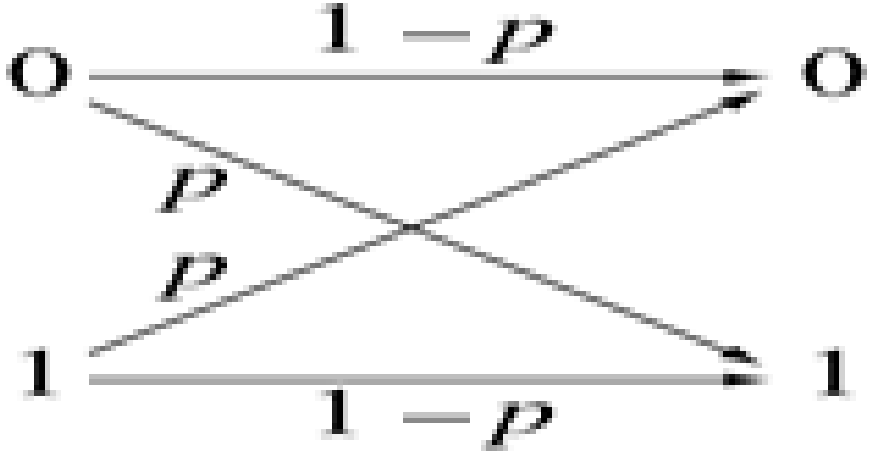
Error correcting codes III

Self-Dual codes

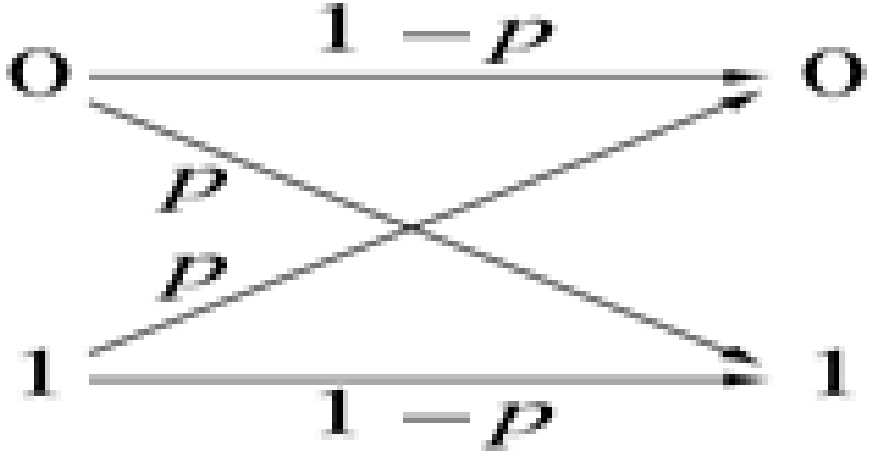
Högskolan i Skövde
Yohannes Tadesse

January 18, 2018

- Consider a binary symmetric channel

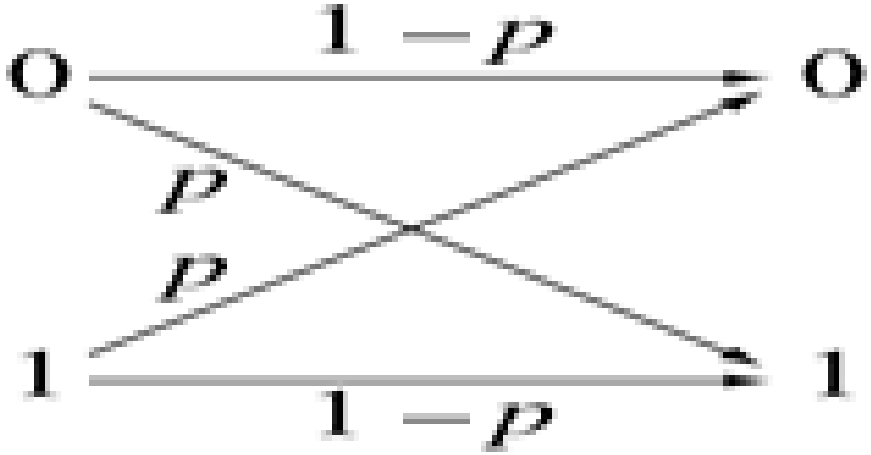


- Consider a binary symmetric channel



- Problem: We want to send as many message as possible quickly and safely.

- Consider a binary symmetric channel



- Problem: We want to send as many message as possible quickly and safely.
- Solution: Only send a certain sequences of 0's and 1's. This leads us to the definition of an **error correcting code**.

- $\mathbb{F}_q$ is a finite field where $q = p^m$ and p is a prime.

- $\mathbb{F}_q$ is a finite field where $q = p^m$ and p is a prime.
- A **(binary) block code** of length N is simply any subset $\mathcal{C}$ of $\mathbb{F}_q^N$ where $(q = 2^m)$ $q = p^m$. An element of the code is called a **codeword**.

- $\mathbb{F}_q$ is a finite field where $q = p^m$ and p is a prime.
- A **(binary) block code** of length N is simply any subset $\mathcal{C}$ of $\mathbb{F}_q^N$ where $(q = 2^m)$ $q = p^m$. An element of the code is called a **codeword**.
- A code is described by its parameters:
  - the size of $\mathcal{C} = |\mathcal{C}|$,
  - the length of the code N,
  - the rate of $\mathcal{C} = \frac{\log_q |\mathcal{C}|}{N}$ which measures by how much disparity is the code completed during transmission,
  - the minimum Hamming distance $d_{\min}$.

- $\mathbb{F}_q$ is a finite field where $q = p^m$ and p is a prime.
- A **(binary) block code** of length N is simply any subset $\mathcal{C}$ of $\mathbb{F}_q^N$ where $(q = 2^m)$ $q = p^m$. An element of the code is called a **codeword**.
- A code is described by its parameters:
  - the size of $\mathcal{C} = |\mathcal{C}|$,
  - the length of the code N,
  - the rate of $\mathcal{C} = \frac{\log_q |\mathcal{C}|}{N}$ which measures by how much disparity is the code completed during transmission,
  - the minimum Hamming distance d_{min}.

The code $\mathcal{C}$ can correct $\lfloor \frac{d-1}{2} \rfloor$ errors.

Some examples of Codes.

Example

- **Repetition codes** $\mathcal{C} = \{\overline{0}, \overline{1}\} \in \mathbb{F}_2^N$.
- **Single Parity Check (SPC)** code

$$\mathcal{C} = \{\overline{x} = (x_t)_{t=0}^{N-1} \in \mathbb{F}_2^N \mid \sum_{t=0}^{N-1} x_t \cong 0 \mod 2\}.$$

- A **linear code** of block length N over $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^N$.
- **Cyclic codes** A cyclic code $\mathcal{C}$ of length N over $\mathbb{F}_q$ is a collection of N-tuples

$$(c_t)_{t=0}^{N-1} \in \mathbb{F}_q^N.$$

suct that

$\mathcal{C}$ is linear subspace of $\mathbb{F}_q^N$.
$\mathcal{C}$ is closed under cyclic shift, i.e. if $(c_t) = (c_0, c_1, \ldots, c_{N-1}) \in \mathcal{C}$, then $(c_{t-\tau}) = (c_{N-\tau}, c_{N-\tau+1}, \ldots, c_{N-\tau-1}) \in \mathcal{C}$.

In order to define dual codes we need to equip $\mathbb{F}_q^N$ with an inner product, denoted by $\langle\ ,\ \rangle$. This inner product satisfies:

- bi-additivity (or additive on each coordinates)
  - $\langle x_1 + x_2, y\rangle = \langle x_1, y\rangle + \langle x_2, y\rangle$.
  - $\langle x, y_1 + y_2\rangle = \langle x, y_1\rangle + \langle x, y_2\rangle$.
- (conjugate) homogeneity $\langle \alpha x, y\rangle = \langle x, \overline{\alpha} y\rangle$.
- $\langle x, y\rangle = 0$ for all x, $\Rightarrow y = 0$.

In order to define dual codes we need to equip $\mathbb{F}_q^N$ with an inner product, denoted by $\langle\ ,\ \rangle$. This inner product satisfies:

- bi-additivity (or additive on each coordinates)
  - $\langle x_1 + x_2, y\rangle = \langle x_1, y\rangle + \langle x_2, y\rangle$.
  - $\langle x, y_1 + y_2\rangle = \langle x, y_1\rangle + \langle x, y_2\rangle$.
- (conjugate) homogeneity $\langle \alpha x, y\rangle = \langle x, \overline{\alpha} y\rangle$.
- $\langle x, y\rangle = 0$ for all x, $\Rightarrow y = 0$.

Definition

Given a linear code $\mathcal{C} \subset \mathbb{F}_q^N$, its dual is defined by

$$\mathcal{C}^{\perp} = \{x \in \mathbb{F}_q^N \mid \langle x, y\rangle = 0, \forall y \in \mathcal{C}\}.$$

A code $\mathcal{C}$ is called self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$.

In general, $|\mathcal{C}^{\perp}| = \frac{|\mathbb{F}_q|^N}{|\mathcal{C}|}$.

Some examples of self-dual codes

Example

The code $\mathcal{C} = \{00, 11\}$ is self-dual.

Some examples of self-dual codes

Example

The code $\mathcal{C} = \{00, 11\}$ is self-dual.
The code $\mathcal{C} = \{00000, 11111\}$ is not self-dual. Its dual is SPC code of length 5.

Some examples of self-dual codes

Example

The code $\mathcal{C} = \{00, 11\}$ is self-dual.
The code $\mathcal{C} = \{00000, 11111\}$ is not self-dual. Its dual is SPC code of length 5.

Example

The **Hamming code** H_8 of length 8 is a single error correcting code.

Construction of H_8:

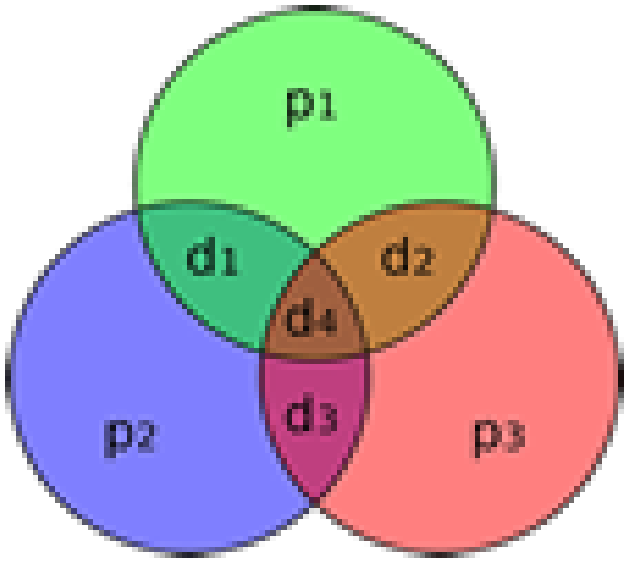
- We consider the quadratic residues modulo 7:

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 2, \quad 5^2 = 4, \quad 6^2 = 1.$$

- We construct a table with 0-6 on the first row and 1's under the quadratic residues modulo 7.
- Apply cyclic shift on the row, all-zero codeword
- Put one control column and construct the complements of all the code words.
- H_8 contains 16 codewords and has parameters $[4, 8, 4]$

Another ways to construct H_8.

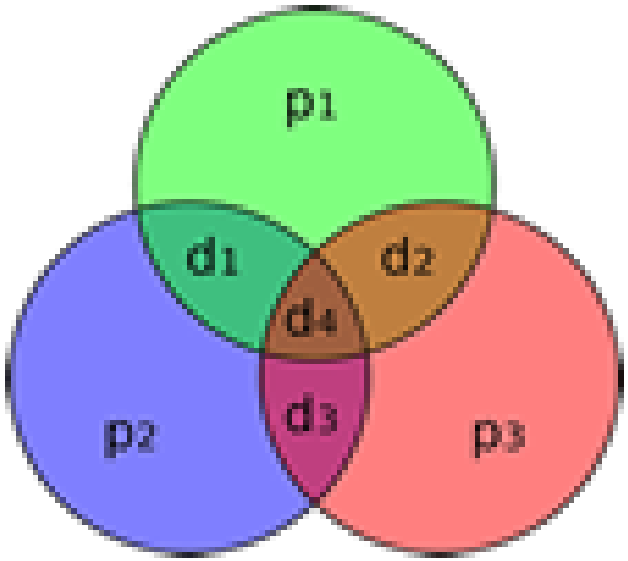
- The parity in each of the circles should be zero.



- This gives a homogeneous equations system with four free variables.

Another ways to construct H_8.

- The parity in each of the circles should be zero.



- This gives a homogeneous equations system with four free variables.
- We can also construct H_8 geometrically by considering the incidence matrix of the projective plane of order 2 contains 7 lines each containing exactly three points.

Example

The **Golay code** G_{24} of length 24 is a self dual code.

Construction of G_{24}.

- We consider the quadratic residues of 0 to 22 modulo 23.
- Continue with similar construction as in H_8.

Example

The **Golay code** G_{24} of length 24 is a self dual code.

Construction of G_{24}.

- We consider the quadratic residues of 0 to 22 modulo 23.
- Continue with similar construction as in H_8.
- G_{24} contains
  - one codeword with all zeros
  - 759 codewords with 8 ones
  - 2576 codewords of 12 ones
  - 779 codewords of 16 ones
  - 1 codeword of 24 ones
- The Golay code contains 4096 codewords and has parameter $[12, 24, 8]$.

Weight enumerator

We want to tell how many codewords there are of each weight.

$$W_{\mathcal{C}}(x,y) = \sum_{c \in \mathcal{C}} x^{c(0)} y^{c(1)}$$

where $c(0)$ is the number of 0's in c.

Example

If $\mathcal{C} = \{00000, 11111\}$, then $W_{\mathcal{C}}(x,y) = x^5 + y^5$ and

$$W_{\mathcal{C}^\perp} = x^5 + 10x^3y^2 + 5xy^4.$$

Weight enumerator

We want to tell how many codewords there are of each weight.

$$W_{\mathcal{C}}(x,y) = \sum_{c \in \mathcal{C}} x^{c(0)} y^{c(1)}$$

where $c(0)$ is the number of 0's in c.

Example

If $\mathcal{C} = \{00000, 11111\}$, then $W_{\mathcal{C}}(x,y) = x^5 + y^5$ and

$$W_{\mathcal{C}^\perp} = x^5 + 10x^3y^2 + 5xy^4.$$

Theorem (MacWilliams '62)

If $\mathcal{C}$ is a code, then

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

Weight enumerator for self-dual codes.

- If $\mathcal{C}$ is self-dual, then

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

- We know that $|C| = 2^{\frac{N}{2}}$ and $W_{\mathcal{C}}$ is homogeneous polynomial of degree N. This gives

$$W_{\mathcal{C}}(x,y) = W_{\mathcal{C}}(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}).$$

Weight enumerator for self-dual codes.

- If $\mathcal{C}$ is self-dual, then

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

- We know that $|C| = 2^{\frac{N}{2}}$ and $W_{\mathcal{C}}$ is homogeneous polynomial of degree N. This gives

$$W_{\mathcal{C}}(x,y) = W_{\mathcal{C}}(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}).$$

- $W_{\mathcal{C}}(x,y)$ is invariant under the linear transformation

$$(x,y)^t \mapsto \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} (x,y)^t.$$

- In particular, for H_8 and G_{24}, we know that every weight is divisible by 4.
- The weight enumerators W_{H_8} and $W_{H_{24}}$ are invariant under the transformation:

$$(x, y)^t \mapsto \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} (x, y)^t.$$

- In particular, for H_8 and G_{24}, we know that every weight is divisible by 4.
- The weight enumerators W_{H_8} and $W_{H_{24}}$ are invariant under the transformation:

$$(x, y)^t \mapsto \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} (x, y)^t.$$

Definition

The set of all finite multiplication of these two complex matrices and their inverses gives an algebraic structure called **group**, G_{192}.

- In particular, for H_8 and G_{24}, we know that every weight is divisible by 4.
- The weight enumerators W_{H_8} and $W_{H_{24}}$ are invariant under the transformation:

$$(x, y)^t \mapsto \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} (x, y)^t.$$

Definition

The set of all finite multiplication of these two complex matrices and their inverses gives an algebraic structure called **group**, G_{192}.

Theorem (Molien, 1897)

Assume that G a subgroup of invertible matrises $GL_n(\mathbb{C})$, $\mathbb{C}[x_1, \cdots, x_n] = \sum_{d \geq 0} R_d$ is the ring polynomials and R_d its homogeneous components, then the Molien series

$$\Phi_G(\lambda) = \sum_{d \geq 0} \dim_{\mathbb{C}}((R_d)^G)\lambda^d := \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - \lambda g)}.$$

Example

Let $G = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\}$ and $R = \mathbb{C}[x, y]$. Then invariants are

$$x^2, xy, y^2, x^4, x^3y, x^2y^2, xy^3, y^4, \ldots$$

. Thus $R^G = \mathbb{C}[x^2, y^2] + xy\mathbb{C}[x^2, y^2]$, and the Molien series will be

$$\Phi_G(\lambda) = \frac{1}{2}\left(\frac{1}{(1-\lambda)^2} + \frac{1}{(1+\lambda)^2}\right) = \frac{1}{(1-\lambda^2)^2} + \frac{\lambda^2}{(1-\lambda^2)^2}.$$

Example

Let $G = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\}$ and $R = \mathbb{C}[x, y]$. Then invariants are

$$x^2, xy, y^2, x^4, x^3y, x^2y^2, xy^3, y^4, \ldots$$

. Thus $R^G = \mathbb{C}[x^2, y^2] + xy\mathbb{C}[x^2, y^2]$, and the Molien series will be

$$\Phi_G(\lambda) = \frac{1}{2}\left(\frac{1}{(1-\lambda)^2} + \frac{1}{(1+\lambda)^2}\right) = \frac{1}{(1-\lambda^2)^2} + \frac{\lambda^2}{(1-\lambda^2)^2}.$$

This series plays an important role in finding generators for the invariant ring R^G.

Theorem

A good basis for R^G exists. In particular, R^G is a polynomial ring iff G is generated by reflections.

Example (Gleason 71')

Let $G = G_{192}$ and $R = \mathbb{C}[x, y]$. The Molien series will be

$$\Phi_G(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})}$$

Example (Gleason 71')

Let $G = G_{192}$ and $R = \mathbb{C}[x, y]$. The Molien series will be

$$\Phi_G(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})}$$

This tells us that the invariant ring $R^{G_{192}}$ is generated by the weight enumerating polynomials og H_8 and G_{24}. In fact,

$$R^{G_{192}} = \mathbb{C}[x^8 + 14x^4y^4 + y^8, x^4y^4(x^4 - y^4)].$$

Thank you!