Graphs and Combinatorics (2019) 35:633–652 https://doi.org/10.1007/s00373-019-02019-0

Special LCD codes from Peisert and generalized Peisert graphs

J.D. Key*and B.G. Rodrigues‡
School of Mathematics, Statistics and Computer Science
University of KwaZulu-Natal
Durban 4000, South Africa

February 23, 2019

Abstract

We examine binary and ternary codes from adjacency matrices of the Peisert graphs, $\mathcal{P}^*(q)$, and the generalized Peisert graphs, $G\mathcal{P}^*(q)$, in particular those instances where the code is LCD and the dual of the code from the graph is the code from the reflexive graph. This occurs for all the binary codes and for those ternary codes for which $q \equiv 1 \pmod 3$. We find words of small weight in the codes, which, in the reflexive case, are likely to be minimum words. In addition we propose a decoding algorithm that can be feasible for these LCD codes.

Keywords: LCD codes; Peisert graphs; strongly regular graphs
Mathematics Subject Classifications: 05C50, 94B05

1 Introduction

We examine LCD (linear with complementary dual) [8] codes from adjacency matrices of the strongly regular Peisert self-complementary graphs $\mathcal{P}^*(q)$ [10], and the strongly regular generalized Peisert $G\mathcal{P}^*(q)$ [9] graphs, where $q = p^{2t}$, $t \geq 1$, and $p \equiv 3 \pmod 4$ is a prime, in the case when the dual code is the code of the reflexive graph; these graphs have the same parameters as those of Paley graphs, $P(q)$ [3, p.35], *viz.* $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$. We find words of small weight in the binary and ternary codes of these, and some indications from computations that the square root bound holds for the codes, as it is shown to hold for those from Paley graphs when q is a prime: see [1, Chapter 2], for example.

When Massey [8] introduced the terminology for LCD codes, i.e. p-ary linear codes C for which $C \cap C^{\perp} = \{0\}$, he showed that a specific map, the orthogonal projector map Π_C (see Section 3 below), is defined for such codes, and that this map is of relevance in decoding as it specifies how a vector in the ambient space is written uniquely as a sum of two vectors, one in C and the other in $C^{\perp}$. In [6] we showed that if the code C from the row span of an adjacency matrix A for a graph has the property that its dual, $C^{\perp}$, is the row span of $A + I$, where I is the identity matrix, then the code is LCD and the projector map Π_C is given immediately. We called

*Email:keyj@clemson.edu
†Email:rodrigues@ukzn.ac.za
‡This work is based on the research supported by the National Research Foundation of South Africa (Grant Numbers 95725 and 106071)

such codes reflexive LCD codes, $RLCD$ for short. We showed in [6] that p-ary codes of strongly regular graphs with parameters those of Paley graphs, are $RLCD$ if $q \equiv 1 \pmod p$. Massey [8] also introduced a decoding method for LCD codes that involved a map φ from $C^\perp$ to C where for $v \in C^\perp$, $\varphi(v)$ is the word in C closest to C. We show how this can be done for $RLCD$ codes using a computational method, feasible for a small number of errors.

In this work we examine the binary and ternary $RLCD$ codes from the Peisert and generalized Peisert graphs, and find words of small weight in the codes.

We summarize our results in the following theorem:

Theorem 1 *Let $q = p^{2t}$ where $p \equiv 3 \pmod 4$ is a prime, and let Γ denote either the Peisert graph, $\mathcal{P}^*(q)$, or the generalized Peisert graph, $G\mathcal{P}^*(q)$. Let $K = \mathbb{F}_q$, ω a primitive root for $K^\times$, and $F = \mathbb{F}_{p^t}$. Let C_r, for $r = 2, 3$, denote the binary or ternary code, respectively, from an adjacency matrix for Γ, and RC_r that for the reflexive graph $R\Gamma$. Then*

1. *$RC_2 = C_2^\perp$ for all q and $RC_3 = C_3^\perp$ for all q with $3 \nmid q$.*

2. *for $r = 2$, or $r = 3$ and $3 \nmid q$, C_r is a $[q, \frac{1}{2}(q-1), d]_r$ code and RC_r is a $[q, \frac{1}{2}(q+1), d^\perp]_r$ code where*

   (a) for $\Gamma = \mathcal{P}^*(q)$ and $p^t \equiv 3 \pmod 4$, $\frac{1}{2}(p^t + 5) \le d \le 2(p^t - 1)$ with C_r containing words of weight $2(p^t - 1)$ with support $F^\times \cup \omega F^\times$, and $d^\perp \le p^t$ with RC_r containing words of weight p^t with support yF for certain $y \in K$; for $r = 2$ and $p^t \equiv 1 \pmod 4$, $d \le \frac{1}{4}(q-1)$ with C_r containing words of weight $\frac{1}{4}(q-1)$ with support $\langle \omega^4 \rangle$.

   (b) for $\Gamma = G\mathcal{P}^*(q)$, $d \le 2(p^t - 1)$ with C_r containing words of weight $2(p^t - 1)$ with support $u_1F^\times \cup u_2F^\times$ where u_1, u_2 are suitable elements of K, and $d^\perp \le p^t$ with RC_r containing words of weight p^t with support yF for certain $y \in K$.

3. *If $P = \mathrm{Aut}(\mathcal{P}^*(q))$ and $GP = \mathrm{Aut}(G\mathcal{P}^*(q))$, then both P and GP contain the translation group on K. In addition, P contains automorphisms $\gamma : x \mapsto \omega^4 x$ and $\delta : x \mapsto \omega x^p$, while GP contains automorphisms $\gamma : x \mapsto \omega^{p^t+1} x$ and $\delta : x \mapsto \omega^{(p^t-1)/2} x^{p^t}$.*

The paper is organised as follows: Section 2 gives some basic terminology. Section 3 gives some background on LCD and $RLCD$ codes, along with some of Massey's [8] original results . We include here some applications as to how his ideas can be used for decoding in the case of our binary $RLCD$ codes from graphs, and give an algorithm, following from Lemmas 1,2 in that section. Section 4 describes the Peisert and generalized Peisert graphs and their automorphisms; Section 5 finds small words in the binary codes; Section 6 examines the ternary codes. The nature of the small words is summarised in Tables 1 and 4. A lower bound for the minimum weight of the codes $C_p(\mathcal{P}^*(q))$ for $p^t \equiv 3 \pmod 4$ is found in Section 7. The proof of the theorem follows from the lemmas and propositions.

2 Background and terminology

The notation for codes and codes from incidence structures and graphs is as in [1]. For an incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{J})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{J}$, the **code $\boldsymbol{C_F(\mathcal{D}) = C_q(\mathcal{D})}$** of $\mathcal{D}$ over the finite field $F = \mathbb{F}_q$ is the space spanned by the incidence vectors of the blocks over F. If $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the **incidence vector** of $\mathcal{Q}$

by $\boldsymbol{v^{\mathcal{Q}}}$, and if $\mathcal{Q} = \{x\}$ where $x \in \mathcal{P}$, then we will write v^x. Thus $C_F(\mathcal{D}) = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F. For any $w \in F^{\mathcal{P}}$ and $P \in \mathcal{P}$, $\boldsymbol{w(P)}$ denotes the value of w at P.

All the codes here are **linear codes**, and the notation $[n, k, d]_q$ will be used for a q-ary code C of length n, dimension k, and minimum weight d, where the **weight** $\mathbf{wt}(\boldsymbol{v})$ of a vector v is the number of non-zero coordinate entries. Vectors in a code are also called **words**. For two vectors u, v the **distance** $\mathbf{d}(\boldsymbol{u}, \boldsymbol{v})$ between them is $\mathrm{wt}(u - v)$. The **support**, $\mathrm{Supp}(v)$, of a vector v is the set of coordinate positions where the entry in v is non-zero. So $|\mathrm{Supp}(v)| = \mathrm{wt}(v)$. A **generator matrix** for C is a $k \times n$ matrix made up of a basis for C, and the **dual** code $C^{\perp}$ is the orthogonal under the standard inner product $(,)$, i.e. $C^{\perp} = \{v \in F^n \mid (v, c) = 0 \text{ for all } c \in C\}$. The **hull**, $\mathrm{Hull}(C)$, of a code C is the self-orthogonal code $\mathrm{Hull}(C) = C \cap C^{\perp}$. A **check matrix** for C is a generator matrix for $C^{\perp}$. The **all-one vector** will be denoted by $\boldsymbol{\jmath}$, and is the vector with all entries equal to 1. If we need to specify the length **m** of the all-one vector, we write $\boldsymbol{\jmath}_{\mathbf{m}}$. A **constant vector** is a non-zero vector in which all the non-zero entries are the same. We call two linear codes **isomorphic** (or permutation isomorphic) if they can be obtained from one another by permuting the coordinate positions. An **automorphism** of a code C is an isomorphism from C to C. The automorphism group will be denoted by $\mathrm{Aut}(C)$, also called the permutation group of C, and denoted by $\mathrm{PAut}(C)$ in [5].

The **graphs**, $\Gamma = (V, E)$ with vertex set V and edge set E, discussed here are undirected with no loops, apart from the case where **all** loops are included, in which case the graph is called the **reflexive** associate of Γ, denoted by $R\Gamma$. If $x, y \in V$ and x and y are adjacent, we write $x \sim y$, and xy for the **edge** in E that they define. We can also consider the **complementary** graph, $\overline{\Gamma} = (V, \overline{E})$ where for $x, y \in V$, $x \neq y$, $x \sim y$ in Γ if and only if $x \not\sim y$ in $\overline{\Gamma}$. The **set of neighbours** of $x \in V$ is denoted by $N(x)$, and the **valency of** x is $|N(x)|$. Γ is **regular** if all the vertices have the same valency. A graph $\Gamma = (V, E)$, neither complete nor null, is **strongly regular graph** of type (n, k, λ, μ) if it is regular on $n = |V|$ vertices, has valency k, and is such that any two adjacent vertices are together adjacent to λ vertices and any two non-adjacent vertices are together adjacent to μ vertices. The complement $\overline{\Gamma}$ of the strongly regular graph Γ is also strongly regular of type $(n, n - k - 1, n - 2k + \mu - 2, n - 2k + \lambda)$. A graph is **symmetric** if its automorphism group acts transitively on both vertices and edges.

An **adjacency** matrix $A = [a_{x,y}]$ for Γ is a $|V| \times |V|$ matrix with rows and columns labelled by the vertices $x, y \in V$, and with $a_{x,y} = 1$ if $x \sim y$ in Γ, and $a_{x,y} = 0$ otherwise. Then $RA = A + I$ is an adjacency matrix for $R\Gamma$, and $\overline{A} = J - I - A$ one for $\overline{\Gamma}$, where $I = I_{|V|}$ and J is the $|V| \times |V|$ all-ones matrix. The row corresponding to $x \in V$ in A will be denoted by r_x, that in RA by s_x, and that in $\overline{A}$ by c_x. In the following, we may simply identify r_x and s_x with the support of the row, so $r_x = \{y \mid x \sim y\}$ and $s_x = \{x\} \cup \{y \mid x \sim y\}$.

The **code** over a field F of Γ will be the row span of an adjacency matrix A for Γ, and written as $C_F(A)$, $C_F(\Gamma)$, or $C_p(A)$, $C_p(\Gamma)$, respectively, if $F = \mathbb{F}_p$.

3 *LCD* and *RLCD* codes

The definition of *LCD* codes is from [8]:

Definition 1 (Massey[8]) *A linear code C over any field is a* **linear code with complementary dual** (*LCD*) *code if* $\mathrm{Hull}(C) = C \cap C^{\perp} = \{0\}$.

If C is an LCD code of length n over a field F, then $F^n = C \oplus C^\perp$. Thus the **orthogonal projector map** Π_C from F^n to C can be defined as a linear map [1] such that: for $v \in F^n$,

$$v\Pi_C = \begin{cases} v & \text{if } v \in C, \\ 0 & \text{if } v \in C^\perp \end{cases}, \tag{1}$$

This map is only defined if C (and hence also $C^\perp$) is an LCD code. Similarly then $\Pi_{C^\perp}$ is defined.

Note that for all $v \in F^n$,

$$v = v\Pi_C + v\Pi_{C^\perp}. \tag{2}$$

We will use [8, Proposition 4]:

Result 1 (Massey) *Let C be an LCD code of length n over the field F and let φ be a map $\varphi : C^\perp \mapsto C$ such that $u \in C^\perp$ maps to one of the closest codewords v to it in C. Then the map $\tilde{\varphi} : F^n \mapsto C$ such that*

$$\tilde{\varphi}(w) = w\Pi_C + \varphi(w\Pi_{C^\perp})$$

maps each $w \in F^n$ to one of it closest neighbours in C. [2]

Note: In Result 1, if $w \in C$ then $\tilde{\varphi}(w) = w$, and if $w \in C^\perp$ then $\tilde{\varphi}(w) = \varphi(w)$.

The terms we use here for the special LCD codes from graphs are from [6]:

Definition 2 *Let $\Gamma = (V, E)$ be a graph with adjacency matrix A. Let p be any prime, $C = C_p(A)$, $RC = C_p(RA)$ (for the reflexive graph). If $C = RC^\perp$ we call C a* **reflexive** *LCD code, and write $RLCD$ for such a code.*

Note: 1. As observed in [6], if C is a q-ary code of length n such that $C + C^\perp = \mathbb{F}_q^n$ then C is LCD.

2. In [6] we also defined the concept "complementary LCD" code, for short $CLCD$ codes, for graphs for which $C_p(\Gamma) = C_p(\overline{\Gamma})^\perp$ since such codes also give the components in C and $C^\perp$ of any word $w \in \mathbb{F}_p^V$. However, this concept is not of use to us here, so we omit discussion of it.

If $\Gamma = (V, E)$ is a graph, A an adjacency matrix for Γ and p a prime, let $C = C_p(A)$ and $RC = C_p(RA)$ using the notation as defined in Section 2, i.e. $RA = A + I$.

For any $x \in V$, with r_x, s_x as defined in Section 2, we have,

$$s_x = v^x + r_x. \tag{3}$$

From [6, Proposition 1]

Result 2 *Let $\Gamma = (V, E)$ be a graph, A an adjacency matrix, $R\Gamma$ its associated reflexive graph. Let p be any prime, $C = C_p(A)$, and $RC = C_p(RA)$.*

If $C = RC^\perp$, then C and RC are LCD codes. Further, if $v \in \mathbb{F}_p^V$, then

$$v = \sum_{x \in V} v(x)v^x = -\sum_{x \in V} v(x)r_x + \sum_{x \in V} v(x)s_x = v\Pi_C + v\Pi_{C^\perp},$$

where $v\Pi_C = -\sum_{x \in V} v(x)r_x$ and $v\Pi_{C^\perp} = \sum_{x \in V} v(x)s_x$. In particular, if $p = 2$ and if $v \in C$, $T = \mathrm{Supp}(v)$ then $v = \sum_{x \in T} r_x$, and similarly if $v \in C^\perp$, $R = \mathrm{Supp}(v)$ then $v = \sum_{x \in R} s_x$.

[1] Note typographical error on p.338, l.-11, in [8]

[2] Note typographical error on p.341, l.-7, in [8]

Thus the map $\tilde{\varphi}$ in Result 1 for an $RLCD$ code from an adjacency matrix A becomes, for $v \in \mathbb{F}_p^V$:

$$\tilde{\varphi}(v) = -\sum_{x \in V} v(x) r_x + \varphi(\sum_{x \in V} v(x) s_x),$$

given the map $\varphi : RC \mapsto C$ as described.

For $RLCD$ codes we can define the map φ partially and deduce a decoding algorithm for such codes, as described below.

Lemma 1 *Let $C = C_2(\Gamma)$ be the RLCD binary code from an adjacency matrix A for the graph $\Gamma = (V, E)$. Suppose C has minimum distance d and $t = \lfloor \frac{d-1}{2} \rfloor$.*

1. *For $J \subset V$ with $|J| \leq t$, the word in C closest to $\sum_{x \in J} s_x$ is $\sum_{x \in J} r_x$, distant $|J|$ from $\sum_{x \in J} s_x$.*
2. *For $|J| \leq t$ the map φ of Result 1 can be uniquely defined by $\varphi(\sum_{x \in J} s_x) = \sum_{x \in J} r_x$.*
3. *If $w = \sum_{x \in J} s_x$ where $|J| \leq t$ and also $w = \sum_{x \in K} s_x$ where $|K| \leq t$, then $K = J$*

Proof: For $|J| \leq t$, $K \subseteq V$, and $J \Delta K$ the symmetric difference of J and K,

$$\begin{aligned} d(\sum_{x \in J} s_x, \sum_{x \in K} r_x) &= \mathrm{wt}(\sum_{x \in J} s_x + \sum_{x \in K} r_x) = \mathrm{wt}(v^J + \sum_{x \in J \Delta K} r_x) \\ &= |J| + \mathrm{wt}(\sum_{x \in J \Delta K} r_x) - 2\mathrm{wt}(v^J \cap \sum_{x \in J \Delta K} r_x) \\ &\geq |J| + (2t+1) - 2|J| = 2t + 1 - |J| \geq t + 1 \end{aligned}$$

unless $K = J$, and the statements (1), (2) above follow.

For (3), suppose $\sum_{x \in J} s_x = \sum_{x \in K} s_x$. Then $\sum_{x \in J \Delta K} s_x = 0$. Thus $v^{J \Delta K} = \sum_{x \in J \Delta K} r_x \in C$. However, C has minimum distance $d \geq 2t+1$, so we must have $|J \Delta K| \geq 2t+1$. This is impossible since both J and K have size at most t. ■

This lemma allows for an algorithm to decode an $RLCD$ code $C = C_2(\Gamma)$ using the partial definition of φ for sums of at most t rows s_x as introduced in Lemma 1(2), provided that it is assured that no more than t errors can occur in the communication system.

We need first another lemma:

Lemma 2 *Let $C = C_2(\Gamma)$ have minimum distance d and $t = \lfloor \frac{d-1}{2} \rfloor$. If the transmitted word from C has no more than t errors, it can be correctly decoded.*

Proof: Suppose $c \in C$ is sent and $w = v^S = c + v^J$ is received, where $|J| \leq t$. Then $w = \sum_{x \in S} r_x + \sum_{x \in S} s_x = c + \sum_{x \in J} r_x + \sum_{x \in J} s_x$, so $\sum_{x \in S} r_x = c + \sum_{x \in J} r_x$ and $\sum_{x \in S} s_x = \sum_{x \in J} s_x$. By Lemma 1(3) the set J is unique, so if such a set J can be found to satisfy $\sum_{x \in S} s_x = \sum_{x \in J} s_x$ then the corrected word $\tilde{\varphi}(w) = \sum_{x \in S} r_x + \varphi(\sum_{x \in J} s_x) = \sum_{x \in S} r_x + \sum_{x \in J} r_x = c$, from what we said above. ■

To find the set J that will satisfy this we first compute separately all the sums $\sum_{x \in K} s_x$ for every subset $K \subset V$ of size k where $1 \leq k \leq t$. Let $\mathcal{S}_k = \{\sum_{x \in K} s_x \mid K \subset V, |K| = k\}$, for $1 \leq k \leq t$.

Suppose $w = v^S$ is the received word and that $s \leq t$ errors have occured. Form the sum $v = \sum_{x \in S} s_x$. If $v = 0$ then no errors have occurred. If $v \neq 0$ then we check the sets $\mathcal{S}_k$ to see if $v \in \mathcal{S}_k$, starting with $k = 1$ and then increasing k to s. Checking v against a vector involves $n = |V|$ computations and since $|\mathcal{S}_k| = \binom{n}{k}$ the worst case that can occur is that we need to make $n \sum_{k=1}^{s} \binom{n}{k}$ computations. This involves $\mathcal{O}(n^{s+1})$ computations. Once a set J is found such that $v = \sum_{x \in J} s_x$, we decode as $\sum_{x \in S} r_x + \sum_{x \in J} r_x = v^S + v^J$, which involves at most n computations, so that the worst case complexity remains at $\mathcal{O}(n^{s+1})$. For corrections up to the maximum for the code, i.e. $s = t$, this would be $\mathcal{O}(n^{t+1})$. For a small number of errors s this could be feasible.

Note: If the system allows more errors, then this method will not necessarily correct the received vector since one can have $\sum_{x \in J} s_x = \sum_{x \in K} s_x$ where $|J| > t$ and $|K| \leq t$. Since the set K will be unique, from what we showed above, the received word will be decoded incorrectly and the error will not be detected. However, if d is even, as in the graphs we study here, $d = 2t + 2$ then if $t + 1$ errors occur, the fact that there are errors will be detected, since if $\sum_{x \in J} s_x = \sum_{x \in K} s_x$ where $|J| = t + 1$ and $|K| \leq t$, then $|J \Delta K| \leq 2t + 1$ and thus $v^{J \Delta k}$ cannot be a codeword. Thus in this case the set K will not be found, which will show that more than t errors have occurred.

Example: The binary code C from the graph $\mathcal{P}^*(7^2)$ has parameters $[49, 24, 10]_2$ and thus will correct up to four errors, and, from what we said above, it will be able to detect five errors. With Magma the code was constructed, and the four sets of vectors $\mathcal{S}_k$ for $k = 1, 2, 3, 4$ constructed and stored. A random vector c from C was chosen, and then a random subset T of size $k \leq 4$ from the set of labelled vertices $\{1, \ldots, 49\}$ was taken. The word $c + v^T$ was then considered to be the received vector, and its support S obtained. The vector $v = \sum_{x \in S} s_x$ was formed and Magma then searched through the sets $\mathcal{S}_k$ for $k = 1, 2, 3, 4$ to find v. When the vector was found the decoding as explained above correctly gave the original vector $c \in C$. When five errors were introduced and the set $\mathcal{S}_5$ also examined, no vector was found, so decoding was not achieved, and thus we deduced that more than four errors had occurred.

The following two links give the Magma routine and the results of a run for $\mathcal{P}^*(7^2)$.
`http://cecas.clemson.edu/~keyj/Key/PeisertDecode49.m`
`http://cecas.clemson.edu/~keyj/Key/run49.txt`

4 The graphs

The Peisert graphs $\mathcal{P}^*(q)$ are defined in [10]:

Definition 3 *Let $q = p^{2t}$ where p is prime and $p \equiv 3 \pmod 4$. If ω is a primitive root of $\mathbb{F}_q$, let*

$$M = \langle \omega^4 \rangle \cup \omega \langle \omega^4 \rangle = \{\omega^j \mid j \equiv 0, 1 \pmod 4\}. \tag{4}$$

The graph $\mathcal{P}^*(q) = (V, E)$, where $V = \mathbb{F}_q$, has adjacency defined by $x \sim y$ if and only if $(x - y) \in M$.

It follows that $q \equiv 1 \pmod 8$, $\mathbb{F}_p^\times \subset M$, and it is shown in [10] that $\mathcal{P}^*(q)$ is a self-complementary symmetric graph, strongly regular with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$.

As mentioned in Section 2, we will write $r_x = \{x + y \mid y \in M\}$ and $s_x = \{x\} \cup \{x + y \mid y \in M\}$.

Peisert [10] determines the automorphism group of $\mathcal{P}^*(q)$ and we summarise his results from Theorem 3.1 and Lemma 4.1 in [10] as follows:

Result 3 *If $\Gamma = \mathcal{P}^*(q)$ where $q = p^{2t}$, p is prime, $p \equiv 3 \pmod 4$, and ω is a primitive root of $\mathbb{F}_q$, then, apart from $q = 3^2, 7^2, 9^2$ (where there are further automorphisms), $A = \mathrm{Aut}(\mathcal{P}^*(q))$ has order $qt(q-1)/2$ and is generated by the translations T and the automorphisms $\gamma : x \mapsto \omega^4 x$ and $\delta : x \mapsto \omega x^p$. In addition, if $p^t \equiv 1 \pmod 4$ then the involution $x \mapsto x^{p^t}$ is also in $\mathrm{Aut}(\mathcal{P}^*(q))$.*

Further, A is a rank-3 primitive permutation group with the two orbits of A_a, where $a \in \mathbb{F}_q$, consisting of those elements adjacent to a as one orbit, and those not adjacent to a as the other.

The automorphisms γ and δ of $\mathcal{P}^*(q)$ have order $\frac{q-1}{4}$ and $2t(p-1)$, respectively. Further, $\delta^{2t} = \gamma^{\frac{q-1}{4(p-1)}}$ and $|\langle\gamma,\delta\rangle| = \frac{t(q-1)}{2}$.

Generalized Peisert graphs $G\mathcal{P}^*(q)$ that give strongly regular graphs with the same parameters are defined in [9]:

Definition 4 *Let $q = p^{2t}$ where p is an odd prime, and let $n = p^t + 1$. If ω is a primitive root of $\mathbb{F}_q$, let*

$$\widehat{M} = \{\omega^{i+kn} \mid k \in \mathbb{Z}, 0 \le i \le \frac{n}{2} - 1\} = \dot{\bigcup}_{0 \le i \le \frac{n}{2}-1} \omega^i F^\times, \tag{5}$$

where $F = \mathbb{F}_{p^t}$, so $F^\times = \langle \omega^n \rangle$. The graph $G\mathcal{P}^*(q) = (V, E)$, where $V = \mathbb{F}_q$, has adjacency defined by $x \sim y$ if and only if $(x - y) \in \widehat{M}$.

As for the Peisert graphs, it follows that $q \equiv 1 \pmod 8$, $\mathbb{F}_p^\times \subset \widehat{M}$, and it is shown in [9] that $G\mathcal{P}^*(q)$ is strongly regular with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$.

So here, $r_x = \{x + y \mid y \in \widehat{M}\}$ and $s_x = \{x\} \cup \{x + y \mid y \in \widehat{M}\}$.

From [3, (2.18)Theorem], for example, we have the eigenvalues and multiplicities for these strongly regular graphs, where the λ_i are the eigenvalues for an adjacency matrix A and λ_i^* those for $A + I$:

- $\lambda_0 = \frac{1}{2}(q-1)$, $\lambda_0^* = \frac{1}{2}(q+1)$, $m_0 = 1$;
- $\lambda_1 = \frac{1}{2}(-1+p^t)$, $\lambda_1^* = \frac{1}{2}(1+p^t)$, $m_1 = \frac{1}{2}(q-1)$;
- $\lambda_2 = \frac{1}{2}(-1-p^t)$, $\lambda_2^* = \frac{1}{2}(1-p^t)$, $m_2 = \frac{1}{2}(q-1)$.

Lemma 3 *Let $\Gamma = G\mathcal{P}^*(q)$, where $q = p^{2t}$, $n = p^t + 1$. Then $\mathrm{Aut}(\Gamma)$ contains the subgroup G of $A\Gamma L_1(q)$ generated by the translations T, the automorphisms $\gamma : x \mapsto \omega^n x$ and $\delta : x \mapsto \omega^{n/2-1} x^{p^t}$ and of order $2q(p^t - 1)$.*

Proof: Clearly G contains T of order q, and $\gamma \in G_0$, of order $(p^t - 1)$. It is easy to verify that δ is in $\mathrm{Aut}(\Gamma)$, and $\delta \in G_0$. Now note that $\delta^2 = \gamma^{n/2-1}$, and that $|\delta| = 4$. Thus $|\langle\gamma,\delta\rangle| = 4(n-2)/2 = 2(p^t - 1)$, and $|G| = 2q(p^t - 1)$. ■

Note: Computations with Magma [4, 2] indicate that for $q \ge 13^2$, $G = \mathrm{Aut}(\Gamma)$. For smaller q, other automorphisms can be found: for $q = 11^2$, the map $\tau : x \mapsto \omega^{10} x^{11}$ is an involution and is not in $\langle\gamma,\delta\rangle$. The full automorphism group is not given in [9], but it is proved there in [9, Lemma 5.3.5] that $G\mathcal{P}^*(q)$ is self-complementary. It does not seem to be symmetric for $q \ge 3^4$ as computations with Magma indicate. It is thus likewise, from [10, Lemma 4.1], not rank-3 for $q \ge 3^4$.

5 The codes from the graphs

In [6, Corollary 2,(3)] the following is shown for the Paley graphs and follows for any graphs with the same parameters, and hence for the Peisert and generalized Peisert graphs:

Result 4 *If $\Gamma = P(q)$, the Paley graph with parameters $(q, \frac{1}{2}(q-1), \frac{1}{4}(q-5), \frac{1}{4}(q-1))$, where $q \equiv 1 \pmod 4$, then for any prime p, $C_p(\Gamma)$ is $RLCD$ of dimension $\frac{1}{2}(q-1)$ for $p = 2$ and $q \equiv 1 \pmod 8$, or for p odd and $q \equiv 1 \pmod p$.*

Since $q \equiv 1 \pmod 8$ for the Peisert and the generalized Peisert graphs, the binary codes are always $RLCD$. Ternary codes will be $RLCD$ if $q \equiv 1 \pmod 3$. We will deal with the binary codes in this section and discuss the ternary codes when they are $RLCD$ in the next.

For the Peisert graph, as in [11], let us write $C_0 = \langle \omega^4 \rangle$ and $C_1 = \omega \langle \omega^4 \rangle$ and so

$$M = C_0 \cup C_1 = \langle \omega^4 \rangle \cup \omega \langle \omega^4 \rangle. \tag{6}$$

In the following we use notation for codewords as in [1, Definition 1.2.5], described in Section 2, and in particular we write v^S for the word in the space F^Ω with support $S \subseteq \Omega$.

The following proposition shows that the word v^{C_0} is in $C_2(\mathcal{P}^*(q))$ when $p^t \equiv 1 \pmod 4$.

Proposition 1 *Let $\Gamma = \mathcal{P}^*(q)$, where $q = p^{2t}$, p is prime, $p \equiv 3 \pmod 4$, and so $q \equiv 1 \pmod 8$. Let A be an adjacency matrix for Γ and r_x the row corresponding to $x \in \mathbb{F}_q$. Over $\mathbb{F}_2$, let $u = \sum_{x \in C_0} r_x$. Then for $x \in C_0$, $u(x) = 1$. In addition, $u(0) = 0$ and for all k, m, $u(\omega^{4k+1}) = 0$, and $u(\omega^{4k+2}) = u(\omega^{4m+3})$.*

If $p^t \equiv 1 \pmod 4$, then $u(\omega^{4k+2}) = u(\omega^{4m+3}) = 0$ for all k, m, so $\mathrm{Supp}(u) = C_0$, and thus $C_2(\mathcal{P}^*(q))$ has words of weight $\frac{q-1}{4}$ for $p^t \equiv 1 \pmod 4$.

Proof: Let $x \in C_0$. Then $x \in r_y$ for $y \in C_0$, i.e. $x \in N(y)$, if $x = y + z$ where $z \in M$.

So suppose $x \in r_y$, i.e. $x = y + z$, where $x, y \in C_0$ and $z \in M$. Then $xy^{-1}x = x + xy^{-1}z$, i.e. $x = x^2y^{-1} - xy^{-1}z$, and $x^2y^{-1} \in C_0$, $-xy^{-1}z \in M$, so $x \in r_{x^2y^{-1}}$.

Now y and x^2y^{-1} are distinct unless $y^2 = x^2$, i.e. $y = \pm x$. Clearly $y \neq x$, but we can have $y = -x$ since $x = -x + 2x$ where $-x \in C_0$ and $2x \in M$. This follows since $\mathbb{F}_p^\times \subset C_0$, due to the fact that $\mathbb{F}_p^\times = \langle \omega^{(q-1)/(p-1)} \rangle$, and with $q \equiv 1 \pmod 8$ and $p \equiv 3 \pmod 4$, we have $4 \mid \frac{q-1}{p-1}$.

Thus $r_y(x) = 1$ implies that $r_{x^2y^{-1}}(x) = 1$, in pairs, apart from $r_{-x}(x) = 1$. Thus $u(x) = 1$ for $x \in C_0$.

Note that $0 \in r_y$ for $y \in C_0$ and thus $u(0) = |C_0| \equiv 0 \pmod 2$.

Now let $x = \omega^{1+4k} = y + z$ where $y \in C_0$ and $z \in M$. If $z \in C_0$ then clearly $r_y(x) = r_z(x) = 1$, so the two entries cancel in the sum u.

So suppose $z = \omega v$ where $v \in C_0$. Then $x = y + \omega v = \omega^{1+4k}$, so $xv^{-1}\omega^{4k} = yv^{-1}\omega^{4k} + \omega^{1+4k}$, so $x = -yv^{-1}\omega^{4k} + \omega v^{-1}\omega^{8k}$. Thus $x \in N(-yv^{-1}\omega^{4k})$. If $-yv^{-1}\omega^{4k} = y$ then $v = -\omega^{4k}$, so $x = w^{1+4k} = y - \omega^{1+4k}$, so $y = 2\omega^{1+4k}$, which is not possible since $y \in C_0$. Thus the entries in u at y and $-yv^{-1}\omega^{4k}$ cancel out, and $u(\omega^{1+4k}) = 0$.

Now let $x = \omega^2$ and suppose $x \in r_y$ where $y \in C_0$. Thus $x = y + z$ for some $z \in M$. If $z = \omega^{4j} \in C_0$ then with $y = \omega^{4i}$, $x = \omega^{4i} + \omega^{4j}$, we have $x \in r_z$ and since we cannot have $y = z$ the entry in r_y cancels with that in r_z. Thus we may suppose that $x = \omega^2 = \omega^{4i} + \omega^{1+4j}$. Then $\omega^{2p} = \omega^{4ip} + \omega^{(1+4j)p}$. Multiplying both sides of this by $\omega^{-(2p-3)}$ gives $\omega^3 = \omega^{4ip-2p+3} + \omega^{(1+4j)p-2p+3}$. Using the fact that $p \equiv 3 \pmod 4$, we have $4ip - 2p + 3 \equiv 1 \pmod 4$, and $(1 + 4j)p - 2p +$

$3 \equiv 0 \pmod 4$, thus showing that for $\omega^2 \in r_{\omega^{4i}}$ there corresponds a row r_z for some $z \in C_0$, with $\omega^3 \in r_z$. Similarly, for $\omega^3 = \omega^{4i} + \omega^{1+4j}$ we have $\omega^{3p} = \omega^{4ip} + \omega^{(1+4j)p}$, and multiplying both sides by $\omega^{-(3p-2)}$ gives $\omega^2 = \omega^{4ip-3p+2} + \omega^{(1+4j)p-3p+2}$. Since $4ip - 3p + 2 = 1 + 4 \equiv 1 \pmod 4$ and $(1+4j)p - 3p + 2 \equiv 0 \pmod 4$ we have ω^3 in a row r_x for $x \in C_0$ giving a corresponding ω^2 in a row r_y for $y \in C_0$, we have the entries in u occurring in pairs, and thus we must have $u(\omega^2) = u(\omega^3)$. Since $u(x\omega^{4k}) = u(x)$ for any x, this completes the assertion.

For the final assertion, suppose $\omega^3 = \omega^{4i} + \omega^{1+4j}$, i.e. $w^3 \in r_{w^{4i}}$. Then $\omega^{3p^t} = \omega^{4ip^t} + \omega^{p^t(1+4j)}$. Multiply both sides by $w^{-(3p^t-3)}$ gives $w^3 = w^{4ip^t-3(p^t-1)} + w^{p^t+4jp^t-3(p^t-1)}$. If $p^t \equiv 1 \pmod 4$, this gives $4ip^t - 3(p^t-1) \equiv 0 \pmod 4$ and $1 + 4jp^t - 3(p^t-1) \equiv 1 \pmod 4$. Thus if $z = w^{4ip^t-3(p^t-1)}$, then $w^3 \in r_z$. If $z = w^{4i}$ then $w^{4ip^t-3(p^t-1)} = w^{4i}$, so $(w^{4i-3})^{p^t-1} = 1$, so that $w^{4i-3} \in \mathbb{F}_{p^t}$ and hence $(p^t+1) \mid (4i-3)$. This is impossible, so the rows in which w^3 occurs, occur in pairs, and thus $u(w^3) = 0$, and hence $u(\omega^{4k+2}) = u(\omega^{4m+3}) = 0$ from the first part. ■

Note: 1. Computation with Magma indicates that $v^{C_0} \notin C_2(\mathcal{P}^*(q))$ for $p^t \equiv 3 \pmod 4$ in general.
2. For the graph $\mathcal{P}^*(q)$ where $q = p^{2t}$ with ω a primitive element for $\mathbb{F}_q^\times$, since $\mathbb{F}_p^\times = \langle \omega^{\frac{q-1}{p-1}} \rangle$, it follows that $\mathbb{F}_p^\times \subset C_0$. If $p^t \equiv 3 \pmod 4$ then also $\mathbb{F}_{p^t}^\times \subset C_0$.

In the following proposition we construct words of weight $2(p^t-1) = 2(\sqrt{q}-1)$ in $C_2(\mathcal{P}^*(q))$ when $p^t \equiv 3 \pmod 4$.

Proposition 2 *Let* $\Gamma = \mathcal{P}^*(q)$, *where* $q = p^{2t}$, p *is prime,* $p \equiv 3 \pmod 4$, *and suppose that* $p^t \equiv 3 \pmod 4$. *Let* A *be an adjacency matrix for* Γ *and* r_x *the row corresponding to* $x \in \mathbb{F}_q$, *and let* C *be the binary code of* Γ. *Let* $K = \mathbb{F}_q$, $F = \mathbb{F}_{p^t}$.

Then the word w *with support* $S = F^\times \cup \omega F^\times$ *of weight* $2(p^t-1)$ *is in* C, *and*

$$w = v^S = \sum_{x \in F^\times \cup \omega F^\times} r_x.$$

Proof: We first remark that if we can show that $w = v^S$ is in C then it will necessarily be the sum of the rows shown, by Result 2 since C is *RLCD* by Result 4.

We consider the field $K = \mathbb{F}_q$ as a quadratic extension of the field $F = \mathbb{F}_{p^t}$. The elements of K can be written as $a\omega + b$, where $a, b \in F$. Since $F^\times = \langle \omega^{p^t+1} \rangle$, and $p^t \equiv 3 \pmod 4$, let us write $m = \frac{p^t+1}{4}$, and note that $F^\times \subset C_0$. Then

$$C_0 = F^\times \cup \dot{\bigcup}_{i=1}^{m-1} F^\times(a_i\omega + b_i),\ \ C_1 = \omega C_0 = \omega F^\times \cup \dot{\bigcup}_{i=1}^{m-1} F^\times(c_i\omega + d_i),$$

and

$$C_2 = \omega^2 C_0 = \dot{\bigcup}_{i=1}^{m} F^\times(e_i\omega + f_i),\ \ C_3 = \omega^3 C_0 = \dot{\bigcup}_{i=1}^{m} F^\times(g_i\omega + h_i),$$

where $a_i, b_i, c_i, d_i, e_i, f_i, g_i, h_i \in F^\times$, and each of the C_i are partitioned into m disjoint sets of size $p^t - 1$, consisting of all the multiples of an element of C_i by elements of $F^\times$.

We show that $w = \sum_{x \in F^\times \cup \omega F^\times} r_x$ has support S as asserted. We look at the value of $w(u)$ for each $u \in K$. Recall that $u \in r_x$ (i.e. $u \in N(x)$) if and only if $u = x + y$ where $y \in M$. Clearly $0 \in N(x)$ for all $x \in S$, so $w(0) = 2(p^t-1) = 0$. We consider the non-zero cases.
(i) $u = a \in F^\times$.
Then $a = b + (a-b)$, so $a \in r_b$ for $b \neq a$, and occurs $p^t - 2$ times.

If $a \in r_{b\omega}$ then $a = b\omega + y$ where $y \in M$. Clearly y cannot be in $F^\times$ nor in $\omega F^\times$.

If $y = \alpha(c\omega + d) \in C_0$, then $a = b\omega + \alpha(c\omega + d)$ for $a = \alpha d$ and $b = -\alpha c = -ac/d$. So $a \in r_{-(ac/d)\omega}$ for each of the $m-1$ distinct elements $c\omega + d$ in C_0.

Now suppose $y = \alpha(e\omega + f) \in C_1$. Then similarly we obtain $a \in r_{-(ae/f)\omega}$ for each of the $m-1$ distinct elements $e\omega + f$ in C_1.

Thus the $2(m-1)$ entries cancel, and $w(a) = 1$ for all $a \in F^\times$.

(ii) $u = a\omega \in \omega F^\times$.

Then $u = a\omega = b\omega + (a-b)\omega$, so $a\omega \in r_{b\omega}$ for each $b \neq a$, and occurs $p^t - 2$ times.

If $u = a\omega \in r_b$ then $a\omega = b + y$ where $y \in M$. So if $y = \alpha(c\omega+d) \in C_0$ then $a\omega = b + \alpha(c\omega + d)$, and $a = \alpha c$, $b = -\alpha d$. Thus $b = -ad/c$, and $a\omega \in r_{-ad/c}$, and this is for each of the $m-1$ partitions in C_0. Similarly if $y = \alpha(e\omega + f) \in C_1$ we have $a\omega \in r_{-af/e}$, for each of the $m-1$ partitions in C_1. Hence they cancel. Thus $w(a\omega) = 1$ for all $a \in F^\times$.

(iii) $u = a\omega + b \in C_0 \setminus F^\times$, $a, b \in F^\times$.

If $u \in r_c$ where $c \in \mathbb{F}^\times$, then $u = a\omega + b = c + y$ where $y \in M$. Clearly we cannot have $y \in F^\times$. If $y = d\omega$, then $a\omega + b = c + d\omega$, so $d = a$ and $c = b$, i.e. $u \in r_b$, and $u \in r_{a\omega}$.

If $y = \alpha(d\omega + e) \in C_0$, but not a scalar multiple of u, then $a\omega + b = c + \alpha(d\omega + e)$ so $a = \alpha d$ and $b = c + \alpha e = c + ae/d$, so $c = b - ae/d$ and $u \in r_c$ for each such $y \in C_0$. Clearly if $d\omega + e$ is not a scalar multiple of $d_1\omega + e_1$, then $e/d \neq e_1/d_1$, so the $m-2$ rows are different. Including also the row r_b, gives $m-1$ rows.

Similarly if $y = \alpha(f\omega + g) \in C_1$ we obtain $u \in r_c$ for $c = b - ag/f$, and we have $m-1$ of these. Thus these $2(m-1)$ entries cancel for the rows r_c for $c \in F^\times$.

Now consider $u \in r_{c\omega}$. Then $u = c\omega + y$ where $y \in M$. The case $y = d \in F^\times$ occurs for $u = a\omega + b = c\omega + d$, i.e. $c = a$ and $d = b$, so $u \in r_{a\omega}$, as already noted above.

If $y = \alpha(d\omega + e) \in C_0$, but not a scalar multiple of u, then $a\omega + b = c\omega + \alpha(d\omega + e)$, so $b = \alpha e$, $a = c + \alpha d$, and so $c = a - bd/e$. Thus $u \in r_{c\omega}$ for these $m-2$ elements of C_0, and together with $r_{a\omega}$, gives $m-1$ rows in this set.

Similarly if $y = \alpha(f\omega + g) \in C_1$ we obtain $u \in r_{c\omega}$ for $c = b - ag/f$, and we have $m-1$ of these. Thus these $2(m-1)$ entries cancel for the rows $r_{c\omega}$ for $c \in F^\times$.

Thus $w(a\omega + b) = 0$ for $a\omega + b \in C_0 \setminus F^\times$.

(iv) $u = a\omega + b \in C_1 \setminus \omega F^\times$, $a, b \in F^\times$.

Again clearly $u \in r_b, r_{a\omega}$.

For other rows r_c, if $u = a\omega + b = c + y$ for $y \in M$, for $y = \alpha(d\omega + e) \in C_0$ we get $m-1$ solutions arguing as in (iii) above, and for $y = \alpha(d\omega + e) \in C_1$, but not a scalar multiple of u, we get $m-2$ solutions. Including also r_b then gives $2(m-1)$ solutions as in (iii).

For other rows $r_{c\omega}$, consider cases in the same way, and again we get $2(m-1)$ solutions, and thus $w(a\omega + b) = 0$ for $a\omega + b \in C_1 \setminus \omega F^\times$.

(v) $u = a\omega + b \in \omega^2 M$, $a, b \in F^\times$.

First, clearly, $u \in r_b, r_{a\omega}$. Then it follows precisely as in the preceding cases that $u \in r_c$ for each of the $2(m-1)$ members of M excluding $F^\times \cup \omega F^\times$. This gives $1 + 2(m-1)$ rows. However if we now count in the same way the rows $r_{c\omega}$ containing u, we get another $1 + 2(m-1)$ rows. Thus they cancel out and $w(u) = 0$ as required. ■

Note: In this and the following propositions, to show that $v^S \in RC, C$, one could have shown directly that $(r_x, v^S) \equiv 0 \pmod 2$ (respectively $(s_x, v^S) \equiv 0 \pmod 2$) for all $x \in K$. However, this requires the cases as we have considered above, so does not apparently provide any simplification of the proof.

Next we construct words of weight $2(p^t-1)$ in $C_2(G\mathcal{P}^*(q))$ for $p^t \equiv 1, 3 \pmod 4$ and words of weight p^t in $RC_2(G\mathcal{P}^*(q))$ for $p^t \equiv 1 \pmod 4$.

Proposition 3 *Let $\Gamma = G\mathcal{P}^*(q)$, where $q = p^{2t}$, p is prime. Let $\widehat{M}$ be as in Equation (5), $n = p^t + 1$. Let A be an adjacency matrix for Γ and r_x, s_x the row corresponding to $x \in \mathbb{F}_q$ in A and $A+I$, respectively. Let C be the binary code of Γ and RC that of the reflexive graph $R\Gamma$. Let $K = \mathbb{F}_q$, $F = \mathbb{F}_{p^t}$.*

1. *If $p^t \equiv 3 \pmod 4$, the word w with support $S = F^\times \cup \omega F^\times$ of weight $2(p^t-1)$ is in C and*
$$w = v^S = \sum_{x \in F^\times \cup \omega F^\times} r_x.$$

2. *If $p^t \equiv 1 \pmod 4$, $u_1, u_2 \notin \widehat{M}$, $u_1 \neq u_2$, then the word w with support $S = u_1 F^\times \cup u_2 F^\times$ of weight $2(p^t-1)$ is in C and*
$$w = v^S = \sum_{x \in u_1 F^\times \cup u_2 F^\times} r_x.$$

3. *If $p^t \equiv 1 \pmod 4$, then the word w with support F and weight p^t is in $RC = C^\perp$ and*
$$w = v^F = \sum_{x \in F} s_x.$$

Proof: As remarked in the proof of Proposition 2 if we can show that $w = v^S$ is in C, respectively v^F in RC, then it will necessarily be the sum of the rows shown, by Result 2 since C is $RLCD$ by Result 4.

As in Proposition 2 we consider the field $K = \mathbb{F}_q$ as a quadratic extension of the field $F = \mathbb{F}_{p^t}$, so that the elements of K can be written as $a\omega + b$, where $a, b \in F$. Since $F^\times = \langle \omega^{p^t+1} \rangle$, the defining set $\widehat{M}$ for Γ can be written

$$\widehat{M} = \dot{\bigcup}_{0 \leq i \leq \frac{n}{2}-1} \omega^i F^\times = F^\times \cup \omega F^\times \cup \dot{\bigcup}_{i=1}^{m} F^\times (a_i \omega + b_i), \tag{7}$$

where $m = \frac{n}{2} - 2 = \frac{p^t+1}{2} - 2 = \frac{p^t-3}{2}$, and the $a_i, b_i \in F^\times$ are non-zero.
(1) We first take the case $p^t \equiv 3 \pmod 4$ and show that $w = \sum_{x \in F^\times \cup \omega F^\times} r_x$ is v^S, where $S = \{a \mid a \in F^\times\} \cup \{\omega a \mid a \in F^\times\}$. We look at the value of $w(u)$ for each $u \in K$. Recall that $u \in r_x$ (i.e. $u \in N(x)$) if and only if $u = x + y$ where $y \in \widehat{M}$. Clearly $0 \in N(x)$ for all $x \in S$, so $w(0) = 2(p^t - 1) = 0$. We consider the non-zero cases.
(i) $u = a \in F^\times$.
If $u \in r_b$ then $a = b + y$ where $y \in \widehat{M}$. Clearly $y = a - b$ will satisfy this and that $u \in r_b$ for all $b \in F^\times \setminus \{a\}$, so it occurs in $p^t - 2 \equiv 1 \pmod 2$ rows r_b.

If $u \in r_{b\omega}$ then $a = b\omega + y$ for $y \in \widehat{M}$. Clearly $y \notin F^\times \cup \omega F^\times$. If $y = \alpha(a_i\omega + b_i)$, then $a = b\omega + \alpha(a_i\omega + b_i)$, so $a = \alpha b_i$ and $b\omega = -\alpha a_i$, so $b = -aa_i/b_i$ will have $a \in r_{b\omega}$, and this will occur for each of the $\frac{n}{2} - 2$ partitions, giving an extra $\frac{n}{2} - 2 = \frac{p^t-3}{2} \equiv 0 \pmod 2$ non-zero entries. Thus from the first $p^t - 2$ rows we get $w(a) = 1$.

(ii) $u = a\omega$, $a \in F^\times$.
If $u \in r_b$, then $a\omega = b + y$ for some $y \in \widehat{M}$. Clearly $y \notin F^\times \cup \omega F^\times$. If $a\omega = b + \alpha(a_i\omega + b_i)$ then $b = -ab_i/a_i$, and we get a solution for each of the $\frac{n}{2} - 2$ values of i which again gives zero contribution to the value of $w(u)$.

For $u \in r_{b\omega}$, we have $u = a\omega = b\omega + (a-b)\omega$, so $u \in r_{b\omega}$ for all $b \neq a$, and thus for $p^t - 2$ values, giving $w(a\omega) = 1$.
(iii) $u = \alpha(a_i\omega + b_i) \in \widehat{M} \setminus (F^\times \cup \omega F^\times)$, $\alpha \in F^\times$.
Clearly $u \in r_{\alpha b_i}$ and $u \in r_{\alpha a_i \omega}$.

If $u \in r_a$, then $\alpha(a_i\omega + b_i) = a + y$ for some $y \in \widehat{M}$. Clearly $y \notin F^\times$. If $y = c\omega$ then $\alpha(a_i\omega + b_i) = a + c\omega$ giving $c = \alpha a_i$, $a = \alpha b_i$, already noted. If $y = \beta(a_j\omega + b_j)$ then $a = \alpha(b_i - a_ib_j/a_j)$. The number of such choices in $\frac{n}{2} - 3 = \frac{p^t-1}{2} \equiv 1 \pmod 2$, but including $r_{\alpha b_i}$ gives 0.

If $u \in r_{a\omega}$, then we have $u \in r_{\alpha a_i \omega}$ mentioned above. If $\alpha(a_i\omega + b_i) = a\omega + y$ for some $y \in \widehat{M}$ where $y = \beta(a_j\omega + b_j)$, then $\alpha a_i = a + \beta a_j$ and $\alpha b_i = \beta b_j$, giving $a = \alpha(a_i - a_jb_i/b_j)$. A count similar to the above gives an odd number, but again including $r_{\alpha a_i\omega}$ gives $w(u) = 0$.
(iv) $u = a\omega + b \in K^\times \setminus \widehat{M}$, $a, b \in F^\times$.
Clearly $u \in r_{a\omega}, r_b$.

If $u \in r_c$ then $u = a\omega + b = c + y$ for some $y \in \widehat{M}$. So $y = \alpha(a_i\omega + b_i)$, and $a = \alpha a_i$, $b = c + \alpha b_i$. Thus $c = b - ab_i/a_i$. The number of such choices for c is $\frac{n}{2} - 2 \equiv 0 \pmod 2$, so an odd number including r_b.

If $u \in r_{c\omega}$, $u = a\omega + b = c\omega + y$ for some $y \in \widehat{M}$. So $y = \alpha(a_i\omega + b_i)$, and $a = c + \alpha a_i$, $b = \alpha b_i$. Thus $c = a - ba_i/b_i$ and the number of choices for c is $\frac{n}{2} - 2 \equiv 0 \pmod 2$, so an odd number including $r_{a\omega}$. Combined these give an even number and thus $w(u) = 0$.

This completes the first assertion of the proposition. For the second part, the arguments are similar but there are some differences.
(2) Now take $p^t \equiv 1 \pmod 4$, and show that $w = \sum_{x \in u_1F^\times \cup u_2F^\times} r_x$ is v^S. We look at the value of $w(u)$ for each $u \in K$. First notice that $w(0) = 0$ since $0 \notin u_1F^\times, u_2F^\times$. Suppose $u_1 = c_1\omega + d_1$, $u_2 = c_2\omega + d_2$.
(i) $u = au_1$ or $u = au_2$, $a \in F^\times$.
If $u = au_1 \in r_{cu_1}$ then $a(c_1\omega + d_1) = c(c_1\omega + d_1) + y$ for $y \in \widehat{M}$, where $c \neq a$. Clearly $y \neq d, d\omega$ for $d \in F$. Suppose $y = d(a_i\omega + b_i)$, $d \in F^\times$. Then $ac_1 = cc_1 + da_i$ and $ad_1 = cd_1 + db_i$, and $(a-c)c_1 = da_i$, $(a-c)d_1 = db_i$, so $c_1/d_1 = a_i/b_i$ which is impossible since $u_1 \notin \widehat{M}$. So $u_1 \notin r_{cu_1}$ for any $c \in F^\times$.

If $u \in r_{cu_2}$ then $a(c_1\omega + d_1) = c(c_2\omega + d_2) + y$ for $y \in \widehat{M}$. If $y = d \in F^\times$ then $a(c_1\omega + d_1) = c(c_2\omega + d_2) + d$, so $ac_1 = cc_2$, $ad_1 = cd_2 + d$, and $c = ac_1/c_2$, $d = ad_1 - cd_2$ will give a solution. Similarly $y = d\omega$ for $d \in F^\times$ gives $a(c_1\omega + d_1) = c(c_2\omega + d_2) + d\omega$, so $ac_1 = cc_2 + d$, $ad_1 = cd_2$, so $c = ad_1/d_2$ with $d = ac_1 - cc_2$ will give a solution.

If $y = d(a_i\omega + b_i)$ where $d \in F^\times$, then $a(c_1\omega + d_1) = c(c_2\omega + d_2) + d(a_i\omega + b_i)$, and $ac_1 = cc_2 + da_i$, $ad_1 = cd_2 + db_i$. Solving gives $c = \frac{a(d_1a_i - c_1b_i)}{d_2a_i - c_2b_i}$. Thus there are $\frac{n}{2} = \frac{p^t+1}{2} \equiv 1 \pmod 2$ solutions so $w(au_1) = 1$ for all $a \in F^\times$. Likewise $w(au_2) = 1$ for all $a \in F^\times$.
(ii) $u = a \in F^\times$.
If $u \in r_{cu_1}$ then $a = c(c_1\omega + d_1) + y$ for $y \in \widehat{M}$. Clearly $y \notin F^\times$. If $y = d\omega$ then $a = cd_1$ and $cc_1 + d = 0$. Thus $c = a/d_1$ gives a solution, and $a = \frac{a}{d_1}(c_1\omega + d_1) - \frac{ac_1}{d_1}\omega$.

If $y = d(a_i\omega + b_i)$, then $a = c(c_1\omega + d_1) + d(a_i\omega + b_i)$, so $a = cd_1 + db_i$ and $cc_1 + da_i = 0$. This

has the solution $c = \frac{aa_i}{d_1a_i - c_1b_i}$ for each of the values of i. This gives $\frac{n}{2} - 1 \equiv 0 \pmod 2$ entries. The same holds for the second set of rows r_{cu_2}, and thus $w(a) = 0$.
(iii) $u = a\omega \in \omega F^\times$.
If $u \in r_{cu_1}$ then $a\omega = c(c_1\omega + d_1) + y$ for $y \in \widehat{M}$. Clearly $y \notin \omega F^\times$. If $y = d$ then $a\omega = c(c_1\omega + d_1) + d$ so $a = cc_1$ and $cd_1 + d = 0$, giving the solution $c = a/c_1$.

If $y = d(a_i\omega + b_i)$, then $a\omega = c(c_1\omega + d_1) + d(a_i\omega + b_i)$, so $a = cc_1 + da_i$ and $cd_1 + db_i = 0$, giving the solution $c = \frac{ab_i}{c_1b_i - d_1a_i}$. This gives $\frac{n}{2} - 1 \equiv 0 \pmod 2$ entries. The same holds for the second set of rows r_{cu_2}, and thus $w(a\omega) = 0$.
(iv) $u = a(a_i\omega + b_i) \in \widehat{M}$, $a \in F^\times$.
If $u \in r_{cu_1}$ then $a(a_i\omega + b_i) = c(c_1\omega + d_1) + y$ for $y \in \widehat{M}$. If $y = d$ then $aa_i = cc_1$ and $ab_i = cd_1 + d$, so $c = aa_i/c_1$ gives a solution. If $y = d\omega$ then $aa_i = cc_1 + d$ and $ab_i = cd_1$, giving $c = ab_i/d_1$ as a solution.

If $y = d(a_j\omega + b_j)$ then $a(a_i\omega + b_i) = c(c_1\omega + d_1) + d(a_j\omega + b_j)$ so clearly $j \neq i$. This gives a solution for c for each $j \neq i$, and thus we have $\frac{n}{2} - 1 \equiv 0 \pmod 2$ for the entry from the first set of rows. We have the same argument for the second set of rows, so $w(u) = 0$.
(v) $u = a\omega + b \notin \widehat{M}, \neq u_1F^\times, u_2F^\times$.
If $u \in r_{cu_1}$ then $a\omega + b = c(c_1\omega + d_1) + y$ for $y \in \widehat{M}$. If $y = d$ then $a = cc_1$ and $b = cd_1 + d$, so $c = a/c_1$ and $d = b - ad_1/c_1$. If $y = d\omega$ then $c = b/d_1$ will give a solution. Similarly if $y = d(a_j\omega + b_j)$ then $a\omega + b = c(c_1\omega + d_1) + d(a_j\omega + b_j)$ will give a solution from $a = cc_1 + da_j$ and $b = cd_1 + db_j$, i.e. $c = \frac{ba_j - ab_j}{d_1a_j - c_1b_j}$. Thus there are $\frac{n}{2} \equiv 1 \pmod 2$ solutions, but the same number from the second set of rows r_{cu_2}, and hence $w(u) = 0$. This completes the proof of (2).
(3) Now take $p^t \equiv 1 \pmod 4$, and show that $w = \sum_{x \in F} s_x$ is v^F. We look at the value of $w(u)$ for each $u \in K$. Since $0 \in s_x$ for all $x \in F$, we have $w(0) = p^t \equiv 1 \pmod 2$.
(i) $u = a \in F^\times$.
Here $a \in s_a$, and $a \in s_b$ for all $b \neq a \in F^\times$, so it occurs $p^t - 1 \equiv 0 \pmod 2$ times, and $w(a) = 1$ for all $a \in F$.
(ii) $u = a\omega$, $a \in F^\times$.
As in the previous case for C, we have $a\omega \in s_b$ for $\frac{n}{2} - 2$ values of b, and thus occurs $\frac{p^t - 3}{2} \equiv 0 \pmod 2$ times. Since also $a\omega \in s_0$, we have $w(a\omega) = 0$.
(iii) $u = \alpha(a_i\omega + b_i) \in \widehat{M} \setminus (F^\times \cup \omega F^\times)$, $\alpha \in F^\times$.
Clearly $u \in s_{\alpha b_i}$ and $u \in s_0$.

If $u \in s_a$, then $\alpha(a_i\omega + b_i) = a + y$ for some $y \in \widehat{M}$. Clearly $y \notin F^\times$. If $y = c\omega$ then $\alpha(a_i\omega + b_i) = a + c\omega$ giving $c = \alpha a_i$, $a = \alpha b_i$, already noted. If $y = \beta(a_j\omega + b_j)$ then $a = \alpha(b_i - a_ib_j/a_j)$. The number of such choices is $\frac{n}{2} - 3 = \frac{p^t - 5}{2} \equiv 0 \pmod 2$, and including $s_{\alpha a_i}$ and s_0 gives $\equiv 0 \pmod 2$, so $w(u) = 0$.
(iv) $u = a\omega + b \in K^\times \setminus \widehat{M}$.
Clearly $u \in s_b$ and $u \notin s_0$. Also $a, b \neq 0$.

If $u \in s_c$ then $u = a\omega + b = c + y$ for some $y \in \widehat{M}$. So $y = \alpha(a_i\omega + b_i)$, and $a = \alpha a_i$, $b = c + \alpha b_i$. Thus $c = b - ab_i/a_i$. The number of such choices for c is $\frac{n}{2} - 2 \equiv \frac{n}{2} = \frac{p^t + 1}{2} \equiv 1 \pmod 2$, so $\equiv 0 \pmod 2$ including s_b. Thus $w(u) = 0$.

This completes the proof of the proposition.■

In the following proposition we construct words of weight p^t for $p^t \equiv 3 \pmod 4$, in $RC_2(\mathcal{P}^*(q))$ and of the same form in $RC_2(G\mathcal{P}^*(q))$.

Proposition 4 *Let $\Gamma = \mathcal{P}^*(q)$ or $G\mathcal{P}^*(q)$, where $q = p^{2t}$, p is prime, $p \equiv 3 \pmod 4$ for Γ, and suppose that $p^t \equiv 3 \pmod 4$. Let A be an adjacency matrix for Γ and r_x, s_x the row corresponding to $x \in \mathbb{F}_q$ in A and $A+I$, respectively. Let C be the binary code of Γ and RC that of the reflexive graph $R\Gamma$. Let M and $\widehat{M}$ be as defined above for the two types of graph. Let $F = \mathbb{F}_{p^t}$, $K = \mathbb{F}_q$.*

Then the word with support yF, where $y \notin M, \widehat{M}$, respectively, is in RC.

Proof: We will consider the two graphs simultaneously. The proof follows in a similar manner to the previous propositions.

Without loss of generality we may assume that $\omega + b \notin M, \widehat{M}$ respectively for some $b \in F^\times$, since $M, \widehat{M}$ are closed under multiplication by $F^\times$ for $p^t \equiv 3 \pmod 4$ for M, and for all odd p for $\widehat{M}$. We show, as before, that $w = \sum_{x \in (\omega+b)F} s_x$ has support $(\omega + b)F$. We determine the value of $w(u)$ for each $u \in K$, considering the various cases for u. As in the earlier propositions, $m = \frac{p^t+1}{4}$ for $\mathcal{P}^*(q)$ and $n = p^t + 1$, with $m = \frac{p^t-3}{2}$, for $G\mathcal{P}^*(q)$. Both M and $\widehat{M}$ are expressed as disjoint unions of $\frac{p^t+1}{2}$ sets of size $(p^t - 1)$.
(i) $u = c(\omega + b)$, where $c \in F$.
For $u = 0$, $u \in s_0$ but not in $s_{c(\omega+b)}$ for any $c \neq 0$. Likewise, $c(\omega+b) \in s_{c(\omega+b)}$ but not in $s_d(\omega+b)$ for $d \neq c$, since clearly $(c-d)(\omega + b) \notin M, \widehat{M}$. Thus $w(u) = 1$ for $u \in (\omega + b)F$.
(ii) $u = a \in F^\times$.
Clearly $u \in s_0$. If $u \in s_{c(\omega+b)}$, then $a = c(\omega + b) + y$ for $y \in M, \widehat{M}$ respectively. Clearly $y \notin F^\times$, but $a \in s_{\frac{a}{b}(\omega+b)}$ taking $y = -\frac{a}{b}\omega$. If $y = \alpha(a_i\omega + b_i)$ then $a = cb + \alpha b_i$ and $c = -\alpha a_i$, so $c = aa_i/(ba_i - b_i)$. The number of such possibilities is thus $2 + 2(m-1) \equiv 0 \pmod 2$ for M and $2 + \frac{n}{2} - 2 = \frac{p^t+1}{2} \equiv 0 \pmod 2$ for $\widehat{M}$ since $p^t \equiv 3 \pmod 4$. Thus $w(a) = 0$ for $u = a \in F^\times$.
(iii) $u = a\omega$, $a \in F^\times$.
Clearly $u \in s_0$. If $u \in s_{c(\omega+b)}$, then $a\omega = c(\omega + b) + y$ for $y \in M, \widehat{M}$ respectively. So $a\omega \in s_{a(\omega+b)}$ taking $y = -ab$. If $a\omega = c(\omega + b) + \alpha(a_i\omega + b_i)$ then $a = c + \alpha a_i$ and $cb = -\alpha b_i$, so $c = ab_i/(b_i - a_i b)$. Thus the number of occurrences is again $2 + 2(m-1) \equiv 0 \pmod 2$ for M and $2 + \frac{n}{2} - 2 = \frac{p^t+1}{2} \equiv 0 \pmod 2$ for $\widehat{M}$. Thus $w(a\omega) = 0$.
(iv) $u = \alpha(a_i\omega + b_i) \in M, \widehat{M}$, respectively, $\alpha \in F^\times$.
Clearly $u \in s_0$. If $u \in s_{c(\omega+b)}$, then $\alpha(a_i\omega + b_i) = c(\omega + b) + y$ for $y \in M, \widehat{M}$ respectively.

If $y = d \in F^\times$, then $\alpha a_i = c$ and $\alpha b_i = cb + d$. Thus $d = \alpha(b_i - a_i b)$ and $u \in s_{\alpha a_i(\omega+b)}$. If $y = d\omega$ then $\alpha a_i = c + d$ and $\alpha b_i = cb$. Thus $c = \alpha b_i/b$ and $d = \alpha(a_i - b_i/b)$, and $u \in s_{\alpha\frac{b_i}{b}(\omega+b)}$.

If $y = \beta(a_j\omega + b_j)$, where $j \neq i$, then $\alpha a_i = c + \beta a_j$ and $\alpha b_i = cb + \beta b_j$. Thus $c = \alpha\frac{a_i b_j - a_j b_i}{b_j - a_j b}$ and $u \in s_{c(\omega+b)}$ for this value of c.

This gives $3 + (m-1) + (m-2) = 2m \equiv 0 \pmod 2$ rows for M and $3 + \frac{n}{2} - 3 = \frac{n}{2} \equiv 0 \pmod 2$ for $\widehat{M}$, so $w(u) = 0$.
(v) $u = a\omega + d \notin M, \widehat{M}$ respectively.
Here $u \notin s_0$. If $u \in s_{c(\omega+b)}$, then $a\omega + d = c(\omega + b) + y$ for $y \in M, \widehat{M}$ respectively.

Clearly $u \in s_{a(w+b)}$ and $s_{\frac{d}{b}(\omega+b)}$. Thus take $y = \alpha(a_i\omega + b_i)$. Then $a\omega + d = c(\omega + b) + \alpha(a_i\omega + b_i)$, so $a = c + \alpha a_i$ and $d = cb + \alpha b_i$. Thus $c = \frac{a_i d - ab_i}{ba_i - b_i}$. The number of solutions is then $2 + 2(m-1) \equiv 0 \pmod 2$ for M, and $2 + \frac{n}{2} - 2 = \frac{n}{2} \equiv 0 \pmod 2$ for $\widehat{M}$.

This completes the proof.■

We summarise our findings from the propositions on small words in the binary codes in the following table. In the table u_1, u_2, y are elements of $\mathbb{F}_q$ that are not in $M, \widehat{M}$, as required in the propositions. The field $F = \mathbb{F}_{p^t} = \mathbb{F}_{\sqrt{q}}$, so the words of the form $F^\times \cup \omega F^\times$ have weight $2(\sqrt{q}-1)$, those of the form yF have weight $\sqrt{q}$ and for $p^t \equiv 1 \pmod 4$ those of the form C_0 have weight $\frac{q-1}{4}$. Note that only for the case $RC_2(\mathcal{P}^*(p^{2t}))$ where $p^t \equiv 1 \pmod 4$ have we not been able to find a small word, although we did find some computationally with Magma for $p^t = 9$, in which the minimum weight is p^t, as it is in all the other cases. The next case is $p^t = 49$ which is harder to work with computationally.

$q = p^{2t}$	cong. mod. 4	$C_2(\mathcal{P}^*(q))$	$RC_2(\mathcal{P}^*(q))$	$C_2(G\mathcal{P}^*(q))$	$RC_2(G\mathcal{P}^*(q))$
p^t	3	$F^\times \cup \omega F^\times$	yF	$F^\times \cup \omega F^\times$	yF
p^t	1	C_0	?	$u_1F^\times \cup u_2F^\times$	F

Table 1: Supports of words of small weight in binary codes for $\mathcal{P}^*(q)$ and $G\mathcal{P}^*(q)$

We examined with Magma those codes from Peisert and generalized Peisert graphs that are $RLCD$ and attach tables below for the binary codes. In the cases where p-ary codes for some odd p give $RLCD$ codes, for those small cases for which the minimum weights could be determined easily with Magma, there were no differences from the binary codes. All the other items remain the same over these fields.

The columns of the tables show the value of q, the strongly regular graph parameters, the order of the automorphism group, the dimension of C_2, the dimension of RC_2, the minimum weight of C_2, and the minimum weight of RC_2. It is clear from the parameters that, for any prime p for which the codes are $RLCD$, $\dim(C_p(\Gamma)) = \dim(RC_p(\Gamma)) - 1 = \frac{1}{2}(q-1)$, since in order to be $RLCD$ we need $p | \frac{1}{2}(q-1)$, so the null space, $RC_p(\Gamma)$, has the larger dimension.

q	Γ	$\lvert\mathrm{Aut}(\Gamma)\rvert$	$\dim(C)$	$\dim(RC)$	$MW(C)$	$MW(RC)$
3^2	$(9,4,1,2)$	$2^3 3^2$	4	5	4(4)	3(3)
7^2	$(49,24,11,12)$	$2^3 3^2 7^2$	24	25	10(12)	7(10)
3^4	$(81,40,19,20)$	$2^5 3^5 5^1$	40	41	12(16)	9(14)
11^2	$(121,60,29,30)$	$2^2 3^1 5^1 11^2$	60	61	18(20)	11(20)
19^2	$(361,180,89,90)$	$2^2 3^2 5^1 19^2$	180	181	$\geq 12, \leq 36$	≤ 19
23^2	$(529,264,131,132)$	$2^3 3^1 11^1 23^2$	264	265	$\geq 14, \leq 44$	≤ 23
3^6	$(729,364,181,182)$	$2^2 3^7 7^1 13^1$	364	365	$\geq 16, \leq 52$	≤ 27
31^2	$(961,480,239,240)$	$2^5 3^1 5^1 31^2$	480	481	$\geq 18, \leq 60$	≤ 31

Table 2: Peisert graphs $\mathcal{P}^*(q)$ codes over $\mathbb{F}_2$

In Tables 2, 3 we include the upper bounds for the minimum weight that follow from the propositions. In parentheses behind the minimum weights that we have determined are the values of the best known minimum weights for codes of the those parameters, as given in http://www.codetables.de. For ternary codes (see Section 6), there are known codes with better minimum weight in all the computed cases, from the same web database.

q	Γ	$\lvert\mathrm{Aut}(\Gamma)\rvert$	$\dim(C)$	$\dim(RC)$	$MW(C)$	$MW(RC)$
3^2	$(9,4,1,2)$	$2^3 3^2$	4	5	4(4)	3(3)
5^2	$(25,12,5,6)$	$2^3 3^1 5^2$	12	13	6(8)	5(6)
7^2	$(49,24,11,12)$	$2^3 3^2 7^2$	24	25	10(12)	7(10)
3^4	$(81,40,19,20)$	$2^7 3^4$	40	41	10(16)	9(14)
11^2	$(121,60,29,30)$	$2^3 5^1 11^2$	60	61	16(20)	11(20)
13^2	$(169,84,41,42)$	$2^3 3^1 13^2$	84	85	20(24)	13(24)
17^2	$(289,144,71,72)$	$2^5 17^2$	144	145	≤ 32	≤ 17
19^2	$(361,180,89,90)$	$2^2 3^2 19^2$	180	181	≤ 36	≤ 19
23^2	$(529,264,131,132)$	$2^2 11^1 23^1$	264	265	≤ 44	≤ 23
5^4	$(625,312,155,156)$	$2^4 3^1 5^4$	312	313	≤ 48	≤ 25
3^6	$(729,364,181,182)$	$2^2 3^6 13$	364	365	≤ 52	≤ 27

Table 3: Generalized Peisert graphs $G\mathcal{P}^*(q)$ codes over $\mathbb{F}_2$

6 Ternary codes

By Result 4, p-ary codes from adjacency matrices of strongly regular graphs with parameters those of the Paley graphs will be $RLCD$ if $q \equiv 1 \pmod{p}$. For the ternary codes, if $q = p^{2t}$, then if $p^t \equiv 1, 2 \pmod{3}$ we will have $q = p^{2t} \equiv 1 \pmod{3}$. Thus all of the graphs for which $p^t \neq 3^r$ as considered before will have $RLCD$ codes over $\mathbb{F}_3$.

Apart from Proposition 1, all the proofs of the propositions that give us small words in the binary codes from $\mathcal{P}^*(q)$ and $G\mathcal{P}^*(q)$, as summarized in Table 1, go through with minor modification for the ternary codes. We show the words in Table 4. In the table u_1, u_2, y are elements of $\mathbb{F}_q$ that are not in $M, \widehat{M}$, as required in the propositions for the binary case. The field $F = \mathbb{F}_{p^t} = \mathbb{F}_{\sqrt{q}}$, so the words of the form $F^\times \cup \omega F^\times$ have weight $2(\sqrt{q}-1)$ and those of the form yF have weight $\sqrt{q}$. Also note that for the Peisert graphs we will still need $p^t \equiv 3 \pmod{4}$ for the codes, as we have not settled the reflexive case for the binary codes when $p^t \equiv 1 \pmod{4}$, and the proof of Proposition 1 for the non-reflexive case does not go through directly to the ternary case; indeed, by computation we find that the word v^{C_0} is not in C for small values of $p^t \equiv 1 \pmod{3}$. Thus for the Peisert case we need t odd. Again, of course, clearly if $w = v^{S_1} - v^{S_2}$ where $S_1 = u_1 F^\times$ and $S_2 = u_2 F^\times$ then $\mathrm{wt}(w) = 2(p^t - 1)$ and if $w = v^{yF}$ then $\mathrm{wt}(w) = p^t$. In the table the support $S_1 - S_2$ implies the vector $v^{S_1} - v^{S_2}$.

$q = p^{2t}$	cong. mod. 3	$C_3(\mathcal{P}^*(q))$	$RC_3(\mathcal{P}^*(q))$	$C_3(G\mathcal{P}^*(q))$	$RC_3(G\mathcal{P}^*(q))$
p^t	1	$u_1F^\times - u_2F^\times$	F	$u_1F^\times - u_2F^\times$	F
p^t	2	$F^\times - \omega F^\times$	yF	$F^\times - \omega F^\times$	yF

Table 4: Supports of words of small weight in ternary codes for $\mathcal{P}^*(q)$ (t odd) and $G\mathcal{P}^*(q)$

7 Lower bound for minimum weight

Using the fact that for $p^t \equiv 3 \pmod 4$, $RC_r(\mathcal{P}^*(q))$ for $r = 2, 3$ contains words with support uF where $F = \mathbb{F}_{p^t}$, and $u \in \mathbb{F}_q$, we can get a lower bound on the minimum weight of $C_r(\mathcal{P}^*(q))$ for $r = 2, 3$.

First note a small lemma:

Lemma 4 *For $K = \mathbb{F}_q$ where $q = p^{2t}$ and E any subfield of K, then if $u_1, u_2 \in K$ are distinct, $u_1E \cap u_2E = \{0\}$ or $u_1E = u_2E$. Likewise, $v_1 + u_1E$ and $v_2 + u_2E$, for $v_1, v_2 \in K$, meet in $0, 1$ or $|E|$ elements.*

This holds in particular for $E = F = \mathbb{F}_{p^t}$.

Proof: Suppose $x \in u_1E \cap u_2E$. Then $x = u_1a = u_2b$ where $a, b \in E$. Thus $u_1 = u_2b/a$, so that for any $c \in E$, $u_1c = u_2cb/a$, and so $u_1E = u_2E$.

Suppose $x, y \in (v_1 + u_1E) \cap (v_2 + u_2E)$. Then $x = v_1 + u_1a_1 = v_2 + u_2a_2$ and $y = v_1 + u_1b_1 = v_2 + u_2b_2$, where $a_1, a_2, b_1, b_2 \in E$, so $x - y = u_1(a_1 - b_1) = u_2(a_2 - b_2)$, and $u_1 = cu_2$ where $c \in E$. Thus $u_1E = u_2E$ and $v_1 = v_2$. ■

Proposition 5 *Let $\Gamma = \mathcal{P}^*(q)$, where $q = p^{2t}$, p is prime, $p \equiv 3 \pmod 4$, and suppose that $p^t \equiv 3 \pmod 4$. If d is the minimum weight of $C_r(\Gamma)$ where $r = 2, 3$, then $\frac{p^t+5}{2} \leq d \leq 2(p^t - 1) < \frac{q-1}{2}$.*

Proof: Let $w \in C_r(\Gamma)$ and suppose $S = \mathrm{Supp}(w)$, $|S| = s$. Without loss of generality suppose that $0 \in S$. The word with support uF, where $F = \mathbb{F}_{p^t}$ is in $RC_r(\Gamma)$ for appropriate choice of u as determined by the earlier propositions. If $G = \mathrm{Aut}(\Gamma)$ then the stabilizer G_0 of 0 has two orbits, both of length $\frac{q-1}{2}$, one being the elements of $\mathbb{F}_q^\times$ that are adjacent to 0, i.e. M, and the other those that are not, i.e. ω^2M. Since $\gamma : uF \mapsto \omega^4uF$, and $\delta : uF \mapsto \omega u^pF$, the sets uF will be mapped onto sets of the same form, within one or the other orbit. Since G_0 is transitive on elements in each orbit, and the sets of this form do not intersect, the number of sets of the form $(uF)^\sigma$ for $\sigma \in G_0$, in an orbit will be $\frac{q-1}{2(p^t-1)} = \frac{p^t+1}{2}$. Each of these must meet the set S again at least once, and since these sets do not intersect we must have at least $\frac{p^t+1}{2} + 1$ elements (including 0) in S. Thus $s \geq \frac{p^t+1}{2} + 1 = \frac{p^t+3}{2}$.

Now suppose $s = \frac{p^t+3}{2}$. The $s - 1$ sets uF^σ can be written as $u^{\sigma_i}F = u_iF$ for $i = 1, \ldots, s - 1$. Thus if $s = \frac{p^t+3}{2}$ then we can assume $S = \{0, u_1, \ldots, u_{s-1}\}$. For any $x \in S$, $x + u_kF$ is an image of uF under G and thus is the support of a word in $RC_r(\Gamma)^\perp$ that contains x. It must thus meet S again and since there are s such sets and $s-1$ available points (other than x) we must have every point of $S \setminus \{x\}$ on one of these sets. Taking $x = u_i$ then for every $j \neq i$ there is a $k \neq i, j$ such that $u_j \in u_i + u_kF$. Since $u_j \in u_i + u_kF$ implies $u_i \in u_j + u_kF$, the points of S are partitioned into pairs $\{u_i, u_j\}$ according as $u_j \in u_i + u_kF$, with $0 \in u_k + u_kF$, paired with u_k. The set S thus forms a complete graph on $s = \frac{p^t+3}{2}$ points that has a parallelism for each k. However, $\frac{p^t+3}{2}$ is odd, so the complete graph on S cannot have a parallelism. Thus $|S| > \frac{p^t+3}{2}$, i.e. $|S| \geq \frac{p^t+5}{2}$. ■

Note: 1. Since clearly $\jmath \in RC_r(\Gamma)$ for both $r = 2$ or 3, we cannot have the weight of a constant vector in $C_r(\Gamma)$ not divisible by 2, respectively 3. As already noted $\frac{p^t+3}{2}$ is odd, and also it is not divisible by 3 since $p^t \not\equiv 0 \pmod 3$, so it follows from this that $|S| \geq \frac{p^t+5}{2}$.

2. This bound for the minimum weight of C will apply to the binary codes from the Paley graph $P(q)$ where q is the square of a prime power, since if $F = \mathbb{F}_{\sqrt{q}}$ then $v^{aF} \in C^{\perp} = RC$, for some a, according to [7].
3. The same argument cannot be used for $G\mathcal{P}^*(q)$ for $q \geq 3^4$ as its automorphism group is not, according to computation, rank-3, as noted at the end of Section 4 above.

The preceding lemmas and propositions give the proof of Theorem 1 stated in Section 1.

References

[1] E. F. Assmus, Jr and J. D. Key, *Designs and their codes*, Cambridge: Cambridge University Press, 1992, Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24, 3/4** (1997), 235–265.

[3] P. J. Cameron and J. H. van Lint, *Designs, graphs, codes and their links*, Cambridge: Cambridge University Press, 1991, London Mathematical Society Student Texts 22.

[4] J. Cannon, A. Steel, and G. White, *Linear codes over finite fields*, Handbook of Magma Functions (J. Cannon and W. Bosma, eds.), Computational Algebra Group, Department of Mathematics, University of Sydney, 2006, V2.13, http://magma.maths.usyd.edu.au/magma, pp. 3951–4023.

[5] W. Cary Huffman, *Codes and groups*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), Amsterdam: Elsevier, 1998, Volume 2, Part 2, Chapter 17, pp. 1345–1440.

[6] J. D. Key and B. G. Rodrigues, *LCD codes from adjacency matrices of graphs*, Appl. Algebra Engrg. Comm. Comput. **29 (3)** (2018), 227–244.

[7] J. Limbupasiriporn, *Partial permutation decoding for codes from designs and finite geometries*, Ph.D. thesis, Clemson University, 2005.

[8] James L. Massey, *Linear codes with complementary duals*, Discrete Math. **106/107** (1992), 337–342.

[9] Natalie Mullin, *Self-complementary arc-transitive graphs and their imposters*, Master's thesis, University of Waterloo, 2009.

[10] Wojciech Peisert, *All self-complementary symmetric graphs*, J. Algebra **240** (2001), 209–229.

[11] Peter Sin, *The critical groups of the Peisert graphs $\mathcal{P}^*(q)$*, J. Algebraic Combin. **48(2)** (2018), 227–245, DOI 10.1007/s10801-017-0797-8; arXiv: 1606.00870v1.