MATHEMATICS

R. R. VARSHAMOV

1957

SovietRxiv

Abstract

Full Text

MATHEMATICS

R. R. VARSHAMOV

AN ESTIMATE OF THE NUMBER OF SIGNALS IN ERROR-CORRECTING CODES

(Presented by Academician A. N. Kolmogorov, 10 VI 1957)

Coding systems have become widespread in which the signals are sequences consisting of elementary symbols of two kinds. Such a signal can be denoted by a sequence of ones and zeros, for example, in the form 1101001101. The set D^n of $N = 2^n$ sequences of the form $a = (a_1, a_2, \dots, a_n)$, where each symbol a_i can take only two values: 0 or 1, is natural to regard as a vector n-dimensional space over the field D of residues modulo 2 (this field consists of the two elements 0 and 1). In the space D^n it is natural to introduce a **norm** $|a|$, equal to the number of ones occurring in the sequence a, and to take $\rho(a', a'') = |a' - a''|$ as the **distance** between the elements a' and a''.

If signals are transmitted with errors and it is desired to correct these errors, then not all N possible signals a are used for transmitting messages, but some subset of M signals. It is known ([1]) that, for it to be possible to correct r erroneous symbols, it is necessary and sufficient that the pairwise distances between the signals used be not less than $d = 2r + 1$. In this connection there arises the question of for which n, r, and M it is possible, among the N signals, to find M signals with pairwise distances not less than d*. Apart from more special results, for this the following necessary condition is known ([2]):

$$M \leqslant \frac{N}{S_n^r} \tag{1}$$

and the sufficient condition

$$M \leqslant \frac{N}{S_n^{d-1}}, \tag{2}$$

where

$$S_n^q = 1 + C_n^1 + \cdots + C_n^q, \qquad C_n^p = \frac{n!}{p!(n-p)!}.$$

If the signals a are used for transmitting messages $b = (b_1, b_2, \dots, b_m)$ from D^m, then $M = 2^m$.

Putting $n = m + k$, one can for this special case write conditions (1) and (2) in the form

$$S_n^r \leqslant 2^k, \tag{1a}$$

$$S_n^{d-1} \leqslant 2^k. \tag{2a}$$

The main result, which will be proved below, is that the sufficient condition (2a) can be weakened in the following way:

$$S_{n-1}^{d-2} = S_k^0 C_{m-1}^{d-2} + S_k^1 C_{m-1}^{d-3} + \cdots + S_k^{d-3} C_{m-1}^1 + S_k^{d-2} C_{m-1}^0 < 2^k. \tag{3}$$

* This problem can also be posed for even d, but the case of even d is trivially reduced to the case of odd d. Throughout, for us $d = 2r + 1$ is odd.

In the case $r = 1$ (correction of one error), the necessary condition (1a) and the sufficient condition (3) coincide and reduce to the inequality

$$n + 1 \leq 2^k, \tag{4}$$

which can also be written in the form

$$m \leq 2^k - k - 1 \tag{4a}$$

(here the relation between the number of symbols m in the transmitted message and the number k of "additional"symbols added to make error correction possible is directly visible).

A coding method allowing the correction of one error under condition (4) was indicated by Hamming ([2]). We shall obtain Hamming' s result as a special case of a general coding method with the possibility of correcting r errors under condition (3).

Like Hamming's method, our coding method is **linear**, i.e., if messages $b' \in D^m$, $b'' \in D^m$ are transmitted by signals a' and a'', then the message $b' + b''$ is transmitted by the signal $a' + a''$. In order to specify a linear coding method, it is enough to specify the signals $a^1, a^2, \dots, a^m$ by which the "basic" messages $e^1, e^2, \dots, e^m$ are transmitted, where $e^i = (e_1^i, e_2^i, \dots, e_m^i)$, $e_j^i = 1$ for $i = j$; $e_j^i = 0$ for $i \neq j$.

We first solve an auxiliary problem: choose, in D^k, a set C of m elements such that for any pairwise distinct $c^1, c^2, \dots, c^{d-1}$ from C the inequalities

$$\begin{gathered} |c^1| \geq d-1, \\ |c^1+c^2| \geq d-2, \\ \ldots\ldots\ldots\ldots \\ |c^1+c^2+\cdots+c^{d-1}| \geq 1. \end{gathered} \tag{5}$$

are satisfied.

We shall solve the problem by successively choosing the elements c^q, one after another. It is easy to calculate that, when $q-1$ elements c^p have already been chosen, there are no more than

$$C_{q-1}^{d-2} + S_k^1 C_{q-1}^{d-3} + \cdots + S_k^{d-3} C_{q-1}^1 + S_k^{d-2}$$

elements $c \in D^k$ which, because of the imposed restrictions, cannot be chosen as c^q. In order that it be possible to choose all elements c^q up to and including the m-th, it is sufficient that, at the last choice of the m-th element, the number of forbidden elements be less than the total number of elements in D^k, i.e., less than 2^k. This is precisely our condition (3).

The elements a^q from D^n that we need are constructed as follows:

$$\begin{gathered} a^1 = (1, 0, \ldots, 0, c_1^1, c_2^1, \ldots, c_k^1), \\ a^2 = (0, 1, \ldots, 0, c_1^2, c_2^2, \ldots, c_k^2), \\ \ldots\ldots\ldots\ldots \\ a^m = (0, 0, \ldots, 1, c_1^m, c_2^m, \ldots, c_k^m). \end{gathered}$$

The set $A \subseteq D^n$ of elements a used for transmitting messages consists of elements of the form

$$a = \sum_{q=1}^{m} b_q a^q. \tag{6}$$

The distance between two elements a' and a'' from A is equal to the norm $|a|$ of the difference $a = a'' - a'$, which also belongs to A. It is easy to see that for a of the form (6), $|a| = |b| + |c|$, where

$$c = \sum_{q=1}^{m} b_q c^q.$$

If $|b| \geqslant d$, then $|a| \geqslant d$. If $|b| < d$, then c is the sum of $|b|$ vectors c^q different from zero, and, by virtue of condition (5), $|c| \geqslant d - |b|$, i.e. $|a| \geqslant d$. This

completes the proof that the distance between two elements of A cannot be less than d.

Conditions (1a), (2a), and (3) make it possible to obtain lower and upper estimates for the minimal number $k_d(m)$ of additional symbols that allow messages of m symbols to be transmitted by signals with pairwise distances $\geqslant d$, i.e. with the possibility of correcting r errors. It is easy to establish that the lower estimate corresponding to (1a) has the form

$$k_d(m) \geqslant \underline{k}_d^a(m) \sim r \log_2 m; \tag{7}$$

while the upper estimates obtained from (2a) and (3) have, respectively, the form:

$$k_d(m) \leqslant \overline{k}_d^a(m) \sim (d-1) \log_2 m, \tag{8}$$

$$k_d(m) \leqslant \overline{k}_d(m) \sim (d-2) \log_2 m, \tag{9}$$

where $f \sim g$ denotes $f : g \to 1$.

Received
10 VI 1957

CITED LITERATURE

[1] A. A. Kharkevich, *Essays on the General Theory of Communication*, Moscow, 1955. [2] R. W. Hamming, Bell Syst. Techn. J., **29**, 2, 147 (1950).

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