Subcodes of Reed-Solomon code with special properties

Alexander A. Davydov, Victor V. Zyablov, Rustam E. Kalimullin

adav@iitp.ru, zyablov@iitp.ru, rustamka@iitp.ru

Institute for Information Transmission Problems

Russian Academy of Sciences

Moscow, B. Karetny per. 19, Russia

Literature

W. Chu, C. J. Colbourn, P. J. Dukes,
"Permutation codes for powerline communication,"
Des. Codes Crypt., **32**, 51–64, 2004

P. Frankl, M. Deza,
"On the maximum number of permutations with given maximal or minimal distance,"
J. Combin. Theory Ser. A, **22**, 352–360, 1977

T. Tao, V. Vu, *Additive Combinatorics*,
Cambridge Univ. Press, New-York, 2006

A-codes & permutation codes

A-word - *symbols* on all positions are *distinct*

A-subcode - code subset, consisting of A-words

A-code - all codewords are A-words

Permutation code (**Permutation array**)
codeword $\Leftrightarrow$ a permutation of code alphabet

$(n, M, d)_Q$ code, n - length, Q - alphabet size

A-code $n \leq Q$

Permutation code $n = Q$

$$(Q, M, d)_Q \longrightarrow (Q - t, M, d - t)_Q$$

shortening (puncturing)

Terminology

A-code = Repetition free code

RF-code

RF-subcode

$[n, k, n-k+1]_q$ RS codes, $k = 2, 3$

L_u - a location of the u-th position, $L_i \neq L_j$ if $i \neq j$

Generating matrices $n \leq q + b$

$$G = \begin{bmatrix} 1 & 1 \dots & 1 \\ L_1 & L_2 \dots & L_n \\ L_1^2 & L_2^2 \dots & L_n^2 \end{bmatrix}, \qquad b = 0$$

$$G = \begin{bmatrix} L_1^{-1} & L_2^{-1} \dots & L_n^{-1} \\ 1 & 1 \quad \dots & 1 \\ L_1 & L_2 \quad \dots & L_n \end{bmatrix}, \quad b = -1$$

Goal of this work

$M_q^{(b)}(n, n-k+1)$ - maximal possible cardinality of A-subcode of $[n, k, n-k+1]_q$ RS code. $b = 0, -1$

To estimate the values $M_q^{(b)}(n, n-k+1)$ for $k = 2, 3$ and distinct n and q

To obtain RS codes having maximal, by possibility, cardinality of an A-subcode

We study *special combinatorial properties* of *Reed-Solomon codes* and try to optimize them

Main results. Exact values

A-subcodes of any $[n, 2, n-1]_q$ RS codes, $k = 2$

$M_q^{(b)}(n, n-1) = q(q-1)$ for all n

A-subcodes of long $[n, 3, n-2]_q$ RS codes, $k = 3$

$$\left\lfloor \frac{q+1}{2} \right\rfloor < n \leq q + b$$

$M_q^{(-1)}(n, n-2) = 2q(q-1)$, arbitrary q

$M_q^{(0)}(n, n-2) = 2q(q-1)$, even q

$M_q^{(0)}(n, n-2) = q(q-1)$, odd q

Main results. Lower estimates

$(n, M, n-2)_q$ **A-subcodes of short** $[n, 3, n-2]_q$

RS codes. $n \leq \left\lfloor \frac{q+1}{2} \right\rfloor$

$$\mathbf{M = (q + c - n)q(q - 1)}, \quad c = 1, 2 \qquad (!)$$

$n|(q-1)$ if $b = -1$. $n|q$ if $b = 0$

$$M = (q + 1 - \xi n)q(q-1), \;\; \xi \geq \tfrac{p}{p-1}, \;\; q = p^m$$

$$M = (q + 3 - 2n + \Delta)q(q-1), \;\; 0 \leq \Delta \leq \tfrac{n}{2}$$

Comparison. Permutation codes

$(n, M, n-2)_q$ A-subcodes of RS codes

vs shortened permutation codes (SPC)

1. Cardinalities of A-subcodes are **greater** :

$q-1$ is *not* a prime power

RS $(q+2-n)q(q-1) \Rightarrow 2q(q-1)$ SPC $n \leq \frac{q+1}{2}$

RS $2q(q-1) \Rightarrow q(q-1)$ SPC $n > \frac{q+1}{2}$

2. Cardinalities of A-subcodes are **smaller** :

$q-1$ is a prime power

RS $(q+2-n)q(q-1) \Leftarrow q(q-1)(q-2)$ SPC

P. Frankl, M. Deza 1977

Bunches of code words

$[n, k, d]_q$ code $\mathcal{C}$. $u = (1, \ldots, 1) \in \mathcal{C}$

Bunch $\mathcal{B} = \{\lambda c + \gamma u : \lambda \in F_q^*, \gamma \in F_q, c \in \mathcal{C}\}$

c - **basic word** of the bunch

$c = (f(L_1), f(L_2), ..., f(L_n))$

$f(x)$ - **basic polynomial** of the bunch is the information polynomial of the basic word

$b = 0 \quad \rightarrow f(x) = x^2 + a_1 x$ or $f(x) = x$

$b = -1 \rightarrow f(x) = x + a_{-1} x^{-1}$ or $f(x) = x^{-1}$

$a_i \in F_q$

Repeating compositon of vectors

c - word of length n

s_j - the number of the alphabet symbols repeating in the word j times, $j = 0, 1, \ldots, n$

$$\mathrm{comprep}(c) = (s_0,\ s_1,\ s_2, \ldots)$$

Theorem 1. All words of a bunch have the same repeating composition

4 types of code words and bunches with distinct repeating compositions: A, B, C, D $\quad s_j = 0,\ j \geq 3$

B-word c : $\mathrm{comprep}(c) = \left(\frac{1}{2}q, 0, \frac{1}{2}q\right)$

Conditions

Lemma 4. Let the basic polynomials of a bunch be

$$b = 0 \quad \Rightarrow \quad f(x) = x^2 + a_1 x$$

$$b = -1 \quad \Rightarrow \quad f(x) = x + a_{-1} x^{-1}$$

Then in the basic word of this bunch, symbols on *distinct* positions with locations L and T are the same,

i.e. $f(L) = f(T)$ for $L \neq T$, iff

$$b = 0 \quad \Rightarrow \quad L + T = -a_1$$

$$b = -1 \quad \Rightarrow \quad LT = a_{-1}$$

Assignment of locations

$\Lambda_n = \{L_1, L_2, \ldots, L_n\}$ - set of locations

$$\Sigma_n = \{L + T : L, T \in \Lambda_n, L \neq T\}$$

- set of sums of *distinct* locations

$$\Pi_n = \{LT : L, T \in \Lambda_n, L \neq T\}$$

- set of products of *distinct* locations

Lemma 5. B-,C- or D-bunch of a non shortened RS code becomes an A-bunch of the shortened code iff

$b = 0 \quad \Rightarrow \quad -a_1 \in F_q \setminus \Sigma_n$

$b = -1 \quad \Rightarrow \quad a_{-1} \in F_q^* \setminus \Pi_n$

$|\Sigma_n|, \ |\Pi_n|$ - **additive combinatorics problem**

Locations as subgroups. $b = 0$

$(n, M, n-2)_q$ A-subcode of RS code

$$M = (q + 1 - |\Sigma_n|)q(q-1)$$

$$q = p^m, \;\; n = p^{m-v}, \;\; n|q$$

Λ_n is an **additive subgroup** of F_q

q odd $\rightarrow |\Sigma n| = n$. $\quad q$ even $\rightarrow |\Sigma_n| = n - 1$

$$\mathbf{M} = (\mathbf{q} + \mathbf{c} - \mathbf{n})\mathbf{q}(\mathbf{q} - \mathbf{1}), \quad c = 1, 2 \qquad (!)$$

Locations as subgroups. $b = -1$

$(n, M, n-2)_q$ A-subcode of RS code

$M = (q + 1 - |\Pi_n|)q(q-1)$

$n|(q-1)$

Λ_n is a **multiplicative subgroup** of F_q^*

$\Pi_n = \Lambda_n$. $\quad |\Pi_n| = n$

$$\mathbf{M = (q + 1 - n)q(q-1)} \qquad (!)$$

Thank you   Spasibo

Mille grazie

Premnogo blagodarya

¡Muchas gracias

Toda raba

Merci beaucoup

Dankeschön

Dank u wel

Domo arigato