Formal-dual subsets of cyclic groups of prime power order

Robert Schüler*

May 20, 2016

Abstract

We study the notion of formal-duality over finite cyclic groups of prime power order as introduced by Cohn, Kumar, Reiher and Schürmann. We will prove that for any cyclic group of odd prime power order, as well as for any cyclic group of order $2^{2l+1}$, there is no primitive pair of formally-dual subsets. This partially proves a conjecture, made by the priorly mentioned authors, that the only cyclic groups with a pair of primitive formally-dual subsets are $\{0\}$ and $\mathbb{Z}/4\mathbb{Z}$.

1 Introduction

This work contains new results for the understanding of formal-dual sets. There is a deep interest in the study of the minimization of potential energies over the space of periodic sets. During several numerical experiments, Cohn, Kumar and Schürmann found in [3] that, in low dimensions, each (at least numerically) optimal configuration has a formally-dual periodic set. This is remarkable since this property is very rare among general periodic-sets. Formal-duality arises from a generalisation of the Poisson-summation formula for lattices and was introduced in [3, Chapter 6]. Nevertheless, the exact relationship between local optimality of energy minimization problems and formal-dual sets is not well understood so far. Also the characterization of formal-dual periodic sets is incomplete, even in dimension one. The work of Cohn, Kumar, Reiher and Schürmann [2] reduced the study of formal-dual periodic sets to the study of formal-dual subsets of finite abelian groups. Furthermore they gave a proof that each abelian group $\mathbb{Z}/p^2\mathbb{Z}$, where $p$ is an odd prime, does not contain any primitive formal-dual subset (see Definition 2.6). In the case of $\mathbb{Z}/4\mathbb{Z}$ there is the (up to translation) unique subset TITO = $\{0,1\} \subset \mathbb{Z}/4\mathbb{Z}$ which is formally-dual to itself. A conjecture mentioned in [2, Chapter 4.2] claims that $\{0\} \subset \mathbb{Z}/\mathbb{Z}$ and TITO $\subset \mathbb{Z}/4\mathbb{Z}$ are the only primitive formal-dual subsets of cyclic groups. In this article we will show that there is no primitive formal-dual subset of $\mathbb{Z}/p^k\mathbb{Z}$ if $p$ is an odd prime. On the way we will also obtain several restrictions for primitive formal-dual subsets of arbitrary finite cyclic groups.

This paper is organized as follows: In Section 2 we recall the term of formal-duality and clarify all notions that are necessary to understand Theorem 1.1. Furthermore we develop an alternative view on formal-duality which is useful for the

*Universität Rostock, robert.schueler2@uni-rostock.de
purposes of this paper. In Section 2 we give some general restrictions on weight
enumerators of formal-dual sets (see Definition 2.1). Using these we are able to
prove in Section 3 the following main theorem of this article:

Theorem 1.1. Let \( p \) be an odd prime and \( k \geq 1 \). There is no primitive formal-dual
subset of \( \mathbb{Z}/p^k\mathbb{Z} \).

2 Formal duality

In this section we clarify all terms to understand the main theorem. In particular,
will recall the definition of formal-duality from [2] and give an equivalent definition
of formal-dual subsets of finite cyclic groups. Furthermore, we recall several results
about formal-duality and define the term of a primitive formal-dual set.

First, we consider a function which plays a central role in this article.

Definition 2.1. Let \( T \) be a subset of an (additive) abelian Group \( G \). Then the
weight enumerator of \( T \) is defined as

\[
\nu_T : G \to \mathbb{N}_0, \quad \nu_T(y) = \# \{ (v, w) \in T \times T : v - w = y \}.
\]

It counts all differences of elements of \( T \) which are equal to \( y \).

Now we recall the definition of formal-dual subsets from [2, Definition 2.9], and
develop an equivalent formulation which relates the weight enumerators directly.

Definition 2.2. Let \( S \) be a subset of the finite abelian group \( G \) and \( T \) a subset of
the dual group \( \hat{G} \) (that is the group of all homomorphism \( G \to \mathbb{C}^* \)). Then \( S \) and
\( T \) are said to be formally-dual to each other if

\[
\left| \frac{1}{|T|} \nu_T(y) \right|^2 = \left| \frac{1}{|S|} \sum_{x \in S} \langle x, y \rangle \right|^2
\]

for every \( y \in \hat{G} \) where \( \langle x, y \rangle = y(x) \).

In [2, Remark 2.10] it was mentioned that this definition is actually symmetric.
So one can interchange the roles of \( S \) and \( T \) in the formula (this is possible via
the natural isomorphism between \( G \) and \( \hat{G} \)). For the purposes of this paper it is
convenient to use an alternative formulation of formal-duality which relates only
the weight enumerators of \( S \) and \( T \) to each other.

Lemma 2.3. Let \( S \) be a subset of the finite abelian group \( G \) and \( T \) a subset of the
dual group \( \hat{G} \). Then \( S \) and \( T \) are formally-dual to each other if and only if

\[
\frac{|S|^2}{|T|} \nu_T(y) = \sum_{v \in G} \nu_S(v) \langle v, y \rangle
\]

for every \( y \in \hat{G} \).
Proof. By a short computation using the facts \( \langle v, y \rangle = \langle -v, y \rangle \) and \( \langle x, y \rangle \cdot \langle x', y \rangle = \langle x + x', y \rangle \), we get

\[
\left| \frac{1}{|S|} \sum_{x \in S} \langle x, y \rangle \right|^2 = \frac{1}{|S|^2} \left( \sum_{x \in S} \langle x, y \rangle \right) \left( \sum_{x \in S} \overline{\langle x, y \rangle} \right) = \frac{1}{|S|^2} \sum_{x, x' \in S} \langle x, y \rangle \overline{\langle x', y \rangle} = \frac{1}{|S|^2} \sum_{x, x' \in S} \langle x - x', y \rangle = \frac{1}{|S|^2} \sum_{v \in G} \nu_S(v) \langle v, y \rangle.
\]

By applying this formula to Definition 2.2, we get the required equivalence. \( \Box \)

In the following we will give a structure analysis of \( \nu_S \) on cyclic groups \( G = \mathbb{Z}/n\mathbb{Z} \). On that account we identify \( \hat{G} \) with \( G \) itself, using \( \langle x, y \rangle = e^{2\pi i xy/n} = \zeta_n^{xy} \) for \( \zeta_n := e^{2\pi i/n} \). Thereby an equivalent notion of formal-duality arises:

**Definition 2.4.** Two sets \( S, T \subset \mathbb{Z}/n\mathbb{Z} \) are said to be formally-dual to each other if

\[
\left| \frac{|S|^2}{|T|} \nu_T(y) \right|^2 = \sum_{v \in \mathbb{Z}/n\mathbb{Z}} \nu_S(v) \zeta_n^{vy}
\]

holds for each \( y \in \mathbb{Z}/n\mathbb{Z} \). Furthermore, a set \( S \subset \mathbb{Z}/n\mathbb{Z} \) is said to be formal-dual if there exists a set \( T \subset \mathbb{Z}/n\mathbb{Z} \) such that \( S \) and \( T \) are formally-dual to each other.

Using Lemma 2.3, we can reformulate all results about pairs \( S, T \subset G, T \subset \hat{G} \) of formally-dual sets as results about pairs of formally-dual sets of \( \mathbb{Z}/n\mathbb{Z} \). One useful example is the following lemma from [2, end of Proof 2.8]:

**Lemma 2.5.** Let \( S, T \subset \mathbb{Z}/n\mathbb{Z} \) be formally-dual to each other. Then

\[
n = |S| \cdot |T|.
\]

Another key definition is the notion of primitive formal-dual subsets, that is:

**Definition 2.6.** A pair of formally-dual subsets \( S, T \subset \mathbb{Z}/n\mathbb{Z} \) is said to be primitive if neither \( S \) nor \( T \) is contained in some proper coset of \( \mathbb{Z}/n\mathbb{Z} \). A formal-dual subset \( S \subset \mathbb{Z}/n\mathbb{Z} \) is said to be primitive if there is some set \( T \subset \mathbb{Z}/n\mathbb{Z} \) such that \( S \) and \( T \) form a primitive pair.

By Lemma 2.3 this definition is equivalent to the notion of primitive formal-dual sets in [2, Section 4.1]. According to [2, Lemma 4.1, 4.2] and the discussion below, any pair of sets that are formally-dual to each other can be constructed from some primitive pair. Therefore it suffices for the characterisation of formal-dual sets to find all primitive formal-dual sets.

We end this section with the currently only known examples of primitive formal-dual sets of finite cyclic groups as stated in [2, Section 3.1 and discussion before].

3
Example 2.7. The simplest example is the set \( \{0\} \subset \{0\} = \mathbb{Z}/\mathbb{Z} \) which is formally-dual to itself as is easily checked. This relates to lattices and dual lattices. Another example is the configuration \( \text{TITO} = \{0,1\} \subset \mathbb{Z}/4\mathbb{Z} \) which is formally dual to itself. In [2, Section 3.1] this was checked by using Definition 2.2, but this is also easily checked by Definition 2.4 after computing the weight enumerator

\[
\nu_{\text{TITO}}(v) = \begin{pmatrix}
0 & 1 & 2 & 3 \\
\{(x,y) : x - y = v\} & \{(0,0),(1,1)\} & \{(1,0)\} & \emptyset & \{(0,1)\}
\end{pmatrix}.
\]

Now we have introduced the vocabulary to understand the main theorem, i.e. Theorem 1.1.

3 Restrictions of the weight enumerator of formal-dual sets

In this section we will prove some restrictions of the weight enumerators of formal-dual sets. In Theorem 3.1 which is the main theorem of this section, we will see that the weight enumerator of a formal-dual subset of some finite cyclic group only takes a small number of different values. Likely, there are similar results about weight enumerators in more general cases.

Using the structure of the weight enumerator, we are able to prove several further results. Some of those results are even valid for arbitrary finite cyclic groups. In general, there is no function satisfying all of these conditions as we see in the following section.

During this section we will use the notation \( \gcd(y,n) \) for \( y \in \mathbb{Z}/n\mathbb{Z} \). Since any representative in some coset of \( n\mathbb{Z} \) has the same greatest common divisor with \( n \), this notation is well defined. First, we will prove the main theorem of this section:

Theorem 3.1. Let \( T \) be a formal-dual subset of \( \mathbb{Z}/n\mathbb{Z} \). Then the weight enumerator satisfies

\[
\nu_T(y) = \nu_T(\gcd(y,n))
\]

for all \( y \in \mathbb{Z}/n\mathbb{Z} \).

Proof. For all \( y \in \mathbb{Z}/n\mathbb{Z} \) with \( \gcd(y,n) = 1 \) let \( \sigma_y \in \text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \) be defined by \( \sigma_y : \mathbb{Q}(\zeta_n) \rightarrow \mathbb{Q}(\zeta_n), \zeta_n \mapsto \zeta_n^y \).

Since \( T \) is a formal-dual set there is some set \( S \subset \mathbb{Z}/n\mathbb{Z} \) that is formally-dual to \( T \). Then, by definition

\[
\frac{|S|^2}{|T|} \nu_T(y) = \sum_{v \in \mathbb{Z}/n\mathbb{Z}} \nu_S(v) \zeta_n^{vy} = (*)
\]

for arbitrary \( y \in \mathbb{Z}/n\mathbb{Z} \). Now let \( d = \gcd(y,n) \). There is some \( y' \in \mathbb{Z}/n\mathbb{Z} \) relatively prime to \( n \) with \( y = dy' \). Then

\[
\frac{|S|^2}{|T|} \nu_T(y) = \sum_{v \in \mathbb{Z}/n\mathbb{Z}} \nu_S(v) \zeta_n^{vy} = \sigma_y' \left( \sum_{v \in \mathbb{Z}/n\mathbb{Z}} \nu_S(v) \zeta_n^{vd} \right)
\]
Note that the inner sum is exactly $\frac{|S|^2}{|T|} \nu_T(d) \in \mathbb{Q}$ since $S$ and $T$ are formally-dual to each other. Since the elements of $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ fix $\mathbb{Q}$ point-wise, we have

$$\frac{|S|^2}{|T|} \nu_T(y) = \sigma_y \left( \frac{|S|^2}{|T|} \nu_T(d) \right) = \frac{|S|^2}{|T|} \nu_T(d).$$

This equation is equivalent to the assertion of the theorem since $d = \gcd(y, n)\] \square$

The strong restriction of \ref{thm:main} can be used to simplify the formulas appearing in Definition \ref{def:ramanujan}. In order to do so, we first cite a lemma from \cite[Theorem 271]{ref} which helps to compute sums of roots of unity. Then we will slightly generalize it to fit our needs.

**Lemma/Definition 3.2.** For any $n, d \in \mathbb{N}$ the sum

$$C_n(d) := \sum_{v=1, \ldots, n \atop \gcd(v,n)=1} \zeta_n^{vd}$$

is called Ramanujan’s sum. The function $\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}$ defined by

$$\mu(m) := \begin{cases} (-1)^k & \text{if } m \text{ is square-free, where } k \text{ is the number of prime factors of } m \\ 0 & \text{otherwise} \end{cases}$$

is called Möbius function. Ramanujan’s sum can be evaluated as

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

**Lemma/Definition 3.3.** For any $n \in \mathbb{N}$ and $d, e | n$ the following equality holds:

$$C_n(d, e) := \sum_{v \in \mathbb{Z}/n\mathbb{Z} \atop \gcd(v,n)=e} \zeta_n^{vd} = \sum_{g | \gcd(d,n/e)} \mu(n/eg)g.$$

Note that for $e = 1$ this is exactly Lemma \ref{lem:ramanujan}. If furthermore $(n/e)|d$, then

$$C_n(d, e) = \varphi(n/e),$$

where $\varphi$ is Euler’s totient function. For $d = 1$ the stated formula simplifies to

$$C_n(1, e) = \mu(n/e).$$

**Proof.** Using Lemma \ref{lem:ramanujan} the first statement is valid due to the following computation:

$$\sum_{v \in \mathbb{Z}/n\mathbb{Z} \atop \gcd(v,n)=e} \zeta_n^{vd} = \sum_{v=1, \ldots, (n/e)-1 \atop \gcd(v,n/e)=1} \zeta_n^{dv} = \sum_{v' = 1, \ldots, (n/e)} \zeta_n^{dv' \gcd(v', n)/e} = C_{n/e}(d) = \sum_{g | \gcd(d,n/e)} \mu(n/eg)g.$$
Since \( \sum_{g|n} \mu(n/g)g = \varphi(n) \), which is a well known identity in number theory (see for example [1, page 48]), we have

\[
C_n(d,e) = \varphi(n/e).
\]

This is the second assertion. The third assertion easily follows from

\[
C_n(1,e) = \sum_{g|\gcd(1,n/e)} \mu(n/eg)g = \sum_{g=1}^{\varphi(n/e)} g = \varphi(n/e).
\]

These lemmata are used for the following corollary which simplifies all sums appearing in Definition 2.4. They provide a new perspective on formal-duality and are useful to prove non-existence of formal-dual sets under certain conditions.

**Corollary 3.4.** Let \( S, T \subset \mathbb{Z}/n\mathbb{Z} \) be formally-dual to each other. Then for each \( y \in \mathbb{Z}/n\mathbb{Z} \), we have

\[
\frac{|S|^2}{|T|} \nu_T(y) = \sum_{e|n} C_n(\gcd(y,n), e) \cdot \nu_S(e),
\]

where \( C_n(\gcd(y,n), e) \) are natural numbers defined in Lemma 3.3. Furthermore, the following special cases turn out to be very useful for our purposes:

1. \( \frac{|S|^2}{|T|} \nu_T(1) = \sum_{e|n} \varphi(n/e) \nu_S(e) \) and
2. \( |S|^2 = \frac{|S|^2}{|T|} \nu_T(0) = \sum_{e|n} \varphi(n/e) \nu_S(e). \)

If \( n = p^k \) for some prime \( p \) this can be simplified further as

3. \( \frac{|S|^2}{|T|} \nu_T(1) = \nu_S(0) - \nu_S(p^{k-1}) \) and
4. \( |S|^2 = \frac{|S|^2}{|T|} \nu_T(0) = \nu_S(0) + \sum_{l=0}^{k-1} (p-1)p^{k-l-1} \nu_S(p^l). \)

**Proof.** Let \( d = \gcd(y,n) \). Since \( T \) is a formal-dual subset of \( \mathbb{Z}/n\mathbb{Z} \) we can apply Theorem 3.1 to gain

\[
\frac{|S|^2}{|T|} \nu_T(y) = \frac{|S|^2}{|T|} \nu_T(d).
\]

According to Definition 2.4 with \( y = d \) we then have

\[
\frac{|S|^2}{|T|} \nu_T(y) = \sum_{v \in \mathbb{Z}/n\mathbb{Z}} \nu_S(v) \zeta_{p^k}^{dv} = \sum_{e|n} \sum_{v \in \mathbb{Z}/n\mathbb{Z}} \nu_S(v) \zeta_{p^k}^{dv}.
\]

We again apply Theorem 3.1 to see that all terms \( \nu_S(v) \) appearing in any of the inner sums are in fact the same. This yields

\[
\frac{|S|^2}{|T|} \nu_T(y) = \sum_{e|n} \nu_S(e) \sum_{v \in \mathbb{Z}/n\mathbb{Z}} \zeta_{p^k}^{dv}.
\]
Now we can apply the definition of $C_n(d,e)$ in Lemma 3.3 to see
\[
\frac{|S|^2}{|T|} \nu_T(y) = \sum_{e \mid n} \nu_S(e) C_n(d,e).
\]
This is exactly the stated assertion.

For the special cases 1 and 3, we observe the general formula for $d = 1$. According to Lemma 3.3,
\[
\frac{|S|^2}{|T|} \nu_T(1) = \sum_{e \mid n} C_n(1,e) \nu_S(e) = \sum_{e \mid n} \mu(n/e) \nu_S(e).
\]
If $n = p^k$ we can write all divisors $e$ of $n$ as $p^l$ for $l = 0, \ldots, k$. Furthermore
\[
\mu(n/p^l) = \mu(p^{k-l}) = \begin{cases} 
1 & \text{if } p^{k-l} \text{ is square-free and has an even number of prime divisors} \\
-1 & \text{if } p^{k-l} \text{ is square-free and has an odd number of prime divisors} \\
0 & \text{otherwise}
\end{cases}
\]
\[
= \begin{cases} 
1 & \text{if } l = k \\
-1 & \text{if } l = k - 1 \\
0 & \text{otherwise}
\end{cases}
\]
Therefore,
\[
\frac{|S|^2}{|T|} \nu_T(1) = \sum_{e \mid n} \mu(n/e) \nu_S(e) = \nu_S(0) - \nu_S(p^{k-1})
\]
which is Assertion 3.

For the special cases 2 and 4 we observe the general formula for $y = 0$. According to Lemma 3.3 we have
\[
\frac{|S|^2}{|T|} \nu_T(0) = \sum_{e \mid n} C_n(\gcd(0,n),e) \nu_S(e) = \sum_{e \mid n} C_n(n,e) \nu_S(e) = \sum_{e \mid n} \varphi(n/e) \nu_S(e)
\]
since $(n/e) \mid n$ for all $e \mid n$. This proves assertion 2. To see the validity of assertion 4 we simply write the divisors $e$ as $p^l$ for $l = 0, \ldots, k$ and use the facts $\varphi(1) = 1$ and $\varphi(p^l) = (p - 1)p^{l-1}$ for $l \geq 1$.

The definition of primitive subsets describes a property of the set $S$ and some set that is formally-dual to $S$. In the following corollary of Theorem 3.1 we see that in $\mathbb{Z}/p^k\mathbb{Z}$ all sets that are formally-dual to a primitive set $S$ form a primitive pair of formal-dual sets with $S$. It is not yet confirmed that this is true in general since in general there is no unique set (even up to translations and automorphisms) that is formally-dual to $S$, as can be seen in [2, Theorem 3.2, Remark 3.3].

**Corollary 3.5.** Let $S \subset \mathbb{Z}/p^k\mathbb{Z}$ be a primitive formal-dual set and $T \subset \mathbb{Z}/p^k\mathbb{Z}$ formally-dual to $S$. Then $T$ is also primitive. Thus $S$ and $T$ form a primitive pair.
Proof. We recall that by Definition 2.6, $S$ is primitive if it is not contained in a proper coset of $\mathbb{Z}/n\mathbb{Z}$ and there is some set $T'$ formally-dual to $S$ that also is not contained in a proper coset of $\mathbb{Z}/n\mathbb{Z}$.

It suffices to show that $T$ is also not contained in a proper coset.

First we claim that any formal-dual set $Q \subset \mathbb{Z}/p^k\mathbb{Z}$ is contained in a proper coset if and only if $\nu_Q(1) = 0$. Note that $Q$ is contained in a proper coset if and only if all differences of elements of $Q$ are divisible by $p$. Equivalently, no difference of two elements of $Q$ equals $v \in \mathbb{Z}/p^k\mathbb{Z}$ with $\gcd(v, p^k) = 1$. Therefore $\nu_Q(v) = 0$ for all $v \in \mathbb{Z}/p^k\mathbb{Z}$ with $\gcd(v, p^k) = 1$. According to Theorem 3.1, this is equivalent to $\nu_Q(1) = 0$.

So $T$ is not contained in a proper coset if and only if $\nu_T(1) \neq 0$. By Definition 2.4, we have

$$\frac{|S|^2}{|T|} \nu_T(1) = \sum_{v \in \mathbb{Z}/p^k\mathbb{Z}} \nu_S(v) c_p^v = \frac{|S|^2}{|T'|} \nu_{T'}(1),$$

and according to Lemma 2.5, we have $n = |S| \cdot |T| = |S| \cdot |T'|$ and therefore $\nu_T(1) = \nu_{T'}(1)$. Since $T'$ is not contained in a proper coset, we have $\nu_T(1) = \nu_{T'}(1) \neq 0$. Altogether, $T$ is not contained in a proper coset.

At the end of this section we will give some more restrictions of the weight enumerator. It turns out that there are even more structural results for primitive formal-dual subsets of $\mathbb{Z}/p^k\mathbb{Z}$.

Lemma 3.6. For an arbitrary subset $S$ of $\mathbb{Z}/n\mathbb{Z}$ the weight enumerator satisfies

$$\nu_S(v) \leq |S|$$

for all $v \in \mathbb{Z}/n\mathbb{Z}$. If $S$ is a primitive formal-dual subset of $\mathbb{Z}/p^k\mathbb{Z}$, then $\nu_S(p^{k-1}) < |S|$ and $\nu_S(1) > 0$. If additionally $|S| = p^l$ for some $l$ with $2l \leq k$ then $\nu_S(1) = 1$.

Proof. Let $v \in \mathbb{Z}/p^k\mathbb{Z}$. For every element $x \in S$ there is one unique element $y$ such that $x - y = v$. Therefore $\nu_S(v)$ is also the number of elements $x \in S$ such that $x - v \in S$ which is at most $|S|$.

Now we suppose $S$ is primitive as in Definition 2.6. As has been seen in the proof of Corollary 3.5, $\nu_S(1) > 0$. Now assume $\nu_S(p^{k-1}) = |S|$. Using Corollary 3.4, we have

$$\frac{|S|^2}{|T|} \nu_T(1) = \nu_S(0) - \nu_S(p^{k-1}) = |S| - |S| = 0$$

where $T \subset \mathbb{Z}/p^k\mathbb{Z}$ is some set formally-dual to $S$. But then, as discussed in the proof of Corollary 3.5, $T$ would be contained in a proper coset of $\mathbb{Z}/p^k\mathbb{Z}$. But since $S$ is primitive $T$ has to be primitive too according to Corollary 3.5. This is a contradiction.

Finally suppose $S$ is primitive and $|S| = p^l$ with $2l \leq k$. We already discussed $\nu_S(1) > 0$. Suppose $\nu_S(1) \geq 2 \geq \frac{p^l}{p-1} \geq \frac{p^{2l-k+1}}{p-1}$. Using Corollary 3.4 and $\nu_S(0) = |S| > 0$, we obtain the formula

$$p^{2l} = |S|^2 \geq \nu_S(0) + (p-1)p^{k-1}\nu_S(1) > (p-1)p^{k-1}\frac{p^{2l-k+1}}{p-1} = p^{2l},$$

which is a contradiction. Therefore, $\nu_S(1) = 1$. \qed
In the next section we will see that in general there is no function satisfying all of the restrictions given here.

4 Formal dual sets of $\mathbb{Z}/p^k\mathbb{Z}$

In this section we will use the restrictions developed in Section 3 to show Theorem 1.1. First, we show for $\mathbb{Z}/p^k\mathbb{Z}$ that there is in general no function satisfying all of these restrictions. This instantly yields that, in most cases, there is no primitive formal-dual subset of $\mathbb{Z}/p^k\mathbb{Z}$. The exceptional case is if we are looking for a formal-dual subset of $\mathbb{Z}/p^2\mathbb{Z}$ with size $p^l$. For example the functions $\nu : \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{N}_0$ defined by $\nu(0) = p$, $\nu(1) = 1$ and $\nu(p) = 0$ satisfy all restrictions of Section 3. But for odd $p$ there is no subset $S$ of $\mathbb{Z}/p^2\mathbb{Z}$ with $\nu_S = \nu$. In the subsequent discussion we will see that even in the exceptional case there is no primitive formal-dual set for odd $p$.

During this section, we assume without loss of generality that $|S| = p^l$ and $|T| = p^{k-l}$ by using Lemma 2.5.

The following result is a very strong restriction of possible candidates of primitive formal-dual sets of $\mathbb{Z}/p^k\mathbb{Z}$, even for $p = 2$.

**Theorem 4.1.** Let $S \subset \mathbb{Z}/p^k\mathbb{Z}$ be a primitive formal-dual set. Then $k$ has to be even and $|S| = p^{k/2}$.

**Proof.** As discussed above, we might assume $|S| = p^l$ and there is a set $T$ formally-dual to $S$ with $|T| = p^{k-l}$.

First assume $2l \geq k$ (and therefore $2(k-l) \leq k$). Since $S$ and $T$ are formally-dual to each other we can apply Corollary 3.5 to get

$$p^{3l-k} \nu_T(1) = \frac{|S|^2}{|T|} \nu_T(1) = \nu_S(0) - \nu_S(p^{k-1}) = p^l - \nu_S(p^{k-1}).$$

(1)

The set $T$ is a primitive formal-dual set since $S$ is primitive as has been seen in Corollary 3.5. According to Lemma 3.6 we therefore know $\nu_T(1) = 1$ (note that $|T| = p^{k-l}$ with $2(k-l) \leq k$). Reordering the terms of (1) we therefore get

$$\nu_S(p^{k-1}) = p^l(1 - p^{2l-k}).$$

(2)

Note that, since $2l \geq k$, the right hand side is a negative number unless $k = 2l$ while the left hand side is a non-negative number. Therefore $k$ is even and $|S| = p^l = p^{k/2}$.

Now assume $|S| = p^l$ with $2l \leq k$. Then one can interchange the roles of $S$ and $T$ in the arguments above to get to the same result.

According to Theorem 4.1, we only have to study subsets of $\mathbb{Z}/p^2\mathbb{Z}$ of size $p^l$. In the following we will see, that for odd $p$ none of those subsets is a primitive formal-dual set. Note that all known examples of primitive formal-dual sets of finite cyclic groups as seen in Example 2.7 are of the exceptional type.

To proof Theorem 4.3 we will need one technical lemma and a very helpful technique which was used first by Gregory Minton in [2, Lemma 4.4].
Lemma 4.2. Let $S \subset \mathbb{Z}/n\mathbb{Z}$ and $m$ be a divisor of $n$. If there are exactly $|S|^2/m$ ordered pairs of points of $S$ with a difference divisible by $m$, then each coset of $m\mathbb{Z}/n\mathbb{Z}$ contains the same number of elements of $S$, namely $|S|/m$. (Note that divisibility by $m|n$ in $\mathbb{Z}/n\mathbb{Z}$ can be inherited from divisibility by $m$ in $\mathbb{Z}$ since this notion is independent from the exact choice of representatives, i.e. if $m|v$ then $m|w$ for all $v \in v + n\mathbb{Z}$)

Proof. Two points have a difference divisible by $m$ if and only if they are contained in the same coset of $m\mathbb{Z}/n\mathbb{Z}$. Therefore the number of pairs of points in $S$ with a distance divisible by $m$ can also be computed as

$$
\sum_{0 \leq a \leq m-1} |S \cap (a + m\mathbb{Z}/n\mathbb{Z})|^2 = (\ast).
$$

It is not difficult to check the following by simple analysis: The only configuration of $m$ variables $\mu_1, \ldots, \mu_m \geq 0$ with $\sum_{i=1}^m \mu_i = c$ that minimizes $\sum_{i=1}^m \mu_i^2$ is $\mu_1 = \cdots = \mu_m = c/m$. Especially, since $\sum_{0 \leq a \leq m-1} |S \cap (a + m\mathbb{Z}/n\mathbb{Z})| = |S|$ this yields

$$(\ast) \geq \sum_{0 \leq a \leq m-1} \left( \frac{|S|}{m} \right)^2 = \frac{|S|^2}{m}.
$$

By applying the preconditions this inequality holds with equality and therefore $|S \cap (a + m\mathbb{Z}/n\mathbb{Z})| = |S|/m$ for all $0 \leq a \leq m-1$ which proves the lemma.

Now we are able to proof the non-existence of formal-dual sets in the exceptional case.

Theorem 4.3. Let $p$ be an odd prime and $l \geq 1$. There is no primitive formal-dual subset of $\mathbb{Z}/p^{2l}\mathbb{Z}$ of size $p^l$.

Proof. Suppose there is such a primitive formal-dual set $S \subset \mathbb{Z}/p^{2l}\mathbb{Z}$ of size $p^l$. Since $S$ is a primitive formal-dual set we can apply Lemma 4.2 to get $\nu_S(1) = 1$. Using Theorem [3.1] we know that the number of ordered pairs with a difference not divisible by $p$ can be computed as

$$
\sum_{v \in \mathbb{Z}/p^{2l}\mathbb{Z} \atop \gcd(v,p^{2l}) = 1} \nu_S(v) = (p - 1)p^{2l-1} = (p - 1)p^{2l-1}.
$$

Therefore there are exactly $p^{2l} - (p - 1)p^{2l-1} = p^{2l-1} = \frac{|S|^2}{p}$ ordered pairs of points with a distance divisible by $p$. By Lemma 4.2 we know that each coset of $p\mathbb{Z}/p^{2l}\mathbb{Z}$ contains exactly $|S|/p = p^{l-1}$ elements of $S$. Therefore, there are unique values $0 \leq a_{i,j} < p^{2l-1}$ such that the elements of $S$ can be denoted as

$$
x_{i,j} \equiv i + a_{i,j} \cdot p \mod p^{2l} \text{ for } 0 \leq i \leq p - 1, 1 \leq j \leq p^{l-1}.
$$

Furthermore, we can write down the differences of pairs of elements of $S$ lying in $1 + p\mathbb{Z}/p^{2l}\mathbb{Z}$ as

1. $x_{i,j} - x_{i-1,k} \equiv 1 + (a_{i,j} - a_{i-1,k})p = 1 + A_{i,j,k} \cdot p \mod p^{2l}$ for $1 \leq i \leq p - 1, 1 \leq j, k \leq p^{l-1}$

2. $x_{0,j} - x_{p-1,k} \equiv 1 + (a_{0,j} - a_{p-1,k})p = 1 + A_{0,j,k} \cdot p \mod p^{2l}$ for $1 \leq j, k \leq p^{l-1}$
where
\[ A_{i,j,k} = a_{i,j} - a_{(i-1 \mod p),k} - \delta_{i=0} = \begin{cases} a_{i,j} - a_{i-1,k} & \text{if } i \neq 0 \\ a_{0,j} - a_{p-1,k} - 1 & \text{if } i = 0. \end{cases} \]

Note that any difference \( v \in 1 + p\mathbb{Z}/p^2\mathbb{Z} \) satisfies \( \gcd(v, p^2) = 1 \) and by Theorem 3.1 we have \( \nu_S(v) = \nu_S(1) = 1 \). So for every \( v \in 1 + p\mathbb{Z}/p^2\mathbb{Z} \) we have exactly one ordered pair of elements of \( S \) with difference \( v \). This yields that the differences listed in [1] and [2] are exactly the elements of \( 1 + p\mathbb{Z}/p^2\mathbb{Z} \). In particular, the coefficients \( A_{i,j,k} \) need to be distinct modulo \( p^{2l-1} \). Since there are exactly \( p \cdot p^{l-1} \cdot p^{l-1} = p^{2l-1} \) coefficients \( A_{i,j,k} \), we know that these numbers restricted to \( \mathbb{Z}/p^{2l-1}\mathbb{Z} \) are exactly all elements of \( \mathbb{Z}/p^{2l-1}\mathbb{Z} \). Therefore
\[
\sum_{0 \leq i \leq p-1 \atop 1 \leq j, k \leq p^{l-1}} A_{i,j,k} \equiv 0 + 1 + 2 + \cdots + (p^{2l-1} - 1) = \frac{1}{2} p^{2l-1} (p^{2l-1} - 1) \mod p^{2l-1}.
\]

(3)

On the other hand, observing the definition of \( A_{i,j,k} \), we have
\[
\sum_{0 \leq i \leq p-1 \atop 1 \leq j, k \leq p^{l-1}} A_{i,j,k} = \sum_{0 \leq i \leq p-1 \atop 1 \leq j, k \leq p^{l-1}} (a_{i,j} - a_{(i-1 \mod p),k} - \delta_{i=0})
= \left( \sum_{0 \leq i \leq p-1 \atop 1 \leq j, k \leq p^{l-1}} a_{i,j} \right) - \left( \sum_{0 \leq i \leq p-1 \atop 1 \leq j, k \leq p^{l-1}} a_{(i-1 \mod p),k} \right) - p^{2l-2} = -p^{2l-2}.
\]

(4)

Comparing (3) and (4) we obtain
\[-p^{2l-2} \equiv \frac{1}{2} p^{2l-1} (p^{2l-1} - 1) \mod p^{2l-1}.
\]

For odd \( p \) the term \( (p^{2l-1} - 1) \) is even and therefore
\[
\frac{1}{2} p^{2l-1} (p^{2l-1} - 1) \equiv 0 \neq -p^{2l-2} \mod p^{2l-1}.
\]

This is a contradiction, therefore there is no such set \( S \). Note that for \( p = 2 \) this formula always holds.

Now it is no difficulty to proof the main theorem of this article. So if we search for more primitive formal-dual sets of cyclic groups of prime power order, we can restrict to subsets of \( \mathbb{Z}/2^l\mathbb{Z} \) of size \( 2^l \).

Proof of Theorem 1.1 Suppose \( S \) is a primitive formal-dual set of \( \mathbb{Z}/p^k\mathbb{Z} \), where \( p \) is an odd prime and \( k \geq 1 \). According to Theorem 4.1 \( k \) is even and \( |S| = p^{k/2} \). If we write \( k = 2l \) for \( l \geq 1 \), we have that \( S \) is a primitive subset of \( \mathbb{Z}/p^l\mathbb{Z} \) of size \( p^l \) which is impossible due to Theorem 4.3. This is a contradiction, therefore there is no such set \( S \).

Due to this article we know that primitive formal-dual sets of cyclic groups of prime power order are in some sense very rare. We like to end this paper with a discussion that there also is no primitive formal dual set of \( \mathbb{Z}/16\mathbb{Z} \). To study the still unknown cases \( \mathbb{Z}/64\mathbb{Z}, \mathbb{Z}/256\mathbb{Z} \) and so on, further arguments are needed.
Example 4.4. Suppose $S$ is a primitive formal-dual subset of $\mathbb{Z}/16\mathbb{Z}$. Then $|S| = 4$ as has been seen in Theorem 4.1. Following the arguments of the proof of Theorem 4.3 we have $\nu_S(0) = 4$, $\nu_S(1) = 1$ and $\nu_S(8) = 0$. Moreover according to Corollary 3.4.4 we know

$$16 = |S|^2 = \nu_S(0) + 8\nu_S(1) + 4\nu_S(2) + 2\nu_S(4) + \nu_S(8)$$

which simplifies to the equality

$$4 = 4\nu_S(2) + 2\nu_S(4).$$

Therefore, there are only two possible choices for $\nu_S$ namely

| $d$ | $\nu_1(d)$ | $\nu_2(d)$ |
|-----|------------|------------|
| 1   | 1          | 1          |
| 2   | 1          | 0          |
| 4   | 0          | 2          |
| 8   | 0          | 0          |
| 16  | 0          | 4          |

In either case it is impossible to construct a set with such weight enumerator. This will be briefly argued. Without loss of generality we can assume $\{0, 1\} \subset S$ since there is some pair of points with a difference of 1 and formal-duality is invariant to translation. It follows a diagram for $\nu_S = \nu_1$ of $\mathbb{Z}/16\mathbb{Z}$ where $\bullet$ stands for an element that is assured to be in $S$, $\times$ stands for an element that is surely not in $S$ and $\circ$ is used for unsure elements:

$$\bullet \times \times \times \times \times \times \times \times \times \times \circ \circ \circ \circ \circ \circ .$$

One can explain each $\times$ by the weight enumerator. Elements that provide a difference of $\{1, 4, 8, 12, 15\}$ with some $\bullet$ element can not be in $S$ ($\nu_1(4) = \nu_1(8) = 0$, $\nu_1(1) = \nu_1(15) = 1$). There has to be a pair of elements with a difference of two since $\nu_1(2) = 1$. Therefore either 3 or 14 have to be contained in $S$. Due to the symmetry of the construction we assume without loss of generality 3 $\in S$ which yields the following diagram:

$$\bullet \times \times \times \times \times \times \times \times \times \times \times \times .$$

This is since no element with a difference of $\{1, 2, 3, 4, 8, 12, 13, 14, 15\}$ to some $\bullet$ element can be in $S$. Now we see the only choice left is $S = \{0, 1, 3, 10\}$. But now there are two ordered pairs of points with a difference of 7 namely $(10, 3)$ and $(1, 10)$ which is a contradiction to $\nu_1(7) = \nu_1(1) = 1$.

Now assume $\nu_S = \nu_2$. Then we start with the diagram

$$\bullet \times \times \times \times \times \times \times \times \times \times \times$$

since no element of $S$ can have a difference of $\{1, 2, 6, 8, 10, 14, 15\}$ to some $\bullet$ element. Moreover some pair of elements need to have a difference of 3 since $\nu_2(3) = 1$. Therefore we know 4 $\in S$ or 13 $\in S$ but due to the symmetry of the construction we might assume without loss of generality 4 $\in S$ which yields the following diagram:

$$\bullet \times \times \bullet \times \times \times \times \times \times \times \times \times \times \times$$

since the distances to some $\bullet$ element can not be $\{1, 2, 3, 6, 8, 10, 13, 14, 15\}$. We see that we do not have any possibility left to choose a fourth element, which is again a contradiction.
Acknowledgement

I like to thank Erik Friese for several inspirations, pointers to literature and verification’s of arguments. Moreover I am grateful to Frieder Ladisch for plenty helpful remarks and inspiring a shorter, more elegant proof. Furthermore I like to express my sincere gratitude to Achill Schürmann for suggesting this interesting question as well as many patient reviews of preliminary versions of this paper and for pointing out several mistakes.

References

[1] P. Bundschuh. *Einführung in die Zahlentheorie*. Springer-Lehrbuch. [Springer Textbook]. Springer-Verlag, Berlin, second edition, 1992.

[2] H. Cohn, A. Kumar, C. Reiher, and A. Schürmann. Formal duality and generalizations of the Poisson summation formula. In *Discrete geometry and algebraic combinatorics*, volume 625 of *Contemp. Math.*, pages 123–140. Amer. Math. Soc., Providence, RI, 2014.

[3] H. Cohn, A. Kumar, and A. Schürmann. Ground states and formal duality relations in the gaussian core model. *Physical Review E*, 80(6):061116, 2009.

[4] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.