

On lifted codes and p -adic codes

- their weight enumerators

Young Ho Park

Department of Mathematics
Kangwon National University

2012 KIAS International Conference
on Coding Theory and Applications
November 16, 2012

Motivations

This talk is based on the followings:

- 1 (CS) A.R. Calderbank and N.J.A. Sloane, *Modular and p -adic cyclic codes*, DCC, **6** (1995), 21–35
- 2 S.T. Dougherty, S.Y. Kim and Y.H. Park, *Lifted codes and their weight enumerators*, Discrete Math. **305** (2005), 123–135
- 3 S.T. Dougherty and Y.H. Park, *Codes over the p -adic integers*, Des. Codes. Cryptogr. **39** (2006), 65–80
- 4 Recent work of S. Han on computing number of codewords of given weight (2011)
- 5 an unpublished note of mine (2012)

- 1 Codes over \mathbb{Z}_{p^e}
- 2 p -adic integers
- 3 p -adic codes
- 4 Quadratic residue codes
 - QR codes over fields
 - QR codes over \mathbb{Z}_{p^e}
 - p -adic QR codes
- 5 Weight enumerators
- 6 Examples
- 7 References

Terminology

- Let m be a positive integer. A \mathbb{Z}_m -submodule of \mathbb{Z}_m^n is called a **(modular) code** over \mathbb{Z}_m of length n .
- (**Hamming weight**) For $\mathbf{x} = x_1 x_2 \cdots x_n$, $wt_H(\mathbf{x})$ is the number of nonzero components.
- $d(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x} - \mathbf{y})$ and d_C is minimum of $d(\mathbf{x})$ for $0 \neq \mathbf{x} \in C$.
- For $\mathbf{x}, \mathbf{y} \in C$, the **inner product** is defined by $\mathbf{x} \cdot \mathbf{y} = \sum x_i y_i$.
- $C^\perp = \{\mathbf{x} \in C \mid \mathbf{x} \cdot \mathbf{y} = 0 \ \forall \mathbf{y} \in C\}$. C is **self-dual** if $C = C^\perp$.

Terminology

- Let m be a positive integer. A \mathbb{Z}_m -submodule of \mathbb{Z}_m^n is called a **(modular) code** over \mathbb{Z}_m of length n .
- **(Hamming weight)** For $\mathbf{x} = x_1 x_2 \cdots x_n$, $wt_H(\mathbf{x})$ is the number of nonzero components.
- $d(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x} - \mathbf{y})$ and d_C is minimum of $d(\mathbf{x})$ for $0 \neq \mathbf{x} \in C$.
- For $\mathbf{x}, \mathbf{y} \in C$, the **inner product** is defined by $\mathbf{x} \cdot \mathbf{y} = \sum x_i y_i$.
- $C^\perp = \{\mathbf{x} \in C \mid \mathbf{x} \cdot \mathbf{y} = 0 \ \forall \mathbf{y} \in C\}$. C is **self-dual** if $C = C^\perp$.

Terminology

- Let m be a positive integer. A \mathbb{Z}_m -submodule of \mathbb{Z}_m^n is called a **(modular) code** over \mathbb{Z}_m of length n .
- (**Hamming weight**) For $\mathbf{x} = x_1 x_2 \cdots x_n$, $wt_H(\mathbf{x})$ is the number of nonzero components.
- $d(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x} - \mathbf{y})$ and d_C is minimum of $d(\mathbf{x})$ for $0 \neq \mathbf{x} \in C$.
- For $\mathbf{x}, \mathbf{y} \in C$, the **inner product** is defined by $\mathbf{x} \cdot \mathbf{y} = \sum x_i y_i$.
- $C^\perp = \{\mathbf{x} \in C \mid \mathbf{x} \cdot \mathbf{y} = 0 \ \forall \mathbf{y} \in C\}$. C is **self-dual** if $C = C^\perp$.

Terminology

- Let m be a positive integer. A \mathbb{Z}_m -submodule of \mathbb{Z}_m^n is called a **(modular) code** over \mathbb{Z}_m of length n .
- (**Hamming weight**) For $\mathbf{x} = x_1 x_2 \cdots x_n$, $wt_H(\mathbf{x})$ is the number of nonzero components.
- $d(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x} - \mathbf{y})$ and d_C is minimum of $d(\mathbf{x})$ for $0 \neq \mathbf{x} \in C$.
- For $\mathbf{x}, \mathbf{y} \in C$, the **inner product** is defined by $\mathbf{x} \cdot \mathbf{y} = \sum x_i y_i$.
- $C^\perp = \{\mathbf{x} \in C \mid \mathbf{x} \cdot \mathbf{y} = 0 \ \forall \mathbf{y} \in C\}$. C is **self-dual** if $C = C^\perp$.

Terminology

- Let m be a positive integer. A \mathbb{Z}_m -submodule of \mathbb{Z}_m^n is called a **(modular) code** over \mathbb{Z}_m of length n .
- (**Hamming weight**) For $\mathbf{x} = x_1 x_2 \cdots x_n$, $wt_H(\mathbf{x})$ is the number of nonzero components.
- $d(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x} - \mathbf{y})$ and d_C is minimum of $d(\mathbf{x})$ for $0 \neq \mathbf{x} \in C$.
- For $\mathbf{x}, \mathbf{y} \in C$, the **inner product** is defined by $\mathbf{x} \cdot \mathbf{y} = \sum x_i y_i$.
- $C^\perp = \{\mathbf{x} \in C \mid \mathbf{x} \cdot \mathbf{y} = 0 \ \forall \mathbf{y} \in C\}$. C is **self-dual** if $C = C^\perp$.

Basis for a code over \mathbb{Z}_{p^e}

Definition

- The vectors $\mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{Z}_{p^e}^n$ are said to be **modular independent** if $\sum a_i \mathbf{v}_i = \mathbf{0}$ implies that all a_i are nonunits, i.e., $p \mid a_i$ for all i .
- The codewords $\mathbf{v}_1, \dots, \mathbf{v}_k$ form a **basis** for C if they are modular independent and generate C .
- A $k \times n$ matrix G is a **generator matrix** of C of length n if its rows form a basis for C . A generator matrix for C^\perp is called a **parity check** matrix of C .

Basis for a code over \mathbb{Z}_{p^e}

Definition

- The vectors $\mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{Z}_{p^e}^n$ are said to be **modular independent** if $\sum a_i \mathbf{v}_i = \mathbf{0}$ implies that all a_i are nonunits, i.e., $p \mid a_i$ for all i .
- The codewords $\mathbf{v}_1, \dots, \mathbf{v}_k$ form a **basis** for C if they are modular independent and generate C .
- A $k \times n$ matrix G is a **generator matrix** of C of length n if its rows form a basis for C . A generator matrix for C^\perp is called a **parity check** matrix of C .

Basis for a code over \mathbb{Z}_{p^e}

Definition

- The vectors $\mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{Z}_{p^e}^n$ are said to be **modular independent** if $\sum a_i \mathbf{v}_i = \mathbf{0}$ implies that all a_i are nonunits, i.e., $p \mid a_i$ for all i .
- The codewords $\mathbf{v}_1, \dots, \mathbf{v}_k$ form a **basis** for C if they are modular independent and generate C .
- A $k \times n$ matrix G is a **generator matrix** of C of length n if its rows form a basis for C . A generator matrix for C^\perp is called a **parity check** matrix of C .

Let M be an $m \times n$ matrix over \mathbb{Z}_{p^e} . Then by performing operations of the type

(R1) Permutation of the rows,

(R2) Multiplication of a row by a unit of \mathbb{Z}_{p^e} ,

(R3) Addition of a scalar multiple of one row to another, and

(C1) Permutation of the columns,

M can be transformed to the **standard form**

$$\begin{bmatrix} I_{k_0} & A_{01} & A_{02} & A_{03} & \dots & A_{0,e-1} & A_{0e} \\ 0 & pI_{k_1} & pA_{12} & pA_{13} & \dots & pA_{1,e-1} & pA_{1e} \\ 0 & 0 & p^2I_{k_2} & p^2A_{23} & \dots & p^2A_{2,e-1} & p^2A_{2e} \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & p^{e-1}I_{k_{e-1}} & p^{e-1}A_{e-1,e} \\ 0 & 0 & 0 & 0 & \dots & 0 & 0I_{k_e} \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix} \quad (1)$$

where the columns are grouped into square blocks of sizes $k_0, k_1, \dots, k_{e-1}, k_e$ and the k_i are nonnegative integers adding to n .

Type of a code

A matrix in this standard form is said to be of **type**

$$(1)^{k_0}(p)^{k_1}(p^2)^{k_2} \cdots (p^{e-1})^{k_{e-1}} 0^{k_e}, \quad (2)$$

omitting terms with zero exponents, if any. Often the 0^{k_e} is left off the type, but we retain it since we use k_e later. Some uses the notation

$$\{k_0, k_1, \dots, k_{e-1}, k_e\} \quad \text{or} \quad (p^e)^{k_0}(p^{e-1})^{k_1} \cdots (1)^{k_{e-1}}$$

instead.

The type of a code is the type of the generator matrix of the code.

Let C be a code over \mathbb{Z}_{p^e} . Then

p -adic numbers

Definition

Fix a prime number p . For a nonzero $r \in \mathbb{Q}$, write

$$r = p^k \frac{a}{b}, \quad (a, p) = (b, p) = 1.$$

The p -adic absolute value is defined by

$$|r|_p = p^{-k}.$$

$|\cdot|_p$ defines a metric on \mathbb{Q} . By completing \mathbb{Q} with respect to this metric, we obtain a field of p -adic numbers

$$\mathbb{Q}_p = \left\{ \sum_{i=n_0}^{\infty} a_i p^i \mid 0 \leq a_i < p, n_0 \in \mathbb{Z} \right\} \supset \mathbb{Q}.$$

p -adic integers

Its subring

$$\mathbb{Z}_{p^\infty} = \left\{ \sum_{i=0}^{\infty} a_i p^i \mid 0 \leq a_i < p \right\} = \{ \alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1 \}$$

is called the ring of **p -adic integers**. It is a principal ideal domain. The standard notation for \mathbb{Z}_{p^∞} is \mathbb{Z}_p !

\mathbb{Z}_{p^∞} can be defined as the inverse limit of the system

$$\mathbb{Z}_p \leftarrow \mathbb{Z}_{p^2} \leftarrow \mathbb{Z}_{p^3} \leftarrow \cdots$$

where the maps $\mathbb{Z}_{p^{e+1}} \rightarrow \mathbb{Z}_{p^e}$ is $x \mapsto x \pmod{p^e}$. Thus two p -adic integers $\alpha = \beta$ iff $\alpha \equiv \beta \pmod{p^e}$ for all e .

Theorem (Ostrowski)

Every metric on \mathbb{Q} is equivalent to the metric induced by the usual absolute value $|\cdot| = |\cdot|_\infty$ or the p -adic absolute value $|\cdot|_p$ for some prime p .

Theorem (Product Formula)

For $r \in \mathbb{Q}$,

$$\prod_{p \leq \infty} |r|_p = 1.$$

Theorem (Hasse-Minkowski)

$r \in \mathbb{Q}$ is a square iff r is a square in \mathbb{Q}_p for all $p \leq \infty$.

Some surprises or fun

- 1 $1 + 2 + 2^2 + 2^3 + \cdots = \frac{1}{1-2} = -1$ in \mathbb{Q}_2 ($\because |2| = \frac{1}{2} < 1$).
- 2 (Freshmen's Dream) A series $\sum a_n$ converges iff $\lim a_n = 0$ in \mathbb{Q}_p .
- 3 We have the inequality

$$|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\} \text{ (non-archimedian)}$$

and any element in the sphere $S_\epsilon(\alpha) = \{x \in \mathbb{Q}_p \mid |x - \alpha|_p < \epsilon\}$ is a center.

- 4 $(2121342303 \cdots_{(5)})^2 = -1$ in \mathbb{Q}_5 . Indeed, -1 is a square in \mathbb{Q}_p iff $p \equiv 1 \pmod{4}$.

Some surprises or fun

- 1 $1 + 2 + 2^2 + 2^3 + \cdots = \frac{1}{1-2} = -1$ in \mathbb{Q}_2 ($\because |2| = \frac{1}{2} < 1$).
- 2 (Freshmen's Dream) A series $\sum a_n$ converges iff $\lim a_n = 0$ in \mathbb{Q}_p .
- 3 We have the inequality

$$|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\} \text{ (non-archimedean)}$$

and any element in the sphere $S_\epsilon(\alpha) = \{x \in \mathbb{Q}_p \mid |x - \alpha|_p < \epsilon\}$ is a center.

- 4 $(2121342303 \cdots_{(5)})^2 = -1$ in \mathbb{Q}_5 . Indeed, -1 is a square in \mathbb{Q}_p iff $p \equiv 1 \pmod{4}$.

Some surprises or fun

- 1 $1 + 2 + 2^2 + 2^3 + \cdots = \frac{1}{1-2} = -1$ in \mathbb{Q}_2 ($\because |2| = \frac{1}{2} < 1$).
- 2 (Freshmen's Dream) A series $\sum a_n$ converges iff $\lim a_n = 0$ in \mathbb{Q}_p .
- 3 We have the inequality

$$|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\} \text{ (non-archimedean)}$$

and any element in the sphere $S_\epsilon(\alpha) = \{x \in \mathbb{Q}_p \mid |x - \alpha|_p < \epsilon\}$ is a center.

- 4 $(2121342303 \cdots_{(5)})^2 = -1$ in \mathbb{Q}_5 . Indeed, -1 is a square in \mathbb{Q}_p iff $p \equiv 1 \pmod{4}$.

Some surprises or fun

- 1 $1 + 2 + 2^2 + 2^3 + \cdots = \frac{1}{1-2} = -1$ in \mathbb{Q}_2 ($\because |2| = \frac{1}{2} < 1$).
- 2 (Freshmen's Dream) A series $\sum a_n$ converges iff $\lim a_n = 0$ in \mathbb{Q}_p .
- 3 We have the inequality

$$|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\} \text{ (non-archimedean)}$$

and any element in the sphere $S_\epsilon(\alpha) = \{x \in \mathbb{Q}_p \mid |x - \alpha|_p < \epsilon\}$ is a center.

- 4 $(2121342303 \cdots_{(5)})^2 = -1$ in \mathbb{Q}_5 . Indeed, -1 is a square in \mathbb{Q}_p iff $p \equiv 1 \pmod{4}$.

Generator matrix of p -adic codes

Any code over \mathbb{Z}_{p^∞} has a generator matrix of the form:

$$\begin{pmatrix} p^{m_0} I_{k_0} & p^{m_0} A_{0,1} & p^{m_0} A_{0,2} & p^{m_0} A_{0,3} & \cdots & \cdots & p^{m_0} A_{0,r+1} \\ 0 & p^{m_1} I_{k_1} & p^{m_1} A_{1,2} & p^{m_1} A_{1,3} & \cdots & \cdots & p^{m_1} A_{1,r+1} \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & p^{m_r} I_{k_r} & p^{m_r} A_{r,r+1} \end{pmatrix}, \quad (3)$$

where I_{k_i} is the identity matrix of size k_i , giving its type as before.

Theorem

$\mathcal{C} = (\mathcal{C}^\perp)^\perp$ if and only if \mathcal{C} has type 1^k for some k . In particular, any self-dual code has type 1^k .

We will only consider p -adic codes \mathcal{C} of type 1^k .

Define a map $\Psi_e : \mathbb{Z}_{p^\infty} \rightarrow \mathbb{Z}_{p^e}$ by

$$\Psi_e\left(\sum_{i=0}^{\infty} a_i p^i\right) = \sum_{i=0}^{e-1} a_i p^i.$$

Definition

Let $1 \leq e_1 \leq e_2$ be integers. An $[n, k]$ code C_1 over $\mathbb{Z}_{p^{e_1}}$ **lifts** to an $[n, k]$ code C_2 over $\mathbb{Z}_{p^{e_2}}$, denoted by $C_1 \prec C_2$, if C_2 has a generator matrix G_2 such that $\Psi_{e_1}(G_2)$ is a generator matrix of C_1 .

By projecting \mathcal{C} to \mathbb{Z}_{p^e} , we get series of lifts of codes $\mathcal{C}^e = \Psi_e(\mathcal{C})$ of type 1^k over \mathbb{Z}_{p^e} .

Conversely, if C is an $[n, k]$ code over \mathbb{Z}_p , and $G = A_0$ is its generator matrix, then

$$G_e = A_0 + pA_1 + p^2A_2 \cdots + p^{e-1}A_{e-1}$$

define a series of generator matrices and a p -adic generator matrix G_∞ which defines a unique p -adic code \mathcal{C} such that the generator matrix of \mathcal{C}^e is G_e .

Therefore, a *p -adic code is the same as a series of lifts from a code over \mathbb{Z}_p .*

p -adic self-dual codes

- 1 Let $p \neq 2$. Self-dual codes exist over \mathbb{Z}_{p^∞} if and only if

$$\begin{cases} n \equiv 0 \pmod{4} & \text{if } p \equiv 3 \pmod{4} \\ n \equiv 0 \pmod{2} & \text{if } p \equiv 1 \pmod{4}. \end{cases}$$
 - 2 Self-dual codes exist over \mathbb{Z}_{2^∞} if and only if the length is a multiple of 8.
 - 3 A self-dual code over \mathbb{Z}_2 lifts to a self-dual code over \mathbb{Z}_{2^∞} if and only if every codeword has the weight divisible by 4.
 - 4 For $p \neq 2$, any self-dual code C over \mathbb{Z}_p lifts to a self-dual code over p -adic integers.
 - 5 MDS codes exist over the p -adics for all n and k with $k \leq n$ (MDS if $d = n - k + 1$ and type 1^k).
- ([DP] Codes over the p -adic integers)

p -adic self-dual codes

- 1 Let $p \neq 2$. Self-dual codes exist over \mathbb{Z}_{p^∞} if and only if

$$\begin{cases} n \equiv 0 \pmod{4} & \text{if } p \equiv 3 \pmod{4} \\ n \equiv 0 \pmod{2} & \text{if } p \equiv 1 \pmod{4}. \end{cases}$$
 - 2 Self-dual codes exist over \mathbb{Z}_{2^∞} if and only if the length is a multiple of 8.
 - 3 A self-dual code over \mathbb{Z}_2 lifts to a self-dual code over \mathbb{Z}_{2^∞} if and only if every codeword has the weight divisible by 4.
 - 4 For $p \neq 2$, any self-dual code C over \mathbb{Z}_p lifts to a self-dual code over p -adic integers.
 - 5 MDS codes exist over the p -adics for all n and k with $k \leq n$ (MDS if $d = n - k + 1$ and type 1^k).
- ([DP] Codes over the p -adic integers)

p -adic self-dual codes

- 1 Let $p \neq 2$. Self-dual codes exist over \mathbb{Z}_{p^∞} if and only if

$$\begin{cases} n \equiv 0 \pmod{4} & \text{if } p \equiv 3 \pmod{4} \\ n \equiv 0 \pmod{2} & \text{if } p \equiv 1 \pmod{4}. \end{cases}$$
- 2 Self-dual codes exist over \mathbb{Z}_{2^∞} if and only if the length is a multiple of 8.
- 3 A self-dual code over \mathbb{Z}_2 lifts to a self-dual code over \mathbb{Z}_{2^∞} if and only if every codeword has the weight divisible by 4.
- 4 For $p \neq 2$, any self-dual code C over \mathbb{Z}_p lifts to a self-dual code over p -adic integers.
- 5 MDS codes exist over the p -adics for all n and k with $k \leq n$ (MDS if $d = n - k + 1$ and type 1^k).

([DP] Codes over the p -adic integers)

p -adic self-dual codes

- 1 Let $p \neq 2$. Self-dual codes exist over \mathbb{Z}_{p^∞} if and only if

$$\begin{cases} n \equiv 0 \pmod{4} & \text{if } p \equiv 3 \pmod{4} \\ n \equiv 0 \pmod{2} & \text{if } p \equiv 1 \pmod{4}. \end{cases}$$
- 2 Self-dual codes exist over \mathbb{Z}_{2^∞} if and only if the length is a multiple of 8.
- 3 A self-dual code over \mathbb{Z}_2 lifts to a self-dual code over \mathbb{Z}_{2^∞} if and only if every codeword has the weight divisible by 4.
- 4 For $p \neq 2$, any self-dual code C over \mathbb{Z}_p lifts to a self-dual code over p -adic integers.
- 5 MDS codes exist over the p -adics for all n and k with $k \leq n$ (MDS if $d = n - k + 1$ and type 1^k).

([DP] Codes over the p -adic integers)

p -adic self-dual codes

- 1 Let $p \neq 2$. Self-dual codes exist over \mathbb{Z}_{p^∞} if and only if

$$\begin{cases} n \equiv 0 \pmod{4} & \text{if } p \equiv 3 \pmod{4} \\ n \equiv 0 \pmod{2} & \text{if } p \equiv 1 \pmod{4}. \end{cases}$$
 - 2 Self-dual codes exist over \mathbb{Z}_{2^∞} if and only if the length is a multiple of 8.
 - 3 A self-dual code over \mathbb{Z}_2 lifts to a self-dual code over \mathbb{Z}_{2^∞} if and only if every codeword has the weight divisible by 4.
 - 4 For $p \neq 2$, any self-dual code C over \mathbb{Z}_p lifts to a self-dual code over p -adic integers.
 - 5 MDS codes exist over the p -adics for all n and k with $k \leq n$ (MDS if $d = n - k + 1$ and type 1^k).
- ([DP] Codes over the p -adic integers)

Minimum distances

Let \mathcal{C} be a p -adic $[n, k]$ code \mathcal{C} of type 1^k , and G, H be a generator matrix and a parity-check matrix of \mathcal{C} , respectively. Let

$$\mathcal{C}^e = \Psi_e(\mathcal{C}), \quad G_e = \psi_e(G), \quad H_e = \Psi_e(H)$$

and $d = d(\mathcal{C}^1)$, d_∞ be the minimum distances of \mathcal{C}^1 and \mathcal{C} , respectively.

Note that we have well-defined maps

$$\begin{array}{ccc} \mathbb{Z}_{p^e}^n & \rightarrow & \mathbb{Z}_{p^{e+1}}^n, \\ \mathbf{v} & \mapsto & p\mathbf{v} \end{array} \quad \begin{array}{ccc} \mathbb{Z}_{p^{e+1}}^n & \rightarrow & \mathbb{Z}_{p^e}^n \\ p\mathbf{v} & \mapsto & \mathbf{v} \end{array}$$

Lemma

- 1 $p\mathcal{C}^e \subset \mathcal{C}^{e+1}$.
- 2 $\mathbf{v} = p\mathbf{v}_0 \in \mathcal{C}^e$ iff $\mathbf{v}_0 \in \mathcal{C}^{e-1}$.

Lemma

For a p -adic code \mathcal{C} ,

- 1 $d(\mathcal{C}^e)$ is equal to $d = d(\mathcal{C}^1)$ for all $e < \infty$.
- 2 d_∞ is at least d .

Quadratic residue codes over fields

Setting:

- 1 n a prime (length)
- 2 another prime p which is a quadratic residue modulo n (base)
- 3 α a primitive n^{th} root of 1 in some extension of \mathbb{Z}_p
- 4 Q quadratic residues mod n , N quadratic nonresidues mod n
- 5 $Q(x) = \prod_{i \in Q} (x - \alpha^i)$, $N(x) = \prod_{i \in N} (x - \alpha^i)$

Then

$$x^n - 1 = (x - 1)Q(x)N(x)$$

is a factorization in $\mathbb{Z}_p[x]$ ($\because p \in Q$).

Definition

Quadratic residue codes $\mathcal{Q} \supset \mathcal{Q}_1, \mathcal{N} \supset \mathcal{N}_1$ are cyclic codes of length n with generator polynomials (respectively)

$$Q(x), \quad (x - 1)Q(x), \quad N(x), \quad (x - 1)N(x).$$

Quadratic residue codes over fields

Setting:

- 1 n a prime (length)
- 2 another prime p which is a quadratic residue modulo n (base)
- 3 α a primitive n^{th} root of 1 in some extension of \mathbb{Z}_p
- 4 Q quadratic residues mod n , N quadratic nonresidues mod n
- 5 $Q(x) = \prod_{i \in Q} (x - \alpha^i)$, $N(x) = \prod_{i \in N} (x - \alpha^i)$

Then

$$x^n - 1 = (x - 1)Q(x)N(x)$$

is a factorization in $\mathbb{Z}_p[x]$ ($\because p \in Q$).

Definition

Quadratic residue codes $\mathcal{Q} \supset \mathcal{Q}_1, \mathcal{N} \supset \mathcal{N}_1$ are cyclic codes of length n with generator polynomials (respectively)

$$Q(x), \quad (x - 1)Q(x), \quad N(x), \quad (x - 1)N(x).$$

Quadratic residue codes over fields

Setting:

- 1 n a prime (length)
- 2 another prime p which is a quadratic residue modulo n (base)
- 3 α a primitive n^{th} root of 1 in some extension of \mathbb{Z}_p
- 4 Q quadratic residues mod n , N quadratic nonresidues mod n
- 5 $Q(x) = \prod_{i \in Q} (x - \alpha^i)$, $N(x) = \prod_{i \in N} (x - \alpha^i)$

Then

$$x^n - 1 = (x - 1)Q(x)N(x)$$

is a factorization in $\mathbb{Z}_p[x]$ ($\because p \in Q$).

Definition

Quadratic residue codes $\mathcal{Q} \supset \mathcal{Q}_1, \mathcal{N} \supset \mathcal{N}_1$ are cyclic codes of length n with generator polynomials (respectively)

$$Q(x), \quad (x - 1)Q(x), \quad N(x), \quad (x - 1)N(x).$$

Quadratic residue codes over fields

Setting:

- 1 n a prime (length)
- 2 another prime p which is a quadratic residue modulo n (base)
- 3 α a primitive n^{th} root of 1 in some extension of \mathbb{Z}_p
- 4 Q quadratic residues mod n , N quadratic nonresidues mod n
- 5 $Q(x) = \prod_{i \in Q} (x - \alpha^i)$, $N(x) = \prod_{i \in N} (x - \alpha^i)$

Then

$$x^n - 1 = (x - 1)Q(x)N(x)$$

is a factorization in $\mathbb{Z}_p[x]$ ($\because p \in Q$).

Definition

Quadratic residue codes $\mathcal{Q} \supset \mathcal{Q}_1, \mathcal{N} \supset \mathcal{N}_1$ are cyclic codes of length n with generator polynomials (respectively)

$$Q(x), \quad (x - 1)Q(x), \quad N(x), \quad (x - 1)N(x).$$

Quadratic residue codes over fields

Setting:

- 1 n a prime (length)
- 2 another prime p which is a quadratic residue modulo n (base)
- 3 α a primitive n^{th} root of 1 in some extension of \mathbb{Z}_p
- 4 Q quadratic residues mod n , N quadratic nonresidues mod n
- 5 $Q(x) = \prod_{i \in Q} (x - \alpha^i)$, $N(x) = \prod_{i \in N} (x - \alpha^i)$

Then

$$x^n - 1 = (x - 1)Q(x)N(x)$$

is a factorization in $\mathbb{Z}_p[x]$ ($\because p \in Q$).

Definition

Quadratic residue codes $\mathcal{Q} \supset \mathcal{Q}_1, \mathcal{N} \supset \mathcal{N}_1$ are cyclic codes of length n with generator polynomials (respectively)

$$Q(x), \quad (x - 1)Q(x), \quad N(x), \quad (x - 1)N(x).$$

Facts on QR codes

- 1 $\dim \mathcal{Q} = \dim \mathcal{N} = (n+1)/2$, $\dim \mathcal{Q}_1 = \dim \mathcal{N}_1 = (n-1)/2$,
- 2 minimum distance $d \geq \sqrt{n}$
- 3 If $p \equiv -1 \pmod{4}$, then $\mathcal{Q}^\perp = \mathcal{Q}_1$, $\mathcal{N}^\perp = \mathcal{N}_1$
- 4 If $p \equiv 1 \pmod{4}$, then $\mathcal{Q}^\perp = \mathcal{N}_1$, $\mathcal{N}^\perp = \mathcal{Q}_1$
- 5 Extended codes $\hat{\mathcal{Q}}, \hat{\mathcal{N}}$ are **self-dual** if $p \equiv -1 \pmod{4}$.
If $(a_0, \dots, a_{n-1}) \in \mathcal{Q}(\text{or } \mathcal{N})$, then the extended coordinate is $a_\infty = -y \sum_{i=0}^{n-1} a_i$, where $1 + y^2 n = 0$.
- 6 $\text{Aut } \hat{\mathcal{Q}}$ contains $PSL_2(n)$.
- 7 Hamming code of length 7, ternary Golay code of length 11, and binary Golay code of length 23 are QR codes.

Idempotent generators

Let

$$f_Q(x) = \sum_{i \in Q} x^i, \quad f_N(x) = \sum_{i \in N} x^i.$$

1 $p = 2$ and $n = 4k - 1$: Idempotents of \mathcal{Q} and \mathcal{N} are

$$f_Q, \quad f_N$$

2 $p > 2$ and $n = 4k - 1$: Idempotents of \mathcal{Q} and \mathcal{N} are

$$E_q(x) = \frac{n+1}{2n} + \frac{1+\theta}{2n} f_Q(x) + \frac{1-\theta}{2n} f_N(x)$$

$$E_n(x) = \frac{n+1}{2n} + \frac{1-\theta}{2n} f_Q(x) + \frac{1+\theta}{2n} f_N(x)$$

where $\theta^2 = -n$ (in \mathbb{Z}_p).

Quadratic residue codes over \mathbb{Z}_{p^e}

Setting:

- 1 n a prime (length)
- 2 another prime p which is a quadratic residue modulo n and $e \geq 1$
- 3 α a primitive n^{th} root of 1 in some extension of \mathbb{Z}_{p^e}
- 4 Q quadratic residues mod n , N quadratic nonresidues mod n
- 5 $Q_e(x) = \prod_{i \in Q} (x - \alpha^i)$, $N_e(x) = \prod_{i \in N} (x - \alpha^i)$

$\mathbb{Z}_{p^e}[\alpha]/\mathbb{Z}_{p^e}$ is a Galois ring extension with the automorphism group generated by the Frobenius map $\alpha \mapsto \alpha^p$. This implies that

$$x^n - 1 = (x - 1)Q_e(x)N_e(x)$$

is a factorization in $\mathbb{Z}_{p^e}[x]$ ($\because p \in Q$).

Definition

Quadratic residue codes $\mathcal{Q}^e \supset \mathcal{Q}_1^e, \mathcal{N}^e \supset \mathcal{N}_1^e$ are cyclic codes of length n with generator polynomials (respectively)

$$Q_e(x), \quad (x - 1)Q_e(x), \quad N_e(x), \quad (x - 1)N_e(x).$$

Hensel's Lemma version 1

Let $f(x) \in \mathbb{Z}_{p^\infty}[x]$ and suppose that

- 1 there exists $\beta_1 \in \mathbb{Z}_p$ such that $f(\beta_1) \equiv 0 \pmod{p}$
- 2 $f'(\beta_1) \not\equiv 0 \pmod{p}$.

Then there exists a unique p -adic integer β such that $f(\beta) = 0$

Example

$x^2 + x + 6 = 0$ has solutions

- 1 $x = 0, 1 \pmod{2}$,
- 2 $x = 0, 2 \pmod{3}$
- 3 $x = 4, 8 \pmod{13}$

Note that $f'(\beta) = 2\beta + 1 \not\equiv 0 \pmod{p}$ in every case. Thus $f(x)$ has two roots in \mathbb{Z}_{p^∞} for $p = 2, 3, 13$, respectively.

Hensel's Lemma for cyclic codes

Suppose that $f(x) \in \mathbb{Z}_{p^e}[x]$ (or $\mathbb{Z}_{p^\infty}[x]$) is monic and

$$f(x) \equiv g_1(x)g_2(x) \cdots g_k(x) \pmod{p}$$

is a factorization into pairwise relatively prime polynomials $g_i \in \mathbb{Z}_p[x]$. Then there exist unique pairwise relatively prime polynomials $g_i^e(x) \in \mathbb{Z}_{p^e}[x]$ such that

$$f = g_1^e(x)g_2^e(x) \cdots g_k^e(x)$$

with $g_i^e \equiv g_i \pmod{p}$. g_i^e are called **Hensel lifts** of g_i to \mathbb{Z}_{p^e} .

In practice we lift $g_i(x)$ to $g_i^2(x) \in \mathbb{Z}_{p^2}[x]$, then to $g_i^3(x) \in \mathbb{Z}_{p^3}[x]$, \dots , inductively to $g_i^e(x) \in \mathbb{Z}_{p^e}[x]$ such that

$$f = g_1^j(x)g_2^j(x) \cdots g_k^j(x) \pmod{p^j}$$

for all $j \leq e$.

An example for binary Hamming code of length 7:

$$1 \quad x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1) \text{ in } \mathbb{Z}_2[x]$$

$$2 \quad x^7 - 1 = (x - 1)(x^3 + 2x^2 + x - 1)(x^3 + 3x^2 + 2x - 1) \text{ in } \mathbb{Z}_4[x]$$

$$3 \quad x^7 - 1 = (x - 1)(x^3 + 6x^2 + 5x - 1)(x^3 + 3x^2 + 2x - 1) \text{ in } \mathbb{Z}_8[x]$$

$$\vdots$$

$$\infty \quad x^7 - 1 = (x - 1)(x^3 - \lambda x^2 - (\lambda + 1)x - 1)(x^3 + (\lambda + 1)x^2 + \lambda x - 1),$$

where $\lambda^2 + \lambda + 6 = 0$.

Idempotent generators

Let

$$f_Q(x) = \sum_{r \in Q} x^r, \quad f_N(x) = \sum_{n \in N} x^r.$$

1 $p = 2$ and $n = 4k - 1$: Idempotents of \mathcal{Q} and \mathcal{N} are

$$f_Q, \quad f_N$$

2 $p > 2$ and $n = 4k - 1$: Idempotents of \mathcal{Q} and \mathcal{N} are

$$E_q(x) = \frac{n+1}{2n} + \frac{1+\theta}{2n} f_Q(x) + \frac{1-\theta}{2n} f_N(x)$$

$$E_n(x) = \frac{n+1}{2n} + \frac{1-\theta}{2n} f_Q(x) + \frac{1+\theta}{2n} f_N(x)$$

where $\theta^2 = -n$ (in \mathbb{Z}_{p^e}).

p -adic QR codes

Setting.

- 1 $n = 4k - 1$ prime, $p \neq n$ prime, quadratic residue mod n
- 2 n^{th} root α of unity of 1 in some extension of \mathbb{Z}_{p^∞}
- 3 Q quadratic residues mod n , N quadratic nonresidues mod n
- 4 $Q_\infty(x) = \prod_{i \in Q} (x - \alpha^i)$, $N_\infty(x) = \prod_{i \in N} (x - \alpha^i)$

Then

$$x^n - 1 = (x - 1)Q_\infty(x)N_\infty(x)$$

is a factorization in $\mathbb{Z}_{p^\infty}[x]$.

Definition

The **p -adic quadratic residue codes** $\mathcal{Q}^\infty \supset \mathcal{Q}_1^\infty, \mathcal{N}^\infty \supset \mathcal{N}_1^\infty$ are cyclic codes of length n with generator polynomials (respectively)

$$Q_\infty(x), \quad (x - 1)Q_\infty(x), \quad N_\infty(x), \quad (x - 1)N_\infty(x).$$

First step to obtain $Q_\infty(x)$

Recall that $n = 4k - 1$.

Let

- 1 λ and μ be roots of $x^2 + x + k = 0$ in \mathbb{Z}_{p^∞} ($\lambda + \mu = -1$),
- 2 θ a root of $x^2 = -n$ in \mathbb{Z}_{p^∞} .

Then

$$\theta = \pm(\lambda - \mu)$$

and

$$\lambda = \frac{\theta - 1}{2}, \quad \mu = \frac{-\theta - 1}{2}$$

Thus $\{\lambda, \mu\}$ and $\{\theta\}$ determine each other.

Equation $\theta^2 = -n$

Suppose $n = 4k - 1$.

1 $p \neq 2$.

$$\left(\frac{-n}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{p}{n}\right) (-1)^{\frac{p-1}{2} \frac{n-1}{2}} = (-1)^{\frac{p-1}{2} \frac{n+1}{2}} = 1$$

Hensel's Lemma implies that there are two solutions for θ in \mathbb{Z}_{p^e} and in \mathbb{Z}_{p^∞} also.

2 $p = 2$.

1 $\left(\frac{2}{n}\right) = 1$ iff $n = 8r \pm 1$.

2 $\theta^2 = -n$ in \mathbb{Z}_{p^∞} iff $-n \equiv 1 \pmod{8}$.

For $n = 8r - 1$, there exists two solutions for θ in \mathbb{Z}_{p^∞} .

However $\theta^2 \equiv -n \pmod{2^e}$ has four solutions for $e \geq 3$.

$(\mathbb{Z}_{2^n}^* \simeq \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_2.)$

Newton's Identities

The **elementary symmetric polynomials** $s_0, s_1, s_2, \dots, s_t$ in $S[X_1, X_2, \dots, X_t]$ over a ring S are

$$s_i(X_1, X_2, \dots, X_t) = \sum_{i_1 < i_2 < \dots < i_t} X_{i_1} X_{i_2} \cdots X_{i_t}, \quad \text{for } i = 1, 2, \dots, t.$$

We define $s_0(X_1, X_2, \dots, X_t) = 1$.

For all $i \geq 1$, the **i -power symmetric polynomials** are defined by

$$p_i(X_1, X_2, \dots, X_t) = X_1^i + X_2^i + \cdots + X_t^i.$$

Theorem (Newton's identities)

For each $i \geq 1$,

$$p_i = p_{i-1}s_1 - p_{i-2}s_2 + \cdots + (-1)^i p_1 s_{i-1} + (-1)^{i+1} i s_i, \quad (4)$$

where $s_i = s_i(X_1, X_2, \dots, X_t)$ and $p_i = p_i(X_1, X_2, \dots, X_t)$.

Let $Q = \{q_1, q_2, \dots, q_t\}$ and

$$s_i(\alpha^Q) = s_i(\alpha^{q_1}, \alpha^{q_2}, \dots, \alpha^{q_t}), \quad p_i(\alpha^Q) = p_i(\alpha^{q_1}, \alpha^{q_2}, \dots, \alpha^{q_t}).$$

Theorem

$$p_i(\alpha^Q) = \begin{cases} \lambda, & i \in Q, \\ \mu = -\lambda - 1, & i \in N. \end{cases}$$

We have

$$Q_\infty(X) = \prod_{i \in Q} (X - \alpha^i) = \sum_{i=0}^{(n-1)/2} (-1)^i s_i(\alpha^Q) X^{t-i}.$$

Formula for $Q^\infty(x)$

Theorem

Let $t = (n - 1)/2$ and $Q_{p^\infty}(X) = a_0X^t + a_1X^{t-1} + \cdots + a_t$. Then

1 $a_0 = 1, a_1 = -\lambda.$

2 $a_i \in \mathbb{Z}_{p^\infty}$ can be determined inductively by the formula

$$a_i = -\frac{p_i a_0 + p_{i-1} a_1 + p_{i-2} a_2 + \cdots + p_1 a_{i-1}}{i},$$

where $p_i = p_i(\alpha^Q).$

3 each a_i has the form $a\lambda + b \in \mathbb{Z}[\lambda].$

An example

- 1 $n = 23 = 4k - 1$ with $k = 6$.
- 2 $Q = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$, so we may take $p = 2, 3, 13$.
- 3 λ is a root of $x^2 + x + 6 = 0$ in \mathbb{Z}_{p^e} . ($\lambda^2 = -\lambda - 6$)
- 4 $a_0 = 1, a_1 = -\lambda$, and with $p_i = \lambda$ for $i \in Q$

$$a_2 = -\frac{p_2 a_0 + p_1 a_1}{2} = -\frac{\lambda \cdot 1 + (\lambda)(-\lambda)}{2} = -\lambda - 3$$

$$a_3 = -\frac{p_3 a_0 + p_2 a_1 + p_1 a_2}{3} = -\frac{\lambda \cdot 1 + (\lambda)(-\lambda) + \lambda(-\lambda - 3)}{3} = -4$$

$$\vdots$$

The generator polynomial for Q^∞ is

$$\begin{aligned} Q_\infty(x) = & x^{11} - \lambda x^{10} - (\lambda + 3)x^9 - 4x^8 + (\lambda - 3)x^7 + (2\lambda - 1)x^6 \\ & + (2\lambda + 3)x^5 + (\lambda + 4)x^4 + 4x^3 - (\lambda - 2)x^2 - (\lambda + 1)x - 1 \end{aligned}$$

It is Universal!

$N_\infty(x)$ is obtained by replacing λ by μ in $Q_\infty(X)$.

Taking $Q_\infty(x)$, $N_\infty(x)$, $(x-1)Q_\infty(x)$, $(x-1)N_\infty(x)$ modulo p^e

1 with roots λ, μ of $x^2 + x + 6 \equiv 0 \pmod{p^e}$ for $p = 2, 3, 13$

2 for all $e \geq 1$

we obtain ALL QR codes for \mathbb{Z}_{p^e} for $p = 2, 3, 13$.

p -adic Idempotents ($n = 4k - 1$)

Idempotent generators of $\mathcal{Q}^\infty \supset \mathcal{Q}_1^\infty, \mathcal{N}^\infty \supset \mathcal{N}_1^\infty$ are given as follows:

$$E_q(x) = a + bf_Q(x) + cf_N(x),$$

$$F_n(x) = a' - cf_Q(x) - bf_N(x) = 1 - E_n(x),$$

$$E_n(x) = a + cf_Q(x) + bf_N(x),$$

$$F_q(x) = a' - bf_Q(x) - cf_N(x) = 1 - E_q(x),$$

respectively. Here

$$a = \frac{n+1}{2n}, \quad a' = 1 - a = \frac{n-1}{2n}$$

and

$$b = -\frac{\mu}{n} = \frac{1+\theta}{2n}, \quad c = -\frac{\lambda}{n} = \frac{1-\theta}{2n},$$

(Binary case with θ by Calderbank and Sloane)

- 1 Reducing these modulo p^e , we obtain the idempotent generators of QR codes over \mathbb{Z}_{p^e} . The actual explicit formula depends on the length n , producing many cases.
- 2 Formulas involving θ given by [CS] work for odd primes only.
- 3 Several authors defined QR codes over \mathbb{Z}_{p^e} by giving their idempotent generators.
 - 1 V.S. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over \mathbb{Z}_4* , IEEE Trans. Inform. Theory, **42** (1996), 1594–1600
 - 2 M.H. Chiu, S.S. Yau and Y. Yu, *\mathbb{Z}_8 -cyclic codes and quadratic residue codes*, Advances in Applied Math., **25** (2000), 12–33
 - 3 B. Taeri, *Quadratic residue codes over \mathbb{Z}_9* , J. Korean Math Soc., **46** (2009), 13–30
 - 4 S. J. Kim, *Generator polynomials of the p -adic quadratic residue codes*, Kangweon-Kyungki Math. J, **13** (2005), 103–112
 - 5 X. Tan, *A family of quadratic residue codes over \mathbb{Z}_{2^m}* , preprint, 2011

Idempotents for QR codes over \mathbb{Z}_9 B. Taeri, Quadratic residue codes over \mathbb{Z}_9 , J. Korean Math Soc. (2009)

Take $p = 3$, $e = 2$, and $n = 12r \pm 1$. ($n \in Q$ iff $n \equiv \pm 1 \pmod{12}$).

1 $n = 12r - 1$

1 $r = 3\ell, n \equiv 8 \pmod{9}$.

1 $\theta = \pm 1, (2n)^{-1} = 4, a = 0, a' = 1, b, c = 0, 8$.

2 idempotents : $8f_Q, 8f_N, 1 + f_Q, 1 + f_N$.

2 $r = 3\ell + 1, n \equiv 2 \pmod{9}$.

1 $\theta = \pm 4, (2n)^{-1} = 7, a = 3, a' = 7, b, c = 6, 8$.

2 idempotents : $3 + 8f_Q + 6f_N, 3 + 6f_Q + 8f_N, 7 + f_Q + 3f_N, 7 + 3f_Q + f_N$.

3 $r = 3\ell + 2, n \equiv 5 \pmod{9}$.

1 $\theta = \pm 2, (2n)^{-1} = 1, a = 6, a' = 4, b, c = 3, 8$.

2 idempotents : $6 + 3f_Q + 8f_N, 6 + 8f_Q + 3f_N, 4 + 6f_Q + f_N, 4 + f_Q + 6f_N$.

2 $n = 12r + 1$.

1 $r = 3\ell, n \equiv 1 \pmod{9}$.

idempotents : $1 + f_N, 1 + f_Q, 8f_Q, 8f_N$.

2 $r = 3\ell + 1, n \equiv 4 \pmod{9}$.

idempotents : $6 + 3f_Q + 8f_N, 6 + 8f_Q + 3f_N, 4 + 6f_Q + f_N, 4 + f_Q + 6f_N$.

3 $r = 3\ell + 2, n \equiv 7 \pmod{9}$.

idempotents : $7 + f_Q + 3f_N, 7 + 3f_Q + f_N, 3 + 8f_Q + 6f_N, 3 + 6f_Q, 8f_N$.

Idempotents for QR codes over \mathbb{Z}_8

Take $p = 2$, $e = 3$, and $n = 4k - 1 = 8r - 1$ ($n \in Q$ iff $n \equiv \pm 1 \pmod{8}$) so $n^{-1} \equiv -1 \pmod{8}$.

We need to solve $x^2 + x + 2r \equiv 0 \pmod{8}$ for λ and μ .

Recall $a \equiv (n+1)/(2n) \equiv -4r$, $b \equiv -\mu/n \equiv \mu$, $c \equiv -\lambda/n \equiv \lambda$.

1 $r \equiv 0 \pmod{4}$

1 $\lambda, \mu = 0, 7$, $a = 0$, $b = 7$, $c = 0$.

2 idempotents : $7f_Q, 7f_N, 1 + f_Q, 1 + f_N$

2 $r \equiv 1 \pmod{4}$

1 $\lambda, \mu = 2, 5$, $a = 4$, $b = 5$, $c = 2$.

2 idempotents :

$$4 + 2f_Q + 5f_N, 4 + 5f_Q + 2f_N, 5 + 6f_Q + 3f_N, 5 + 3f_Q + 6f_N$$

3 $r \equiv 2 \pmod{4}$

1 $\lambda, \mu = 3, 4$, $a = 0$, $b = 4$, $c = 3$.

2 idempotents : $3f_Q + 4f_N, 4f_Q + 3f_N, 1 + 5f_Q + 4f_N, 1 + 5f_Q + 4f_N$

4 $r \equiv 3 \pmod{4}$

1 $\lambda, \mu = 1, 6$, $a = 4$, $b = 6$, $c = 1$.

2 idempotents : $4 + f_Q + 6f_N, 4 + 6f_Q + f_N, 5 + f_Q + 6f_N, 5 + 6f_Q + f_N$

Extended QR codes

Let G_1 be the generator matrix for Q_1^∞ . Then the generator matrix of the extended QR code \hat{Q}^∞ is given by

$$\begin{pmatrix} G & 0 \\ \mathbf{1} & \gamma n \end{pmatrix}$$

where $\mathbf{1} = (1, 1, \dots, 1)$ of length n and $1 + \gamma^2 n = 0$ in \mathbb{Z}_{p^∞} .

Thus $c_0 c_1 \cdots c_{n-1} c_\infty \in \mathcal{Q}$ if and only if

$$1 \quad \gamma \sum_{j=0}^{n-1} c_j + c_\infty = 0$$

$$2 \quad \sum_{j=0}^{n-1} c_j \alpha^{ij} = 0 \text{ for all } i.$$

From this we obtain the following:

Theorem

For a prime $n = 4k - 1$ and another prime p which is a quadratic residue mod n , the extended QR code \hat{Q}^∞ is a self-dual MDS codes of length $n + 1$ with minimal distance $(n + 3)/2$ over \mathbb{Z}_{p^∞} .

MacWilliams identities

Let \mathcal{C} be a p -adic $[n, k]$ code and A_i^e be the number of codewords of weight i in \mathcal{C}^e . Then

$$W_{\mathcal{C}^e}(x, y) = \sum_{i=0}^n A_i^e x^{n-i} y^i$$

is called the **weight enumerator** of \mathcal{C}^e .

Theorem (MacWilliams Identity)

$$W_{\mathcal{C}^\perp}(x, y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x + (p^e - 1)y, x - y), \quad (\mathcal{C} = \mathcal{C}^e)$$

Theorem (Gleason's type theorem Rains + Sloane, *Self-dual codes*)

Suppose \mathcal{C} is a self-dual code over \mathbb{Z}_{p^e} of even length $n = 2k$. Then

$$W_{\mathcal{C}}(x, y) = \sum_{i=0}^k c_i (x^2 + (p^e - 1)y^2)^i (xy - y^2)^{k-i}.$$

Minimum weight vectors

Let \mathcal{C} be a p -adic code of type 1^k and H be its parity check matrix. Let $d = d(\mathcal{C}^1)$. For each subset $S \subset \{1, 2, \dots, n\}$ of d elements, let

$$H_S = (\mathbf{h}_i)_{i \in S}$$

be the matrix whose columns are the i -th columns of H for $i \in S$. H_S has the standard form

$$\begin{pmatrix} I_{d-1} & 0 \\ 0 & p^j \end{pmatrix}$$

for some $j = -\infty, 0, 1, \dots$. Here we let $p^{-\infty} = 0$.
Let

μ_j : the number of subsets S for which H_S has the type

$$1^{d-1}(p^j)^1$$

Theorem

$$A_d^e = \left(\mu_{-\infty} + \sum_{j \geq e} \mu_j \right) (p^e - 1) + \sum_{j=1}^{e-1} \mu_j (p^j - 1). \quad (5)$$

Corollary

If $A_d^f = A_d^{f+1}$, then $A_d^e = A_f^e$ for all $e \geq f$.

Theorem

$d_\infty > d$ if and only if $\mu_{-\infty} = 0$.

Larger weights

Theorem

For $d \leq j < d_\infty$, let

$$K_j = \{m \mid p^m \text{ appears in the type of } H_S, |S| = j\}$$

Let $N = 1 + \max_{j=d}^{d_\infty-1} K_j$. Then for every $d \leq j < d_\infty$,

$$A_j^e = A_j^N$$

for all $e \geq N$. Thus every codeword of weight j in \mathcal{C}^e is of the form $p^{e-N} \mathbf{v}_0$ for some codeword \mathbf{v}_0 of weight j in \mathcal{C}^N .

Theorem

Suppose that $A_i^{f+1} = A_i^f$ for all $i \leq j$. Then $A_j^e = A_j^f$ for all $e \geq f$.

	...	i	...	j
\vdots				
$e = f$	A	B	C	D
$e = f + 1$	A	B	C	D
\vdots	A	B	C	D

QR codes

Theorem

Let $\mathcal{C} = \hat{\mathcal{Q}}^\infty$ be the self-dual extended p -adic QR code of length $n+1$, rank $(n+1)/2$, and minimum distance $d_\infty = (n+3)/2$. Then the weight enumerator $W^e(x, y)$ of \mathcal{C}^e is completely determined by $A_d^e, \dots, A_{d_\infty-1}^e$ as follows:

$$\begin{aligned} W_{\mathcal{C}^e}(x, y) &= \sum_{i=0}^{n+1} A_i^e x^{n+1-i} y^i \\ &= \sum_{j=0}^{(n+1)/2} c_j (x^2 + (q-1)y^2)^j (xy - y^2)^{4-j}. \end{aligned}$$

Weight enumerators for quadratic residue codes over \mathbb{Z}_{p^e} can be determined after finite computation of A_j^e for $e = 1, \dots, N-1$ and $j = 0, \dots, (n+1)/2$.

Hamming code

- 1 $n = 7 = 4k - 1$ with $k = 2$, and $p = 2$.
- 2 roots λ (and μ) of $x^2 + x + 2 = 0$ in \mathbb{Z}_{2^∞} .
 $\lambda = \dots 1111001111110100101, \dots 110001110000001011010$.
- 3 $Q_\infty(x) = x^3 - \lambda x^2 - (\lambda + 1)x - 1$.
- 4 \hat{Q} is an $[8, 4, 5]$ -code and its projections \hat{Q}^e are $[8, 4, 4]$ -code.
 Generator matrix for \hat{Q}^∞ is

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

- 5 For example, $\lambda \pmod{4} = 1, 2$. Substitution of λ gives a generator matrix for \hat{Q}^1, \hat{Q}^2 .

Hamming code

- 1 $n = 7 = 4k - 1$ with $k = 2$, and $p = 2$.
- 2 roots λ (and μ) of $x^2 + x + 2 = 0$ in \mathbb{Z}_{2^∞} .
 $\lambda = \dots 1111001111110100101, \dots 11000110000001011010$.
- 3 $Q_\infty(x) = x^3 - \lambda x^2 - (\lambda + 1)x - 1$.
- 4 \hat{Q} is an $[8, 4, 5]$ -code and its projections \hat{Q}^e are $[8, 4, 4]$ -code.
 Generator matrix for \hat{Q}^∞ is

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

- 5 For example, $\lambda \pmod{4} = 1, 2$. Substitution of λ gives a generator matrix for \hat{Q}^1, \hat{Q}^2 .

Hamming code

- 1 $n = 7 = 4k - 1$ with $k = 2$, and $p = 2$.
- 2 roots λ (and μ) of $x^2 + x + 2 = 0$ in \mathbb{Z}_{2^∞} .
 $\lambda = \dots 111001111110100101, \dots 11000110000001011010$.
- 3 $Q_\infty(x) = x^3 - \lambda x^2 - (\lambda + 1)x - 1$.
- 4 \hat{Q} is an $[8, 4, 5]$ -code and its projections \hat{Q}^e are $[8, 4, 4]$ -code.
 Generator matrix for \hat{Q}^∞ is

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

- 5 For example, $\lambda \pmod{4} = 1, 2$. Substitution of λ gives a generator matrix for \hat{Q}^1, \hat{Q}^2 .

Hamming code

- 1 $n = 7 = 4k - 1$ with $k = 2$, and $p = 2$.
- 2 roots λ (and μ) of $x^2 + x + 2 = 0$ in \mathbb{Z}_{2^∞} .
 $\lambda = \dots 1111001111110100101, \dots 11000110000001011010$.
- 3 $Q_\infty(x) = x^3 - \lambda x^2 - (\lambda + 1)x - 1$.
- 4 \hat{Q} is an $[8, 4, 5]$ -code and its projections \hat{Q}^e are $[8, 4, 4]$ -code.
 Generator matrix for \hat{Q}^∞ is

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

- 5 For example, $\lambda \pmod{4} = 1, 2$. Substitution of λ gives a generator matrix for \hat{Q}^1, \hat{Q}^2 .

Hamming code

- 1 $n = 7 = 4k - 1$ with $k = 2$, and $p = 2$.
- 2 roots λ (and μ) of $x^2 + x + 2 = 0$ in \mathbb{Z}_{2^∞} .
 $\lambda = \dots 1111001111110100101, \dots 11000110000001011010$.
- 3 $Q_\infty(x) = x^3 - \lambda x^2 - (\lambda + 1)x - 1$.
- 4 \hat{Q} is an $[8, 4, 5]$ -code and its projections \hat{Q}^e are $[8, 4, 4]$ -code.
 Generator matrix for \hat{Q}^∞ is

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

- 5 For example, $\lambda \pmod{4} = 1, 2$. Substitution of λ gives a generator matrix for \hat{Q}^1, \hat{Q}^2 .

Weight enumerators

- 1 $d_\infty = 5$, so we need A_i^e for $i = 0, \dots, 4$.

weight	0	4
$e = 1$	1	14
$e = 2$	1	14

- 2 Using the Gleason type theorem

$$W_C(x, y) = \sum_{i=0}^4 c_i (x^2 + (q-1)y^2)^i (xy - y^2)^{k-i} \quad (q = p^e),$$

we obtain

$$A_5^e = 56(-2 + q),$$

$$A_6^e = 28(8 - 6q + q^2),$$

$$A_7^e = 8(-22 + 21q - 7q^2 + q^3),$$

$$A_8^e = 49 - 56q + 28q^2 - 8q^3 + q^4.$$

3-adic Golay code

- 1 $n = 11 = 4k - 1$ with $k = 3$, and $p = 3$.
- 2 λ is a root of $x^2 + x + 3 = 0$ in \mathbb{Z}_{3^∞} .
- 3 $Q_\infty(x) = x^5 - \lambda x^4 - x^3 + x^2 - (\lambda + 1)x - 1$.
- 4 \hat{Q}^∞ is an $[12, 6, 7]$ -code and its projections \hat{Q}^e are $[12, 6, 6]$ -code.

weight	0	6
--------	---	---

- 5

$e = 1$	1	264
$e = 2$	1	264

- 6 By MacWilliams identities or Gleason type theorem, ($q = 3^e$)

$$A_7^e = 792(-3 + q),$$

$$A_8^e = 495(15 - 8q + q^2),$$

$$A_9^e = 220(-52 + 36q - 9q^2 + q^3),$$

$$A_{10}^e = 66(144 - 120q + 45q^2 - 10q^3 + q^4),$$

$$A_{11}^e = 12(-342 + 330q - 165q^2 + 55q^3 - 11q^4 + q^5),$$

$$A_{12}^e = 726 - 792q + 495q^2 - 220q^3 + 66q^4 - 12q^5 + q^6.$$

3-adic Golay code

- 1 $n = 11 = 4k - 1$ with $k = 3$, and $p = 3$.
- 2 λ is a root of $x^2 + x + 3 = 0$ in \mathbb{Z}_{3^∞} .
- 3 $Q_\infty(x) = x^5 - \lambda x^4 - x^3 + x^2 - (\lambda + 1)x - 1$.
- 4 \hat{Q}^∞ is an $[12, 6, 7]$ -code and its projections \hat{Q}^e are $[12, 6, 6]$ -code.

weight	0	6
--------	---	---

5	$e = 1$	1	264
	$e = 2$	1	264

- 6 By MacWilliams identities or Gleason type theorem, ($q = 3^e$)

$$A_7^e = 792(-3 + q),$$

$$A_8^e = 495(15 - 8q + q^2),$$

$$A_9^e = 220(-52 + 36q - 9q^2 + q^3),$$

$$A_{10}^e = 66(144 - 120q + 45q^2 - 10q^3 + q^4),$$

$$A_{11}^e = 12(-342 + 330q - 165q^2 + 55q^3 - 11q^4 + q^5),$$

$$A_{12}^e = 726 - 792q + 495q^2 - 220q^3 + 66q^4 - 12q^5 + q^6.$$

3-adic Golay code

- 1 $n = 11 = 4k - 1$ with $k = 3$, and $p = 3$.
- 2 λ is a root of $x^2 + x + 3 = 0$ in \mathbb{Z}_{3^∞} .
- 3 $Q_\infty(x) = x^5 - \lambda x^4 - x^3 + x^2 - (\lambda + 1)x - 1$.
- 4 \hat{Q}^∞ is an $[12, 6, 7]$ -code and its projections \hat{Q}^e are $[12, 6, 6]$ -code.

weight	0	6
--------	---	---

5	$e = 1$	1	264
	$e = 2$	1	264

- 6 By MacWilliams identities or Gleason type theorem, ($q = 3^e$)

$$A_7^e = 792(-3 + q),$$

$$A_8^e = 495(15 - 8q + q^2),$$

$$A_9^e = 220(-52 + 36q - 9q^2 + q^3),$$

$$A_{10}^e = 66(144 - 120q + 45q^2 - 10q^3 + q^4),$$

$$A_{11}^e = 12(-342 + 330q - 165q^2 + 55q^3 - 11q^4 + q^5),$$

$$A_{12}^e = 726 - 792q + 495q^2 - 220q^3 + 66q^4 - 12q^5 + q^6.$$

3-adic Golay code

- 1 $n = 11 = 4k - 1$ with $k = 3$, and $p = 3$.
- 2 λ is a root of $x^2 + x + 3 = 0$ in \mathbb{Z}_{3^∞} .
- 3 $Q_\infty(x) = x^5 - \lambda x^4 - x^3 + x^2 - (\lambda + 1)x - 1$.
- 4 \hat{Q}^∞ is an $[12, 6, 7]$ -code and its projections \hat{Q}^e are $[12, 6, 6]$ -code.

weight	0	6
--------	---	---

5	$e = 1$	1	264
	$e = 2$	1	264

- 6 By MacWilliams identities or Gleason type theorem, ($q = 3^e$)

$$A_7^e = 792(-3 + q),$$

$$A_8^e = 495(15 - 8q + q^2),$$

$$A_9^e = 220(-52 + 36q - 9q^2 + q^3),$$

$$A_{10}^e = 66(144 - 120q + 45q^2 - 10q^3 + q^4),$$

$$A_{11}^e = 12(-342 + 330q - 165q^2 + 55q^3 - 11q^4 + q^5),$$

$$A_{12}^e = 726 - 792q + 495q^2 - 220q^3 + 66q^4 - 12q^5 + q^6.$$

3-adic Golay code

- 1 $n = 11 = 4k - 1$ with $k = 3$, and $p = 3$.
- 2 λ is a root of $x^2 + x + 3 = 0$ in \mathbb{Z}_{3^∞} .
- 3 $Q_\infty(x) = x^5 - \lambda x^4 - x^3 + x^2 - (\lambda + 1)x - 1$.
- 4 \hat{Q}^∞ is an $[12, 6, 7]$ -code and its projections \hat{Q}^e are $[12, 6, 6]$ -code.

weight	0	6
--------	---	---

- 5

$e = 1$	1	264
$e = 2$	1	264

- 6 By MacWilliams identities or Gleason type theorem, ($q = 3^e$)

$$A_7^e = 792(-3 + q),$$

$$A_8^e = 495(15 - 8q + q^2),$$

$$A_9^e = 220(-52 + 36q - 9q^2 + q^3),$$

$$A_{10}^e = 66(144 - 120q + 45q^2 - 10q^3 + q^4),$$

$$A_{11}^e = 12(-342 + 330q - 165q^2 + 55q^3 - 11q^4 + q^5),$$

$$A_{12}^e = 726 - 792q + 495q^2 - 220q^3 + 66q^4 - 12q^5 + q^6.$$

3-adic Golay code

- 1 $n = 11 = 4k - 1$ with $k = 3$, and $p = 3$.
- 2 λ is a root of $x^2 + x + 3 = 0$ in \mathbb{Z}_{3^∞} .
- 3 $Q_\infty(x) = x^5 - \lambda x^4 - x^3 + x^2 - (\lambda + 1)x - 1$.
- 4 \hat{Q}^∞ is an $[12, 6, 7]$ -code and its projections \hat{Q}^e are $[12, 6, 6]$ -code.

weight	0	6
--------	---	---

- 5

$e = 1$	1	264
$e = 2$	1	264

- 6 By MacWilliams identities or Gleason type theorem, ($q = 3^e$)

$$A_7^e = 792(-3 + q),$$

$$A_8^e = 495(15 - 8q + q^2),$$

$$A_9^e = 220(-52 + 36q - 9q^2 + q^3),$$

$$A_{10}^e = 66(144 - 120q + 45q^2 - 10q^3 + q^4),$$

$$A_{11}^e = 12(-342 + 330q - 165q^2 + 55q^3 - 11q^4 + q^5),$$

$$A_{12}^e = 726 - 792q + 495q^2 - 220q^3 + 66q^4 - 12q^5 + q^6.$$

Another lift of ternary Golay code

There exists a very simple 3-adic self-dual lift \mathcal{P} of the ternary Golay code defined by the generator matrix

$$G = \left(I_6 \mid \begin{array}{cccccc} 0 & b & b & b & b & b \\ b & 0 & b & -b & -b & b \\ b & b & 0 & b & -b & -b \\ b & -b & b & 0 & b & -b \\ b & -b & -b & b & 0 & b \\ b & b & -b & -b & b & 0 \end{array} \right) \quad (6)$$

where b is a 3-adic number satisfying $5b^2 + 1 = 0$ with $\Psi_1(b) = 2$. \mathcal{P} has minimum distance 6. One can check that

$$\mu_{-\infty} = 72, \quad \mu_1 = 60, \quad \mu_j = 0 \text{ for all } j \geq 2$$

By a theorem

$$A_6^e = 72(q-1) + 60(3-1) = 24(2+3q).$$

As before, we then get the weight enumerators of \mathcal{P}^e as follows, with $q = 3^e$.

$$A_6^e = 24(2 + 3q),$$

$$A_7^e = 360(-3 + q),$$

$$A_8^e = 45(93 - 64q + 11q^2),$$

$$A_9^e = 20(-356 + 324q - 99q^2 + 11q^3),$$

$$A_{10}^e = 6(1044 - 1140q + 495q^2 - 110q^3 + 11q^4),$$

$$A_{11}^e = 12(-234 + 294q - 165q^2 + 55q^3 - 11q^4 + q^5),$$

$$A_{12}^e = 510 - 720q + 495q^2 - 220q^3 + 66q^4 - 12q^5 + q^6.$$

2-adic Golay code of length 24

- 1 $n = 23 = 4k - 1$ with $k = 6$, and $p = 2$.
- 2 λ is a root of $x^2 + x + 6 = 0$ in \mathbb{Z}_{2^∞} .
- 3 $Q_\infty(x) = x^{11} - \lambda x^{10} + (-\lambda - 3)x^9 - 4x^8 + (\lambda - 3)x^7 + (2\lambda - 1)x^6 + (2\lambda + 3)x^5 + (\lambda + 4)x^4 + 4x^3 - (\lambda - 2)x^2 - (\lambda + 1)x - 1$
- 4 \hat{Q} is a $[24, 12, 13]$ -code and its projections \hat{Q}^e are $[24, 12, 8]$ -code.

weight	0	8	9	10	11	12
$e = 1$	1	759	0	0	0	2576
$e = 2$	1	759	0	121444	0	172592
$e = 3$				121444	48576	658352
$e = 4$					48576	1629872
$e = 5$						2504240
$e = 6$						3281456
$e = 7$						3281456

5

2-adic Golay code of length 24

- 1 $n = 23 = 4k - 1$ with $k = 6$, and $p = 2$.
- 2 λ is a root of $x^2 + x + 6 = 0$ in \mathbb{Z}_{2^∞} .
- 3 $Q_\infty(x) = x^{11} - \lambda x^{10} + (-\lambda - 3)x^9 - 4x^8 + (\lambda - 3)x^7 + (2\lambda - 1)x^6 + (2\lambda + 3)x^5 + (\lambda + 4)x^4 + 4x^3 - (\lambda - 2)x^2 - (\lambda + 1)x - 1$
- 4 \hat{Q} is a $[24, 12, 13]$ -code and its projections \hat{Q}^e are $[24, 12, 8]$ -code.

weight	0	8	9	10	11	12
$e = 1$	1	759	0	0	0	2576
$e = 2$	1	759	0	121444	0	172592
$e = 3$				121444	48576	658352
$e = 4$					48576	1629872
$e = 5$						2504240
$e = 6$						3281456
$e = 7$						3281456

2-adic Golay code of length 24

- 1 $n = 23 = 4k - 1$ with $k = 6$, and $p = 2$.
- 2 λ is a root of $x^2 + x + 6 = 0$ in \mathbb{Z}_{2^∞} .
- 3 $Q_\infty(x) = x^{11} - \lambda x^{10} + (-\lambda - 3)x^9 - 4x^8 + (\lambda - 3)x^7 + (2\lambda - 1)x^6 + (2\lambda + 3)x^5 + (\lambda + 4)x^4 + 4x^3 - (\lambda - 2)x^2 - (\lambda + 1)x - 1$
- 4 \hat{Q} is a $[24, 12, 13]$ -code and its projections \hat{Q}^e are $[24, 12, 8]$ -code.

weight	0	8	9	10	11	12
$e = 1$	1	759	0	0	0	2576
$e = 2$	1	759	0	121444	0	172592
$e = 3$				121444	48576	658352
$e = 4$					48576	1629872
$e = 5$						2504240
$e = 6$						3281456
$e = 7$						3281456

2-adic Golay code of length 24

- 1 $n = 23 = 4k - 1$ with $k = 6$, and $p = 2$.
- 2 λ is a root of $x^2 + x + 6 = 0$ in \mathbb{Z}_{2^∞} .
- 3 $Q_\infty(x) = x^{11} - \lambda x^{10} + (-\lambda - 3)x^9 - 4x^8 + (\lambda - 3)x^7 + (2\lambda - 1)x^6 + (2\lambda + 3)x^5 + (\lambda + 4)x^4 + 4x^3 - (\lambda - 2)x^2 - (\lambda + 1)x - 1$
- 4 \hat{Q} is a $[24, 12, 13]$ -code and its projections \hat{Q}^e are $[24, 12, 8]$ -code.

weight	0	8	9	10	11	12
$e = 1$	1	759	0	0	0	2576
$e = 2$	1	759	0	121444	0	172592
$e = 3$				121444	48576	658352
$e = 4$					48576	1629872
$e = 5$						2504240
$e = 6$						3281456
$e = 7$						3281456

5

2-adic Golay code of length 24

- 1 $n = 23 = 4k - 1$ with $k = 6$, and $p = 2$.
- 2 λ is a root of $x^2 + x + 6 = 0$ in \mathbb{Z}_{2^∞} .
- 3 $Q_\infty(x) = x^{11} - \lambda x^{10} + (-\lambda - 3)x^9 - 4x^8 + (\lambda - 3)x^7 + (2\lambda - 1)x^6 + (2\lambda + 3)x^5 + (\lambda + 4)x^4 + 4x^3 - (\lambda - 2)x^2 - (\lambda + 1)x - 1$
- 4 \hat{Q} is a $[24, 12, 13]$ -code and its projections \hat{Q}^e are $[24, 12, 8]$ -code.

weight	0	8	9	10	11	12
$e = 1$	1	759	0	0	0	2576
$e = 2$	1	759	0	121444	0	172592
$e = 3$				121444	48576	658352
$e = 4$					48576	1629872
$e = 5$						2504240
$e = 6$						3281456
$e = 7$						3281456

5

$W^e(x, y)$ for binary Golay code of length 24

For $e \geq 6$ with $q = 2^e$,

$$1 \quad A_{13}^e = 4416(-12092 + 711q)$$

$$2 \quad A_{14}^e = 12144(27727 - 2844q + 170q^2)$$

$$3 \quad A_{15}^e = 8096(-150842 + 21330q - 2550q^2 + 163q^3)$$

$$4 \quad A_{16}^e = 759(3841377 - 682560q + 122400q^2 - 15648q^3 + 970q^4)$$

$$5 \quad A_{17}^e = 6072(-803456 + 170640q - 40800q^2 + 7824q^3 - 970q^4 + 57q^5)$$

$$6 \quad A_{18}^e = 1012(5826836 - 1433376q + 428400q^2 - 109536q^3 + 20370q^4 - 2394q^5 + 133q^6)$$

$$7 \quad A_{19}^e = 6072(-856808 + 238896q - 85680q^2 + 27384q^3 - 6790q^4 + 1197q^5 - 133q^6 + 7q^7)$$

$$8 \quad A_{20}^e = 1518(2194384 - 682560q + 285600q^2 - 109536q^3 + 33950q^4 - 7980q^5 + 1330q^6 - 140q^7 + 7q^8)$$

$$9 \quad A_{21}^e = 2024(-746656 + 255960q - 122400q^2 + 54768q^3 - 20370q^4 + 5985q^5 - 1330q^6 + 210q^7 - 21q^8 + q^9)$$

$$10 \quad A_{22}^e = 276(1672076 - 625680q + 336600q^2 - 172128q^3 + 74690q^4 - 26334q^5 + 7315q^6 - 1540q^7 + 231q^8 - 22q^9 + q^{10})$$

$$11 \quad A_{23}^e = 24(-3550856 + 1439064q - 860200q^2 + 494868q^3 - 245410q^4 + 100947q^5 - 33649q^6 + 8855q^7 - 1771q^8 + 253q^9 - 23q^{10} + q^{11})$$

$$12 \quad A_{24}^e = 7199713 - 3139776q + 2064480q^2 - 1319648q^3 + 736230q^4 - 346104q^5 + 134596q^6 - 42504q^7 + 10626q^8 - 2024q^9 + 276q^{10} - 24q^{11} + q^{12}$$

Ternary QR code of length 24

- 1 $n = 23 = 4k - 1$ with $k = 6$, and $p = 3$.
- 2 \hat{Q} is a $[24, 12, 13]$ -code and its projections \hat{Q}^e are $[24, 12, 9]$ -code.

weight	0	9	10	11	12
$e = 1$	1	4048	0	0	61824
$e = 2$	1	4048	0	72864	717600
$e = 3$				72864	658352
$e = 4$					1956288
$e = 5$					2721360
$e = 6$					2721360

Ternary QR code of length 24

- 1 $n = 23 = 4k - 1$ with $k = 6$, and $p = 3$.
- 2 \hat{Q} is a $[24, 12, 13]$ -code and its projections \hat{Q}^e are $[24, 12, 9]$ -code.

weight	0	9	10	11	12
$e = 1$	1	4048	0	0	61824
$e = 2$	1	4048	0	72864	717600
$e = 3$				72864	658352
$e = 4$					1956288
$e = 5$					2721360
$e = 6$					2721360

Ternary QR code of length 24

- 1 $n = 23 = 4k - 1$ with $k = 6$, and $p = 3$.
- 2 \hat{Q} is a $[24, 12, 13]$ -code and its projections \hat{Q}^e are $[24, 12, 9]$ -code.

weight	0	9	10	11	12
$e = 1$	1	4048	0	0	61824
$e = 2$	1	4048	0	72864	717600
$e = 3$				72864	658352
$e = 4$					1956288
$e = 5$					2721360
$e = 6$					2721360

3

$W^e(x, y)$ for ternary QR code of length 24

For $e \geq 5$ with $q = 3^e$,

$$1 \quad A_{13}^e = 6624(-6999 + 452q)$$

$$2 \quad A_{14}^e = 18216(16217 - 1808q + 111q^2)$$

$$3 \quad A_{15}^e = 12144(-88651 + 13560q - 1665q^2 + 108q^3)$$

$$4 \quad A_{16}^e = 2277(1132101 - 216960q + 39960q^2 - 5184q^3 + 323q^4)$$

$$5 \quad A_{17}^e = 18216(-237270 + 54240q - 13320q^2 + 2592q^3 - 323q^4 + 19q^5)$$

$$6 \quad A_{18}^e = 1012(5170156 - 1366848q + 419580q^2 - 108864q^3 + 20349q^4 - 2394q^5 + 133q^6)$$

$$7 \quad A_{19}^e = 6072(-761184 + 227808q - 83916q^2 + 27216q^3 - 6783q^4 + 1197q^5 - 133q^6 + 7q^7)$$

$$8 \quad A_{20}^e = 1518(1951476 - 650880q + 279720q^2 - 108864q^3 + 33915q^4 - 7980q^5 + 1330q^6 - 140q^7 + 7q^8)$$

$$9 \quad A_{21}^e = 2024(-664584 + 244080q - 119880q^2 + 54432q^3 - 20349q^4 + 5985q^5 - 1330q^6 + 210q^7 - 21q^8 + q^9)$$

$$10 \quad A_{22}^e = 276(1489410 - 596640q + 329670q^2 - 171072q^3 + 74613q^4 - 26334q^5 + 7315q^6 - 1540q^7 + 231q^8 - 22q^9 + q^{10})$$

$$11 \quad A_{23}^e = 24(-3165054 + 1372272q - 842490q^2 + 491832q^3 - 245157q^4 + 100947q^5 - 33649q^6 + 8855q^7 - 1771q^8 + 253q^9 - 23q^{10} + q^{11})$$

$$12 \quad A_{24}^e = 6421278 - 2994048q + 2021976q^2 - 1311552q^3 + 735471q^4 - 346104q^5 + 134596q^6 - 42504q^7 + 10626q^8 - 2024q^9 + 276q^{10} - 24q^{11} + q^{12}$$

13-ary QR code of length 24

- 1 $n = 23 = 4k - 1$ with $k = 6$, and $p = 13$.
- 2 \hat{Q} is a $[24, 12, 13]$ -code and its projections \hat{Q}^e are $[24, 12, 10]$ -code.

weight	0	10	11	12
$e = 1$	1	36432	0	1032240
$e = 2$	1	36432	0	1032240

13-ary QR code of length 24

- 1 $n = 23 = 4k - 1$ with $k = 6$, and $p = 13$.
- 2 \hat{Q} is a $[24, 12, 13]$ -code and its projections \hat{Q}^e are $[24, 12, 10]$ -code.

3	weight	0	10	11	12
	$e = 1$	1	36432	0	1032240
	$e = 2$	1	36432	0	1032240

13-ary QR code of length 24

- 1 $n = 23 = 4k - 1$ with $k = 6$, and $p = 13$.
- 2 \hat{Q} is a $[24, 12, 13]$ -code and its projections \hat{Q}^e are $[24, 12, 10]$ -code.

3	weight	0	10	11	12
	$e = 1$	1	36432	0	1032240
	$e = 2$	1	36432	0	1032240

Weight Enumerator of 13-ary QR code







For all e with $q = 13^e$, $W_e(x, y)$ is given as follows:

$$\begin{aligned}
 & 1x^{24} + \\
 & 36432x^{14}y^{10} + \\
 & 1032240x^{12}y^{12} + \\
 & 1104(-25493 + 2723q)x^{11}y^{13} + \\
 & 6072(33437 - 5446q + 329q^2)x^{10}y^{14} + \\
 & 4048(-193601 + 40845q - 4935q^2 + 323q^3)x^9y^{15} + \\
 & 2277(851845 - 217840q + 39480q^2 - 5168q^3 + 323q^4)x^8y^{16} + \\
 & 18216(-182420 + 54460q - 13160q^2 + 2584q^3 - 323q^4 + 19q^5)x^7y^{17} + \\
 & 7084(576536 - 196056q + 59220q^2 - 15504q^3 + 2907q^4 - 342q^5 + 19q^6)x^6y^{18} + \\
 & 6072(-600924 + 228732q - 82908q^2 + 27132q^3 - 6783q^4 + 1197q^5 - 133q^6 + 7q^7)x^5y^{19} + \\
 & 1518(1554180 - 653520q + 276360q^2 - 108528q^3 + 33915q^4 - 7980q^5 + 1330q^6 - 140q^7 + 7q^8)x^4y^{20} + \\
 & 2024(-533010 + 245070q - 118440q^2 + 54264q^3 - 20349q^4 + 5985q^5 - 1330q^6 + 210q^7 - 21q^8 + q^9)x^3y^{21} + \\
 & 276(1201430 - 599060q + 325710q^2 - 170544q^3 + 74613q^4 - 26334q^5 + 7315q^6 - 1540q^7 + 231q^8 - 22q^9 + q^{10})x^2y^{22} + \\
 & 24(-2565398 + 1377838q - 832370q^2 + 490314q^3 - 245157q^4 + 100947q^5 - 33649q^6 + \\
 & \quad 8855q^7 - 1771q^8 + 253q^9 - 23q^{10} + q^{11})xy^{23} + \\
 & (5226014 - 3006192q + 1997688q^2 - 1307504q^3 + 735471q^4 - 346104q^5 + 134596q^6 - 42504q^7 + \\
 & \quad 10626q^8 - 2024q^9 + 276q^{10} - 24q^{11} + q^{12})y^{24}
 \end{aligned}$$







Thank you for listening!









References I

-  R. Blahut, *The Gleason-Prange theorem*, IEEE Trans. Inform. Theory, **37** (1991), 1269–1273 4p
-  A.R. Calderbank and N.J.A. Sloane, *Modular and p -adic and cyclic codes*, DCC, **6** (1995), 21–35
-  A.R. Calderbank, W.C. Winnie and B. Poonen, *A 2-adic approach to the analysis of cyclic codes*, IEEE Trans. Inform. Theory, **43** (1997), 977–986
-  M.H. Chiu, S.S. Yau and Y. Yu, *\mathbb{Z}_8 -cyclic codes and quadratic residue codes*, Advances in Applied Math., **25** (2000), 12–33
-  S.T. Dougherty, S.Y. Kim and Y.H. Park, *Lifted codes and their weight enumerators*, Discrete Math. **305** (2005), 123–135
-  S.T. Dougherty and Y.H. Park, *Codes over the p -adic integers*, Des. Codes. Cryptogr. **39** (2006), 65–80

References II

-  P. Galborit, C.S. Nedeloaia and A. Wassermann, *On the weight enumerators of duadic and quadratic residue codes*, IEEE Trans. Inform. Theory, **51** (2005), 402–407
-  M. Grassl, *On the minimum distance of some quadratic residue codes*, ISIT 2000, Sorrento, Italy, 253
-  S. Han, *On the weight enumerators of the projections of the 2-adic Golay codes of length 24*, 2012, submitted
-  W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge, 2003
-  S. J. Kim, *Generator polynomials of the p -adic quadratic residue codes*, Kangweon-Kyungki Math. J, **13** (2005), 103–112
-  C.D. Lee, Y.H. Chen and Y. Chang, *A unified method for determining the weight enumerators of binary extended quadratic residue codes*, IEEE Comm. Letters, **13** (2009), 139–141

References III

-  F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.
-  K. Nagata, F. Nemenzo and H. Wada, *Constructive algorithm of self-dual error-correcting codes*, Eleventh international workshop on algebraic and combinatorial coding theory, June 16-22, Bulgaria, 215–220, 2008
-  G. Nebe, E. Rains and N.J.A. Sloane, *Self-dual codes and invariant theory*, Springer-Verlag, 2006
-  Y.H. Park, *Modular independence and generator matrices for codes over \mathbb{Z}_m* , Des. Codes. Crypt **50** (2009), 147–162
-  V.S. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over \mathbb{Z}_4* , IEEE Trans. Inform. Theory, **42** (1996), 1594–1600
-  B. Taeri, *Quadratic residue codes over \mathbb{Z}_9* , J. Korean Math Soc., **46** (2009), 13–30

References IV



X. Tan, *A family of quadratic residue codes over \mathbb{Z}_{2^m}* , preprint, 2011