A lower bound on the number of nonequivalent propelinear extended perfect codes

J. Borges, I. Mogilnykh, J. Rifà, F. Solov'eva

Sobolev Institute of Mathematics
Universitat Autònoma de Barcelona
e-mails: {joaquim.borges,josep.rifa}@autonoma.edu
{ivmog84,fainasoloveva}@gmail.com

Presented at ACCT XIII, 20 June 2012

Isometries of F_q^n

Let F_q^n be the Hamming space of dimension n over F_q.

Isometries of F_q^n

The action of *an isometry* ϕ of F_q^n can be presented using a permutation π of the coordinates $\{1, \ldots, n\}$:
$\pi(x) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})$ and
a mapping $\sigma = (\sigma_1, \ldots, \sigma_n)$, called a *multi-permutation*, where $\sigma_i, 1 \leq i \leq n$ are permutations of the elements of F_q:
$\sigma(x) = (\sigma_1(x_1), \ldots, \sigma_n(x_n))$,
so $\phi(x) = (\sigma, \pi)(x) = (\sigma_1(x_{\pi^{-1}(1)}), \ldots, \sigma_n(x_{\pi^{-1}(n)}))$

Isometries of F_q^n

Let F_q^n be the Hamming space of dimension n over F_q.

Isometries of F_q^n

The action of *an isometry* ϕ of F_q^n can be presented using
a permutation π of the coordinates $\{1, \ldots, n\}$:
$\pi(x) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})$ and
a mapping $\sigma = (\sigma_1, \ldots, \sigma_n)$, called a *multi-permutation*, where $\sigma_i, 1 \leq i \leq n$ are permutations of the elements of F_q:
$\sigma(x) = (\sigma_1(x_1), \ldots, \sigma_n(x_n))$,
so $\phi(x) = (\sigma, \pi)(x) = (\sigma_1(x_{\pi^{-1}(1)}), \ldots, \sigma_n(x_{\pi^{-1}(n)}))$

Isometries of F_q^n

Let F_q^n be the Hamming space of dimension n over F_q.

Isometries of F_q^n

The action of *an isometry* ϕ of F_q^n can be presented using a permutation π of the coordinates $\{1, \ldots, n\}$:
$\pi(x) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})$ and
a mapping $\sigma = (\sigma_1, \ldots, \sigma_n)$, called a *multi-permutation*, where $\sigma_i, 1 \leq i \leq n$ are permutations of the elements of F_q:
$\sigma(x) = (\sigma_1(x_1), \ldots, \sigma_n(x_n))$,
so $\phi(x) = (\sigma, \pi)(x) = (\sigma_1(x_{\pi^{-1}(1)}), \ldots, \sigma_n(x_{\pi^{-1}(n)}))$

Isometries of F_q^n

Let F_q^n be the Hamming space of dimension n over F_q.

Isometries of F_q^n

The action of *an isometry* ϕ of F_q^n can be presented using a permutation π of the coordinates $\{1, \ldots, n\}$:
$\pi(x) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})$ and
a mapping $\sigma = (\sigma_1, \ldots, \sigma_n)$, called a *multi-permutation*, where $\sigma_i, 1 \leq i \leq n$ are permutations of the elements of F_q:
$\sigma(x) = (\sigma_1(x_1), \ldots, \sigma_n(x_n))$,
so $\phi(x) = (\sigma, \pi)(x) = (\sigma_1(x_{\pi^{-1}(1)}), \ldots, \sigma_n(x_{\pi^{-1}(n)}))$

Isometries of F_q^n

Let F_q^n be the Hamming space of dimension n over F_q.

Isometries of F_q^n

The action of *an isometry* ϕ of F_q^n can be presented using a permutation π of the coordinates $\{1, \ldots, n\}$:
$\pi(x) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})$ and
a mapping $\sigma = (\sigma_1, \ldots, \sigma_n)$, called a *multi-permutation*, where $\sigma_i, 1 \leq i \leq n$ are permutations of the elements of F_q:
$\sigma(x) = (\sigma_1(x_1), \ldots, \sigma_n(x_n))$,
so $\phi(x) = (\sigma, \pi)(x) = (\sigma_1(x_{\pi^{-1}(1)}), \ldots, \sigma_n(x_{\pi^{-1}(n)}))$

The isometry group of a code

A q-ary *code* of length n is a subset of F_q^n.

The *isometry group Iso(C)* of a code is a maximum subgroup that stabilizes the code set-wise.

The isometry group of a code

A q-ary *code* of length n is a subset of F_q^n.

The *isometry group Iso(C)* of a code is a maximum subgroup that stabilizes the code set-wise.

Propelinear code

Let C be a q-ary code of length n. The code is *propelinear* if there exists a mapping $x \to (\sigma_x, \pi_x)$, $(\sigma_x, \pi_x) \in Iso(C)$ such that:
(i) if the subgroup generated by $\{(\sigma_x, \pi_x) : x \in C\}$ acts transitively on the codewords of C. *(Then the code C is transitive)*
(ii) if the order of the subgroup generated by $\{(\sigma_x, \pi_x) : x \in C\}$ is $|C|$.

Define an operation $\star$: $x \star y = (\sigma_x; \pi_x)(y)$ for any $x, y \in C$.

Lemma

The code C with the operation $\star$ is a group $(C, \star)$, called a propelinear structure on C.

There can exist many different propelinear structures on a given code (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

Propelinear code

Let C be a q-ary code of length n. The code is *propelinear* if there exists a mapping $x \to (\sigma_x, \pi_x)$, $(\sigma_x, \pi_x) \in Iso(C)$ such that:
(i) if the subgroup generated by $\{(\sigma_x, \pi_x) : x \in C\}$ acts transitively on the codewords of C. *(Then the code C is transitive)*
(ii) if the order of the subgroup generated by $\{(\sigma_x, \pi_x) : x \in C\}$ is $|C|$.

Define an operation $\star$: $x \star y = (\sigma_x; \pi_x)(y)$ for any $x, y \in C$.

Lemma

The code C with the operation $\star$ is a group $(C, \star)$, called a propelinear structure on C.

There can exist many different propelinear structures on a given code (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

Propelinear code

Let C be a q-ary code of length n. The code is *propelinear* if there exists a mapping $x \to (\sigma_x, \pi_x)$, $(\sigma_x, \pi_x) \in Iso(C)$ such that:
(i) if the subgroup generated by $\{(\sigma_x, \pi_x) : x \in C\}$ acts transitively on the codewords of C. *(Then the code C is transitive)*
(ii) if the order of the subgroup generated by $\{(\sigma_x, \pi_x) : x \in C\}$ is $|C|$.

Define an operation $\star$: $x \star y = (\sigma_x; \pi_x)(y)$ for any $x, y \in C$.

Lemma

The code C with the operation $\star$ is a group $(C, \star)$, called a propelinear structure on C.

There can exist many different propelinear structures on a given code (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

Propelinear code

Let C be a q-ary code of length n. The code is *propelinear* if there exists a mapping $x \to (\sigma_x, \pi_x)$, $(\sigma_x, \pi_x) \in Iso(C)$ such that:
(i) if the subgroup generated by $\{(\sigma_x, \pi_x) : x \in C\}$ acts transitively on the codewords of C. *(Then the code C is transitive)*
(ii) if the order of the subgroup generated by $\{(\sigma_x, \pi_x) : x \in C\}$ is $|C|$.

Define an operation $\star$: $x \star y = (\sigma_x; \pi_x)(y)$ for any $x, y \in C$.

Lemma

The code C with the operation $\star$ is a group $(C, \star)$, called a propelinear structure on C.

There can exist many different propelinear structures on a given code (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

Propelinear code

Let C be a q-ary code of length n. The code is *propelinear* if there exists a mapping $x \to (\sigma_x, \pi_x)$, $(\sigma_x, \pi_x) \in Iso(C)$ such that:
(i) if the subgroup generated by $\{(\sigma_x, \pi_x) : x \in C\}$ acts transitively on the codewords of C. *(Then the code C is transitive)*
(ii) if the order of the subgroup generated by $\{(\sigma_x, \pi_x) : x \in C\}$ is $|C|$.

Define an operation $\star$: $x \star y = (\sigma_x; \pi_x)(y)$ for any $x, y \in C$.

Lemma

The code C with the operation $\star$ is a group $(C, \star)$, called a propelinear structure on C.

There can exist many different propelinear structures on a given code (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

Propelinear code

Let C be a q-ary code of length n. The code is *propelinear* if there exists a mapping $x \to (\sigma_x, \pi_x)$, $(\sigma_x, \pi_x) \in Iso(C)$ such that:
(i) if the subgroup generated by $\{(\sigma_x, \pi_x) : x \in C\}$ acts transitively on the codewords of C. *(Then the code C is transitive)*
(ii) if the order of the subgroup generated by $\{(\sigma_x, \pi_x) : x \in C\}$ is $|C|$.

Define an operation $\star$: $x \star y = (\sigma_x; \pi_x)(y)$ for any $x, y \in C$.

Lemma

The code C with the operation $\star$ is a group $(C, \star)$, called a propelinear structure on C.

There can exist many different propelinear structures on a given code (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

Propelinearity and transitivity

Q:

Does there exist transitive codes, that are not propelinear?

A:

Yes, the binary (10,40,4) Best code is a transitive nonpropelinear code (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

Propelinearity and transitivity

Q:

Does there exist transitive codes, that are not propelinear?

A:

Yes, the binary (10,40,4) Best code is a transitive nonpropelinear code (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

Propelinear codes: constructions

The class of propelinear codes includes linear, Z_2Z_4-linear and translation-invariant codes (Rifa, Pujol, 1997);

All 15 transitive perfect codes, obtained by one step switchings from Hamming code, classified by Malugin, are propelinear (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

The application of Plotkin, Vasiliev and Mollard constuctions (with proper functions) to propelinear codes yields propelinear codes (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

Propelinear codes: constructions

The class of propelinear codes includes linear, Z_2Z_4-linear and translation-invariant codes (Rifa, Pujol, 1997);

All 15 transitive perfect codes, obtained by one step switchings from Hamming code, classified by Malugin, are propelinear (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

The application of Plotkin, Vasiliev and Mollard constuctions (with proper functions) to propelinear codes yields propelinear codes (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

Propelinear codes: constructions

The class of propelinear codes includes linear, Z_2Z_4-linear and translation-invariant codes (Rifa, Pujol, 1997);

All 15 transitive perfect codes, obtained by one step switchings from Hamming code, classified by Malugin, are propelinear (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

The application of Plotkin, Vasiliev and Mollard constuctions (with proper functions) to propelinear codes yields propelinear codes (Borges, Mogilnykh, Rifa, Solovyeva, 2012).

Lower bounds on the number of propelinear extended perfect codes

Old lower bound

For $n = 2^m$, $m \geq 4$ the number of propelinear extended perfect codes is at least $\lfloor \log_2(n/2) \rfloor^2$.

New lower bound (main result of the talk)

We show that there exists at least $\frac{1}{8n^2\sqrt{3}} e^{\pi\sqrt{2n/3}}(1 + o(1))$ propelinear extended perfect codes.

Lower bounds on the number of propelinear extended perfect codes

Old lower bound

For $n = 2^m, m \geq 4$ the number of propelinear extended perfect codes is at least $\lfloor \log_2(n/2) \rfloor^2$.

New lower bound (main result of the talk)

We show that there exists at least $\frac{1}{8n^2\sqrt{3}} e^{\pi\sqrt{2n/3}}(1 + o(1))$ propelinear extended perfect codes.

Propelinear code

Propelinear code

C is *propelinear* if there exists a collection $\{(\sigma_x; \pi_x) : x \in C\}$ such that:

(i) *Code C is transitive:* The group generated by the set $\{(\sigma_x; \pi_x) : x \in C\}$ acts transitively on the codewords of C.

(ii) The order of the group generated by $\{(\sigma_x; \pi_x) : x \in C\}$ equals $|C|$.

Isotopic transitive and propelinear codes

Isotopic propelinear code

C is *isotopic propelinear* if there exists a collection $\{\sigma_x : x \in C\}$ such that:

(i) *Code C is isotopic transitive:* The group generated by the set $\{\sigma_x : x \in C\}$ acts transitively on the codewords of C.

(ii) The order of the group generated by $\{\sigma_x : x \in C\}$ equals $|C|$.

Phelps construction for extended perfect codes

Phelps construction

Let H be an extended binary Hamming code of length n,
M be a quaternary MDS code of length n,
$C_0^0, \dots, C_3^0$ ($C_0^1, \dots, C_3^1$) be a partition of even (odd) weight vectors of length 4 into extended perfect codes.
Then the code

$$\bigcup_{h_1 \dots h_n \in H} \bigcup_{a_1 \dots a_n \in M} C_{a_1}^{h_1} \times \dots \times C_{a_n}^{h_n}$$

is an extended binary perfect code of length $4n$.

Potapov transitive extended perfect codes and isotopic transitive codes

Theorem (Potapov 2006)

Let M be isotopic transitive MDS code. Then the Phelps code

$$\bigcup_{h_1 \dots h_n \in H} \bigcup_{a_1 \dots a_n \in M} C_{a_1}^{h_1} \times \dots \times C_{a_n}^{h_n}$$

is an transitive extended perfect code of length $4n$.

Theorem (Potapov 2006)

There exists at least $\frac{1}{4(n-1)\sqrt{3}} e^{\pi\sqrt{2(n-1)/3}}(1 + o(1))$ nonequivalent quaternary isotopic transitive MDS codes of length n, for n going to infinity.

Potapov transitive extended perfect codes and isotopic transitive codes

Theorem (Potapov 2006)

Let M be isotopic transitive MDS code. Then the Phelps code

$$\bigcup_{h_1 \ldots h_n \in H} \bigcup_{a_1 \ldots a_n \in M} C_{a_1}^{h_1} \times \ldots \times C_{a_n}^{h_n}$$

is an transitive extended perfect code of length $4n$.

Theorem (Potapov 2006)

There exists at least $\frac{1}{4(n-1)\sqrt{3}} e^{\pi\sqrt{2(n-1)/3}}(1 + o(1))$ nonequivalent quaternary isotopic transitive MDS codes of length n, for n going to infinity.

Potapov transitive extended perfect codes and isotopic transitive codes

Corollary (Potapov 2006)

There exist at least $\frac{1}{8n^2\sqrt{3}}e^{\pi\sqrt{2n/3}}(1+o(1))$ nonequivalent transitive extended perfect binary codes of length $4n$, for n going to infinity.

Main Result

Theorem

Let M be isotopic propelinear MDS code. Then the Phelps code

$$\bigcup_{h_1 \ldots h_n \in H} \bigcup_{a_1 \ldots a_n \in M} C_{a_1}^{h_1} \times \ldots \times C_{a_n}^{h_n}$$

is propelinear extended perfect code of length $4n$.

Theorem

There exists at least $\frac{1}{4(n-1)\sqrt{3}} e^{\pi\sqrt{2(n-1)/3}}(1+o(1))$ nonequivalent quaternary isotopic propelinear MDS codes of length n, for n going to infinity.

Main Result

Corollary 1

There exist at least $\frac{1}{8n^2\sqrt{3}}e^{\pi\sqrt{2n/3}}(1+o(1))$ nonequivalent propelinear extended perfect binary codes of length $4n$, for n going to infinity.

Corollary 2

Each one of a half of the codes has at least 2^{n-2} propelinear structures for fixed n.

Main Result

Corollary 1

There exist at least $\frac{1}{8n^2\sqrt{3}}e^{\pi\sqrt{2n/3}}(1+o(1))$ nonequivalent propelinear extended perfect binary codes of length $4n$, for n going to infinity.

Corollary 2

Each one of a half of the codes has at least 2^{n-2} propelinear structures for fixed n.

Conclusion

The concept of propelinear codes is extended to the codes over arbitrary field.

Showed that any transitive Potapov code is propelinear
(A new exponential bound for the number of propelinear extended perfect codes).

A half of the codes has many (exponent of n) propelinear structures.