Doctoral School of Mathematics and Computer Science
Bolyai Institute
Faculty of Science and Informatics
University of Szeged

Ph.D. thesis

Constructions, classifications and embeddings of abstract unitals

Dávid Csaba Mezőfi

Szeged, 2020

Supervisor: Dr. Gábor Péter Nagy

Acknowledgements

I would like to express my gratitude to my supervisor, dr. Gábor Péter Nagy, for his advices, time and support from the beginning of my studies at the university. I learned much from him during my years of study. I would also like to thank everyone in the Bolyai Institute.

I am extremely grateful to my family for their support, this thesis would not been possible without them.

Contents

List of tables

List of GAP codes

List of algorithms

1. Introduction

The classification of combinatorial structures has been a significant research topic for a long time and our main concern is designs with parameters $t = 2$ and $\lambda = 1$. Important classes of such 2-designs are affine and projective planes, Steiner triple systems and abstract unitals. The thesis concentrates on abstract unitals, especially on the embeddability of unitals into the classical projective plane taking advantage of the full points of unitals and on creating new unitals via paramodification.

The structure of the thesis is as follows. Chapter 2 introduces some fundamental concepts and results essentially to understand better the notion of full points and paramodifications of unitals, presented later in Chapters 3 and 4. In Section 2.1 we examine the topic of t-(v, k, λ) designs. The necessary preliminary material about projective planes and polarities is covered in Section 2.2. The combinatorial properties of Hermitian curves in $\mathrm{PG}\big(2, q^2\big)$ will lead us to abstract unitals, defined as 2-$\big(n^3 + 1, n + 1, 1\big)$ designs. Sections 2.3 and 2.4 define the semidirect products of groups, construct the 1-dimensional affine group $\mathrm{AGL}(1, q)$ as a semidirect product and classifies the subgroups of $\mathrm{AGL}(1, q)$ with the help of translations.

In Chapter 3 we present a construction, called paramodification (as the construction modifies the parallelism of a subsystem) of 2-designs, which can produce new Steiner 2-designs from old ones with the same parameter set, based on the paper *New Steiner 2-designs from old ones by paramodifications* [39]. As shown in Section 3.2, a paramodification of a 2-$(v, k, 1)$ design affects k columns of the incidence matrix, all belonging to the k points of a fixed block. We prove that paramodifications affecting exactly two columns are switches (or switchings), and we give a sufficient condition for a Steiner 2-design not to allow a switching. This condition implies that Hermitian unitals have no switchings, but they do have non-trivial paramodifications. Section 3.3 examines paramodifications of affine planes, Steiner triple systems, and unitals in details. In Sections 3.4 and 3.5, we give an overview of the algorithmic and complexity aspects of the computation of paramodifications, and we present the computational results showing that paramodifications can construct many new unitals.

Chapter 4 summarises the results of the paper *On the geometry of full points of abstract unitals* [38]. In Section 4.1 we give definitions and basic combinatorial properties of full points and related concepts. The main result of this paper is proved in Section 4.2. It shows that for any abstract unital of order q embedded in the finite classical projective plane $\mathrm{PG}(2, q^2)$, the set of full points of two disjoint blocks is contained in a line. Moreover, the perspectivities of two disjoint blocks generate a semi-regular cyclic permutation group acting on each block. Unitals fulfilling these necessary conditions will be called strongly full point regular unitals. Section 4.3 describes the structure of full points in the classical Hermitian unitals. In Section 4.4 we give an overview of the computational results about full points in abstract unitals of order 3 and 4 belonging to known libraries. For the computation we used the GAP package UnitalSZ [42].

Computing paramodifications, full points and other properties of unitals described in Chapters 3 and 4 by hand is tedious. Chapter 5 describes the main tools implemented in the GAP [14] package UnitalSZ [42] for these purposes. The author of this thesis and his supervisor dr. Gábor Péter Nagy developed the package to extend the popular computer algebra system GAP with features related to unitals, since GAP doesn't have built-in support of them. Section 5.1 describes functions for constructing unitals using incidence (boolean) matrices or the list of blocks, and functions to retrieve basic properties of unitals: the set of points, blocks, the automorphism group, and isomorphism between unitals. In Section 5.2 we list the available classes and libraries (unitals resulting from [2, 8, 34, 35]) of unitals, e.g. Hermitian unitals, Buekenhout–Metz unitals, KRC and KNP unitals. Section 5.3 displays the functions related to computing full points and perspectivity groups of unitals. Some implementations are outlined using pseudocode, and the usage of the presented functions are also illustrated including the output of the code.

In Chapter 6 we summarise the main concepts and results of the thesis in English and in Hungarian as well. Appendix A contains the source code of the implementation of paramodifications using the package UnitalSZ.

2. Preliminaries

2.1. Designs

This section introduces the concept of incidence structures, with an emphasis on Steiner 2-designs following the terminology of [7].

Incidence structures

The triple $(\mathcal{P}, \mathcal{B}, I)$ is an *incidence structure*, provided $\mathcal{P}$, $\mathcal{B}$ are disjoint sets, and $I \subseteq \mathcal{P} \times \mathcal{B}$. The elements of $\mathcal{P}$ and $\mathcal{B}$ will be called *points* and *blocks*, respectively. One may simply write $P\ I\ b$ instead of $(P, b) \in I$.

Definition 2.1.1. The incidence structure is *simple*, if $(b_1) \neq (b_2)$ whenever b_1 and b_2 are distinct blocks. Here (b) denotes the set $\{P \in \mathcal{P} \colon P\ I\ b\}$.

For a simple incidence structure we may identify each block b with the corresponding point set (b) and we can assume that $I = \in$, the membership relation.

Definition 2.1.2. Let $\mathbf{D} = (\mathcal{P}, \mathcal{B}, I)$ be a finite incidence structure, and label the points as $P_1, P_2, \ldots, P_v$ and the blocks as $b_1, b_2, \ldots, b_b$. Then the matrix $\mathbf{M} = (m_{ij})$, $(i = 1, 2, \ldots, v;\ j = 1, 2, \ldots, b)$ defined by

$$m_{ij} = \begin{cases} 1 & \text{if } P_i\ I\ b_j \\ 0 & \text{otherwise} \end{cases}$$

is called the *incidence matrix* of $\mathbf{D}$.

Proposition 2.1.3. *Let* $\mathbf{D}$ *be an incidence structure with v points, b blocks such that every point is incident with r blocks and every block is incident with k points. Then*

$$vr = bk.$$

Proof. See the proof of [7, Proposition 1.6]. □

Definition 2.1.4. Let $\mathbf{D} = (\mathcal{P}, \mathcal{B}, I)$ be a finite incidence structure. For subsets $\mathcal{P}' \subseteq \mathcal{P}$ and $\mathcal{B}' \subseteq \mathcal{B}$ and $I' = I \cap (\mathcal{P}' \times \mathcal{B}')$, one has the *incidence substructure* $(\mathcal{P}', \mathcal{B}', I')$.

By some abuse of notation, we may denote the latter by $(\mathcal{P}', \mathcal{B}', I)$ as well. The substructure *induced by* $\mathcal{P}' \subseteq \mathcal{P}$ is defined with the set $\mathcal{B}'$ of blocks meeting $\mathcal{P}'$ in at least two points. Notice that for a substructure, a block $b \in \mathcal{B}'$ is not necessarily a subset of $\mathcal{P}'$.

Steiner systems

Let t and λ be positive integers and $\mathbf{D} = (\mathcal{P}, \mathcal{B}, I)$ a finite incidence structure. Then $\mathbf{D}$ is called a *t-design* with parameters k and λ if and only if

(i) any t-subset $\mathcal{Q}$ of the point set $\mathcal{P}$ is incident with exactly λ blocks, and

(ii) any block is incident with exactly k points.

A t-design on v points is called an $\mathrm{S}_\lambda(t, k, v)$ or a t-(v, k, λ) design. In case $\lambda = 1$, it is called a *Steiner system* $\mathrm{S}(t, k, v)$. A 2-design on v points is called a *block design*.

Theorem 2.1.5. *Let* $\mathbf{D}$ *be an* 2-(v, k, λ) *design. Then we have:*

(i) every point P is incident with r blocks and

$$r = \frac{\lambda\,(v-1)}{k-1};$$

(ii) for the number of blocks $|\mathcal{B}|$

$$|\mathcal{B}| = \lambda \frac{v\,(v-1)}{k\,(k-1)}.$$

Proof. See the proof of [7, Theorem 2.10]. □

Definition 2.1.6. An $\mathrm{S}(2, 3, v)$ is called a *Steiner triple system* $\mathrm{STS}(v)$.

Definition 2.1.7. A 1-design $\mathrm{S}_r(1, k, v)$ is called a *tactical configuration* (or simply configuration) with parameters v, r, k and the number of blocks $b = vr/k$.

Partitions of the set of blocks and resolvability

Let $\mathbf{D} = (\mathcal{P}, \mathcal{B}, I)$ be an incidence structure and let $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_m$ be a partition of the set of blocks. Then the induced substructures $\mathbf{D}_i = (\mathcal{P}, \mathcal{B}_i, I \cap (\mathcal{P} \times \mathcal{B}_i))$ $(i = 1, \ldots, m)$ are said to form a *partition* of $\mathbf{D}$. We will often call $\mathcal{B}_1, \ldots, \mathcal{B}_m$ a partition of $\mathbf{D}$, too. Each $\mathbf{D}_i$ (or briefly each $\mathbf{B}_i$) is called a part of $\mathbf{D}$.

Definition 2.1.8. Let $\mathbf{D}$ be a t-design. If a part of $\mathbf{D}$ is an $\mathrm{S}_r(1, k, v)$, it is called an *r-factor* or, for $r = 1$, a *parallel class* of $\mathbf{D}$. If every part in a partition $\mathbf{B}_1 \cup \cdots \cup \mathbf{B}_m$ of $\mathbf{D}$ is an r-factor, then the partition is called an *r-factorisation* and D is said to be *r-resolvable*. A 1-factorisation is also called a *parallelism* or a *resolution*; instead of 1-resolvable one simply uses the term *resolvable*.

A resolvable Steiner system $\mathrm{S}_\lambda(t, k, v)$ is abbreviated as $\mathrm{RS}_\lambda(t, k, v)$.

2.2. Unitals

This section presents a brief introduction to projective planes, collineations, etc. based on [5, 30], focusing on concepts closely related to Hermitian curves, the so-called *classical unitals*.

Projective planes

A *projective plane* Π is a set of objects, called points, together with certain subsets of points, called lines, such that

1. any two distinct points are contained in a unique common line,
2. any two distinct lines meet in a unique point,
3. there exist four points, no three of which are contained in a common line.

The axioms for a projective plane are *self-dual*, in the sense that one may interchange points and lines and thereby obtain another projective plane, called the *dual* of the original projective plane.

Theorem 2.2.1 (Principle of Duality)**.** *If a theorem is valid for all projective planes, then the dual theorem obtained by interchanging the notions of point and line is also valid for all projective planes.*

However, a projective plane and its dual need not be isomorphic.

Definition 2.2.2. Let Π_1 and Π_2 be projective planes. An *isomorphism* from Π_1 to Π_2 is a bijection ϕ from the points and lines of Π_1 to the points and lines of Π_2 that preserves containment. That is, a point P lies on a line ℓ of Π_1 if and only if the point P^ϕ lies on the line ℓ^ϕ of Π_2. If such a map exists, then Π_1 and Π_2 are called *isomorphic*, denoted by $\Pi_1 \cong \Pi_2$. If $\Pi_1 = \Pi_2$, then an isomorphism from Π_1 to itself is called an *automorphism* (or *collineation*) of Π_1.

Example 2.2.3. Let V be a three-dimensional vector space over some field (or skew field) $\mathbb{F}$. Take as *points* the one-dimensional subspaces of V and as *lines* the two-dimensional subspaces of V. A point is said to lie on a line if the one-dimensional subspace associated with the point is contained in the two-dimensional subspace associated with the line. Then the resulting structure is a projective plane, denoted by $\mathrm{PG}(2, \mathbb{F})$. Once again, if $\mathbb{F}$ is a finite field, one obtains a finite projective plane.

Remark 2.2.4. There do exist projective planes which are not isomorphic to $\mathrm{PG}(2, \mathbb{F})$ for any field (or skew field) $\mathbb{F}$. One example is the so-called Moulton plane (see [9], for instance). The projective planes isomorphic to some $\mathrm{PG}(2, \mathbb{F})$ will be called *classical projective planes*.

In the finite setting $\mathbb{F} = \mathrm{GF}(q)$ for some prime power q, where $\mathrm{GF}(q)$ denotes the Galois field of order q (unique up to isomorphism). In this case we denote $\mathrm{PG}(2, \mathbb{F})$ by $\mathrm{PG}(2, q)$. Straightforward counting shows that each line of $\mathrm{PG}(2, q)$ has $q + 1$ points, each point lies on $q + 1$ lines, and the total number of points (or lines) is $q^2 + q + 1$. This pattern holds in general for any finite projective plane, whether or not it is classical. An elementary counting argument yields the following.

Theorem 2.2.5. *Let Π be any finite projective plane. Then there is some integer $n \geq 2$, called the* order *of Π , such that*

1. *each line of Π contains $n + 1$ points,*
2. *each point of Π lies on $n + 1$ lines,*
3. *the number of points of Π is $n^2 + n + 1$,*
4. *the number of lines of Π is $n^2 + n + 1$.*

One can axiomatize a projective geometry in general, but that is beyond the scope of this thesis. Analogously to the method described in Example 2.2.3 the *classical projective geometry of dimension d*, denoted by $\mathrm{PG}(d, \mathbb{F})$, could also be constructed.

Classical projective planes are also called *Desarguesian*. This is because a result involving the Desargues' configuration holds in a projective geometry if and only if the projective geometry arises from a vector space over a skew field; that is, if and only if the projective geometry is classical.

In the classical (Desarguesian) setting, one has the advantage of working with the underlying vector space. Consider the projective plane $\mathrm{PG}(2, \mathbb{F})$ for some (skew) field $\mathbb{F}$, and let V denote the underlying three-dimensional vector space over $\mathbb{F}$. Fix some ordered basis for V, and represent each vector uniquely as a 3-tuple of scalars with respect to this basis. These are the so-called *homogeneous coordinates* of P. Since each point P of $\mathrm{PG}(2, \mathbb{F})$ is a one-dimensional subspace $\langle \mathbf{v} \rangle$ of V, the coordinates of P are determined only up to nonzero scalar multiples:

$$\{\mathbf{x} = (x_0, x_1, x_2) : x_0, x_1, x_2 \in \mathbb{F}, \text{ not all zero}\},$$

with the convention that (x_0, x_1, x_2) and $t\,(x_0, x_1, x_2)$, $t \in \mathbb{F} \setminus \{0\}$, represent the same point.

Any line ℓ of $\mathrm{PG}(2, \mathbb{F})$ is represented by a homogeneous linear equation

$$u_0 X_0 + u_1 X_1 + u_2 X_2 = 0$$

in the three variables X_0, X_1, X_2 for some coefficients a $u_0, u_1, u_2 \in \mathbb{F}$, not all 0. The ordered coefficients $\mathbf{u} = (u_0, u_1, u_2)$ of such an equation, unique up to nonzero scalar multiples, are the *homogeneous dual coordinates* of the line ℓ.

Finite fields

Recall that every finite field must have prime power order, and given any prime power q, there is a unique field (up to isomorphism) with q elements. As introduced in earlier, we will use the notation $\mathrm{GF}(q)$ to denote this field. The multiplicative group $\mathrm{GF}^*(q) = \mathrm{GF}(q) \setminus \{0\}$ of $\mathrm{GF}(q)$ is cyclic, and any generator of this multiplicative group is called a *primitive element* of the field. The additive group of $\mathrm{GF}(q)$ is an elementary abelian p-group, where q is a power of the prime p, the *characteristic* of $\mathrm{GF}(q)$, denoted by $\operatorname{char} \mathrm{GF}(q) = p$. The mapping $x \mapsto x^p$ is a field automorphism of $\mathrm{GF}(q)$, often called the *Frobenius automorphism*. In fact, if $q = p^e$, the automorphism group of $\mathrm{GF}(q)$ is cyclic of order e, generated by the Frobenius automorphism.

We will primarily be interested in finite fields which admit an *involutory* field automorphism; that is, an automorphism of order 2. The order of such a field must be square, and the mapping

$$\sigma\colon \mathrm{GF}(q^2) \to \mathrm{GF}(q^2), \quad x \mapsto x^q$$

will then be the (unique) involutory field automorphism of $\mathrm{GF}(q^2)$. Its fixed field is the subfield $\mathrm{GF}(q)$ of $\mathrm{GF}(q^2)$.

Polarities

Let $\mathbf{A}$ be a nonsingular 3×3 matrix over $\mathrm{GF}(q)$. Then the map

$$\mathbf{x} \mapsto \mathbf{x}\mathbf{A}$$

determines a collineation $\varphi_{\mathbf{A}}$ of $\mathrm{PG}(2, q)$, that is called a *projectivity* or *projective linear transformation*. Note that, $\varphi_{\mathbf{A}} = \varphi_{\mathbf{B}}$ if and only if $\mathbf{A} = \lambda \mathbf{B}$ for some scalar $\lambda \in \mathrm{GF}(q)$. If $\mathbf{A}$ is the matrix of a projectivity transforming points, then $\left(\mathbf{A}^{-1}\right)^\top$ is transforming lines.

Let σ be an automorphism of $\mathrm{GF}(q)$. Then the map

$$(x_0, x_1, x_2) = \mathbf{x} \mapsto \mathbf{x}^\sigma = (x_0^\sigma, x_1^\sigma, x_2^\sigma)$$

determines also a collineation of $\mathrm{PG}(2, q)$.

The previous transformations are collineations analogously in higher dimension projective geometries as well. Surprisingly, there are no other types of collineations:

for a proof of the following fundamental result see the references before [30, Theorem 4.10].

Theorem 2.2.6. *Every collineation of* $\mathrm{PG}(d, \mathbb{F})$*,* $d \geq 2$*, can be written as*

$$\mathbf{x} \mapsto \mathbf{x}^{\sigma}\mathbf{A},$$

where σ *is an automorphism of* $\mathbb{F}$ *and* $\mathbf{A}$ *is a* $(d+1) \times (d+1)$ *nonsingular matrix over* $\mathbb{F}$*.*

Definition 2.2.7. Let Π be a projective plane and let Π^* denote its dual plane. Then an $\alpha\colon \Pi \to \Pi^*$ bijection which preserves containment, is called a *correlation*. Any α correlation is also a $\Pi^* \to \Pi$ correlation as well. If the correlation α has order two, namely $\alpha \circ \alpha$ is the identity collineation of Π, then α is called a *polarity*.

Let ρ be a polarity of some projective plane. If P is a point, the line P^{ρ} is called the *polar line* of P. Similarly, if ℓ is a line, the point ℓ^{ρ} is called the *pole* of ℓ.

Definition 2.2.8. Let ρ be a polarity of some projective plane Π. A point P of Π is called *absolute* (or *self-conjugate*) if $P \in P^{\rho}$; else, P is called *nonabsolute*. Similarly, a line ℓ of Π is called absolute (or self-conjugate) if $\ell^{\rho} \in \ell$; or nonabsolute otherwise.

Our goal is to describe a special case of polarities in $\mathrm{PG}(2, q)$. If ρ is a polarity and $\mathbf{x}$ denotes the coordinate vector of an arbitrary point in the plane, then using Theorem 2.2.6

$$(\mathbf{x}^{\rho})^{\rho} = (\mathbf{x}^{\sigma}\mathbf{A})^{\rho} = (\mathbf{x}^{\sigma}\mathbf{A})^{\sigma}\left(\mathbf{A}^{-1}\right)^{\top} = \mathbf{x}^{\sigma^2}\mathbf{A}^{\sigma}\left(\mathbf{A}^{-1}\right)^{\top}.$$

As ρ is a polarity, there exists some $0 \neq t \in \mathrm{GF}(q)$, such that

$$t\mathbf{x} = \mathbf{x}^{\sigma^2}\mathbf{A}^{\sigma}\left(\mathbf{A}^{-1}\right)^{\top}$$

holds for every $\mathbf{x}$. This is true if and only if σ^2 is the identity and $t\mathbf{A}^{\top} = \mathbf{A}^{\sigma}$. We are interested in the case when σ is *not* the identity. We have seen, that q must be a square in this case, hence we can assume without loss of generality that our plane is $\mathrm{PG}(2, q^2)$ and σ is the unique involutory automorphism $x \mapsto x^q$ of $\mathrm{GF}(q^2)$. This type of polarity is called *unitary polarity*.

Nondegenerate Hermitian curves

Let ρ be a unitary polarity of $\mathrm{PG}(2, q^2)$. The set of absolute points of ρ and is called a *nondegenerate Hermitian curve* denoted by $\mathcal{H}(q)$.

Remark 2.2.9. Over finite fields all Hermitian curves are nonempty.

It is easy to verify that exactly the points of a nondegenerate Hermitian curve satisfies the equation $\mathbf{x}^{\sigma}\mathbf{A}\mathbf{x}^{\top} = 0$. Also, any nondegenerate Hermitian curve of $\mathrm{PG}(2, q^2)$ can be mapped to any other nondegenerate Hermitian curve of $\mathrm{PG}(2, q^2)$ by some projectivity of $\mathrm{PG}(2, q^2)$. We thus say that $\mathcal{H}$ is uniquely determined, up to *projective equivalence*. Hence, choosing $\mathbf{A}$ to be the identity matrix, the canonical form of the equation of $\mathcal{H}$ is

$$X_0^{q+1} + X_1^{q+1} + X_2^{q+1} = 0.$$

For the proofs of the following theorems please refer to [5, Section 2.1].

Theorem 2.2.10. *A nondegenerate Hermitian curve $\mathcal{H}$ in $\mathrm{PG}(2, q^2)$ has precisely $q^3 + 1$ points.*

Theorem 2.2.11. *Let $\mathcal{H}$ be a nondegenerate Hermitian curve in $\mathrm{PG}(2, q^2)$. Then every line of $\mathrm{PG}(2, q^2)$ meets $\mathcal{H}$ in 1 or $q + 1$ points.*

A line meeting $\mathcal{H}$ in one point will be called a *tangent line* of the curve, and a line meeting $\mathcal{H}$ in $q + 1$ points will be called a *secant line* of the curve.

Abstract unitals

Let $\mathcal{H} = \mathcal{H}(q)$ be a nondegenerate Hermitian curve in $\mathrm{PG}(2, q^2)$. Any two distinct points of $\mathcal{H}$ uniquely determine a line of $\mathrm{PG}(2, q^2)$, which is necessarily a secant line meeting $\mathcal{H}$ in $q + 1$ points. Hence, if we take the $q^3 + 1$ points of $\mathcal{H}$ as the points of our design and take all the secant line intersections with $\mathcal{H}$ as our blocks, we obtain a 2-$(q^3 + 1, q + 1, 1)$ design.

Definition 2.2.12. Let n be an integer, $n \geq 3$. A *unital of order n* is any 2-$(n^3 + 1, n + 1, 1)$ design.

Remark 2.2.13. Note that if $n = 2$, then a 2-$(9, 3, 1)$ design is an affine plane of order 3. Thus we require $n \geq 3$ in our definition of a unital.

The nondegenerate Hermitian curve $\mathcal{H}(q)$ is often called the *classical unital* of order q. We say that a unital U is *embedded* in a projective plane if the points of U are points of the plane and each block is a set of collinear points of the plane.

2.3. Semidirect products of groups

In this section we define the semidirect product of groups, for further details we refer the reader to [24, Chapter 19].

Outer semidirect product

Let us consider two groups N and S, and a homomorphism $\phi\colon S \to \mathrm{Aut}\,(N)$ from S to the automorphism group of N. Now we can define an operation over the Cartesian product $S \times N$ the following way: let the product of (s_1, n_1) and (s_2, n_2) be

$$(s_1, n_1)\,(s_2, n_2) = \left(s_1 s_2, n_1^{\phi(s_2)} n_2\right). \tag{2.1}$$

This operation is well-defined and it yields an element from the set $S \times N$. Let us denote by $S \ltimes_\phi N$ the Cartesian product $S \times N$ equipped with the product operation defined as in (2.1). It is easy to verify that $S \ltimes_\phi N$ is a group, indeed.

Definition 2.3.1. The group $S \ltimes_\phi N$ is called the (outer) *semidirect product* of the groups S and N with respect to the homomorphism $\phi\colon S \to \mathrm{Aut}(N)$.

When it is clear from the context, which homomorphism ϕ from S to the automorphism group of N is considered, then we often omit the homomorphism ϕ and only use the notation $S \ltimes N$.

Let us denote the semidirect product of S and N by G, namely $G = S \ltimes_\phi N$ and consider the projection

$$\pi_S\colon G \to S, \quad (s, n) \mapsto s.$$

The fact that the projection π_S from $G = S \ltimes_\phi N$ to the group S is a surjective homomorphism is an immediate consequence of the definition of G. The kernel of the homomorphism π_S is $\{1_S\} \times N$, hence N is isomorphic to the kernel of π_S, i.e. $\mathrm{Ker}(\pi_S) \cong N$. Since $\{1_S\} \times N$ is the kernel of some homomorphism on G, it is a normal subgroup of G. Moreover, notice that $S \times \{1_N\}$ is a subgroup of G.

Inner semidirect product

Consider a group G and a normal subgroup $N \lhd G$ and a subgroup $S \leq G$, such that $G = NS$, and the intersection of S and N consists of only the identity 1. In this case we say, that S is a complement of N in G. Let us take the elements s_1, s_2 and n_1, n_2 from S and N respectively and write up the product

$$s_1 n_1 \cdot s_2 n_2 = s_1 s_2 \cdot \left(s_2^{-1} n_1 s_2\right) n_2. \tag{2.2}$$

Notice that the term in the parentheses is the conjugate of n_1 by s_2.

Let us denote by $\phi(s)$ the conjugation by an element s from S, namely

$$\phi(s)\colon N \to N, \quad n \mapsto s^{-1} n s = n^{\phi(s)}.$$

Since N is a normal subgroup of G, then $\phi(s)$ is an automorphism of N, namely $\phi(s) \in \operatorname{Aut}(N)$, therefore $\phi\colon S \to \operatorname{Aut}(N)$. Now we can reformulate (2.2) as

$$s_1 n_1 \cdot s_2 n_2 = s_1 s_2 \cdot n_1^{\phi(s_2)} n_2, \tag{2.3}$$

where $\phi\colon S \to \operatorname{Aut}(N)$. Notice the resemblance between (2.1) and (2.3): now G is a semidirect product of its normal subgroup N and subgroup S, indeed.

2.4. The general affine group and its subgroups

The example of general affine groups illustrates semidirect products quite well. The construction is based on the ideas in [23] and [10].

The general affine group as a semidirect product

Let $\mathbb{F}$ be field and define the 1-dimensional affine group as follows.

Definition 2.4.1. The set of affine maps from $\mathbb{F}$ to itself of the form

$$z \mapsto az + b, \quad a, b \in \mathbb{F} \text{ and } a \neq 0$$

is called the *1-dimensional* affine group over $\mathbb{F}$ and is denoted by $\mathrm{AGL}(1, \mathbb{F})$. In the special case when $\mathbb{F}$ is the finite field of order q the notation $\mathrm{AGL}(1, q)$ is often used in place of $\mathrm{AGL}(1, \mathbb{F})$.

Affine maps are closed under composition and inverses, hence $\mathrm{AGL}(1, \mathbb{F})$ is a group, indeed. To see that $\mathrm{AGL}(1, \mathbb{F})$ is a semidirect product, let us consider two subsets of the affine group. Let N be the set of *translations* and let S be the set of *scalings*, namely

$$\begin{aligned} N &= \{z \mapsto z + b \colon b \in \mathbb{F}\} = \{\tau_b \colon b \in \mathbb{F}\}\,; \\ S &= \{z \mapsto az \colon a \in \mathbb{F}^*\} = \{\sigma_a \colon a \in \mathbb{F}^*\}\,, \end{aligned} \tag{2.4}$$

where $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$. These two sets are subgroups of the affine group and $NS = \mathrm{AGL}(1, \mathbb{F})$. Moreover N and S are isomorphic to the additive and multiplicative subgroups of $\mathbb{F}$ respectively, i.e.

$$\begin{aligned} N &= \{\tau_b \colon b \in \mathbb{F}\} \cong (\mathbb{F}; +)\,; \\ S &= \{\sigma_a \colon a \in \mathbb{F}^*\} \cong (\mathbb{F}^*; \cdot)\,. \end{aligned} \tag{2.5}$$

It is easy to see that the projection

$$\pi_S\colon \mathrm{AGL}(1,\mathbb{F}) \to S, \quad (z \mapsto az+b) \mapsto \sigma_a$$

is a surjective homomorphism and its kernel is N, hence $N \lhd \mathrm{AGL}(1,\mathbb{F})$, namely N is a normal subgroup of the affine group. Also the only element of $N \cap S$ is the identity map and $NS = \mathrm{AGL}(1,\mathbb{F})$, therefore the affine group is a(n inner) semidirect product of N and S, namely $\mathrm{AGL}(1,\mathbb{F}) = S \ltimes N$.

Subgroups of the general affine group

From now on we assume that the field $\mathbb{F}$ is finite, namely $\mathbb{F} = \mathrm{GF}(q)$ for some prime power q and $\operatorname{char}\mathrm{GF}(q) = p$. Let α be an arbitrary element of the affine group $\mathrm{AGL}(1,q)$. There are three possible cases for the number of fixed points by α.

1. *There is only one fixed point*. This is the case when $\alpha \in \mathrm{AGL}(1,q)$ has the form $z \mapsto az+b$ where $a \neq 1$. Moreover, for the order of α denoted by $o(\alpha)$

$$o(\alpha) = o(a) \mid |\mathrm{GF}^*(q)| = q-1 \tag{2.6}$$

since

$$z^{\alpha^{o(a)}} = a^{o(a)}z + b\frac{a^{o(a)}-1}{a-1} = z.$$

2. *There is no fixed point*. This occurs when $\alpha \in N$ is a *translation*, i.e. α has the form $z \mapsto z+b$ where b is a nonzero element of $\mathbb{F}$. Then for the order of α holds

$$o(\alpha) = o(b) = p = \operatorname{char}\mathrm{GF}(q). \tag{2.7}$$

3. *Every point is fixed*. This is the simplest case: α is the identity.

Let G be a subgroup of $\mathrm{AGL}(1,q)$ and examine this subgroup G in the aspect of its intersection with the normal subgroup N as defined in (2.4).

If $|G \cap N| = 1$, meaning that the intersection consists only of the identity element, then there is no proper translation in G. By the First Isomorphism Theorem

$$GN/N \cong G/G \cap N \cong G$$

as $G \cap N$ is trivial group. On the other hand

$$G \cong GN/N \leq \mathrm{AGL}(1,q)/N \cong S \cong \mathrm{GF}^*(q) \tag{2.8}$$

by (2.5), which means that G is isomorphic to a subgroup of the multiplicative group of $\mathrm{GF}(q)$, thus G is cyclic and Abelian. Let α_1 be an arbitrary element of G different from the identity. Since α_1 can't be a translation, it must have a fixed point, denote it by z_1, namely $z_1^{\alpha_1} = z_1$. Moreover, this is the only fixed point of α_1. Let α_2 be an other element of G: then since G is Abelian

$$\begin{aligned} \alpha_2\alpha_1 &= \alpha_1\alpha_2 \\ \alpha_1 &= \alpha_2^{-1}\alpha_1\alpha_2 \end{aligned}$$

and $z_1^{\alpha_2}$ is clearly a fixed point of $\alpha_2^{-1}\alpha_1\alpha_2$, i.e. a fixed point of α_1. This means that $z_1 = z_1^{\alpha_2}$ as z_1 is the unique fixed point of α_1, thus z_1 is fixed by α_2 as well. Therefore z_1 is fixed by all elements of G.

If $|G \cap N| \neq 1$ then $G \cap N = M \lhd G$, namely the intersection M is a normal subgroup of G. Moreover, $M \leq N$ and as $N \cong (\mathrm{GF}(q); +)$ by (2.5), the subgroup M is isomorphic to a subgroup of the additive group of the finite field $\mathrm{GF}(q)$.

3. Paramodifications of unitals

In general, the classification of combinatorial structures with a given set of parameters is an old and important research topic; for details, we refer the reader to the monographs [1, 28, 7]. Our main concern yields to designs with parameters $t = 2$ and $\lambda = 1$, which are called *Steiner 2-designs* or *linear spaces* in the literature, see [1, Definition 2.4.9]. Important classes of Steiner 2-designs are affine and projective planes of order q, Steiner triple systems, and abstract unitals of order q; the respective parameters (v, k) are (q^2, q), $(q^2 + q + 1, q + 1)$, $(v, 3)$ and $(q^3 + 1, q + 1)$.

This chapter is based on the paper *New Steiner 2-designs from old ones by paramodifications* [39]. The main result of this paper is a general construction which can produce new Steiner 2-designs from old ones, with the same parameters. We call this construction *paramodification* of 2-designs, since it modifies the parallelism of a subsystem. Our research has been motivated by a construction of Grundhöfer, Stroppel and Van Maldeghem [19], which produced new abstract unitals with many translation centers, see also [40]. Our construction is not completely new, in essence, Petrenjuk and Petrenjuk described it in technical reports of the University of Kirovograd (Ukraine) in the 1980s, see [45] and its references. In particular, A. J. Petrenjuk used the method, named *cut-transformations,* to construct new abstract unitals of order 3.

As shown in Section 3.2, a paramodification of a 2-$(v, k, 1)$ design affects k rows of the incidence matrix, all belonging to the k points of a fixed block. We prove that paramodifications affecting exactly two rows are *switches*. A switch or *switching* is a local transformation of a combinatorial structure, which was studied for graphs, partial geometries, Steiner triples systems, codes, and other objects since the early 1980s. For the presentation of the switching principle, unification of earlier results and computational applications, see the excellent paper [44] by Östergård. In Proposition 3.2.3, we give a sufficient condition for a Steiner 2-design not to allow a switching. This condition implies that Hermitian unitals have no switchings, but they do have non-trivial paramodifications.

In Section 3.3, we study in more detail the paramodifications of affine planes, Steiner triple systems, and unitals. In the last two sections, we give an overview of the algorithmic and complexity aspects of the computation of the paramodification. We also present computational results which show that that paramodification can construct many new unitals.

3.1. Paramodification of 2-designs

Let $\mathbf{D} = (\mathcal{P}, \mathcal{B}, I)$ be a t-(v, k, λ) design. By [7, Theorem 1.9], the integer

$$r = \lambda \frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}} = \frac{|\mathcal{B}|\, k}{n} \tag{3.1}$$

is the number of blocks through a given point. The map $\chi\colon \mathcal{B} \to X$ is called a *proper block coloring* of $\mathbf{D}$, if for different blocks b, b', $b \cap b' \neq \emptyset$ implies $\chi(b) \neq \chi(b')$. If $|X| = m$ and $\mathbf{D}$ has a proper block coloring $\chi\colon \mathcal{B} \to X$ then we say that $\mathbf{D}$ is *block m-colorable.*

Lemma 3.1.1. *Let $\mathbf{D} = (\mathcal{P}, \mathcal{B}, I)$ be a t-(v, k, λ) design.*

(i) Any proper block coloring of $\mathbf{D}$ needs at least r colors.

(ii) Any parallelism of $\mathbf{D}$ defines a block coloring with r colors when mapping each block to its parallel class.

(iii) The color classes of a block coloring with r colors form a parallelism of $\mathbf{D}$.

(iv) $\mathbf{D}$ is block r-colorable if and only if it is resolvable.

Proof. Since $r = |\mathcal{B}|\, k/n$ is the number of blocks through a point, and these blocks must have different colors, we have (i). (ii) is trivial by definition. If we have r colors, then for any point P and color x, there is a unique block on P with color x. That is, the color class $\chi^{-1}(x)$ is a partition of $\mathcal{P}$, i.e. (iii) holds. (iv) follows from (ii) and (iii). □

From now on, $\mathbf{D} = (\mathcal{P}, \mathcal{B}, I)$ denotes a Steiner 2-design on v points. The incidence relation $I = \in$, that is, the blocks of $\mathbf{D}$ are subsets of size k of $\mathcal{P}$. Notice that for subsets $\mathcal{P}' \subseteq \mathcal{P}$ and $\mathcal{B}' \subseteq \mathcal{B}$, we may consider the subsystem $\mathbf{D}' = (\mathcal{P}', \mathcal{B}', I)$, even if an element $b' \in \mathcal{B}'$ is not a subset of $\mathcal{P}'$.

Fix a block $b \in \mathcal{B}$ and consider the subset

$$C(b) = \left\{ b' \in \mathcal{B} \colon |b' \cap b| = 1 \right\} \tag{3.2}$$

of blocks. We write $\mathbf{D}_b$ for the subsystem $(\mathcal{P} \setminus b, C(b), I)$. We define the map $\chi_b \colon C(b) \to b$ by

$$\chi_b \colon b' \mapsto b' \cap b; \tag{3.3}$$

this is clearly a block coloring of $\mathbf{D}_b$.

Lemma 3.1.2. *$\mathbf{D}_b$ is a resolvable 1-$(v-k, k-1, k)$ design.*

Proof. Trivially, each block $b' \in C(b)$ is incident with $k-1$ point $P \in \mathcal{P} \setminus b$, that is, $\mathbf{D}_b$ is 1-$(v-k, k-1, k)$ design. In $\mathbf{D}_b$, (3.1) implies $r = k$ and the map $\chi_b \colon b' \mapsto b' \cap b$ is a block coloring with k colors. By Lemma 3.1.1, $\mathbf{D}_b$ is resolvable. □

We aim to show that any parallelism of $\mathbf{D}_b$ leads to a block design $\mathbf{D}'$ such that $\mathbf{D}$ and $\mathbf{D}'$ have the same parameters, and they may or may not be isomorphic. To use consistent notation, we identify the notions of a parallelism and a block coloring with r colors.

Definition 3.1.3. Let $\mathbf{D} = (\mathcal{P}, \mathcal{B}, I)$ be a Steiner 2-$(v, k, 1)$ design. Let $b \in \mathcal{B}$ be a block and $\chi \colon C(b) \to b$ a block coloring of the subsystem $\mathbf{D}_b$ with k colors. Define the incidence relation $I^* \subseteq \mathcal{P} \times \mathcal{B}$ by

$$P \ I^* \ b' \Leftrightarrow \begin{cases} P \ I \ b', & \text{if } b' \notin C(b) \text{ or } P \not I b \\ P = \chi(b'), & \text{if } P \ I \ b \text{ and } b' \in C(b). \end{cases} \tag{3.4}$$

We call the incidence structure

$$\mathbf{D}^* = \mathbf{D}^*_{\chi,b} = (\mathcal{P}, \mathcal{B}, I^*)$$

the (χ, b)-*paramodification* of $\mathbf{D}$.

Theorem 3.1.4 ([39, Theorem 2.4])**.** *Let $\mathbf{D} = (\mathcal{P}, \mathcal{B}, I)$ be a Steiner 2-$(v, k, 1)$ design. Let $b \in \mathcal{B}$ be a block and $\chi \colon C(b) \to b$ a block coloring of the subsystem $\mathbf{D}_b$ with k colors. Then, $\mathbf{D}^*_{\chi,b}$ is a Steiner 2-design with the same parameters.*

Proof. We have to show that any two points are incident with a unique block of $\mathbf{D}^* = \mathbf{D}^*_{\chi,b}$. Let $P_1, P_2 \in \mathcal{P}$ be distinct points, and $\beta \in \mathcal{B}$ the unique $\mathbf{D}$-block such that $P_1 \ I \ \beta$ and $P_2 \ I \ \beta$.

1. $P_1, P_2 \notin b$. Then $P_1 \ I^* \ \beta$ and $P_2 \ I^* \ \beta$ by (3.4). Let $\gamma \in \mathcal{B}$ be a block such that $P_1 \ I^* \ \gamma$ and $P_2 \ I^* \ \gamma$. Then $P_1 \ I \ \gamma$ and $P_2 \ I \ \gamma$ also by (3.4), therefore $\gamma = \beta$ as $\mathbf{D} = (\mathcal{P}, \mathcal{B}, I)$ is a Steiner 2-$(v, k, 1)$ design.

2. $P_1, P_2 \in b$. Then $\beta = b$ as $\mathbf{D}$ is a Steiner 2-$(v,k,1)$ design. Note that $b \notin C(b)$ by the definition of $C(b)$ in (3.2), hence $P_1\ I^*\ b$ and $P_2\ I^*\ b$. Let $\gamma \in \mathcal{B}$ be a block such that $P_1\ I^*\ \gamma$ and $P_2\ I^*\ \gamma$. If $\gamma \notin C(b)$, then $P_1\ I\ \gamma$ and $P_2\ I\ \gamma$ by (3.4), therefore $\gamma = b = \beta$. If $\gamma \in C(b)$, then by (3.4)
$$\chi(\gamma) = P_1 \neq P_2 = \chi(\gamma),$$
a contradiction.
3. $P_1 \notin b$ and $P_2 \in b$. In this case, $\beta \in C(b)$ and $P_2\ I^*\ \beta$ if and only if $\chi(\beta) = P_2$. By Lemma 3.1.1, χ defines a parallelism, and the color class $\chi^{-1}(P_2)$ is a parallel class in $\mathbf{D}_b$. Hence, there is a unique block $\gamma \in C(b)$ such that $P_1\ I\ \gamma$ and $\chi(\gamma) = P_2$. Equation (3.4) implies $P_1, P_2\ I^*\ \gamma$. □

In general, it is not easy to determine if two paramodifications of $\mathbf{D}$ are isomorphic. We introduce the following terminology.

Definition 3.1.5. The block coloring $\chi_b \colon C(b) \to b$, $b' \mapsto b \cap b'$ is the *trivial block coloring* of the Steiner 2-design $\mathbf{D}$. Two block colorings χ and ψ of $C(b)$ are said to be *equivalent* if they have the same color classes. The Steiner system $\mathbf{D}$ is said to be *para-rigid* if, for any block b, all block colorings of $\mathbf{D}_b$ are equivalent to the trivial one.

Remark 3.1.6.

(i) One has $\mathbf{D} = \mathbf{D}^*_{\chi_b,b}$.

(ii) The block colorings χ and ψ are equivalent if there is a permutation π of the points on b such that $\psi(b') = \pi(\chi(b'))$ holds for all $b' \in C(b)$.

(iii) We claim that equivalent block colorings result isomorphic paramodifications. Indeed, we can extend π to $\mathcal{P}$ such that $\pi(P) = P$ when $P \notin b$. Then, π determines an isomorphism between $\mathbf{D}^*_{\psi,b}$ and $\mathbf{D}^*_{\chi,b}$.

(iv) If all paramodifications of the Steiner 2-design $\mathbf{D}$ are isomorphic to $\mathbf{D}$, then we say that the paramodifications of $\mathbf{D}$ do not yield new Steiner 2-designs. Paramodifications of a para-rigid Steiner 2-design do not yield new Steiner 2-designs. The converse is not valid; see Remark 3.3.2.

3.2. Paramodification and the incidence matrix

In this section, we describe the effect of paramodifications to the incidence matrix.

Proposition 3.2.1 ([39, Proposition 3.1]). *Let $\mathbf{D}$ be a Steiner 2-$(v, k, 1)$ design and $\mathbf{D}^* = \mathbf{D}^*_{\chi,b}$ be a (χ, b)-paramodification of $\mathbf{D}$. Let $r = (v-1)/(k-1)$. Then, the respective incidence matrices $\mathbf{M}$ and $\mathbf{M}^*$ differ at most in a $k \times k(r-1)$ submatrix.*

Proof. Equation (3.4) implies that the incidence matrices differ in the rows corresponding to the points of b, and in the columns corresponding to blocks in $C(b)$. Clearly, $|b| = k$ and $|C(b)| = k\,(r-1)$. □

To have a more detailed description of the structure of the incidence matrices, consider the $v \times b$ incidence matrix $\mathbf{M}$ of the system $\mathbf{D}$ in the following way:

1. Let the first k rows of $\mathbf{M}$ correspond to the points $P_1, P_2, \ldots, P_k \in b$.
2. Let the first $r-1$ columns of $\mathbf{M}$ correspond to the blocks in $C(b)$ incident with P_1, then let the second $r-1$ columns correspond to the blocks in $C(b)$ incident with P_2, and so on until P_k.
3. Right behind the columns corresponding to $C(b)$, put the column corresponding to b.
4. Then comes the rest of the blocks $\mathcal{B} \setminus (C(b) \cup b)$ in any order.

The incidence matrix has the form

$$\mathbf{M} = \begin{pmatrix} \mathbf{C}_b & \mathbf{j}_k & \mathbf{0} \\ \mathbf{M}_1 & \mathbf{0}_{v-k} & \mathbf{M}_2 \end{pmatrix}, \tag{3.5}$$

where

$$\mathbf{C}_b = \begin{pmatrix} \mathbf{j}^\top & \mathbf{0}^\top & \cdots & \mathbf{0}^\top \\ \mathbf{0}^\top & \mathbf{j}^\top & \cdots & \mathbf{0}^\top \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}^\top & \mathbf{0}^\top & \cdots & \mathbf{j}^\top \end{pmatrix}$$

is a $k \times k\,(r-1)$ matrix, and $\mathbf{j}$, $\mathbf{0}$ are column vectors of length $r-1$.

It is easy to see by the definition of I^* in (3.4), that the incidence matrix $\mathbf{M}^*$ of the new system $\mathbf{D}^*$ has the form

$$\mathbf{M}^* = \begin{pmatrix} \mathbf{C}^*_b & \mathbf{j}_k & \mathbf{0} \\ \mathbf{M}_1 & \mathbf{0}_{v-k} & \mathbf{M}_2 \end{pmatrix},$$

where except $\mathbf{C}^*_b$ all the other submatrices are the same as in (3.5). Hence $\mathbf{M}$ and $\mathbf{M}^*$ differ at most in a $k \times k\,(r-1)$ submatrix. Finally, we notice that equivalent block colorings correspond to the permutations of the first k rows of $\mathbf{M}$.

In [44], the author defines the switching operation for constant weight codes as a transformation that concerns exactly two coordinates and keeps the studied parameter of the code unchanged. For a design $\mathbf{D}$, this means that the incidence matrix is modified in exactly two rows. As the number of 1s is constant in each column, one can interchange the 0-1 and 1-0 combinations of the two rows only. This implies the following proposition:

Proposition 3.2.2 ([39, Proposition 3.2]). *Let P, Q be two points of the Steiner 2-design $\mathbf{D}$. Let b be the unique block on P and Q. A switching with respect to P and Q is a (χ, b)-paramodification. Moreover, if the block $b' \in C(b)$ is not incident with P or Q, then it has trivial color: $\chi(b') = b \cap b'$. Conversely, a (χ, b)-paramodification is a switching if and only if precisely two color classes of χ are non-trivial.* □

In a Steiner 2-design, a *Pasch configuration* consists of six points $P_1, \ldots, P_6$ such that the triples $\{P_1, P_3, P_4\}$, $\{P_1, P_5, P_6\}$, $\{P_2, P_3, P_5\}$, $\{P_2, P_4, P_6\}$ are collinear. The design is *anti-Pasch* if it does not contain any Pasch configuration. Pasch configurations are known to play an important role in switches of Steiner 2-designs.

Proposition 3.2.3 ([39, Proposition 3.3]). *Let $\mathbf{D}$ be an anti-Pasch 2-$(v, k, 1)$ design. If*

$$v < 2k^3 - 8k^2 + 13k - 6,$$

then no switching can be carried out for $\mathbf{D}$.

Proof. Each point is incident with $r = (v-1) \,/\, (k-1)$ blocks, and the condition is

$$(k-1)\,(k-2) + 1 > \frac{1}{2}\,(r-1)\,.$$

Assume that a switching can be carried out with respect to the points R, Q. Let $C(Q, R)$ be the set of blocks containing precisely one of Q and R. The $2\,(r-1)$ blocks are colored with two colors, say red and blue such that blocks with the same color intersect in Q or R. As the switching is non-trivial, there are both red and blue blocks on Q. We can assume that at least half of the blocks on Q are red. Let a be a blue block on Q, incident with the points $Q, A_1, \ldots, A_{k-1}$. For each $i \in \{1, \ldots, k-1\}$, the block RA_i is all red; let $R, A_i, P_{i1}, \ldots, P_{i,k-2}$ be its points. If the points Q, P_{is}, P_{jt} are collinear with $i \neq j$, then the six points $Q, R, A_i, A_j, P_{is}, P_{jt}$ form a Pasch configuration. Hence, the blocks QP_{is} are different for all $i \in \{1, \ldots, k-1\}$ and $s \in \{1, \ldots, k-2\}$. Moreover, QP_{is} is blue since it meets the red RA_i. This shows that there are at least $(k-1)\,(k-2) + 1$ blue blocks on Q, a contradiction. □

3.3. Paramodification for classes of 2-designs

In this section, we discuss the paramodification of certain well-known classes of Steiner 2-designs.

Projective and affine planes

The case of a finite projective plane is trivial. While the case of a finite affine plane is easy, we are not aware of any occurrence of this construction in the literature, and we give a detailed proof.

Proposition 3.3.1 ([39, Proposition 4.1])**.**

(i) Paramodifications of a finite projective plane are isomorphic. In other words, finite projective planes are para-rigid.

(ii) Paramodifications of a finite affine plane are associated with the same projective plane.

Proof.

(i) Let $\mathbf{D}$ be a projective plane of order q. For any line b, $\mathbf{D}_b$ is an affine plane of order q with a unique parallelism. Hence, the proper block colorings of $C(b)$ are equivalent, and the corresponding paramodifications are isomorphic.

(ii) Let $\mathbf{D} = (\mathcal{P}, \mathcal{B}, I)$ be an affine plane of order q. $\mathbf{D}$ can be embedded in a projective plane $\Pi = \left(\overline{\mathcal{P}}, \overline{\mathcal{B}}, \overline{I}\right)$ of order q, and Π is unique up to isomorphism. We show that any paramodification $\mathbf{D}^*_{\chi,b}$ of $\mathbf{D}$ can be embedded in Π. This is obvious if χ and χ_b are equivalent. From now on, we assume that this is not the case, that is, there are distinct lines $\ell_1, \ell_2 \in C(b)$ such that $\chi(\ell_1) = \chi(\ell_2)$ and $\ell_1 \cap \ell_2 \notin b$. Not meeting on b and being disjoint off b, the lines ℓ_1, ℓ_2 must be parallel in $\mathbf{D}$. Take a third line $\ell_3 \in C(b)$ in the same color class, $\ell_3 \neq \ell_1, \ell_2$. At least one of $\ell_1 \cap \ell_3$, $\ell_2 \cap \ell_3$ does not lie on b, we must have $\ell_1 \parallel \ell_2 \parallel \ell_3$. Being of the same size q, the color class of ℓ_1 coincides with its parallel class.

We claim that any color class κ of χ is a parallel class of $\mathbf{D}$. To show this, it suffices to find two lines $m_1, m_2 \in \kappa$ such that $m_1 \cap m_2 \notin b$. Then, the argument above proves that κ is indeed a parallel class. Fix $m_1 \in \kappa$ and define $Q = m_1 \cap b$. Let ℓ be the unique line which is parallel to ℓ_1 and incident with Q. Then $\ell \notin \kappa$, and therefore κ has a line m_2 with is not incident with Q. Hence, $m_1 \cap m_2 \notin b$, and the claim follows.

Let ℓ_∞ be the line at infinity with respect to $\mathbf{D}$ in Π. For the (affine) point $P \in b$, let $\varepsilon(P)$ be the infinite point of the parallel class $\chi^{-1}(P)$. For $P \in \mathcal{P} \setminus b$, we put $\varepsilon(P) = P$. It is straightforward to show that ε is an embedding of $\mathbf{D}^*_{\chi,b}$ in Π, which finishes the proof. □

Remark 3.3.2. Let $\mathbf{D}$ be a finite Desarguesian affine plane. While $\mathbf{D}$ is not para-rigid, it is isomorphic to any of its paramodifications.

Steiner triple systems

A Steiner triple system $\mathrm{STS}(v)$ is a 2-$(v,3,1)$ design; an $\mathrm{STS}(v)$ exists if and only if $v \equiv 1,3 \pmod 6$. Steiner triples systems, cubic graphs (regular graphs of degree 3), and edge colorings are much connected from different points of view. For example, many recent papers deal with edge colorings of cubic graphs by Steiner triples systems, see [18] and the references therein. Our approach seems to have in common with the study of cubic trades in Steiner triples systems [12].

Let $\mathbf{T} = (\mathcal{P}, \mathcal{B}, I)$ be an $\mathrm{STS}(v)$ and fix a triple $b = \{x, y, z\} \in \mathcal{B}$. Then, the meaning Lemma 3.1.2 is that $\mathbf{T}_b$ is a simple cubic graph whose edges can be colored by three colors. Vizing's celebrated edge-coloring theorem asserts that any cubic graph can be edge-colored by three or four colors in such a way that adjacent edges receive distinct colors. Although three colors are not enough to color all cubic graphs, and the corresponding decision problem is difficult [22]. Paramodifications of $\mathbf{T}$ correspond to edge 3-colorings of $\mathbf{T}_b$. Let Γ be an edge 3-colored cubic graph. The union of two color classes is a regular subgraph of degree 2; hence it is the disjoint union of cycles of even length. Let $\gamma = \{v_1, \dots, v_{2m}\}$ be such a cycle. By switching the two colors in γ we obtain a new edge 3-coloring of Γ which is equivalent to the original one if and only if $v = 2m + 1$. Recently, cycles in cubic graphs, their length and especially Hamiltonian cycles are a central and well-studied topic in graph theory, see [11, 41, 17, 15]. The authors of this paper are not aware of any results which could help to describe the structure of edge 3-colored cubic graphs, which occur as $\mathbf{T}_b$ for a Steiner triples system $\mathbf{T}$.

We close the paramodifications of Steiner triple systems by formulating an open problem. Notice that the Steiner triple system $\mathbf{T}$ is para-rigid, if the cubic graph $\mathbf{T}_b$ has a unique edge 3-coloring for each block b.

Problem 3.3.3. *Are there para-rigid Steiner triple systems?*

This problem could be tested on anti-Pasch (quadrilateral-free) Steiner triple systems, for which switching gives nothing. Anti-Pasch Steiner triple systems are very scarce, see [37] and the references therein.

Unitals with many translation centers

The idea of the paramodification of Steiner 2-designs has been motivated by the following construction of Grundhöfer, Stroppel and Van Maldeghem [19]. Our presentation restricts to the finite case.

Let q be an integer, G a group of order $q^3 - q$. Let T be a subgroup of order q such that conjugates T^g and T^h have trivial intersection unless they coincide (i.e., the conjugacy class T^G forms a T.I. set). Assume that there is a subgroup S of order $q + 1$ and a collection $\mathcal{D}$ of subsets of G such that

(D1) each set $D \in \mathcal{D}$ contains 1,

(D2) any $D \in \mathcal{D}$ has size $q + 1$,

(D3) $|\mathcal{D}| = q - 2$.

(D4) For each $D \in \mathcal{D}$, the map

$$(D \times D) \setminus \{(x, x) : x \in D\} \to G, \quad (x, y) \mapsto xy^{-1}$$

is injective.

Furthermore, we assume that the following property holds:

(P) The system consisting of $S \setminus \{1\}$, all conjugates of $T \setminus \{1\}$ and all sets

$$D^* = \left\{xy^{-1} \colon x, y \in D, x \neq y\right\}$$

with $D \in \mathcal{D}$ forms a partition of $G \setminus \{1\}$.

We define an incidence structure with point set $\mathcal{P} = G \cup [\infty]$ and block set $\mathcal{B} = \mathcal{B}^\infty \cup \{[\infty]\}$, where

$$\mathcal{B}^\infty = \{Sg \colon g \in G\} \cup \left\{T^h g \colon h, g \in G\right\} \cup \{Dg \colon D \in \mathcal{D}, g \in G\}$$

and the block at infinity

$$[\infty] = \left\{T^h \colon h \in G\right\}$$

consists of the conjugates of T in G. We define two incidence relations I and $I^\flat$. For both, $g \in G$ and $b \in \mathcal{B}^\infty$ are incident if and only if $g \in b$. Moreover, the points on the block at infinity $[\infty]$ are precisely the conjugates of T. One defines the incidence between an affine block and a point at infinity in two different ways.

(a) Make each T^h incident with each coset $T^{hg^{-1}}g = gT^h$ (and no other block in $\mathcal{B}^\infty$). This gives an incidence structure $\mathbb{U}_\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$.

(b) Make each conjugate T^h incident with each coset $T^h g$ (and no other block in $\mathcal{B}^\infty$). This gives an incidence structure $\mathbb{U}^\flat_\mathcal{D} = \left(\mathcal{P}, \mathcal{B}, I^\flat\right)$.

Then both $\mathbb{U}_\mathcal{D}$ and $\mathbb{U}^\flat_\mathcal{D}$ are linear spaces and the following hold.

(i) $\mathbb{U}_{\mathcal{D}}$ and $\mathbb{U}^\flat_{\mathcal{D}}$ are 2-$\left(q^3+1, q+1, 1\right)$ designs; i.e., unitals of order q.

(ii) Via multiplication from the right on G and conjugation on the point row of $[\infty]$, the group G acts as a group of automorphisms on $\mathbb{U}_{\mathcal{D}}$.

(iii) On $\mathbb{U}_{\mathcal{D}}$ the group G also acts by automorphisms via multiplication from the right on G but trivially on the point row of $[\infty]$.

(iv) On the unital $\mathbb{U}_{\mathcal{D}}$ each conjugate of T acts as a group of translations. Thus each point on the block $[\infty]$ is a translation center, and G is two-transitive on $[\infty]$.

(v) On the unital $\mathbb{U}^\flat_{\mathcal{D}}$ the group G contains no translation except the trivial one.

It is immediate that $\mathbb{U}_{\mathcal{D}}$ and $\mathbb{U}^\flat_{\mathcal{D}}$ are paramodifications. Indeed, the set

$$C([\infty]) = \left\{T^h g \colon h, g \in G\right\}$$

of blocks consists of right cosets of a conjugate of T, which are at the same time left cosets of another conjugate of T. With $b' = T^h g = g T^{hg} \in C([\infty])$, the two block colorings are

$$\chi(b') = T^h, \quad \chi^\flat(b') = T^{hg}.$$

Starting with $G = \mathrm{SU}(2, q)$, the subgroups T, S and the system $\mathcal{D}$ can be chosen such that $\mathbb{U}_{\mathcal{D}}$ is isomorphic to the classical Hermitian unital of order q, and $\mathbb{U}^\flat_{\mathcal{D}}$ is isomorphic to Grüning's unital [20], embedded in Hall planes and their duals, see [19, Section 3.1]. In particular, Grüning's unitals are paramodifications of the classical Hermitian unitals.

In [19], the authors construct two more non-classical unitals $\mathbb{U}_{\mathcal{E}}$, $\mathbb{U}^\flat_{\mathcal{E}}$ of order 4. In this case, $G = \mathrm{SU}(2, 4) \cong \mathrm{SL}(2, 4) \cong A_5$. Using a computer, Verena Möhler (Karlsruhe) [40] found further non-classical unitals of the form $\mathbb{U}_{\mathcal{D}}$ and $\mathbb{U}^\flat_{\mathcal{D}}$ for $G = \mathrm{SL}(2, 8)$.

We finish this section with an observation on finite Hermitian unitals.

Proposition 3.3.4 ([39, Proposition 4.4])**.** *Finite Hermitian unitals have no switchings, but they do have non-trivial paramodifications.*

Proof. As Hermitian unitals are anti-Pasch by O'Nan's result [43, Section 3], Proposition 3.2.3 implies that finite Hermitian unitals have no switchings. However, as mentioned above, Grüning's unitals are non-isomorphic paramodifications of finite Hermitian unitals. □

3.4. Effective computation of block colorings

Let $\mathbf{D} = (\mathcal{P}, \mathcal{B}, I)$ be a Steiner 2-$(v, k, 1)$ design. Let $b \in \mathcal{B}$ be a block and consider the subsystem $\mathbf{D}_b = (\mathcal{P} \setminus b, C(b), I)$. We are interested in the effective computation of all block colorings of $\mathbf{D}_b$ to construct new Steiner 2-designs of given parameters by paramodification. We formulate the problem in the language of vertex colorings of simple graphs, which is known to be NP-complete in general. However, there are methods to deal with it for certain ranges of parameters. We compare two methods, the first one is based on clique partitions, and the other is based on integer linear programming.

The *line graph* $\Gamma = (V, E)$ of $\mathbf{D}_b$ is defined by $V = C(b)$, and $(b_1, b_2) \in E$ if and only if b_1 and b_2 have a unique point $P \notin b$ in common. A straightforward consequence of Lemma 3.1.2 is that Γ is a $(k-1)^2$-regular simple graph. A proper block coloring $\chi\colon C(b) \to b$ of the subsystem $\mathbf{D}_b$ is equivalent with a proper vertex coloring of the graph Γ using k colors. We can make this equivalence more precise by using the notion of vertex b-colorings. The latter has been introduced by Irving and Manlove [25], see also the recent survey paper [27] with special emphasis on the complexity and algorithmic aspects of computing the b-chromatic number of a simple graph.

Definition 3.4.1. Let $G = (V, E)$ be a simple graph and $\chi\colon V \to C$ a proper vertex coloring. The vertex $v \in V$ is called *dominant*, if for any color $c' \in C \setminus \{\chi(v)\}$ there is a neighbor v' of v such that $\chi(v') = c'$. The coloring χ is said to be a *b-coloring* if there is at least one dominant vertex in each color class.

Lemma 3.4.2. *The map $\chi\colon C(b) \to b$ is a proper block coloring of $\mathbf{D}_b$ if and only if it is a b-coloring of the line graph Γ of $\mathbf{D}_b$.*

Proof. If χ is a b-coloring of Γ, then it is also a proper block coloring of $\mathbf{D}_b$ trivially. Let $\chi\colon C(b) \to b$ be a proper block coloring of $\mathbf{D}_b$ using k colors. We show that each block β is a dominant vertex of Γ. Fix a point $P \in \beta \setminus b$. By Lemma 3.1.2, there are precisely k blocks in $C(b)$ incident with P; hence these k blocks (including the block β) form a k-clique in Γ. Therefore the block coloring χ must assign different colors to these k blocks, which means that every block in the clique is dominant, and the blocks are colored with k different colors. □

Colorings by the set cover method

One way to compute all b-colorings of the graph Γ is to find all solutions of a set cover problem of independent sets. In fact, a color class is an independent set of size

$K = (v - k) / (k - 1)$ and the k color classes of a coloring χ are pairwise disjoint. The first step is to compute the set Y of independent K-sets of Γ. In the second step, one constructs the graph Γ^* with vertex set Y and edges (S_1, S_2) with disjoint S_1, S_2. In the last step, we determine all cliques of size k of Γ^*. Using the GRAPE package [46] of GAP [14], this approach is easy to implement. Moreover, GRAPE allows the user to exploit the automorphism group of the Steiner 2-design **D** and the automorphism group of the graph Γ, which makes the computation quite efficient.

Colorings by integer linear programming

The b-coloring problem can be formulated as an integer linear programming (ILP) problem [27, Section 8.4], for an exact formulation see [31, Section 2]. Most of the ILP solvers are optimized to find one solution to each problem. However, for our block coloring problem, we are interested in finding all solutions. Up to our knowledge, this is only possible with the MILP solver SCIP [16].

As mentioned above, there are many ways to give the ILP formulation of a graph coloring problem. The assignment-based model [26, Subsection 2.2] is the standard formulation of the vertex coloring problem. This formulation uses only binary variables, one for each color and one for each vertex-color pair, and the objective is to minimize the number of used colors. Since we are only interested in k-colorings, this allows us to simplify the model slightly.

There are other approaches as well, based on partial ordering, like POP and POP2 [26, Section 3]. The idea is to introduce a partial ordering on the union of the vertices and the color set, and encode these relations with binary variables. The authors also provide the relation between these new variables and the variables occurring in the standard assignment-based model.

A drawback of the ILP formulations is that, in contrast to the set cover method, it is hard to make use of the symmetry of the underlying graph. We conclude that since GRAPE is very efficient in coping with symmetries of a line graph, it is better suited to compute all paramodifications of a given Steiner 2-design.

3.5. Paramodification of unitals of orders 3 and 4

In this section we present computational results on paramodifications of known small unitals. In this way we construct 173 new unitals of order 3, and 25 712 new unitals of order 4. We study the following libraries and classes of abstract unitals of order at most 6:

BBT 909 unitals of order 3 by Betten, Betten and Tonchev [8].

KRC 4466 unitals of order 3 by Krčadinac [34]. This class contains all abstract unitals of order 3 with a non-trivial automorphism group. 722 of the BBT unitals appear in KRC.

KNP 1777 unitals of order 4 by Krčadinac, Nakić and Pavčević [35],

BB two cyclic unitals of orders 4 and 6 by Bagchi and Bagchi [2]. The cyclic BB unital of order 4 is contained in KNP, as well.

We access the libraries of small unitals and carry out the computations using the GAP package UnitalSZ [42]. If $\mathbf{D}$ is a BB unital of order 6, then $\mathbf{D}_b$ has a unique block coloring for each block b; that is, paramodification gives no new unitals of order 6, cf. Listing 3.1.

Listing 3.1: Block colorings of the BB unital of order 6

```
u := BagchiBagchiCyclicUnital( 6 );;
blocks := BlocksOfUnital( u );;
rep_blocks := List( Orbits( AutomorphismGroup( u ), blocks, OnSets ),
                    orb -> Representative( orb ) );
##  [ [ 1, 2, 37, 44, 65, 73, 132 ], [ 1, 32, 63, 94, 125, 156, 187 ] ]
colorings_perblock := [];;
for b in rep_blocks do
  Cb := Filtered( blocks, x -> Size( Intersection( x, b ) ) = 1 );
  Cb := List( Cb, x -> Difference( x, b ) );
  b_stab := Stabilizer( AutomorphismGroup( u ), b, OnSets );
  colorings := AllRegularBlockColorings( Cb, 6 + 1, b_stab );
  Add( colorings_perblock,
       rec( b := b, ncoloring := Length( colorings ) ) );
od;
colorings_perblock;
##  [ rec( b := [ 1, 2, 37, 44, 65, 73, 132 ], ncoloring := 1 ),
##    rec( b := [ 1, 32, 63, 94, 125, 156, 187 ], ncoloring := 1 ) ]
```

The *paramodification graph* Ψ_n for a given order n consists of one vertex for each equivalence class of unitals of order n and with edges between two vertices whenever one can get from one equivalence class to the other via a paramodification. As paramodifications are reversible, we may consider undirected graphs. The connected components of the paramodification graph are called *paramodification classes*. Paramodification graphs are defined analogously to *switching graphs* in [44].

We carried out computations to determine the paramodification classes of Ψ_3 and Ψ_4, containing at least one unital from the classes BBT, KRC or KNP. For the case of order 3, we found all such classes, resulting 173 new unitals of order 3. This subgraph of Ψ_3 is complete in the sense that all paramodifications of all vertices are known, see Table 3.1.

Table 3.1.: Distribution of the sizes of the paramodification classes

Class size	Ψ_3	Ψ_4
1	3182	1458
2–5	466	99
6–10	35	13
11–100	13	16
101–1000		14
1001–2000		2
2557		1^*
3487		1^*
4035		1^*
7596		1^*

Consider the switching graph on the unitals from the classes BBT, KRC, and the newly found 173 paramodifications of them. As switches are special cases of paramodifications, this switching graph is a subgraph of the graph mentioned above. By restricting the type of transformations to switches, we lose 623 edges between the unitals in contrast to paramodifications, and only 131 of the new 173 unitals are reachable via switching. In the paramodification subgraph, there are 3182 isolated vertices according to Table 3.1; in the switching graph, this number is 3525.

In the case of order 4, out of the 1777 unitals of KNP, 1458 turn out to be isolated vertices of Ψ_4. By repeating the paramodification step, we produced 25 712 new unitals of order 4. However, the graph is incomplete as it has unfinished vertices; these are unitals whose paramodifications have not been computed yet. Not counting the isolated vertices, the number of complete paramodification classes is 144. The remaining 4 classes are all incomplete (see the starred entries in Table 3.1), with 12 484 unfinished vertices in total. Concerning the growth of the connected components, it is hard to say anything mathematically reasonable. The largest component with 7596 known vertices has 8 vertices of KNP type, and its growth computed until the fourth layer of the breadth-first tree is

$$8, \quad 45, \quad 425, \quad 7118,$$

but the search stopped there, and probably there are more unitals in further layers.

In Table 3.2, we present the comparison of run-times of different algorithms for the computation of (χ, b)-paramodifications. The reader can find further scientific data on the paramodification of unitals on the web page https://davidmezofi.github.io/unitals/.

Table 3.2.: Mean and maximal run-times of different methods in milliseconds of 30 random KNP unitals and a random block

Method	Mean	Maximum
Set cover (GAP)	142	316
Assignment (SCIP)	3369	9804
POP (SCIP)	4082	12 266
POP2 (SCIP)	4444	14 707

4. Full points of abstract unitals

This chapter summarises the results of the paper *On the geometry of full points of abstract unitals* [38], and some new computational results will be also presented. The structure of the chapter is as follows. In Section 4.1, we give definitions and basic combinatorial properties of full points and related concepts. The main result of this paper is proved in Section 4.2. It shows that for any abstract unital of order q, which is embedded in the Galois plane $\mathrm{PG}(2, q^2)$, the set of full points of two disjoint blocks is contained in a line. Moreover, the perspectivities of two disjoint blocks generate a semi-regular cyclic permutation group acting on each block. In Section 4.3, we give a complete description of the structure of full points in the classical Hermitian unitals. Section 4.4 gives an overview of computational results about full points in abstract unitals of order 3 and 4, which belong to known classes [2, 8, 35, 34]. For the computation we used the GAP package UnitalSZ [42].

Recall that, an abstract unital of order n is a 2-$(n^3 + 1, n + 1, 1)$ design. We say that an abstract unital $(\mathcal{P}, \mathcal{B})$ is *embedded* in a projective plane Π, if $\mathcal{P}$ consists of points of Π and each block $b \in \mathcal{B}$ has the form $\mathcal{P} \cap \ell$ for some line ℓ of Π. For results on embeddings of abstract unitals see the paper [33] by Korchmáros, Siciliano and Szőnyi, and the references therein. The authors of [33] introduced the concept of *full point*, which is essential to study the embedding problem.

4.1. Combinatorial properties of the set of full points

Definition 4.1.1. Let $U = (\mathcal{P}, \mathcal{B})$ be an abstract unital of order n and fix two blocks b_1, b_2. We say that $P \in \mathcal{P}$ is a *full point with respect to* (b_1, b_2) if $P \notin b_1 \cup b_2$ and for each $Q \in b_1$, the block connecting P and Q intersects b_2.

In other words, there is a well defined projection π_{b_1,P,b_2} from b_1 to b_2 with center P. We denote by $F_U(b_1, b_2)$ the set of full points of U with respect to the blocks b_1, b_2. Clearly, $F_U(b_1, b_2) = F_U(b_2, b_1)$.

Bounds on the number of full points

We start with an easy observation on the number of full points of two blocks b_1, b_2 of U. The result seems to be rather weak.

Lemma 4.1.2. *Let $U = (\mathcal{P}, \mathcal{B})$ be an abstract unital of order $n \geq 2$. Then*

$$|F_U(b_1, b_2)| \leq \begin{cases} n^2 - n & \textit{if } b_1, b_2 \textit{ have a point in common,} \\ n^2 - 1 & \textit{if } b_1, b_2 \textit{ are disjoint.} \end{cases}$$

Proof. For a fixed point $P \in b_1$ we define the set S'_P as the union of the blocks connecting P with $Q \in b_2 \setminus b_1$, and the set $S_P = S'_P \setminus (b_1 \cup b_2)$. Clearly,

$$|S_P| = \begin{cases} n^2 - n & \text{if } b_1, b_2 \text{ have a point in common,} \\ n^2 - 1 & \text{if } b_1, b_2 \text{ are disjoint.} \end{cases}$$

As $F_U(b_1, b_2) \subseteq S_P$, the lemma follows. □

In most (but not all) known examples of abstract unitals, the set of full points is contained in a block. This motivates the following definition.

Definition 4.1.3. Let $U = (\mathcal{P}, \mathcal{B})$ be an abstract unital and $b_1, b_2 \in \mathcal{B}$ disjoint blocks.

(i) The triple (U, b_1, b_2) is *full point regular* if the set of full points $F_U(b_1, b_2) \subseteq c$ for some block $c \in \mathcal{B}$ such that $b_1 \cap c = b_2 \cap c = \emptyset$.

(ii) The abstract unital U is *full point regular* if for any two disjoint blocks b_1, b_2 the triple (U, b_1, b_2) is full point regular.

Full points and perspectivities

By definition, any full point P of the blocks b_1, b_2 defines a bijective map $\pi_{b_1,P,b_2} \colon b_1 \to b_2$; we call it the *perspectivity with center P*.

Definition 4.1.4. Let b_1, b_2 be blocks of the abstract unital U. Define the *group of perspectivities of b_1* as

$$\mathrm{Persp}_{b_2}(b_1) = \left\langle \pi_{b_1,P,b_2} \pi_{b_2,Q,b_1} \colon P, Q \in F_U(b_1, b_2) \right\rangle .$$

It is easy to see that $\mathrm{Persp}_{b_2}(b_1)$ and $\mathrm{Persp}_{b_1}(b_2)$ are isomorphic permutation groups, the former acting on b_1 and the latter acting on b_2. For different full points Q, R, the perspectivities π_{b_1,Q,b_2} and π_{b_1,R,b_2} are different. This implies $\left|\mathrm{Persp}_{b_2}(b_1)\right| \geq |F_U(b_1, b_2)|$. In particular, $\mathrm{Persp}_{b_2}(b_1)$ is nontrivial if $|F_U(b_1, b_2)| > 1$. An important case will be when $\mathrm{Persp}_{b_2}(b_1)$ is a cyclic semi-regular permutation group on b_1.

Dual k-nets in abstract unitals

We will present examples of abstract unitals when the set of full points with respect to the blocks b_1, b_2 form a third block b_3. More generally, we introduce the concept of an embedded dual k-net of an abstract unital. An abstract k-net is a structure consisting of a set $\mathcal{P}$ of points and a set $\mathcal{B}$ of blocks, which is partitioned into k disjoint families $\mathcal{B}_1, \dots, \mathcal{B}_k$ for which the following hold: (1) every point is incident with exactly one block of every $\mathcal{B}_i$, $(i = 1, \dots, k)$; (2) two blocks of different families have exactly one point in common; (3) there exist 3 blocks belonging to 3 different $\mathcal{B}_i$ which are not incident with the same point. See [4, 6] as reference on abstract k-nets.

Definition 4.1.5. Let $U = (\mathcal{P}, \mathcal{B})$ be an abstract unital of order n and $k \geq 3$ an integer. We say that the blocks $b_1, \dots, b_k$ form an *embedded dual k-net* in U, if the following hold for all $1 \leq i < j \leq k$:

(i) $b_i \cap b_j = \emptyset$.

(ii) For all $P \in b_i$, $Q \in b_j$, the block containing P, Q intersects all $b_1, \dots, b_k$ in a point.

It is clear that for an embedded dual k-net $b_1, \dots, b_k$ of U, $b_3 \cup \dots \cup b_k \subseteq F_U(b_1, b_2)$. The converse needs some explanation.

Lemma 4.1.6. *Let U be an abstract unital of order n, $k \geq 3$ an integer and $b_1, \dots, b_k$ blocks of U.*

(i) If $b_3 \subseteq F_U(b_1, b_2)$, then b_1 and b_2 are disjoint.

(ii) If $b_3 \subseteq F_U(b_1, b_2)$, then $b_1 \subseteq F_U(b_2, b_3)$ and $b_2 \subseteq F_U(b_1, b_3)$.

(iii) If $b_3 \cup b_4 \subseteq F_U(b_1, b_2)$, then b_3 and b_4 are disjoint.

(iv) The blocks $b_1, \dots, b_k$ form an embedded dual k-net if and only if $b_3 \cup \dots \cup b_k \subseteq F_U(b_1, b_2)$.

Proof.

(i) Assume that $\{Z\} = b_1 \cap b_2$ and $b_3 \subseteq F_U(b_1, b_2)$. Clearly, b_3 is disjoint from $b_1 \cup b_2$. Fix an arbitrary point $P \in b_1 \setminus \{Z\}$. Each point $R \in b_3$ projects P to $b_2 \setminus \{Z\}$. Hence, there are points $R_1, R_2 \in b_3$ such that $\pi_{b_1,R_1,b_2}(P) = \pi_{b_1,R_2,b_2}(P)$. This means that $P \in b_2$, hence $b_1 = b_2$, a contradiction.

(ii) For any $P_1 \in b_1$, $P_3 \in b_3$, the block P_1P_3 intersects b_2. Now fix P_1 and let P_3 run through b_3 in order to obtain the bijection π_{b_3,P_1,b_2}. Thus, $P_1 \in F_U(b_2, b_3)$. Since this holds for all $P_1 \in b_1$, the claim follows.

(iii) It suffices to show $b_1 \subseteq F_U(b_3, b_4)$. Take $P \in b_1$, $Q \in b_3$ arbitrary points. From Q, P projects to $R \in b_2$ and using $b_2 \subseteq F_U(b_1, b_4)$, P projects to $S \in b_4$ from R. Hence, Q projects to b_4 from P.

(iv) The "only if" part follows from the definition. Assume now $b_3 \cup \cdots \cup b_k \subseteq F_U(b_1, b_2)$. By (i) and (iii), all blocks $b_1, \ldots, b_k$ are disjoint. For the indices $3 \leq i < j \leq k$, there is an injective map $\alpha \colon b_1 \times b_2 \to b_i \times b_j$ mapping $(P_1, P_2) \mapsto (P_i, P_j)$ with collinear quadruple P_1, P_2, P_i, P_j. Moreover α is bijective, hence any pair of points $(P_i, P_j) \in b_i \times b_j$ determines a block b' of U such that $b' \cap b_i = P_i$, $i = 1, 2$. The block joining P_1 and P_2 intersects any block $b_s \subseteq F_U(b_1, b_2)$ in P_s for $3 \leq s \leq k$, therefore $b_1, \ldots, b_k$ form a dual k-net in U. □

Bounds on dual k-nets in abstract unitals

For embedded dual k-nets, the trivial bound is $k \leq n+1$. With some elementary counting, we can improve this to $k \leq n-1$. This implies that an abstract unital of order 3 has no embedded dual 3-nets.

Proposition 4.1.7 ([38, Proposition 2.6]). *Let U be an abstract unital of order $n \geq 3$.*

(i) If U has an embedded dual k-net $\{b_1, \ldots, b_k\}$, then $k \leq n-1$.

(ii) For two blocks b_1, b_2, $F_U(b_1, b_2)$ cannot contain more than $n-3$ blocks.

Proof.

(i) Let us assume that $k > n-1$ and let $\mathcal{P}_0 = b_1 \cup b_2 \cup \cdots \cup b_k$. Any block of U intersects $\mathcal{P}_0$ in 0, 1, k or $n+1$ points, the latter being the blocks b_i themselves. Without loss of generality consider the disjoint blocks b_1, b_2. Any pair of points chosen from b_1 and b_2 determines the unique block in $\mathcal{B}$ which is a k-secant to $\mathcal{P}_0$, therefore the number of k-secants is $(n+1)^2$. Then, fix an arbitrary block b_i of the dual k-net and a point P on the block b_i. The number of 1-secant blocks on P is $n^2 - n - 2$. Thus the number 1-secant blocks to $\mathcal{P}_0$ is $k(n+1)(n^2 - n - 2)$. Since $|\mathcal{B}| = n^2(n^2 - n + 1)$ we have

$$k + (n+1)^2 + k(n+1)\left(n^2 - n - 2\right) \leq n^2\left(n^2 - n + 1\right),$$

which gives $n^3 - 3n^2 + n + 1 \leq 0$ by $k \geq n \geq 3$, a contradiction.

(ii) If $F_U(b_1, b_2)$ contains the $k-2$ blocks $b_3, \ldots, b_k$, then $\{b_1, \ldots, b_k\}$ is an embedded dual k-net in U by Lemma 4.1.6 (iv). Hence, $k - 2 \leq n - 3$ by (i).

□

Embedded dual 3-nets and latin squares

An embedded dual 3-net $\{b_1, b_2, b_3\}$ determines a latin square L of order $n+1$ in the following way. Label the points of b_1, b_2, b_3 by the set $\{1, \ldots, n+1\}$:

$$b_s = \{P_{s,1}, \ldots, P_{s,n+1}\}, \quad s = 1, 2, 3.$$

For $i, j \in \{1, \ldots, n+1\}$, let c be the block connecting $P_{1,i}$ and $P_{2,j}$. Define s by $\{P_{3,s}\} = b_3 \cap c$ and write s in row i and column j of L. Choosing a different labeling for b_1, b_2, b_3 results in an *isotope* latin square. By reordering the three blocks, one gets *conjugate* or *parastrophe* latin squares. The set of all parastrophes of a latin square L is also called the *main class* of L. Latin squares are naturally related to (the multiplication tables of) finite *quasigroups*. See [29, Section 1.4] for more details and further references on conjugacy and parastrophy of latin squares.

A property which, for each class C, either holds for all members of C or for no member of C is said to be a *class invariant*. Properties of the underlying (dual) 3-nets are *main class invariants* of the corresponding coordinate latin square. In particular, the groups of perspectivities can be defined for (dual) 3-nets and they are useful examples of *main class invariants*. In the primal setting, perspectivities of 3-nets have been presented in [4] and [6].

Let L be a latin square of order n. We say that L is group-based if it is a parastrophe to the Cayley table of a group G of order n. As the group G only depends on the main class of L, the following concept is well-defined.

Definition 4.1.8. Let $\mathbf{B} = \{b_1, b_2, b_3\}$ be an embedded dual 3-net of the abstract unital U. We say that $\mathbf{B}$ is cyclic, if the corresponding latin square is a parastrophe of the Cayley table of the cyclic group of order $n+1$, where n is the order of U.

Proposition 4.1.9 ([38, Proposition 2.8])**.** *Let U be an abstract unital of order n and $\mathbf{B} = \{b_1, b_2, b_3\}$ be an embedded dual 3-net of U. The following are equivalent:*

(i) $\mathbf{B}$ *is cyclic.*

(ii) $\mathrm{Persp}_{b_i}(b_j)$ *is the cyclic group of order $n+1$ for all $1 \leq i, j \leq 3$, $i \neq j$.*

Proof. Let L be the latin square associated to $\mathbf{B}$. By [4, Proposition 1.2], (ii) implies that the rows of L are elements of the cyclic group of order n, hence L is cyclic and (i) holds. Conversely, assume that $\mathbf{B}$ is labeled in such a way that the the coordinate latin square L is the Cayley table of the cyclic group. Then [4, Theorem 6.1] implies (ii). □

4.2. Full point regularity of embedded unitals

The questions on the embeddings of abstract unitals in projective planes are long studied problems, with special focus on the embeddings of abstract unitals of order q in the desarguesian plane $\mathrm{PG}(2,q^2)$. Korchmáros, Siciliano and Szőnyi [33] introduced the concept of *full point* to study the embedding problem. Their approach was to look at the group of perspectivities with respect to blocks. We notice that while the permutation group $\mathrm{Persp}_{b_2}(b_1)$ depends only on the abstract unital structure of $\mathcal{U} = (\mathcal{P}, \mathcal{B})$, we may be able compute it more easily when a projective embedding of $\mathcal{U}$ is given.

Although the definition of the group of perspectivities works for intersecting blocks b_1, b_2, in the sequel, we will only deal with the case when b_1, b_2 are disjoint. The next definition gives a stronger version of the full point regular property, using the structure of the group of perspectivities.

Definition 4.2.1. Let $\mathcal{U} = (\mathcal{P}, \mathcal{B})$ be an abstract unital and $b_1, b_2 \in \mathcal{B}$ disjoint blocks.

(i) If $(\mathcal{U}, b_1, b_2)$ is a full point regular triple and $\mathrm{Persp}_{b_2}(b_1)$ is a cyclic semi-regular permutation group of b_1, then $(\mathcal{U}, b_1, b_2)$ is said to be *strongly full point regular.*

(ii) The abstract unital $\mathcal{U}$ is *strongly full point regular* if for any two disjoint blocks b_1, b_2 the triple $(\mathcal{U}, b_1, b_2)$ is strongly full point regular.

Notice that $\mathcal{U}$ is strongly full point regular if it has no full points at all. The next two lemmas deal with elementary properties of the groups of affinities (cf. Section 2.4) of projective lines in $\mathrm{PG}(2,q^2)$, where q is a power of the prime p.

Lemma 4.2.2. *Let p be a prime.*

(i) Let g be an element of the affine linear group $\mathrm{AGL}(1,p^e)$ such that $o(g) \mid p^e - 1$. Then g has a unique fixed point $v \in \mathbb{F}_{p^e}$ and permutes $\mathbb{F}_{p^e}$ in orbits of length $o(g)$.

(ii) Let S be a subgroup of $\mathrm{AGL}(1,p^e)$ such that $p \nmid |S|$. Then, S is cyclic and $|S|$ divides $p^e - 1$. Moreover, S has a unique fixed point in $\mathbb{F}_{p^e}$. □

Lemma 4.2.3. *Let ℓ_1, ℓ_2 be two lines of $\mathrm{PG}(2,q^2)$ and P, Q be two points off $\ell_1 \cup \ell_2$. Write $Z = \ell_1 \cap \ell_2$ and $V_i = \ell_i \cap PQ$, $i = 1,2$. The perspectivity $\pi_{\ell_1,P,\ell_2}\pi_{\ell_2,Q,\ell_1}$ fixes Z and V_1 and permutes $\ell_1 \setminus \{Z, V_1\}$ in orbits of equal lengths.*

Proof. Elementary. □

Let S be any set of $n+1$ points in the projective plane Π of order n. A *nucleus* of S is a point P such that each line of Π through P intersects S in a unique point. It follows that $P \notin S$. We denote by $\mathcal{N}(S)$ the set of all nuclei of S.

Let $U = (\mathcal{P}, \mathcal{B})$ be a unital of order q embedded in $\mathrm{PG}(2, q^2)$ and let $b_1, b_2 \in \mathcal{B}$ be two (not necessarily disjoint) blocks of U. Denote the lines containing the blocks b_1 and b_2 by ℓ_1 and ℓ_2 respectively. Using the notations in [32] let $B = b_1 \cup (\ell_2 \setminus b_2)$: the set B consists of $q^2 + 1$ non collinear points, it is contained in the union of the lines ℓ_1 and ℓ_2. Note that $Z = \ell_1 \cap \ell_2$ belongs to B. Let $\mathcal{N}(B)$ denote the set of all nuclei of B. Clearly, if P is a full point with respect to the blocks b_1, b_2 then P is a nucleus of B, hence $F_U(b_1, b_2) \subseteq \mathcal{N}(B)$.

The next lemma formulates [32, Propositions 2 and 3] in our setting.

Lemma 4.2.4. *Let $U = (\mathcal{P}, \mathcal{B})$ be a unital of order q embedded in $\mathrm{PG}(2, q^2)$ and let $b_1, b_2 \in B$ be two blocks of U. Denote the lines containing the blocks b_1 and b_2 by ℓ_1 and ℓ_2 respectively. Write $Z = \ell_1 \cap \ell_2$ and $B = b_1 \cup (\ell_2 \setminus b_2)$. Define the set $\Gamma_1 = \{\pi_{\ell_1,P,\ell_2}\pi_{\ell_2,Q,\ell_1} \mid P, Q \in \mathcal{N}(B)\}$ where $\mathcal{N}(B)$ denotes the set of all nuclei of B. Then the following hold:*

(i) Γ_1 *leaves b_1 invariant.*

(ii) Γ_1 *is a group of affinities of the affine line $\ell_1 \setminus \{Z\}$.* □

Define the integer r by $q^2 = p^r$. The order of the group Γ_1 is tp^h, where $p \nmid t$, and Γ_1 is isomorphic to some group $\Gamma = \mathbf{AB}$ of affinities where $\mathbf{B}$ is an additive subgroup of order p^h of $\mathrm{GF}(q^2)$ and $\mathbf{A}$ is a multiplicative subgroup of order t of $\mathrm{GF}(q^2)$ such that $t \mid p^{\gcd(r,h)} - 1$. Let $m = \left(p^{r-h} - 1\right)/t$ and let $\mathbf{B}_1 \cup \mathbf{O}_1 \cup \ldots \cup \mathbf{O}_m$ be the partition of $\ell_1 \setminus \{Z\}$ into Γ_1-orbits. We have by [32, Section 2] that $\mathbf{B}_1$ has length p^h and for each $i = 1, 2, \ldots, m$ the orbit $\mathbf{O}_i$ has length tp^h.

Let $B_i = \ell_i \cap B$ for $i = 1, 2$ and let $\widehat{B}_1 = B_1 \setminus \{Z\}$, then $\widehat{B}_1$ is union of Γ_1-orbits. It follows that the size of $\widehat{B}_1$ must be divisible by p^h, and we must distinguish between two cases:

1. If the blocks b_1 and b_2 are disjoint, it means $b_1 = B_1 = \widehat{B}_1$, hence $p^h \mid q + 1$. It is possible only for $h = 0$, thus the group $\mathbf{B}$ is trivial.
2. Otherwise $b_1 \cap b_2 = \{Z\}$, meaning $b_1 = B_1 = \widehat{B}_1 \cup \{Z\}$, hence the size of $\widehat{B}_1$ is q. In this case $q = ap^h + btp^h$, where $b \in \{0, 1, \ldots, m\}$ and $a = 1$ or 0, depending on whether $\mathbf{B}_1 \subseteq \widehat{B}_1$ or not. If $a = 0$, then $q = btp^h$, and as $p \nmid t$ we have $t = 1$, therefore the group $\mathbf{A}$ is trivial.

Lemma 4.2.5. *Let $U = (\mathcal{P}, \mathcal{B})$ be a unital of order q embedded in $\mathrm{PG}(2, q^2)$ and let $b_1, b_2 \in \mathcal{B}$ be two disjoint blocks of U. Denote the lines containing the blocks b_1 and b_2 by ℓ_1 and ℓ_2 respectively. Write $Z = \ell_1 \cap \ell_2$ and $B = b_1 \cup (\ell_2 \setminus b_2)$. Define the group Γ_1 generated by the perspectivities $\pi_{\ell_1,P,\ell_2}\pi_{\ell_2,Q,\ell_1}$ with $P, Q \in \mathcal{N}(B)$ where $\mathcal{N}(B)$ denotes the set of all nuclei of B. Then the following hold:*

(i) $p \nmid |\Gamma_1|$.

(ii) Γ_1 *is cyclic and* $|\Gamma_1| \mid q^2 - 1$.

(iii) Γ_1 *has a unique fixed point* $V_1 \notin b_1 \cup \{Z\}$.

(iv) The set of full points $F_U(b_1, b_2)$ *is contained in a line* m *through* V_1 *with* $Z \notin m$.

Proof. Assume that Γ_1 has an element γ of order p. Since b_1 is Γ_1-invariant, γ has a fixed point in b_1, different from Z as $Z \notin b_1$. However, affinities with two fixed points have order dividing $q^2 - 1$. This proves (i).

Together with Lemma 4.2.2 and Lemma 4.2.3, (i) implies (ii) and (iii). Notice that Lemma 4.2.2 (i) is needed to show that $V_1 \notin b_1$.

Since $\mathbf{B}$ is trivial, the set of nuclei $\mathcal{N}(B)$ is contained in a line m such that $Z \notin m$ (cf. [32, p. 67]). In particular $F_U(b_1, b_2)$ is contained in m as $F_U(b_1, b_2) \subseteq \mathcal{N}(B)$. Furthermore, by Lemma 4.2.3, for any $P, Q \in \mathcal{N}(B)$ the line PQ contains V_1, hence $V_1 \in m$. This proves (iv). □

We can now state and prove the main theorem of this section.

Theorem 4.2.6 ([38, Theorem 3.6])**.** *If the unital* U *of order* q *is embedded in* $\mathrm{PG}(2, q^2)$ *then it is strongly full point regular.*

Proof. Let us assume that U is embedded in $\mathrm{PG}(2, q^2)$. Let b_1, b_2 be two disjoint blocks of U. If $|F_U(b_1, b_2)| \leq 1$ then we have nothing to prove. Otherwise, by Lemma 4.2.5 $F_U(b_1, b_2)$ is contained in a block c, which is disjoint to b_1 and b_2. Furthermore, $\mathrm{Persp}_{b_2}(b_1)$ is cyclic, its order divides $q^2 - 1$ and b_1 decomposes into orbits of equal lengths. This means that (U, b_1, b_2) is a strongly full point regular triple. □

4.3. Full points of the Hermitian unital

For a prime power q, let ρ be a Hermitian polarity of $\mathrm{PG}(2, q^2)$. Two points P, Q are said to be *conjugate* if $P \in Q^\rho$. Similarly, the lines ℓ, m are *conjugate* if $\ell^\rho \in m$. Let R^+ be the set of pairs (ℓ, m), where ℓ, m are conjugate lines to each other but not self-conjugate. The projective unitary group $\mathrm{PGU}(3, q)$ acts transitively on R^+. Given two conjugate lines ℓ_1, ℓ_2, one constructs $\ell_3 = (\ell_1 \cap \ell_2)^\rho$, conjugate to both ℓ_1 and ℓ_2. We say that ℓ_1, ℓ_2, ℓ_3 form a *polar triangle.* The projective unitary group $\mathrm{PGU}(3, q)$ acts transitively on the set of polar triangles. Consider the set $\mathcal{P}$ of self-conjugate points of ρ; $|\mathcal{P}| = q^3 + 1$. The line ℓ intersects $\mathcal{P}$ in 1 or $q + 1$ points, depending on whether ℓ is self-conjugate or not. Let ℓ be a non self-conjugate line and m be a line connecting ℓ^ρ and a point $P \in \mathcal{P} \cap \ell$. Since $\ell^\rho \in P^\rho$, we have $m = P^\rho$ which must be a self-conjugate line. This means that $(\ell, \ell') \in R^+$ implies that $\ell \cap \ell' \notin \mathcal{P}$. It follows that any non self-conjugate line ℓ is contained in exactly $q\,(q-1)\,/2$ polar triangles. For further details and background, see [21, Section 7.3]

The abstract Hermitian unital $\mathcal{H}(q)$ is constructed from the set $\mathcal{P}$ of self-conjugate points of ρ. The subsets cut out by the $(q+1)$-secants (not self-conjugate lines) form the set $\mathcal{B}$ of blocks of $\mathcal{H}(q)$. Notice that we consider $\mathcal{H}(q)$ as an abstract unital, having a natural embedding in $\mathrm{PG}(2, q^2)$. The following proposition gives a characterization of the conjugate relation in terms of the abstract unital $\mathcal{H}(q)$ for q even.

Proposition 4.3.1 ([38, Proposition 4.1]). *Let q be even, let ρ be a Hermitian polarity of $\mathrm{PG}(2, q^2)$ and let $\mathcal{P}$ be the set of self-conjugate points of ρ. Let ℓ_1, ℓ_2 be not self-conjugate lines and define the blocks $b_i = \ell_i \cap \mathcal{P}$ of $\mathcal{H}(q)$, $i = 1, 2$. Then the following hold:*

(i) If ℓ_1, ℓ_2 are conjugate, then $F_{\mathcal{H}(q)}\,(b_1, b_2) = b_3$, where $b_3 = \ell_3 \cap X$ with $\ell_3 = (\ell_1 \cap \ell_2)^\rho$. In other words, the blocks contained in a polar triangle form an embedded dual 3-net of $\mathcal{H}(q)$.

(ii) If ℓ_1, ℓ_2 are not conjugate then either $b_1 \cap b_2 \neq \emptyset$, or $\left| F_{\mathcal{H}(q)}\,(b_1, b_2) \right| = 1$.

Proof.

(i) Up to projective equivalence, we can assume that the matrix of ρ is the identity. Since the unitary group $\mathrm{PGU}(3, q)$ acts transitively on R^+, we can assume $\ell_1\colon X_1 = 0$ and $\ell_2\colon X_2 = 0$. Then, $\ell_1 \cap \ell_2 = (0, 0, 1)$ and $\ell_3\colon X_3 = 0$. Let ε be a $(q+1)$th root of unity in $\mathbb{F}_{q^2}$. The elements of $b_s = \ell_s \cap X$, $s = 1, 2, 3$, have the form

$$A_i = \left(0, 1, \varepsilon^i\right), \quad B_j = \left(\varepsilon^j, 0, 1\right), \quad C_k = \left(1, \varepsilon^k, 0\right),$$

respectively, with $i, j, k = 0, 1, \ldots, q$. Since the points A_i, B_j, C_k are collinear if and only if $\varepsilon^{i+j+k} = 1$, we see that A_i projects from C_k to B_{-i-k}. In particular, $b_3 \subseteq F_{\mathcal{H}(q)}\,(b_1, b_2)$, and equality holds by Theorem 4.2.6.

(ii) The case when ℓ_1, ℓ_2 are not conjugate and $b_1 \cap b_2 = \emptyset$ was elaborated in [33, Section 2.2]. □

Remark 4.3.2. Proposition 4.3.1 shows that for q even, $\mathcal{H}(q)$ has embedded dual 3-nets. More precisely, any block of $\mathcal{H}(q)$ is contained in $q\,(q-1)\,/2$ polar triangles. The group of automorphisms of $\mathcal{H}(q)$ acts transitively on the set of embedded dual 3-nets.

Let ρ_0 be a Hermitian polarity of the projective line $\mathrm{PG}(1, q^2)$. The set of self-conjugate points of ρ_0 forms a subline $\mathrm{PG}(1, q)$, cf. [21, Lemma 6.2]. Let ℓ be a line of $\mathrm{PG}(2, q^2)$. A *Baer subline* of ℓ is subset of size $q+1$, consisting of self-conjugate points of some Hermitian polarity ρ of $\mathrm{PG}(2, q^2)$. Equivalently, a Baer subline S is isomorphic to $\mathrm{PG}(1, q)$, and $S = \ell \cap \Pi$ for some line ℓ and a Baer subplane Π.

Proposition 4.3.3 ([38, Proposition 4.3]). *Let $U = (\mathcal{P}, \mathcal{B})$ be an abstract unital of order q, embedded in $\mathrm{PG}(2, q^2)$. Let b_1, b_2, b_3 form an embedded dual 3-net. Then b_1, b_2, b_3 are Baer sublines.*

Proof. Let ℓ be the projective line containing b_1. By Theorem 4.2.6, $C = \mathrm{Persp}_{b_2}(b_1)$ is a cyclic subgroup of order $q+1$, preserving b_1. Since C is obtained using projections in $\mathrm{PG}(2, q^2)$, it is a subgroup of the projectivity group of ℓ. By the arguments of [33, Section 3] one shows that b_1 is a Baer subline of ℓ. □

Remark 4.3.4. Let q be even, and consider an *arbitrary* embedding of the Hermitian unital $\mathcal{H}(q)$ in $\mathrm{PG}(2, q^2)$. By Remark 4.3.2 and Proposition 4.3.3, all blocks correspond to Baer sublines of $\mathrm{PG}(2, q^2)$. Using the characterization of Hermitian curves from [13, 36], plus the arguments of [33, Section 3], this observation gives an alternative proof of the uniqueness result of [33] in the even q case.

4.4. Full points and dual 3-nets of known small unitals

In this section we present computational results on the structure of full points of known small unitals. More precisely, we study the following libraries and classes of abstract unitals of order at most 6:

BBT 909 unitals of order 3 by Betten, Betten and Tonchev [8],
KRC 4466 unitals of order 3 with nontrivial automorphism groups by Krčadinac [34],
P3M 173 unitals obtained as paramodifications of the KRC and BBT unitals,
KNP 1777 unitals of order 4 by Krčadinac, Nakić and Pavčević [35],
P4M 25 641 unitals obtained as paramodifications of the KNP unitals,
BB two cyclic unitals of order 4 and 6 by Bagchi and Bagchi [2].

Notice that KRC contains all abstract unitals of order 3 with a nontrivial automorphism group. As mentioned in [34], 722 of the BBT unitals appear in KRC. Moreover, the cyclic BB unital of order 4 is contained in KNP. The BB unital of order 6 has no full points (see Listing 4.1), therefore we omit the BB class from the tables of this section. We access the libraries of small unitals and carry out the computations using the GAP4 package UnitalSZ [42].

Listing 4.1: The BB unital of order 6 has no full points

```
u := BagchiBagchiCyclicUnital( 6 );;
FullPointsOfUnitalRepresentatives( u );
## [ ]
```

The number of full points and the structure of the group of perspectivities

We only consider disjoint pairs of blocks admitting at least two full points as for only one full point the perspectivitiy group is trivial. In Tables 4.1 and 4.2 we summarize the existing number of full points, the structure of the group of perspectivities and the number of unitals (0s omitted) with such pairs for each library (BBT, KRC, P3M, KNP and P4M).

Table 4.1.: Full points of unitals of order 3

Full points	Group of perspectivities	BBT	KRC	P3M
2	C_2	477	1015	41
2	C_3	94	379	7
2	C_4	290	897	65
3	S_4		6	

The structure of the full points

The structure of the full points is only interesting when there is at least 3 of them, hence the BBT unitals are out of our scope. Even the case of 3 full points is simple: they are either contained in a block or not. As KRC unitals admit at most 3 full points and none of these “large” full point sets is contained in a block, we are only interested in the KNP and P4M unitals.

The computation in [42] showed that in the case of the KNP unitals if there are 4 or 5 full points (in the case of disjoint blocks) then either the whole set of full points is contained in a single block, or no three points are collinear. Now by “collinear” we mean that the points form a subset of some block of the unital.

The P4M unitals do not show such strict structure regarding their full points. There are unitals with 4 full points which do not form a subset of any of the blocks, but 3 of these fullpoints are collinear, see Listing 4.2.

Listing 4.2: P4M unital with 3 collinear full points

```
u := P4MAbstractUnital( 141 );;
b1 := [ 9, 35, 46, 53, 60 ];;
```

Table 4.2.: Full points of unitals of order 4

Full points	Group of perspectivities	KNP	P4M
2	C_2	93	4084
2	C_4	71	9737
2	C_5	107	17 434
2	C_6	5	6724
3	A_5	2	4819
3	$C_2 \times C_2$	1	87
3	C_4	32	308
3	C_5	30	10 022
3	S_5	3	7811
4	C_5	8	12 541
5	C_5	165	13 968
6	$C_5 \rtimes C_4$	72	1308
6	D_{10}	53	550
3	$C_5 \rtimes C_4$		300
3	D_{10}		107
4	A_5		5198
4	$C_5 \rtimes C_4$		125
4	S_5		6995
5	A_5		472
5	$C_5 \rtimes C_4$		180
5	D_{10}		11
5	S_5		12 406
6	S_5		154

```
b2 := [ 5, 11, 27, 29, 54 ];;
fullpts := FullPointsOfUnitalsBlocks( u, b1, b2 );
##  [ 3, 17, 44, 51 ]
ForAny( BlocksOfUnital( u ), x -> IsSubset( x, fullpts ) );
##  false
First( BlocksOfUnital( u ),
       x -> Length( Intersection( x, fullpts ) ) = 3 );
##  [ 1, 17, 44, 51, 63 ]
```

Also there are unitals with 5 full points which do not form a subset of any of the blocks (or equivalently, they do not form a block), but 4 of these fullpoints are collinear (cf. Listing 4.3).

Listing 4.3: P4M unital with 4 collinear full points

```
u := P4MAbstractUnital( 138 );;
b1 := [ 16, 20, 22, 34, 62 ];;
b2 := [ 6, 10, 27, 35, 41 ];;
fullpts := FullPointsOfUnitalsBlocks( u, b1, b2 );
##  [ 5, 30, 37, 42, 61 ]
ForAny( BlocksOfUnital( u ), x -> IsSubset( x, fullpts ) );
##  false
First( BlocksOfUnital( u ),
       x -> Length( Intersection( x, fullpts ) ) = 4 );
##  [ 2, 30, 37, 42, 61 ]
```

The case of 6 full points is the same in both the KNP and the P4M libraries: either 5 of the full points form a block or no 3 of them are collinear.

Unitals with large full point sets

Let us denote by Ω the subset of unitals with at least one *large* full point set, that is, $|F_U(b_1, b_2)| \geq 3$ for a pair (b_1, b_2) of disjoint blocks. We have seen that Ω is the empty set for BBT unitals. By Table 4.1, $|\Omega| = 6$ for KRC unitals. Hence, the interesting cases are the KNP and P4M libraries, where the size of Ω is 206 and 18 788, repsectively. In Table 4.3 we present the number of KNP and P4M unitals with some restrictions on the structure of full points. Clearly $A \subseteq B$, $C \subseteq \overline{B}$ and $\Omega = B \cup \overline{B}$.

Table 4.3.: Units of order 4 with large full point sets

Set	Property	KNP	P4M
Ω	At least one *large* full point set	206	18 788
A	All large full point sets form a block	42	1053
B	All large full point sets are contained in a block	80	4191
$\overline{B}$	Some large full point sets are not contained a block	126	14 597
C	No large full point set is contained in a block	1	399

Full point regularity

In Table 4.4 one sees how many of the unitals of the different libraries are full point regular (FPR) and strongly full point regular (SFPR). In fact, if a unital is not strongly full point regular then is not embeddable into $\mathrm{PG}(2, q^2)$. Hence 94 BBT unitals, 385 KRC unitals, 7 P3M unitals, 195 KNP unitals and 16 661 P4M unitals are definitely not embeddable into $\mathrm{PG}(2, q^2)$. Notice that [3] proves a much stronger result, where the authors show that there are just two orbits of unitals in $\mathrm{PG}(2, 16)$, containing the Hermitian unitals and Buekenhout–Metz unitals, respectively.

Table 4.4.: Full point regularity

Library	Unitals	FPR	SFPR
BBT	909	815	815
KRC	4466	4081	4081
P3M	173	166	166
KNP	1777	1586	1582
P4M	25 641	9196	8980

Embedded dual 3-nets

By Proposition 4.1.7 (ii), one can find embedded dual 3-nets only among the KNP or P4M unitals. The computation shows us that among the KNP unitals the latin squares constructed from the dual 3-nets are always of cyclic type, namely, any embedded dual 3-net is cyclic. However, there are many P4M unitals admitting a non-cyclic embedded dual 3-net. As the computation in Listing 4.4 shows, the group of perspectivities is isomorphic to S_5, hence the corresponding embedded dual 3-net is non-cyclic.

Listing 4.4: Non-cyclic embedded dual 3-net

```
u := P4MAbstractUnital( 137 );;
d3nets := EmbeddedDual3NetsOfUnitalRepresentatives( u );;
noncyc := First( d3nets, x -> not IsCyclic(
    PerspectivityGroupOfUnitalsBlocks( u, x[1], x[2], x[3] ) ) );
##  [ [ 1, 2, 3, 4, 5 ], [ 6, 36, 52, 58, 63 ], [ 9, 34, 50, 59, 64 ] ]
StructureDescription( PerspectivityGroupOfUnitalsBlocks( u, noncyc[1],
    noncyc[2], noncyc[3] ) );
##  "S5"
```

5. The GAP package UnitalSZ

Computing full points, paramodifications and other properties of unitals elaborated in Chapters 3 and 4 is not feasible by hand at a certain point: one will eventually need to use some software for the computation. One popular choice in the fields of group theory and discrete mathematics is the computer algebra system GAP [14]. Unfortunately, GAP doesn't have built-in support for unitals, hence the author of this thesis and his supervisor dr. Gábor Péter Nagy decided to extend GAP with features related to unitals by developing a GAP package, called UnitalSZ [42] (the "SZ" stands for Szeged).

The current version of the package is version 0.6, available in a tarball on the website `https://nagygp.github.io/UnitalSZ`, and the source code can be found on GitHub under the GNU General Public License v3.0. The package requires a GAP version 4.8 or higher, and the GAP packages GAPDoc, Digraphs and IO to be installed.

This chapter demonstrates the features of the package and outlines some implemented algorithms.

5.1. Abstract unitals

This section presents how one can create a unital object using the package UnitalSZ via boolean and incidence matrices and via the list of blocks. Methods computing some basic properties of a unital are also implemented, e.g. the points, the list of blocks, the automorphism group of the unital, and one may check whether to unitals are isomorporphic or not.

AbstractUnitalByBlistList

The function `AbstractUnitalByBlistList( bmat )` returns a unital object corresponding to the list of boolean lists `bmat`. The argument `bmat` is fundamentally the transposed incidence matrix $\mathbf{M}^\top$ (cf. Definition 2.1.2) of size $b \times v$, where b and v denotes the number of blocks and points, respectively.

The function returns with an error, if the size of `bmat` is incorrect, namely by Theorem 2.1.5

$$\begin{aligned} b &= n^2\left(n^2 - n + 1\right) \\ v &= n^3 + 1. \end{aligned} \tag{5.1}$$

The function checks whether the incidence structure corresponding to the argument is a unital, namely a 2-$\left(n^3+1, n+1, 1\right)$ design $(n \geq 3)$ or not. Algorithm 5.1 shows how this check is implemented. The function stores `bmat` and sets the order of the unital to n.

Algorithm 5.1 Checking wether the given incidence structure is a unital or not

```
Input: boolean matrix $\mathbf{M}^\top$ of size $b \times v$ as in (5.1)
Output: boolean value TRUE or FALSE
procedure AxiomCheck($\mathbf{M}^\top$)
    $n \leftarrow \mathrm{wt}\left(\mathbf{M}^\top_{1\cdot}\right) - 1$        ▷ $\mathrm{wt}\left(\mathbf{M}^\top_{1\cdot}\right)$ is the number of TRUEs in the first row.
    if $\exists j \in \{1,\dots,b\}$ : $\mathrm{wt}\left(\mathbf{M}^\top_{j,\cdot}\right) \neq n+1$ then
        return FALSE
    $\mathbf{M} \leftarrow \left(\mathbf{M}^\top\right)^\top$
    for $i \in \left\{1,\dots,n^3\right\}$ do
        for $j \in \left\{i+1,\dots,n^3+1\right\}$ do
            if $\mathrm{wt}\left(\mathbf{M}_{i\cdot} \wedge \mathbf{M}_{j\cdot}\right) \neq 1$ then        ▷ $\wedge$ denotes the element-wise "and"
                return FALSE
    return TRUE
```

AbstractUnitalByDesignBlocks

The function `AbstractUnitalByDesignBlocks( blocklist )` returns a unital corresponding to the list of blocks `blocklist`. The function creates the transpose of the boolean incidence matrix `bmat` based on the given list of blocks, and performs the same check as `AbstractUnitalByBlistList`. It also stores `bmat`, sets the order of the unital to n.

AbstractUnitalByIncidenceMatrix

The function `AbstractUnitalByIncidenceMatrix( incmat )` returns a unital corresponding to the $b \times v$ 0-1 incidence matrix `incmat`. The function creates `bmat` based on the given incidence matrix, and performs the same check as the previous functions. It also stores `bmat` and sets the order of the unital to n.

Methods for abstract unitals

There are several methods implemented for unitals for getting the points, blocks, incidence graph, etc. of a unital of order n.

Order Returns the order n of the unital.

PointsOfUnital Returns the list `[ 1 .. n^3 + 1 ]`.

BlocksOfUnital Returns the list of the blocks of the unital, each block represented by a list of length $n+1$.

IncidenceDigraph Returns the bipartite directed graph constructed from the boolean incidence matrix `bmat` of the unital.

AutomorphismGroup Returns the automorphism group of the unital computed with the help of its incidence directed graph.

Isomorphism Returns an isomorphism between two unitals if they are isomorphic, and `fail` otherwise. The isomorphism is a permutation which sends the points of a unital U_1 to the points of an other unital U_2 such that the it preserves the incidence between the points and the blocks. The function computes the isomorphism with the help of the incidence directed graphs of the unitals U_1 and U_2.

Listing 5.1: Examples of several methods for abstract unitals

```
LoadPackage( "UnitalSZ", false );
u := HermitianAbstractUnital( 3 );;
Order( u );
##  3
PointsOfUnital( u );
##  [ 1 .. 28 ]
BlocksOfUnital( u ){[1..3]}; # The first 3 blocks
##  [ [ 1, 2, 17, 22 ], [ 1, 3, 9, 12 ], [ 1, 4, 14, 18 ] ]
IncidenceDigraph( u );
##  <immutable digraph with 91 vertices, 252 edges>
AutomorphismGroup( u );
##  <permutation group with 5 generators>
Isomorphism( BBTAbstractUnital(9), KrcadinacAbstractUnital(675) );
##  (1,4)(5,27,15,21,25,7,18,26,12,22,13,20,24,16,19,14)(6,10,17,23,11)
    (8,9,28)
```

5.2. Libraries and classes of abstract unitals

In this section we review most of the commands about the available classes and libraries of unitals in the package. On a better notebook the following constructions work up to order 16, for instance the construction of the Hermitian unital of order 16 takes approximately 3 minutes.

HermitianAbstractUnital

The function `HermitianAbstractUnital( q )` returns the classical unital, which is the abstract unital of order q isomorphic to the Hermitian curve in the classical projective plane. The Hermitian curve has the canonical equation: $X_0^{q+1} + X_1^{q+1} + X_2^{q+1} = 0$. The function computes the blocks of the unital with the help of $\mathrm{PGU}(3,q)$ as shown in Algorithm 5.2.

Recall from classical group theory, that the group $\mathrm{PGU}(3,q)$ acts transitively on the points of the Hermitian curve $\mathcal{H}$ and transitively on the points of $\mathrm{PG}(2,q^2) \setminus \mathcal{H}$. For further details, see [5, Section 1.5].

Algorithm 5.2 Constructing the classical (Hermitian) unital

```
Input: order $q \geq 3$
Output: unital object isomorphic to the classical unital of order $q$
procedure HermitianAbstractUnital($q$)
    $\mathcal{P} \leftarrow \{1, 2, \cdots, q^3 + 1\}$
    $\mathcal{H} \leftarrow$ the orbit under $\mathrm{PGU}(3,q)$ of length $q^3 + 1$
    $G \leftarrow$ Action($\mathrm{PGU}(3,q)$, $\mathcal{H}$)        ▷ $G$ is a permutation group of $\mathcal{P}$
    $G_{\mathrm{stab.}} \leftarrow$ the stabilizer of the pair $(1,2)$ in $\mathrm{PGU}(3,q)$
    $\beta_0 \leftarrow$ the orbit under $G_{\mathrm{stab.}}$ of length $q - 1$
    $\beta \leftarrow \{1,2\} \cup \beta_0$
    $\mathcal{B} \leftarrow$ the orbit of $\beta$ under $G$
    return AbstractUnitalByDesignBlocks($\mathcal{B}$)
```

AllBuekenhoutMetzAbstractUnitalParameters

The function `AllBuekenhoutMetzAbstractUnitalParameters( q )` returns all the pairs of parameters over $\mathrm{GF}(q^2)$ which yield non-isomorphic (orthogonal) Buekenhout–Metz unitals of order q. The argument q must be a prime power (if even, then at least 4).

If q is an odd prime power and (α, β) is 2-tuple of $\mathrm{GF}(q^2)$, then this pair is a suitable parameter of an orthogonal Buekenhout–Metz unital, if $(\beta^q - \beta)^2 + 4\alpha^{q+1}$

is a nonsquare in $\mathrm{GF}(q)$.

If q is an even prime power and (α, β) is 2-tuple of $\mathrm{GF}(q^2)$, then this pair is a suitable parameter of an orthogonal Buekenhout-Metz unital, if $\beta \notin \mathrm{GF}(q)$ and $\alpha^{q+1} / (\beta^q + \beta)^2$ has absolute trace 0.

In both cases $\alpha = 0$ yields the Hermitian classical unital, hence we omit the tuples with $\alpha = 0$. For further details on the parameters and the conditions of non-isomorphic (in the sense of the resulting unitals) parameter pairs, we refer the reader to [5, Section 4.2].

OrthogonalBuekenhoutMetzAbstractUnital

The function `OrthogonalBuekenhoutMetzAbstractUnital( q, alpha, beta )` returns the unital object, which is the abstract unital of order q isomorphic to the orthogonal Buekenhout-Metz unital with parameters α and β in the classical projective plane.

The argument q must be a prime power (if even, then at least 4), the other arguments α and β, elements of $\mathrm{GF}(q^2)$, must be one of the pairs returned by the function computing the parameter pairs described above.

The point set

$$U_{\alpha,\beta} = \left\{ \left(x, \alpha x^2 + \beta x^{q+1} + r, 1 \right) \right\} \cup \{(0,1,0)\}, \quad x \in \mathrm{GF}(q^2),\ r \in \mathrm{GF}(q)$$

in $\mathrm{PG}(2, q^2)$ is a unital (called the orthogonal Buekenhout-Metz unital, cf. [5, Theorem 4.8]) if the pair of parameters (α, β) satisfies the requirements mentioned earlier.

The construction of a Buekenhout–Metz unital (including its blocks) is shown in Algorithm 5.3. We use the fact, that if a line of $\mathrm{PG}(2, q^2)$ meets $U_{\alpha,\beta}$ in $q+1$ points, this set of forms a block of the abstract unital. How can we enumerate all the lines of $\mathrm{PG}(2, q^2)$? By somehow "normalizing" the homogeneous coordinates of the lines, for example

$$\{(0,0,1)\} \cup \{(1,0,\gamma) : \gamma \in \mathrm{GF}(q^2)\} \cup \{(\gamma,1,\delta) : \gamma, \delta \in \mathrm{GF}(q^2)\}.$$

It is easy to see, that every homogeneous triple corresponds to a different line, and the number of lines enumerated is $1 + q^2 + q^4$, which is the number of lines in $\mathrm{PG}(2, q^2)$, indeed. Note that, the line $(0,0,1)$ meets $U_{\alpha,\beta}$ in only 1 point, $(0,1,0)$.

BuekenhoutTitsAbstractUnital

The function `BuekenhoutTitsAbstractUnital( q )` returns the unital object, which is the abstract unital of order q isomorphic to the Buekenhout–Tits unital in the classical projective plane.

Algorithm 5.3 Constructing orthogonal Buekenhout–Metz unitals

```
Input: order $q \geq 3$, if even, then $q \geq 4$; $\alpha$, $\beta$ appropriate parameters
Output: unital object isomorphic to $U_{\alpha,\beta}$
procedure OrthogonalBuekenhoutMetzAbstractUnital($q$, $\alpha$, $\beta$)
    $\mathcal{P} \leftarrow \{(x, \alpha x^2 + \beta x^{q+1} + r, 1) : x \in \mathrm{GF}(q^2), r \in \mathrm{GF}(q)\} \cup \{(0,1,0)\}$
    $\mathcal{B} \leftarrow \emptyset$
    for $\gamma \in \mathrm{GF}(q^2)$ do
        $\mathbf{u} \leftarrow (1, 0, \gamma)$                    ▷ Homogeneous coordinates of a line
        $\beta \leftarrow \{\mathbf{x} \in \mathcal{P} : \mathbf{x}\mathbf{u}^\top = 0\}$
        if $|\beta| = q + 1$ then
            $\mathcal{B} \leftarrow \mathcal{B} \cup \{\beta\}$
    for $(\gamma, \delta) \in \mathrm{GF}(q^2) \times \mathrm{GF}(q^2)$ do
        $\mathbf{u} \leftarrow (\gamma, 1, \delta)$
        $\beta \leftarrow \{\mathbf{x} \in \mathcal{P} : \mathbf{x}\mathbf{u}^\top = 0\}$
        if $|\beta| = q + 1$ then
            $\mathcal{B} \leftarrow \mathcal{B} \cup \{\beta\}$
    return AbstractUnitalByDesignBlocks($\mathcal{B}$)
```

The argument q must be a power of 2, such that the exponent is an odd integer at least 3. The point set

$$U_T = \left\{ \left(x_0 + x_1\delta, y_0 + \left(x_0^{\tau+2} + x_1^{\tau} + x_0 x_1 \right) \delta, 1 \right) : x_0, x_1, y_0 \in \mathrm{GF}(q) \right\} \cup \{(0,1,0)\}$$

in $\mathrm{PG}(2, q^2)$ is a unital (called the Buekenhout–Tits unital, cf. [5, Subsection 4.2.2]) if $\delta \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(4)$ and $\delta^q = 1 + \delta$. This δ is just a basis element along with 1 in $\mathrm{GF}(q^2)$ over $\mathrm{GF}(q)$, hence we can omit it as a parameter. The function $\tau \colon \mathrm{GF}(q) \to \mathrm{GF}(q)$ assigns to the field element x the following: $x \mapsto x^{2^{\frac{k+1}{2}}}$, where $q = 2^k$.

The construction of the blocks of the unital is the same as for the Buekenhout–Metz unitals outlined in Algorithm 5.3. Note that, the line $(0,0,1)$ meets U_T in only 1 point, $(0,1,0)$.

BagchiBagchiCyclicUnital

The function `BagchiBagchiCyclicUnital( n )` returns u unital object of order n, with a cyclic automorphism group acting on the points. The cyclic unital of order six is due to Bagchi and Bagchi [2].

The construction method needs a positive integer n such that $n + 1$ and $n^2 - n + 1$ are primes. For $n \leq 20$, only the parameters $n = 4$ and $n = 6$ yield an abstract unital.

Libraries

The package UnitalSZ contains the following libraries of abstract unitals:

BBT 909 unitals of order 3 by Betten, Betten and Tonchev [8].

Krčadinac 4466 unitals of order 3 with nontrivial automorphism groups by Krčadinac [34]. 722 of the BBT unitals appear in this class.

P3M 173 unitals of order 3, constructed by paramodification (see Section 3.5 and [39]) from the BBT and Krčadinac libraries.

KNP 1777 unitals of order 4 by Krčadinac, Nakić and Pavčević [35].

P4M 25 641 unitals of order 4, constructed by paramodification (see [39]) from the KNP library.

SL28inv 6 $\mathrm{SL}(2,8)$-invariant unitals of order 8 with many translation centers, constructed by Möhler [40] using the method by Grundhöfer, Stroppel and Van Maldeghem [19] described in Section 3.3.

There are other functions regarding the libraries as well:

- `DisplayUnitalLibraryInfo()` prints the information about the available libraries of unitals, while
- `NumberOfAbstractUnitalsInLibrary( name )` returns the number of abstract unitals in the library `name`.

In Listing 5.2 there are examples of the usage of the commands described in this section.

Listing 5.2: Example commands regarding the available classes and libraries

```
params := AllBuekenhoutMetzAbstractUnitalParameters( 5 );
##  [ [ Z(5^2)^23, Z(5)^3 ], [ Z(5^2)^22, Z(5^2)^23 ] ]
OrthogonalBuekenhoutMetzAbstractUnital( 5, params[2][1], params[2][2] );
##  OrthogonalBuekenhoutMetzAbstractUnital(5,Z(5^2)^22,Z(5^2)^23)
BuekenhoutTitsAbstractUnital( 8 );
##  BuekenhoutTitsAbstractUnital(8)
BBTAbstractUnital( 349 );
##  BBTAbstractUnital(349)
P4MAbstractUnital( 24798 );
##  P4MAbstractUnital(24798)
SL28InvariantAbstractUnital( 5 );
##  SL28InvariantAbstractUnital(5)
NumberOfAbstractUnitalsInLibrary( "P4M" );
##  25641
```

5.3. Full points and perspectivities

This section describes the built-in commands of the package regarding full points of unitals.

FullPointsOfUnitalsBlocks

The function `FullPointsOfUnitalsBlocks( u, b1, b2 )` returns the list full point of `u` w.r.t. the blocks `b1`, `b2`. The arguments `b1`, `b2` are either blocks of the unital, or indices of blocks in `BlocksOfUnital( u )`.

As defined in [33] by Korchmáros, Siciliano and Szőnyi, the point P is a full point of the unital U w.r.t. the blocks b_1, b_2 if P is not contained in b_1 or b_2, and, the projection with center P from b_1 to b_2 is a well-defined bijection. Algorithm 5.4 shows how to compute full points for a pair of blocks (not indices). In the implementation we check, if the arguments b_1 and b_2 are valid distinct blocks or indices of the unital U. Note, that the blocks may intersect.

Algorithm 5.4 Computing full points of a pair of blocks

Input: unital U and blocks b_1, b_2 blocks of U
Output: full points of U w.r.t the blocks b_1 and b_2

```
procedure FullPointsOfUnitalsBlocks($U$, $b_1$, $b_2$)
    $\mathcal{P} \leftarrow$ PointsOfUnital($U$)
    $\mathcal{B} \leftarrow$ BlocksOfUnital($U$)
    $\mathcal{P}_0 \leftarrow \{P \in \mathcal{P} \colon P \notin b_1 \cup b_2\}$
    $F_U(b_1, b_2) \leftarrow \emptyset$
    for $P \in \mathcal{P}_0$ do
        $\mathcal{B}_P \leftarrow \{b \in \mathcal{B} \colon P \in b \text{ and } |b \cap b_1| > 0\}$
        $\hat{b}_2 \leftarrow \bigcup_{b \in \mathcal{B}_P} b \cap b_2$
        if $\hat{b}_2 = b_2$ then
            $F_U(b_1, b_2) \leftarrow F_U(b_1, b_2) \cup \{P\}$
    return $F_U(b_1, b_2)$
```

FullPointsOfUnitalRepresentatives

The function `FullPointsOfUnitalRepresentatives( u )` returns a list of records `r` containing the fields `r.block1`, `r.block2`, `r.fullpts`, where `r.fullpts` is the set of full points of `u` w.r.t. the blocks `r.block1`, `r.block2`.

The returned list contains all possible full points of `u` up to the automorphism group of `u`. That is, if P is a full point w.r.t. the blocks b_1, b_2, then there is an automorphism α of U such that $P^\alpha, b_1^\alpha, b_2^\alpha$ are in the list. The computation of the block pairs up to the automorphism group of the unital is outlined in Algorithm 5.5.

Algorithm 5.5 Computing full points of a unital up to its automorphism group

Input: unital U

Output: a record consisting of the list of full points, and the corresponding blocks

```
procedure FullPointsOfUnitalRepresentatives($U$)
    $\mathcal{B} \leftarrow$ BlocksOfUnital($U$)        ▷ $\mathcal{B} = \{b_1, b_2, \dots, b_{|\mathcal{B}|}\}$
    $G \leftarrow$ Action(Aut($U$), $\mathcal{B}$)        ▷ $G$ is a permutation group of $\{1, 2, \dots, |\mathcal{B}|\}$
    $\mathcal{B}_{\text{rep.}} \leftarrow \{\min o \colon o$ is an orbit of $G\}$        ▷ Block representatives (indices)
    $\mathcal{B}_{\text{pairs}} \leftarrow \emptyset$
    for $i \in \mathcal{B}_{\text{rep.}}$ do
        $O \leftarrow \{\min o \colon o$ is an orbit of the stabilizer of $i$ in $G\}$
        $\mathcal{B}_{\text{pairs}} \leftarrow \mathcal{B}_{\text{pairs}} \cup \{(i, j) : j \in O, i < j\}$
    $F_U \leftarrow \emptyset$
    for $(i, j) \in \mathcal{B}_{\text{pairs}}$ do
        $r \leftarrow$ EmptyRecord
        $r$.Block$_1 \leftarrow b_i$
        $r$.Block$_2 \leftarrow b_j$
        $r$.FullPoints $\leftarrow$ FullPointsOfUnitalsBlocks($U, b_i, b_j$)
        $F_U \leftarrow F_U \cup \{r\}$
    return $F_U$
```

PerspectivityGroupOfUnitalsBlocks

The function `PerspectivityGroupOfUnitalsBlocks( u, b1, b2 )` returns the group generated by perspectivies from block `b1` to block `b2` of the unital `u`. Notice that the returned group consists of permutations of $\{1, 2, \dots, n\}$, where n is the order of the unital.

A list of full points can be given as the fourth argument. It is not checked if the elements of the given list of full points are indeed full points. Perspectivities between blocks b_1, b_2 of an abstract unital U are projections from b_1 to b_2 from a center P. In order to the perspectivity be well-defined, P must be a full point w.r.t. b_1, b_2. A method to compute the group of perspectivities (cf. Definition 4.1.4) is presented in Algorithm 5.6. For examples of the previous commands, see Listing 5.3.

EmbeddedDual3NetsOfUnitalRepresentatives

The function `EmbeddedDual3NetsOfUnitalRepresentatives( u )` returns a list of lists each having the form `[ b1, b2, b3 ]`, where `b1`, `b2`, `b3` are three blocks of the unital `u` forming an embedded dual 3-net. The returned list contains all possible

Algorithm 5.6 Computing the perspectivity group of two blocks

Input: unital U and two distinct blocks b_1 and b_2 of U

Output: the group of perspectivities of b_1 w.r.t. b_2

```
procedure PerspectivityGroupOfUnitalsBlocks($U$, $b_1$, $b_2$)
    $F_U(b_1, b_2) \leftarrow$ FullPointsOfUnitalsBlocks$(U, b_1, b_2)$
    $P_0 \leftarrow$ an arbitrary element of $F_U(b_1, b_2)$
    $(Q_1, Q_2, \dots Q_{n+1}) \leftarrow$ the ordered points of $b_1$        ▷ $n$ is the order of $U$
    for $i \in \{1, 2, \dots, n+1\}$ do
        $\beta_i \leftarrow$ the unique block connecting $P_0$ and $Q_i$
        $R_i \leftarrow \beta_i \cap b_2$        ▷ The image of $Q_i$
    $\mathcal{G} \leftarrow \emptyset$
    for $P \in F_U(b_1, b_2)$ do
        for $i \in \{1, 2, \dots, n+1\}$ do
            $\gamma_i \leftarrow$ the unique block connecting $P$ and $R_i$
            $Q'_i \leftarrow \gamma_i \cap b_1$        ▷ The image of $R_i$
        $\pi \leftarrow \left((Q_1, Q_2, \dots Q_{n+1}) \mapsto (Q'_1, Q'_2, \dots, Q'_{n+1})\right)$        ▷ A permutation of $b_1$
        $\mathcal{G} \leftarrow \mathcal{G} \cup \{\pi\}$
    $\mathrm{Persp}_{b_2}(b_1) \leftarrow \langle \mathcal{G} \rangle$
    return $\mathrm{Persp}_{b_2}(b_1)$
```

Listing 5.3: Examples of full point related commands

```
u := KNPAbstractUnital( 1421 );;
B := BlocksOfUnital( u );;
FullPointsOfUnitalsBlocks( u, B[77], B[180] );
##  [ 13, 44, 45, 48, 60, 63 ]
Length( FullPointsOfUnitalRepresentatives( u ) );
##  35
persp := PerspectivityGroupOfUnitalsBlocks( u, B[77], B[180] );;
StructureDescription( persp );
##  "C5 : C4"
```

embedded dual 3-nets of u up to the automorphism group of u. That is, if the blocks b_1, b_2, b_3 form an embedded dual 3-net, then there is an automorphism α of U such that $b_1^\alpha, b_2^\alpha, b_3^\alpha$ are in the list. Algorithm 5.7 shows how the computation of embedded dual 3-nets (cf. Definition 4.1.5) is implemented.

LatinSquareOfEmbeddedDual3Net

The function `LatinSquareOfEmbeddedDual3Net( u, ed3net )` returns a latin square associated to the embedded dual 3-net `ed3net` of the unital `u`. For the definition of

Algorithm 5.7 Computing the embedded dual 3-nets of a unital

```
Input: unital $U$
Output: the list of embedded dual 3-nets up to the automorphism group of $U$
procedure EmbeddedDual3NetsOfUnitalRepresentatives($U$)
    $F_U \leftarrow$ FullPointsOfUnitalRepresentatives($U$)
    $\mathcal{B} \leftarrow$ BlocksOfUnital($U$)
    $F'_U \leftarrow \{r \in F_U : \exists b \in \mathcal{B}$ such that $b \subseteq r.$FullPoints$\}$
    $D_3 \leftarrow \emptyset$
    for $r \in F'_U$ do
        $\mathcal{B}_0 \leftarrow \{b \in \mathcal{B} : b \subseteq r.$FullPoints$\}$
        for $b \in \mathcal{B}_0$ do
            $d_3 \leftarrow \{r.$Block$_1, r.$Block$_2, b\}$
            $D_3 \leftarrow D_3 \cup \{d_3\}$
    return $D_3$
```

a latin square associated to an embedded dual 3-net, see Section 4.1. The returned latin square is "normalized" in the sense, that the values in the first row and column are in ascending order. For examples of embedded dual 3-nets and the corresponding latin squares, see Listing 5.4.

Listing 5.4: Computing the latin square of an embedded dual 3-net

```
u := HermitianAbstractUnital(4);;
ed3net := EmbeddedDual3NetsOfUnitalRepresentatives( u );
##  [ [ [ 1, 2, 55, 64, 65 ], [ 3, 5, 10, 39, 59 ], [ 30, 31, 35, 46, 48 ] ] ]
Display( LatinSquareOfEmbeddedDual3Net( u, ed3net[1] ) );
##  [ [  1,  2,  3,  4,  5 ],
##    [  2,  4,  1,  5,  3 ],
##    [  3,  1,  5,  2,  4 ],
##    [  4,  5,  2,  3,  1 ],
##    [  5,  3,  4,  1,  2 ] ]
```

IsFullPointRegularUnital

The function `IsFullPointRegularUnital( u )` returns the boolean **`true`** if the unital `u` is full point regular (cf. Definition 4.1.3), **`false`** otherwise.

IsStronglyFullPointRegularUnital

The function `IsStronglyFullPointRegularUnital( u )` returns the boolean **`true`** if the unital `u` is strongly full point regular (cf. Definition 4.2.1), **`false`** otherwise.

Listing 5.5 shows a unital wich is full point regular, but not strongly full point regular.

Listing 5.5: Ful point regularity of a unital

```
u := KNPAbstractUnital( 17 );;
IsFullPointRegularUnital( u );
##  true
IsStronglyFullPointRegularUnital( u );
##  false
```

6. Summary

6.1. Summary

In this thesis mainly abstract unitals, their embeddability into the classical projective plane using their full points, and creating new unitals via paramodifications are considered. Chapter 1 serves as an introduction: it outlines the structure of the thesis.

In Chapter 2 we introduce concepts and present some results necessary for better understanding of the notion of full points and paramodifications of unitals. Namely, in Section 2.1 we define incidence structures on points and blocks, the corresponding incidence matrix, and an important type of these structures, the t-(v,k,λ) designs or Steiner systems $\mathrm{S}_\lambda(t,k,v)$. A partition of the set of blocks into parallel classes will be called a resolution, and resolvable designs play an essential role in the existence of paramodifications. We cover the necessary preliminary material about projective planes and polarities in Section 2.2. Unitary polarities lead us to Hermitian curves in $\mathrm{PG}(2,q^2)$, and using their combinatorial properties we define abstract unitals of order n as 2-$(n^3+1,n+1,1)$ designs. Section 2.3 gives the definition of semidirect products of groups, while Section 2.4 introduces the 1-dimensional affine group $\mathrm{AGL}(1,q)$ as a semidirect product, and classifies the subgroups of $\mathrm{AGL}(1,q)$ in the context of the intersection with the normal subgroup of translations.

Chapter 3 is based on the paper *New Steiner 2-designs from old ones by paramodifications* by Mezőfi and Nagy [39]. In Section 3.1 we show that a t-(v,k,λ) design $\mathbf{D}$ is resolvable if and only if it is block r-colorable (cf. Lemma 3.1.1), where r denotes the number of blocks incident with an arbitrary point of the design. For a fixed block b we define the subsystem $\mathbf{D}_b$, which is a resolvable 1-$(v-k,k-1,k)$ design, see Lemma 3.1.2.

From now on, let us assume that $t=2$ and $\lambda=1$. Let χ be a block k-coloring of the subsystem $\mathbf{D}_b$ and modify the original 2-$(v,k,1)$ design $\mathbf{D}$ only in $\mathbf{D}_b$ according to the coloring χ, resulting a design $\mathbf{D}^*$, called a paramodification of $\mathbf{D}$. Theorem 3.1.4 states that $\mathbf{D}^*$ is also 2-$(v,k,1)$ design.

Section 3.2 describes the effect of a paramodification on the incidence matrix of the 2-$(v, k, 1)$ design $\mathbf{D}$. We prove in Proposition 3.2.1 that the incidence matrices of $\mathbf{D}$ and $\mathbf{D}^*$ differ at most in a $k \times k\,(r-1)$ submatrix. It is also shown, that switchings as defined in [44], are special cases of paramodifications, see Proposition 3.2.2. In a 2-$(v, k, 1)$ design, a Pasch configuration consists of six points $P_1, \ldots, P_6$ such that the triples $\{P_1, P_3, P_4\}$, $\{P_1, P_5, P_6\}$, $\{P_2, P_3, P_5\}$, $\{P_2, P_4, P_6\}$ are collinear. The design is anti-Pasch if it does not contain any Pasch configuration. Proposition 3.2.3 claims, that no switching can be carried out for the anti-Pasch Steiner 2-design if the number of points v is below a certain bound.

Section 3.3 discusses the paramodification of certain well-known classes of Steiner 2-designs, e.g. it is shown in Proposition 3.3.1 that paramodifications of a finite projective plane are isomorphic. We also examine Steiner triples systems, i.e. 2-$(v, 3, 1)$ designs, denoted by STS(v), and the problem of the existence of para-rigid Steiner triple systems is stated. Unitals with many translation centers constructed by Grundhöfer, Stroppel and Van Maldeghem [19] are discussed (only in the finite case), as the idea of the paramodification of Steiner 2-designs has been motivated by their construction. We close the section with Proposition 3.3.4, which states that Hermitian unitals do not admit any switchings, but they do admit nontrivial paramodifications.

In Section 3.4 some methods to compute block colorings of a subsystem $\mathbf{D}_b$ are presented. We are interested in the computation of all block colorings of in order to construct new Steiner 2-designs by paramodification. We define the line graph Γ of the subsystem $\mathbf{D}_b$, and according to Lemma 3.4.2, proper block k-colorings of $\mathbf{D}_b$ are essentially k-colorings of Γ. One way to compute all k-colorings of Γ is to find all solutions of a set cover problem of independent K-sets, where $K = (v-k)\,/\,(k-1)$. Using the GRAPE package [46] of GAP [14] this approach is easy to implement. There are many ways to give the integer linear programming (ILP) formulation of a graph coloring problem. The assignment-based model [26, Subsection 2.2] is the standard formulation of the vertex coloring problem, while there are other approaches as well, based on partial ordering, like POP and POP2 [26, Section 3].

Section 3.5 presents computational results on paramodifications of known small unitals (of order up to 6). This way we construct 173 new unitals of order 3, and 25 712 new unitals of order 4. We introduce the concept of paramodification graph Ψ_n: for a given order n consisting of vertices for each equivalence class of unitals of order n and with edges between two vertices whenever one can get from one equivalence class to the other via a paramodification. The connected components of the paramodification graph are called paramodification classes analogously to switching classes in [44]. As switches are special cases of paramodifications, the switching graph is a subgraph of the paramodification graph. Computations were carried out to determine the paramodification classes of Ψ_3 and Ψ_4, containing at least one unital from the libraries BBT, KRC or KNP. For the case of order 3, we found all such classes, namely this subgraph of Ψ_3 is complete in the sense that all paramodifications of all vertices are known. In the case of order 4 the graph is incomplete as it has unfinished vertices; these are unitals whose paramodifications have not been computed yet. Four classes are incomplete (see the starred entries in Table 3.1), with 12 484 unfinished vertices in total. Further data on the paramodification of unitals are available on the web page https://davidmezofi.github.io/unitals/.

In Chapter 4 the results of the paper *On the geometry of full points of abstract unitals* by Mezőfi and Nagy [38] are presented. In Section 4.1 we define full points, full point regularity, group of perspectivities, and embedded dual k-nets of unitals. The upper bounds $n^2 - 1$ and $n^2 - n$ on the number of full points are proved depending on whether the two blocks are disjoint or not, respectively. We also prove, that a unital of order n can have at most embedded dual $(n-1)$-nets, which yields that any full point set contains at most $n - 3$ blocks. At the end of this section we show that embedded dual 3-nets can be viewed as latin squares.

The aim of Section 4.2 is to prove that any embedded unital of order q into the classical projective plane $\mathrm{PG}(2, q^2)$ is strongly full point regular (cf. Theorem 4.2.6). In order to do so, we need several lemmas and results from [32].

In Section 4.3 we show that for an even prime power q, the blocks of the Hermitian unital $\mathcal{H}(q)$ contained in a polar triangle form an embedded dual 3-net, cf. Proposition 4.3.1. Another proposition proven about an arbitrary unital embedded into $\mathrm{PG}(2, q^2)$ is that if three blocks form an embedded dual 3-net, then they are Baer-sublines in $\mathrm{PG}(2, q^2)$, see Proposition 4.3.3.

Section 4.4 presents computational results on the structure of full points of known small unitals, e.g. that the cyclic unital of order 6 by Bagchi and Bagchi [2] has no full points at all. The number of unitals of order 3 and 4 according to the he number of full points and to the structure of the group of perspectivities are shown in Tables 4.1 and 4.2. The number of (strongly) full point regular unitals in the examined libraries are shown in Table 4.4. Note that unitals which are not strongly full point regular cannot be embedded into $\mathrm{PG}(2, q^2)$.

In Chapter 5 the features of the GAP package UnitalSZ [42] developed by the author of the thesis and his supervisor dr. Gábor Péter Nagy are presented, along with some implemented algorithms. The current version of the package is version 0.6, and it is available in a tarball on the website `https://nagygp.github.io/UnitalSZ`, and the source code can be found on GitHub. Throughout the chapter there are example GAP code snippets to illustrate the described functions.

Section 5.1 presents how one can create a unital object using the package UnitalSZ via boolean and incidence matrices and via the list of blocks. Algorithm 5.1 shows, how the check of the conditions is implemented in the package. Methods computing some basic properties of a unital are also demonstrated, e.g. the points, the list of blocks, the automorphism group of the unital, and one may check whether to unitals are isomorporphic or not. In Section 5.2 the commands regarding the available classes and libraries of unitals in the package are shown. Algorithms 5.2 and 5.3 illustrate how the construction of Hermitian unitals and Buekenhout–Metz unitals are implemented in the package.

In Section 5.3 we describe the commands regarding full points of unitals: one can compute the full points of a unital U with respect to the distinct blocks b_1 and b_2, and not just the full points, but the group of perspectivities as well, see Algorithms 5.4 and 5.6. Algorithm 5.5 shows how the computation of all full points of a unital U up to the automorphism group of U are implemented in the package. The functions for determining the embedded dual 3-nets, and the (strong) full point regularity of a unital are also presented.

6.2. Összefoglaló

A disszertáció főként absztrakt unitálokat, ezeknek a klasszikus projektív síkba való beágyazhatóságát, valamint ún. paramodifikációk segítségével új unitálok keresését tárgyalja. A 4. fejezet bevezetésként szolgál: vázolja a disszertáció szerkezetét.

A 2. fejezetben az unitálok teljes pontjainak és paramodifikációiknak mélyebb megértéséhez elengedhetetlen fogalmakat és állításokat írjuk le. A 2.1. szakaszban definiáljuk az illeszkedési struktúra fogalmát, ezek illeszkedési mátrixát, illetve az illeszkedési struktúrák egy fontos típusát, a t-(v,k,λ) dizájnokat vagy $\mathrm{S}_\lambda(t,k,v)$ Steiner-rendszereket. Ha egy dizájn blokkhalmaza párhuzamossági osztályokra partícionálható, akkor feloldhatónak nevezzük: ezek a dizájnok fontos szerepet játszanak a paramodifikációk létezésében. A projektív síkok és polaritások szükséges előismereteit a 2.2. szakaszban tárgyaljuk. Az unitér polaritások vezetnek a $\mathrm{PG}(2,q^2)$-beli Hermite-görbékhez, és ezen görbék kombinatorikus tulajdonságaik alapján definiáljuk az n-edrendű absztrakt unitálokat 2-$(n^3+1,n+1,1)$ dizájnokként. A 2.3. szakaszban adjuk meg a csoportok szemidirekt szorzatának definícióját, míg a 2.4. szakasz vezeti be az 1-dimenziós affin csoport, $\mathrm{AGL}(1,q)$ fogalmát mint szemidirekt szorzatot, és osztályozza $\mathrm{AGL}(1,q)$ részcsoportjait a transzlációk normálosztójával vett metszetük szerint.

A 3. fejezet Mezőfi és Nagy *New Steiner 2-designs from old ones by paramodifications* c. dolgozatán alapul. A 3.1. szakaszban megmutatjuk, hogy egy t-(v,k,λ) dizájn akkor és csak akkor feloldható, ha r-blokkszínezhető (vö. 3.1.1. Lemma), ahol r egy tetszőleges pontra illeszkedő blokkok számát jelöli. Egy rögzített b blokk esetén definiáljuk a $\mathbf{D}_b$ részrendszert, amely egy feloldható 1-$(v-k,k-1,k)$ dizájn, ld. 3.1.2. Lemma.

A továbbiakban tegyük fel, hogy $t=2$ és $\lambda=1$. Legyen χ egy k-blokkszínezése a $\mathbf{D}_b$ részrendszernek, és módosítsuk az eredeti 2-$(v,k,1)$ dizájnt, $\mathbf{D}$-t, a $\mathbf{D}_b$ részrendszerben a χ színezés szerint: a keletkező új $\mathbf{D}^*$ dizájnt $\mathbf{D}$ paramodifikációjának nevezzük. A 3.1.4. Tétel állítása szerint $\mathbf{D}^*$ is egy 2-$(v,k,1)$ dizájn.

A 3.2. szakasz a paramodifikáció hatását írja le a 2-$(v,k,1)$ dizájn illeszkedési mátrixán. A 3.2.1. Állításban bizonyítjuk, hogy $\mathbf{D}$ és $\mathbf{D}^*$ illeszkedési mátrixai egy legfeljebb $k \times k\,(r-1)$ részmátrixban különböznek. Megmutatjuk, hogy a [44]-ben definiált ún. switchingek a paramodifikációk speciális esetei, ld. 3.2.2. Állítás. Egy 2-$(v,k,1)$ dizájnban egy Pasch-konfiguráció hat pontból áll $(P_1,\ldots,P_6)$ úgy, hogy a $\{P_1,P_3,P_4\}$, $\{P_1,P_5,P_6\}$, $\{P_2,P_3,P_5\}$, $\{P_2,P_4,P_6\}$ hármasok kollineárisak. Egy dizájnt anti-Paschnak nevezünk, ha nem található benn Pasch-konfiguráció. A 3.2.3. Állítás szerint egy anti-Pasch Steiner-féle 2-dizájnon nem végezhető el switching, ha a pontok száma v egy bizony felső korlát alatt van.

A 3.3. szakasz jól ismert Steiner-féle 2-dizájnok paramodifikációit tárgyalja, például a 3.3.1. Állítás szerint véges projektív síkok paramodifikációi izomorfak. Steiner-rendszereket, azaz 2-$(v,3,1)$ dizájnokat, jelölésben $\mathrm{STS}(v)$, is vizsgálunk, és megfogalmazzuk a para-rigid Steiner-rendszerek létezésének problémáját. Grundhöfer, Stroppel és Van Maldeghem sok transzlációs középponttal rendelkező unitáljait is elemezzük (csak véges esetben), mivel a paramodifikáció ötletét az ő konstrukciójuk motiválta. A szakaszt a 3.3.4. Állítással zárjuk, miszerint a Hermite-féle unitálokon nem lehet switchinget végrehajtani, azonban létezik nem triviális paramodifikációjuk.

A 3.4. szakaszban a $\mathbf{D}_b$ részrendszer blokkszínezéseinek meghatározásához mutatunk be különböző módszereket. Új Steiner-féle 2-dizájnok konstruálásához paramodifikáció segítségével az összes blokkszínezés megtalálásában vagyunk érdekeltek. Definiáljuk a $\mathbf{D}_b$ részrendszer Γ vonalgráfját, és a 3.4.2. Lemma szerint $\mathbf{D}_b$

jó k-blokkszínezései lényegében Γ jó k-színezéseinek feleltethetők meg. A Γ gráf k-színezései egy halmazfedési feladat megoldásai független K-halmazokkal, ahol $K = (v - k) / (k - 1)$.

A GRAPE [46] GAP-csomag [14] segítségével ez módszer könnyen implementálható. A gráfszínezési probléma felírható egészértékű programozási (integer linear programming, ILP) feladatként is. A hozzárendeléses modell [26, 2.2. alszakasz] a standard megfogalmazása a csúcsszínezési problémának, de vannak más megközelítések is, például a POP és a POP2 [26, 3. szakasz], melyek részbenrendezésen alapulnak.

A 3.5. szakasz ismert kis unitálok (legfeljebb 6-odrendű) paramodifikációira vonatkozó számítási eredményeket mutat be. Ezzel a módszerrel 173 új 3-adrendű unitált és 25 712 új 4-edrendű unitált konstruáltunk. Bevezetjük a Ψ_n paramodifikációs gráf fogalmát: adott n rend esetén a gráf csúcsai n-edrendű unitálok ekvivalenciaosztályai, és két csúcsot éllel kötünk össze, ha az egyik ekvivalenciaosztályból megkapható a másik paramodifikációval. A paramodifikációs gráf összefüggő komponenseit paramodifikáció-osztályoknak nevezzük a switching osztályok [44] mintájára. Mivel a switch-ek a paramodifikációk speciális esetei, a switching gráf a paramodifikációs gráf részgráfja. Számításokat végeztünk Ψ_3 és Ψ_4 azon paramodifikáció-osztályainak meghatározására, amelyek legalább egy unitált tartalmaznak a BBT, KRC vagy KNP könyvtárak valamelyikéből. A 3-adrendű esetben megtaláltuk az összes paramodifikáció-osztályt, azaz Ψ_3 ezen részgráfja teljes abban az értelemben, hogy minden csúcs összes paramodifikációja ismert. A 4-edrendű esetben a részgráf hiányos, mivel vannak befejezetlen csúcsai: ezen unitálok paramodifikációi nem lettek kiszámolva. Négy osztály hiányos (lásd a csillaggal jelölt sorokat a 3.1. táblázatban), összesen 12 484 befejezetlen csúccsal. További adatok az unitálok paramodifikációiról a `https://davidmezofi.github.io/unitals/` honlapon érhetők el.

A 4. fejezetben Mezőfi és Nagy *On the geometry of full points of abstract unitals* c. cikkének [38] eredményeit mutatjuk be. A 4.1. szakaszban definiáljuk unitálok teljes pontjait, teljespont-regularitását, perspektivitási csoportjaikat és beágyazott duális k-neteiket. Az teljes pontok számára vonatkozó $n^2 - 1$ és $n^2 - n$ felső korlátokat bizonyítjuk diszjunkt, illetve metsző blokkpárok esetén. Megmutatjuk, hogy egy n-edrendű unitálnak legfeljebb beágyazott duális $(n-1)$-nete lehet, amiből következik, hogy bármely teljespont-halmaz legfeljebb $n - 3$ blokkot tartalmazhat. A szakasz azzal fejeződik be, hogy miként tekinthetünk a beágyazott duális 3-netekre mint latin négyzetekre.

A 4.2. szakasz célja belátni, hogy bármely, a klasszikus projektív síkba, azaz

$\mathrm{PG}(2,q^2)$-be ágyazott q-adrendű unitál erősen teljespont-reguláris (ld. 4.2.6. Tétel). Ehhez több lemmára és [32]-beli eredményekre is szükségünk van.

A 4.3. szakaszban megmutatjuk, hogy bármely q páros prímhatvány esetén, ha a $\mathcal{H}(q)$ Hermite-féle unitál blokkjai egy polár háromszögben vannak, akkor a három blokk beágyazott duális 3-netet alkot (vö. 4.3.1. Állítás). Egy másik bizonyított állítás szerint, ha egy tetszőleges absztrakt unitál be van ágyazva $\mathrm{PG}(2,q^2)$-be, akkor ha három blokkja beágyazott duális 3-netet alkot, akkor ezek a blokkok Baer-részegyenesek $\mathrm{PG}(2,q^2)$-ben, ld. 4.3.3. Állítás.

A 4.4. szakasz kis unitálok teljes pontjainak struktúrájára vonatkozó számítási eredményeket mutat be, például hogy a 6-odrendű Bagchi–Bagchi-unitálban [2] nincsenek teljes pontok. A 4.1 és 4.2. táblázatok 3-ad- és 4-edrendű unitálok számát tartalmazzák a teljes pontok száma és perspektivitási csoport struktúrája szerinti bontásban. A vizsgált könyvtárakban található (erősen) teljespont-reguláris unitálok száma a 4.4. táblázatban található. Megjegyezzük, hogy a nem erősen teljespont-reguláris unitálok nem ágyazhatók be $\mathrm{PG}(2,q^2)$-be.

Az 5. fejezet a UnitalSZ [42] GAP-csomagot és néhány kapcsolódó algoritmust mutatja be, melyet a jelen disszertáció szerzője, valamint témavezetője, dr. Nagy Gábo Péter feljesztett. A csomag jelenlegi verziója 0.6, a kiadás elérhető a `https://nagygp.github.io/UnitalSZ` honlapon, illetve a forráskód elérhető a GitHubon. A fejezet során példa GAP-kódok illusztrálják az ismertetett függvényeket.

Az 5.1. szakasz betekintést ad, hogy miként lehet unitál objektumokat létrehozni igaz-hamis, és illeszkedési mátrixok, valamint blokklisták által. Az 5.1. Algoritmusban látható, hogy az unitálokra vonatkozó feltételek hogyan vannak a csomagban implementálva. Ismertetünk az unitálok néhány alapvető tulajdonságára, attribútumára vonatkozó metódust, például hogyan lehet az unitál pontjait, blokkjait, automorfizmus-csoportját lekérni, illetve hogy ellenőrízhető, hogy két unitál izomorf-e. Az 5.2. szakaszban az elérhető unitálosztályokhoz és -könyvtárakhoz kapcsolódó parancsokat mutatjuk be. Az 5.2. és 5.3. Algoritmusok a Hermite- és a Buekenhout–Metz-unitálok implementációját illusztrálják.

Az 5.3. szakaszban ismertetjük az unitálok teljes pontjaira vonatkozó parancsokat: meghatározható egy U unitál teljes pontjai két különböző blokkra vonatkoztatva, sőt, kiszámolható a perspektivitási csoport is (vö. 5.4. és 5.6. Algoritmusok). Az 5.5. Algoritmus bemutatja, hogy egy unitál teljes pontjainak kiszámítása az U unitál automorfizmus-csoportjának erejéig hogyan van implementálva a csomagban. A beágyazott duális 3-netek, illetve az (erős) teljespont-regularitás meghatározására szolgáló függvények leírása a szakasz végén található.

Appendix A.

GAP implementation of paramodification

```
DeclareInfoClass( "InfoParamod" );

AllRegularBlockColorings := function( bls, nr_colors, gr )
  local Gamma, complete_subgraphs, graph_of_cliques, colorings, ret,
        new_blocks, c, c_vec, i, j;
  Gamma := Graph( gr, bls, OnSets,
                  function( x, y )
                    return x <> y and Intersection( x, y ) = [];
                  end );
  complete_subgraphs := CompleteSubgraphs( Gamma, Size( bls ) / nr_colors, 1 );
  complete_subgraphs := Union( List( complete_subgraphs,
    x -> Orbit( AutomorphismGroup( Gamma ), x, OnSets ) ) );
  Info( InfoParamod, 3, "cliques of the line graph computed..." );
  graph_of_cliques := Graph( Gamma.group, complete_subgraphs, OnSets,
    function( x, y )
      return x <> y and Intersection( x, y ) = [];
    end );
  colorings := CompleteSubgraphs( graph_of_cliques, nr_colors, 1 );
  Info( InfoParamod, 3, Size( colorings ), " block colorings computed... " );
  ret := [];
  for c in colorings do
    c_vec := 0*[1..Size(bls)];
    for i in [1..nr_colors] do
      for j in VertexNames( graph_of_cliques )[c[i]] do
```

```
        c_vec[ Position( bls, VertexNames( Gamma )[j] ) ] := i;
      od;
    od;
    Add(ret, Transformation( c_vec ) );
  od;
  return ret;
end;

ParamodificationOfUnitalNC := function( u, b, chi )
  local Cb, n_Cb, C_star_b, intact_blks, B_star;
  Cb := Filtered( BlocksOfUnital( u ),
    x -> Size( Intersection( x, b ) ) = 1 );
  n_Cb := Length( Cb );
  C_star_b := List( [1..n_Cb],
    i -> Union( Difference( Cb[i], b ), [ b[i^chi] ] ) );
  intact_blks := Difference( BlocksOfUnital( u ), Cb );
  B_star := Union( intact_blks, C_star_b );
  return AbstractUnitalByDesignBlocks( B_star );
end;

ParamodificationOfUnital := function( u, b, chi )
  local Cb;
  if not b in BlocksOfUnital( u ) then
    Error( "argument 2 must be a block of argument 1");
  fi;
  Cb := Filtered( BlocksOfUnital( u ),
                   x -> Size( Intersection( x, b ) ) = 1 );
  Cb := List( Cb, x -> Difference( x, b) );
  if not ForAll( Combinations( [1..Size(Cb)], 2 ),
      p -> Intersection( Cb{p} ) = [] or ( p[1]^chi <> p[2]^chi ) ) then
    Error( "argument 3 is not a proper block coloring" );
  fi;
  return ParamodificationOfUnitalNC( u, b, chi );
end;

ParamodificationsOfUnitalWithBlock := function( u, b )
```

```
  local q, Cb, b_stab, new_unitals, all, allchibmod, i, isom_class,
   colorings;
  if not b in BlocksOfUnital( u ) then
    Error( "argument 2 must be a block of argument 1");
  fi;
  q := Order( u );
  Cb := Filtered( BlocksOfUnital( u ),
    x -> Size( Intersection( x, b ) ) = 1 );
  Cb := List( Cb, x -> Difference( x, b ) );
  b_stab := Stabilizer( AutomorphismGroup( u ), b, OnSets );
  colorings := AllRegularBlockColorings( Cb, q + 1, b_stab );
  Info( InfoParamod, 4, Size( colorings ), " coloring(s) for the given
   unital-block pair computed..." );
  new_unitals := List( colorings, c -> ParamodificationOfUnitalNC( u, b,
    c ) );
  all := [1..Length( new_unitals )];
  allchibmod := [];
  while all <> [] do
    i := Remove( all );
    isom_class := Filtered( all, x -> Isomorphism( new_unitals[i],
      new_unitals[x] ) <> fail ) ;
    all := Difference( all, isom_class );
    Add( allchibmod, new_unitals[i] );
  od;
  return allchibmod;
end;

AllParamodificationsOfUnital := function( u )
  local blocks, rep_blocks, allchibmods, uus, b;
  blocks := BlocksOfUnital( u );
  rep_blocks := List( Orbits( AutomorphismGroup( u ), blocks, OnSets ),
    orb -> Representative( orb ) );
  Info( InfoParamod, 3, Size( rep_blocks ), " block representatives for
   the unital computed..." );
  allchibmods := [];
  for b in rep_blocks do
```

```
    uus := ParamodificationsOfUnitalWithBlock( u, b );
    uus := Filtered( uus, x -> Isomorphism( x, u ) = fail and
        ForAll( allchibmods, y -> Isomorphism( y, x ) = fail ) );
    Append( allchibmods, uus );
  od;
  return allchibmods;
end;
```

Bibliography

[1] E. F. Assmus, Jr. and J. D. Key. *Designs and their codes*, volume 103 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1992.

[2] Sunanda Bagchi and Bhaskar Bagchi. Designs from pairs of finite fields. I. A cyclic unital $U(6)$ and other regular Steiner 2-designs. *J. Combin. Theory Ser. A*, 52(1):51–61, 1989.

[3] John Bamberg, Anton Betten, Cheryl E. Praeger, and Alfred Wassermann. Unitals in the Desarguesian projective plane of order 16. *J. Statist. Plann. Inference*, 144:110–122, 2014.

[4] Adriano Barlotti and Karl Strambach. The geometry of binary systems. *Adv. in Math.*, 49(1):1–105, 1983.

[5] Susan Barwick and Gary Ebert. *Unitals in projective planes*. Springer Monographs in Mathematics. Springer, New York, 2008.

[6] V. D. Belousov. Алгебраические сети и квазигруппы. Izdat. "Štiinca", Kishinev, 1971.

[7] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1999.

[8] Anton Betten, Dieter Betten, and Vladimir D. Tonchev. Unitals and codes. volume 267, pages 23–33. 2003. Combinatorics 2000 (Gaeta).

[9] Albrecht Beutelspacher and Ute Rosenbaum. *Projective geometry: from foundations to applications*. Cambridge University Press, Cambridge, 1998.

[10] Garrett Birkhoff and Saunders Mac Lane. *A survey of modern algebra*. Third edition. The Macmillan Co., New York; Collier-Macmillan Ltd., London, 1965.

[11] Simona Bonvicini and Tomaž Pisanski. A novel characterization of cubic Hamiltonian graphs via the associated quartic graphs. *Ars Math. Contemp.*, 12(1):1–24, 2017.

[12] Nicholas J. Cavenagh and Terry S. Griggs. Subcubic trades in Steiner triple systems. *Discrete Math.*, 340(6):1351–1358, 2017.

[13] G. Faina and G. Korchmáros. A graphic characterization of Hermitian curves. In *Combinatorics '81 (Rome, 1981)*, volume 18 of *Ann. Discrete Math.*, pages 335–342. North-Holland, Amsterdam-New York, 1983.

[14] GAP – Groups, Algorithms, and Programming, Version 4.11.0, Feb 2020. Avaible as `https://www.gap-system.org`.

[15] Heidi Gebauer. Enumerating all Hamilton cycles and bounding the number of Hamilton cycles in 3-regular graphs. *Electron. J. Combin.*, 18(1):Paper 132, 28, 2011.

[16] Ambros Gleixner, Michael Bastubbe, Leon Eifler, Tristan Gally, Gerald Gamrath, Robert Lion Gottwald, Gregor Hendel, Christopher Hojny, Thorsten Koch, Marco E. Lübbecke, Stephen J. Maher, Matthias Miltenberger, Benjamin Müller, Marc E. Pfetsch, Christian Puchert, Daniel Rehfeldt, Franziska Schlösser, Christoph Schubert, Felipe Serrano, Yuji Shinano, Jan Merlin Viernickel, Matthias Walter, Fabian Wegscheider, Jonas T. Witt, and Jakob Witzig. The SCIP Optimization Suite 6.0. Technical report, Optimization Online, July 2018.

[17] Henry H. Glover, Klavdija Kutnar, and Dragan Marušič. Hamiltonian cycles in cubic Cayley graphs: the $\langle 2, 4k, 3\rangle$ case. *J. Algebraic Combin.*, 30(4):447–475, 2009.

[18] Mike J. Grannell, Terry S. Griggs, Edita Máčajová, and Martin Škoviera. Coloring cubic graphs by point-intransitive Steiner triple systems. *J. Graph Theory*, 74(2):163–181, 2013.

[19] Theo Grundhöfer, Markus J. Stroppel, and Hendrik Van Maldeghem. A non-classical unital of order four with many translations. *Discrete Math.*, 339(12):2987–2993, 2016.

[20] Klaus Grüning. A class of unitals of order q which can be embedded in two different planes of order q^2. *J. Geom.*, 29(1):61–77, 1987.

[21] J. W. P. Hirschfeld. *Projective geometries over finite fields*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, second edition, 1998.

[22] Ian Holyer. The NP-completeness of edge-coloring. *SIAM J. Comput.*, 10(4):718–720, 1981.

[23] Daniel R. Hughes and Fred C. Piper. *Projective planes*. Springer-Verlag, New York-Berlin, 1973. Graduate Texts in Mathematics, Vol. 6.

[24] John F. Humphreys. *A course in group theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1996.

[25] Robert W. Irving and David F. Manlove. The *b*-chromatic number of a graph. *Discrete Appl. Math.*, 91(1-3):127–141, 1999.

[26] Adalat Jabrayilov and Petra Mutzel. New integer linear programming models for the vertex coloring problem. In *LATIN 2018: Theoretical informatics*, volume 10807 of *Lecture Notes in Comput. Sci.*, pages 640–652. Springer, Cham, 2018.

[27] Marko Jakovac and Iztok Peterin. The b-chromatic number and related topics—a survey. *Discrete Appl. Math.*, 235:184–201, 2018.

[28] Petteri Kaski and Patric R. J. Östergård. *Classification algorithms for codes and designs*, volume 15 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006. With 1 DVD-ROM (Windows, Macintosh and UNIX).

[29] A. Donald Keedwell and József Dénes. *Latin squares and their applications*. Elsevier/North-Holland, Amsterdam, second edition, 2015. With a foreword to the previous edition by Paul Erdös.

[30] György Kiss and Tamás Szőnyi. *Véges geometriák*. Polygon Könyvtár. Polygon, Szeged, 2001.

[31] Ivo Koch and Javier Marenco. An integer programming approach to b-coloring. *Discrete Optim.*, 32:43–62, 2019.

[32] G. Korchmáros and F. Mazzocca. Nuclei of point sets of size $q + 1$ contained in the union of two lines in $\mathrm{PG}(2, q)$. *Combinatorica*, 14(1):63–69, 1994.

[33] Gábor Korchmáros, Alessandro Siciliano, and Tamás Szőnyi. Embedding of classical polar unitals in $\mathrm{PG}(2, q^2)$. *J. Combin. Theory Ser. A*, 153:67–75, 2018.

[34] Vedran Krčadinac. Some new Steiner 2-designs $S(2,4,37)$. *Ars Combin.*, 78:127–135, 2006.

[35] Vedran Krčadinac, Anamari Nakić, and Mario Osvin Pavčević. The Kramer-Mesner method with tactical decompositions: some new unitals on 65 points. *J. Combin. Des.*, 19(4):290–303, 2011.

[36] Christiane Lefèvre-Percsy. Characterization of Hermitian curves. *Arch. Math. (Basel)*, 39(5):476–480, 1982.

[37] A. C. H. Ling, C. J. Colbourn, M. J. Grannell, and T. S. Griggs. Construction techniques for anti-Pasch Steiner triple systems. *J. London Math. Soc. (2)*, 61(3):641–657, 2000.

[38] Dávid Mezőfi and Gábor P. Nagy. On the geometry of full points of abstract unitals. *Des. Codes Cryptogr.*, 87(12):2967–2978, 2019.

[39] Dávid Mezőfi and Gábor P. Nagy. New Steiner systems from old ones by paramodifications. *arXiv e-prints*, page arXiv:2003.09233, March 2020.

[40] Verena Möhler. *SL(2,q)-Unitals*. PhD thesis, Karlsruher Institut für Technologie (KIT), 2020.

[41] Janina Müttel, Dieter Rautenbach, Friedrich Regen, and Thomas Sasse. On the cycle spectrum of cubic Hamiltonian graphs. *Graphs Combin.*, 29(4):1067–1076, 2013.

[42] G. P. Nagy and D. Mezőfi. UnitalSZ, algorithms and libraries of abstract unitals and their embeddings, Version 0.6, Mar 2020. GAP package.

[43] Michael E. O'Nan. Automorphisms of unitary block designs. *J. Algebra*, 20:495–511, 1972.

[44] Patric R. J. Östergård. Switching codes and designs. *Discrete Math.*, 312(3):621–632, 2012.

[45] L. P. Petrenjuk and A. J. Petrenjuk. Weighted blocking designs and their transformations. *Svitohliad*, 3:45–72, 1996.

[46] L. H. Soicher. GRAPE, GRaph Algorithms using PErmutation groups, Version 4.8.3, Dec 2019. Refereed GAP package.