

Universität
Rostock



Traditio et Innovatio

Formal duality

Der Mathematisch Naturwissenschaftlichen Fakultät der
Universität Rostock
zur Erlangung des akademischen Grades eines

Doctor rerum naturalium (Dr. rer. nat.)

eingereichte Dissertation

von

Herrn M.Sc. Robert Schüler

aus

Mühlhausen (Thüringen).

Datum der Einreichung: 23.07.2019

Gutachter:

Prof. Dr. Achill Schürmann

Universität Rostock

Prof. Dr. Alexander Pott

Otto von Guericke Universität Magdeburg

Tag der mündlichen Prüfung: 18.10.2019



Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung
- Nicht kommerziell - Keine Bearbeitungen 4.0 International Lizenz.

Abstract

In this thesis we provide an overview of formal duality with an emphasis on the authors contributions. Formal duality has been introduced during the study of energy minimization problems. Every formally dual set can be obtained from a primitive formally dual set or, more generally from an irreducible formally dual set. By interpreting formally dual sets as even sets, we obtain results about the structure of its multiset of differences. Using several methods, including even set theory and the field-descent method, it is possible to obtain examples of primitive/irreducible formally dual sets as well as non-existence results. In the cases where no result is known, a graph search algorithm can be used for further investigation. Overall, primitive formally dual sets seem rare in cyclic groups, but occasionally exist in finite abelian groups.

Zusammenfassung

In dieser Dissertation geben wir einen Überblick über formale Dualität wobei die Beiträgen des Autors den Schwerpunkt bilden. Formale Dualität wurde bei der Untersuchung von Energieminimierungsproblemen eingeführt. Jede formal duale Menge kann von einer primitiven, oder allgemeiner von einer irreduziblen, formal dualen Menge, konstruiert werden. Wenn formal duale Mengen als 'even sets' interpretiert werden erhält man Resultate über die Multimenge aller ihrer Differenzen. Mehrere Methoden, wie die 'even set' Theorie oder die 'field-descent' Methode, können genutzt werden um Beispiele für primitive/irreduzible formal duale Mengen sowie nicht-Existenz Resultate zu erhalten. In Fällen in denen kein anderes Resultat bekannt ist kann ein graphentheoretischer Suchalgorithmus genutzt werden. Insgesamt scheinen primitive formal duale Mengen in zyklischen Gruppen selten zu sein, kommen aber gelegentlich in endlichen abelschen Gruppen vor.

Contents

List of Symbols	VI
1 Introduction	1
2 Background	3
2.1 Cyclotomic fields and linear characters	3
2.2 The rational group algebra	5
2.3 The sub-algebra $\mathcal{M}(G)$	9
3 Motivation and Definition	13
3.1 Energy minimization	13
3.2 Definition of formal duality	16
3.3 Formal duality of energy minimizers	26
4 The even set approach	27
4.1 Introduction to even sets	27
4.2 Hasse-type diagrams	30
4.3 Even set approach on formally dual sets	35
4.4 Formally dual sets of small rank	45
5 Non-existence results	49
5.1 The field-descent method	51
5.2 Further restrictions	54
6 Constructions of primitive formally dual sets	61
6.1 Constructions	61
6.2 Irreducibility	69

7	Algorithmic approach	73
7.1	Graph search algorithm	73
7.2	Comparison	77
8	Conclusions	79
	Bibliography	86
	Index	89
	Appendix	89
A	Table of results	89
B	Cd appendix	91
C	Algorithm and Comparison	92

List of Symbols

ζ_n	$e^{2\pi i/n}$	3
$\mathbb{Q}(\zeta_n)$	n -th cyclotomic field	3
$\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$	Galois group of $\mathbb{Q}(\zeta_n)$ over \mathbb{Q}	3
\mathbb{Z}_n	Additive cyclic group of order n , i.e. $\mathbb{Z}/n\mathbb{Z}$	4
C_n	Multiplicative cyclic group of order n	4
G_p	p -Sylow group of G	4
$\text{exp}(G)$	Exponent of G	4
\hat{G}	Dual group of G	4
H^\perp	Annihilator of H	4
$\text{DFT}(v)$	Discrete Fourier transform of v	4
$\langle a, b \rangle_\Delta$	$[\Delta a](b)$ for isomorphism $\Delta : G \rightarrow \hat{G}$, $a, b \in G$	5
$\mathbb{Q}G$	Rational Group algebra over an abelian group G	5
$[A]_g$	Coefficient of g in $A \in \mathbb{Q}G$	6
$\text{supp}(A)$	Support of A	6
$\mathcal{M}(G)$	Sub-algebra of $\mathbb{Q}G$ spanned by the subgroups of G	6
$A^{(\phi)}$	Group Ring element A under homomorphism ϕ	6
$A^{(k)}$	Group Ring element A under $g \mapsto g^k$	6
$\chi(A)$	$\sum_{g \in G} a_g \chi(g)$	7
μ	Moebius function	7
E_8	Prominent root lattice	14
E_f	Energy function for pair potential f	14
A_2	Hexagonal lattice	15
D_d	Checkerboard lattice	15
D_d^+	$D_d \cup (1/2, \dots, 1/2) + D_d$	15
$D_d^+(\alpha)$	Periodic set derived from D_d^+ by scaling the last coordinate	15
P_6	Periodic set with period lattice $D_3 \times D_3$	15

$P_6(\alpha)$	Periodic set obtained from P_6	15
\hat{f}	Fourier-transform of f	16
$\Sigma_f(P)$	Average pair sum of a periodic set P with pair potential f	17
$\delta(P)$	Point density of P	17
TITO	Two in two out example	18
$v_{\mathcal{T}}$	Weight enumerator of T	19
\hat{H}	$\Delta^{-1}(H^\perp)$ for a given isomorphism $\Delta : G \rightarrow \hat{G}$	23
DS	Difference set	28
RDS	Relative difference set	28
$C_n(d, e)$	$\sum_{g \gcd(d,n/e)} \mu(n/(eg))g$	50
$\text{rad}(N)$	Radical of N , i.e. the product of distinct prime divisors	51
$\text{GR}(p^t, s)$	Galois ring of characteristic p^t and rank s	61
(p^t)	Principal ideal of a Galois Ring spanned by p^t	61
$v_p(v)$	$\max\{k : 0 \leq k \leq t, v \in (p^k)\}$	61
$\text{GR}(p^t, s)^\times$	Multiplicative group of the Galois ring	61
\mathcal{T}	Teichmüller set	61
Tr	Generalized trace function of a Galois ring	62
π	Lifting operator	65
v_{S_0, S_1}	Generalized weight enumerator with respect to S_0 and S_1	65
$A_{k,l}$	Heuristic using condition k and equivalence relation l	77
$t_{i,j}$	Time in milliseconds that the implementation of heuristic $A_{i,j}$ needed	77
$q_{i,j}$	Quality measure for heuristic $A_{i,j}$, i.e. $\log(t_{i,j}/t_{1,1})$	77

1 Introduction

The concept of duality is wide spread in mathematics. Roughly said, it guarantees for certain given mathematical objects a dual object of the same type such that some properties of the original can be easily derived from the dual and vice versa. This concept has been established for polytopes, lattices, groups, vector spaces, optimization problems and many more. In this thesis we study the concept of formal duality which is a generalization of duality. In general we might say that from the formal dual of an object some properties of the original object can be easily derived and vice versa. But unlike duality, there does not need to exist a formal dual for every given object. Therefore, the question of the characterization of all objects that permit a formal dual seems natural. The concept of formal duality has only been introduced for periodic sets and subsets of finite abelian groups so far. It is an interesting topic due to its connections to energy minimization, which is studied in physics, as well as difference sets and relative difference sets, which are studied in combinatorics.

Formal duality is an active field of research. During the study of energy minimization problems Cohn, Kumar and Schürmann introduced in 2009 the concept of formal duality of periodic lattices and displayed its relation to energy minimization problems (see [CKS09]). In 2014, Cohn, Kumar, Reiher and Schürmann added a detailed mathematical foundation and presented a way to reduce the study of formal duality of periodic sets to the study of formal duality in finite abelian groups (see [CKRS14]). In 2017 the author used elementary number theory to characterize formally dual sets in cyclic groups of odd prime power order (see [Sch17]). The characterization of formal duality in cyclic groups of even prime power order as well as the study of further examples has then been added by Xia in 2016 as an unpublished preprint¹ (see [Xia16]). In the year 2018¹, Malikiosis, inspired by a talk of Schürmann, used the field descent method and the polynomial method to

¹Since some of the cited sources are only published as preprints which are based on preprints of the preceding papers, the dates in the overview do not appear chronological.

give numerous non-existent results in the cyclic case, especially for cyclic groups whose order is divisible by exactly two distinct primes (see [Mal18]). Later on in 2019 Li and Pott in collaboration with the author introduced the concept of even sets to study formal duality and gave various new examples and non-existence results (see [LPS19]). They also detected a strong connection of formal duality to difference sets and relative difference sets. Inspired by this, Li and Pott also proposed in 2018¹ a construction framework yielding a family of formally dual sets of unequal size (see [LP18]). In 2019¹ the same authors provided an alternative direct construction of this example (see [LP19]).

In this thesis we give a summary of the study of formal duality with an emphasis on the authors contributions, especially the even set theory. The thesis is structured in eight chapters. In Chapter 2 we give the necessary mathematical background, in particular on linear characters and group algebras. Next, we provide an overview of the energy minimization problem in Chapter 3 and define formal duality in this context. In the same chapter we discuss the relation of formal duality of periodic sets and formal duality in finite abelian groups. In Chapter 4 we introduce the even set theory and its results, which are used on several occasions in the rest of the thesis. The results are formulated in a new visual language based on Hasse-diagrams, introduced in Section 4.2. That chapter also contains some yet unpublished results, for example Proposition 4.23 as well as several about formally dual sets of small rank in Section 4.4. Then we discuss non-existence results in Chapter 5. This includes unpublished results of the author (for example Theorems 5.7 and 5.11) as well as alternative proofs (for example Corollary 5.12). Within that chapter we see that formal duality in cyclic groups seems rare. On the contrary we state in Chapter 6 several infinite families of examples in non-cyclic groups. This includes an unpublished discussion of irreducibility in Section 6.2. In Chapter 7, we discuss an algorithmic framework which is useful to produce complete lists of formally dual sets in cases where no theoretical result is known. This algorithm has been applied to small groups to find the complete list of formally dual sets of small size (see Table A.1 in the appendix). A comparison of the resulting heuristics is also contained. In the last Chapter, we conclude the thesis with several open questions for future investigation.

2 Background

In this chapter we present the mathematical background needed to understand this thesis. The discussion includes cyclotomic fields, (linear) characters of groups (see Section 2.1) as well as rational group algebras (see Section 2.2) and a discussion of the subalgebra $\mathcal{M}(G)$ defined in Section 2.2 which plays a special role during the rest of the thesis. We require basic knowledge about finite abelian groups and number theory.

2.1 Cyclotomic fields and linear characters

First we give some background about cyclotomic fields which are subfields of the complex plane. Further information on cyclotomic fields can be found, for example, in [Bou03] or [Edw84]. We start with the definition of roots of unity: An n -th root of unity ζ is a root of the polynomial $z^n = 1$ in the complex plane \mathbb{C} . It is called *primitive n -th root of unity* if $\zeta^k \neq 1$ for all $k < n$. We define $\zeta_n = e^{2\pi i/n}$ and note that the n -th roots of unity are exactly the powers of ζ , i.e. ζ_n^k for $k = 0, \dots, n-1$. Furthermore, ζ_n^k is primitive if and only if $\gcd(n, k) = 1$.

The n -th cyclotomic field is obtained by adjoining a primitive n -th root of unity to the field of rational numbers, i.e. $\mathbb{Q}(\zeta_n)$. We define the set $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ to contain all automorphism of $\mathbb{Q}(\zeta_n)$ that fix \mathbb{Q} pointwise. An element of $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ is called a *Galois automorphism* of $\mathbb{Q}(\zeta_n)$ over \mathbb{Q} . In fact, the Galois automorphism of $\mathbb{Q}(\zeta_n)$ over \mathbb{Q} are exactly the linear extensions of $\zeta_n \mapsto \zeta_n^k$ for any k relative prime to n .

Another important tool is the concept of algebraic integers which is a generalization of integer numbers. An *algebraic integer* is a complex root of a monic polynomial in $\mathbb{Z}[X]$. The sum and the product of two algebraic integers are again algebraic integers and the rational algebraic integers are exactly the integer numbers.

Now we give the needed background about group theory (see also [Hum96]) and linear characters (see also [Ste12]). During this thesis, G will always be a finite abelian group which can be written additively or multiplicatively (which way is used should be obvious in the respective context). For any integer n we denote the group of integers modulo n , by $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Similiar, we denote the multiplicative cyclic group of order n by C_n . Recall, that for any finite abelian group G there are integers $n_1 | \dots | n_m$ such that

$$G \simeq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_m}.$$

Furthermore, $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \simeq \mathbb{Z}_{n_1 \cdot n_2}$ if and only if $\gcd(n_1, n_2) = 1$. For a prime p a p -group is a group such that each element has an order which is a power of p . The p -Sylow group $G_p \leq G$ is the unique maximal p -subgroup of G . The *exponent* of G , i.e. $\exp(G)$ is the size of the largest cyclic subgroup of G . The *differences* of a set $S \subset G$ are elements that can be written as $a - b$ (if the group is written additively) or as ab^{-1} (if the group is written multiplicatively) for any $a, b \in S$.

In the following we define the group of linear characters of G , also called the *dual group* as

$$\hat{G} = \{\chi : G \rightarrow \mathbb{C}^* : \chi \text{ is a homomorphism}\}.$$

We have $\hat{\hat{G}} \simeq G$ by setting $a(\chi) = \chi(a)$. Moreover, we define the *annihilator* of $H \leq G$ as

$$H^\perp = \{\chi \in \hat{G} : \chi(h) = 1 \text{ for all } h \in H\}$$

and for every subgroup $L \leq \hat{G}$ as

$$L^\perp = \{g \in G : \chi(g) = 1 \text{ for all } \chi \in L\}.$$

Note that $H^{\perp\perp} = H$. The groups \hat{G}/H^\perp and \hat{H} are isomorphic by the identification

$$[\chi \cdot H^\perp](h) = \chi(h)$$

for all $h \in H$. For any set S , we say a character χ is *principal* on S if $\chi(g) = 1$ for all $g \in S$. Or equivalently, χ is principal on S if $\chi \in \langle S \rangle^\perp$. Furthermore, we have

$$H_1^\perp \cap \dots \cap H_r^\perp = \langle H_1, \dots, H_r \rangle^\perp.$$

The *discrete Fourier transform* of a function $\nu : G \mapsto \mathbb{C}$ is defined as

$$[\text{DFT}(\nu)](\chi) = \sum_{g \in G} \overline{\chi(g)} \nu(g).$$

Note, if $\nu(g) = \nu(g^{-1})$ for all g , then also

$$[\text{DFT}(\nu)](\chi) = \sum_{g \in G} \chi(g)\nu(g).$$

The dual group \hat{G} is non-canonically isomorphic to G . So we have several choices of isomorphism $\Delta : G \rightarrow \hat{G}$. For every isomorphism Δ there is an *adjoint isomorphism* Δ_* given by $[\Delta_* a](b) = [\Delta b](a)$ for all $a, b \in G$.

A similar approach is to take a bi-linear function $\langle \cdot, \cdot \rangle : G \times G \rightarrow \mathbb{C}^*$ which we call a *pairing*. We define the *standard pairing* of $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ as

$$\langle (a_1, \dots, a_m), (b_1, \dots, b_m) \rangle = \zeta_{n_1}^{a_1 b_1} \cdots \zeta_{n_m}^{a_m b_m}.$$

Note that the standard pairing depends on the representation of G as a product of cyclic subgroups. The isomorphisms from G to \hat{G} and the bi-linear functions correspond to each other by setting $\langle a, b \rangle_\Delta = [\Delta a](b)$ for a given isomorphism Δ and vice versa. Observe that $\langle a, b \rangle_\Delta = \langle b, a \rangle_{\Delta_*}$. Furthermore, note that:

Lemma 2.1. *We have $\Delta_* H = (\Delta^{-1} H^\perp)^\perp$.*

Proof. The assertion follows by

$$\begin{aligned} \Delta_* H &= \Delta_* \{g : \psi(g) = 1 \text{ for all } \psi \in H^\perp\} \\ &= \{\Delta_* g : [\Delta_* g](\Delta^{(-1)} \psi) = 1 \text{ for all } \psi \in H^\perp\} \\ &= \{\chi : \chi(a) = 1 \text{ for all } a \in \Delta^{(-1)} H^\perp\} = (\Delta^{(-1)} H^\perp)^\perp. \end{aligned}$$

□

2.2 The rational group algebra

In the following we give some background about the rational group algebra which is essential for the even set approach in Chapter 4 and other results of this thesis. More information can be found in [Lan02, page 104]. Here, for a finite abelian group (G, \cdot) , the *group algebra* $\mathbb{Q}G$ is the set of formal sums $A = \sum_{g \in G} a_g g$ with coefficients $a_g \in \mathbb{Q}$.

We define addition in $\mathbb{Q}G$ by

$$\left(\sum_{g \in G} a_g g \right) + \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} (a_g + b_g) g$$

and multiplication by

$$\left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} \sum_{h \in G} (a_g a_h) g \cdot h = \sum_{g \in G} \left(\sum_{h \in G} a_h a_{h^{-1}g} \right) g.$$

Under this addition and multiplication $\mathbb{Q}G$ is indeed an algebra.

We write $[A]_g = a_g$ to refer to the coefficient of g in A . The *support* $\text{supp}(A)$ of a group algebra element is defined as the set of elements with nonzero coefficients, i.e.

$$\text{supp}(A) = \{g \in G : [A]_g \neq 0\}.$$

For any $S \subset G$ there is an element of the group algebra associated with S , i.e. $\sum_{g \in S} g$. During this thesis we use various group algebra equations where almost all elements involved are of type $\sum_{g \in S} g$. To avoid overcomplicated formulas, we abuse notation by identifying

$$S = \sum_{g \in S} g \in \mathbb{Q}G.$$

In this sense, a *linear combination of subgroups* refers to $\sum_{i=1}^r \lambda_i H_i \in \mathbb{Q}G$ for some subgroups $H_i \leq G$ and coefficients $\lambda_i \in \mathbb{Q}$. We define $\mathcal{M}(G) \leq \mathbb{Q}G$ to be the set spanned by the subgroups of G .

The multiplication of two subsets $S \cdot T$ always refers to the multiplications $(\sum_{g \in S} g) \cdot (\sum_{g \in T} g) \in \mathbb{Q}G$. For subgroups spanned by the elements of sets we use the notation

$$\langle S_1, \dots, S_k \rangle = \left\{ \prod_{g \in S_1 \cup \dots \cup S_k} g^{k_g} : k_g \in \mathbb{Z} \right\}.$$

If we use any set operation like \cup , \cap or \setminus that do not involve any form of addition or multiplication, we treat the present variables as sets.

For example $S \cap T = \sum_{g \in S \cap T} g$. Whenever group algebra operations and group operations might be confused we use $[\dots]$ to indicate a group operation. For example $[S \cdot T] = \{a \cdot b : a \in S, b \in T\}$.

For any homomorphism $\phi : G \mapsto H$ we define $A^{(\phi)} = \sum_{g \in G} a_g \phi(g) \in \mathbb{Q}H$ and for any integer k we define $A^{(k)} = \sum_{g \in G} a_g g^k$. Note if $\text{gcd}(k, |G|) = 1$, then $g \mapsto g^k$ is an automorphism. For further simplification of the notation, we set $q = q \cdot 1_G \in \mathbb{Q}G$ for any $q \in \mathbb{Q}$.

Remark 2.2. For a set $S \subset G$ and an element $v \in G$ we have

1. $vS = [vS]$,

2. $SS^{(-1)}$ is the multiset of differences of S , that means $\text{supp}(SS^{(-1)})$ contains all differences of S and $[SS^{(-1)}]_g = \#\{(x, y) \in S \times S : xy^{-1} = g\}$.

Note that any character $\chi \in \hat{G}$ can be applied to $A = \sum_{g \in G} a_g g \in \mathbb{Q}G$ as $\chi(A) = \sum_{g \in G} a_g \chi(g)$.

An element $A = \sum_{g \in G} a_g g$ can be interpreted as a function $g \mapsto a_g$ and the discrete fourier transform can be applied to group algebra elements.

Thus, the coefficients of A can be recovered given all character values:

Theorem 2.3 (Fourier inversion formula, [Ste12, Theorem 5.3.6]¹). *If $A = \sum_{g \in G} a_g g$ then*

$$a_g = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(A) \overline{\chi(g)}.$$

Also, the moebius inversion formula can be used in the group algebra:

Theorem 2.4 (Moebius inversion formula, [Sta12, Proposition 3.7.1]). *For any partially ordered set (V, \leq) we define the Moebius function $\mu : V \times V \mapsto \mathbb{Z}$ recursively by: $\mu(s, s) = 1$ and $\mu(s, u) = -\sum_{s \leq t < u} \mu(s, t)$ for $s \neq u$. Let $f : V \rightarrow \mathbb{Q}$ be a function and $g : V \rightarrow \mathbb{Q}$ be defined by*

$$g(t) = \sum_{s \leq t} f(s).$$

Then we have

$$f(t) = \sum_{s \leq t} g(s) \mu(s, t).$$

Note that the moebius inversion is still valid for $f : V \rightarrow \mathbb{Q}G$ and $g : V \rightarrow \mathbb{Q}G$ since group algebra addition is evaluated component wise.

In the set of integers partially ordered by divisibility we simplify the formula using number theoretic functions: The Moebius function of an integer n with k distinct prime factors is defined as

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n \text{ is squarefree} \\ 0 & \text{otherwise} \end{cases}.$$

For any $f : \mathbb{N} \mapsto \mathbb{Q}$ and $g : \mathbb{N} \mapsto \mathbb{Q}$ given by $g(t) = \sum_{s|t} f(s)$ we have

$$g(t) = \sum_{s|t} g(s) \mu(s/t) = \sum_{s|t} g(s/t) \mu(s).$$

¹Note, that this version can be easily derived from the cited version by setting $f : g \mapsto a_g$ and the simple fact that then $[\text{DFT } f](\chi^{-1}) = \chi(A)$

Subgroups of G have additional properties in the group algebra. The product of subgroups is easily evaluated:

Lemma 2.5. *Let $H, L \leq G$ and $A \in \mathbb{Q}G$, then*

$$H \cdot A = \sum_{vH \in G/H} \left(\sum_{g \in vH} [A]_g \right) \cdot vH.$$

In particular

$$H \cdot L = |H \cap L| \langle H, L \rangle.$$

Multiplying by a subgroup is related to natural projections in the following way:

Lemma 2.6. *Let $L \leq G$, $A \in \mathbb{Q}G$ and $\varphi : G \mapsto G/L$ the natural projection map. We have*

1. $(L \cdot A)^{(\varphi)} = |L| \cdot A^{(\varphi)}$,
2. $H^{(\varphi)} = |L| \cdot H/L$ for every group H with $L \leq H$,
3. $S^{(\varphi)} = k \cdot \varphi(S)$ for every $S \subset G$ such that $|S \cap aL| \in \{0, k\}$ for all $a \in G$ and some integer k .

Proof. We have

$$L^{(\varphi)} = \sum_{g \in L} \varphi(g) = \sum_{g \in L} 1_{G/L} = |L|.$$

Therefore,

$$(L \cdot A)^{(\varphi)} = L^{(\varphi)} A^{(\varphi)} = |L| \cdot A^{(\varphi)}.$$

Moreover,

$$H^{(\varphi)} = \sum_{g \in H} \varphi(g) = \sum_{[vL] \in H/L} \sum_{g \in vL} \varphi(g) = |L| \cdot H/L$$

and

$$S^{(\varphi)} = \sum_{[aL] \in G/L} |S \cap aL| [aL] = k \cdot \sum_{\substack{[aL] \in G/L \\ |S \cap aL| \neq 0}} [aL] = k\varphi(S).$$

□

When applying characters to subgroups the following result easily follows from the fact that the sum of all n -th roots of unity is zero:

Lemma 2.7. For any $\chi \in \hat{G}$ and any group $H \leq G$ we have

$$\chi(H) = \begin{cases} |H| & \text{if } \chi \in H^\perp \\ 0 & \text{otherwise} \end{cases} .$$

On the other hand, for any $g \in G$ and any group $L \leq \hat{G}$ we have

$$g(L) = \sum_{\chi \in L} \chi(g) = \begin{cases} |L| & \text{if } g \in L^\perp \\ 0 & \text{otherwise} \end{cases} .$$

Moreover, we have

$$\text{DFT}(H) = |H| \cdot H^\perp$$

2.3 The sub-algebra $\mathcal{M}(G)$

The subalgebra $\mathcal{M}(G)$ is an important tool for the study of even sets in Chapter 4. We introduce some related results:

Lemma 2.8. For any cyclic group $C \leq G$ define $\tau(C) = \{h \in G : \langle h \rangle = C\}$. We have

1. the set $\mathcal{T} = \{\tau(C) : C \leq G, C \text{ cyclic}\}$ is a basis of $\mathcal{M}(G)$,
2. the cyclic groups form a basis of $\mathcal{M}(G)$,
3. the set $\mathcal{E} = \{\tilde{C} : C \leq G, C \text{ cyclic}\}$ is a basis of $\mathcal{M}(G)$ (for fixed isomorphism Δ).

Epecially, if $[A]_g = [A]_h$ for all g, h such that $\langle g \rangle = \langle h \rangle$ then $A \in \mathcal{M}(G)$.

Proof. Clearly G is a disjoint union of the sets in \mathcal{T} . Thus, the elements of \mathcal{T} are indeed linear independent in $\mathbb{Q}G$. Furthermore, for any cyclic group $C \leq G$ we have $C = \sum_{D \leq C} \tau(D)$. Note, that the set of cyclic subgroups of G is partially ordered by inclusion. By Moebius inversion (Theorem 2.4) we therefore have

$$\tau(C) = \sum_{D \leq C} \mu(D, C)D.$$

Thus, \mathcal{T} and the cyclic groups span the same sub-algebra $M \leq \mathbb{Q}G$. Since the cardinalities are identical and \mathcal{T} contains linear independent elements, both sets

are bases of M . Note that cyclic groups are contained in $\mathcal{M}(G)$ and therefore $M \leq \mathcal{M}(G)$. Furthermore,

$$H = \sum_{C \leq H : C \text{ cyclic}} \tau(C)$$

for any subgroup $H \leq G$ which shows that $\mathcal{M}(G) \leq M$.

The last fact follows by using the discrete fourier transform. Suppose $H \leq G$ is an arbitrary subgroup. Then $(\Delta H)^\perp$ is also a subgroup of G and can thus be written as linear combination of cyclic groups, say

$$(\Delta H)^\perp = \sum_{i \in I} \lambda_i C_i.$$

Now we use the discrete fourier transform on both sides and get by Lemma 2.7

$$|(\Delta H)^\perp| \Delta H = \sum_{i \in I} \lambda_i |C_i| C_i^\perp.$$

Applying the isomorphism Δ^{-1} we then have

$$H = \sum_{i \in I} \lambda_i |C_i| / |(\Delta H)^\perp| \tilde{C}_i = \sum_{i \in I} \lambda_i |C_i| \cdot |H| / |G| \cdot \tilde{C}_i.$$

Thus \mathcal{C} generates $\mathcal{M}(G)$. Due to the cardinality of \mathcal{C} it is also a basis. By summarizing everything, the assertion follows. \square

By considering the transformation rules given in the proof above we get the following:

Corollary 2.9. *If $A \in \mathcal{M}(G)$ has integer coefficients then*

1. *there are cyclic groups C_1, \dots, C_r such that $A = \sum_{i=1}^r \lambda_i C_i$ with $\lambda_i \in \mathbb{Z}$,*
2. *there are cyclic groups C_1, \dots, C_r such that $A = \sum_{i=1}^r \frac{\lambda_i |C_i|}{|G|} \tilde{C}_i$ with $\lambda_i \in \mathbb{Z}$.*

Proof. The first fact follows directly from the proof of Lemma 2.8. For the second fact consider $A = \sum_{j=1}^r \mu_j C_j$ for cyclic groups C_j and $\mu_j \in \mathbb{Z}$. Also, there are integer coefficients $\mu_{i,j}$ such that $(\Delta C_j)^\perp = \sum_{i=1}^r \mu_{i,j} C_i$. Analog to the proof of Lemma 2.8 we then have

$$C_j = \sum_{i=1}^r \mu_{i,j} \frac{|C_i| \cdot |C_j|}{|G|} \tilde{C}_i.$$

Altogether,

$$A = \sum_{i=1}^r \left(\sum_{j=1}^r \mu_j \mu_{i,j} |C_j| \right) \frac{|C_i|}{|G|} \tilde{C}_i$$

and by choosing $\lambda_i = \sum_{j=1}^r \mu_j \mu_{i,j} |C_j|$ the assertion follows. \square

Another way to characterize the sub algebra $\mathcal{M}(G)$ is the following:

Lemma 2.10. *Let $A = \sum_{g \in G} a_g g \in \mathbb{Q}G$ be a group algebra element. We have $A \in \mathcal{M}(G)$ if and only if $\chi(A) \in \mathbb{Q}$ for all $\chi \in \hat{G}$.*

Proof. Suppose $A = \sum_{i=1}^r \lambda_i H_i$ is a linear combination of subgroups in $\mathbb{Q}G$. By Lemma 2.7 we have

$$\chi(A) = \sum_{i=1}^r \lambda_i \chi(H_i) \in \mathbb{Q}$$

for all $\chi \in \hat{G}$. On the other hand, assume $\chi(A) \in \mathbb{Q}$ for every $\chi \in \hat{G}$. Fix an element $g \in G$ and an integer k with $\gcd(k, \text{ord}(g)) = 1$ where $n = |G|$. There is an integer $k' \equiv k \pmod{\text{ord}(g)}$ such that $\gcd(k', n) = 1$. Then $\sigma_{k'} : \zeta_n \mapsto \zeta_n^{k'}$ is a Galois automorphism in $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$. By the Fourier inversion formula (Theorem 2.3) we have

$$a_g = \sigma_{k'}(a_g) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \sigma_{k'}(\chi(A)) \cdot \sigma_{k'}(\overline{\chi(g)}) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(A) \cdot \overline{\chi(g^k)} = a_{g^k}.$$

If g and h span the same subgroup, then there is a k relative prime to the order of g such that $h = g^k$. By Lemma 2.8 this shows the assertion. \square

3 Motivation and Definition

There are various multi-particle systems in the physical world. Such systems tend to loose energy, until they reach a state of minimal possible energy (a so called ground state). A description of these ground states is of great interest among physicists. Related mathematical models are the *Thomson problem* and the *energy minimization problem*. While studying the Energy Minimization Problem, Cohn, Kumar and Schürmann introduced the concept of *formal duality*. Later on, they translated it in a combinatorial setting. This chapter gives a detailed motivation of the formal duality concept. Furthermore, it states the main definitions of the thesis.

In Section 3.1 we give a brief overview of energy minimization of periodic sets. In Section 3.2 we define formal duality and discuss the relation between formal duality of periodic sets and formal duality in finite abelian groups. To conclude this chapter, we derive the combinatorial counterpart of energy minimizers in Section 3.3.

3.1 Energy minimization

In 1904 J.J. Thomson, the inventor of a famous atom model, considered the problem of minimizing potential energy of point configurations (see [Tho04]). He studied in which configuration electrons will appear if they minimize the Coulomb potential.

From a mathematical point of view this is a question about point configurations on the unit sphere that minimize some notion of energy. Say for some pair potential function $f : (0, 2] \rightarrow \mathbb{R}$ (depending only on distances between distinct points) we ask to find a set $C \subset S^d$ of given size k such that

$$\sum_{\substack{x,y \in C \\ x \neq y}} f(|x - y|)$$

is minimal. This is called the *Thomson problem*.

Many authors discussed this question for different functions f and different values of k , for example Yudin, Kolushov and Andreev (see [Yud93],[KY97], [KY94], [And96], [And97]). They related energy minimization to interesting configurations, such as the E_8 root lattice or the Leech lattice. Cohn and Kumar showed in [CK07] that these configurations are optimal for a much wider class of functions, continuing the work of Leech (see [Lee57]) about configurations that are optimal for any 'law of force'.

The Thomson problem can be altered in several ways. One way is to minimize potential energy among periodic sets. A significant example is the Gaussian Core Model described, for example, in [Sti76]. In the following, we give a short summary of these minimization problems.

A periodic set is defined as follows:

Definition 3.1. A *periodic set* is a set $P \subset \mathbb{R}^d$ which can be written as

$$P = \bigcup_{i=1}^m (t_i + \Lambda),$$

where Λ is a full dimensional lattice (called the *period lattice*) in \mathbb{R}^d and $t_1, \dots, t_m \in \mathbb{R}^d$ are arbitrary translation vectors.

The energy minimization problem can be stated as follows: For a given 'pair potential' function $f : \mathbb{R}_{>0} \mapsto \mathbb{R}$ and a given period m , find the periodic set $P = \bigcup_{i=1}^m (t_i + \Lambda)$ such that

$$E_f(P) := \frac{1}{m} \sum_{j,k=1}^m \sum_{\substack{x \in \Lambda \\ x+t_j-t_k \neq 0}} f(|x+t_j-t_k|)$$

is minimal.

The value of $E_f(P)$ can be seen as the average potential energy among any pair of points in P .

A huge numerical computation to find Energy minimizing configurations for Gaussian core functions has been described by Cohn, Kumar, Reiher and Schürmann in [CKS09]. Table 3.1 displays a summary of their results (compare with [CKS09, Table I]).

For the lattices A_2 , D_4 , E_8 and the Leech lattice it has been proven, that these are, at least locally, optimal structures for a wide range of pair potentials (see [CS12], [CKM⁺19]).

Dimension	(probable) Optimal Structure
1	\mathbb{Z}
2	A_2
3	D_3 or D_3^*
4	D_4
5	$D_5^+(1.99750 \dots)$ or $D_5^+(0.50062 \dots)$
6	$\mathcal{P}_6(1.0525 \dots)$
7	D_7^+
8	E_8

Table 3.1: energy minimizers in small dimensions

Here

$$D_d = \{(x_1, \dots, x_d) \in \mathbb{Z}^d : x_1 + \dots + x_d \equiv 0 \pmod{2}\}$$

is a root lattice, known as the d -dimensional checkerboard lattice. Furthermore D_d^+ is a periodic set with period lattice D_d , namely

$$D_d^+ = D_d \cup (1/2, \dots, 1/2) + D_d$$

and $D_d^+(\alpha)$ can be obtained from the periodic set D_d by scaling the last coordinate by α , i.e.

$$D_d^+(\alpha) = \{(x_1, \dots, x_{d-1}, \alpha x_d) : (x_1, \dots, x_d) \in D_d^+\}.$$

Furthermore \mathcal{P}_6 is the periodic set given by the period lattice $D_3 \times D_3$ and the translation vectors

$$(0, 0, 0, 0, 0, 0), \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right), \left(1, 1, 1, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right), \left(-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, 1, 1, 1\right).$$

From this periodic set we obtain the structure $\mathcal{P}_6(\alpha)$ by taking

$$\mathcal{P}_6(\alpha) = \{(\alpha x_1, \alpha x_2, \alpha x_3, \alpha^{-1} x_4, \alpha^{-1} x_5, \alpha^{-1} x_6) : (x_1, \dots, x_6) \in \mathcal{P}_6\}.$$

Surprisingly, all structures listed in Table 3.1 share the property of formal duality (see Definition 3.3). In Section 3.3 we will come back to these examples and see their relation to formal duality in finite abelian groups.

Due to these results, a better understanding of formal duality is desirable.

3.2 Definition of formal duality

In this section we introduce the notion of formal duality for periodic sets and derive the (somehow comparable) notion of formal duality in abelian groups. The shown results are a short overview of the work of Cohn, Kumar, Reiher and Schürmann [CKRS14] supplemented with further results, mostly from [LPS19].

Formal duality of periodic sets can be considered as a generalization of the duality among lattices. In particular, a lattice and its dual provide a formally dual pair. However, duality can not be easily generalized from the common definition of the dual lattice of a lattice Λ :

$$\Lambda^* = \{y \in \mathbb{R}^d : \langle x, y \rangle \in \mathbb{Z} \text{ for all } x \in \Lambda\}.$$

Instead, the definition of formal duality of periodic sets has been given in [CKS09] and is a generalization of the Poisson summation formula introduced by Stein and Weiß in [SW71, VII. Corollary 2.6]. We state a version, that can be easily derived and was used before by various authors (for example see [CKRS14, Beginning of Chapter 2]).

Theorem 3.2 (Poisson summation formula, [SW71, VII. Corollary 2.6]). *Let $f : \mathbb{R}^d \rightarrow \mathbb{R}$ be any function such that the Fourier-transform*

$$\hat{f}(y) = \int_{\mathbb{R}^d} f(x) e^{-2\pi i \langle x, y \rangle} dx$$

exists and there is a constant C such that $|f(x)|, |\hat{f}(x)| \leq C(1 + |x|)^{-d-\delta}$ holds for all choices of $x \in \mathbb{R}^d$ and $\delta > 0$. Then we have the following identity for any full dimensional lattice $\Lambda \subset \mathbb{R}^d$ and any vector $t \in \mathbb{R}^d$:

$$\sum_{x \in \Lambda} f(x + t) = \frac{1}{|\Lambda|} \sum_{y \in \Lambda^*} \hat{f}(y) e^{2\pi i y t}. \quad (3.1)$$

Especially, by setting $t = 0$ and restricting the choice of f to Schwartz functions we have

$$\sum_{x \in \Lambda} f(x) = \frac{1}{|\Lambda|} \sum_{y \in \Lambda^*} \hat{f}(y) \quad (3.2)$$

for all Schwartz-Functions f .

Here, a Schwartz-Function is a function such that all derivatives decrease faster than any polynomial, i.e.

$$\forall \alpha, \beta \in \mathbb{N}^d : \sup_{x \in \mathbb{R}^n} x^\alpha D^\beta f(x) < \infty.$$

In order to generalize this formula we define the *average pair sum* of a periodic set $P = \bigcup_{i=1}^m (t_i + \Lambda)$ to be

$$\Sigma_f(P) = \frac{1}{m} \sum_{i,j=1}^m \sum_{x \in \Lambda} f(x + t_i - t_j).$$

The average pair sum of a lattice can be evaluated as $\Sigma_f(\Lambda) = \sum_{x \in \Lambda} f(x)$, so that Equation (3.2) can be rewritten as

$$\Sigma_f(\Lambda) = \delta(\Lambda) \Sigma_{\hat{f}}(\Lambda^*),$$

where $\delta(\Lambda) = \frac{1}{\det \Lambda}$ is the point density of Λ . Thus, the following definition of formal duality might be seen as a generalization thereof:

Definition 3.3 ([CKRS14, Definition 2.1]). Two periodic sets $P = \bigcup_{i=1}^m t_i + \Lambda, Q \subset \mathbb{R}^d$ are called a *formally dual pair* if

$$\Sigma_f(P) = \delta(P) \Sigma_f(Q)$$

for all Schwartz functions f . Here $\delta(P) = \frac{m}{\det(\Lambda)}$ is the point density of P .

For a given formally dual pair, we can construct others using a linear transformation:

Lemma 3.4 ([CKS09, Lemma 2]). *Let $P, Q \subset \mathbb{R}^d$ form a formally dual pair and A be an invertible linear transformation. Then AP and $A^{-T}Q$ also form a formally dual pair.*

One prominent example of formal duality is the periodic set TITO. In Section 3.3 we will see its relation to the energy minimizing configurations in Table 3.1 and in Chapter 5 we will explain its special role in the study of formally dual sets.

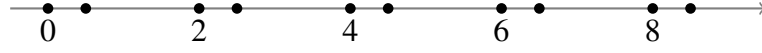


Figure 3.1: The periodic set TITO

Example 3.5. The set $\text{TITO} = 2\mathbb{Z} \cup (\frac{1}{2} + 2\mathbb{Z})$ (two in - two out) is formally dual to itself.

To see this we make exhaustive use of Equation (3.1):

$$\begin{aligned}
2 \cdot \Sigma_f(\text{TITO}) &= 2 \sum_{x \in 2\mathbb{Z}} f(x) + \sum_{x \in 2\mathbb{Z}} f(x + \frac{1}{2}) + \sum_{x \in 2\mathbb{Z}} f(x - \frac{1}{2}) \\
&= \sum_{y \in \frac{1}{2}\mathbb{Z}} \hat{f}(y) + \frac{1}{2} \sum_{y \in \frac{1}{2}\mathbb{Z}} \hat{f}(y) e^{2\pi i y \cdot \frac{1}{2}} + \frac{1}{2} \sum_{y \in \frac{1}{2}\mathbb{Z}} \hat{f}(y) e^{2\pi i y \cdot (-\frac{1}{2})} \\
&= \sum_{y \in \frac{1}{2}\mathbb{Z}} \hat{f}(y) (1 + \frac{1}{2} \zeta_2^y + \frac{1}{2} \zeta_2^{-y}) \\
&= 2 \sum_{y \in 2\mathbb{Z}} \hat{f}(y) + \sum_{y \in 2\mathbb{Z}} \hat{f}(y + \frac{1}{2}) + \sum_{y \in 2\mathbb{Z}} \hat{f}(y - \frac{1}{2}) \\
&= 2 \cdot \Sigma_{\hat{f}}(\text{TITO})
\end{aligned}$$

$$\text{since } (1 + \frac{1}{2} \zeta_2^y + \frac{1}{2} \zeta_2^{-y}) = \begin{cases} 2 & \text{if } y \in 2\mathbb{Z} \\ 0 & \text{if } y \in \mathbb{Z} \setminus 2\mathbb{Z} \\ 1 & \text{if } y \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z} \end{cases} .$$

Furthermore, Cohn, Kumar, Reiher and Schürmann noticed that the property of formal duality only depends on some 'underlying group'. Therefore it can be reduced to the study of formal duality in finite abelian groups:

Theorem 3.6 ([CKRS14, Corollary 2.6, Theorem 2.8]). *Let $P, Q \subset \mathbb{R}^d$ be periodic sets with period lattice Λ and Γ respectively. If P and Q form a formally dual pair, then without loss of generality we may assume $\Lambda \subset P \subset \Gamma^*$ and $\Gamma \subset Q \subset \Lambda^*$. Thus P is characterized by the underlying lattice Λ and a system of representatives $S \subset G := \Gamma^*/\Lambda$. Analogously Q is given by Γ and some $T \subset \hat{G} \simeq \Lambda^*/\Gamma$ (Note that Λ^*/Γ is isomorphic to the dual group of Γ^*/Λ by the natural pairing $\langle \chi + \Gamma, x + \Lambda \rangle = e^{2\pi i \langle x, \chi \rangle}$). Then P and Q form a formally dual pair, if and only*

if for every $\chi \in \hat{G}$ we have

$$\left| \frac{1}{|S|} \sum_{v \in S} \chi(v) \right|^2 = \frac{1}{|T|} v_T(\chi) \quad (3.3)$$

where $v_T(\chi) = \#\{(\phi + \Gamma, \psi + \Gamma) \in T \times T : (\phi - \psi) + \Gamma = \chi + \Gamma\}$.

Or equivalently, by recalling that $\chi(S) = \sum_{v \in S} \chi(v)$, P and Q form a formally dual pair if and only if

$$\frac{|S|^2}{|T|} v_T(\chi) = |\chi(S)|^2. \quad (3.4)$$

Note that the groups that may occur in Theorem 3.6 are exactly the finite abelian groups, thus it is sufficient to study subsets of finite abelian groups if we are interested in the formal duality property:

Definition 3.7 ([CKRS14, Definition 2.9]). Let G be some (multiplicative) finite abelian group and \hat{G} be its dual group. Two sets $S \subset G$ and $T \subset \hat{G}$ form a formally dual pair if for all $\chi \in \hat{G}$ we have

$$|\chi(S)|^2 = \frac{|S|^2}{|T|} v_T(\chi), \quad (3.5)$$

where

$$v_T(\chi) = \#\{(\phi, \psi) \in T \times T : \phi \cdot \psi^{-1} = \chi\} = [TT^{(-1)}]_\chi$$

is called the *weight enumerator* of T . A set S is called a *formally dual set* if there is a set T such that S and T form a formally dual pair.

This definition is symmetric under the identification of \hat{G} and G . We give some remarks regarding this definition:

Remark 3.8. Equation (3.5) is equivalent to

$$\frac{|S|^2}{|T|} v_T = \text{DFT}(v_S)$$

(see [Sch17, Lemma 2.1]).

Remark 3.9. The left hand side of Equation (3.5) is an algebraic integer while the right hand side is rational. Thus both sides are in fact integer numbers.

An elementary observation about the respective sizes of formally dual sets is:

Lemma 3.10 ([CKRS14, End of Proof 2.8]). *Let $S \subset G$, $T \subset \hat{G}$ form a formally dual set. Then $|G| = |S| \cdot |T|$.*

We continue by describing the combinatorial equivalent of the TITO example:

Example 3.11 ([CKRS14, Section 3.1] [Sch17, Example 2.1]). *Recall the set TITO from Example 3.5. Then $\Lambda = \Gamma = 2\mathbb{Z}$ and $\Lambda^* = \Gamma^* = \frac{1}{2}\mathbb{Z} \subset 2\mathbb{Z}$. Thus $\Gamma^*/\Lambda = \frac{1}{2}\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}_4$ and TITO can be interpreted as $\text{TITO} = \{0, 1\} \pmod{4}$. Therefore we might compute the weight enumerator as:*

$$\left. \begin{array}{c} v \\ \{(x, y) : x - y = v\} \\ v_{\text{TITO}}(v) \end{array} \right| \begin{array}{cccc} 0 & 1 & 2 & 3 \\ \{(0, 0), (1, 1)\} & \{(1, 0)\} & \emptyset & \{(0, 1)\} \\ 2 & 1 & 0 & 1 \end{array} .$$

Now we can check formal duality as defined in Definition 3.7. For example take $\chi : v \mapsto \zeta_4^v = i^v$. It is easy to compute

$$\left| \frac{1}{2} (\zeta_4^0 + \zeta_4^1) \right|^2 = \frac{1}{4} |1 + i|^2 = \frac{1}{2}.$$

On the other hand we might interpret χ as an element of the group G by the isomorphism $\Delta : \chi \mapsto 1$. According to the table above we know

$$\frac{1}{|\text{TITO}|} v_{\text{TITO}}(\Delta\chi) = \frac{1}{2} \cdot 1 = \frac{1}{2}.$$

Note that there are a lot of possibilities to lift a formally dual pair in an abelian group to a formally dual pair of periodic sets as can be seen in the following example:

Example 3.12. *Suppose S and T form a formally dual pair in a finite abelian group $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_l}$. Take the lattices $\Lambda = \mathbb{Z}^d$ and $\Gamma = n_1\mathbb{Z} \times \cdots \times n_l\mathbb{Z} \times \mathbb{Z}^{d-l}$. Furthermore define*

$$P = \bigcup_{(x_1, \dots, x_l) \in S} \left(\frac{x_1}{n_1}, \dots, \frac{x_l}{n_l}, 0, \dots, 0 \right) + \Lambda$$

and

$$Q = \bigcup_{(y_1, \dots, y_n) \in T} (y_1, \dots, y_n, 0, \dots, 0) + \Gamma.$$

By Theorem 3.6 P and Q indeed form a formally dual pair. By Lemma 3.4 same is true for AP and $A^{-T}Q$ for any invertible matrix A . Since AP is a periodic set with period lattice $A\mathbb{Z}^d$ the example can be concluded as: A formally dual pair in an abelian group can be realized as a formally dual pair of periodic sets for any period lattice with sufficiently high dimension.

The translation of formally dual pairs of periodic sets into the abelian group setting involves an implicit isomorphism $\Lambda^*/\Gamma \rightarrow \widehat{(\Gamma^*/\Lambda)}$. Therefore, it is not surprising that the formal duality property is invariant under automorphisms:

Lemma 3.13 ([LPS19, Proposition 2.16]). *If $S \subset G$ and $T \subset \hat{G}$ form a formally dual pair and ϕ is an automorphism of \hat{G} . Then $\hat{\phi} : \hat{G} \rightarrow \hat{G}, \chi \mapsto \chi \circ \phi$ is an automorphism of \hat{G} (called the adjoint of ϕ) and $\phi(S)$ and $\hat{\phi}^{(-1)}(T)$ form a formally dual pair.*

Proof. Observe

$$v_{\hat{\phi}^{(-1)}(T)}(\chi) = \#\{(\psi, \rho) \in T \times T : (\psi \cdot \rho^{-1}) \circ \phi^{-1} = \chi\} = v_T(\chi \circ \phi)$$

Thus

$$\frac{|\phi(S)|^2}{|\hat{\phi}^{(-1)}(T)|} v_{\hat{\phi}^{(-1)}(T)}(\chi) = \frac{|S|^2}{|T|} v_T(\chi \circ \phi) = |(\chi \circ \phi)(S)|^2 = |\chi(\phi(S))|^2.$$

And thus $\phi(S)$ and $\hat{\phi}(T)$ form a formally dual pair. \square

This might be seen as the combinatorial equivalent to Lemma 3.4.

During this work, we denote two sets $S_1 \subset G_1$ and $S_2 \subset G_2$ as equivalent, if there is an isomorphism $\phi : G_1 \rightarrow G_2$ and an element $v \in G_2$ such that $S_2 = v \cdot \phi(S_1)$. The advantage of this notion of equivalence is given in the following corollary, which follows directly from Lemma 3.13

Corollary 3.14. *Let $S_1, S_2 \subset G$ such that S_1 is equivalent to S_2 . Then S_1 is a formally dual set if and only if S_2 is a formally dual set.*

It is natural to ask for a characterization of formally dual sets. One step towards an answer to this question is the following result:

Theorem 3.15 ([CKRS14, Lemma 4.2]). *Let $S \subset G$ and $T \subset \hat{G}$ form a formally dual pair. The set S is contained in a proper coset $a \cdot H$ of G if and only if T is invariant under translations by H^\perp . If $S \subset a \cdot H$ then S under the canonical map $a \cdot H \rightarrow H$ and T under the natural reduction map $\hat{G} \rightarrow \hat{G}/H^\perp \simeq \hat{H}$ also form a formally dual pair.*

Proof. In the proof of [CKRS14, Lemma 4.2] the main part of this Theorem already has been proven. However, the implication from 'T is a union of cosets' to 'S is contained in a coset' is missing. A proof thereof is given below.

Let $T = \bigcup(x \cdot H^\perp)$. Thus

$$v_T(\chi) = |T| \text{ for all } \chi \in H^\perp.$$

But then

$$|S|^2 = \frac{|S|^2}{|T|} v_T(\chi) = |\chi(S)|^2 \text{ for all } \chi \in H^\perp.$$

This is only possible if χ is principal on the set of distances of S , namely all distances are contained in $H^{\perp\perp} = H$ and thus S is contained in a proper coset of H . \square

Consequently, it is easy to find formally dual pairs in an arbitrary group:

Example 3.16 ([LPS19, Example 2.3]). *Let G be a group and $H \leq G$ be a subgroup. Then H and $H^\perp \leq \hat{G}$ form a formally dual pair.*

As seen above it is sufficient to study formal duality for such sets on which Theorem 3.15 can not be applied:

Definition 3.17 ([LPS19, Definition 2.5]). A set $S \subset G$ is called *primitive* if none of the following is true:

1. S is contained in a proper coset of G ,
2. S is a union of cosets of some proper subgroup of G

A pair of subsets S and T form a *primitive formally dual pair* if they are primitive sets that form a formally dual pair.

If S and T form a formally dual pair, then it is clear by Theorem 3.15 that S is primitive if and only if T is primitive. Thus, this definition is equivalent to the definition given in [CKRS14, Below Lemma 4.2].

The following lemma gives a simple technique to construct primitive formally dual sets out of smaller ones.

Lemma 3.18 (Cross product construction, [LPS19, Proposition 3.2]). *Let $S_1 \subset G_1$ and $T_1 \subset \hat{G}_1$ as well as $S_2 \subset G_2$ and $T_2 \subset \hat{G}_2$ form primitive formally dual pairs. Then $S = S_1 \times S_2$ and $T = T_1 \times T_2$ also form a primitive formally dual pair.*

Proof. Observe $v_{T_1 \times T_2}(\chi, \psi) = v_{T_1}(\chi) \cdot v_{T_2}(\psi)$ and

$$|(\chi, \psi)(S_1 \times S_2)|^2 = \left| \sum_{\substack{x \in S_1 \\ y \in S_2}} \chi(x) \cdot \psi(y) \right|^2 = |\chi(S_1)|^2 \cdot |\psi(S_2)|^2.$$

Therefore, using Definition 3.7 we have

$$\frac{|S|^2}{|T|} v_{T_1 \times T_2}(\chi, \psi) = \frac{|S_1|^2}{|T_1|} v_{T_1}(\chi) \cdot \frac{|S_2|^2}{|T_2|} v_{T_2}(\psi) = |(\chi, \psi)(S_1 \times S_2)|^2$$

and thus S and T form indeed a formally dual pair. We claim that S is primitive. Indeed, if S would be contained in a proper coset, then at least one of S_1 or S_2 also would, contradicting their primitivity. On the other hand, if S would be a union of cosets then, using Theorem 3.15, T would be contained in a proper coset. This is a contradiction as seen before. \square

In perspective of Lemma 3.13 and Lemma 3.18 the 'building block' formally dual pairs are the following:

Definition 3.19. A formally dual pair S and T is called *irreducible* if it is primitive and not equivalent to a cross product of non-trivial formally dual sets.

The characterization of irreducible formally dual pairs is an interesting open problem.

In the following we will further simplify the notion of formally dual pairs by omitting the group \hat{G} . It is possible to 'get rid' of the dual group in the definition of formal duality by choosing an isomorphism from G to \hat{G} :

Definition 3.20 ([LPS19, Definition 2.7]). Let $\Delta : G \rightarrow \hat{G}$ be a group isomorphism. Then $S \subset G$ and $T \subset G$ form a *formally dual pair under isomorphism Δ* if S and $\Delta(T)$ form a formally dual pair (in G and \hat{G}). Alternatively, we say S and T form a formally dual pair under the pairing $\langle \cdot, \cdot \rangle_\Delta$. We call a set S formally self dual, when it is formally dual to itself under some isomorphism.

For fixed Δ , we set $\tilde{H} = \Delta^{-1}(H^\perp)$ for any $H \leq G$.

By choosing a different isomorphism, it is easy to see that S and T form a formally dual pair under isomorphism Δ_1 if and only if S and $\Delta_2^{-1}\Delta_1(T)$ form a formally dual pair under isomorphism Δ_2 (see [LPS19, Proposition 2.9]).

Note that this notion is not symmetric. I.e. if S and T form a formally dual pair under an isomorphism Δ then T and S do not necessarily form a formally dual pair under Δ . Instead we have the following:

Lemma 3.21. *Let G be a finite abelian group and $\Delta : G \rightarrow \hat{G}$ an isomorphism. Then $S \subset G$ and $T \subset G$ form a formally dual pair under Δ if and only if T and S form a formally dual pair under Δ_* .*

Proof. We have $v_{\Delta T}(\chi) = v_T(\Delta^{-1}\chi)$ as well as

$$[\Delta^{-1}\chi](\Delta_*S) = \langle S, \Delta^{-1}\chi \rangle_{\Delta_*} = \langle \Delta^{-1}\chi, S \rangle_{\Delta} = \chi(S).$$

By substituting $g = \Delta^{-1}\chi$ we therefore have

$$\frac{|S|^2}{|\Delta T|} v_{\Delta T}(\chi) = |\chi(S)|^2 \text{ for all } \chi \in \hat{G}$$

if and only if

$$\frac{|\Delta_*S|^2}{|T|} v_T(g) = |g(\Delta_*S)|^2 \text{ for all } g \in G.$$

This is equivalent to the assertion. □

The introduced notion of formal self duality differs from the notion introduced in [Xia16, Section 6] where they only consider formal duality under the standard pairing. Since the choice of isomorphism is arbitrary, Definition 3.20 seems more natural.

We examine formal self duality further:

Proposition 3.22. *Suppose $S \subset G$ is a formally self dual set under an isomorphism Δ . Furthermore, assume S is contained in some coset of $H \leq G$ such that $(\tilde{H})^\perp = \Delta H$.*

Then $\tilde{H} \leq H$ and

$$S' = \{v\tilde{H} : v \in S\} \subset H/\tilde{H}$$

is formally self dual under the isomorphism Δ' given by $\langle a\tilde{H}, b\tilde{H} \rangle_{\Delta'} = \langle a, b \rangle_{\Delta}$.

Proof. By Theorem 3.15 we know that ΔS is invariant under translations by H^\perp . Equivalently $S = \bigcup_{v \in V} v\tilde{H} \subset xH$ for some $V \subset H$, $x \in G$ and therefore $\tilde{H} \leq H$. Note, that Δ' is well defined since for all $h \in \tilde{H}$ and $b \in H$ we have $\langle h, b \rangle_{\Delta} = 1$ since $\Delta h \in H^\perp$ and $\langle b, h \rangle_{\Delta} = 1$ since $\Delta b \in \Delta H = \tilde{H}^\perp$. Then we

have for all $a\tilde{H} \in H/\tilde{H}$ that $v_{S'}(a\tilde{H}) = v_S(a)/|\tilde{H}|$ as well as $|S'| = |S|/|\tilde{H}|$ and

$$\langle a, S \rangle_{\Delta} = \sum_{v \in S} \langle a, v \rangle_{\Delta} = |\tilde{H}| \cdot \sum_{v\tilde{H} \in S'} \langle a\tilde{H}, v\tilde{H} \rangle_{\Delta'} = |\tilde{H}| \cdot \langle a\tilde{H}, S' \rangle_{\Delta'}.$$

Altogether, we have

$$\frac{|S'|^2}{|S'|} v_{S'}(a\tilde{H}) = \frac{1}{|\tilde{H}|^2} \frac{|S|^2}{|S|} v_S(a) = \frac{1}{|\tilde{H}|^2} |\langle a, S \rangle_{\Delta}|^2 = \left| \langle a\tilde{H}, S' \rangle_{\Delta'} \right|^2.$$

Thus, S' is formally dual to itself under Δ' . \square

Note that this result could also be proven by using Theorem 3.15. We conjecture that this result could be extended to arbitrary isomorphisms:

Conjecture 3.23. *If $S \subset H \leq G$ is formally self dual under an isomorphism Δ , then S' as defined in Proposition 3.22 is also formally self dual.*

If this conjecture is true, then we would only need to characterize the primitive formally self dual sets in order to characterize all formally self dual sets.

In [Xia16, Theorems 6.1, 6.3] Xia described¹ the following examples of formal self duality:

Example 3.24. *The set $S = \{n \cdot k : k \in \mathbb{Z}_{n^2}\}$ is formally self dual in \mathbb{Z}_{n^2} under the standard pairing. By using Proposition 3.22 and observing that $H = \tilde{H} = n\mathbb{Z}_{n^2}$, this example can be reduced to the trivial primitive formally self dual set.*

For any prime p and any α with $\alpha^2 \equiv -1 \pmod{p}$ the set

$$S = \{(k, k \cdot \alpha) : k \in \mathbb{Z}_p\}$$

is formally self dual in $(\mathbb{Z}_p)^2$ under the standard pairing (by the choice of α , we might only consider p with $p \equiv 3 \pmod{4}$). Note that $S = H = \tilde{H}$ when $H = \langle (1, \alpha) \rangle$, since

$$\tilde{H} = \langle (-\alpha, 1) \rangle = \langle \alpha(-\alpha, 1) \rangle = \langle (1, \alpha) \rangle = H.$$

Thus by using Proposition 3.22 this example also reduces to the trivial primitive formally self dual set.

¹with a minor typo

3.3 Formal duality of energy minimizers

In this Section we link the examples of Table 3.1 to their counterpart in finite abelian groups. The formal duality property of these examples has already been studied in [CKS09, Chapter VI], but not by explicitly translating them into subsets of groups.

Example 3.25 ([CKS09]). *We will study the energy minimizer $D_n^+(\alpha)$ for odd n and see that it is formally dual to $D_n^+(\alpha^{-1})$. In this example we will use the notation*

$$P(\alpha) = \{(x_1, \dots, x_{n-1}, \alpha x_n) : (x_1, \dots, x_n) \in P\}$$

for all sets $P \subset \mathbb{R}^n$. The underlying lattices are $D_n(\alpha)$ and $D_n(\alpha^{-1})$ respectively. Note that

$$D_n^* = \frac{1}{2} \{(x_1, \dots, x_n) : x_1 \equiv \dots \equiv x_n \pmod{2}\}$$

and thus $(D_n(\alpha))^* = D_n^*(\alpha^{-1})$ and $(D_n(\alpha^{-1}))^* = D_n^*(\alpha)$. It is easy to validate that $D_n(\alpha) \subset \mathbb{Z}^n(\alpha) \subset D_n^*(\alpha)$ and $D_n(\alpha^{-1}) \subset \mathbb{Z}^n(\alpha) \subset D_n^*(\alpha^{-1})$. Furthermore, the factor groups are

$$D_n(\alpha)/D_n^*(\alpha) \simeq D_n(\alpha^{-1})/D_n^*(\alpha^{-1}) \simeq \mathbb{Z}_4.$$

It is easy to see that $D_n^+(\alpha)/D_n^*(\alpha) \simeq \text{TITO}$. Same is true when we interchange α with α^{-1} . Therefore, the $D_n^+(\alpha)$ example is equivalent to Example 3.11.

Example 3.26. *Next we observe $\mathcal{P}_6(\alpha)$ which is formally dual to $\mathcal{P}_6(\alpha^{-1})$. In this example we will use the notation*

$$P(\alpha) = \{(\alpha x_1, \alpha x_2, \alpha x_3, \alpha^{-1} x_4, \alpha^{-1} x_5, \alpha^{-1} x_6) : (x_1, \dots, x_6) \in P\}.$$

The underlying lattice of $\mathcal{P}_6(\alpha)$ is $(D_3 \times D_3)(\alpha)$ which has dual lattice $((D_3 \times D_3)(\alpha))^* = (D_3^* \times D_3^*)(\alpha^{-1})$. Same is true when interchanging α and α^{-1} . It is easy to see that $(D_3 \times D_3)(\alpha) \subset (D_3^* \times D_3^*)(\alpha)$. Furthermore, the factor groups are

$$(D_3 \times D_3)(\alpha)/(D_3^* \times D_3^*)(\alpha) \simeq (D_3 \times D_3)(\alpha^{-1})/(D_3^* \times D_3^*)(\alpha^{-1}) \simeq \mathbb{Z}_4 \times \mathbb{Z}_4.$$

By taking the translation vectors into account, the $\mathcal{P}_6(\alpha)$ example is equivalent to $\{(0, 0), (1, 1), (2, 3), (3, 2)\} \subset \mathbb{Z}_4 \times \mathbb{Z}_4$. By taking the group automorphism generated by $(2, 3) \mapsto (1, 0), (3, 2) \mapsto (0, 1)$ we see that it is equivalent to TITO^2 which is formally self dual by Lemma 3.18.

So the energy minimizer of Table 3.1 are either lattices or related to the TITO example.

4 The even set approach

In this chapter we introduce the concept of *even sets* which includes formally dual sets. This approach provides a new perspective on formal duality and allows generalizations of known results. In Section 4.1 we define even sets using a group algebra equation and explain the relation to formally dual sets (see Theorem 4.5). We emphasize on the fact that an even set representation of a formally dual set is easily obtained given an even set representation of its formal dual. In Section 4.2 we introduce Hasse-type diagrams: a visual language which helps to distinguish between different kinds of even sets. In Section 4.3 we use this language to discuss restrictions for primitive formally dual sets of certain types. Furthermore, we emphasize on the relation among formally dual sets and relative difference sets. These results will be used in Section 4.4 to discuss formally dual sets with small rank and to give a complete characterization of formally dual sets of rank up to three, i.e. these are either trivial or certain relative difference sets. Here, rank is a measure of complexity introduced below Lemma 4.2.

4.1 Introduction to even sets

In this section we define the concept of even sets. We observe that any formally dual set is an even set (see Theorem 4.4). Therefore, the study of even sets provides new insights for the study of formally dual sets. Even sets are defined by a group algebra equation:

Definition 4.1. An *even set* is a subset $S \subset G$ with respect to some subgroups $H_1, \dots, H_r \leq G$ if

$$SS^{(-1)} = \sum_{i=1}^r \lambda_i H_i$$

for $0 \neq \lambda_i \in \mathbb{Q}$. The right hand side is called an *even set representation* with parameters λ_i and respective subgroups H_i .

Thus, a set $S \subset G$ is an even set if and only if $SS^{(-1)} \in \mathcal{M}(G)$. Note, that by Remark 2.2 $v_S(g) = [SS^{(-1)}]_g$ and $SS^{(-1)}$ might be seen as the multiset of differences of S . Significant examples of even sets which have been studied extensively are difference sets and relative difference sets:

Example 4.2. A (v, k, λ) -difference set (DS) is a set $S \subset G$ where $|G| = v$, $|S| = k$ and

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

So each non-trivial difference appears exactly λ times.

An (m, n, k, λ) -relative difference set (RDS) with respect to some subgroup $N \leq G$ is a set $S \subset G$ with $|G| = m \cdot n$, $|N| = n$, $|S| = k$ and

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

So any difference in $G \setminus N$ appears exactly λ times, while differences in $N \setminus \{1\}$ don't appear at all. The group N is referred to as the forbidden subgroup. Note that TITO is an $(2, 2, 2, 1)$ -RDS.

Any even set might also be written in terms of cyclic groups. If done so, the corresponding representation is unique as can be seen from Lemma 2.8.

Another way to simplify a linear combination of subgroups in the group algebra is obtained by using as few groups as possible. Such a representation is called *minimal representation*. The number of subgroups involved is called the *rank*. The concept of rank can easily be adapted to even sets.

The following corollary follows directly from Lemma 2.8 and summarizes some different notions of even sets.

Corollary 4.3 ([LPS19, Propositions 4.5, 4.7]). *The following are equivalent*

1. S is an even set,
2. S is an even set with respect to cyclic subgroups,
3. $v_S(g) = v_S(g^k)$ for any $g \in G$ and k that is relative prime to the order of g .

With these facts we can prove the connection between formally dual sets and even sets. For cyclic groups this has essentially been done in [Sch17, Theorem 3.1] and has been generalized in [LPS19, Corollary 4.8].

Theorem 4.4 ([LPS19, Corollary 4.8]). *Every formally dual set is an even set.*

Proof. Let S and T form a formally dual pair with respect to some isomorphism $g \mapsto \chi_g$. By Remark 3.9 $|\chi_g(S)|^2 = \chi_g(SS^{(-1)})$ are in fact integer numbers. Therefore the assertion follows from Lemma 2.10. \square

In the following, we fix the isomorphism $\Delta : g \mapsto \chi_g$. Recall that

$$\tilde{H} = \{g \in G : \chi_g(v) = 1 \text{ for all } v \in H\} = \Delta^{-1}H^\perp.$$

Many results of Section 3.2 can easily be reformulated using \tilde{H} instead of H^\perp and will be used in the following.

Given an even set representation of a formally dual set, we easily can compute an even set representation of the formal dual:

Theorem 4.5 ([LPS19, Theorem 4.9]). *Let $S, T \subset G$. Then the following is equivalent:*

1. S and T form a formally dual pair in G
2. S and T are even sets, and for any even set representation $SS^{(-1)} = \sum_{i=1}^r \lambda_i H_i$ of S we have $TT^{(-1)} = \sum_{i=1}^r \tilde{\lambda}_i \tilde{H}_i$ with parameters $\tilde{\lambda}_i = \frac{|G|}{|S|^3} \lambda_i |H_i|$.

Proof. Suppose S and T form a formally dual pair. Then by Theorem 4.4 we can choose a vrepresentation $SS^{(-1)} = \sum_{i=1}^r \lambda_i H_i$. Similar to Lemma 2.7 we have

$$\chi_g(H_i) = \begin{cases} |H_i| & \text{if } g \in \tilde{H}_i \\ 0 & \text{otherwise} \end{cases}.$$

Therefore,

$$v_T(g) = \frac{|T|}{|S|^2} |\chi_g(S)|^2 = \frac{|G|}{|S|^3} \sum_{i=1}^r \lambda_i \chi_g(H_i) = \frac{|G|}{|S|^3} \sum_{i : g \in \tilde{H}_i} \lambda_i |H_i|. \quad (4.1)$$

This yields $TT^{(-1)} = \sum_{i=1}^r \tilde{\lambda}_i \tilde{H}_i$.

On the other hand let $SS^{(-1)} = \sum_{i=1}^r \lambda_i H_i$ and $TT^{(-1)} = \sum_{i=1}^r \tilde{\lambda}_i \tilde{H}_i$. Then

$$v_T(g) = \sum_{i : g \in \tilde{H}_i} \tilde{\lambda}_i = \sum_{i=1}^r \tilde{\lambda}_i \chi_g(H_i) / |H_i| = \frac{|G|}{|S|^3} \sum_{i=1}^r \lambda_i \chi_g(H_i) = \frac{|T|}{|S|^2} |\chi_g(S)|^2.$$

This implies that S and T form a formally dual pair. \square

Given this insight, we can deduce the following result:

Corollary 4.6. *Let S and T form a formally dual pair, then the ranks of S and T are equal.*

Proof. Choose a minimal even set representation $SS^{(-1)} = \sum_{i=1}^r \lambda_i H_i$ for S by Theorem 4.4. By Theorem 4.5 we have $TT^{(-1)} = \sum_{i=1}^r \tilde{\lambda}_i \tilde{H}_i$. Therefore, the rank of T is not bigger than the rank of S . The dual argument shows that the rank of S is also not bigger than the rank of T , yielding the assertion. \square

Also, this approach can be used to prove formal duality as illustrated by the following result.

Corollary 4.7 ([LPS19, Theorem 3.7]). *Let S be an $(n, n, n, 1)$ -RDS with forbidden subgroup $N \leq G$. The sets S and T form a formally dual pair if and only if T is an $(n, n, n, 1)$ -RDS with respect to \tilde{N} .*

Proof. We have $SS^{(-1)} = G - N + n$. Observe that $|S| = n$, $|G| = n^2$. Thus, by Theorem 4.5 we know that S and T form a formally dual pair if and only if

$$TT^{(-1)} = \frac{|G|}{|S|^3} \left(n \cdot G - |N|\tilde{N} + 1 \cdot |G| \right) = G - \tilde{N} + n.$$

Equivalently T is an $(n, n, n, 1)$ -relative difference set with respect to \tilde{N} . \square

Note that all known relative difference sets share the property $N \simeq \tilde{N}$. In these cases S is formally self dual under any isomorphism such that $\tilde{N} = N$.

As seen above, the even set approach gives a nice tool to prove formal duality of given sets. Furthermore it can be used to display the connection of formally dual sets and relative difference sets (see Theorem 4.30 and Proposition 4.23). This is examined in the following sections.

4.2 Hasse-type diagrams

Recall that a representation of a formally dual set S has the form $\sum_{i=1}^r \lambda_i H_i$ with respective subgroups H_1, \dots, H_r . Apparently, the relations among the respective subgroups influence the level sets of the weight enumerator. Therefore, it is vital to consider such relations when using the even set approach on formally dual sets.

In this section, we develop a diagram, related to the Hasse-diagram, to visualize types of such relations.

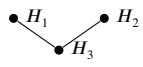
Definition 4.8. A *Hasse-diagram* is a visualization of a partially ordered set (V, \leq) with nodes identified with V and edges connecting the nodes as follows: The direction of an edge is given by the relative arrangements of the nodes. The edge always starts at the lower node and ends in the higher. There is an edge from a to b if and only if $a < b$ and there is no $c \in V$ with $a < c < b$. Therefore, the resulting diagram is an antitransitive directed graph (i.e. $ab, bc \in E \rightarrow ac \notin E$) with the following property: Two nodes a and b are connected via a directed path p if and only if $a < b$.

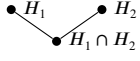
In particular, the set of subgroups of G is partially ordered by the subgroup relation and thus induces a Hasse-diagram. When considering even sets, it is useful to examine the Hasse-diagrams of the subgroups of G with a focus on the respective subgroups. We aim for a graphical language capable to express common conditions on Hasse-diagrams in a way that is quickly applicable. In the following, we define Hasse-type diagrams which enhance Hasse-diagrams with further elements.

Definition 4.9. A *Hasse-type diagram* (D, c) consists of two components. The first component $D = D(V, E)$ is a visualization of an antitransitive directed graph where the direction of the edges is indicated by the relative position of the nodes similar to the edges of the Hasse-diagram. The nodes are chosen from three types (namely real nodes \bullet , appended nodes \circ and subgraph nodes ☁) and the edges are chosen from two types (namely regular edges $|$ and 'less-or-equal' edges $|;$). We set $V(\bullet) = \{v \in V : v \text{ is of type } \bullet\}$ and $V(\circ), V(\text{☁}), E(|), E(|;)$ respectively.

The second component c refers to a set of equations with variables in V , where nodes of type \bullet or \circ are treated as subgroups and nodes of type ☁ are treated as sets of subgroups.

These diagrams have the property that they distinguish between respective subgroups and other subgroups (\bullet and \circ nodes), they can unify subgraphs in single nodes (☁ nodes) and can visualize a \leq condition among the nodes (by the additional type of edge $|;$). Since we emphasize on the respective subgroups, we only require those to be present in the diagram while other subgroups can be added to provide additional information. For further simplification we might visualize equations of the form $H = \text{Expression}$ within D by writing the Expression next to

the node H (for example we condense $D =$ , $c = \{H_3 = H_1 \cap H_2\}$ to



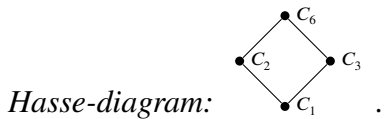
). Thus, a Hasse-type diagram helps to distinguish between different types of respective subgroups \mathcal{H} . To be precise:

Definition 4.10. Let $\Lambda = \mathcal{H} \dot{\cup} \mathcal{L}$ be the set of subgroups of G and $(D(V, E), c)$ a Hasse-type diagram. We say \mathcal{H} fits $(D(V, E), c)$ if we can identify the nodes in V with sets of subgroups by an *admissible identification map* $\phi : V \mapsto 2^\Lambda$ satisfying

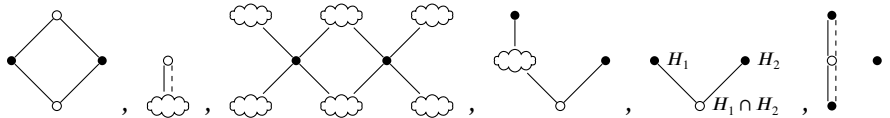
1. any node h of type \bullet is identified by exactly one subgroup in \mathcal{H} ,
i.e. $\phi(h) = \{H\} \subseteq \mathcal{H}$,
2. any node l of type \circ is identified with exactly one subgroup,
i.e. $\phi(l) = \{L\} \subseteq \Lambda = \mathcal{H} \dot{\cup} \mathcal{L}$,
3. any node K of type ☁ is identified with a subset of \mathcal{H} of arbitrary size,
i.e. $\phi(K) \subseteq \mathcal{H}$ (Note that $\phi(K)$ is possibly empty),
4. all subgroups in \mathcal{H} are represented by a \bullet or ☁ node,
i.e. $\phi(V(\bullet) \cup V(\text{☁})) = \mathcal{H}$ (subgroups in \mathcal{H} need to be represented in the diagram while subgroups in \mathcal{L} don't),
5. the edges among nodes which are not identified with the empty set are inherited from the Hasse-diagram of Λ , where an \parallel edge indicates the possibility to be identified with the same subgroup;
i.e. two nodes $h_1, h_2 \in V$ with $\phi(h_1), \phi(h_2) \neq \emptyset$ are connected via a directed path p (where the direction is given by the relative positions of the nodes) if and only if $H_1 \leq H_2$ for all $H_1 \in \phi(h_1), H_2 \in \phi(h_2)$; Furthermore, if $\phi(h_1) \cap \phi(h_2) \neq \emptyset$ ($H_1 = H_2$ for some $H_1 \in \phi(h_1), H_2 \in \phi(h_2)$) then *all* edges of p are of type \parallel ;
6. a node K (of type ☁) which is identified with the empty set might be contained in arbitrary edges (☁ nodes can be ignored by identifying them with the empty set),
7. all equations in c are satisfied under the identification (after substituting all nodes $h \in V(\bullet) \cup V(\circ)$ by H , where $\phi(h) = \{H\}$ and all ☁ nodes K by $\phi(K)$).

Note, that the structure of \mathcal{H} is represented by the \bullet and ☁ nodes. The \circ nodes give additional information. It follows from Definition 4.10 that a \circ node will be identified with a subgroup in \mathcal{L} unless there is a || connection which allows otherwise. We provide an example to comprehend the capabilities of Hasse-type diagrams:

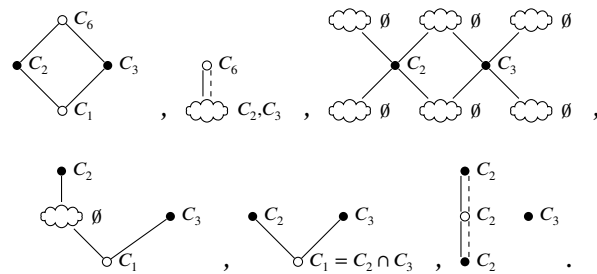
Example 4.11. Let $G = C_6$ and $\mathcal{H} = \{C_2, C_3\}$. The group G has the following



Observe, that \mathcal{H} fits all of the following Hasse-type diagrams:



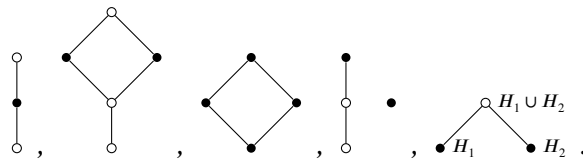
This can be easily verified by using the following identifications:



Note that the admissible identifications are not unique, for example the identifica-



On the other hand \mathcal{H} does not fit the following Hasse-type diagrams:



We give some reasoning for that using the properties of an admissible identification map as in Definition 4.10:

1. doesn't contain enough \bullet nodes (see Properties (1), (4)),
2. has to be identified with five distinct subgroups, but there are only four (see Properties (1), (2), (5)),
3. has to be identified with four distinct subgroups in \mathcal{H} but $|\mathcal{H}| = 2$ (see Properties (1), (5)),
4. there is no subgroup of C_2 which is not a subgroup of C_3 and vice versa, therefore there is no admissible identification to justify this example (see Properties (1), (2), (5)),
5. we need to identify H_1, H_2 with C_2, C_3 (in any order) and the upper \circ node with C_6 , but $C_6 \neq C_2 \cup C_3$ (see Properties (1), (2), (5), (7))

For an easy applicable way to use Hasse-type diagrams in theorems we use the following notation:

Let (D, c) be a Hasse-type diagram. A statement in the nodes of D is supposed to be true if and only if it is true under every admissible identification map for every set \mathcal{H} fitting (D, c) .

For example, in the diagram $\begin{array}{c} \bullet \\ \vdots \\ \bullet \end{array} \begin{array}{l} H_2 \\ \\ H_1 \end{array}$ the statement $H_1 \leq H_2$ is true and the statement $H_1 < H_2$ is false (since it is false for $\mathcal{H} = \{C_2\}$ and the identification given by $\begin{array}{c} \bullet \\ \vdots \\ \bullet \end{array} \begin{array}{l} C_2 \\ \\ C_2 \end{array}$).

We conclude this section with a notion that allows to apply Hasse-type diagrams to even sets and in particular to formally dual sets.

Definition 4.12. Let S be an even set and (D, c) be a Hasse-type diagram. We say that S is of type (D, c) if there is a representation $SS^{(-1)} = \sum_{i=1}^r \lambda_i H_i$ of S such that the set of respective subgroups $\mathcal{H} = \{H_1, \dots, H_r\}$ fits (D, c) .

In account to study formally dual pairs, it is useful to use the dual Hasse-type diagram:

Definition 4.13. Let $(D(V, E), c)$ be a Hasse-type diagram. The *dual Hasse-type diagram* is defined to be $(D(V', E'), c')$ where

$$V' = \{\tilde{h} : h \in V\}, \quad E' = \{(\tilde{h}, \tilde{l}) : (l, h) \in E\}$$

and c' is obtained by substituting all equations $E = F$ from c by $\tilde{E} = \tilde{F}$.

The benefit of this notion is shown by the following result:

Lemma 4.14. *If S and T form a formally dual pair and S is of type (D, c) , then T is of type (D', c') where (D', c') is the dual Hasse-type diagram of (D, c) .*

Proof. Let $D = D(V, E)$ and \mathcal{H} be a set of respective subgroups of S fitting (D, c) by the admissible identification ϕ . Denote $\tilde{\mathcal{H}} = \{\tilde{H} : H \in \mathcal{H}\}$ and $\tilde{\phi} : V' \rightarrow 2^\Lambda, \tilde{h} \mapsto \overline{\phi(h)}$. It is easy to show that $\tilde{\phi}$ is an admissible identification for $\tilde{\mathcal{H}}$ and (D', c') by the observation that $H_1 \leq H_2$ if and only if $\tilde{H}_1 \geq \tilde{H}_2$ and Definition 4.10. \square

In the following sections we use this formulation to simplify various results.

4.3 Even set approach on formally dual sets

In this section we examine several additional conditions of formally dual sets when written in terms of even sets. Especially, we will examine formally dual sets of certain types, thereby formulating many alternative proofs of known results. For the rest of this chapter we consider $S, T \subset G$ with $SS^{(-1)} = \sum_{i=1}^r \lambda_i H_i$ and $TT^{(-1)} = \sum_{i=1}^r \tilde{\lambda}_i \tilde{H}_i$ where $\tilde{\lambda}_i = \frac{|G|}{|S|^3} |H_i| \lambda_i$ and $\mathcal{H} = \{H_1, \dots, H_r\}$.

First we study the even set representations of primitive formally dual sets.

Lemma 4.15 ([LPS19, Lemma 4.11]). *If S is a primitive formally dual set, then:*

1. $\langle \mathcal{H} \rangle = \langle H_1, \dots, H_r \rangle = G$,
2. $\bigcap \mathcal{H} = H_1 \cap \dots \cap H_r = \{1\}$.

Proof. Suppose S is not contained in a proper coset. Then the nonzero addends of $SS^{(-1)} = \sum_{i=1}^r \lambda_i H_i$ are not contained in a proper subgroup. Thus the H_i span G . By Lemma 3.21 we know that T and S form a formally dual pair under Δ_* and by Lemma 2.1

$$\tilde{\tilde{H}}_i = \Delta_*^{-1}(\tilde{H}_i)^\perp = \Delta_*^{-1} \Delta_* H_i = H_i.$$

Therefore $\tilde{H}_1, \dots, \tilde{H}_r$ also span G and

$$H_1 \cap \dots \cap H_r = \tilde{\tilde{H}}_1 \cap \dots \cap \tilde{\tilde{H}}_r = \tilde{G} = \{1\}.$$

□

Of course, the representation as an even set is strongly connected to the weight enumerator. The following lemma inherits inequalities of the weight enumerator to the even set representation:

Lemma 4.16. *If S is a formally dual set, then we have*

1. $\sum_{i=1}^r \lambda_i = |S|$,
2. $\sum_{i=1}^r \lambda_i |H_i| = |S|^2$.

Furthermore, for all $g \in G$ with $g \neq 1$ we have

3. $v_S(g) = \sum_{i: g \in H_i} \lambda_i \in \mathbb{Z}$, $0 \leq \sum_{i: g \in H_i} \lambda_i \leq |S|$,
4. $\frac{|S|^3}{|G|} v_T(g) = \sum_{i: g \in \tilde{H}_i} \lambda_i |H_i| \in \mathbb{Z}$, $0 \leq \sum_{i: g \in \tilde{H}_i} \lambda_i |H_i| \leq |S|^2$.

Moreover, S is primitive if and only if the inequalities (3) and (4) are strict.

Proof. It is easy to see that $v_S(g) = [SS^{-1}]_g = \sum_{i: g \in H_i} \lambda_i$. Furthermore,

$$\frac{|S|^3}{|G|} v_T(g) = \sum_{i: g \in \tilde{H}_i} \frac{|S|^3}{|G|} \tilde{\lambda}_i = \sum_{i: g \in \tilde{H}_i} \lambda_i |H_i|.$$

The assertion follows by applying

$$v_S(1) = |S|, v_T(1) = |T|, 0 \leq v_S(g) \leq |S|, 0 \leq v_T(g) \leq |T| = \frac{|G|}{|S|}.$$

Note that S is a union of cosets of H if and only if $v_S(g) = |S|$ for every $g \in H$.

On the other hand, by Theorem 3.15 S is contained in a coset of H if and only if T is a union of cosets of \tilde{H} if and only if $v_T(g) = |T|$ for all $g \in \tilde{H}$. This is equivalent to

$$\sum_{i: g \in \tilde{H}_i} \lambda_i |H_i| = \frac{|S|^3}{|G|} v_T(g) = \frac{|S|^2}{|T|} \cdot |T| = |S|^2.$$

Thus, if S is primitive, then the inequalities (3) and (4) are strict. □

It is possible to have a formally dual set which is an even set with integer parameters, but the parameters of its formal dual given by Theorem 4.5 are non-integral. For example for $G = C_2 \times C_2 = \langle g \rangle \times \langle h \rangle$ it is possible to write

$$G = \langle g \rangle + \langle h \rangle + \langle gh \rangle - 2.$$

We know that $S = G$ and $T = \{1\}$ form a formally dual pair. Theorem 4.5 gives a non-integral even set representation for T

$$SS^{(-1)} = |G|G = 4G = 4\langle g \rangle + 4\langle h \rangle + 4\langle gh \rangle - 8$$

and thus

$$TT^{(-1)} = \frac{1}{2}\widetilde{\langle g \rangle} + \frac{1}{2}\widetilde{\langle h \rangle} + \frac{1}{2}\widetilde{\langle gh \rangle} - \frac{1}{2}G = \{1\}\{1\}^{(-1)}.$$

Note, that in contrary to above the minimal representations of S and T given by Theorem 4.5 are both integral.

Thus we conjecture the following:

Conjecture 4.17. *A minimal representation of an even set has integral parameters. Thereby, the even set representation obtained by Theorem 4.5 of the formal dual has also integral parameters.*

A sufficient condition for the integrality of the even set parameters is given by the following notion:

Definition 4.18. Let \mathcal{L} be a family of subgroups of G . An element $L \in \mathcal{L}$ is called *impartible* in \mathcal{L} if

$$L \not\subset \bigcup_{L' \in \mathcal{L} : L \not\leq L'} L'.$$

A set $S \subset \mathcal{L}$ is called *impartible* in \mathcal{L} if every element is impartible.

We shed light on this definition by the following Lemma:

Lemma 4.19. *Let $SS^{(-1)} = \sum_{i=1}^r \lambda_i H_i$ be an even set representation. If H_i is impartible in \mathcal{H} and $\lambda_j \in \mathbb{Z}$ for all j such that $H_i < H_j$, then $\lambda_i \in \mathbb{Z}$. Especially, if $\{H \in \mathcal{H} : H_i \leq H\}$ is impartible in \mathcal{H} then $\lambda_i \in \mathbb{Z}$.*

Proof. Since H_i is impartible, we can choose $g \in H_i \setminus \bigcup_{H \in \mathcal{H} : H_i \not\leq H} H$. Then

$$v_S(g) = \sum_{j : g \in H_j} \lambda_j = \lambda_i + \underbrace{\sum_{j : H_i < H_j} \lambda_j}_{\in \mathbb{Z}} \in \mathbb{Z}$$

and thus $\lambda_i \in \mathbb{Z}$. □

The impartible property might be tedious to check. However, the following lemma describes a weaker criterion:

Lemma 4.20. *Let \mathcal{L} be a family of subgroups of G and $L \in \mathcal{L}$. Define*

$$I(L) = \{L' \in \mathcal{L} : L \not\subseteq L'\}.$$

Furthermore, denote by $i(L)$ the size of a smallest set $J \subset I(L)$ such that $\bigcup J = \bigcup I(L)$. If $i(L) \leq 2$ then L is impartible in \mathcal{L} .

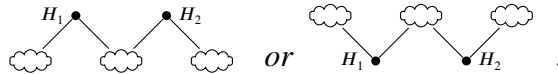
Proof. Suppose $L \in \mathcal{L}$ is not impartible and therefore $L \subset \bigcup I(L)$ but $i(L) \leq 2$. If $i(L) = 0$ then $L \subset \emptyset$ which is a contradiction.

If $i(L) = 1$ then there is a $K \in I(L)$ such that $L \subset K$ which is a contradiction to the definition of $I(L)$.

If $i(L) = 2$ then there are $K, K' \in I(L)$ such that $L \subset K \cup K'$. The set $(L \cap K) \setminus K'$ is nonempty since otherwise $L \cap K \subset K'$ and therefore $L \subset K'$ and $i(L) \leq 1$. Same is true for $(L \cap K') \setminus K$. But if $x \in (L \cap K) \setminus K'$ and $y \in (L \cap K') \setminus K$ then $xy \in L \setminus (K \cup K')$ which is a contradiction. \square

Furthermore, we notice that a primitive formally dual set cannot have two maximal or minimal subgroups in the following sense:

Lemma 4.21 ([LPS19, Lemma 4.15]). *Let S be a primitive formally dual set. Then S is not of type*



Proof. First suppose that S is of the first type. Fix $v \in S$.

We claim that there are some $x, y \in S$ such that $v \cdot x^{-1} \in H_1 \setminus H_2$ and $v \cdot y^{-1} \in H_2 \setminus H_1$. Indeed, if for all $w \in S$ we would have $v \cdot w^{-1} \in H_1$ this would contradict the primitivity of S .

But then

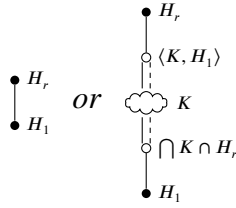
$$x \cdot y^{-1} = (x \cdot v^{-1}) \cdot (v \cdot y^{-1}) \notin H_1 \cup H_2$$

which is a contradiction.

Now suppose S is of the second type, then its formal dual T is of the first type by Lemma 4.14. This contradicts the fact shown above. \square

The following Lemma examines a special case that leads to further structural properties of S and is a generalization of [LPS19, Proposition 4.12]. We emphasize that in this case it follows that $|S| = |T|$ which is true for many known examples.

Proposition 4.22. *If S is a primitive formally dual set of type*



then $|G|$ is a square number and $|T| = |S| = \sqrt{|G|}$. Furthermore, $H_r = G$, $H_1 = \{1\}$, $\lambda_1 = \tilde{\lambda}_r = |S|$ and $\tilde{\lambda}_1 = \lambda_r = 1$.

Proof. By Lemma 4.15 it is obvious that $H_1 = \{1\}$ and $H_r = G$.

Let $g \in H_2 \cap \dots \cap H_r \setminus H_1$. Then we have

$$\lambda_1 = \underbrace{\sum_{i=1}^r \lambda_i}_{=|S|} - \underbrace{\sum_{i=2}^r \lambda_i}_{=v_S(g)} .$$

Applying Lemma 4.16 we thus have $0 < \lambda_1 \leq |S|$ and $\lambda_1 \in \mathbb{Z}$. In a similar manner, taking $h \in \tilde{H}_1 \setminus (\widetilde{\bigcap K \cap H_r})$ we have $\tilde{\lambda}_1 = v_T(h)$ and thus $\tilde{\lambda}_1$ is a positive integer. So by Theorem 4.5 we have

$$1 \leq \tilde{\lambda}_1 = \frac{|G|}{|S|^3} \lambda_1 |H_1| \leq \frac{|G|}{|S|^2} .$$

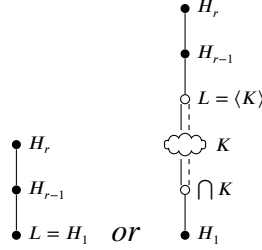
An analog argument in T using Lemma 4.14 can be used to show $1 \leq \frac{|G|}{|T|^2} = \frac{|S|^2}{|G|}$.

Altogether, $|S|^2 = |G|$ and equivalently $|S| = |T| = \sqrt{|G|} \in \mathbb{Z}$. Using the above inequalities, we thus have $\tilde{\lambda}_1 = \lambda_r = 1$, $\lambda_1 = \tilde{\lambda}_r = |S|$.

□

The following result shows a strong connection among formally dual sets of a certain type and relative difference sets. The proof uses ideas from [Sch17, Lemma 4.1] and [Xia16, Section 3.2] in a new context.

Proposition 4.23. *Let S be a primitive formally dual set of type*



and $\phi : G \rightarrow G/L$ be the natural reduction map. Then $|S \cap a \cdot H_{r-1}| = \frac{|H_{r-1}|}{|S|}$ for all $a \in G$ and $\phi(S)$ is an $\left(\frac{|S|^2}{|H_{r-1}|}, \frac{|H_{r-1}|}{|L|}, \frac{|S|^2}{|H_{r-1}|}, \frac{|L| \cdot |S|^2}{|H_{r-1}|^2} \right)$ -RDS. In particular $\lambda_{r-1} = -1$.

Proof. By applying Proposition 4.22 we have

$$H_r = G, H_1 = \{1\}, \lambda_r = 1, \lambda_1 = |S| \text{ and } |S|^2 = |G|.$$

Furthermore, we take $g \in \tilde{L} \setminus \tilde{H}_{r-1}$ and get

$$\sum_{i=1}^{r-2} \lambda_i |H_i| = \sum_{i: g \in \tilde{H}_i} \lambda_i |H_i| \geq 0$$

by Lemma 4.16. The same Lemma also yields

$$\sum_{i=1}^{r-1} \lambda_i |H_i| + |S|^2 = \sum_{i=1}^r \lambda_i |H_i| = |S|^2$$

which is equivalent to $\sum_{i=1}^{r-1} \lambda_i |H_i| = 0$. Altogether,

$$-\lambda_{r-1} |H_{r-1}| = \sum_{i=1}^{r-2} \lambda_i |H_i| \geq 0$$

which yields $\lambda_{r-1} < 0$. For any $g \in H_{r-1} \setminus L$ we apply Lemma 4.16 again to get $v_S(g) = \lambda_{r-1} + 1 = \lambda_{r-1} + \lambda_r \geq 0$ and thus $v_S(g) = 0$, $\lambda_{r-1} = -1$.

Furthermore, we have

$$H_{r-1} \cdot SS^{(-1)} = \sum_{i=1}^r \lambda_i H_i H_{r-1} = \underbrace{\left(\sum_{i=1}^{r-1} \lambda_i |H_i| \right)}_{=0} H_{r-1} + |H_{r-1}|G = |H_{r-1}|G.$$

Therefore by Lemma 2.5 the differences of S in aH_{r-1} are exactly

$$\sum_{g \in aH_{r-1}} \nu_S(g) = \sum_{g \in aH_{r-1}} [SS^{(-1)}]_g = |H_{r-1}|$$

for all $a \in G$. In particular for $a = 1$.

Let \mathcal{A} be a system of representatives of G/H_{r-1} in G . Clearly any sum of squares $\sum_{i=1}^m \mu_i^2$ is minimized under the conditions $\sum_{i=1}^m \mu_i = c$ and $\mu_i \geq 0$ if and only if $\mu_i = \frac{c}{m}$. Thus, we can bound the number of differences in H_{r-1} as

$$|H_{r-1}| = \sum_{a \in \mathcal{A}} |S \cap a \cdot H_{r-1}|^2 \geq \sum_{a \in \mathcal{A}} \left(\frac{|S|}{[G : H_{r-1}]} \right)^2 = \frac{|S|^2}{[G : H_{r-1}]} = |H_{r-1}|.$$

Therefore we get $|S \cap a \cdot H_{r-1}| = \frac{|S|}{[G : H_{r-1}]} = \frac{|H_{r-1}|}{|S|}$ for all $a \in \mathcal{A}$.

Now let $a \cdot H_{r-1}$ be an arbitrary coset. We claim that the elements of $S \cap a \cdot H_{r-1}$ are all contained in the same coset of L . Indeed, suppose there are $x, y \in S \cap a \cdot H_{r-1}$, and $x \notin yL$. Clearly $xy^{-1} \in H_{r-1} \setminus L$ and $xy^{-1} \in \text{supp}(SS^{(-1)})$ which is a contradiction since $\nu_S(xy^{-1}) = \lambda_r + \lambda_{r-1} = 0$.

Therefore $|S \cap aL| \in \{0, \frac{|H_{r-1}|}{|S|}\}$ for all $a \in G$ and by Lemma 2.6 we have

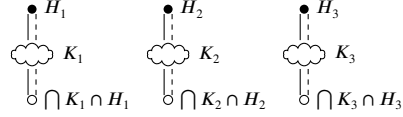
$$\begin{aligned} \phi(S) \cdot (\phi(S))^{(-1)} &= \frac{|S|^2}{|H_{r-1}|^2} (SS^{(-1)})^{(\phi)} = \frac{|S|^2}{|H_{r-1}|^2} \left(\sum_{i=1}^r \lambda_i H_i^{(\phi)} \right) \\ &= \frac{|S|^2}{|H_{r-1}|^2} \left(\underbrace{\sum_{i=1}^{r-2} \lambda_i |H_i|}_{=|H_{r-1}|} - |L \cdot H_{r-1}/L + |L \cdot G/L \right) \\ &= \frac{|S|^2 \cdot |L|}{|H_{r-1}|^2} (G/L - H_{r-1}/L) + \frac{|S|^2}{|H_{r-1}|} \end{aligned}$$

Thus, we have that $\phi(S)$ is a relative difference set of size $\frac{|S|^2}{|H_{r-1}|}$ with forbidden subgroup H_{r-1}/L and parameter $\frac{|L| \cdot |S|^2}{|H_{r-1}|^2}$ in a group of size $\frac{|G|}{|L|} = \frac{|S|^2}{|H_{r-1}|} \cdot \frac{|H_{r-1}|}{|L|}$ and thus an $(\frac{|S|^2}{|H_{r-1}|}, \frac{|H_{r-1}|}{|L|}, \frac{|S|^2}{|H_{r-1}|}, \frac{|L| \cdot |S|^2}{|H_{r-1}|^2})$ -RDS as asserted. \square

Remark 4.24. *The results of Proposition 4.22 and Proposition 4.23 are in particular true if S is an even set with respect to a sufficiently long chain of subgroups.*

In the following we present a lemma which generalizes [LPS19, Lemma 4.18] and is preparatory for Lemma 4.26.

Lemma 4.25. *Let S be a primitive formally dual set of type*



with $1 \in S$.

Let $S_1 = \{x \in S : x \in H_1, x \notin H_2, x \notin H_3\}$ and S_2, S_3 analogously. Furthermore, let $S_{12} = \{x \in S : x \in H_1, x \in H_2, x \notin H_3\}$ and S_{13}, S_{23} analogously.

Then the following is true:

1. either $S_1 = \emptyset$ or $S_{23} = \emptyset$,
2. if $S_1 \neq \emptyset, S_2 \neq \emptyset$ then $\text{supp}(S_1 S_1^{(-1)}) \subset H_1 \cap H_3$ and
3. $\text{supp}(S_1 S_2^{-1}) \subset H_3 \setminus (H_1 \cup H_2)$.

Note that these statements also hold for any permutation of the indices $\{1, 2, 3\}$.

Proof. 1. Suppose $x \in S_1$ and $y \in S_{23}$. Observe that $xy^{-1} \notin H_1 \cup H_2 \cup H_3$ which contradicts the type of S .

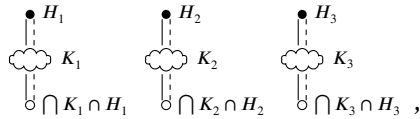
2. Let $x, y \in S_1$. Furthermore let $z \in S_2$, thus $xz^{-1}, yz^{-1} \notin H_1 \cup H_2$. Since $xz^{-1}, yz^{-1} \in \text{supp}(S S^{(-1)})$ we can see by the type of S that $xz^{-1}, yz^{-1} \in H_3$. Therefore, $H_1 \ni xy^{-1} = (xz^{-1})(yz^{-1}) \in H_3$.

3. The assertion is apparent noticing that $xy^{-1} \notin (H_1 \cup H_2)$ for all $x \in S_1, y \in S_2$ and the type of S .

□

With these insights we are able to prove an upper bound of primitive formally dual sets of a certain type.

Lemma 4.26. *Let S be a primitive formally dual set of type*



such that $\{H_1, H_2, H_3\}$ is impartible in \mathcal{H} . Then $|S| \leq 6|H_1 \cap H_2 \cap H_3|$.

Proof. We use the same notation as in the condition of Lemma 4.26. By Lemma 4.19 $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}$ and we can choose $g \in H_1 \setminus (H_2 \cup H_3)$ such that g is not contained in any other subgroup of K_1 . We have $v_S(g) = \lambda_1 > 0$. Therefore there is a pair $x, y \in S$ such that $xy^{-1} \in H_1 \setminus (H_2 \cup H_3)$. Thus the set $y^{-1}S$ contains $1 = y^{-1}y$ and $y^{-1}S \cap H_1 \neq \emptyset$ since $y^{-1}x \in y^{-1}S \cap H_1$. So without loss of generality (after translation of S) we might assume $1 \in S$ and $S_1 \neq \emptyset$

Next, we discuss three cases:

$S_2, S_3 \neq \emptyset$:

Then $S_{12}, S_{13}, S_{23} = \emptyset$ by Lemma 4.26. Furthermore, we have

$$\text{supp}(S_i S_i^{(-1)}) \subset H_1 \cap H_2 \cap H_3 \text{ for every } i = 1, 2, 3.$$

Therefore S_i is contained in a coset of $H_1 \cap H_2 \cap H_3$ and thus $|S_i| \leq |H_1 \cap H_2 \cap H_3|$. Altogether $|S| = 1 + |S_1| + |S_2| + |S_3| \leq 1 + 3|H_1 \cap H_2 \cap H_3|$.

One of S_2, S_3 is empty, the other is nonempty:

Without loss of generality we might assume that $S_2 \neq \emptyset$ and $S_3 = \emptyset$. By Lemma 4.26 we have $S_{13}, S_{23} = \emptyset$. Furthermore, we have for any $v \in H_3 \cap \bigcap K_3 \setminus (H_1 \cup H_2)$:

$$v_S(v) = [SS^{(-1)}]_v = [S_1 S_2^{(-1)}]_v + [S_2 S_1^{(-1)}]_v.$$

Let $x, y \in S_1$ such that $xv, yv \in S_2$. Then, by Lemma 4.26

$$H_1 \cap H_3 \ni xy^{(-1)} = (xv)(yv)^{(-1)} \in H_2 \cap H_3.$$

Therefore x and y are in the same coset of $H_1 \cap H_2 \cap H_3$ yielding

$$\lambda_1 + \sum_{i: H_i \in K_1} \lambda_i = v_S(v) \leq 2 \cdot |H_1 \cap H_2 \cap H_3|.$$

Like seen above, we can translate S such that $1 \in S$ and $S_2 = \emptyset$. An analog argument shows that $\lambda_2 + \sum_{i: H_i \in K_2} \lambda_i \leq 2 \cdot |H_1 \cap H_2 \cap H_3|$. In a similar manner we also show $\lambda_3 + \sum_{i: H_i \in K_3} \lambda_i \leq 2 \cdot |H_1 \cap H_2 \cap H_3|$.

Altogether

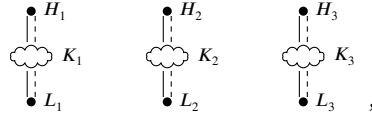
$$|S| = \sum_{i=1}^r \lambda_i = \sum_{j=1}^3 \left(\lambda_j + \sum_{i: H_i \in K_j} \lambda_i \right) \leq 6|H_1 \cap H_2 \cap H_3|.$$

$S_2 = S_3 = \emptyset$:

This case is a contradiction to the primitivity of S since then $S \subset H_1$. \square

If we are in a situation where we can apply above result on both sets of a formally dual pair, we obtain the following:

Corollary 4.27. *Let S be a primitive formally dual set of type*



such that $\{H_1, H_2, H_3\}$ is impartible in \mathcal{H} and $\{\tilde{H}_1, \tilde{H}_2, \tilde{H}_3\}$ is impartible in $\tilde{\mathcal{H}}$. Then $|\langle L_1, L_2, L_3 \rangle| \leq 36 \cdot |H_1 \cap H_2 \cap H_3|$.

Proof. Apparently the asserted Hasse-type diagram as well as its dual diagram fit the assumption of Lemma 4.25. Thus, by Lemma 4.14 we have

$$|S| \leq 6|H_1 \cap H_2 \cap H_3|$$

and

$$|T| \leq 6 \cdot |\tilde{L}_1 \cap \tilde{L}_2 \cap \tilde{L}_3| = 6 \cdot |\langle L_1, L_2, L_3 \rangle| = 6 \cdot \frac{|G|}{|\langle L_1, L_2, L_3 \rangle|}.$$

By multiplying both inequalities we have

$$|G| \leq 36 \cdot |H_1 \cap H_2 \cap H_3| \cdot \frac{|G|}{|\langle L_1, L_2, L_3 \rangle|}$$

which is equivalent to the assertion. \square

The results on the even set structure of formally dual sets are a useful tool that we use in Sections 4.4 and 5.2.

4.4 Formally dual sets of small rank

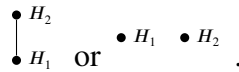
In this section we study primitive formally dual sets of rank less or equal to four. We characterize primitive formally dual sets up to rank three and give some statements about rank four primitive formally dual sets.

Lemma 4.28. *If S is a primitive formally dual set of rank one, then $S = G = \{1\}$.*

Proof. Since S has rank one, $SS^{(-1)} = \lambda H$. Lemma 4.15 yields, that $H = \{1\}$ and on the other hand $H = G$. Thus $S = G = \{1\}$. \square

Lemma 4.29. *There is no primitive formally dual set of rank two.*

Proof. Suppose S is as asserted. There are only two possible Hasse-diagrams for two subgroups, namely

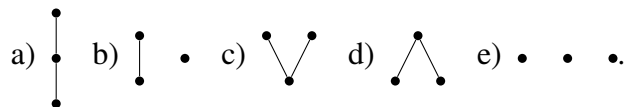


By Lemma 4.21 we can exclude the second case. Thus by Proposition 4.22 we have $H_1 = \{1\}$, $H_2 = G$, $\lambda_1 = |S|$, $\lambda_2 = 1$, but this is a contradiction to Lemma 4.16 since $\lambda_1 + \lambda_2 \neq |S|$. \square

Certain relative difference sets are examples of primitive formally dual pairs of rank three (see Corollary 4.7). The following theorem shows, that there are no other examples:

Theorem 4.30 ([LPS19, Theorem 4.19]). *If S is a primitive formally dual set of rank three, then it is an $(n, n, n, 1)$ -RDS.*

Proof. There are the following possible Hasse-diagrams of three subgroups:



By Lemma 4.21 we can exclude the possibilities b), c) and d) from our discussion.

If S has a Hasse-diagram of type a) it follows by Proposition 4.22 that its Hasse-

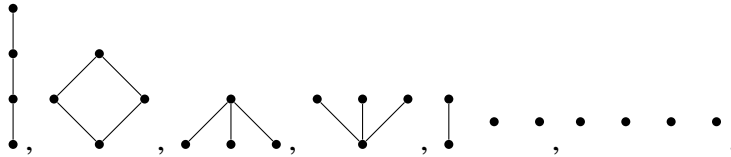
diagram is $\begin{matrix} \bullet & H_3 = G \\ | \\ \bullet & H_2 \\ | \\ \bullet & H_1 = \{1\} \end{matrix}$ and $\lambda_1 = |S|$, $\lambda_3 = 1$, $|G| = |S|^2$. By Proposition 4.23 S is an $\left(\frac{|S|^2}{|H_2|}, |H_2|, \frac{|S|^2}{|H_2|}, \frac{|S|^2}{|H_2|^2}\right)$ -RDS. Therefore $|S| = \frac{|S|^2}{|H_2|}$ yielding $|H_2| = |S|$ and therefore S is an $(n, n, n, 1)$ -RDS for $n = |S|$.

If S has a Hasse-diagram of type e) it follows by Corollary 4.27, Lemma 4.20 and Lemma 4.15 that

$$|G| = |\langle H_1, H_2, H_3 \rangle| \leq 36 \cdot |H_1 \cap H_2 \cap H_3| = 36.$$

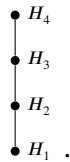
By Table A.1 in the Appendix we see that all rank three primitive formally dual sets in groups of order not bigger than 36 are $(n, n, n, 1)$ -RDS. Note that if S is a product of two RDS then S is not an $(n, n, n, 1)$ -RDS and $\text{supp}(SS^{(-1)})$ is not a union of three subgroups. By the above discussion these examples can not have rank three. \square

When examining formally dual sets, we have examples which are even with respect to a chain of subgroups of odd length (see Example 6.2). But there are also examples that don't seem to permit such a structure (see Theorem 6.4). The following question remains open: which is the smallest rank of a formally dual set which is not even with respect to a chain of subgroups? At this point it cannot be completely ruled out that such a set has rank four. By Lemma 4.21 we know that the respective subgroups of a rank four primitive formally dual set has to have one of the following types:



In the following we present partial results on some of these types.

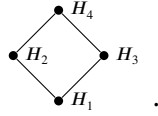
Lemma 4.31. *There is no primitive formally dual set of type*



Proof. Suppose $S \subset G$ is such a set. Due to Lemma 4.15 and Proposition 4.22, we have $H_1 = \{1\}$, $H_4 = G$, $\lambda_1 = |S|$, $\lambda_4 = 1$ and $|G| = |S|^2$.

We apply Proposition 4.23 to see that $\lambda_3 = -1$. But then, by Lemma 4.16 $|S| + \lambda_2 - 1 + 1 = |S|$ yielding $\lambda_2 = 0$ which is a contradiction. \square

Lemma 4.32. *There is no primitive formally dual set of type*



Proof. Suppose S is such a primitive formally dual set. By Lemma 4.15 we have $H_4 = G$ and $H_1 = \{1\}$. Let T be a formal dual of S . Since T is by Lemma 4.14 also of the asserted type we assume without loss of generality $|S|^2 \leq |G| \leq |T|^2$. By Lemma 4.20 we know that both \mathcal{H} and $\tilde{\mathcal{H}}$ are impartible in \mathcal{H} and $\tilde{\mathcal{H}}$ respectively. Thus, by Lemma 4.19 we have $\lambda_i, \tilde{\lambda}_i \in \mathbb{Z}$ for all i . In particular,

$$\lambda_4 = \frac{|G|}{|T|^3} \tilde{\lambda}_4 |\tilde{H}_4| = \frac{|S|}{|T|^2} \tilde{\lambda}_4 \in \mathbb{Z}$$

and therefore $|T|^2$ divides $|S| \cdot \tilde{\lambda}_4$. Furthermore, using Lemma 4.16 we have

$$|T| = \tilde{\lambda}_1 + \tilde{\lambda}_2 + \tilde{\lambda}_3 + \tilde{\lambda}_4 = \underbrace{(\tilde{\lambda}_1 + \tilde{\lambda}_2)}_{0 \leq \dots < |T|} + \underbrace{(\tilde{\lambda}_1 + \tilde{\lambda}_3)}_{0 \leq \dots < |T|} - \underbrace{\tilde{\lambda}_1}_{0 \leq \dots < |T|} + \tilde{\lambda}_4$$

and therefore $-|T| < \tilde{\lambda}_4 < 2|T|$ which is equivalent to

$$-|G| < |S| \cdot \tilde{\lambda}_4 < 2|G|. \quad (4.2)$$

Since $|T|^2 \geq |G|$ divides $|S| \cdot \tilde{\lambda}_4$ this yields $\tilde{\lambda}_4 = \frac{|T|^2}{|S|} \geq |T|$ and $|T| < 2|S|$.

By applying Lemma 4.16 again we additionally have $\tilde{\lambda}_1 + \tilde{\lambda}_2, \tilde{\lambda}_1 + \tilde{\lambda}_3 \geq 0$ and $\tilde{\lambda}_1 + \tilde{\lambda}_2 + \tilde{\lambda}_3 \leq 0$ and thus $\tilde{\lambda}_2, \tilde{\lambda}_3 < 0, \tilde{\lambda}_1 > 0$.

By Theorem 4.5 we then have

$$\lambda_4 = \frac{|G|}{|T|^3} |\tilde{H}_4| \tilde{\lambda}_4 = \frac{|S|}{|T|^2} \cdot \frac{|T|^2}{|S|} = 1, \lambda_2, \lambda_3 < 0$$

as well as $\lambda_1 > 0$. By Lemma 4.16 we have $\lambda_4 + \lambda_2 = 1 + \lambda_2 \geq 0$, $\lambda_4 + \lambda_3 = 1 + \lambda_3 \geq 0$ and thus $\lambda_2 = \lambda_3 = -1$. Altogether

$$|S| = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = \lambda_1 - 1$$

and thus $\lambda_1 = |S| + 1$.

We have

$$\tilde{\lambda}_1 = \frac{|G|}{|S|^3} \lambda_1 = \frac{|T|}{|S|^2} (|S| + 1) \in \mathbb{Z}.$$

Thus we know that $|S|^2$ divides $|T| \cdot (|S| + 1)$. Since $\gcd(|S|, |S| + 1) = 1$ this yields that $|S|^2$ divides $|T|$. So $|S|^2 \leq |T| < 2|S|$ yielding $|S| = 1$. This is only possible if $S = T = G = \{1\}$ which is not of the assumed type. Therefore the assertion follows by contradiction. \square

The remaining cases of rank four primitive formally dual sets might be examined by Lemma 4.15 and Lemma 4.26 for some additional restriction. But not much more is known. Furthermore, the smallest example, in terms of rank, of a primitive formally dual set which is not even with respect to a chain of subgroups is not known yet. In particular, we conjecture the following:

Conjecture 4.33. *Every primitive formally dual set of rank at most four is either trivial or an $(n, n, n, 1)$ -RDS. Furthermore, there is a formally dual set of rank 5 which is not even with respect to a chain of subgroups.*

5 Non-existence results

In this chapter we examine conditions under which no primitive formally dual pair can exist. In Chapter 4 we have seen such conditions on the type of even set (Lemmata 4.21, 4.28, 4.29, 4.31, 4.32). In this chapter we focus on the group structure and the size of the set. It seems, that especially in cyclic groups formal duality is very rare. In particular the following has been conjectured by Cohn, Kumar, Reiher and Schürmann:

Conjecture 5.1 ([CKRS14, Beginning of Section 4.2]). *If S is a primitive formally dual set in a cyclic group, then $G = C_4$ and S is equivalent to TITO.*

Many results in this chapter are in favor of this conjecture. But it remains open.

For the rest of this chapter we examine formal duality in additive groups if not said otherwise. By applying Theorem 4.5 to cyclic groups we essentially get the following:

Corollary 5.2 ([Sch17, Theorem 3.1]). *Let S be a formally dual subset of \mathbb{Z}_n . The weight enumerator satisfies*

$$v_S(y) = v_S(\gcd(y, n))$$

for all $y \in \mathbb{Z}_n$.

Furthermore, Theorem 4.5 can be transformed into a linear equation among the weight enumerators in the cyclic case. This is possible since in this case the annihilator of a cyclic subgroup is again cyclic.

Corollary 5.3. *Let S and T form a formally dual pair in $G = \mathbb{Z}_n$. Furthermore, let*

$$SS^{(-1)} = \sum_{d|n} \lambda_d [d\mathbb{Z}_n], \quad TT^{(-1)} = \sum_{d|n} \tilde{\lambda}_d [\widetilde{d\mathbb{Z}_n}] = \sum_{d|n} \tilde{\lambda}_{n/d} [d\mathbb{Z}_n]$$

the unique even set representations of S and T (see Lemma 2.8). Then for any divisor d of n we have

1. $v_S(d) = \sum_{e|d} \lambda_e$,
2. $v_T(d) = \sum_{e|d} \tilde{\lambda}_{n/e}$,
3. $\lambda_d = \sum_{e|d} \mu(n/e)v_S(e)$,
4. $\frac{|S|^2}{|T|} v_T(d) = \sum_{e|n} C_n(d, e)v_S(e)$,

where $C_n(d, e) = \sum_{g|\gcd(d, n/e)} \mu(n/(eg))g$.

Proof. We have

$$v_S(d) = \sum_{e: d \in e\mathbb{Z}_n} \lambda_e = \sum_{e|d} \lambda_e$$

as well as

$$v_T(d) = \sum_{e: d \in [e\mathbb{Z}_n]} \tilde{\lambda}_e = \sum_{\frac{n}{e}|d} \tilde{\lambda}_e = \sum_{e|d} \tilde{\lambda}_{n/e}.$$

Furthermore, we define an arithmetic function λ by

$$\lambda(e) = \begin{cases} \lambda_e & \text{if } e|n \\ 0 & \text{otherwise} \end{cases}.$$

Observe that by Corollary 5.2 we have

$$v_S(y) = v_S(\gcd(y, n)) = \sum_{d|\gcd(y, n)} \lambda_d = \sum_{d|y} \lambda(d)$$

for all y . By the Moebius inversion formula (Theorem 2.4) we have for any $d|n$:

$$\lambda_d = \lambda(d) = \sum_{e|d} \mu(n/e)v_S(e).$$

The last assertion follows by Theorem 4.5 as

$$\frac{|S|^2}{|T|} v_T(d) = \sum_{g|d} \frac{|S|^3}{|\mathbb{Z}_n|} \tilde{\lambda}_{n/g} = \sum_{g|d} \lambda_{n/g} \cdot \left| \left[\frac{n}{g} \mathbb{Z}_n \right] \right| = \sum_{g|d} \sum_{e|\frac{n}{g}} \mu(n/(eg))v_S(e) \cdot g.$$

Note that $g|d$ and $e|\frac{n}{g}$ is equivalent to $e|n$ and $g|\gcd(d, n/e)$ and thus

$$\frac{|S|^2}{|T|} v_T(d) = \sum_{e|n} \sum_{g|\gcd(d, n/e)} \mu(n/(eg))g \cdot v_S(e) = \sum_{e|n} C_n(d, e) \cdot v_S(e).$$

□

In [Sch17, Corollary 3.1] the author proved Corollary 5.3 (4) in a different way using sums of roots of unity. A similar result regarding the discrete Fourier transform of so called r -even functions is given in [TH11, Proposition 2]. We presented the above proof of this result to show the connection to even set theory.

We proceed in Section 5.1 to examine non-existence results obtained with the so called Field-descent method. The results obtained this way are non-existence results up to finitely many exceptions. In Section 5.2 we state restrictions of the groups that contain primitive formally dual sets of a given size. Thereby, we emphasize on cyclic groups and observe that formal duality in cyclic groups seems indeed very rare.

5.1 The field-descent method

In this section we describe the field descent method and its application on formal duality. For more background information about the field descent method see [Sch99], [Sch02] or [LS05].

For the rest of the section, we use the *radical* of an integer N that is defined as

$$\text{rad}(N) = \prod_{\substack{p|N \\ p \text{ prime}}} p.$$

The main observation we use is that an element of $\mathbb{Z}[\zeta_m]$ whose squared absolute value is an integer, is contained in a rotation of some smaller $\mathbb{Z}[\zeta_{m'}]$. The size of this smaller $\mathbb{Z}[\zeta_{m'}]$ basically depends on the prime factorizations of m and n . To be precise:

Theorem 5.4 ([Sch02, Proposition 2.2.7, Theorem 2.2.8]). *Let $A \in \mathbb{Z}[\zeta_m]$, such that $|A|^2 = n \in \mathbb{Z}$. Then, there is a number $F(m, n)$ dividing m such that*

$$A \in \zeta_m^j \mathbb{Z}[\zeta_{F(m,n)}]$$

for some $j \in \mathbb{Z}$. Furthermore, there is an explicit computable value $C(P)$ such that

$$F(m, n) \leq C(P)$$

for all $m, n, P \in \mathbb{Z}$ such that $\text{rad}(m \cdot n) | P$.

Furthermore, the field descent method gives an upper bound on the absolute value of elements of $\mathbb{Z}[\zeta_m]$:

Theorem 5.5 ([Sch02, Theorem 2.3.2]). *Let $X \in \mathbb{Z}[\zeta_m]$ with*

$$X = \sum_{i=0}^{m-1} a_i \zeta_m^i$$

where the a_i are integer numbers with $0 \leq a_i \leq C$ for some constant C . Furthermore, assume that $|X|^2 = n \in \mathbb{Z}$. Then

$$n \leq \frac{C^2 F(m, n)^2}{4\varphi(F(m, n))}.$$

Note that the character values $|\chi(S)|^2$ of a formally dual set S are indeed integers (see Remark 3.9). So the field descent method can be applied.

In [Mal18] Malikiosis used these results to give an alternative proof of the characterization of primitive formally dual sets in cyclic groups of prime power order (see Corollary 5.12) as well as the following:

Theorem 5.6 ([Mal18, Theorem 7.3. and proof]). *Let p, q be two distinct primes. There is a constant $D(p, q)$ such that no group \mathbb{Z}_N with $\text{rad}(N) = pq$ and $N > D(p, q)$ contains primitive formally dual subsets.*

Thus, for any fixed pair p, q of primes, there are at most finitely many cyclic groups \mathbb{Z}_N that permit a primitive formally dual subset.

We generalize this result:

Theorem 5.7. *Let p, q be two distinct primes and N' an arbitrary integer. There is a constant $D(p, q, N')$ such that no group of the form $\mathbb{Z}_N \times G'$ where $\text{rad}(N) | pq$, $|G'| = N'$ and $N > D(p, q, N')$ contains primitive formally dual subsets.*

Proof. Suppose $S, T \subset G$ form a primitive formally dual pair and without loss of generality $|T|^2 \leq |G| \leq |S|^2$ as well as $(0, 0) \in S, T$.

We claim that there is an element of $\text{supp}(TT^{(-1)})$ whose order is at least N :

If $\text{rad}(N) = p$ the claim follows directly by the primitivity of T . Suppose $\text{rad}(N) = pq$ and $\text{supp}(TT^{(-1)})$ does not contain any element of order N or higher. Since T is primitive, it is not contained in one of the subgroups $pq\mathbb{Z}_N \times G'$, $p\mathbb{Z}_N \times G'$ or $q\mathbb{Z}_N \times G'$. Therefore, there are elements $(a, x) \in p\mathbb{Z}_N \times G'$, $(a', x') \in q\mathbb{Z}_N \times G'$ such that $p \nmid a$ and $q \nmid a'$. But then $(a - a', x - x') \in \text{supp}(TT^{(-1)})$. Since $a - a'$ is not divisible by p or q we have $\gcd(a - a', N) = 1$ and therefore $\text{ord}(a - a', x - x') \geq N$ which proves the claim.

So let $a \in \text{supp}(TT^{(-1)})$ be an element of order at least N . Thus the kernel of the respective character χ_a has at most size N' . Due to Corollary 4.3 the weight enumerator is constant on the set of generators of $\langle a \rangle$. Note that $\langle a \rangle \simeq \mathbb{Z}_M$ for some M with $N|M$. By counting differences in T we have

$$v_T(a) \cdot \varphi(N) \leq v_T(a) \cdot \varphi(M) < |T|^2 \leq |G| = N \cdot N',$$

or in other terms $v_T(a) < \frac{N}{\varphi(N)} \cdot N' \leq \frac{pq}{(p-1)(q-1)} N' < pqN'$. Define

$$n = |\chi_a(S)|^2 = \frac{|S|^2}{|T|} v_T(a), \quad m = |G| = N \cdot N'.$$

and $R(p, q, N') = \text{rad}((pqN')!)$. Note that since $|S|$ divides $|G|$ we have

$$\text{rad}(|S|^2) \mid \text{rad}(G) \mid \text{rad}(pqN') \mid R(p, q, N').$$

Moreover, since $v_T(a) < pqN'$ we also have $\text{rad}(v_T(a)) \mid \text{rad}((pqN')!)$ and thus $\text{rad}(n) \mid R(p, q, N')$. Also m divides $|G|$ and thus $\text{rad}(m) \mid R(p, q, N')$. Furthermore, $\chi_a(S) = \sum_{i=1}^m a_i \zeta_m^i$ where $0 \leq a_i \leq \ker(\chi_a) \leq N'$. Using Theorems 5.4, 5.5 and the fact that $F(m, n)$ divides $|G|$ and therefore $\frac{F(m, n)}{\varphi(F(m, n))} \leq \frac{\text{rad}(pqN')}{\varphi(\text{rad}(pqN'))}$ we have

$$\sqrt{N \cdot N'} \leq \frac{|S|^3}{|G|} v_T(a) = n \leq \frac{N'^2 F(m, n)^2}{4\varphi(F(m, n))} \leq N'^2 \cdot C(R(p, q, N')) \cdot \frac{\text{rad}(pqN')}{4\varphi(\text{rad}(pqN'))}$$

and thus

$$N \leq \frac{1}{16} N'^3 \cdot \left(C(R(p, q, N')) \cdot \frac{\text{rad}(pqN')}{\varphi(\text{rad}(pqN'))} \right)^2 = D(p, q, N').$$

□

Note that the field descent method can be applied any time we can control the size of $\ker(\chi_a)$ for some a with $v_T(a) > 0$ as well as $\text{rad}(F(m, n))$. The following result from a private communication with Malikiosis also uses these ideas:

Theorem 5.8 ([Mal17]). *Let $P = p_1 \cdot \dots \cdot p_r$ be a product of distinct primes. Suppose there is a constant $F(P)$ such that for any primitive formally dual set $S \subset \mathbb{Z}_N$ with $\text{rad}(N) \mid P$ there exists a $d \leq F(P)$ with $v_S(d) \neq 0$. Then there is a constant $D(P)$ such that no group \mathbb{Z}_N with $\text{rad}(N) \mid P$ and $N > D(P)$ contains a primitive formally dual subset.*

Therefore, an answer of the following conjecture would yield further non-existence results in the cyclic case:

Conjecture 5.9. *For any product of distinct primes $P = p_1 \cdot \dots \cdot p_r$, there is a constant $F(P)$ such that for any primitive formally dual set $S \subset \mathbb{Z}_N$ with $\text{rad}(N) \mid P$ there exists a $d \leq F(P)$ with $v_S(d) \neq 0$.*

5.2 Further restrictions

In this section we discuss further restrictions on primitive formally dual sets and the groups which possess them.

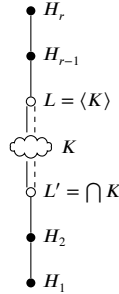
We continue with a result that generalizes the characterization of formally dual sets in cyclic p -groups. This characterization has been proven elementary in [Sch17], [Xia16, Section 3.2]. An alternative proof that uses the field descent method is given in [Mal18, Theorem 6.1]. We state a proof using the even set approach to emphasize on the strong connection between relative difference sets and formally dual sets.

Therefore, we need the following theorem:

Theorem 5.10 ([Pot95a, Theorem 4.1.1]). *Let D be an $(\lambda n, n, \lambda n, \lambda)$ -RDS and $g \in G$. Then the order of g divides λn or D is equivalent to TITO. Especially if G is cyclic then D is equivalent to TITO.*

We use this to prove the following, which can be seen as a generalization of the characterization of formally dual sets in groups of prime power order:

Theorem 5.11. *There is no primitive formally dual set of type*



such that L' and G/L are cyclic groups.

Proof. Suppose S is as asserted. By using Proposition 4.22 we have $|G| = |S|^2$, $H_1 = \{1\}$, $\lambda_1 = |S|$ and $\lambda_r = 1$. We apply Proposition 4.23 on S to see that \bar{S} (the reduction of S to G/L) is an $\left(\frac{|S|^2}{|H_{r-1}|}, \frac{|H_{r-1}|}{|L|}, \frac{|S|^2}{|H_{r-1}|}, \frac{|L||S|^2}{|H_{r-1}|^2}\right)$ -RDS in G/L . By Theorem 5.10 with $n = \frac{|H_{r-1}|}{|L|}$ and $\lambda = \frac{|L||S|^2}{|H_{r-1}|^2}$ we have without loss of generality $n = 2$, $\lambda = 1$, $\bar{S} = \text{TITO}$, $G/L = C_4$. Comparing parameters we get

$$|G| = |S|^2 = 2|H_{r-1}| = 4|L|.$$

Note that $G/\tilde{L}' \simeq L'$ which is also cyclic. Thus, we can use the same approach on the formal dual of S which yields that $|H_2| = 2$, $|L'| = 4$, $\tilde{\lambda}_1 = 1$, $\tilde{\lambda}_2 = -1$ (see Lemma 4.14). Furthermore, by Theorem 4.4 we have

$$\lambda_2 = \frac{|G|}{|T|^3} \tilde{\lambda}_2 |\tilde{H}_2| = -\frac{|S|}{2}.$$

Let a be a generator of L' , i.e. $L' = \langle a \rangle = \{1, a, a^2, a^3\}$. Then we have by Lemma 4.16

$$v_S(a) = v_S(a^3) = \sum_{i=3}^r \lambda_i = \underbrace{\sum_{i=1}^r \lambda_i}_{=|S|} - \underbrace{\lambda_1}_{=|S|} - \underbrace{\lambda_2}_{=-\frac{|S|}{2}} = \frac{|S|}{2}$$

and on the other hand

$$v_S(a^2) = \sum_{i=2}^r \lambda_i = |S| - \lambda_1 = 0.$$

Thus, S is a union of translates of $\{1, a\}$.

Recall that $\bar{S} = \text{TITO}$ and therefore $S \cap L, S \cap vL \neq \emptyset$ for some element v such that vL is a generator of G/L . Without loss of generality, let $x \in S \cap vL$, $y \in S \cap L$ such that $xa, ya \in S$. Then $xy^{-1} = (xa)(ya)^{-1} \in S \cap vL \subset G \setminus H_{r-1}$. But then $2 \leq v_S(xy^{-1}) = \lambda_r = 1$ which is a contradiction. \square

Theorem 5.11 might be seen as a generalization of the characterization in cyclic p -groups since it implies this result as follows:

Corollary 5.12. *If S is a primitive formally dual set in a cyclic group G of prime power order, then $G = C_4$ and S is equivalent to TITO.*

Proof. By the structure of G it is obvious that S is a formally dual set with respect to a chain of subgroups. Combining Lemma 4.28, Lemma 4.29, Lemma 4.31 and Theorem 5.11 we see that the rank of S is three. Thus by Theorem 4.30 it is an $(n, n, n, 1)$ -RDS and by Theorem 5.10 it has to be equivalent to TITO. \square

As mentioned in [LPS19] the even set approach could yield even more insights on primitive formally dual sets in cyclic groups if the following is true

Conjecture 5.13. *A primitive formally dual set in a cyclic group has at most rank three.*

In fact the Conjectures 5.13 and 5.1 are equivalent by Theorem 4.30 and since TITO is the only $(n, n, n, 1)$ -RDS in a cyclic group by Theorem 5.10.

If we consider cyclic groups that are divisible by at most two primes, we get a simple bound on the set size:

Lemma 5.14 ([Mal18, Lemma 4.8, Lemma 7.1]). *Let N be an integer that is divisible by exactly two primes. If S is a primitive formally dual set, then*

$$|S|(|S| - 1) \geq \varphi(N).$$

In some special cases Malikiosis was able to use the so called polynomial in order to obtain non-existence results. This method identifies any element

$$a = \sum_{k=0}^{\text{ord}(g)-1} a_{g^k} g^k \in \mathbb{Q}\langle g \rangle$$

of the group algebra over a cyclic group as polynomial by defining

$$a[X] = \sum_{k=0}^{\text{ord}(g)-1} a_{g^k} X^k.$$

This allows to use algebraic and number theoretic methods. He could derive the following for cyclic groups with an order that is divisible by two primes (see also [LPS19, Proposition 2.12]):

Theorem 5.15 ([Mal18, Propositions 7.4 - 7.7, A.2 - A.4, Theorems 7.3, 8.3]). *There is no primitive formally dual subset of \mathbb{Z}_N if one of the following is true for two distinct primes p, q*

1. $N = p^a q$ for $a \geq 1$,

2. $N = p^a q^2$ for $a = 2$ or a odd,
3. $N = p^4 q^3$,
4. $N = p^3 q^3$ except we have simultaneously $|p - q| = 2$ and $p^2 | q^{p-1} - 1$ and $q^2 | p^{q-1} - 1$ (simultaneously twin primes and a Wieferich pair) or
5. $N = p^a q^3$ where $a \geq 4$ and $p, q < 10^3$.

Furthermore, if $p, q \geq 5$ and $N = p^a q^b$ for $a \in \{1, 2, 3, 4, 5, 7\}$ or $a, b \in \{6, 8, 10\}$ then there is no primitive formally dual subset of \mathbb{Z}_N with size unequal to \sqrt{N} (from a private communication with Schlage-Puchta [SP17]).

In the following we need some more number theoretic background. Let b be an integer with prime factorization $\prod p^{b_p}$. An integer a is called *self-conjugate modulo b* if for each prime divisor $p|a$ there is an exponent $e(p)$ such that

$$a^{e(p)} \equiv -1 \pmod{\frac{b}{p^{b_p}}}.$$

Something more can be said under the self conjugacy assumption:

Theorem 5.16 ([LPS19, Theorem 5.8]). *Let G be a group and p be a self-conjugate prime modulo $\exp(G)$ such that the p -Sylow group of G is cyclic. If $p^k || |G|$ then G does not contain a primitive formally dual set unless $k = 2$. In this case p is a common divisor of $|S|$ and $|T|$, whenever S and T form a formally dual pair.*

Now we examine results that restrict the size of a primitive formally dual set. In the following, we use

$$a_S = \frac{|S|^2}{\gcd(|S|^2, |T|)}, \quad b_S = \frac{|S|}{\gcd(|S|, |T|^2)}$$

and a_T, b_T analogously.

Recall, that $\frac{|S|^2}{|T|} v_T(y) \in \mathbb{Z}$ by Remark 3.9 and thus $b_T | v_T(y)$. If additionally T is supposed to be primitive, then $b_T \neq |T|$ (otherwise there would be an y such that $v_T(y) = |T|$, since the weight enumerator can not be zero everywhere). It easily follows that $\gcd(|S|^2, |T|) \neq 1$ as well as $\gcd(|S|, |T|) \neq 1$ and thus $|G| = |S| \cdot |T|$ is not squarefree (see also [Xia16, Theorems 3.6, 3.7]).

Next we state a restriction regarding the prime divisors of $|S|$. This is an adaptation of [LPS19, Theorem 5.1].

Proposition 5.17 ([LPS19, Theorem 5.1]). *Let S and T form a primitive formally dual pair in G . Furthermore, let p be a prime divisor of $|G|$ such that the p -Sylow group of G is cyclic. Moreover, suppose $p^r \mid a_S$, then*

$$\gcd(|S|, |T|^2) \cdot \gcd(b_S, p^r) \geq p^r.$$

The following result gives an exponent-bound of the size of S :

Proposition 5.18. [LPS19, Proposition 5.10] *Let G be a group and p be a prime divisor of $|G|$. Furthermore, let p^e be the exponent of the p -Sylow group of G , then for any primitive even set S we have*

$$|S|(|S| - 1) \geq p^{e-1}(p - 1).$$

Epecially this is true for primitive formally dual sets.

For very small sizes, the following Lemma often suffices to justify the non-existence of a primitive formally dual set:

Lemma 5.19 ([LPS19, Proposition 5.9]). *Let S be a primitive subset of a group G and s be the minimal number of generators of G . Then*

$$|S| \geq s + 1.$$

Next we state two lemmata which then are combined to a non-existence result:

Lemma 5.20 ([LPS19, Theorem 5.3]). *Let S and T form a formally dual pair in G . Furthermore, let p be a prime dividing the order of $|G|$. For any element $y \in G$ of order p we have:*

$$p|T| \text{ divides } |S|^2(|T| - v_T(y)) \text{ and } p|S| \text{ divides } |T|^2(|S| - v_S(y)).$$

Note, that if S and T are primitive the right hand sides are positive and non zero.

Lemma 5.21 ([LPS19, Proposition 5.6 and proof]). *Let S be a primitive formally dual set in G . Furthermore, suppose $G = H \times N$ such that $H \simeq G/N \simeq \mathbb{Z}_{p^e}$ for some prime p . Moreover, let q be a prime that generates $\mathbb{Z}_{p^e}^*$ (a so called primitive root modulo p^e). If $q^f \mid a_S$ and f is odd, then $q^{f+1} \mid |\chi(S)|^2$ for every linear character $\chi \in \hat{G}$.*

We use these results to show the following, which generalizes [LPS19, Example 5.7] (details of the proof have been inspired by a private communication with S. Li [Li19]):

Theorem 5.22. *Let S and T form a primitive formally dual pair in G . Moreover, let p be a prime and e an integer such that $G \simeq \mathbb{Z}_{p^e} \times G'$. Furthermore, let Q be the set of all primes q that fulfill the following conditions:*

1. $q^s \parallel |T|$ for odd s ,
2. $q^s \mid |S|^2$,
3. q is a primitive root modulo p^e if p is odd
4. $q \neq p$ if $p = 2$

and let $\overline{Q} = \prod_{q \in Q} q$. Then

$$p \cdot \overline{Q} \leq \gcd(p \cdot |T|, |S|^2).$$

Proof. Suppose S, T, p and e are as asserted and $p \cdot \overline{Q} > \gcd(p \cdot |T|, |S|^2)$. Let y be an element of order p . Due to Lemma 5.20 we know that $p|T|$ divides $|S|^2(|T| - v_T(y))$. Thus $p \cdot |T| / \gcd(p \cdot |T|, |S|^2)$ divides $|T| - v_T(y)$, say $|T| - v_T(y) = k \cdot p \cdot |T| / \gcd(p \cdot |T|, |S|^2)$. Note that

$$|T| \geq |T| - v_T(y) = k \cdot \frac{p \cdot |T|}{\gcd(p \cdot |T|, |S|^2)} > 0$$

and therefore

$$\overline{Q} > \frac{\gcd(p \cdot |T|, |S|^2)}{p} \geq k > 0.$$

If $Q = \emptyset$ then $\overline{Q} = 1$ and we have a contradiction. Otherwise, there is a $q \in Q$ that does not divide k . Note that q also does not divide $p \cdot |T| / \gcd(p \cdot |T|, |S|^2)$ due to the definition of Q . Therefore, q also does not divide

$$v_T(y) = |T| - k \cdot \frac{p \cdot |T|}{\gcd(p \cdot |T|, |S|^2)}.$$

Choose k such that $q^k \parallel |S|^2$ and note that $q^s \parallel \gcd(|S|^2, |T|)$. It is easy to see that

$$q^{2k-s} \parallel \frac{|S|^2}{|T|} v_T(y) = |\chi_y(S)|^2. \quad (5.1)$$

If $p = 2$ then χ_y has order two. Therefore $\chi_y(S) \in \mathbb{Z}$ and $|\chi_y(S)|^2$ is a square number, which is a contradiction to Equation (5.1) since $2k - s$ is odd. If p is odd, then we know that $q^{2k-s+1} \mid |\chi_y(S)|^2$ by Lemma 5.21 which is again a contradiction to Equation (5.1). □

We continue by stating restrictions on groups that can contain a primitive formally dual set of prime size.

Proposition 5.23 ([LPS19, Corollary 5.11]). *We have*

1. TITO is the only primitive formally dual set of size 2
2. If S is a primitive formally dual subset of G with $|S| = p$ where p is an odd prime. Then the p -Sylow group of G has to be isomorphic to $(\mathbb{Z}_p)^k$ for $k \geq 2$.

Combining all non-existence results of this section, the only groups of order ≤ 63 that can contain primitive formally dual sets are isomorphic to one of

$$\begin{aligned} &\mathbb{Z}_4, \quad \mathbb{Z}_3^2, \quad \mathbb{Z}_4 \times \mathbb{Z}_2^2, \quad \mathbb{Z}_4^2, \quad \mathbb{Z}_8 \times \mathbb{Z}_2, \\ &\mathbb{Z}_5^2, \quad \mathbb{Z}_4^2 \times \mathbb{Z}_2, \quad \mathbb{Z}_8 \times \mathbb{Z}_2^2, \quad \mathbb{Z}_8 \times \mathbb{Z}_4, \quad \mathbb{Z}_{16} \times \mathbb{Z}_2, \\ &\mathbb{Z}_6^2, \quad \mathbb{Z}_{18} \times \mathbb{Z}_2, \quad \mathbb{Z}_{12} \times \mathbb{Z}_3, \quad \mathbb{Z}_7^2 \end{aligned}$$

(see also Table A.1 in the appendix, or Appendix B (1)). Moreover, if S is a primitive formally dual set in \mathbb{Z}_N with $|S|^2 \leq N \leq 1000$ then the pair $(N, |S|)$ is one of the following:

$(600, 10)$, $(784, 28)$ or $(900, 30)$ (see [LPS19, Remark 5.12]). A complete list of open cases in cyclic groups up to order 10000 can be found in Appendix B (2).

Especially, the case $N = 900 = 2^2 \cdot 3^2 \cdot 5^2$, $|S| = 30 = 2 \cdot 3 \cdot 5$ seems exceptional as it is the first square number with more than two prime factors. Therefore, we state a conjecture in contrary to Conjecture 5.1:

Conjecture 5.24. *There is a primitive formally dual subset of \mathbb{Z}_{900} of size 30.*

6 Constructions of primitive formally dual sets

This chapter is organized as follows. We introduce all known constructions of formally dual sets in Section 6.1 and discuss their irreducibility in Section 6.2.

6.1 Constructions

In this section we discuss ways to construct primitive formally dual sets in addition to Corollary 4.7 and Example 6.2.

First note that by Corollary 4.7 any pair of $(n, n, n, 1)$ -RDS with forbidden subgroups N and \tilde{N} respectively form a primitive formally dual pair. For a detailed treatment of relative difference sets with various examples see [Pot95b].

In the following we examine Galois Rings and an example defined in a cross product of Galois Rings. Let p^t be a prime power and $\mathbb{Z}_{p^t}[x]$ be the polynomial ring over \mathbb{Z}_{p^t} . Furthermore, let f be a monic polynomial in $\mathbb{Z}_{p^t}[x]$ such that f is irreducible over \mathbb{Z}_p . We denote by $\text{GR}(p^t, s) = \mathbb{Z}_{p^t}[x]/(f(x))$ the *Galois ring* of characteristic p^t and rank $s = \deg f$. The additive group of $\text{GR}(p^t, s)$ is isomorphic to $(\mathbb{Z}_{p^t})^s$. Furthermore, there is a chain of principal ideals

$$\{0\} = (p^t) \subset (p^{t-1}) \subset \dots \subset (p) \subset \text{GR}(p^t, s).$$

We define for any $v \in \text{GR}(p^t, s)$:

$$v_p(v) = \max\{k : 0 \leq k \leq t, v \in (p^k)\}.$$

Moreover, the multiplicative group $\text{GR}(p^t, s)^\times = \text{GR}(p^t, s) \setminus (p)$ contains a unique cyclic group of order $p^s - 1$. The *Teichmüller set* \mathcal{T} is the union of this cyclic group and 0.

The p -adic representation of an element $v \in \text{GR}(p^t, s)$ is the unique representation of v as

$$v = \sum_{i=0}^{t-1} p^i v_i \text{ for suitable } v_i \in \mathcal{T}.$$

The *generalized Frobenius automorphism* is given by $\sigma : \sum_{i=0}^{t-1} p^i v_i \mapsto \sum_{i=0}^{t-1} p^i v_i^p$ and generates a cyclic group of size s . The *generalized Trace function* is given by

$$\text{Tr}(x) = \sum_{i=0}^{s-1} \sigma^i(x)$$

and has the following properties:

1. $\text{Tr}(x) \in \mathbb{Z}_{p^t}$ and $\text{Tr} : G \rightarrow \mathbb{Z}_{p^t}$ is surjective,
2. $\text{Tr}(x + y) = \text{Tr}(x) + \text{Tr}(y)$,
3. $\text{Tr}(\lambda x) = \lambda \text{Tr}(x)$.

We identify $\text{GR}(p^t, s)$ with its dual group by the *trace isomorphism* given by the pairing $\langle a, x \rangle = \chi_a(x) = \zeta_{p^t}^{\text{Tr}(a \cdot x)}$.

More information about Galois Rings can be found in [Yam90, Section 2] and [Wan03, Chapter 14].

We start with a preparatory lemma:

Lemma 6.1. *We have $\widetilde{(p^i)} = (p^{t-i})$ under the trace isomorphism.*

Proof. It suffices to show that $\text{Tr}(a \cdot x) = 0$ for all $x \in (p^i)$ if and only if $a \in (p^{t-i})$.

Suppose $\text{Tr}(a \cdot x) = 0$ for all $x \in (p^i)$. Let $a = p^k a_k + \dots + p^{t-1} a_{t-1}$ be the p -adic representation of a (we choose k to be the smallest index such that $a_k \neq 0$).

We claim that $k \geq t - i$. Indeed: Suppose $k < t - i$. Let $v \in \text{GR}(p^t, s)$ such that $\text{Tr}(v) = 1$.

Then $p^{t-k-1} a_k^{-1} v \in (p^i)$ and

$$p^{t-1} = p^{t-1} \text{Tr}(v) = \text{Tr}(p^{t-1} v) = \text{Tr}(a \cdot p^{t-k-1} v a_k^{-1}) = 0$$

which is a contradiction.

On the other hand, suppose $a \in (p^{t-i})$ and $x \in (p^i)$ say $a = p^{t-i} a'$ and $x = p^i x'$. Then $\text{Tr}(a \cdot x) = \text{Tr}(p^t \cdot a' \cdot x') = 0$. \square

We continue by stating the announced example with an alternative proof based on even set theory.

Example 6.2 ([LPS19, Theorem 3.13]). *Let p be an odd prime and s, t arbitrary integers. The sets*

$$S = \{(x, x^2) : x \in \text{GR}(p^t, s)\}$$

and

$$T = \{(x^2, x) : x \in \text{GR}(p^t, s)\}$$

form a formally dual pair under the isomorphism canonically induced by the trace isomorphism.

Proof. Any $a \in \text{GR}(p^t, s)$ is invertible if and only if $a \notin (p)$. Using this fact we compute the weight enumerator $v_S(a, b)$ as solutions of the equations $x - y = a$, $a(x + y) = x^2 - y^2 = b$. If $v_p(a) > v_p(b)$ this equation has no solution. If $v_p(a) \leq v_p(b)$ we might write

$$a = p^{v_p(a)} a' \in (p^{v_p(a)}) \setminus (p^{v_p(a)+1}), \text{ with } a' \in \text{GR}(p^t, s)^\times.$$

So we need to solve

$$x - y = a, p^{v_p(a)}(x + y) = (a')^{-1}b$$

which is equivalent to $y = \frac{1}{2}((x + y) - a)$, $p^{v_p(a)}(x + y) = (a')^{-1}b$ (note that 2 is invertible since p is odd). By restricting this equation by $(p^{v_p(a)})$ it can be seen that it has $|(p^{t-v_p(a)})| = p^{v_p(a)s}$ solutions. Thus

$$v_S(a, b) = \begin{cases} p^{v_p(a)s} & \text{if } v_p(a) \leq v_p(b) \\ 0 & \text{otherwise} \end{cases}$$

or equivalently

$$SS^{(-1)} = \sum_{i=0}^t p^{is} ((p^i) \times (p^i)) - \sum_{i=0}^{t-1} p^{is} ((p^{i+1}) \times (p^i)).$$

In a similiar manner and additionally using Lemma 6.1 as well as $|G| = p^{2ts}$, $|S| =$

p^{ts} , $|(p^i)| = p^{t-i}$ we see

$$\begin{aligned}
TT^{(-1)} &= \sum_{i=0}^t p^{is} ((p^i) \times (p^i)) - \sum_{i=0}^{t-1} p^{is} ((p^i) \times (p^{i+1})) \\
&= \sum_{i=0}^t p^{(t-i)s} ((p^{t-i}) \times (p^{t-i})) - \sum_{i=0}^{t-1} p^{(t-i-1)s} ((p^{t-i-1}) \times (p^{t-i})) \\
&= \sum_{i=0}^t \frac{|G|}{|S|^3} p^{is} |(p^i) \times (p^i)| \left(\widetilde{(p^i) \times (p^i)} \right) \\
&\quad - \sum_{i=0}^{t-1} \frac{|G|}{|S|^3} p^{is} |(p^i) \times (p^{i+1})| \left(\widetilde{(p^{i+1}) \times (p^i)} \right).
\end{aligned}$$

Thus by Theorem 4.5 the sets S and T form a formally dual pair. \square

In [LPS19] a set with an even set representation as seen in the proof of Example 6.2 has been referred to as *generalized relative difference set*. Note that for $s = 1$ this example simplifies to an example in $\mathbb{Z}_p \times \mathbb{Z}_p$ which has been introduced in [Xia16, Theorem 3.1]. The special case of $s = t = 1$ has already been given in [CKRS14, Theorem 3.2]. Furthermore, it is easy to see that S is formally self dual under the isomorphism $(a, b) \mapsto (t(b), t(a))$ where t is the trace isomorphism.

In the following, we present a construction of primitive formally dual sets that use a certain kind of difference set:

Definition 6.3. A *skew Hadamard difference set* D is a difference set such that the following group algebra equation holds:

$$1 + D + D^{(-1)} = G.$$

The set

$$D_* = \left\{ a \in \mathbb{Z}_p^m : \chi_a(D) = \frac{-1 + i\sqrt{|G|}}{2} \right\}$$

is the *dual skew Hadamard difference set*. Note that D_* is indeed a skew Hadamard difference set by [WH09, Corollary 2.7].

A given skew Hadamard difference set in \mathbb{Z}_p^m can be lifted to a formally dual set in \mathbb{Z}_p^{2m} in the following way:

Theorem 6.4 ([LPS19, Theorem 3.20]). *Let D be a skew Hadamard difference set in \mathbb{Z}_p^m . For any $\alpha, \beta \in \mathbb{Z}_p \setminus \{0\}$ define a group homomorphism $\phi_{\alpha, \beta} : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p^m \times \mathbb{Z}_p^m$ by $x \mapsto (\alpha x, \beta x)$. For any distinct scalars $\alpha, \beta \in \mathbb{Z}_p$ the sets*

$$S = (0, 0) \dot{\cup} \phi_{1, \alpha}(D) \dot{\cup} \phi_{1, \beta}(D^{(-1)}) \text{ and,}$$

$$T = (0, 0) \dot{\cup} \phi_{\frac{\alpha}{\alpha-\beta}, \frac{1}{\beta-\alpha}}(D_*) \dot{\cup} \phi_{\frac{\beta}{\alpha-\beta}, \frac{1}{\beta-\alpha}}(D_*^{(-1)})$$

form a formally dual pair in \mathbb{Z}_p^m under the standard pairing.

The following example gives such a formally dual set:

Example 6.5. *The set $\{1, 2, 4\} \subset \mathbb{Z}_7$ is a skew Hadamard difference set. By taking $\alpha = 1, \beta = 2$ in Theorem 6.4 we know that*

$$\{(0, 0), (1, 1), (2, 2), (4, 4), (3, 6), (5, 3), (6, 5)\} \subset \mathbb{Z}_7 \times \mathbb{Z}_7$$

is a primitive formally dual set.

Next we discuss a method developed by Li and Pott [LP18] to generate primitive formally dual sets in $\mathbb{Z}_2 \times G$, given a suitable primitive formally dual set in G . Note that this construction leads to formally dual sets of unequal size, unlike all other known constructions.

First we need some notation: We define a *lifting operator* π on two sets $S_0, S_1 \subset G$ as

$$\pi(S_0, S_1) = \{(0, x) : x \in S_0\} \dot{\cup} \{(1, x) : x \in S_1\} \subset \mathbb{Z}_2 \times G.$$

The following theorem determines under which circumstances a partition of a formally dual set can be lifted by π to another formally dual set. To this extend we define the *generalized weight enumerator* as

$$v_{S_0, S_1}(v) = \#\{(x, y) \in S_0 \times S_1 : x - y = v\} = [S_0 S_1^{-1}]_v.$$

Note that $v_S = v_{S, S}$.

Now we have everything to state the following result, called *lifting construction*:

Theorem 6.6. [LP18, Theorem 3.1, Corollary 3.4] *Let G be a finite abelian group. Let $\Delta : G \rightarrow \hat{G}, z \mapsto \chi_z$ be an isomorphism, Δ_* be the adjoined isomorphism and $\hat{\chi}_z = \Delta_*(z)$. Furthermore, let S and T form a formally dual pair in G under Δ . Let $S_0, S_1, T_0, T_1 \subset G$ be such that $S = S_0 \dot{\cup} S_1$ and $|T_0| + |T_1| = 2|T|$.*

The sets $\pi(\mathcal{S}_0, \mathcal{S}_1)$ and $\pi(T_0, T_1)$ form a primitive formally dual pair under the isomorphism Δ_2 given by $\langle (x, y), (a, b) \rangle_{\Delta_2} = (-1)^{ax} \cdot \langle y, b \rangle_{\Delta}$ if and only if

$$|\hat{\chi}_z(T_0 + T_1)|^2 = 4 \frac{|T|^2}{|S|} (v_{\mathcal{S}_0}(z) + v_{\mathcal{S}_1}(z)), \text{ for every } z \in G \text{ and} \quad (6.1)$$

$$|\hat{\chi}_z(T_0 - T_1)|^2 = 4 \frac{|T|^2}{|S|} (v_{\mathcal{S}_0, \mathcal{S}_1}(z) + v_{\mathcal{S}_1, \mathcal{S}_0}(z)), \text{ for every } z \in G. \quad (6.2)$$

In particular, $\pi(\mathcal{S}_0, \mathcal{S}_1)$ and $\pi(T, T^{(-1)})$ form a formally dual pair under Δ_2 if and only if

$$|\hat{\chi}_z(T + T^{(-1)})|^2 = 4 \frac{|T|^2}{|S|} (v_{\mathcal{S}_0}(z) + v_{\mathcal{S}_1}(z)), \text{ for every } z \in G.$$

These conditions might be stated in terms of even sets by using the same approach as in Theorem 4.5:

Corollary 6.7. *Under the same assumptions as in Theorem 6.6 we have: The sets $\pi(\mathcal{S}_0, \mathcal{S}_1)$ and $\pi(T_0, T_1)$ form a primitive formally dual pair under the isomorphism Δ_2 defined in Theorem 6.6 if and only if there are parameters $\lambda_1, \dots, \lambda_r, \mu_1, \dots, \mu_s$ and subgroups $H_1, \dots, H_r, L_1, \dots, L_s$ such that*

1. $\mathcal{S}_0 \mathcal{S}_0^{(-1)} + \mathcal{S}_1 \mathcal{S}_1^{(-1)} = \sum_{i=1}^r \lambda_i H_i$,
2. $(T_0 + T_1)(T_0 + T_1)^{(-1)} = 4 \frac{|G|}{|S|^3} \sum_{i=1}^r \lambda_i |H_i| \tilde{H}_i$,
3. $\mathcal{S}_0 \mathcal{S}_1^{(-1)} + \mathcal{S}_1 \mathcal{S}_0^{(-1)} = \sum_{i=1}^s \mu_i L_i$,
4. $(T_0 - T_1)(T_0 - T_1)^{(-1)} = 4 \frac{|G|}{|S|^3} \sum_{i=1}^s \mu_i |L_i| \tilde{L}_i$.

Also, if $T_0 = T$ and $T_1 = T^{(-1)}$ only the first two statements need to be satisfied.

Proof. Suppose Equations (1) - (4) are satisfied. We have

$$\begin{aligned} |\hat{\chi}_z(T_0 + T_1)|^2 &= 4 \frac{|G|}{|S|^3} \sum_{i=1}^r \lambda_i |H_i| \hat{\chi}_z(\tilde{H}_i) = 4 \frac{|G|}{|S|^3} \sum_{i: z \in H_i} \lambda_i |G| \\ &= 4 \frac{|T|^2}{|S|} [\mathcal{S}_0 \mathcal{S}_0^{(-1)} + \mathcal{S}_1 \mathcal{S}_1^{(-1)}]_z = 4 \frac{|T|^2}{|S|} (v_{\mathcal{S}_0}(z) + v_{\mathcal{S}_1}(z)). \end{aligned}$$

Analogously,

$$\begin{aligned} |\hat{\chi}_z(T_0 - T_1)|^2 &= 4 \frac{|G|}{|S|^3} \sum_{i: z \in L_i} \mu_i |G| = 4 \frac{|T|^2}{|S|} [S_0 S_1^{(-1)} + S_1 S_0^{(-1)}]_z \\ &= 4 \frac{|T|^2}{|S|} (v_{S_0, S_1}(z) + v_{S_1, S_0}(z)). \end{aligned}$$

Thus, $\pi(S_0, S_1)$ and $\pi(T_0, T_1)$ form a primitive formally dual pair by Theorem 6.6.

On the other hand, given equations (6.1), (6.2) we see that the right hand sides are rational for every $z \in G$. By Lemma 2.10 this yields that

$$(T_0 - T_1)(T_0 - T_1)^{(-1)}, (T_0 + T_1)(T_0 + T_1)^{(-1)} \in \mathcal{M}(G).$$

Thus, there are $H_1, \dots, H_r, L_1, \dots, L_s \leq G$, $\lambda_1, \dots, \lambda_r, \mu_1, \dots, \mu_r \in \mathbb{Q}$ such that Equations (2) and (4) are satisfied. Equations (1) and (3) then follow similar to the first part of the proof. \square

If we construct two primitive formally dual sets in the terms of Theorem 6.6, we can combine them to get a new one of the same type. This construction can be applied succesively and is therefore called the *recursive lifting construction*:

Theorem 6.8 ([LP18, Theorem 5.1]). *Let $S, T \subset G$ form a primitive formally dual pair under Δ and $U, V \subset H$ form a primitive formally dual pair under Γ . Let $\langle (x, y), (a, b) \rangle_{\Delta_2} = (-1)^{ax} \cdot \langle y, b \rangle_{\Delta}$ and Γ_2 analogously. Furthermore, suppose $S = S_0 \dot{\cup} S_1$ and $U = U_0 \dot{\cup} U_1$ such that*

1. $\pi(S_0, S_1)$ and $\pi(T, T^{(-1)})$ form a formally dual pair in $\mathbb{Z}_2 \times G$ under Δ_2 and
2. $\pi(U_0, U_1)$ and $\pi(V, V^{(-1)})$ form a formally dual pair in $\mathbb{Z}_2 \times H$ under Γ_2 .

Then the sets

$$\pi(S_0 \times U_0 \cup S_1 \times U_1, S_0 \times U_1 \cup S_1 \times U_0)$$

and

$$\pi(T \times V, T^{(-1)} \times V^{(-1)})$$

form a formally dual pair in $\mathbb{Z}_2 \times G \times H$ under

$$\langle (x, y, z), (a, b, c) \rangle = \zeta_2^{ax} \cdot \langle y, b \rangle_{\Delta} \cdot \langle z, c \rangle_{\Gamma}.$$

Note that Theorems 6.6 and 6.8 only describe a general framework to lift primitive formally dual sets. However, a suitable partition $S = S_0 \dot{\cup} S_1$ has to be chosen first. The next result is a concrete infinite family of primitive formally dual sets obtained by the lifting construction:

Example 6.9 ([LP18, Theorem 5.1]). *Let $G = \mathbb{Z}_4^{2m}$ and $S = T = \text{TITO}^{2m} \subset G$. Note that S is formally self dual under the standard pairing by Lemma 3.18 and Example 3.11. Let*

$$\begin{aligned} S_0 &= \{(x_1, \dots, x_{2m}) \in S : x_1 + \dots + x_{2m} \equiv 0, 1 \pmod{4}\} \\ S_1 &= \{(x_1, \dots, x_{2m}) \in S : x_1 + \dots + x_{2m} \equiv 2, 3 \pmod{4}\} \end{aligned}$$

Then $\pi(S_0, S_1)$ and $\pi(T, T^{(-1)})$ form a primitive formally dual pair in $\mathbb{Z}_2 \times \mathbb{Z}_4^{2m}$ under the standard pairing.

For $m = 1$ this construction yields $S_0 = \{(0, 0), (1, 0), (0, 1)\}$, $S_1 = \{(1, 1)\}$ and

$$\{(0, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1)\} \subset \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4.$$

Note that this is also the smallest example of a primitive formally dual pair of unequal size (see also Table A.1 in the Appendix).

The formally dual sets of Example 6.9 can be used as building blocks for Theorem 6.8 to obtain a huge number of non-equivalent primitive formally dual sets in groups of the form $\mathbb{Z}_2 \times \mathbb{Z}_4^{2m}$ for $m \geq 2$. An alternative direct construction of these examples is presented in [LP19].

To conclude this chapter we give a list of groups that contain primitive formally dual sets:

1. $\mathbb{Z}_{p'}^{2s}$ for odd p by Example 6.2 or Theorem 6.4,
2. $\mathbb{Z}_2 \times \mathbb{Z}_4^{2m}$ by Example 6.9 or Theorem 6.6,
3. any group that contains an $(n, n, n, 1)$ -RDS with forbidden subgroup N as well as an $(n, n, n, 1)$ -RDS with forbidden subgroup \tilde{N} for some subgroup $N \leq G$ by Corollary 4.7,
4. cross products of the preceding groups by Lemma 3.18.

6.2 Irreducibility

Due to Lemma 3.18 it is an interesting question whether the examples constructed in the above section are irreducible or not. We prove irreducibility for three known examples.

First of all, note the following:

Lemma 6.10. *A primitive formally dual set $S \subset G$ with $1 \in S$ is not irreducible if and only if $S = \Delta(S_1 \times S_2)$ for some non-trivial formally dual sets $S_1 \subset G_1$, $S_2 \subset G_2$ with $1 \in S_1$, $1 \in S_2$ and some isomorphism $\Delta : G_1 \times G_2 \rightarrow G$.*

Proof. Suppose S is not irreducible. Then there are non-trivial formally dual sets $S_1 \subset G_1$, $S_2 \subset G_2$ an element $v \in G$ and an isomorphism Δ such that

$$S = v \cdot \Delta(S_1 \times S_2).$$

Furthermore $1 = v \cdot \Delta(\Delta^{-1}(v^{-1})) \in S$ and therefore

$$\Delta^{-1}(v^{-1}) = (w_1^{-1}, w_2^{-1}) \in S_1 \times S_2$$

where $(w_1, w_2) = \Delta^{-1}(v)$. Then $S = \Delta([w_1 \cdot S_1] \times [w_2 \cdot S_2])$. Since $w_1 \cdot S_1$ and $w_2 \cdot S_2$ are again non-trivial primitive formally dual subsets and $1 = w_1 \cdot w_1^{-1} \in [w_1 \cdot S_1]$, $1 = w_2 \cdot w_2^{-1} \in [w_2 \cdot S_2]$ the assertion follows. \square

In the following we show that many primitive examples from the previous section are in fact irreducible.

Corollary 6.11. *If S is a primitive formally dual set of one of the following forms, then it is irreducible:*

1. an $(n, n, n, 1)$ -RDS,
2. $S = \{(x, x^2) : x \in \text{GR}(p^t, s)\}$ from Example 6.2,
3. $S = \pi(S_0, S_1)$ as given in Example 6.9 or
4. S is lifted from a skew Hadamard DS for $m = 1$ as in Theorem 6.4.

Proof. The first three assertions follow by Lemma 6.10 as:

1. Write G multiplicatively. Let S be an $(n, n, n, 1)$ -RDS and assume without loss of generality that $1 \in S$. Suppose there is an isomorphism $\Delta : G_1 \times G_2 \rightarrow G$ such that $\Delta(S_1 \times S_2) = S$ for some non-trivial primitive formally dual sets S_1, S_2 . Note that $S_1 \times S_2$ is also an $(n, n, n, 1)$ -RDS. Since S_1 is not trivial there is an $x \in G_1 \setminus \{1\}$ such that $v_{S_1}(x) \neq 0$. But due to the RDS property we have $v_{S_1 \times S_2}(x, 1) = v_{S_1}(x) \cdot |S_2| = 1$ and thus $|S_2| = 1$ which is a contradiction since S_2 is supposed to be non-trivial.
2. Note that G is written additively. Suppose there are primitive formally dual sets $S_1 \subset \mathbb{Z}_{p^t}^{s_1}$ and $S_2 \subset \mathbb{Z}_{p^t}^{s_2}$ such that $s_1 + s_2 = 2s$ and there is an isomorphism $\Delta : \mathbb{Z}_{p^t}^{s_1} \times \mathbb{Z}_{p^t}^{s_2} \rightarrow \text{GR}(p^t, s)^2$ such that $\Delta(S_1 \times S_2) = S$ and $0 \in S_1$ and $0 \in S_2$.

Since S_1 and S_2 are primitive we can choose elements $x_1 \in S_1$ and $x_2 \in S_2$ of order p^t respectively. Now let $b, c \in \text{GR}(p^t, s)$ such that $\Delta(x_1, 0) = (b, b^2)$ and $\Delta(0, x_2) = (c, c^2)$.

Then $\Delta(x_1, x_2) = (b + c, b^2 + c^2) \in S$ and thus $(b + c)^2 = b^2 + c^2$ which is only possible if $2bc = 0$. Note that b and c are units. Indeed, if $b \in (p)$ then $\Delta(p^{t-1}x_1, 0) = (0, 0)$ which is not possible since Δ is an isomorphism. Thus $2bc = 0$ is equivalent to $2 = 0$ but since p is odd this is a contradiction.

3. Note that G is written additively. Let $S = \pi(S_0, S_1)$ as given in Example 6.9. Note that $(0, 0) \in S$ due to the definition of S_0 . Suppose there is an isomorphism Δ such that $\Delta(S' \times S'') = S$ for some primitive formally dual sets $S' \subset G_1, S'' \subset G_2$ with $0 \in S', 0 \in S''$.

Note that $U = \Delta(S' \times 0) \subset S$ and $V = \Delta(0 \times S'') \subset S$ have to be two sets such that $u + v \in S$ for all $u = (u', u_1, \dots, u_{2m}) \in U, v = (v', v_1, \dots, v_{2m}) \in V$ and $U \cap V = \{0\}$. Define the support of U as

$$\text{supp}(U) = \{i : \text{there is an } u = (u', u_1, \dots, u_{2m}) \in U \text{ such that } u_i \neq 0\}$$

and the $\text{supp}(V)$ analogously. Note that $u + v \in S$ yields that $u_i, v_i, u_i + v_i \in \{0, 1\}$ and thus the support of U and the support of V have to be disjoint. Consider the following table of pairs $(u' + v', \sum_i (u_i + v_i))$:

	$u' = 0, \sum_i u_i \equiv 1$	$u' = 1, \sum_i u_i \equiv 3$
$v' = 0, \sum_i v_i \equiv 1$	0, 2	1, 0
$v' = 1, \sum_i v_i \equiv 3$	1, 0	0, 2

The occurring entries can not be achieved by elements of S by definition. Thus at most one of $\sum_i u_i$ or $\sum_i v_i$ can be odd.

Therefore we assume without loss of generality that only U contains elements with odd sums and V does not. Thus, U contains at most all elements associated with subsets of $\text{supp}(U)$ while V contains at most all vectors associated with subsets of even size of $\text{supp}(V)$. Since S'' is not trivial we have $|S''| = |V| \geq 2$ and therefore $|\text{supp}(V)| \geq 1$ and $|S''| = |V| < 2^{|\text{supp}(V)|}$ as well as $|S'| = |U| \leq 2^{\text{supp}(U)}$. Altogether, we have

$$2^{|\text{supp}(U)|+|\text{supp}(V)|} \leq 2^{2m} = |S| = |S'| \cdot |S''| < 2^{|\text{supp}(U)|} \cdot 2^{|\text{supp}(V)|}$$

which is a contradiction.

The last assertion follows simply by Corollary 5.12 since $S \subset (\mathbb{Z}_p)^2$ for some odd prime p . \square

We are not able to show irreducibility for all examples presented. We close the section by collecting the open cases in the following question:

Question 6.12. Which of the following examples of primitive formally dual sets are irreducible?

1. Sets constructed using Theorem 6.4 for $m > 1$,
2. Sets constructed using Theorem 6.8 with sets from Example 6.9 as building blocks.

7 Algorithmic approach

In this chapter we discuss an algorithmic approach to find all primitive formally dual pairs in a given group. We discuss a general framework yielding twelve different heuristic approaches in Section 7.1. We compare the performance of respective implementations in Section 7.2 and give a recommendation which one to use. Our implementation can be used to compute a complete list of primitive formally dual pairs in cases, where no non-existence result is known. This algorithm has been used to compute Table A.1 in the appendix. First, we state the problem that the algorithm solves:

Problem 7.1. Given a group $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ of order n and a divisor b of n with $b \leq \sqrt{n}$ compute a list of all primitive formally dual pairs S, T such that $b \leq |S| \leq \sqrt{n}$.

7.1 Graph search algorithm

To compute an answer of Problem 7.1 we propose to use a graph search algorithm on a special graph to compute a set of candidates for formally dual sets before explicitly checking formal duality. We begin with some preparatory definitions.

Let $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ be a finite abelian group. We can define an order on G and $\{S \subset G : |S| = r\}$ as follows:

Definition 7.2. We inherit the order of \mathbb{Z}_n from \mathbb{Z} , i.e. $a + \mathbb{Z}_n < b + \mathbb{Z}_n$ if and only if $a' < b'$ where a' and b' is the smallest non-negative integer such that $a' \in a + n\mathbb{Z}$ and $b' \in b + n\mathbb{Z}$ respectively. An abelian group $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ is ordered lexicographically. I.e. $(x_1, \dots, x_m) < (y_1, \dots, y_m)$ if and only if there is an integer k with $1 \leq k \leq m$ such that $x_i = y_i$ for all $i < k$ and $x_k < y_k$. Furthermore, we use the same approach to order subsets of G of size r : Suppose $S = \{s_1, \dots, s_r\}$,

$T = \{t_1, \dots, t_r\}$ with $s_1 < \dots < s_r$ and $t_1 < \dots < t_r$. We say $S < T$ if and only if there is an index k such that $s_i = t_i$ for all $i < k$ as well as $s_k < t_k$.

Furthermore, we consider equivalence relations which are suitable for the graph search algorithm:

Definition 7.3. An equivalence relation \sim is called *feasible* if for all S, S' with $S \sim S'$ we have

1. $|S| = |S'|$
2. S is a formally dual set if and only if S' is a formally dual set
3. if $S \subset U$ then there is a set $U' \sim U$ such that $S' \subset U'$

Another concept we use are *monotone conditions*:

Definition 7.4. A *monotone condition* $C : 2^G \rightarrow \{0, 1\}$ for formal duality is a boolean function such that

1. if $C(S) = 0$ and $S \subset U$ then $C(U) = 0$
2. if S is a primitive formally dual set then $C(S) = 1$.

In the following, fix a finite abelian group $G = \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_m}$ of order n , a divisor d of n , a feasible relation \sim and a monotone condition C .

Consider the directed graph $G(V, E)$ where

$$V = \{S \subset G : S \leq S' \text{ for all } S' \sim S, |S| \leq n/d, C(S) = 1, 0 \in S\}$$

and $SU \in E$ if and only if there is an $x > \max(S)$ such that $U = S \cup \{x\}$.

The size of this graph depends on the sizes of equivalence classes of \sim and the support of C .

Theorem 7.5. *The graph $G(V, E)$ defined above is a directed tree and*

$$\Sigma = \{S' : S' \sim S \text{ for some } S \in V\}$$

contains all primitive formally dual sets of size up to n/d .

Proof. It is clear that any set $S \subset G$ of size 2 is connected to $\{0\}$. Let $U \in \mathcal{V}$ at least of size two and $S = U \setminus \max(U)$. Note that $C(S) = 1$ since $C(U) = 1$ and C is monotone. Furthermore, suppose there is a set S' such that $S > S'$ and $S \sim S'$. Since \sim is feasible there also is a set $U' \supset S'$ with $U \sim U'$, say $U' = S' \cup \{x\}$. Since $U = S \cup \{\max(U)\} \leq U'$ we also have $S \leq S'$. Therefore, $S \in \mathcal{V}$ and $SU \in E$. Due to the definition of E there also is no other set $S' \in \mathcal{V}$ such that $S'U \in E$. Altogether, $G(\mathcal{V}, E)$ is a directed tree.

Next, suppose S is a primitive formally dual set of size $k \leq \frac{n}{d}$. Let \hat{S} be the minimal set such that $\hat{S} \sim S$ and $0 \in \hat{S}$. Note that $C(\hat{S}) = 1$ since \sim is feasible and thus $\hat{S} \in \mathcal{V}$ and $S \in \Sigma$. \square

We propose to execute a breath-first search on $G(\mathcal{V}, E)$ to get a list of candidates for formally dual sets. Note that $G(\mathcal{V}, E)$ has to be computed first. Due to the monotone condition, we don't need to check the condition on every node when computing the graph. Instead we can 'cut off' whole branches when the condition in one node is 0. The candidates for primitive formally dual sets of size k and the candidates for formally dual sets of size n/k can then be examined pairwise to get a complete list of primitive formally dual sets of size k (respecting \sim). A pseudo code of this algorithm with an implicitly generated search tree is given in Algorithm 1 in the appendix.

In the following we introduce three types of conditions and four types of equivalence relations which can be combined to twelve different heuristic approaches.

The most simple monotone condition is constant to one. Other examples of monotone conditions are given by a list \mathcal{V} such that every possible weight enumerator of a formally dual set is contained in \mathcal{V} . The respective monotone condition is defined by

$$C(S) = \begin{cases} 1 & \text{if } \exists v \in \mathcal{V} : v_S(x) \leq v(x) \forall x \in G \\ 0 & \text{otherwise} \end{cases}.$$

Such a list can be computed with the help of even set theory as an integer point problem in polytopes. To this extend, observe that by Corollary 2.9 and Lemma 4.16 we have:

Corollary 7.6. *Let S be a primitive formally dual set and $SS^{(-1)} = \sum_{i=1}^r \lambda_i C_i$ be the unique even set representation with respect to cyclic groups. Then we have:*

$$\lambda_i \in \mathbb{Z}, \quad (7.1)$$

$$\frac{|G|^2}{|S|^3} \lambda_i \in \mathbb{Z}, \quad (7.2)$$

$$\sum_{i=1}^r \lambda_i = |S|, \quad (7.3)$$

$$0 \leq \sum_{i: g \in C_i} \lambda_i < |S|, \quad (7.4)$$

$$0 \leq \sum_{i: g \in \tilde{C}_i} \lambda_i |C_i| < |S|^2. \quad (7.5)$$

Proof. Equation (7.1) follows directly from Corollary 2.9. For equation (7.2) consider

$$TT^{(-1)} = \sum_{i=1}^r \tilde{\lambda}_i \tilde{C}_i.$$

Due to Corollary 2.9 we have $\tilde{\lambda}_i \cdot \frac{|G|}{|C_i|} \in \mathbb{Z}$ and by Theorem 4.5 we have

$$\tilde{\lambda}_i \cdot \frac{|G|}{|C_i|} = \frac{|G|}{|S|^3} |C_i| \lambda_i \cdot \frac{|G|}{|C_i|} = \frac{|G|^2}{|S|^3} \lambda_i$$

yielding the assertion. The rest of the assertions easily follow from Lemma 4.16. \square

Furthermore, note that by computing all possible λ_i we can compute the weight enumerator as

$$v_S(g) = [SS^{(-1)}]_g = \sum_{i: g \in C_i} \lambda_i.$$

Finding λ_i that satisfy the conditions in Corollary 7.6 is equivalent to the problem of computing lattice points in a polytope. There are several programs to solve such a problem, for example Normaliz [BIR⁺] (which is used in our implementation Appendix B (3)).

We state three different conditions derived by a list of suitable weight enumerators:

1. constant condition ($\mathcal{V} = \mathbb{Z}^n$),

2. \mathcal{V} corresponds to the assumptions in Corollary 7.6 except for (7.2)
3. \mathcal{V} corresponds to the assumptions in Corollary 7.6 including (7.2)

Furthermore, we describe four different kinds of equivalence relations which are feasible due to Corollary 3.14:

1. $S \sim S'$ if and only if $S = S'$,
2. $S \sim S'$ if and only if $S = \phi(S')$ for some automorphism ϕ of G ,
3. $S \sim S'$ if and only if $S = v + S'$ for some $v \in G$,
4. $S \sim S'$ if and only if S and S' are equivalent.

Note, that the knowledge from Chapters 5 and 6 is not included in the algorithm. The graph search approach is therefore only recommended in cases where no other theoretic result is known.

7.2 Comparison

For convenience we use the notation $A_{k,l}$ for the heuristic presented in the previous section that uses condition k and equivalence relation l .

It is not easy to calculate the runtime classes. We conjecture, that all heuristics have the same runtime class. A stronger condition or relation will result in a smaller search tree, but maybe needs longer to compute the graph in the first place.

Thus, we compare the running times of the heuristics on small examples. Therefore, we implemented the framework of Algorithm 1 in gap [GAP19] (see Appendix B (3)). To solve the integer point problem that yields the list of possible weight enumerator we used Normaliz [BIR⁺].

We proceed by defining a measure of quality. Define $t_{i,j}(G, b)$ to be the time in milliseconds that the implementation of $A_{i,j}$ needed to solve Problem 7.1 for a given group G and $b \mid |G|$. Since $A_{1,1}$ is the most naive approach (it is basically brute force), we will use it as a 'baseline' and compare the quality of the heuristics by the quality measure

$$q_{i,j}(G, b) = \log(t_{i,j}(G, b)/t_{1,1}(G, b)).$$

Thus, a 'fast' heuristic has a negative quality measure $q_{i,j}(G, b)$.

First of all observe Figure A.1 in the appendix which compares the heuristics $A_{i,j}$ for fixed equivalence relation j .

Note, that in some cases the preparation of the condition failed or took an unbearable amount of time which is represented in the figure as bars that exceed the boundaries of the diagram. Due to this unstable behavior we do not recommend to use conditions 2 or 3 in the current implementation. However, in some examples, presumably groups that are large enough and have a 'controllable' amount of cyclic subgroups, Condition 3 had a much better performance than the other conditions (see $(\mathbb{Z}_{25}, 5)$, $(\mathbb{Z}_4 \times \mathbb{Z}_3, 2)$, $(\mathbb{Z}_{12}, 2)$, $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3, 2)$ in Figure A.1). Therefore, more investigation is needed, either to find a more stable implementation or to characterize the groups in which Condition 3 behaves well.

Next, observe Figure A.2 in the appendix which compares the implementations $A_{i,j}$ for fixed condition i .

It is apparent, that the heuristics using Relations 2, 3, 4 are, in many cases, faster than the respective heuristic using Relation 1. From the available data we recommend using Relation 3 since this heuristic is in all presented examples faster than Relation 1 and therefore is the most stable.

On the other hand, heuristics using Relation 4 are occasionally faster (see $(\mathbb{Z}_4 \times \mathbb{Z}_4, 4)$, $t_{1,i}$). So, further investigation is needed in order to decide whether other heuristics are more suitable for larger examples.

Overall we recommend the use of Heuristic $A_{1,3}$. Note that this is also the only implementation which has been faster than $A_{1,1}$ in every considered example.

8 Conclusions

In this chapter we summarize the results and open questions of this thesis for future investigations.

As seen in Section 3.1 formal duality of periodic sets is strongly motivated by the so called energy minimization problem. Still a better understanding about the connection of these two problems is needed, i.e.

Question 8.1. Is every energy minimizer a formally dual periodic set?

The study of formal duality of periodic sets can be reduced to the setting of finite abelian groups by using the Poisson summation formula (see Section 3.2). In this new setting, it has been shown that the 'formally dual' property is invariant under translations and automorphisms, yielding the notion of equivalence of formally dual sets (see Corollary 3.14).

A simple way to create a new formally dual set out of a given formally dual set S , is to regard S as a subset of a larger group. A related approach is to take a union of cosets whose natural restriction is S (see Theorem 3.15). The 'building blocks' of this operation are the primitive formally dual sets. Also, taking the cross product of two formally dual sets will produce a new one as shown in Lemma 3.18. The 'building blocks' regarding all these operations are called irreducible formally dual sets. The following questions seem natural and might be seen as the overall goal of the study of formally dual sets:

Question 8.2. Is there a characterization of all primitive formally dual sets? Is there a characterization of all irreducible formally dual sets?

After choosing an isomorphism we are able to define formal self duality which seems to behave very similar to formal duality. In Proposition 3.22 we showed, that in many cases the study of formally self dual sets can be reduced to the study of primitive formally self dual sets. However, it is an open question for arbitrary isomorphisms (see also Conjecture 3.23):

Question 8.3. Suppose $S \subset H \leq G$ is formally self dual.

Is $\{v\tilde{H} : v \in S\} \subset H/\tilde{H}$ a formally self dual set?

All conjectured energy minimizers correspond to the trivial formally dual set or to TITO^k (see Section 3.3). This yields the question, if anything else is possible at all:

Question 8.4. Is there an energy minimizer that does not reduce to $\{1\}$ or TITO^k ?

In the subsequent chapter, we presented the even set approach. An even set can be interpreted as a set such that its multiset of differences lies in the algebra $\mathcal{M}(G)$. Even sets are a broader class of sets than formally dual sets. The most important tool that is provided by even sets is given in Theorem 4.5. It shows that the respective parameters of a formally dual set and its formally dual partner translate into each other in a simple manner. Moreover, there are many results about formally dual sets of certain types. Many of the results in the even set theory could be reformulated if we only allow integer coefficients, which yields the following question (see also Conjecture 4.17):

Question 8.5. Does a minimal representation of an even set always have integral parameters?

Note that this question can also be reformulated in terms of $\mathcal{M}(G)$.

In Section 4.4 it has been shown that all primitive formally dual sets up to rank three are either trivial or $(n, n, n, 1)$ -RDS. And in Corollary 4.7 we have seen a condition for $(n, n, n, 1)$ -RDS to be formally dual. This condition holds for any known examples of RDS, which yields the following question:

Question 8.6. Is every $(n, n, n, 1)$ -RDS a formally dual set?

For higher rank these questions are still open, i.e. we have the following two open questions (see also Conjecture 4.33):

Question 8.7. Is there a characterization of all primitive formally dual sets of rank four? Is there a primitive formally dual set of rank five which is not even with respect to a chain of subgroups?

Moreover, there are many groups without primitive formally dual sets as seen in Chapter 5. For example, the field descent method can be used to show non-existence in cyclic groups. This method would yield even more results if we could answer the following questions (see also Conjecture 5.9):

Question 8.8. Let $P = p_1 \cdot \dots \cdot p_r$ be an arbitrary product of distinct primes. Is there a constant $F(P)$, depending only on P , such that for any primitive formally dual set $S \subset \mathbb{Z}_N$ with $\text{rad}(N) \mid P$ there exists a $d \leq F(P)$ with $v_S(d) \neq 0$?

A weaker, related question is the following:

Question 8.9. Is there a primitive formally dual set S in a cyclic group \mathbb{Z}_N such that $v_S(1) = 0$?

In Section 5.2 we have seen properties of groups that can not contain a primitive formally dual set. However, there are still many groups where no theoretic result is known. This naturally yields the following question:

Question 8.10. Are there non-existence results in the cases that are listed as 'no result' or 'computer search' in Table A.1 or Appendix B (1)?

An important conclusion of Chapter 5 is, that primitive formal duality in cyclic groups seems rare. But it is still not clear whether there are only two primitive formally dual sets in cyclic groups or not. In particular we have the following open questions (see also Conjecture 5.24):

Question 8.11. Is there a primitive formally dual set in a cyclic group other than TITO and the trivial example? Is there a primitive formally dual set in a cyclic group which is divisible by exactly two primes? Is there a primitive formally dual set in \mathbb{Z}_{900} of size 30?

In Chapter 6 we have seen several constructions of families of primitive formally dual sets. Some questions are the following:

Question 8.12. Can you construct primitive/irreducible formally dual sets in groups that are not yet covered? Can you use the lifting construction framework (Theorems 6.6 and 6.8) to construct other examples than the lifted TITO example (Example 6.9)?

In Section 6.2 we checked most of the examples for irreducibility. Two open cases are left. For convenience of the reader we state Question 6.12 here one more time:

Question 8.13. Which of the following examples of primitive formally dual sets are irreducible?

1. Sets constructed using Theorem 6.4 for $m > 1$,

2. Sets constructed using Theorem 6.8 with sets from Example 6.9 as building blocks.

Finally, in Chapter 7 we proposed a graph search algorithm for cases where no theoretic result yields non-existence. This yields the following open problems:

Question 8.14. Is there a faster algorithm than the proposed graph search algorithm? Can the unstable behavior of the non-trivial conditions be fixed? Are there other monotone conditions and feasible equivalence relations which yield faster heuristics? How do the heuristics compare for big examples?

The study of formal duality is far from being finished. It is neither a common phenomenon, since there are many groups without primitive formally dual sets, nor is it impossible to achieve since there are several examples. Due to this and its relations to other fields of mathematics, formal duality is an interesting topic which deserves further investigation.

Acknowledgment

I have been supported by DFG grant SCHU 1503/7. Moreover, I wish to express my sincere gratitude to Achill Schürmann and Alexander Pott for their careful reviews. Furthermore, I like to thank Frieder Ladisch for many helpful discussions.

Bibliography

- [And96] N.N. Andreev. An extremal property of the icosahedron. *East J. Approx.*, 2(4):459–462, 1996.
- [And97] N.N. Andreev. Location of points on a sphere with minimal energy. *Tr. Mat. Inst. Steklova*, 219(Teor. Priblizh. Garmon. Anal.):27–31, 1997.
- [BIR⁺] W. Bruns, B.B. Ichim, T. Römer, R. Sieg, and C. Söger. Normaliz. algorithms for rational cones and affine monoids. Available at <https://www.normaliz.uni-osnabrueck.de>.
- [Bou03] N. Bourbaki. *Algebra II. Chapters 4–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 2003. Translated from the 1981 French edition by P. M. Cohn and J. Howie, Reprint of the 1990 English edition [Springer, Berlin; MR1080964 (91h:00003)].
- [CK07] H. Cohn and A. Kumar. Universally optimal distribution of points on spheres. *J. Amer. Math. Soc.*, 20(1):99–148, 2007.
- [CKM⁺19] H. Cohn, A. Kumar, S.D. Miller, D. Radchenko, and M. Viazovska. Universal optimality of the E_8 and Leech lattices and interpolation formulas. *arXiv e-prints*, page arXiv:1902.05438, Feb 2019.
- [CKRS14] H. Cohn, A. Kumar, C. Reiher, and A. Schürmann. Formal duality and generalizations of the Poisson summation formula. 625:123–140, 2014.
- [CKS09] H. Cohn, A. Kumar, and A. Schürmann. Ground states and formal duality relations in the gaussian core model. *Phys. Rev. E*, 80:061116, Dec 2009.

- [CS12] R. Coulangen and A. Schürmann. Energy minimization, periodic sets and spherical designs. *Int. Math. Res. Not. IMRN*, (4):829–848, 2012.
- [Edw84] H. M. Edwards. *Galois theory*, volume 101 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1984.
- [GAP19] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.10.1*, 2019.
- [Hum96] J.F. Humphreys. *A course in group theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1996.
- [KY94] A.V. Kolushov and V.A. Yudin. On korkin-zolotarev’s construction. *Discrete Mathematics and Applications*, 4:143–146, 01 1994.
- [KY97] A.V. Kolushov and V.A. Yudin. Extremal dispositions of points on the sphere. *Anal. Math.*, 23(1):25–34, 1997.
- [Lan02] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [Lee57] J. Leech. Equilibrium of sets of particles on a sphere. *Math. Gaz.*, 41:81–90, 1957.
- [Li19] S. Li. private communication, 2019. july.
- [LP18] S. Li and A. Pott. Constructions of Primitive Formally Dual Pairs Having Subsets with Unequal Sizes. *arXiv e-prints*, page arXiv:1810.05433, October 2018.
- [LP19] S. Li and A. Pott. A Direct Construction of Primitive Formally Dual Pairs Having Subsets with Unequal Sizes. *arXiv e-prints*, page arXiv:1907.04208, Jul 2019.
- [LPS19] S. Li, A. Pott, and R. Schüler. Formal duality in finite abelian groups. *J. Combin. Theory Ser. A*, 162:354–405, 2019.
- [LS05] K.H. Leung and B. Schmidt. The field descent method. *Des. Codes Cryptogr.*, 36(2):171–188, 2005.

- [Mal17] R.D. Malikiosis. private communication, 2017.
- [Mal18] R.D. Malikiosis. Formal duality in finite cyclic groups. *Constructive Approximation*, Mar 2018.
- [Pot95a] A. Pott. *Finite geometry and character theory*, volume 1601 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1995.
- [Pot95b] A. Pott. *Finite geometry and character theory*, volume 1601 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1995.
- [Sch99] B. Schmidt. Cyclotomic integers and finite geometry. *J. Amer. Math. Soc.*, 12(4):929–952, 1999.
- [Sch02] B. Schmidt. *Characters and cyclotomic fields in finite geometry*, volume 1797 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2002.
- [Sch17] R. Schüler. Formally dual subsets of cyclic groups of prime power order. *Beitr. Algebra Geom.*, 58(3):535–548, 2017.
- [SP17] J.C. Schlage-Puchta. private communication, 2017. july.
- [Sta12] R.P. Stanley. *Enumerative combinatorics. Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2012.
- [Ste12] B. Steinberg. *Representation theory of finite groups*. Universitext. Springer, New York, 2012. An introductory approach.
- [Sti76] F.H. Stillinger. Phase transitions in the gaussian core system. *The Journal of Chemical Physics*, 65(10):3968–3974, 1976.
- [SW71] E.M. Stein and G. Weiss. *Introduction to Fourier analysis on Euclidean spaces*. Princeton University Press, Princeton, N.J., 1971. Princeton Mathematical Series, No. 32.
- [TH11] L. Tóth and P. Haukkanen. The discrete Fourier transform of r -even functions. *Acta Univ. Sapientiae Math.*, 3(1):5–25, 2011.

- [Tho04] J.J. Thomson. Xxiv. on the structure of the atom: an investigation of the stability and periods of oscillation of a number of corpuscles arranged at equal intervals around the circumference of a circle; with application of the results to the theory of atomic structure. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 7(39):237–265, 1904.
- [Wan03] Z. Wan. *Lectures on finite fields and Galois rings*. World Scientific Publishing Co., Inc., River Edge, NJ, 2003.
- [WH09] G. Weng and L. Hu. Some results on skew Hadamard difference sets. *Des. Codes Cryptogr.*, 50(1):93–105, 2009.
- [Xia16] J. Xia. Classification of formal duality with an example in sphere packing. <https://math.mit.edu/research/undergraduate/urop-plus/documents/2016/Xia.pdf>, 2016. Accessed 2019-01-31.
- [Yam90] M. Yamada. Distance-regular digraphs of girth 4 over an extension ring of $\mathbf{Z}/4\mathbf{Z}$. *Graphs Combin.*, 6(4):381–394, 1990.
- [Yud93] V.A. Yudin. The minimum of potential energy of a system of point charges. *Discrete Mathematics and Applications*, 3:75–82, 01 1993.

Index

- p -group, 4
 - Sylow group, 4, 57–60
- Algebraic integer, 3, 19
- Cyclotomic field, 3, 51–54
 - Galois automorphism, 3, 11
 - root of unity, 3, 5, 52
- Difference set, 28
 - skew Hadamard difference set, 64–65, 69
- Differences of a set, 4, 6, 28, 40, 52, 80
- Dual group, 4, 5, 18, 23, 62
 - annihilator, 4, 5, 21, 22, 62
 - discrete fourier transform, 4, 7, 9, 11, 19
 - fourier inversion, 7, 11
 - principal character, 4, 21
- Energy minimization problem, 14–15, 26, 79
 - pair potential, 13–14
 - Thomson problem, 14
- Equivalent sets, 21, 26, 54, 55, 76
- Even set, 27–30, 35–49, 75, 80
 - minimal representation, 28, 37, 80
 - rank, 28, 30, 45–48, 80
 - representation, 27, 29, 35–75
 - respective subgroups, 27
 - with respect to cyclic subgroups, 28, 49, 75
- Exponent of a group, 4, 57, 58
- Field descent method, 51–54, 81
- Formal duality in abelian groups, 18–79
 - TITO, 20, 26, 49, 54, 55, 60, 68, 80
 - cross product construction, 22, 68, 79
 - formally dual pair, 19–24, 29, 30, 35, 49, 58, 59, 63, 65–67, 73
 - formally dual set, 19–21, 28, 35, 36, 42, 44–49, 52, 54–56, 58, 60, 75, 80, 81
 - formally self dual, 24, 25, 30, 64, 79
 - in cyclic groups, 49, 52, 53, 60, 81
 - irreducible, 23, 69–71, 81
 - primitive, 22, 35, 36, 38, 42, 44, 52, 54, 56–60, 65–67, 69, 73, 75, 79–81
 - under isomorphism, 23–25, 79
 - under pairing, 23
- Formal duality of periodic sets, 17, 18, 20, 79, 80
 - TITO, 18
 - average pair sum, 17
 - formally dual pair, 58
- Fourier-transform, 16
- Galois ring, 61–64

- Graph search algorithm, 73–78, 82
 - feasible relation, 74, 77, 82
 - monotone condition, 74–76, 82
 - order in abelian group, 73
- Group algebra, 5–11, 27–48, 64, 66
 - linear combination of subgroups, 6
 - support, 6
- Hasse-type diagram, 30–35, 38–40, 42, 44–47, 54
 - admissible identification, 32, 35
 - dual diagram, 35
 - fitting a family of subgroups, 32–34
 - Hasse-diagram, 31, 33, 45
- Impartible subgroup, 37, 38
- Isomorphism, 5, 23
 - adjoint automorphism, 21
 - adjoint isomorphism, 5, 24, 65
 - pairing, 5, 19, 62, 65, 67
 - standard pairing, 5, 24, 25, 68
 - trace isomorphism, 62, 63
- Lifting construction, 65–69, 81
 - lifted TITO, 68, 81
 - lifting operator, 65
 - recursive lifting construction, 67, 71, 82
- Moebius inversion, 7, 11, 49
- Periodic set, 14–19
 - Checkerboard lattice, 15
 - Leech lattice, 14
 - period lattice, 15
 - point density, 17
- Poisson summation formula, 16, 79
- Relative difference set, 28, 30, 40, 45, 48, 54, 61, 68, 69, 80
 - generalized relative difference set, 64
- Schwartz function, 16
- Self conjugate, 57
- Weight enumerator, 18, 19, 28, 36, 49, 58, 75, 81
 - generalized weight enumerator, 65, 66

Appendix

A Table of results

(G , S)	G	prim. f.d.s.	reasoning
(4, 2)	\mathbb{Z}_2^2	none	Lemma 5.19
	\mathbb{Z}_4	TITO	Example 3.11
		list complete	Proposition 5.23 (1)
(8, 2)	arbitrary	none	Proposition 5.23 (1)
(9, 3)	\mathbb{Z}_3^2	(3, 3, 3, 1)-RDS	Example 6.2
		list complete	computer search
	\mathbb{Z}_9	none	Proposition 5.23(2)
(12, -)	arbitrary	none	Theorem 5.16 with $p = 3$
(16, 2)	arbitrary	none	Proposition 5.23 (1)
(16, 4)	\mathbb{Z}_2^4	none	Lemma 5.19
	$\mathbb{Z}_4 \times \mathbb{Z}_2^2$	none	computer search
	\mathbb{Z}_4^2	product of smaller examples	Lemma 3.18
		self dual (4, 4, 4, 1)-RDS	Corollary 4.7
		list complete	computer search
	$\mathbb{Z}_8 \times \mathbb{Z}_2$	none	computer search
	\mathbb{Z}_{16}	none	Corollary 5.12
(18, -)	arbitrary	none	Theorem 5.16 with $p = 2$
(20, 2)	arbitrary	none	Proposition 5.23 (1)
(24, 2)	arbitrary	none	Proposition 5.23 (1)
(24, 4)	$\mathbb{Z}_6 \times \mathbb{Z}_2^2$	none	Theorem 5.16 with $p = 3$
	$\mathbb{Z}_{12} \times \mathbb{Z}_2$	none	Theorem 5.16 with $p = 3$
	\mathbb{Z}_{24}	none	Theorem 5.15 (1)
(25, 5)	\mathbb{Z}_5^2	(5, 5, 5, 1)-RDS	Example 6.2

		list complete	computer search
	\mathbb{Z}_{25}	none	Proposition 5.23(2)
(27, 3)	\mathbb{Z}_3^3	none	Lemma 5.19
	$\mathbb{Z}_9 \times \mathbb{Z}_3$	none	Proposition 5.23(2)
	\mathbb{Z}_{27}	none	Proposition 5.23(2)
(28, -)	arbitrary	none	Theorem 5.16 with $p = 7$
(32, 2)	arbitrary	none	Proposition 5.23 (1)
(32, 4)	\mathbb{Z}_2^5	none	Lemma 5.19
	$\mathbb{Z}_4 \times \mathbb{Z}_2^3$	none	Lemma 5.19
	$\mathbb{Z}_4^2 \times \mathbb{Z}_2$	lifted TITO	Example 6.9
		list complete	computer search
	$\mathbb{Z}_8 \times \mathbb{Z}_2^2$	none	computer search
	$\mathbb{Z}_8 \times \mathbb{Z}_4$	none	computer search
	$\mathbb{Z}_{16} \times \mathbb{Z}_2$	none	computer search
	\mathbb{Z}_{32}	none	Corollary 5.12
(36, 2)	arbitrary	none	Proposition 5.23 (1)
(36, 3)	\mathbb{Z}_6^2	none	Theorem 5.22 with $p = 2, e = 1$
	$\mathbb{Z}_{18} \times \mathbb{Z}_2$	none	Proposition 5.23(2)
	$\mathbb{Z}_{12} \times \mathbb{Z}_3$	none	Theorem 5.16 with $p = 2$
	\mathbb{Z}_{36}	none	Proposition 5.23(2)
(36, 6)	\mathbb{Z}_6^2	none	computer search
	$\mathbb{Z}_{18} \times \mathbb{Z}_2$	none	computer search
	$\mathbb{Z}_{12} \times \mathbb{Z}_3$	product of smaller examples	Lemma 3.18
		list complete	computer search
	\mathbb{Z}_{36}	none	Theorem 5.15 (2)
(40, 2)	arbitrary	none	Proposition 5.23 (1)
(40, 4)	$\mathbb{Z}_{10} \times \mathbb{Z}_2^2$	none	Theorem 5.16 with $p = 5$
	$\mathbb{Z}_{20} \times \mathbb{Z}_2$	none	Proposition 5.17 with $p = 5$ on T
	\mathbb{Z}_{40}	none	Theorem 5.15 (1)
(44, -)	arbitrary	none	Theorem 5.16 with $p = 11$
(45, -)	arbitrary	none	Theorem 5.16 with $p = 5$
(48, 2)	arbitrary	none	Proposition 5.23 (1)
(48, 4)	$\mathbb{Z}_6 \times \mathbb{Z}_2^3$	none	Lemma 5.19
	$\mathbb{Z}_{12} \times \mathbb{Z}_2^2$	none	Theorem 5.16 with $p = 3$
	$\mathbb{Z}_{12} \times \mathbb{Z}_4$	none	Theorem 5.16 with $p = 3$
	$\mathbb{Z}_{24} \times \mathbb{Z}_2$	none	computer search
	\mathbb{Z}_{48}	none	Theorem 5.15 (1)

(48, 6)	$\mathbb{Z}_6 \times \mathbb{Z}_2^3$	none	Theorem 5.16 with $p = 3$
	$\mathbb{Z}_{12} \times \mathbb{Z}_2^2$	none	Theorem 5.16 with $p = 3$
	$\mathbb{Z}_{12} \times \mathbb{Z}_4$	none	Theorem 5.16 with $p = 3$
	$\mathbb{Z}_{24} \times \mathbb{Z}_2$	none	Proposition 5.17 with $p = 3$
	\mathbb{Z}_{48}	none	Theorem 5.15 (1)
(49, 7)	\mathbb{Z}_7^2	(7, 7, 7, 1)-RDS from skew Hadamard DS list complete	Example 6.2 Theorem 6.4 computer search
	\mathbb{Z}_{49}	none	Proposition 5.23(2)
(50, -)	arbitrary	none	Theorem 5.16 with $p = 2$
(52, 2)	arbitrary	none	Proposition 5.23 (1)
(54, -)	arbitrary	none	Theorem 5.16 with $p = 2$
(56, -)	arbitrary	none	Theorem 5.16 with $p = 7$
(60, 2)	arbitrary	none	Proposition 5.23 (1)
(60, 6)	$\mathbb{Z}_{30} \times \mathbb{Z}_2$	none	Theorem 5.16 with $p = 3$
	\mathbb{Z}_{60}	none	Proposition 5.17 with $p = 3$
(63, 3)	$\mathbb{Z}_{21} \times \mathbb{Z}_3$	none	Proposition 5.17 with $p = 7$ on T
	\mathbb{Z}_{63}	none	Proposition 5.23(2)

B Cd appendix

On the in the printed version enclosed CD are the following files:

1. giantTable.pdf - a table similar to Table A.1 for groups up to order 10^3 ,
2. cyclicExceptions.pdf - a list of cyclic groups without known non-existence result up to order 10^4 .
3. searchv3.gap - the source code of the gap implementation of Algorithm 1 and several more useful functions.
4. template.tex - a tex file to visualize LateX tables produced with the command `GetExampleTable(range)` contained in (3).

C Algorithm and Comparison

Algorithm 1 A general framework to compute Problem 7.1

```

1: Prepare monoton conditions  $C$  and a feasible relation  $\sim$ 
2: for  $k = 1, \dots, n/d$  do                                 $\triangleright$  Compute candidate sets of size  $\leq n/d$ 
3:   if  $k = 1$  then
4:      $S^*(k) \leftarrow [\{0\}]$                                  $\triangleright$  w.l.o.g.  $0 \in S$ 
5:   else
6:      $S^*(k) \leftarrow []$                                      $\triangleright$  initialize  $S^*(k)$  that will contain nodes of size  $k$ 
7:     for  $S' \in S^*(k-1)$  do                                 $\triangleright$  start with smaller set  $S'$ 
8:       for  $x > \max(S')$  do
9:          $S'' \leftarrow S' \cup \{x\}$                          $\triangleright$  create branches
10:        if  $S'' \leq S$  for all  $S \sim S''$  and  $S''$  satisfies  $C$  then
11:          Add  $S''$  to  $S^*(k)$                                  $\triangleright$  Add if it is a graph node
12:        end if
13:      end for
14:    end for
15:  end if
16: end for
17: If necessary, delete all non-primitive sets, and all non-even sets from  $S^*$ 
18:  $L \leftarrow \emptyset$                                      $\triangleright$  Initializing list  $L$  of formally dual sets
19: for  $d|n : b \leq d \leq \sqrt{n}$  do
20:   for  $S \in S^*(d), T \in S^*(n/d)$  do
21:     for  $T' : T' \sim T$  do
22:       If  $S$  and  $T'$  form a formally dual pair, add  $(S, T')$  to  $L$ .
23:     end for
24:   end for
25: end for
26: return  $L$ 

```

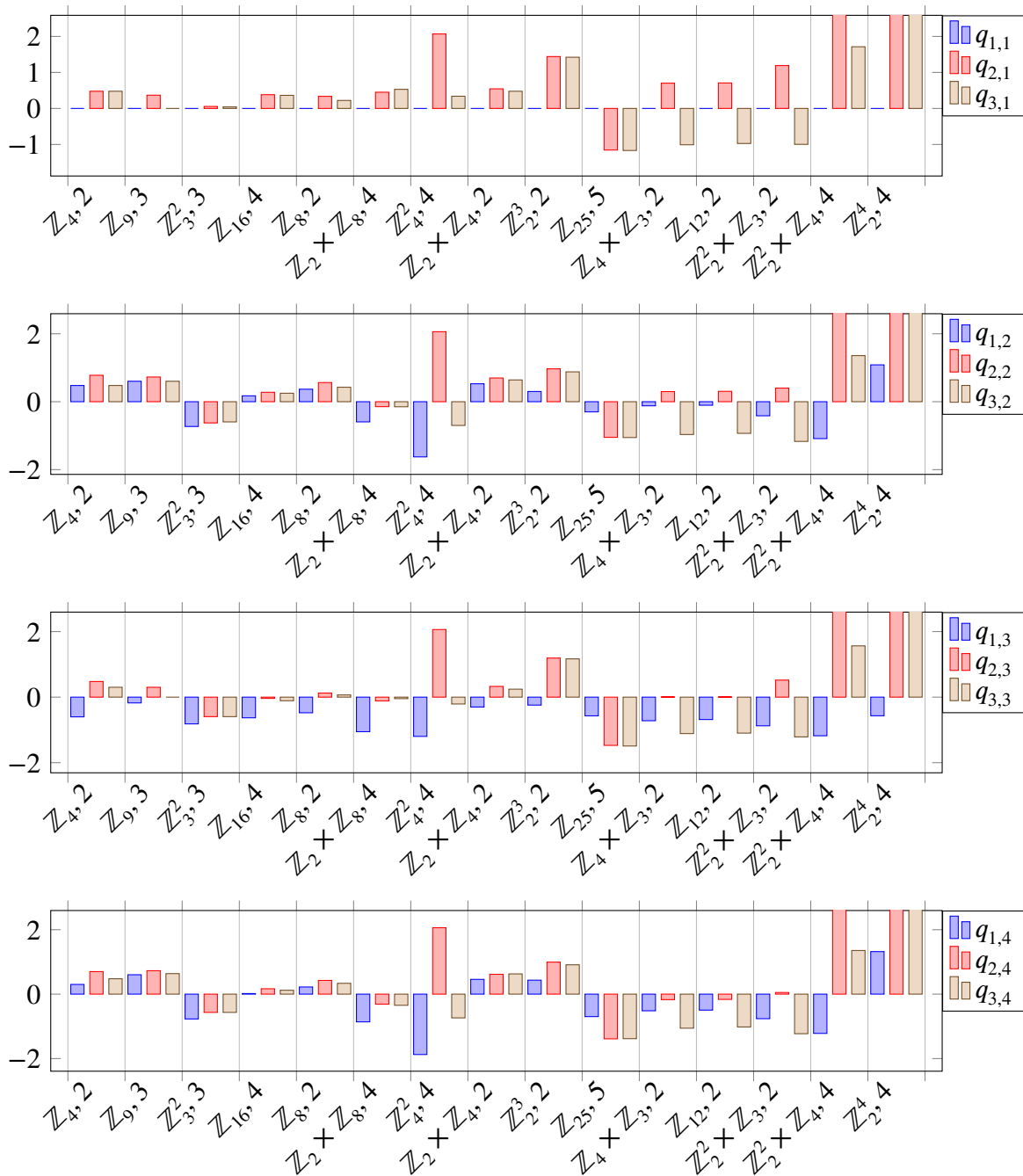


Figure A.1: Comparison of Heuristics where the equivalence relation is fixed, bars that exceed the boundaries are either infinite or bigger than 5

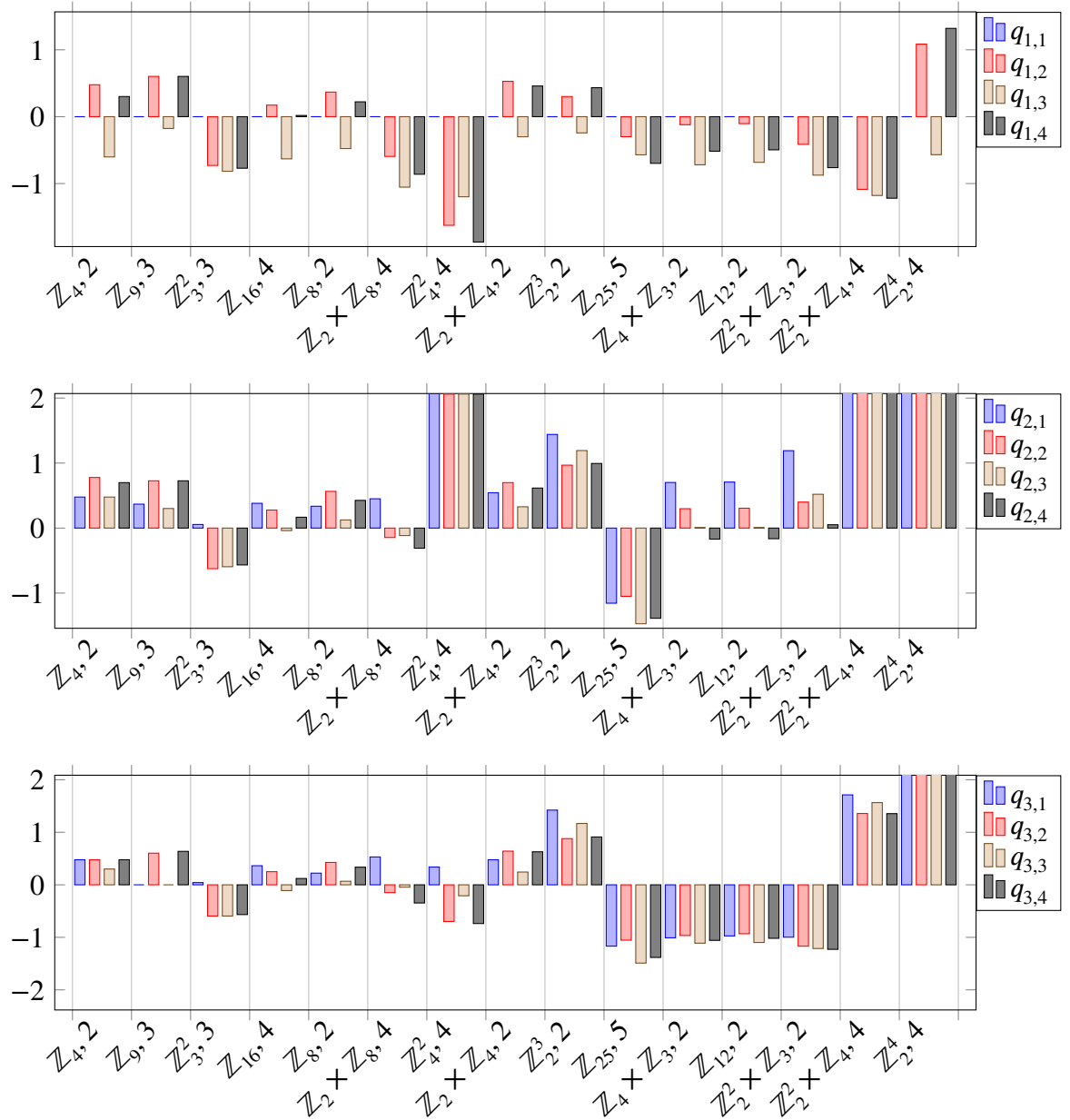


Figure A.2: Comparison of Heuristics where the type of conditions is fixed, bars that exceed the boundaries are either infinite or bigger than 5