Completely regular codes with different parameters and the same intersection arrays

Josep C. Rifà [1], Victor A. Zinoviev [2]

[1]**Universitat Autònoma de Barcelona, Spain**

[2]**Harkevich Institute for Problems of Information Transmission, Moscow, Russia**

**International Workshop:
Algebraic and Combinatorial Coding Theory
(ACCT-2016).
Albena, Bulgaria, June 18-24, 2016**

Outline

Summary

We obtain several classes of completely regular codes with different parameters, but identical intersection array.

Summary

We obtain several classes of completely regular codes with different parameters, but identical intersection array. Given a prime power q and any two natural numbers a, b, we construct completely transitive codes over different fields with covering radius $\rho = \min\{a, b\}$ and identical intersection array, specifically, one code over $\mathbb{F}_{q^r}$ for each divisor r of a or b.

Introduction

Let $\mathbb{F}_q$ be a finite field of the order q and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. A q-ary linear code C of length n is a k-dimensional subspace of $\mathbb{F}_q^n$.

Introduction

Let $\mathbb{F}_q$ be a finite field of the order q and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. A q-ary linear code C of length n is a k-dimensional subspace of $\mathbb{F}_q^n$. Given any vector $\boldsymbol{v} \in \mathbb{F}_q^n$, its *distance to the code* C is $d(\boldsymbol{v}, C) = \min_{\boldsymbol{x} \in C}\{d(\boldsymbol{v}, \boldsymbol{x})\}$, and the *covering radius* of the code C is $\rho = \max_{\boldsymbol{v} \in \mathbb{F}_q^n}\{d(\boldsymbol{v}, C)\}$.

Introduction

Let $\mathbb{F}_q$ be a finite field of the order q and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. A q-ary linear code C of length n is a k-dimensional subspace of $\mathbb{F}_q^n$. Given any vector $\boldsymbol{v} \in \mathbb{F}_q^n$, its *distance to the code* C is $d(\boldsymbol{v}, C) = \min_{\boldsymbol{x} \in C}\{d(\boldsymbol{v}, \boldsymbol{x})\}$, and the *covering radius* of the code C is $\rho = \max_{\boldsymbol{v} \in \mathbb{F}_q^n}\{d(\boldsymbol{v}, C)\}$. We say that C is a $[n, k, d; \rho]_q$-code. Let $D = C + \boldsymbol{x}$ be a *coset* of C, where $+$ means the component-wise addition in $\mathbb{F}_q$.

Introduction

For a given q-ary code C with covering radius $\rho = \rho(C)$ define

$$C(i) \ = \ \{\boldsymbol{x} \in \mathbb{F}_q^n : \ d(\boldsymbol{x}, C) = i\}, \ \ i = 1, 2, ..., \rho.$$

Introduction

For a given q-ary code C with covering radius $\rho = \rho(C)$ define

$$C(i) \ = \ \{\boldsymbol{x} \in \mathbb{F}_q^n : \ d(\boldsymbol{x}, C) = i\}, \ \ i = 1, 2, ..., \rho.$$

Say that two vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ are *neighbors* if $d(\boldsymbol{x}, \boldsymbol{y}) = 1$.

Introduction

Definition 1.

(Neumaier, 1992) A $q$ary code C is completely regular, if for all $l \geq 0$ every vector $x \in C(l)$ has the same number c_l of neighbors in $C(l-1)$ and the same number b_l of neighbors in $C(l+1)$.

Introduction

Definition 1.

(Neumaier, 1992) A $q$ary code C is completely regular, if for all $l \geq 0$ every vector $x \in C(l)$ has the same number c_l of neighbors in $C(l-1)$ and the same number b_l of neighbors in $C(l+1)$. Define $a_l = (q-1)n - b_l - c_l$ and $c_0 = b_\rho = 0$.

Introduction

Definition 1.

(Neumaier, 1992) A $q$ary code C is completely regular, if for all $l \geq 0$ every vector $x \in C(l)$ has the same number c_l of neighbors in $C(l-1)$ and the same number b_l of neighbors in $C(l+1)$. Define $a_l = (q-1)n - b_l - c_l$ and $c_0 = b_\rho = 0$. Denote by $(b_0, \ldots, b_{\rho-1}; c_1, \ldots, c_\rho)$ the intersection array of C.

Introduction

The group $\mathrm{Aut}(C)$ acts on the set of cosets of C in the following way: for all $\sigma \in \mathrm{Aut}(C)$ and for every vector $\boldsymbol{v} \in \mathbb{F}_q^n$ we have $(\boldsymbol{v} + C)^\sigma = \boldsymbol{v}^\sigma + C$.

Definition 2.

(Sole, 1990; Giudici-Praeger, 1999) Let C be a linear code over $\mathbb{F}_q$ with covering radius ρ. Then C is completely transitive if $\mathrm{Aut}(C)$ has $\rho + 1$ orbits when acts on the cosets of C.

Since two cosets in the same orbit should have the same weight distribution, it is clear, that any completely transitive code is completely regular.

Introduction

In (Rifà-Zinoviev, 2010) we described an explicit construction, based on the Kronecker product of parity check matrices, which provides, for any natural number ρ and for any prime power q, an infinite family of q-ary linear completely regular codes with covering radius ρ.

Introduction

In (Rifà-Zinoviev, 2010) we described an explicit construction, based on the Kronecker product of parity check matrices, which provides, for any natural number ρ and for any prime power q, an infinite family of q-ary linear completely regular codes with covering radius ρ. In (Rifà-Zinoviev, 2011) we presented another class of q-ary linear completely regular codes with the same property, based on lifting of perfect codes.

Introduction

In (Rifà-Zinoviev, 2010) we described an explicit construction, based on the Kronecker product of parity check matrices, which provides, for any natural number ρ and for any prime power q, an infinite family of q-ary linear completely regular codes with covering radius ρ. In (Rifà-Zinoviev, 2011) we presented another class of q-ary linear completely regular codes with the same property, based on lifting of perfect codes. Here we extend the Kronecker product construction to the case when component codes have different alphabets and connect the resulting completely regular codes with codes obtained by lifting q-ary perfect codes.

Introduction

In (Rifà-Zinoviev, 2010) we described an explicit construction, based on the Kronecker product of parity check matrices, which provides, for any natural number ρ and for any prime power q, an infinite family of q-ary linear completely regular codes with covering radius ρ. In (Rifà-Zinoviev, 2011) we presented another class of q-ary linear completely regular codes with the same property, based on lifting of perfect codes. Here we extend the Kronecker product construction to the case when component codes have different alphabets and connect the resulting completely regular codes with codes obtained by lifting q-ary perfect codes. This gives several different infinite classes of completely regular codes with different parameters and with identical intersection arrays.

Preliminary results

Definition 3.

For two matrices $A = [a_{r,s}]$ and $B = [b_{i,j}]$ over $\mathbb{F}_q$ define a new matrix H which is the Kronecker product $H = A \otimes B$, where H is obtained by changing any element $a_{r,s}$ in A by the matrix $a_{r,s}B$.

Preliminary results

Definition 3.

For two matrices $A = [a_{r,s}]$ and $B = [b_{i,j}]$ over $\mathbb{F}_q$ define a new matrix H which is the Kronecker product $H = A \otimes B$, where H is obtained by changing any element $a_{r,s}$ in A by the matrix $a_{r,s}B$.

Definition 4.

Let C be the $[n, k, d]_q$ code with parity check matrix H where $1 \leq k \leq n-1$ and $d \geq 3$. Denote by C_r the $[n, k, d]_{q^r}$ code over $\mathbb{F}_{q^r}$ with the same parity check matrix H. Say that code C_r is obtained by lifting C to $\mathbb{F}_{q^r}$.

Preliminary results

Denote by $C(H)$ the code defined by the parity check matrix H.

Preliminary results

Denote by $C(H)$ the code defined by the parity check matrix H. By H_m^q we denote the parity check matrix of the q-ary Hamming $[n, n-m, 3]_q$ code $C = C(H_m^q)$ of length $n = (q^m - 1)/(q-1)$.

Preliminary results

Denote by $C(H)$ the code defined by the parity check matrix H. By H_m^q we denote the parity check matrix of the q-ary Hamming $[n, n-m, 3]_q$ code $C = C(H_m^q)$ of length $n = (q^m - 1)/(q - 1)$. By $C_r(H_m^q)$ we denote the code (of the same length $n = (q^m - 1)/(q - 1)$) obtained by lifting $C(H_m^q)$ to the field $\mathbb{F}_{q^r}$.

Preliminary results

Denote by $C(H)$ the code defined by the parity check matrix H. By H_m^q we denote the parity check matrix of the q-ary Hamming $[n, n-m, 3]_q$ code $C = C(H_m^q)$ of length $n = (q^m - 1)/(q-1)$. By $C_r(H_m^q)$ we denote the code (of the same length $n = (q^m - 1)/(q-1)$) obtained by lifting $C(H_m^q)$ to the field $\mathbb{F}_{q^r}$. The following statement generalizes the results in (Rifa-Zinoviev, 2010; Rifa-Zinoviev, 2011).

Preliminary results

Denote by $C(H)$ the code defined by the parity check matrix H. By H^q_m we denote the parity check matrix of the q-ary Hamming $[n, n-m, 3]_q$ code $C = C(H^q_m)$ of length $n = (q^m - 1)/(q-1)$. By $C_r(H^q_m)$ we denote the code (of the same length $n = (q^m - 1)/(q-1)$) obtained by lifting $C(H^q_m)$ to the field $\mathbb{F}_{q^r}$. The following statement generalizes the results in (Rifa-Zinoviev, 2010; Rifa-Zinoviev, 2011).
Let $C(H^{q^u}_{m_a})$ and $C(H^q_{m_b})$ be two Hamming codes with parameters $[n_a, n_a - m_a, 3]_{q^u}$ and $[n_b, n_b - m_b, 3]_q$, respectively, where $n_a = (q^{u\,m_a} - 1)/(q^u - 1)$, $n_b = (q^{m_b} - 1)/(q-1)$, q is a prime power, $m_a, m_b \geq 2$, and $u \geq 1$.

Preliminary results

Theorem 5.

(i) The code C *with parity check matrix* $H = H^{q^u}_{m_a} \otimes H^q_{m_b}$*, the Kronecker product of* $H^{q^u}_{m_a}$ *and* $H^q_{m_b}$*, is a completely transitive, and so completely regular,* $[n, k, d; \rho]_{q^u}$ *code with parameters*

$$n = n_a\, n_b, \quad k = n - m_a\, m_b, \quad d = 3, \quad \rho = \min\{u\, m_a,\ m_b. \qquad (1)$$

Preliminary results

Theorem 5.

(i) The code C *with parity check matrix* $H = H^{q^u}_{m_a} \otimes H^{q}_{m_b}$, *the Kronecker product of* $H^{q^u}_{m_a}$ *and* $H^{q}_{m_b}$, *is a completely transitive, and so completely regular,* $[n,k,d;\rho]_{q^u}$ *code with parameters*

$$n = n_a\, n_b, \quad k = n - m_a\, m_b, \quad d = 3, \quad \rho = \min\{u\, m_a,\ m_b. \qquad (1)$$

(ii) The code C *has the intersection numbers:*

$$b_\ell \;=\; \frac{(q^{u\, m_a} - q^\ell)(q^{m_b} - q^\ell)}{(q-1)}, \quad c_\ell \;=\; q^{\ell-1}\frac{q^\ell - 1}{q-1}.$$

Preliminary results

Theorem 5.

(i) The code C *with parity check matrix* $H = H^{q^u}_{m_a} \otimes H^q_{m_b}$, *the Kronecker product of* $H^{q^u}_{m_a}$ *and* $H^q_{m_b}$, *is a completely transitive, and so completely regular,* $[n, k, d; \rho]_{q^u}$ *code with parameters*

$$n = n_a n_b, \quad k = n - m_a m_b, \quad d = 3, \quad \rho = \min\{u\, m_a,\; m_b. \qquad (1)$$

(ii) The code C *has the intersection numbers:*

$$b_\ell = \frac{(q^{u\, m_a} - q^\ell)(q^{m_b} - q^\ell)}{(q-1)}, \quad c_\ell = q^{\ell-1}\frac{q^\ell - 1}{q-1}.$$

(iii) The lifted code $C_{m_b}(H^q_{um_a})$ *is a completely regular code with the same intersection array as* C.

Main results

Theorem 6.

Let q be a prime number and a, b, u natural numbers. Then:

Main results

Theorem 6.

Let q be a prime number and a, b, u natural numbers. Then:
(i) There exist the following completely regular codes with different parameters $[n, k, d; \rho]_{q^r}$, where $d = 3$ and $\rho = \min\{ua, b\}$:

Main results

Theorem 6.

Let q be a prime number and a, b, u natural numbers. Then:
(i) There exist the following completely regular codes with different parameters $[n, k, d; \rho]_{q^r}$, where $d = 3$ and $\rho = \min\{ua, b\}$:
$C_{ua}(H_b^q)$ *over* $\mathbb{F}_q^{ua}$ *with* $n = \frac{q^b-1}{q-1},\ k = n - b;$

Main results

Theorem 6.

Let q be a prime number and a, b, u natural numbers. Then:
(i) There exist the following completely regular codes with different parameters $[n, k, d; \rho]_{q^r}$, where $d = 3$ and $\rho = \min\{ua, b\}$:
$C_{ua}(H_b^q)$ *over* $\mathbb{F}_q^{ua}$ *with* $n = \frac{q^b-1}{q-1}$, $k = n - b$;
$C_b(H_{ua}^q)$ *over* $\mathbb{F}_q^b$ *with* $n = \frac{q^{ua}-1}{q-1}$, $k = n - ua$;

Main results

Theorem 6.

Let q be a prime number and a, b, u natural numbers. Then:
(i) There exist the following completely regular codes with different parameters $[n, k, d; \rho]_{q^r}$, where $d = 3$ and $\rho = \min\{ua, b\}$:
$C_{ua}(H_b^q)$ *over* $\mathbb{F}_q^{ua}$ *with* $n = \frac{q^b-1}{q-1}$, $k = n - b$;
$C_b(H_{ua}^q)$ *over* $\mathbb{F}_q^b$ *with* $n = \frac{q^{ua}-1}{q-1}$, $k = n - ua$;
$C(H_b^q \otimes H_{ua}^q)$ *over* $\mathbb{F}_q$ *with* $n = \frac{q^{ua}-1}{q-1} \times \frac{q^b-1}{q-1}$, $k = n - bua$;

Main results

Theorem 6.

Let q be a prime number and a, b, u natural numbers. Then:
(i) There exist the following completely regular codes with different parameters $[n, k, d; \rho]_{q^r}$, where $d = 3$ and $\rho = \min\{ua, b\}$:

$C_{ua}(H_b^q)$ *over* $\mathbb{F}_q^{ua}$ *with* $n = \frac{q^b-1}{q-1},\ k = n - b;$
$C_b(H_{ua}^q)$ *over* $\mathbb{F}_q^b$ *with* $n = \frac{q^{ua}-1}{q-1},\ k = n - ua;$
$C(H_b^q \otimes H_{ua}^q)$ *over* $\mathbb{F}_q$ *with* $n = \frac{q^{ua}-1}{q-1} \times \frac{q^b-1}{q-1},\ k = n - bua;$
$C(H_b^q \otimes H_u^{q^a})$ *over* $\mathbb{F}_q^a$ *with* $n = \frac{q^b-1}{q-1} \times \frac{q^{ua}-1}{q^u-1},\ k = n - bu;$

Main results

Theorem 6.

Let q be a prime number and a, b, u natural numbers. Then:
(i) There exist the following completely regular codes with different parameters $[n, k, d; \rho]_{q^r}$, where $d = 3$ and $\rho = \min\{ua, b\}$:

$C_{ua}(H_b^q)$ *over* $\mathbb{F}_q^{ua}$ *with* $n = \frac{q^b-1}{q-1},\ k = n - b;$

$C_b(H_{ua}^q)$ *over* $\mathbb{F}_q^b$ *with* $n = \frac{q^{ua}-1}{q-1},\ k = n - ua;$

$C(H_b^q \otimes H_{ua}^q)$ *over* $\mathbb{F}_q$ *with* $n = \frac{q^{ua}-1}{q-1} \times \frac{q^b-1}{q-1},\ k = n - bua;$

$C(H_b^q \otimes H_u^{q^a})$ *over* $\mathbb{F}_q^a$ *with* $n = \frac{q^b-1}{q-1} \times \frac{q^{ua}-1}{q^u-1},\ k = n - bu;$

$C(H_b^q \otimes H_a^{q^u})$ *over* $\mathbb{F}_q^u$ *with* $n = \frac{q^b-1}{q-1} \times \frac{q^{ua}-1}{q^u-1},\ k = n - ba;$

Main results

Theorem 6.

Let q be a prime number and a, b, u natural numbers. Then:
(i) There exist the following completely regular codes with different parameters $[n, k, d; \rho]_{q^r}$, where $d = 3$ and $\rho = \min\{ua, b\}$:
$C_{ua}(H_b^q)$ *over* $\mathbb{F}_q^{ua}$ *with* $n = \frac{q^b-1}{q-1},\ k = n - b;$
$C_b(H_{ua}^q)$ *over* $\mathbb{F}_q^b$ *with* $n = \frac{q^{ua}-1}{q-1},\ k = n - ua;$
$C(H_b^q \otimes H_{ua}^q)$ *over* $\mathbb{F}_q$ *with* $n = \frac{q^{ua}-1}{q-1} \times \frac{q^b-1}{q-1},\ k = n - bua;$
$C(H_b^q \otimes H_u^{q^a})$ *over* $\mathbb{F}_q^a$ *with* $n = \frac{q^b-1}{q-1} \times \frac{q^{ua}-1}{q^u-1},\ k = n - bu;$
$C(H_b^q \otimes H_a^{q^u})$ *over* $\mathbb{F}_q^u$ *with* $n = \frac{q^b-1}{q-1} \times \frac{q^{ua}-1}{q^u-1},\ k = n - ba;$

Main results

Theorem 6 (continuation)
(ii) All the above codes have the same intersection numbers

$$b_\ell = \frac{(q^b - q^\ell)(q^{ua} - q^\ell)}{(q-1)}, \ \ell = 0, \ldots, \rho{-}1, \ \ c_\ell = q^{\ell-1}\frac{q^\ell - 1}{q-1}, \ \ell = 1, \ldots, \rho$$

Main results

Theorem 6 (continuation)
(ii) All the above codes have the same intersection numbers

$$b_\ell = \frac{(q^b - q^\ell)(q^{ua} - q^\ell)}{(q-1)}, \ \ell = 0, \ldots, \rho{-}1, \ \ c_\ell = q^{\ell-1}\frac{q^\ell - 1}{q-1}, \ \ell = 1, \ldots, \rho$$

(iii) All codes above coming from Kronecker constructions are completely transitive.

Distance-regular graphs

Let Γ be a finite connected simple graph (i.e., undirected, without loops and multiple edges). Let $d(\gamma, \delta)$ be the distance between two vertices γ and δ (i.e., the number of edges in the minimal path between γ and δ). The *diameter* D of Γ is its largest distance. Two vertices γ and δ from Γ are *neighbors* if $d(\gamma, \delta) = 1$. Define

$$\Gamma_i(\gamma) \;=\; \{\delta \in \Gamma : \; d(\gamma, \delta) = i\}.$$

An *automorphism* of a graph Γ is a permutation π of the vertex set of Γ such that, for all $\gamma, \delta \in \Gamma$ we have $d(\gamma, \delta) = 1$ if and only if $d(\pi\gamma, \pi\delta) = 1$.

Distance-regular graphs

Definition 7.

Brouwer-Cohen-Neumaier, 1989) A simple connected graph Γ is called *distance-regular* if it is regular of valency k, and if for any two vertices $\gamma, \delta \in \Gamma$ at distance i apart, there are precisely c_i neighbors of δ in $\Gamma_{i-1}(\gamma)$ and b_i neighbors of δ in $\Gamma_{i+1}(\gamma)$. Furthermore, this graph is called *distance-transitive*, if for any pair of vertices γ, δ at distance $d(\gamma, \delta)$ there is an automorphism π from $\mathrm{Aut}(\Gamma)$ which moves this pair (γ, δ) to any other given pair γ', δ' of vertices at the same distance $d(\gamma, \delta) = d(\gamma', \delta')$.

Distance-regular graphs

Let C be a linear completely regular code with covering radius ρ and intersection array $(b_0, \ldots, b_{\rho-1}; c_1, \ldots c_\rho)$. Let $\{B\}$ be the set of cosets of C. Define the graph Γ_C, which is called the *coset graph of* C, taking all different cosets $B = C + \mathbf{x}$ as vertices, with two vertices $\gamma = \gamma(B)$ and $\gamma' = \gamma(B')$ adjacent if and only if the cosets B and B' contain neighbor vectors, i.e., there are $\mathbf{v} \in B$ and $\mathbf{v}' \in B'$ such that $d(\mathbf{v}, \mathbf{v}') = 1$.

Distance-regular graphs

Lemma 8.

(Brouwer-Cohen-Neumaier, 1989; Rifà-Pujol, 1991) Let C *be a linear completely regular code with covering radius* ρ *and intersection array* $(b_0, \ldots, b_{\rho-1}; c_1, \ldots c_\rho)$ *and let* Γ_C *be the coset graph of* C*. Then* Γ_C *is distance-regular of diameter* $D = \rho$ *with the same intersection array. If* C *is completely transitive, then* Γ_C *is distance-transitive.*

Distance-regular graphs

Theorem 9.

Let C_1, C_2, ..., C_k be a family of linear completely transitive codes constructed by Theorem 5 and let $\Gamma_{C_1}, \Gamma_{C_2}, \ldots, \Gamma_{C_k}$ be their corresponding coset graphs. Then:
(i) Any graph Γ_{C_i} is a distance-transitive graph, induced by bilinear forms.
(ii) If any two codes C_i and C_j have the same intersection array, then the graphs Γ_{C_i} and Γ_{C_j} are isomorphic.
(iii) If the graph Γ_{C_i} has q^m vertices, where m is not a prime, then it can be presented as a coset graph by several different ways, depending on the number of factors of m.

References

A.E. Brouwer, A.M. Cohen, A. Neumaier, Distance-Regular Graphs, ed., Springer, Berlin, 1989.

P. Delsarte, Bilinear forms over a finite field with applications to coding theory, Journal of Combinatorial Theory, Series A, 25 (1978) 226-241.

M. Giudici, C.E. Praeger, Completely Transitive Codes in Hamming Graphs, Europ. J. Combinatorics 20 (1999) 647–662.

A. Neumaier, Completely regular codes, Discrete Maths., 106/107 (1992) 335-360.

References

J. Rifà, J. Pujol, Completely transitive codes and distance-transitive graphs, in: Proc. 9th International Conference, AAECC-9, in: LNCS, vol. 539, 1991,

J. Rifà, V.A. Zinoviev, New completely regular q-ary codes, based on Kronecker products, IEEE Transactions on Information Theory, 56.1 (2010) 266-272.

J. Rifà, V.A. Zinoviev, On lifting perfect codes, IEEE Transactions on Information Theory, 57.9 (2011) 5918-5925.

P. Solé, "Completely Regular Codes and Completely Transitive Codes," *Discrete Maths.*, vol. 81, pp. 193-201, 1990.