreasing sequence $(c_i)_{i=1}^{\infty}$, $c_i \in \mathbb{N} \cup \{0\}$, such that

$$P_i = 2 \cdot 2^{c_i} = 2^{c_i+1} \quad \text{for each } i \geq 1,$$

where $c_1 = 0$ and $c_{j+1} - c_j \leq 1$ for each $j \geq 1$.

LEMMA 5.5. *Let $c, s \in \mathbb{N} \cup \{0\}$. Then $a_{2^s+1,2^{c+1}} = 0$ if and only if one of the following conditions holds:*

- *$s < c$ or*
- *$s > c$ and $s - c$ is odd.*

PROOF. By (27), $a_{2^s+1,2^{c+1}} = 0$ if and only if the numbers $d_0(2^s+1, 2^{c+1})$, $d_1(2^s+1, 2^{c+1})$, and $d_2(2^s+1, 2^{c+1})$ have the same parity.

For $0 \le m \le 2^s$ put

$$B(c, s, m) = \binom{m + 2^c - 1}{2^c - 1}\binom{2^s - m + 2^c - 1}{2^c - 1}.$$

Then

$$d_k(2^s+1, 2^{c+1}) = \sum_{l=0}^{\left\lceil \frac{2^s+1-k}{3} \right\rceil - 1} B(c, s, k+3l).$$

For $k = 0, 1, 2$ denote

$$M_k = \left|\{m;\ m \equiv k \pmod 3,\ 0 \le m \le 2^s,\ B(c, s, m) \text{ is odd}\}\right|.$$

Then $d_k(2^s+1, 2^{c+1})$ is even if and only if M_k is even. It implies that $d_0(2^s+1, 2^{c+1})$, $d_1(2^s+1, 2^{c+1})$, $d_2(2^s+1, 2^{c+1})$ have the same parity if and only if M_0, M_1 and M_2 have the same parity.

Assume $s < c$. Then by Lemma 3.11, $B(c, s, m)$ is even for each $0 \le m \le 2^s$ and hence $M_0 = M_1 = M_2 = 0$.

Suppose that $s \ge c$. Then, by Lemma 3.11, $B(c, s, m)$ is odd if and only if $2^c \mid m$. Thus

$$M_k = \left|\{m;\ m \equiv k \pmod 3,\ m \equiv 0 \pmod{2^c},\ 0 \le m \le 2^s\}\right|.$$

The mapping $r \mapsto r2^c$ is a bijection between the set $\{r;\ 0 \le r \le 2^{s-c}\}$ and the set $\{m;\ m \equiv 0 \pmod{2^c},\ 0 \le m \le 2^s\}$. Moreover, $r_1 2^c \equiv r_2 2^c \pmod 3$ if and only if $r_1 \equiv r_2 \pmod 3$, and hence

$$M_{(k2^c) \bmod 3} = \left|\{r;\ r \equiv k \pmod 3,\ 0 \le m \le 2^{s-c}\}\right|.$$

Then $M_{(k2^c) \bmod 3} = \left\lceil \frac{2^{s-c}+1-k}{3} \right\rceil$ by Lemma 3.8.

If $2^{s-c} \equiv 1 \pmod 3$ then $\left\lceil \frac{2^{s-c}}{3} \right\rceil = \left\lceil \frac{2^{s-c}-1}{3} \right\rceil + 1$, which means that $M_{(1\cdot 2^c) \bmod 3} = M_{(2\cdot 2^c) \bmod 3} + 1$. For $2^{s-c} \equiv 2 \pmod 3$, $M_{(k2^c) \bmod 3} = \left\lceil \frac{2^{s-c}+1-k}{3} \right\rceil = \frac{2^{s-c}+1}{3}$ for each $k = 0, 1, 2$. This implies that the numbers M_0, M_1 and M_2 have the same parity if and only if $2^{s-c} \equiv 2 \pmod 3$, which is equivalent to $s - c$ being odd.

□

THEOREM 5.6. *Suppose that (K2) holds. Then*

$$P_i = 2^{\lceil \log_2 i \rceil + 1} \quad \text{for } i \ge 1.$$

PROOF. By Corollary 4.13, $P_1 = 2$. We show that $P_i = 2^{s+2}$ for $2^s + 1 \le i \le 2^{s+1}$, $s \ge 0$, using an induction in i.

By Lemma 5.5, $a_{2,2} \ne 0$. Hence $P_2 = 4$ by Corollary 4.13 and Corollary 4.17.

Assume that the statement holds for some $i \ge 2$. If $2^s + 1 \le i < 2^{s+1}$ then

$$\binom{k + 3l + 2^{s+1} - 1}{2^{s+1} - 1}\binom{i - (k+3l) + 2^{s+1} - 1}{2^{s+1} - 1}$$

is even for each $0 \le l \le \left\lceil \frac{i+1-k}{3} \right\rceil - 1$ and $k = 0, 1, 2$, by Lemma 3.11. Then $d_0(i+1, 2^{s+2})$, $d_1(i+1, 2^{s+2})$, and $d_2(i+1, 2^{s+2})$ are even, and hence $a_{i+1,2^{s+2}} = 0$ by (27). Thus $P_{i+1} = P_i = 2^{s+2}$ by Corollary 4.13.

In case that $i = 2^{s+1}$, we have $a_{2^{s+1}+1,P_i} = a_{2^{s+1}+1,2^{s+2}} \neq 0$ by Lemma 5.5. Hence $P_{i+1} = P_{2^{s+1}+1} = 2P_i = 2^{s+3}$ by Corollary 4.13 and Corollary 4.17.

□

2.3. Case (K3). By Proposition 4.35 we have that

$$a_{i,j} = d_0(i,j)(\alpha\beta)^{i-1}\alpha^{j-i} + d_1(i,j)(\alpha\beta)^{i-3}\alpha^{j-i} + d_2(i,j)(\alpha\beta)^{i-5}\alpha^{j-i},$$

where

$$d_k(i,j) = \sum_{l=0}^{\lceil \frac{i-k}{3} \rceil - 1} \binom{\lfloor \frac{i+j-2}{2} \rfloor}{i-1-(k+3l)} \binom{\lfloor \frac{i+j-1}{2} \rfloor}{k+3l} \quad \text{for } j \geq i \geq 0. \tag{28}$$

Because the automorphisms $(\alpha\beta)^{i-1}\alpha^{j-i} = (\alpha\beta)^{(i-1) \bmod 3}\alpha^{(j-i) \bmod 2}$, $(\alpha\beta)^{i-3}\alpha^{j-i} = (\alpha\beta)^{i \bmod 3}\alpha^{(j-i) \bmod 2}$ and $(\alpha\beta)^{i-5}\alpha^{j-i} = (\alpha\beta)^{(i-2) \bmod 3}\alpha^{(j-i) \bmod 2}$ are either three distinct rotations or three distinct reflections in D_6, by Lemma 5.1

$$a_{i,j} = 0 \text{ if and only if } d_0(i,j),\ d_1(i,j),\ d_2(i,j) \text{ have the same parity.} \tag{29}$$

By Corollary 4.18 there exists a non-decreasing sequence $(c_i)_{i=1}^{\infty}$, $c_i \in \mathbb{N} \cup \{0\}$, such that

$$P_i = 2 \cdot 2^{c_i} = 2^{c_i+1} \quad \text{for each } i \geq 1,$$

where $c_1 = 0$ and $c_{j+1} - c_j \leq 1$ for each $j \geq 1$.

THEOREM 5.7. *Suppose that (K3) holds. Then*

$$P_i = 2^{\lceil \log_2 i \rceil + 1} \quad \textit{for } i \geq 1.$$

PROOF. Corollary 4.13 gives that $P_1 = 2$. Next, we want to prove that

$$P_i = 2^{c+2} \quad \text{for } 2^c + 1 \leq i \leq 2^{c+1},\ c \geq 0.$$

According to Corollary 4.13 and Corollary 4.17 it is sufficient to show that for any $c \geq 0$,

$$a_{2^c+1,2^{c+1}} \neq 0 \quad \text{and} \quad a_{i,2^{c+2}} = 0 \quad \text{for } 2^c + 1 < i \leq 2^{c+1}.$$

By (29) this is equivalent to

(i) $d_0(2^c+1, 2^{c+1})$, $d_2(2^c+1, 2^{c+1})$, and $d_2(2^c+1, 2^{c+1})$ do not all have the same parity,
(ii) for each $2^c + 1 < i \leq 2^{c+1}$ the three numbers $d_0(i, 2^{c+2})$, $d_1(i, 2^{c+2})$, and $d_2(i, 2^{c+2})$ have the same parity.

First, we will prove (i). For $c = 0$, by the definition of the matrix $A_{\alpha,\beta}$, $a_{2^0+1,2^{0+1}} = a_{2,2} = \alpha\beta + \beta\alpha = \alpha\beta + (\alpha\beta)^2$. Using Lemma 5.1, $a_{2,2} \neq 0$. Now, suppose that $c \geq 1$. Since $2^{c+1} \geq 2^c + 1$, we may use (28) and so

$$d_k(2^c+1, 2^{c+1}) = \sum_{l=0}^{\lceil \frac{2^c+1-k}{3} \rceil - 1} \binom{2^{c-1}+2^c-1}{2^c-(k+3l)} \binom{2^{c-1}+2^c}{k+3l}.$$

By Lemma 3.13, the number $\binom{2^c+2^{c-1}-1}{2^c-m}\binom{2^c+2^{c-1}}{m}$ is odd if and only if $m = 0$ or $m = 2^c$. This means that $d_0(2^c+1, 2^{c+1})$ and $d_{2^c \bmod 3}(2^c+1, 2^{c+1})$ are odd and $d_{2^{c+1} \bmod 3}(2^c+1, 2^{c+1})$ is even.

Next, we will show (ii). Suppose that $c \geq 1$ and $2^c + 1 < i \leq 2^{c+1}$. Because $i < 2^{c+2}$, we can use (28).

If i is even then

$$d_k(i, 2^{c+2}) = \sum_{l=0}^{\lceil \frac{i-k}{3} \rceil - 1} \binom{\frac{i}{2}+2^{c+1}-1}{i-1-(k+3l)} \binom{\frac{i}{2}-1+2^{c+1}}{k+3l}.$$

If $\frac{i}{2}-1 < m \leq i-1$ then $\frac{i}{2}-1 < m < 2^{c+1}$ and hence $\binom{\frac{i}{2}-1+2^{c+1}}{m}$ is even by Lemma 3.12. If $0 \leq m < \frac{i}{2}$ then $\frac{i}{2}-1 < i-1-m < 2^{c+1}$ and so $\binom{\frac{i}{2}-1+2^{c+1}}{i-1-m}$ is even again by Lemma 3.12. Thus the number $\binom{\frac{i}{2}+2^{c+1}-1}{i-1-m}\binom{\frac{i}{2}-1+2^{c+1}}{m}$ is even for all $0 \leq m \leq i-1$, and hence $d_k(i, 2^{c+2})$ is even for each $k = 0, 1, 2$.

For i odd,

$$d_k(i, 2^{c+2}) = \sum_{l=0}^{\lceil \frac{i-k}{3} \rceil - 1} \binom{\frac{i-1}{2} + 2^{c+1} - 1}{i-1-(k+3l)} \binom{\frac{i-1}{2} + 2^{c+1}}{k+3l}.$$

If $\frac{i-1}{2} < m \leq i-1$ then $\frac{i-1}{2} < m < 2^{c+1}$ and hence $\binom{\frac{i-1}{2}+2^{c+1}}{m}$ is even by Lemma 3.12. If $0 \leq m < \frac{i-1}{2}+1$ then $\frac{i-1}{2}-1 < i-1-m < 2^{c+1}$ and so $\binom{\frac{i-1}{2}-1+2^{c+1}}{i-1-m}$ is even by Lemma 3.12. Therefore the number $\binom{\frac{i-1}{2}+2^{c+1}-1}{i-1-m}\binom{\frac{i-1}{2}+2^{c+1}}{m}$ is even for all $0 \leq m \leq i-1$, which implies that $d_k(i, 2^{c+2})$ is even for each $k = 0, 1, 2$.

□

3. Summary

In the previous sections we computed the minimal periods P_i for the central quasigroups of order 4. Corollary 4.13 says that the minimal period of the first row is $\mathrm{ord}(\alpha)$. The minimal periods P_i for $i > 1$ are in Table 7. The number of the isomorphism class refers to Table 1. Notice that the non-medial central quasigroups can have smaller periods than the medial quasigroups, although the structure of the medial quasigroups is simpler.

Theorem 4.15 says that $e_G \cdot \mathrm{lcm}(P_X, P_i)$ is a period of the ith row of the matrix $T_{(G,*),X,Y}$, where P_X is a period of X. Hence we can see at $e_G \cdot \mathrm{lcm}(P_X, P_i)$ as an upper estimate of the minimal period of the matrix $T_{(G,*),X,Y}$.

Isomorphism class	Quasigroup type	Underlying group	P_i	$e_G \,\mathrm{lcm}(P_X, P_i)$
1,2,3,4,6	Medial	V_4	$2^{\lceil \log_2 i \rceil}$	$2\,\mathrm{lcm}(P_X, 2^{\lceil \log_2 i \rceil})$
11,14	Central, non-medial	V_4	$\frac{3}{2}{\cdot}2^{\lceil \log_2 i \rceil}$	$2\,\mathrm{lcm}(P_X, \frac{3}{2} \cdot 2^{\lceil \log_2 i \rceil})$
10,12,13,15	Central, non-medial	V_4	$2{\cdot}2^{\lceil \log_2 i \rceil}$	$2\,\mathrm{lcm}(P_X, 2 \cdot 2^{\lceil \log_2 i \rceil})$
16,17,18,19	Medial	$\mathbb{Z}_4$	$2{\cdot}2^{\lceil \log_2 i \rceil}$	$4\,\mathrm{lcm}(P_X, 2 \cdot 2^{\lceil \log_2 i \rceil})$
5,7,8,9	Medial	V_4	$3{\cdot}2^{\lceil \log_2 i \rceil}$	$2\,\mathrm{lcm}(P_X, 3 \cdot 2^{\lceil \log_2 i \rceil})$

TABLE 7. The periods of $A_{\alpha,\beta}$ and $T_{(G,*),X,Y}$ for quasigroups of order 4

This implies that the minimal period of the ith row the matrix $T_{(G,*),X,Y}$ is less than $C \cdot i$ for some $C \in \mathbb{R}$.

CHAPTER 6

Stream cipher Edon-80

1. Description of the cipher

Edon-80 is a binary additive stream cipher (see Introduction), where the keystream is generated by a keystream generator.

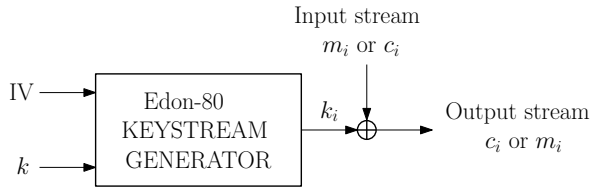


FIGURE 3. Graphical representation of Edon-80

Next, we will describe the keystream generator of Edon-80. It is composed of three phases: *KeySetup*, *IVSetup* and *Keystream* and it uses four quasigroups of order 4 which we will be denoted by $(Q, \cdot_i)$, $i = 0, 1, 2, 3$. These quasigroups are fixed. On Figure 3 we can see that the keystream generator has as input values IV and k. These values are called initial vector and key and both of them are some binary strings of length 80 bits. Because each number $0, 1, 2, 3$ corresponds to a 2-bit value, the binary strings k and IV can be represented as

$$k = K_0 \dots K_{39} \quad \text{and} \quad IV = v_0 \dots v_{39},$$

where $K_i, v_i \in \{0, 1, 2, 3\}$ for each $0 \le i \le 39$.

1. In *KeySetup* we define 80 quasigroups by

$$(Q, *_i) = \begin{cases} (Q, \cdot_{K_i}) & 0 \le i \le 39, \\ (Q, \cdot_{K_{i-40}}) & 40 \le i \le 79. \end{cases}$$

2. In *IVSetup* we construct from the vector IV values $y_0, \dots, y_{79}$, $y_i \in \{0, 1, 2, 3\}$. Let $\tau_{y,*} \colon \{0, 1, 2, 3\}^{80} \to \{0, 1, 2, 3\}^{80}$ be a left iterated translation defined in Chapter 4. Then

$$(y_0, \dots, y_{79}) = \tau_{K_0,*_{79}} \circ \tau_{K_1,*_{78}} \circ \dots \circ \tau_{K_{39},*_{40}} \circ \tau_{v_0,*_{39}} \circ \dots \circ \tau_{v_{39},*_0}(K_0, \dots, K_{39}, v_0, \dots, v_{39}).$$

$*_i$		K_0	$\cdots$	K_{39}	v_0	$\cdots$	v_{39}
$*_0$	v_{39}	$s_{0,0}$	$\cdots$	$s_{0,39}$	$s_{0,40}$	$\cdots$	$s_{0,79}$
$*_1$	v_{38}	$s_{1,0}$	$\cdots$	$s_{1,39}$	$s_{1,40}$	$\cdots$	$s_{1,79}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$*_{39}$	v_0	$s_{39,0}$	$\cdots$	$s_{39,39}$	$s_{39,40}$	$\cdots$	$s_{39,79}$
$*_{40}$	K_{39}	$s_{40,0}$	$\cdots$	$s_{40,39}$	$s_{40,40}$	$\cdots$	$s_{40,79}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$*_{78}$	K_1	$s_{78,0}$	$\cdots$	$s_{78,39}$	$s_{78,40}$	$\cdots$	$s_{78,79}$
$*_{79}$	K_0	y_0	$\cdots$	y_{39}	y_{40}	$\cdots$	y_{79}

FIGURE 4. *IVSetup*

3. In *Keystream* we generate the sequence $(t_{79,i})_{i=0}^{\infty}$ using $(y_0, \ldots, y_{79})$ from *IVSetup*. The mapping $\tau_{y,*}\colon \{0,1,2,3\}^{\mathbb{N}} \to \{0,1,2,3\}^{\mathbb{N}}$ is also a left iterated translation defined in Chapter 4. The output $(t_{79,i})_{i=0}^{\infty}$ is given by

$$(t_{79,i})_{i=0}^{\infty} = \tau_{y_{79},*_{79}} \circ \cdots \circ \tau_{y_0,*_0}((i \bmod 4)_{i=0}^{\infty}).$$

Then the keystream is the sequence $(k_i)_{i=1}^{\infty} = (t_{79,2i+1})_{i=0}^{\infty}$ (we take every second value of the output).

$*_i$		0	1	2	3	0	1	2	3	0	...
$*_0$	y_0	$t_{0,0}$	$t_{0,1}$	$t_{0,2}$	$t_{0,3}$	$t_{0,4}$	$t_{0,5}$	$t_{0,6}$	$t_{0,7}$	$t_{0,8}$	$\cdots$
$*_1$	y_1	$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$t_{1,3}$	$t_{1,4}$	$t_{1,5}$	$t_{1,6}$	$t_{1,7}$	$t_{1,8}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$				
$*_{79}$	y_{79}	$t_{79,0}$	$\boldsymbol{t_{79,1}}$	$t_{79,2}$	$\boldsymbol{t_{79,3}}$	$t_{79,4}$	$\boldsymbol{t_{79,5}}$	$t_{79,6}$	$\boldsymbol{t_{79,7}}$	$t_{79,8}$	$\cdots$

FIGURE 5. *Keystream*

2. Quasigroups in Edon-80

The stream cipher Edon-80 uses four fixed quasigroups of order 4, see Figure 6.

$\cdot_0$	0	1	2	3
0	0	2	1	3
1	2	1	3	0
2	1	3	0	2
3	3	0	2	1

$\cdot_1$	0	1	2	3
0	1	3	0	2
1	0	1	2	3
2	2	0	3	1
3	3	2	1	0

$\cdot_2$	0	1	2	3
0	2	1	0	3
1	1	2	3	0
2	3	0	2	1
3	0	3	1	2

$\cdot_3$	0	1	2	3
0	3	2	1	0
1	1	0	3	2
2	0	3	2	1
3	2	1	0	3

FIGURE 6. The quasigroups used in Edon-80

The quasigroups $(Q, \cdot_0)$, $(Q, \cdot_1)$, $(Q, \cdot_2)$, $(Q, \cdot_3)$ are isomorphic to the quasigroups from Table 1 with numbers 28, 23, 30 and 25, respectively. This means that the quasigroups $(Q, \cdot_1)$ and $(Q, \cdot_3)$ are right holomorphic, and $(Q, \cdot_0)$, $(Q, \cdot_3)$ are only isotopic to the Abelian group $\mathbb{Z}_4$.

These quasigroups were chosen based on computer experiments, because they gave the longest periods and no regular output. (To test this, the authors use modified keystream mode with only one quasigroup operation.)

Let $(Q, *)$ be a quasigroup and $Y = (y_i)_{i=1}^{\infty}$ be a sequence of elements from Q. From a periodic sequence $X \in Q^{\infty}$ we generated sequences using the left iterated translations $\tau_{y_i,(Q,*)}$ and we tried to describe how the periods of the generated sequence change. We have found out that for central quasigroup $(Q, *)$ of order 4 the periods of these sequences increase at most linearly. This means that the periods increase slowly, however Edon-80 needs to generate sequences whose periods grow rapidly. It means that the central quasigroups of order 4 are not very suitable for implementation in Edon-80.

Corollary 4.30 indicates that the periods increase much faster when using the quasigroups for which the exponent of the underlying group factorises to a bigger number of distinct primes. Further, it is more convenient to use non-central quasigroups. For those the authors of Edon-80 conjecture that the periods increase exponentially.

Moreover, it appears that the use of the sequence $012301230123\ldots$ which has period 4 as a vector X is a mistake. Indeed, by Lemma 4.7, the longer the period of X, the longer the period of the keystream.

Bibliography

[D1] Aleš Drápal, *On multiplication groups of relatively free quasigroups isotopic to Abelian groups*, Czechoslovak Math. J. **55** (2005), 61–86.

[D2] Aleš Drápal, *Group isotopes and a holomorphic actions*, to appear in Results in Mathematics.

[D3] Aleš Drápal, *Teorie grup základní aspekty*, Karolinum, Praha, 2000.

[E] eSTREAM, ECRYPT stream cipher project,
`http://www.ecrypt.eu.org/stream/edon80p3.html`

[H] J. Hong, *Remarks on the Period of Edon80*, eSTREAM, ECRYPT stream cipher project,
`http://www.ecrypt.eu.org/stream/papersdir/041.pdf`

[HV] Václav J. Havel, Alena Vanžurová, *Medial Quasigroups and Geometry*, Palacký University, Olomouc, 2006.

[G] D. Gligoroski, S. Markovski, L. Kocarev and M. Gušev, *Understanding Periods in Edon80*, eSTREAM, ECRYPT stream cipher project,
`http://www.ecrypt.eu.org/stream/papersdir/054.pdf`

[P] `http://planetmath.org/encyclopedia/KummersTheorem.html`

[PJS] Heinz-Otto Peitgen, Hartmut Jürgens, Dietmar Saupe, *Chaos and fractals: new frontiers of science*, Springer-Verlag, New York, 2004.

[S] Jonathan D. H. Smith, *An Introduction to Quasigroups and Their Representations*, Studies in Advanced Mathematics, Chapman & Hall/CRC, 2007.