LCD codes from adjacency matrices of graphs

J.D. Key*
Institute of Mathematics, Physics and Computer Science
Aberystwyth University, Aberystwyth SY23 3BZ, U.K.

B.G. Rodrigues†
School of Mathematics, Statistics and Computer Science
University of KwaZulu-Natal
Durban 4000, South Africa

August 4, 2017

Abstract

It is shown how LCD codes with a particularly useful feature can be found from row spans over finite fields of adjacency matrices of graphs by considering these together with the codes from the associated reflexive graphs and complementary graphs. Application is made to some particular classes, including uniform subset graphs and strongly regular graphs where, if a p-ary code from a graph has this special LCD feature, the dimension can be found from the multiplicities modulo p of the eigenvalues of an adjacency matrix and, bounds on the minimum weight of the code and the dual code follow from the valency of the graph.

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

1 Introduction

In [28] Massey defines an LCD code (linear code with complementary dual) as a code for which the hull is zero, i.e. if C is a linear code, C is LCD if $\text{Hull}(C) = C \cap C^{\perp} = \{0\}$. Thus $C^{\perp}$ is also LCD, and if C is of length n over a field F, then $F^n = C \oplus C^{\perp}$.

It is shown in [28] that for an LCD code C to correct errors by nearest neighbour decoding, one needs only to find the nearest word to the received word in the code $C^{\perp}$. This reduces the computation of error correction. In order to achieve this, one first needs to be able to say exactly how any vector $w \in F^n$ can be written as its unique sum of vectors in C and $C^{\perp}$. In this work here we show how consideration of codes from the adjacency matrix of undirected graphs, together with their reflexive associates, and their complementary graphs, leads to a simple way to achieve this representation. Furthermore, in this event, since C and $C^{\perp}$ are the codes from graphs or reflexive graphs, respectively, information regarding the codes can be obtained from properties of the graph, including that the minimum weight of C is at most the valency ν, and that of $C^{\perp}$ at most $\nu + 1$. For some classes of graphs there is already information to be found in the literature regarding the properties of the codes from adjacency matrices of graphs and their reflexive associates.

*Email:keyj@clemson.edu
†Email:rodrigues@ukzn.ac.za

We show, in Proposition 1 (in Section 3), how, for these LCD codes C, the representation of any vector as a unique sum of vectors in C and $C^{\perp}$ can be achieved for the codes from adjacency matrices of graphs that satisfy certain properties, and in Proposition 2 we show some graph theoretic properties that will suffice to establish this. In Sections 4 and 5 we show how this can be done explicitly for uniform subset graphs (Proposition 3), and for strongly regular graphs (Proposition 4).

Section 2 gives some terminology and background.

2 Background and definitions

The notation for codes and codes from incidence structures and graphs is as in [2]. 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**. 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 [20].

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 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.

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.

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 $F = \mathbb{F}_p$.

The background on LCD codes from [28] is described below.

Definition 1 *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 follows: for $v \in F^n$,

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

and Π_C is defined to be linear. [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 [28, 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*

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

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

We make the following observation which will be of use in the next section:

Lemma 1 *If C is a q-ary code of length n such that $C + C^{\perp} = \mathbb{F}_q^n$ then C is LCD.*

Proof: Since $(C + C^{\perp})^{\perp} = C^{\perp} \cap C = (\mathbb{F}_q^n)^{\perp} = \{0\} = \mathrm{Hull}(C)$, C (and $C^{\perp}$) are LCD. ■

3 Special LCD codes from graphs

We note first that we are considering a particular class of LCD codes from adjacency matrices of undirected graphs. There are indeed many cases of LCD codes from adjacency, and also incidence, matrices of graphs in the literature: for example, refer to [21, 23, 18, 17, 14, 29]. However in this paper we are only looking at a particular type of LCD code from a graph, as we will describe below.

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

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

$$s_x = v^x + r_x, \quad c_x = \jmath - v^x - r_x = \jmath - s_x. \tag{3}$$

Proposition 1 *Let $\Gamma = (V, E)$ be a graph, A an adjacency matrix, $R\Gamma$ its associated reflexive graph, $\overline{\Gamma}$ its complementary graph. Let p be any prime, and $C = C_p(A)$, $RC = C_p(RA)$, $\overline{C} = C_p(\overline{A})$. Then:*

[1] Note typographical error on p.338, l.-11, in [28]

[2] Note typographical error on p.341, l.-7, in [28]

1. *If $C = RC^{\perp}$, then C and RC are LCD codes. Further, if $v \in \mathbb{F}_p^V$, and $v = \sum_{x\in V} v(x)v^x$, 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 $v = \sum_{x\in R} s_x$.

2. *If Γ is regular of valency ν, and $C = \overline{C}^{\perp}$, then C and $\overline{C}$ are LCD codes. Further, if $v \in \mathbb{F}_p^V$, and $v = \sum_{x\in V} v(x)v^x$, then*
$$v = \sum_{x\in V} v(x)v^x = (\sum_{x\in V} v(x))\boldsymbol{\jmath} - \sum_{x\in V} v(x)r_x - \sum_{x\in V} v(x)c_x = v\Pi_C + v\Pi_{C^{\perp}}$$
where $v\Pi_C = (\sum_{x\in V} v(x))\boldsymbol{\jmath} - \sum_{x\in V} v(x)r_x$ if $p \not| \nu$, and $v\Pi_C = -\sum_{x\in V} v(x)r_x$ if $p|\nu$.

Proof: (1): Since $v^x = s_x - r_x$ implies that $\mathbb{F}_p^V = C + RC$, that C and RC are LCD follows from Lemma 1.

Since for any $x \in V$, $s_x = v^x + r_x$, for any $v \in \mathbb{F}_p^V$, $v = \sum_{x\in V} v(x)v^x = \sum_{x\in V} v(x)(s_x - r_x)$, we have $v\Pi_C = -\sum_{x\in V} v(x)r_x$ and $v\Pi_{C^{\perp}} = \sum_{x\in V} v(x)s_x$. If $p = 2$ then $v = v^S = \sum_{x\in S} s_x + \sum_{x\in S} r_x$, where $S = \mathrm{Supp}(v)$. In particular, if $v \in C$, and $\mathrm{Supp}(v) = T$, then $v = v^T = \sum_{x\in T} r_x + \sum_{x\in T} s_x = \sum_{x\in T} r_x$, since $\sum_{x\in T} s_x = 0$ because $C \cap C^{\perp} = \{0\}$.
(2): Suppose $C = \overline{C}^{\perp}$. Since $\nu\boldsymbol{\jmath} = \sum_{x\in V} r_x$, if $p \not| \nu$ then $\boldsymbol{\jmath} \in C$; if $p|\nu$ then $\boldsymbol{\jmath} \in C^{\perp} = \overline{C}$. Thus, since for any $x \in V$, $v^x = \boldsymbol{\jmath} - r_x - c_x$, we have in either case that $\mathbb{F}_p^V = C + C^{\perp}$ and thus C and $\overline{C}$ are LCD by Lemma 1.

For $v \in \mathbb{F}_p^V$, $v = \sum_{x\in V} v(x)v^x = (\sum_{x\in V} v(x))\boldsymbol{\jmath} - \sum_{x\in V} v(x)r_x - \sum_{x\in V} v(x)c_x$. Since $\nu\boldsymbol{\jmath} = \sum_{x\in V} r_x$, if $p \not| \nu$ then $v\Pi_C = (\sum_{x\in V} v(x))\boldsymbol{\jmath} - \sum_{x\in V} v(x)r_x$; if $p|\nu$ then $\boldsymbol{\jmath} \in C^{\perp} = \overline{C}$, so $v\Pi_C = -\sum_{x\in V} v(x)r_x$. ■

Because the conditions on the relations amongst the code of a graph and its reflexive and complementary graphs lead to LCD codes with a given split of any vector into its parts in the disjoint components, for convenience, for the purposes of this paper, we give these conditions special names.

With notation as defined above:

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), and $\overline{C} = C_p(\overline{A})$. Then*

- *if $C = RC^{\perp}$, then we call C a* **reflexive** *LCD code, and write RLCD for such a code;*
- *if Γ is regular and $C = \overline{C}^{\perp}$, then we call C a* **complementary** *LCD code, and write CLCD for such a code.*

Note: If Γ is regular and $C_p(\Gamma)$ is both $RLCD$ and $CLCD$, then $C_p(R\Gamma) = C_p(\overline{\Gamma})$.

In [26] it was noted that the triangular graph $T(n)$ for $n \equiv 1 \pmod 4$ has binary code that is $CLCD$, and the question was raised as to the existence of other graphs with such a property. The authors of that paper did find some more codes acted on by subgroups of the McLaughlin group: see [26, Theorem 1].

We will find more infinite classes of graphs with $RLCD$ or $CLCD$ codes in what follows.

Note: If we know the eigenvalues of A, and if they are integral, we can use them to get information regarding the possible dimension of the codes C, RC and $\overline{C}$. Since if λ is an eigenvalue for a matrix M then $\lambda+1$ is an eigenvalue for $M+I$, this will also give information about RC. If M is a $v \times v$ integral matrix with integral eigenvalues, then modulo p these will still be eigenvalues, but not necessarily all distinct. If none or at most one reduce to 0 modulo p then the p-rank of M will be v or $v-m_j$, respectively, where m_j is the multiplicity of the eigenvalue that is zero. In any case, the dimension of the zero eigenspace over $\mathbb{F}_p$ of the matrix A or $A+I$ is at most the sum m of the multiplicities of the eigenvalues that reduce to 0 modulo p, and thus the p-rank of A or $A+I$ is at least $v-m$.

Likewise, for Γ regular of valency ν, the spectrum for $\overline{A} = J - I - A$ can be obtained from that of Γ as being $|V|-1-\nu$ and $-1-\theta$, where the θ is an eigenvalue of A with eigenvector w such that $w\boldsymbol{\jmath}^T = 0$, i.e. w is orthogonal to $\boldsymbol{\jmath}$. So these are also all integral if the θ are.

We note the following result from [19], which is given there for $p=2$ but it holds for all primes p, so we state it for all p:

Result 2 (Proposition 2.2 [19]) *If A is a symmetric integral matrix, and C_A, C_{A+I} denote the row span over $\mathbb{F}_p$, where p is a prime, of A, $A+I$ respectively, then $C_A^\perp \subseteq C_{A+I}$ with equality if and only if $A(A+I) \equiv 0 \pmod{p}$.*

Lemma 2 *If $\Gamma = (V,E)$ is regular of valency ν, $|V| = n$, p is a prime, and A is an adjacency matrix for Γ, then both $C_p(\Gamma)$ and $C_p(\overline{\Gamma})$ can be RLCD if and only if $n - 2\nu - 1 \equiv 0 \pmod{p}$.*

Proof: With the usual notation, $\overline{A}(\overline{A}+I) = (J-I-A)(J-A) = J^2 - 2AJ - J + A(A+I) = (n-2\nu-1)J + A(A+I)$, so the assertion follows. ■

Proposition 2 *Let $\Gamma = (V,E)$ be a graph with adjacency matrix A, $|V| = n$. Let $C = C_p(A)$, $RC = C_p(RA)$ and $\overline{C} = C_p(\overline{A})$. Then*

1. *if $C \subseteq RC^\perp$, then $C = RC^\perp$ and C is RLCD;*

2. *if Γ is regular of valency ν, A has integral eigenvalues, and $C \subseteq \overline{C}^\perp$, then $C = \overline{C}^\perp$ and C is CLCD, except, possibly, if $p|\nu$ and $p|(|V|-1)$. In any case,* $\dim C \leq \dim(\overline{C}^\perp) \leq \dim(C)+1$.

Proof: (1): This is clear by Result 2.
(2) Suppose $C \subseteq \overline{C}^\perp$. Denote the eigenvalues for A by $\{e_i \mid 1 \leq i \leq r\}$ with multiplicity m_i, and suppose that in $\mathbb{F}_p$, $e_1, \ldots, e_s \equiv 0 \pmod{p}$, and $e_i \not\equiv 0 \pmod{p}$ for $i \geq s+1$. If $\nu \notin \{e_1, \ldots, e_s\}$, then the corresponding eigenvalues for $\overline{A}$ are $-1-e_1, \ldots, -1-e_s$ and are $\not\equiv 0 \pmod{p}$. From the argument regarding the eigenvalues above, $\dim(Null(C)) \leq \sum_{i=1}^s m_i$, so $\dim(C) \geq n - \sum_{i=1}^s m_i$, and $\dim(C^\perp) \leq \sum_{i=1}^s m_i$. Now $\dim(Null(\overline{C})) \leq \sum_{i=s+1}^r m_i$, so $\dim(\overline{C}) \geq n - \sum_{i=s+1}^r m_i = \sum_{i=1}^s m_i$, and we have $C = \overline{C}^\perp$.

Now suppose that $\nu \in \{e_1, \ldots, e_s\}$, i.e. that $p|\nu$. The corresponding eigenvalue of $\overline{A}$ is $n-1-\nu$ and if this is not $\equiv 0 \pmod{p}$ then the argument goes through as above. If however $n-1-\nu \equiv 0 \pmod{p}$, i.e. $p|(n-1)$, then we cannot deduce equality, although we do have $\dim(\overline{C}^\perp) \leq \dim(C)+1$. ■

When we have a graph Γ with integral eigenvalues for which $C_p(\Gamma)$ is $RLCD$, we can say exactly what the dimension is from the values of the eigenvalues modulo p:

Lemma 3 *Let $\Gamma = (V, E)$ be a graph with adjacency matrix A that has integral eigenvalues and suppose p is a prime for which $C_p(\Gamma)$ is RLCD. Then $\dim(C_p(\Gamma))$ is the sum of the multiplicities of the eigenvalues that are non-zero modulo p.*

Proof: Let $C = C_p(A)$, $RC = C_p(RA) = C_p(A + I)$. We have $C^\perp = RC$. Suppose the eigenvalues for A are $\{e_i \mid 1 \le i \le r\}$ with multiplicity m_i. Suppose that $e_1, \dots, e_s \equiv 0 \pmod{p}$, and $e_i \not\equiv 0 \pmod{p}$ for $i \ge s+1$. Thus the eigenvalues $e_1+1, \dots, e_s+1$ of $A+I$ are $\not\equiv 0 \pmod{p}$. From the argument regarding the eigenvalues above, $\dim(Null(C)) \le \sum_{i=1}^{s} m_i$, so $\dim(C) \ge v - \sum_{i=1}^{s} m_i$, and $\dim(C^\perp) \le \sum_{i=1}^{s} m_i$. Now $\dim(Null(RC)) \le \sum_{i=s+1}^{r} m_i$, so $\dim(RC) \ge v - \sum_{i=s+1}^{r} m_i = \sum_{i=1}^{s} m_i$. Thus $\dim(RC) = \dim(C^\perp) = \sum_{i=1}^{s} m_i$, and $\dim(C) = v - \sum_{i=1}^{s} m_i = \sum_{i=s+1}^{r} m_i$. ■

4 Uniform subset graphs

The **uniform subset graph** $\Gamma(n, k, r)$ (also called a Johnson graph $J(n, k, r)$ in the literature) has for vertices $V = \Omega^{\{k\}}$, the set of all subsets of size k of a set of size n, with two k-subsets x and y defined to be adjacent if $|x \cap y| = r$. The valency of $\Gamma(n, k, r)$ is $\binom{k}{r}\binom{n-k}{k-r}$. The symmetric group S_n always acts on $\Gamma(n, k, r)$, transitively on vertices and edges. Similarly for $R\Gamma(n, k, r)$, the corresponding reflexive graph, and $\overline{\Gamma}$, the complementary graph.

Let $A_r^k, RA_r^k = A_r^k + I, \overline{A_r^k} = J - I - A_r^k$ be adjacency matrices for $\Gamma(n, k, r)$, $R\Gamma(n, k, r)$ and $\overline{\Gamma}$, respectively, where $0 \le r \le k-1$. For any fixed prime p, and fixed n, k, let $C_r, RC_r, \overline{C_r}$ denote the row span over $\mathbb{F}_p$ of $A_r^k, RA_r^k, \overline{A_r^k}$, respectively.

Rows of $A_r^k, RA_r^k, \overline{A_r^k}$ for $r = 0, 1, \dots, k-1$ are denoted by r_x^r, s_x^r, c_x^r respectively, for $x \in V$, where we assume a fixed value of $k \ge 2$. Thus, from Equation (3),

$$s_x^r = r_x^r + v^x, \quad c_x^r = \boldsymbol{\jmath} - v^x - r_x^r.$$

We will simply write A, r_x, and so on, instead of A_r^k, r_x^r, and so on, when speaking generally of a fixed k and r in $\Gamma(n, k, r)$.

The codes W_i for $1 \le i \le k-1$ are defined in [11]: for $1 \le s \le n$ let $\Omega^{\{s\}}$ denote the set of s-subsets of Ω. For $\Lambda \in \Omega^{\{s\}}$ and $0 \le s \le k$, define

$$w_\Lambda = \sum_{\substack{\Lambda_1 \in \Omega^{\{k-s\}} \\ \Lambda \cap \Lambda_1 = \emptyset}} v^{\Lambda \cup \Lambda_1}, \quad W_s = \langle w_\Lambda \mid \Lambda_i \in \Omega^{\{s\}} \rangle, \quad E(W_s) = \langle w_{\Lambda_1} - w_{\Lambda_2} \mid \Lambda_i \in \Omega^{\{s\}} \rangle. \tag{4}$$

A further code W_Π is obtained by taking the partitions of subsets of size $2k$ of Ω. Let such a partition π of the $2k$-set $\Lambda = \{a_1, a_2, b_1, b_2, \dots, k_1, k_2\}$ be $[[a_1, a_2], [b_1, b_2], \dots, [k_1, k_2]]$. The word w_π, of weight 2^k is given by

$$w_\pi = \sum \pm v^{\{a_{i_1}, b_{i_2}, \dots, k_{i_k}\}}$$

where all the subsets of Λ of k-sets of the form $\{a_{i_1}, b_{i_2}, \dots, k_{i_k}\}$, where $i_j \in \{1, 2\}$, are present, with the sign being determined by giving $x = \{a_1, b_1, \dots, k_1\}$ the sign "+", and then demanding that any other k-set in the support with intersection of size $k-1$ with x will have sign "−", and then applying this in general to get the signs on all the 2^k vertices. Then

$$W_\Pi = \langle w_\pi \mid \pi \text{ partition of } \Lambda \subset \Omega, |\Lambda| = 2^k \rangle. \tag{5}$$

Note that $W_\Pi \subseteq W_s^\perp$ for all p, n, k, r, $0 \le s \le k-1$.

We mention these codes as they show themselves in the codes from uniform subset graphs, as demonstrated in [11] (but see also [22, 21, 23, 17, 14] for $k = 2, 3$): what was found for $k = 2, 3$, all p, and for other values of k (for example for Johnson and odd graphs for all k and $p = 2$, from Fish [16]) was that the codes of $\Gamma(n, k, r)$ and $R\Gamma(n, k, r)$ were all some combination of the codes C, where C is W_s, $E(W_s)$, W_Π, $\langle \jmath \rangle$, $\mathbb{F}_p^V$, along with their duals and hulls.

In particular, from [22, 21, 23, 17, 14, 11, 16], we have the following $RLCD$ candidates from the codes from adjacency matrices of uniform subset graphs.

Result 3 *For $n \geq 7$, $k = 3$, C_i, RC_i for $i = 0, 1, 2$ as defined, $C_i^\perp = RC_i$ in the following cases:*

1. *For $p \geq 5$, $n \equiv 5 \pmod p$, $C_0^\perp = RC_0 = W_2$, and RC_0 is a $[\binom{n}{3}, \binom{n}{2}, n-2]_p$ code, C_0 is a $[\binom{n}{3}, \binom{n}{3} - \binom{n}{2}, \delta]_p$ code, where $\delta \leq 8$.*
2. *For $p = 2$, $n \equiv 1 \pmod 4$, $C_0^\perp = RC_0 = W_1 + W_2$, and RC_0 is a $[\binom{n}{3}, \binom{n}{2}, n-2]_2$ code, C_0 is a $[\binom{n}{3}, \binom{n}{3} - \binom{n}{2}, 8]_2$ code.*
3. *For $p = 3$, $n \equiv 5 \pmod 9$, $C_0^\perp = RC_0 = W_2 + \langle \jmath \rangle$, and RC_0 is a $[\binom{n}{3}, \binom{n}{2} + 1, n-2]_3$ code, C_0 is a $[\binom{n}{3}, \binom{n}{3} - \binom{n}{2} - 1, 8]_3$ code.*
4. *For $p = 2$, $n \equiv 0 \pmod 4$, $C_1^\perp = RC_1 = W_1$ and RC_1 is a $[\binom{n}{3}, n, \binom{n-1}{2}]_2$ code, C_1 is a $[\binom{n}{3}, \binom{n}{3} - n, 4]_2$ code.*
5. *For $p = 2$, $n \equiv 1, 3 \pmod 4$, $C_2^\perp = RC_2 = W_2$ and RC_2 is a $[\binom{n}{3}, \binom{n}{2}, n-2]_2$ code, C_2 is a $[\binom{n}{3}, \binom{n}{3} - \binom{n}{2}, 4]_2$ code.*

For $n \geq 5$, $k = 2$, $p = 2$,

1. *For $n \equiv 3 \pmod 4$ then $C_0^\perp = RC_0 = W_1 + \langle \jmath \rangle$ and RC_0 is a $[\binom{n}{2}, n, n-1]_2$ code, C_0 is a $[\binom{n}{2}, \binom{n}{2} - n, 4]_2$ code; $C_1 = W_1 = RC_1^\perp$ and C_1 is a $[\binom{n}{2}, n-1, n-1]_2$ code, RC_1 is a $[\binom{n}{2}, \binom{n}{2} - n, 3]_2$ code.*
2. *For $n \equiv 1 \pmod 4$, $C_1 = W_1 = RC_1^\perp$ and C_1 is a $[\binom{n}{2}, n-1, n-1]_2$ code, RC_1 is a $[\binom{n}{2}, \binom{n}{2} - n, 3]_2$ code; $C_0 = E(W_1)^\perp$ is LCD.*

Since the paper [11] concerns the relationship of the codes from the $\Gamma(n, k, r)$ and the W codes (see Equations (4) and (5)) as defined above, we mention a couple of results from [11] concerning these codes, since they occur frequently amongst the $RLCD$ and $CLCD$ codes for this class of graphs.

Result 4 *For all n, $\dim(W_1) = n$ if $p \not| k$ and $\dim(W_1) = n - 1$ if $p | k$.*

For $p = 2$, $k \geq 2$, $n \geq 7$, the non-zero words of W_1 have weight n_r for $1 \leq r \leq \lfloor n/2 \rfloor$ where

$$n_r = \sum_{i=0}^{\lfloor (k-1)/2 \rfloor} \binom{r}{2i+1} \binom{n-r}{k-(2i+1)}$$

and also of weight $\binom{n}{k} - n_r$ if k is odd. There are $\binom{n}{r}$ of weight n_r.

For $k = 3$ the minimum weight is $\binom{n-1}{2}$.

Result 5 *For $n \geq 2k + 1$, any $k \geq 2$, p prime, W_{k-1} has minimum weight $n - k + 1$. For $n > 2k + 1$, the minimum words are the scalar multiples of the w_Λ for $\Lambda \subset \Omega$ with $|\Lambda| = k - 1$. Further, $\dim(W_{k-1}) \geq \binom{n-1}{k-1}$ for all p, with equality when $p = 2$.*

The fact that for uniform subset graphs where $C = C_i$ and $C^\perp = RC_i$ or $\overline{C_i}$ (or vice versa) and thus LCD, it is immediate how to split any $v \in \mathbb{F}_p^V$ into its orthogonal parts, should be a help in correcting errors.

Example 1 Consider $\Gamma(n, 3, 1)$ for $n \equiv 0 \pmod 4 > 7$. Then from Result 3, for $p = 2$, let $C = RC_1 = W_1$, and then $C^\perp = C_1 = W_1^\perp$. From Result 4, C is a $[\binom{n}{3}, n, \binom{n-1}{2}]_2$ LCD code, and $C^\perp$ is a $[\binom{n}{3}, \binom{n}{3} - n, 4]_2$ code.

To decode, suppose r is the received vector. If $S = \mathrm{Supp}(r)$ then $r = v^S = \sum_{x\in S} s_x^1 + \sum_{x\in S} r_x^1 = u_1 + u_2$ where $u_1 = \sum_{x\in S} s_x^1 = r\Pi_C \in C$, $u_2 = \sum_{x\in S} r_x^1 = r\Pi_{C^\perp} \in C^\perp$. We can also write $u_2 = v^T = \sum_{x\in T} r_x^1$ where $T = \mathrm{Supp}(u_2)$. Thus $|T| = \mathrm{wt}(u_2)$.

Now we wish to find first $m = \min\{\mathrm{wt}(w - u_2) \mid w \in C\}$, and then $\{w|w \in C|\mathrm{wt}(w - u_2) = m\}$. If the number of errors is less than $\frac{1}{2}\binom{n-1}{2}$ then there will be a unique member of this set. Thus we look for a coset leader c of $C - u_2 = W_1 - u_2$, and decode as $u_1 + (c + u_2) = r + c$. Since $C = W_1$ is a small code, it seems that this is quite speedily done by computer, although a real formula or algorithm for this would be desirable. ■

Computational findings

Using Magma [7, 3] some further $RLCD$ and $CLCD$ codes were found:

- $k = 4$, $p = 2$:
  $n = 9$, $C_1^\perp = RC_1 = \overline{C_1}$, $C_3^\perp = RC_3 = \overline{C_3}$; $n = 11$, $C_0^\perp = \overline{C_0}$, $C_3^\perp = RC_3 = \overline{C_3}$; $n = 13$, $C_1^\perp = RC_1$, $C_3^\perp = RC_3$; $n = 15$, $C_0^\perp = RC_0$, $C_3^\perp = RC_3$; $n = 17$, $C_1^\perp = RC_1 = \overline{C_1}$, $C_3^\perp = RC_3 = \overline{C_3}$;
- $k = 4$, $p = 3$: $n = 15$, $C_1^\perp = RC_1 = \overline{C_1}$;
- $k = 5$, $p = 2$
  $n = 11$, $C_4^\perp = RC_4 = \overline{C_4}$; $n = 12$, $C_3^\perp = RC_3 = \overline{C_3}$; $n = 13$, $C_2^\perp = RC_2$, $C_4^\perp = RC_4$; $n = 15$, $C_4^\perp = RC_4$.

All these computational findings are justified below in the lemmas and propositions to follow.

Uniform subset graphs of particular interest and that have been especially studied are those with $r = 0$ and $r = k-1$: $\Gamma(n, k, 0)$ is the **Kneser graph** $KG_{n,k}$, with eigenvalues for $j = 0$ to k:

$$\lambda_j = (-1)^j \binom{n-k-j}{k-j} \tag{6}$$

with multiplicity $m_j = \binom{n}{j} - \binom{n}{j-1}$ for $j > 0$ and 1 for $j = 0$. Here $KG_{2k+1,k} = \mathcal{O}_k$, is the odd graph of valency $k + 1$.

Further, the graph $\Gamma(n, k, k-1)$ is the **Johnson graph** $J(n, k)$,with eigenvalues for $j = 0$ to k:

$$\theta_j = k(n-k) - j(n+1-j) \tag{7}$$

with multiplicity m_j as above.

For the general case $\Gamma(n, k, r)$, the eigenvalues are found from the Eberlein polynomials in [25, Theorem 5.1] (see also [9, 1, 5, 8] and [5, Theorem 4.6]) for $j = 0$ to k:

$$\varepsilon_j = \sum_{i=Max\{0,j-r\}}^{Min\{j,k-r\}} (-1)^i \binom{j}{i}\binom{k-j}{k-r-i}\binom{n-k-j}{k-r-i} \tag{8}$$

with multiplicity m_j as given above.

Note that in all cases $\varepsilon_0 = \binom{k}{k-r}\binom{n-k}{k-r}$, the valency of $\Gamma(n,k,r)$, and $\varepsilon_k = (-1)^{k-r}\binom{k}{k-r}$.

For $r = 1$, i.e. $\Gamma(n,k,1)$, this can be written more simply, for $j = 0$ to k:

$$\varepsilon_j = (-1)^{j-1} j \binom{n-k-j}{k-j} + (-1)^j (k-j) \binom{n-k-j}{k-j-1}. \tag{9}$$

Since the eigenvalues of all the uniform subset graphs are integral we can use Proposition 2 to determine for what p and for what values of n, k they have $RLCD$ or $CLCD$ codes, and also to determine the dimnsion of the code in the $RLCD$ case, using Lemma 3. We need to determine when the inner product (s_x, r_y) or (c_x, r_y) is zero for all choices of x, y. This value depends on $|x \cap y|$.

Note: For $\Gamma = \Gamma(n,k,r)$, $\overline{\Gamma}$ is not a uniform subset graph unless $k = 2$. The eigenvalues of $R\overline{A} = J - A$ are also integral and given by $|V| - \nu$, and $-\theta$, where ν is the valency of Γ and the θ are the eigenvalues of A with eigenvectors w orthogonal to $\jmath$, as discussed earlier for $\overline{A}$. If we denote the rows of $R\overline{A}$ by d_x for $x \in V$, then $d_x = \jmath - r_x = v^x + c_x$.

Proposition 3 *Let* $\Gamma = \Gamma(n,k,r) = (V,E)$ *of valency* $\nu = \binom{k}{r}\binom{n-k}{k-r}$, *where* $0 \leq r \leq k-1$, p *any prime, and* A *an adjacency matrix for* Γ. *Let* $C = C_p(\Gamma)$, $RC = C_p(R\Gamma)$, $\overline{C} = C_p(\overline{\Gamma})$, *and* $\overline{\nu} = |V| - 1 - \nu$, *the valency of* $\overline{\Gamma}$.

For $j = 0, \ldots, k$, *let* $i_j = (r_x, r_y)$ *for* $|x \cap y| = j$. *Then* $(s_x, r_y) = i_j$ *for* $j \neq r$, $(s_x, r_y) = 1 + i_r$ *for* $|x \cap y| = r$, $i_k = \nu$, *and*

$$i_j = \sum_{i=0}^{j} \binom{k-j}{r-i}^2 \binom{j}{i} \binom{n-(2k-j)}{k-(2r-i)}.$$

Further:

1. $C \subseteq RC^\perp$ *if and only if* $i_j \equiv 0 \pmod{p}$ *for* $0 \leq j \leq k$, $j \neq r$, *and* $i_r^* = i_r + 1 \equiv 0 \pmod{p}$, *in which case* $C = RC^\perp$.
2. $C \subseteq \overline{C}^\perp$ *if and only if for* $0 \leq j \leq k$, $j \neq r$, $\ell_j = i_k - i_j \equiv 0 \pmod{p}$, *and* $\ell_r = i_k - i_r - 1 = i_k - i_r^* \equiv 0 \pmod{p}$. *Further,* $C = \overline{C}^\perp$ *unless, possibly,* $p|\nu$ *and* $p|(|V|-1)$.
3. $\overline{C} = R\overline{C}^\perp$ *if and only if* $t_j = \overline{\nu} - \ell_j \equiv 0 \pmod{p}$ *for* $0 \leq j \leq k$. *Then* $C \subseteq \overline{C}^\perp$, *and if* $p|\nu$ *then* $C = RC^\perp$, *or if* $p \not| \nu$, *then* $C = \overline{C}^\perp = R\overline{C}$.

Proof: (1) The value for i_j is a direct count of vertices adjacent to both x and y, and then the requirement that the inner product must be 0 for any pair of rows of A and $A+I$, so that $C \subseteq RC^\perp$. That $C = RC^\perp$ follows from Proposition 2 and the above statement regarding the eigenvalues of Γ.

(2) Since $c_x = \jmath - v^x - r_x$, for any $y \in V$, $(c_x, r_y) = i_k - (v^x, r_y) - (r_x, r_y)$. Thus $(c_x, r_x) = \ell_k = 0$, $(c_x, r_y) = i_k - i_j$ if $j \neq r$, and $(c_x, r_y) = i_k - i_r - 1$. Similarly, Proposition 2 can be used for the equality.

(3) $d_x = \jmath - r_x$, so $(d_x, c_y) = (\jmath - r_x, \jmath - v^y - r_y) = \overline{\nu} + (r_x, v^y) + (r_x, r_y) - i_k$. Thus $(d_x, c_y) = \overline{\nu} + (i_j - i_k) = \overline{\nu} - \ell_j = t_j$ for $j \neq r$, and $(d_x, c_y) = \overline{\nu} + (i_r^* - i_k) = \overline{\nu} - \ell_r = t_r$ for $|x \cap y| = r$. If all these are zero modulo p then we will have $\overline{C} = R\overline{C}^\perp$ and $C \subseteq \overline{C}^\perp$. If $p|\nu$ then $C = RC^\perp$, and if $p \not| \nu$ then $C = \overline{C}^\perp$. ■

Example 2 Special cases:

- For $\Gamma = J(n,k) = \Gamma(n,k,k-1)$,
  $i_j = 0$ for $0 \le j \le k-3$, $i_{k-2} = 4$, $i^*_{k-1} = n-1$, $i_k = k(n-k)$;
  $\ell_j = k(n-k)$ for $0 \le j \le k-3$, $\ell_{k-2} = k(n-k) - 4$, $\ell_{k-1} = k(n-k) - (n-1)$, $\ell_k = 0$;

- For $\Gamma = KG_{n,k} = \Gamma(n,k,0)$, for $0 \le j \le k$,
  $i_j = \binom{n-(2k-j)}{k}$, $i^*_0 = 1 + \binom{n-2k}{k}$;
  $\ell_0 = \binom{n-k}{k} - 1 - \binom{n-2k}{k}$, $\ell_j = \binom{n-k}{k} - \binom{n-(2k-j)}{k}$ for $1 \le j \le k$.

- For $\Gamma(n,k,1)$, for $0 \le j \le k$,
$$i_j = j\binom{n-(2k-j)}{k-1} + (k-j)^2\binom{n-(2k-j)}{k-2},$$
  and $i^*_1 = 1 + \binom{n-(2k-1)}{k-1} + (k-1)^2\binom{n-(2k-1)}{k-2}$.

Corollary 1 *1. For $C = C_p(J(n,k))$, C is RLCD if and only if $p = 2$ and n is odd. C is CLCD (and $\overline{C} = RC$), only for $p = 2$ and n odd, unless, possibly, $\binom{n}{k}$ is odd.*

2. If $C = C_p(KG_{2k+1,k}) = C_p(\mathcal{O}_k)$, then C is neither RLCD nor CLCD for any p or k.

3. if $C = C_p(\Gamma(n,k,r))$ and $C \subseteq RC^\perp$ then $C \subseteq (\overline{C})^\perp$ and $RC = C^\perp$. Conversely, $C \subseteq (\overline{C})^\perp \not\Rightarrow C = RC^\perp$.

Proof: (1): Clearly since $i_{k-2} = 4$, we must have $p = 2$, and then for $i_{k-1} = n-1$ to be even we need n odd. Then $i_k = k(n-k)$ is even for any k. Similarly for $CLCD$.
(2) For the odd graph $i^*_0 = 1 + \binom{1}{k} = 1$, so this is never zero. Similarly for $CLCD$.
(3)The first statement is clear, and as a counterexample to illustrate the second, take $\Gamma = \Gamma(13,3,1)$, $p = 2$. Here $C_1 = C = (\overline{C})^\perp \neq RC^\perp$ ■

Note: For any regular graph Γ of valency ν, with the same notation for $r_x, s_x, c_x, C, RC, \overline{C}$ as above, since $(c_x, r_y) = \nu - (s_x, r_y)$, it follows that $C \subseteq RC^\perp \Rightarrow C \subseteq (\overline{C})^\perp$, but the converse implication only holds if $p|\nu$.

For $J(n,k)$ the following result, giving $C = C_2(J(n,k))$ in terms of the code W_k, is from [11, 16]:

Result 6 *For $k \ge 3$, $n \ge 2k+1$, $p = 2$, $\Gamma = J(n,k)$, let $C = C_2(\Gamma)$, $RC = C_2(R\Gamma)$. Then*

1. *for n, k odd, $C = W_{k-1}^\perp$, $RC = W_{k-1}$, $\mathrm{Hull}(C) = \{0\}$;*

2. *for n odd, k even, $C = W_{k-1}$, $RC = W_{k-1}^\perp$, $\mathrm{Hull}(C) = \{0\}$;*

3. *for n, k even, $C \subseteq \mathrm{Hull}(W_{k-1})$, $RC = \mathbb{F}_2^V$;*

4. *for n even, k odd, $C = \mathbb{F}_2^V$, $RC \subseteq \mathrm{Hull}(W_{k-1})$.*

From Example 2, putting the $i_j \equiv 0 \pmod p$ (respectively $\ell_j \equiv 0 \pmod p$) for $j \neq r$, and $i^*_r \equiv 0 \pmod p$ (respectively $\ell_r \equiv 0 \pmod p$), we can deduce the following:

- for $C = C_p(\Gamma)$ for $\Gamma = KG_{n,k} = \Gamma(n,k,0)$:

  - For $k = 2$, C is *RLCD* precisely when $p = 2$ and $n \equiv 3 \pmod 4$. (Since $\Gamma(n, 2, 0)$ is strongly regular, this also follows from Corollary 2 (1).) C is *CLCD* when $p = 2$ and $n \equiv 1 \pmod 4$.
  - For $k = 3$, C is *RLCD* precisely when $p = 2$ and $n \equiv 1 \pmod 4$, and C is also *CLCD*; C is *RLCD* for $p = 3$ and $n \equiv 5 \pmod 9$, and C is *CLCD* for $p = 3$ and $n \equiv 2, 8 \pmod 9$; C is *RLCD* for $p \geq 5$ only for $n \equiv 5 \pmod p$, and likewise C is *CLCD* only in this case.
  - For $k = 4$, C is *RLCD* precisely when $p = 2$ and $n \equiv 7 \pmod 8$; C is *CLCD* precisely when $p = 2$ and $n \equiv 3 \pmod 8$.

- for $C = C_p(\Gamma)$ for $\Gamma = \Gamma(n, k, 1)$:
  - For $k = 3$, C is *RLCD* precisely when $p = 2$ and $n \equiv 0 \pmod 4$; C is *CLCD* precisely when $p = 2$ and $n \equiv 0, 1 \pmod 4$.
  - For $k = 4$, for $p = 2$ C is *RLCD* precisely when $n \equiv 1 \pmod 4$ and C is *CLCD* for $p = 2$ when $n \equiv 1 \pmod 8$; for $p = 3$ C is *RLCD* precisely when $n \equiv 6 \pmod 9$, and likewise C is *CLCD*; for $p \geq 5$, C is neither *RLCD* nor *CLCD*.

Using the formula for the eigenvalues as given in Equation (8), we can get the precise dimension in the cases above when the code is *RLCD*, from Lemma 3.

Example 3 1. From the above observations we have $C_2(\Gamma(n, 3, 1))$ is *RLCD* if $n \equiv 0 \pmod 4$. From Equation (9) the eigenvalues are $\varepsilon_0 = 3\binom{n-3}{2}, \varepsilon_1 = \binom{n-4}{2} - 2(n-4), \varepsilon_2 = -2n+11, \varepsilon_3 = 3$. Only ε_2 and ε_3 are non-zero modulo 2, so $\dim(C_2(\Gamma(n, 3, 1)) = m_2 + m_3 = \binom{n}{3} - n$. This agrees with [21] where the dimensions of the binary codes were found by other methods.

2. For $\Gamma(n, 4, 1)$, the eigenvalues are $\varepsilon_0 = 4\binom{n-4}{3}$, $\varepsilon_1 = \binom{n-5}{3} - 3\binom{n-5}{2}$, $\varepsilon_2 = -(n-6)(n-9)$, $\varepsilon_3 = 3n - 22$, $\varepsilon_4 = -4$. Thus for $p = 2$ and $n \equiv 1 \pmod 4$, from the observations above, $C_2(\Gamma(n, 4, 1))$ is *RLCD*, and since only $\varepsilon_3 \not\equiv 0 \pmod 2$, $C_2(\Gamma(n, 4, 1))$ is a $[\binom{n}{4}, \binom{n}{3} - \binom{n}{2}, d]_2$ code, where $d \leq 4\binom{n-4}{3}$.

3. For $C_3(\Gamma(n, 4, 1))$ and $n \equiv 6 \pmod 9$, from the expressions for ε_i in (2) above, only ε_3 and ε_4 are non-zero modulo 3, so $C_3(\Gamma(n, 4, 1))$ is a $[\binom{n}{4}, \binom{n}{4} - \binom{n}{2}, d]_3$ code, where $d \leq 4\binom{n-4}{3}$.

5 Strongly regular graphs

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 graph Γ is also strongly regular of type $(n, n-k-1, n-2k+\mu-2, n-2k+\lambda)$.

Let Γ be a strongly regular graph with parameters (n, k, λ, μ) and A an adjacency matrix for Γ. From [6, Chapter 2], the eigenvalues for A are λ_i for $0 \leq i \leq 2$ with multiplicities m_i respectively, those for $R\Gamma$ are $\lambda_i^* = \lambda_i + 1$ with multiplicities m_i for $0 \leq i \leq 2$, and those for $\overline{\Gamma}$ are $\overline{\lambda_0} = n - 1 - k$, $\overline{\lambda_i} = -\lambda_i - 1$ for $i = 1, 2$, where where

- $\lambda_0 = k$, $\lambda_0^* = k + 1$, $\overline{\lambda_0} = n - 1 - k, m_0 = 1$;
- $\lambda_1 = \frac{1}{2}(\lambda - \mu + \sqrt{(\lambda - \mu)^2 + 4(k - \mu)})$, $\lambda_1^* = \frac{1}{2}(\lambda - \mu + 2 + \sqrt{(\lambda - \mu)^2 + 4(k - \mu)})$, $\overline{\lambda_1} = -\lambda_2 - 1$, $m_1 = \frac{1}{2}(n - 1 + \frac{(n-1)(\mu-\lambda)-2k}{\sqrt{(\mu-\lambda)^2+4(k-\mu)}})$;

- $\lambda_2 = \frac{1}{2}(\lambda - \mu - \sqrt{(\lambda-\mu)^2 + 4(k-\mu)})$, $\lambda_2^* = \frac{1}{2}(\lambda - \mu + 2 - \sqrt{(\lambda-\mu)^2 + 4(k-\mu)})$, $\overline{\lambda_2} = -\lambda_1 - 1$, $m_2 = \frac{1}{2}(n - 1 - \frac{(n-1)(\mu-\lambda)-2k}{\sqrt{(\mu-\lambda)^2+4(k-\mu)}})$.

Note that $\lambda_1 + \lambda_2 = \lambda - \mu$.

Strongly regular graphs are of two types: Type I where $(n-1)(\mu-\lambda) = 2k$, in which case it follows that $\lambda = \mu - 1$, $k = 2\mu$, $n = 4\mu + 1$, and n is the sum of two integer squares (see [6, (2.18)Theorem]). Or, of Type II, where $(\mu - \lambda)^2 + 4(k - \mu)$ is the square of an integer, and in this case it follows that the eigenvalues are all integral.

Examples 1 1. Triangular graph $T(m) = \Gamma(n, 2, 1)$:
$(n, k, \lambda, \mu) = (\binom{m}{2}, 2(m-2), m-2, 4)$ so $\lambda - \mu = m - 6, k - \mu = 2m - 8$.

- $\lambda_0 = 2m - 4$, $\lambda_0^* = 2m - 3$, $\overline{\lambda_0} = \binom{m-2}{2}$, $m_0 = 1$;
- $\lambda_1 = m - 4$, $\lambda_1^* = m - 3$, $\overline{\lambda_1} = -3$, $m_1 = m - 1$;
- $\lambda_2 = -2$, $\lambda_2^* = -1$, $\overline{\lambda_2} = -m + 4$, $m_2 = \frac{1}{2}m(m-3)$;

2. Paley graph $P(q) = \overline{P(q)}$, where $q \equiv 1 \pmod 4$:
$(n, k, \lambda, \mu) = (q, \frac{1}{2}(q-1), \frac{1}{4}(q-5), \frac{1}{4}(q-1))$ so $\lambda - \mu = -1, k - \mu = \frac{1}{4}(q-1)$.

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

Note: The eigenvalues of $P(q)$ are integral if q is a square prime power.

For $x \in V$, as before, let r_x denote the row for x in A, s_x the row in $A + I$, c_x the row for x in $\overline{A} = J - I - A$.

With this notation:

Proposition 4 *Let Γ be a strongly regular graph with parameters (n, k, λ, μ) and A an adjacency matrix for Γ. Let p be any prime, $C = C_p(A)$, $RC = C_p(A + I)$, $\overline{C} = C_p(\overline{A})$. Then,*

1. *$C \subseteq RC^\perp$ if and only if $k \equiv 0 \pmod p$, $\lambda \equiv -1 \pmod p$, and $\mu \equiv 0 \pmod p$. If this is the case then $C = RC^\perp$ and if the eigenvalues of A are integral, then $\dim(C) = m_1$ or m_2, i.e. $\frac{1}{2}(n - 1 \pm \frac{(n-1)(\mu-\lambda)-2k}{\sqrt{(\mu-\lambda)^2-4(k-\mu)}})$.*

2. *$C \subseteq \overline{C}^\perp$ if and only if $k - 1 - \lambda \equiv 0 \pmod p$ and $k - \mu \equiv 0 \pmod p$. Further, if all the eigenvalues of A are integral, $C = \overline{C}^\perp$, unless, possibly, $k \equiv 0 \pmod p$ and $n-1 \equiv 0 \pmod p$. In any case, $\dim C \leq \dim(\overline{C}^\perp) \leq \dim(C) + 1$.*

Proof: (1): $(r_x, s_x) = k$; if $x \sim y$ then $(r_x, s_y) = 1 + \lambda$; if $x \not\sim y$ then $(r_x, s_y) = \mu$. Thus $C \subseteq RC^\perp$ if and only if $k \equiv 0 \pmod p$, $\lambda \equiv -1 \pmod p$, and $\mu \equiv 0 \pmod p$. If this is the case then $C = RC^\perp$, by Proposition 2.

We have $\lambda_0 = k \equiv 0 \pmod p$, $\lambda \equiv -1 \pmod p$, and $\mu \equiv 0 \pmod p$, so $\lambda - \mu \equiv -1 \pmod p$, and $\lambda_1 + \lambda_2 \equiv -1 \pmod p$. If both λ_1 and λ_2 are non-zero modulo p, then $\dim(C) = n - 1$, and $\dim(RC) \leq 1$, which is impossible. So one of λ_1, λ_2 is 0 modulo p, and suppose $\lambda_i \equiv 0 \pmod p$.

It follows that $\dim(C) \geq n - (1 + m_i) = m_j$. Since $\lambda_i^* \equiv 1 \pmod p$ and $\lambda_0^* \equiv 1 \pmod p$, we must have $\lambda_j^* \equiv 0 \pmod p$, since $RC \neq \mathbb{F}_p^n$, and thus $\dim(RC) = 1 + m_i \leq \dim(C^\perp) \leq n - m_j = 1 + m_i$, proving equality.
(2): $(r_x, c_y) = (r_x, \boldsymbol{\jmath}) - (r_x, v^y) - (r_x, r_y)$, so $(r_x, r_x) = 0$; if $x \sim y$ then $(r_x, c_y) = k - 1 - \lambda$; if $x \not\sim y$, then $(r_x, s_y) = k - \mu$. Thus $C \subseteq \overline{C}^\perp$ if and only if $k - 1 - \lambda \equiv 0 \pmod p$ and $k - \mu \equiv 0 \pmod p$. However, if all the eigenvalues of A are integral, in the case where $\lambda_0 = k \equiv 0 \pmod p$ and $\overline{\lambda_0} = n - k - 1 \equiv 0 \pmod p$, we cannot use the dimension argument as in the *RLCD* case, so we might have $C \subset \overline{C}^\perp$, in which case, following Proposition 2, $\dim(\overline{C}^\perp) = \dim(C) + 1$. ■

Note: 1: $\Gamma = T(m)$, $p = 2$, and $m \equiv 3 \pmod 4$ has $\binom{m}{2} \equiv 1 \pmod 4$, and $C \subset \overline{C}^\perp$, so the excluded case mentioned in (2) above does occur.
2: See [4, 19] for the p-ranks of strongly regular graph when the eigenvalues are not necessarily integral, in which case we only have $C \subseteq \overline{C}^\perp$, so other arguments must be used to obtain equality.

Corollary 2

1. *If $\Gamma = T(m) = \Gamma(m, 2, 1)$, the triangular graph with parameters $(\binom{m}{2}, 2(m-2), m-2, 4)$, then if m is odd and $p = 2$, $C = C_2(\Gamma)$ is RLCD, and $\dim(C) = m - 1$. Further, $T(m)$ is CLCD for $p = 2$ and $m \equiv 1 \pmod 4$.*

   The complement $\overline{T(m)} = \Gamma(m, 2, 0)$, is a $(\binom{m}{2}, \binom{m-2}{2}, \binom{m-4}{2}, \binom{m-3}{2})$ strongly regular graph. Here $C = C_p(\overline{T(m)})$ is RLDC only for $p = 2$ and $m \equiv 3 \pmod 4$.

2. *If $\Gamma = L_2(m)$, the square lattice graph, the parameters are $(m^2, 2(m-1), m-2, 2)$. For $p = 2$ and m odd $C = C_2(\Gamma)$ is RLCD with $\dim(C) = m_1 = 2m - 2$.*

   $\overline{\Gamma}$ is $(m^2, (m-1)^2, (m-2)^2, (m-1)(m-2))$ and is RLCD if $p = 2$ and m is odd. Then $\dim(C) = m_1 = (m-1)^2$.

3. *If $\Gamma = P(q) = \overline{P(q)}$, 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 $\frac{1}{2}(q-1)$ if $p = 2$ and $q \equiv 1 \pmod 8$ or p is odd and $q \equiv 1 \pmod p$.*

4. *Γ is the graph #12 of [4, p. 342] with parameters $(81, 20, 1, 6)$ is RLCD if $p = 2$, and $\dim(C) = 20$.*

Proof: (1): Referring to Proposition 4 for $T(m)$, since $\mu = 4$ this can only be 0 modulo p if $p = 2$. Then we need m to be odd for $\lambda + 1 \equiv 0 \pmod 2$. Since $\lambda_1 \equiv 0 \pmod 2$, from the proposition $\dim(C) = m_1 = m - 1$. For $\overline{T(m)}$, the parameters follow from [6, Chapter 2]. The conclusions also follow from Result 3.
(2),(3),(4): Similarly clear from the parameters. ■

Note: 1. Since the Petersen graph is $\overline{T(5)}$, i.e. also the odd graph $\Gamma(5, 2, 0) = \mathcal{O}(2)$, its p-ary code is not *RLCD* for any p.
2. If $\Gamma = Sp_{2m}(q)$, the symplectic graph with point set the projective points of $PG_{2m-1}(q)$, then Γ is strongly regular with parameters

$$n = \frac{q^{2m} - 1}{q - 1}, k = \frac{q^{2m-1} - 1}{q - 1} - 1, \lambda = \frac{q^{2m-2} - 1}{q - 1} - 2, \mu = \frac{q^{2m-2} - 1}{q - 1}$$

with spectrum $k^1, (q^{m-1} - 1)^f, (-q^{m-1} - 1)^g$, where $f = \frac{1}{2}(\mu - 1 + q^m)$ and $g = \frac{1}{2}(\mu - 1 - q^m)$: see, for example, [4]. Thus the eigenvalues are all integral and both parts of Proposition 4 can be applied.

Also, $\overline{\Gamma}$ has $\overline{\lambda} = \overline{\mu}$. Since $\mu = \lambda + 2$, we cannot have $\mu \equiv 0 \pmod p$ and $\lambda \equiv -1 \pmod p$, so Γ is never $RLCD$, and neither is $\overline{\Gamma}$. Similarly, it cannot be $CLCD$ for any of the parameters, since $k - 1 - \lambda \equiv 0 \pmod p$ implies that $k - \mu + 1 \equiv 0 \pmod p$, so we cannot have $k - \mu \equiv 0 \pmod p$, i.e. the conditions of Proposition 4 are not satisfied in any case.

5.1 Generalized Paley graphs

It was found computationally in [27], using Magma, that some of the generalized Paley graphs, $GP(q, k)$ are strongly regular with q odd, and the parameters tell us that those found are $RLCD$. A **generalized Paley graph** $GP(q, k)$ (see also [30]) is defined as follows: q is a prime power, $k|(q-1)$, $k \geq 2$ and either q or $\frac{q-1}{k}$ is even. S is the subgroup of $\mathbb{F}_q^\times$ of order $s = \frac{q-1}{k}$. Then $GP(q, k) = (V, E)$ where $V = \mathbb{F}_q$ and, for $x, y \in V$, $x \sim y$ if $x - y \in S$. The conditions imply that $GP(q, k)$ is an undirected graph, and for q odd, $s = |S| = \frac{q-1}{k}$ even. If $k = 2$ then q is odd, and $GP(q, 2) = P(q)$, the Paley graph.

The computational results (excluding $k = 2$, so that the graphs are of Type II) from [27] for $GP(q, k)$ to be strongly regular are given in Table 1, using also our Proposition 4 to show where the codes are $RLCD$, since all the eigenvalues are integral. In the table the columns are headed by $GP(q, k)$, the parameters of the strongly regular graph, the code parameters, and the nature of the minimum words, if found computationally, respectively. None of these are $CLCD$.

(q, k)	p	type	$C_p(\Gamma)$	min wds C	$RC_p(\Gamma)$
$(25, 3)$	2	$(25, 8, 3, 2)$	$[25, 8, 8]_2$	rows of A	$[25, 17, 4]_2$
$(49, 4)$	2	$(49, 12, 5, 2)$	$[49, 12, 12]_2$	rows of A	$[49, 37, 4]_2$
$(81, 4)$	2	$(81, 201, 1, 6)$	$[81, 20, 20]_2$	rows of A	$[81, 61, 6]_2$
$(81, 5)$	2	$(81, 16, 7, 2)$	$[81, 16, 16]_2$	rows of A	$[81, 65, 4]_2$
$(121, 3)$	2	$(121, 40, 15, 12)$	$[121, 40, 20]_2$		$[121, 81, 8]_2$
$(121, 4)$	2	$(121, 30, 11, 6)$	$[121, 90, 6]_2$		$[121, 31, 11]_2$
$(121, 4)$	3	$(121, 30, 11, 6)$	$[121, 30, 20]_3$		$[121, 91, 6]_3$
$(121, 6)$	2	$(121, 20, 9, 2)$	$[121, 20, 20]_2$	rows of A	$[121, 101, 4]_2$
$(3^5, 11)$	2	$(243, 22, 1, 2)$	$[243, 110, d]_2$	$d \leq 22$	$[243, 133, \delta \leq 23]_2$
$(3^6, 4)$	2	$(729, 182, 55, 42)$	$[729, 546, d]_2$	$d \leq 182$	$[729, 183, \delta \leq 183]_2$
$(3^6, 7)$	2	$(729, 104, 31, 12)$	$[729, 104, d]_2$	$d \leq 104$	$[729, 625, \delta \leq 105]_2$
$(3^6, 14)$	2	$(729, 52, 25, 2)$	$[729, 52, d]_2$	$d \leq 52$	$[729, 677, \delta \leq 53]_2$

Table 1: Strongly regular generalized Paley graphs

It is shown in [30, Corollary 1] that the number of common neighbours to two adjacent vertices in $GP(q, k)$ is $|N(1) \cap S|$, so λ is a constant for all these graphs. In [27] it is shown that $\lambda - \mu$ is odd if $GP(q, k)$ is strongly regular, and $k > 2$.

6 Other LCD codes from graphs

Some of the papers mentioned here concerning codes from adjacency matrices from graphs have cases where the hull is zero, but the code is not $RLCD$ nor $CLCD$. However, in some of these papers the proofs that the hull was zero did involve expressing a weight-1 vector as a sum of vectors in C and $C^\perp$, so this would facilitate the expression of $w \in \mathbb{F}_p^V$ as a sum of vectors in C and $C^\perp$.

For example, in [21], where binary codes from the graphs $\Gamma(n,3,r)$ are studied, for $C = C_2(\Gamma(n,3,2))$ and n odd, in Proposition 1 it is shown that $C^\perp = W_2$, and that $\mathrm{Hull}(C) = \{0\}$, by showing that for $x = \{a,b,c\}$,

$$v^x = r_x^2 + w_{a,b} + w_{a,c} + w_{b,c},$$

where r_x^i denotes the row corresponding to x in an adjacency matrix for $\Gamma(n,3,i)$. (Note that there are typographical errors in that paper: on page 175, line -18, $v^{\{a,b,x\}}$ should read $v^{\{a,b,c\}}$, four times, at the end of the display.)

In [23], where ternary codes from the graphs $\Gamma(n,3,r)$ are studied, in Proposition 18, looking at $C = C_3(\Gamma(n,3,0))$ when $n \equiv 1 \pmod 3$, the set of equations at the end of the proof give, for $x = \{a,b,c\}$,

$$v^x = \jmath - r_x^0 + r_x^1 + w_a + w_b + w_c,$$

where $\jmath \in C$ or $C^\perp$, $w_i \in C^\perp$, and $r_x^1 \in C$.

However, the expression for $w = \sum_{i=1}^{|V|} \alpha_i v^{x_i} = (\alpha_1, \ldots, \alpha_{|V|})$, where $V = [x_1, \ldots, x_{|V|}]$, as the sum of a vector in C and $C^\perp$ is not as neatly expressed as in the case of $RLCD$ and $CLCD$. Thus, for this last expression, we have, for $w = \sum_{i=1}^{|V|} \alpha_i v^{x_i}$,

$$w = \sum_{i=1}^{|V|} \alpha_i \jmath - \sum_{i=1}^{|V|} \alpha_i r_{x_i}^0 + \sum_{i=1}^{|V|} \alpha_i r_{x_i}^1 + \sum_{i=1}^{|V|} \alpha_i \sum_{a \in x_i} w_a.$$

Further, in [10], a similar formula for v^x is established in Lemma 3.8 of that paper for the binary code C for the odd graph $\mathcal{O}_k = \Gamma(2k+1,k,0)$, where it is shown that $\mathrm{Hull}(C) = \{0\}$ for all k. The formula for v^x is

$$v^x = \sum_{i=1}^{k-2} \sum_{\substack{A \subset x \\ |A|=i}} \sum_{\substack{Y \subset \Omega \setminus x \\ |Y|=k-1-i}} \sum_{a \notin A \cup Y} v^{A \cup Y \cup \{a\}} + \sum_{y \subset \Omega \setminus x} r_y + k\jmath,$$

where $\jmath \in C$ for k even, and $\jmath \in C^\perp$ for k odd. Here the first term on the right-hand side is in $C^\perp$.

7 Conclusion

Many other classes of graphs are likely to have codes that are $RLCD$ or $CLCD$: we found, by computation, some from the Hamming graphs $H^k(n,m)$ (see [13, 12, 24] for the notation) where $H^1(n,2) = H(n,2) = \mathcal{Q}_n$, the n-cube. For example, for $n = 6, 8, 10$, $\Gamma = H^1(n,2)$, $C_2(\Gamma) = C_2(\overline{\Gamma})^\perp$; for $n = 6, 9$, $\Gamma = H^2(n,2)$, $C_3(\Gamma) = C_3(R\Gamma)^\perp$; for $k = 1, 2$, $\Gamma = H^k(6,3)$, $C_2(\Gamma) = C_2(R\Gamma)^\perp$. Also, in [26] codes acted on by subgroups of the McLaughlin group are found to have this property.

The codes from the Hamming graphs $H^k(n,m)$ are examined with respect to these properties in [15] and many classes of these graphs are found to satisfy them.

References

[1] José Araujo and Tim Bratten, *On the spectrum of the Johnson graphs $J(n,k,r)$*, Proceedings of the XXIIrd "Dr. Antonio A. R. Monteiro" Congress, 2016, Univ. Nac. Sur Dep. Mat. Inst. Mat., Baha Blanca, 2015, pp. 57–62.

[2] 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).

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

[4] A. E. Brouwer and C. J. van Eijl, *On the p-rank of the adjacency matrices of strongly regular graphs*, J. Algebraic Combin. **1** (1992), 329–346.

[5] A.E. Brouwer and W.H. Haemers, *Association schemes*, Handbook of Combinatorics (R.L. Graham, M. Grötschel, and L. Lovász, eds.), Elsevier; MIT, Cambridge,MA, 1995, Chapter 15, Vol. 1, pp. 749–771.

[6] 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.

[7] 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.

[8] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Tech. report, Philips Research Laboratorie, 1973, Philips Research Reports, Supplement No. 10.

[9] Philippe Delsarte and Vladimir I. Levenshtein, *Association schemes and coding theory*, IEEE Trans. Inform. Theory **44** (1998), 2477–2504.

[10] W. Fish, R. Fray, and E. Mwambene, *Binary codes and partial permutation decoding sets from the odd graphs*, Cent. Eur. J. Math. **12 (9)** (2014), 1362 –1371.

[11] W. Fish, J. D. Key, and E. Mwambene, *Codes from adjacency matrices of uniform subset graphs*, (Submitted).

[12] ______, *Codes, designs and groups from the Hamming graphs*, J. Combin. Inform. System Sci. **34** (2009), 169–182, No.1 – 4.

[13] ______, *Graphs, designs and codes related to the n-cube*, Discrete Math. **309** (2009), 3255–3269.

[14] ______, *Ternary codes from reflexive graphs on* 3*-sets*, Appl. Algebra Engrg. Comm. Comput. **25** (2014), 363–382.

[15] W. Fish, J. D. Key, E. Mwambene, and B.G. Rodrigues, *Hamming graphs and LCD codes*, (In preparation).

[16] Washiela Fish, *Codes from uniform subset graphs and cycle products*, Ph.D. thesis, University of the Western Cape, 2007.

[17] Washiela Fish, Jennifer D. Key, and Eric Mwambene, *Binary codes from reflexive graphs on* 3*-sets*, Adv. Math. Commun. **9** (2015), 211–232.

[18] D. Ghinelli, J. D. Key, and T. P. McDonough, *Hulls of codes from incidence matrices of connected regular graphs*, Des. Codes Cryptogr. **70** (2014), 35–54, http://dx.doi.org/10.1007/s10623-012-9635-0.

[19] Willem H. Haemers, René Peeters, and Jeroen M. van Rijckevorsel, *Binary codes of strongly regular graphs*, Des. Codes Cryptogr. **17** (1999), 187–209.

[20] 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.

[21] J. D. Key, J. Moori, and B. G. Rodrigues, *Binary codes from graphs on triples*, Discrete Math. **282/1-3** (2004), 171–182.

[22] ———, *Permutation decoding for binary codes from triangular graphs*, European J. Combin. **25** (2004), 113–123.

[23] ———, *Ternary codes from graphs on triples*, Discrete Math. **309** (2009), 4663–4681.

[24] Jennifer D. Key, Washiela Fish, and Eric Mwambene, *Codes from the incidence matrices and line graphs of Hamming graphs* $H^k(n,2)$ *for* $k \geq 2$, Adv. Math. Commun. **5** (2011), 373–394.

[25] M. Krebs and A. Shaheen, *On the spectra of Johnson graphs*, Electron. J. Linear Algebra **17** (2008), 154–167.

[26] D. Leemans and B. G. Rodrigues, *Linear codes with complementary duals from some strongly regular subgraphs of the McLaughlin graph*, Math. Commun. **21 (2)** (2016), 239–249.

[27] J. Limbupasiriporn and P. Limbupasiriporn, *Codes from adjacency matrices of generalized Paley graphs*, In preparation.

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

[29] B. G. Rodrigues, *Linear codes with complementary duals related to the complement of the Higman-Sims graph*, To appear: Bull. Iranian Math. Soc.

[30] P. Seneviratne and J. Limbupasiriporn, *Permutation decoding of codes from generalized Paley graphs*, Appl. Algebra Eng. Commun. Comput. **24** (2013), 225–236.