ISSN 0032-9460, Problems of Information Transmission, 2010, Vol. 46, No. 4, pp. 321–345. © Pleiades Publishing, Inc., 2010.
Original Russian Text © A.A. Davydov, V.V. Zyablov, R.E. Kalimullin, 2010, published in Problemy Peredachi Informatsii, 2010, Vol. 46, No. 4, pp. 56–82.

CODING THEORY

Special Sequences as Subcodes of Reed–Solomon Codes

A. A. Davydov, V. V. Zyablov, and R. E. Kalimullin

Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow
adav@iitp.ru zyablov@iitp.ru rustamka@iitp.ru

Received April 8, 2010; in final form, August 16, 2010

Abstract—We consider sequences in which every symbol of an alphabet occurs at most once. We construct families of such sequences as nonlinear subcodes of a q-ary $[n, k, n-k+1]_q$ Reed–Solomon code of length $n \le q$ consisting of words that have no identical symbols. We introduce the notion of a bunch of words of a linear code. For dimensions $k \le 3$ we obtain constructive lower estimates (tight bounds in a number of cases) on the maximum cardinality of a subcode for various n and q, and construct subsets of words meeting these estimates and bounds. We define codes with words that have no identical symbols, observe their relation to permutation codes, and state an optimization problem for them.

DOI: 10.1134/S0032946010040046

1. INTRODUCTION

In a number of real-world systems, such as broadband systems [1] and data transmission systems in powerline communications [2], it is required to construct sequences in which any symbol of an alphabet occurs at most once and at the same time the sequences differ from each other in a maximum possible number of symbols. We consider the possibility of solving this problem with the help of Reed–Solomon (RS) codes.

Let q be a prime or a power of a prime. Denote by $\mathbb{F}_q$ the Galois field of q elements. Let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Denote by $\mathbb{F}_q[x]$ the polynomial ring over $\mathbb{F}_q$. Let $[n, k, d]_q$ be a linear code over $\mathbb{F}_q$ of length n and dimension k with minimum distance d. We denote by $(n, M, d)_Q$ a nonlinear code of length n and cardinality M with minimum distance d defined over an arbitrary alphabet of size Q.

Definition 1. A vector is called an *A-word* if its symbols in all positions are different. A subset of a code consisting of A-words is called an *A-subcode*. A code is said to be an *A-code* if all its codewords are A-words. An A-code will also be referred to as a *repetition-free code*.

Recall that an $(n, M, d)_n$ *permutation code* is defined over an arbitrary alphabet of n symbols [2, 3]. Each word of a permutation code is some permutation of the alphabet. The set of codewords of an $(n, M, d)_n$ permutation code is called a permutation array and is denoted by $(n, d)PA$ or $(n, M, d)PA$. Also, the notation $PA(n, d)$ is used. Permutation codes belong to a wider class of constant-composition codes, whose words contain each symbol of an alphabet a given number of times. Definition 1 implies that an $(n, M, d)_Q$ A-code is a permutation code if and only if $n = Q$.

In data transmission, using A-codes with large cardinalities and distances often happens to be helpful. For permutation codes (whose length equals the alphabet size), the problem was posed in the literature of increasing the cardinality for given length and distance [2, 3]. In the present paper this problem is naturally generalized so that the length of an optimized A-code can be less than the alphabet size.

Open problem. *Estimate $M_Q^{\mathrm{A}}(n,d)$, the maximum possible cardinality of an A-code of length n with minimum distance d over an alphabet of size Q. Construct A-codes with large cardinalities and distances for fixed n and Q.*

To construct "good" A-codes, it is natural to use A-subcodes of maximum-distance separable (MDS) codes. In the present paper we consider A-subcodes of an RS code. An advantage of this approach is, in particular, that *encoding/decoding algorithms for RS codes* are developed and well studied.

In Sections 4–8 we consider the $[n,k,n-k+1]_q$ *extended* RS code of length $n \le q$.

Denote the location of the uth position of a codeword by L_u, where $u = 1,2,\dots,n$, $L_u \in \mathbb{F}_q$, $L_u \ne L_y$ for $u \ne y$. In an extended code, the location 0 can be used (see [4]). A codeword c of an extended RS code is given by an *information polynomial*

$$f(x) = \sum_{i=0}^{k-1} a_i x^i \in \mathbb{F}_q[x], \quad a_i \in \mathbb{F}_q. \tag{1.1}$$

The coefficients a_i are information symbols. A word c is of the form (see [4])

$$\begin{gathered} c = (c_1, c_2, \dots, c_n) = (f(L_1), f(L_2), \dots, f(L_n)), \\ c_u = f(L_u), \quad u = 1,2,\dots,n. \end{gathered} \tag{1.2}$$

This encoding is nonsystematic. The generator matrix G of the extended $[n,k,n-k+1]_q$ RS code with encoding (1.1) and (1.2) can be written in the form

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ L_1 & L_2 & \dots & L_n \\ L_1^2 & L_2^2 & \dots & L_n^2 \\ \dots & \dots & \dots & \dots \\ L_1^{k-1} & L_2^{k-1} & \dots & L_n^{k-1} \end{pmatrix}, \quad n \le q, \quad L_u \in \mathbb{F}_q, \quad L_u \ne L_y \text{ for } u \ne y. \tag{1.3}$$

There are other constructions of RS codes (see, e.g., [4–7] and bibliography therein). Here is a variant of the generator matrix:

$$G = \begin{pmatrix} L_1^b & L_2^b & \dots & L_n^b \\ L_1^{b+1} & L_2^{b+1} & \dots & L_n^{b+1} \\ \dots & \dots & \dots & \dots \\ L_1^{b+k-1} & L_2^{b+k-1} & \dots & L_n^{b+k-1} \end{pmatrix}, \quad 1 \le b \le q-2, \quad n \le q-1, \quad L_u \in \mathbb{F}_q^*. \tag{1.4}$$

The code (1.4) is *nonextended*; the location 0 is not used. The matrix (1.3) can be obtained from (1.4) by setting $b = 0$, $L_u \in \mathbb{F}_q$, assuming that $0^0 = 1$.

Let $b = q-2 \equiv -1 \pmod{q-1}$. Then the generator matrix (1.4) is of the form

$$G = \begin{pmatrix} L_1^{q-2} & L_2^{q-2} & \dots & L_n^{q-2} \\ L_1^{q-1} & L_2^{q-1} & \dots & L_n^{q-1} \\ L_1^{q} & L_2^{q} & \dots & L_n^{q} \\ \dots & \dots & \dots & \dots \\ L_1^{q+k-3} & L_2^{q+k-3} & \dots & L_n^{q+k-3} \end{pmatrix} = \begin{pmatrix} L_1^{-1} & L_2^{-1} & \dots & L_n^{-1} \\ 1 & 1 & \dots & 1 \\ L_1 & L_2 & \dots & L_n \\ \dots & \dots & \dots & \dots \\ L_1^{k-2} & L_2^{k-2} & \dots & L_n^{k-2} \end{pmatrix}, \tag{1.5}$$

where $L_u \in \mathbb{F}_q^*$, $n \le q-1$, $L_u \ne L_y$ for $u \ne y$. RS codes of the form (1.5) are considered in Sections 4, 5, 9, and 10.

Note that to write x^{q-2} in the form x^{-1}, one should have $x \neq 0$. Furthermore, the definition of a polynomial as an expression [8] of the form $\sum\limits_{i=0}^{n} a_i x^i$, $n \geq 0$, is formally violated. The notation x^{q-2} is often used to avoid formal obstacles.

A codeword c of a nonextended RS code with generator matrix (1.5) can be defined by an *information polynomial*

$$f(x) = a_{-1}x^{q-2} + \sum_{i=0}^{k-2} a_i x^i = \sum_{i=-1}^{k-2} a_i x^i, \quad a_i \in \mathbb{F}_q, \quad i = -1, 0, 1, \ldots, k-2. \tag{1.6}$$

The coefficients a_i are information symbols. The word c has the form (1.2).

RS codes with generator matrices (1.3) and (1.5) contain words consisting of identical nonzero symbols. This makes it possible to introduce *bunches* of codewords of size $q(q-1)$ (see Section 3); in a bunch, it suffices to study one base word only.

We introduce the notation for the maximum possible cardinality of an A-subcode:

- $M_q^{(0)}(n,d)$, for the $[n,k,d]_q$ RS code with generator matrix (1.3);
- $M_q^{(-1)}(n,d)$, for the $[n,k,d]_q$ RS code with generator matrix (1.5);
- $M_q^{\mathrm{MDS}}(n,d)$, for an arbitrary $[n,k,d]_q$ MDS code.

Let $M_q^{(0,-1)}(n,d) = \max\{M_q^{(0)}(n,d), M_q^{(-1)}(n,d)\}$. Clearly,

$$M_q^{(0,-1)}(n,d) \leq M_q^{\mathrm{MDS}}(n,d) \leq M_q^{\mathrm{A}}(n,d).$$

The goal of the paper is to estimate $M_q^{(0)}(n, n-k+1)$ and $M_q^{(-1)}(n, n-k+1)$ for $k \leq 3$ and construct $[n, k, n-k+1]_q$ RS codes with generator matrices (1.3) and (1.5) that have the maximum possible cardinality of an A-subcode.

We may say that the goal of the paper is *studying special combinatorial properties of RS codes* with generator matrices (1.3) and (1.5).

In what follows, we call $[n,k,n-k+1]_q$ RS codes *long* codes if $n > \left\lfloor \frac{q+1}{2} \right\rfloor$, and *short* codes if $n \leq \left\lfloor \frac{q+1}{2} \right\rfloor$.

In the present paper we obtain *exact values* of $M_q^{(0)}(n, n-1)$ and $M_q^{(-1)}(n, n-1)$ for all n and of $M_q^{(0)}(n, n-2)$ and $M_q^{(-1)}(n, n-2)$ for long codes. We specify RS codes that attain these values. For short codes, we obtain constructive lower bounds for $M_q^{(0)}(n, n-2)$ and $M_q^{(-1)}(n, n-2)$, which are provided by codes with simple descriptions.

Denote by $M^{\mathrm{PA}}(n,d)$ the maximum possible cardinality of a permutation array $(n,d)PA$ [2,3]. Definition 1 implies the following fact.

Lemma 1. *Let $\mathcal{C}$ be an $(n,M,d)_Q$ A-code. Denote by $\mathcal{C}_t$ the $(n-t, M, d_t)_Q$ code obtained by deleting some t positions from $\mathcal{C}$. Then, independently of the indices of the deleted positions, $\mathcal{C}_t$ is an A-code with distance $d_t \geq d-t$. If $\mathcal{C}$ is an MDS code, then $d_t = d-t$. Moreover,*

$$M_Q^{\mathrm{A}}(n, n-t) \geq M_Q^{\mathrm{A}}(Q, Q-t) = M^{\mathrm{PA}}(Q, Q-t), \quad n \leq Q. \tag{1.7}$$

Thus, in principle, A-codes can be constructed as appropriate permutation codes and their shortenings. From lower estimates for $M^{\mathrm{PA}}(Q, Q-t)$, one can get lower estimates for $M_Q^{\mathrm{A}}(n, n-t)$. In the present paper, the problem of surpassing the best known permutation codes and their shortenings (in cardinality) *is not considered*. Our goal is finding A-subcodes of large cardinalities exactly in the RS codes (1.3) and (1.5). However, some comparison is made (see Section 11). As follows from the comparison, for $k = 2, 3$, A-subcodes of the $[n, k, n-k+1]_q$ RS codes with

generator matrices (1.3) and (1.5) in a rather wide range of the parameters n and q are either better (in cardinality) than shortenings of known permutation codes or not worth than known codes and their shortenings. On the other hand, in a number of cases known codes are better than RS codes.

Some result of this paper were presented without proofs in [9].

The paper is organized as follows. In Section 2 we briefly state the main results. In Section 3 we define bunches of words of a linear code. In Section 4 we show basic properties of bunches for the codes (1.3) and (1.5). Section 5 considers codes with $k = 2$. Sections 6–8 consider codes (1.3) with $k = 3$. Sections 9 and 10 considers codes (1.5) with $k = 3$. In Section 11 we compare the results and give a table of exact values and lower estimates for $M_{\mathrm{RS}}^{(0,-1)}(n, n-2, q)$ for small q obtained in this paper.

2. MAIN RESULTS

Denote by N_q the full length of an RS code:

$$N_q = \begin{cases} q & \text{for the code (1.3),} \\ q-1 & \text{for the code (1.5).} \end{cases}$$

We use the function (the least nonnegative residue modulo p)

$$\theta_p(x) \equiv x \pmod p, \quad \theta_p(x) \in \{0, 1, \ldots, p-1\}. \tag{2.1}$$

For long $[n, 3, n-2]_q$ RS codes (1.3) and (1.5) with $\left\lfloor \frac{q+1}{2} \right\rfloor < n \le N_q$, we obtain the following *exact values* (see Theorems 6 and 9 and relations (6.3) and (9.2)).

Theorem 1. *For any choice of locations in long shortened $[n, 3, n-2]_q$ RS codes with generator matrices* (1.3) *and* (1.5), *we have*

$$M_q^{(0)}(n, n-2) = (2 - \theta_2(q))q(q-1), \quad \left\lfloor \frac{q+1}{2} \right\rfloor < n \le q, \tag{2.2}$$

$$M_q^{(-1)}(n, n-2) = 2q(q-1), \quad \left\lfloor \frac{q+1}{2} \right\rfloor < n \le q-1. \tag{2.3}$$

Here we note formula (2.3), which for odd $q \ne 2^m + 1$ provides the best presently known results.

For short $[n, 3, n-2]_q$ RS codes (1.3) and (1.5) of length $n \le \left\lfloor \frac{q+1}{2} \right\rfloor$, we obtain many lower estimates and exact values for various n and q; see Theorems 7, 8, 10, and 11 and the corollary. Also, depending on the values of n and q, we find A-subcodes of cardinalities M_j, where

$$\begin{aligned} M_1 &= (q + c_1 - n)q(q-1), \quad c_1 = 1, 2, \quad n \mid N_q, \\ M_2 &= (q + 1 - wn)q(q-1), \quad 2 > w > 1, \\ M_3 &= (q + c_2 - 2n)q(q-1), \quad c_2 = 3, 4, \\ M_4 &= \left(q + 1 - 2n + \frac{n}{t}\right) q(q-1), \quad t \ge 2, \quad t \mid n. \end{aligned} \tag{2.4}$$

Clearly, the cardinality M_1 seems to be the most attractive, but (using methods of the present paper) it can be attained only in the case $n \mid N_q$. Moreover, in a number of cases M_3 is a tight bound for A-subcodes of these RS codes. In the case of M_2, the constant w, in principle, can be relatively close to 1.

Because of importance of subcodes with cardinality M_1 (and partly M_2), we specify in more detail the conditions (see Theorems 7, 8, and 11; the corollary; and relations (7.8), (7.11), (8.2), (10.4), and (10.6)–(10.8)) under which such subcodes can be constructed.

Theorem 2. *Let $3 \le n \le \left\lfloor \frac{q+1}{2} \right\rfloor$. Let p be a prime, and v be a positive integer. Then for $[n, 3, n-2]_q$ RS codes with generator matrices* (1.3) *and* (1.5) *we have*

$$M_q^{(0)}(n, n-2) \ge (q+2-\theta_2(q)-n)q(q-1), \quad q = p^m, \quad n = p^{m-v}, \quad p \ge 2, \quad m \ge 2, \tag{2.5}$$

$$M_q^{(-1)}(n, n-2) \ge (q+1-n)q(q-1), \quad n \mid (q-1), \tag{2.6}$$

$$M_q^{(0)}(n, n-2) \ge \Big(q+1-\frac{p}{\gamma}n\Big)q(q-1), \quad q = p^m, \quad n = \gamma p^{m-v}, \quad p \ge 5, \quad m \ge 3, \quad v \ge 2, \quad \frac{p+3}{2} \le \gamma \le p-1. \tag{2.7}$$

In particular, in (2.6) *we can put $n = (p^{bm}-1)/(p^b-1)$ for $q = p^{bm}$, $p \ge 2$, $b \ge 1$, and $n = \frac{1}{2}(q-1)$ for odd q.*

3. BUNCHES OF WORDS OF A LINEAR CODE

Definition 2. Let a linear $[n, k, d]_q$ code $\mathcal{C}$ contain the all-one codeword[1] $e = (1, \ldots, 1)$. A *bunch* W is a set of $q(q-1)$ codewords such that

$$W = \{\lambda c + \gamma e \mid \lambda \in \mathbb{F}_q^*,\ \gamma \in \mathbb{F}_q,\ c \in \mathcal{C}\},$$

where a codeword c contains at least two distinct symbols. The notation λc means that each symbol of c is multiplied by λ. Similarly, $\gamma e = (\gamma, \ldots, \gamma)$. The word c is referred to as a *base codeword of the bunch*. Any codeword of a bunch can be taken as its base codeword.

It is easily seen that codewords of the code $\mathcal{C}$ in Definition 2 that do not consist of identical symbols *split into* disjoint *bunches*. For an $[n, k, d]_q$ code, the total number $S_q(k)$ of bunches is

$$S_q(k) = \frac{q^k - q}{q(q-1)} = \frac{q^{k-1}-1}{q-1} = \sum_{i=0}^{k-2} q^i. \tag{3.1}$$

Note that using codewords of an RS code that consist of identical symbols as a research tool is known in the literature. For instance, in [10] the $[n, 2, n-1]_q$ RS code is considered as a union of cosets of the $[n, 1, n]_q$ code with codewords of the form $(\gamma, \ldots, \gamma)$, $\gamma \in \mathbb{F}_q$. Moreover, the LDPC code constructed in [10] uses all codewords of the RS code, regardless of whether there are repetitions of symbols.

Note also that the set of the q codewords of an $[n, k, d]_q$ code that consist of identical symbols is an example of an n-simplex in the space of q-ary vectors of length n equipped with the Hamming distance; see [11].

Definition 3. Consider a word c of length n over an alphabet of Q elements. Let $s_j(c)$ be the number of symbols of the alphabet that occur j times in c, $j = 0, 1, \ldots, n$. Let $J(c)$ be the smallest value of j such that $s_j(c) \ne 0$. Then the vector $\mathrm{comprep}(c) = (s_0(c), s_1(c), \ldots, s_{J(c)}(c))$ is called the *repeating composition* of c.

Clearly, for the word c in Definition 3 we have $\sum\limits_{j=1}^{J(c)} j s_j(c) = n$ and $\sum\limits_{j=0}^{J(c)} s_j(c) = Q$.

We call a vector containing ψ different symbols a ψ-word. For a ψ-word c, we have $\sum\limits_{j=1}^{J(c)} s_j(c) = \psi$. An A-word of an $(n, M, d)_Q$ code is an n-word with repeating composition $(\max(Q-n, 0), n)$.

Definitions 2 and 3 imply the following result.

[1] This means that the code contains $q-1$ words consisting of identical nonzero symbols.

Theorem 3. *If a base word of a bunch contains different* (*respectively*, *identical*) *symbols in some positions*, *then all words of this bunch also contain different* (*respectively*, *identical*) *symbols in these positions. All words of a bunch have the same repeating composition.*

By Theorem 3, to study A-words of a code containing the all-one codeword, it suffices to study base words of bunches and subsets of their positions.

A bunch of a code where a base word (and therefore every word) is an A-word is referred to as an *A-bunch*. A bunch of a code where a base word (and therefore every word) is a ψ-word is referred to as a *ψ-bunch*.

4. BUNCHES OF WORDS OF RS CODES WITH GENERATOR MATRICES (1.3) AND (1.5)

Definition 4. Consider $[n, k, n-k+1]_q$ RS codes with generator matrices (1.3) and (1.5). An information polynomial defining according to (1.2) a base word of a bunch is called a *base polynomial of the bunch*. As base polynomials of bunches, we always consider normalized polynomials without free terms. Then for codes (1.3) a base polynomial is of the form

$$f(x) = x^w + \sum_{i=1}^{w-1} a_i x^i, \quad 1 \le w \le k-1, \quad a_i \in \mathbb{F}_q, \quad i = 1, 2, \ldots, w-1, \tag{4.1}$$

where $f(x) = x$ for $w = 1$. In turn, for codes (1.5), as a base polynomial of a bunch we consider either a polynomial of the form

$$\begin{gathered} f(x) = x^w + \sum_{i=1}^{w-1} a_i x^i + a_{-1} x^{q-2}, \quad 1 \le w \le k-2, \\ a_i \in \mathbb{F}_q, \quad i = -1, 1, 2, \ldots, w-1, \end{gathered} \tag{4.2}$$

or the polynomial

$$f(x) = x^{q-2} = x^{-1}. \tag{4.3}$$

Denote by $A_q(k)$ the number of A-bunches of a *nonshortened* $[N_q, k, N_q - k + 1]_q$ RS code.

We emphasize that A-bunches are defined for codes of lengths $n \le N_q$, i.e., for both shortened and nonshortened codes. In cases where we are interested in the number and properties of A-bunches of precisely a nonshortened code with $n = N_q$, we always note this. After shortening, the number of A-bunches may become larger, which is shown below.

A polynomial $f \in \mathbb{F}_q[x]$ is called [8] a *permutation polynomial of the field* $\mathbb{F}_q$ if the corresponding polynomial function, taking an element $e \in \mathbb{F}_q$ to $f(e) \in \mathbb{F}_q$, is a permutation of elements of the field $\mathbb{F}_q$.

Lemma 2 [8]. (i) *Provided that* $f(0) = 0$, *in the ring* $\mathbb{F}_q[x]$ *there are only two normalized permutation polynomials* $f(x)$ *of degree* 2 *or less*: $f(x) = x$ *for any* q *and* $f(x) = x^2$ *for even* q.

(ii) $f(x) = x^{q-2}$ *is a permutation polynomial for any* q.

The aforesaid implies the following fact.

Lemma 3. *A bunch of a nonshortened* $[N_q, k, N_q - k + 1]_q$ *RS code* (1.3) *or* (1.5) *is an A-bunch if and only if its base polynomial is a permutation polynomial.*

We define the following types of words of length N_q for *nonshortened* $[N_q, k, N_q - k + 1]_g$ RS codes.

A $\left\lfloor\frac{q+1}{2}\right\rfloor$-codeword c of the code (1.3) is called a *B-word* if it has the repeating composition

$$\operatorname{comprep}(c)=\left(\left\lceil\frac{q-1}{2}\right\rceil,\theta_2(q),\left\lceil\frac{q-1}{2}\right\rceil\right)=\begin{cases}\left(\frac{q-1}{2},1,\frac{q-1}{2}\right), & q \text{ odd},\\ \left(\frac{q}{2},0,\frac{q}{2}\right), & q \text{ even}.\end{cases}$$

A $\left\lfloor\frac{q+1}{2}\right\rfloor$-codeword c of the code (1.5) is called a *C-word* if it has the repeating composition

$$\operatorname{comprep}(c)=\left(\left\lceil\frac{q-1}{2}\right\rceil,\theta_2(q)+1,\left\lceil\frac{q-1}{2}\right\rceil-1\right)=\begin{cases}\left(\frac{q-1}{2},2,\frac{q-1}{2}-1\right), & q \text{ odd},\\ \left(\frac{q}{2},1,\frac{q}{2}-1\right), & q \text{ even}.\end{cases}$$

A $\left\lfloor\frac{q-1}{2}\right\rfloor$-codeword c of the code (1.5) is called a *D-word* if it has the repeating composition

$$\operatorname{comprep}(c)=\left(\frac{q+1}{2},0,\frac{q+1}{2}-1\right),\quad q \text{ odd}.$$

A bunch of an RS code in which the base word (and therefore each word) is a B-word (respectively, C-word or D-word) is called a *B-bunch* (respectively, *C-bunch* or *D-bunch*). B-, C-, and D-bunches are defined only for a *nonshortened* code. After shortening a code, B-, C-, and D-bunches may become A-bunches.

Denote by $B_q(k)$, $C_q(k)$, and $D_q(k)$, respectively, the number of B-, C-, and D-bunches of a *nonshortened* $[N_q,k,N_q-k+1]_q$ RS code. Here $D_q(k)=0$ if q is even.

For a *nonshortened* $[N_q,k,N_q-k+1]_q$ RS code, denote by $T_q(k)$ the maximum number of different elements of $\mathbb{F}_q$ in words that contain at least two distinct elements (i.e., are not A-words). Clearly, $T_q(k)<N_q$.

Theorem 4. *For any parameters q and k, we have*

$$M_q^{(j)}(n,n-k+1)=A_q(k)q(q-1),\quad T_q(k)+1\le n\le N_q,\quad j=0,-1,$$
$$M_q^{(j)}(n,n-k+1)\ge(A_q(k)+1)q(q-1),\quad n\le T_q(k),\quad j=0,-1.$$

Proof. From each A-bunch of a nonshortened $[N_q,k,N_q-k+1]_q$ code one can obtain $q(q-1)$ A-words of length $n\le N_q$. Also, in principle, A-words of length $n<N_q$ can be obtained from other bunches. For $T_q(k)+1\le n\le N_q$, one can use only A-bunches to obtain A-words. This explains the exact equality in the first relation of the theorem. If $n\le T_q(k)$, than to obtain A-words of length n one can use not only A-bunches but also at least one $T_q(k)$-bunch. This is represented in the second relation. $\triangle$

5. RS CODES (1.3) AND (1.5) WITH TWO INFORMATION SYMBOLS

Theorem 5. (i) *For any q, in nonshortened $[N_q,k,N_q-k+1]_q$ RS codes* (1.3) *and* (1.5) *we have*

$$S_q(2)=A_q(2)=1.$$

Furthermore, the unique A-bunch has the base polynomial $f(x)=x$ for the code (1.3) *and $f(x)=x^{q-2}$ for the code* (1.5).

(ii) *For any q and for any choice of locations in shortened $[n,2,n-1]_q$ RS codes with generator matrices* (1.3) *and* (1.5), *we have*

$$M_q^{(j)}(n,n-1)=q(q-1),\quad n\le N_q,\quad j=0,-1. \tag{5.1}$$

Proof. The value of $S_q(2)$ follows from (3.1). By Lemma 2, $f(x) = x$ and $f(x) = x^{q-2}$ are permutation polynomials for any q. Now we use Theorem 4 and Lemma 3. The equality in (5.1) follows from the uniqueness of the bunch. $\triangle$

6. LONG $[n, 3, n-2]_q$ RS CODES (1.3)

Lemma 4. *Consider the nonshortened $[q, 3, q-2]_q$ RS code with matrix (1.3). Let the base polynomial of a bunch W be of the form $f(x) = x^2 + a_1 x$, $a_1 \in \mathbb{F}_q$. Then*

(i) *In the base word of W, symbols in different positions with locations L and T coincide, i.e., $f(L) = f(T)$ for $L \neq T$, if an only if*

$$L + T = -a_1; \tag{6.1}$$

(ii) *If q is even, then W is an A-bunch for $a_1 = 0$ and a B-bunch for $a_1 \neq 0$;*

(iii) *If q is odd, then for any a_1 the bunch W is a B-bunch, and the element that occurs in the base word exactly once is in the position with location $-\frac{1}{2}a_1$.*

Proof. (i) Let $f(L) = f(T)$, $L \neq T$. Then $L^2 + a_1 L = T^2 + a_1 T$ and $L^2 - T^2 = -a_1(L - T)$.

(ii) If q is even, then $f(x) = x^2$ is a permutation polynomial by Lemma 2. Now we apply Lemma 3. If q is even and $a_1 \neq 0$, then for any location L there is a location $T \neq L$ satisfying (6.1).

(iii) If q is odd, then $T = -L - a_1$, whence $T = L$ if and only if $L = -\frac{1}{2}a_1$. $\triangle$

Lemma 5. *In the nonshortened $[q, 3, q-2]_q$ RS code (1.3) with three information sysmbols, any bunch is either an A-bunch or a B-bunch; i.e.,*

$$S_q(3) = q + 1 = A_q(3) + B_q(3). \tag{6.2}$$

The numbers of A- and B-bunches of the nonshortened $[q, 3, q-2]_q$ code (1.3) are

$$A_q(3) = \begin{cases} 1, & q \text{ odd}, \\ 2, & q \text{ even}, \end{cases} \qquad B_q(3) = \begin{cases} q, & q \text{ odd}, \\ q-1, & q \text{ even}. \end{cases}$$

Base polynomials of A-bunches are of the form $f_1(x) = x$ (for any q) and $f_2(x) = x^2$ (for even q).

Proof. Apply Lemma 4, whence (6.2) follows. The value of $S_q(3)$ follows from (3.1). For base polynomials, Lemma 2 is used. $\triangle$

Lemma 6. *For a nonshortened $[q, 3, q-2]_q$ RS code (1.3), we have $T_q(3) = \left\lfloor \frac{q+1}{2} \right\rfloor$.*

Proof. This follows from Lemma 5. $\triangle$

Theorem 6. *For any choice of locations in the shortened $[n, 3, n-2]_q$ RS code with generator matrix (1.3), we have*

$$M_q^{(0)}(n, n-2) = \begin{cases} q(q-1), & q \text{ odd}, \quad \frac{q+1}{2} + 1 \le n \le q, \\ 2q(q-1), & q \text{ even}, \quad \frac{q}{2} + 1 \le n \le q. \end{cases} \tag{6.3}$$

Proof. Use Theorem 4 and Lemmas 5 and 6. $\triangle$

Remark 1. It follows from (5.1) and (6.3) that in the interval $\left\lfloor \frac{q+1}{2} \right\rfloor + 1 \le n \le q$ we have $M_q^{(0)}(n, n-2) = 2M_q^{(0)}(n, n-1)$ for even q, but $M_q^{(0)}(n, n-2) = M_q^{(0)}(n, n-1)$ for odd q. Thus, in this interval RS codes (1.3) with $k = 3$ for odd q are inefficient. For odd q in the interval $\frac{q+1}{2} + 1 \le n \le q - 1$, RS codes (1.5) with $k = 3$ are efficient, which provide $M_q^{(-1)}(n, n-2) = 2M_q^{(0)}(n, n-2)$ (see Theorem 9).

7. SHORT $[n, 3, n-2]_q$ RS CODES (1.3), q ODD

Let $q = p^m$, $p \geq 2$ being a prime, $m \geq 1$. We represent elements of the prime field $\mathbb{F}_p$ by numbers from 0 to $p-1$; i.e., $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$. An element e of $\mathbb{F}_q$ can be written as a polynomial in powers of a primitive element α of the field $\mathbb{F}_q$ or as the corresponding m-vector:

$$\begin{gathered} e \in \mathbb{F}_q, \quad e = \sum_{i=0}^{m-1} e_i \alpha^i = (e_{m-1}, \ldots, e_1, e_0), \quad e_i \in \mathbb{F}_p, \\ i = 0, \ldots, m-1, \quad q = p^m, \quad p \geq 2. \end{gathered} \tag{7.1}$$

Let $\hat{e}$ denote the m-digit number in the p-ary notation that corresponds to the vector representation of e, i.e.,

$$e = (e_{m-1}, \ldots, e_1, e_0) \quad \Longleftrightarrow \quad \hat{e} = \sum_{i=0}^{m-1} e_i p^i, \quad p \geq 2. \tag{7.2}$$

Let u denote a position number. In Sections 7 and 8, locations L_u of the nonshortened $[q, 3, q-2]_q$ RS code with generator matrix (1.3) are assigned in such a way that

$$\begin{aligned} L_u &= \sum_{i=0}^{m-1} \ell_i^{(u)} \alpha^i = (\ell_{m-1}^{(u)}, \ldots, \ell_1^{(u)}, \ell_0^{(u)}), \quad \ell_i^{(u)} \in \mathbb{F}_p, \\ \widehat{L}_u &= \sum_{i=0}^{m-1} \ell_i^{(u)} p^i = u - 1, \quad p \geq 2. \end{aligned} \tag{7.3}$$

In other words, vector representations of locations considered as m-digit numbers in the p-ary notation are arranged in *ascending lexicographic order*.

If $m = 1$, then $q = p$, m-vectors become numbers, and in (7.2) we have $e = \hat{e}$.

Below we give two constructions for shortened RS codes with generator matrix (1.3). The constructions are based on the following approach. By Lemma 5, in a nonshortened code, bunches with base polynomials $f_1(x) = x$ for any q and $f_2(x) = x^2$ for even q are A-bunches, while bunches with other base polynomials are B-bunches. When the code is shortened to length n, $q - n$ positions and their locations are deleted. For an A-bunch, any shortening is admissible. If locations are deleted "favorably," a B-bunch of the nonshortened code transforms into an A-bunch of the shortened code. Denote by Λ_n the set of assigned locations, and by Σ_n, the set of their pairwise sums. Here the summands are always distinct, whence $\Sigma_n \subset \mathbb{F}_q$ for odd q and $\Sigma_n \subset \mathbb{F}_q^*$ for even q. Equality (6.1) cannot hold for $L, T \in \Lambda_n$ and $-a_1 \in \mathbb{F}_q \setminus \Sigma_n$. Therefore, B-bunches of the nonshortened code with base polynomials $f(x) = x^2 + a_1 x$ with $-a_1 \in \mathbb{F}_q \setminus \Sigma_n$ turn into A-bunches of the shortened code. The number of new A-bunches is $q - 1 + \theta_2(q) - |\Sigma_n|$. To make the constructions efficient, one should reduce the cardinality $|\Sigma_n|$.

Thus, we are interested in the following additive combinatorics problem.

Let $0 < n < q$, and let $\Lambda_n \subset \mathbb{F}_q$ be a subset of elements of $\mathbb{F}_q$ of cardinality $|\Lambda_n| = n$. The set $\Sigma_n = \{L + T : L, T \in \Lambda_n, L \neq T\}$ composed of sums of *distinct* elements of the subset Λ_n is called the *restricted sum set*. The problem is to find the minimum cardinality $\min\limits_{\Lambda_n} |\Sigma_n|$ and to determine the structure of the minimizing set Λ_n.

For an introduction to the problem, see [12, Chapters 2 and 9; 13] and bibliography therein.

Lemma 7 [12, Theorem 9.5, Exercise 9.2.3]. *Let $q \geq 3$ be a prime. Then we have* $\min\limits_{\Lambda_n} |\Sigma_n| = \min\{2n - 3, q\}$.

Lemmas 4 and 5 imply that we have $\min\limits_{\Lambda_n} |\Sigma_n| < q - 1 + \theta_2(q)$ if and only if $n \leq \left\lfloor \dfrac{q+1}{2} \right\rfloor$ (cf. [12, Exercise 9.2.1]). For such n, the constructions given below provide lower bounds on

$q-1+\theta_2(q)-\min\limits_{\Lambda_n}|\Sigma_n|$ and thus upper bounds on $\min\limits_{\Lambda_n}|\Sigma_n|$. In particular, the bounds of Lemmas 8 and 9 are realized.

Lemma 8. *Let $q \ge 3$ be a prime, $n \le \dfrac{q+1}{2}$, and $\Lambda_n = \{0,1,\dots,n-1\}$. Then $\Sigma_n = \{1,2,\dots,2n-3\}$ and $|\Sigma_n| = 2n-3 = \min\limits_{\Lambda_n}|\Sigma_n|$.*

Proof. The set Σ_n is constructed directly. Then take into account that $2n-3 < q$ and use Lemma 7. $\triangle$

For $q = p^m$, $m > v \ge 1$, and $b \in \mathbb{F}_p$, introduce the following notation: H_v is the additive subgroup of $\mathbb{F}_q$ consisting of p^{m-v} elements of the form $(\underbrace{0,\dots,0}_{v}, e_{m-v-1},\dots,e_1,e_0)$ (see (7.1)); $s_b = (\underbrace{0,\dots,0}_{v-1}, b, \underbrace{0,\dots,0}_{m-v})$ is an element of $\mathbb{F}_q$; $H_v(s_b)$ is an additive coset of H_v with generator s_b. Clearly, $H_v(s_0) = H_v$.

Lemma 9. *Let $q = p^m$, p being a prime, $m > v \ge 1$.*

(i) *Let $n = p^{m-v} \ge 3$ and $\Lambda_n = H_v$. Then $\Sigma_n = H_v \setminus \{0\}$, $|\Sigma_n| = p^{m-v}-1$, for even q; and $\Sigma_n = H_v$, $|\Sigma_n| = p^{m-v}$, for odd q.*

(ii) *Let*

$$n = \gamma p^{m-v} < \frac{q+1}{2}, \quad p \ge 3, \quad 2 \le \gamma \le \begin{cases} \dfrac{p-1}{2} & v = 1, \\ p-1 & v \ge 2, \end{cases} \qquad \Lambda_n = \bigcup_{b=0}^{\gamma-1} H_v(s_b).$$

Then $\Sigma_n = \bigcup\limits_{b=0}^{\tau-1} H_v(s_b)$ and $|\Sigma_n| = \tau p^{m-v}$, where $\tau = \min\{2\gamma-1, p\}$.

Proof. (i) Use the fact that H_v is a subgroup. Furthermore, since the set Σ_n is composed of sums of *distinct* elements of the subgroup, we have $0 \notin \Sigma_n$ in the case of an even q.

(ii) The restriction $\gamma \le \dfrac{p-1}{2}$ for $v = 1$ is imposed because we have to ensure the inequality $\gamma p^{m-v} < \dfrac{q+1}{2}$. The set Σ_n is composed of set-theoretic sums of the form $H_v(s_{b_1}) + H_v(s_{b_2})$, where the equality $b_1 = b_2$ is possible. In the last case, distinct elements of the coset $H_v(s_{b_1})$ are summed. Since

$$H_v(s_{b_1}) + H_v(s_{b_2}) = H_v(s_{b_1+b_2}),$$

we have $\Sigma_n = \bigcup\limits_{b\in\sigma} H_v(s_b)$, where σ is the set consisting of all possible pairwise sums of elements of the set $\{0,1,\dots,\gamma-1\} \subset \mathbb{F}_p$. Here summands are not necessarily distinct. Clearly, we have $\sigma = \{0,1,\dots,2\gamma-2\} \subseteq \mathbb{F}_p$. If $2\gamma-2 \ge p-1$, then we can write $\sigma = \{0,1,\dots,p-1\} = \mathbb{F}_p$. Finally, note that $\tau = |\sigma|$. $\triangle$

To make constructions regular and universal, and also for describing, proving, and realizing them, it is important to have simple rules for assigning and deleting locations and for defining the coefficients a_1 in base polynomials that generate new A-bunches. The rules used in the constructions described below are simple and convenient to realize.

In this section, we assume in what follows that p is *odd*.

Set $\mathcal{P} = \dfrac{1}{2}(p-1)$.

In Table 1, for the nonshortened $[q,3,q-2]_q$ RS code (1.3), we present numbers of positions u and locations $L_u = (\ell_{m-1}^{(u)},\dots,\ell_1^{(u)},\ell_0^{(u)})$. The last entry of each row gives the value of δ for which this position (and its location) are deleted when forming the shortened $[n,3,n-2]_q$ code of length $n = \dfrac{q+1}{2} - \delta$.

Construction 1. Let $q = p^m$, $p \ge 3$ being a prime, $m \ge 1$. Locations in the nonshortened $[q,3,q-2]_q$ RS code with generator matrix (1.3) are defined in (7.1)–(7.3). A shortened $[n,3,n-2]_q$

Table 1. Position numbers u and locations L_u of the $[q, 3, q-2]_q$ RS code (1.3)

u	$\ell_{m-1}^{(u)}$	$\ell_{m-2}^{(u)}$	$\dots$	$\ell_2^{(u)}$	$\ell_1^{(u)}$	$\ell_0^{(u)}$	δ
1	0	0	$\dots$	0	0	0	
2	0	0	$\dots$	0	0	1	
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	
$\mathcal{P}p^{m-1}$	$\mathcal{P}-1$	$p-1$	$\dots$	$p-1$	$p-1$	$p-1$	
$\mathcal{P}p^{m-1}+1$	$\mathcal{P}$	0	$\dots$	0	0	0	
$\mathcal{P}p^{m-1}+2$	$\mathcal{P}$	0	$\dots$	0	0	1	
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	
$\mathcal{P}p^{m-1}+p$	$\mathcal{P}$	0	$\dots$	0	0	$p-1$	
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	
$(q-p^2)/2+1$ $=(q-(p-2)p)/2-p+1$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	0	0	$\mathcal{P}+1+\mathcal{P}p$
$(q-(p-2)p)/2-p+2$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	0	1	$\mathcal{P}+\mathcal{P}p$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$(q-(p-2)p)/2$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	0	$p-1$	$\mathcal{P}+2+(\mathcal{P}-1)p$
$(q-(p-2)p)/2+1$ $=(q-(p-4)p)/2-p+1$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	1	0	$\mathcal{P}+1+(\mathcal{P}-1)p$
$(q-(p-4)p)/2-p+2$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	1	1	$\mathcal{P}+(\mathcal{P}-1)p$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$(q-(p-4)p)/2$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	1	$p-1$	$\mathcal{P}+2+(\mathcal{P}-2)p$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$(q-3p)/2+1$ $=(q-p)/2-p+1$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	$\mathcal{P}-1$	0	$\mathcal{P}+1+p$
$(q-p)/2-p+2$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	$\mathcal{P}-1$	1	$\mathcal{P}+p$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$(q-p)/2$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	$\mathcal{P}-1$	$p-1$	$\mathcal{P}+2$
$(q-p)/2+1$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	$\mathcal{P}$	0	$\mathcal{P}+1$
$(q-p)/2+2$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	$\mathcal{P}$	1	$\mathcal{P}$
$(q-p)/2+3$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	$\mathcal{P}$	2	$\mathcal{P}-1$
$\dots$	$\dots$	$\dots$	$\dots$		$\dots$	$\dots$	$\dots$
$(q-1)/2=(q-p)/2+\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}-1$	2
$(q+1)/2=(q-p)/2+\mathcal{P}+1$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	1
$(q+1)/2+1$	$\mathcal{P}$	$\mathcal{P}$	$\dots$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}+1$	0
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$p^m-1=q-1$	$p-1$	$p-1$	$\dots$	$p-1$	$p-1$	$p-2$	0
$p^m=q$	$p-1$	$p-1$	$\dots$	$p-1$	$p-1$	$p-1$	0

code of length $n=\dfrac{q+1}{2}-\delta\geq 3$, $\delta\geq 0$, is formed. Here, in a codeword of the nonshortened code, $q-n$ rightmost positions are deleted, with numbers $n+1, n+2, \dots, q$.

A-words of length n are chosen from $\varphi(n)$ bunches with base polynomials

$$f_1(x)=x, \qquad f_j(x)=x^2+a_{1,j}x,$$
$$a_{1,j}=\left(\theta_p\left(\left\lceil\frac{j-1}{p^{m-1}}\right\rceil\right),\dots,\theta_p\left(\left\lceil\frac{j-1}{p^2}\right\rceil\right),\theta_p\left(\left\lceil\frac{j-1}{p}\right\rceil\right),\theta_p(j-2)\right), \tag{7.4}$$

where the function $\theta_p(x)$ is defined in (2.1), $j = 2, 3, \ldots, \varphi(n)$,

$$\varphi(n) = \begin{cases} 3 + 2h = q + 1 - (2n - 3), \\ \qquad\qquad n = \dfrac{q+1}{2} - h \geq \dfrac{q-p}{2} + 2,\ m \geq 1, \\ p + 1 = q + 1 - (2n - 2), \\ \qquad\qquad n = \dfrac{q-p}{2} + 1,\ m \geq 2, \\ 2p^t + 1 + 2hp^t = q + 1 - (2n - p^t), \\ \qquad\qquad n = \dfrac{q-p^t}{2} - hp^t \geq \dfrac{q-p^{t+1}}{2} + p^t,\ m \geq 2, \\ p^{t+1} + 1 - p^t = q + 1 - (2n - p^t), \\ \qquad\qquad n = \dfrac{q-p^{t+1}}{2} + p^t \geq \dfrac{q}{p},\ m \geq 2, \\ q + 1 - \dfrac{q}{p^v} = q + 1 - n, \\ \qquad\qquad n = \dfrac{q}{p^v} = p^{m-v},\ m \geq 2, \end{cases} \tag{7.5}$$

$$h = \begin{cases} 0, 1, \ldots, \mathcal{P} - 2 & m = 1, \\ 0, 1, \ldots, \mathcal{P} - 1 & m \geq 2, \end{cases} \quad t = 1, 2, \ldots, m-1, \quad v = 1, 2, \ldots, m-1. \tag{7.6}$$

Note that for $m = 1$ we have $h \leq \mathcal{P} - 2$ to ensure that $n \geq 3$.

Theorem 7. *Let $q = p^m$, $p \geq 3$ being a prime, $n = \dfrac{q+1}{2} - \delta \geq 3$, $\delta \geq 0$. For the $[n, 3, n-2]_q$ RS code with generator matrix* (1.3)*, we have the following.*

(i) *Let $m \geq 1$, and let $\varphi(n)$ be defined as in* (7.5) *and* (7.6)*. Then*

$$M_q^{(0)}(n, n-2) \geq \varphi(n) q(q-1), \tag{7.7}$$

$$M_q^{(0)}(n, n-2) \geq (q + 1 - n) q(q-1), \quad n = p^{m-v}, \quad m \geq 2, \tag{7.8}$$

$$M_q^{(0)}(n, n-2) = \varphi(n) q(q-1), \quad \text{if} \quad m = 1, \quad n = \frac{q+1}{2} - h. \tag{7.9}$$

The required number of A-words in (7.7)–(7.9) *is guaranteed, for instance, by Construction* 1.

(ii) *Let*

$$m > v \geq 1, \qquad 2 \leq \gamma \leq \begin{cases} \dfrac{p-1}{2} & \text{for } v = 1, \\ p - 1 & \text{for } v \geq 2. \end{cases}$$

Then

$$M_q^{(0)}(n, n-2) \geq \left(q + 1 - 2n + \frac{n}{\gamma}\right) q(q-1), \quad n = \gamma p^{m-v}, \quad 2 \leq \gamma \leq \frac{p+1}{2}, \tag{7.10}$$

$$M_q^{(0)}(n, n-2) \geq \left(q + 1 - \frac{p}{\gamma} n\right) q(q-1), \quad n = \gamma p^{m-v}, \quad \frac{p+3}{2} \leq \gamma \leq p - 1. \tag{7.11}$$

Proof. (i) Let us prove that estimates (7.7) hold if we use Construction 1. By Lemma 5, in the nonshortened code the bunch with the base polynomial $f_1(x)$ is an A-bunch, and bunches with other base polynomials are B-bunches. For an A-bunch, any shortening is admissible. We show that the choice of locations according to Construction 1 takes B-bunches of the nonshortened code with base polynomials specified in the construction to A-bunches of the shortened code.

In all cases, for all nonpermutation polynomials $f_j(x)$ from (7.4) that we consider, we try to find locations L and T in the shortened code such that $L \neq T$ and $f_j(L) = f_j(T)$. Then, based on (6.1), we show that there are no such locations; i.e., the equality $T + L = -a_{1,j}$ cannot be

provided. By the construction, when shortening a code, we always delete positions with numbers $\frac{q+1}{2}+1, \frac{q+1}{2}+2, \dots, q$. Hence,

$$\begin{gathered} L, T \in \{L_1, \dots, L_{\frac{q+1}{2}}\} = \{(0, \dots, 0), \dots, (\mathcal{P}, \dots, \mathcal{P})\}, \\ \widehat{L}, \widehat{T} \in \Big\{0, 1, \dots, \frac{q-1}{2}\Big\}. \end{gathered} \tag{7.12}$$

For $\delta > 0$, we also delete positions with numbers $n+1 \le u \le \frac{q+1}{2}$.

Now we consider various situations as δ grows. Counting and analyzing the coefficients $a_{1,j}$ and deleted locations, which was made previously for smaller values of δ, is not repeated, since Construction 1 is of iterative character with respect to δ.

Case a. Let

$$n = \frac{q+1}{2} - h \ge \frac{q-p}{2} + 2, \quad \delta = h, \quad m \ge 1, \quad \text{with values of } h \text{ given in (7.6)}.$$

Then (7.1)–(7.4) imply that $2 \le j \le 3 + 2\delta \le p$, $a_{1,j} = (1, \dots, 1, j-2)$, $-a_{1,j} = (p-1, \dots, p-1, \theta_p(p-j+2))$, $\theta_p(p-j+2) \in \{0, p-1-2\delta, p-2\delta, \dots, p-1\} = M$. Hence, according to (7.1)–(7.3), (7.12), and Table 1, to ensure $T + L = -a_{1,j}$ we must have

$$\begin{gathered} L = (\mathcal{P}, \dots, \mathcal{P}, \ell_0^{(L)}), \quad T = (\mathcal{P}, \dots, \mathcal{P}, \ell_0^{(T)}), \quad \ell_0^{(L)} \ne \ell_0^{(T)}, \\ \ell_0^{(L)} + \ell_0^{(T)} = \theta_p(p-j+2). \end{gathered} \tag{7.13}$$

For $1 \le \delta \le \mathcal{P}-1$, positions with numbers $\frac{q+1}{2} - i$ and locations $(\mathcal{P}, \dots, \mathcal{P}, \mathcal{P}-i)$, $i = 0, 1, \dots, \delta-1$, are deleted; see Table 1. Therefore, for $0 \le \delta \le \mathcal{P}-1$ we have $\ell_0^{(L)}, \ell_0^{(T)} \in \{0, 1, \dots, \mathcal{P}-\delta\}$, $\ell_0^{(L)} + \ell_0^{(T)} \in \{1, 2, \dots, 2\mathcal{P}-1-2\delta\} = \{1, 2, \dots, p-2-2\delta\} = V$. Hence, $\ell_0^{(L)} + \ell_0^{(T)} \ne \theta_p(p-j+2)$, since the sets M and V are disjoint.

Case b. Let

$$n = \frac{q-p}{2} + 1, \quad \delta = \mathcal{P}, \quad m \ge 2.$$

Now we have $a_{1,p+1} = (1, \dots, 1, p-1)$, $-a_{1,p+1} = (p-1, \dots, p-1, 1)$. The position with number $\frac{1}{2}(q+1) - (\mathcal{P}-1) = \frac{1}{2}(q-p) + 2$ and location $(\mathcal{P}, \dots, \mathcal{P}, 1)$ is deleted. Relation (7.13) must hold for $\theta_p(p-j+2) = 1$. However, after deleting locations, only one location of the required form remains, namely, $(\mathcal{P}, \dots, \mathcal{P}, 0)$; see Table 1.

Case c. Let

$$n = \frac{q-p^t}{2} - hp^t, \quad \delta = \frac{p^t+1}{2} + hp^t, \quad m \ge 2, \quad \text{where } h \text{ and } t \text{ are defined in (7.6)}.$$

The largest number of a base polynomial f_j used in Case b is $j = p+1$. In Case c, $2p^t + 2hp^t - p$ new polynomials with numbers $k(i) = p+2+i$ are used, where $i = 0, 1, \dots, 2p^t + 2hp^t - p - 1 \le p^{t+1} - p^t - p - 1$. Obviously, $p+1 \le k(i) - 1 \le p^{t+1} - p^t$. Let $K_r(i) = \Big\lceil \frac{k(i)-1}{p^r} \Big\rceil$. It follows from the above that $K_t(i) \in \{1, 2, \dots, 2+2h\}$, $1 \le K_t(i) \le p-1$,

$$\begin{aligned} a_{1,k(i)} &= \big(1, \dots, 1, K_t(i), \theta_p(K_{t-1}(i)), \dots, \theta_p(K_2(i)), \theta_p(K_1(i)), \theta_p(i)\big), \\ -a_{1,k(i)} &= \big(p-1, \dots, p-1, p-K_t(i), \theta_p(p-K_{t-1}(i)), \dots, \theta_p(p-K_1(i)), \theta_p(p-i)\big). \end{aligned}$$

Here, $\frac{p^t+1}{2}+hp^t-\frac{p-1}{2}$ positions are deleted (see Table 1 for $t=1$) with numbers $\frac{q-p}{2}+1$, $\frac{q-p}{2},\dots,\frac{q-p^t}{2}+1-hp^t$ in descending order. According to (7.1)–(7.3), to the position with number $\frac{q-p^v}{2}+1$ the location $(\underbrace{\mathcal{P},\dots,\mathcal{P}}_{m-v},\underbrace{0,\dots,0}_{v})$ corresponds. Hence, the locations

$$(\mathcal{P},\dots,\mathcal{P},0),(\mathcal{P},\dots,\mathcal{P},\mathcal{P}-1,p-1),\dots,(\underbrace{\mathcal{P},\dots,\mathcal{P}}_{m-t-1},\mathcal{P}-h,\underbrace{0,\dots,0}_{t})$$

are deleted, where $\mathcal{P}\ge\mathcal{P}-h\ge 1$.

To ensure the equality $T+L=-a_{1,k(i)}$ for $L\ne T$, we must have

$$\begin{gathered}L=(\mathcal{P},\dots,\mathcal{P},\ell_t^{(L)},\dots,\ell_1^{(L)},\ell_0^{(L)}),\qquad T=(\mathcal{P},\dots,\mathcal{P},\ell_t^{(T)},\dots,\ell_1^{(T)},\ell_0^{(T)}),\\ \ell_t^{(L)}+\ell_t^{(T)}=p-K_t(i).\end{gathered}\tag{7.14}$$

Thus, we obtain $p-K_t(i)\in\{p-2-2h,p-1-2h,\dots,p-2,p-1\}=M$, $\ell_1^{(L)},\ell_1^{(T)}\in\{0,1,\dots,\mathcal{P}-h-1\}$, $\ell_1^{(L)}+\ell_1^{(T)}\in\{0,1,\dots,2\mathcal{P}-2h-2\}=\{0,1,\dots,p-3-2h\}=V$. Therefore, the sets M and V are disjoint, and (7.14) cannot hold.

Case d. Let

$$n=\frac{q-p^{t+1}}{2}+p^t,\quad \delta=\frac{p^{t+1}+1}{2}-p^t,\quad m\ge 2,\quad t=1,2,\dots,m-1.$$

This is an instance of Case c, with $h=\mathcal{P}-1$.

Case e. Let

$$n=\frac{q}{p^v},\quad \delta=\frac{q+1}{2}-\frac{q}{p^v},\quad m\ge 3,\quad v=2,3,\dots,m-1.$$

Note that for $v=1$ this reduces to Case d with $t=m-1$.

In Case e, Lemma 9(i) is realized, since by Construction 1 we have $\Lambda_n=H_v$. Then the values $-a_{1,j}$, additive inverse to coefficients of the polynomials that generate new A-bunches, belong to $\mathbb{F}_q\setminus\Sigma_n$. By Lemma 9(i), we have $\Sigma_n=H_v$. Hence, $\mathbb{F}_q\setminus\Sigma_n$ consists of $q-p^{m-v}$ elements of the form $(e_{m-1},\dots,e_1,e_0)$ with $(e_{m-1},e_{m-2},\dots,e_{m-v})\ne(0,\dots,0)$. This means that in this case the coefficients $a_{1,j}$ themselves must belong to $\mathbb{F}_q\setminus\Sigma_n$.

The largest number j of base polynomials f_j used in this case is $\varphi(n)=p^m+1-p^{m-v}$. Hence, $1\le j-1\le p^m-p^{m-v}$. If $1\le j-1\le p^m-p^{m-1}$, then $1\le\left\lceil\frac{j-1}{p^{m-1}}\right\rceil\le p-1$ and $\theta_p\Big(\left\lceil\frac{j-1}{p^{m-1}}\right\rceil\Big)\ne 0$.

Let $p^m-p^{m-(r-1)}+1\le j-1\le p^m-p^{m-r}$, $2\le r\le v$. Then $j-1=p^m-p^{m-(r-1)}+\Delta$, $1\le\Delta\le p^{m-r}(p-1)$, and $\left\lceil\frac{j-1}{p^{m-r}}\right\rceil=\left\lceil p^r-p+\frac{\Delta}{p^{m-r}}\right\rceil$. Since $\frac{1}{p^{m-r}}\le\frac{\Delta}{p^{m-r}}\le p-1$, we have $\theta_p\Big(\left\lceil\frac{j-1}{p^{m-r}}\right\rceil\Big)\ne 0$.

Thus, for all polynomials of Construction 1 used in this case, in coefficients $a_{1,j}$ we have $(e_{m-1},e_{m-2},\dots,e_{m-v})\ne(0,\dots,0)$.

Estimate (7.8) is a particular case of (7.7), with $n=p^{m-v}$.

The equality in (7.9) follows from (7.7) and Lemma 8.

(ii) The assertion of the theorem follows in this case from Lemma 9(ii). Taking this lemma into account, we have $M_q^{(0)}(n,n-2)\ge(q+1-\tau p^{m-v})q(q-1)$, where $\tau=\min\{2\gamma-1,p\}$. $\triangle$

Example 1. In Table 2 we present coefficients a_2,a_1,a_0 of base polynomials f_j and base words c_j of twenty-one bunch for the $[n,3,n-2]_{25}$ RS code (1.3) with $q=5^2$ and $n\le\frac{q+1}{2}=13$. We show

Table 2. Base polynomials f_j and base codewords c_j of bunches of the $[n, 3, n-2]_{25}$ RS code (1.3)

					1	2	3	4	5	6	7	8	9	10	11	12	13	u
					0	0	0	0	0	1	1	1	1	1	2	2	2	$\ell_1^{(u)}$
					0	1	2	3	4	0	1	2	3	4	0	1	2	$\ell_0^{(u)}$
f_j	$\widehat{a}_2$	$\widehat{a}_{1,j}$	$\widehat{a}_0$	$-a_1^{(1,j)}$	$-a_0^{(1,j)}$	0	1	2	3	4	5	6	7	8	9	10	11	12	$\widehat{L}_u$
f_1	0	1	0			0	1	2	3	4	5	6	7	8	9	10	11	12	c_1
f_2	1	5	0	4	0	0	6	14	19	21	16	7	20	10	2	23	24	22	c_2
f_3	1	6	0	4	4	0	7	11	17	20	21	13	2	18	6	8	5	9	c_3
																			$\delta = 0$
f_4	1	7	0	4	3	0	8	13	15	24	1	19	9	21	10	18	16	16	c_4
f_5	1	8	0	4	2	0	9	10	18	23	6	20	11	4	19	3	2	3	c_5
																		$*$	$\delta = 1$
f_6	1	9	0	4	1	0	5	12	16	22	11	1	18	7	23	13	13	10	c_6
																	$*$	$*$	$\delta = 2$
f_7	1	10	0	3	0	0	11	24	9	16	14	5	3	23	15	14	15	23	c_7
f_8	1	11	0	3	4	0	12	21	7	15	19	11	5	1	24	24	1	5	c_8
f_9	1	12	0	3	3	0	13	23	5	19	24	17	12	9	3	9	12	17	c_9
f_{10}	1	13	0	3	2	0	14	20	8	18	4	23	19	12	7	19	23	4	c_{10}
f_{11}	1	14	0	3	1	0	10	22	6	17	9	4	21	15	11	4	9	11	c_{11}
																$*$	$*$	$*$	$\delta = 3$
f_{12}	1	15	0	2	0	0	16	9	24	11	7	8	6	6	8	0	11	24	c_{12}
f_{13}	1	16	0	2	4	0	17	6	22	10	12	14	13	14	12	10	22	6	c_{13}
														$*$	$*$	$*$	$*$	$*$	$\delta = 5$
f_{14}	1	17	0	2	3	0	18	8	20	14	17	15	15	17	16	20	8	18	c_{14}
f_{15}	1	18	0	2	2	0	19	5	23	13	22	21	22	20	20	5	19	0	c_{15}
													$*$	$*$	$*$	$*$	$*$	$*$	$\delta = 6$
f_{16}	1	19	0	2	1	0	15	7	21	12	2	2	4	3	4	15	0	12	c_{16}
												$*$	$*$	$*$	$*$	$*$	$*$	$*$	$\delta = 7$
f_{17}	1	20	0	1	0	0	21	19	14	6	0	6	14	19	21	16	7	20	c_{17}
f_{18}	1	21	0	1	4	0	22	16	12	5	5	12	16	22	0	1	18	7	c_{18}
f_{19}	1	22	0	1	3	0	23	18	10	9	10	18	23	0	9	11	4	19	c_{19}
f_{20}	1	23	0	1	2	0	24	15	13	8	15	24	0	8	13	21	10	1	c_{20}
f_{21}	1	24	0	1	1	0	20	17	11	7	20	0	7	11	17	6	21	13	c_{21}
											$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$\delta = 8$

the cases of Construction 1 with $0 \le \delta \le \mathcal{P} + 1 + p$. Also, we show the cases $\delta = 5, 6, 7$, which are not included in Construction 1. The coefficients a_i, locations L_u, and symbols of base words of the bunches are represented as numbers $\hat{e}$ according to (7.2). Negations of $a_{1,j}$ and locations L_u are also written as two-dimensional vectors $-a_{1,j} = (-a_1^{(1,j)}, -a_0^{(1,j)})$ and $L_u = (\ell_1^{(u)}, \ell_0^{(u)})$. The generator polynomial of the field is x^2+x+2. Position that are deleted in the shortened code are denoted by $*$.

Remark 2. Shortened A-codes with lengths that are not given in Theorem 7 can be obtained with the help of Lemma 1. For particular values of p and δ, the results of Theorem 7 can be improved and extended; for instance, see the cases $q = 5^2$ and $\delta = 5, 6, 7$ in Table 2, which are not included in Construction 1. As an example, we also give the following statement, which can be proved using ideas of Construction 1 and techniques of the proof of Theorem 7.

Let $q = 3^m$, $m \geq 3$, $\delta = 0, 1, 2, 3$. For the $[n, 3, n-2]_q$ RS code with generator matrix (1.3) we have

$$\frac{1}{q(q-1)} M_q^{(0)}(n, n-2) \geq \begin{cases} 3 + 2\delta = q + 4 - 2n & \text{if } n = \dfrac{q+1}{2} - \delta, \\ 10 = q + 3 - 2n & \text{if } n = \dfrac{q+1}{2} - 4. \end{cases} \tag{7.15}$$

8. SHORT $[n, 3, n-2]_q$ RS CODES (1.3), q EVEN

Let $q = p^m$, $p = 2$, $m \geq 3$. Similarly to Section 7, we represent elements of $\mathbb{F}_q$ according to (7.1) and (7.2).

Construction 2. Let $q = p^m$, $p = 2$, $m \geq 3$. Locations in the nonshortened $[q, 3, q-2]_q$ RS code with generator matrix (1.3) are given by formulas (7.1)–(7.3). We form a shortened $[n, 3, n-2]_q$ code of length

$$n = \frac{q}{2^b} = 2^{m-b} \geq 4, \quad b = 1, 2, 3, \ldots, m-2.$$

Then, similarly to Construction 1, we delete $q - n$ rightmost codeword positions, with numbers $n+1, n+2, \ldots, q$.

A-words of length n are chosen from $q - n + 2$ bunches with base polynomials

$$f_1(x) = x, \qquad f_2(x) = x^2, \qquad f_j(x) = x^2 + a_{1,j}x, \quad j = 3, 4, \ldots, q - n + 2,$$

where

$$a_{1,j} = (a_{m-1}^{(1,j)}, \ldots, a_1^{(1,j)}, a_0^{(1,j)}), \quad a_i^{(1,j)} \in \{0, 1\}, \qquad \widehat{a}_{1,j} = \sum_{i=0}^{m-1} 2^i a_i^{(1,j)} = 2^m - j + 2.$$

In other words,

$$\{\widehat{a}_{1,j} \mid j = 3, 4, \ldots, q - n + 2\} = \{2^{m-b}, 2^{m-b} + 1, \ldots, 2^m - 1\}; \tag{8.1}$$

i.e., in the base polynomials $f_j(x)$, the coefficients $a_{1,j}$, considered in a vector representation as binary numbers, fill the whole range $2^{m-b} \ldots 2^m - 1$.

Construction 2 realizes Lemma 9(i).

Theorem 8. *Let $q = 2^m$, $m \geq 3$. Then for the $[n, 3, n-2]_q$ RS code with generator matrix* (1.3) *we have*

$$M_q^{(0)}(n, n-2) \geq (q + 2 - n)q(q-1), \quad n = \frac{q}{2^b} \geq 4, \quad b = 1, 2, \ldots, m-2. \tag{8.2}$$

The required number of A-words in guaranteed, for instance, by Construction 2.

Proof. Let us prove that estimate (8.2) holds if we use Construction 2. By Lemma 5, in the nonshortened code, bunches with base polynomials $f_1(x)$ and $f_2(x)$ are A-bunches, and bunches with other base polynomials are B-bunches. For an A-bunch, any shortening is admissible. Let us show that the choice of locations according to Construction 2 transforms B-bunches of the nonshortened code with base polynomials specified in the construction into A-bunches of the shortened code.

Similarly to Theorem 7, for nonpermutation polynomials $f_j(x)$ we try to find locations L and T in the shortened code such that $L \neq T$ and $f_j(L) = f_j(T)$. Then, based on (6.1), we show that there are no such locations; i.e., the equality $T + L = a_{1,j}$ cannot be provided. In this equality we take into account that $a_{1,j} = -a_{1,j}$ in a field of characteristic 2.

By the construction, when shortening a code, we delete $q - n$ rightmost positions with locations $L_{n+1}, L_{n+2}, \ldots, L_q$. Since $n = 2^{m-b}$, from (7.1)–(7.3) we have

Table 3. Base polynomials f_j and base codewords c_j of bunches of the $[n, 3, n-2]_{16}$ RS code (1.3)

				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	u
				0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	$\ell_3^{(u)}$
				0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	$\ell_2^{(u)}$
				0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	$\ell_1^{(u)}$
				0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	$\ell_0^{(u)}$
	$\widehat{a}_2$	$\widehat{a}_{1,j}$	$\widehat{a}_0$	$a_3^{(1,j)}$	$a_2^{(1,j)}$	$a_1^{(1,j)}$	$a_0^{(1,j)}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	$\widehat{L}_u$
f_1	0	1	0					0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	c_1
f_2	1	0	0	0	0	0	0	0	1	4	5	9	8	13	12	15	14	11	10	6	7	2	3	c_2
																								$\frac{q}{2} < n \le q$ Theorem 6
f_3	1	15	0	1	1	1	1	0	14	3	13	7	9	4	10	10	4	9	7	13	3	14	0	c_3
f_4	1	14	0	1	1	1	0	0	15	1	14	3	12	2	13	2	13	3	12	1	14	0	15	c_4
f_5	1	13	0	1	1	0	1	0	12	7	11	15	3	8	4	3	15	4	8	12	0	11	7	c_5
f_6	1	12	0	1	1	0	0	0	13	5	8	11	6	14	3	11	6	14	3	0	13	5	8	c_6
f_7	1	11	0	1	0	1	1	0	10	11	1	14	4	5	15	1	11	10	0	15	5	4	14	c_7
f_8	1	10	0	1	0	1	0	0	11	9	2	10	1	3	8	9	2	0	11	3	8	10	1	c_8
f_9	1	9	0	1	0	0	1	0	8	15	7	6	14	9	1	8	0	7	15	14	6	1	9	c_9
f_{10}	1	8	0	1	0	0	0	0	9	13	4	2	11	15	6	0	9	13	4	2	11	15	6	c_{10}
																$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$n = \frac{q}{2}$
f_{11}	1	7	0	0	1	1	1	0	6	10	12	12	10	6	0	5	3	15	9	9	15	3	5	c_{11}
f_{12}	1	6	0	0	1	1	0	0	7	8	15	8	15	0	7	13	10	5	2	5	2	13	10	c_{12}
f_{13}	1	5	0	0	1	0	1	0	4	14	10	4	0	10	14	12	8	2	6	8	12	6	2	c_{13}
f_{14}	1	4	0	0	1	0	0	0	5	12	9	0	5	12	9	4	1	8	13	4	1	8	13	c_{14}
												$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$n = \frac{q}{4}$
f_{15}	1	3	0	0	0	1	1	0	2	2	0	5	7	7	5	14	12	12	14	11	9	9	11	c_{15}
f_{16}	1	2	0	0	0	1	0	0	3	0	3	1	2	1	2	6	5	6	5	7	4	7	4	c_{16}
f_{17}	1	1	0	0	0	0	1	0	0	6	6	13	13	11	11	7	7	1	1	10	10	12	12	c_{17}

$$L, T \in \{L_1, \ldots, L_n\} \subseteq \{L_1, \ldots, L_{2^{m-b}}\},$$
$$\widehat{L}, \widehat{T} \in \{0, 1, \ldots, n-1\} \subseteq \{0, 1, \ldots, 2^{m-b}-1\}.$$

Taking into account the addition rule in a field of characteristic 2, we may write $\widehat{L+T} \in \{0, 1, \ldots, 2^{m-b}-1\}$. Now (8.1) implies that $T + L \neq a_1^{(j)}$. $\triangle$

Note that shortened A-codes with lengths that are not given in Theorem 8 can be obtained with the help of Lemma 1.

Example 2. In Table 3 we present coefficients a_2, a_1, a_0 of base polynomials f_j and base words c_j of fourteen bunches for the $[n, 3, n-2]_{16}$ RS code (1.3) with $q = 2^4$. The coefficients a_i, locations L_u, and symbols of base words of the bunches are written as numbers $\hat{e}$ according to (7.2). The coefficient $a_{1,j}$ for polynomials of degree 2 and locations L_u are also written as 4-vectors $a_1 = (a_3^{(1,j)}, a_2^{(1,j)}, a_1^{(1,j)}, a_0^{(1,j)})$ and $L_u = (\ell_3^{(u)}, \ell_2^{(u)}, \ell_1^{(u)}, \ell_0^{(u)})$. The generator polynomial of the field is $x^4 + x^3 + 1$. Positions that are deleted in the shortened code are marked with $*$. We also present three bunches that are not used in shortening.

9. LONG $[n, 3, n-2]_q$ RS CODES (1.5)

Lemma 10. *Consider the nonshortened $[q-1, 3, q-3]_q$ RS code with generator matrix* (1.5). *Let the base polynomial of a bunch W be of the form $f(x) = x + a_{-1}x^{q-2} = x + a_{-1}x^{-1}$, $a_{-1} \in \mathbb{F}_q$. Then we have the following statements.*

(i) *In a base word of W, symbols in different positions with locations L and T coincide, i.e., $f(L) = f(T)$ for $L \neq T$, if and only if*

$$LT = a_{-1}; \tag{9.1}$$

(ii) *If $a_{-1} = 0$, then for any q the bunch W is an A-bunch;*

(iii) *If q is even and $a_{-1} \neq 0$, then W is a C-bunch. The element that occurs in the base word precisely once is zero and is in the position with location $\sqrt{a_{-1}}$;*

(iv) *Let q be odd. If a_{-1} is a nonzero square in $\mathbb{F}_q$, then W is a C-bunch, and the two elements that occur in the base word precisely once are at positions with locations $\pm\sqrt{a_{-1}}$. If a_{-1} is not a square in $\mathbb{F}_q$, then W is a D-bunch.*

Proof. Below we take into account that all locations are nonzero.

(i) Let $f(L) = f(T)$. Then $L + a_{-1}L^{-1} = T + a_{-1}T^{-1}$ and $LT(L-T) = a_{-1}(L-T)$.

(ii) By Lemma 2 we obtain that $f(x) = x$ is a permutation polynomial. Then we use Lemma 3.

(iii) If q is even, then a_{-1} is always a square. For any location $L \neq \sqrt{a_{-1}}$ there exists a location $T \neq L$ satisfying (9.1). If $L = \sqrt{a_{-1}}$, then $T = L$ and $f(L) = 0$.

(iv) Let q be odd. If a_{-1} is a nonzero square, then from (9.1) we have $T = a_{-1}L^{-1}$. For $L = \pm\sqrt{a_{-1}}$ we obtain $T = L$. If a_{-1} is not a square, then always $T \neq L$. $\triangle$

Lemma 11. *In the nonshortened $[q-1, 3, q-3]_q$ RS code* (1.5), *each bunch is either an A-bunch, or C-bunch, or D-bunch; i.e.,*

$$S_q(3) = q + 1 = A_q(3) + C_q(3) + D_q(3).$$

The numbers of A-, C-, and D-bunches of the nonshortened $[q-1, 3, q-3]_q$ code (1.5) *are, respectively,*

$$A_q(3) = 2, \qquad C_q(3) = \begin{cases} \dfrac{q-1}{2}, & q \text{ odd}, \\ q-1, & q \text{ even}, \end{cases} \qquad D_q(3) = \frac{q-1}{2}, \quad q \text{ odd}.$$

For all q, base polynomials of A-bunches are of the form $f_1(x) = x$, $f_2(x) = x^{q-2} = x^{-1}$.

Proof. Use (3.1), Lemma 10, and its proof. $\triangle$

Lemma 12. *For the nonshortened $[q-1, 3, q-3]_q$ RS code* (1.5), *we have $T_q(3) = \left\lfloor \dfrac{q+1}{2} \right\rfloor$.*

Proof. The assertion follows from Lemma 11. $\triangle$

Theorem 9. *For any choice of locations in the shortened $[n, 3, n-2]_q$ RS code with generator matrix* (1.5), *we have*

$$M_q^{(-1)}(n, n-2) = 2q(q-1), \quad q \text{ is arbitrary}, \quad \left\lfloor \frac{q+1}{2} \right\rfloor + 1 \leq n \leq q-1. \tag{9.2}$$

Proof. Use Theorem 4 and Lemmas 11 and 12. A-words of length n can be obtained from the A-bunches of the nonshortened code specified in Lemma 11. $\triangle$

10. SHORT $[n, 3, n-2]_q$ RS CODES (1.5)

The following two constructions are conceptually close to Constructions 1 and 2, but instead of (6.1) we use (9.1). By Lemma 11, bunches with the base polynomials $f_1(x) = x$ and $f_2(x) = x^{-1}$

are A-bunches, whereas all other polynomials generate C- and D-bunches. When a code is shortened to length n, $q-1-n$ positions are deleted. Denote by Λ_n the set of assigned locations, and by Π_n, the set of products of the assigned locations. Recall that the zero location is not used in the RS code (1.5). If $|\Pi_n| < q-1$, then the equality $LT = a_{-1}$ (see (9.1)) cannot hold for $L, T \in \Lambda_n$ and $a_{-1} \in \mathbb{F}_q^* \setminus \Pi_n$. Therefore, C- and D-bunches of the nonshortened code with base polynomials $f(x) = x + a_{-1}x^{-1}$, where $a_{-1} \in \mathbb{F}_q^* \setminus \Pi_n$, turn into A-bunches of the shortened code. The number of new A-bunches is $q-1-|\Pi_n|$. To make the construction efficient, one should reduce the cardinality $|\Pi_n|$, thus increasing the cardinality $|\mathbb{F}_q^* \setminus \Pi_n| = q-1-|\Pi_n|$.

Thus, we are interested in the following combinatorial problems.

Let $\Lambda_n \subset \mathbb{F}_q^*$ be a subset of the multiplicative group of the field $\mathbb{F}_q$ of cardinality $|\Lambda_n| = n$, where $0 < n < q-1$. Introduce the set $\Pi_n = \{LT : L, T \in \Lambda_n,\ L \neq T\}$ composed of products of *distinct* elements of Λ_n. It is required to find the minimum $\min\limits_{\Lambda_n} |\Pi_n|$ and determine the structure of the minimizing subset Λ_n.

Since, when elements are multiplied, their logarithms are added modulo $q-1$, the problem can be reformulated as follows (cf. Section 7).

Let $0 < n < q-1$, and let $\Upsilon_n \subset \mathbb{Z}_{q-1}$ be a subset of the residue class ring modulo $q-1$ of cardinality $|\Upsilon_n| = n$. Introduce the restricted sum set $\Sigma_n^{\log} = \{\lambda + \tau \pmod{q-1} :\ \lambda, \tau \in \Upsilon_n,\ \lambda \neq \tau\}$. It is required to find the minimum $\min\limits_{\Upsilon_n} |\Sigma_n^{\log}|$ and determine the structure of the minimizing subset Υ_n.

Next, define $\Lambda_n = \{\alpha^i \mid i \in \Upsilon_n\}$, where α is a primitive element of $\mathbb{F}_q$. Then $|\Pi_n| = |\Sigma_n^{\log}|$ and $\min\limits_{\Lambda_n} |\Pi_n| = \min\limits_{\Upsilon_n} |\Sigma_n^{\log}|$.

As in Section 7, we use results of [12, chs. 2 and 9; 13, Problem 2.1]. If $q-1$ is a prime number, we can use Lemmas 7 and 8.

Lemmas 10 and 11 imply that $\min\limits_{\Lambda_n} |\Pi_n| < q-1$ if and only if $n \le \left\lfloor \dfrac{q+1}{2} \right\rfloor$. For such lengths n, constructions given below yield lower bounds on $q-1-\min\limits_{\Lambda_n} |\Pi_n|$ and thus upper bounds on $\min\limits_{\Lambda_n} |\Pi_n|$. In particular, the estimates obtained in Lemmas 8 and 13 are realized.

Let $v \ge 2$ be a divisor of $q-1$, and let $r = \dfrac{q-1}{v}$. Let $G_v = \{ir \mid i = 0, 1, \ldots, v-1\}$ be the additive subgroup of the ring $\mathbb{Z}_{q-1}$ consisting of v elements forming an arithmetic progression with common difference r. Denote by $G_v(w)$ the additive coset of G_v with generator $w \in \mathbb{Z}_{q-1}$, where $0 \le w \le r-1$ and $G_v(0) = G_v$.

Lemma 13. *Let* $v \mid (q-1)$, $r = \dfrac{q-1}{v}$, $n = tv \ge 3$, $1 \le t \le \dfrac{r}{2}$, $\Upsilon_n = \bigcup\limits_{w=0}^{t-1} G_v(w)$, *and* $\Lambda_n = \{\alpha^i \mid i \in \Upsilon_n\}$. *Then* $\Sigma_n = \bigcup\limits_{w=0}^{2t-2} G_v(w)$ *and* $|\Pi_n| = |\Sigma_n^{\log}| = (2t-1)v = 2n - \dfrac{n}{t}$.

Proof. Similarly to Lemma 9, we have the equality $G_v(w_1) + G_v(w_2) = G_v(w_1 + w_2)$, where the first sum is of set-theoretic sense; in the light of our problem, in the case of $w_1 = w_2$, distinct elements of the coset $H_v(w_1)$ are summed. $\triangle$

Construction 3. Locations L_u in the nonshortened $[q-1, 3, q-3]_q$ RS code with generator matrix (1.5) are chosen such that $L_u = \alpha^{u-1}$, where u is the position number, $u = 1, 2, \ldots, q-1$, and α is a primitive element of $\mathbb{F}_q$. A shortened $[n, 3, n-2]_q$ code of length $3 \le n \le \left\lfloor \dfrac{q+1}{2} \right\rfloor$ is formed. Here, $q-1-n$ rightmost positions in a codeword are deleted, with numbers $n+1, n+2, \ldots, q-1$ and locations $\alpha^n, \alpha^{n+1}, \ldots, \alpha^{q-2}$.

A-words of length n are chosen from $q+4-2n$ bunches with base polynomials

$$f_1(x) = x, \quad f_2(x) = x^{q-2} = x^{-1}, \quad f_j(x) = x + \alpha^{3-j}x^{-1}, \quad j = 3, 4, \ldots, q+4-2n.$$

Theorem 10. *Let* $3 \le n \le \left\lfloor \frac{q+1}{2} \right\rfloor$. *Then for the shortened* $[n, 3, n-2]_q$ *RS code with generator matrix* (1.5), *we have*

$$M_q^{(-1)}(n, n-2) \ge (q+4-2n)q(q-1), \tag{10.1}$$

$$M_q^{(-1)}(n, n-2) = (q+4-2n)q(q-1) \quad \text{if } q-1 \text{ is odd.} \tag{10.2}$$

The required number of A-words of length n *is guaranteed, for example, by Construction* 3.

Proof. By Lemma 11, bunches with base polynomials $f_1(x)$ and $f_2(x)$ are A-bunches, whereas all other polynomials generate C- and D-bunches. For an A-bunch, any shortening is admissible. We show that the choice of locations according to Construction 3 transforms C- and D-bunches of the nonshortened code into A-bunches of the shortened code. Indeed, let L and T be locations of positions of a shortened word, $T \ne L$. Then by the construction we have $L, T \in \{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{n-1}\}$, and the product is $LT \in \{\alpha^1, \alpha^2, \ldots, \alpha^{2n-3}\}$. On the other hand, the coefficient in a base polynomial $f_j(x)$ is $a_{-1} = \alpha^{3-j} \in \{\alpha^0, \alpha^{q-2}, \alpha^{q-3}, \ldots, \alpha^{2n-2}\}$. Thus, the equality $TL = a_{-1}$ is impossible, and according to Lemma 10(i) and equation (9.1) we have $f_j(L) \ne f_j(T)$, $j = 3, 4, \ldots, q+4-2n$.

The equality in (10.2) follows from Lemmas 7 and 8. $\triangle$

Construction 4. Let $v \mid (q-1)$, $r = \frac{q-1}{v}$, $n = tv \ge 3$, $1 \le t \le \frac{r}{2}$. A shortened $[n, 3, n-2]_q$ code with generator matrix (1.5) is formed. The set Λ_n of locations and the set Π_n of products of locations are of the form (see Lemma 13)

$$\begin{aligned} \Lambda_n &= \bigcup_{w=0}^{t-1} \{\alpha^{ir+w} : i = 0, 1, \ldots, v-1\}, \\ \Pi_n &= \bigcup_{w=0}^{2t-2} \{\alpha^{ir+w} : i = 0, 1, \ldots, v-1\}, \end{aligned} \tag{10.3}$$

where α is a primitive element of $\mathbb{F}_q$. (Thus, these sets are unions of multiplicative cosets of some subgroup of the multiplicative group of $\mathbb{F}_q$.) From (10.3) we get $|\Pi_n| = (2t-1)v = 2n - \frac{n}{t}$.

A-words of length n are chosen from $q + 1 - 2n + \frac{n}{t}$ bunches with base polynomials

$$f_1(x) = x, \qquad f_2(x) = x^{q-2} = x^{-1}, \qquad f_j(x) = x + a_{-1,j}x^{-1}, \quad a_{-1,j} \in \mathbb{F}_q^* \setminus \Pi_n,$$

where $j = 3, 4, \ldots, q + 1 - 2n + \frac{n}{t}$.

Theorem 11. *Let* $n \le \frac{q-1}{2}$. *For the shortened* $[n, 3, n-2]_q$ *RS code with generator matrix* (1.5), *we have*

$$M_q^{(-1)}(n, n-2) \ge (q+1-n)q(q-1), \quad n \mid (q-1), \tag{10.4}$$

$$M_q^{(-1)}(n, n-2) \ge \left(q + 1 - 2n + \frac{n}{t}\right) q(q-1), \quad n = tv, \quad v \mid (q-1), \quad 2 \le t \le \frac{q-1}{2v}. \tag{10.5}$$

The required number of A-words of length n *is guaranteed, for example, by Construction* 4.

Proof. The theorem directly follows from Lemmas 10(i) and 13 and from Construction 4. $\triangle$

Corollary. *Let* $n \le \frac{q-1}{2}$, *and let* $p \ge 2$ *be a prime. For the shortened* $[n, 3, n-2]_q$ *RS code with generator matrix* (1.5), *we have*

$$M_q^{(-1)}(n, n-2) \ge (q+1-n)q(q-1), \quad q \text{ odd}, \quad n = \frac{q-1}{2}, \tag{10.6}$$

$$M_q^{(-1)}(n,n-2)\geq (q+1-n)q(q-1),\quad q=p^{bm},\quad b\geq 1,\quad n=\frac{p^{bm}-1}{p^b-1}, \tag{10.7}$$

$$\begin{gathered}M_q^{(-1)}(n,n-2)\geq \left(q+1-2n+\frac{n}{t}\right)q(q-1),\quad n=tv,\quad q=p^{bm},\quad b\geq 1,\\ v=\frac{p^{bm}-1}{p^b-1},\quad 2\leq t\leq \frac{p^b-1}{2}.\end{gathered} \tag{10.8}$$

11. COMPARISON OF THE RESULTS

If we compare Theorems 6–11, the corollary, Remark 2, and equations (6.3), (7.7)–(7.11), (7.15), (8.2), (9.2), (10.1), (10.2), and (10.4)–(10.7), we see the following.

For an *odd* q, the estimates $M_q^{(-1)}(n,n-2)$ are better than $M_q^{(0)}(n,n-2)$ at least in the following cases:

$$\frac{q+1}{2}+1\leq n\leq q-1;$$

$$q=p^m,\quad p\geq 5,\quad n=\frac{q+1}{2}-\frac{p-1}{2}=\frac{q-p}{2}+1;$$

$$q=3^m,\quad n=\frac{q+1}{2}-4;$$

$$n=\frac{q-1}{2}.$$

If $n\mid (q-1)$, then, for both even and odd q, the estimates $M_q^{(-1)}(n,n-2)$ are often better than $M_q^{(0)}(n,n-2)$. Here we can also use Lemma 1.

On the other hand, for both even and odd q, the estimates $M_q^{(0)}(n,n-2)$ are in many cases better or at least not worse than $M_q^{(-1)}(n,n-2)$. In particular, for $n=q$ only the codes (1.3) exist.

Thus, in various situations, from the point of view of the cardinality of an A-subcode, both the code (1.3) or the code (1.5) can prove to be better. In a number of cases, both codes yield the same results.

To illustrate this, in Table 4 we present, using all the obtained results, the values of and lower estimates for $M_q^{(0,-1)}(n,n-2)=\max\{M_q^{(0)}(n,d),M_q^{(-1)}(n,d)\}$ in the $[n,3,n-2]_g$ RS code with $n\leq q$, $13\leq q\leq 32$. In the last-but-one column, we present two formulas if they give the same result. The shortened A-codes of lengths that are not specified in Theorems 6–11 and in the corollary are obtained with the use of Lemma 1.

Now we make some comparison of the obtained results with known parameters of permutation codes and their shortenings based on Lemma 1.

In [2, Propositions 1.2 and 1.3, Theorem 2.4, Table 2, Corollary 2.8], the following exact values of and estimates for the maximum possible cardinality $M^{\mathrm{PA}}(n,d)$ of a permutation array $(n,d)PA$ are given (the values (11.1) and (11.2) are given with references to earlier works):

$$M^{\mathrm{PA}}(q,q-1)=q(q-1),\quad q \text{ a prime power}, \tag{11.1}$$

$$M^{\mathrm{PA}}(Q,Q-2)=Q(Q-1)(Q-2),\quad (Q-1) \text{ a prime power}, \tag{11.2}$$

$$M^{\mathrm{PA}}(q,q-2)\geq \begin{cases}q(q-1), & q \text{ odd},\\ 2q(q-1), & q \text{ even},\end{cases}\quad q \text{ a prime power}, \tag{11.3}$$

$$M^{\mathrm{PA}}(q,q-2)\geq q^2,\quad q \text{ a prime power},\quad q\equiv 2 \pmod 3. \tag{11.4}$$

The exact value (11.2) was obtained in [14]. The estimate (11.4) was given in [2, Corollary 2.8] with a misprint, which is corrected here. The correct estimate was shown by P.J. Dukes.

If q is a prime power, equations (11.1)–(11.4) and Theorems 4–11 imply the following.

Table 4. Values of and lower estimates for $M_q^{(0,-1)}(n, n-2)$ in the $[n, 3, n-2]_q$ RS code

q	n	$d = n-2$	$M_q^{(0,-1)}(n, n-2)$		
13	13	11	$= 13 \cdot 12 = 156$	(6.3)	(1.3)
13	$8 \le n \le 12$	$6 \le d \le 10$	$= 2 \cdot 13 \cdot 12 = 312$	(9.2)	(1.5)
13	7	5	$\ge 3 \cdot 13 \cdot 12 = 468$	(7.7), (10.1)	(1.3), (1.5)
13	6	4	$\ge 8 \cdot 13 \cdot 12 = 1248$	(10.6)	(1.5)
$16 = 2^4$	16	14	$= 2 \cdot 16 \cdot 15 = 480$	(6.3)	(1.3)
$16 = 2^4$	$9 \le n \le 15$	$7 \le d \le 13$	$= 2 \cdot 16 \cdot 15 = 480$	(6.3), (9.2)	(1.3), (1.5)
$16 = 2^4$	$6 \le n \le 8$	$4 \le d \le 6$	$\ge 10 \cdot 16 \cdot 15 = 2400$	(8.2)	(1.3)
$16 = 2^4$	5	3	$\ge 12 \cdot 16 \cdot 15 = 2880$	(10.7)	(1.5)
17	17	15	$= 17 \cdot 16 = 272$	(6.3)	(1.3)
17	$10 \le n \le 16$	$8 \le d \le 14$	$= 2 \cdot 17 \cdot 16 = 544$	(9.2)	(1.5)
17	9	7	$\ge 3 \cdot 17 \cdot 16 = 816$	(7.7), (10.1)	(1.3), (1.5)
17	$6 \le n \le 8$	$4 \le d \le 6$	$\ge 10 \cdot 17 \cdot 16 = 2720$	(10.6)	(1.5)
19	19	17	$= 19 \cdot 18 = 342$	(6.3)	(1.3)
19	$11 \le n \le 18$	$9 \le d \le 16$	$= 2 \cdot 19 \cdot 18 = 684$	(9.2)	(1.5)
19	10	8	$\ge 3 \cdot 19 \cdot 18 = 1026$	(7.7), (10.1)	(1.3), (1.5)
19	$7 \le n \le 9$	$5 \le d \le 7$	$\ge 11 \cdot 19 \cdot 18 = 3762$	(10.6)	(1.5)
19	6	4	$\ge 14 \cdot 19 \cdot 18 = 4788$	(10.4)	(1.5)
23	23	21	$= 23 \cdot 22 = 506$	(6.3)	(1.3)
23	$13 \le n \le 22$	$11 \le d \le 20$	$= 2 \cdot 23 \cdot 22 = 1012$	(9.2)	(1.5)
23	12	10	$\ge 3 \cdot 23 \cdot 22 = 1518$	(7.7), (10.1)	(1.3), (1.5)
23	$8 \le n \le 11$	$6 \le d \le 9$	$\ge 13 \cdot 23 \cdot 22 = 6578$	(10.6)	(1.5)
$25 = 5^2$	25	23	$= 25 \cdot 24 = 600$	(6.3)	(1.3)
$25 = 5^2$	$14 \le n \le 24$	$12 \le d \le 22$	$= 2 \cdot 25 \cdot 24 = 1200$	(9.2)	(1.5)
$25 = 5^2$	13	11	$\ge 3 \cdot 25 \cdot 24 = 1800$	(7.7), (10.1)	(1.3), (1.5)
$25 = 5^2$	$9 \le n \le 12$	$7 \le d \le 10$	$\ge 14 \cdot 25 \cdot 24 = 8400$	(10.6)	(1.5)
$25 = 5^2$	8	6	$\ge 18 \cdot 25 \cdot 24 = 10800$	(10.4)	(1.5)
$27 = 3^3$	27	25	$= 27 \cdot 26 = 702$	(6.3)	(1.3)
$27 = 3^3$	$15 \le n \le 26$	$13 \le d \le 24$	$= 2 \cdot 27 \cdot 26 = 1404$	(9.2)	(1.5)
$27 = 3^3$	14	12	$\ge 3 \cdot 27 \cdot 26 = 2106$	(7.7), (10.1)	(1.3), (1.5)
$27 = 3^3$	$10 \le n \le 13$	$8 \le d \le 11$	$\ge 15 \cdot 27 \cdot 26 = 10530$	(10.6)	(1.5)
$27 = 3^3$	9	7	$\ge 19 \cdot 27 \cdot 26 = 13338$	(7.7)	(1.3)
29	29	27	$= 29 \cdot 28 = 812$	(6.3)	(1.3)
29	$16 \le n \le 28$	$14 \le d \le 26$	$= 2 \cdot 29 \cdot 28 = 1624$	(9.2)	(1.5)
29	15	13	$\ge 3 \cdot 29 \cdot 28 = 2436$	(7.7), (10.1)	(1.3), (1.5)
29	$9 \le n \le 14$	$7 \le d \le 12$	$\ge 16 \cdot 29 \cdot 28 = 12992$	(10.6)	(1.5)
29	8	9	$\ge 17 \cdot 29 \cdot 28 = 13804$	(7.7), (10.1)	(1.3), (1.5)
31	31	29	$= 31 \cdot 30 = 930$	(6.3)	(1.3)
31	$17 \le n \le 30$	$15 \le d \le 28$	$= 2 \cdot 31 \cdot 30 = 1860$	(9.2)	(1.5)
31	16	14	$\ge 3 \cdot 31 \cdot 30 = 2790$	(7.7), (10.1)	(1.3), (1.5)
31	$11 \le n \le 15$	$9 \le d \le 13$	$\ge 17 \cdot 31 \cdot 30 = 15810$	(10.6)	(1.5)
31	$7 \le n \le 10$	$5 \le d \le 8$	$\ge 22 \cdot 31 \cdot 30 = 20460$	(10.4)	(1.5)
31	$5 \le n \le 6$	$3 \le d \le 4$	$\ge 26 \cdot 31 \cdot 30 = 24180$	(10.4)	(1.5)
$32 = 2^5$	32	30	$= 2 \cdot 32 \cdot 31 = 1984$	(6.3)	(1.3)
$32 = 2^5$	$17 \le n \le 31$	$15 \le d \le 29$	$= 2 \cdot 32 \cdot 31 = 1984$	(6.3), (9.2)	(1.3), (1.5)
$32 = 2^5$	$10 \le n \le 16$	$8 \le d \le 14$	$\ge 18 \cdot 32 \cdot 31 = 17856$	(8.2)	(1.3)
$32 = 2^5$	9	7	$= 18 \cdot 32 \cdot 31 = 17856$	(8.2), (10.2)	(1.3), (1.5)
$32 = 2^5$	$6 \le n \le 8$	$4 \le d \le 6$	$\ge 26 \cdot 32 \cdot 31 = 25792$	(8.2)	(1.3)
$32 = 2^5$	5	3	$= 26 \cdot 32 \cdot 31 = 25792$	(8.2), (10.2)	(1.3), (1.5)

• The cardinality $M_q^{(0,-1)}(n, n-k+1)$ is *greater* than the estimates $M^{\mathrm{PA}}(q, q-k+1)$ if

$$\begin{aligned} &k=3,\ (q-1) \text{ is not a prime power},\ q \text{ odd},\ n \le q-1,\\ &k=3,\ (q-1) \text{ is not a prime power},\ q \text{ even},\ n \le \frac{q}{2}; \end{aligned} \tag{11.5}$$

• The cardinality $M_q^{(0,-1)}(n, q-k+1)$ *coincides* with the estimates $M^{\mathrm{PA}}(q, q-k+1)$ if

$$\begin{aligned} &k=2,\ q \text{ even or odd},\ n \le q,\\ &k=3,\ (q-1) \text{ is not a prime power},\ q \text{ even},\ \frac{q}{2}+1 \le n \le q,\\ &k=3,\ (q-1) \text{ is not a prime power},\ q \text{ odd},\ q \not\equiv 2 \pmod 3,\ n=q; \end{aligned} \tag{11.6}$$

• The cardinality $M_q^{(0,-1)}(n, q-k+1)$ is *less* than the estimates $M^{\mathrm{PA}}(q, q-k+1)$ if

$$\begin{aligned} &k=3,\ (q-1) \text{ is a prime power},\ q \text{ even or odd},\ n \le q,\\ &k=3,\ (q-1) \text{ is not a prime power},\ q \text{ odd},\ q \equiv 2 \pmod 3,\ n=q. \end{aligned} \tag{11.7}$$

Thus, under conditions (11.5), A-subcodes of RS codes with generator matrices (1.3) and (1.5) surpass (in cardinality) known shortened permutation codes, and under conditions (11.6), they are at least not worse than known codes and their shortenings. On the other hand, under conditions (11.7), known codes are better than the RS codes.

Taking into account the equality in (1.7), it follows from (11.1) and Theorem 5 (see (5.1)) that

$$M_q^{(0)}(q, q-1) = M^{\mathrm{PA}}(q, q-1) = M_q^{\mathrm{A}}(q, q-1) = q(q-1). \tag{11.8}$$

Thus, in a nonshortened RS code with generator matrix (1.3), A-subcodes of the $[q, 2, q-1]_q$ code are optimal A-codes.

12. CONCLUSION

In this paper, for q-ary $[n, k, n-k+1]_q$ RS codes of length $n \le q$ with dimension $k \le 3$ and with generator matrices (1.3) and (1.5), we obtain tight bounds and lower estimates for the maximum cardinality of an A-subcode, i.e., of a subset of codewords without identical symbols in a codeword. We construct codes attaining these bounds and estimates. Note that the problem in this paper was stated precisely for RS codes with generator matrices (1.3) and (1.5).

In solving this problem, the following approaches were found to be useful:

– Using and studying "classical" coding (1.2) with the help of information polynomials;

– Introducing the notion of a "*bunch of codewords*," where it suffices to analyze only one (base) word;

– Assigning locations in the code (1.3) considered as m-digit p-ary numbers for $q = p^m$, in ascending lexicographic order. Based on this, simple and efficient constructions of shortened codes;

– Efficient use of "standard" location assignment in the code (1.5);

– Specifying a set of locations in a shortened code as an additive or multiplicative subgroup.

It seems that some lower estimates for the maximum cardinality of an A-subcode obtained in the paper are in fact tight bounds.

To increase the cardinality of an A-subcode for given q and n, one has to study RS codes of larger cardinality, i.e., with $k \ge 4$. However, this would result in smaller distances between words of the A-subcode. Also, degrees of the analyzed polynomials would increase, which would make the

results more laborious and less transparent. Nevertheless, the proposed methods and approaches can be used in this case too.

Note also that the proposed methods can be applied for studying any linear codes that contain words of identical symbols; for instance, MDS codes related to projective spaces over finite fields. Here it is possible to solve problems that are not related to A-subcodes; for instance, finding the complete weight function of a code, constructing constant-composition codes, or finding the set of values of a nonpermutation polynomial on all elements of a field (see the bunch types in Section 4).

As is noted in Section 1, the considered problem is a part of a more general problem: *constructing A-codes with large cardinalities and distances*, including *construction of MDS codes with A-subcodes of large cardinalities*.

In these problems, the following directions of investigation can be marked out.

• Other variants of defining an RS code.

In particular, codes with generator matrix (1.4) for various values of b should be studied. Considering shortened codes of the doubly extended $[q+1, k, q-k+2]_q$ RS code might be of use.

• Other variants of coding for RS codes.

As an example, we mention systematic coding [4].

• Generalized Reed–Solomon (GRS) code.

Codewords of a GRS code can be obtained from words of an RS code by scalar multiplication by an arbitrary vector with nonzero elements [4]. Using GRS codes extends possibilities for solving the problem, but theoretical results for arbitrary vectors are difficult to obtain, which might lead to the necessity of computer-based estimates and constructions, say based on greedy algorithms.

• MDS codes nonequivalent to RS and GRS codes.

This is an extremely wide research area (see, e.g., [4–7] and bibliography therein). For instance, we mention cyclic $[q+1, k, q-k+2]_q$ MDS codes from [4, Theorem 11.9]. Note also MDS codes based on Cauchy matrices. An important role in solving this problem might be played by MDS codes related to projective spaces over finite fields.

• Permutation and constant-composition codes.

• Complete weight enumerator of a code.

The complete weight enumerator [4, Section 5.6; 15] yields a detailed information on the composition of symbols in codewords.

• The set of values of a nonpermutation polynomial on all elements of a field [8, ch. 7, Comments].

The authors are grateful to V.B. Afanas'ev for a useful discussion of the problems and to P.J. Dukes for sending copies of his works and comments to them. The authors are grateful to participants of the coding theory seminar at the Institute for Information Transmission Problems of the Russian Academy of Sciences for detailed discussion of the results and valuable remarks.

REFERENCES

1. Varakin, L.E., *Sistemy svyazi s shumopodobnymi signalami* (Communication Systems with Noise-like Signals), :, 1985.
2. Chu, W., Colbourn, C.J., and Dukes, P., Constructions for Permutation Codes in Powerline Communications, *Des. Codes Cryptogr.*, 2004, vol. 32, no. 1–3, pp. 51–64.
3. Dukes, P.J., Permutation Codes and Arrays, Section VI.44 of *Handbook of Combinatorial Designs*, Colbourn, C.J. and Dinitz, J.H., Eds., Boca Raton: Chapman & Hall, 2007, 2nd ed., pp. 568–571.
4. MacWilliams, F.J. and Sloane, N.J.A., *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977. Translated under the title *Teoriya kodov, ispravlyayushchikh oshibki*, Moscow: Svyaz', 1979.

5. Roth, R.M. and Seroussi, G., On Generator Matrices of MDS Codes, *IEEE Trans. Inform. Theory*, 1985, vol. 31, no. 6, pp. 826–830.

6. Roth, R.M. and Lempel, A., On MDS Codes via Cauchy Matrices, *IEEE Trans. Inform. Theory*, 1989, vol. 35, no. 6, pp. 1314–1319.

7. Kéri, G., Types of Superregular Matrices and the Number of n-Arcs and Complete n-Arcs in $\mathrm{PG}(r, q)$, *J. Combin. Des.*, 2006, vol. 14, no. 5, pp. 363–390; 2008, vol. 16, no. 3, pp. 262.

8. Lidl, R. and Niederreiter, H., *Finite Fields*, Reading: Addison-Wesley, 1983. Translated under the title *Konechnye polya*, 2 vols., Moscow: Mir, 1988.

9. Davydov A.A., Zyablov V.V., Kalimullin R.E. Subcodes of Reed–Solomon Code with Special Properties, in *Proc. 12th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2010), Novosibirsk, Russia, 2010*, pp. 116–122.

10. *Djurdjevic I., Xu J., Abdel-Ghaffar K.A.S., Lin S.* A Class of Low-Density Parity-Check Codes Constructed Based on Reed–Solomon Codes with Two Information Symbols, *Proc. 15th Int. Sympos. on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-15), Toulouse, France, 2003*, Fossorier, M.P.C., Høholdt, T., and Poli, A., Eds., Lect. Notes Comp. Sci., vol. 2643, Berlin: Springer, 2003, pp. 98–107.

11. Bassalygo, L.A., Dodunekov, S.M., Zinoviev, V.A., and Helleseth, T., The Grey–Rankin Bound for Nonbinary Codes, *Probl. Peredachi Inf.*, 2006, vol. 42, no. 3, pp. 37–44 [*Probl. Inf. Trans.* (Engl. Transl.), 2006, vol. 42, no. 3, pp. 197–203].

12. Tao, T. and Vu, V.H., *Additive Combinatorics*, New York: Cambridge Univ. Press, 2006.

13. Croot, E.S., III, and Lev, V.F., Open Problems in Additive Combinatorics, *Additive Combinatorics*, Granville, A., Nathanson, M.B., and Solymosi, J., Eds., CRM Proc. Lecture Notes, vol. 43, Providence: AMS, 2007, pp. 207–233.

14. Frankl, P. and Desa, M., On the Maximum Number of Permutations with Given Maximal or Minimal Distance, *J. Combin. Theory, Ser. A*, 1977, vol. 22, no. 3, pp. 352–360.

15. Blake, I.F. and Kith, K., On the Complete Weight Enumerator of Reed–Solomon Codes, *SIAM J. Discrete Math.*, 1991, vol. 4, no. 2, pp. 164–171.