Quasiregular Projective Planes of Order 16

A Computational Approach

Marc Röder

Vom Fachbereich Mathematik der Technischen Universität Kaiserslautern
zur Verleihung des akademischen Grades Doktor der Naturwissenschaften
(Doctor rerum naturalium, Dr. rer. nat.) genehmigte Dissertation

1. Gutachter: Prof. Dr. U. Dempwolff
2. Gutachter: Prof. Dr. D. Held

Vollzug der Promotion: 21. November 2006

D386

Abstract

This thesis discusses methods for the classification of finite projective planes via exhaustive search. In the main part the author classifies all projective planes of order 16 admitting a large quasiregular group of collineations. This is done by a complete search using the computer algebra system GAP. Computational methods for the construction of relative difference sets are discussed. These methods are implemented in a GAP-package, which is available separately.

As another result –found in cooperation with U. Dempwolff– the projective planes defined by planar monomials are classified. Furthermore the full automorphism group of the non-translation planes defined by planar monomials are classified.

Zusammenfassung

Die Arbeit befasst sich mit Methoden zur Klassifikation endlicher projektiver Ebenen mittels vollständiger Suche. Im Hauptteil werden die projektiven Ebenen der Ordnung 16 klassifiziert, die eine große quasireguläre Kollineationsgruppe besitzen. Dies geschieht durch eine vollständige Suche mit Hilfe des Computeralgebra Systems GAP. Dafür werden Methoden zur Konstruktion relativer Differenzmengen erörtert. Diese Methoden wurden vom Verfasser in einem GAP-Paket implementiert und sind separat erhältlich.

Ein weiteres Resultat (in Zusammenarbeit mit U. Dempwolff) ist die Klassifikation der projektiven Ebenen, die durch planare Monome definiert sind. Für Ebenen, die durch Monome definiert und keine Translationsebenen sind, wird die volle Automorphismengruppe berechnet. Damit sind für alle planare Monome die Automoprhismengruppen der zugehörigen Ebenen bekannt.

Mathematics Subject Classification (MSC 2000):

05B25 Finite geometries

05B10 Difference sets (number-theoretic, group-theoretic etc.)

51E15 Affine and projective planes

51A35 Non-Desarguesian affine and projective planes

12E10 Special polynomials over general fields

Keywords:

relative difference set, projective plane, quasiregular group, Dembowski-Piper classification, planar function, non-Desarguesian plane, GAP

Schlagworte:

relative Differenzmenge, projektive Ebene, quasireguläre Gruppe, Dembowski-Piper Klassifikation, planare Funktion, nicht- desarguessche Ebene, GAP

Preface

During the last two decades, computational group theory and computational finite geometries have become very active fields of research. The most prominent result from this area is the proof of the non-existence of projective planes of order 10 [LTS89]. But besides the proof of conjectures by complete enumeration of the problem –or part of it– there is another reason for the popularity of computational methods. Experiments using computer algebra systems sometimes lead to new constructions or theorems as they encourage "inspired guessing". Computer algebra systems like GAP are of great help here as they are easy to use and provide plenty of functionality. So it is not necessary to do a lot of programming to just "have a look" at a few sample cases.

The present thesis shows one instance of either case. In the main part, a computer search is done to classify a certain type of projective planes. In chapter 6 we prove a theorem (in cooperation with U. Dempwolff) which grew from related experiments and a close investigation of a sample case.

This text is structured as follows:

In chapter 1 we will have a look at the connection between projective planes and difference sets. Section 1.3 relates relative difference sets to projective planes and divisible designs. With a view towards a computer search for relative difference sets, section 1.4 develops a tool called "coset signature". This tool enables us to use information about the subgroup structure of a group for the generation of relative difference sets in this group (and even in others with a similar subgroup structure).

For the case of ordinary difference sets, chapter 2 demonstrates the use of representation theory to calculate coset signatures in a certain class of groups. As a result, a search for difference sets in groups of this class can (normally) be done much easier.

In chapter 3 we approach the main objective of this thesis. The types of planes given by the classification of Dembowski and Piper [DP67] are studied to find all projective planes of order 16 admitting a large quasiregular automorphism group. For each case, a difference set construction is given and the results of the corresponding computer search are stated as a theorem. The algorithmic part of this search is considered in chapter 4. After a general outline of the search algorithms, several aspects of the algorithms receive special attention. Some examples for the implementation in GAP are given in appendix B. In chapter 5 a few experiments in higher order are documented. This illustrates some possibilities for further searches using similar methods.

Chapter 6 shows an example of how computer experiments may lead to general results. Calculations for projective planes of order 81, as described in chapter 5, led to the problem of identifying a projective plane (which turned out to be the one of Coulter and Matthews [CM97]). From the attempt to construct the full automorphism group of the projective plane and to find the defining planar polynomial, arguments for the classification of planar monomials in general were derived. The result is a theorem which classifies the projective planes defined by planar monomials and determines the full automorphism group for each of them. This part was done in cooperation with Prof. Dempwolff and is submitted to "Innovations in Incidence Geometry" [DR].

Finally, some open problems and possibilities for further work in this field are discussed.

Most of the functionality needed for the computational part of this text is implemented as a GAP package called "RDS" and is freely available from the "Packages" section of the GAP homepage [Röd06]. The implementation was done such that relative difference sets with $\lambda > 1$ –which do not play a role in thesis– can also be studied.

I would like to thank several people and institutions for their support. Prof. Dr. Dempwolff for giving me the chance to write this dissertation and for his advice in doing so. The state Rhineland-Palatinate for supporting my work with a scholarship. The University of Kaiserslautern, especially the Department of Mathematics and the RHRK for letting me use their Computers and other infrastructure. And all my friends and family for their support during this time.

Contents

List of Algorithms

Chapter 1

General theory

1.1 Notation

Let $\mathcal{D}$ be an incidence structure and p a point of $\mathcal{D}$. Then $[p]$ denotes the set of blocks of $\mathcal{D}$ incident with p. Analogously, for a block B, the set of points incident with B is denoted by $[B]$. We will also identify blocks with point sets writing $B = \{p_1, \dots, p_n\} = [B]$. For a set $\{a_1, \dots, a_n\}$ of points (blocks), $[a_1, \dots, a_n]$ is the set of blocks (points) incident with all of $a_1, \dots, a_n$. When talking about projective planes, blocks will also be called lines.

Let p be a point and B a block of an incidence structure $\mathcal{D}$. The pair (p, B) is called a *flag* if p is incident with B and *anti-flag* otherwise.

The set of all prime numbers will be denoted by $\mathbb{P}$. All groups and incidence structures are assumed to be finite. For $n \in \mathbb{N}$, the cyclic group of order n is denoted by C_n. For $p \in \mathbb{P}$ and $n \in \mathbb{N}$ the elementary abelian group of order p^n is denoted by E_{p^n}. For a group G, let $\mathrm{Aut}(G)$ denote the group of automorphisms and $\mathrm{Aut}^\circ(G)$ the group of automorphisms and anti-automorphisms.

1.1 Definition. Let M be a set and $\mu\colon M \to \mathbb{N}$, the pair (M, μ) is called a *multiset*. For all $m \in M$, the number $\mu(m)$ is called *multiplicity* of m.

Let M be a set and $n \in \mathbb{N}$. Let $m \in M^n$ and let $\tilde{m} := \{x \in M \mid x \in m\}$ be the set containing the entries of the tuple m. Furthermore, let $\mu_{\tilde{m}}\colon \tilde{m} \to \mathbb{N}$ map $x \in \tilde{m}$ onto the number of times x occurs in then n-tuple m. Then $\|m\| = (\tilde{m}, \mu_{\tilde{m}})$ is the multiset of m.

Loosely speaking, a *multiset* is a set which may contain the same element several times. For $M \subseteq \mathbb{N}$ (or any totally ordered set) with $|M| < \infty$, the multiset (M, μ) can be identified with the tuple $(m_1, \ldots, m_n)$ where $m_i \leq m_{i+1}$ for all $1 \leq i < n = \sum_{m \in M} \mu(m)$. So finite multisets may be compared pointwise.

1.2 Ordinary difference sets

1.2 Definition. Let $1 < n$ and G a finite group. A set $D \subseteq G$ with $k = |D|$ is called *difference set* of order $n = k - \lambda$, if for all $1 \neq g \in G$ there exist exactly λ pairs $(a, b) \in D \times D$ such that $ab^{-1} = g$. A difference set D is called (v, k, λ)-difference set for $v = |G|$.

The following observations show the connection between difference sets and projective planes.

1.3 Lemma. *Let $D \subseteq G$ be a (v, k, λ)-difference set. Then also D^{-1} is a (v, k, λ)-difference set. In other words: for every $1 \neq g \in G$ there are exactly λ pairs $(d_1, d_2) \in D \times D$ with $g = d_1^{-1} d_2$ and exactly λ pairs $(d_3, d_4) \in D \times D$ with $g = d_3 d_4^{-1}$.*

Proof. First, let $aD = bD$. Then there are exactly $|D| = k > \lambda$ pairs $(d_1, d_2) \in D^2$ such that $b^{-1}a = d_1 d_2^{-1}$ holds. Hence $a = b$.

Now let $1 \neq g \in G$. Then there are exactly λ solutions for $d_1 d_2^{-1} = g$, i.e. $|D \cap gD| = \lambda$. So $(D, \{gD \mid g \in G\})$ is a symmetric (v, k, λ)-design.

We may assume $1 \in D$ without loss of generality. Then 1 is contained exactly in the blocks $d^{-1}D$ where $d \in D$. By the same argument $g \neq 1$ is contained exactly in the blocks $gd^{-1}D$ with $d \in D$.

But $|[1] \cap [g]| = \lambda$ and so there are exactly λ pairs $(d_1, d_2) \in D^2$ satisfying

$$d_1^{-1} D = g d_2^{-1} D$$

and exactly λ pairs $(d_1, d_2) \in D^2$ satisfying

$$d_1^{-1} = g d_2^{-1}$$

□

1.4 Corollary. *Let $D \subseteq G$ be a (v, k, λ)-difference set and $g, h \in G$. Furthermore, let $d_{1_i} d_{2_i}^{-1} = gh^{-1}$ be the presentations as quotients in D with $d_{1_i}, d_{2_i} \in D$ and $1 \leq i \leq \lambda$. Then g and h are connected exactly by the lines $Dd_{2_i}^{-1}h$ with $1 \leq i \leq \lambda$.*

Proof. Obviously $g \in Dd_{2_i}^{-1}h$. On the other hand, $Dd_{2_i}^{-1}h \ni d_{1_i}d_{2_i}^{-1}h = h$. And as $d_1 g = d_2 h \iff gh^{-1} = d_1^{-1}d_2$ these are all lines connecting h to g. □

1.5 Definition. Let G be a group and $D \subseteq G$. Define $B = \{Dg \mid g \in G\}$, then the incidence structure $\operatorname{dev} D := (G, B, \in)$ is called *development of D*.

1.6 Theorem. *Let G be a group and $D \subseteq G$ a $(n^2+n+1, n+1, 1)$-difference set. Then* $\operatorname{dev} D$ *is a projective plane of order n.*

Via right multiplication, G defines a group of collineations of $\operatorname{dev} D$ *acting regularly on points and blocks.*

Proof. Let $x, y \in G$ with $x \neq y$. By definition and 1.3 there is exactly one pair $(d_1, d_2) \in D \times D$ satisfying $yx^{-1} = d_1^{-1}d_2$ and hence $yd_1 = d_2 x$. So the blocks xD and yD have exactly one point in common.

Now let $x, y \in G$ be distinct points. Again, there is exactly one pair $(d_3, d_4) \in D \times D$ with $xy^{-1} = d_3 d_4^{-1}$. Set $z = d_4^{-1}y$, then $x = d_3, d_4^{-1}y = d_3 z$ and $y = d_4 z$. Hence the block Dz contains the points x and y.

Let $g \in G$. Then there are exactly $|D|$ blocks incident with g (as G acts regularly). For the same reason all blocks have size $|D|$. □

1.7 Definition. Let $\mathcal{D}$ be a design and let $G \leq \operatorname{Aut}(\mathcal{D})$ act regularly on the points and blocks of $\mathcal{D}$. Then G is called *Singer group* of $\mathcal{D}$.

An important tool in the study of difference sets is the presentation as elements of the group ring $\mathbb{Z}[G]$. This is done as follows:

$$\begin{aligned} \widehat{\ }\colon \operatorname{Pot}(G) &\to \mathbb{Z}[G] \\ M &\mapsto \sum_{g \in G} v_g g \qquad \text{where} \quad v_g := \chi_M(g) \end{aligned}$$

where χ_M denotes the characteristic function of M. If there is no risk of confusion, we identify D with its image under $\widehat{\ }$ and write $D = \sum_{g \in G} v_g g$. Define

$$\begin{aligned} D^{-1} &:= \sum_{g \in G} v_g g^{-1} \\ |D| &:= \sum_{g \in G} v_g \end{aligned}$$

So difference sets may also be defined by the equation

$$DD^{-1} = n \cdot 1 + \lambda G.$$

Let $\varphi\colon G \to H$ be an epimorphism with $\ker \varphi = U$. Then φ is canonically lifted to the group ring by

$$\left(\sum v_g g\right)^{\varphi} = \sum v_g g^{\varphi}. \tag{1.7.1}$$

Then

$$(DD^{-1})^{\varphi} = n \cdot 1^{\varphi} + \lambda(\widehat{G})^{\varphi} = n \cdot 1^{\varphi} + \lambda |U| H. \tag{1.7.2}$$

Note. *As the same letter is used for the lifted and the original homomorphism, the problem arises that in general* $(\widehat{G})^{\varphi}$ *is not equal to* $\widehat{G^{\varphi}}$*. So in this case, the* $\widehat{\ }$ *may not be omitted.*

If $\varphi\colon G \to 1$ *is the trivial homomorphism, and* $D \in \mathbb{Z}[G]$*, then* $D\varphi = |D| \cdot 1 = k$*.*

1.3 Relative difference sets

1.8 Definition. Let G be a finite group and $1 \in N \subseteq G$. Then $D \subseteq G$ with $k = |D|$ is called *relative difference set with forbidden set* N, if for some $\lambda \in \mathbb{N}$ the following equation in $\mathbb{Z}[G]$ holds:

$$DD^{-1} = k + \lambda(G - N).$$

D is called $(|G|/|N|, |N|, k, \lambda)$-difference set.

Note that $|G|/|N|$ isn't necessarily an integer. This may be inconvenient but as this notation is customary for $N \leq G$, we will also use it in the general case.

Note. (a) *Sometimes, difference sets with* $1 \in D$ *are called "regular" difference sets. For the ease of notation, we do only consider regular difference sets.*

(b) *Relative difference sets with* $N = \{1\}$ *are ordinary difference sets as defined on page 7.*

(c) *Relative difference sets with forbidden* sets *(as opposed to those having forbidden groups) are sometimes called neo-difference sets (see [Sch02, GJ03b]).*

1.9 Definition. Let G be a finite group. The set $D \subseteq G$ is called *partial relative difference set* with forbidden set $N \subseteq G$, if in $\mathbb{Z}[G]$

$$DD^{-1} = \kappa + \sum_{g \in G-N} v_g g$$

holds for some $1 \leq \kappa \leq k$ and $0 \leq v_g \leq \lambda$ for all $g \in G - N$.

Clearly, relative difference sets are also partial relative difference sets (with $\kappa = k$ and $v_g = \lambda$ for all $g \in G - N$). Let $D \subseteq G$ be a partial relative difference set. We say that D can be *extended*, if there is a relative difference set $D' \subseteq G$ with the same forbidden set and $D \subseteq D'$. Clearly not every partial relative difference set can be extended to a full relative difference set.

For a relative difference set D, the translates of D together with the elements of G do not form a projective plane. Yet sometimes the incidence structure defined by D may be lifted to a projective plane having G as a group of collineations. In this case G will have one orbit of length $|G|$ and N will fix a substructure.

As for ordinary difference sets (see 1.3), we have

1.10 Lemma. *Let $D \subseteq G$ be a relative (m_1, m_2, k, λ)-difference set with forbidden set $N \subseteq G$. Then also D^{-1} is a relative (m_1, m_2, k, λ)-difference set with forbidden set N. In other words: for every $g \in G - N$ there are exactly λ pairs $(d_1, d_2) \in D \times D$ satisfying $g = d_1^{-1} d_2$ and exactly λ pairs $(d_3, d_4) \in D \times D$ with $d_3 d_4^{-1} = g$.*

Proof. Let $a, b \in G - N$ and $aD = bD$. As there are exactly $|D| = k > \lambda$ pairs $(d_1, d_2) \in D^2$ solving $b^{-1}a = d_1 d_2^{-1}$, we have $a = b$.

Now let $g \in G - N$. Then there are exactly λ solutions for $d_1 d_2^{-1} = g$, in other words $|D \cap gD| = \lambda$.

W.l.o.g. $1 \in D$, then 1 is contained exactly in the blocks $d^{-1}D$ with $d \in D$. By the same argument, we see that $g \neq 1$ is contained exactly in the k blocks $gd^{-1}D$ with $d \in D$. So $(G - N, \{gD \mid g \in G - N\})$ is a symmetric design. Therefore $|[1] \cap [g]| = \lambda$ and there are exactly λ pairs $(d_1, d_2) \in D^2$ solving

$$d_1^{-1} D = g d_2^{-1} D$$

and exactly λ pairs with

$$d_1^{-1} = gd_2^{-1}$$

We have $d_1^{-1}d_2 = 1 \iff d_1d_2^{-1} = 1$ and every element of $G - N$ may be represented in exactly λ ways as $d_1^{-1}d_2$. Every element of $G - N$ may also be represented as $d_1d_2^{-1}$ in exactly λ ways. Hence, there is no pair $(d_1, d_2) \in D \times D$ with $d_1 \neq d_2$ for which $d_1^{-1}d_2 \in N$. □

Now we will investigate some of the geometric properties of the forbidden set N. And we will see which geometric objects are associated with relative difference sets.

1.11 Lemma. *Let $D \subseteq G$ be a relative $(|G|/|N|, |N|, k, \lambda)$-difference set with forbidden set N and $g, h \in G$ with $gh^{-1} \notin N$. Moreover, let $d_{1_i}d_{2_i}^{-1} = gh^{-1}$ be the presentations as quotients in D with $d_{1_i}, d_{2_i} \in D$ and $1 \leq i \leq \lambda$. Then g and h are connected exactly by the lines $Dd_{2_i}^{-1}h$ with $1 \leq i \leq \lambda$.*

In particular, the points $g, h \in G$ are disconnected in $\operatorname{dev} D$ *iff $gh^{-1} \in N$.*

Proof. Obviously $h \in Dd_{2_i}^{-1}h$. On the other hand, $Dd_{2_i}^{-1}h \ni d_{1_i}d_{2_i}^{-1}h = g$. And as $d_1g = d_2h \iff gh^{-1} = d_1^{-1}d_2$ these are all lines connecting h to g.

Now assume g, h to be disconnected. Then $g \notin Dc^{-1}h$ for all $c \in D$. Hence $gh^{-1} \notin Dc^{-1}$ for all $c \in D$. Therefore gh^{-1} is not a quotient of two elements of D. This shows $gh^{-1} \in N$. □

1.12 Corollary. *Let $D \subseteq G$ be a relative difference set with forbidden set $N \subseteq G$ and $U \leq G$ with $U \subseteq N$. Then the cosets of U are totally disconnected in* $\operatorname{dev} D$. *Moreover, D contains at most one element from each coset modulo U.*

Proof. Let $n_1g, n_2g \in Ug$ with $g \in G$. As U is a group, we have $n_1g(n_2g)^{-1} \in U$ and so from 1.11 we know that n_1g and n_2g must be disconnected. □

1.13 Corollary. *Let D be a relative $(|G|/|N|, |N|, k, \lambda)$-difference set with forbidden set $N \subseteq G$. Then $NN^{-1} \subseteq N$ in $\mathbb{Z}[G]$. In particular, N is closed under inversion. Moreover, N is the union of all disconnected subsets of* $\operatorname{dev} D$ *containing* 1.

Proof. By 1.11, the points 1 and $g \in G$ are disconnected if and only if $g^{-1} \in N$.

The fact that $N^{-1} = N$ can also be seen like this: Assume $x \in N^{-1} - N$. Then x can be written as a quotient in D but not in D^{-1}. This contradicts 1.10. □

Note that this does not mean that N is a group or the union of groups. Corollary 1.13 immediately implies

1.14 Corollary. *Let $D \subseteq G$ be a relative difference set with forbidden subgroup $N \leq G$, then the cosets of N are exactly the maximal totally disconnected point-sets of* $\operatorname{dev} D$.

Proof. By 1.12, the cosets of N are totally disconnected.

Let $h \in G - Ng$ with $g \in G$. Then g and h are in different cosets modulo N and therefore $gh^{-1} \notin N$. So g and h are connected and the cosets of N are maximal totally disconnected.

If a set of points is totally disconnected, then each quotient of points is in N. So the set is contained in a coset of N. □

Designs admitting a partition of the point set such that every pair of points from different classes has exactly λ lines joining them and every pair of points from the same class has no line in common are called *divisible designs*.

As seen above, designs defined by relative difference sets with forbidden group are divisible designs. The point classes are given by the cosets of the forbidden group. This implies that the forbidden group acts (via right multiplication) on the point classes.

In fact, relative difference sets with forbidden group are essentially the same as divisible designs with Singer group (for definition see 1.7):

1.15 Theorem. *Let $\mathcal{D}$ be a divisible design with Singer group G. Let $N \leq G$ be the stabiliser of a point class and $D \subseteq G$ a block of $\mathcal{D}$.*

Then D is a relative difference set with forbidden group N and $\operatorname{dev} D \simeq \mathcal{D}$.

Moreover, N can be identified with the point class containing 1 *in* $\operatorname{dev} D$.

Proof. Identify G with the points of $\mathcal{D}$. The action of G on $\mathcal{D}$ is then equivalent to the right regular representation of G. As G acts transitively on the point classes, all classes have the same size and the stabiliser of a point class acts transitively on that class.

We may therefore identify the stabiliser of a point class with the point class containing 1.

The translates of D are the blocks of $\mathcal{D}$, as G is a Singer group. Let $g \in G$. The blocks containing g are exactly the ones of the form $Dd^{-1}g$ with $d \in D$. But $|[1] \cap [g]| = \lambda$ for $g \in G - N$ and $|[1] \cap [g]| = 0$ if $g \in N$. Hence D is a relative difference set with forbidden group N. □

For more about divisible designs and relative difference sets, see Jungnickel [Jun82].

It is natural to call two difference sets isomorphic, if their devlopments are isomorphic as incidence structures. However, this is rarely used. The more general notion of equivalence is much easier to handle "from within the group".

1.16 Definition. Two partial relative difference sets $D, D' \subseteq G$ are called *equivalent* if there is a $g \in G$ and $\varphi \in \mathrm{Aut}(G)$ such that $D = (Dg)^{\varphi}$. The pair (g, φ) is called *equivalence.*

Two partial relative difference sets $D, D' \subseteq G$ are called *strongly equivalent*, if they are equivalent and have the same forbidden set.

Obviously, equivalent difference sets induce isomorphic designs. As seen in 1.10, the inverse of a relative difference set is again a relative difference set. In general, $\operatorname{dev} D^{-1}$ does not have the same isomorphism class as $\operatorname{dev} D$. Instead we have:

1.17 Lemma. *Let $D \subseteq G$ be a relative difference set with forbidden set $N \subseteq G$. Then $\operatorname{dev} D \simeq (\operatorname{dev} D^{-1})^d$ where $\cdot^d$ denotes the dual structure.*

Proof. Let $g \in G$. Then $[g] = \{Da^{-1}g \mid a \in D\}$. So the blocks of $\operatorname{dev} D$ meeting g can be identified with $D^{-1}g$. In particular, $D^{-1}g$ is a block of $(\operatorname{dev} D)^d$ and hence D^{-1} is a difference set for $(\operatorname{dev} D)^d$. □

So inverting a difference set means dualising the corresponding design. As forbidden subsets are closed under inversion (1.13), we may introduce a "weak" version of strong equivalence by admitting not only automorphisms, but also anti-automorphisms of G. This is the form of equivalence we will be concerned with.

1.4 Quotient images and signatures

1.18 Definition (Similar to [Bec04])**.** Let G be a finite group. $D = \sum v_i g_i \in \mathbb{Z}[G]$ is called *"quotient image"* of a relative difference set, if there are $k, \lambda, s \in \mathbb{N}$ and $N = \sum_{i=1}^{|G|} n_i g_i \in \mathbb{Z}[G]$ satisfying

$$\begin{aligned} 0 &\leq v_i \quad \text{for all } i \\ 0 &\leq n_i \leq s v_i \quad \text{for all } i \\ DD^{-1} &= k + \lambda(sG - N) \end{aligned} \tag{1.18.1}$$

Let $D \subseteq G$ be a relative difference set with forbidden set N. As before, we identify D with the corresponding element $\widehat{D} \in \mathbb{Z}[G]$ of the group ring and omit the $\widehat{\ }$. From the defining group ring equation for relative difference sets

$$DD^{-1} = k \cdot 1 + \lambda(G - N)$$

we see that D (read as an element of the group ring) is a quotient image of a relative difference set (with $s = 1$).

Let $U \trianglelefteq G$ and $\varphi \colon G \to G/U$ be the canonical epimorphism. Use the bar convention for homomorphic images of φ. We lift φ to the group rings as before and rewrite (1.7.2) for our case:

$$(DD^{-1})^{\varphi} = k \cdot 1^{\varphi} + \lambda(\widehat{G} - \widehat{N})^{\varphi} = k \cdot 1^{\varphi} + \lambda(|U|\bar{G} - \hat{N}^{\varphi}) \tag{1.18.2}$$

Which is a quotient image in $\mathbb{Z}[G/U]$. So homomorphic images of relative difference sets do also induce quotient images of relative difference sets. Now consider the special case of $U \leq N \leq G$ and $U \trianglelefteq G$. From (1.18.2) we get

$$\begin{aligned}(DD^{-1})^{\varphi} &= k \cdot 1^{\varphi} + \lambda(|U|\bar{G} - \hat{N}^{\varphi}) = k \cdot 1^{\varphi} + \lambda(|U|\bar{G} - |U|\bar{N}) \\ &= k \cdot 1^{\varphi} + \lambda|U|(\bar{G} - \bar{N}).\end{aligned}$$

So the image of D under φ induces a quotient image of a relative difference set which is actually a relative difference set itself (in G/U and with parameters $(|G|/|N|, |N|/|U|, k, \lambda|U|)$). Remember that D contains at most one element from each coset modulo U, so $|D| = |D^{\varphi}|$.

And in particular, if $U = N \trianglelefteq G$, the quotient image is even an ordinary difference set with $\lambda' = \lambda|N|$. And hence D^{φ} is an ordinary $(v/|N|, k, \lambda|N|)$-difference set in $\bar{G} = G/N$.

When doing computer searches, this can be used to find relative difference sets in a group G with $\lambda > 1$ by searching relative difference sets with $\lambda' = 1$ in a group G' with $G \simeq G'/U'$. Here $U' \trianglelefteq G'$ and $\lambda = |G' : U'|$. This technique is used by Hiramine [Hir04] to classify the relative difference sets in Alt(5).

1.19 Theorem. *Let $G = \{g_1, \ldots, g_{|G|}\}$ be a finite group and $g_1 = 1_G$. Furthermore let $D = \sum v_i g_i = \sum v_{g_i} g_i$ be the quotient image of a relative difference set in G. Then by definition $DD^{-1} = k + \lambda(sG - N)$ with $s \in \mathbb{N}$ and $N = \sum n_i g_i \in \mathbb{Z}[G]$.*

Writing $\sum v_i = k$ and $v_{ij} = v_{g_i g_j}$ for the coefficient of $g_i g_j$, we get

$$\sum v_i^2 = \lambda(s - n_1) + k \tag{1.19.1}$$

$$\sum_j v_j v_{ij} = \lambda(s - n_i) \quad \textit{for } i \neq 1 \tag{1.19.2}$$

Proof. We have

$$\begin{aligned} DD^{-1} &= \Big(\sum_{i=1}^{|G|} v_i g_i\Big)\Big(\sum_{j=1}^{|G|} v_j g_j^{-1}\Big) = \sum_i g_i \Big(\sum_{\substack{j,k \\ g_k g_j^{-1} = g_i}} v_k v_j\Big) \\ &= \sum_{i=1}^{|G|} g_i \Big(\sum_{j=1}^{|G|} v_j v_{ij}\Big). \end{aligned} \tag{1.19.3}$$

On the other hand,

$$DD^{-1} = k + \lambda(sG - N) = k + \lambda\Big(s \sum_{i=1}^{|G|} g_i - \sum n_i g_i\Big) \tag{1.19.4}$$

Comparing (1.19.3) and (1.19.4), we get

$$\sum_j v_j v_{1j} = \sum v_j^2 = k + \lambda(s - n_1) \quad \text{and} \quad \sum_j v_j v_{ij} = \lambda(s - n_i)$$

for $i \neq 1$. □

From this we get a generalisation of a result of Bruck [Bru55] about ordinary difference sets:

1.20 Corollary. *Let G be a finite group and $U \trianglelefteq G$. Furthermore, let $D \subseteq G$ be a relative difference set with forbidden set N. We define $v_i := |D \cap g_i|$, where $\{g_1, \ldots, g_{|G:U|}\} = G/U = G^\rho$ and ρ is the natural homomorphism. Let $g_1 = U$ and $v_{ij} = |D \cap g_i g_j|$. Then*

$$\sum v_i = k \tag{1.20.1}$$

$$\sum v_i^2 = \lambda(|U| - |U \cap N|) + k \tag{1.20.2}$$

$$\sum_j v_j v_{ij} = \lambda(|U| - |g_i \cap N|) \textit{ for } i \neq 1. \tag{1.20.3}$$

If $N \leq G$*, then*

$$\sum_j v_j v_{ij} = \begin{cases} \lambda(|U| - |U \cap N|) & \textit{if } g_1 \neq g_i \in N^\rho \\ \lambda |U| & \textit{if } g_i \notin N^\rho \end{cases} \tag{1.20.4}$$

Proof. By definition, $\hat{D} = \sum_{g \in G} \chi_D(g) g$ and hence $\hat{D}^\rho = \sum v_i g_i$. We recall (1.18.2):

$$(\hat{D}\hat{D}^{-1})^\rho = k + \lambda(|U|G/U - \hat{N}^\rho).$$

Theorem 1.19 then yields (1.20.1)–(1.20.3). Moreover, $|N \cap g^\rho| = |N \cap U|$ for all $g \in G$ with $g^\rho \cap N \neq \emptyset$, because if $g^\rho = Un$ with $n \in N$, then $|Un \cap N| \geq |U \cap N| = |Unn^{-1} \cap N| \geq |Un \cap N|$. And if $g_i \neq N^\rho$, then there is no $n \in N$ such that $Un = g_i$, hence $g_i \cap N = \emptyset$. This shows (1.20.4). □

Note.

- *If we take* $N = 1$ *and* $\lambda = 1$*, we get the case of ordinary difference sets.*
- *Equation* (1.20.1) *does only depend on* $|G : U|$*.*
- *Equation* (1.20.2) *does not depend on* G*, but only on* $|U|$ *and* $|U \cap N|$*.*
- *Equation* (1.20.3) *does not depend on the isomorphism class of* G*, but only on the one of* G^ρ *and on the relation of* N^ρ *and* U^ρ*.*

Given a group G with $N \subseteq G$ and $U \leq G$ the right sides of (1.20.1)–(1.20.3) are known. So we may ask for possible solutions $(v_1, \ldots, v_{|G:U|})$. Here we choose the enumeration of the v_i to be the same as the one of G/U. So if $G/U = \{g_1, \ldots, g_{|G:U|}\}$ and $g_{ij} = g_i g_j$, we write $v_i = v_{g_i}$ and $v_{ij} = v_{g_{ij}}$. Then (1.20.1) and (1.20.2) only give information about the multiset $\|(v_1, \ldots, v_{|G:U|})\|$ while (1.20.3) is a condition on the v_i themselves (loosely speaking, a condition on the order of the entries of $(v_1, \ldots, v_{|G:U|})$).

1.21 Definition. Let $N \subseteq G$ and $U \trianglelefteq G$. Let $G/U = \{g_1, \ldots, g_{|G:U|}\}$ with $g_1 = U$ and $v = (v_{g_1}, \ldots, v_{g_{|G:U|}}) = (v_1, \ldots, v_{|G:U|})$ a solution of (1.20.1)–(1.20.3) (with $v_{ij} = v_{g_i g_j}$). Then v is called *"ordered signature"* for U (relative to N). The multiset $\|v\|$ is called *"admissible signature"* for U (relative to N).

As with (ordered) signatures of relative difference sets, we do also study (ordered) signatures of quotient images of relative difference sets. Those are the solutions of (1.19.1) and (1.19.2).

Of course, interesting quotient images are the ones which are induced by images of relative difference sets under some group-homomorphism. In this case s is the order of the kernel of the homomorphism. And N is the image of the forbidden set.

1.22 Definition. Let $S \subseteq G$. For every $U \trianglelefteq G$ let $\{g_1U, g_2U, \ldots, g_{|G:U|}U\}$ be an enumeration of cosets modulo U with $g_1 \in$U. Define the mapping

$$s_U \colon \operatorname{Pot}(G) \to \mathbb{N}^{|G:U|} \qquad\qquad s_U(S)(i) = |S \cap g_iU|$$

And $\sigma_U = \|s_U\|$.

For every relative difference set D and every $U \trianglelefteq G$, the tuple $s_U(D)$ is an ordered signature and the multiset $\sigma_U(D)$ is an admissible signature. If we search for relative difference sets, this yields a necessary condition for the extendability of partial relative difference sets:

1.23 Corollary. *Let $S \subseteq G$ be a partial relative difference set. If S can be extended to a relative difference set (see page 10), then for every $U \trianglelefteq G$, we have that $\sigma_U(S)$ is pointwise less or equal to at least one admissible signature for U. Moreover, S can only be extended, if $s_U(S)$ is pointwise less or equal to at least one ordered signature.*

The signature maps can also be used to test for equivalence of partial relative difference sets:

1.24 Lemma. *Let $S \subseteq G$ be a partial relative difference set with forbidden set $N \subseteq G$. Let $\mathcal{N} \subseteq \{n \in \mathbb{N} \mid n \mid |G|\}$ and $\mathcal{U} = \{U \trianglelefteq G \mid |G : U| \in \mathcal{N}\}$. Then for all $g \in G$ and all $\varphi \in \operatorname{Aut}^\circ(G)_N$ we have*

$$\|\big(\sigma_U(S)\big)_{U\in\mathcal{U}}\| = \|\big(\sigma_U((Sg)^\varphi)\big)_{U\in\mathcal{U}}\|.$$

Note. *Lemma 1.24 does only state an equation for multisets, one cannot hope for $\sigma_U(S) = \sigma_U((Sg)^\varphi)$.*

1.5 Central collineations of projective planes

Let $\mathfrak{P}$ be a projective plane and α a collineation of $\mathfrak{P}$. Recall that if α fixes a point $p \in \mathfrak{P}$ line-wise, then p is called "centre" of α. And if α fixes a line L pointwise, L is called "axis" of α.

The collineation α is called “axial”, if it has an axis. It is called “central” if it has a centre. The following results are well known and can be found in [Dem68, HP73].

1.25 Theorem. *Let $\mathfrak{P}$ be a projective plane and α a collineation of $\mathfrak{P}$. Then α possesses a centre if and only if it has an axis.*

If α is a central collineation with axis L and centre p, then α is called “(p, L)-elation” if $p \in L$ and “(p, L)-homology” if $p \notin L$.

1.26 Lemma. *Let α be a non-trivial central collineation with axis L and centre p, then α does not fix any point outside $L \cup \{p\}$. And α does not fix any line other than the lines $[p]$.*

In particular, a central collineation is completely determined by the image of one moved point (one moved line). And if a central collineation fixes any point outside $L \cup \{p\}$ or any line other than $[p] \cup \{L\}$, it is the identity.

For a given point- line pair (p, L), the central collineations with centre p and axis L form a group. The elations with given axis or given centre do also form a group. And if α is a central collineation with centre p and axis L and γ is any collineation, then α^γ is a central collineation with centre p^γ and axis L^γ.

1.27 Theorem ([HP73, Thm. 4.14])**.** *Let $\mathfrak{P}$ be a finite projective plane of order n and L a line of $\mathfrak{P}$. Let N be a group of (x, L)–elations. Let α be an elation with axis L and centre $y \neq x$. Then the group $\langle N, \alpha\rangle$ is an elementary abelian p-group and $p \mid n$.*

1.28 Definition. Let $\mathfrak{P}$ be a projective plane of order n. A line L of $\mathfrak{P}$ is called *translation line*, if the group of elations with axis L is transitive on the points $\mathfrak{P} - L$.

The projective plane is called *translation plane* if it has a translation line. The group of elations which have the translation line as its axis is called *translation group* of $\mathfrak{P}$.

The definition of dual translation planes, translation points (dual translation lines) and dual translation groups is obvious.

1.29 Lemma. *Let $\mathfrak{P}$ be a projective plane and L a line of $\mathfrak{P}$ with $p, q \in L$. Let then $L \neq M \ni p$ be another line. If α is a (q, M)-homology and β is a (p, L)-elation then $\alpha\beta = \beta\alpha$*

Proof. α^β is a homology with centre q and axis M as β fixes L pointwise and p line-wise. Now observe that for a point $x \in L$ with $x \notin \{p, q\}$ we have $x^{\beta^{-1}\alpha\beta} = x^\alpha$ as β fixes x and x^α. Hence $\alpha\beta = \beta\alpha$. □

1.30 Lemma. *Let $\mathfrak{P}$ be a projective plane and L, M two distinct lines of $\mathfrak{P}$. Let $p \in L - M$ and $q \in M - L$. If α is a (p, M)-homology and β is a (q, L)-homology, then $\alpha\beta = \beta\alpha$.*

Proof. Obviously, α^β is a (p, M)-homology. Let $x \in L$ and $x \neq p$. As β fixes L pointwise, we have $x^{\alpha^\beta} = x^{\beta^{-1}\alpha\beta} = x^\alpha$. □

Chapter 2

Representation theoretic methods

Let φ be a representation of the group G with $|\ker\varphi| = s$. We lift φ to the group ring as in (1.7.1)

$$\left(\sum v_g g\right)^{\varphi} := \sum v_g g^{\varphi}. \tag{2.0.1}$$

The defining equation for ordinary difference sets then transforms to

$$(DD^{-1})^{\varphi} = n \cdot 1^{\varphi} + \lambda \hat{G}^{\varphi} = n \cdot 1^{\varphi} + \lambda s \widehat{\operatorname{Im}\varphi} \tag{2.0.2}$$

Here $\operatorname{Im}\varphi$ is the image of φ as a homomorphism of groups. If $1 \neq \varphi$ is an irreducible representation, we have $\hat{G}^{\varphi} = 0$. Hence $(DD^{-1})^{\varphi} = n$.

For relative difference sets with forbidden set N we get

$$(DD^{-1})^{\varphi} = k \cdot 1^{\varphi} + \lambda(\widehat{G-N})^{\varphi} = k \cdot 1^{\varphi} + \lambda(s\widehat{\operatorname{Im}\varphi} - \hat{N}^{\varphi}) \tag{2.0.3}$$

and for a non-trivial and irreducible φ we have $(DD^{-1})^{\varphi} = k - \lambda\hat{N}^{\varphi}$.

Now let $U \trianglelefteq G$ and $\rho\colon G \to G/U$ be the canonical epimorphism. Let $\{g_1, \dots, g_{|G:U|}\}$ be a system of representatives of G/U (sometimes called cross-section) and D an ordinary difference set in G. Consider the mapping $s_U\colon \operatorname{Pot}(G) \to \mathbb{N}^{|G:U|}$ from definition 1.22. It maps $D \in \mathbb{Z}[G]$ onto the tuple of coefficients $(v_1, \dots, v_{|G:U|})$ of $\hat{D}^{\rho} = \sum v_i g_i^{\rho}$.

2.1 Corollary. *Let $(w_1, \dots, w_{|G:U|})$ be an ordered signature for U. If for one $D \in \mathbb{Z}[G]$ we have $s_U(D) = (w_1, \dots, w_{|G:U|})$, then for every irreducible,* *non-trivial representation φ of G/U*

$$\left(\sum_{i=1}^{|G:U|} w_i g_i^{\rho}\right)^{\varphi} \left(\sum_{i=1}^{|G:U|} w_i g_i^{-\rho}\right)^{\varphi} = n \tag{2.1.1}$$

In fact, the quotient images of difference sets can also be described using representation theory:

2.2 Theorem ([Bec04]). *Let H be a finite group and $\delta = \sum d_h h \in \mathbb{Z}[H]$ with $|\delta| = k$ and $d_h \geq 0$. Furthermore, let $|H| \bigm| v \in \mathbb{N}$ and $n + \lambda v = k^2$. δ is a quotient image of an ordinary difference set if and only if for every non-trivial irreducible representation φ of H the equation $\delta^{\varphi}(\delta^{-1})^{\varphi} = n1^{\varphi}$ holds.*

2.0.1 Induced signatures

Let G be a finite group, $U \trianglelefteq G$ and let $\varphi \colon G \to G/U$ be the canonical homomorphism. Furthermore let let $\{g_1, \dots, g_m\}$ be a cross-section of G/U and $D = \sum_{i=1}^{m} v_i g_i \in \mathbb{Z}[G]$ a relative difference set in G. Then $D^{\varphi} = \sum_{i=1}^{m} w_i g_i U \in \mathbb{Z}[G/U]$ is a quotient image of a relative difference set in G/U. And we have $\sum_{g \in g_i U} v_g = |(\widehat{g_i U \cap D})^{\varphi}| = w_{g_i^{\varphi}}$.

Choosing a suitable enumeration, we get

$$\overbrace{v_1, \dots, v_{|U|}}^{\sum v_i = w_1}, \dots, \overbrace{v_{|G|-|U|+1}, \dots, v_{|G|}}^{\sum v_i = w_{|G:U|}}$$

So, if we know the ordered signature of a quotient image, we may use this information to calculate ordered signatures of the pre-images. This will be applied in the following setting:

Let G be a finite group and $U, V \trianglelefteq G$ with $U \trianglelefteq V$. Let $\varphi \colon G \to G/U$ and $\psi \colon G \to G/V$ be the canonical epimorphisms. Then $V^{\varphi} \trianglelefteq G/U$ and

$$G/V \simeq (G/U)\big/(V/U).$$

Hence $\left\{g^{\psi^{-1}\varphi} \mid g \in G/V\right\}$ is a partition of G/U. This is the partition into cosets modulo V/U.

Let $D \subseteq G$ be a relative difference set and $\{g_1, \dots, g_{|G:V|}\}$ a system of representatives of G/V, then $s_V(D)(i) = \sum_{g \in (g_i V)^{\psi^{-1}\varphi}} |D \cap g|$. In this way, we get a refinement of signatures (going from signatures for V to signatures for $U \trianglelefteq V$).

2.1 Difference sets in extensions of $\mathrm{C}_s \ltimes \mathrm{C}_q$

For some groups, it is easy to find representations which are useful for searching difference sets. We will now study the case of extensions of $\mathrm{C}_s \ltimes \mathrm{C}_q$. These groups have an unitary representation which is convenient for searching difference sets with the aid of a computer.

Let G be a finite group and $U \trianglelefteq G$ with $G/U \simeq \mathrm{C}_s \ltimes \mathrm{C}_q$We write $G/U = \langle a, b\rangle$ with $|a| = q,\ |b| = s$ and $a^b = a^m$ for some $m \in \mathbb{N}$ and $m^s \equiv 1 \mod q$. Furthermore let ζ be a primitive q^{th} root of unity. We define an s-dimensional unitary representation Φ of G/U by

$$a^\Phi = \operatorname{diag}(\zeta, \zeta^m, \zeta^{m^2}, \dots, \zeta^{m^{s-1}}), \quad b^\Phi = \pi = \begin{pmatrix} 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 1 & 0 \end{pmatrix}; \tag{2.2.1}$$

here multiplying π from the right side permutes columns as $(1, 2, \dots, s)$.

Let now $D \subseteq G$ be an ordinary difference set of order n (i.e. $N = 1$ and $\lambda = 1$). For $0 \le i < q$ and $0 \le j < s$ we define $v_{ij} = |D \cap a^{i-1}b^{j-1}|$. Let $\tilde{D}$ be the image of $D \in \mathbb{Z}[G]$ under the canonical epimorphism lifted onto the group rings. Then we have

$$(\tilde{D}^\Phi)_{\mu\nu} = \sum_i v_{i(\mu-\nu+1)} \zeta^{im^{\mu-1}}. \tag{2.2.2}$$

With $\vartheta = \pi^{-1}$ and $\operatorname{Gal}_{\mathbb{Q}}(\mathbb{C}) \ni \alpha \colon \zeta \mapsto \zeta^m$ we get
(2.2.3)

$$\tilde{D}^\Phi = \begin{pmatrix} M_1 & \dots & M_s \\ M_{1\vartheta}^\alpha & \dots & M_{s\vartheta}^\alpha \\ \vdots & \ddots & \vdots \\ M_{1\vartheta^{s-1}}^{\alpha^{s-1}} & \dots & M_{s\vartheta^{s-1}}^{\alpha^{s-1}} \end{pmatrix} = \begin{pmatrix} M_1 & M_2 & \dots & M_s \\ M_s^\alpha & M_1^\alpha & \dots & M_{s-1}^\alpha \\ \vdots & \vdots & \ddots & \vdots \\ M_2^{\alpha^{s-1}} & M_3^{\alpha^{s-1}} & \dots & M_1^{\alpha^{s-1}} \end{pmatrix} = M$$

Hence we get the equations

$$M\bar{M}^t = (\tilde{D}\tilde{D}^{-1})^\Phi = k\,\mathbb{1} + \lambda(G-N)^\Phi = n\,\mathbb{1}$$

$$\sum_{i=1}^{s} M_i \bar{M}_i = n$$

$$\sum_{i=1}^{s} M_i \bar{M}_{i\vartheta^j}^{\alpha^j} = 0 \quad \text{for all } 1 \le j < s.$$

2.3 Definition. Let $M_1, \ldots, M_s \in \mathbb{Q}[\zeta]$ with primitive q^{th} root of unity ζ and $\alpha \in \mathrm{Gal}(\mathbb{Q}[\zeta])$ with $|\alpha| = s$ and $\alpha\colon \zeta \mapsto \zeta^m$. Let $\vartheta \in \mathrm{Sym}(s)$ be a cycle of order s. Then the matrix

$$M(M_1, \ldots, M_s, \alpha, \vartheta) = \begin{pmatrix} M_1 & \ldots & M_s \\ M_{1\vartheta}^{\alpha} & \ldots & M_{s\vartheta}^{\alpha} \\ \vdots & \ddots & \vdots \\ M_{1\vartheta^{s-1}}^{\alpha^{s-1}} & \ldots & M_{s\vartheta^{s-1}}^{\alpha^{s-1}} \end{pmatrix}$$

is called *semi-circulant*.

2.4 Theorem. *Let $M = M(M_1, \ldots, M_s, \alpha, \vartheta)$ be a semi-circulant matrix. Then:*

$$(M\bar{M}^t)_{ij} = \left((M\bar{M}^t)_{1(j-i+1)}\right)^{\alpha^{i-1}} \quad \textit{for } i \le j \tag{2.4.1}$$

$$(M\bar{M}^t)_{ii} = \left((M\bar{M}^t)_{11}^{t}\right)^{\alpha^{i-1}} \tag{2.4.2}$$

$$(M\bar{M}^t)^t = \overline{M\bar{M}^t} \tag{2.4.3}$$

Proof. For the sake of simplicity we write $^{-} = \gamma$ for complex conjugation. Then

$$\begin{aligned} (M\bar{M}^t)_{(i+1)(j+1)} &= \sum_k M_{k\vartheta^i}^{\alpha^i} \bar{M}_{k\vartheta^j}^{\alpha^j} \\ &= \sum_k \left(M_{k\vartheta^i} M_{k\vartheta^j}^{\gamma\alpha^{j-i}}\right)^{\alpha^i} = \sum_k \left(M_k M_{k\vartheta^{j-i}}^{\gamma\alpha^{j-i}}\right)^{\alpha^i} \\ &= (M\bar{M}^t)_{1(j-i+1)}^{\alpha^i} \end{aligned}$$

shifting indices we get (2.4.1). A special case of this is (2.4.2). Statement (2.4.3) does not even depend on the form of M:

$$(M\bar{M}^t)^t = \bar{M}M^t = \overline{M\bar{M}^t}$$

□

The semi-circulant matrices with fixed ϑ and α form a $\mathbb{Q}$-algebra. For $\alpha = 1$ we obtain the $\mathbb{Q}[\zeta]$-algebra of circulant matrices.

2.1.1 Calculation of ordered signatures

If we want to calculate all ordered signatures for $U \trianglelefteq G$, we first have to calculate all possible entries $M_1, \dots, M_s$ of $\tilde{D}^\Phi$ where $D \subseteq G$ is a difference set. Thereafter, the preimage of Φ can be computed.
So we are looking for the semi-circulant matrices M satisfying $M\bar{M}^t = n\,\mathbb{1}$. And $M = M(M_1, \dots, M_s, \alpha, \vartheta)$ where $M_i \in \mathbb{Z}[\zeta]$ for all i and all coefficients of M_i are non-negative, as the multiset of coefficients of M_i is an admissible signature.

For the rest of this section let $D \subseteq G$ be an ordinary difference set with $U \trianglelefteq G$ and $G/U = \langle b, a\rangle \simeq \mathrm{C}_s \ltimes \mathrm{C}_q$. Furthermore, let $\varphi \colon G \to G/U$ be the natural epimorphism, $\tilde{D} = \hat{D}^\varphi$ and let the representation Φ be defined as in 2.1.

Lemma. *If $\tilde{D}^\Phi = M(M_1, \dots, M_s, \alpha, \vartheta)$, the sum of the coefficients of M_i is $|\{d \in D \mid d^\varphi \in b^{-i+1}\}|$.*

Proof. This is just another way to write (2.2.2). □

Here we have to be careful, as the presentation of $\mathbb{Z}[\zeta] \ni z = \sum a_i\zeta^i$ is not unique. For example $\sum_{i=0}^{q-1} \zeta^i = 0$.

The right formulation is:

2.5 Lemma. *Let $\tilde{D}^\Phi = M(M_1, \dots, M_s, \alpha, \vartheta)$. Then there is a presentation of the $M_i \in \mathbb{Z}[\zeta]$ as $M_i = \sum a_i\zeta^i$, such that the coefficients of every M_i are non- negative and their sum is $|\{d \in D \mid d^\varphi \in b^{-i+1}\}|$.*

As already mentioned, the set of coefficients of the M_i is an admissible signature for U. Because of lemma 2.5 the sums of the coefficients of the M_i are an admissible signature for $\langle a\rangle$ and as in 2.0.1 we can use the signatures for $\langle a\rangle \trianglelefteq (G^\varphi)^\Phi$ to calculate the coefficients of the M_i.

2.6 Lemma. *Let $U' \trianglelefteq G$ with $|G : U'| = s$ and $U'^\varphi = \langle a\rangle$. If there is exactly one admissible signature $\|(s_1, \dots, s_s)\|$ (read as an s-tuple as on page 6) for U', then there is a permutation η, such that $(s_{1\eta}, \dots, s_{s\eta}) = (S_{M_1}, \dots, S_{M_s})$ holds. Here S_{M_i} is the sum of the coefficients of M_i.*

Proof. Let $\{g_1, \dots, g_s\}$ be a cross-section of G/U'. Then $\{g_1, \dots, g_s\}^\varphi$ is a cross-section of $(G/U)/\langle a\rangle$ because $U'^\varphi = \langle a\rangle$. As $\|(s_1, \dots, s_s)\|$ is an admissible signature and $\{g_1, \dots, g_s\}^\varphi$ is a system of representatives, we get

$$\|(s_1, \dots, s_s)\| = \|(|D \cap g_1U'|, \dots, |D \cap g_sU'|)\| = \|(S_{M_1}, \dots, S_{M_s})\|$$

So there is a permutation η as desired. □

Lemma 2.6 and 2.5 enables us to refine known signatures: The signature $\|(s_1,\dots,s_s)\|$ induces a set of signatures $\|(a^{(\ell)}_{1,1},\dots,a^{(\ell)}_{1,q},a^{(\ell)}_{2,1},\dots,a^{(\ell)}_{s,q})\|_{\ell\in\mathfrak{I}}$ with $\sum_j a^{(\ell)}_{i,j}\zeta^{j-1} = M_i$ for all ℓ in some index set $\mathfrak{I}$.

Note. (a) *Using Φ, we do not only get admissible, but even ordered signatures for U from the coefficients of the M_i.*

(b) *If s is a prime power and $U' \trianglelefteq G$ is an s'-Hall group, then $U'^{\varphi} \trianglelefteq G^{\varphi}$ is the unique Hall group of the solvable group G^{φ} and therefore $U'^{\varphi} = \langle a\rangle$. So if there is a unique signature for U, we may use 2.6*

To lower the cost for calculating the M_i, the following symmetry argument can be used.

2.7 Theorem. *Let $n \in \mathbb{N}$ and $M = M(M_1,\dots,M_s,\alpha,\vartheta)$ be a semi-circulant matrix with $M\bar{M}^t = n\,\mathbb{1}$. Then also $M' = M(M_1\zeta^{a_1},\dots,M_s\zeta^{a_s},\alpha,\vartheta)$ is semi-circulant and $M'\bar{M}'^t = n\,\mathbb{1}$ with*

$$a_1 := 0; \qquad a_{i\vartheta^{(j+1)}} \equiv m(a_{i\vartheta^j} + c) \mod |\zeta|. \tag{2.7.1}$$

Here $\alpha\colon \zeta \mapsto \zeta^m$ as in definition 2.3 and $1 \le c \le |\zeta| - 1$ may be chosen arbitrarily.

Proof. M' is semi-circulant by definition. So we only have to verify $M'\bar{M}'^t = n\,\mathbb{1}$. According to (2.4.1) we only have to care for the entries of the first row of $M'\bar{M}'^t$. Obviously, $(M'\bar{M}'^t)_{11} = n$. So let's look at $l \neq 1$:

$$\begin{aligned}(M'\bar{M}'^t)_{1l} &= \sum_i M_i\zeta^{a_i}\bar{M}^{\alpha^{l-1}}_{i\vartheta^{l-1}}\zeta^{-a_{i\vartheta^{l-1}}m^{l-1}} = \sum_i M_i\bar{M}^{\alpha^{l-1}}_{i\vartheta^{l-1}}\zeta^{a_i - a_{i\vartheta^{l-1}}m^{l-1}}\\ &\overset{(2.7.1)}{=} \sum_i M_i\bar{M}^{\alpha^{l-1}}_{i\vartheta^{l-1}}\zeta^{(a_{i\vartheta^{l-1}} - a_{i\vartheta^{l-1}})m^{l-1} + c_l} = (M\bar{M}^t)_{1l}\zeta^{c_l}\end{aligned}$$

with $c_l = \sum_{j=1}^{l-1} cm^j$. Because of $M\bar{M}^t = n\,\mathbb{1}$ the theorem is proven. □

Note. (a) *From 2.7 we get a group μ acting on the tuples $(M_1,\dots,M_s)$. So instead of testing all tuples, we may then choose one representative $M = M(M_1,\dots,M_s,\alpha,\vartheta)$ from every orbit of μ and test, if it satisfies $M\bar{M}^t = n\,\mathbb{1}$.*

(b) *As seen in the proof of 2.7, it is not necessary to have $a_1 = 0$. Any other value may be used. But $a_1 = 0$ was chosen for computational reasons.*

Chapter 3

Quasiregular relative difference sets

We will now turn to the main objective of this text. First, we give a definition of quasiregular planes and state the theorem of Dembowski and Piper. Every instance of the theorem is dealt with in a separate section. We give difference set constructions of the respective planes and discuss special problems of the classification. At the end of each section, a classification theorem for order 16 planes of the respective type is stated. We conclude this Chapter with a theorem combining all the partial classifications of this chapter to get a full classification of the quasiregular projective planes of order 16.

3.1 Definition. Let $\mathfrak{P}$ be a projective plane of order n. Let G be a group of collineations of $\mathfrak{P}$. The group G is called *quasiregular* if it acts regularly on its point and block orbits.

So a quasiregular action means that for every point (every block) the stabiliser of this point (block) is a normal subgroup in G.

In other words: If $p^g = p$ for some point (block) p and $g \in G$, then $q^g = q$ for all $q \in p^G$.

3.2 Definition. A quasiregular group G of collineations of the projective plane $\mathfrak{P}$ of order n is called *large*, if

$$|G| > \frac{1}{2}(n^2 + n + 1). \tag{3.2.1}$$

By [Dem68, 4.2.8, p.181], a group of collineations of a projective plane acts faithfully on at least one orbit. We may assume that this is an orbit of points. So a large quasiregular group of collineations has exactly one orbit of size $|G|$ on points.

3.3 Theorem (Dembowski-Piper, [DP67], [Dem68, 4.2.10, p.182])**.** *Let G be a quasiregular collineation group of the projective plane $\mathfrak{P}$ of order n. Denote by $m = m(G)$ the number of point (or line) orbits of G, and by $\mathbf{F} = \mathbf{F}(G)$ the substructure of the elements fixed by G. If $|G| > \frac{1}{2}(n^2+n+1)$, then there are only the following possibilities:*

$\mathbf{DP}_a$ *$|G| = n^2 + n + 1$, $m = 1$ and $\mathbf{F} = \emptyset$. Here G is transitive.*

$\mathbf{DP}_b$ *$|G| = n^2$, $m = 3$ and $\mathbf{F}$ is a flag.*

$\mathbf{DP}_c$ *$|G| = n^2$, $m = n + 2$ and $\mathbf{F}$ is either a unique line A and all $x \in A$ or dually a unique point c and all lines $X \in [c]$.*

$\mathbf{DP}_d$ *$|G| = n^2 - 1$, $m = 3$ and $\mathbf{F}$ is a unique non-incident point-line pair.*

$\mathbf{DP}_e$ *$|G| = n^2 - \sqrt{n}$, $m = 2$ and $\mathbf{F} = \emptyset$. In this case, one point and one line orbit together form a Baer subplane.*

$\mathbf{DP}_f$ *$|G| = n(n - 1)$, $m = 5$ and $\mathbf{F}$ consists of two points u, v, the line containing u and v and one other line through one of u, v.*

$\mathbf{DP}_g$ *$|G| = (n - 1)^2$, $m = 7$ and $\mathbf{F}$ consists of the vertices and sides of a triangle.*

Examples are known for all of these cases (for $\mathbf{DP}_e$ only one example is known. In this example, $n = 4$).

In [Dem68, 4.2.10] another case is mentioned. In this case G is elementary abelian and $|G| = (n - \sqrt{n} + 1)^2$. But Ganley and McFarland have shown in [GM75] that a projective plane with a quasiregular group of collineations of order $(n - \sqrt{n} + 1)^2$ exists if and only if $n = 4$. And as $|G| = (4 - 2 + 1)^2 = 9 \not> \frac{1}{2}(16 + 4 + 1) = \frac{21}{2}$ this case is not part of theorem 3.3.

Let $\mathfrak{P}$ be a quasiregular projective plane and G a large quasiregular group of collineations of $\mathfrak{P}$. Define $\mathfrak{P}'$ to be the incidence structure defined by the point orbit of length $|G|$. We will find difference sets $D \subseteq G$ such that $\operatorname{dev} D \simeq \mathfrak{P}'$ and then recover $\mathfrak{P}$ from $\mathfrak{P}'$. Fortunately the extension of $\mathfrak{P}'$ is unique in all cases, so we can really recover $\mathfrak{P}$ from the relative difference set defining $\mathfrak{P}'$.

Now we will run through the types of planes of theorem 3.3 and give difference set constructions for each of them. Some of the arguments used can also be found in [GJ03a, GJ03b, Pot95]. The focus will be on the case of projective planes of order 16.

3.1 Ordinary difference sets: $\mathbf{DP}_a$

Let $|G| = n^2 + n + 1$, $m = 1$ and $\mathbf{F} = \emptyset$. Here $\mathfrak{P} = \mathfrak{P}'$ and we have to consider ordinary $(|G|, n+1, 1)$-difference sets (i.e. $N = \{1\}$).

For $n = 16$, we have $|G| = 273 = 3 \cdot 7 \cdot 13$. The theorems of Sylow show that the subgroups of the orders 7 and 13 are normal in G. So there is a unique normal subgroup of order $7 \cdot 13 = 91$. Hence for all groups G of order 273 we have $\mathrm{C}_{91} \trianglelefteq G$. An easy calculation shows that the only solution for (1.20.1) and (1.20.2) with $V = \mathrm{C}_{91}$, $N = 1$, $k = 17$ and $\lambda = 1$ is the multiset $\|(v_1, v_2, v_3)\| = \|(3, 7, 7)\|$. And we may assume that $v_3 = 3$ by choosing a suitable translate.

As some of the groups in this case are extensions of $\mathrm{C}_3 \ltimes \mathrm{C}_7$ or $\mathrm{C}_3 \ltimes \mathrm{C}_{13}$, we may use the results of section 2.1 to calculate ordered signatures.

The following steps are used to find all difference sets of this type (up to equivalence). For a more detailed description of the algorithms see chapter 4.

(a) Calculate possible ordered signatures.

(b) Calculate possible admissible (unordered) signatures.

(c) Generate partial difference sets containing 7 elements of $V \trianglelefteq G$, $V \simeq \mathrm{C}_{91}$. This step uses costly algorithms to test equivalence of partial difference sets (algorithm 6 of page 43).

(d) Extend partial difference sets to 14 elements by adding 7 elements of the first non-trivial coset modulo V. Here we only check that the list of quotients is duplicate-free.

(e) Reduce the partial difference sets using algorithm 9 of page 46.

(f) Add 3 more elements from the last coset modulo V and reduce as above.

(g) Generate projective planes from difference sets and determine the isomorphism class using algorithm 11 of page 48.

From a computer search, we get

3.4 Theorem. *Let G be a group of order 273 and $D \subseteq G$ a difference set of type $\mathbf{DP}_a$. Then D induces a Desarguesian plane and G is cyclic or* $G \simeq \mathrm{C}_3 \ltimes \mathrm{C}_{91} = \left\langle a, b \;\middle|\; |a| = 3,\ |b| = 91,\ b^a = b^{16} \right\rangle$.

Note that Kibler [Kib78] claims that there are two noncyclic relative $(273, 17, 1)$-difference sets. But a quick calculation using `GAP` shows that the group in case 13 of [Kib78] is cyclic of order 21 (and the set given is not a difference set, as it has 11 elements in C_{21}).

3.2 The case $\mathbf{DP}_b$

Here $|G| = n^2$ and $m = 3$ and $\mathbf{F}$ is a flag (a, M). In this case, $\mathfrak{P}'$ is a divisible design with Singer group G. By 1.15, we may represent $\mathfrak{P}'$ by an $(n, n, n, 1)$–difference set D with forbidden subgroup $N \leq G$ of order n. So $\mathfrak{P}' = \operatorname{dev} D$.

As seen in section 1.3, the forbidden subgroup N can be identified with the point class containing 1. The other point classes of $\mathfrak{P}'$ are exactly the cosets of N. For any block Dg with $g \in G$, the parallel class containing Dg is $\{ Dgn \mid n \in N \}$.

Each point class defines an ideal line. And a can be identified with the ideal point on all point classes of $\mathfrak{P}'$ (all cosets of N). Dually, the parallel classes of $\mathfrak{P}'$ (the translates of "ordinary", i.e. non-ideal, lines by an element of N) define ideal points and $M - \{a\}$ may be identified with the set of parallel classes of $\mathfrak{P}'$. In this way, $\mathfrak{P}$ can be reconstructed from $\mathfrak{P}'$. As M is a line of ideal points, we will write $M = \ell_\infty$.

The lines $[a] - \{\ell_\infty\}$ (that is, the point classes of $\mathfrak{P}'$) are an orbit of G and as G acts quasiregular on the lines of $\mathfrak{P}$, all lines meeting a are stabilised by N. Hence $N \trianglelefteq G$ and as N also stabilises all parallel classes of $\mathfrak{P}'$, we have that N is a group of elations of $\mathfrak{P}$.

3.5 Lemma. *Let $D \subseteq G$ be a relative difference set of type $\mathbf{DP}_b$ with forbidden group $N \trianglelefteq G$. Then one of the following holds:*

- *N is the full group of elations with axis ℓ_∞.*
- *N is elementary abelian.*

Proof. By 1.27, a group of elations with axis ℓ_∞ is elementary abelian if it contains two elations with different centres. □

For planes of even order, there is a restriction on possible forbidden groups:

3.6 Lemma. *Let $D \subseteq G$ be a relative difference set of order $n \equiv 0 \mod 2$ relative to the forbidden subgroup $N \trianglelefteq G$. Let $\iota \in G$ be an involution. Then $\iota \in N$.*

Proof. Let $\mathfrak{P}$ be the projective plane defined by D and $\iota \in G$ be an involution. Then ι acts either as a Baer involution or as an elation on $\mathfrak{P}$ as n is even (see [Dem68, 4.1.9]).

Assume that ι is an elation with axis $L \neq \ell_\infty$. Then ι fixes a point outside ℓ_∞ and as G acts regularly, ι fixes all affine points. So ι has axis ℓ_∞. Let $L \neq \ell_\infty$ be a line fixed by ι. Then L must be an ideal line, as G acts regularly on the other lines. So ι fixes all cosets of N and therefore $\iota \in N$.

If ι fixes a Baer subplane, then ι fixes a point outside ℓ_∞. But as G acts regularly on the affine points, this is a contradiction □

And for abelian groups, we even have:

3.7 Theorem ([Gan76, Jun87])**.** *Let G be an abelian group or order n^2 with even n and $D \subseteq G$ a relative difference set of type $\mathbf{DP}_b$. Then n is a power of 2, the forbidden subgroup is elementary abelian and $G \simeq \mathrm{C}_4 \times \cdots \times \mathrm{C}_4$.*

3.8 Theorem. *Let G be a group of order 256 and $D \subseteq G$ a relative difference set of type $\mathbf{DP}_b$. Then the projective plane defined by D is one of the following:*

- *The Desarguesian plane.*
- *The semifield plane with kernel* GF(2)*.*
- *The semifield plane with kernel* GF(4)*.*
- *The Mathon Plane.*
- *The dual Mathon Plane.*

See appendix A for the full list of groups of order 16^2 which admit a relative difference set of type $\mathbf{DP}_b$.

3.2.1 A word about implementation

Let $D \subseteq G$ be a relative difference set of type $\mathbf{DP}_b$ and $N \trianglelefteq G$ the forbidden subgroup. Then D is a system of representatives of the cosets modulo N by 1.12 as $|G : N| = |D|$.

This fact is used to implement a special case of startset generation (algorithm 1). If a startset has a nonempty intersection with one of the cosets modulo N, this coset is removed from the list of possible completions. In fact, this is nothing but testing a particular coset signature (the one for N). One advantage of this is, that startsets are generated *after* doing this test, whereas in the other cases, the startsets are first generated and then tested. This reduces the number of signature tests as well as the list operations needed to generate and discard startsets. A further improvement comes from adding only elements from *one* coset modulo some other normal subgroup $V \trianglelefteq G$ to existing startsets to generate new ones. This helps keeping the number of startsets small. The group $V \trianglelefteq G$ will be chosen as in the other cases (see 4.2).

For the special case of $n = 16$, lemma 3.6 can be used. So any group G which has no normal subgroup N of order 16 such that all involutions of G lie in N can be discarded right away.

Algorithm 1 New startsets for case $\mathbf{DP}_b$

```
procedure NewStartsets(S,N,u,a)
# $S$: list of startsets; $N$: forbidden group; $u \in G/V$; $a \in \mathbb{N}$: number of elements from
$u$ in a full relative difference set
    $C := \{n \cap u \mid n \in G/N\}$
    $R := \emptyset$
    for $s \in S$ do
        $l := \left\{c \in \bigcup_{X \in C} X \;\middle|\; s \cup \{c\} \text{ is a partial relative difference set}\right\}$
        $C' := \{c \cap l \mid c \in C\}$
        if $l \neq \emptyset$ and $|C'| + |s| = a$ then
            let $\emptyset \neq c' \in C'$ be of minimal size
            add the sets $\{s \cup \{c\} \mid c \in c'\}$ to $R$
        end if
    end for
    return $R$
end procedure
```

Another problem in this case is to recognise projective planes. This test is done in the following way:

(a) Calculate the Fano invariant as in algorithm 11.

(b) If the Fano invariant matches the one of a translation plane, calculate the translation group of $\mathfrak{P}$ (that is, the group of all elations with axis M). If this group is transitive on the affine points, $\mathfrak{P}$ is a translation plane. And as all translation planes of order 16 are known [DR83, Rei84] and have pairwise different Fano invariants [Roy], we know the isomorphism type of $\mathfrak{P}$.

(c) If the Fano invariant is the one of the Mathon plane, construct an isomorphism by mapping a generating quadrangle of $\mathfrak{P}$ onto a generating quadrangle of the Mathon plane.

(d) To test for the dual Mathon plane, we calculate the dual plane of $\mathfrak{P}$ and test as in point (c) above.

The needed data (Fano invariant and the Mathon plane) for this calculation is available from Gordon Royle [Roy].

3.3 Case DP$_c$, translation planes

Here $|G| = n^2$ and $m = n + 2$. The fixed structure $\mathbf{F}$ is a line and all its points or a point and the according lines.

Consider the case that G fixes a line B pointwise. Then G is a group of central collineations with axis B. As G acts quasiregular, there is a point-orbit of length n^2 and hence, G acts transitively on the points outside B. So G is a group of translations and $\mathfrak{P}$ is a translation plane. Dually, if G fixes a point and its lines, $\mathfrak{P}$ is a dual translation plane.

As G is the translation group of a translation plane, G is elementary abelian by 1.27 (for more on translation planes, see [Lün80]).

The translation planes of order 16 have been classified by U. Dempwolff and A. Reifart [DR83, Rei84]. So this case will not be considered further.

3.4 $\mathbf{DP}_d$: Affine difference sets

Let $|G| = n^2 - 1$ and $m = 3$ with $\mathbf{F}$ an anti-flag (a, M).

Here there are $n^2 - 1$ points different from a, which do not lie on M. A point class is defined by the points on a line through a. In the same way the lines are partitioned into classes: every point on M defines a class of lines containing it.

The following argument reconstructs $\mathfrak{P}$ from $\mathfrak{P}'$ in this case:
First, define a as a new point and add a to each of the point classes of $\mathfrak{P}'$. Then each of these extended point classes is defined to be a new line. This extension of $\mathfrak{P}'$ is an affine plane which defines $\mathfrak{P}$.

So $\mathfrak{P}'$ is a divisible design with point classes defined by the lines (of $\mathfrak{P}$) containing a. By 1.15, we may describe $\mathfrak{P}'$ by a $(n+1, n-1, n, 1)$-difference set D with forbidden subgroup N. Again, $N \trianglelefteq G$ because G acts quasiregularly.

For $n = 16$ we have $|G| = 16^2 - 1 = 255 = 3 \cdot 5 \cdot 17$ and the theorems of Sylow imply $G = \mathrm{C}_{255}$.

The program listed in appendix B.1 finds

3.9 Theorem. *The only projective plane which admits* C_{255} *as a collineation group of type* $\mathbf{DP}_d$ *is the Desarguesian plane.*

3.5 The case $\mathbf{DP}_e$

For $|G| = n^2 - \sqrt{n},\ m = 2$ and $\mathbf{F} = \emptyset$, one point orbit (and one line orbit) defines a Baer subplane. Let $\mathfrak{B}$ be the Baer subplane defined by G.

Piper [Pip75] has shown that quasiregular projective planes of type $\mathbf{DP}_e$ are equivalent to relative $(n+\sqrt{n}+1, n-\sqrt{n}, n, 1)$-difference sets. Using the results from section 1.3, a much shorter proof can be given as follows:

By 5.3, each line of $\mathfrak{P}$ meets $\mathfrak{B}$ in either 1 or $\sqrt{n}+1$ points. G acts transitively on these two classes of lines. The stabiliser N of a line meeting $\mathfrak{B}$ in $\sqrt{n}+1$ points is a normal subgroup in G because of quasiregularity. Furthermore, N consists of Baer collineations.

The points of $\mathfrak{P} - \mathfrak{B}$ together with the lines meeting $\mathfrak{B}$ in just one point, define the divisible design $\mathfrak{P}'$. A point class of this design can be written as $L \cap \mathfrak{P}'$ for some line L meeting $\mathfrak{B}$ in $\sqrt{n}+1$ points. By definition, the stabiliser of each point class is N.

So by 1.15, a line of $\mathfrak{P}'$ defines a relative $(n + \sqrt{n} + 1, n - \sqrt{n}, n, 1)$-difference set with forbidden normal subgroup N. It is easily seen that $\mathfrak{P}$

can be reconstructed from $\mathfrak{P}'$. Ganley and Spence have shown in [GS75], that $n = 4$ is the only prime power, for which an *abelian* relative difference set of this type exists.

For $n = 16$ there are 13 non-abelian groups of order $16^2 - 4 = 252$ having a normal subgroup of order $16 - 4 = 12$. Using `GAP`, we get

3.10 Theorem. *There is no projective plane of order* 16 *of type* $\mathbf{DP}_e$.

3.6 Type $\mathbf{DP}_f$: direct product difference sets

In case $\mathbf{DP}_f$ we have a quasiregular group G of order $n(n-1)$ which fixes two points a, b and the line M containing them as well as another line L through one of the fixed points (say, a).

The design $\mathfrak{P}'$ admits two partitions into point classes. These are defined by the lines $[a]$ and $[b]$ of $\mathfrak{P}$. So $\mathfrak{P}'$ is not a divisible design as defined on page 12. But using similar arguments as for the proof of 1.15, we see that $\mathfrak{P}'$ is represented by a relative difference set with a forbidden *set* which is the union of two normal subgroups.

The forbidden normal subgroups have orders n and $n - 1$. They are the line wise stabilisers of a and b, respectively, and consist of (a, M)-elations and (b, L)-homologies, respectively. Let H be the group of homologies and E the group of elations. Then H and E centralise each other by 1.29 and $G = HE$. The arguments for the reconstruction of $\mathfrak{P}$ from $\mathfrak{P}'$ are similar to those used in case $\mathbf{DP}_b$.

3.11 Theorem ([Pot95])**.** *Let $D \subseteq G$ is a relative difference set of type* $\mathbf{DP}_f$ *of order n in an abelian group G.*

- *If* $n \equiv 0 \mod 2$ *then the Sylow* 2*-subgroup of G is elementary abelian.*
- *If* $n \equiv 1 \mod 2$*, then the Sylow* 2*-subgroup of G is cyclic.*

As seen above, projective planes of type $\mathbf{DP}_b$ and order $n = 16$ are represented by relative $(n/2, 2(n-1), n-1, 1) = (8, 30, 15, 1)$-difference sets and $G = H \times E$ with H and E the forbidden normal subgroups.

The algorithm used to calculate all relative difference sets of this type is outlined below.

(a) Calculate possible admissible unordered signatures.

(b) Generate partial difference sets containing 6 elements. This is a variant of algorithm 6. It also exploits the fact that the difference set D to be found is a system of representatives for G/E. And D contains exactly one element from each nontrivial coset modulo H. This is also used in a similar way as in algorithm 1 in case $\mathbf{DP}_b$.
This step uses costly algorithms to test equivalence of partial difference sets.

(c) Extend partial difference sets to length 15 as above but without testing for equivalence.

(d) Generate the projective plane from difference set and determine the isomorphism class using Algorithm 11.

3.12 Theorem. *Let $\mathfrak{P}$ be a projective plane of order* 16 *and G a group of collineations acting quasiregularly on $\mathfrak{P}$ of type $\mathbf{DP}_f$. Then $\mathfrak{P}$ is the Desarguesian plane and $G \simeq \mathrm{C}_{15} \times \mathrm{E}_{16}$*

3.7 Type $\mathbf{DP}_g$: Neofields

The case $\mathbf{DP}_g$ is $|G| := (n-1)^2$ with 7 orbits on points and lines. Ghinelli and Jungnickel have shown

3.13 Theorem ([GJ03b, 3.7] and [GJ03a, 8.1])**.** *Let $\mathfrak{P}$ be a projective plane and G a collineation group with $|G| = (n-1)^2$ then the following statements are equivalent:*

(a) *G is of Lenz-Barlotti type I.4*

(b) *G is quasiregular of type $\mathbf{DP}_g$*

(c) *$\mathfrak{P}$ is the extension of an affine plane coordinised by a neofield K with $|K| = n-1$ and $G \simeq K^* \times K^*$*

(d) *$\mathfrak{P}$ can be represented by a relative difference set with forbidden set*

under these conditions, G is necessarily abelian.

So for order 16 we have $G \simeq \mathrm{C}_{15} \times \mathrm{C}_{15}$. In particular K is a cyclic neofield of order 16. The following relative difference set is given in [GJ03b] as an example for this case:

$$D = \{ (\xi, \psi) \in K^* \times K^* \mid \xi + \psi = 1 \} . \tag{3.13.1}$$

If K is actually a field, the projective plane defined by this difference set is the Desarguesian plane. Ghinelli and Jungnickel [GJ03a] point out that Hughes has shown in [Hug55] that any cyclic neofield of order 16 is a field.

The difference set construction is similar to that in case $\mathbf{DP}_b$ and $\mathbf{DP}_f$. This is the general idea: G fixes a triangle, so there are three sorts of point classes in $\mathfrak{P}'$ (corresponding to the vertices of the triangle). The stabiliser of such a point class is a normal subgroup in G and the union of the three stabilisers is the forbidden set.

The stabiliser of a point class has order $n-1$ (the factor group acts transitively on the point classes for this vertex). So $\mathfrak{P}$ is represented by a relative $(\frac{(n-1)^2}{(3(n-2)+1)}, 3(n-2)+1, n-1, 1)$-difference set with forbidden set.

A Computer search shows

3.14 Theorem. *Let $D \subseteq \mathrm{C}_{15} \times \mathrm{C}_{15}$ be a relative difference set of type $\mathbf{DP}_g$. Then D is Desarguesian.*

3.8 Concluding theorem

We will close this chapter with the classification theorem for projective planes of order 16 admitting a large quasiregular group of collineations. This collects the classification theorems for cases $\mathbf{DP}_a$–$\mathbf{DP}_g$ stated before and includes the classification of the translation planes of order 16 by Dempwolff and Reifart [DR83].

3.15 Theorem. *Let $\mathfrak{P}$ be a projective plane of order* 16 *and G a group with $\frac{273}{2} < |G|$ acting quasiregularly on $\mathfrak{P}$. Then $\mathfrak{P}$ is one of the following:*

(a) *The Desarguesian plane. In this case, G is of type $\mathbf{DP}_a$, $\mathbf{DP}_b$, $\mathbf{DP}_c$, $\mathbf{DP}_d$, $\mathbf{DP}_f$ or $\mathbf{DP}_g$.*

(b) *The semifield plane with kernel* GF(2) *or* GF(4)*. Here G acts as a group of type $\mathbf{DP}_b$ or $\mathbf{DP}_c$.*

(c) *The Mathon plane (or its dual) and G acts as a group of type $\mathbf{DP}_b$.*

(d) *A translation plane with G acting as a group of type $\mathbf{DP}_c$. According to [DR83], the isomorphism class of $\mathfrak{P}$ is one of the following (or their dual): the plane of Hall plane, the Lorimer-Rahilly plane, the Johnson-Walker plane, the derived semifield plane, or the Dempwolff plane.*

Chapter 4

Implementation

In this chapter, some of the algorithms used to calculate relative difference sets will be outlined. The basic functions are implemented as a `GAP` package called "`RDS`" [Röd06]. For the sake of readability, the algorithms listed here differ in some points from those implemented in `GAP` to find relative difference sets. In particular, we will not describe the data structures used and will always prefer "readable" descriptions over "fast" ones.

Throughout this section, G will be a finite group and $N \subseteq G$ will be the forbidden set.

We will now construct relative $(|G|/|N|, |N|, k, \lambda)$-difference sets in G with the aid of a computer. The general idea for such a search is outlined in algorithm 2.

In line 3 of algorithm 2, the set of normal subgroups may be chosen as $\mathfrak{U} := \{U \trianglelefteq G \mid |G : U| \leq a\}$ for some $a \in \mathbb{N}$. Of course, there may not be $V \in \mathfrak{U}$ as desired in line 7. In this case, V has to be chosen such that it has only few signatures and the following lines have to be processed for each of these signatures. Finding all difference sets in line 10 is done by a fairly simple recursive algorithm. No invariants are used in this step. Isomorphism tests (line 13) are done using special invariants and by explicitly calculating isomorphisms if necessary.

4.1 Calculation of admissible signatures

Algorithm 3 calculates the solutions of (1.20.1) and (1.20.2) (see page 15) as multisets. Note that we represent multisets as tuples (with entries ordered as

Algorithm 2 General idea for finding difference sets

Require: group G, parameters $|N|$, k, λ

```
Find all possible forbidden sets $N \subseteq G$.
for all $N$ do
    Choose set $\mathcal{U}$ of normal subgroups of $G$
    for $U \in \mathcal{U}$ do
        Calculate/test admissible signatures for $U$    #algs. 3, 4, 5
    end for
    Find $V \in \mathcal{U}$ having only one ordered signature
    Generate set $\mathcal{S}$ of startsets using cosets modulo $V$    #alg. 6
    for all $S \in \mathcal{S}$ do
        Find all difference sets $D \supseteq S$    #alg.10
    end for
end for
Generate projective planes from the difference sets found and apply isomorphism checks    #sec. 4.4
```

on page 6). For the solution of (1.20.3), we have to take care of the ordering of the coefficients. Given a multiset of coefficients $\|(p_1, \dots, p_{|G|/|U|})\|$ solving (1.20.1) and (1.20.2), as calculated by algorithm 3, we will have to check every permutation of these coefficients to see if the permuted tuple is a solution of (1.20.3). This is done by algorithm 4.

In this step, a tuple $(p_1, \dots, p_{|G/U|})$ can only be rejected if it has no permutation which solves (1.20.3). Because of the computational efforts needed to calculate all permutations, algorithm 4 does not calculate ordered signatures, but only verifies if a tuple defines an admissible signature (i.e. has an ordering which is an ordered signature). For ordered signatures, all permutations have to be tested. Also to verify that a tuple does not define an admissible signature, all permutations have to be considered. So if a tuple has too many permutations, it is advisable not to do a full test but to assume that the tuple defines an admissible signature. A suitable bound has to be chosen depending on computer power.

As noted on page 16, admissible signatures do not depend on the isomorphism class of the group the relative difference set lives in. Especially in case $\mathbf{DP}_b$ and order $n = 16$ –where many groups have to be considered– repeated tests of the same signature can be avoided by storing information about the subgroup structure of the groups together with the calculated signatures.

Algorithm 3 Calculation of admissible signatures for relative difference sets

```
Require: $|G|, |U|, |N|, |U \cap N|, k, \lambda$

  $R := \emptyset$
  $L := \{0, \dots, k - \lambda\}$
  while $L \neq \emptyset$ do
      $l := \max L$
      if $l^2 \leq k + \lambda(|U| - |U \cap N|)$ then
          $\Pi := \left\{(p_1, \dots, p_{|G|/|U|}) \,\middle|\, p_i \in L,\ p_1 = l,\ k = \sum_i p_i\right\}$
  # $\Pi$ is the set of partitions of $k$ into sums of Length $|G|/|U|$ containing $l$.
          if $\sum p_i^2 = k + \lambda(|U| - |U \cap N|)$ then
              Add $(p_1, \dots, \pi_{|G|/|U|})$ to $R$
          end if
      end if
      Remove $l$ from $L$
  end while
  return R
```

As seen in section 2.1, ordered signatures of ordinary difference sets may be calculated with less effort in extensions of $\mathrm{C}_s \ltimes \mathrm{C}_p$. This is done by algorithm 5.

Let ζ be a primitive q^{th} root of unity. Algorithm 5 calculates non-negative integers M_{ij}, $1 \leq j \leq q$, $1 \leq i \leq s$ with $\sum_{j=1}^{q} M_{ij} = S_i$ such that $M = M(M_1, \dots, M_s, \alpha, \vartheta)$ is a semi- circulant matrix with $M\bar{M}^t = n\,\mathbb{1}$. Here $M_i = \sum_{j=1}^{q} M_{ij}\zeta^{j-1}$ and $\alpha \colon \zeta \mapsto \zeta^m$ and $\vartheta := (1 \dots s)$.

Algorithm 5 uses lemma 2.7 and therefore can only be used to calculate ordinary difference sets. Here the group of mappings from 2.7 acts on each tuple $(M_{ij})_j$, as well as on the concatenation of the tuples (and of course on the corresponding algebraic integers).

A generalisation of algorithm 5 to relative difference sets is possible by omitting the calculations using 2.7 and testing $M\bar{M}^t = k\,\mathbb{1} - \lambda N^{\Phi}$ instead of $M\bar{M}^t = (k - \lambda)\,\mathbb{1}$. Here N is the forbidden group and Φ is the unitary representation defined in (2.2.1).

Algorithm 4 Test for signatures of relative difference sets with forbidden subgroup

```
Require: $G, U, G/U, |U \cap N|$, and signature $\sigma = (p_1, \dots, p_{|G|/|U|})$ as returned
  by algorithm 3
  Assume that the signature is indexed by the elements of $G/U$.

  Define $N/U := \{g \in G/U \mid g \cap N \neq \emptyset\}$.
  if $|U| = |U \cap N|$ and $|N/U| = 1$ then     #i.e. if $U = N$
      if $p_i \in \{0, 1\}$ for all $p_i \in \sigma$ then
          return true
      else
          return false
      end if
  end if
  Define $\Pi$ to be the set of all permutations of $(p_1, \dots, p_{|G/U|})$
  for $\pi \in \Pi$ do
      if $\forall 1 \neq o \in N/U\colon \sum_{g \in G/U} p_g p_{go} = \lambda(|U| - |U \cap N|)$
       and $\forall o \in G/U - N/U\colon \sum_{g \in G/U} p_g p_{go} = \lambda|U|$ then
          return true
      end if
  end for
  return false
```

Algorithm 5 Calculation of ordered signatures for extensions of $\mathrm{C}_s \ltimes \mathrm{C}_q$

```
Require: $(S_1, \dots, S_s), n, \zeta, \alpha$

  $\pi := (1 \dots, q)$
  $\mathrm{Sym}_q \ni \gamma \colon i \mapsto q - i + 1$ for $2 \leq i \leq q/2$      #comp. conj. on indices $\{1 \dots q\}$
  $\iota_i \colon \{1, \dots, q\} \to \{(i-1)q, \dots, iq - 1\}$ for $1 \leq i \leq s$. $j \mapsto j + (i-1)q$
  for $B \in \{1, \dots, s\}$ do
      $t_B := 0$
      for $b \in \{1, \dots, s-1\}$ do
          $t_{B\pi^b} := (t_{B\pi^{b-1}+1})m \mod q$
      end for
      define $\mathrm{Sym}_q \ni \tau_B \colon j \mapsto t_j$
      $\alpha_B := \prod \tau_i^{\iota_i}$
  end for
  $\Gamma := \langle \tau_B, \prod_{i=1}^{s} \gamma^{\iota_s} \rangle$      #the group from lemma 2.7 operating on indices
  $\gamma := \langle \tau_B \rangle_{(2q+1, \dots, sq)}$      #stabiliser of erverything but the first block
  for each $S_i$ calculate the set $C_i$ of all $\mathbb{N}[\zeta] \ni z = \sum_{i=0}^{q-1} a_i \zeta^i$ with $\sum a_i = S_i$.
  identify $(a_1 \dots, a_q)$ with $\sum_{i=0}^{q-1} a_{i+1} \zeta^i$.
  $\hat{C}_i := \{ x\bar{x} \mid x \in C_i \}$ for $1 \leq i \leq s$
  $T := \hat{C}_1 \times \cdots \times \hat{C}_{s-1}$
  for $t \in T$ do
      if $n - \sum_{i=1}^{s-1} t_i \in \hat{C}_s$ then
          $\widetilde{t_i} := \{x \in C_i \mid x\bar{x} = t_i\}$ for $1 \leq i < s$.
          $\widetilde{\tau_t} := \widetilde{t_1} \times \cdots \times \widetilde{t_{s-1}}$
          choose one representative from each orbit of $\gamma$ on $\widetilde{\tau_t}$ and remove the
  rest from $\widetilde{\tau_t}$.
  # $\gamma$ and $\Gamma$ operate naturally on the components of $\tau \in \tau_t$
          $\tau_t := \widetilde{\tau_t} \times \{ x \in C_s \mid x\bar{x} = n - \sum t_i \}$
      end if
  end for
  $T_0 := \{ \tau_t \mid t \in T \}$      #we now have $\sum M_i \bar{M}_i = n$ and $\sum_{m \in \{M_i\}} m = S_i$
  for $t \in T_0$ do
      define $\tau_t$ as a system of representatives of the orbits of $\Gamma$ on $t$
  end for
  $R := \left\{ \tau \in \bigcup_{t \in T_0} \tau_t \;\middle|\; M\bar{M}^t = (k - \lambda)\,\mathbb{1},\ \text{for } M = M((\tau)_1, \dots, (\tau)_s, \alpha, \pi) \right\}$
  # here the elements of $\tau$ are treated as cyclotomics
  for each $\tau \in R$ let $\hat{\tau}$ be the concatenation of the elements (tuples) of $\tau$.
  return $\{\hat{\tau} \mid \tau \in R\}^{\Gamma}$.
```

4.2 Startsets

Let G be a finite group and $V \trianglelefteq G$. We assume that there is a unique ordered signature for V. To find relative difference sets in G, we first generate start sets (partial relative difference sets) "coset by coset" and then reduce the list of start sets as outlined in algorithm 6. If S is a partial difference set, then any $C \subseteq G$ such that $S \cup \{c\}$ is still a partial difference set for all $c \in C$ will be called a set of "possible completions" for S. Given a partial difference set and any set $C \subseteq G$, algorithm 7 returns the subset of all possible completions of C for S.

Algorithm 6 Generate startsets

Require: unique ordered signature $(p_1, \ldots, p_{|G:V|})$ for $V \trianglelefteq G$, cosets $u_1V, \ldots, u_{|G:V|}V$, forbidden set N, a set $\mathcal{U}$ of normal subgroups of G, the set $\mathcal{S}$ of signatures for all $U \in \mathcal{U}$ and $A \leq \mathrm{Aut}^{\circ}(G)$. (see page 45)

```
$S := \{(1)\}$    #the smallest partial difference set
for $1 \leq i < |G:V|$ do
    $R := u_iV$
    repeat
        $\mathcal{O} := \emptyset$
        for all $s \in S$ do
            C:=RemainingCompletions($S, R, N$)    #alg.7
            for $i \in C$ do
                Add $s \cup \{i\}$ to $\mathcal{O}$
            end for
        end for
        $S := \mathcal{O}$    #overwrite $S$ with $\mathcal{O}$
        ReduceStartSets($A, S, \mathcal{S}, \mathcal{U}$)    #alg. 9
    until $\forall d \in S: \ |d| = \sum_{j \leq i} p_j$
end for
```

The assumption to have just one ordered signature is very strong. But for normal subgroups of low index, chances are good to have just one admissible signature. In some of these cases it is possible to choose an ordered signature without loss of generality (if there is just one admissible signature and all entries of this signature –with at most one exception– are equal). In all other cases the algorithm has to be applied to every ordered signature.

Algorithm 7 Remaining completions

```
procedure RemainingCompletions($S, C, N$)
# $S$: partial difference set, $C \subseteq G$, N: forbidden set
    $P := \{ab^{-1} \mid a, b \in S\}$.
    $W := \emptyset$
    $C' := C - (P \cup N)$
    for all $c \in C'$ do
        if $Sc^{-1} \cap (N \cup P) \neq \emptyset$ then
            add $c$ to $W$.
        end if
    end for
    return $C - W$
end procedure
```

The known admissible (ordered) signatures are now used in the algorithms 8 and 9.

Let the mappings σ_U and s_U be the signature maps as in definition 1.22. Algorithm 8 calculates the value of the signature map for every normal subgroup $U \in \mathfrak{U}$. For those normal subgroups for which ordered signatures are known, the ordered signature is also calculated. It furthermore tests if the (ordered) signatures of a partial difference set are compatible with the known admissible (ordered) signatures. If this is not the case, “false” is returned.

Algorithm 8 Signatures of partial difference sets

```
Require: partial difference set $S$, admissible signatures for a set $\mathfrak{U}$ of normal
  subgroups of $G$.
  for $U \in \mathfrak{U}$ do
      if not ($\sigma_U(S) \leq \sigma$ (pointwise) for any admissible signature $\sigma$) then
          return false
      else if $U$ has admissible ordered signatures then
          if not ($s_U(S) \leq \sigma$ (pointwise) for any ordered signature $\sigma$) then
              return false
          end if
      end if
  end for
  return $\|(\sigma_U(S), s_U(S))_{U \in \mathfrak{U}}\|$
```

Algorithm 9 takes a set S of partial differences sets and $A \leq \mathrm{Aut}^\circ(G)$. As we generate difference sets "coset by coset", we will choose A to be the stabiliser of N and all cosets modulo U. So

$$A := \mathrm{Aut}^\circ(G)_N \cap \Big(\bigcap_{g_iU \in G/U} \mathrm{Aut}^\circ(G)_{g_iU} \Big).$$

It is assumed that the admissible signatures are already calculated and can be used. The algorithm returns a subset of S, the elements of which have pairwise different signatures.

Note. *For algorithm 9, a suitable group of (anti-)automorphisms of G has to be chosen. The above choice of A ensures that all difference sets generated have the* same *forbidden set.*

If A is very large, the reduction can be done using a list of subgroups of A. Line 7 and 8 are then processed for every subgroup in this list. This results in a considerable speedup in some cases.

Moreover, the set $\mathfrak{U}$ of normal subgroups of G has to be chosen such that the multiset $\|(\sigma_U(D))_{U \in \mathfrak{U}}\|$ is still an invariant for partial relative difference sets. The natural choice for $\mathfrak{U}$ is to take all normal subgroups of some given orders. More intelligent choices are possible if some orbits of A on the set of normal subgroups of G are known.

4.3 Brute force

The method for reducing startsets gets ever more time-consuming, as the startsets get longer. Normally, we will generate startsets containing only elements from one or two cosets modulo the normal subgroup V chosen in line 7 of algorithm 2. After this, a recursive brute force method is applied to each startset S to find all difference sets containing S. This is described in algorithm 10. Note that the set C in algorithm 10 must be a set of completions as calculated by algorithm 7 (otherwise, the algorithm will produce wrong results). In line 3, the variable k is the length of a full difference set. In line 6, we will normally not run over all elements from C but use an ordering argument to add only elements larger than the ones previously added. This avoids duplicates.

We may also generate partial difference sets using algorithm 10, choosing a $k' < k$ and a suitable set C. For example, one could choose C to be a subset

Algorithm 9 Reduction of startsets

```
procedure ReduceStartSets($A, S, \mathcal{S}, \mathcal{U}$)
# $A \leq \mathrm{Aut}^\circ(G)$, $S$: set of partial difference sets, $\mathcal{S}$: admissible signatures for all $U \in \mathcal{U}$, $\mathcal{U}$: set of normal subgroups of $G$ (see note on page 45)
    Define Partition $\Pi$ on $S$ by $x \sim y :\Leftrightarrow \|(\sigma_U(x))_{U \in \mathcal{U}}\| = \|(\sigma_U(y))_{U \in \mathcal{U}}\|$ using algorithm 8
    for $\pi \in \Pi$ with $|\pi| > 1$ do
        for $s \in \pi$ do
            $T := \{(l, \{lx^{-1} \mid x \in l\}) \mid l \in \pi\}$
            $T' := \left\{(l, M) \in T \mid \exists x \in M\colon x \in s^A\right\}$
            choose a representative of $\{t \mid (t, M_t) \in T'$ and $t \in \pi\}$ and remove the rest from $\pi$.
        end for
    end for
    return $\bigcup_{\pi \in \Pi} \pi$
end procedure
```

of a coset gV and k' as the number of elements a difference set contains from gV plus the length of S (as we assume to know ordered signatures modulo V, this is possible). After this step, we may make a reduction step and continue with brute force.

4.4 Tests for the isomorphism class of projective planes

After all relative difference sets (up to equivalence) are found, the projective plane has to be reconstructed from the difference set. Chapter 3 gives constructions for all cases $\mathbf{DP}_a$–$\mathbf{DP}_g$. The algorithms for this are not listed here. They generally look like this:

1. Define points G and lines $\{Dg \mid g \in G\}$
2. Find parallel classes and add ideal points to each line.
3. Find point classes and add ideal lines.

When this is done, we use invariants for projective planes do determine the isomorphism class of the planes generated. In some cases, there are

Algorithm 10 Brute force generation of difference sets

```
procedure AllDifferenceSets($S$, $C$, $N$, $\mathcal{D}$)
# $S$: partial difference set, $C \subseteq G$: possible completions, $N$: forbidden set, $\mathcal{D}$: set of difference sets already found
    if $|S| = k - 1$ then
        Add $\{S \cup \{c\} \mid c \in C\}$ to $\mathcal{D}$
    else
        for all $i \in C$ do
            $S' := S \cup \{i\}$
            $\tilde{C}$:=RemainingCompletions($S', C$)
            if $|S'| + |\tilde{C}| \geq k - 1$ and $|S'| \leq k - 1$ then
                AllDifferenceSets($S', \tilde{C}, N, \mathcal{D}$)
            end if
        end for
    end if
end procedure
```

full invariants (for example for the translation planes of order 16). In the other cases, we will have to construct isomorphism between the planes found and “known” planes with the same invariants. We will now consider some invariants which were used for planes of order 16.

4.4.1 The Fano invariant

4.1 Theorem. *Let $\mathfrak{P}$ be a finite projective plane. For each point P of $\mathfrak{P}$ let n_P denote the number of Fano- subplanes (the subplanes of order 2) containing this point.*

If $\mathfrak{P}'$ is another projective plane and $\varphi\colon \mathfrak{P} \to \mathfrak{P}'$ an isomorphism, then $n_{P^\varphi} = n_P$ for all points P of $\mathfrak{P}$.

So the multiset $F(\mathfrak{P}) = \|(n_P)_{P\in\mathfrak{P}}\|$ is an invariant of the isomorphism class of $\mathfrak{P}$.

4.2 Corollary. *Let G be a group of collineations of the projective plane $\mathfrak{P}$, and P a point of $\mathfrak{P}$. Then $n_P = n_Q$ for all $Q \in P^G$.*

If we know a group of collineations of a projective plane, we choose a representative of each point orbit and calculate the number of Fano-subplanes in these points using algorithm 11. Gordon Royle [Roy] has a collection of all known projective planes of order 16 and their respective Fano numbers. This serves well for identification of the projective planes constructed from relative difference sets. Note that the numbers calculated by algorithm 11 are only 2/7 of the numbers Royle calculated.

Algorithm 11 Fano counter

```
procedure NrFanoPlanesAtPoints($\{P_1, \dots, P_n\}$)
    for $x \in \{P_1, \dots, P_n\}$ do
        $n_x := 0$
        for all $(b_1, b_2, b_3) \in [x]^3$ with pairwise different $b_i$ do
            for all $\pi_2, \pi_3 \in [b_1] - \{x\}$ with $\pi_2 \neq \pi_3$ do
                for all $\pi_4 \in [b_2] - \{x\}$ do
                    $b_{24} := [\pi_2, \pi_4]$
                    $\pi_{24} := [b_{24}, b_3]$
                    $b_{34} := [\pi_3, \pi_4]$
                    $\pi_{34} := [b_{34}, b_3]$
                    $b_{324} := [\pi_3, \pi_{24}]$
                    $b_{234} := [\pi_2, \pi_{34}]$
                    if $[b_3, b_{234}] = [b_2, b_{324}]$ then
                        increment $n_x$ by 1.
                    end if
                end for
            end for
        end for
    end for
    return $\{(x, n_x) \mid x \in \{P_1, \dots, P_n\}\}$.
end procedure
```

4.4.2 Fingerprint and p-rank

The following invariant can be found in [Moo95] and is said to be due to Conway.

Let $\mathfrak{P}$ be a projective plane of order n and (P, ℓ) an anti-flag of $\mathfrak{P}$. Write

$$[\ell] = \{E_1, \dots, E_{n+1}\}$$
$$[P] = \{m_1, \dots, m_{n+1}\}$$

And assume that E_i is incident with m_i for all $1 \leq i \leq n+1$. Now label the points of m_i as $P = P_{i,1}, \ldots, P_{i,n+1} = E_i$ and label the lines of E_i as $\ell = \ell_{i,1}, \ldots, \ell_{i,n+1} = m_i$.

Let $i \neq j$. Then each $P_{j,k}$ lies on exactly one line $\ell_{i,k\sigma_{ij}}$ through E_i for some permutation σ_{ij}. Now define the $(n+1) \times (n+1)$ sign matrix

$$A_{ij} := \begin{cases} \operatorname{sgn}(\sigma_{ij}) & \text{for } i \neq j \\ 0 & \text{for } i = j \end{cases}$$

The *partial fingerprint* of $\mathfrak{P}$ with respect to (P, ℓ) is defined as the multiset $\|(|\sum_{k=1}^{n+1} a_{ik}a_{jk}|)_{i,j}\|$ (with $1 \leq i, j \leq n+1$) of the modulus of the entries of AA^t. Obviously, the fingerprint is an invariant for $\mathfrak{P}$ depending on the anti-flag (P, ℓ). For translation planes, the canonical choice for (P, ℓ) is (P_0, ℓ_∞) with ℓ_∞ the line at infinity and some affine point P_0.

For projective planes in general, we may define the *complete fingerprint*, which is generated from an $(n^2+n+1) \times (n^2+n+1)$ sign matrix: Let $P_1, \ldots, P_{n^2+n+1}$ be the points of $\mathfrak{P}$ and $\ell_1, \ldots, \ell_{n^2+n+1}$ the lines of $\mathfrak{P}$. For each point P_i and each line ℓ_i define an arbitrary but fixed ordering of the respective lines (points) as $[P_i] = \{\ell_{i,1}, \ldots, \ell_{i,n+1}\}$ and $[\ell_i] = \{P_{i,1}, \ldots, P_{i,n+1}\}$. For each anti-flag (P_i, ℓ_j) there is a canonical bijection between $[P_i]$ and $[\ell_j]$. Now define σ_{ij} to be the permutation of the indices induced by this bijection and the chosen ordering of points and lines.

Again, we define a sign matrix $A_{ij} := \operatorname{sgn}(\sigma_{ij})$ for $i \neq j$ and $A_{ii} = 0$ for all $1 \leq i \leq n^2+n+1$. And the complete fingerprint is the multiset $\|(|c_{ij}|)\|$ with $C = AA^t$.

A very basic invariant is the so-called p-rank:

4.3 Theorem. *Let $p \in \mathbb{P}$ and $\mathfrak{P}$ a projective plane. Then the rank of the incidence matrix of $\mathfrak{P}$ as a matrix over* GF(p) *is an invariant for the isomorphism class of $\mathfrak{P}$.*

4.4.3 How to choose an invariant

Which of the above invariants is suitable for an isomorphism test does obviously depend on the order n of the projective planes tested. Here are a few observations from computer experiments for orders ≤ 81. These experiments were done on a standard desktop computer.

For the Fano invariant in one point, $\binom{n+1}{3}\binom{n}{2}n$ quadrangles have to be tested (see algorithm 11 on page 11). And each test is a sequence of list operations. The Fano invariant is very strong in the sense that it is a complete invariant for the known projective planes of order 16 and the semifield planes of order 81, for example. For planes of order 32 the Fano can still be calculated with little effort, while for order 81 it is very hard.

The partial fingerprint needs about n^3 list operations per anti-flag. Consequently, the full fingerprint takes n^5 list operations and much more memory than the partial fingerprint (the full fingerprint calculates a square matrix with n^2+n+1 lines, whereas the partial fingerprint uses an $(n+1)\times(n+1)$ matrix). For translation planes, there is a canonical choice for the anti-flag, so the partial fingerprint is a good choice here. For translation planes of order 81, for example, the partial fingerprint is easy to calculate but does not distinguish all semifield planes (on the 27 semifields of order 81, the partial fingerprint has only 4 different values, see [Dem]).

The p-rank needs about n^2 list operations to generate the incidence matrix. Calculating the rank of the matrix needs about $(n^2)^3$ operations in the general case. Furthermore, the incidence matrix takes a lot of memory. Nonetheless, calculating the p-rank is still faster than calculating the Fano number.

And, of course, groups of elations and homologies can be combined with the invariants mentioned before. In the example of semifield planes of order 81, using the partial fingerprint and the size of a group of homologies with axis ℓ_∞ gives 8 different values.

Chapter 5

Computer aided experiments in higher order

Using GAP and the routines described in chapter 4, we may look for projective planes in orders larger than 16. Interesting orders may be 25, 27 or 81.

A problem with higher order planes is that the groups involved are very large, so a complete search of all planes with large quasiregular collineation group as in the case $n = 16$ is very difficult. So we will restrict ourselves to difference sets which are fixed under a given group-automorphism. In case $\mathbf{DP}_b$, the following lemma characterises such automorphisms.

5.1 Lemma. *Let $1 \in D \subseteq G$ be a relative difference set of type $\mathbf{DP}_b$ with forbidden group $N \trianglelefteq G$. Let $\mathfrak{P}$ be the projective plane defined by D. Then* $\mathrm{Aut}(\mathfrak{P}) \cap \mathrm{Aut}(G) = (\mathrm{Aut}(G)_N)_D$.

Elements of $\mathrm{Aut}(G)$ can be extended to act on the points of $\mathfrak{P}$. However, the extension may not be a collineation of $\mathfrak{P}$. So $\mathrm{Aut}(\mathfrak{P}) \cap \mathrm{Aut}(G)$ is just the group of extensions of group automorphisms which respect incidence.

Proof. Let ℓ_∞ be the ideal line and p_∞ the ideal point of $\mathfrak{P}$ (see the construction on page 29). The points of $\ell_\infty - \{p_\infty\}$ can be identified with the parallel classes of $\operatorname{dev} D$. So $\mathrm{Aut}(G)$ fixes ℓ_∞. By 1.14, the cosets of the forbidden subgroup N are exactly the point classes of $\operatorname{dev} D$. But the point classes of $\operatorname{dev} D$ are exactly the lines of $\mathfrak{P}$ which are different from ℓ_∞ and contain p_∞.

And as $\mathrm{Aut}(G)$ fixes the point $1 \in G$ and acts on the point classes of $\operatorname{dev} D$, we have $\mathrm{Aut}(\mathfrak{P}) \cap \mathrm{Aut}(G) \leq \mathrm{Aut}(G)_N = \mathrm{Aut}(G)_{\ell_0}$ where ℓ_0 is the line containing p_∞ and $1 \in G$.

The parallel class of D in $\operatorname{dev} D$ is $\{ Dn \mid n \in N\}$ and $D \cap N = \{1\}$ by assumption. So $\operatorname{Aut}(G) \cap \operatorname{Aut}(\mathfrak{P})$ does also fix the parallel class of D which is a point $p_D \in \ell_\infty$ and it also fixes D because $1 \in D$.

So we have $\operatorname{Aut}(G) \cap \operatorname{Aut}(\mathfrak{P}) \leq (\operatorname{Aut}(G)_N)_D$. On the other hand, every element of $(\operatorname{Aut}(G)_N)_D$ clearly induces a collineation on $\mathfrak{P}$. □

So in this case the elements of $\operatorname{Aut}(G)$ extending to collineations (sometimes called "multipliers") of $\mathfrak{P}$ automatically fix the difference set defining $\mathfrak{P}$.

5.1 Type $\mathbf{DP}_b$ and a Baer involution

In this section we will consider relative difference sets of type $\mathbf{DP}_b$. Moreover we assume that there is an involutorial group automorphism fixing a Baer subplane. This is not a very big restriction, as we have

5.2 Theorem ([Dem68, 3.1.2, 3.1.6])**.** *Let $\mathfrak{P}$ be a projective plane. The fixed structure of an involutorial collineation is either of the form*

$$\{p, L\} \cup [p] \cup [L]$$

with some point-line pair p, L or a Baer subplane (fixed pointwise). Involutorial collineations fixing a Baer subplane pointwise are called "Baer involutions".

5.3 Lemma. *Let $\mathfrak{P}$ be a projecive plane of order n^2 and $\mathfrak{B}$ a Baer subplane of $\mathfrak{P}$. For every line $l \in \mathfrak{P}$ we have $|l \cap \mathfrak{B}| \in \{n+1, 1\}$.*

Proof. As $\mathfrak{B}$ is projectively closed, l has to have $n+1$ points in $\mathfrak{B}$ as soon as more than 2 points are in $\mathfrak{B}$. Assume that $l \cap \mathfrak{B} = \emptyset$. Then every line of $\mathfrak{B}$ meets l and no point of l is met by two lines of $\mathfrak{B}$, as $\mathfrak{B}$ is closed. So l has at least $n^2 + n + 1$ points. But $\mathfrak{P}$ has order n^2, so l does only contain $n^2 + 1$ points. □

5.4 Lemma. *Let $\mathfrak{P}$ be a projective plane of order n^2 and ι a Baer involution. Let ℓ_∞ be a line of $\mathfrak{P}$, for which $\ell_\infty^\iota = \ell_\infty$. Then $|\mathfrak{B} \cap \ell_\infty| = n+1$, where $\mathfrak{B}$ is the Baer subplane.*

Proof. Let $\mathfrak{B}$ be the Baer subplane fixed by ι. Then ℓ_∞ meets $\mathfrak{B}$ in either 1 or $n+1$ points. Suppose $\mathfrak{B} \cap \ell_\infty = \{p\}$. Then none of the points of $\ell_\infty - \{p\}$ is fixed by ι. So the lines which do not contain p are tangents for $\mathfrak{B}$ (they do only contain one point of $\mathfrak{B}$). But this leaves $\mathfrak{B}$ with only $n^2 - 1 < n^2 + n + 1$ lines (the ones meeting p). A contradiction. □

5.5 Corollary. *Let $D \subseteq G$ be a relative difference set of type $\mathbf{DP}_b$ of order n^2. Let $\mathfrak{P}$ be the projective plane defined by D. Let $\iota \in \mathrm{Aut}(G)$ be an involution fixing the Baer subplane $\mathfrak{B} \subseteq \mathfrak{P}$. Assume that $1 \in D$ and $1 \in \mathfrak{B}$. Then there is $a \in D$ such that $|Da^{-1} \cap \mathfrak{B}| = n$.*

Proof. D is of type $\mathbf{DP}_b$ and hence $\ell_\infty^\iota = \ell_\infty$. So by 5.4, ℓ_∞ has $n+1$ points in $\mathfrak{B}$ and every line in $\mathfrak{B}$ contains a point of ℓ_∞.

The translates of D containing 1 are exactly those of the form Da^{-1} with $a \in D$. And as there are lines connecting 1 to points inside the Baer subplane and meet ℓ_∞ in different points, there is a translate of D which contains more than one point of $\mathfrak{B}$. This finishes the proof. □

5.1.1 Order 25

For $n = 25$, a computer search shows:

5.6 Theorem. *Let $D \subseteq G$ be a relative difference set of type $\mathbf{DP}_b$ and order 25. Let $\mathfrak{P}$ be the corresponding projective plane. If $\mathrm{Aut}(G)$ contains a Baer involution of $\mathfrak{P}$, then $\mathfrak{P}$ has the 5-rank and fingerprint (see section 4.4) of one of the following three planes*

(a) *The Desarguesian plane*

(b) *The Walker plane*

(c) *The dual Walker plane*

For the search, we first calculate all possible Baer involutions in $\mathrm{Aut}(G)$. Another possibility is to calculate all $F \leq G$ with $|F| = 25$ (up to conjugacy under $\mathrm{Aut}(G)_N$) and then find all involutions from $\mathrm{C}_{\mathrm{Aut}(G)_N}(F)$.

Once we have an involution $\iota \in \mathrm{Aut}(G)_N$ and the group F fixed by ι, we proceed as follows:

1. Generate startsets of length 5 consisting of elements of F.

2. Calculate the Partition $\mathcal{O}$ of $G - F$ into orbits of $\langle\iota\rangle$.

3. Generate relative difference sets by adding elements of $\mathcal{O}$ to the startsets of order 5. Use a slightly modified version of algorithm 1 (using orbits instead of points).

The identification of the planes found is done using the data provided by [Moo00], namely the 5-rank and the fingerprint.

Note that this does only proof that a plane of this type, which is not a Desarguesian plane has the same invariants as the Walker plane (or dual Walker plane). A strict test for isomorphism was not done.

5.1.2 Planes of order 81

To find planes $\mathfrak{P}$ of type $\mathbf{DP}_b$ and order 81 we will assume that $\mathfrak{P}$ admits a group isomorphism α of order 4 which fixes a subplane of order 3 such that α^2 is a Baer involution. Here the Baer subplane consists of the fixed points of α and the orbits of $\langle\alpha\rangle$ of length 2.

A computer search using `GAP` shows

5.7 Theorem. *Let $G = \mathrm{E}_{81^2}$ and $\alpha \in \mathrm{Aut}(G)$ with $|\alpha| = 4$. Let α fix a subgroup of order 9 element wise and α^2 fix a subgroup of order 81 element wise. Then a projective plane of order 81 and type $\mathbf{DP}_b$ admitting α as a collineation is one of the following:*

(a) *The Desarguesian plane*

(b) *A translation plane defined by a Dickson semifield with kernel $GF(9)$*

(c) *The Coulter-Matthews plane of order 81 defined by the monomial X^5 over $\mathrm{GF}(3^4)$*

Difference sets are constructed first as difference sets in the subplane of order 3 defined by the fixed points of α and then extended by adding $\langle\alpha\rangle$-orbits of length 2 until difference sets for the Baer subplane are found. Then $\langle\alpha\rangle$-orbits of length 4 are added to find all of the difference sets in question. The isomorphism class of the projective plane found is determined by calculating translation groups and groups of elations as well as the fingerprint (see 4.4.2). The semifields of order 81 are classified by U. Dempwolff [Dem]. The semifield planes of order 81 are almost uniquely determined by the combination of the partial fingerprint (with respect to ℓ_∞ and an affine point), the 3-rank and the order of a group of homologies with centre ℓ_∞. Only two cases have the same invariants (and our case is one of the others). A full invariant for the semifield planes of order 81 is given by the number of Fano subplanes in an affine point. In case of the Coulter-Matthews plane, an isomorphism is constructed explicitly.

Chapter 6

A result on planar functions

Here we will have a look at another construction for a special class of projective planes of type $\mathbf{DP}_b$. After the definition of planar functions, we turn to the special class of planar monomials over finite fields. In a theorem found together with U. Dempwolff [DR], a partition of planar monomials is defined which coincides with the isomorphism classes of the projective planes defined by planar monomials. Furthermore, the automorphism group of such projective planes is determined.

6.1 Definition. Let M, N be finite groups. A map $f\colon M \to N$ is called *planar function*, if for every $1 \neq a \in M$ the mapping $\Delta_{f,a}\colon M \to N$, $x \mapsto f(ax)f(x)^{-1}$ is bijective.

Every planar function f defines a projective plane $\mathfrak{P}(f)$ as follows. Let

$$\begin{aligned} P &:= (M \times N) \cup \{\,(a) \mid a \in M\} \cup \{(\infty)\} \\ L(a,b) &:= \big\{\,(x, f(xa^{-1})b) \bigm| x \in M\big\} \cup \{(a)\} \quad (a,b) \in M \times N \\ L(c) &:= \{\,(c,y) \mid y \in N\} \cup \{(\infty)\} \quad c \in M \\ L_\infty &:= \{\,(a) \mid a \in M\} \cup \{(\infty)\} \\ \mathfrak{L} &:= \{\,L(a,b) \mid (a,b) \in M \times N\} \cup \{\,L(c) \mid c \in M\} \cup \{L_\infty\} \end{aligned} \tag{6.1.1}$$

Then $\mathfrak{P}(f) := (P, \mathfrak{L})$ is a projective plane. The group $M \times N$ acts as a regular and faithful group of collineations on $\mathfrak{P} - \{L_\infty\}$, the affine points of $\mathfrak{P}$. And $M \times N$ fixes (∞) and acts transitively on $L_\infty - (\infty)$. The group N induces the full group of elations with centre (∞) and axis L_∞. So we have

6.2 Lemma. *Let $f\colon M \to N$ be a planar function. Then $M \times N$ acts on $\mathfrak{P}(f)$ as a quasiregular group of type $\mathbf{DP}_b$.*

Planar functions are commonly studied [DO68, Dem68, Pot95, CM97] for $M \simeq N \simeq \mathrm{E}_{p^n}$ with $2 \neq p \in \mathbb{P}$ and $n \in \mathbb{N}$. In this case, f can be written as a polynomial of degree less than p^n over $\mathrm{GF}(p^n)$. In fact, all known planar functions are planar polynomials.

6.1 Planar monomials

As seen above, relative difference sets of type $\mathbf{DP}_b$ in elementary abelian groups are equivalent to planar polynomials. The following series of planar monomials are known to the author:

- Dembowski and Ostrom [DO68] found that $\mathfrak{P}(X^2)$ is Desarguesian and $\mathfrak{P}(X^{p^a+1})$ is a commutative twisted semifield plane for $0 < a < n$ if $n/(n,a) \equiv 1 \mod 2$.
- Coulter and Matthews [CM97] have shown that $X^{(1+3^\alpha)/2}$ is planar over $\mathrm{GF}(3^n)$ for every $\alpha \not\equiv \pm 1 \mod 2n$ and that the according planes are not translation planes.

For planar monomials over prime fields, the following was found independently by several authors.

6.3 Theorem ([Joh87, Hir89, RS89, Glu90])**.** *Let $p \in \mathbb{P}$ and $1 \leq n < p$. Then X^n is a planar polynomial over $\mathrm{GF}(p)$ if and only if $n = 2$.*

For $q \equiv 0 \mod 2$ there is no planar polynomial over $\mathrm{GF}(q)$. This follows immediately from 3.7. A search for relative difference sets in E_{3^8} led to the following observations for planar monomials in general:[1]

Let $F := \mathrm{GF}(p^n)$ for some $2 \neq p \in \mathbb{P}$ and $2 \leq n \in \mathbb{N}$.

6.4 Theorem. *Let X^m and $X^{m'}$ be planar functions over $F \simeq \mathrm{GF}(p^n)$.*

(a) *$\mathfrak{P}(X^m)$ and $\mathfrak{P}(X^{m'})$ are isomorphic iff $m' \equiv mp^k \mod p^n$ for some k.*

(b) *$\mathfrak{P}(X^m)$ is a translation plane or a dual translation plane iff this plane is Desarguesian with $m \equiv 2p^k \mod p^n$ or a commutative twisted semifield plane with $m \equiv (p^a+1)p^k \mod p^n$ for $0 < a < n$ and $n/(n,a)$ odd.*

[1] in cooperation with U. Dempwolff. Submitted to “Innovations in Incidence Geometry” in 9/2006 [DR]

Note. *For every planar monomial X^m, the automorphism group of $\mathfrak{P}(X^m)$ contains the multiplicative group of F and the Galois group of F:*

- $Z := \{\varepsilon_a \colon (x,y) \mapsto (ax, a^m y);\ (x) \mapsto (ax) \mid a \in F^*\} \simeq F^*$
- $D := \langle \delta \colon (x,y) \mapsto (x^p, y^p);\ (x) \mapsto (x^p) \rangle \simeq \mathrm{C}_n$

The automorphism groups of the translation planes in question are known (for the semifield case, see [Alb59, Alb61, BJJ99]). For the remaining cases, it turns out that the automorphism group of $\mathfrak{P}(X^m)$ is just the obvious one:

6.5 Theorem. *Assume that $\mathfrak{P}(X^m)$ is not a translation plane. Then*

$$\mathrm{Aut}(\mathfrak{P}(X^m)) \simeq \Gamma\mathrm{L}(1,p^n) \cdot (F \times F)$$

For the proof of 6.4 and 6.5 a few lemmas are needed. The following lemma on Singer cycles is well known and follows from [Hup67, Satz 3.10], for example.

6.6 Lemma. *Let Z be a cyclic group of order $p^n - 1$ and V an n-dimensional $\mathrm{GF}(p)$-space and $D \colon Z \to \mathrm{GL}(V)$ a faithful representation.*

(a) *Let $D' \colon Z \to \mathrm{GL}(V)$ be an irreducible representation. Then D' is equivalent to a representation $D^k \colon Z \to \mathrm{GL}(V)$ for some $k \in \{0, \dots, p^n - 1\}$, where D^k is defined by $D^k(x) = D(x)^k$.*

(b) *Two irreducible representations D^k and D^ℓ are equivalent iff $\ell \equiv kp^a \mod p^n$ with $0 \le a < n$ suitable.*

6.7 Lemma. *Let $\mathfrak{P} = \mathfrak{P}(X^m)$ be a translation plane or a dual translation plane and $Z \le \mathrm{Aut}(\mathfrak{P})$ a cyclic group fixing the triangle $\{(0), (\infty), (0,0)\}$. Suppose further, that the action of Z on $L_\infty - \{(0), (\infty)\}$ is faithful and regular. Then:*

(a) *$\mathfrak{P}$ is Desarguesian or a commutative twisted semifield plane.*

(b) *Let $W \le \mathrm{Aut}(\mathfrak{P})_{L_\infty}$ be an elementary abelian, Z-invariant p-group such that $\mathrm{C}_W(x) = 1$ for $1 \ne x \in Z$ and W contains no translation. Assume that $W \times N$ acts regular on the affine points of $\mathfrak{P}$ and denote by D_W (D_N) the representation of Z on W (N). Assume that D_N is irreducible. Then $D_N \sim D_W^{p^\ell + 1}$ for some $0 \le \ell < n$.*

Proof. By [CM97, Cor. 5.12], $\mathfrak{P}$ is a semifield-plane. Using [Dem88] we see that $\mathfrak{P}$ twisted field plane which is even commutative by [DO68]. This proves (a).

For the proof of (b) let E be the group of elations with axis $L(0)$ and centre (∞). Denote by P the group of translations with centre (0). Then $T = N \times P$ is the translation group of order p^{2n} with respect to L_∞ and $N \times E$ is the dual translation group of order p^{2n} with respect to (∞). Moreover $V = ET$ has order p^{3n} and $H = \mathrm{Aut}(\mathfrak{P})_{(\infty),L_\infty} = KV$. Here $Z \leq K = H_{(0),(0,0)}$ is isomorphic to a subgroup of $\Gamma\mathrm{L}(1,p^n) \times \Gamma\mathrm{L}(1,p^n)$ (see [Alb59, Alb61] or [BJJ99]). Use the bar convention for homomorphic images modulo N. Then $\overline{V} = \overline{E} \oplus \overline{P}$ is a decomposition into Z-modules.

By assumption, W contains no translation, so $W \cap T = 1$ and $W \cap NE = 1$, because W acts regularly on the affine lines through (∞). Clearly, $W \cap V \neq 1$, so that $W \leq V$ follows from $W = [W, Z]$. Therefore $\overline{W}$ projects faithfully on $\overline{E}$ and $\overline{P}$. Hence $\overline{W} \simeq \overline{E} \simeq \overline{P}$ as Z-modules. The commutator induces a nontrivial, Z-invariant bilinear mapping $(\cdot,\cdot)\colon \overline{E} \times \overline{P} \to N$.

Claim. $D_N \sim D_{\overline{W}}^{p^\ell+1} \sim D_W^{p^\ell+1}$, ℓ suitable.

We sketch a Lie ring type argument which can be found for instance in G. Higmans work [Hig63, sec. 4] on Suzuki 2-groups:

By our assumptions, $D_{\overline{E}}$ is irreducible (as $D_{\overline{W}}$ is). Let z be a generator of Z. Let λ be an eigenvalue of $D_{\overline{E}}(z)$. Then $\overline{E} \simeq \mathrm{GF}(p)(\lambda) \simeq F$, in particular, $\langle \lambda \rangle = F^*$ and the eigenvalues of $D_{\overline{E}}(z)$ are the Galois-conjugates $\lambda^{p^i}, 0 \leq i < n$. In $\overline{E} \otimes_{\mathrm{GF}(p)} F$, we may choose a basis $u_0, \ldots, u_{n-1}$ such that $u_i z = \lambda^{p^i} u_i$; and we may furthermore suppose that $u_0, \ldots, u_{n-1}$ are conjugate over $\mathrm{GF}(p)$, so that the elements of $\overline{E}$ are exactly the elements $\sum \alpha^{p^i} u_i$ for $\alpha \in F$. Higman calls such a basis a "conjugate basis for $\overline{E}$ adapted to z". Of course, we can also choose a conjugate basis for $D_{\overline{P}}(z)$ adapted to z. The bilinear map $(\cdot,\cdot)$ extends to the tensored modules $\overline{E} \otimes_{\mathrm{GF}(p)} F$ and $\overline{P} \otimes_{\mathrm{GF}(p)} F$ and at least one product of an eigenvector for $D_{\overline{E}}(z)$ and one for $D_{\overline{P}}(z)$ is nontrivial as this mapping is nontrivial. This shows that $D_N(z)$ has eigenvalues which are conjugates of a $\lambda^{p^\ell+1}$, ℓ suitable. By (a) of lemma 6.6 this implies the claim. □

Using 6.3, Coulter and Matthews prove

6.8 Lemma ([CM97, Prop. 2.4]). *If X^m is a planar polynomial over $\mathrm{GF}(p^n)$ then there are precisely two $y \in \mathrm{GF}(p^n)$ with $y^m = 1$. And $m \equiv 2 \mod p-1$ and $(m, p^n - 1) = 2$.*

Now let $A := \mathrm{Aut}(\mathfrak{P}(X^m))$ and $A_0 = DZMN$ with D and Z as in the note on page 58. And remember that $M \times N = F \times F$.

6.9 Lemma. *Assume that $\mathfrak{P}$ is not a translation plane or a dual translation plane. Then*

(a) $A = \mathrm{Aut}(\mathfrak{P})$ *leaves L_∞ and (∞) fixed.*

(b) *N is the group of all central collineations with axis L_∞. In particular $N \trianglelefteq A$.*

(c) *$C_A(N) = \langle z_0 \rangle MN$, where z_0 is the unique involution in Z. In particular $M = [C_A(N), C_A(N)] \trianglelefteq A$.*

Proof. (a) is pretty easy: Assume that L_∞ or (∞) are not fixed by A, then suitable conjugates of N form the translation group with respect to a translation line or a translation point. But then $\mathfrak{P}$ is a translation plane or a dual translation plane. A contradiction.

For (b) let K be the group of central collineations with axis L_∞. Assume that $K - N$ contains a translation. Using the action of M we even find a translation $1 \neq \tau$ with centre (0). But then $\langle \tau^Z \rangle$ would be the full group of elations with respect to the flag $((0), L_\infty)$ and $\mathfrak{P}$ is a translation plane, a contradiction.

Therefore $K - N$ is a set of homologies. If this set is not empty we get (using the group action as before) a homology $1 \neq \kappa$ with centre $(0, 0)$. The involution z_0 is a homology with axis $L(0)$ and centre (0) since m is even by 6.8. Thus $z_0\kappa = \kappa z_0$ by 1.30. Moreover $[M \times N, \kappa] \leq C_A(N) \cap K = N$ and $[M \times N, z_0] = M$ which shows $[M, \kappa] = 1$. But then M woud fix the centre $(0, 0)$ of κ, a contradiction.

For (c) let $\gamma \in C_A(N)$. Replacing γ by a suitable element from γM we may assume that γ fixes the line $L(0)$. Again replacing γ by a suitable element from γN we may even assume that γ is a central collineation with axis $L(0)$. Therefore it's centre lies on L_∞.

Assume $\gamma \neq 1$. As γ fixes L_∞ the centre of γ lies on this line. If γ is an elation with centre (∞) then $\langle \gamma^Z \rangle$ is the full elation group with respect to the flag $((\infty), L(0))$ and $\mathfrak{P}$ is a dual translation plane, a contradiction. Thus γ is a homology. If the centre of γ is not (0) then $\beta = z_0 z_0^\gamma$ is a central collineation with axis $L(0)$ which is inverted by z_0 and z_0^γ. Hence β is an elation with centre (∞). But this case is ruled out already.

So (0) is the centre of γ and $C_A(N) = CMN$ with a group C of homologies with respect to the anti flag $((0), L(0))$. The group $C_A(N)/N$ is represented faithfully as a permutation group on $L_\infty - \{(\infty)\}$ and $CN/N \cap (CN/N)^{xN} = 1$ for $xN \in C_A(N)/N - CN/N$. Hence $C_A(N)/N$ is a Frobenius group with Frobenius kernel MN/N. This implies that C normalises $M = [MN, z_0]$ as $\langle z_0 \rangle \leq Z(C)$. If $\langle z_0 \rangle < C$ this group has on $L(0,0)$ an orbit containing (at least) three points of the form $(a_1, b), (a_2, b), (a_3, b)$, a contradiction to 6.8. □

With these tools, we will now turn to the proofs of 6.4 and 6.5.

Proof of 6.5. Use the bar convention for homomorphic images modulo N. The group $\bar{A}_0$ has a 2-transitive, faithful action on $L_\infty - \{(\infty)\}$. So

$$\mathrm{GL}(\bar{M}_{\mathrm{GF}(p)}) \gtrsim \bar{A}/\bar{M} \geq \bar{A}_0/\bar{M} \simeq \Gamma\mathrm{L}(1, p^n).$$

By [Kan80] $\bar{A} \simeq \mathrm{A}\Gamma\mathrm{L}(a, p^b)$ with $ab = n$. If $a = 1$, we are done.

Consider the case $a > 2$. The group $\bar{A}$ contains an involution xN such that $|\,\mathrm{C}_{L_\infty} xN| \notin \{1,\ 2,\ p^{n/2}+1,\ p^n+1\}$. As xN contains an involution, this involution is either a homology or planar, a contradiction.

Thus $a = 2$. By 6.9 we have $A/\,\mathrm{C}_A(N) \simeq \Gamma\mathrm{L}(2, p^{n/2})/\langle -\mathbb{1}\rangle$. Choose $B < A$ such that $B/\,\mathrm{C}_A(N) \simeq \mathrm{PSL}(2, p^{n/2})$. Then $z_0 MN \in B/MN \simeq \mathrm{SL}(2, p^{n/2})$. Set $B_0 = \mathrm{C}_B(z_0)$. As $M = [M, z_0]$ a Frattini argument shows $B = B_0 M$ and $B_0 \cap M = 1$. Moreover B_0 induces by conjugation the group $\mathrm{PSL}(2, p^{n/2})$ on N. Choose $u \in B_0$ of order 4 such that $u^2 = z_0$. Then $|\,\mathrm{C}_N(u)| > 1$ as the involutions in $\mathrm{PSL}(2, p^{n/2})$ are conjugate. As u normalizes M we see that $\langle u \rangle$ has on $L(0,0)$ an orbit of length 4 of the form $\{(a_1, b), \ldots, (a_4, b)\}$, contradicting 6.8. □

Proof of 6.4. Part (b) of the theorem follows directly from part (a) of lemma 6.9.

For the non trivial direction of part (a) of 6.4 assume that $\varphi\colon \mathfrak{P} = \mathfrak{P}(X^m) \to \mathfrak{P}' = \mathfrak{P}(X^{m'})$ is an isomorphism. By slight abuse of notation, the points and lines of $\mathfrak{P}'$ will be named as those of $\mathfrak{P}$. Because of transitivity of $A' = \mathrm{Aut}(\mathfrak{P}')$ we may assume that $L_\infty \varphi = L_\infty$ and that the points $(0), (0,0), (\infty)$ are mapped onto the corresponding points in $\mathfrak{P}'$. The isomorphism φ induces an isomorphism $\tau\colon A \to A'$; $\alpha \mapsto \varphi^{-1}\alpha\varphi$. Now set $N' = N\tau$, $M' = M\tau$ etc. The group Z acts on $M \times N$ and (via τ) on $M' \times N'$. Denote by $D_N, D_{N'}, D_M, D_{M'}$ the representations on the respective submodules. As τ is an isomorphism from ZMN to $Z'M'N'$, we have $D_N \sim D_{N'}$ and $D_M \sim D_{M'}$.

If $\mathfrak{P}'$ is not a translation plane, theorem 6.5 implies that $M \times N$ is characteristic in A and therefore $(M \times N)^\tau = M' \times N'$. Moreover $Z = \mathrm{C}_{DZ}([DZ, DZ])$ and hence Z' is the *unique* normal cyclic subgropup in $D'Z'$ of order $p^n - 1$, i.e. this group induces collineations of type ε_a on $M' \times N'$. Thus $D_N \sim D_M^m$ and $D_{N'} \sim D_{M'}^{m'}$ and therefore $D_M^m \sim D_M^{m'}$. By 6.6 we have $m \equiv mp^k \mod p^n$ for some k.

Now suppose that $\mathfrak{P}'$ is a translation plane. Then $\mathfrak{P}$ and $\mathfrak{P}'$ are commutative twisted field or Desarguesian planes. The group N' is still a group of $((\infty), L_\infty)$ elations, but the group M' may not be the one used in the definition of the planar function. Let $\tilde{M} \leq A'$ be the group used for the definition of the planar function. Then lemma 6.7 implies (with M and $\tilde{M}$ in the role of W) that $D_N \sim D_M^{p^l+1}$ and $D_{N'} \sim D_{\tilde{M}}^{p^{\ell'}+1}$. So $m \equiv (p^\ell + 1)p^k \mod p^n$ and $m' \equiv (p^\ell + 1)p^{k'} \mod p^n$.

As the plane $\mathfrak{P}'$ is a commutative semifield plane, it has a description as $\mathfrak{P}(F, p^a, p^{-a}, -1)$ with $0 \leq a < n$ and $n/(n, a) \equiv 1 \mod 2$. For $a > 0$, the plane is non-Desarguesian and $\mathfrak{P}'$ is Desarguesian if $a = 0$ (see [BJJ99] for details). Two such planes $\mathfrak{P}(F, p^a, p^{-a}, -1)$, $\mathfrak{P}(F, p^b, p^{-b}, -1)$ are isomorphic iff $a = b$ or $a = -b$. But planes of type $\mathfrak{P}(X^{p^k+1})$ are always translation planes if X^{p^k+1} is planar [DO68]. So $(p^\ell + 1) \equiv (p^{\ell'} + 1)p^c \mod p^n$ or $m' \equiv mp^d \mod p^n$, respectively, for some c, d. □

Note that theorem 6.4 also shows that the planes of Coulter and Matthews are not translation planes. But the techniques used for the proof are completely different from those of [CM97]. Theorem 5.7 shows that for order 81 the only planar monomials are equivalent to X^2 or the Coulter Matthews monomial.

Future work

In the present text, we discussed computational methods for the classification of projective planes. Here we will have a look at the possibilities for further work in this area. And as this thesis addresses theoretical and computational matters, naturally open questions also fall in both of these areas.

Theoretical problems

In section 2.1, a special representation Φ was introduced to find invariants for partial ordinary difference sets. A similar approach may also be of interest for relative difference sets. The question, whether Φ can be used to get information about the possible forbidden sets N is of particular interest. More generally, the study of matrix representations for more general classes of groups seems to be desirable in order to get restrictions on difference sets from the defining equation.

As the result from chapter 6 relates the isomorphism class of a projective plane to a notion of equivalence on monomials, it is tempting to ask if analogous results can be found for a more general class of planar polynomials. Another part of the theory of planar functions seems to be little studied. It is not yet known if there are planar functions, which are not defined on elementary abelian groups. Only a few results for general planar functions are known to the author [Hir90, Nak97, Nak93].

Computational issues

As seen in chapter 4, a key point for the generation of startsets is the knowledge of admissible signatures. Algorithm 4 is very crude as it always computes all permutations of a list and just gives up if the number of permutations seems too big. For special classes of groups, more sophisticated algorithms should be possible. Representations seem to be a very powerful tool for this purpose. One task could be to develop a variant of algorithm 5 to calculate signatures not only for ordinary but also for relative difference sets. The central part of algorithm 5 consists of the calculation of all elements of $\mathbb{Z}[\zeta]$ with non-negative coefficients and given modulus. Finding all $z \in \mathbb{Z}[\zeta]$ with $z\bar{z} = n \in \mathbb{N}$ seems to be a quite hard problem in number theory. The study of this problem using computational number theory may lead to some methods for a more effective calculation.

Searching for new planes

With the tools developed in this text –and the implementation– computational experiments may be undertaken to find new planes. When planes of order 25 are considered, the method from 5.1 can also be used for the other cases of the Dembowski-Piper classification. For order 27 Baer involutions are not available. In this case, one could search for difference sets which are fixed by a group automorphism α. Further, one would suppose that α has order 3 and fixes a subplane of order 3. In this case, it can be shown that for planes of type $\mathbf{DP}_b$, the subplanes on which α acts are also of type $\mathbf{DP}_b$ (for cases $\mathbf{DP}_d$, $\mathbf{DP}_f$ and $\mathbf{DP}_g$ the same should be true). So the search can start with generating difference sets of the subplanes.

As seen in chapter 5 relative difference sets of order 81 can be calculated if automorphisms are known. Interesting cases may be the automorphism groups of the semifield planes of order 81 as calculated by U. Dempwolff [Dem]. Acting on E_{81^2}, some of these groups may have subgroups which also admit an operation on another (possibly non-Desarguesian) projective plane. So using these groups for orbit-wise generation of difference sets looks quite promissing.

Appendix A

The planes of order 16 and type $\mathbf{DP}_b$

The following table contains the 590 groups of order 256 which admit relative difference sets of type $\mathbf{DP}_b$.

The column labels "Des", "Semi 2", "Semi 4" and "Mathon" stand for the Desarguesian plane, the semifield planes with kernel 2 and 4, respectively, and the Mathon plane. Note that a group acts on the Mathon plane if and only if it acts on the dual Mathon plane. So there is no extra column for the dual Mathon plane. And, of course, a mark means that there is an action on the corresponding plane. Groups which are not in the table do not admit a relative difference set of type $\mathbf{DP}_b$.

The groups are numbered as in the small groups library of `GAP`:

```
There are 56092 groups of order 256.
They are sorted by their ranks.
   1 is cyclic.
   2 - 541 have rank 2.
   542 - 6731 have rank 3.
   6732 - 26972 have rank 4.
   26973 - 55625 have rank 5.
   55626 - 56081 have rank 6.
   56082 - 56091 have rank 7.
   56092 is elementary abelian.
```

Group number 6732 is C_4^4. From this we get

A.1 Corollary. *Let* $\mathfrak{P}$ *be a projective plane* $\mathbf{DP}_b$ *and order* 16*. Let* G *be a* *group of order* $|G| = 256$ *operating as a quasiregular collineation group of* $\mathfrak{P}$. *Then*

- *G has rank at most* 5.
- *G acts on at most two of the following three kinds of planes: Desarguesian plane, semifield plane (with kernels* GF(2) *or* GF(4)*), Mathon plane.*

The projective planes of order 16 and type $\mathbf{DP}_b$

Nr.	Des	Semi 2	Semi 4	Mathon
296	●	●	●	
331	●			●
420				●
843		●	●	●
855	●	●		
874				●
876				●
909				●
938		●	●	
947	●	●		
956				●
961				●
963		●	●	
978				●
980				●
985				●
1001				●
1038				●
1052				●
1053				●
1060		●	●	
1066				●
1081				●
1086		●	●	
1101				●
1104				●
1108				●
3322				●
4509	●			●
5287				●
5688		●	●	
5848	●	●	●	
6732	●			
6738			●	
6753		●		
6756		●		
6760		●		
6769		●		
6774			●	
6775		●		
6781		●	●	
6785		●		
6792		●		
6794			●	
6800		●		
6807		●		
6814		●	●	
6817	●			
6821		●	●	
6822		●		
6838			●	
6842		●	●	
6843		●		
6844		●		
6848		●	●	
6851		●		
6852		●		
6873		●		
6897		●		
6916		●		
6917		●		
6919		●	●	
6920		●		
6922		●		
6938		●	●	
6942		●		
6943		●		
6949		●	●	
6952		●	●	
6964		●		
6966		●		
6973		●		
6988		●		
6991			●	
6994		●		
6997		●		
7012		●	●	
7030		●		
7036		●		
7039		●		
7043		●		
7045		●		
7046			●	
7048		●		

Nr.	Des	Semi 2	Semi 4	Mathon
7049		●		
7050		●		
7053		●		
7057		●		
7071		●		
7079		●		
7080		●		
7082		●	●	
7093		●		
7101		●		
7103		●	●	
7109		●		
7111		●		
7114		●		
7121		●		
7130		●		
7139		●		
7143		●	●	
7148		●		
7149			●	
7150		●		
7151		●		
7152		●	●	
7156			●	
7162		●	●	
7167		●		
7174		●		
7179		●		
7180		●		
7191		●		
7202		●		
7205		●		
7211		●		
7214		●		
7224		●		
7226		●		
7227		●		
7233			●	
7235		●		
7238		●		
7240		●		
7258		●		

Nr.	Des	Semi 2	Semi 4	Mathon
7268		●		
7272			●	
7274		●		
7284		●		
7296		●		
7306		●		
7308		●		
7316		●		
7318		●		
7334		●		
7344		●		
7366			●	
7382		●		
7402		●		
7423		●		
7429	●			
7438		●	●	
7446		●		
7447		●		
7453		●		
7454		●	●	
7458		●		
7459	●	●	●	
7460		●		
7465		●		
7471		●	●	
7473		●		
7477		●	●	
7478		●		
7489		●		
7490		●		
7498	●			
7499		●		
7519		●		
7526			●	
7538		●		
7540		●		
7542		●		
7549		●		
7562	●			
7581		●		
7583		●		

Nr.	Des	Semi 2	Semi 4	Mathon
7585		●		
7586		●		
7587		●	●	
7589		●		
7593		●		
7596			●	
7602			●	
7622		●	●	
7626		●	●	
7636		●		
7638		●		
7651			●	
7652	●			
7656		●	●	
7691	●	●		
7697	●			
7698		●		
7767		●		
7769		●		
7775		●	●	
7779		●		
7788		●		
7792		●		
7838		●		
7839		●	●	
7851		●		
7855		●		
7860		●		
7866		●		
7869		●	●	
7872		●		
7926		●		
7930		●		
7938		●		
7950		●		
7963		●		
7980		●		
7982		●		
7988		●		
7996		●		
7999		●	●	
8001			●	

Nr.	Des	Semi 2	Semi 4	Mathon
8016			●	
8017		●		
8024		●		
8030		●		
8032		●		
8036			●	
8039		●		
8040		●		
8041			●	
8044			●	
8048		●		
8063		●		
8073		●		
8074		●		
8077		●	●	
8082		●	●	
8084		●		
8085		●	●	
8086		●	●	
8087		●		
8092		●		
8096		●	●	
8104			●	
8107		●	●	
8109		●		
8116		●	●	
8121		●		
8131		●		
8134		●		
8152		●		
8154		●		
8172		●		
8179			●	
8181		●		
8198		●		
8227		●		
8239		●	●	
8241		●	●	
8244		●		
8306		●		
8335		●		
8337		●		
8348		●		
8355		●		
8362		●		
8370		●		
8402		●		
8423		●		
8425	●	●		
8488		●		
8491		●		
8498		●		
8509		●		
8518		●		
8521		●		
8524		●		
8530		●		
8546		●		
8561		●		
8562		●		
8569		●		
8584		●		
8589		●		
8651		●		
8671		●		
8673		●		
8679		●	●	
8680		●		
8686		●		
8687		●	●	
8691		●		
8695		●		
8708		●		
8712		●		
8717		●		
8728		●		
8735		●		
8740		●		
8748		●		
8750		●	●	
8754		●		
8755		●		
8766		●		
8767		●		
8778		●		
8781		●		
8782			●	
8787		●		
8801		●		
8805		●		
8835		●		
8837	●	●		
8842		●	●	
8845		●	●	
8846		●	●	
8848		●		
8849		●		
8850		●		
8855		●		
8860		●		
8875		●		
8876		●		
8878		●		
8879		●		
8884			●	
8891		●		
8906		●		
8921		●		
8923			●	
8925		●		
8930		●		
8952		●		
8987		●		
8989		●		
8991	●			
8995		●		
8997		●		
9010	●			
9019		●		
9021		●		
9025		●		
9028		●		
9029		●		
9046		●		
9051		●	●	
9053		●		

Nr.	Des	Semi 2	Semi 4	Mathon
9054		●		
9056		●		
9063		●		
9069		●		
9070		●		
9074		●		
9081		●	●	
9083		●		
9084		●		
9096		●		
9097		●	●	
9098		●	●	
9100	●	●		
9101		●		
9104			●	
9110	●		●	
9116		●		
9118		●		
9125		●		
9126		●		
9127		●		
9128		●	●	
9131		●		
9138		●		
9143		●		
9150		●		
9151	●			
9153		●		
9154			●	
9155		●		
9156			●	
9158			●	
9160		●		
9162		●		
9164		●		
9166		●		
9167		●		
9168		●	●	
9172		●		
9173			●	
9174	●	●	●	
9176		●		
9182		●		
9189		●		
9191		●	●	
9192		●		
9204		●		
9208		●	●	
9209		●		
9213		●		
9218		●		
9219		●		
9220			●	
9223		●		
9224		●		
9225		●		
9227		●		
9229		●		
9231		●		
9236		●		
9269		●	●	
9281		●		
9364			●	
9375		●		
9376		●		
9377		●		
9394		●		
9395		●		
9397		●		
9398		●		
9400		●		
9401		●		
9424		●		
9432		●		
9436		●		
9441		●		
9448		●		
9470		●		
9471		●		
9473		●		
9481		●		
9512		●		
9541		●		
9542		●		
9553		●		
9558		●		
9564		●		
9582		●		
9586		●		
9598			●	
9599		●		
9613		●		
9617		●	●	
9618		●	●	
9674		●	●	
9675		●		
9676		●		
9683		●		
9697		●		
9698		●		
9699		●		
9701		●		
9704		●		
9709		●		
9714		●		
9720		●		
9722		●		
9727		●		
9732		●		
9733			●	
9738		●		
9740			●	
9745		●		
9748		●		
9754		●		
9757		●		
9758		●		
9764		●		
9771		●		
9772		●		
9778			●	
9780		●		
9784		●		
9794		●		
9801		●		
9814		●		

Nr.	Des	Semi 2	Semi 4	Mathon
9815		●		
9828		●		
9831		●		
9837		●		
9862		●	●	
9868		●		
9877			●	
9878		●		
9885		●		
9893		●	●	
9896		●		
9900		●		
9903		●		
9906		●		
9912	●			
9919		●		
9926			●	
9930		●	●	
9932		●		
9934		●		
9935		●		
9936		●		
9938		●		
9946		●		
9947		●		
9959		●		
9960		●		
9963		●		
9967		●		
9971		●		
9976		●		
9978		●		
9981		●		
9982		●		
9983		●		
9984			●	
9986		●		
9988		●		
9990		●		
9991		●		
10009		●		
10020		●		

Nr.	Des	Semi 2	Semi 4	Mathon
10022		●		
10024		●		
10030		●		
10039			●	
10041		●	●	
10042		●	●	
10043		●		
10060		●	●	
10066	●			
10069		●		
10073		●		
10100			●	
10116		●		
10120		●		
10142		●		
10150		●		
10166		●		
10173		●	●	
10179		●		
10190		●		
10197		●		
10198			●	
10200		●		
10206		●		
10207		●		
10234			●	
10244			●	
10246		●		
10254		●		
10263		●		
10266		●		
10268			●	
10269		●	●	
10272		●	●	
10277		●	●	
10283		●		
10285		●		
10287		●		
10294		●		
10295		●	●	
10296		●		
10297	●	●	●	
10313				●

Nr.	Des	Semi 2	Semi 4	Mathon
10437		●	●	
10528				●
10572				●
10636				●
10655	●	●		
10730		●		
10734			●	●
10739				●
10785				●
10796				●
10808				●
13317				●
13780				●
14204				●
14819				●
14829				●
27067		●		
27101		●		
27106		●		
27131		●		
27333		●	●	
27534		●	●	
27588		●		
27677		●		
27848			●	
27880		●		
27887		●		
27916		●		
27928		●		
27932			●	
29622	●			
29676		●		
29677		●		
45194		●		
45224		●		
45244		●		
45253		●		
45257		●		
45259		●	●	
45274	●	●	●	
53237				●
53830				●
53959				●

Appendix B

Some GAP programs

This appendix presents some example GAP programs to illustrate the implementation of the methods described in the previous chapters. It is also meant as a demonstration of implementations using the GAP-package “RDS”.

The listings are presented to exhibit the underlying ideas. The programs actually used contain parts producing visual feedback and data files for later use. These parts are not included. For more documentation of the functions used, see [GAP, Röd06].

B.1 A simple example: Case DP_d

As seen in section 3.4, we do only have to look for difference sets in the cyclic group of order 255. Calculating the admissible signatures with respect to the normal subgroup U of index 3 gives:

```
gap> CosetSignatures(255,15,255/3,5,16,1);
[ [ 4, 4, 8 ] ]
```

So we may assume that the difference set we search contains 8 elements from U and 4 from each other coset modulo U. The following program finds all relative difference sets in C_{255}.

Relative difference sets are represented as lists of integers. An ordering of the elements of G is defined by `PermutationRepForDiffsetCalculations`. When adding elements to a partial difference set, this ordering is used. Only elements larger then the last entry of the partial difference set are added (this is done by `ExtendedStartsets`). As the cosets modulo U may not be compatible with the ordering defined on G, this ordering must be disregarded when changing the coset modulo U. At this point, the function `ExtendedStartsetsNoSort` is used.

```
LoadPackage("RDS");
k:=16;
lambda:=1;
groupOrder:=255;
forbiddenGroupOrder:=15;
maxtest:=10^7;
G:=CyclicGroup(groupOrder);
Gdata:=PermutationRepForDiffsetCalculations(G);;
MakeImmutable(Gdata);
N:=First(NormalSubgroups(G),i->Size(i)=forbiddenGroupOrder);
Np:=GroupList2PermList(Set(N),Gdata);
globalSigData:=[];
normals:=Filtered(NormalSubgroups(Gdata.G),
                 n->Size(n) in [2..groupOrder-1]);
sigdat:=SignatureDataForNormalSubgroups(normals,globalSigData,N,Gdata,
                                       [k,1,maxtest,true]);;
U:=First(sigdat,s->s.sigs=[ [ 4, 4, 8 ] ]).subgroup;
cosets:=RightCosets(G,U);;
U1:=cosets[2];
U2:=cosets[3];
Up:=GroupList2PermList(Set(U),Gdata);
ssets:=List(Difference(Up,Np),i->[i]);
comps:=Difference(Up,Np);;
ssets:=ReducedStartsets(ssets,[Gdata.Aac],sigdat,Gdata.diffTable);
repeat
    ssets:=ExtendedStartsets(ssets,comps,Np,7,Gdata);
    ssets:=ReducedStartsets(ssets,[Gdata.Aac],sigdat,Gdata.diffTable);;
until ssets=[] or Size(ssets[1])=7;
comps:=Difference(GroupList2PermList(Set(U1),Gdata),Np);
ssets:=ExtendedStartsetsNoSort(ssets,comps,Np,11,Gdata);
ssets:=ReducedStartsets(ssets,[Gdata.Aac],sigdat,Gdata.diffTable);;
repeat
    ssets:=ExtendedStartsets(ssets,comps,Np,11,Gdata);
    ssets:=ReducedStartsets(ssets,[Gdata.Aac],sigdat,Gdata.diffTable);;
until ssets=[] or Size(ssets[1])=11;
comps:=Difference(GroupList2PermList(Set(U2),Gdata),Np);
ExtendedStartsetsNoSort(ssets,comps,Np,15,Gdata);
repeat
    ssets:=ExtendedStartsets(ssets,comps,Np,15,Gdata);
    ssets:=ReducedStartsets(ssets,[Gdata.Aac],sigdat,Gdata.diffTable);;
until ssets=[] or Size(ssets[1])=15;
```

B.2 Case $\mathbf{DP}_b$

In case $\mathbf{DP}_b$, the difference set to find is a system of representatives of the forbidden normal subgroup. This property is used for the generation of startsets. As a consequence, special methods are implemented to find difference sets of type $\mathbf{DP}_b$. These methods are listed in section B.2.1. For $n = 16$, relative difference sets of type $\mathbf{DP}_b$ occur in several groups. Tests for the isomorphism class of these planes are done by reconstructing the projective plane from the difference set and then testing invariants and isomorphisms, if needed. A program for reconstruction and testing is given in section B.2.3. Section B.2.2 has a program for finding relative difference sets of type $\mathbf{DP}_b$ with order $n = 16$ using the methods of B.2.1 and the "RDS" package.

B.2.1 Special methods

```
NewStartSets_potversion:=function(ssets,cosets,forbidden,aim,data)
local returnsets, set, lcomps, local_cosets, min, comps;
if ssets=[] or aim<=Size(ssets[1]) or Size(Set(ssets,Size))>1
  then
   Error("wrong parameters");
  fi; returnsets:=[];
for set in ssets
 do
  lcomps:=Set(Flat(cosets));
  lcomps:=RemainingCompletionsNoSort(set,lcomps,forbidden,data);
  local_cosets:=List(cosets,i->Intersection(i,lcomps));
  local_cosets:=Filtered(local_cosets,i->i<>[]);
  if lcomps<>[] and Size(local_cosets)+Size(ssets[1])=aim
   then
    min:=Minimum(List(local_cosets,Size));
    comps:=First(local_cosets,i->Size(i)=min);
    Append(returnsets,List(comps,c->UnionSet(set,[c])));
   fi;
 od;
return Set(returnsets);
end;

MathonIsomorphism:=function(fixpoint,infline,data,mathon_quad,mathon_data)
   local   blocks,  points,  wlogpoint,  block,  point,  point2,
           iso;
if not Size(ProjectiveClosureOfPointSet(Set(mathon_quad),16,mathon_data))
   =Size(data.blocks)
   then
    Error("Mathon plane must be given by generating quadrangle");
fi;
blocks:=Filtered(data.blocks,b->fixpoint in b);
RemoveSet(blocks,infline);
points:=Difference(data.points,infline);
wlogpoint:=First(points,p->not p in infline);
RemoveSet(points,wlogpoint);
```

```
for block in blocks
  do
    for point in Filtered(block,p->p<>fixpoint)
      do
        for point2 in Difference(points,block)
          do
            quad:=Concatenation([fixpoint,wlogpoint],[point,point2]);
            iso:=IsomorphismProjPlanesByGenerators(mathon_quad,
                                     mathon_data, quad,data);
            if iso<>fail
             then
              return iso;
            fi;
        od;
    od;
od;
return fail;
end;
```

B.2.2 A program for finding difference sets of type $\mathbf{DP}_b$

The file `functions_b.gap` should contain the functions from B.2.1. The file `mathondata.gap` is supposed to contain the Mathon plane in the variable *"mathondata"* and a generating quadrangle of the Mathon plane as *"mathon_quadrangle"*. This data is used for isomorphism testing (section B.2.3). The Function `SignatureDataForNormalSubgroups` calculates admissible signatures and stores them *"globalSigData"* so that they can be reused when the next group is processed (see 1.20 and the note on page 16).

The program uses the group of (anti-)automorphisms of G for the reduction process. By lemma 1.17, the consequence is to treat difference sets as equivalent, if they induce dual planes. On the other hand, a group acting on a projective plane defined by a relative difference set does also act on the dual plane, as the forbidden sets are always closed under inversion (1.13). So we do not loose information here, but must keep in mind that planes always come with their duals.

```
LoadPackage("RDS");
Read("functions_b.gap");
Read("mathondata.gap");
groupOrder:=256;
forbiddenGroupOrder:=16;
k:=16;
lambda:=1;
maxtest:=10^7;
for case in [1..NrSmallGroups(groupOrder)]
```

```
 do
isgoodgroup:=true;
foundsets:=[];
if not IsBound(results)
   then
    results:=[];
fi;
global_time_tmp:=Runtime();
G:=SmallGroup(groupOrder,case);
if Number(Set(G),i->Order(i)=2) >= forbiddenGroupOrder
   then
    isgoodgroup:=false;
    Print("Too many involutions.\n");
else
    n16s:=Filtered(NormalSubgroups(G),n->Order(n)=16);
    if n16s=[]
       then
        isgoodgroup:=false;
    else
        n16s:=Filtered(n16s,n->ForAll(Difference(G,n),g->Order(g)<>2));
    fi;
    if n16s=[]
       then
        isgoodgroup:=false;
    fi;
fi;
  if isgoodgroup
   then
    Gdata:=PermutationRepForDiffsetCalculations(G);;
  forbiddenGroups:=n16s;
  if not IsBound(globalSigData)
   then
    globalSigData:=[];
fi;
for N in forbiddenGroups
do
Normals:=Filtered(NormalSubgroups(G),i->
         (not (i=G or IsTrivial(i)) and Index(G,i)<17));
  normalSubgroupsData:=SignatureDataForNormalSubgroups(Normals,
                                 globalSigData,N,
                                 Gdata,[k,1,maxtest,true]);;
if normalSubgroupsData=fail or ForAny(normalSubgroupsData,i->i.sigs=[])
   then
    isbadforbiddengroup:=true;
else
    isbadforbiddengroup:=false;
fi;
  if not isbadforbiddengroup
```

```
then
   niceone:=First(normalSubgroupsData,d->d.sigs=[[8,8]]);
 if niceone<>fail
    then
     U:=niceone.subgroup;
     Usig:=niceone.sigs[1];
     Up:=First(niceone.cosets,c->1 in c);
     Ucosets:=niceone.cosets;
 else
     niceone:=First(normalSubgroupsData,d->d.sigs=[[4,4,4,4]]);
     if niceone<>fail
        then
         U:=niceone.subgroup;
         Usig:=niceones.sigs[1];
         Up:=First(niceone.cosets,c->1 in c);
         Ucosets:=niceone.cosets;
     else
         #### if the above does not work, this works:
         niceones:=Filtered(normalSubgroupsData,d->Size(d.sigs)=1
                            and Index(G,d.subgroup)>=2
                            and Size(Set(d.sigs[1]))<=2);
         niceones:=Filtered(niceones,d->1 in
                   List(Collected(d.sigs[1]),i->i[2])
                   or Size(Set(d.sigs[1]))=1 or Size(d.sigs[1])=2);
         max:=Maximum(List(niceones,n->Maximum(n.sigs[1])));
         niceones:=Filtered(niceones,n->Maximum(n.sigs[1])=max);
             if Size(niceones)=1
            then
             U:=niceones[1].subgroup;
             Usig:=niceones[1].sigs[1];
             Up:=First(niceones[1].cosets,c->1 in c);
             Ucosets:=niceones[1].cosets;
         else
             if ForAny(niceones,n->Set(n.sigs[1])=[max])
                then
                 niceones:=Filtered(niceones,n->
                                    Set(n.sigs[1])=[max])[1];
             elif ForAny(niceones,n->(Number(n.sigs[1],i->i=max)=1
                                      and Size(Set(n.sigs[1]))=2))
               then
                 niceones:=Filtered(niceones,n->
                                    (Number(n.sigs[1],i->i=max)=1
                                     and Size(Set(n.sigs[1])=2)));
             else
                 max:=Minimum(List(niceones,n->Size(n.sigs[1])));
                 niceones:=Filtered(niceones,n->Size(n.sigs[1])=max);
                 max:=Maximum(List(niceones,n->
                              Size(Intersection(N,n.subgroup))));
                niceones:=Filtered(niceones,n->
                                Size(Intersection(N,n.subgroup))=max);
            fi;
            U:=niceones[1].subgroup;
            Usig:=niceones[1].sigs[1];
            Up:=First(niceones[1].cosets,c->1 in c);
            Ucosets:=niceones[1].cosets;
        fi;
    fi;
fi;
  aims:=Reversed(SortedList(Usig));
aims[1]:=aims[1]-1;
for i in [2..Size(aims)]
  do
    aims[i]:=Sum(aims{[1..i]});
od;
aims:=Filtered(aims,i->i<=k*1/2);
Np:=GroupList2PermList(Set(N),Gdata);
Ncosets:=Set(RightCosets(Gdata.G,N),g->
             GroupList2PermList(Set(g),Gdata));
RemoveSet(Ncosets,Np);
  Ucosets:=niceone.cosets;
autlist:=[Intersection(Stabilizer(Gdata.Ai,Np,OnSets),
          Intersection(List(Ucosets,c->
                            Stabilizer(Gdata.Ai,c,OnSets))))];
  for aimpos in [1..Size(aims)]
  do
    aim:=aims[aimpos];
    Ncosetscomps:=List(Ncosets,i->
                       Intersection(i,Ucosets[aimpos]));
    if aimpos=1
       then
        ssets:=Set(Flat(Ncosetscomps),i->[i]);
        ssets:=ReducedStartsets(ssets,autlist,
                                normalSubgroupsData,
                                Gdata.diffTable);;
    fi;
    while (ssets<>[] and Size(ssets[1])<aim)
      do
        ssets:=NewStartSets_potversion(ssets,Ncosetscomps,
                                       Np,aim,Gdata);
        ssets:=ReducedStartsets(ssets,autlist,
                                normalSubgroupsData,
                                Gdata.diffTable);;
    od;
od;
  if ssets<>[]
   then
```

```
        comps:=Difference(Union(Ucosets{[Size(aims)+1..Size(Usig)]}),Np);
        foundsets:=[];
        counter:=1;
        ssets:=ExtendedStartsetsNoSort(ssets,comps,Np,k,Gdata);
        for set in ssets
          do
            setcomps:=RemainingCompletions(set,comps,Np,Gdata);
            Append(foundsets,AllDiffsets(set,setcomps,k-1,Np,Gdata));
        od;
         if foundsets<>[]
          then
           foundsets:=ReducedStartsets(
                             Set(foundsets,i->Difference(i,[1])),
                             [Stabilizer(Gdata.Ai,Np,OnSets)],
                             normalSubgroupsData,Gdata.diffTable
                                       );
           Apply(foundsets,i->Union(i,[1]));
           Read("build_n_test.gap");
        fi;
    fi;
fi; #if not isbadforbiddengroup
od; #for  N in forbiddenGroups
fi; # <\if isgoodgroup>
od; # <\for case in [1..NrSmallGroups(groupOrder)]
```

B.2.3 Reconstruction and isomorphism testing

The following program is contained in a file called “build_n_test.gap” and is called from the program of section B.2.2. Note that the translation planes of order 16 are known [DR83, Rei84]. And the translation planes of order 16 have pairwise different Fano-invariants [Roy]. So identification of the constructed plane is done using the list “fanoparameters”. If the Fano-invariant matches the one of the Mathon plane, an isomorphism is constructed explicitly. For this test, the Mathon plane must be stored as “mathondata” and a generating quadrangle of the Mathon plane must be known (called “mathon_quadrangle”).

```
 fanoparameters:=[[1/2*[2611200],"DESARGUESIAN","des"],
 [2/7*[426720,1161216,4569600],"SEMI2","semi2"],
 [2/7*[856128,1666560,4569600],"SEMI4","semi4"],
 [2/7*[900480,953400,1989120],"HALL","hall"],
 [2/7*[900480,1041600,4569600],"dualHALL","dhall"],
 [2/7*[520044,1268736,2161152],"LMRH","lmrh"],
 [2/7*[515424,778176,4569600],"dualLMRH","dlmrh"],
 [2/7*[1001616,1268736,2161152],"JOWK","jowk"],
 [2/7*[962976,1257984,4569600],"dualJOWK","djowk"],
 [2/7*[586572,1021440,2161152],"MATHON? ",0],
 [2/7*[606480,702912,2161152],"dualMATHON?",0]];
 mathon_parameters:=2/7*[586572,1021440,2161152];
for diffnumber in [1..Size(foundsets)]
  do
istransplane:=false;
diff:=PermList2GroupList(foundsets[diffnumber],Gdata);
trans:=Set(G,g->Set(diff*g));
parclasses:=Set(trans,t->Set(N,n->Set(t*n)));;
Apply(parclasses,c->Set(c,i->GroupList2PermList(i,Gdata)));
rawlines:=Set(trans,l->Set(GroupList2PermList(l,Gdata)));
lines:=StructuralCopy(rawlines);
for line in lines
  do
    AddSet(line,groupOrder+Position(parclasses,
                                    First(parclasses,p->line in p)));
od;
rawnewlines:=Set(RightCosets(G,N),Set);
rawnewlines:=Set(rawnewlines,l->GroupList2PermList(l,Gdata));
newlines:=StructuralCopy(rawnewlines);
fixpoint:=groupOrder+Size(parclasses)+1;
Apply(newlines,l->Concatenation(l,[fixpoint]));
  points:=[1..groupOrder+Size(parclasses)+1]; #=256+16+1=273
infline:=[groupOrder+1..Size(points)];
blocks:=Set(Concatenation([lines,newlines,[infline]])); #add \ell_\infty.
rawblocks:=Set(Concatenation([rawlines,rawnewlines]));
planedata:=ElationPrecalc(blocks);;
pointsforfano:=[fixpoint,
                First(points,p->not p in infline),
                First(infline,p->not p=fixpoint)];
fanoinvar:=NrFanoPlanesAtPoints(pointsforfano,planedata);
Print(First(fanoparameters,i->i[1]=Set(fanoinvar,j->j[2]))[2],"\n");
desabb:=First(fanoparameters,i->i[1]=Set(fanoinvar,j->j[2]))[3];
if Set(fanoinvar,i->i[2])=mathon_parameters
 then
  if MathonIsomorphism(fixpoint,infline,planedata,
                       mathon_quadrangle,mathondata)<>fail
     then
      Print("Yes!\n");
      if desabb=0
         then
          desabb:="mathon";
      fi;
  else
      Print("No!\n");
      if desabb=0
         then
          desabb:="strange";
      fi;
  fi;
else
  transgroup:=Group(AllElationsAx(infline,planedata));
  if NrMovedPoints(transgroup)=256 and Transitivity(transgroup)=1
     then
      istransplane:=true;
      Print("Translation Plane!\n");
  fi;
fi;
Gac:=Action(Gdata.G,Gdata.Glist,OnRight);
if not istransplane and not desabb="mathon"
 then
  Print("Not a translation plane. Testing dual:\n");
  dualGac:=Action(Gac,rawblocks,OnSets);
  dualplane:=DualPlane(blocks);;
  dualblocks:=dualplane.blocks;;
  line1:=dualplane.image[fixpoint];
  line2:=Random(dualplane.image{Difference(infline,[fixpoint])});
  dualplanedata:=ElationPrecalc(dualblocks);;
  dualtransgroup:=Group(AllElationsAx(line1,dualplanedata));
  dualfanoinvar:=NrFanoPlanesAtPoints(List(Orbits(dualGac,[1..273]),
                                           Representative),dualplanedata);
  Print(First(fanoparameters,i->i[1]=Set(dualfanoinvar,j->j[2]))[2],"\n");
  dualdesabb:=First(fanoparameters,i->i[1]=Set(dualfanoinvar,j->j[2]))[3];
  if Set(dualfanoinvar,i->i[2])=mathon_parameters
   then
    if MathonIsomorphism(First(Orbits(dualGac,[1..Size(dualblocks)]),
                               o->Size(o)=1)[1],
                         line1,dualplanedata,mathon_quadrangle,
                         mathondata)<>fail
       then
         Print("Yes!\n");
         if dualdesabb=0
           then
             dualdesabb:="dualmathon";
             desabb:="dmathon";
         fi;
     else
         Print("No!\n");
         if dualdesabb=0
            then
             dualdesabb:="strange";
         fi;
     fi;
   fi;
fi;
od;
```

Bibliography

[Alb59] A. Adrian Albert, *On the collineation groups associated with twisted fields*, Calcutta Math. Soc., Golden Jubilee Commemorat. Vol. (1958–59) Part 2, 1959, pp. 485–497.

[Alb61] ______, *Isotopy for generlized twisted fields*, Anais Acad. Brasil. Ci. **33** (1961), 265–275.

[Bec04] Paul E. Becker, *Investigation of solvable (120,35,10) difference sets*, Journal of Combinatorial Designs **13** (2004), no. 2, 79–107.

[BJJ99] M. Biliotti, V. Jha, and N. Johnson, *The collineation groups of the generalized twisted field planes*, Geometriae Dedicata **76** (1999), no. 1, 97–126.

[Bru55] Richard H. Bruck, *Difference sets in a finite group*, Transactions of the American Mathematical Society **78** (1955), 464–481.

[CM97] Robert S. Coulter and Rex W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Designs Codes and Cryptography **10** (1997), no. 2, 167–184.

[Dem] Ulrich Dempwolff, *The semifield planes of order* 81, to appear.

[Dem68] Peter Dembowski, *Finite geometries*, Ergebnisse der Mathematik und ihrer Genzgebiete, no. 44, Springer Verlag, Berlin Heidelberg, 1968.

[Dem88] Ulrich Dempwolff, *A characterization of the generalized twisted field planes*, Archiv der Mathematik **50** (1988), no. 5, 477–480.

[DO68] Peter Dembowski and T.G. Ostrom, *Planes of order n with collineation groups of order n^2*, Mathematische Zeitschrift **103** (1968), 239–258.

[DP67] Peter Dembowski and Fred Piper, *Quasiregular collineation groups of finite projective planes*, Mathematische Zeitschrift **99** (1967), 53–75.

[DR] Ulrich Dempwolff and Marc Röder, *On finite projective planes defined by planar functions*, submitted to Innovations in Incidence Geometry.

[DR83] Ulrich Dempwolff and Arthur Reifart, *The classification of the translation planes of order 16. I*, Geometriae Dedicata **15** (1983), 137–153.

[Gan76] Michael J. Ganley, *On a paper of Dembowski and Ostrom*, Archiv der Mathematik **27** (1976), 93–98.

[GAP] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, `http://www.gap-system.org`.

[GJ03a] Dina Ghinelli and Dieter Jungnickel, *Finite projective planes with a large abelian group*, Surveys in combinatorics (Cambridge), London Mathematical Society Lecture Notes, no. 307, Cambridge University Press, 2003, pp. 175–237.

[GJ03b] ______, *On finite projective planes in Lenz-Barlotti class at least I.3*, Advances in Geometry **Special Issue** (2003), 28–48.

[Glu90] David Gluck, *Affine planes and permutation polynomials*, Discrete Mathematics **80** (1990), no. 1, 97–100.

[GM75] Michael J. Ganley and Robert L. McFarland, *On quasiregular collineation groups*, Archiv der Mathematik **26** (1975), 327–331.

[GS75] Michael J. Ganley and Edward Spence, *Relative difference sets and quasiregular collineation groups*, Journal of Combinatorial Theory, Series A **19** (1975), 134–153.

[Hig63] Graham Higman, *Suzuki 2-groups*, Illinois Journal of Mathematics **7** (1963), 79–96.

[Hir89] Yutaka Hiramine, *A conjecture on affine planes of prime order*, Journal of Combinatorial Theory, Series A **52** (1989), no. 1, 44–50.

[Hir90] ———, *On planar functions*, Journal of Algebra **133** (1990), no. 1, 103–110.

[Hir04] ———, *Relative difference sets in Alt(5)*, Journal of Combinatorial Theory, Series A **110** (2004), no. 2, 179–191.

[HP73] Daniel R. Hughes and Fred C. Piper, *Projective planes*, Graduate Texts in Mathematics, no. 6, Springer Verlag, Berlin Heidelberg, 1973.

[Hug55] Daniel R. Hughes, *Planar division neo-rings*, Ph.D. thesis, University of Wisconsin, Madison, 1955.

[Hup67] Bertram Huppert, *Endliche Gruppen I*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, no. 134, Springer Verlag, Berlin Heidelberg, 1967.

[Joh87] Norman L. Johnson, *Projective planes of prime order p that admit collineation groups of order p^2*, Journal of Geometry **30** (1987), 49–68.

[Jun82] Dieter Jungnickel, *On automorphism groups of divisible designs*, Canadian Journal of Mathematics **34** (1982), no. 2, 257–297.

[Jun87] ———, *On a theorem of Ganley*, Graphs and Combinatorics **3** (1987), 141–143.

[Kan80] William M. Kantor, *Linear groups containing a Singer cycle*, Journal of Algebra **62** (1980), 232–234.

[Kib78] Robert E. Kibler, *A summary of noncyclic difference sets, $k < 20$*, Journal of Combinatorial Theory, Series A **25** (1978), 62–67.

[LTS89] C.W.H. Lam, L. Thiel, and S. Swiercz, *The non-existence of finite projective planes of order 10*, Canadian Journal of Mathematics **41** (1989), no. 6, 1117–1123.

[Lün80] Heinz Lüneburg, *Translation planes*, Springer Verlag, Berlin Heidelberg, 1980.

[Moo95] G. Eric Moorhouse, *Two-graphs and skew two-graphs in finite geometries*, Linear Algebra and its Applications **226–228** (1995), 529–551.

[Moo00] ______, *Projective planes of order 25*, `http://www.uwyo.edu/moorhouse/pub/planes25/`, September 2000.

[Nak93] Nobuo Nakagawa, *The non-existence of right cyclic planar functions of degree p^n for $n \geq 2$*, Journal of Combinatorial Theory, Series A **63** (1993), no. 1, 55–64.

[Nak97] ______, *Left cyclic planar functions of degree p^n*, Utilitas Mathematica **51** (1997), 89–96.

[Pip75] Fred Piper, *On relative difference sets and projective planes*, Glasgow Mathematical Journal **15** (1975), 150–154.

[Pot95] Alexander Pott, *Finite geometry and character theory*, Lecture Notes in Mathematics, no. 1601, Springer Verlag, Berlin Heidelberg, 1995.

[Rei84] Arthur Reifart, *The classification of the translation planes of order 16. II*, Geometriae Dedicata **17** (1984), 1–9.

[Röd06] Marc Röder, *RDS — a GAP4 package for relative difference sets*, 2006, `http://www.gap-system.org/Packages/packages.html`.

[Roy] Gordon Royle, *Gordon Royle's planes of order 16*, `http://www.csse.uwa.edu.au/~gordon/remote/planes16/index.html`.

[RS89] L. Rónyai and T. Szőnyi, *Planar functions over finite fields*, Combinatorica **9** (1989), no. 3, 315–320.

[Sch02] Bernhard Schmidt, *Characters and cyclotomic fields in finite geometry*, Lecture Notes in Mathematics, vol. 1797, Springer Verlag, Berlin Heidelberg, 2002.

Werdegang des Verfassers

1997 Technisches Gymnasium Ludwigshafen
Allgemeine Hochschulreife

2000 Universität Kaiserslautern
Vordiplom in Mathematik mit Nebenfach Physik

2000–2004 Universität Kaiserslautern
Mehrfach wissenschaftliche Hilfskraft am Fachbereich Mathematik.

2003 Universität Kaiserslautern
Diplom in Mathematik mit Nebenfach Physik
Diplomarbeit: “Fahnentransitive Steinersysteme”

2004–2006 Universität Kaiserslautern
Stipendiat des Landes Rheinland-Pfalz nach LGFG.

About the author

2004–2006 University of Kaiserslautern
Doctoral grant of the state Rheinland-Palatinate

2000–2004 University of Kaiserslautern
Employed by the Department of Mathematics at several times as teaching assistant (“Wissenschaftliche Hilfskraft”)

1998–2003 University of Kaiserslautern
“Diplom” in Mathematics with minor Physics
Thesis: “Fahnentransitive Steinersysteme”