The Type of a code

Gabriele Nebe, RWTH Aachen University

Vlora, April 28, 2008.

- A brief history of Types (I,II,III,IV).
- The Gleason-Pierce theorem, Gleason's theorem.
- A formal notion of Type.
- Automorphisms and equivalence of codes of a given Type.

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.
$C^\perp := \{v \in \mathbb{F}^N \mid v \cdot c = \sum_{i=1}^N v_i c_i = 0\}$ the **dual code**.
C is called **self-dual**, if $C = C^\perp$.
Important for the error correcting properties of C is the **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 Gleason-Pierce Theorem (1967):
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 $m = 2$ (self-dual binary codes).
II) $q = 2$ and $m = 4$ (doubly even self-dual binary codes).
III) $q = 3$ and $m = 3$ (ternary codes).
IV) $q = 4$ and $m = 2$ (Hermitian self-dual codes).
o) $q = 4$ and $m = 2$ (certain Euclidean self-dual codes).
d) q arbitrary, $m = 2$ and $\text{hwe}_C(x, y) = (x^2 + (q-1)y^2)^{N/2}$. In this case $C = \perp^{N/2} [1, a]$ is the orthogonal sum of self-dual codes of length 2 where either q is even and $a = 1$ or $q \equiv 1 \pmod 4$ and $a^2 = -1$ or C is Hermitian self-dual and $a\overline{a} = -1$.

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

The **Hamming weight enumerator** of a code $C \leq \mathbb{F}^N$ is

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

Gleason-Pierce Theorem implies that for codes of Type I, II and IV the Hamming weight enumerator is a polynomial in x^2 and y^2 and for Type III codes, it is a polynomial in x and y^3.

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.**

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

is also of Type II with Hamming weight enumerator

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

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

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

The **ternary Golay code.**

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

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

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

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

The **hexacode**

$$h_6 = \begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \end{bmatrix} \leq \mathbb{F}_4^6$$

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

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

Proof of Gleason's theorem.

Let $C \leq \mathbb{F}_q$ be a code of Type $T =$ I,II,III or IV. Then $C = C^\perp$ hence hwe_C is invariant under MacWilliams transformation h_q. Because of the Gleason-Pierce theorem, 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 code is divisible by 8.
Proof: $\zeta_8 I_2 \in G_{\mathrm{II}}$.

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 $N \pmod{24} = 22$ and 0 else.

G. Nebe, E.M. Rains. N.J.A. Sloane,

Self-dual codes and invariant theory.

(ACM volume 17, Springer 2006, 48.10 Euro until July 31st)

- Introduce a formal notion of a Type of a code.
- Prove a Theorem à la Gleason for a quite general class of rings (including higher genus complete weight enumerators of all classical Types of codes)
- many examples how to apply our theory.
- shadows of codes, maximal isotropic codes
- unimodular lattices, maximal even lattices
- extremal codes, classifications, mass formulas
- Quantum codes

A formal notion of a Type of a code.

Let R be a finite ring (with 1), $\,^J : R \to R$ an involution of R,

$$(ab)^J = b^J a^J \text{ and } (a^J)^J = a \text{ for all } a, b \in R$$

and let V be a finite left R-module.
Then $V^* = \mathrm{Hom}_{\mathbb{Z}}(V, \mathbb{Q}/\mathbb{Z})$ is also a left R-module via

$$(rf)(v) = f(r^J v) \text{ for } v \in V, f \in V^*, r \in R.$$

We assume that $V \cong V^*$ as left R-modules, which means that there is an isomorphism

$$\beta^* : V \to V^*, \beta^*(v) : w \to \beta(v, w)$$

$\beta : V \times V \to \mathbb{Q}/\mathbb{Z}$ is hence biadditive and satisfies

$$\beta(rv, w) = \beta(v, r^J w) \text{ for } r \in R, v, w \in V.$$

A **code** over the alphabet V of length N is an R-submodule $C \leq V^N$.

The **dual code** (with respect to β) is

$$C^{\perp} := \{x \in V^N \mid \beta^N(x,c) = \sum_{i=1}^{N} \beta(x_i, c_i) = 0 \text{ for all } c \in C\} \ .$$

C is called **self-dual** (with respect to β) if $C = C^{\perp}$.

To obtain $(C^{\perp})^{\perp} = C$ we impose the condition that β is ϵ-Hermitian for some central unit ϵ in R, satisfying $\epsilon^J \epsilon = 1$,

$$\beta(v,w) = \beta(w, \epsilon v) \text{ for } v,w \in V.$$

If $\epsilon = 1$ then β is symmetric,

if $\epsilon = -1$ then β is skew-symmetric.

Isotropic codes.

For any **self-orthogonal** code $C \subset C^{\perp}$

$$\beta^N(c, rc) = 0 \text{ for all } c \in C, r \in R.$$

The mapping $x \mapsto \beta(x, rx)$ is a **quadratic mapping** in $\mathrm{Quad}_0(V, \mathbb{Q}/\mathbb{Z}) := \{\phi : V \to \mathbb{Q}/\mathbb{Z} \mid \phi(0) = 0$ and

$$\phi(x+y+z)-\phi(x+y)-\phi(x+z)-\phi(y+z)+\phi(x)+\phi(y)+\phi(z) = 0\} .$$

This is the set of all mappings $\varphi : V \to \mathbb{Q}/\mathbb{Z}$ for which

$$\lambda(\varphi) : V \times V \to \mathbb{Q}/\mathbb{Z}, (v, w) \mapsto \varphi(v + w) - \varphi(v) - \varphi(w)$$

is biadditive. Let $\Phi \subset \mathrm{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$ and let $C \leq V^N$ be a code. Then C is called **isotropic** (with respect to Φ) if

$$\phi^N(c) := \sum_{i=1}^{N} \phi(c_i) = 0 \text{ for all } c \in C \text{ and } \phi \in \Phi.$$

The quadruple (R, V, β, Φ) is called a **Type** if

a) $\Phi \leq \text{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$ is a subgroup and for all $r \in R$, $\phi \in \Phi$ the mapping $\phi[r] : x \mapsto \phi(rx)$ is again in Φ.
Then Φ is an R-**qmodule.**

b) For all $\phi \in \Phi$ there is some $r_\phi \in R$ such that

$$\lambda(\phi)(v, w) = \beta(v, r_\phi w) \text{ for all } v, w\ inV.$$

c) For all $r \in R$ the mapping

$$\phi_r : V \to \mathbb{Q}/\mathbb{Z}, v \mapsto \beta(v, rv) \text{ lies in } \Phi.$$

Type I codes (2_{I})

$$R = \mathbb{F}_2 = V,\ \beta(x,y) = \frac{1}{2}xy,\ \Phi = \{\varphi : x \mapsto \frac{1}{2}x^2 = \beta(x,x), 0\}$$

Type II code (2_{II}).

$$R = \mathbb{F}_2 = V,\ \beta(x,y) = \frac{1}{2}xy,\ \Phi = \{\phi : x \mapsto \frac{1}{4}x^2, 2\phi = \varphi, 3\phi, 0\}$$

Type III codes (3).

$$R = \mathbb{F}_3 = V,\ \beta(x,y) = \frac{1}{3}xy,\ \Phi = \{\varphi : x \mapsto \frac{1}{3}x^2 = \beta(x,x), 2\varphi, 0\}$$

Type IV codes (4^H).

$$R = \mathbb{F}_4 = V,\ \beta(x,y) = \frac{1}{2}\mathrm{trace}(x\overline{y}),\ \Phi = \{\varphi : x \mapsto \frac{1}{2}x\overline{x}, 0\}$$

where $\overline{x} = x^2$.

Additive codes over $\mathbb{F}_4$. (4^{H+})

$$R=\mathbb{F}_2,\ V=\mathbb{F}_4,\ \beta(x,y)=\frac{1}{2}\text{trace}(x\overline{y}),\ \Phi=\{\varphi : x\mapsto \frac{1}{2}x\overline{x}, 0\}$$

Generalized doubly-even codes over $\mathbb{F}_q$, $q=2^f$ (q^E_{II}).

$$R=\mathbb{F}_q=V,\ \beta(x,y)=\frac{1}{2}\text{trace}(xy),\ \Phi=\{x\mapsto \frac{1}{4}\text{trace}(ax^2) : a\in\mathbb{F}_q\}.$$

Euclidean self-dual codes over $\mathbb{F}_q$, $q=p^f$ odd, (q^E).

$$R=\mathbb{F}_q=V,\ \beta(x,y)=\frac{1}{p}\text{trace}(xy),\ \Phi=\{\varphi_a : x\mapsto \frac{1}{p}\text{trace}(ax^2) : a\in\mathbb{F}_q\}.$$

Euclidean self-dual codes over $\mathbb{F}_q$ containing the all ones vector, $q=p^f$ odd, (q^E_1). $R=\mathbb{F}_q=V$,

$$\beta(x,y)=\frac{1}{p}\text{trace}(xy),\ \Phi=\{\varphi_{a,b} : x\mapsto \frac{1}{p}(\text{trace}(ax^2+bx)) : a,b\in\mathbb{F}_q\}.$$

The automorphism group of a Type.

Let $T := (R, V, \beta, \Phi)$ be a Type. Then Aut$(T) :=$

$\{\varphi \in \text{End}_R(V) \mid \beta(\varphi(v), \varphi(w)) = \beta(v, w), \phi(\varphi(v)) = \phi(v)$ for all $v, w \in V, \phi \in \Phi\}$

is the **automorphism group** of the Type T.

Examples.

Hermitian codes over $\mathbb{F}_4$: Aut$(4^H) = \mathbb{F}_4^* = \{1, \omega, \omega^2\}$

Euclidean codes over $\mathbb{F}_4$: Aut$(4^E) = \{1\}$.

Equivalence of codes of a given Type.

$$\mathrm{Aut}_N(T) := \mathrm{Aut}(T) \wr S_N = \{(\varphi_1, \ldots, \varphi_N)\pi \mid \pi \in S_N, \varphi_i \in \mathrm{Aut}(T)\}$$

Two codes $C, D \leq V^N$ of Type T are called T-**equivalent**, if there is $\sigma \in \mathrm{Aut}_N(T)$ such that $\sigma(C) = D$.
The **automorphism group** of C is

$$\mathrm{Aut}_T(C) := \{\sigma \in \mathrm{Aut}(T) \wr S_N \mid \sigma(C) = C\}$$

The codes $(1,1)$ and $(1,\omega)$ are equivalent as Hermitian codes over $\mathbb{F}_4$ but not as Euclidean codes.

So equivalence is not a property of the codes alone but a property of the Type.

Classification and mass formulae.

Annika Günther will show in her talk a method to classify all self-dual codes of a given Type. This method is based on an algorithm originally formulated by Martin Kneser to enumerate unimodular lattices (up to equivalence).

Also for Type T codes $C \leq V^N$ one is mainly interested in equivalence classes

$$[C] := \{D \leq V^N \text{ of Type } T \mid D = \pi(C) \text{ for some } \pi \in \mathrm{Aut}_N(T)\}.$$

Number of equivalence classes of codes of Type T

N	I	II	III	IV
2	1(1)	–	–	1(1)
4	1(1)	–	1(1)	1(1)
6	1(1)	–	–	2(1)
8	2(1)	1(1)	1(1)	3(1)
10	2	–	–	5(2)
12	3	–	3(1)	10
14	4	–	–	21(1)
16	7	2(2)	7(1)	55(4)
18	9	–	–	244
20	16	–	24(6)	
22	25	–	–	
24	55	9(1)	338(2)	
26	103	–	–	
28	261	–	(6931)	
30	731	–	–	
32	3295	85(5)		
34	24147	–	–	

In brackets the number of extremal codes.

The mass formula.

Let $M_N(T) := \{C \le V^N \mid C \text{ of Type } T\}$, $m_N(T) := |M_N(T)|$ and $a_N(T) := |\operatorname{Aut}_N(T)|$.
Then $M_N(T) = \dot\bigcup_{j=1}^{h} [C_j]$ is the disjoint union of equivalence classes.

$$\textbf{mass formula:} \quad \sum_{j=1}^{h} \frac{1}{|\operatorname{Aut}(C_j)|} = \frac{m_N(T)}{a_N(T)}.$$

Proof. $\operatorname{Aut}_N(T)$ acts on $M_N(T)$ and the equivalence classes are precisely the $\operatorname{Aut}_N(T)$-orbits. So

$$|[C_j]| = \frac{|\operatorname{Aut}_N(T)|}{|\operatorname{Aut}(C_j)|}$$

is the index of the stabilizer and

$$|M_N(T)| = \sum_{j=1}^{h} |[C_j]| = \sum_{j=1}^{h} \frac{|\operatorname{Aut}_N(T)|}{|\operatorname{Aut}(C_j)|}.$$

Type	$m_N(T)$	$a_N(T)$
I	$\prod_{i=1}^{N/2-1}(2^i+1)$	$N!$
II	$2\prod_{i=1}^{N/2-2}(2^i+1)$	$N!$
III	$2\prod_{i=1}^{N/2-1}(3^i+1)$	$2^N N!$
IV	$\prod_{i=0}^{N/2-1}(2^{2i+1}+1)$	$3^N N!$