SPHERICAL 3-DESIGNS AND LATTICES FROM BINARY CODES

JACQUES MARTINET (*)

Abstract. Lifting binary codes over $\mathbb{Z}^n$ produces lattices, with some of which we construct spherical 3-designs. The case when the set of minimal vectors is a 3-design corresponds to the notion of *strongly eutactic lattices*, introduced by Boris Venkov in [V]. In this paper we consider a kind of counterpart of this notion for (linear) binary codes, with special emphasis on codes of weight 3.

1. Introduction

Let $\mathcal{C}$ be a linear binary code of length n. Denote by E the Euclidean space $\mathbb{R}^n$, equipped with its canonical basis $\mathcal{B} = (\varepsilon_1, \dots, \varepsilon_n)$ and its canonical scalar product $(x_i) \cdot (y_i) = \sum x_i y_i$, and by $\mathbb{Z}^n$ the lattice with $\mathbb{Z}$-basis $\mathcal{B}$. The *norm of* $x \in E$ is $N(x) = x \cdot x$, the *Gram matrix of the basis* $(e_1, \dots, e_n)$ is $\operatorname{Gram}(\mathcal{B}) = (e_i \cdot e_j)$, the *determinant of* $\mathcal{B}$ is $\det(\mathcal{B}) = \det(\operatorname{Gram}(\mathcal{B}))$.

The minimum of a lattice $\Lambda \subset E$ is $\min \Lambda = \min_{x \in \Lambda \smallsetminus \{0\}} N(x)$. We set $S(\Lambda) = \{x \in \Lambda \mid N(x) = \min \Lambda\}$, (the set of *minimal vectors of* Λ), $s(\Lambda) = \frac{|S|}{2}$ (the [*half-*]*kissing number of* Λ), and define the *determinant of* Λ as the determinant of one of its bases over $\mathbb{Z}$.

With each word α of $\mathcal{C}$ we associate the vector $e_\alpha = \frac{\sum_{\alpha(i)=1} \varepsilon_i}{2}$, and with $\mathcal{C}$ the lattice

$$\Lambda_{\mathcal{C}} = \langle \mathbb{Z}^n, e_\alpha \mid \alpha \in \mathcal{C} \rangle \,.$$

The aim of this note is to study for such lattices $\Lambda_{\mathcal{C}}$ some notions related to perfection and eutaxy, the definitions of which we recall below. We also consider a second construction for *even* codes $\mathcal{C}$, namely

$$L_{\mathcal{C}} = \langle \mathbb{D}_n, e_\alpha \mid \alpha \in \mathcal{C} \rangle \,.$$

where $\mathbb{D}_n = \{x \in \mathbb{Z}^n \mid \sum x_i \equiv 0 \mod 2\}$ is the even sublattice of $\mathbb{Z}^n$.

For reasons which will be explained in the next section we shall essentially consider four situations:

(a) $\Lambda_{\mathcal{C}}$ with $\operatorname{wt}(\mathcal{C}) = 3$; (b) $\Lambda_{\mathcal{C}}$ with $\operatorname{wt}(\mathcal{C}) = 4$;

(c) $L_{\mathcal{C}}$ with $\operatorname{wt}(\mathcal{C}) = 6$; (d) $L_{\mathcal{C}}$ with $\operatorname{wt}(\mathcal{C}) = 8$.

Key words and phrases. Euclidean lattices, binary codes, spherical designs, eutaxy

(*) Univ. Bordeaux, IMB & CNRS, UMR 5251.

Consider a finite, symmetric set S of vectors of E having the same norm, and set $s = \frac{1}{2}|S|$; the definitions below will then be applied to the set S of minimal vectors of a lattice, and sometimes more generally to various layers of the lattice. The notions relative to perfection and eutaxy that we recall below stem from papers of Korkine & Zolotareff (1873–1877) and Vorononoi (1907–1908); more details can be read in [M1], Chapter 3. Given a subspace F of E, we denote by $p_F \in \operatorname{End}^s(E)$ the orthogonal projection to F, and for $x \in E$, $x \neq 0$, we denote by p_x the orthogonal projection to the line $\mathbb{R}\,x$.

The *perfection rank of S* is the rank $r = r(S)$ in $\operatorname{End}^s(E)$ of the p_x, $x \in S$. One has $r \leq \frac{n(n+1)}{2} = \dim \operatorname{End}^s(E)$. The difference $\frac{n(n+1)}{2} - r$ is the *perfection co-rank of S*. We say that S is *perfect* if its perfection co-rank is zero. A relation $\sum_{x \in S/\pm 1} \lambda_x p_x = 0$ is called a *perfection relation.*

A *eutaxy relation* is a relation of the form $\mathrm{Id} = \sum_{x \in S/\pm 1} \rho_x p_x$ with real coefficients ρ_x. Since $\operatorname{Tr}(p_x) = 1$, we have $\sum_{x \in S/\pm 1} \rho_x = n$. We say that S is *weakly eutactic* if the set of eutaxy relations on S is not empty, in which case it is an affine space over the real vector space of perfection relations. We say that S is *semi-eutactic* (resp. *eutactic*) if there exists a eutaxy relation with $\rho_x \geq 0$ (resp. $\rho_x > 0$). We say that a lattice is *extreme* if its Hermite invariant achieves a local minimum (then necessarily strict modulo similarities). By a theorem of Vorononoi, a lattice is extreme if and only if it is perfect and eutactic.

Finally, we say that S is *strongly eutactic* if there exists a eutaxy relation with equal coefficients ρ_x, then equal to $\frac{n}{s}$; equivalent formulation: $\sum_{x \in S/\pm} p_x$ is proportional to the identity. This condition amounts to saying that S is a *spherical* 3*-design*; see [V], Sections 3 and 6 for the application to lattices of the Delsarte-Goethals-Seidel theory of spherical designs; see also [B], [B-V], and [M-V1].

In the next section we consider the connection between codes and lattices with respect to the various notions of eutaxy and perfection. The following sections are then devoted to (linear, binary) codes, especially of weight 3, but we also consider related codes of various weights, which show up for instance as dual codes, or even subcodes or extended codes (by the parity check) of odd codes.

2. Lifting binary codes

Recall that $\mathcal{C}$ is a code of length n. We assume that $\mathcal{C}$ is non-zero, and denote by $k \geq 1$ its dimension and d its *weight* or *minimal distance.* (For short, $\mathcal{C}$ is a (linear, binary) $[n,k]$- or $[n,k,d]$-code.) The code $\mathcal{C}$ is *even* if all its weights are even and *odd* otherwise, and *doubly even* if all its weights are divisible by 4. The *dual of $\mathcal{C}$* is

$$\mathcal{C}^\perp = \{y \in \mathbb{F}_2^n \mid \forall\, x \in \mathcal{C},\ x \cdot y = 0\}\,,$$

and we say that $\mathcal{C}$ is *self-orthogonal* if $\mathcal{C} \subset \mathcal{C}^\perp$ and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$; note that doubly even codes are self-orthogonal.

Codes lift to lattices $\Lambda_\mathcal{C}$, of minimum $\min(1, \frac{d}{4})$, and $L_\mathcal{C}$, of minimum $\min(2, \frac{d}{4})$. We shall often rescale $\Lambda_\mathcal{C}$ to minimum $\min(4, d)$ and $L_\mathcal{C}$ to minimum $\min(8, d)$. In these scales they become integral, with determinants $\det(\Lambda_\mathcal{C}) = 4^{n-k}$ and $\det(L_\mathcal{C}) = 4^{n-k+1}$, respectively. Then $\Lambda_\mathcal{C}$ is even is if and only if $\mathcal{C}$ is even whereas $L_\mathcal{C}$ is even for every $\mathcal{C}$, and these lattices are primitive if and only if $\mathcal{C}$ *is not* self-dual. Otherwise, they become integral when rescaled to half their minimum (and are then primitive because $\mathcal{C}$ is not zero).

To calculate $s = s(\Lambda_\mathcal{C})$ in full generality, we need the invariant below of $\mathcal{C}$.

Definition 2.1. *Let $M_m = M_m(\mathcal{C})$ be the number of words of $\mathcal{C}$ having a given weight m. When m is the weight d of $\mathcal{C}$, we omit the subscript m.*

Proposition 2.2. *If $d = 3$, $d = 4$, $d \geq 5$, then $s(\Lambda_\mathcal{C}) = 4M$, $8M + n$, n, respectively; if $d = 6$, $d = 8$, $d \geq 10$, then $s(L_\mathcal{C}) = 16M$, $64M + n(n-1)$, $n(n-1)$, respectively.*

Proof. Lifting a word x of weight $\mathrm{wt}(x)$ produces $2^{\mathrm{wt}(x)-1}$ pairs of vectors of norm $\frac{\mathrm{wt}(x)}{4}$ in $\Lambda_\mathcal{C}$; the same kind of calculation applies to $L_\mathcal{C}$. □

[In the proposition above we have disregarded construction $L_\mathcal{C}$ with $\mathrm{wt}(\mathcal{C}) = 2$ or 4, since replacing $\mathbb{Z}^n$ by $\mathbb{D}_n$ does not produce interesting new sets of minimal vectors. We also left aside lattices $\Lambda_\mathcal{C}$ constructed with codes of weight $w \leq 2$. These yield lattices of minimum 1 or 2, and the sublattice generated by vectors of norm 1 or 2 is a *root lattice*, thus isometric to an orthogonal sum of well-known irreducible lattices ($\mathbb{Z}$, $\mathbb{A}_n, n \geq 1$, $\mathbb{D}_n, n \geq 4$, $\mathbb{E}_n, n = 6, 7, 8$). A look at the determinants of lifts of doubly even codes generated by words of weight 4 shows that we may only obtain $\mathbb{D}_n$ ($n \geq 4$ even), $\mathbb{E}_7$, and $\mathbb{E}_8$, which shows that these codes are concatenations of irreducible codes that we may call d_n ($n \geq 4$ even), e_7, and e_8. The latter two are related to Hamming codes on which we shall return below; $d_n, n = 2m$ is obtained by dividing $\{1, \dots, n\}$ into the m blocks $\{1, 2\}, \dots, \{n-1, n\}$ and taking for words all words with support an even number of blocks.]

Example 2.3. We give here a few examples of construction $L_\mathcal{C}$. Note that all lattices quoted below are strongly eutactic by Theorem 3.6 of next section.

(1) Doubling the code d_4 (resp. d_6) we obtain for $L_\mathcal{C}$ a scaled copy of $\mathbb{E}_8$ (resp. of the laminated lattice $\Lambda_{12}^{\max}$, for which $s = 64 \times 3 + 12 \times 11 = 324$; see [M2], Section 8.2).

(2) There are unique $[15, 4, 8]$- and $[16, 5, 8]$-codes. The corresponding lattices $L_\mathcal{C}$ are the laminated lattices Λ_{15} and Λ_{16} (the Barnes-Wall lattice BW_{16}). Note that BW_{16} as well as $\mathbb{D}_4$, $\mathbb{E}_7$ and $\mathbb{E}_8$ which can be obtained by construction $\Lambda_\mathcal{C}$, are spherical designs of level $\ell \geq 5$.

(3) Similarly rescaling the unique self-dual $[16, 6, 6]$-code of [B-G] produces the lattice O_{16} (with even sublattice Λ_{16}), again a spherical 5-design.

(4) Using the binary Golay code $\mathcal{G}$, we obtain a lattice with $s = 759 \times 64 + 24 \times 23 = 49128$, indeed the orthogonal in the Leech lattice of a norm-6 vector. To obtain the Leech lattice Λ_{24} we must use codes over $\mathbb{Z}/4\mathbb{Z}$, for instance, adjoin to L the vector $\frac{1}{4}(-3, 1^{23})$; this construction is better understood in terms of *Kneser neighbours* of $\Lambda_{\mathcal{G}}$.

Recall that the *dual lattice of a lattice* Λ is

$$\Lambda^* = \{x \in \mathbb{R}^n \mid \forall\, y \in \Lambda,\ x \cdot y \in \mathbb{Z}\}\,.$$

We have $[\Lambda_{\mathcal{C}} : \mathbb{Z}^n] = 2^d$, hence $[\mathbb{Z}^n : \Lambda_{\mathcal{C}^\perp}] = 2^d$, and $[\mathbb{Z}^n : (2\mathbb{Z})^n] = 2^n$. Now $\Lambda_{\mathcal{C}^\perp}$ contains $(2\mathbb{Z})^n$ and we have $[\Lambda_{\mathcal{C}^\perp} : (2\mathbb{Z})^n] = 2^{n-k} = 2^{\dim \mathcal{C}^\perp}$, which implies

$$\Lambda^*_{\mathcal{C}^\perp} = \langle (2\mathbb{Z})^n, e_w \mid w \in \mathcal{C}^\perp \rangle\,.$$

3. Perfection and eutaxy

We keep the notation of the previous sections.

Lemma 3.1. *The set* $S = \{\frac{\pm\varepsilon_1 \pm \cdots \pm \varepsilon_n}{2}\}$ *is strongly eutactic.*

Proof. We apply the projection formula $p_e(x) = \frac{e\cdot x}{e\cdot e}\, e$ with $e \in S$ and and x equal to an ε_i. We have $e \cdot \varepsilon_i = \pm\frac{1}{2}$ and $e \cdot e = \frac{n}{4}$, hence $p_e(\varepsilon_i) = \pm\frac{2}{n}\, e$, so that the component of $p_e(\varepsilon_i)$ is $+\frac{1}{n}$ on ε_i, whereas it is $\pm\frac{1}{n}$ on ε_j, $j \neq i$, with the sign of ε_j in e. The sum of the $p_e(\varepsilon_i)$ on a half-system of S is

$$\frac{1}{2} \sum_{e\in S} p_e(\varepsilon_i) = \frac{2^{n-1}}{n}\, \varepsilon_i\,,$$

since there are in the sum above the same number of minus signs on the ε_j, $j \neq i$. This shows that $\sum_{e\in S/\pm} p_e$ and $\frac{2^{n-1}}{n}$ Id, which agree on the basis $\mathcal{B}$ for E, are indeed equal. □

Proposition 3.2. *Let* $\mathcal{C}$ *be a* $[n, k, 4]$ *binary code. Then:*

(1) *In situation (b),* $\Lambda_{\mathcal{C}}$ *is eutactic.*
(2) *In situation (d),* $L_{\mathcal{C}}$ *is extreme.*
(3) *In situation (b),* $\Lambda_{\mathcal{C}}$ *is perfect if and only if every pair* i, j *of coordinates belongs to the support of a weight* 4 *word.*
(4) *In situation (a),* $\Lambda_{\mathcal{C}}$ *is perfect if and only if every pair* i, j *of coordinates belongs to the support of a (unique) weight* 3 *word.*

Proof. The proof of eutaxy in situation (b) is dealt with in [K-M-S] by induction on the number w of weight-4 words of $\mathcal{C}$, using when $w = 0$ the fact that $\mathbb{Z}^n$ is (strongly) eutactic. The same kind of proof applies to situation (d) with $\mathbb{D}_n$ instead of $\mathbb{Z}^n$ when $w = 0$. In this latter case, since $L_{\mathcal{C}}$ contains the perfect lattice $\mathbb{D}_n$ scaled to $\min L_{\mathcal{C}}$, it is moreover perfect, hence extreme by Voronoi's theorem.

Assertion (3) is also proved (in a more general form) in [K-M-S], (Lemma 7.2), and this proof adapts easily to the last two assertions. □

Remark 3.3. Property (4) in the proposition above amounts to saying that the code $\mathcal{C}$ (of weight 3 in this case) is *perfect* in the sense of coding theory; perfect codes are then the generalized Hamming codes defined in Section 4 below. The notions which appear in Assertions (3) and (5) are less restrictive than the corresponding notions of perfection for codes. In [K-M-S], for situation (b), such codes are called *complete codes.*

We now consider unions of sets S having a common length $m \le n$.

Proposition 3.4. *Let k, m $(m \le n)$ be positive integers, let $\mathcal{E}_j$, $j = 1, \dots, k$ be subsets of $\{1, 2, \dots, n\}$ of cardinality m, and for each j, let $S_j = \frac{\sum_{i \in \mathcal{E}_j} \varepsilon_j}{2}$. Then $S = \cup_j S_j$ is strongly eutactic if and only if the number of sets $\mathcal{E}_j$ containing a given index i is independent of i.*

Proof. For each $j \le k$, denote by F_j be the span of the $\varepsilon_i, i \in \mathcal{E}_j$, and for $i = 1, \dots, n$, let μ_i be the number of $j \le k$ with $i \in \mathcal{E}_j$.

The set S is strongly eutactic if and only if the sum $T := \sum_{j=1}^{k} \sum_{e \in S_j} p_e$ is proportional to the identity. Using Lemma 3.1, we see that the inner sum is equal to $\frac{2^{m-1}}{m} p_{F_j} = \frac{2^{m-1}}{m} \sum_{i \in \mathcal{E}_j} p_{\varepsilon_i}$. We thus have $T = \frac{2^{m-1}}{m} \sum_{i=1}^{n} \mu_i p_{\varepsilon_i}$, which shows that T is proportional to the identity if and only if the μ_i have a common value μ (and then we have $\sum_{e \in S/\pm} = \frac{2^{m-1}\mu}{m}$ Id). □

We now return to the data of a code $\mathcal{C}$ and the lattices $\Lambda_{\mathcal{C}}$ and $L_{\mathcal{C}}$.

Definition 3.5. Let $\mathcal{C}$ be a (linear, binary) code and let m be a weight of $\mathcal{C}$.

(1) We denote by $t_m(i)$ the number of words w of weight m of $\mathcal{C}$ such that $w(i) = 1$.

(2) We say that $\mathcal{C}$ is *m-equidistributed* if $t_m(i)$ does not depend on i ; the common value of the $t_m(i)$ is then called the *m-distribution weight of* $\mathcal{C}$ and denoted by $t_m = t_m(\mathcal{C})$.

We omit the notation m when $m = \mathrm{wt}(\mathcal{C})$ is the weight of $\mathcal{C}$, and also say that an equidistributed code is *strongly eutactic.*

In terms of *combinatorial designs*, this definition means that the words of weight m in $\mathcal{C}$ equip $\mathcal{C}$ with the structure of a $1 - (n, m, t_m)$ design. So various examples can be found in Bachoc-Gaborit's paper [B-G].

Theorem 3.6. *Let $\mathcal{C}$ be an equidistributed code. Then the lattices $\Lambda_{\mathcal{C}}$ in situations (a) and (b), and $L_{\mathcal{C}}$ in situations (c) and (d) are strongly eutactic.*

Proof. Let S_0 be the set of vectors in $\Lambda_{\mathcal{C}}$ or $L_{\mathcal{C}}$ which lift the words of weight $wt(C)$. By Proposition 3.4, S_0 is strongly eutactic. In situations (a) and (c), we have $S(\Lambda_{\mathcal{C}}) = S_0$ and $S(L_{\mathcal{C}}) = S_0$, respectively, which proves the result in these two cases. In situations (b) and (d), the set of minimal vectors of the lattice is the disjoint union $S_0 \cup S_1$ with $S_1 = S(\mathbb{Z}^n)$ in case (b) and $S_1 = S(\mathbb{D}^n)$ in case (d). In both cases, S_1 is strongly eutactic, hence the result in these latter cases. □

Note that the various notions of eutaxy as well as that of perfection for a lattice Λ solely depend on the set of minimal vectors of Λ. For this reason we shall most of the time restrict ourselves to lattices which are generated by their minimal vectors. Moreover, when this condition holds, these notions are easily tested using the corresponding knowledge for the irreducible components of Λ: the perfection rank is additive on the components, (weak, semi-, proper) eutaxy holds if and only if it holds on each component, and strong eutaxy holds if and only if (1) it holds on each component and (2) the ratio $\frac{s}{n}$ is the same for all components.

As a consequence we shall mainly consider lattices which are *irreducible* and *generated by their minimal vectors.*

When performing one of the construction (a) to (d) with a code $\mathcal{C}$, the condition above is satisfied if and only if $\mathcal{C}$ is *generated by its words of minimal weight* and is *irreducible* (i.e. not the concatenation of codes of smaller length). In particular, this *excludes equidistributed codes with* $k = 1$.

4. Equidistributed codes

We keep the notation of the previous section. We denote by $\mathcal{C}$ a (linear, binary) $[n, k, d]$-code, and refer to Definitions 2.1 and 3.5 for the notation M_m, M, $t_m(i)$, $t(i)$, t_m, t.

We denote by $\mathbf{0}$ the word 0 and by $\mathbf{1}$ the all ones word. We moreover denote by $\mathrm{Aut}(\mathcal{C})$ the automorphism group of $\mathcal{C}$ (and shall often use the letter G).

We first state two propositions, of which we omit the evident proofs.

Proposition 4.1. (1) *The dual code $\mathcal{C}^\perp$ is even if and only if $\mathbf{1} \in \mathcal{C}$.*

(2) *For every weight m of $\mathcal{C}$, the weight-m words of $\mathcal{C}$ add to the word $\big(k_m(1), \dots, k_m(n)\big)$.*

(3) *If $\mathcal{C}$ is m-equidistributed, this sum is $\mathbf{0}$ if k_m is even and $\mathbf{1}$ if k_m is odd.* □

Proposition 4.2. (1) *We have $\sum_{i=1}^n t_m(i) = m \cdot M_m$. In particular if $\mathcal{C}$ is m-equidistributed, then*

$$t_m \cdot n = m \cdot M_m \,.$$

(2) *If the automorphism group of $\mathcal{C}$ acts transitively on the coordinates, then $\mathcal{C}$ and $\mathcal{C}^\perp$ are m-equidistributed for every m.* □

We now consider the connections which might exist between a code $\mathcal{C}$ of weight 3, its *even subcode* and its extended even code (by the *parity check*).

Definition 4.3. Let $\mathcal{C}$ be an odd code. We denote by $\mathcal{C}'$ its even subcode and by $\overline{\mathcal{C}}$ its extended code. We also write $t' = t(\mathcal{C}')$, $\overline{t} = t(\overline{\mathcal{C}})$, $M' = M(\mathcal{C}')$, $\overline{M} = M(\overline{\mathcal{C}})$.

This definition will mainly be applied when $\mathrm{wt}(\mathcal{C}) = 3$. Thus we shall consider codes with parameters

$$\mathcal{C} \,:\, [n, k, 3]\,; \quad \mathcal{C}' \,:\, [n, k-1, 4 \,\mathrm{or}\, 6]\,; \quad \overline{\mathcal{C}} \,:\, [n+1, k, 4]\,.$$

[Under the conditions listed at the end of Section 3, one has $\mathrm{wt}(\mathcal{C}') = 4$, since weight-3 words may not all have disjoint supports.]

Proposition 4.4. *Let $\mathcal{C}$ be a code of weight 3. Assuming that $\mathcal{C}'$ has weight 4, we have*

$$\bar{t}(i) = t(i) + t'(i)\ (1 \le i \le n),\ \bar{t}(n+1) = M\ ,\ \text{ and } \overline{M} = M + M'\ .$$

Proof. The words of weight 4 of $\overline{\mathcal{C}}$ are those of $\mathcal{C}'$ and the extensions of words of weight 3 of $\mathcal{C}$. □

This proposition, which reduces to $\bar{t}(i) = t + t'$ if $i \le n$ and $\bar{t}(n+1) = M$ when both $\mathcal{C}$ and $\mathcal{C}'$ are equidistributed, allows calculations for $\overline{\mathcal{C}}$, but says nothing on putative relations between $\mathcal{C}$ and $\mathcal{C}'$. We shall construct examples in which $\mathcal{C}$ but not $\mathcal{C}'$, or $\mathcal{C}'$ but not $\mathcal{C}$, is equidistributed.

In the remaining of this section we concentrate on codes of weight 3, giving three important examples.

Recall that the (*generalized*) *Hamming codes* $\mathcal{H}_n$ of length $n = 2^p - 1$, $p \ge 3$, are $[n, n-p, 3]$-codes defined up to equivalence by their *parity check matrix* A, a $p \times n$ matrix having for columns the n non-zero columns of zeros or ones.

We order them so has to have $A = (I_p \mid A_0)$, which gives the codes the *generator matrices* $H_n = (I_{n-p} \mid {}^t\!A_0)$. The weight-3 words of $\mathcal{H}_n$ can be viewed as the lines of the projective space $P_p(\mathbb{F}_2)$, thus $\mathrm{Aut}(\mathcal{H}_n)$ as the group $\mathrm{PSL}_p(\mathbb{F}_2)$, of order $2^{p(p-1)/2} \cdot (2^p - 1) \cdots (2^2 - 1) \cdot (2 - 1)$, acting 2-fold transitively on the coordinates, hence transitively on the weight-3 words. Let w be weight-4 word with support $\{i, j, i', j'\}$. Then (i, j, i_w) is a weight-3 word of $\mathcal{C}$ for a uniquely defined coordinate i_w, and (i', j', i_w) also belongs to $\mathcal{C}$. We see that $M_3(\mathcal{H}_n) = \frac{1}{3}\binom{n}{2}$ and $M_4(\mathcal{H}_n) = \frac{n-3}{4} M_3$. A closer look at the automorphism group moreover shows that $\mathrm{Aut}(\mathcal{H}_n)$ also acts transitively on the sets of weight-4 words.

The following proposition easily follows from the data above.

Proposition 4.5. *The codes $\mathcal{H}_n$, $\mathcal{H}'_n$ and $\overline{\mathcal{H}}_n$, $n = 2^p - 1$, $p \ge 3$ are equidistributed, with the following invariants:*

(1) $\mathcal{H}_n$*:* $t = \frac{n-1}{2}$, $M = \frac{n(n-1)}{6}$ *;*
(2) $\mathcal{H}'_n$*:* $t' = \frac{(n-1)(n-3)}{6}$, $M' = \frac{n(n-1)(n-3)}{24}$ *;*
(3) $\overline{\mathcal{H}}_n$*:* $\bar{t} = \frac{n(n-1)}{6}$, $\overline{M} = \frac{n(n^2-1)}{24}$ *.* □

Note that one has $\mathrm{PSL}_p(\mathbb{F}_2) = \mathrm{GL}_p(\mathbb{F}_2)$, so that $\mathrm{Aut}(\overline{\mathcal{H}}_n)$ can be identified with the affine group $\mathrm{AGL}_p(\mathbb{F}_2)$, which is 3-fold transitive on the coordinates.

The Hamming codes are the only *perfect codes* of weight 3. (For weight-3 codes, perfection amounts to saying that there exists for each set $\{i, j\}$ of coordinates a (unique) word w of weight 3 with $w(i) = w(j) = 1$.)

Thanks to the transitivity properties of the Hamming codes, we can associate with $\mathcal{H}_n$ (canonically up to isomorphism) an $[n-1, k-1, 3]$-code $\mathcal{H}_{n-1}$, its *punctured code*, obtained by removing one coordinate i and all the words with $w(i) = 1$. Thanks to the 2-fold transitivity of $\mathrm{Aut}(\mathcal{H}_n)$, the punctured code of $\mathcal{H}_n$ is well defined up to isomorphism and its automorphism group again acts transitively on the coordinates. We *denote this code by* $\mathcal{H}p_n$, this time with $n = 2^p - 2$, $p \geq 3$. Using Proposition 4.5 above, we obtain:

Proposition 4.6. *The codes $\mathcal{H}p_n$ and $\mathcal{H}p'_n$ ($n = 2^p - 2$) are equidistributed codes having the following invariants:*

$$t = \tfrac{n-2}{2},\ M = \tfrac{n(n-2)}{6},\ t' = \tfrac{(n-2)(n-3)}{6},\ \textit{and } M' = \tfrac{n(n-2)(n-3)}{24}\,;$$

$\overline{\mathcal{H}p_n}$ *is isomorphic to* $\mathcal{H}'_{n+1}$. □

Our last family, though having nothing to do with the previous two families except for a coincidence with $\mathcal{H}p_6$ for $n = 6$, again relies on a parameter $p \geq 3$. We define it through its dual codes. We first state a lemma, without writing its evident proof.

Lemma 4.7. *Let $\mathcal{C}$ be an $[n, k]$-code and let A be a generator matrix for $\mathcal{C}$. The words of weight ℓ in $C^{\perp}$ are in one-to-one correspondence with the sets of ℓ columns of A adding to zero in $\mathcal{C}^{\perp}$. In particular we have* $\mathrm{wt}(\mathcal{C}^{\perp}) \geq 3$ *if and only if the columns of A are distinct and non-zero. This implies the bound $n \leq 2^k - 1$, attained only on the duals of Hamming codes.* □

Proposition 4.8. *For any $p \geq 3$, there exists (up to isomorphism) a unique $[n = \frac{p(p+1)}{2}, p, p]$-code $\mathcal{K}'(p)$ having $M = p + 1$ words of weight p which have pairwise a unique 1 in common (thus they add to $\mathbf{0}$). Its automorphism group is isomorphic to S_{p+1} acting faithfully on the $p + 1$ words of weight p and on the coordinates as the action on the 2-subsets of $\{1, 2, \dots, p + 1\}$.*

The dual code $\mathcal{K}_n$ of $\mathcal{K}'(p)$ is an equidistributed $[n = \frac{p(p+1)}{2}, k = \frac{p(p-1)}{2}, 3]$-code with $M = \frac{p(p^2-1)}{6}$ and $t = p - 1$; its even subcode has $M' = \frac{p(p^2-1)(p-2)}{8}$ and $t' = (p - 1)(p - 2)$.

Proof. We just sketch it. In the spirit of coding theory, a canonical construction for such a code can be done inductively as follows: start with the matrix I_p, then extend it to the right by $p - 1$ ones on the first row and by I_{p-1} below this row, then complete the first row by 0's, forget it, and go on inductively, putting $p - 2$ ones on the second row and writing down I_{p-2} below, etc. The lines of this matrix define p words $w_1, \dots, w_p$ which add to $w_{p+1} = (1^p, 0^{p(p-1)/2})$. Here is the generator matrix for $p = 4$:

$$\begin{pmatrix} 1&0&0&0&1&1&1&0&0&0 \\ 0&1&0&0&1&0&0&1&1&0 \\ 0&0&1&0&0&1&0&1&0&1 \\ 0&0&0&1&0&0&1&0&1&1 \end{pmatrix}$$

Uniqueness is proved by noticing that two words w, w' can be exchanged by exchanging conveniently the $p - 1$ coordinates at which they differ. (If $w(i) = 1$, let w'' be the word having $w''(i) = 1$ and $w''(i') = 1$ where i' satisfies $w'(i') = 1$, and exchange i and i'). This also shows that the automorphism group is generated by products of $p - 1$ transpositions on the coordinates which induce all possible transpositions on the set of words of weight p, and that the action on the coordinates is induced by the action of S_{p+1} on the 2-sets, each coordinate being associated with the pair (w,w') of weight-3 words such that $w(i)=w'(i)=1$.

We have $n=\frac{p(p+1)}{2}$ and $\dim\mathcal{K}(p)=p$, and it is clear that for any pair (i,j) of coordinates of $\mathcal{K}(p)$, there are words having components $(1,0)$ and $(0,1)$ at (i,j). This shows that $\mathcal{K}(p)^\perp$ is a $[\frac{p(p+1)}{2},\frac{p(p-1)}{2},d\geq 3]$-code.

Pick any coordinate i, denote by w_1 and w_2 the words of weight 3 such that $w_1(i)=w_2(i)=1$. and choose $j\neq i$ such that $w_1(j)=1$. Then there is a unique word w_3 of weight 3 such that $w_3(j)=1$ and a unique coordinate ℓ such that $w_3(\ell)=w_2(\ell)=1$. The set of $p-1$ weight-3 words we obtain this way does not depend on the choice of w_1 among $\{w_1,w_2\}$. This shows that $\mathrm{wt}(\mathcal{K}^\perp)=3$ and that $M=\frac{n(p-1)}{3}=\frac{p(p^2-1)}{6}$. By the transitivity of its automorphism group, $\mathcal{K}^\perp$ is equidistributed, and by Proposition 4.2 we have $t=\frac{3M}{n}=p-1$.

The same kind of argument then allows us to enumerate weight-4 words, which completes the proof of the proposition. □

Remark 4.9. The only known perfect, integral lattices of minimum 3 in the range $[2,15]$ are those which lift the codes $\mathcal{H}_7$ (similar to $\mathbb{E}_7^*$) and $\mathcal{H}_{15}$. I conjecture that these two lattices are the only such perfect lattices, and even that the perfection bound $\frac{n(n+1)}{2}$ is not attained by the kissing number for $n\leq 13$, $n\neq 7$. This is proved in [M-V2] for $n\leq 9$. For $n=14$ (resp. 15), the largest known value for s is 112, given by the lift of $\mathcal{H}p_{14}$ (resp. 160).

Remark 4.10. The codes dual to $\mathcal{K}_n,\mathcal{H}p_n,\mathcal{H}_n$ all have weight $t+1$, and can be constructed using design structures on their sets of words of minimal weight. Probably, other examples could be constructed following the method we used for $\mathcal{K}(p)$. Due to the big gap which exists between $\frac{p(p+1)}{2}$ and 2^p-2, I do not expect the three examples above to be the only ones. *!e*

We end this section by describing a construction which doubles both the length and the distribution weight of an equidistributed code of weight 3. Let $\mathcal{C}$ be an $[n,k,3]$-code and let $\mathcal{D}$ be the code obtained by repeating $\mathcal{C}^\perp$. If $\mathcal{C}^\perp$ has minimal distance δ, this is an $[2(n-k),n-k,2\delta]$-code, having pairwise equal columns for any choice of a generator matrix G for it, an $(n-k)\times n$ matrix invariant under each of the n transpositions $(1,n+1)$, $(2,n+2)$, …, $(n,2n)$. Enlarge G to an $(n-k+1)\times n$ matrix $\widetilde{G}$ by adjoining a row having a one and a zero at each pair of equal columns of G. Then up to isomorphism, the code $\widetilde{\mathcal{D}}$ defined by $\widetilde{G}$ does not depend on the choice of G nor on the distribution of the ones and zeros in the last row (we shall for convenience put a 1 at the first n coordinates and a o at the last n), and its dual $\widetilde{\mathcal{C}}$ has weight 3.

We state the proposition below without giving its easy proof.

Proposition 4.11. *Let $\mathcal{C}$ be an $[n,k,3]$-code having M words of weight 3. The its double $\widetilde{\mathcal{C}}$ is a $[2n,n+k-1,3]$-code having $\widetilde{M}=4M$ words of weight 3. If $\mathcal{C}$ is equidistributed with distribution weight k, $\widetilde{\mathcal{C}}$ is equidistributed with distribution weight $2k$.*

Applied to $\mathcal{C}=\mathcal{H}_n$, this construction yields $\mathcal{H}p_{2n}$; applied to $\mathcal{C}=\mathcal{H}p_n$, it yields the orthogonal of the (well-defined) code deduced from $\mathcal{H}_{2n+1}^{\perp}$ by deleting three columns adding to 0 [1].

5. Codes of weight 3: low length classification

In this section we consider an irreducible, equidistributed $[n,k,3]$ code $\mathcal{C}$ generated by its words of weight 3. This implies that $t\ge 2$. We shall often denote a word w of weight ℓ by its coordinates having $w(i)=1$: $w=(i_1,i_2,\dots,i_\ell)$, and most of the time, begin the enumeration of its weight-3 words with $w_1=(1,2,3)$, $w_2=(1,4,5)$, ..., $w_t=(1,2t,2t+1)$. We have

$$n\ge 2t+1 \quad\text{and}\quad \mathrm{wt}(C^{\perp})\ge t+1\,.$$

[For the second inequality, observe that a word $w\in C^{\perp}$ with $w(1)=1$ satisfies $w(i)=1$ for exactly one coordinate i in each of the 2-sets $\{2,3\}$,...,$\{2t,2t+1\}$, and may be for some coordinates $j>2t+1$.]

When n is close to its lower bound $2t+1$, we have:

Proposition 5.1. (1) *If $n>2t+1$ and $\mathbf{1}\in\mathcal{C}$, and in particular if t is odd, then $n\ge 2t+4$.*

(2) *If $n=2t+1$, then $n=2^p-1$ for some $p\ge 3$ and C is isomorphic to $\mathcal{H}_n$.*

(3) *If $n=2t+2$, then $n=2^p-2$ for some $p\ge 3$ and C is isomorphic to $\mathcal{H}p_n$.*

Proof. (1) The words $w_1,\dots,w_t$ and $\mathbf{1}$ add to $w=(2t+2,\dots,n)$, of weight $n-2t-1$.

(2) We may assume that $\mathcal{C}^{\perp}$ contains a word w of the form $(1,2,4,\dots,2t)$. Then words of weight 3 containing an even index i are of the form (i,i',j) with even i' and odd $j=j(i,i')$. Since $(1,i,i+1)$, $(1,i',i+1)$ and (i,i',j) add to $(i+1,i'+1,j)$, we see that for every pair (i_1,i_2) of coordinates, $\mathcal{C}$ contains a word of the form (i_1,i_2,i_3). This proves that $\mathcal{C}$ is perfect, hence that $n=2^p-1$ for some $p\ge 3$ and that $\mathcal{C}$ is isomorphic to $\mathcal{H}_n$.

(3) We assume as usual that $\mathcal{C}$ contains the words $w_1=(1,2,3)$, ..., $w_t=(1,2t,2t+1)$. Then $\mathcal{C}$ must also contain t words (i,j,n) with $1<i<j<n$ and $(1,i,j)\notin\mathcal{C}$. With (i,j,n), $\mathcal{C}$ also contain (i',j',n) such

[1] This produces a fourth family of codes of weight 3 whose automorphism group acts transitively on the coordinates; the code with $(n,k)=(12,4)$ of Theorem 5.6 is $\widetilde{\mathcal{H}p_6}$. Deleting from $\mathcal{H}_{2n+1}^{\perp}$two columns of three columns which do not add to zero yields non-equidistributed codes.

that $(1,i,i')$ and $(1,j,j') \in \mathcal{C}$; we may assume that these words are $(2,4,n)$, $(6,8,n)$, ..., and their "odd" counterparts $(3,5,n)$, $(7,9,n)$, ...

We now consider the code $\widetilde{\mathcal{C}}$ which extends $\mathcal{C}$ to length $n+1$, generated by $\mathcal{C}$ and the word $w_0 = (1,n,n+1)$. The words of $\widetilde{\mathcal{C}}$ are those of $\mathcal{C}$ and the new words $\widetilde{w} = w + w_0$, $w \in \mathcal{C}$. Note that the number r of components that w and w_0 have in common is at most 2, and that denoting by m the weight of w, that of $\widetilde{w}$ is $m+3$, $m+1$, or $m-1$ if $r = 0,1,2$, respectively, and that if $m = 3$, then $r = 0$ or 1. This shows the lower bounds $\mathrm{wt}(\widetilde{w} \ge m+1 \ge 4$ if $m = 3$ or $w = 0$, and $\mathrm{wt}(\widetilde{w} \ge m-1 \ge 4$ if $m > 3$. Hence $\mathrm{wt}(\widetilde{\mathcal{C}}) = 3$.

For the number $\tilde{t}(i)$ of weight-3 words of $\widetilde{\mathcal{C}}$ containing a given component i, we have $\tilde{t}(i) = t+1$ if $i = 1$ or n, and if $i \in (2,n)$, then $\mathcal{C}$ contains a unique word of the form (i,j,n), and also the related word (i',j',n). We have

$$(i',j',n) + (1,i,i') + (1,n,n+1) = (i,j',n+1)\,,$$

which bounds from below by $t+1$ all $\tilde{t}(i)$ with $2 \le i \le n-1$ and also $\tilde{t}(n+1)$. Hence $\mathcal{C}$ is an equidistributed code of length $2t(\widetilde{\mathcal{C}})+1$, which is consequently isomorphic to $\mathcal{H}_{n+1}$, and $\mathcal{C}$ is its punctured code $\mathcal{H}p_n$. □

Given an equidistributed code, we know the value of M $(= \frac{tn}{3})$ by Proposition 4.2. The proposition below gives the value of the dimension k for codes with $t = 2$. It would be interesting to prove formulae for larger values of t, or at least to find sharp lower and upper bounds for the dimension.

Proposition 5.2. *If $\mathcal{C}$ is an equidistributed code with $t = 2$ (irreducible, generated by weight-3 words), then*

$$M = \tfrac{2n}{3} \text{ and } k = M - 1\,.$$

Proof. Let W be the set of weight-3 words of $\mathcal{C}$, let W' be a minimal subset of W on which we have $\sum_{w \in W'} w = 0$, and let T' be the support of W'. Every coordinate $i \in T'$ belongs to an even number of words of W', hence to exactly two words because $k = 2$. Hence a word $x \in W \smallsetminus W'$ cannot meet any word of W', and since $\mathcal{C}$ is generated by W, it is the concatenation of the codes generated by W' and by $W \smallsetminus W'$. Since $\mathcal{C}$ is irreducible, we have $W = W'$, hence $\sum_{w \in W} w = 0$ is the unique linear relation between weight-3 words of $\mathcal{C}$. □

The following proposition provides a classification result in (very) low dimensions together with some information on the weight of the dual codes, which we shall use later to push forward the classification results stated below.

Proposition 5.3. *Let $\mathcal{C}$ is an equidistributed code with $t \ge 2$ (irreducible, generated by weight-3 words).*

(1) *If $t = 2$ then either $\mathcal{C}$ is isomorphic to $\mathcal{H}p_6 \simeq \mathcal{K}_6$, or to a code containing the words $w_1 = (1,2,3)$, $w_2 = (1,4,5)$, $w_3 = (2,6,7)$, and $w_4 = (3,8,9)$.*

(2) *If* $n \leq 10$*, the* $\mathcal{C}$ *is isomorphic to* $\mathcal{H}p_6 \simeq \mathcal{K}_6$*,* $\mathcal{H}_7$*,* $\mathcal{K}_{10}$*, or to the* $[9,5,3]$*-code* $\mathcal{C}_9$ *with* $k=2$ *and weight-*3 *words* w_1, w_2, w_3, w_4*,* $w_5 = (4,6,8)$ *and* $w_6 = (5,7,9)$*.*

(3) $\mathrm{wt}(\mathcal{C}^\perp)$ *is bounded from below by* 4 *if* $t=2$ *and by* 6 *if* $t \geq 3$ *except it* $\mathcal{C}$ *is one of the four codes* $\mathcal{H}p_6$ $(k=2,\ \mathrm{wt}(\mathcal{C}^\perp)=3)$*,* $\mathcal{H}_7$ *or* $\mathcal{K}_{10}$ $(t=3$ and $\mathrm{wt}(\mathcal{C}^\perp)=4)$*, and* $\mathcal{C} = \mathcal{K}_{15}$ $(k=4,\ \mathrm{wt}(\mathcal{C}^\perp)=5)$*.*

Proof. We first observe that because of the inequalities $n \geq 2t+1$ and $\mathrm{wt}(\mathcal{C}^\perp) \geq t+1$, it suffices to consider codes with $t=2$, 3 or 4; and that the four codes listed in (3) are indeed exceptions (note in particular that $\mathcal{H}p_6$ is isodual). We now consider successively the three possible values for t.

$\underline{t=2}$. We may assume that $\mathcal{C}$ contains the words $w_1 = (1,2,3)$ and $w_2 = (1,4,5)$. If $\mathcal{C}$ contains a word $w_3 = (i_1, i_2, j)$ with $i_1 \in \{2,3\}$ and $i_2 \in \{4,5\}$, we may assume that $w_3 = (2,4,6)$, then w_1, w_2, w_3 generate a code $\mathcal{C}_0$ isomorphic to $\mathcal{H}_6$, and since $\mathcal{C}$ is irreducible, we have $\mathcal{C} = \mathcal{C}_0$. Otherwise we may assume that $\mathcal{C}$ also contains the words w_3 and w_4 above.

This proves (1), and shows that we may assume that a word $w \in \mathcal{C}^\perp$ with $w(1)=1$ also has $w(2)=w(4)=1$, hence also $w(6)=1$ or $w(7)=1$, which proves (3) for $t=2$.

Finally if $n>6$, since $n \equiv 0 \mod 3$, we have $n \geq 12$ or $n=9$, and in the latter case, for a word $(4,i,j) \in \mathcal{C}$, we must have, say, $i \in \{6,7\}$ and $j \in \{8,9\}$, and we obtain a code isomorphic to $\mathcal{C}_9$, with e.g. $w_5 = (4,6,8)$ and $w_6 = (5,7,9)$.

$\underline{t=3}$. We start with $w_1 = (1,2,3)$, $w_2 = (1,4,5)$ and $w_3 = (1,6,7)$. If there is a word $w_4 = (i_1,i_2,i_3)$ with $i_j \leq 7$, say, $w_4 = (2,4,6)$ (which is necessary if $n=7$), then $\mathcal{C}$ also contains the three words $(3,5,6)$, $(3,4,7)$ and $(2,5,7)$. We obtain this way a unique code with $t=3$, necessarily isomorphic to $\mathcal{H}_7$, and such a code does not extend to a code with $t=3$ and $n>7$.

If $n>7$, we have $n \geq 10$ by Proposition 5.1, and if $n=10$, then $\mathcal{C}$ contains $w_0 = (8,9,10)$. This shows that $\mathcal{C}$ may not contain words of the form (i,j,j') with $i \leq 7$ and $j,j' \geq 8$, so that we may assume that $\mathcal{C}$ contains $w_4 = (2,4,8)$, $w_5 = (2,6,9)$ and $w_6 = (4,6,10)$ (we have $w_4+w_5+w_6 = w_0$). This unique code is necessarily isomorphic to $\mathcal{K}_{10}$.

Finally if $\mathrm{wt}(\mathcal{C}^\perp) = 4$, we may assume that $\mathcal{C}^\perp$ contains $w = (1,2,4,6)$. Then words of weight 3 containing 2 or 4 may be assumed to be $(2,4,8)$ and $(2,6,9)$, unless one of them is $(2,4,7)$, and $\mathcal{C}$ is then one of the codes $\mathcal{K}_{10}$ or $\mathcal{H}_7$.

$\underline{t=4}$. We start with $w_1 = (1,2,3)$, $w_2 = (1,4,5)$, $w_3 = (1,6,7)$ and $w_4 = (1,8,9)$. We may assume that $\mathcal{C}^\perp$ contains a word w with ones at $1,2,4,6,8$. If $\mathrm{wt}(w) > 5$, we then have $n \geq 10$, hence $n \geq 12$, which proves (2) in this case. It now suffices to consider the case when $w = (1,2,4,6,8)$.

We now show that $\mathcal{C}$ may not contain a word of the form (i_1,i_2,j) with $i_1, i_2 \leq 8$ even and $j \leq 9$ odd, say, $w_5 = (2,4,7)$, hence also $(2,5,6)$, $(3,4,6)$, and $(3,5,7)$. To push $t(i)$, $i=2,4,6$ to $t(i)=4$, we need add words such as $(2,8,10)$, $(4,8,11)$, $(6,8,12)$, hence also $(3,9,10)$, $(5,9,11)$, $(7,9,12)$, and since $(3,5,7)+(5,9,11)+(7,9,12)=(3,11,12)$, we have $t(3)\ge 5$, a contradiction.

We may now assume that $\mathcal{C}$ contains $w_5=(2,4,10)$, $w_6=(2,6,11)$ and $w_7=(2,8,12)$. We exclude as above a word of the form $(4,6,12)$ (which would imply $t(12)\ge 5$), and may thus go on with $w_8=(4,6,13)$, $w_9=(4,8,14)$ and $w_{10}=(6,8,15)$. We have found a unique code, which must be isomorphic to $\mathcal{K}_{15}$.

This proves (2) and (3) for $t=4$ and completes the proof of the proposition. □

Remark 5.4. The automorphism groups of the four codes of Proposition 5.3 are all generated by products of a constant number of disjoint transpositions and act transitively on the coordinates and on the sets of words having a given weight. Only $\mathcal{C}_9$ needs a proof. One checks that $\mathrm{Aut}(\mathcal{C}_9)$ is a group of order 72 generated by convenient products of 3 disjoint transpositions (typically, $(2\,5)(3\,4)(6\,9)$), which can be identified by its action on weight-3 words with a maximal solvable transitive subgroup of $\mathfrak{S}_6$.

Remark 5.5. The classification of Proposition 5.3 remains true without any restriction on the codes. This is no longer true in higher dimensions: the code $\mathcal{H}_6\perp\mathcal{H}_6$ is reducible, and possesses an irreducible enlargement with a weight-4 word; both have $t=2$.

We now turn to classification in higher dimensions. We shall make direct calculations when $k=2$ and make use when $k=3$ of results on the dual code proved in Proposition 5.3. We observe that Lemma 4.7 shows that for the dimension k^* of the dual code, we have $2^{k^*}\ge n+1$, and even $2^{k^*}\ge n+2$ if $\mathcal{C}$ is not a Hamming code $\mathcal{H}_n$, and that given k^*, a code with weight $w\ge 3$ is dual to a code extracted from the columns of the $k^*\times n$ matrix defining the dual of $\mathcal{H}_n$, $n=2^{k^*}-1$. This extraction procedure can be used when k^* is known and $n-k^*$ not too large.

Theorem 5.6. *Let $\mathcal{C}$ is an equidistributed code with $t\ge 2$ (irreducible, generated by weight-3 words), of dimension $n\le 14$. Then $\mathcal{C}$ is one of the eight codes displayed in the numerical appendix:*

$t=2$: $\mathcal{C}_6$, $\mathcal{C}_9$, $\mathcal{C}_{12a}$, $\mathcal{C}_{12b}$; $t=3$: $\mathcal{C}_7$, $\mathcal{C}_{10}$; $t=4$: $\mathcal{C}_{12c}$; $t=6$: $\mathcal{C}_{14}\simeq\mathcal{H}p_{14}$.

In dimension 15, there exists such codes with $t=2$ (at least two), 3, 4 and 7.

Proof. By Proposition 5.3, it suffices to consider lengths $n\in[11,15]$, and the case when $n=15$ results from the numerical appendix.

First consider a code C with $t=3$. We then have $\mathrm{wt}(C^\perp)\ge 6$ and $\dim C^\perp\ge 4$, and an easy inductive calculation shows that for $n=9,11,12$, the maximal dimension of a code of weight $w\ge 6$ is 2, 3, and 12, respectively. In each case there a unique code, which is even. Using this result, we easily check that in length 13, the maximal dimension is again 4. This proves the theorem for $n = 11$, an and inspection of the sections of H_{15}^* shows that there is no equidistributed code in of length 13 and a unique one of length 12, which has $t = 4$.

The case of length 14 is more difficult. We must have $t = 3$ or 6, and if $t = 6$, the unique possibility is $\mathcal{H}p_{14}$. Otherwise $C^\perp$ must be an even code of weight 6 and dimension $k^* \geq 5$, hence 5. This is proved by classifying $[n \leq 13, 4, 3]$-codes; see Appendix 2.

There remains to consider the case when $t = 2$. By Proposition 5.3, we may start with $w_1 = (1, 2, 3)$, $w_2 = (1, 4, 5)$, $w_3 = (2, 6, 7)$ and $w_4 = (3, 8, 9)$, and must avoid words (i_1, i_2, i_3) with $i_j \leq 9$; also there can be at most three words of the form (i, i_2, i_3) with $i \leq 9$ and $j_1, j_2 \geq 10$, and three such words will add to a word (i_1, i_2, i_3), a possibility which we have discarded. Hence we may go on with $w_5 = (4, 6, 10)$ and either $w_6 = (5, 7, 11)$ or $w_6 = (5, 8, 11)$.

If $w_6 = (5, 7, 11)$ then $w_1 + w_2 + w_4 + w_5 + w_6 = (3, 10, 11)$, which implies $t(3) > 2$. Hence we choose $w_6 = (5, 8, 11)$, and the last two words must must be of the form $(i, j, 12)$ and $(i', j', 12)$, with $i = 7$ and $j = 9, 10, 11$, but if $w_7 = (7, 10, 11)$, we then have $w_3 + w_5 + w_7 = (2, 4, 12)$, hence $t(2) > 2$. Choosing, $j = 9, 11$ we obtain the codes $\mathcal{C}_{a12}$, $\mathcal{C}_{b12}$, respectively. □

Remark 5.7. (1) The automorphism groups of the codes of length $n \leq 15$ displayed in the numerical appendix act transitively on the coordinates, except those of $\mathcal{C}_{a12}$, $\mathcal{C}_{a15}$ and $\mathcal{C}_{b15}$.

(2) The same transitivity property holds for the even extension to length 16 of $\mathcal{C}_{c15}$, a code which is dual to Bachoc-Gaborit's $[16, 6, 6]$-code quoted in Example 2.3, (3).

APPENDIX 1: GENERATOR MATRICES of WEIGHT 3

The list below together with $\mathcal{C}_{14} = \mathcal{H}p_{14}$ is complete up to length 14.

$$\mathcal{C}_6 \simeq \mathcal{H}p_6 \simeq \mathcal{K}_6 \, : \begin{pmatrix} 1&1&1&0&0&0 \\ 1&0&0&1&1&0 \\ 0&1&0&1&0&1 \end{pmatrix} ; \qquad \mathcal{C}_7 \simeq \mathcal{H}_7 \, : \begin{pmatrix} 1&1&1&0&0&0&0 \\ 1&0&0&1&1&0&0 \\ 1&0&0&0&0&1&1 \\ 0&1&0&1&0&1&0 \end{pmatrix} .$$

$$\mathcal{C}_9 \, : \begin{pmatrix} 1&1&1&0&0&0&0&0&0 \\ 1&0&0&1&1&0&0&0&0 \\ 0&1&0&0&0&1&1&0&0 \\ 0&0&1&0&0&0&0&1&1 \\ 0&0&0&1&0&1&0&0&1 \end{pmatrix} ; \qquad \mathcal{C}_{10} \simeq \mathcal{K}_{10} \, : \begin{pmatrix} 1&1&1&0&0&0&0&0&0&0 \\ 1&0&0&1&1&0&0&0&0&0 \\ 1&0&0&0&0&1&1&0&0&0 \\ 0&1&0&1&0&0&0&1&0&0 \\ 0&0&1&0&0&1&0&0&1&0 \\ 0&0&0&1&0&1&0&0&0&1 \end{pmatrix} .$$

$$\mathcal{C}_{a12} \, : \begin{pmatrix} 1&1&1&0&0&0&0&0&0&0&0&0 \\ 1&0&0&1&1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&1&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0&1&1&0&0&0 \\ 0&0&0&1&0&1&0&0&0&1&0&0 \\ 0&0&0&0&1&0&0&1&0&0&1&0 \\ 0&0&0&0&0&0&1&0&1&0&0&1 \end{pmatrix} \qquad \mathcal{C}_{b12} \, : \begin{pmatrix} 1&1&1&0&0&0&0&0&0&0&0&0 \\ 1&0&0&1&1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&1&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0&1&1&0&0&0 \\ 0&0&0&1&0&1&0&0&0&1&0&0 \\ 0&0&0&0&1&0&0&1&0&0&1&0 \\ 0&0&0&0&0&0&1&0&0&0&1&1 \end{pmatrix}$$

$$\mathcal{C}_{c12}\ :\ \begin{pmatrix} 1&1&1&0&0&0&0&0&0&0&0&0\\ 1&0&0&1&1&0&0&0&0&0&0&0\\ 1&0&0&0&0&1&1&0&0&0&0&0\\ 1&0&0&0&0&0&0&1&1&0&0&0\\ 0&1&0&1&0&0&0&0&0&1&0&0\\ 0&1&0&0&0&1&0&0&0&0&1&0\\ 0&1&0&0&0&0&0&1&0&0&0&1\\ 0&0&0&1&0&0&1&0&0&0&0&1 \end{pmatrix}\ .$$

$$\mathcal{C}_{a15}\ :\ \begin{pmatrix} 1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\ 1&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&1&1&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&1&1&0&0&0&0&0&0\\ 0&0&0&1&0&1&0&0&0&1&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&0&0&1&1&0&0&0\\ 0&0&0&0&0&0&1&0&0&0&1&0&1&0&0\\ 0&0&0&0&0&0&0&1&0&1&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&1&0&0&1&0&0&1 \end{pmatrix}\ ;\qquad \mathcal{C}_{b15}\ :\ \begin{pmatrix} 1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\ 1&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&1&1&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&1&1&0&0&0&0&0&0\\ 0&0&0&1&0&1&0&0&0&1&0&0&0&0&0\\ 0&0&0&0&1&0&0&1&0&0&1&0&0&0&0\\ 0&0&0&0&0&0&1&0&0&0&0&1&1&0&0\\ 0&0&0&0&0&0&0&0&1&0&0&0&0&1&1\\ 0&0&0&0&0&0&0&0&0&1&0&1&0&1&0 \end{pmatrix}\ .$$

$$\mathcal{C}_{c15}\ :\ \begin{pmatrix} 1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\ 1&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\ 1&0&0&0&0&1&1&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&1&1&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0&0&1&1&0&0&0&0\\ 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\ 0&0&0&1&0&0&0&0&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&0&1&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0&0&1&0&0&0&0&1\\ 0&0&0&0&1&0&0&0&1&0&0&0&0&0&1 \end{pmatrix}\ ;\quad \mathcal{C}_{d15}\simeq\mathcal{K}_{15}\ :\ \begin{pmatrix} 1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\ 1&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\ 1&0&0&0&0&1&1&0&0&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\ 0&1&0&1&0&0&0&0&0&1&0&0&0&0&0\\ 0&1&0&0&0&1&0&0&0&0&1&0&0&0&0\\ 0&1&0&0&0&0&0&1&0&0&0&1&0&0&0\\ 0&0&0&1&0&1&0&0&0&0&0&0&1&0&0\\ 0&0&0&1&0&0&0&1&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&1&0&0&0&0&0&0&1 \end{pmatrix}\ .$$

Remark.

- $\mathcal{C}_{14}=\mathcal{H}p_{14}$ and $\mathcal{C}_{e15}=\mathcal{H}_{15}$ must be added to the list above.
- $\mathcal{C}_{c15}$ is dual to Bachoc-Gaborit's C_{15} of [B-G]; see Remark 5.7.

APPENDIX 2: GENERATOR MATRICES of WEIGHT 6

To complete the proof of Theorem 5.6 we list the even $[13,4,w\geq 6]$-codes, which is done inductively from the even $[11,2,w\geq 6]$- and $[12,3,w\geq 6]$-codes. We only list below *primitive codes*, those which do not trivially extend a code of lower length, and thus consider primitive codes of length $n\leq 11,12,13$ having dimensions $d=2,3,4$, respectively. Actually it suffices to consider codes of weight 6.

For $d=2$ we trivially have one code for each length $n=9,10,11$. The $[9,2,6]$-codes is made of the three blocks $\{1,2,3\}$, $\{4,5,6\}$ and $\{7,8,9\}$. It has a unique extension to $n=11$ and three primitive extensions to $n=12$, generated! by a word with ones at $\{10,11,12\}$ and three extra ones belonging to one, two, or three of the blocks above.

The $[11,3,6]$-code, that we denote by $F_{11,3}$ is better understood as a kind of concatenation of the $[8,4,3]$-code d_8 with the $[3,2,2]$-code. It has a unique extension to $n=12$, in which we replace d_8 by d_8^+, the code for $\mathbb{E}_8$. We display below a generator matrix for this code, the dual of which is $\mathcal{C}_{c12}$; $F_{11,3}$ is obtained by deleting from it the last row and the last column:

$$F_{12,4}=\begin{pmatrix} 1&1&1&1&0&0&0&0&1&1&0&0\\ 1&1&0&0&1&1&0&0&1&0&1&0\\ 1&1&0&0&0&0&1&1&0&1&1&0\\ 1&0&1&0&1&0&1&0&1&0&0&1 \end{pmatrix}\ .$$

We now turn to the classification of even $[n \leq 13, 4, 6]$-codes, making use of automorphisms of the codes of dimension 3 that we found above. It turns out that the generator matrices of extensions of the three primitive $[12, 3, 6]$-codes all have a pair of columns of the form ${}^t(0, 0, 0, 1)$, so that all these extensions indeed extend the $[11, 3, 6]$-code. Simple calculations show that there exactly four primitive even $[12, 3, 6]$-codes, namely

$$F_{13,4a} = \begin{pmatrix} 1&1&1&1&0&0&0&0&1&1&0&0&0 \\ 1&1&0&0&1&1&0&0&1&0&1&0&0 \\ 1&1&0&0&0&0&1&1&0&1&1&0&0 \\ 1&0&0&0&0&0&0&0&1&1&1&1&1 \end{pmatrix} ; \quad F_{13,4b} = \begin{pmatrix} 1&1&1&1&0&0&0&0&1&1&0&0&0 \\ 1&1&0&0&1&1&0&0&1&0&1&0&0 \\ 1&1&0&0&0&0&1&1&0&1&1&0&0 \\ 1&1&1&0&1&0&0&0&0&0&0&1&1 \end{pmatrix} ;$$

$$F_{13,4c} = \begin{pmatrix} 1&1&1&1&0&0&0&0&1&1&0&0&0 \\ 1&1&0&0&1&1&0&0&1&0&1&0&0 \\ 1&1&0&0&0&0&1&1&0&1&1&0&0 \\ 1&0&1&0&1&0&0&0&1&0&0&1&1 \end{pmatrix} ; \quad F_{13,4d} = \begin{pmatrix} 1&1&1&1&0&0&0&0&1&1&0&0&0 \\ 1&1&0&0&1&1&0&0&1&0&1&0&0 \\ 1&1&0&0&0&0&1&1&0&1&1&0&0 \\ 1&0&1&0&1&0&1&0&0&0&0&1&1 \end{pmatrix} .$$

Using these data it is easy to run through all extensions to length 14 and dimension 5 of the five matrices above, discarding those which have a zero column or two equal columns, so as to keep only those defining a dual code of weight at least 3, and to check that no equidistributed dual code shows up. This completes the proof of Theorem 5.6.

I have also constructed inductively some $[n, n-9, 6]$-codes for $n = 14$ to 18, keeping at each step one code per weight distribution. I obtained this way one code with $n = 17$ and $n = 18$, both equidistributed with $t = 24$ and $t = 34$, respectively. Here is a generator matrix for length 18; deleting the last row and the last column yields the code for $n = 17$:

$$F_{18,9} = \begin{pmatrix} 1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0 \\ 1&0&0&1&0&1&0&0&1&1&1&0&0&0&0&0&0&0 \\ 1&1&0&0&0&1&1&0&0&1&0&1&0&0&0&0&0&0 \\ 1&1&0&1&0&0&0&0&1&0&0&0&1&1&0&0&0&0 \\ 1&1&1&0&0&0&0&0&0&1&0&0&1&0&1&0&0&0 \\ 1&1&0&0&0&0&1&0&0&0&1&0&0&0&1&1&0&0 \\ 1&1&0&1&0&0&0&0&0&1&0&0&0&0&0&1&1&0 \\ 1&1&0&0&1&0&0&0&1&0&0&0&0&0&0&0&1&1 \end{pmatrix} .$$

By lack of a reliable isomorphism test I cannot assert that the list lattices I found in lengths $14-18$ is complete. If it is, $F_{18,9}$ is then necessarily isodual, and $F_{17,8}$ is isomorphic to the even subcode of its dual (of weight 5).

References

[B] C. Bachoc, *Designs, groups, and Lattices*, J. Th. Nombres de Bordeaux (issue dedicated to the Journées Arithmétiques of Graz, 2003) **17** (2005), 25–44.

[B-G] C. Bachoc, Ph. Gaborit, *Designs and self-dual codes with long shadows*, J. Comb. Th., A **105** (2004), 15–34.

[B-V] C. Bachoc, B. Venkov, *Modular forms, lattices and spherical designs*, [M1], 87–111.

[C-vL] P.J. Cameron, J.H. van Lint, Designs, Graphs, Codes and their Links, Student Text **22** of the London Mathematical Society, Cambridge University Press, Cambridge, 1991.

[M1] J. Martinet (ed), *Réseaux Euclidiens, designs sphériques et formes modulaires*, Monogr. Enseign. Math. **37**, Genève (2001).

[M2] J. Martinet, *Perfect lattices in Euclidean spaces*, Grundlehren **327**, Springer-Verlag, Heidelberg, 2003.

[K-M-S] W. Keller, J. Martinet, A. Schürmann, *On classifying Minkowskian sublattices*, Math. Comp., **81** (2012), 1063-1092; see also arXiv:0904.3110v3 [math.NT].

[M-V1] J. Martinet, B. Venkov, *Les réseaux fortement eutactiques (with an appendix by R. Coulangeon)*, [M1], 112–134.

[M-V2] J. Martinet, B. Venkov, *On integral lattices having an odd minimum*, Algebra and Analysis (Saint-Petersburg) **16, 3** (2004), 99–142.

[V] B. Venkov, *Réseaux et "designs" sphériques (notes by J. Martinet)*, [M1], 10–86.

Université de Bordeaux, Institut de Mathématiques, 351, cours de la Libération, 33405 Talence cedex, France

E-mail address: `Jacques.Martinet@math.u-bordeaux1.fr`