CODES CORRECTING AN ARBITRARY SET OF ERRORS

by M. DEZA (*), M. G. KARPOVSKY (**)
and V. D. MILMAN (***)

RÉSUMÉ

Étant donné un groupe fini abélien G, nous étudions les sous-groupes (considérés comme codes correcteurs d'erreurs) de sous-espaces quelconques donnés (considérés comme ensemble d'erreurs). Cet article est une synthèse des résultats contenus dans [6]-[11].

La partie 2 donne des conditions suffisantes d'existence de codes linéaires corrigeant un ensemble d'erreurs donné dans un espace linéaire G. La partie 3 considère des codes qui sont des sous-groupes d'un groupe abélien G. La partie 4 fournit des estimations pour les meilleurs codes (linéaires ou non) corrigeant (ou détectant) un ensemble donné d'erreurs.

SUMMARY

Given a finite Abelian group G, we study the subgroups (considered as correcting codes) of arbitrary given subsets (considered as sets of errors). This paper is a survey of results from references [6]-[11].

The Section 2 gives sufficient conditions for existence of linear codes correcting given set of errors in linear space G. The Section 3 consider codes which are subgroups of Abelian group G. The Section 4 gives the estimations of best (linear or not) codes, correcting (or detecting) a given set of errors.

(*) C.N.R.S., Paris.

(**) State University of New York at Binghamton, Binghamton, N. Y., U.S.A.,

(***) Tel-Aviv University, Ramat-Aviv, Israël.

1.1. Let G be the group of n-vectors $(x^{(1)}, \ldots, x^{(n)})$, where $x^{(i)} \in \{0, \ldots, q_i - 1\}$ $(i = 1, \ldots, n)$, with the operation $\oplus$ of componentwise addition, so that the i-th components of the vectors add up modulo q_i $(i = 1, \ldots, n)$. Let $F \subseteq G$ $(0 = (0, \ldots, 0) \in F)$.

We shall say that a subset ξ of G is a code which corrects the error set F if, for any $x_1, x_2 \in \xi$ $(x_1 \neq x_2)$ and any $e_1, e_2 \in F$:

$$x_1 \oplus e_1 \neq x_2 \oplus e_2.$$

If ξ is a subgroup of G, ξ is called a linear code in G.

If $q_i = q$ $(i = 1, \ldots, n)$, where q is a prime, we shall refer to a code ξ in G as a code in a linear n-space [writing $E(n)$ instead of G]; otherwise ξ will be called a code in the Abelian group G.

1.2. The case, when G is a linear n-dimensional space over $GF(q)$ and F is a set of errors of a given multiplicity in the Hamming or Lee metric or the set of bursts of a given length, have been studied fairly well (*see*, e.g., [1, 2]). Recently a few papers have appeared on the construction of codes for the case G is an Abelian group and F is a set of errors of a given multiplicity [3, 4, 5]. The present paper is devoted to both types of codes and contains a survey of results from [6]-[11] about sufficient conditions of existence of codes that correct an arbitrary set of errors, methods for finding such codes and estimations for their cardinality.

The problem of correcting of a given set of errors arises when transmitted messages are outputs of some logical network. In this case an error in a single element of a network may result in an error of the multiplicity more than one in the vector of the output (by the multiplicity of the error we mean the number of distorted output lines). Thus for every error in a single element of the network we have some vector of error at the output, and for the network with m elements we have a set F of errors with $|F| = m$ at the output ($|F|$ is the cardinality of F). This set F depends only on the logical structure of our network.

Example 1: Let us consider the logical network of the Figure with n input binary lines $x_1, \ldots, x_n$ and 5 output lines $y_1, \ldots, y_5$. The error in the block B_1 may result in distortion of the signals at the outputs y_1, y_2 and the corresponding vector of error will be $e_1 = (1, 1, 0, 0, 0)$; for the error in B_2 the

$$F = \{e_1, e_2, e_3, e_4, e_5\}$$
$$= \{1, 1, 0, 0, 0), (1, 0, 1, 1, 1), (0, 1, 1, 1, 1), (1, 0, 0, 0, 0), (0, 1, 0, 0, 0), (0, 0, 1, 0, 0), (0, 0, 0, 1, 0), (0, 0, 0, 0, 1)\}$$

of errors at the output of the network.

Another example when the problem of correction of a given set of errors arises is the case of "artificial" noise when we consider a process of data-transmission as a game situation [8]. Section 2 of this paper will be devoted to sufficient conditions for the existence of linear codes in linear spaces $E(n)$, which correct a prescribed set of errors F.

1.3. In Section 3 we shall consider linear codes in Abelian groups, represented as a direct product of cyclic groups:

$$G = \underbrace{G_1 \times \ldots \times G_1}_{n_1} \times \underbrace{G_2 \times \ldots \times G_2}_{n_2} \times \ldots \times \underbrace{G_s \times \ldots \times G_s}_{n_s},$$

where each G_i is a cyclic group of order $|G_i| = q_i$ and the q_i's are distinct primes $(i = 1, \ldots, s)$.

All the results of these sections may be rephrased to apply to codes which detect a prescribed set F of errors.

Section 4 will be devoted to the estimations of the cardinalities of the best linear and nonlinear codes in linear spaces correcting or detecting a given set of errors.

2. CODES IN LINEAR SPACES

2.1. Let $E(n)$ denote n-space over $GF(q)$ and $F \subseteq E(n)$, $0 \in F$. Define:

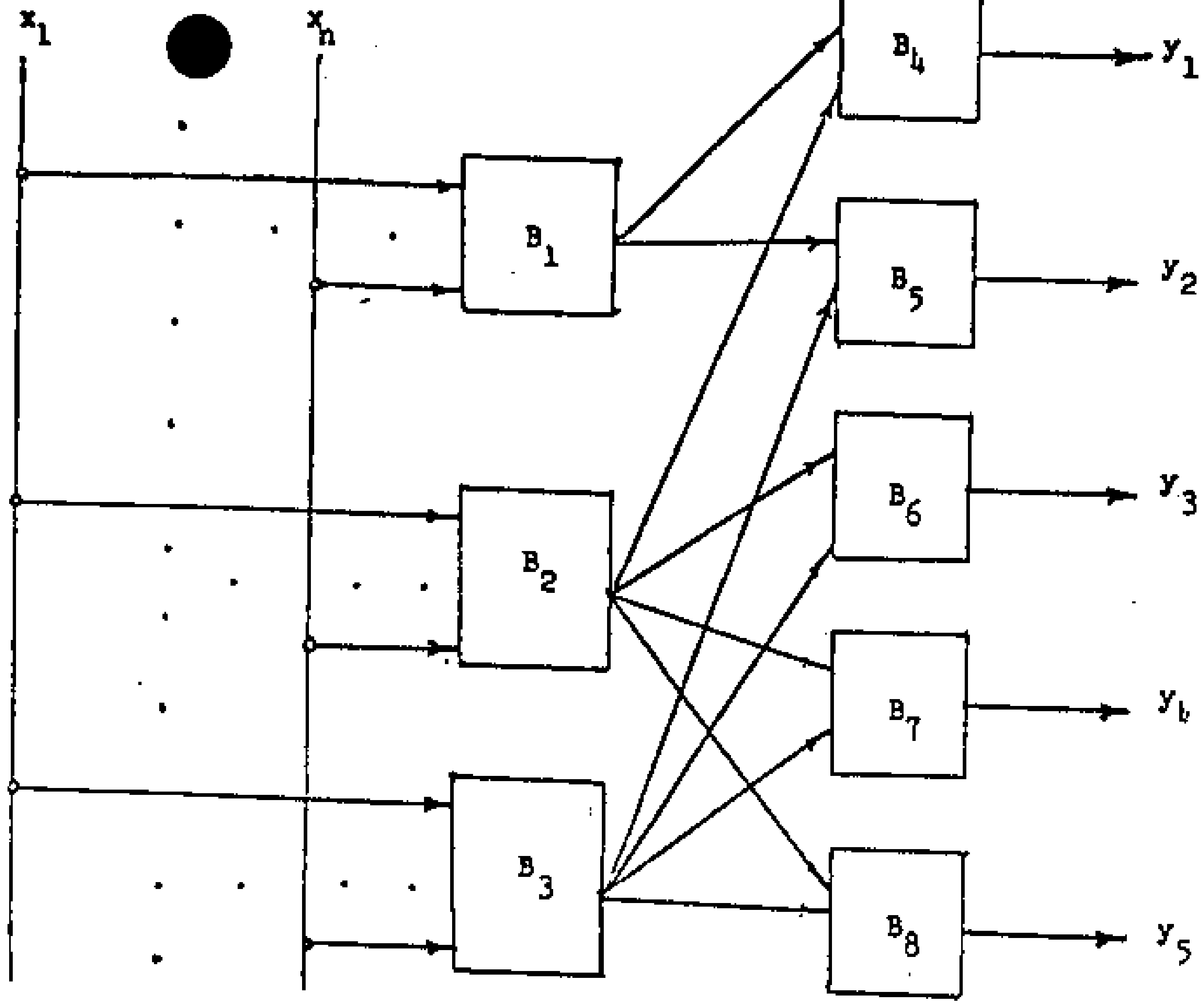
$$\theta(F) = \{e_i \theta e_j \mid e_i, e_j \in F\},$$

where θ is the symbol for componentwise subtraction mod q.

Theorem 1 [6, 11], the case $E(n)$ over $GF(2)$ [8]: *For any* $F \subseteq E(n)$ *if:*

$$|\theta(F)| \leq \frac{1}{q-1}(q^{n-k+1} - 1), \quad (1)$$

then there exists a linear (n, k)*-code correcting the error set* F.



Logical Network of Example 1.

According to Theorem 1, all we need in order to construct sufficient conditions for the existence of linear code correcting a prescribed set of errors is a satisfactory upper bound for $|\theta(F)|$.

Corollary 1 [6]: *If:*

$$\sum_{i=d}^{d+\varepsilon} \binom{n}{i} (q-1)^i \geqq q^n - \frac{1}{(q-1)} (q^{n-k+1} - 1), \tag{2}$$

then there exists a linear (n, k)-code ξ with base q and Hamming distance d such that:

$$\max_{x,\, y \in \xi - 0} \big| \|x\| - \|y\| \big| \leqq \varepsilon$$

(where $\|z\|$ is a number of nonzero components in a q-ary n-vector z). Note that in the case $\varepsilon = n - d$ the condition (2) *is very close to the well-known Varshamov-Gilbert bound* [1].

As another example, let us consider sufficient conditions for the existence of a linear binary $(q=2)$ code $\xi \subseteq E(n)$ correcting arbitrary "solid" burst errors of length b and multiplicity at most l. By a solid burst of length b and

... $E(n)$ such that:

$$e = \bigoplus_{i=0}^{n-b} c_i \gamma_i,$$

where $c_i \in \{0, 1\}$, $\sum_{i=0}^{n-b} c_i \leqq l$, and:

$$\gamma_i = (\underbrace{0, \ldots, 0}_{i}, \underbrace{1, 1, \ldots, 1}_{b}, \underbrace{0, \ldots, 0}_{n-b-i}) \qquad (i = 0, \ldots, n-b).$$

Corollary 2: *If:*

$$2^k \leq \frac{2^{n+1}}{\sum_{i=0}^{2l} \binom{n-b+1}{i} + 1}, \tag{3}$$

then there exists a linear binary (n, k)-code correcting solid bursts of length b and multiplicity at most l, where $l < 1/2\,(n-b+1)$.

2.2. Let $G(k)$ be the set of all k-dimensional subspaces of $E(n)$.

Theorem 2 [7]: *The number N_ξ of linear codes ξ in $E(n)$ such that $|\xi| = q^k$ and ξ corrects the error set F satisfies the condition:*

$$N_\xi \geqq \left(1 - \left(1 - \frac{q^n - |\theta(F)|}{q^n - 1}\right)(q^k - 1)\right) |G(k)|. \tag{4}$$

Note that $P(\xi) = N_\xi / |G(k)|$ may be interpreted as the probability that an arbitrarily selected subspace of dimension k in $E(n)$ will be a code ξ correcting the errors in F (assuming, naturally, that each k-dimensional subspace has the same probability of being selected).

It follows from (4) that even a small reduction in the number k of information digits of the code implies a rapid increase in the lower bound for $P(\xi)$. Thus, for large n, a relatively small number of tests will suffice to find a linear code ξ correcting the given error set F, having a number of information digits which is fairly close (and asymptotically equal) to the "best" number k defined by Theorem 1. We note also that for computing the weight distributions of codes constructed by Theorem 2, we may use the method described in [13].

3. ERROR-CORRECTING CODES IN ABELIAN GROUPS

3.1. Let G be finite Abelian group, with direct-product decomposition:

$$G = \underbrace{G_1 \times \ldots \times G_1}_{n_1} \times \underbrace{G_2 \times \ldots \times G_2}_{n_2} \times \ldots \times \underbrace{G_s \times \ldots \times G_s}_{n_s},$$

where G_i are cyclic groups, $|G_i| = q_i$, with q_i distinct primes $(i = 1, \ldots, s)$.

where $x_i \in E(n_i)$ $(i=1, \ldots, s)$.

A linear code in G, correcting a set $F \subseteq G$ $(0 \in F)$ of errors, is defined to be a subgroup ξ of G such that, for any $x, y \in \xi$ and $e, f \in F$,

$$x \oplus e \neq y \oplus f \ (x \neq y).$$

(Throughout, $\oplus$ is the symbol for componentwise addition of vectors $x=(x_1, \ldots, x_2)$ and $y=(y_1, \ldots, y_s)$ in G $(x_i, y_i \in E(n_i))$ the components of vectors x_i and y_i being added mod q_i.)

We now consider the question of sufficient conditions for the existence of linear codes $\xi \subseteq G$ correcting a prescribed error set F.

Note that if $G=\prod_{i=1}^{s} E(n_i)$, q_i are distinct primes, then any subgroup ξ of G such that $|\xi| = \prod_{i=1}^{s} q_i^{k_i}$ $(k_i \leqq n_i)$ is a direct product of subgroups $\xi_i = E(k_i)$ of the order $|\xi_i| = q_i^{k_i}$.

Consequently, if $F = F_1 \times \ldots \times F_s$, where $F_i \subseteq E(n_i)(0 \in F_i)$, then ξ is a linear code correcting the error set F, such that $|\xi| = \prod_{i=1}^{s} q_i^{k_i}$, iff ξ is a direct product of linear codes ξ_i in the linear spaces $E(n_i)$ correcting the error sets F_i, $|\xi_i| = q_i^{k_i}$ $(i=1, \ldots, s)$.

Thus, if $F = \prod_{i=1}^{s} F_i$, $F_i \subset E(n_i)$ we may utilize the method of Section 2 to find a linear code in the group $G = \prod_{i=1}^{s} E(n_i)$ which corrects the error set F.

We now consider the question of sufficient conditions for the existence of linear codes in groups when the set F fails to satisfy the condition formulated above.

3.2. Let $F \subset G = \prod_{i=1}^{s} E(n_i)$ be a set of errors and put $\theta(F) = \{ e \theta f \mid e, f \in F \}$, where θ denotes componentwise subtraction of vectors e and f, subtraction of each f_i from e_i being performed mod q_i $(i=1, \ldots, s)$.

Let:

$$C=(c_1, \ldots, c_s) \in \{0, 1\}^s (c_i \in \{0, 1\}; i=1, \ldots, s).$$

Denote:

$$G^{(C)} = \{ (c_1 x_1, \ldots, c_s x_s) \in G \mid x_i \in E(n_i), x_i \neq 0; i=1, \ldots, s) \},$$

$$\left(c_i x_i = \begin{cases} x_i, & c_i = 1 \\ 0, & c_i = 0 \end{cases} \right).$$

... be the set of all subgroups ξ in $G = \prod_{i=1}^{s} E(n_i)$ such that $|\xi| = \prod_{i=1}^{s} q_i^{k_i}$.

Theorem 3 [7]: *Let $F \subset \prod_{i=1}^{s} E(n_i)$ and N_ξ be the number of linear codes in $\prod_{i=1}^{s} E(n_i)$ such that ξ corrects the error set F and:*

$$|\xi| = \prod_{i=1}^{s} q_i^{k_i} (1 \leqq k_i \leqq n_i).$$

Let $P(\xi) = N_\xi |G(k_1, \ldots, k_s)|^{-1}$, and for every $C=(c_1, \ldots, c_s) \in \{0, 1\}^s$:

$$\alpha^{(C)} = \prod_{i=1}^{s} \frac{q_i^{k_i}-1}{q_i^{n_i}-1} |G^{(C)} \cap \theta(F)|. \tag{5}$$

If $\sum_{C \neq 0} \alpha^{(C)} < 1$, then $N_\xi \geqq 1$; moreover:

$$P(\xi) \geqq 1 - \sum_{C \neq 0} \alpha^{(C)}. \tag{6}$$

Example 2: Let $s=2$, $q_1=2$, $q_2=3$, $n_1=n_2=2$. Then:

$$E(n_1) = \{0, 1\}^2, \quad E(n_2) = \{0, 1, 2\}^2, \quad G = E(n_1) \times E(n_2),$$
$$|G| = q_1^{n_1} q_2^{n_2} = 36;$$

for every:

$$x \in G, \quad x=(x_1, x_2), \quad x_1 \in E(n_1), \quad x_2 \in E(n_2);$$
$$G^{(0,1)} = \{ (0, 0, x_2) \mid x_2 \in E(n_2) - 0 \},$$
$$G^{(1,0)} = \{ (x_1, 0, 0) \mid x_1 \in E(n_1) - 0 \},$$
$$G^{(1,1)} = \{ (x_1, x_2) \mid x_1 \in E(n_1) - 0, x_2 \in E(n_2) - 0 \}.$$

Suppose that the error set:

$$F = \{ (0, 0, 0, 0), (1, 1, 1, 1), (1, 1, 2, 2) \}.$$

Then:

$$\theta(F) = F \cup \{ (0, 0, 1, 1), (0, 0, 2, 2) \},$$
$$|G^{(0,1)} \cap \theta(F)| = 2, \quad |G^{(1,0)} \cap \theta(F)| = 0 \quad \text{and} \quad |G^{(1,1)} \cap \theta(F)| = 2$$

Let us estimate how many codes may be constructed such that every code ξ corrects the given error set F and:

$$|\xi| = q_1^1 q_2^1 = 6 \ (k_1 = k_2 = 1).$$

From (5), (6) we have $\alpha^{(0,1)} = 0.5$, $\alpha^{(1,0)} = 0$, $\alpha^{(1,1)} = 1/6$, and $P(\xi) \geqq 1/3$. Since our group G contains $|G(k_1, k_2)| = |G(1, 1)| = 12$ subgroups with six

It follows from Theorem 3 that (as in the case of codes in linear spaces) a relatively small reduction in the numbers k_i ($i=1, \ldots, s$) of information digits $\left(\text{in such a way that the transmission rate } \sum_{i=1}^{s} k_i / \sum_{i=1}^{s} n_i \text{ does not change as } n \to \infty\right)$ will bring the probability $P(\xi)$ close to unity, where $P(\xi)$ is the probability that any subgroup from $G(k_1, \ldots, k_s)$ is the desired code ξ. This implies a very simple procedure for searching for linear codes in finite Abelian groups, yielding codes which are sufficiently close to optimal.

The number of elements $|\xi|$ of a code ξ found with the aid of Theorem 3 depends on the choice of the parameters $\alpha^{(C)}$ for all $0 \in \{0, 1\}^s$. This motivates the following corollary from Theorem 3, which gives a sufficient condition that is more convenient, though coarser.

Corollary 3 [7]: *If:*

$$\prod_{i=1}^{s} (q_i^{k_i} - 1)^{c_i} \leqq (\sqrt[s]{2} - 1)^{\|C\|} \prod_{i=1}^{s} (q_i^{n_i} - 1)^{c_i} |G^{(C)} \cap \theta(F)|^{-1}, \tag{7}$$

for all $C = (c_1, \ldots, c_s) \in \{0, 1\}^s$ $(C \neq 0)$, *where* $\|C\| = \sum_{i=1}^{s} c_1$, *then for any* $F \subset \prod_{i=1}^{s} E(n_i)$ *there exists a code* $\xi \subset \prod_{i=1}^{s} E(n_i)$ *with* $|\xi| = \prod_{i=1}^{s} q_i^{k_i}$ $(1 \leqq k_i \leqq n_i)$, *correcting the error set* F.

We note also that all the results of Sections 1 and 2 may be generalized to linear codes ξ in linear space $E(n)$ or Abelian group $\prod_{i=1}^{s} E(n_i)$ correcting a given set F of errors and satisfying the additional restriction $\xi \subseteqq R$, where R is a given subset of $E(n)$ or $\prod_{i=1}^{s} E(n_i)$.

4. BOUNDS FOR THE CARDINALITIES OF THE BEST LINEAR AND NONLINEAR CODES CORRECTING OR DETECTING A GIVEN SET OF ERRORS

4.1. Let $E(n)$ be a linear n-dimensional space over $GF(q)$ and F $(0 \in F \subset E(n))$ be a given set of errors. Denote by $\eta(F)$ any largest code $(0 \subset \eta \subset E(n))$ correcting the errors of the set F [i.e., $\theta(\eta(F)) \cap \theta(F) = 0$] and

$$\frac{q^n}{|\theta(F)|} \leqq |\eta(F)| \leqq \frac{q^n}{|F|}. \tag{8}$$

In the classical case (when F is a sphere in a Hamming metric):

(i) right side of (8) is just Rao-Hamming sphere-packing bound and in case of equality $\eta(F)$ is a perfect code [1]; Analog of it is given in [14].

(ii) left side of (8) is just Gilbert bound and the case $q^n(|\theta(F)|)^{-1} \leqq |\xi(F)|$ corresponds to Varshamov modification of Gilbert bound [1]. In [12] Goppa has shown (in other notations) that $q^n(|\theta(F)|)^{-1} \leqq |\xi(F)|$ as $n \to \infty$ if $\xi(F)$ restricted to be subspace which is a irreducible Goppa code. In [11] is given the same bound for other specification of concept of subspace.

Some improvement of this generalized Gilbert bound (8) is given by the following result which is the corollary from Theorem 1.

Corollary 4: *For any* $0 \in F \subset E(n)$:

$$q^{n+1-]\log_q((q-1)|\theta(F)|+1)[} \leqq |\xi(F)| \leqq |\eta(F)| \tag{9}$$

(*where* $]a[$ *is a smallest integer* $\geqq a$).

We note also that Corollary 4 is an analog of Varshamov bound for arbitrary set of errors.

4.2. We shall call F_w $(0 \in F_w \subset E(n))$ a worst noise if $|\eta(F_w)| \geqq |\eta(F)|$ for any F such that $|F| = |F_w|$ and we shall call F_b $(0 \in F_b \subset E(n))$ a best noise if $|\eta(F_b)| \leqq |\eta(F)|$ $(|F| = |F_b|)$.

We shall estimate now the values $|\eta(F_w)|$, $|\xi(F_w)|$, $|\eta(F_b)|$, $|\xi(F_b)|$.

Theorem 4 [8-10]: (i) *For any* $1 \leqq m \leqq q^n$ *there exists the worst noise* F'_w *with* $|F'_w| = m$ *such that there exists subspace* $F(n-t)$, $F_w \subset E(n-t)$ *and* $|\theta(F'_w) \cap (g)| \geqq 2$ *for any* $g \in E(n-t)$, $g \neq 0$, *where* $(g) = \{k.g \mid k = 0, \ldots, q-1\}$. *So* $\xi(F'_w) = E(t)$ *where* $E(t) \oplus E(n-t) = E(n)$ *and for* $q = 2, 3$ $\eta(F'_w) = \xi(F'_w) = E(t)$, $|\eta(F_w)| = |\xi(F_w)|$;

(ii) *If* $\eta(F_w) \neq 0$ *then:*

$$1 < |\eta(F_w) q^{-n} |F_w|^2 < (q+1)^2, \tag{10}$$

and for $q = 2$:

$$2 < |\eta(F_w) 2^{-n} |F_w|^2 < 9. \tag{11}$$

We note also that left sides of (10) and (11) are valid for every error set F of (11) may be improved for $|F|>4$ even for linear codes. Namely, we have for $q=$ [illegible] from the Corollary 4 and for any F:

(12) $$2+\frac{|F|-4}{|\theta(F)|+1} \leqq |\xi(F)|2^{-n}|F|^2 \leqq |\eta(F)|2^{-n}|F|^2.$$

Thus asymptotically $(n\to\infty)$ $|\eta(F_w)|$ and $|\xi(F_w)|$ have the same order as generalized Gilbert and Varshamov bounds.

4.3. Let us consider now the bounds for cardinality of codes correcting the best noise F_b.

Theorem 5 [8-9]: *For any F_b we have:*

(13) $$|\xi(F_b)| = q^{n-]\log_q|F_b|[},$$

(14) $$\max\left(\frac{1}{q},\frac{1}{5}\right) < |\eta(F_b)|q^{-n}|F_b| \leqq 1.$$

Lower bound $1/q < |\eta(F_b)|q^{-n}|F_b|$ is valid for arbitrary noise F even for linear codes $\xi(F)$.

Thus for every q:

(15) $$n-]\log_q|F_b|[=\log_q|\xi(F_b)| \leqq \log_q|\eta(F_b)| \leqq n-\log_q|F_b|$$

and if $|F_b|=q^l$, then:

(16) $$|\xi(F_b)| = |\eta(F_b)| = q^{n-l}.$$

We can show [8, 9] that very "concentrated" [in some subspace of $E(n)$] or very "scattered" [in $E(n)$] subsets F are the best noises. The intermediary constructions (given in Theorem 4) between these two "inefficient extremes" are on the contrary the worst noises.

So, asymptotically $(n\to\infty)$ $|\xi(F_b)|$ and $|\eta(F_b)|$ have the order of generalized Rao-Hamming bound (8). We note, that all bounds given in Theorems 4 and 5 for codes correcting F_w and F_b are constructive.

4.4. The problem of finding $|\xi(F)|$ and $|\eta(F)|$ for any given set F is very complicated and, perhaps, any general algorithm will be not shorter than complete scanning. But the evident implication $F' \subseteq F \subseteq F'' \Rightarrow |\eta(F'')| \leqq |\eta(F)| \leqq |\eta(F')|$ give us the possibility to approximate "real" noise F by two "artificial" noises F′ and F″ such that it is easy to compute $|\eta(F')|$ and $|\eta(F'')|$.

We shall illustrate this situation for the linear codes by the following theorem.

$$E(m_1)\cup E(m_2) \subseteq F \subseteq E(m_1)\cup E(m_2)\cup E(m_3)$$

where $m_1 \geqq m_2 \geqq m_3$ and:

$$E(m_1)\cap E(m_2) = E(m_1)\cap E(m_3) = E(m_2)\cap E(m_3) = \{0\}.$$

Then:

(17) $$|\xi(F)| = q^{n-m_1-m_2}.$$

4.5. Let us estimate now the cardinality of the best codes detecting the given set F of errors. Code $0\in\eta\subseteq E(n)$ detects the errors from the set F iff:

$$\theta(\eta)\cap F = 0.$$

We denote the largest (linear) code detecting the errors from the set F by $(\xi^d(F))\ \eta^d(F)$.

It is evident that code η corrects F iff it detects $\theta(F)$. So, determination of $|\xi^d(F)|$ and $|\eta^d(F)|$ is more general problem that determination of $|\xi(F)|$ and $|\eta(F)|$.

One can easily see that:

(18) $$\frac{q^n}{|F\cup(-F)|} \leqq |\eta^d(F)| \leqq q^n - |F| + 1.$$

We can define by analogy noises F_b^d and F_w^d best and worst for detection and develop the similar results. For example, from [8, 9] follows:

(19) $$|\eta^d(F_b^d)| = |\xi^d(F_b^d)| = q^{]\log_q(q^n-|F_b^d|+1)[},$$

(20) $$|\eta^d(F_w^d)| = |\xi^d(F_w^d)| = q^{n-]\log_q|F_w^d|[}.$$

REFERENCES

[1] W. W. PETERSON, *Error-Correcting Codes*, 2nd edition, MIT Press, Cambridge, Mass., 1972.

[2] E. R. BERLEKAMP, *Algebraic Coding Theory*, McGraw-Hill, 1968.

[3] G. M. TENENGOLTS, Coding Systems with the Combined use of Pulse Tests in: *Abstract and Structure Theory of Relay Systems* (in Russian), *Izd. Nauka*, Moscow, 1966.

[4] B. LINDSTROM, On Group and Nongroup Perfect Codes in q Symbols, *Math. Scand.*, Vol. 25, pp. 149-158, 1969.

[5] M. HERZOG and I. SHONHEIM, Linear and Nonlinear Single-Error-Correcting Perfect Mixed Codes, *Information and Control*, Vol. 18, No. 4, May 1971.

[6] M. G. KARPOVSKY and V. D. MILMAN, On Subspaces Contained in Subsets of Finite Homogeneous Spaces, *Discrete Math.*, Vol. 22, pp. 273-280, 1978.

[7] M. G. KARPOVSKY and V. D. MILMAN, *Error Correcting Codes in Subsets of Linear Spaces and Abelian Groups* (submitted).

[8] M. DEZA, Comparison of arbitrary additive noises (in Russian), *Problemy Peredatchi Informatsii*, Vol. 3, pp. 29-38, 1965.

[9] M. DEZA, *Codage dans les conditions d'un bruit additif arbitraire*, preprint CRM-515, University of Montreal, 1975, pp. 1-69.

[10] M. DEZA, Racine minimum d'un groupe élémentaire abélien, *Can. J. Math.*, Vol. 27-34, pp. 619-826, 1975.

[11] M. DEZA and F. HOFFMAN, Some results related to generalized Varshamov-Gilbert bound, *I.E.E.E. I.T.*, pp. 517-518, July 1977.

[12] V. D. GOPPA, On Correcting of Arbitrary Noise with Irreducible Codes, *Problemy Peredatchi Informatsii*, Vol. 10, pp. 111-112, 1974.

[13] M. KARPOVSKY, On Weight Distribution of Binary Linear Codes, *I.E.E.E. on Information Theory*, Vol. 25, p. 1, 1979.

[14] G. COHEN and P. FRANKL, On tilings of the binary vector space, *Discrete Math.*, Vol. 31, pp. 271-277, 1980.