Strongly perfect lattices sandwiched between Barnes-Wall lattices

Sihuang Hu [*], Gabriele Nebe [†]

May 16, 2018

Abstract. New series of 2^{2m}-dimensional universally strongly perfect lattices Λ_I and Γ_J are constructed with

$$2\mathrm{BW}_{2m}^{\#} \subseteq \Gamma_J \subseteq \mathrm{BW}_{2m} \subseteq \Lambda_I \subseteq \mathrm{BW}_{2m}^{\#}.$$

The lattices are found by restricting the spin representations of the automorphism group of the Barnes-Wall lattice to its subgroup $\mathcal{U}_m := \mathcal{C}_m(4_{\mathbf{1}}^H)$. The group $\mathcal{U}_m$ is the Clifford-Weil group associated to the Hermitian self-dual codes over $\mathbb{F}_4$ containing $\mathbf{1}$, so the ring of polynomial invariants of $\mathcal{U}_m$ is spanned by the genus-m complete weight enumerators of such codes. This allows us to show that all the $\mathcal{U}_m$-invariant lattices are universally strongly perfect. We introduce a new construction, $\mathrm{D}^{(\mathrm{cyc})}$, for chains of (extended) cyclic codes to obtain (bounds on) the minimum of the new lattices.

1 Introduction

The famous Barnes-Wall lattices BW_{2m} of dimension 2^{2m} (with $m \in \mathbb{N}$) form an important infinite family of even lattices. They have several constructions allowing to determine discriminant group and minimum

$$\mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m} \cong \mathbb{F}_2^{2^{2m-1}},\ \min(\mathrm{BW}_{2m}) = 2^m,$$

and even the kissing number and the shortest vectors in a very explicit way [4], [5]. Also their automorphism groups

$$\mathcal{G}_{2m} := \mathrm{Aut}(\mathrm{BW}_{2m}) \cong 2_+^{1+4m}.O_{4m}^+(2)$$

are of relevance in various places:

The groups $\mathcal{G}_{2m}$ are maximal finite subgroups of $\mathrm{GL}_{2^{2m}}(\mathbb{Q})$ all of whose invariant lattices are scalar multiples of BW_{2m} and its dual $\mathrm{BW}_{2m}^{\#}$. The lattice BW_{2m} is 2-modular in the sense of [16], i.e. there is a similarity h of norm $1/2$ with $h(\mathrm{BW}_{2m}) = \mathrm{BW}_{2m}^{\#}$. Then h is in the normalize of $\mathcal{G}_{2m}$ in $\mathrm{GL}_{2^{2m}}(\mathbb{Q})$ (see [13]). The group $\mathcal{G}_{2m}.\langle\sqrt{2}h\rangle$ is the real Clifford group (see [14]) whose ring of invariant polynomials is spanned by the genus $2m$ complete weight enumerators of self-dual binary codes. This identification is used in [2] to deduce that all layers of the Barnes-Wall lattices form spherical 6-designs, showing that the Barnes-Wall lattices are universally strongly perfect lattices. In particular BW_{2m} realizes a local maximum of the density function on the space of all similarity classes of 2^{2m}-dimensional lattices (see [19]). In the present paper we construct new infinite series of lattices Λ_I and Γ_J with

$$2\mathrm{BW}_{2m}^{\#} \subseteq \Gamma_J \subseteq \mathrm{BW}_{2m} \subseteq \Lambda_I \subseteq \mathrm{BW}_{2m}^{\#}$$

[*] husihuang@gmail.com, Humboldt fellow supported by the AvH foundation.
[†] nebe@math.rwth-aachen.de

for subsets $I, J \subseteq \{0, \ldots, m\}$ such that $m-i$ is odd and $m-j$ is even for all $i \in I$, $j \in J$. We call them *sandwiched* lattices, as they are sandwiched between two Barnes-Wall lattices. For $m \geq 3$ the densest of these lattices is Λ_{I_0} for $I_0 := \{m-i \mid m \geq i \geq 3, i \text{ odd }\}$, whose minimum is the same as $\min(\mathrm{BW}_{2m})$; in particular these lattices are denser than the Barnes-Wall lattices.

To find these lattices we consider the sandwiched lattices that are invariant under the subgroup

$$\mathcal{C}_m(4^H_{\mathbf{1}}) = 2^{1+4m}_+.\Gamma\mathrm{U}_{2m}(\mathbb{F}_4) =: \mathcal{U}_m \leq \mathcal{G}_{2m}.$$

The group $\mathcal{U}_m$ is the genus-m Clifford-Weil group $\mathcal{C}_m(4^H_{\mathbf{1}})$ associated to the Type of Hermitian self-dual codes over $\mathbb{F}_4$ that contain the all ones vector. As in [2] the invariant theory of this Clifford-Weil group allows to predict that all its invariant lattices are universally strongly perfect (see Section 8 for more details). To parametrize these lattices, we restrict the spin representations $\mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m}$ respectively $\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#}$ of the orthogonal group $O^+_{4m}(\mathbb{F}_2)$ to its subgroup $\Gamma\mathrm{U}_{2m}(\mathbb{F}_4)$. It turns out that these restrictions are both multiplicity free and all their composition factors are absolutely irreducible self-dual modules, Y_k ($k \in \{0, \ldots, m\}$, $m-k$ odd respectively even). Theorem 7.1 lists the $\mathcal{U}_m$-invariant sandwiched lattices. In particular for $m = 2$ we discover a new pair of universally strongly perfect lattices $\Gamma_{\{2\}}$ and $2\Gamma^{\#}_{\{2\}} = \Gamma_{\{0\}}$ in dimension 16 thus adding the first new entry to [19, Tableau 19.1] which was created 20 years ago.

One way to construct BW_{2m} is by applying Construction D to a chain of Reed-Muller codes. The Reed-Muller codes are extended cyclic codes for which the minimum distance is obtained by the well known BCH bound. The main problem of Construction D is that it depends not only on the chain of codes but also on the choice of suitable bases. For chains of (extended) cyclic codes over prime fields, however, there is a unique way, which we call Construction $\mathrm{D}^{(\mathrm{cyc})}$, to define a lattice that is again invariant under the cyclic permutation (see Section 2.3). This construction also yields (lower bounds on) the minimum of the lattices Γ_J and Λ_I (Theorems 5.8 and 7.3).

2 Preliminaries

2.1 Cyclic codes

Let q be a prime power and n some positive integer prime to q. Cyclic codes $\mathcal{C}$ are ideals in the finite ring $\mathcal{M} := \mathbb{F}_q[X]/(X^n - 1)$. We identify $\mathcal{M}$ with $\mathbb{F}_q^n$ using the classes of $1, X, \ldots, X^{n-1}$ as a basis. Then the multiplication by X acts on $\mathcal{M}$ as a cyclic permutation σ. In particular the eigenvalues of σ on $\mathcal{M}$ (or more precisely $\overline{\mathbb{F}_q} \otimes_{\mathbb{F}_q} \mathcal{M} =: \overline{\mathbb{F}_q}\mathcal{M}$) are all n-th roots of unity in the algebraic closure of $\mathbb{F}_q$, say the elements of $\mathcal{Z} := \{\alpha^u \mid 0 \leq u < n\}$ for some primitive n-th root of unity $\alpha \in \overline{\mathbb{F}_q}$.

Based on these data there are (at least) three descriptions of a given cyclic code $\mathcal{C}$.

- The *generator polynomial* $p = p(\mathcal{C})$ which is the monic divisor of $X^n - 1$ such that the classes of $p, Xp, \ldots, X^{d-1}p$ form a basis of $\mathcal{C}$, where d is the degree of $(X^n - 1)/p$.
- The *zero set* $Z(\mathcal{C})$ which is the subset of $\mathcal{Z}$ such that $(c_0, \ldots, c_{n-1}) \in \mathcal{C}$, if and only if $\sum_{i=0}^{n-1} c_i z^i = 0$ for all $z \in Z(\mathcal{C})$.
- The *eigenvalues* $\Theta(\mathcal{C})$ which is the set of eigenvalues of σ in the $\overline{\mathbb{F}_q}[\sigma]$-module $\overline{\mathbb{F}_q}\mathcal{C} \leq \overline{\mathbb{F}_q}\mathcal{M}$.

Clearly we may specify a cyclic code by either of the three data, which are related according to the following remark.

Remark 2.1. $\Theta(C) = \mathcal{Z} \setminus Z(C)$, $Z(C) = \mathcal{Z} \setminus \Theta(C)$, and $Z(C) = \{z \in \mathcal{Z} \mid p(z) = 0\}$ where $p := p(\mathcal{C})$.

One important feature of cyclic codes is the fact that one can read off a lower bound, the so called BCH bound, on the minimum Hamming distance $\mathrm{dist}\,(\mathcal{C})$.

Theorem 2.2. *(see [12, Chapter 7, Theorem 8]) Let $\mathcal{C} \leq \mathbb{F}_q^n$ be a cyclic code. Assume that there is some primitive n-th root of unity $\alpha \in \overline{\mathbb{F}_q}$ and some $b \geq 0$, $n \geq \delta \geq 1$ such that*

$$\{\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}\} \subseteq Z(\mathcal{C}).$$

Then the minimum Hamming distance $\mathrm{dist}\,(\mathcal{C})$ *of $\mathcal{C}$ is at least δ.*

For any ring R the *extended code* of a code $\mathcal{C} \leq R^n$ is defined as the code

$$\{(c_1, \dots, c_n, -\sum_{i=1}^{n} c_i) \mid (c_1, \dots, c_n) \in \mathcal{C}\} \leq R^{n+1}.$$

The projection on the first n coordinates is an isomorphism between the extended code and the code. For cyclic codes, one extends the action of σ to the $n+1$ coordinates by $\sigma(n+1) = n+1$; then the isomorphism above is an $R[\sigma]$-module isomorphism, in particular for codes over fields, the eigenvalues of σ on $\mathcal{C}$ and its extended code coincide.

2.2 Chains of cyclic codes and cyclic codes over chain rings

Let $q = p^f$ be some power of a prime p, $m \in \mathbb{N}$ and $R := GR(p^m, f)$ denote the Galois ring with $R/pR \cong \mathbb{F}_q$ and characteristic p^m. Let $n \in \mathbb{N}$ be not divisible by p. Then the polynomial

$$X^n - 1 = f_1 f_2 \cdots f_s$$

is a product of pairwise distinct monic irreducible polynomials $f_j \in \mathbb{F}_q[X]$. By Hensel's lemma (see also [9] for a more specific reference) there are unique monic irreducible polynomials $F_j \in R[X]$ such that

$$X^n - 1 = F_1 F_2 \cdots F_s \in R[X] \text{ and } F_j \pmod{p} = f_j.$$

Any chain

$$(\mathcal{C}_\star) \; : \; \mathcal{C}_0 = (p_0) \subseteq \mathcal{C}_1 = (p_1) \subseteq \ldots \subseteq \mathcal{C}_{m-1} = (p_{m-1}) \leq \mathbb{F}_q[X]/(X^n - 1) \cong \mathbb{F}_q^n$$

of cyclic codes is given by a sequence of generator polynomials

$$p_{m-1} \mid p_{m-2} \mid \ldots \mid p_1 \mid p_0 \mid (X^n - 1) \in \mathbb{F}_q[X].$$

Let $P_j \in R[X]$ be the monic divisor of $X^n - 1$ that lifts p_j. Then we define the lift of $(\mathcal{C}_\star)$ to be the ideal

$$\widehat{(\mathcal{C}_\star)} := (p^j P_j \mid j = 0, \dots, m-1) \leq R[X]/(X^n - 1) \cong R^n.$$

We can recover the sequence $(\mathcal{C}_\star)$ from $\widehat{(\mathcal{C}_\star)}$ by defining $\widehat{(\mathcal{C}_\star)}_j := \widehat{(\mathcal{C}_\star)} \cap p^j R^n$. Then

$$\mathcal{C}_j = \{(c_1 + pR, \dots, c_n + pR) \mid (p^j c_1, \dots, p^j c_n) \in \widehat{(\mathcal{C}_\star)}_j\} \cong \frac{\widehat{(\mathcal{C}_\star)}_j}{\widehat{(\mathcal{C}_\star)}_{j+1}} \tag{1}$$

Hence we conclude

Remark 2.3. Cyclic codes in R^n are in bijection to the chains of length m of cyclic codes in $\mathbb{F}_q^n$.

As before we denote by σ the cyclic shift induced by multiplication by X on $\mathbb{F}_q[X]/(X^n-1)$ and on $R[X]/(X^n-1)$. Then $\mathbb{F}_q[\sigma] \cong \mathbb{F}_q[X]/(X^n-1)$ is a semisimple algebra.

Lemma 2.4. *Assume that we are given two sequences* $(\mathcal{C}_\star) : (\mathcal{C}_i)_{i=0}^{m-1}$ *and* $(\mathcal{D}_\star) : (\mathcal{D}_i)_{i=0}^{m-1}$ *of cyclic codes such that*

$$\mathcal{C}_i \subseteq \mathcal{D}_i \subseteq \mathcal{C}_{i+1}$$

for all i*. Then*

$$p\widehat{(\mathcal{D}_\star)} \subseteq \widehat{(\mathcal{C}_\star)} \subseteq \widehat{(\mathcal{D}_\star)} \subseteq R^n$$

and for all $j = 0, \dots, m-1$

$$\frac{\widehat{(\mathcal{D}_\star)}_j}{\widehat{(\mathcal{C}_\star)}_j} \cong \frac{\mathcal{D}_j}{\mathcal{C}_j} \oplus \frac{\mathcal{D}_{j+1}}{\mathcal{C}_{j+1}} \oplus \cdots \oplus \frac{\mathcal{D}_{m-1}}{\mathcal{C}_{m-1}}$$

as $\mathbb{F}_q[\sigma]$*-modules.*

Proof. We first note that $p\widehat{(\mathcal{D}_\star)} = \widehat{(\mathcal{D}_\star^{(1)})}$ where $\mathcal{D}_0^{(1)} = \{0\}$ and $\mathcal{D}_i^{(1)} = \mathcal{D}_{i-1}$ for $i = 1, \dots m-1$. As $\mathcal{D}_{i-1} \subseteq \mathcal{C}_i$ we conclude that $p\widehat{(\mathcal{D}_\star)} \subseteq \widehat{(\mathcal{C}_\star)}$. In particular $\widehat{(\mathcal{D}_\star)}/\widehat{(\mathcal{C}_\star)}$ is an $\mathbb{F}_q[\sigma]$-module. As this algebra is semisimple, all modules are semisimple and it is enough to compare composition factors. For $0 \le j < m$ consider the $R[\sigma]$-module epimorphism

$$\varphi_j : p^j R^n \to \mathbb{F}_q^n \text{ defined by } (p^j c_1, \dots, p^j c_n) \mapsto (c_1 + pR, \dots, c_n + pR).$$

The kernel of φ_j is $p^{j+1}R^n$. We get

$$\varphi_j(\widehat{(\mathcal{D}_\star)}_j) = \mathcal{D}_j \text{ and } \varphi_j(\widehat{(\mathcal{C}_\star)}_j) = \mathcal{C}_j.$$

As $p^{j+1}R^n \cap \widehat{(\mathcal{D}_\star)}_j = \widehat{(\mathcal{D}_\star)}_{j+1}$ and $p^{j+1}R^n \cap \widehat{(\mathcal{C}_\star)}_j = \widehat{(\mathcal{C}_\star)}_{j+1}$ the $\mathbb{F}_q[\sigma]$ modules $\widehat{(\mathcal{D}_\star)}_j/\widehat{(\mathcal{C}_\star)}_j$ and $\mathcal{D}_j/\mathcal{C}_j \oplus \widehat{(\mathcal{D}_\star)}_{j+1}/\widehat{(\mathcal{C}_\star)}_{j+1}$ have the same composition factors. So the lemma follows using induction. □

For chains $(\mathcal{C}_\star)$ of extended cyclic codes, we first lift the cyclic codes and then extend the lifted code. The lifted extended code is again denoted by $\widehat{(\mathcal{C}_\star)}$. Then Remark 2.3 and Lemma 2.4 hold accordingly.

2.3 Lattices: Construction $\mathrm{D}^{(\mathrm{cyc})}$

Given a chain of binary codes one may apply Construction D to obtain a lattice with a good bound on its minimum (see [6, Chapter 8, Section 8]). Construction D, however, depends on the choice of a suitable basis and hence might not preserve automorphisms. For chains of cyclic codes and extended cyclic codes we may first apply the methods of Section 2.2 to obtain a cyclic or extended cyclic code over $R = \mathbb{Z}/p^m\mathbb{Z}$ and then apply Construction A to this code. This construction allows to imitate the proof in [3] to obtain good bounds on the minimum of the lattice.

We keep the notation of the previous section, assume that $q = p$ is a prime, so $R = \mathbb{Z}/p^m\mathbb{Z}$, and put N to be one of n (cyclic codes) or $n+1$ (extended cyclic codes). Additionally we fix an orthogonal basis

$$(b_i \mid 1 \le i \le N) \text{ of } \mathbb{R}^N \text{ with } (b_i, b_i) = p^{-m} \text{ for } i = 1, \dots, N.$$

We put $\Omega := \langle b_i \mid 1 \le i \le N \rangle_{\mathbb{Z}}$ to be the lattice spanned by this orthogonal basis and denote by $\Phi : \Omega/p^m\Omega \to R^N$ the canonical isomorphism.

Definition 2.5. Construction $\mathrm{D}^{(\mathrm{cyc})}$ associates to a chain

$$(\mathcal{C}_\star) \ : \ \mathcal{C}_0 \subseteq \mathcal{C}_1 \subseteq \ldots \subseteq \mathcal{C}_{m-1} \subseteq \mathbb{F}_p^N$$

of cyclic codes or extended cyclic codes the lattice

$$\mathcal{L}(\widehat{(\mathcal{C}_\star)}) := \Phi^{-1}(\widehat{(\mathcal{C}_\star)}) = \{\sum_{i=1}^{N} a_i b_i \in \Omega \mid (a_1 + p^m\mathbb{Z}, \ldots, a_N + p^m\mathbb{Z}) \in \widehat{(\mathcal{C}_\star)}\}.$$

The lattice $\mathcal{L}(\widehat{(\mathcal{C}_\star)})$ obtained by construction $\mathrm{D}^{(\mathrm{cyc})}$ satisfies $p^m\Omega \subseteq \mathcal{L}(\widehat{(\mathcal{C}_\star)}) \subseteq \Omega$ and is invariant under the cyclic permutation σ of the basis vectors $(b_i \mid 1 \le i \le N)$.

Lemma 2.6. *Given two sequences $(\mathcal{C}_\star) : \ (\mathcal{C}_i)_{i=0}^{m-1}$ and $(\mathcal{D}_\star) : \ (\mathcal{D}_i)_{i=0}^{m-1}$ of cyclic or extended cyclic codes such that $\mathcal{C}_i \subseteq \mathcal{D}_i \subseteq \mathcal{C}_{i+1}$ for all i. Then we have the following isomorphisms of $\mathbb{F}_p[\sigma]$ modules:*

$$\frac{\mathcal{L}(\widehat{(\mathcal{D}_\star)})}{\mathcal{L}(\widehat{(\mathcal{C}_\star)})} \cong \frac{\widehat{(\mathcal{D}_\star)}}{\widehat{(\mathcal{C}_\star)}} \cong \frac{\mathcal{D}_0}{\mathcal{C}_0} \oplus \frac{\mathcal{D}_1}{\mathcal{C}_1} \oplus \cdots \oplus \frac{\mathcal{D}_{m-1}}{\mathcal{C}_{m-1}}.$$

Proof. Both lattices $\mathcal{L}(\widehat{(\mathcal{D}_\star)})$ and $\mathcal{L}(\widehat{(\mathcal{C}_\star)})$ contain $p^m\Omega$ so

$$\frac{\mathcal{L}(\widehat{(\mathcal{D}_\star)})}{\mathcal{L}(\widehat{(\mathcal{C}_\star)})} \cong \frac{\mathcal{L}(\widehat{(\mathcal{D}_\star)})/p^m\Omega}{\mathcal{L}(\widehat{(\mathcal{C}_\star)})/p^m\Omega} \cong \frac{\widehat{(\mathcal{D}_\star)}}{\widehat{(\mathcal{C}_\star)}}.$$

The second isomorphism is from Lemma 2.4 putting $j = 0$. □

Proposition 2.7. *The determinant of a Gram matrix of $\mathcal{L}(\widehat{(\mathcal{C}_\star)})$ is $\det(\mathcal{L}(\widehat{(\mathcal{C}_\star)})) = p^d$ with*

$$d = mN - 2\sum_{i=0}^{m-1} \dim(\mathcal{C}_i).$$

Proof. Put $L := \mathcal{L}(\widehat{(\mathcal{C}_\star)})$ and for $0 \le j \le m$ put $L_j := \Phi^{-1}(\widehat{(\mathcal{C}_\star)}_j) = L \cap p^j\Omega$. Then clearly all the L_j are σ invariant sublattices of Ω, $L_0 = L$ and $L_m = p^m\Omega$. Furthermore by Equation (1)

$$L_j/L_{j+1} \cong \widehat{(\mathcal{C}_\star)}_j/\widehat{(\mathcal{C}_\star)}_{j+1} \cong \mathcal{C}_j \text{ as } \mathbb{F}_p[\sigma] \text{ modules.}$$

To compute the determinant of L we compute the index

$$|L/p^m\Omega| = \prod_{j=0}^{m-1} |L_j/L_{j+1}| = \prod_{j=0}^{m-1} |\mathcal{C}_j| = p^{\sum_{j=0}^{m-1}\dim(\mathcal{C}_j)}.$$

Therefore we find

$$d = \log_p(\det(L)) = \log_p(\det(p^m\Omega)) - 2\log_p(|L/p^m\Omega|) = mN - 2\sum_{j=0}^{m-1}\dim(\mathcal{C}_j).$$

□

The new Construction $D^{(\mathrm{cyc})}$ allows to prove the same bound for the minimum of the lattice as Construction D. To state this bound for arbitrary primes p recall that the *Euclidean weight* of $c = (c_1, \dots, c_N) \in \mathbb{F}_p^N$ is

$$w_E(c) := \min\{\sum_{i=1}^{N} a_i^2 \mid a_i \in \mathbb{Z}, a_i + p\mathbb{Z} = c_i \text{ for } i = 1, \dots, N\}.$$

Then $\operatorname{dist}_E(\mathcal{C}) := \min\{w_E(c) \mid 0 \neq c \in \mathcal{C}\}$ is the *Euclidean distance* of the code $\mathcal{C} \leq \mathbb{F}_p^N$. Note that $\operatorname{dist}_E(\mathcal{C}) = \operatorname{dist}(\mathcal{C})$ is the usual Hamming distance if $p = 2$ or $p = 3$.

Theorem 2.8. *Let $(\mathcal{C}_\star)$ be as in Definition 2.5. Assume moreover that there is $\gamma \geq 1$ such that $\operatorname{dist}_E(\mathcal{C}_i) \geq p^{2m-2i}/\gamma$ for all $0 \leq i \leq m-1$. Then $\min(\mathcal{L}(\widehat{(\mathcal{C}_\star)})) \geq p^m/\gamma$.*

Proof. We keep the notation of the proof of Proposition 2.7. Let $0 \neq x \in L$ and let j be maximal such that $x \in p^j\Omega$. If $j < m$ then $x \in L_j$ and $x = p^j y = p^j \sum_{i=1}^{N} y_i b_i$ with $y_i \in \mathbb{Z}$ such that

$$0 \neq \overline{y} := (y_1 + p\mathbb{Z}, \dots, y_N + p\mathbb{Z}) \in \mathcal{C}_j.$$

As $\operatorname{dist}_E(\mathcal{C}_j) \geq p^{2m-2j}/\gamma$, we have $\sum_{i=1}^{N} y_i^2 \geq p^{2m-2j}/\gamma$ so

$$(x, x) = p^{2j}(y, y) \geq p^{2j} \frac{p^{2m-2j}}{\gamma}(b_1, b_1) = \frac{p^{2m}}{p^m\gamma} = \frac{p^m}{\gamma}.$$

If $j \geq m$ then $x \in p^m\Omega$, so $(x, x) \geq p^m$. $\square$

3 Setup and some notation

Throughout the rest of the paper we fix $m \in \mathbb{Z}_{>0}$ and consider codes of length 2^{2m} and lattices of dimension 2^{2m}. We index our basis by the elements of $\mathcal{V} := \mathbb{F}_2^{2m}$. In particular binary codes of length 2^{2m} will be considered as subspaces of the space of functions $\mathbb{F}_2^{\mathcal{V}} := \{f : \mathcal{V} \to \mathbb{F}_2\}$. For any $f \in \mathbb{F}_2^{\mathcal{V}}$ the support of f is $\operatorname{supp}(f) := \{v \in \mathcal{V} \mid f(v) \neq 0\}$. If $S = \operatorname{supp}(f)$, then clearly $f = \chi_S$ is the *characteristic function* of $S \subseteq \mathcal{V}$ defined by

$$\chi_S : \mathcal{V} \to \mathbb{F}_2, v \mapsto \begin{cases} 1 & v \in S \\ 0 & v \notin S \end{cases}$$

The affine group $\operatorname{Aff}(\mathcal{V}) := \mathcal{V} : \operatorname{GL}(\mathcal{V})$ acts on $\mathbb{F}_2^{\mathcal{V}}$ by permuting the elements of $\mathcal{V}$. The Reed-Muller codes from Definition 4.1 below are invariant under $\operatorname{Aff}(\mathcal{V})$. This invariance is used to view the Reed-Muller codes as extended cyclic codes. To this aim we fix a "Singer-cycle"

$$\sigma \in \operatorname{GL}(\mathcal{V}) \leq \operatorname{Aff}(\mathcal{V}),$$

i.e. an element of order $2^{2m} - 1$ permuting the non-zero elements of $\mathcal{V}$ transitively. The element σ is not unique, even up to conjugacy in $\operatorname{GL}(\mathcal{V})$. Any such σ gives rise to an identification of $\mathcal{V}$ with the field of 2^{2m} elements. The eigenvalues of the action of σ as an element of $\operatorname{GL}(\mathcal{V})$ are the elements of

$$\{\zeta, \zeta^2, \zeta^4, \dots, \zeta^{2^{2m-1}}\}$$

for a certain primitive $(4^m - 1)$st root of unity $\zeta \in \overline{\mathbb{F}}_2$ which we fix for the rest of the paper.

For later use we will fix a vector space structure of $\mathcal{V}$ over $\mathbb{F}_4$ that is defined by σ. To this aim define $\omega := \zeta^{(4^m-1)/3}$ to be a primitive third root of unity in the algebraic closure of $\mathbb{F}_2$ (i.e. a primitive element of $\mathbb{F}_4$).

Remark 3.1. Let $\eta := \sigma^{(4^m-1)/3} \in \mathrm{GL}(\mathcal{V})$. For $v \in \mathcal{V}$ we put $\omega v := \eta(v)$. This turns $\mathcal{V} \cong \mathbb{F}_2^{2m}$ into an m-dimensional vector space $\mathcal{V}_{\mathbb{F}_4} \cong \mathbb{F}_4^m$ over the field $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$. As σ commutes with η, the element σ acts $\mathbb{F}_4$-linearly on $\mathcal{V}_{\mathbb{F}_4}$, so

$$\sigma \in \mathrm{GL}(\mathcal{V}_{\mathbb{F}_4}) \leq \mathrm{Aff}(\mathcal{V}_{\mathbb{F}4}) \cong \mathbb{F}_4^m : \mathrm{GL}_m(\mathbb{F}_4).$$

Identifying the $\mathbb{F}_4$-space $\mathcal{V}_{\mathbb{F}_4}$ with the ω-eigenspace of η we compute the eigenvalues of σ on $\mathcal{V}_{\mathbb{F}_4} \cong \mathbb{F}_4^m$ as $\zeta, \zeta^4, \ldots, \zeta^{4^{m-1}}$.

The following notation will be used throughout the paper.

Notation 3.2. *(a) Any $0 \leq u \leq 4^m - 1$ has a unique expression as $u = \sum_{i=0}^{2m-1} u_i 2^i$ with $u_i \in \{0, 1\}$. Then the 2-weight of u is*

$$\mathrm{wt}_2(u) := |\{i \in \{0, \ldots, 2m-1\} \mid u_i = 1\}| = \sum_{i=0}^{2m-1} u_i \in \mathbb{Z}_{\geq 0}.$$

We also define

$$O(u) := |\{i \in \{0, \ldots, m-1\} \mid u_{2i+1} = 1\}| \text{ and } E(u) := |\{i \in \{0, \ldots, m-1\} \mid u_{2i} = 1\}|.$$

(b) For $-1 \leq r < 2m$ we put

$$Z_r := \{\zeta^u \mid 0 < u \leq 4^m - 1, \mathrm{wt}_2(u) \leq 2m - 1 - r\}.$$

(c) For $0 \leq r \leq 2m$ let

$$\Theta^{(r)} := \{\zeta^u \mid 0 \leq u \leq 4^m - 1, \mathrm{wt}_2(u) = 2m - r\}.$$

So $\Theta^{(0)} = \Theta^{(2m)} = \{1\}$.

(d) $$M_r := \begin{cases} M_+ := \{0 \leq k \leq m \mid m - k \text{ even }\} & \text{if } r \text{ is even} \\ M_- := \{0 \leq k \leq m \mid m - k \text{ odd }\} & \text{if } r \text{ is odd.} \end{cases}$$

(e) For $0 \leq k \leq m$ we put

$$\Theta_k := \{\zeta^u \mid 0 \leq u \leq 4^m - 1, \ |O(u) - E(u)| = m - k\}.$$

(f) Finally, for $0 \leq r \leq 2m$ and $k \in M_r$, we define

$$\Theta_k^{(r)} := \{\zeta^u \mid 0 \leq u \leq 4^m - 1, \mathrm{wt}_2(u) = 2m - r, |O(u) - E(u)| = m - k\} = \Theta^{(r)} \cap \Theta_k.$$

Obviously $\Theta^{(r)} \cap \Theta_k = \emptyset$ if $k \notin M_r$.

Lemma 3.3. *Let $0 \leq r \leq 2m$ and $0 \leq k \leq m$.*

(a) $|\Theta^{(r)}| = \binom{2m}{r}$.

(b) $|\Theta_k| = \begin{cases} 2\dbinom{2m}{k} & \text{if } k < m \\ \dbinom{2m}{m} - 1 & \text{if } k = m. \end{cases}$

(c) If $k \in M_r$ *we have*

$$|\Theta_k^{(r)}| = \begin{cases} 2\dbinom{m}{(m-r+k)/2}\dbinom{m}{(k+r-m)/2} & \text{if } k < m \\ \dbinom{m}{r/2}^2 & \text{if } m = k \end{cases}$$

where we put $\binom{a}{b} := 0$ *if* $b < 0$.

Proof. (a) is clear and to see (b) let $0 \le u \le 4^m - 1$ be such that $O(u) - E(u) = m - k$. Write $u = \sum_{i=0}^{2m-1} u_i 2^i$ with $u_i \in \{0,1\}$ and define

$$I := \{i \in \{0,\ldots,2m-1\} \mid i \text{ even and } u_i = 1 \text{ or } i \text{ odd and } u_i = 0\}.$$

Then $|I| = E(u) + (m - O(u)) = E(u) - O(u) + m = m - (m-k) = k$. So $X_k := \{u \in \{0,\ldots,4^m-1\} \mid O(u) - E(u) = m - k\}$ is in bijection with the k-element subsets $I \subset \{0,\ldots,2m-1\}$ and hence has $\binom{2m}{k}$ elements. X_k contains 0 and $4^m - 1$ if and only if $k = m$ so $|\Theta_m| = |X_m| - 1$ and $|\Theta_k| = 2|X_k|$ if $k < m$.
(c) follows by a straightforward counting argument. □

4 Reed-Muller codes and related extended cyclic codes

4.1 Binary Reed-Muller codes of length 2^{2m}

Definition 4.1. For $0 \le r \le 2m$ let

$$\mathcal{R}(r,2m) := \langle \chi_{a+\mathcal{U}} \mid a \in \mathcal{V},\ \mathcal{U} \le \mathcal{V} \text{ a subspace of dimension } \dim(\mathcal{U}) = 2m - r\rangle$$

denote the r^{th} order *binary Reed-Muller code* of length 2^{2m}.
To simplify notation we put $\mathcal{R}(-1,2m) := \{0\}$.

Some well known properties of the Reed-Muller codes are collected in the following remark.

Remark 4.2. (a) $\mathbb{F}_2^{2^{2m}} = \mathcal{R}(2m,2m) \supset \mathcal{R}(2m-1,2m) \supset \ldots \supset \mathcal{R}(1,2m) \supset \mathcal{R}(0,2m) = \langle \mathbf{1} \rangle$.

(b) The dimension of $\mathcal{R}(r,2m)$ is $\dim(\mathcal{R}(r,2m)) = \sum_{\ell=0}^{r} \binom{2m}{\ell}$.

(c) The dual code is $\mathcal{R}(r,2m)^\perp = \mathcal{R}(2m-r-1,2m)$.

(d) For the minimum distance we have $\operatorname{dist}(\mathcal{R}(r,2m)) = 2^{2m-r}$ where $0 \le r \le 2m$. Moreover the minimum weight vectors in $\mathcal{R}(r,2m)$ are the elements of

$$\{\chi_{a+\mathcal{U}} \mid a \in \mathcal{V},\ \mathcal{U} \le \mathcal{V},\ \dim(\mathcal{U}) = 2m - r\}.$$

To define a convenient basis of the Reed-Muller codes we fix a basis $(v_1, \ldots, v_{2m})$ of $\mathcal{V}$ and put

$$\mathcal{T}_r := \{\mathcal{U} \leq \mathcal{V} \mid \mathcal{U} = \langle v_i \mid i \in I \rangle_{\mathbb{F}_2} \text{ where } I \subseteq \{1, \ldots, 2m\} \text{ with } |I| = r\}.$$

Then we find

Proposition 4.3. *(cf. [4, p. 51]) For $0 \leq r \leq 2m$ the set*

$$\{\chi_{\mathcal{U}} \mid \mathcal{U} \in \mathcal{T}_s, 2m - r \leq s \leq 2m\}$$

is a basis of $\mathcal{R}(r, 2m)$ and the classes of

$$\{\chi_{\mathcal{U}} \mid \mathcal{U} \in \mathcal{T}_{2m-r}\}$$

form a basis of $\mathcal{R}(r, 2m)/\mathcal{R}(r-1, 2m)$.

The affine group $\mathrm{Aff}(\mathcal{V}) := \mathcal{V} : \mathrm{GL}(\mathcal{V})$ acts on $\mathbb{F}_2^{\mathcal{V}}$ by permuting the elements of $\mathcal{V}$. As affine transformations preserve the set of affine subspaces of a given dimension, the Reed-Muller codes are invariant under $\mathrm{Aff}(\mathcal{V})$. In particular the Singer-cycle σ defined in Section 3 is an automorphism of all the Reed-Muller codes from Definition 4.1 and these codes are extended cyclic codes as given in the following remark.

Remark 4.4. (cf. [12, Chapter 13, Theorem 11]) For $-1 \leq r < 2m$, define $\mathcal{R}(r, 2m)^*$ to be the length $4^m - 1$ binary cyclic code with zeros $Z(\mathcal{R}(r, 2m)^*) = Z_r$ where Z_r is as in Notation 3.2 (b). The extended code of $\mathcal{R}(r, 2m)^*$ is the r^{th} order binary Reed-Muller code $\mathcal{R}(r, 2m)$. Note that $\mathcal{R}(2m, 2m) = \mathbb{F}_2^{2^{2m}}$ is the universe code which is not an extended cyclic code.

Applying Remark 2.1 we obtain the eigenvalues of σ on $\mathcal{R}(r, 2m)/\mathcal{R}(r-1, 2m)$:

Proposition 4.5. *For $0 \leq r \leq 2m$ the eigenvalues of σ on*

$$\mathcal{R}(r, 2m)/\mathcal{R}(r-1, 2m)$$

are exactly the elements in $\Theta^{(r)}$ from Notation 3.2 (c).

4.2 Extended cyclic codes sandwiched between Reed-Muller codes

In this section we construct some new extended cyclic codes that are invariant under $\mathrm{Aff}(\mathcal{V}_{\mathbb{F}_4})$. We use the notation introduced in Section 3.

Definition 4.6. Let $0 \leq r < 2m$ and $I \subset M_r$ be given. Put

$$Z_{r,I} := Z_{r-1} \setminus (\bigcup_{k \in I} \Theta_k^{(r)}).$$

Note that $Z_r \subseteq Z_{r,I} \subseteq Z_{r-1}$. Then let $\mathcal{C}(r, I, 2m)^* \leq \mathbb{F}_2^{2^{2m}-1}$ be the cyclic code with zero set $Z_{r,I}$ and $\mathcal{C}(r, I, 2m) \leq \mathbb{F}_2^{2^{2m}}$ the extended code of $\mathcal{C}(r, I, 2m)^*$. Also we define

$$\mathcal{C}(2m, I, 2m) = \begin{cases} \mathcal{R}(2m-1, 2m) & \text{if } m \notin I \\ \mathcal{R}(2m, 2m) = \mathbb{F}_2^{2^{2m}} & \text{otherwise.} \end{cases}$$

Comparing zero sets we immediately get the following remark.

Remark 4.7. (a) $\mathcal{R}(r-1,2m) \subseteq \mathcal{C}(r,I,2m) \subseteq \mathcal{R}(r,2m)$.

(b) $\mathcal{R}(r-1,2m) = \mathcal{C}(r,\emptyset,2m)$.

(c) $\mathcal{R}(r,2m) = \mathcal{C}(r,M_r,2m)$.

(d) If $I \subseteq J \subseteq M_r$ then $\mathcal{C}(r,I,2m) \subseteq \mathcal{C}(r,J,2m)$.

(e) The eigenvalues of σ on $\mathcal{C}(r,I,2m)/\mathcal{R}(r-1,2m)$ are exactly the elements in $\bigcup_{k\in I} \Theta_k^{(r)}$.

(f) $\dim(\mathcal{C}(r,I,2m)) = \dim(\mathcal{R}(r-1,2m)) + \sum_{k\in I} |\Theta_k^{(r)}| = \sum_{\ell=0}^{r-1} \binom{2m}{\ell} + \sum_{k\in I} |\Theta_k^{(r)}|$ where $|\Theta_k^{(r)}|$ can be obtained from Lemma 3.3 (c).

The next proposition can be obtained from the arguments in Section 7.3 as $\mathrm{Aff}(\mathcal{V}_{\mathbb{F}_4}) \subseteq \mathrm{Aff}(\mathcal{V}) \cap \mathcal{U}_m$ where $\mathcal{U}_m$ is defined in Definition 6.2. It also follows from [1, Theorem 5.5].

Proposition 4.8. *For all $0 \le r \le 2m$ and all $I \subseteq M_r$ the automorphism group of $\mathcal{C}(r,I,2m)$ contains $\mathrm{Aff}(\mathcal{V}_{\mathbb{F}_4})$.*

Applying the BCH bound, we find the following lower bounds on the minimum distance of the codes $\mathcal{C}(r,I,2m)$.

Theorem 4.9. *Let $1 \le r \le 2m-1$ and $I \subseteq M_r$. Then*

$$\mathrm{dist}\,(\mathcal{C}(r,I,2m)) \begin{cases} = 2^{2m-r+1} = \mathrm{dist}\,(\mathcal{R}(r-1,2m)) & \text{if } \{m,m-1,m-2\} \cap I = \emptyset \\ \ge 2^{2m-r} = \mathrm{dist}\,(\mathcal{R}(r,2m)) & \text{if } \{m,m-1\} \cap I \ne \emptyset \\ \ge 3 \cdot 2^{2m-r-1} & \text{if } \{m,m-2\} \cap I = \{m-2\} \end{cases}$$

Proof. Clearly

$$2^{2m-r} = \mathrm{dist}\,(\mathcal{R}(r,2m)) \le \mathrm{dist}\,(\mathcal{C}(r,I,2m)) \le \mathrm{dist}\,(\mathcal{R}(r-1,2m)) = 2^{2m-r+1}.$$

To obtain the minimum distance of $\mathcal{R}(r-1,2m)$ one uses the BCH bound (cf. Theorem 2.2), showing that

$$Z := \{\zeta^u \mid 0 < u < 2^{2m-r+1} - 1\}$$

are in the zero set of $\mathcal{R}(r-1,2m)^*$ as all these exponents u have 2-weight $\le 2m-r$. The zero set of $\mathcal{C}(r,I,2m)^*$ contains all these $\zeta^u \in Z$ with $\mathrm{wt}_2(u) < 2m-r$ and those $\zeta^u \in Z$ with $\mathrm{wt}_2(u) = 2m-r$ such that $|E(u)-O(u)| = m-k$ with $k \notin I$. So let $0 < u < 2^{2m-r+1}-1$ be such that $\mathrm{wt}_2(u) = 2m-r$. Then $u = \sum_{i=0}^{2m-r} u_i 2^i$ with $u_i = 0$ for exactly one i.

If r is odd then one easily concludes that $|O(u)-E(u)| = 1$. So if r is odd and $m-1 \notin I$ then Z is in the zero set of $\mathcal{C}(r,I,2m)^*$, so the BCH bound allows to conclude that $\mathrm{dist}\,(\mathcal{C}(r,I,2m)) = \mathrm{dist}\,(\mathcal{R}(r-1,2m))$.

If r is even, then $|O(u)-E(u)| \in \{0,2\}$, showing again that $Z \subseteq Z(\mathcal{C}(r,I,2m)^*)$ and $\mathrm{dist}\,(\mathcal{C}(r,I,2m)) = \mathrm{dist}\,(\mathcal{R}(r-1,2m))$ if $I \cap \{m,m-2\} = \emptyset$. The minimal u such that $|O(u)-E(u)| = 2$ is $u = 2^{2m-r-1} - 1 + 2^{2m-r} = 3 \cdot 2^{2m-r-1} - 1$ so the BCH bound gives $\mathrm{dist}\,(\mathcal{C}(r,I,2m)) \ge 3 \cdot 2^{2m-r-1}$ if $I \cap \{m,m-2\} = \{m-2\}$. □

5 Unitary invariant sandwiched lattices

5.1 The Barnes-Wall construction

To construct the Barnes-Wall lattice $\mathrm{BW}_{2m} \leq \mathbb{R}^{2^{2m}}$ and related lattices we fix an orthogonal basis

$$(b_v \mid v \in \mathcal{V}) \text{ of } \mathbb{R}^{2^{2m}} \text{ with } (b_v, b_v) = 2^{-m}.$$

We put $\Omega := \langle b_v \mid v \in \mathcal{V}\rangle_{\mathbb{Z}}$ to be the lattice spanned by this orthogonal basis. Then [4] constructs the Barnes-Wall lattices BW_{2m} and its dual $\mathrm{BW}_{2m}^{\#}$ as lattices L with

$$2^m\Omega \subseteq L \subseteq \Omega$$

by scaling the basis of the Reed-Muller codes given in Proposition 4.3.

Definition 5.1. ([4, Theorem 3.1])

$$\mathrm{BW}_{2m} := \langle 2^{\lfloor \frac{2m-r+1}{2} \rfloor} \sum_{v \in \mathcal{U}} b_v \mid \mathcal{U} \in \mathcal{T}_r, r = 0, \ldots, 2m\rangle_{\mathbb{Z}}$$

is the Barnes-Wall lattice of dimension 2^{2m} and its dual lattice is given as

$$\mathrm{BW}_{2m}^{\#} = \langle 2^{\lfloor \frac{2m-r}{2} \rfloor} \sum_{v \in \mathcal{U}} b_v \mid \mathcal{U} \in \mathcal{T}_r, r = 0, \ldots, 2m\rangle_{\mathbb{Z}}.$$

Note that the generators for the lattices in Definition 5.1 form a basis of BW_{2m} and $\mathrm{BW}_{2m}^{\#}$.
The parameters for the Barnes-Wall lattices are

$$\det(\mathrm{BW}_{2m}) = 2^{2^{2m-1}}, \min(\mathrm{BW}_{2m}) = 2^m, \mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m} \cong \mathbb{F}_2^{2^{2m-1}}$$

(see [4] and [5]).

The Barnes-Wall construction in Definition 5.1 is a very specific variant of Construction D applied to the two chains of Reed-Muller codes:

$$\begin{array}{rcccccccl} (\mathcal{R}_{2\star}) & : & \mathcal{R}(0,2m) & \subset & \mathcal{R}(2,2m) & \subset & \ldots & \subset & \mathcal{R}(2m-2,2m) \quad \text{and} \\ (\mathcal{R}_{2\star-1}) & : & \mathcal{R}(1,2m) & \subset & \mathcal{R}(3,2m) & \subset & \ldots & \subset & \mathcal{R}(2m-1,2m). \end{array}$$

Note that Construction D in general depends on the chosen basis adapted to the chain of codes as explained in detail in [10], where the authors compare Construction D and D' with Forney's Code-Formula construction. Their main result is [10, Theorem 1] showing that Construction D and Forney's Code-Formula construction yield the same lattice if and only if the chain of nested binary codes is closed under the Schur product. Only then Construction D does not depend on the choice of the basis.

Warning 5.2. *For $m \geq 4$ then $(\mathcal{R}_{2\star})$ and $(\mathcal{R}_{2\star-1})$ are not closed under the Schur product. So in contrast to many remarks in the literature (e.g. [10, bottom of p. 447]) the lattice constructed by Construction D from these chains of codes will depend on the chosen basis.*

Proof. Recall that the Schur product is a function $\mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ mapping (c, d) to $c * d$ with $(c * d)_i = c_i d_i$. By [12, Section (13.3)] $\mathcal{R}(r, 2m)$ is the set of all vectors f, where $f(v_1^*, \ldots, v_{2m}^*)$ is a Boolean function, which can be written as a polynomial of degree at most r in the symmetric algebra of $\mathcal{V}^*$.

So f is a linear combination of $\prod_{i\in I} v_i^*$ where $I \subseteq \{1,\dots,2m\}$, $|I| \le r$. The Schur product of Boolean functions translates into the product of polynomials subject to the relations ${v_i^*}^2 = v_i^*$ for all i. If $m \ge 4$ then $v_1^*v_2^*v_3^*v_4^*$ and $v_5^*v_6^*v_7^*v_8^*$ are in $\mathcal{R}(4,2m)$ but their product has degree 8, hence does not belong to $\mathcal{R}(6,2m)$, the next member of the chain $(\mathcal{R}_{2\star})$. A similar argument also applies to $(\mathcal{R}_{2\star-1})$, where it is enough to assume $m \ge 3$. $\square$

5.2 Construction $\mathrm{D}^{(\mathrm{cyc})}$ for the Barnes-Wall lattices

By [4, Theorem 3.2] the affine group $\mathrm{Aff}(\mathcal{V})$ acts on the lattice BW_{2m} and its dual lattice $\mathrm{BW}_{2m}^{\#}$ by permuting the basis vectors $(b_v \mid v \in \mathcal{V})$. This action also preserves the Reed-Muller codes and in particular these codes and the lattices BW_{2m} and $\mathrm{BW}_{2m}^{\#}$ are invariant under the cyclic permutation σ. Hence also their quotients $\mathrm{BW}_{2m}/2^m\Omega$ and $\mathrm{BW}_{2m}^{\#}/2^m\Omega$ are invariant under σ. As the sums of the coefficients in the given basis vectors of BW_{2m} and $\mathrm{BW}_{2m}^{\#}$ sum up to a multiple of 2^m these are extended cyclic codes in $\Omega/2^m\Omega \cong (\mathbb{Z}/2^m\mathbb{Z})^{2^{2m}}$. In the notation of Section 2.2 Remark 2.3 hence tells us

$$\mathrm{BW}_{2m}/2^m\Omega \cong \widehat{(\mathcal{R}_{2\star})} \text{ and } \mathrm{BW}_{2m}^{\#}/2^m\Omega \cong \widehat{(\mathcal{R}_{2\star-1})}.$$

Remark 5.3. $\mathrm{BW}_{2m} = \mathcal{L}(\widehat{(\mathcal{R}_{2\star})})$ and $\mathrm{BW}_{2m}^{\#} = \mathcal{L}(\widehat{(\mathcal{R}_{2\star-1})})$ are the lattices obtained by Construction $\mathrm{D}^{(\mathrm{cyc})}$ from the two chains of Reed-Muller codes above.

Proposition 5.4. *As $\mathbb{F}_2[\sigma]$-modules we have*

$$\mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m} \cong \bigoplus_{r=0}^{m-1} \mathcal{R}(2r+1,2m)/\mathcal{R}(2r,2m)$$

and

$$\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#} \cong \mathcal{R}(0,2m) \oplus \bigoplus_{r=1}^{m} \mathcal{R}(2r,2m)/\mathcal{R}(2r-1,2m).$$

The eigenvalues of σ on $\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#}$ are the elements of

$$\Theta^{(+)} := \{\zeta^u \mid 0 \le u < 2^{2m}-1 \text{ of even 2-weight }\} = \bigcup_{r=1}^{m} \Theta^{(2r)}$$

where $\zeta^0 = 1$ occurs with multiplicity 2 (and the others with multiplicity 1) in $\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#}$ and the one on $\mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m}$ are the elements of

$$\Theta^{(-)} := \{\zeta^u \mid 0 \le u < 2^{2m}-1 \text{ of odd 2-weight }\} = \bigcup_{r=1}^{m} \Theta^{(2r-1)}$$

each occurring with multiplicity 1.

Proof. The isomorphism of $\mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m}$ follows directly by applying Lemma 2.6. With a variant of this lemma we may also see the isomorphism of $\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#}$, but this may be also seen from the following consideration: We have $\Omega/2\Omega \cong \mathcal{R}(2m,2m) = \mathbb{F}_2^{2^{2m}}$ as $\mathbb{F}_2[\sigma]$-modules. As $\mathbb{F}_2[\sigma]$ is semisimple, it is enough to compare composition factors so the chain of Reed-Muller codes in Remark 4.2 (a) shows that

$$\Omega/2\Omega \cong \bigoplus_{r=0}^{2m} \mathcal{R}(r,2m)/\mathcal{R}(r-1,2m)$$

(note that $\mathcal{R}(-1,2m)=\{0\}$). Now $\mathrm{BW}_{2m}^{\#}$ and Ω are lattices in the same $\mathbb{Q}[\sigma]$-module, so $\mathrm{BW}_{2m}^{\#}/2\mathrm{BW}_{2m}^{\#}$ and $\Omega/2\Omega$ have the same composition factors (see [17, Theorem 32]), therefore

$$\mathrm{BW}_{2m}^{\#}/2\mathrm{BW}_{2m}^{\#} \cong \mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m} \oplus \mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#} \cong \bigoplus_{r=0}^{2m} \mathcal{R}(r,2m)/\mathcal{R}(r-1,2m)$$

so $\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#} \cong \mathcal{R}(0,2m) \oplus \bigoplus_{r=1}^{m} \mathcal{R}(2r,2m)/\mathcal{R}(2r-1,2m)$. The eigenvalues are obtained from Proposition 4.5. □

5.3 Admissible sandwiched lattices

Definition 5.5. A σ-invariant lattice Γ with $2\mathrm{BW}_{2m}^{\#} \subseteq \Gamma \subseteq \mathrm{BW}_{2m}$ is said to be *admissible*, if either 1 does not occur as an eigenvalue of σ on $\Gamma/2\mathrm{BW}_{2m}^{\#}$ or it occurs with multiplicity 2. Let

$$\mathcal{L}_+ := \{\Gamma \mid 2\mathrm{BW}_{2m}^{\#} \subseteq \Gamma \subseteq \mathrm{BW}_{2m}, \sigma(\Gamma)=\Gamma, \Gamma \text{ admissible}\}$$

and

$$\mathcal{L}_- := \{\Lambda \mid \mathrm{BW}_{2m} \subseteq \Lambda \subseteq \mathrm{BW}_{2m}^{\#}, \sigma(\Lambda)=\Lambda\}$$

denote the set of σ-invariant *admissible sandwiched lattices*.

By definition, the admissible sandwiched lattices are in bijection with the monic factors in $\mathbb{F}_2[X]$ of the minimal polynomial of the action of σ on $\mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m}$ and $\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#}$, so by Proposition 5.4 with the subsets of $\Theta^{(-)}$ resp. $\Theta^{(+)}$ that are closed under squaring:

Proposition 5.6. *(a) Let $S \subseteq \Theta^{(+)}$ be a Frobenius-invariant subset, i.e. $s \in S$ if and only if $s^2 \in S$. Then there is a unique lattice $\Gamma \in \mathcal{L}_+$ such that the characteristic polynomial of the action of σ on $\Gamma/2\mathrm{BW}_{2m}^{\#}$ is $\prod_{s\in S}(X-s) \in \mathbb{F}_2[X]$ if $1 \notin S$ respectively $(X-1)\prod_{s\in S}(X-s) \in \mathbb{F}_2[X]$ if $1 \in S$.*

(b) Let $S \subseteq \Theta^{(-)}$ be a Frobenius-invariant subset, i.e. $s \in S$ if and only if $s^2 \in S$. Then there is a unique lattice $\Lambda \in \mathcal{L}_-$ such that the characteristic polynomial of the action of σ on Λ/BW_{2m} is $\prod_{s\in S}(X-s) \in \mathbb{F}_2[X]$.

5.4 Unitary invariant sandwiched lattices

Recall the definition of M_+ and M_- in Notation 3.2. For proper subsets $\emptyset \neq I \subset M_-$ or $\emptyset \neq J \subset M_+$ we put

$$\begin{array}{llllllllll}
(\mathcal{C}_{\star I}) & : & \mathcal{C}(1,I,2m) & \subseteq & \mathcal{C}(3,I,2m) & \subseteq & \ldots & \subseteq & \mathcal{C}(2m-1,I,2m) & \text{if } I \subseteq M_-, \\
(\mathcal{C}_{\star J}) & : & \mathcal{C}(0,J,2m) & \subseteq & \mathcal{C}(2,J,2m) & \subseteq & \ldots & \subseteq & \mathcal{C}(2m-2,J,2m) & \text{if } m \in J \subseteq M_+, \\
(\mathcal{C}_{\star J}) & : & \mathcal{C}(2,J,2m) & \subseteq & \mathcal{C}(4,J,2m) & \subseteq & \ldots & \subseteq & \mathcal{C}(2m,J,2m) & \text{if } m \notin J \subseteq M_+.
\end{array}$$

Note that for $J \subseteq M_+$ we have $\mathcal{C}(2m,J,2m)=\mathcal{R}(2m,2m)=\mathbb{F}_2^{2^{2m}}$ if $m \in J$ and $\mathcal{C}(0,J,2m)=\{0\}$ if $m \notin J$.

Remark 5.7. We will see in Section 7.3 that the lattices $\mathcal{L}(\widehat{(\mathcal{C}_{\star I})})$ and $\mathcal{L}(\widehat{(\mathcal{C}_{\star J})})$ constructed from these chains of extended cyclic codes with Construction $\mathrm{D}^{(\mathrm{cyc})}$ are invariant under the Clifford-Weil group

$$\mathcal{U}_m = \mathcal{C}_m(4^H_{\mathbf{1}}) \cong 2_+^{1+4m} : \Gamma\mathrm{U}_{2m}(\mathbb{F}_4)$$

associated to the Type of Hermitian self-dual codes over $\mathbb{F}_4$ that contain the all ones vector (see [15, Proposition 7.3.1]). Therefore we call the lattices $\mathcal{L}(\widehat{(\mathcal{C}_{\star I})})$ and $\mathcal{L}(\widehat{(\mathcal{C}_{\star J})})$, obtained by applying Construction $\mathrm{D}^{(\mathrm{cyc})}$ to the chain of codes $(\mathcal{C}_{\star I})$ and $(\mathcal{C}_{\star J})$ above *unitary invariant sandwiched lattices.*

Theorem 5.8. *(a) If $\emptyset \neq I \subset M_-$ then $\mathcal{L}(\widehat{(\mathcal{C}_{\star I})}) \in \mathcal{L}_-$ and the eigenvalues of σ on $\mathcal{L}(\widehat{(\mathcal{C}_{\star I})})/\mathrm{BW}_{2m}$ are the elements of $\bigcup_{k\in I}\Theta_k$. We get*

$$\log_2(\det(\mathcal{L}(\widehat{(\mathcal{C}_{\star I})}))) = 2^{2m-1} - 4\sum_{k\in I}\binom{2m}{k}.$$

If $m-1 \notin I$, then

$$\min(\mathcal{L}(\widehat{(\mathcal{C}_{\star I})}) = \min(\mathrm{BW}_{2m}) = 2^m.$$

(b) For $\emptyset \neq J \subset M_+$ with $m \in J$ then $\mathcal{L}(\widehat{(\mathcal{C}_{\star J})}) \in \mathcal{L}_+$ and the eigenvalues of σ on $\mathcal{L}(\widehat{(\mathcal{C}_{\star J})})/2\mathrm{BW}_{2m}^{\#}$ are the elements of $\bigcup_{k\in J}\Theta_k$. We get

$$\log_2(\det(\mathcal{L}(\widehat{(\mathcal{C}_{\star J})}))) = 2^{2m-1} + 4\sum_{k\in M_+\setminus J}\binom{2m}{k}.$$

(c) For $\emptyset \neq J \subset M_+$ with $m \notin J$ then $2\mathcal{L}(\widehat{(\mathcal{C}_{\star J})}) \in \mathcal{L}_+$ and the eigenvalues of σ on $2\mathcal{L}(\widehat{(\mathcal{C}_{\star J})})/2\mathrm{BW}_{2m}^{\#}$ are the elements of $\bigcup_{k\in J}\Theta_k$. We get

$$\log_2(\det(2\mathcal{L}(\widehat{(\mathcal{C}_{\star J})}))) = 2^{2m-1} + 4\sum_{m\neq k\in M_+\setminus J}\binom{2m}{k} + 2\binom{2m}{m}.$$

If, furthermore, $m-2 \notin J$ then

$$\min(2\mathcal{L}(\widehat{(\mathcal{C}_{\star J})}) = \min(2\mathrm{BW}_{2m}^{\#}) = 2^{m+1}.$$

Proof. Here we only present the proof of (a), as (b) and (c) can be proved very similarly. For (a), from Remark 5.3 we know that $\mathrm{BW}_{2m} = \mathcal{L}(\widehat{(\mathcal{R}_{2\star})})$. Note that the sequences $(\mathcal{C}_{\star I})$ and $(\mathcal{R}_{2\star})$ satisfy the condition of Lemma 2.6. Hence

$$\frac{\mathcal{L}(\widehat{(\mathcal{C}_{\star I})})}{\mathrm{BW}_{2m}} \cong \frac{\mathcal{C}(1,I,2m)}{\mathcal{R}(0,2m)} \oplus \frac{\mathcal{C}(3,I,2m)}{\mathcal{R}(2,2m)} \oplus \cdots \oplus \frac{\mathcal{C}(2m-1,I,2m)}{\mathcal{R}(2m-2,2m)}$$

as $\mathbb{F}_2[\sigma]$-modules. By (e) of Remark 4.7 it follows that the eigenvalues of σ on $\mathcal{L}(\widehat{(\mathcal{C}_{\star I})})/\mathrm{BW}_{2m}$ are the elements of $\bigcup_{k\in I}\Theta_k$. Now the determinant follows directly by Lemma 3.3. As $\mathcal{L}(\widehat{(\mathcal{C}_{\star I})}) \supseteq \mathrm{BW}_{2m}$, we have $\min(\mathcal{L}(\widehat{(\mathcal{C}_{\star I})}) \leq \min(\mathrm{BW}_{2m}) = 2^m$. If $m-1 \notin I$, then by Theorems 2.8 and 4.9, $\min(\mathcal{L}(\widehat{(\mathcal{C}_{\star I})}) \geq 2^m$. This concludes our proof. $\square$

6 Automorphism groups

6.1 The automorphism group of the Barnes-Wall lattices

The automorphism groups of the Barnes-Wall lattices have been described by Broué and Enguehard and independently in a series of papers by Barnes, Wall, Bolt, and Room.

Theorem 6.1. *([5], [20, Theorem 3.2])* $\mathcal{G}_{2m} := \mathrm{Aut}(\mathrm{BW}_{2m}) = 2_+^{1+4m}.O_{4m}^+(2)$.

Here $O_{4m}^+(2)$ is the orthogonal group of a quadratic form q of dimension $4m$ over $\mathbb{F}_2$ and Witt defect 0. Let $\mathcal{E}_{2m} \cong 2_+^{1+4m} \leq \mathcal{G}_{2m}$ denote the maximal normal 2-subgroup of $\mathcal{G}_{2m}$. Then $Z := Z(\mathcal{E}_{2m}) \cong C_2$ and

$$q : \mathcal{E}_{2m}/Z \to Z, xZ \mapsto x^2$$

can be viewed as the $O_{4m}^+(2)$-invariant quadratic form. The affine group $\mathrm{Aff}(\mathcal{V})$ acts as orthogonal mappings on $\mathbb{R}^{2^{2m}}$ by permuting the basis vectors $(b_v \mid v \in \mathcal{V})$. This action stabilizes the Barnes-Wall lattice, so $\mathrm{Aff}(\mathcal{V}) \leq \mathcal{G}_{2m}$. In fact this embedding is made explicit in [4, Lemma 3.2]. The additive group of $\mathcal{V}$ can be seen as a maximal isotropic subgroup $\mathbb{F}_2^{2m} \leq \mathcal{E}_{2m}$ with respect to the quadratic form q from above and $\mathrm{GL}(\mathcal{V})$ is its stabilizer in the orthogonal group of q. In particular we obtain an explicit elements σ and $\eta = \sigma^{(4^m-1)/3}$ (from Remark 3.1) in $\mathcal{G}_{2m}$.

Definition 6.2. Define $\mathcal{U}_m \leq \mathcal{G}_{2m}$ to be the normaliser in $\mathcal{G}_{2m}$ of $\mathcal{E}_{2m} : \langle \eta \rangle$.

Note that η defines an $\mathbb{F}_4$-linear structure on $\mathbb{F}_2^{4m}$ (similar as in Remark 3.1) turning the natural quadratic $O_{4m}^+(2)$-module into a Hermitian space over $\mathbb{F}_4$. Then $\mathcal{U}_m \cong \mathcal{E}_{2m}.\Gamma\mathrm{U}_{2m}(\mathbb{F}_4)$ is the extension of $\mathcal{E}_{2m}$ by the semi-linear unitary group $\Gamma\mathrm{U}_{2m}(\mathbb{F}_4)$ of this Hermitian space. Intersecting the subgroup $\mathrm{Aff}(\mathcal{V})$ of $\mathcal{G}_{2m}$ with $\mathcal{U}_m$ we find that $\mathrm{Aff}(\mathcal{V}_{\mathbb{F}_4}) \leq \mathcal{U}_m$.

One name for $\mathcal{G}_{2m}$ is Clifford collineation group, because the modules

$$\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#} \cong \mathbb{F}_2^{2^{2m-1}} \text{ and } \mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m} \cong \mathbb{F}_2^{2^{2m-1}}$$

are simple modules for the even Clifford algebra. In particular $\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#}$ and $\mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m}$ are simple $\mathbb{F}_2\mathcal{G}_{2m}$-modules (called a spin representation) having $\mathcal{E}_{2m}$ in their kernel. So $\mathcal{E}_{2m}$ is in the automorphism group of every sandwiched lattice $L \in \mathcal{L}_+ \cup \mathcal{L}_-$. Our aim is to construct all admissible sandwiched lattices L that are invariant under $\mathcal{U}_m$. By [18, Theorem 1.3 (A2)] these lattices L are universally strongly perfect as will be explained in Section 8 below. To describe the lattices we need to restrict the spin representation of the orthogonal group $O_{4m}^+(2)$ to its subgroup $\Gamma\mathrm{U}_{2m}(\mathbb{F}_4)$ which is the topic of the next paragraph.

6.2 The spin representations of the orthogonal group.

The results of this section might be well known, but we did not find them explicitly in the literature. We follow the exposition of the textbook [8], in particular [8, Chapter 20], and thank Jan Frahm for helpful hints. To avoid extra complications we restrict to the relevant case and only consider the algebraic group $G := O_{4m}^+$. This is the automorphism group of a split quadratic space Q of dimension $4m$. The Clifford algebra $C(Q)$ is the split central simple algebra of dimension 2^{4m} and G acts on $C(Q)$ as algebra automorphisms preserving the even subalgebra $C_0(Q)$. This action gives rise to a (projective) representation of G on the simple $C(Q)$-module V of dimension 2^{2m} which is in fact a linear representation of the spin group Spin_{4m} and decomposes as the direct sum of two non-isomorphic absolutely irreducible representations

$$V = V_+ \oplus V_-$$

called the even and odd spin representations of G each of dimension 2^{2m-1} (see [8, Proposition 20.15]).

[8, Proposition 20.15] analyses the modules V_+ and V_- and computes the weights occurring in these modules. This allows to find the decomposition of the restrictions of the spin representations to the general linear unitary group $U_{2m} \leq \mathrm{SO}^+_{4m}$. To state the result let χ be the linear character of a suitable covering group of U_{2m} defined by $\chi(g) := (\det(g))^{1/2}$ and

$$\Delta = \Delta_+ + \Delta_- : \mathrm{Spin}_{4m} \to \mathrm{GL}(V)$$

denote the spin representations of SO^+_{4m}.

Theorem 6.3. *The restriction of $\chi \otimes \Delta$ is a linear representation of U_{2m} with*

$$\chi \otimes \Delta \cong \bigoplus_{k=0}^{2m} \Lambda^k(W)$$

where W denotes the natural U_{2m}-module. In this decomposition

$$\chi \otimes \Delta_+ \cong \bigoplus_{k=0}^{m} \Lambda^{2k}(W) \text{ and } \chi \otimes \Delta_- \cong \bigoplus_{k=1}^{m} \Lambda^{2k-1}(W).$$

Proof. The weight lattice of the Lie algebra so_{4m} is the dual lattice $D^{\#}_{2m}$ of the even sublattice of the standard lattice. So the weights are of the form

$$(k_1, \dots, k_{2m}) \in \mathbb{Z}^{2m} \cup (\frac{1}{2} + \mathbb{Z})^{2m}.$$

The proof of [8, Proposition 20.15] exhibits explicit weight vectors of the spin representation Δ for all 2^{2m} weights $(\pm\frac{1}{2}, \dots, \pm\frac{1}{2})$. A maximal torus in the subgroup U_{2m} of SO^+_{4m} has the same rank, so all these weights are distinct when restricted to the subalgebra. The weight of χ is $(\frac{1}{2}, \dots, \frac{1}{2})$ and so the weights occurring in the restriction of $\chi \otimes \Delta$ to U_{2m} are exactly the orbits under the symmetric group S_{2m} of

$$w_k := (\underbrace{1, \dots, 1}_{k}, \underbrace{0, \dots, 0}_{2m-k}) \text{ for } k = 0, 1, \dots, 2m$$

where the w_k for even k occur in $\chi \otimes \Delta_+$ and those for odd k in $\chi \otimes \Delta_-$. As w_k is the highest weight of the representation $\Lambda^k(W)$ the result follows. □

We now apply this result that is true for algebraic groups to our special situation by restricting the representations to the finite groups of Lie type $O^+_{4m}(\mathbb{F}_2) \geq U_{2m}(\mathbb{F}_4)$. In abuse of notation we denote by V_+ and V_- the restriction of the even and odd spin representations to $O^+_{4m}(\mathbb{F}_2)$. These are linear representations of this finite group. Also $\det^{-1/2} = \det : U_{2m}(\mathbb{F}_4) \to \mathbb{F}_4^*$ is a well defined linear representation. We put $W \cong \mathbb{F}_4^{2m}$ the natural $U_{2m}(\mathbb{F}_4)$ module.

Corollary 6.4. *The restriction of V_+ (resp. V_-) to the general unitary group is isomorphic to*

$$(V_+)_{|U_{2m}(\mathbb{F}_4)} \cong \bigoplus_{k=0}^{m} \det \otimes \Lambda^{2k}(W) \textit{ resp. } (V_-)_{|U_{2m}(\mathbb{F}_4)} \cong \bigoplus_{k=1}^{m} \det \otimes \Lambda^{2k-1}(W)$$

To simplify notation we denote by

$$W_k := \det \otimes \Lambda^k(W).$$

Remark 6.5. The semi-linear unitary group $\Gamma\mathrm{U}_{2m}(\mathbb{F}_4) = U_{2m}(\mathbb{F}_4) : 2$ is the extension of the full unitary group $U_{2m}(\mathbb{F}_4)$ by the Galois group of $\mathbb{F}_4$ over $\mathbb{F}_2$. The latter interchanges the two modules W_k and W_{2m-k} and fixes W_m. For $0 \leq k \leq m-1$ the $\mathbb{F}_2\Gamma\mathrm{U}_{2m}(\mathbb{F}_4)$ modules

$$Y_k \text{ with } (Y_k)_{|U_{2m}(\mathbb{F}_4)} = W_k \oplus W_{2m-k} \text{ and } Y_m \text{ with } (Y_m)_{|U_{2m}(\mathbb{F}_4)} = W_m$$

are self-dual, absolutely irreducible, $\mathbb{F}_2\Gamma\mathrm{U}_{2m}(\mathbb{F}_4)$-modules of dimension

$$d_k := \dim(Y_k) = 2\binom{2m}{k} (0 \leq k \leq m-1) \text{ and } d_m := \dim(Y_m) = \binom{2m}{m}.$$

6.3 The action of σ on W_k

The element σ from Section 3 is an element of $\mathrm{GL}_m(\mathbb{F}_4) \leq \mathrm{Aff}(\mathcal{V}_{\mathbb{F}_4})$. The natural $U_{2m}(\mathbb{F}_4)$-module then can be realized as ω-eigenspace of η on the natural $O_{4m}(\mathbb{F}_2)$-module and $\mathrm{GL}(\mathcal{V}_{\mathbb{F}_4})$ is the stabilizer in $U_{2m}(\mathbb{F}_4)$ of a maximal isotropic subspace. More precisely we have the embedding

$$\mathrm{GL}(\mathcal{V}_{\mathbb{F}_4}) \to U_{2m}(\mathbb{F}_4), g \mapsto \mathrm{diag}(g, (g^{[2]})^{-1})$$

where $g^{[2]}$ is the matrix obtained by applying the Frobenius automorphism $x \mapsto x^2$ to all entries of g. So by Remark 3.1 the eigenvalues of σ on the natural $U_{2m}(\mathbb{F}_4)$-module W are

$$\zeta, \zeta^4, \ldots, \zeta^{4^{m-1}}, \zeta^{-2}, \zeta^{-8}, \ldots, \zeta^{-2^{2m-1}}$$

and the determinant of σ on W is $\omega\omega^{-2} = \omega^{-1}$ as $\omega = \zeta\zeta^4 \cdots \zeta^{4^{m-1}} = \zeta^{(4^m-1)/3}$.

Lemma 6.6. *For $0 \leq k \leq 2m$ the eigenvalues of $\sigma \in U_{2m}(\mathbb{F}_4)$ on W_k are the elements of*

$$\{\omega^{-1}\zeta^{\sum_{i\in I}(-2)^i} \mid I \subset \{0, \ldots 2m-1\}, |I| = k\}.$$

Proof. Fix a basis $(e_j : j \in \{0, \ldots, 2m-1\})$ of eigenvectors of σ of the extension to $\mathbb{F}_{4^m}$ of W so that $\sigma(e_j) = \zeta^{(-2)^j} e_j$. Then the exterior products

$$\{e_{i_1} \wedge \ldots \wedge e_{i_k} \mid 1 \leq i_1 < \ldots < i_k \leq 2m\}$$

form an eigenvector basis of W_k where the eigenvalue of σ on $e_{i_1} \wedge \ldots \wedge e_{i_k}$ is $\omega^{-1}\zeta^{\sum_{j=1}^{k}(-2)^{i_j}}$. $\square$

To distinguish between the two spin representations we compare 2-weights of the exponents of the eigenvalues of σ as defined in Notation 3.2.

Lemma 6.7. *For $I \subseteq \{1, \ldots, 2m\}$ with $|I| = k$ let $0 \le u < 2^{2m} - 1$ be such that*

$$\zeta^u = \omega^{-1} \zeta^{\sum_{i\in I}(-2)^i}.$$

Then $O(u) - E(u) = m - k$. In particular the $\mathrm{wt}_2(u)$ is even if and only if $m - k$ is even.

Proof. We have

$$\omega^{-1}\zeta^{\sum_{i\in I}(-2)^i} = \zeta^b \text{ with } b = \sum_{i=0}^{2m-1} b_i 2^i \text{ and } b_i \in \{0, -1\}$$

such that $b_i = -1$ if and only if either $i \in I$ is odd or $i \notin I$ and i is even. As $\zeta^{2^{2m}-1} = 1$ and $2^{2m} - 1 = \sum_{i=0}^{2m-1} 2^i$ we may multiply ζ^b by $\zeta^{2^{2m}-1} = 1$ to obtain $\zeta^b = \zeta^a$ with $a = \sum_{i=0}^{2m-1} a_i 2^i$ such that $a_i = 1 + b_i \in \{0, 1\}$. Then $E(a) = |\{i \in I \mid i \text{ even }\}|$ and $O(a) = |\{i \in \{0, \ldots, 2m-1\} \setminus I \mid i \text{ odd }\}|$. In particular $O(a) - E(a)$ equals the number of odd numbers in $\{0, \ldots, 2m-1\}$ minus the cardinality of I, so $O(a) - E(a) = m - k$. □

Corollary 6.8. *The eigenvalues of σ on Y_k are exactly the elements of Θ_k from Notation 3.2. We have $1 \in \Theta_k$ if and only if $k = m$, and then the eigenvalue 1 of σ occurs twice in Y_m.*

Comparing the eigenvalues of σ on V_+ and V_- with the ones obtained in Proposition 5.4 we find

Corollary 6.9. *If m is even then $\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#} \cong V_+$ and $\mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m} \cong V_-$.*
If m is odd then $\mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m} \cong V_+$ and $\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#} \cong V_-$.

7 The $\mathcal{U}_m$-invariant sandwiched lattices

7.1 The $\mathcal{U}_m$-invariant sandwiched lattices

The results of the previous section (in particular Corollary 6.4 in combination with Remark 6.5) can be summarized to find all lattices $\Lambda \in \mathcal{L}_-$ and $\Gamma \in \mathcal{L}_+$ invariant under $\mathcal{U}_m = 2_+^{1+4m}.\Gamma\mathrm{U}_{2m}(\mathbb{F}_4)$ where $\mathcal{L}_-$ and $\mathcal{L}_+$ are as in Definition 5.5. Note that the lattices Γ are even lattices whereas only $\sqrt{2}\Lambda$ is even. Recall from Remark 6.5 that d_k denotes the dimension of the absolutely irreducible $\mathcal{U}_m$-module Y_k.

Theorem 7.1. *(a)*

$$\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#} \cong \bigoplus_{k\in M_+} Y_k$$

as an $\mathbb{F}_2\Gamma\mathrm{U}_{2m}(\mathbb{F}_4)$ module. The $\mathcal{U}_m$-invariant lattices $\Gamma \in \mathcal{L}_+$ are in bijection with the subsets $J \subseteq M_+$, such that $\Gamma_J/2\mathrm{BW}_{2m}^{\#} \cong \bigoplus_{k\in J} Y_k$ and satisfy $2\Gamma_J^{\#} = \Gamma_{M_+\setminus J}$. The discriminant group is

$$\Gamma_J^{\#}/\Gamma_J \cong (\mathbb{Z}/2\mathbb{Z})^{2^{2m-1}} \oplus (\mathbb{Z}/4\mathbb{Z})^{\sum_{k\in M_+\setminus J} d_k}.$$

(b)

$$\mathrm{BW}_{2m}^{\#}/\mathrm{BW}_{2m} \cong \bigoplus_{k\in M_-} Y_k$$

as an $\mathbb{F}_2\Gamma\mathrm{U}_{2m}(\mathbb{F}_4)$ module. The $\mathcal{U}_m$-invariant lattices $\Lambda \in \mathcal{L}_-$ are in bijection with the subsets $I \subseteq M_-$, such that $\Lambda_I/\mathrm{BW}_{2m} \cong \bigoplus_{k\in I} Y_k$ and satisfy $\Lambda_I^{\#} = \Lambda_{M_-\setminus I}$. $\sqrt{2}\Lambda_I$ is an even lattice with discriminant group

$$(\sqrt{2}\Lambda_I)^{\#}/(\sqrt{2}\Lambda_I) \cong (\mathbb{Z}/2\mathbb{Z})^{2^{2m-1}} \oplus (\mathbb{Z}/4\mathbb{Z})^{\sum_{k\in M_-\setminus I} d_k}.$$

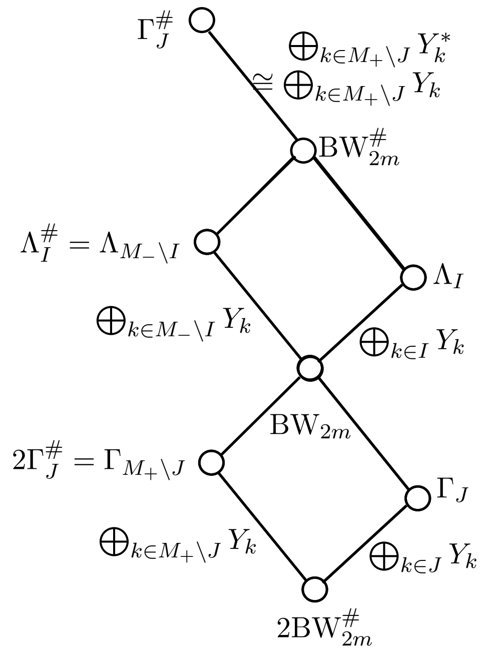

Figure 1: Duality

Proof. The module structure of the quotients of the two lattices follows from Corollaries 6.4 and 6.9. To simplify notation we place ourselves into situation (a). The $\mathcal{U}_m$-invariant lattices Γ with $2\mathrm{BW}_{2m}^\# \subseteq \Gamma \subseteq \mathrm{BW}_{2m}$ are in bijection with the $\Gamma\mathrm{U}_{2m}(\mathbb{F}_4)$-invariant submodules of $\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^\# = \bigoplus_{k\in M_+} Y_k$. As all the Y_k are pairwise non-isomorphic simple $\mathbb{F}_2\Gamma\mathrm{U}_{2m}(\mathbb{F}_4)$-modules, the invariant submodules correspond to subsets of M_+. As all the Y_k are self-dual, so

$$2\Gamma^\#/2\mathrm{BW}_{2m}^\# \cong \mathrm{BW}_{2m}/\Gamma$$

from which one gets the duality as illustrated in Figure 1. Moreover $2\Gamma_J^\# \cap \Gamma_J = 2\mathrm{BW}_{2m}^\#$ and $2\Gamma_J^\# + \Gamma_J = \mathrm{BW}_{2m}$ implies that

$$2(\Gamma_J^\#/\Gamma_J) = \mathrm{BW}_{2m}/\Gamma_J \cong \bigoplus_{k\in M_+\setminus J} Y_k.$$

Together with

$$|\Gamma_J^\#/\Gamma_J| = |\mathrm{BW}_{2m}^\#/\mathrm{BW}_{2m}| \cdot |\mathrm{BW}_{2m}/\Gamma_J| \cdot |\Gamma_J^\#/\mathrm{BW}_{2m}^\#|$$

we obtain the structure of the discriminant group.
Part (b) is proved with the same arguments. □

7.2 The automorphism group of the lattices Γ_J and Λ_I

Theorem 7.2. *For all $\emptyset \neq J \subset M_+$ we have* $\mathrm{Aut}(\Gamma_J) = \mathcal{U}_m$.
For all $\emptyset \neq I \subset M_-$ we have $\mathrm{Aut}(\Lambda_I) = \mathcal{U}_m$.

Proof. Let J be a proper subset of M_+. Then $\Gamma_J + 2\Gamma_J^\# = \mathrm{BW}_{2m}$, so by construction

$$\mathcal{U}_m \leq \mathrm{Aut}(\Gamma_J) \leq \mathrm{Aut}(\mathrm{BW}_{2m}) = \mathcal{G}_{2m}.$$

Moreover $\mathrm{Aut}(\Gamma_J) \neq \mathcal{G}_{2m}$ because $\mathrm{BW}_{2m}/2\mathrm{BW}_{2m}^{\#}$ is a simple $\mathcal{G}_{2m}$-module. As $\Gamma U_{2m}(\mathbb{F}_4)$ is a maximal subgroup of $O_{4m}^{+}(2)$ (see for instance [21, Theorem 3.12]) also $\mathcal{U}_m$ is a maximal subgroup of $\mathcal{G}_{2m}$ so $\mathcal{U}_m = \mathrm{Aut}(\Gamma_J)$. The statement for Λ_I is proved similarly as $\Lambda_I \cap \Lambda_I^{\#} = \mathrm{BW}_{2m}$. $\square$

7.3 Construction $\mathbf{D^{(cyc)}}$ for the lattices Γ_J and Λ_I

In this section we show that the lattices Γ_J and Λ_I from Theorem 7.1 coincide with the lattices $\mathcal{L}(\widehat{(\mathcal{C}_{\star J})})$ and $\mathcal{L}(\widehat{(\mathcal{C}_{\star I})})$ from Section 5.4.

Theorem 7.3. *(a) For $\emptyset \neq J \subset M_+$ the lattice Γ_J from Theorem 7.1 is given by*

$$\Gamma_J = \begin{cases} 2\mathcal{L}(\widehat{(\mathcal{C}_{\star J})}) & m \notin J \\ \mathcal{L}(\widehat{(\mathcal{C}_{\star J})}) & m \in J. \end{cases}.$$

In particular if $\{m, m-2\} \cap J = \emptyset$, then $\min(\Gamma_J) = 2^{m+1} = \min(2\mathrm{BW}_{2m}^{\#})$.

(b) For $\emptyset \neq I \subset M_-$ the lattice Λ_I from Theorem 7.1 is given by

$$\Lambda_I = \mathcal{L}(\widehat{(\mathcal{C}_{\star I})}).$$

In particular if $m-1 \notin I$, then $\min(\Lambda_I) = \min(\mathrm{BW}_{2m}) = 2^m$.

Proof. The lattices Λ_I are clearly σ-invariant, and hence in $\mathcal{L}_-$. Moreover by Corollary 6.8 all Γ_J are admissible and hence in $\mathcal{L}_+$. So we may use Proposition 5.6 to identify the lattices. By Corollary 6.8 the eigenvalues of σ on $\Lambda_I/\mathrm{BW}_{2m}$ (respectively $\Gamma_J/2\mathrm{BW}_{2m}^{\#}$) are exactly the elements of $\bigcup_{k\in I}\Theta_k$ respectively $\bigcup_{k\in J}\Theta_k$. These coincide with the eigenvalues of σ on $\mathcal{L}(\widehat{(\mathcal{C}_{\star I})})/\mathrm{BW}_{2m}$, $\mathcal{L}(\widehat{(\mathcal{C}_{\star J})})/2\mathrm{BW}_{2m}^{\#}$ (if $m \in J$), respectively $2\mathcal{L}(\widehat{(\mathcal{C}_{\star J})})/2\mathrm{BW}_{2m}^{\#}$ (if $m \notin J$) as given in Theorem 5.8. $\square$

Corollary 7.4. *Let $m \geq 3$.*

(a) For $J_0 := M_+ \setminus \{m, m-2\}$ the lattice Γ_{J_0} has minimum 2^{m+1} and discriminant group

$$\Gamma_{J_0}^{\#}/\Gamma_{J_0} \cong (\mathbb{Z}/2\mathbb{Z})^{2^{2m-1}} \oplus (\mathbb{Z}/4\mathbb{Z})^{\binom{2m}{m}+2\binom{2m}{m-2}}.$$

If $m=3$ then $J_0 = \emptyset$ so $\Gamma_{J_0} = 2\mathrm{BW}_{2m}^{\#}$.

(b) For $I_0 := M_- \setminus \{m-1\}$, the rescaled lattice $\mathrm{sBW}_{2m} := \sqrt{2}\Lambda_{I_0}$ *is an even lattice of minimum 2^{m+1} and discriminant group*

$$(\mathrm{sBW}_{2m})^{\#}/(\mathrm{sBW}_{2m}) \cong (\mathbb{Z}/2\mathbb{Z})^{2^{2m-1}} \oplus (\mathbb{Z}/4\mathbb{Z})^{2\binom{2m}{m-1}}.$$

For $m \geq 3$ the lattice sBW_{2m} has the maximum density among the unitary invariant sandwiched lattices that we considered in this paper. In particular these lattices are denser than the Barnes-Wall lattices in the same dimension. More precisely we compute the 2-adic logarithm of the center density (as defined in [6, Chapter 1, Formula (27)]) of sBW_{2m} as

$$\log_2(\delta(\mathrm{sBW}_{2m})) = (2m-3)2^{2m-2} - 2\binom{2m}{m-1}$$

which we tabulate for the first few values of m

m	3	4	5	6	7	8	9	10
$\log_2(\delta(\mathrm{sBW}_{2m}))$	18	208	1372	7632	39050	190112	895524	4120528

Though these lattices are denser than the Barnes-Wall lattices of the same dimension, they do not improve on the asymptotic density of the Barnes-Wall lattices as given in [6, Chapter 1, Formula (30)].

8 Strongly perfect lattices

The notion of strongly perfect lattices has been introduced by Boris Venkov (see [19] for a comprehensive introduction).

Definition 8.1. A lattice L is *strongly perfect*, if its minimal vectors form a spherical 4-design.

One interest of strongly perfect lattices stems from the fact that they provide examples of locally densest lattices. Another point comes from the connection to Riemannian geometry: Recall that a lattice L is called *universally strongly perfect*, if all non-empty layers $L_a := \{\ell \in L \mid (\ell, \ell) = a\}$ form spherical 4-designs. It has been shown in [7] that universally perfect lattices achieve local minima of Epstein's zeta function.

One method to show that a lattice is universally strongly perfect has been used by Bachoc in [2], where she shows that all layers of the Barnes-Wall lattices form spherical 6-designs.

It is based on the following proposition, used in several places of the relevant literature.

Proposition 8.2. *(see e.g. [11, Proposition 2.5]) Let $G \leq O_n(\mathbb{R})$ be a finite subgroup of the compact real orthogonal group. Assume that all G-invariant homogeneous polynomials of degree ≤ 4 are also invariant under $O_n(\mathbb{R})$. Then all G-orbits in $\mathbb{R}^n$ form spherical 4-designs.*

Theorem 8.3. *All the lattices Γ_J and Λ_I from Theorem 7.1 are universally strongly perfect.*

Proof. We show that the assumption of Proposition 8.2 holds for $\mathcal{U}_m = 2_+^{1+4m}.\Gamma\mathrm{U}_{2m}(\mathbb{F}_4) \leq O_{2^{2m}}(\mathbb{R})$. Then the theorem follows as all layers of such invariant lattices are disjoint unions of $\mathcal{U}_m$-orbits. To compute the invariant harmonic polynomials we use the fact that $\mathcal{U}_m = \mathcal{C}_m(4_{\mathbf{1}}^H)$ (see [15, Proposition 7.3.1]). Therefore by [15, Corollary 5.7.5] the space of homogeneous invariants of $\mathcal{U}_m$ of degree d is spanned by the genus m complete weight enumerators of Hermitian self-dual codes $C = C^\perp \leq \mathbb{F}_4^d$ of length d containing the all ones vector. By the classification of these codes, there are up to coordinate permutation unique such codes of lengths 2 and 4, the repetition code $i_2 = \langle(1,1)\rangle \leq \mathbb{F}_4^2$ and its orthogonal sum $i_2 \perp i_2 \leq \mathbb{F}_4^4$. The genus m complete weight enumerator of i_2 is the $O_{2^{2m}}(\mathbb{R})$-invariant quadratic form q and the one of $i_2 \perp i_2$ is q^2. So all invariants of $\mathcal{U}_m$ of degree 2 and 4 are also invariant under $O_{2^{2m}}(\mathbb{R})$. As all layers of any $\mathcal{U}_m$-invariant lattice are disjoint unions of $\mathcal{U}_m$-orbits we conclude that all these layers form spherical 4-designs. So all $\mathcal{U}_m$-invariant lattices are universally strongly perfect. $\square$

Note that this theorem also follows from [18, Theorem 1.3 (A2)].

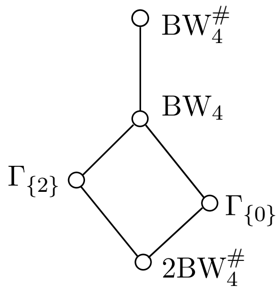

Figure 2: $m = 2$

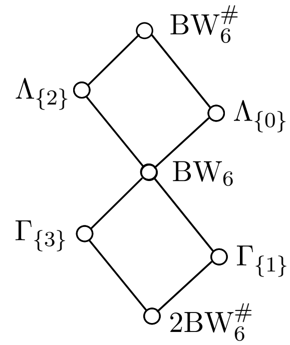

Figure 3: $m = 3$

9 Examples in small dimension

In dimension 16 (so $m = 2$) we find two new universally strongly perfect lattices: $\Gamma_{\{2\}}$ and its dual $\Gamma_{\{2\}}^{\#} = \frac{1}{2}\Gamma_{\{0\}}$. The discriminant groups are

$$\Gamma_{\{2\}}^{\#}/\Gamma_{\{2\}} \cong \mathbb{Z}/2\mathbb{Z}^8 \oplus \mathbb{Z}/4\mathbb{Z}^2 \text{ and } \Gamma_{\{0\}}^{\#}/\Gamma_{\{0\}} \cong \mathbb{Z}/2\mathbb{Z}^8 \oplus \mathbb{Z}/4\mathbb{Z}^6.$$

For the minimum we compute

$$\min(\Gamma_{\{2\}}) = \min(\mathrm{BW}_4) = 4, \min(\Gamma_{\{0\}}) = 6$$

so the Hermite function γ with $\gamma(L) = \frac{\min(L)}{\det(L)^{1/\dim(L)}}$ rounded to 2 decimal places are

$$\gamma(\mathrm{BW}_4) \sim 2.83, \;\; \gamma(\Gamma_{\{2\}}) \sim 2.38, \;\; \gamma(\Gamma_{\{0\}}) \sim 2.52.$$

The kissing numbers are computed with Magma as

$$|\mathrm{Min}(\mathrm{BW}_4)| = 4320, \;\; |\mathrm{Min}(\Gamma_{\{2\}})| = 864, \;\; |\mathrm{Min}(\Gamma_{\{0\}})| = 1536.$$

For dimension 64 (so $m = 3$) we list the invariants of the lattices as computed with Magma in the following table:

name	smith	min	kissing	Hermite
BW_6	$1^{32}2^{32}$	8	$9,694,080$	5.66
$\Gamma_{\{3\}}$	$1^{20}2^{32}4^{12}$	8	$114,048$	4.36
$\Gamma_{\{1\}}$	$1^{12}2^{32}4^{20}$	12	$4,257,792$	5.50
$\frac{1}{\sqrt{2}}\mathrm{sBW}_6 = \Lambda_{\{0\}}$	$\frac{1}{2}^{2}1^{32}2^{30}$	8	$9,694,080$	5.91
$\Lambda_{\{2\}}$	$\frac{1}{2}^{30}1^{32}2^{2}$	4	$2,395,008$	5.42

References

[1] K. Abdukhalikov, Defining sets of extended cyclic codes invariant under the affine group. J. Pure Appl. Algebra 196 (2005) 1–19.

[2] C. Bachoc, Designs, groups and lattices. J. Théor. Nombres Bordeaux 17 (2005) 25–44.

[3] E.S. Barnes, N.J.A. Sloane, New lattice packings of spheres. Can. J. Math. 35 (1983) 117–130

[4] E.S. Barnes, G.E. Wall, Some extreme forms defined in terms of abelian groups. J. Austral. Math. Soc. 1 (1959/1961) 47–63

[5] M. Broué, M. Enguehard, Une famille infinie de formes quadratiques entières; leurs groupes d'automorphismes. Ann. Sci. l'ENS 6 (1973) 17–51

[6] J.H.Conway, N.J.A.Sloane, *Sphere packings, lattices and groups.* Grundlehren der Mathematischen Wissenschaften 290, Springer-Verlag, New York, 1988.

[7] R. Coulangeon, Spherical designs and zeta functions of lattices. Int. Math. Res. Not. 2006, Art. ID 49620, 16 pp.

[8] W. Fulton, J. Harris, *Representation theory. A first course.* Graduate Texts in Mathematics, 129. Readings in Mathematics. Springer-Verlag, New York, 1991.

[9] P. Kanwar, S.R.López-Permouth, Cyclic Codes over the Integers Modulo p^m. Finite fields and their applications 3 (1997) 334–352.

[10] W. Kositwattanarerk, F. Oggier, Connections between Construction D and related constructions of lattices. Des. Codes Cryptogr. 73 (2014) 441–455.

[11] W. Lempken, B. Schröder, P.H. Tiep, Symmetric squares, spherical designs, and lattice minima. With an appendix by Christine Bachoc and Tiep. J. Algebra 240 (2001) 185–208.

[12] J. MacWilliams, N.J.A. Sloane, *The Theory of Error Correcting Codes.* North Holland (1977)

[13] G. Nebe, The normaliser action and strongly modular lattices. Enseign. Math. 43 (1997) 67–76.

[14] G. Nebe, E.M. Rains, N.J.A. Sloane, The invariants of the Clifford groups. Des. Codes Cryptogr. 24 (2001) 99–121.

[15] G. Nebe, E.M. Rains, N.J.A. Sloane, *Self-dual codes and invariant theory.* Algorithms and Computation in Mathematics, 17. Springer-Verlag, Berlin, 2006.

[16] H.-G. Quebbemann, Modular lattices in Euclidean spaces. J. Number Theory 54 (1995) 190–202.

[17] J. P. Serre, *Linear Representations of Finite Groups.* Springer Graduate Texts in Mathematics 42, Springer-Verlag, New York-Heidelberg, 1977

[18] P.H. Tiep, Finite groups admitting Grassmannian 4-designs. J. Algebra 306 (2006) 227–243.

[19] B. Venkov, *Réseaux et designs sphériques.* Monogr. Ens. Math. 37 (2001) 10-86.

[20] G.E. Wall, On the Clifford collineation, transform and similariy groups (IV) An application to quadratic forms. Nagoya Math. J. 21 (1962) 199–222.

[21] R.A. Wilson, *The finite simple groups.* Graduate Texts in Mathematics, 251. Springer-Verlag London, 2009.