HAMBURGER BEITRÄGE
ZUR MATHEMATIK

Heft 482

Formal duality and generalizations of Poisson summation

Henry Cohn, Abhinav Kumar, Christian Reiher, Achill
Schürmann

Formal duality and generalizations of the Poisson summation formula

Henry Cohn, Abhinav Kumar, Christian Reiher, and Achill Schürmann

ABSTRACT. We study the notion of formal duality introduced by Cohn, Kumar, and Schürmann in their computational study of energy-minimizing particle configurations in Euclidean space. In particular, using the Poisson summation formula we reformulate formal duality as a combinatorial phenomenon in finite abelian groups. We give new examples related to Gauss sums and make some progress towards classifying formally dual configurations.

1. Introduction

The Poisson summation formula connects the sum of a function over a lattice $\Lambda \subset \mathbb{R}^n$ with the sum of its Fourier transform over the dual lattice Λ^*; recall that Λ^* is spanned by the dual basis (with respect to the inner product) to any basis of Λ. In fact, Poisson summation completely characterizes the notion of duality for lattices. In a computational study of energy minimization for particle configurations, Cohn, Kumar, and Schürmann [**CKS**] found several examples of non-lattice configurations exhibiting a similar *formal duality* with respect to a version of Poisson summation. In this paper, we place these examples in a broader context, produce new examples using the theory of Gauss sums, and take the first steps towards a classification of formally dual configurations.

Energy minimization is a natural problem in geometric optimization, which generalizes the sphere packing problem of arranging congruent, non-overlapping spheres as densely as possible in $\mathbb{R}^n$. The *energy* $E_f(\mathcal{C})$ of a configuration $\mathcal{C} \subset \mathbb{R}^n$ with respect to a radial potential function $f\colon \mathbb{R}_{>0} \to \mathbb{R}$ is defined to be the average over $x \in \mathcal{C}$ of the energy of x, which is

$$E_f(x,\mathcal{C}) = \sum_{y \in \mathcal{C} \setminus \{x\}} f(|x - y|).$$

Of course these sums might diverge or the average over x might not be well defined. We therefore restrict $\mathcal{C}$ to be a periodic configuration, i.e., the union of finitely many translates of a lattice in $\mathbb{R}^n$, and we consider only potential functions that decrease rapidly enough at infinity to ensure convergence. See Section 9 of [**CK1**] for more details.

For each potential function f, the energy minimization problem asks for the configuration $\mathcal{C}$ that minimizes $E_f(\mathcal{C})$ subject to fixing the point density $\delta(\mathcal{C})$ (i.e., the number of points per unit volume).

In [**CKS**], the authors undertook an experimental study of energy minima in low dimensions for Gaussian potential functions. This is the Gaussian core model from mathematical physics [**S**], and Gaussian potential functions also play a key role in the mathematical theory of universal optimality [**CK1**], because they span the cone of completely monotonic functions of squared distance. (If a configuration minimizes all Gaussian potentials simultaneously, then it minimizes many others as well, such as inverse power laws.) For the potential function $G_c(r) := \exp(-\pi c r^2)$, as $c \to \infty$ the potential energy for each point is dominated by the contribution from its nearest neighbors. In the limit, minimizing the energy requires maximizing the distance between the nearest neighbors and thus maximizing the density of the corresponding sphere packing. We can therefore view energy minimization with c large as a "soft-matter" version of sphere packing, in which small distances between particles are allowed but heavily penalized, and we recover the hard sphere model in the limit as $c \to \infty$.

Maximizing density is a necessary condition for optimality as $c \to \infty$, but it is not sufficient, since two optimal sphere packings needn't have the same energy. For example, one may contain fewer pairs of nearest neighbors, in which case it will have lower energy when c is large. As shown in [**CK2**], the densest lattice packing in $\mathbb{R}^n$ fails to minimize energy for large c when $n = 5$ or $n = 7$. Furthermore, [**CKS**] reported on numerical searches for energy minima among periodic configurations with $1 \le n \le 9$ and a range of values of c. (The results in [**CKS**] are formulated in terms of a fixed potential function and varying particle density, but that is equivalent to our perspective here under rescaling to fix the density.)

The most noteworthy finding from [**CKS**] was that in each dimension, the energy-minimizing structures for the potential functions G_c and $G_{1/c}$ seem to be *formally dual* (except in certain narrow ranges of phase coexistence). Formal duality generalizes the more familiar notion of duality for lattices. We will recall the definition in Section 2; the key property is that if $\mathcal{P}$ and $\mathcal{Q}$ are formal duals, then formal duality relates the f-potential energy of $\mathcal{P}$ to the $\widehat{f}$-potential energy of $\mathcal{Q}$ for all potential functions f, where $\widehat{f}$ is the Fourier transform of f. Note that G_c and $G_{1/c}$ are Fourier transforms of each other, up to scalar multiplication.

To describe the simulation results from [**CKS**], we will need some notation. Let D_n^+ be the periodic configuration consisting of the union of the checkerboard lattice

$$D_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid x_1 + \cdots + x_n \equiv 0 \pmod{2}\}$$

and its translate by the all-halves vector (note that D_n^+ is actually a lattice if n is even), and for $\alpha > 0$ let

$$D_n^+(\alpha) = \{(x_1, \ldots, x_{n-1}, \alpha x_n) \mid (x_1, \ldots, x_n) \in D_n^+\}$$

be obtained by scaling the last coordinate.

The numerical experiments in [**CKS**] indicate that in dimension 5, the family of configurations $D_5^+(\alpha)$ minimize the G_c-energy, with α some function of the parameter c, except in a small interval around $c = 1$ (in this interval there is phase coexistence and the optimal configuration is probably not periodic). For instance, as $c \to \infty$, the minima seem to approach $D_5^+(2)$, which is the tight packing Λ_5^2 in the notation of [**CS1**]. Similarly, in dimension 7 the $D_7^+(\alpha)$ family seems to be optimal.

In three cases there are single configurations that seem to minimize potential energy for the entire family of Gaussian potential functions: D_4 in dimensional 4, E_8 in dimension 8 (consistent with the conjecture of universal optimality from [**CK1**]), and D_9^+ in dimension 9. In dimension 6, the energy minima are experimentally seen to be E_6 and its dual for $c \to \infty$ and $c \to 0$, respectively; around the central point $c = 1$ experiments yield the following periodic configuration $\mathcal{P}_6(\alpha)$, where α depends on c. Let $\mathcal{P}_6$ be the lattice $D_3 \oplus D_3$, along with its translates by the three vectors $v_1 = (-1/2, -1/2, -1/2, 1, 1, 1)$, $v_2 = (1, 1, 1, -1/2, -1/2, -1/2)$, and $v_3 = v_1 + v_2$. Then $\mathcal{P}_6(\alpha)$ is obtained from $\mathcal{P}_6$ by scaling the first three coordinates by α and the last three by $1/\alpha$.

Whether or not these families are the true global minima, they certainly exhibit the phenomenon of formal duality. Namely, $D_n^+(\alpha)$ is formally dual to an isometric copy of $D_n^+(1/\alpha)$, and $\mathcal{P}_6(\alpha)$ is formally dual to an isometric copy of itself. See Section VI of [**CKS**] for a proof for $D_n^+(\alpha)$ and a sketch of the analogous proof for $\mathcal{P}_6(\alpha)$. Formal duality comes as a surprise, because most configurations do not have formal duals at all. The experimental findings lead to a natural question: do the global minima for Gaussian potential energy in Euclidean space always appear in families exhibiting formal duality? Outside of certain narrow ranges for the parameter c, where one observes phase coexistence leading to aperiodic minima, all the numerical data from [**CKS**] is consistent with formal duality.

The structures found in [**CKS**] have been the only known examples of formally dual pairs other than lattices. In this paper, we present a new family of examples based on Gauss sums, we analyze structural properties of formally dual configurations, and we take the first steps towards a classification.

2. Poisson summation formulas and duality

We first recall the Poisson summation formula. Given a well-behaved function $f \colon \mathbb{R}^n \to \mathbb{R}$ (for example, a Schwartz function, though much weaker hypotheses will suffice), define its Fourier transform $\widehat{f} \colon \mathbb{R}^n \to \mathbb{R}$ by

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

Then the Poisson summation formula states that for a lattice $\Lambda \subset \mathbb{R}^n$,

$$\sum_{x \in \Lambda} f(x) = \frac{1}{\mathrm{covol}(\Lambda)} \sum_{y \in \Lambda^*} \widehat{f}(y),$$

where

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

is the dual lattice and $\mathrm{covol}(\Lambda) = \mathrm{vol}(\mathbb{R}^n/\Lambda)$ is the volume of a fundamental domain of Λ. The Poisson summation formula is a useful identity in many areas of mathematics. For instance, it can be used to prove analytic continuation and the functional equation for the Riemann zeta function.

As a consequence of Poisson summation,

$$f(0) + E_f(\Lambda) = \frac{1}{\mathrm{covol}(\Lambda)} \big(\widehat{f}(0) + E_{\widehat{f}}(\Lambda^*) \big)$$

for every lattice Λ. Here $\widehat{f}$ is an abuse of notation, in which we treat the potential function $f \colon \mathbb{R}_{>0} \to \mathbb{R}$ as a radial function on $\mathbb{R}^n$.

It follows that a lattice Λ minimizes E_f among lattices with a fixed covolume if and only if Λ^* minimizes $E_{\widehat{f}}$. The most important special case is the Gaussian potential function $G_c(r) = \exp(-\pi c r^2)$, which has n-dimensional Fourier transform $\widehat{G_c}(r) = c^{-n/2} \exp(-\pi r^2/c)$. In this case Poisson summation relates $E_{G_c}(\Lambda)$ to $E_{G_{1/c}}(\Lambda^*)$.

One could ask if there is a reasonable analogue of the Poisson summation formula for non-lattices. The obvious generalization would be to ask for periodic configurations $\mathcal{P}$ and $\mathcal{Q}$ with

$$\sum_{x \in \mathcal{P}} f(x) = \delta(\mathcal{P}) \sum_{y \in \mathcal{Q}} \widehat{f}(y)$$

for all well-behaved f. Here $\delta(\mathcal{P})$ is the point density of $\mathcal{P}$: if $\mathcal{P}$ consists of N translates of a lattice Λ, then $\delta(\mathcal{P}) = N/\operatorname{covol}(\Lambda)$. However, the requirement above is too stringent, for it forces $\mathcal{P}$ and $\mathcal{Q}$ to be lattices, by Theorem 1 in [**C**]. Instead, we are really interested in the differences between points in $\mathcal{P}$, at least for the purposes of potential energy, so we modify the notion of duality as follows. For a Schwartz function $f \colon \mathbb{R}^n \to \mathbb{R}$ and a periodic configuration $\mathcal{P} = \bigcup_{j=1}^{N}(\Lambda + v_j)$ (where Λ is a lattice), we let

$$\Sigma_f(\mathcal{P}) = \frac{1}{N} \sum_{j,k=1}^{N} \sum_{x \in \Lambda} f(x + v_j - v_k)$$

be the *average pair sum* of f over $\mathcal{P}$. It is also the average over all points $x \in \mathcal{P}$ of $\Sigma_f(x, \mathcal{P}) = \sum_{y \in \mathcal{P}} f(y - x)$, and this interpretation shows that it is independent of the decomposition of $\mathcal{P}$ as $\bigcup_{j=1}^{N}(\Lambda + v_j)$. Note that when f is a radial function, this sum is related to the potential energy by $\Sigma_f(\mathcal{P}) = E_f(\mathcal{P}) + f(0)$, but we do not require f to be radial.

DEFINITION 2.1. We say two periodic configurations $\mathcal{P}$ and $\mathcal{Q}$ in $\mathbb{R}^n$ are *formally dual* to each other if $\Sigma_f(\mathcal{P}) = \delta(\mathcal{P})\Sigma_{\widehat{f}}(\mathcal{Q})$ for every Schwartz function $f \colon \mathbb{R}^n \to \mathbb{R}$.

For a lattice, pair sums reduce to sums over the lattice itself. Thus, two lattices are formally dual if and only if they are actually dual.

We define formal duality only for periodic configurations, although there may be interesting extensions to the aperiodic case. Note also that the formal dual of a configuration needn't be unique. One form of non-uniqueness is obvious: if $\mathcal{Q}$ is a formal dual of $\mathcal{P}$, then so are $\mathcal{Q} + t$ and $-\mathcal{Q} + t$ for all vectors t. However, formal duals are not unique even modulo these transformations. See Remark 3.3 for an example.

REMARK 2.2. If $\mathcal{P}$ and $\mathcal{Q}$ are formally dual as above, then we can prove $\delta(\mathcal{P})\delta(\mathcal{Q}) = 1$ by considering a steep Gaussian $f(x) = \exp(-\pi c|x|^2)$ and letting $c \to \infty$. Therefore the relation of being formally dual is symmetric.

Our notion of formal duality is stronger than another version in the literature (see, for example, the question on p. 185 of [**CS2**]). The other version asks for equality only for radial functions, which is equivalent to a statement about the average theta series. For clarity we call that version radial formal duality:

DEFINITION 2.3. We say two periodic configurations $\mathcal{P}$ and $\mathcal{Q}$ in $\mathbb{R}^n$ are *radially formally dual* to each other if $\Sigma_f(\mathcal{P}) = \delta(\mathcal{P})\Sigma_{\widehat{f}}(\mathcal{Q})$ for every *radial* Schwartz function $f \colon \mathbb{R}^n \to \mathbb{R}$.

If Λ_1 and Λ_2 are distinct lattices in $\mathbb{R}^n$ with the same theta series, then Λ_1 and Λ_2^* are radially formally dual but not dual and hence not formally dual. The most interesting case is when Λ_1 and Λ_2 are not isometric (for example, D_{16}^+ and $E_8 \oplus E_8$), but the simplest case is when Λ_2 is a rotation of Λ_1.

The discrete analogue of radial formal duality has been investigated in the coding theory literature, with several striking examples such as Kerdock and Preparata codes [**HKCSS**].

Radial formal duality is all one needs for studying energy under radial potential functions, but the stronger definition arose in the examples from [**CKS**] and possesses a richer structure theory. For example, Lemma 2.4 below fails for radial formal duality (let $\mathcal{P}$ be $\mathbb{Z}^2$, let $\mathcal{Q}$ be $\mathbb{Z}^2$ rotated by an angle of $\pi/4$, and let ϕ be the diagonal matrix with entries 2 and 1).

We will now transform the notion of formal duality into a more combinatorial definition about subsets in abelian groups, rather than the continuous setting of periodic configurations and potential functions. The first step is the following easy result, which is Lemma 2 in [**CKS**].

LEMMA 2.4. *Let $\mathcal{P}$ and $\mathcal{Q}$ be periodic configurations of $\mathbb{R}^n$ which are formally dual to each other, and let $\phi \in \mathrm{GL}_n(\mathbb{R})$ be an invertible linear transformation of the space. Then $\phi(\mathcal{P})$ and $(\phi^t)^{-1}(\mathcal{Q})$ are formally dual to each other.*

Here ϕ^t is the transpose of the linear transformation ϕ.

PROOF. If f is any Schwartz function, then so is $g = f \circ \phi$, and

$$\widehat{g} = \frac{1}{\det(\phi)} \widehat{f} \circ (\phi^t)^{-1}.$$

Therefore,

$$\begin{aligned}
\Sigma_f\big(\phi(\mathcal{P})\big) = \Sigma_{f \circ \phi}(\mathcal{P}) &= \Sigma_g(\mathcal{P}) \\
&= \delta(\mathcal{P})\, \Sigma_{\widehat{g}}(\mathcal{Q}) \\
&= \delta(\mathcal{P}) \cdot \frac{1}{\det(\phi)} \cdot \Sigma_{\widehat{f} \circ (\phi^t)^{-1}}(\mathcal{Q}) \\
&= \delta\big(\phi(\mathcal{P})\big) \Sigma_{\widehat{f}}\big((\phi^t)^{-1}(\mathcal{Q})\big),
\end{aligned}$$

which shows that $\phi(\mathcal{P})$ and $(\phi^t)^{-1}(\mathcal{Q})$ are formally dual. $\square$

This lemma shows that formal duality is really a property of the underlying abelian groups and cosets, rather than the metric structure or the quadratic forms associated to the underlying lattices of $\mathcal{P}$ and $\mathcal{Q}$. In other words, we may as well assume that the underlying lattice Λ of $\mathcal{P}$ is $\mathbb{Z}^n$, although we will not do so since it would break the notational symmetry between $\mathcal{P}$ and $\mathcal{Q}$.

For further progress in making formal duality more combinatorial, we will need to remove the Fourier transform from the definition. We can do so using Poisson summation, as follows. The statement looks complicated, but it will be an essential tool for simplifying the duality theory.

LEMMA 2.5. *Let $\mathcal{P} = \bigcup_{j=1}^N (\Lambda + v_j)$ and $\mathcal{Q} = \bigcup_{j=1}^M (\Gamma + w_j)$ be periodic configurations with underlying lattices Λ and Γ, respectively. Then $\mathcal{P}$ and $\mathcal{Q}$ are formally*

dual if and only if for all Schwartz functions $f\colon \mathbb{R}^n \to \mathbb{R}$,

$$\sum_{y\in\Lambda^*} \widehat{f}(y) \left| \frac{1}{N} \sum_{j=1}^N e^{2\pi i \langle v_j, y\rangle} \right|^2 = \frac{1}{M} \sum_{j,k=1}^M \sum_{z\in\Gamma} \widehat{f}(z + w_j - w_k).$$

PROOF. Let $v \in \mathbb{R}^n$. By Poisson summation for the function $x \mapsto f(x + v)$,

$$\sum_{x\in\Lambda} f(x+v) = \frac{1}{\operatorname{covol}(\Lambda)} \sum_{y\in\Lambda^*} e^{2\pi i \langle v, y\rangle} \widehat{f}(y).$$

Using this, if $\mathcal{P} = \bigcup_{j=1}^N (\Lambda + v_j)$, then

$$\Sigma_f(\mathcal{P}) = \frac{1}{N} \sum_{j,k=1}^N \sum_{x\in\Lambda} f(x + v_j - v_k)$$

$$= \frac{1}{N\operatorname{covol}(\Lambda)} \sum_{y\in\Lambda^*} \widehat{f}(y) \left| \sum_{j=1}^N e^{2\pi i \langle v_j, y\rangle} \right|^2$$

$$= \delta(\mathcal{P}) \sum_{y\in\Lambda^*} \widehat{f}(y) \left| \frac{1}{N} \sum_{j=1}^N e^{2\pi i \langle v_j, y\rangle} \right|^2.$$

Formal duality holds if and only if this quantity equals

$$\delta(\mathcal{P})\Sigma_{\widehat{f}}(\mathcal{Q}) = \frac{\delta(\mathcal{P})}{M} \sum_{j,k=1}^M \sum_{z\in\Gamma} \widehat{f}(z + w_j - w_k),$$

as desired. □

This lemma has powerful consequences for the cosets of $\mathcal{P}$ in Λ. Recall that for a set A in an abelian group G, we define $A - A = \{x - y \mid x, y \in A\}$.

COROLLARY 2.6. *Let* Λ *and* Γ *be underlying lattices of formally dual configurations* $\mathcal{P}$ *and* $\mathcal{Q}$, *respectively. Then* $\mathcal{P} - \mathcal{P} \subseteq \Gamma^*$ *and* $\mathcal{Q} - \mathcal{Q} \subseteq \Lambda^*$.

PROOF. It is enough to show the latter statement, since the former follows by symmetry. By Lemma 2.5,

$$\sum_{y\in\Lambda^*} \widehat{f}(y) \left| \frac{1}{N} \sum_{j=1}^N e^{2\pi i \langle v_j, y\rangle} \right|^2 = \frac{1}{M} \sum_{j,k=1}^M \sum_{z\in\Gamma} \widehat{f}(z + w_j - w_k)$$

for every Schwartz function f. Since $\widehat{f}$ is an arbitrary Schwartz function, this forces the set $\{z + w_j - w_k \mid 1 \le j, k \le M \text{ and } z \in \Gamma\}$, which is exactly $\mathcal{Q} - \mathcal{Q}$, to be contained in Λ^*. □

The following corollary holds for exactly the same reason.

COROLLARY 2.7. *Let* $\mathcal{P} = \bigcup_{j=1}^N (\Lambda + v_j)$ *and* $\mathcal{Q} = \bigcup_{j=1}^M (\Gamma + w_j)$ *be periodic configurations, such that* $\mathcal{P} - \mathcal{P} \subseteq \Gamma^*$ *and* $\mathcal{Q} - \mathcal{Q} \subseteq \Lambda^*$. *Then* $\mathcal{P}$ *is formally dual to* $\mathcal{Q}$ *if and only if for every* $y \in \Lambda^*$,

$$\left| \frac{1}{N} \sum_{j=1}^N e^{2\pi i \langle v_j, y\rangle} \right|^2 = \frac{1}{M} \cdot \#\{(z, j, k) \mid 1 \le j, k \le M, z \in \Gamma, \text{ and } y = z + w_j - w_k\},$$

i.e., $1/M$ times the number of ways the coset $y + \Gamma$ can be written as a difference of two of the M cosets of Γ in $\mathcal{Q}$.

From now on, we will assume without loss of generality that $0 \in \mathcal{P}$ (and therefore $\Lambda \subseteq \mathcal{P}$), and similarly $0 \in \mathcal{Q}$. We may do so because formal duality is clearly translation-invariant.

Now $\mathcal{P} = \mathcal{P} - 0 \subseteq \mathcal{P} - \mathcal{P} \subseteq \Gamma^*$, so $\mathcal{P}$ can be represented as a subset S of size N in the finite abelian group Γ^*/Λ. Similarly, $\mathcal{Q}$ corresponds to a subset T of M points in Λ^*/Γ. The natural pairing

$$(\Gamma^*/\Lambda) \times (\Lambda^*/\Gamma) \to S^1 \subset \mathbb{C}^*$$

given by

$$(2.1) \qquad \langle x + \Lambda, y + \Gamma \rangle = e^{2\pi i \langle x,y \rangle}$$

identifies the two groups as duals. In other words, we view Λ^*/Γ as the group $\widehat{G}$ of characters on $G := \Gamma^*/\Lambda$, with $\chi \in \widehat{G}$ acting on $g \in G$ via $\chi(g) = \langle g, \chi \rangle$. Note that in (2.1), $\langle \cdot, \cdot \rangle$ denotes both the pairing between G and $\widehat{G}$ and the Euclidean inner product, but the type of the inputs makes the usage unambiguous. We will also canonically identify G with the dual of $\widehat{G}$ and treat the pairing between them as symmetric.

Because $v_1, \ldots, v_N \in \mathcal{P} \subseteq \Gamma^*$, the quantity

$$\left| \frac{1}{N} \sum_{j=1}^{N} e^{2\pi i \langle v_j, y \rangle} \right|^2$$

from Corollary 2.7 only depends on y modulo Γ.

We can now reformulate formal duality as follows. Let the Fourier transform of a function $f \colon G \to \mathbb{C}$ be $\widehat{f} \colon \widehat{G} \to \mathbb{C}$, defined by

$$\widehat{f}(y) = \frac{1}{\sqrt{|G|}} \sum_{x \in G} f(x)\overline{\langle x, y \rangle} = \frac{1}{\sqrt{|G|}} \sum_{x \in G} f(x)y(-x).$$

THEOREM 2.8. *With notation as above, let $\mathcal{P}$ correspond to the translates of Λ by elements of $S = \{v_1, \ldots, v_N\} \subseteq G = \Gamma^*/\Lambda$, and $\mathcal{Q}$ correspond to the translates of Γ by $T = \{w_1, \ldots, w_M\} \subseteq \widehat{G} = \Lambda^*/\Gamma$. Then $\mathcal{P}$ and $\mathcal{Q}$ are formally dual if and only if the following equivalent conditions hold.*

(1) *For every $y \in \widehat{G}$,*

$$\left| \frac{1}{N} \sum_{i=1}^{N} \langle v_i, y \rangle \right|^2 = \frac{1}{M} \cdot \#\{(j,k) \mid 1 \le j, k \le M \text{ and } y = w_j - w_k\}.$$

(2) *For every function $f \colon G \to \mathbb{C}$,*

$$\frac{1}{N^{3/2}} \sum_{j,k=1}^{N} f(v_j - v_k) = \frac{1}{M^{3/2}} \sum_{j,k=1}^{M} \widehat{f}(w_j - w_k).$$

PROOF. The equivalence of statement (1) and formal duality is a mild rephrasing of Corollary 2.7. To see why (1) is equivalent to (2), we first note that

$$f(x) = \frac{1}{\sqrt{|G|}} \sum_{y \in \widehat{G}} \widehat{f}(y)\langle x, y \rangle.$$

We now have

$$
\begin{aligned}
\frac{1}{N^{3/2}} \sum_{j,k=1}^{N} f(v_j - v_k) &= \frac{1}{N^{3/2}} \cdot \frac{1}{\sqrt{|G|}} \sum_{j,k=1}^{N} \sum_{y \in \widehat{G}} \widehat{f}(y) \langle v_j - v_k, y \rangle \\
&= \frac{1}{N^{3/2}} \cdot \frac{1}{\sqrt{|G|}} \sum_{j,k} \sum_{y} \widehat{f}(y) \langle v_j, y \rangle \overline{\langle v_k, y \rangle} \\
&= \frac{1}{N^{3/2}} \cdot \frac{1}{\sqrt{|G|}} \sum_{y} \widehat{f}(y) \sum_{j,k} \langle v_j, y \rangle \overline{\langle v_k, y \rangle} \\
&= \frac{1}{N^{3/2}} \cdot \frac{1}{\sqrt{|G|}} \sum_{y} \widehat{f}(y) \left| \sum_{j} \langle v_j, y \rangle \right|^2 \\
&= \sqrt{\frac{N}{|G|}} \cdot \sum_{y} \widehat{f}(y) \left| \frac{1}{N} \sum_{j} \langle v_j, y \rangle \right|^2.
\end{aligned}
$$

The last expression equals

$$
\frac{1}{M} \sqrt{\frac{N}{|G|}} \sum_{j,k=1}^{M} \widehat{f}(w_j - w_k)
$$

for every f if and only if (1) holds. Thus, we have shown that (1) is equivalent to

$$
(2.2) \qquad \frac{1}{N^{3/2}} \sum_{j,k=1}^{N} f(v_j - v_k) = \frac{1}{M} \sqrt{\frac{N}{|G|}} \sum_{j,k=1}^{M} \widehat{f}(w_j - w_k).
$$

To complete the proof of equivalence, we will show that (1) and (2) each imply $|G| = MN$ (in which case (2.2) is equivalent to (2)).

First, assume (1). If we sum over all $y \in \widehat{G}$ and apply orthogonality of distinct characters on $\widehat{G}$, we find that

$$
\sum_{y \in \widehat{G}} \left| \frac{1}{N} \sum_{i=1}^{N} \langle v_i, y \rangle \right|^2 = \sum_{y \in \widehat{G}} \frac{1}{N^2} \sum_{i=1}^{N} |\langle v_i, y \rangle|^2 = \frac{1}{N^2} N |\widehat{G}|.
$$

Thus, (1) yields

$$
\frac{1}{N^2} N |\widehat{G}| = \frac{1}{M} \cdot M^2,
$$

implying $|G| = |\widehat{G}| = MN$. Assuming (2), we can apply it with f being the characteristic function of the identity in G to obtain

$$
\frac{1}{N^{3/2}} \cdot N = \frac{1}{M^{3/2}} \cdot \frac{1}{\sqrt{|G|}} \cdot M^2,
$$

which again implies $|G| = MN$. $\square$

DEFINITION 2.9. We say that subsets S of a finite abelian group G and T of $\widehat{G}$ are *formally dual* if the following equivalent conditions hold.

(1) For every $y \in \widehat{G}$,

$$\left| \frac{1}{|S|} \sum_{v \in S} \langle v, y \rangle \right|^2 = \frac{1}{|T|} \cdot \#\{(w, w') \in T \times T \,|\, y = w - w'\}.$$

(2) For every function $f \colon G \to \mathbb{C}$,

$$\frac{1}{|S|^{3/2}} \sum_{v, v' \in S} f(v - v') = \frac{1}{|T|^{3/2}} \sum_{w, w' \in T} \widehat{f}(w - w').$$

Thus, Theorem 2.8 reduces formal duality in Euclidean space to the setting of finite abelian groups.

REMARK 2.10. The second criterion in the definition immediately implies that the relation of formal duality is symmetric. However, the first criterion seems to be more useful for concrete calculations, and it is the one we will use in our examples.

3. Examples

The simplest examples of formally dual configurations in $\mathbb{R}^n$ are of course lattices and their duals. These correspond to taking the trivial abelian group $G = \{0\}$, with $S = G$ and $T = \widehat{G} = \{0\}$.

3.1. The TITO configuration. The simplest non-trivial example of a pair of formally dual configurations is the following. Consider the abelian group $G = \mathbb{Z}/4\mathbb{Z}$, and identify $\widehat{G} = \mathbb{Z}/4\mathbb{Z}$ via the pairing $\langle x, y \rangle = e^{2\pi i x y/4}$. Let $S = T = \{0, 1\}$. We check condition (1) of Definition 2.9 as follows for each value of y:

$$y = 0: \quad \left| \frac{1}{2}(1 + 1) \right|^2 = 1 = \frac{1}{2}\#\{(0,0), (1,1)\},$$

$$y = 1: \quad \left| \frac{1}{2}(1 + i) \right|^2 = \frac{1}{2} = \frac{1}{2}\#\{(1,0)\},$$

$$y = 2: \quad \left| \frac{1}{2}(1 - 1) \right|^2 = 0 = \frac{1}{2}\#\{\},$$

$$y = 3: \quad \left| \frac{1}{2}(1 - i) \right|^2 = \frac{1}{2} = \frac{1}{2}\#\{(0,1)\}.$$

Thus, S and T are formally dual to each other. We call this configuration TITO, which stands for "two-in two-out":

$$\cdots \quad \bullet \quad \bullet \quad \circ \quad \circ \quad \bullet \quad \bullet \quad \circ \quad \circ \quad \cdots$$

TITO yields the following formally self-dual configuration in one-dimensional Euclidean space $\mathbb{R}$:

$$\mathcal{P} = \mathcal{Q} = 2\mathbb{Z} \cup (2\mathbb{Z} + 1/2).$$

All of the examples from [**CKS**] described in the introduction are products of copies of $\mathbb{Z}$ and the TITO configuration $\mathcal{P}$, up to linear transformations. For example, it is not hard to check that for odd n we can obtain D_n^+ from the product $\mathcal{P} \times \mathbb{Z}^{n-1}$. (For even n, D_n^+ is a lattice.) Similarly, the putative optimum $\mathcal{P}_6$ in six dimensions can be obtained from $\mathcal{P}^2 \times \mathbb{Z}^4$. These product decompositions imply formal duality, by the following lemma.

LEMMA 3.1. *Let $S_1 \subseteq G_1$ and $T_1 \subseteq \widehat{G_1}$ be formal duals, and let $S_2 \subseteq G_2$ and $T_2 \subseteq \widehat{G_2}$ be formal duals. Then $S_1 \times S_2 \subseteq G_1 \times G_2$ is formally dual to $T_1 \times T_2 \subseteq \widehat{G_1} \times \widehat{G_2}$.*

PROOF. This follows directly from the second criterion in Definition 2.9. (Of course the first criterion also leads to a simple proof.) Setting $G = G_1 \times G_2$, $S = S_1 \times S_2$, and $T = T_1 \times T_2$ and identifying $\widehat{G}$ with $\widehat{G_1} \times \widehat{G_2}$, we must show that every function $f \colon G \to \mathbb{C}$ satisfies

$$\frac{1}{|S|^{3/2}} \sum_{v,v' \in S} f(v - v') = \frac{1}{|T|^{3/2}} \sum_{w,w' \in T} \widehat{f}(w - w').$$

This identity follows immediately from taking the product of the corresponding identities for G_1 and G_2 if there are functions $f_i \colon G_i \to \mathbb{C}$ such that $f(x_1, x_2) = f_1(x_1) f_2(x_2)$ for all $(x_1, x_2) \in G_1 \times G_2$. Such functions span all the functions on $G_1 \times G_2$, which completes the proof. □

3.2. The Gauss sum configurations. We now consider the case $G = (\mathbb{Z}/p\mathbb{Z})^2$ and $\widehat{G} = (\mathbb{Z}/p\mathbb{Z})^2$, with p an odd prime. The pairing is given by

$$\langle (a, b), (c, d) \rangle = \zeta_p^{ac+bd},$$

where $\zeta_p = e^{2\pi i/p}$.

THEOREM 3.2. *For all nonzero elements α and β of $\mathbb{Z}/p\mathbb{Z}$, the subsets $S = \{(\alpha n^2, \beta n) \mid n \in \mathbb{Z}/p\mathbb{Z}\}$ and $T = \{(n, n^2) \mid n \in \mathbb{Z}/p\mathbb{Z}\}$ are formally dual to each other.*

PROOF. Recall that the absolute value squared of the classical Gauss sum $\sum_{n=1}^{p} \zeta_p^{n^2}$ is p. It follows by completing the square that

$$\left| \sum_{n=1}^{p} \zeta_p^{c\alpha n^2 + d\beta n} \right|^2 = \begin{cases} p^2 & \text{if } p \text{ divides } c \text{ and } d, \\ 0 & \text{if } p \text{ divides } c \text{ but not } d, \text{ and} \\ p & \text{if } p \text{ does not divide } c. \end{cases}$$

Thus, to check formal duality using criterion (1) from Definition 2.9, we just need to verify that the system of equations

$$(c, d) = (j - k, j^2 - k^2)$$

has p solutions if $c = d = 0$, no solution if $c = 0, d \neq 0$ and exactly one solution if $c, d \neq 0$. The first two of these statements are obvious. For the last one, note that we may solve $j + k = d/c$, which leads to a unique solution $(j, k) = \left(\frac{1}{2}(\frac{d}{c} + c), \frac{1}{2}(\frac{d}{c} - c) \right)$, since 2 is invertible modulo p. □

REMARK 3.3. Because α and β can vary, the formal dual of a subset is not unique, even modulo translation and automorphisms.

4. Structure theory in the cyclic case

4.1. Basic structure theory. We begin with a few observations on the structure of formally dual sets.

The first basic observation is that if $S \subseteq G$ and $T \subseteq \widehat{G}$ are formally dual, and $x \in G$, $y \in \widehat{G}$, then $S + x$ and $T + y$ are also formally dual (since formal duality only cares about differences of elements).

Let G be a finite abelian group, and H a subgroup of G. Viewing $\widehat{G} = \text{Hom}(G, S^1)$ and $\widehat{H} = \text{Hom}(H, S^1)$, we have a natural restriction map $\phi \colon \widehat{G} \to \widehat{H}$, with kernel the annihilator of H, i.e.,

$$H^{\perp} := \{y \in \widehat{G} \,|\, \langle x, y \rangle = 1 \text{ for all } x \in H\}.$$

Now, if $S \subseteq H$ and $T \subseteq \widehat{H}$ are formally dual subsets, we may regard S as a subset of G and lift T to $\widehat{G}$ using ϕ^{-1}.

LEMMA 4.1. *The subsets $S \subseteq H$ and $T \subseteq \widehat{H}$ are formally dual if and only if $S \subseteq G$ and $\phi^{-1}(T) \subseteq \widehat{G}$ are formally dual.*

PROOF. The easiest way to see this is to use condition (1) of Definition 2.9, with the roles of G and $\widehat{G}$ reversed. It says that $S \subseteq H$ and $T \subseteq \widehat{H}$ are formally dual iff for all $x \in H$,

$$\left| \frac{1}{|T|} \sum_{w \in T} \langle w, x \rangle \right|^2 = \frac{1}{|S|} \cdot \#\{(v, v') \in S \times S \,|\, x = v - v'\}.$$

Under the above transformation from $(H, \widehat{H}, S, T)$ to $(G, \widehat{G}, S, \phi^{-1}(T))$, the right side remains unchanged if $x \in H$, while the left side becomes

$$\left| \frac{1}{(G : H)|T|} \sum_{z \in \phi^{-1}(T)} \langle z, x \rangle \right|^2 = \left| \frac{1}{|T|} \sum_{w \in T} \langle w, x \rangle \right|^2$$

since for every $z \in \widehat{G}$ mapping to $w \in \widehat{H}$ under ϕ, we have $\langle z, x \rangle = \langle w, x \rangle$, and there are exactly $(G : H)$ such z for any w. Thus, for $x \in H$ condition (1) holds for $(G, \widehat{G}, S, \phi^{-1}(T))$ iff it holds for $(H, \widehat{H}, S, T)$.

On the other hand, if $x \notin H$, then

$$\#\{(v, v') \in S \times S \,|\, x = v - v'\} = 0,$$

since $S - S \subseteq H - H = H$. The sum

$$\sum_{z \in \phi^{-1}(T)} \langle z, x \rangle$$

also vanishes: for each $t \in T$, let t_0 be any element of $\phi^{-1}(t)$, and then

$$\sum_{z \in \phi^{-1}(\{t\})} \langle z, x \rangle = \sum_{y \in H^{\perp}} \langle y + t_0, x \rangle = \langle t_0, x \rangle \sum_{y \in H^{\perp}} \langle y, x \rangle = 0,$$

because $y \mapsto \langle y, x \rangle$ is a non-trivial character of $H^{\perp}$, which sums to zero over $H^{\perp}$. This completes the proof of equivalence. $\square$

In fact, this construction is reversible.

LEMMA 4.2. *Let $S \subseteq H \leq G$ be formally dual to $T \subseteq \widehat{G}$. Then T is invariant under addition by any element of $H^{\perp}$, and the image of T under the restriction map ϕ is a formal dual to $S \subseteq H$ in $\widehat{H}$.*

Here $H \leq G$ means H is a subgroup of G.

PROOF. For $y \in \widehat{H}$, define its multiplicity by

$$m(y) = \# \left(\phi^{-1}(y) \cap T \right).$$

Evidently $0 \le m(y) \le (G : H)$ for all $y \in \widehat{H}$. We will begin by refining this to $m(y) \in \{0, (G : H)\}$. Recall that for each $x \in G$,

(4.1) $$\left| \sum_{w \in T} \langle x, w \rangle \right|^2 = \frac{|T|^2}{|S|} \cdot \#\{(v, v') \in S \times S \mid x = v - v'\}.$$

Summing this over all $x \in H$, the left side becomes

$$\sum_{x \in H} \left| \sum_{y \in \widehat{H}} m(y) \langle x, y \rangle \right|^2 = \sum_{x \in H} \sum_{y, y' \in \widehat{H}} m(y) m(y') \langle x, y - y' \rangle.$$

Interchanging the order of summation, we see that this equals

$$|H| \sum_{y, y' \in \widehat{H}} m(y) m(y') \delta_{y, y'} = |H| \sum_{y \in \widehat{H}} m(y)^2.$$

To simplify the right side of (4.1) after summing over $x \in H$, we observe that all differences of the form $v - v'$ are automatically in H. We thus get

$$|H| \sum_{y \in \widehat{H}} m(y)^2 = |T|^2 |S|.$$

Using $|S||T| = |G|$ and $\sum_{y \in \widehat{H}} m(y) = |T|$ and canceling $|H|$, we may rewrite this as

$$\sum_{y \in \widehat{H}} m(y)^2 = (G : H) \sum_{y \in \widehat{H}} m(y).$$

Now for each individual $y \in \widehat{H}$ we have $m(y)^2 \le (G : H) m(y)$, with equality if and only if $m(y) \in \{0, (G : H)\}$. Hence the previous equation is only possible if this is indeed the case for all $y \in \widehat{H}$.

It follows that T is invariant under translation by $H^\perp$, because for each y, $\phi^{-1}(y)$ consists of an $H^\perp$-orbit of size $(G : H)$. Thus, we are in the situation covered by Lemma 4.1, and we conclude that $S \subseteq H$ and $\phi(T) \subseteq \widehat{H}$ are formally dual. $\square$

The above results correspond to producing new formally dual configurations in Euclidean space by taking a smaller underlying lattice. Let us say that S and T are a *primitive* pair of formally dual configurations if S is not contained in a coset of a proper subgroup of G and T is not contained in a coset of a proper subgroup of $\widehat{G}$. In the classification of formal duals, we may restrict to the primitive case.

4.2. The 1-dimensional case. When G is cyclic, we conjecture that there are no primitive formally dual configurations except the trivial example and TITO. We are able to prove the conjecture when $G = \mathbb{Z}/p^2\mathbb{Z}$, with p an odd prime. The same is obviously true for $\mathbb{Z}/p\mathbb{Z}$, since the product of the sizes of the dual configurations would be p. By contrast, Theorem 3.2 shows that there are nontrivial examples in $(\mathbb{Z}/p\mathbb{Z})^2$.

PROPOSITION 4.3. *Let p be an odd prime. Then there are no primitive formally dual configurations in $G = \mathbb{Z}/p^2\mathbb{Z}$ and its dual.*

PROOF. If such configurations exist, then they must both have size p. Let $S = \{v_1, \ldots, v_p\}$ and $T = \{w_1, \ldots, w_p\}$ be formally dual, where we have identified $\widehat{G}$ with $\mathbb{Z}/p^2\mathbb{Z}$ via the pairing $\langle x, y \rangle = \zeta^{xy}$ with $\zeta = e^{2\pi i/p^2}$. We assume without loss of generality that $v_1 = w_1 = 0$.

From the first condition of Definition 2.9, we obtain

$$\left| \sum_{i=1}^{p} \zeta^{yv_i} \right|^2 = p \cdot n_y,$$

where we set $n_y = \#\{(j, k) \mid w_j - w_k = y\}$. That is,

$$p + \sum_{i \neq j} \zeta^{y(v_i - v_j)} = p \cdot n_y.$$

So $Z_y := \sum_{i \neq j} \zeta^{y(v_i - v_j)}$ is the rational integer $p(n_y - 1)$. Now, note that as y ranges over all the numbers modulo p^2 that are coprime to p, the algebraic numbers Z_y are all conjugates of each other. Since they are integers, they are all equal, and so are the numbers n_y. Furthermore, we cannot have $n_y = 0$ for all y coprime to p; otherwise all of $w_1, \ldots, w_p$ would be multiples of p (since $w_1 = 0$) and T would be contained in a subgroup. Thus $n_y \geq 1$, and $Z_y \geq 0$. But their sum

$$\sum_{\gcd(y,p)=1} \sum_{i \neq j} \zeta^{y(v_i - v_j)} = \sum_{i \neq j} \sum_{\gcd(y,p)=1} \zeta^{y(v_i - v_j)}$$

equals zero, because the inner sum is zero for every pair $i \neq j$. (This follows from $\sum_{j=1}^{p^2} \zeta^j = 0$ and $\sum_{j=1}^{p} \zeta^{pj} = 0$.) Therefore $n_y = 1$ for all y, which means the differences $w_i - w_j$ for $i \neq j$ cover all the $p(p-1)$ elements modulo p^2 that are coprime to p exactly once. This is impossible by the following lemma, so we get a contradiction. $\qquad\square$

LEMMA 4.4. *Let p be an odd prime. Then there is no subset S of $\mathbb{Z}/p^2\mathbb{Z}$ whose difference set $\{x - y \mid x, y \in S, \ x \neq y\}$ is the set of elements coprime to p.*

PROOF. Assume there is such a set S. Then the elements of S must be distinct modulo p, since otherwise some difference would be a multiple of p. Without loss of generality $0 \in S$, since we can translate S arbitrarily. We list the elements as

$$x_0 = 0, \quad x_1 = 1 + a_1 p, \quad x_2 = 2 + a_2 p, \quad \ldots, \quad x_{p-1} = (p-1) + a_{p-1} p,$$

where the integers a_i are well defined modulo p. Now, among the differences, the numbers congruent to 1 modulo p are

$$x_1 - x_0 = 1 + a_1 p,$$
$$x_2 - x_1 = 1 + (a_2 - a_1) p,$$
$$\vdots$$
$$x_{p-1} - x_{p-2} = 1 + (a_{p-1} - a_{p-2}) p,$$
$$x_0 - x_{p-1} = p^2 - (p-1) - a_{p-1} p = 1 + (p - 1 - a_{p-1}) p.$$

Since these differences are all distinct modulo p^2, we need $a_1, a_2 - a_1, \ldots, p-1-a_{p-1}$ to be distinct modulo p. Taking their (telescoping) sum, we get

$$p - 1 \equiv 0 + 1 + \cdots + (p-1) = \frac{p(p-1)}{2} \pmod{p},$$

which is impossible for odd p.   □

We thank Gregory Minton for providing the above short proof of the lemma.

5. Non-existence of some formal duals

In this section, we show that some well-known packings do not have formal duals.

5.1. Barlow packings. Recall that the Kepler conjecture was settled by Hales, [**H**] based partially on his work with Ferguson [**HF**]. As a result, the face-centered cubic lattice A_3 gives a densest sphere packing in $\mathbb{R}^3$. It has uncountably many equally dense competitors, the Barlow packings, obtained by layering the densest planar arrangement (i.e., the hexagonal lattice A_2) in different ways. The periodic packings among them are the only periodic packings of maximal density in $\mathbb{R}^3$. The face-centered cubic lattice has a formal dual, namely its dual lattice, and it is natural to ask whether the other periodic Barlow packings have formal duals. Proposition 5.1 shows that they do not.

The periodic Barlow packings can be constructed as follows (see [**CS1**] for more details and a geometric description). Let k be the number of hexagonal layers in a period. The A_2 lattice is spanned by two unit vectors v_1 and v_2, making an angle of $\pi/3$, and the underlying lattice Λ of the Barlow packing is spanned by v_1, v_2, and v_3, where v_3 is a vector of length $k\sqrt{2/3}$ that is orthogonal to v_1 and v_2. In addition to this lattice, we need to specify how much each layer is offset. Let $a_0, \ldots, a_{k-1}$ be elements of $\{0, 1, 2\}$ with $a_j \neq a_{j+1}$ for all j (where we interpret indices modulo k). Then the entire periodic configuration consists of the cosets of Λ by the translation vectors $a_j(v_1 + v_2)/3 + jv_3/k$.

PROPOSITION 5.1. *The only periodic Barlow packing that has a formal dual is the face-centered cubic lattice.*

The face-centered cubic case is when k is a multiple of 3, the sequence $a_0, \ldots, a_{k-1}$ is periodic modulo 3, and $\{a_0, a_1, a_2\} = \{0, 1, 2\}$.

For the proof of Proposition 5.1, consider any periodic Barlow packing, with the notation established above. Transforming to the setting of abelian groups and applying Lemma 4.2, we can let G be the group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ (generated by $(v_1 + v_2)/3$ and v_3/k modulo Λ). The question becomes whether the subset $S = \{(a_j, j) \mid 0 \leq j < k\}$ of G has a formal dual. We identify the dual group $\widehat{G}$ with $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ via the pairing

$$\langle (a, b), (c, d) \rangle = \omega^{ac}\zeta^{bd},$$

where $\omega = e^{2\pi i/3}$ and $\zeta = e^{2\pi i/k}$.

LEMMA 5.2. *If S has a formal dual, then k is a multiple of 3.*

PROOF. Let T be a formal dual of S. If we take $y = (1, 0)$ in

$$\frac{|T|}{|S|^2} \left| \sum_{v \in S} \langle y, v \rangle \right|^2 = \#\{(w, w') \in T : y = w - w'\},$$

we find that

$$\frac{3}{k^2} \left| \sum_{j=0}^{k-1} \omega^{a_j} \right|^2$$

is an integer, which must be 0, 1, 2, or 3. It cannot be 3 because $a_0, \ldots, a_{k-1}$ are not all equal. If it is 1 or 2, then $\left| \sum_{j=0}^{k-1} \omega^{a_j} \right|^2$ is $k^2/3$ or $2k^2/3$ and is also an algebraic integer, so k must be divisible by 3. Finally, if $\sum_{j=0}^{k-1} \omega^{a_j} = 0$, then the polynomial $\sum_{j=0}^{k-1} x^{a_j}$ is divisible by $1 + x + x^2$ in $\mathbb{Z}[x]$, and setting $x = 1$ shows that k is a multiple of 3. □

For the remainder of the proof of Proposition 5.1, suppose S does have a formal dual T. Because k is a multiple of 3, we can replace ω with $\zeta^{k/3}$ and write the condition for formal duality with $y = (r, s)$ as

$$\frac{3}{k^2} \left| \sum_{j=0}^{k-1} \zeta^{r a_j k/3 + sj} \right|^2 = \#\{(w, w') \in T \times T : (r, s) = w - w'\}.$$

Without loss of generality, we can let $T = \{0, t_1, t_2\}$. There are at most six nonzero differences of elements of T, namely $\pm t_1$, $\pm t_2$, and $\pm(t_1 - t_2)$. Thus, there can be at most six nonzero vectors (r, s) for which

$$\sum_{j=0}^{k-1} \zeta^{r a_j k/3 + sj} \neq 0.$$

Our next step is to show that whenever (r, s) satisfies $\sum_j \zeta^{r a_j k/3 + sj} \neq 0$, its second coordinate s must have a large factor in common with k. For example, in the face-centered cubic case s is always divisible by $k/3$, and this divisibility corresponds to the periodicity of $a_0, \ldots, a_{k-1}$ modulo 3.

Let $m = k/3$, and write $\sum_j \zeta^{r a_j m + sj}$ in terms of $\zeta' := \zeta^{\gcd(m,s)}$, which is a primitive root of unity of order $k/\gcd(m, s)$. The automorphisms of $\mathbb{Q}(\zeta')$ are given by $\zeta' \mapsto (\zeta')^u$ with u a unit modulo $k/\gcd(m, s)$. These maps preserve whether $\sum_j \zeta^{r a_j m + sj}$ vanishes, and they amount to multiplying $y = (r, s)$ by u. Note that $us = u's$ in $\mathbb{Z}/k\mathbb{Z}$ iff $u \equiv u' \pmod{k/\gcd(k, s)}$, and $us \neq 0$ if $s \neq 0$.

LEMMA 5.3. *Given positive integers a and b with a dividing b, there exist $\varphi(a)$ units modulo b that are distinct modulo a.*

Here φ denotes the Euler totient function. Lemma 5.3 amounts to the standard fact that the restriction map from $(\mathbb{Z}/b\mathbb{Z})^\times$ to $(\mathbb{Z}/a\mathbb{Z})^\times$ is surjective; we will provide a proof for completeness.

PROOF. Factor b/a as $b'a'$, where a' contains all the prime factors that also divide a and b' contains all those that do not. Then units modulo a are also units modulo aa', and we can use the Chinese remainder theorem to lift them to values that are 1 modulo b' and the same modulo aa'. The result is $\varphi(a)$ units modulo b that are distinct modulo a. □

Given a nonzero element (r, s) for which $\sum_j \zeta^{r a_j m + sj} \neq 0$, we can now apply Lemma 5.3 with $a = k/\gcd(k, s)$ and $b = k/\gcd(m, s)$ to find at least $\varphi\big(k/\gcd(k, s)\big)$ distinct, nonzero elements (ur, us) of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ such that $\sum_j \zeta^{u r a_j m + usj} \neq 0$. Thus, $\varphi\big(k/\gcd(k, s)\big) \leq 6$, which implies $k/\gcd(k, s) \leq 18$.

If $\varphi\big(k/\gcd(k, s)\big) \geq 3$ for some nonzero $(r, s) \in T - T$, then at least three elements of $\{\pm t_1, \pm t_2, \pm(t_1 - t_2)\}$ have the same value of $\gcd(k, s)$ for their second

coordinate s, and it follows that all of them do. Call this common value g. Then every element of T has second coordinate a multiple of g, and $k/g \leq 18$.

The other possibility is that $\varphi\big(k/\gcd(k,s)\big) \leq 2$ for all nonzero $(r,s) \in T - T$. Then $\gcd(k,s) \in \{1,2,3,4,6\}$ for all such (r,s), and the least common multiple of these numbers is 12. Letting g be the greatest common divisor of $\gcd(k,s)$ for all nonzero $(r,s) \in T - T$, we find that every element of T has second coordinate a multiple of g, with $k/g \leq 12$.

Thus, in every case T is contained in the subgroup of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ generated by $(1,0)$ and $(0,g)$, for some g with $k/g \leq 18$. By Lemma 4.2, S must be invariant under the annihilator of this subgroup, which is generated by $(0, k/g)$. In other words, the layers in the Barlow packing are periodic modulo k/g, where $k/g \leq 18$.

This means we can assume without loss of generality that there are at most 18 layers (i.e., $k \leq 18$). Furthermore, we can assume $a_0 = 0$ and $a_1 = 1$. Then there are few enough possibilities to enumerate them by computer, and one can check that the integrality conditions

$$\frac{3}{k^2} \left| \sum_{j=0}^{k-1} \zeta^{ra_j k/3 + sj} \right|^2 \in \mathbb{Z}$$

rule out all cases except the face-centered cubic lattice. This completes the proof of Proposition 5.1.

5.2. The Best packing in $\mathbb{R}^{10}$. The Best packing is the densest known packing in $\mathbb{R}^{10}$. It is a periodic configuration, consisting of 40 translates of a lattice. It can be constructed as the subset of $\mathbb{Z}^{10}$ that reduces modulo 2 to the nonlinear $(10, 40, 4)$ Best binary code (see [**CS2**, p. 140]).

PROPOSITION 5.4. *The Best configuration does not have a formal dual.*

PROOF. Again applying Lemma 4.2, we can assume $G = (\mathbb{Z}/2\mathbb{Z})^{10}$ and $S \subseteq G$ is the Best code. Since $|S| = 40$ does not divide $|G| = 1024$, there cannot be a formal dual. $\qquad\square$

It remains an open question whether the Best packing has a radial formal dual [**CS2**, p. 185]. It seems unlikely that it has one, but radial formal duality does not support the sort of structural analysis we have used to prove Proposition 5.4.

6. Open questions

We conclude with some open questions about formal duality. Formal duality initially arose in the simulations described in [**CKS**], and its occurrence there remains unexplained: although our results in this paper substantially clarify the algebraic foundations of this duality theory, they give no conceptual explanation of why periodic energy minimization ground states in low dimensions seem to exhibit formal duality. That is the most puzzling aspect of the theory.

It would be interesting to classify all formally dual pairs. Is every example derived from the trivial construction, TITO, and the Gauss sum construction by taking products and inflating the group (as in Lemma 4.1)?

TITO feels like a characteristic two relative of the Gauss sum construction, but it occurs in $\mathbb{Z}/4\mathbb{Z}$ rather than $(\mathbb{Z}/2\mathbb{Z})^2$. Is there a unified construction that subsumes TITO and the Gauss sum cases?

Conway and Sloane have given a conjectural list of all the "tight" packings in up to nine dimensions [**CS1**]. Their list is believed to include all the densest periodic packings in these dimensions. Can one analyze which ones have formal duals, perhaps by adapting the proof of Proposition 5.1? Note that the list contains at least a few non-lattice packings with formal duals, namely Λ_5^2, Λ_6^2, and Λ_7^3, as shown in [**CKS**].

Acknowledgments

References

[CK1]   H. Cohn and A. Kumar, *Universally optimal distribution of points on spheres*, J. Amer. Math. Soc. **20** (2007), no. 1, 99–148.

[CK2]   H. Cohn and A. Kumar, *Counterintuitive ground states in soft-core models*, Phys. Rev. E (3) **78** (2008), no. 6, 061113, 7 pp.

[CKS]   H. Cohn, A. Kumar, 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.

[CS1]   J. H. Conway and N. J. A. Sloane, *What are all the best sphere packings in low dimensions?*, Discrete Comput. Geom. **13** (1995), no. 3–4, 383–403.

[CS2]   J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Grundlehren der Mathematischen Wissenschaften **290**, Springer-Verlag, New York, 1999.

[C]   A. Córdoba, *La formule sommatoire de Poisson*, C. R. Acad. Sci. Paris Sér. I Math. **306** (1988), no. 8, 373–376.

[H]   T. C. Hales, *A proof of the Kepler conjecture*, Ann. of Math. (2) **162** (2005), no. 3, 1065–1185.

[HF]   T. C. Hales and S. P. Ferguson, *A formulation of the Kepler conjecture*, Discrete Comput. Geom. **36** (2006), no. 1, 21–69.

[HKCSS] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

[S]   F. H. Stillinger, *Phase transitions in the Gaussian core system*, J. Chem. Phys. **65** (1976), 3968–3974.

MICROSOFT RESEARCH NEW ENGLAND, ONE MEMORIAL DRIVE, CAMBRIDGE, MA 02142
E-mail address: cohn@microsoft.com

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139
E-mail address: abhinav@math.mit.edu

MATHEMATISCHES SEMINAR DER UNIVERSITÄT HAMBURG, BUNDESSTR. 55, D-20146 HAMBURG, GERMANY
E-mail address: Christian.Reiher@uni-hamburg.de

INSTITUTE FOR MATHEMATICS, UNIVERSITY OF ROSTOCK, 18051 ROSTOCK, GERMANY
E-mail address: achill.schuermann@uni-rostock.de