On a Non-Binary Error-Correcting Code

SUGURU ARIMOTO*

In the data processing system containing computers, it may be worth while considering a class of error-correcting codes whose encoding, decoding and error-correcting schemes are easily programmed and require no excessive storage capacity and no long computing time.

Since R. W. Hamming showed the single-error-correcting group code (the so-called Hamming code), many investigations of group codes have been made.

Let us introduce some notations and definitions to describe our results. Let G_n be the set of n-dimensional binary signals (each signal has length n). G_n contains 2^n different signals, and may be considered as an additive group or a vector space on the prime field Z_2 of characteristic 2 under the condition of modulo 2 addition. Hence, signals may be called vectors. We denote by $||X||$ the number of ones in coordinates of the vector. A subspace of G_n norm of each of whose vetors (except the null vector) is equal to or greater than $d=2e+1$, is called an $(n\ d)$ subspace of G_n. Any $(n\ d)$ subspace of G_n can be represented as the kernel of some linear transformation which gives us encoding and decoding schemes. Whenever signals are so encoded that they may belong to the $(n\ d)$ subspace of G_n, it is possible to correct every error whose norm is not greater than e.

Let p be any prime number and each coordinate x_i of X belongs to the prime field Z_p of characteristic p. Then, p-ary group codes can be treated in the same way with binary group codes as described above, the norm being defined by

$$||X||=\sum_{i=1}^{n} {x_i}^{p-1},$$

where $X=(x_1, x_2, \cdots, x_n)$, ${x_i}^{p-1}=1$ for $x_i \neq 0$, and ${x_i}^{p-1}=0$ for $x_i=0$. In the case of binary codes, multi-error-correcting group codes are not so easy to construct and the correction usually requires a significant amount of time.

When $p>n$, we obtain a new multi-error-correction p-ary group code and an interesting error-correcting method. This code is represented as the kernel of the following linear transformation.

This paper first appeared in Japanese in the Journal of Information Processing Society of Japan, Vol. 2, No. 6 (1961), pp. 320-325.

* Faculty of Engineering, University of Tokyo.

$$T=\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{2e-1} \\ & \cdots & \cdots & & \\ 1 & n & n^2 & \cdots & n^{2e-1} \end{pmatrix}.$$

We can easily prove that this code is an $(n\ d)$ subspace of G_n. Therefore, it is possible in principle to correct every error whose norm is not greater than the prescribed value e. But, in this case, there exists another correcting method, that is, every error whose norm is not greater than e can be explicitly corrected by solving an algebraic equation and linear equations on the prime field Z_p.

Let X be an encoded vector, and Y a received vector. The error vector A may be described as $A=Y-X$. By decoding, we have $C=YT$, and

$$AT=(Y-X)T=YT=C. \tag{1}$$

If we know the norm of the vector A, we can solve the equation (1). That is, the equation (1) may be represented as follows:

$$\left.\begin{array}{llll} a_1 & +a_2 & +\cdots+a_k & =c_0, \\ a_1n_1 & +a_2n_2 & +\cdots+a_kn_k & =c_1, \\ & \cdots\cdots\cdots\cdots\cdots\cdots & & \\ a_1{n_1}^{2k-1}+a_2{n_2}^{2k-1}+\cdots+a_k{n_k}^{2k-1} & & & =c_{2k-1}, \end{array}\right\} \tag{2}$$

where a_i is the n_i-th element of the vector A and not zero for $i=1, \cdots, k$.

Now, we shall show that the norm of the vector A can be derived from the known vector C. Let

$$C^{(i)}=\begin{pmatrix} c_0 & c_1 & \cdots & c_{k-1} \\ c_1 & c_2 & \cdots & c_k \\ \cdots & \cdots & & \\ c_{k-1} & c_k & \cdots & c_{2k-2} \end{pmatrix}.$$

Suppose $\mathrm{Det}(C^{(i)})=0$ for $i\geqq k+1$, and $\mathrm{Det}(C^{(k)})\neq 0$ for k, it will be easily proved that the norm of the vector A is equal to k.

This code may be very useful for the easiness of its construction and the generality of the parameters $p(>n)$ and e. The error-correcting method is systematic and easily programmed for a digital computer and requires a small storage capacity.