Classification of Formal Duality with an Example in Sphere Packing

UROP+ Final Paper
Jianqiao Xia
Mentor: Soohyun Park
Project suggested by Henry Cohn

August 29, 2016

Abstract

We study the notion of formal duality, which was introduced and developed by Cohn, Kumar, Reiher, and Schürmann through their study of ground state configurations of particles in Euclidean space. Here, we prove some results in the classification of formally dual pairs in cyclic groups and products of cyclic groups. For example, we prove the non-existence of primitive formally dual pairs in a cyclic group of the form $\mathbb{Z}/2^k\mathbb{Z}$ for $k \geq 2$. Together with Schüler's result on cyclic groups with odd prime order, this completes the classification of formally dual pairs in a cyclic group of prime power order. Finally, we use orthogonality relations to consider the existence of formally dual pairs in Conway's conjectural 5 dimensional packings.

1 Introduction

The notion of formal duality is inspired by Cohn, Kumar and Schürmann's numerical result on ground state configurations of particles in Euclidean space (see [2]). They considered the Gaussian function $G_c := \exp(-\pi c r^2)$ as a potential function and analyzed the ground state configurations under fixed point density. The interesting fact they found is that the ground state configurations for G_c and $G_{1/c}$ seem to be "formally" dual, a generalized notion of the duality of a lattice. The key idea about formal dual configurations $\mathcal{P}$, $\mathcal{Q}$ is that for any function f, the potential energy of $\mathcal{P}$ with potential function f is the same as the energy of $\mathcal{Q}$ with potential function $\hat{f}$, the Fourier transform of f. The Poisson summation formula indicates any lattice and its dual lattice are formally dual. In fact, many non-lattice configurations also have formal duals, though very rare. It is thus interesting to find such configurations.

Later, Cohn, Kumar, Reiher and Schürmann [1] provided a solid algebraic foundations for the theory of formal duality. They reformulated the definition of formal duality for periodic

packings in the setting of finite abelian groups. In addition, they proved the non-existence of formal dual pairs in group $\mathbb{Z}/p^2\mathbb{Z}$, and gave two examples in $(\mathbb{Z}/p\mathbb{Z})^2$, the Gauss sum construction, and $\mathbb{Z}/4\mathbb{Z}$, the TITO construction. However, they could not find any other essentially different formal dual pairs. Therefore they conjectured that all formal dual pairs can be constructed from the two examples, by inflating the group and taking products. Therefore they introduced the notion of primitive formal dual pairs, which are those that cannot be obtained from other pairs using the two methods mentioned. However, in this paper, we found a formal dual pair in $(\mathbb{Z}/p^k\mathbb{Z})^2$. Although it is an analogy to the Gauss sum construction, it is indeed primitive.

By generalizing the proof for $\mathbb{Z}/p^2\mathbb{Z}$, Schüler proved the non-existence of primitive formal dual pairs in $\mathbb{Z}/p^k\mathbb{Z}$ for all odd prime p. He gave a restriction on the cyclic group with order 2, that is only $\mathbb{Z}/2^{2l}\mathbb{Z}$ may have primitive formal dual pairs. In this paper, we solve this case and show that only $\mathbb{Z}/4\mathbb{Z}$ have primitive formal duals.

We first provide relevant tools and background on formal duality such as basic definitions and weight enumerators [4] in Section 2. We also introduce some structural results on formally dual pairs through "parametrized" formal dual pairs to obtain "orthogonality" relations relating formally dual pairs in a subgroup in Section 3.

Then, we discuss some classification of special cases of formally dual pairs in certain special cyclic groups and products of cyclic groups in Section 4. We first use the same method as in the Gauss sum construction from [1] to prove the existence of a primitive formally dual pair in $(\mathbb{Z}/p^k\mathbb{Z})^2$. Next, we prove the non-existence of primitive formally dual pairs in $\mathbb{Z}/2^{2k}\mathbb{Z}$ for $k \geq 2$ by analyzing the identities involving weight enumerators and restrictions in [4] and using the orthogonality relations found earlier. The final main result in this section is the proof of the nonexistence of primitive formal dual pairs in an arbitrary abelian group of squarefree order using basic results on formal duality.

The remaining sections have to do with alternative representations of formally dual pairs and what they may represent in geometric setting (e.g. in sphere packings). Next, we consider relations between formally dual pairs via representations of formally dual sets as graphs in Sections 5 and 6. Finally, we analyze the existence of formally dual pairs in Conways conjectural tight packings in dimension 5 using earlier results on structures of parametrizable formal dual pairs in Section 7.

2 Definitions and Useful Lemmas

In this section, we provide a clear definition of formal duality, and some useful results in [1] and [4]. First, we introduce the weight enumerator, which is used to simplify all the statements in this paper.

Definition 2.1. *For a subset T of an (additive) abelian group G, we define the weight*

enumerator: the function $\nu_T : G \to \mathbb{N}$*, for each* y*,*

$$\nu_T(y) = \#\{(x_1, x_2) | x_1 - x_2 = y, x_1, x_2 \in G\}. \tag{1}$$

The weight enumerator describes the difference set $T - T$ with multiplicity. Using this notation, recall that the dual group of G is the group of homomorphisms $G \to \mathbb{C}^*$, we could define formal duality in abelian group G as

Definition 2.2. *Let* S *be a subset of* G *and* T *be a subset of its dual group* $\hat{G}$*. Then we say* S, T *are* formally dual *to each other if for each* $y \in \hat{G}$

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

In [1], the authors proved the symmetry of this definition, so one can interchange S, T in this definition. Also notice that for an abelian group G, $\hat{G}$ is sometimes identified as G. For example, let $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $x = (u, v)$,and $y = (w, z)$. Then the relation

$$\langle x, y\rangle = \zeta_n^{uw}\zeta_m^{vz}, \tag{3}$$

identifies G with $\hat{G}$, where ζ_n, and ζ_m are primitive n-th, and m-th roots of unity respectively. Furthermore, a restriction relating the cardinality of set S, T is given in [1]

Lemma 2.1. *Let* S *be a subset of* G *and* T *be a subset of* $\hat{G}$*. If* S*, and* T *are formally dual, then*

$$|S| \cdot |T| = |G| = |\hat{G}|. \tag{4}$$

By expanding the left side of Definition 2.2, and using $|z|^2 = z\bar{z}$, Schüler (see [4]) proves the following lemma:

Lemma 2.2. *Let* S *be a subset of* G*, and* T *a subset of* $\hat{G}$*, then* S, T *are formally dual to each other if and only if for each* $y \in \hat{G}$*,*

$$\frac{|S|^2}{|T|}\nu_T(y) = \sum_{v\in G}\nu_S(v)\langle v, y\rangle. \tag{5}$$

Now let us consider the case where $G = \mathbb{Z}/n\mathbb{Z}$. Then we could identify G with $\hat{G}$, by setting $\langle x, y\rangle = \zeta_n^{xy}$. Based on the above equation, together with results in field automorphism, it is proved in [4] that

Lemma 2.3. *In* $\mathbb{Z}/n\mathbb{Z}$*, if* T *is formally dual to some subset of* $\mathbb{Z}/n\mathbb{Z}$*, then for any* $y \in \mathbb{Z}/n\mathbb{Z}$*, let* $d = gcd(y, n)$*,*

$$\nu_T(y) = \nu_T(d). \tag{6}$$

This lemma allow us to focus on $\nu_T(d)$ where d is a divisor of n.

In addition to above conditions on formal dual pairs, there are two main methods described in [1] to construct formal dual pairs from given ones:

1. Let S_1, S_2, T_1 and T_2 be subsets of $G_1, G_2, \hat{G}_1$ and $\hat{G}_2$, respectively. Suppose (S_i, T_i) are formally dual pairs, for $i = 1, 2$, then $S_1 \times S_2$ and $T_1 \times T_2$ are formally dual as subsets of $G_1 \times G_2$, $\hat{G}_1 \times \hat{G}_2$.

2. Let H be a subgroup of G. Then there is a natural restriction map $\phi : \hat{G} \to \hat{H}$ whose kernel the annihilator of H. If $S \subset H$ and $T \subset \hat{H}$ are formally dual, then $S \subset G$ and $\phi^{-1}(T) \subset \hat{G}$ are formally dual.

The two methods above motivate the notion of primitive formal duals, which are defined as

Definition 2.3. *Let S be a subset of G and T be a subset of $\hat{G}$, then we say S, T are* primitive formal dual sets *if they are formally dual and S is not contained in a coset of a proper subgroup of G, T is not contained in a coset of a proper subgroup of $\hat{G}$.*

3 Structures of Parametrizable Formal Dual Pairs

From Definition 2.3, we can see that the notion of formal duality is only determined by the weight enumerator function. Two sets with the same weight enumerator can not be distinguished. In this section, we study the relations of weight enumerators of formally dual pair S, T. We find a nice symmetric result for group $(\mathbb{Z}/p\mathbb{Z})^n$, where p is a prime.

The group $G = (\mathbb{Z}/p\mathbb{Z})^n$ can also be equipped with the structure of an $\mathbb{F}_p^n$ space. We find an identity for the sum of the weight enumerator function over a subspace of $\mathbb{F}_p^n$.

3.1 Orthogonal equation

For a formal dual pair (S, T) in $(\mathbb{Z}/p\mathbb{Z})^n$, where p is a prime, there are some linear equations in Lemma 2.2 relating the weight enumerators ν_S and ν_T to each other. However, these relations usually involve complex numbers and are hard to compute. We use an averaging method to give a relation with only integer coefficients. Here is our main result:

Theorem 3.1. *If S, T are formally dual in $G = (\mathbb{Z}/p\mathbb{Z})^n$, then for any $y \in G$, we have*

$$\frac{|S|^2}{p}(1 + \frac{(p-1)\nu_T(y)}{|T|}) = \sum_{a \in G, a \cdot y = 0} \nu_S(a). \tag{7}$$

Proof. Let $\zeta = e^{2\pi i/p}$. Given a formally dual pair S, T, we have by Lemma 2.2 that

$$\sum_{a \in G} \nu_S(a)\zeta^{a \cdot y} = \frac{|S|^2}{|T|}\nu_T(y), \tag{8}$$

for all $y \in G$. Since $\zeta^p = 1$, we can write the left side as $a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$. The coefficients are

$$a_k = \sum_{a \in G, a \cdot y = k} \nu_S(a). \tag{9}$$

Recall that we have $\nu_T(ky) = \nu_T(y)$ for all $y \in G$, and $k \neq 0$. If $k \neq 0$, we have

$$\sum_{a\cdot y=k} \nu_S(a) = \sum_{a\cdot y=1} \nu_S(ka) = \sum_{a\cdot y=1} \nu_S(a). \tag{10}$$

This means that $a_1 = a_2 = \cdots = a_{p-1}$. So (8) implies that

$$a_0 + a_1 + \cdots + a_{p-1} = |S|^2 \tag{11}$$

$$a_0 - a_1 = \frac{|S|^2}{|T|}\nu_T(y). \tag{12}$$

Thus, we have

$$a_0 = \frac{|S|^2}{p}(1 + \frac{(p-1)\nu_T(y)}{|T|}). \tag{13}$$

This is exactly what we want to prove. ■

One important corollary is the following:

Corollary 3.2. *Let S, T be given as above. Suppose U is a u dimensional subspace in $(\mathbb{F}_p)^n$, and $V = U^\perp$. Then, we have that*

$$p^u \sum_{x\in V} \nu_S(x) = \frac{|S|^2}{|T|} \sum_{y\in U} \nu_T(y). \tag{14}$$

Notice that the equation is clearly true for $U = \{0\}$, and the $u = 1$ case is Theorem 4.1. For general U, this follows from summing some equations like (7).

Proof. We consider (7) as a equation for y. Adding such equations over U, the left hand side is

$$\frac{|S|^2}{p} \cdot p^u + \frac{(p-1)|S|^2}{p|T|} \sum_{y\in U} \nu_T(y). \tag{15}$$

The right hand side is

$$\sum_{y\in U} \sum_{a\cdot y=0} \nu_S(a) = \sum_{a\in G} \nu_S(a) \sum_{y\in U, y\cdot a=0} 1 \tag{16}$$

If $a \in V$, all the $y \in U$ are orthogonal to a. So $\sum_{y\in U, y\cdot a=0} 1 = |U| = p^u$. If $a \notin V$, we can write $a = \alpha + \beta$ with $\alpha \in U, \beta \in V$. Then the $y \in U$ that are orthogonal to a, are the y orthogonal to $\alpha \neq 0$. These y forms a $u-1$ dimensional subspace in U. There are p^{u-1} such y. From these observations, we have

$$\begin{aligned} \frac{|S|^2}{p} \cdot p^u + \frac{(p-1)|S|^2}{p|T|} \sum_{y\in U} \nu_T(y) &= p^u \sum_{x\in V} \nu_S(x) + p^{u-1} \sum_{x\notin V} \nu_S(x) \\ &= (p^u - p^{u-1}) \sum_{x\in V} \nu_S(x) + p^{u-1} \sum_{x\in G} \nu_S(x) \\ &= \frac{p-1}{p} \cdot p^u \sum_{x\in V} \nu_S(x) + p^{u-1}|S|^2. \end{aligned} \tag{17}$$

Comparing both sides of the equation, we get the intended result. ■

Using this corollary, we can analyze some specific kind of subsets, Specifically, we can analyze those which can be parametrized by a subgroup. More formally, in $G = (\mathbb{Z}/p\mathbb{Z})^n = U \times V$, where U, V are subgroups of G, we call S *parametrized* by U if $S = \{(u, a_u), u \in U\}$. For such an S, notice that U is a subspace of G, and U, V are orthogonal complements to each other. Note that ν_S vanishes on $\{0\} \times V$ except at 0. Thus, it follows from the above corollary that $\sum_{y \in U \times \{0\}} \nu_T(y) = |T| = \nu_T(0)$. So, ν_T vanishes on $U \times \{0\}$ except at 0. Combining this with the cardinality of T, T must be parametrized by V. In the following section, we give a more general result.

3.2 Orthogonal relation

Given a general abelian group G, we can always decompose it as a product of cyclic groups, say $G = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \mathbb{Z}/n_k\mathbb{Z}$. In this section, we will prove an "orthogonal" structure for a specific kind of formally dual pair. The main result is that if one of S, T can be parametrized, then the other must also be parametrized on an "orthogonal" subspace. In [3], Conway hypothesized that tight packings fibers over lower dimensional tight packings. Thus almost all tight packings in Conway's list are parametrizable. So results in this section can reduce the difficulty of finding formal dual sets for tight packings.

Theorem 3.3. *Let (S, T) be a formally dual pair in G, $U = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \mathbb{Z}/n_s\mathbb{Z}$, and $V = \mathbb{Z}/n_{s+1}\mathbb{Z} \times \cdots \mathbb{Z}/n_k\mathbb{Z}$ be abelian groups. If $S = \{(u, a_u)\}_{u \in U}$, then $T = \{b_v, v\}_{v \in V}$.*

In the following lemma, we suppose $n_i (1 \leq i \leq s)$ are s positive numbers. And consider group $P = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \mathbb{Z}/n_s\mathbb{Z}$. We consider primitive roots $\zeta_i = e^{2\pi i/n_i}$ for each $1 \leq i \leq s$. We use x^α to represent monomial $x_1^{\beta_1} x_2^{\beta_2} \cdots x_s^{\beta_s}$ for $\beta \in P$. Similarly, we use ζ^β to represent $\zeta_1^{\beta_1} \zeta_2^{\beta_2} \cdots \zeta_s^{\beta_s}$.

Lemma 3.1. *Let $f = \sum_{i=1}^n x^{\alpha_i}$, where $n = \Pi_{i=1}^s n_i$, and $\alpha_i \in P$. If f vanishes on all $x = \zeta^\alpha, \alpha \in P$, and $\alpha \neq 0$, then $f = \Pi_{k=1}^s (1 + x_i + \cdots + x_i^{n_i - 1})$.*

Proof. We prove this by induction on s, which is the number of variables. For $s = 1$, by assumption, f is a sum of n_1 monomials, and f has root ζ^k for $1 \leq k \leq n_1$. So this means f is divisible by $\Pi_{k=1}^{n_1}(x - \zeta^k) = 1 + x + x^2 + \cdots + x^{n_1 - 1}$. Since f is a sum of n_1 monomials with degree smaller than n_1, f must equal to this polynomial.

Now suppose we have proven the case of $s - 1$ variable polynomials. Then we have,

$$f(x) = \sum_{k=0}^{n_1 - 1} x_1^k f_k, \tag{18}$$

for all f satisfying the conditions given in the lemma. Here each f_k is a polynomial with variable $x_2, x_3, \cdots, x_s$. For each $\alpha = (\alpha_2, \alpha_3, \cdots, \alpha_s) \in \mathbb{Z}/n_2\mathbb{Z} \times \cdots \mathbb{Z}/n_s\mathbb{Z}$, $\alpha \neq 0$, we know that f vanishes on $\zeta^{(a,\alpha)}$. Fixing $(x_2, \cdots, x_s) = \zeta^\alpha$, and considering (18) as a polynomial of x_1, it has n_1 roots, namely $x_1 = \zeta_1^k, 0 \leq k \leq n_1 - 1$. Since the degree of f as a polynomial of x_1 is at most $n_1 - 1$, we must have $f = 0$.

This means that f_k vanishes on ζ^α for each k. Using the result for $s-1$ variable polynomial, we have that each $f_k = \Pi_{l=2}^{s}(1 + x_l + \cdots + x_l^{n_l-1})$. Combining this with (18), we get our intended result. ■

Using this lemma, we are able to prove Theorem 3.3.

Proof. The assumption for S given in the theorem implies that $\nu_S(0, 0, \cdots, 0, y) = 0$ for all nonzero $y \in V$. Also the assumption in Theorem 3.3 implies that $|S| = n_1 n_2 \cdots n_s$, with $|T| = n_{s+1} \cdots n_k$. By Definition 2.2, we have

$$\big|\sum_{a\in T} \zeta^{ay}\big|^2 = \frac{|T|^2}{|S|}\nu_S(y). \tag{19}$$

Let g be the k variable polynomial of the form

$$g(x) = \sum_{\alpha\in T} x^\alpha. \tag{20}$$

Let f be the $k-s$ variable polynomial

$$f(x_{s+1}, \cdots, x_k) = g(1, 1, \cdots, 1, x_{s+1}, \cdots, x_k). \tag{21}$$

For each nonzero $y \in V$, $f(\zeta^y) = 0$ if $\nu_S(0, 0, \cdots, 0, y) = 0$. By Lemma 4.1, we have that $f = \Pi_{i=s+1}^{k}(1 + x_i + \cdots x_i^{n_i-1})$. Since $|T| = n_{s+1}n_{s+2} \cdots n_k$, from the definition of f, we must have $T = \{b_v, v\}_{v\in V}$. ■

4 Classification of Formal Duals

In this section, we will first give an example of primitive formal dual pair in $(\mathbb{Z}/p^k\mathbb{Z})^2$. Then we prove the non-existence of primitive formal dual pairs in $\mathbb{Z}/2^k\mathbb{Z}$. Next, we give restrictions on formal duals in the group $(\mathbb{Z}/p\mathbb{Z})^2$. Finally, we use divisibility to show that abelian group with square free order has no primitive formal dual pairs.

4.1 A Primitive Formal Dual Pair in $(\mathbb{Z}/p^k\mathbb{Z})^2$

We use the same method as the Gauss sum construction in [1] to give a formal dual pair in $G = (\mathbb{Z}/p^k\mathbb{Z})^2$, where p is an odd prime. First, we prove a lemma:

Lemma 4.1. *Let p be an odd prime, $\zeta = e^{\frac{2\pi i}{p^k}}$ be a p^k-th root of unity. For $a, b \in G$, let α, β be natural numbers such that $p^\alpha || a$, $p^\beta || b$. Then*

$$\big|\sum_{n\in G} \zeta^{an^2+bn}\big|^2 = \begin{cases} 0 & \beta < \alpha \\ p^{k+\alpha} & \beta \geq \alpha \end{cases} \tag{22}$$

Proof. We expand the left side using $|z|^2 = z\hat{z}$, and change the order of summation. In the equations below, we use $t = n - m$.

$$\begin{aligned}
\big|\sum_{n\in G}\zeta^{an^2+bn}\big|^2 &= (\sum_{n\in G}\zeta^{an^2+bn})(\sum_{n\in G}\zeta^{-an^2-bn}) \\
&= \sum_{n,m}\zeta^{a(n^2-m^2)+b(n-m)} \\
&= \sum_{t\in G}\sum_{m\in G}\zeta^{a(t^2+2mt)+bt} \\
&= \sum_{t\in G}\zeta^{at^2+bt}\sum_{m\in G}\zeta^{2atm} \\
&= p^k\sum_{p^{k-\alpha}|t}\zeta^{at^2+bt} \\
&= p^k\sum_{0\le t'<p^\alpha}\zeta^{bp^{k-\alpha}t'}
\end{aligned} \tag{23}$$

Here we used $t = p^{k-\alpha}t'$ in the last step and notice that at^2 is divisible by p^k for t divisible by p^α. In the last expression, notice when $\beta < \alpha$, $bp^{k-\alpha}$ is not a multiple of p^k, therefore we get 0, otherwise we get $p^{k+\alpha}$. ■

The following pair

$$((a,b),(c,d)) = \zeta^{ac+bd} \tag{24}$$

makes the group $G \times G$ self-dual. So from definition 2.2, the definition of formal dual pair in $(\mathbb{Z}/p^k\mathbb{Z})^2$ becomes:

Definition 4.1. *Let S, T be subsets of $(\mathbb{Z}/p^k\mathbb{Z})^2$, then we say S, T are* formally dual *if and only if for any $(x, y) \in (\mathbb{Z}/p^k\mathbb{Z})^2$,*

$$\big|\sum_{(a,b)\in S}\zeta^{ax+by}\big|^2 = \frac{|S|^2}{|T|}\nu_T(x,y) \tag{25}$$

One example is in the case $k = 1$, (see [1]) where $S = \{(n, n^2)\}$ and $T = \{(n^2, n)\}$ are formally dual. We will prove that the construction as the one used in [1] is still valid for $k \ge 2$.

Theorem 4.1. *Let $S = \{(n, n^2)|n \in G\}$ and $T = \{(n^2, n)|n \in G\}$. Then (S, T) is a primitive formal dual pair in $(\mathbb{Z}/p^k\mathbb{Z})^2$.*

Proof. The theorem contains two parts: one is that S, T are formally dual, the other is that the pair is primitive. From the construction, we see that $|S| = |T| = p^k$, so we need for any $(a, b) \in G \times G$,

$$\big|\sum_{n\in G}\zeta^{an^2+bn}\big|^2 = p^k\nu_T(a,b). \tag{26}$$

$\nu_T(a,b)$ is the number of solutions for following equations,

$$\begin{aligned} n-m &\equiv a(\mathrm{mod}p^k) && (27)\\ n^2-m^2 &\equiv b(\mathrm{mod}p^k) && (28)\end{aligned}$$

We use the same notion of α, β in Lemma 3.1. Clearly if $\beta < \alpha$, then there is no solution. If $\beta > \alpha$, then the above second equation becomes

$$n+m \equiv b(\mathrm{mod}p^{k-\alpha}). \quad (29)$$

Combining equation (27), (29), it is easy to check that the number of solutions is p^α. This coincides with the definition of formal duality.

Now we show that the pair is primitive. First, neither of S, T is contained in a proper subgroup. Otherwise, by symmetry, we assume T is contained in a subgroup H. Since $(x,x^2),(y,y^2),(x+y,(x+y)^2) \in T$, we have $(0,2xy) \in H$, therefore by taking $x=1, y=\frac{p^k+1}{2}$, $(0,1) \in H$. Since $(1,1) \in T \subset H$, $(1,0) = (1,1)-(0,1) \in H$ and therefore $H = G \times G$.

Earlier in the paper, we found a Gaussian construction for $(\mathbb{Z}/p^k\mathbb{Z})^2$, and showed that it is primitive. This only means that the construction cannot be obtained through inflation of smaller pairs. Now we show that it also cannot be obtained by taking products. Recall that the "Product Construction" says: If S_1, T_1 are formally dual in group G_1, and S_2, T_2 are formally dual in G_2, then $S_1 \times S_2$ and $T_1 \times T_2$ are formally dual in $G_1 \times G_2$.

From now on let $G = (\mathbb{Z}/p^k\mathbb{Z})^2$, $S = \{(n,n^2)\}, T = \{(n^2,n)\}$. We shall prove that there is no G_i, S_i, T_i $(i=1,2)$ as above such that $G = G_1 \times G_2$, $T = T_1 \times T_2$, and $S = S_1 \times S_2$. Also G_1, G_2 non-trivial.

The following theorem assures that $G_i \cong \mathbb{Z}/p^k\mathbb{Z}$. Let $A_n = \mathbb{Z}/p^n\mathbb{Z}$.

Theorem 4.2. *If $G \cong A_{a_i} \times A_{a_2} \times \cdots A_{a_s} = P$ and each $a_i > 0$, then $s = 2$ and $a_1 = a_2 = k$.*

Proof. Our main observation is that isomorphism preserves the order of each element. First, we say that $a_i \leq k$. Since for each i, there is an element with order p^{a_i}, and orders in G is not greater than p^k, we must have $a_i \leq k$. Then we say that there exists an i, $a_i = k$. Let $a = \max\{a_i\}$, then for any element in P, say $\alpha = (\alpha_1, \cdots, \alpha_s)$, we have $p^a\alpha = 0$. So the orders in P is not greater than p^a. This means $a = k$, and there is an i, $a_i = k$.

Without loss of generality, we assume that a_i is arranged in ascending order. If there is another j, $a_j = k$, then we are done. Otherwise, $a_i < k$ for $i < s$. With the same notation α above, we have $p^{k-1}\alpha = (0,0,\cdots,p^{k-1}\alpha_s)$. So α has order p^k if and only if α_s is coprime to p. Therefore thereare $p^{2k-1}(p-1)$ elements with order p^k. On the other hand, we notice that there are $p^{k-1}(p^k - p^{k-1})$ more such elements in G, which gives a contradiction. ∎

Now we show that the analogous Gaussian construction is not a product. Otherwise $G = G_1 \times G_2$, where G_i is isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$. (Since we can further decompose G_i to product of cyclic groups.) We realize G_i as subgroups of G and suppose G_1 is generated by $u = (u_1, u_2)$, G_2 is generated by $v = (v_1, v_2)$. So by assumption there exists a_1, b_1, a_2, b_2 such that

$$a_1 u + b_1 v = (1, 0) \tag{30}$$
$$a_2 u + b_2 v = (0, 1) \tag{31}$$

This means

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{32}$$

This is true modulo p^k, and so is modulo p. Consider these elements in $\mathbb{F}_p$, we have

$$(a_1 b_2 - a_2 b_1)(u_1 v_2 - u_2 v_1) = 1 (\text{mod } p). \tag{33}$$

Since $(n, n^2) = (a_1 n + a_2 n^2)u + (b_1 n + b_2 n^2)v$, we have $(a_1 n + a_2 n^2)u \in S_1$. Similarly, $(a_1 n^2 + a_2 n)u \in T_1$ for any n. However, a_1, a_2 are not both multiples of p, by (33). So both S_1, T_1 contain elements with order p^k. (for example one of $a_1 + a_2, 2a_1 + 4a_2$ is not a multiple of p). And notice that both of them contains $0 = a_1 \cdot 0 + a_2 \cdot 0^2$. This means S_1, T_1 is a primitive formal dual pair. However, Schüler has proven that there is no primitive pair in $\mathbb{Z}/p^k\mathbb{Z}$ and we have a contradiction.

■

4.2 Non-existence of Primitive Formal Duals in $\mathbb{Z}/2^n\mathbb{Z}$

Since any abelian group is a product of some cyclic groups, it is natural to analyze the existence of primitive formal duals in cyclic groups. Among them, the simplest cases are $\mathbb{Z}/n\mathbb{Z}$, with n been a prime power. If n is an odd prime power, then primitive formal dual pairs do not exist (see [4]). In the same paper, Schüler gives some restrictions on the case of $\mathbb{Z}/2^k\mathbb{Z}$. So we are only left to consider the case $k = 2l$ and $|S| = |T| = 2^l$. In the following discussion, we always assume $l > 1$.

By analyzing the identities given in [4], we find that the weight enumerator ν_T of T can be solved (see Theorem 3.3). Eventually $\nu_T(2^\alpha) = 1$ for small α, and 0 for large α. And we will then show that there is no T with that weight enumerator.

We first prove the following lemma.

Lemma 4.2. *Suppose T is a subset of $\mathbb{Z}/2^k\mathbb{Z}$, $k = 2l$, and $|T| = 2^l$. If $\nu_t(2^\beta) = 1$ for all $0 \le \beta < \alpha \le l$, let $T_i = \{x \in T | x \equiv i (mod\ 2^\alpha)\}$. Then we have $|T_i| = 2^{l-\alpha}$ for each i.*

Proof. We prove it by induction. For $\alpha = 1$, we have $\nu_t(1) = 1$. The number of pairs (x, y) where $x - y$ is odd is equal to the sum $\sum_{x \text{ odd}} \nu_T(x)$. By Lemma 2.3, each $\nu_T(x) = \nu_T(1) = 1$.

So the sum is 2^{2l-1}. On the other hand, the pair is obtained by taking one element in each of T_0 and T_1. Since $|T_0| + |T_1| = |T| = 2^l$, the quantity equals

$$2|T_0||T_1| \leq \frac{1}{2}(|T_0| + |T_1|)^2 = 2^{2l-1.} \tag{34}$$

So the equality holds and $|T_0| = |T_1| = 2^{l-1} = 2^{l-\alpha}$.

Now suppose the lemma holds for $\alpha < l$. By the induction hypothesis, we have $|T_i| = 2^{l-\alpha}$. Here T_i denote the set of numbers in T with residue i modulo $2^\alpha = u$. For $\alpha + 1$, let T'_i denote the set of numbers with residue i modulo $2^{\alpha+1}$. Then we have $T'_i \cup T'_{i+u} = T_i$, and $T'_i \cap T'_{i+u} = \emptyset$. Note that number $\phi(2^k/2^\alpha)\nu_T(2^\alpha) = 2^{2l-\alpha-1}$, it is the number of pairs with (x, y) in T such that $(x - y, n) = 2^\alpha$. So, we have

$$\begin{aligned} 2^{2l-\alpha-1} &= \sum_{0\leq i\leq 2^\alpha-1} 2|T'_i||T'_{i+u}| \leq \sum_{0\leq i\leq 2^\alpha-1} \frac{1}{2}(|T'_i| + |T'_{i+u}|)^2 \\ &\leq \frac{1}{2} \cdot 2^\alpha \cdot (2^{l-\alpha})^2 = 2^{2l-\alpha-1}. \end{aligned} \tag{35}$$

Thus, equality holds and $|T'_i| = |T'_{i+u}|$, for each i. This means the statement is true for $\alpha + 1$. ■

Let us turn to the original problem, the existence of primitive formal dual pairs in $\mathbb{Z}/2^k\mathbb{Z}$. In the following discussion, we assume $k = 2l$, $|S| = |T| = 2^l$, $\nu_T(1) = \nu_S(1)$ and $\nu_T(2^{k-1}) = \nu_S(2^{k-1}) = 0$ (see [4], Theorem 4.1 and Example 4.4).

Before trying to solve ν_T, we state the following result:

Theorem 4.3. *([4], Corollary 3.4) If S, T are formally dual sets in $\mathbb{Z}/n\mathbb{Z}$, then for each y,*

$$\frac{|S|^2}{|T|}\nu_T(y) = \sum_{e|n} C_n(gcd(y, n), e) \cdot \nu_S(e). \tag{36}$$

Here

$$C_n(d, e) = \sum_{g|gcd(d,n/e)} \mu(n/eg)g, \tag{37}$$

where μ is the möbius function.

Using this result, together with the assumptions above, we could solve the ν_T for T that has a formal dual.

Theorem 4.4. *If S, T are formally dual subsets in $\mathbb{Z}/2^k\mathbb{Z}$, where $k = 2l$, then $\nu_T(2^\alpha) = \nu_S(2^\alpha) = 1$ for $0 \leq \alpha \leq l - 1$; 0 for $l \leq \alpha \leq 2l - 1$. Also, $\nu_T(0) = |T| = 2^l$.*

Proof. We prove by induction that $\nu_T(2^{2l-t}) = \nu_S(2^{2l-t}) = 0$ for each $1 \leq t \leq l$. First of all, our assumption implies that the statement is true if $t = 1$. Assuming that the statement is true for all $0 < t \leq n < l$, we shall prove the case for $n + 1$. Using Theorem 3.2, we have,

$$2^l\nu_T(2^x) = 2^l - 2^x\nu_S(2^{2l-x-1}) + 2^{x-1}\nu_S(2^{2l-x}) + \cdots + 2^0\nu_S(2^{2l-1}), \tag{38}$$

for all $0 < x < 2l$. Then by our assumption, for all $0 < x < n$, all terms of RHS vanishes except the term 2^l. So $\nu_T(2^x) = 1$ for $0 < x < n$. This is also true for S, since S and T satisfy the same assumption. For $x = n$, we have

$$2^l \nu_T(2^n) = 2^l - 2^n \nu_S(2^{2l-n-1}). \tag{39}$$

The left side is a non-negative multiple of 2^l. So $\nu_S(2^{2l-n-1})$ is 0 or 2^{l-n}. If it is 2^{l-n}, we show there is a contradiction. If there exist at least 3 numbers in S with the same residue modulo 2^{2l-n-1}, then we could assume without loss of generality that they have the form $2^{2l-n-1}a$, $2^{2l-n-1}b$ and $2^{2l-n-1}c$. Then at least two of a, b, c have the same residue modulo 2. For example a, b, then $2^{2l-n-1}a - 2^{2l-n-1}b$ is a non-zero number that is divisible by 2^{2l-n}. This contradicts our assumption that $\nu_S(2^{2l-t}) = 0$ for all $0 < t \leq n$.

This fact implies that S contains 2^{l-n} pairs $a_i, a_i + 2^{2l-n-1}$, with $0 \leq i < 2^{l-n}$. And the 2^{l-n+1} numbers are different elements in S. Now notice that

$$a_i + 2^{2l-n-1} - (a_j + 2^{2l-n-1}) = a_i - a_j. \tag{40}$$

Suppose that $(a_i - a_j, n) = 2^d$, this means $\nu_S(2^d) \geq 2$. Since $\nu_S(2^x) = 1$ for $x \leq n-1$, we have that $d \geq n$. Also $n < l$ implies $2l - n - 1 \geq n$, so the 2^{l-n+1} numbers have the same residue modulo 2^n. Applying our Lemma 3.2 for $\alpha = n$, we get a contradiction, since each residue class can only have 2^{l-n} elements. Therefore, $\nu_S(2^{2l-n-1}) = 0$ and the same result is true for T.

Now the induction process is complete and we have for $\nu_S(2^{2l-t}) = 0$ for $0 < t \leq l$. From our discussion under equation (38), we also have $\nu_S(2^t) = 1$ for $0 \leq t \leq l-1$. Here $\nu_S(1) = 1$ is the assumption. ■

Now we show that there is no $S \subset \mathbb{Z}/2^k\mathbb{Z}$ that corresponds to ν_S above. Then we could conclude that there is no primitive formal dual pairs in $\mathbb{Z}/2^k\mathbb{Z}$. Since $\nu_S(2^l) = 0$ and $|S| = 2^l$, we know that S form a complete set of residues modulo 2^l. Suppose $S = \{i + 2^l a_i\}$. Then because for each $0 \leq k \leq 2^l - 1$, $1 + k \cdot 2^l$ is odd, then $\nu_S(1 + k \cdot 2^l) = 1$. Notice that,

$$\nu_S(1) + \nu_S(1 + 2^l) + \cdots + \nu_S(1 + 2^l(2^l - 1)) = 2^l. \tag{41}$$

From the structure of S, there are exactly 2^l pairs with difference the form $1 + k \cdot 2^l$. And they are $1 + 2^l(a_{i+1} - a_i)$. This implies that

$$\{1 + k \cdot 2^l | 0 \leq k \leq 2^l - 1\} = \{1 + 2^l(a_{i+1} - a_i)\}_{i=0}^{2^l-2} \cup \{1 + 2^l(a_0 - a_{2^l-1} - 1)\}. \tag{42}$$

(these elements are understood as elements in $\mathbb{Z}/2^k\mathbb{Z}$) and

$$\{k | 0 \leq k \leq 2^l - 1\} = \{a_{i+1} - a_i | 0 \leq i \leq 2^l - 2\} \cup \{a_0 - a_{2^l-1} - 1\} (\text{mod } 2^l) \tag{43}$$

By taking the sum of all the elements in both sets, we get

$$(2^l - 1)2^{l-1} = -1 (\text{mod } 2^l). \tag{44}$$

This is a contradiction for $l > 1$.

4.3 Conditions on Formally Dual Pairs in $(\mathbb{Z}/p\mathbb{Z})^2$

Although it is difficult to generalize the work above to $\mathbb{Z}/n\mathbb{Z}$ for arbitrary n, we can make some progress on product of groups. And among them the simplest case is $(\mathbb{Z}/p\mathbb{Z})^2$. In [1], the authors give an primitive formal dual pair using Gaussian construction. Although we could not solve the case completely, we find some restrictions. In [2], they prove that invertible linear transformations preserve formal duality, in the setting of $\mathbb{R}^n$. This fact can be proven directly in abelian groups $G = (\mathbb{Z}/p\mathbb{Z})^2$, for p prime. In fact, we have the following result:

Theorem 4.5. *Let $\phi : G \to G$ be a transformation such that $\phi(x, y) = (ax + by, cx + dy)$, with $ad - bc \neq 0 \pmod p$. Then ϕ is invertible. Let S, T be formal dual subsets of G. Then there exists a invertible transformation ψ such that $\phi(S)$ and $\psi^(T)$ are formally dual.*

Proof. In fact, from the assumption in the theorem, we could let $u = (ad - bc)^{-1}$. Define $\psi : G \to G$ such that $\psi(x, y) = (udx - ucy, -ubx + uay)$. Then it is easy to check that ψ is invertible. In fact, if we see elements in G as a column vector, then the matrix associated with ψ is the inverse transpose of the matrix associated with ϕ.

Suppose S, T are formally dual. Let $S' = \phi(S)$, $T' = \psi(T)$. It is easy to verify that $|S'| = |S|, |T'| = |T|$. In addition, for $\alpha \in G$,

$$\nu_{T'}(\alpha) = \#\{(t_1, t_2) \in T'^2, t_1 - t_2 = \alpha\} = \#\{(t_1, t_2) \in T^2, t_1 - t_2 = \psi^{-1}(\alpha)\}. \tag{45}$$

So

$$\nu_{T'}(\alpha) = \nu_T(\psi^{-1}(\alpha)) \tag{46}$$
$$\nu_{S'}(\alpha) = \nu_S(\phi^{-1}(\alpha)) \tag{47}$$

In order to prove that T' and S' are formally dual, we can use Lemma 2.2 for T, S, which shows

$$\frac{|S|^2}{|T|}\nu_T(\alpha) = \sum_{\beta \in G} \nu_S(\beta)\langle\beta, \alpha\rangle. \tag{48}$$

Then, we have

$$\begin{aligned}
\frac{|S'|^2}{|T'|}\nu_{T'}(\alpha) &= \frac{|S|^2}{|T|}\nu_T(\psi^{-1}(\alpha)) \\
&= \sum_{\beta \in G} \nu_S(\beta)\langle\beta, \psi^{-1}(\alpha)\rangle \\
&= \sum_{\beta \in G} \nu_S(\phi^{-1}(\beta))\langle\phi^{-1}(\beta), \psi^{-1}(\alpha)\rangle \\
&= \sum_{\beta \in G} \nu_{S'}(\beta)\langle\beta, \alpha\rangle.
\end{aligned} \tag{49}$$

So S', T' are formally dual. Note that we used the fact $\langle\phi^{-1}(\beta), \psi^{-1}(\alpha)\rangle = \langle\beta, \alpha\rangle$, which can be verified directly from the definition of ψ, ϕ. ■

Eventually we give the following restriction.

Theorem 4.6. *If S and T are formally dual in the group $(\mathbb{Z}/p\mathbb{Z})^2$, where p is an odd prime, then under two invertible transformations, we could write $S = \{(i, a_i)\}$ and $T = \{(b_i, i)\}$, or one of $S, T = (\mathbb{Z}/p\mathbb{Z})^2$, the other contains any single element.*

The theorem is trivial for if one of $|S|, |T| = 1$. In the following discussion, we consider the case $|S| = |T| = p$. First, we have a lemma analagous to Lemma 2.3, which gives some equalities between weight enumerators.

Lemma 4.3. *If x is not zero, then*

$$\nu_T(x, y) = \nu_T(1, yx^{-1}) \tag{50}$$

This lemma can be proved using the same method in section 3 ([4]) by considering the field automorphism $\mathbb{Q}(\zeta_p) \to \mathbb{Q}(\zeta_p^{x^{-1}})$. We take$\zeta = \zeta_p$ be the primitive p-th root of unity, in this section.

Lemma 4.4. *Let $S = \{a_i\}_{i=1}^p$ be a sequence of elements in $\mathbb{Z}/p\mathbb{Z}$. If*

$$\sum_i \zeta^{a_i} = 0, \tag{51}$$

then the image of S is $\mathbb{Z}/p\mathbb{Z}$.

Proof. In fact, (51) implies the polynomial $\sum x^{a_i}$ is a multiple of $\sum_{0 \le i \le p-1} x^i$. ■

Notice that

$$\sum_{(x,y)} \nu_T(x, y) = |T|^2 = p^2. \tag{52}$$

Combined with lemma 3.3 and that $\nu_T(0, 0) = |T| = p$, we have

$$\nu_T(0, 1) + \sum_k \nu_T(1, k) = p. \tag{53}$$

Since the left side is a sum of $p + 1$ non-negative integers, there is at least one zero term. Suppose that $S = \{(a_i, b_i), 0 \le i \le p - 1\}$. If $\nu_T(0, 1) = 0$, then it follows from the definition of formal duality (Definition 3.1) that $\sum_i \zeta^{b_i} = 0$. By Lemma 3.4, $\{b_i\} = \{i\}$. By the same reason, we must have $\{a_i + kb_i\} = \{i\}$ if $\nu_T(1, k) = 0$. Without loss of generality, we can assume that $a_i + b_i k = i$. By taking the invertible transformation, $x \to x + ky, y \to y$, we can assume $S = \{(i, x_i)\}$. Now note that $\nu_S(0, 1) = 0$. If $T = \{(c_i, d_i)\}$, use Lemma 3.3 again and we have $\{d_i\} = \{i\}$. The order does not matter in the definition of formal duality, so we get the form in Theorem 3.5.

4.4 Abelian Group of Square-free Order

In this section, we prove the following theorem:

Theorem 4.7. *There are no primitive formal dual pairs in an abelian group with square-free order.*

Proof. Suppose G is an abelian group with order n square free. We have by Lemma 2.1 that $|S|$ and $|T|$ are coprime to each other. Recall that any abelian group G can be written as product:

$$G = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \cdots \times \mathbb{Z}/n_k\mathbb{Z}. \tag{54}$$

Then we can identify G with $\hat{G}$ using the correspondence $(a_1, a_2, \cdots, a_k)$, $(b_1, b_2, \cdots, b_k) \to \zeta_1^{a_1 b_1}\zeta_2^{a_2 b_2} \cdots \zeta_k^{a_k b_k}$. Notice that in this setting $\langle x, y\rangle$ is an algebraic integer for each pair (x, y). So from Lemma 2.2, $\frac{|S|^2}{|T|}\nu_T(y)$ is an algebraic integer. Since it is rational, it is actually an integer. This means $|T|$ must divide $\nu_T(y)$ for each y. From Lemma 2.2, we have

$$0 \le |S|^2\frac{\nu_T(y)}{|T|} = \big|\sum_{x\in S}\langle x, y\rangle\big|^2\nu_S(x) \le (\sum_{x\in S} 1)^2 = |S|^2. \tag{55}$$

Hence $\nu_T y = 0$ or $|T|$. If S, T form a primitive formal dual pair, then both $|S|, |T| \neq 1$. So there exists a non-zero $y \in G$, such that $\nu_T(y) = |T|$. (55) implies that the equality holds, and thus $\langle x, y\rangle = 1$ for all $x \in S$. So S is contained in the kernel of y, which is a subgroup of G. The subgroup is proper since y is non-zero, and $|S| \neq 1$.

From Definition 2.3, we can conclude that there is no such formal dual in abelian group with square-free order. ■

Notice that the only thing needed was $|S|, |T|$ are coprime to each other. So we have the following more general result:

Theorem 4.8. *If S, T is a primitive formal dual pair, then $gcd(|S|, |T|) > 1$.*

5 A Graph Representing Formal Dual Relations

Now we have many properties for each pair of formal dual sets. However, the relations between formal dual pairs are still not analyzed. In this section, we use a graph to represent the relations of formal duality. Given a finite abelian group A, formal duality is a relationship between two of its subsets. We represent the subsets of A be vertices, and connect two vertices if the subset they represent are formally dual. We call this graph G. This may not be a simple graph, since there may exists formally self-dual sets, which will result in a self-loop. In the following discussion, we do not distinguish the vertex with the subset it represents.

Our first observation is about the neighborhoods of the vertices. Let $N(P)$ be the neighborhood of a vertex P. Since it is the set of all the vertices that are directly connected to P, it represents the set of all subsets of A that are formally dual to P. Then

Theorem 5.1. *Let G be the graph defined above. If $N(A) \cap N(B) \neq \emptyset$, then $N(A) = N(B)$.*

Proof. Let T, S be formally dual sets. By Definition 2.2, the weight function ν_T is uniquely determined by S. In fact, this is the only condition required. If another T' has $\nu_T = \nu_{T'}$, then S, T' are also formally dual.

Now suppose that $N(A) \cap N(B) \neq \emptyset$. Let C be a set formally dual to both A, and B. For any other element $D \in N(A)$, $\nu_D = \nu_C$, since both C, D are formally dual to A. From our discussion above, we have D and B are formally dual, since C is formally dual to B, Thus $N(A) \subset N(B)$. Since $N(B) \subset N(A)$ by symmetry, $N(A) = N(B)$. ■

From this theorem, we have more observations on the graph. In particular, the structure of the graph would be extremely simple, if there is no formally self-dual sets. Such sets do not occur very often, e.g. when the order of the group is not a square.

Corollary 5.2. *Suppose there is a triangle in the graph G. In other words: there exists A, B, and C which are pair-wise formally dual. Then A, B, C are all formally self-dual sets. Note that A, B, C may not be distinct from each other.*

Proof. Since $C \in N(A) \cap N(B)$, we have that $N(A) \cap N(B) \neq \emptyset$. Then $N(A) = N(B)$, which contains A. So, A is formally self-dual. We also have that B, C are formally self-dual by symmetry. ■

In fact, we have a more general result, which follows from the above corollary by induction. The triangle there can be replaced by any n-cycle, with n odd.

Corollary 5.3. *Suppose n is odd. If there exists a n-cycle in G, say $A_i \in G, i = 1, 2, \cdots, n$, with A_i formally dual to A_{i+1}, ($A_{n+1} = A_1$), then these n points forms a complete subgraph, and each A_i is formally self-dual.*

Proof. We use induction on n. The $n = 3$ case was proven in Corollary 5.2. Now suppose the statement is true for $n - 2$. Then consider a n-cycle $A_1 A_2 \cdots A_n$. Consider the four consecutive vertices A_1, A_2, A_3, A_4. Note that $N(A_1) \cap N(A_3)$ is not empty because they both contain A_2. So $A_4 \subset N(A_3) = N(A_1)$. Then we get the $(n-2)$-cycle $A_1 A_4 A_5 \cdots A_n$. By our induction assumption, we know this $(n-2)$ points forms a complete subgraph. And each $A_i, i \neq 2, 3$ is formally self-dual. Since the four points chosen can be any consecutive four points, the n points A_i form a complete subgraph and each A_i is formally self-dual. Now the induction process is complete. ■

From the above Corollary, one can easily see that when G has no formally self-dual set, G is simple and has no odd cycle. This means that G is a bipartite graph. In fact, we can say more in this case.

Theorem 5.4. *If G has no formally self-dual set, then each connected component is a complete bipartite graph.*

Proof. Since G is clearly a finite graph, it suffices to consider one of its connected component. Pick any point P in this graph and let $B = N(P)$ and A be the set of points that are not in B. We prove that this is a complete graph (A, B). First, points in B are not connected to each other. Otherwise there will be a triangle with vertices P and these two points. Since this component is connected, the set $A - \{P\}$ is connected to $\{P\} \cup B$. So, there exists a point $Q \in A - \{P\}$, which is connected to at least one element in $\{P\} \cup B$. The element cannot be P, since $B = N(P)$ are all its neighborhoods. So Q is connected to one of B. From Theorem 5.1, we know $N(Q) = N(P) = B$. We can continue this process until there is no point left. The process must end because there are only finitely many points. ■

Notice that this theorem as well as above ones are also true if we only consider those points with specific orders. For example, consider the group $G = \mathbb{Z}/10\mathbb{Z}$. In this case we can simply consider the subsets with order 2, or 5, then it is naturally a bipartite graph.

6 Formally Self-dual Sets

As seen in the previous section, formally self-dual sets make the graph complicated. However, these kinds of sets are very rare. We could not even find any primitive ones. In this section, we analyze formally self-dual sets in some specific groups.

6.1 Examples in $\mathbb{Z}/n^2\mathbb{Z}$.

Theorem 6.1. *In $G = \mathbb{Z}/n^2\mathbb{Z}$, the set $S = \{kn\}_{k=0}^{n-1}$ is formally self-dual.*

Proof. Let $\zeta = e^{2\pi i/n^2}$. For any $r \in G$, Definition 2.2 gives

$$|\sum_{k=0}^{n-1} \zeta^{knr}|^2 = n\nu_S(r). \tag{56}$$

It is easy to check that the left side is 0 when r is not a multiple of n, and n^2 when r is a multiple of n. In the former case, elements in $S - S$ are multiples of n, since each element in S is a multiple of n. So $\nu_S(r) = 0$ if r is not a multiple of n. In the latter case, it is easy to verify that $\nu_S(r) = n$, since for any $a \in S$, $a + r$ is also in S. ■

6.2 Formal Self-duality in $(\mathbb{Z}/p\mathbb{Z})^2$

In this section, we consider the group $G = (\mathbb{Z}/p\mathbb{Z})^2$. First, we note that the only formally self-dual set in $(\mathbb{Z}/2\mathbb{Z})^2$is $S = \{(0,0),(1,1)\}$ (up to a translation). Since there are only 2 essentially different cases, it is easy to check. In the following discussion, we consider p be a odd prime.

Theorem 6.2. *For $p \equiv 3 \pmod 4$, there is no formally self-dual set in $(\mathbb{Z}/p\mathbb{Z})^2$.*

First, we need a lemma

Lemma 6.1. *Let S and T be a formally dual pair in $(\mathbb{Z}/p\mathbb{Z})^2$. By Theorem 3.4, we can assume $T = \{(i, b_i)\}, S = \{(a_i, i)\}$. Then $\nu_S(a, 1) = \nu_T(1, -a)$, for any $a \in \mathbb{Z}/p\mathbb{Z}$.*

Proof. By Definition 2.2, we have for all $a \in \mathbb{Z}/p\mathbb{Z}$,

$$\left|\sum_{i=0}^{p-1} \zeta^{ai+b_i}\right|^2 = p\nu_S(a, 1). \tag{57}$$

Expanding the left side, we have

$$\left|\sum_{i=0}^{p-1} \zeta^{ai+b_i}\right|^2 = \sum_{i,j} \zeta^{a(i-j)+b_i-b_j} = \sum_{x,y} \nu_T(x, y)\zeta^{ax+y}. \tag{58}$$

So this is a polynomial of ζ. Writing it as $A = a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$, we have the following

$$\begin{aligned} a_1 &= a_2 = \cdots = a_{p-1} && (59)\\ a_0 + a_1 + \cdots a_{p-1} &= |S|^2 = p^2 && (60)\\ a_0 &= \sum_x \nu_T(x, -ax) = p + (p-1)\nu_T(1, -a). && (61) \end{aligned}$$

This implies $a_1 = p - \nu_T(1, -a)$ and that $A = a_0 - a_1 = p\nu_T(1, -a)$. Comparing this with the right side of (57), we get

$$\nu_T(1, -a) = \nu_S(a, 1). \tag{62}$$

■

Now we are able to prove Theorem 6.2.

Proof of Theorem 6.2. We are considering the case $S = T$. Under some proper transformation (see Theorem 3.5), we can assume that $S = T = \{(i, b_i)\} = \{(a_i, i)\}$. This means $\nu_S(0, 1) = \nu_S(1, 0) = 0$. We also have

$$\begin{aligned} p^2 = |S|^2 &= \sum_{x,y} \nu_S(x, y)\\ &= p + (p-1)\nu_S(0, 1) + (p-1)\sum_{a=0}^{p-1} \nu_S(1, a)\\ &= p + (p-1)\sum_{a=1}^{p-1} \nu_S(1, a). \end{aligned} \tag{63}$$

Thus, we have that

$$p = \sum_{a=1}^{p-1} \nu_S(1, a). \tag{64}$$

By Lemma 6.4, we have $\nu_S(1, a) = \nu_S(-a, 1) = \nu_S(1, -a^{-1})$, for $a \neq 0$. If $p \equiv 3 \pmod 4$, there is no a, such that $a = -a^{-1}$. Hence by summing the right side by pairs, it is an even number, which contradicts our assumption that p is odd. ■

When $p \equiv 3 \pmod 4$, $(\mathbb{Z}/p\mathbb{Z})^2$ indeed contains a formally self-dual set.

Theorem 6.3. *If $p \equiv 1 \pmod 4$, $S = \{(i, ai)\}_{i=0}^{p-1}$, with $a^2 \equiv -1 \pmod 4$, is a formally self-dual set.*

7 Formal Duals in Tight Packings with dimension 5

The existence of formal duals for periodic sphere packings is an interesting problem posed in [1]. The authors prove that the only Barlow packing that has a formal dual is the face-centered cubic lattice. The Barlow packings correspond to Conway's conjectural tight packings for dimension 3 (see [3]). For dimension 4, his conjectural tight packing is D_4, which is a lattice, and naturally has a formal dual: its dual lattice. Hence we analyze the existence of formal duals for tight packings in dimension 5 in this section.

7.1 Conway's Conjectural Tight Packings

We describe the conjectural tight packings in Conway's list, and then transform the construction to the language of formal duality. In [3], all tight packings with dimension 5 can be constructed by superposing layers of D_4. With his notation, the four cosets in dual lattice D_4^* are

$$\begin{aligned} &[0] = D_4, [1] = D_4 + (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}) \\ &[2] = D_4 + (0, 0, 0, 1), [3] = D_4 + (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}). \end{aligned} \tag{65}$$

The covering radius of D_4 is 1, so each two adjacent layers are separated by a distance of $\sqrt{2-1} = 1$. In the space with dimension 5, consider $\alpha_0 = 0$, $\alpha_1 = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0)$, $\alpha_2 = (0, 0, 0, 1, 0)$, $\alpha_3 = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, 0)$.

We only consider periodic tight packings, and assume there are n layers in each period. Then the underlying lattice Λ is spanned by $D_4 \times \{0\}$ and $v = (0, 0, 0, 0, n)$. The j-th layer is a translation $a_j + \frac{jv}{n}$ of Λ. Here a_j is one of $\alpha_i, i = 0, 1, 2, 3$. From the discussion in Conway's paper ([3], section 5), the two adjacent layers must have different cosets of D_4, so $a_j \neq a_{j+1}$.

From the above discussion, we could let $G = (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/n\mathbb{Z}$, which is generated by $\alpha_2, \alpha_1, \frac{v}{n}$ modulo Λ. Each element (i, j, k) in G corresponds to a translation $i\alpha_2 + j\alpha_1 + \frac{kv}{n}$ of D_4.

Under this setting, the tight packings correspond to a subset $T = \{(a_i, b_i, i)\}_{i=0}^{n-1}$ of G, with $(a_i, b_i) \neq (a_{i+1}, b_{i+1})$, where subscript is understood modulo n. We would like to know which tight packings corresponds to subsets that have formal duals.

7.2 Existence of Formal Duals

If the set T has a formal dual S, then $|S| = 4$, by Lemma 2.1. By Theorem 4.3, since T is parametrized by $\mathbb{Z}/n\mathbb{Z}$, S is parametrized by $(\mathbb{Z}/2\mathbb{Z})^2$. So, S has the form $\{(0,0,0),(1,0,a),(0,1,b),(1,1,c)\}$ if $0 \in S$. (A translation will not affect formal duality.) In order to determine existence of formal duals for tight packings, we will begin by analyzing possible (a,b,c).

Let $\zeta = e^{\frac{2\pi i}{n}}$. The definition of formal duality becomes,

$$\left|1 + (-1)^x \zeta^{az} + (-1)^y \zeta^{bz} + (-1)^{x+y} \zeta^{cz}\right|^2 = \frac{16}{n} \nu_T(x,y,z), \tag{66}$$

for any x, y, z. Since $(a_i, b_i) \neq (a_{i+1}, b_{i+1})$, we have $\nu_T(0,0,1) = 0$. Substitute this in the above equation, we get

$$1 + \zeta^a + \zeta^b + \zeta^c = 0. \tag{67}$$

Take $(x,y,z) = (1,0,1)$, with the above relation, we have

$$\frac{16}{n} \nu_T(x,y,z) = 4\left|1 + \zeta^b\right|^2. \tag{68}$$

So $|1+\zeta^b|^2$ is a rational number, and thus an integer. This implies that $b \in \{0, \frac{n}{2}, \pm\frac{n}{3}, \pm\frac{n}{4}, \pm\frac{n}{6}\}$ $= A$. If we take $(x,y,z) = (0,1,1),(1,1,1)$, we get $a, c, \in A$. Combining this with (67), there are 4 possible $\{a,b,c\}$ as a set (elements can repeat): $\{0, \frac{n}{2}, \frac{n}{2}\}$, $\{\frac{n}{2}, \frac{n}{4}, -\frac{n}{4}\}$, $\{\frac{n}{2}, \frac{n}{3}, -\frac{n}{6}\}$, $\{\frac{n}{2}, -\frac{n}{3}, \frac{n}{6}\}$. Note that $-S$ and S have the same formal duals. So, formal duals for each possible (a,b,c) from $\{\frac{n}{2}, -\frac{n}{3}, \frac{n}{6}\}$ can be found in $\{\frac{n}{2}, \frac{n}{3}, -\frac{n}{6}\}$. Thus there are three cases. Note that numbers like $\frac{n}{2}$ may not be integers. All the statements below and above should be understood as : If $\frac{n}{2}$ ($\frac{n}{6}$ or $\frac{n}{3}$) exists, then...

One quick observation is that for all the cases, we have $\nu_T(0,0,12) = n$ from equation 66. So the sequence (a_n, b_n) has period 12. This means the uniform packing Λ_5^4, which has period 8, has no formal dual.

Case 1 (a,b,c) is a permutation of $(0, \frac{n}{2}, \frac{n}{2})$. In this case, from (66), we always have $\nu_T(0,0,2) = n$. This means the sequence (a_n, b_n) has period 2. By considering $\nu_T(x,y,1)$, we can determine T. Eventually, those T with formal duals have $\{(a_0,b_0),(a_1,b_1)\} = \{(0,0),(0,1)\},\{(0,0),(1,0)\}$, or $\{(0,0),(1,1)\}$. These three T corresponds to the three uniform packings Λ_5^1: 0101..., 0202..., 0303...

Case 2 (a,b,c) is a permutation of $(\frac{n}{2}, \frac{n}{4}, -\frac{n}{4})$. In this case, we have $\nu_T(0,0,4) = n$, similar to the case above. So the sequence of layers have period 4. For simplicity, we will list those T with formal duals, by showing the first four letters. In the list, we use 0 for (0, 0), 1 for (0, 1), 2 for (1, 0), 3 for (1, 1), which corresponds to Conway's notation of the four cosets of D_4. Those T are : 0213, 0312, 0123, 0321, 0132, 0231. These are uniform packings Λ_5^2.

Case 3 (a,b,c) is a permutation of $(\frac{n}{2}, \frac{n}{3}, -\frac{n}{6})$. In this case, $\nu_T(0,0,6) = n$. Hence the sequence of layers has a period 6. Since we are assuming n is divisible by 6, each

$\nu_T(x, y, 1)$ must be a multiple of $\frac{n}{6}$. However, it is easy to check that for each (a, b, c), there are some (x, y) for which $\nu_T(x, y, 1) = \frac{n}{4}$. This is not a multiple of $\frac{n}{6}$, which is a contradiction.

In sum, the tight packings with formal duals are Λ_5^1 and Λ_5^2.

8 Open Problems

There are still many problems left to analyze from the above sections. It would be interesting to analyze the existence of formal duals in $\mathbb{Z}/n\mathbb{Z}$. In addition, our examples of self-dual sets, our examples are not primitive. One could try to find any primitive formal self-duals. Furthermore, although the construction of formal dual pair in $(\mathbb{Z}/p^k\mathbb{Z})^2$ is primitive, they can still be generated by taking products of Gaussian construction. Can anyone find a real "primitive" example of formal dual pair?

Further, when analyzing the formal duals in product group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, we find that the formal dual pairs can usually be obtained by inflating those in $(\mathbb{Z}/d\mathbb{Z})^2$, where d is the greatest common divisor of m, n. Is this always possible if we add a restriction that S is parametrized by $\mathbb{Z}/m\mathbb{Z}$? For example, this works for the group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, which was analyzed in section 7. If m, n are coprime to each other, the order of S, T are coprime to each other under our restriction. By section 3.4, they are induced by trivial ones.

Acknowledgement

I would like to thank Soohyun Park for suggesting reading materials, pointing potential directions to work on, checking the proofs and making comments on the writing. I am also grateful to professor Henry Cohn for proposing such an interesting project and pointing out some errors in the paper. This project is funded by UROP+ program, organized by the mathematics department at MIT.

References

[1] 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.

[2] H.Cohn, A.Kumar, C.Reiher, and A.Schürmann, *Ground states and formal duality relations in the Gaussian core model*, Phys. Rev. E (3) **80** (2009), no.6, 061116, 7 pp.

[3] J. H. Conway and N. J. A. Sloane *What are all the best sphere packings in low dimensions?*, Discrete Comput. Geom. **13** (1995), no. 34, 383403.

[4] Robert Schüler. *Formal-dual subsets of cyclic groups of prime power order*. `https://arxiv.org/abs/1605.05939` Preprint, 2016.