# Codes and invariant theory.

Gabriele Nebe

Lehrstuhl für Algebra und Zahlentheorie

Around Gleason's Theorem

# Linear codes over finite fields.

- Let $\mathbb{F} := \mathbb{F}_q$ denote the finite field with $q$-elements.
- Classically a linear code $C$ over $\mathbb{F}$ is a subspace $C \leq \mathbb{F}^N$.
- $N$ is called the length of the code.
- $C^\perp := \{v \in \mathbb{F}^N \mid v \cdot c = \sum_{i=1}^N v_i c_i = 0$ for all $c \in C\}$ the dual code.
- $C$ is called self-dual, if $C = C^\perp$.
- Important for the error correcting properties of $C$ is the minimum distance

  $$d(C) := \min\{d(c,c') \mid c \neq c' \in C\} = \min\{w(c) \mid 0 \neq c \in C\}$$

  where

  $$w(c) := |\{1 \leq i \leq N \mid c_i \neq 0\}|$$

  is the Hamming weight of $c$ and $d(c,c') = w(c - c')$ the Hamming distance.
- The Hamming weight enumerator of a code $C \leq \mathbb{F}^N$ is

  $$\mathrm{hwe}_C(x,y) := \sum_{c \in C} x^{N-w(c)} y^{w(c)} \in \mathbb{C}[x,y]_N$$

# The Gleason-Pierce Theorem (1967):

## Theorem.

If $C = C^{\perp} \leq \mathbb{F}_q^N$ such that $w(c) \in m\mathbb{Z}$ for all $c \in C$ and some $m > 1$ then either

- I $q = 2$ and $m = 2$ (all self-dual binary codes).
- II $q = 2$ and $m = 4$ (the doubly-even self-dual binary codes).
- III $q = 3$ and $m = 3$ (all self-dual ternary codes).
- IV $q = 4$ and $m = 2$ (all Hermitian self-dual codes).
- o $q = 4$ and $m = 2$ (certain Euclidean self-dual codes).
- d $q$ arbitrary, $m = 2$ and $\mathrm{hwe}_C(x, y) = (x^2 + (q-1)y^2)^{N/2}$.

## Type

The self-dual codes in this Theorem are called Type I, II, III and IV codes respectively.

# Explanation of Gleason-Pierce Theorem.

## Reason for divisibility condition

For all elements $0 \neq a$ in $\mathbb{F}_2 = \{0, 1\}$ and $\mathbb{F}_3 = \{0, 1, -1\}$ we have that $a^2 = 1$. So for $c \in \mathbb{F}_p^N$ the inner product

$$(c, c) \equiv_p w(c) \text{ for } p = 2, 3.$$

Hermitian self-dual codes satisfy

$$C = \overline{C}^{\perp} = \{x \in \mathbb{F}_{p^2}^N \mid \sum_{i=1}^{N} c_i x_i^p = 0 \text{ for all } x \in C\}$$

For $0 \neq a \in \mathbb{F}_4$ we again have $aa^2 = a^3 = 1$ and hence

$$(c, \overline{c}) \equiv_2 w(c).$$

## Invariance of Hamming weight enumerator

It follows from Gleason-Pierce Theorem that the Hamming weight enumerator of the respective codes is a polynomial in $x$ and $y^m$.

# Some examples for Type I codes.

The **repetition code** $i_2 = \begin{bmatrix} 1 & 1 \end{bmatrix}$ has $\mathrm{hwe}_{i_2}(x, y) = x^2 + y^2$.
The **extended Hamming code**

$$e_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

has $\mathrm{hwe}_{e_8}(x, y) = x^8 + 14x^4y^4 + y^8$ and hence is a Type II code.

# The binary Golay code is another Type II code.

$$g_{24} = \begin{bmatrix} 110101110001100000000000 \\ 101010111000110000000000 \\ 100101011100011000000000 \\ 100010101110001100000000 \\ 100001010111000110000000 \\ 100000101011100011000000 \\ 100000010101110001100000 \\ 100000001010111000110000 \\ 100000000101011100011000 \\ 100000000010101110001100 \\ 100000000001010111000110 \\ 100000000000101011100011 \end{bmatrix}$$

is also of Type II with Hamming weight enumerator

$$\mathrm{hwe}_{g_{24}}(x, y) = x^{24} + 759x^{16}y^{8} + 2576x^{12}y^{12} + 759x^{8}y^{16} + y^{24}$$

# Type III codes: tetracode and ternary Golay code.

The **tetracode.**

$$t_4 := \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix} \leq \mathbb{F}_3^4$$

is a Type III code with

$$\mathrm{hwe}_{t_4}(x, y) = x^4 + 8xy^3.$$

The **ternary Golay code.**

$$g_{12} := \begin{bmatrix} 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 \end{bmatrix} \leq \mathbb{F}_3^{12}$$

$$\mathrm{hwe}_{g_{12}}(x, y) = x^{12} + 264x^6y^6 + 440x^3y^9 + 24y^{12}$$

# Hermitian self-dual codes over $\mathbb{F}_4$.

The **repetition code** $i_2 \otimes \mathbb{F}_4 = \left[\begin{array}{cc} 1 & 1 \end{array}\right]$
has $\mathrm{hwe}_{i_2 \otimes \mathbb{F}_4}(x, y) = x^2 + 3y^2$.
The **hexacode**

$$h_6 = \left[\begin{array}{cccccc} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \end{array}\right] \leq \mathbb{F}_4^6$$

where $\omega^2 + \omega + 1 = 0$. The hexacode is a Type IV code and has Hamming weight enumerator

$$\mathrm{hwe}_{h_6}(x, y) = x^6 + 45x^2y^4 + 18y^6.$$

# The MacWilliams theorem (1962).

## Theorem

Let $C \leq \mathbb{F}_q^N$ be a code. Then

$$\mathrm{hwe}_{C^\perp}(x,y) = \frac{1}{|C|}\,\mathrm{hwe}_C(x+(q-1)y, x-y).$$

In particular, if $C = C^\perp$, then $\mathrm{hwe}_C$ is invariant under the

MacWilliams transformation

$$h_q : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

# Gleason's theorem (ICM, Nice, 1970)

## Theorem.

If $C$ is a self-dual code of Type I,II,III or IV then $\mathrm{hwe}_C \in \mathbb{C}[f, g]$ where

| Type | $f$ | $g$ |
|---|---|---|
| I | $x^2 + y^2$<br>$i_2$ | $x^2y^2(x^2 - y^2)^2$<br>Hamming code $e_8$ |
| II | $x^8 + 14x^4y^4 + y^8$<br>Hamming code $e_8$ | $x^4y^4(x^4 - y^4)^4$<br>binary Golay code $g_{24}$ |
| III | $x^4 + 8xy^3$<br>tetracode $t_4$ | $y^3(x^3 - y^3)^3$<br>ternary Golay code $g_{12}$ |
| IV | $x^2 + 3y^2$<br>$i_2 \otimes \mathbb{F}_4$ | $y^2(x^2 - y^2)^2$<br>hexacode $h_6$ |

# Proof of Gleason's theorem.

Let $C \leq \mathbb{F}_q^N$ be a code of Type $T =$ I,II,III or IV. Then $C = C^\perp$ hence $\mathrm{hwe}_C$ is invariant under MacWilliams transformation $h_q$.
Because of the Gleason-Pierce theorem, $\mathrm{hwe}_C$ is also invariant under the diagonal transformation

$$d_m := \mathrm{diag}(1, \zeta_m) : x \mapsto x, y \mapsto \zeta_m y$$

(where $\zeta_m = \exp(2\pi i/m)$) hence

$$\mathrm{hwe}(C) \in \mathrm{Inv}(\langle h_q, d_m \rangle =: G_T)$$

lies in the invariant ring of the complex matrix group $G_T$. In all cases $G_T$ is a complex reflection group and the invariant ring of $G_T$ is the polynomial ring $\mathbb{C}[f, g]$ generated by the two polynomials given in the table.

## Corollary

The length of a Type II (resp. III) code is a multiple of 8 (resp. 4).

Proof: $\zeta_8 I_2 \in G_{\mathrm{II}}$ and $\zeta_4 I_2 \in G_{\mathrm{III}}$.

# Extremal self-dual codes.

Gleason's theorem allows to bound the minimum weight of a code of a given Type and given length.

**Theorem.**

Let $C$ be a self-dual code of Type $T$ and length $N$. Then $d(C) \leq m + m\lfloor \frac{N}{\deg(g)} \rfloor$.

- I If $T = \mathrm{I}$, then $d(C) \leq 2 + 2\lfloor \frac{N}{8} \rfloor$.
- II If $T = \mathrm{II}$, then $d(C) \leq 4 + 4\lfloor \frac{N}{24} \rfloor$.
- III If $T = \mathrm{III}$, then $d(C) \leq 3 + 3\lfloor \frac{N}{12} \rfloor$.
- IV If $T = \mathrm{IV}$, then $d(C) \leq 2 + 2\lfloor \frac{N}{6} \rfloor$.

Using the notion of the shadow of a code, the bound for Type I codes may be improved.

$$d(C) \leq 4 + 4\lfloor \frac{N}{24} \rfloor + a$$

where $a = 2$ if $N$ (mod 24) $= 22$ and 0 else.