Propelinear codes from multiplicative group of $GF(2^m)$

I.Yu. Mogilnykh, F.I. Solov'eva

Novosibirsk State University
Sobolev Institute of Mathematics

Presented at G2S2

Codes in Hamming space

The Hamming space F_2^n is the n-dimensional vector space over $GF(2)$ with the *Hamming metric*

$$d(x, y) = |\{i \in \{1, \dots, n\} : x_i \neq y_i\}|.$$

A *binary code* is a collection of binary vectors (codewords) from F_2^n, n is the *length* of the code.
The code distance of a binary code is $min_{x,y \in C: x \neq y} d(x, y)$.

Hamming bound

Let C be a binary code of length n and code distance d. Then

$$|C| \leq 2^n / \sum_{i=0,\dots,(d-1)/2} \binom{n}{i}.$$

Codes in Hamming space

The Hamming space F_2^n is the n-dimensional vector space over $GF(2)$ with the *Hamming metric*

$$d(x,y) = |\{i \in \{1,\dots,n\} : x_i \neq y_i\}|.$$

A *binary code* is a collection of binary vectors (codewords) from F_2^n, n is the *length* of the code.
The code distance of a binary code is $min_{x,y \in C: x \neq y} d(x,y)$.

Hamming bound

Let C be a binary code of length n and code distance d. Then

$$|C| \leq 2^n / \sum_{i=0,\dots,(d-1)/2} \binom{n}{i}.$$

Codes in Hamming space

The Hamming space F_2^n is the n-dimensional vector space over $GF(2)$ with the *Hamming metric*

$$d(x,y) = |\{i \in \{1,\dots,n\} : x_i \neq y_i\}|.$$

A *binary code* is a collection of binary vectors (codewords) from F_2^n, n is the *length* of the code.
The code distance of a binary code is $min_{x,y\in C: x\neq y} d(x,y)$.

Hamming bound

Let C be a binary code of length n and code distance d. Then

$$|C| \leq 2^n / \sum_{i=0,\dots,(d-1)/2} \binom{n}{i}.$$

Codes in Hamming space

The Hamming space F_2^n is the n-dimensional vector space over $GF(2)$ with the *Hamming metric*

$$d(x, y) = |\{i \in \{1, \dots, n\} : x_i \neq y_i\}|.$$

A *binary code* is a collection of binary vectors (codewords) from F_2^n, n is the *length* of the code.
The code distance of a binary code is $min_{x,y \in C : x \neq y} d(x, y)$.

Hamming bound

Let C be a binary code of length n and code distance d. Then

$$|C| \leq 2^n / \sum_{i=0,\dots,(d-1)/2} \binom{n}{i}.$$

Perfect codes

A code with minimum distance 3 is *perfect* (sometimes called 1-perfect) if it attains Hamming bound, i.e.

$$|C| = 2^n/(n+1).$$

These codes exist for length $n = 2^r - 1$, size 2^{n-r} and minimum distance 3 for any $r \geq 2$.

A Hamming code is a perfect code which is a linear subspace of F_2^n.

Perfect codes

A code with minimum distance 3 is *perfect* (sometimes called 1-perfect) if it attains Hamming bound, i.e.

$$|C| = 2^n/(n+1).$$

These codes exist for length $n = 2^r - 1$, size 2^{n-r} and minimum distance 3 for any $r \geq 2$.

A Hamming code is a perfect code which is a linear subspace of F_2^n.

The automorphism group of the code

An automorphism of F_2^n is an isometry of Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

$$(x, \pi) : y \rightarrow x + (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(n)}), y \in F_2^n.$$

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi\pi').$$

The group of automorphisms of F_2^n w.t.r. $\cdot$ is $(\{(x, \pi) : x \in F_2^n, \pi \in Sym(n)\}, \cdot)$

The *automorphism group* of a code C is $Stab_C(Aut(F_2^n))$, denoted by $Aut(C)$.

The automorphism group of the code

An automorphism of F_2^n is an isometry of Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

$$(x, \pi) : y \to x + (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(n)}), y \in F_2^n.$$

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi\pi').$$

The group of automorphisms of F_2^n w.t.r. $\cdot$ is $(\{(x, \pi) : x \in F_2^n, \pi \in Sym(n)\}, \cdot)$

The *automorphism group* of a code C is $Stab_C(Aut(F_2^n))$, denoted by $Aut(C)$.

The automorphism group of the code

An automorphism of F_2^n is an isometry of Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

$$(x, \pi) : y \to x + (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(n)}), y \in F_2^n.$$

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi\pi').$$

The group of automorphisms of F_2^n w.t.r. $\cdot$ is $(\{(x, \pi) : x \in F_2^n, \pi \in Sym(n)\}, \cdot)$

The *automorphism group* of a code C is $Stab_C(Aut(F_2^n))$, denoted by $Aut(C)$.

The automorphism group of the code

An automorphism of F_2^n is an isometry of Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

$$(x, \pi) : y \to x + (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(n)}), y \in F_2^n.$$

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi\pi').$$

The group of automorphisms of F_2^n w.t.r. $\cdot$ is $(\{(x, \pi) : x \in F_2^n, \pi \in Sym(n)\}, \cdot)$

The *automorphism group* of a code C is $Stab_C(Aut(F_2^n))$, denoted by $Aut(C)$.

The automorphism group of the code

An automorphism of F_2^n is an isometry of Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

$$(x, \pi) : y \to x + (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(n)}), y \in F_2^n.$$

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi\pi').$$

The group of automorphisms of F_2^n w.t.r. $\cdot$ is
$(\{(x, \pi) : x \in F_2^n, \pi \in Sym(n)\}, \cdot)$

The *automorphism group* of a code C is $Stab_C(Aut(F_2^n))$, denoted by $Aut(C)$.

The automorphism group of the code

An automorphism of F_2^n is an isometry of Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

$$(x, \pi) : y \to x + (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(n)}), y \in F_2^n.$$

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi\pi').$$

The group of automorphisms of F_2^n w.t.r. $\cdot$ is
$(\{(x, \pi) : x \in F_2^n, \pi \in Sym(n)\}, \cdot)$

The *automorphism group* of a code C is $Stab_C(Aut(F_2^n))$, denoted by $Aut(C)$.

Propelinear codes

[Rifa, Phelps, 2002], original definition by [Rifa, Huguet, Bassart, 1989]

A code C is called *propelinear* if there is a subgroup $G < Aut(C)$ acting sharply transitive (regularly) on the codewords, i.e.:

$$\forall x, y \in C \quad \exists! g \in G : g(x) = y$$

The automorphism group of a propelinear code can have many regular subgroups.

Propelinear codes

[Rifa, Phelps, 2002], original definition by [Rifa, Huguet, Bassart, 1989]

A code C is called *propelinear* if there is a subgroup $G < Aut(C)$ acting sharply transitive (regularly) on the codewords, i.e.:

$$\forall x, y \in C \quad \exists! g \in G : g(x) = y$$

The automorphism group of a propelinear code can have many regular subgroups.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0), id), ((1,1), id), ((0,1),(1,2)), ((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1), id)$, so G' has element of order 4.
$(G',\cdot) \cong Z_4$.

The code C has two *nonisomorphic* regular subgroups: $G \ncong G'$.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}.$
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0),id),((1,1),id),((0,1),(1,2)),((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1),id)$, so G' has element of order 4.
$(G',\cdot) \cong Z_4$.

The code C has two *nonisomorphic* regular subgroups: $G \not\cong G'$.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0), id), ((1,1), id), ((0,1),(1,2)), ((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1), id)$, so G' has element of order 4.
$(G',\cdot) \cong Z_4$.

The code C has two *nonisomorphic* regular subgroups: $G \not\cong G'$.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0), id), ((1,1), id), ((0,1),(1,2)), ((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1), id)$, so G' has element of order 4.
$(G',\cdot) \cong Z_4$.

The code C has two *nonisomorphic* regular subgroups: $G \ncong G'$.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0),id),((1,1),id),((0,1),(1,2)),((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1),id)$, so G' has element of order 4.
$(G',\cdot) \cong Z_4$.

The code C has two *nonisomorphic* regular subgroups: $G \ncong G'$.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0),id),((1,1),id),((0,1),(1,2)),((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1),id)$, so G' has element of order 4.
$(G',\cdot) \cong Z_4$.

The code C has two *nonisomorphic* regular subgroups: $G \ncong G'$.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G, \cdot)$ is a regular subgroup of $Aut(C)$.
$(G, \cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0), id), ((1,1), id), ((0,1),(1,2)), ((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1), id)$, so G' has element of order 4.
$(G', \cdot) \cong Z_4$.

The code C has two *nonisomorphic* regular subgroups: $G \not\cong G'$.

Regular subgroups: record for perfect codes of length 16

[M., 2016]

The automorphism group of the extended Hamming code of length 16 has at least 2284 pairwise nonisomorphic regular subgroups.

Propelinear perfect codes: existence

Linear codes [Hamming, 1949]
Translation-invariant perfect codes [Rifa, Pujol, 1997] (their automorphism group has regular subgroups, isomorphic to $Z_2^l \times Z_4^m$*)*
Transitive Malugin codes, i.e. 1-step switchings of Hamming code are propelinear [Borges, M., Rifa, Solov'eva, 2012]
Vasiliev and Mollard can be used to construct propelinear perfect codes [Borges, M., Rifa, Solov'eva, 2012]
Potapov transitive extended perfect codes are propelinear [Borges, M., Rifa, Solov'eva, 2013]
Propelinear Vasil'ev perfect codes from quadratic functions [Krotov, Potapov, 2013]

Preparata codes

Preparata code is a binary code of length $n = 2^m - 1$ for even m, $m \geq 4$ of size $2^{n+1}/(n+1)^2$ with code distance 5.

Theorem [Semakov,Zinoviev, Zaitsev, 1971]

Any Preparata code is a subcode of a unique perfect code.

Constructions of Preparata codes

Baker, van Lint, Wilson, 1983 ([Dumer, 1976]): Preparata codes that are subcodes of Hamming codes.
Hammons, Kumar, Calderbank, Sloane, Sole, 1994: Z_4-linear Preparata codes that are subcodes of Z_4-linear perfect codes.

All known Preparata codes are propelinear.

Preparata codes

Preparata code is a binary code of length $n = 2^m - 1$ for even m, $m \geq 4$ of size $2^{n+1}/(n+1)^2$ with code distance 5.

Theorem [Semakov,Zinoviev, Zaitsev, 1971]

Any Preparata code is a subcode of a unique perfect code.

Constructions of Preparata codes

Baker, van Lint, Wilson, 1983 ([Dumer, 1976]): Preparata codes that are subcodes of Hamming codes.
Hammons, Kumar, Calderbank, Sloane, Sole, 1994: Z_4-linear Preparata codes that are subcodes of Z_4-linear perfect codes.

All known Preparata codes are propelinear.

Preparata codes

Preparata code is a binary code of length $n = 2^m - 1$ for even m, $m \geq 4$ of size $2^{n+1}/(n+1)^2$ with code distance 5.

Theorem [Semakov,Zinoviev, Zaitsev, 1971]

Any Preparata code is a subcode of a unique perfect code.

Constructions of Preparata codes

Baker, van Lint, Wilson, 1983 ([Dumer, 1976]): Preparata codes that are subcodes of Hamming codes.

Hammons, Kumar, Calderbank, Sloane, Sole, 1994: Z_4-linear Preparata codes that are subcodes of Z_4-linear perfect codes.

All known Preparata codes are propelinear.

Preparata codes

Preparata code is a binary code of length $n = 2^m - 1$ for even m, $m \geq 4$ of size $2^{n+1}/(n+1)^2$ with code distance 5.

Theorem [Semakov,Zinoviev, Zaitsev, 1971]

Any Preparata code is a subcode of a unique perfect code.

Constructions of Preparata codes

Baker, van Lint, Wilson, 1983 ([Dumer, 1976]): Preparata codes that are subcodes of Hamming codes.
Hammons, Kumar, Calderbank, Sloane, Sole, 1994: Z_4-linear Preparata codes that are subcodes of Z_4-linear perfect codes.

All known Preparata codes are propelinear.

Preparata codes

Preparata code is a binary code of length $n = 2^m - 1$ for even m, $m \geq 4$ of size $2^{n+1}/(n+1)^2$ with code distance 5.

Theorem [Semakov,Zinoviev, Zaitsev, 1971]

Any Preparata code is a subcode of a unique perfect code.

Constructions of Preparata codes

Baker, van Lint, Wilson, 1983 ([Dumer, 1976]): Preparata codes that are subcodes of Hamming codes.
Hammons, Kumar, Calderbank, Sloane, Sole, 1994: Z_4-linear Preparata codes that are subcodes of Z_4-linear perfect codes.

All known Preparata codes are propelinear.

Preparata codes

Preparata code is a binary code of length $n = 2^m - 1$ for even m, $m \geq 4$ of size $2^{n+1}/(n+1)^2$ with code distance 5.

Theorem [Semakov,Zinoviev, Zaitsev, 1971]

Any Preparata code is a subcode of a unique perfect code.

Constructions of Preparata codes

Baker, van Lint, Wilson, 1983 ([Dumer, 1976]): Preparata codes that are subcodes of Hamming codes.
Hammons, Kumar, Calderbank, Sloane, Sole, 1994: Z_4-linear Preparata codes that are subcodes of Z_4-linear perfect codes.

All known Preparata codes are propelinear.

Main result

1. Let B be the binary primitive BCH code with designed distance 5 of length $n = 2^m - 1$, m is odd.
2. Let P be a Preparata code of length $n = 2^m - 1$, m is even constructed by Dumer, Baker, van Lint, Wilson.
3. Let Γ be a Goethals subcode of Preparata code P.
4. Let C be a Hamming code with subcodes B or P of length $n = 2^m - 1$. 5. Let Π be a Z_4-linear Preparata code, Σ be the Z_4-linear perfect code with subcode Π.

The codes above are propelinear. Moreover:
$B \subset C, \Gamma \subset P \subset C, \Pi \subset \Sigma$.

Theorem

The following codes are propelinear:
$C \setminus B, C \setminus P, P \setminus \Gamma, \Sigma \setminus \Pi$.

Main result

1. Let B be the binary primitive BCH code with designed distance 5 of length $n = 2^m - 1$, m is odd.
2. Let P be a Preparata code of length $n = 2^m - 1$, m is even constructed by Dumer, Baker, van Lint, Wilson.
3. Let Γ be a Goethals subcode of Preparata code P.
4. Let C be a Hamming code with subcodes B or P of length $n = 2^m - 1$. 5. Let Π be a Z_4-linear Preparata code, Σ be the Z_4-linear perfect code with subcode Π.

The codes above are propelinear. Moreover: $B \subset C, \Gamma \subset P \subset C, \Pi \subset \Sigma$.

Theorem

The following codes are propelinear: $C \setminus B, C \setminus P, P \setminus \Gamma, \Sigma \setminus \Pi$.

Main result

1. Let B be the binary primitive BCH code with designed distance 5 of length $n = 2^m - 1$, m is odd.
2. Let P be a Preparata code of length $n = 2^m - 1$, m is even constructed by Dumer, Baker, van Lint, Wilson.
3. Let Γ be a Goethals subcode of Preparata code P.
4. Let C be a Hamming code with subcodes B or P of length $n = 2^m - 1$. 5. Let Π be a Z_4-linear Preparata code, Σ be the Z_4-linear perfect code with subcode Π.

The codes above are propelinear. Moreover:
$B \subset C, \Gamma \subset P \subset C, \Pi \subset \Sigma$.

Theorem

The following codes are propelinear:
$C \setminus B, C \setminus P, P \setminus \Gamma, \Sigma \setminus \Pi$.

Main result

1. Let B be the binary primitive BCH code with designed distance 5 of length $n = 2^m - 1$, m is odd.
2. Let P be a Preparata code of length $n = 2^m - 1$, m is even constructed by Dumer, Baker, van Lint, Wilson.
3. Let Γ be a Goethals subcode of Preparata code P.
4. Let C be a Hamming code with subcodes B or P of length $n = 2^m - 1$. 5. Let Π be a Z_4-linear Preparata code, Σ be the Z_4-linear perfect code with subcode Π.

The codes above are propelinear. Moreover: $B \subset C, \Gamma \subset P \subset C, \Pi \subset \Sigma$.

Theorem

The following codes are propelinear: $C \setminus B, C \setminus P, P \setminus \Gamma, \Sigma \setminus \Pi$.

Main result

1. Let B be the binary primitive BCH code with designed distance 5 of length $n = 2^m - 1$, m is odd.
2. Let P be a Preparata code of length $n = 2^m - 1$, m is even constructed by Dumer, Baker, van Lint, Wilson.
3. Let Γ be a Goethals subcode of Preparata code P.
4. Let C be a Hamming code with subcodes B or P of length $n = 2^m - 1$. 5. Let Π be a Z_4-linear Preparata code, Σ be the Z_4-linear perfect code with subcode Π.

The codes above are propelinear. Moreover: $B \subset C, \Gamma \subset P \subset C, \Pi \subset \Sigma$.

Theorem

The following codes are propelinear: $C \setminus B, C \setminus P, P \setminus \Gamma, \Sigma \setminus \Pi$.

Main result

1. Let B be the binary primitive BCH code with designed distance 5 of length $n = 2^m - 1$, m is odd.
2. Let P be a Preparata code of length $n = 2^m - 1$, m is even constructed by Dumer, Baker, van Lint, Wilson.
3. Let Γ be a Goethals subcode of Preparata code P.
4. Let C be a Hamming code with subcodes B or P of length $n = 2^m - 1$. 5. Let Π be a Z_4-linear Preparata code, Σ be the Z_4-linear perfect code with subcode Π.

The codes above are propelinear. Moreover:
$B \subset C, \Gamma \subset P \subset C, \Pi \subset \Sigma$.

Theorem

The following codes are propelinear:
$C \setminus B, C \setminus P, P \setminus \Gamma, \Sigma \setminus \Pi$.

Main result

1. Let B be the binary primitive BCH code with designed distance 5 of length $n = 2^m - 1$, m is odd.
2. Let P be a Preparata code of length $n = 2^m - 1$, m is even constructed by Dumer, Baker, van Lint, Wilson.
3. Let Γ be a Goethals subcode of Preparata code P.
4. Let C be a Hamming code with subcodes B or P of length $n = 2^m - 1$. 5. Let Π be a Z_4-linear Preparata code, Σ be the Z_4-linear perfect code with subcode Π.

The codes above are propelinear. Moreover:
$B \subset C, \Gamma \subset P \subset C, \Pi \subset \Sigma$.

Theorem

The following codes are propelinear:
$C \setminus B, C \setminus P, P \setminus \Gamma, \Sigma \setminus \Pi$.

Example: The complement of Hamming code

Let C be a Hamming code of length n. Then $F_2^n \setminus C$ is a propelinear code. Sketch:

(i) C is a (prope)linear code. $(C, +) < Aut(C)$, $+$ is the addition in F_2^n.

(ii) C is isomorphic to a cyclic code. There is H, $H \cong (F_2^{log(n+1)})^*$, $H < Aut(C)$, H is regular on the coordinates $\{1,\ldots,n\}$ and cosets $(F_2^n/(C,+)) \setminus C$:

$$e_1 + C, \ldots, e_n + C, \text{ where } e_i = (0, \ldots, 0, 1_i, 0, \ldots, 0).$$

(iii) $H \cap (C, +) = \varnothing$ and $| < H, (C, +) > | = |H||C|$, so $< H, (C, +) >$ is regular on the codewords of $F_2^n \setminus C$.

Example: The complement of Hamming code

Let C be a Hamming code of length n. Then $F_2^n \setminus C$ is a propelinear code. Sketch:

(i) C is a (prope)linear code. $(C, +) < Aut(C)$, $+$ is the addition in F_2^n.

(ii) C is isomorphic to a cyclic code. There is H, $H \cong (F_2^{log(n+1)})^*$, $H < Aut(C)$, H is regular on the coordinates $\{1,\ldots,n\}$ and cosets $(F_2^n/(C, +)) \setminus C$:

$$e_1 + C, \ldots, e_n + C, \text{ where } e_i = (0, \ldots, 0, 1_i, 0, \ldots, 0).$$

(iii) $H \cap (C, +) = \varnothing$ and $| < H, (C, +) > | = |H||C|$, so $< H, (C, +) >$ is regular on the codewords of $F_2^n \setminus C$.

Example: The complement of Hamming code

Let C be a Hamming code of length n. Then $F_2^n \setminus C$ is a propelinear code. Sketch:

(i) C is a (prope)linear code. $(C,+) < Aut(C)$, $+$ is the addition in F_2^n.

(ii) C is isomorphic to a cyclic code. There is H, $H \cong (F_2^{log(n+1)})^*$, $H < Aut(C)$, H is regular on the coordinates {1,...,n} and cosets $(F_2^n/(C,+)) \setminus C$:

$$e_1 + C, \dots, e_n + C, \text{ where } e_i = (0, \dots, 0, 1_i, 0, \dots, 0).$$

(iii) $H \cap (C,+) = \varnothing$ and $| < H, (C,+) > | = |H||C|$, so $< H, (C,+) >$ is regular on the codewords of $F_2^n \setminus C$.

Example: The complement of Hamming code

Let C be a Hamming code of length n. Then $F_2^n \setminus C$ is a propelinear code. Sketch:

(i) C is a (prope)linear code. $(C,+) < Aut(C)$, $+$ is the addition in F_2^n.

(ii) C is isomorphic to a cyclic code. There is H, $H \cong (F_2^{log(n+1)})^*$, $H < Aut(C)$, H is regular on the coordinates $\{1,\ldots,n\}$ and cosets $(F_2^n/(C,+)) \setminus C$:

$$e_1 + C, \ldots, e_n + C, \text{ where } e_i = (0,\ldots,0,1_i,0,\ldots,0).$$

(iii) $H \cap (C,+) = \varnothing$ and $| < H,(C,+) > | = |H||C|$, so $< H,(C,+) >$ is regular on the codewords of $F_2^n \setminus C$.

Example: The complement of Hamming code

Let C be a Hamming code of length n. Then $F_2^n \setminus C$ is a propelinear code. Sketch:

(i) C is a (prope)linear code. $(C,+) < Aut(C)$, $+$ is the addition in F_2^n.

(ii) C is isomorphic to a cyclic code. There is H, $H \cong (F_2^{log(n+1)})^*$, $H < Aut(C)$, H is regular on the coordinates $\{1,\dots,n\}$ and cosets $(F_2^n/(C,+)) \setminus C$:

$$e_1 + C, \dots, e_n + C, \text{ where } e_i = (0,\dots,0,1_i,0,\dots,0).$$

(iii) $H \cap (C,+) = \varnothing$ and $| < H,(C,+) > | = |H||C|$, so $< H,(C,+) >$ is regular on the codewords of $F_2^n \setminus C$.

Example: The complement of Hamming code

Let C be a Hamming code of length n. Then $F_2^n \setminus C$ is a propelinear code. Sketch:

(i) C is a (prope)linear code. $(C,+) < Aut(C)$, $+$ is the addition in F_2^n.

(ii) C is isomorphic to a cyclic code. There is H, $H \cong (F_2^{log(n+1)})^*$, $H < Aut(C)$, H is regular on the coordinates $\{1,\ldots,n\}$ and cosets $(F_2^n/(C,+)) \setminus C$:

$$e_1 + C, \ldots, e_n + C, \text{ where } e_i = (0,\ldots,0,1_i,0,\ldots,0).$$

(iii) $H \cap (C,+) = \varnothing$ and $|<H,(C,+)>| = |H||C|$, so $<H,(C,+)>$ is regular on the codewords of $F_2^n \setminus C$.

THANK YOU FOR YOUR ATTENTION