# CYBERNETICS AND CONTROL THEORY

1964

SovietRxiv

**Abstract**

**Full Text**

# CYBERNETICS AND CONTROL THEORY

**R. R. Varshamov**

# ON CERTAIN FEATURES OF LINEAR CODES CORRECTING ASYMMETRIC ERRORS

*(Presented by Academician V. S. Kulebakin on 28 February 1964)*

One of the important contemporary problems of the general theory of communication is the problem of increasing the reliability of message transmission.

Conventionally, a signal by means of which messages are transmitted may be represented as a sequence from a finite set of elements of the numerical set $\{0, 1, \dots, q-1\}$. Without loss of generality one may assume that $q = 2$. The set $D^n$ of $N = 2^n$ sequences of the form $x = (x_1, x_2, \dots, x_n)$, where each symbol $x_i$ assumes only two values: 0 or 1, is naturally regarded as the vector $n$-dimensional space over the field $D$ of residues modulo 2.

In the space $D^n$ we introduce the norm $|x|$, equal to the number of ones occurring in the sequence $x$, and the quantity $\delta(x, y) = ||x| - |y|| + |x - y|$ will be called the distance between the elements $x$ and $y$.

The generally accepted notion of distance between elements of the vector space $D^n$ is associated with the relation

$$\rho(x, y) = |x - y|, \tag{1}$$

which is the starting point of classical investigations in the constructive theory of coding. Here, however, we shall consider another, much less developed, but in practice no less important part of it, which studies coding systems with a discrete asymmetric channel.

In contrast to a symmetric channel, an asymmetric channel is one with unequal probabilities of damage to different elementary transmissions (pulses). In the binary case this means, for example, that the probability of transition of the symbol 1 into 0 in the signal as it passes through the channel is substantially less than the probability of transition of the symbol 0 into 1, or conversely. In this situation one usually neglects the smallest probabilities and attempts to protect the working signals only against certain partial damages (distortions) which at the present moment have the greatest probability. Such distortions we shall agree to call asymmetric.

In this connection there arises the question of for what $n$, $r$, and $M$ it is possible, among the $N$ possible signals $x$, to find $M$ signals resistant to $r$ asymmetric errors, i.e. permitting correction of $r$ asymmetric errors.

At present only a small number of works are known that give some separate solutions of this problem. This situation, in all probability, is explained by the following two circumstances:

1. The ineffectiveness of the mathematical tools usually used by information theory in solving analogous problems.
2. The impossibility of obtaining new, stronger results by the linear method of coding, which is very widespread in theory and most important in practical application (see, for example, ([2])).

An exact mathematical formulation of the indicated problem and the proof of 2 constitute the main content of the present article.

Mathematically, an asymmetric distortion of a signal $x$ means the ordinary addition to it of some $n$-dimensional vector (noise) $\varepsilon_x$, restricted only by the condition $|\varepsilon_x| = ||x + \varepsilon_x| - |x||$. We note two simple facts:

$$|xy| = \frac{1}{2}(|x| + |y| - |x + y|); \tag{2}$$

$$|xy| = \max\{|x|, |y|\} - {}^1/_2\bar{\rho}(x, y), \tag{3}$$

where $x \in D^n$, $y \in D^n$, $xy = (x_1y_1, x_2y_2, \dots, x_{ny}n)$. The first assertion is obvious; the second follows automatically from the relation

$${}^1/_2\bar{\rho}(x, y) = {}^1/_2(\|x\| - \|y\| - |x - y|) = \max\{|x|, |y|\} - |xy|.$$

**Lemma 1.** *For it to be possible to correct $r$ asymmetric errors, it is necessary and sufficient that the pairwise distances between the signals used be not less than $d = 2r + 1$.*

**Proof. Necessity.** Suppose that the set of signals under consideration is stable with respect to $r$ asymmetric errors. In the case $\bar{\rho}(x, y) \leqslant 2r$, for at least one distinct pair $x$ and $y$, according to (2), (3), and the evident equality

$$x(y + xy) = y(x + xy) = \bar{x}(x + xy) = \bar{y}(y + xy) = \theta$$

($\bar{x} = x + e$, $|e| = n$, $|\theta| = 0$), it is clear that the vectors $y + xy$ and $x + xy$ may serve as admissible interferences for them. If now, depending on the type of distortion, $0 \to 1$ or $1 \to 0$, we put

$$\varepsilon_x = y + xy, \quad \varepsilon_y = x + xy$$

or, respectively,

$$\varepsilon_x = x + xy, \quad \varepsilon_y = y + xy,$$

then in both cases, obviously, we shall have the relation

$$x + \varepsilon_x = y + \varepsilon_y,$$

contradicting the basic principle ($x + \varepsilon_x \neq y + \varepsilon_y,\ x \neq y$) characterizing codes correcting $r$ asymmetric errors.

**Sufficiency.** Suppose $\bar{\rho}(x, y) \geqslant 2r + 1$ ($x \neq y$). Then, according to (3) and the easily verified inequality

$$\bar{\rho}(x + \varepsilon_x,\ y + \varepsilon_y) \geqslant \bar{\rho}(x, y) - \bar{\rho}(\varepsilon_x, \varepsilon_y)$$

($|\varepsilon_x| = \|x + \varepsilon_x\| - |x|,\ |\varepsilon_y| = \|y + \varepsilon_y\| - |y|$) for any values $|\varepsilon_x| \leqslant r,\ |\varepsilon_y| \leqslant r$, we obtain

$$\bar{\rho}(x + \varepsilon_x,\ y + \varepsilon_y) \geqslant 1. \tag{4}$$

This inequality is equivalent to the basic relation for correcting codes ($x + \varepsilon_x \neq y + \varepsilon_y,\ x \neq y$), since otherwise, obviously,

$$\bar{\rho}(x + \varepsilon_x,\ y + \varepsilon_y) = 0,$$

which is impossible in view of (4). Thus, Lemma 1 is fully proved. In what follows we shall rely on the following

**Corollary to Lemma 1.** *The norm of every ($\neq \theta$) element of a vector space stable with respect to $r$ asymmetric errors is not less than $r + 1$.*

**Proof.** The signal space under consideration contains the vector $\theta$ a priori. Hence, by Lemma 1, for any of its elements $x \neq \theta$ the inequality

$$\bar{\rho}(x, \theta) = 2|x| \geqslant 2r + 1$$

holds, which leads to the assertion of the corollary:

$$|x| \geqslant r + 1.$$

**Lemma 2.** *Two isometric and isomorphic vector spaces $H$ and $H'$ are stable with respect to the same number of asymmetric errors.*

**Proof.** Let $x, y$ be any pair of elements of $H$, and let $x', y'$ be their images in $H'$. By hypothesis, the spaces $H$ and $H'$ are isometric and isomorphic; therefore

$$|x| = |x'|, \quad |y| = |y'|, \quad |x + y| = |x' + y'|,$$

whence

$$\bar{\rho}(x, y) = \bar{\rho}(x', y'),$$

which, by Lemma 1, completes the proof.

**Remark 1.** An invariant, with respect to the transformation

$$x \to g(x) \quad (|g| = n_1),$$

space $H$, appearing in Lemma 2, is isomorphic and isometric to some subspace $H' \subset D^{n_1}$, or, more precisely, in the case $H = gH$, the set $H$ can be mapped isometrically and isomorphically into the space $D^{n_1}$.*

Let us denote by $G(n, r)$ the totality of all possible subspaces of $D^n$ of maximal dimension $m_r(n)$, stable with respect to $r$ symmetric errors, and by $\bar{G}(n, r)$ the totality of all possible subspaces of $D^n$ of maximal dimension $\bar{m}_r(n)$, stable with respect to $r$ asymmetric errors. Let us also introduce for consideration the numerical function $V_r(x)$, defined

* An example of such a mapping may be the correspondence $x \to x'$ $(x \in H)$, where the vector $x'$ is obtained from $x$ by deleting from it exactly $|\bar{g}|$ of its coordinates corresponding to the nonzero components of the vector $\bar{g}$.

for all natural $x > 3r$, in the form

$$V_r(x) = \bar{m}_r(x) - \bar{m}_r(x - 2r) - 2r.$$

It is known ([3]) that, for it to be possible to correct $r$ symmetric errors, it is necessary and sufficient that the pairwise distances (in the sense of (1)) between the signals used be not less than $d = 2r + 1$. Therefore it is clear that, for any $n > 2r$,

$$\bar{m}_r(n) \geq m_r(n). \tag{5}$$

**Theorem.** For every zero $n$ of the function $V_r(x)$, the equality

$$G(n, r) = \bar{G}(n, r)$$

holds.

**Proof.** Let $G$ be an arbitrary element of $G(n, r)$. It is immediately clear that, in order to prove the theorem, in view of (5), it suffices to show that the code distance* of the subspace $G$, for any $n$ $(V_r(n) = 0)$, is equal to $2r+1$, or, what is the same ([3]), that the norm of each of its $(\neq 0)$ elements is not less than $2r + 1$. Suppose that in $G$ there exists a vector $\omega$, different from the zero vector, whose norm is

$$|\omega| = q \leq 2r. \tag{6}$$

Consider in $G$ an arbitrary vector $x$. The vector $x + \omega$ $(\neq x)$ will also belong to $G$. If $|x| \geq |x + \omega|$, then $\bar{\rho}(x, x + \omega) = |x| - |x + \omega| + |\omega|$, and, by Lemma 1,

$$2I_\omega(x) = |x| - |x+\omega| + |\omega| \geq 2r+1.$$

If $|x| < |x+\omega|$, then $\bar{\rho}(x, x+\omega) = |x+\omega| - |x| + |\omega| \geq 2r+1$, and, by (6),

$$2I_\omega(x) = |x| - |x+\omega| + |\omega| \leq 2r-1.$$

The last two inequalities give the important relation

$$I_\omega(x) \neq r \qquad (x \in G). \tag{7}$$

The correspondence $x \to \bar{\omega}x$ gives rise to a homomorphism $G \sim \omega G$ with kernel $H = \bar{\omega}H$, invariant with respect to the transformation $x \to \bar{\omega}x$, and, by (2), (6), (7), as well as by the consequence of Lemma 1, with defect $h$ connected by the inequality

$$h \geq \bar{m}_r(n) - q + 1.$$

Since $|\bar{\omega}| = n - |\omega| = n - q$, it follows, according to Lemma 2 and Remark 1, that the isometric and isomorphic mapping of the kernel $H$ into the space $D^{n-q}$ gives rise to a subspace $H' \subset D^{n-q}$, stable with respect to $r$ asymmetric errors. In particular, the spaces $H$ and $H'$ are isomorphic, and therefore $h = h'$, where $h'$ is the dimension of $H'$. This permits one to obtain the inequality

$$\bar{m}_r(n-2r) \geq h - 2r + q \geq \bar{m}_r(n) - 2r + 1,$$

which leads to the relation $V_r(n) \neq 0$, contradicting the condition of the theorem. Thus the assumption $|\omega| \leq 2r$ is false; consequently, $|\omega| \geq 2r+1$, which was required to be proved.

**Remark 2.** By virtue of the well-known estimates of the function $m_r(x)$ and taking (5) into account, it is easy to establish that

$$A(x) = x + O(\log x),$$

where $A(x)$ is the number of zeros of the function $V_r(x)$ not exceeding $x$. Hence it is seen that the requirement (which is essential) $V_r(n) = 0$, appearing in the condition of the theorem, is fulfilled for almost all** natural $n$; consequently, almost always the equality

$$G(n, r) = \bar{G}(n, r)$$

holds.

Institute
of Automation and Telemechanics

Received
26 II 1964

## CITED LITERATURE

1. W. H. Kim, C. V. Freiman, *IRE Trans. Inform. Theory*, **5**, 2, 62 (1959).

2. R. R. Varshamov, *DAN*, **117**, No. 5 (1957).

3. R. R. Varshamov, *Collection of Works of the Scientific-Technical Society of Radio Engineering and Electrical Communications named after A. S. Popov*, **3**, 1959, p. 43.

* The minimum distance (in the sense of (1)) between elements of the code set.

** That is, $\bar{A}(x) = o(x)$ ($\bar{A}(x) = x - A(x)$).

*Note: Figure translations are in progress. See original paper for figures.*