Systematic Codes Using Binary Shift Register Sequences

TADAO KASAMI*

1. *Abstract*

It is shown that most of the systematic codes using binary shift register sequences can be treated with in a unified manner, and their algebraic properties are clarified, from which the basic theory of encoding and decoding is derived.

Further, a new class of systematic codes, denoted by Π_0-type code hereafter, is introduced, which has a remarkable feature as will be stated below. Let C denote the cyclic shift operator. For any two error vectors e and e', if there exists an integer p such that $e'=C^p e$, we define that they belong to the same error-pattern. Then, Π_0-type codes are defined to be the systematic codes with the following property:

If a code S can correct an error e, then S can always correct all errors of the error-pattern including e through a suitable choice of decoding procedure.

Since even in the case of non-independent errors most members of an error-pattern have a common probability of occurrence, it may be reasonable to treat with error-patterns rather than to treat with errors one by one.

This paper presents the necessary and sufficient condition of Π_0-type code, from which all Π_0-type codes with a given odd code length can explicitly be obtained. This class contains several new efficient sodes as well as the cyclic Hamming codes and the the cyclic Golay codes. Also, the codes of Π_0-type may be instrumented in a simple fashion.

2. *Basic Theorems*

Let V_n be the space of binary n-tuples $(x_0, x_1, \cdots, x_{n-1})$; let S, the code, be a k-dimensional subspace and let C, the cyclic shift operator, be defined as

$$C\cdot(x_0, x_1, \cdots, x_{n-1})\equiv(x_{n-1}, x_0, \cdots, x_{n-2})\,.$$

A code S is called a cyclic code if for each vector x in S, the vector Cx is also in S. Some cyclic codes have been studied by Prange from a different point of view[1]. Also, the Abramson codes[2], the Fire codes[3] and the Melas codes[4] are all cyclic.

In the mathematical versions, the definition of Π_0-type code follows

* Faculty of Engineering, Osaka University

such that:

If for any vector $x \notin S$, x, Cx, $\cdots$, $C^{n-1}x$ all belong respectively to n distinct coset of V_n modulo S different from S, then S is defined to be Π_0-type.

From this definition, it follows that Π_0-type codes are of the cyclic codes. In what follows, S is assumed to be a cyclic code except for Section 5. For two vectors x and y, if there exists an integer p such that x and $C^p y$ belong to the some coset of V_n modulo S, then we denote

$$x \sim y .$$

This relation "$\sim$" classifies the vectors of V_n uniquely into disjoint clases, denoted by $\Gamma_0(=S)$, Γ_1, $\cdots$, Γ_r. Γ_i consists of γ_i cosets and is invariant under C. If a member of an error-pattern P is included in Γ_i, all members of P are also included in Γ_i. Then we denote $P \in \Gamma_i$. If S is a Π_0-type code,

$$r_i = n ; \ i = 1, 2, \cdots, \ r = \frac{2^{n-k}-1}{n} .$$

Lemma: For any set of r' error-patterns $\{P_j\}$ such that $P_j \in \Gamma_{i_j}$ $(i_1 < i_2 < \cdots < i_{r'})$ and $\gamma_{i_j} = n$, S can correct all errors belonging to P_j's through a suitable decoding procedure. If S is of Π_0-type, S can correct just r error-patterns.

Let R_n denote the set of all polynomials of degree less than n with coefficients from $GF(2)$. Let $x=(x_0, x_1, \cdots, x_{n-1})$ correspond to the polynomial $x(u) \equiv x_0 + x_1 u + \cdots + x_{n-1} u^{n-1}$, and let I denote the subset of R corresponding to S.

The following theorems are proved.

Theorem 1: The necessary and sufficient condition that S is a cyclic code is that there exists a polynomial $g(u)$ of degree m $(=n-k)$ such that

(i) $$u^n + 1 \equiv 0 \quad [\text{modd } 2, \ g(u)] ,$$

and (ii) a polynomial $x(u)$ in R_n is in I, if and only if

$$x(u) \equiv 0 \quad [\text{modd } 2, \ g(u)] .$$

The polynomial $g(u)$ in Theorem 1 will be called the characteristic polynomial of S and a cyclic code whose characteristic polynomial is $g(u)$ will be designated as $S(g(u))$.

Corrollary: Suppose that

$$x \in \Gamma_i , \qquad y \in \Gamma_j ,$$

then $i \neq j$, if and only if

$$y(u) + u^p x(u) \not\equiv 0 \quad [\text{modd } 2, \ g(u)] ; \quad 0 \leq p \leq n-1 .$$

Theorem 2: A cyclic code $S(g(u))$ is a Π_0-type code, if and only if the characteristic polynomial $g(u)$ is an irreducible polynomial or a product of distinct irreducible polynomials having the common period n.

Based on this theorem, all of Π_0-type codes with any given odd n may be formed by referring to the table of irreducible polynomials over $GF(2)$[2].

In what follows, S is assumed to correct at least any single error. Hence, n is the least integer such that

$$u^n+1\equiv 0 \qquad [\text{modd } 2,\ g(u)]\,.$$

3. *Encoding and Decoding*

Let $SR_m(f)$ denote the m-stage linear feedback shift-register with the characteristic polynomial[8]

$$f(u)\equiv\sum_{i=0}^{m} f_i u^i\,,$$

let $\Xi_i\equiv(\xi_{i+m-1},\cdots,\xi_i)$ denote the state vector of $SR_m(f)$ at the i-th clock-time, and let delay operator D be defined such that

$$D\cdot(\xi_{i+m-1},\cdots,\xi_i)\equiv(\xi_{i+m-2},\cdots,\xi_{i-1})\,.$$

From the definition of the characteristic polynomial, it follows that

$$\xi_j=\sum_{i=1}^{m} f_{m-i}\xi_{j-i}\,.$$

The state diagram of $SR_m(f)$ consists of a cycle of 1-cycle length, K_0, and r cycles $K_1, K_2, \cdots, K_r$.

Theorem 3: Let the initial state vector Ξ_0 be equal to $(1, 0, \cdots, 0)$, and let A denote the $n\times m$ matrix whose i-th row is equal to the state vector Ξ_i of $SR(g)$. Then the transposed matrix of A is a parity-check matrix of the cyclic code $S(g(u))$.

Let us designate the parity-check sequence corresponding to an error vector e as $\eta(e)$, i.e.

$$\eta(e)=e\cdot A\,.$$

Theorem 4: By appropriate numbering of K_i, a one-to-one correspondence between Γ_i and K_i holds in such a manner that:
if $e\in\Gamma_i$, then $\eta(e)\in K_i$ and

$$\eta(C^p e)=D^{-p}\eta(e)\,.$$

Based on Theorems 3 and 4, a cyclic code $S(g(u))$ may be instrumented in a simple fashion by employing $SR_m(g)$ and the reverse shift-register of $SR_m(g)$.

4. *Examples of Π_0-Type Codes*

Several efficient codes of Π_0-type have been found. Let $E_1, E_{11}, E_{101}, \cdots$ denote a single error, a double-adjacent error, a three-binit-wide double error, $\cdots$ respectively.

By forming the state diagram of $SR_m(g)$, the following results (i) and (ii) are easily ascertained from Lemma and Theorems 3 and 4.

(i) The (21, 15) code with $g(u)=u^6+u^4+u^2+u+1$ corrects error-patterns E_1, E_{11} and E_{101}. This code is a quasi-perfect code.

(ii) The (17, 9) code with $g(u)=u^8+u^7+u^6+u^4+u^2+u+1$ can correct error-patterns E_{111}, E_{1101}, E_{10101}, $E_{1010001}$, $E_{10010001}$, $E_{100010001}$ besides all single and double errors. This code is also quasi-perfect, and has the least redundancy among the known double-error-correcting systematic codes with 8 check-digits.

(iii) A simple consideration shows that a perfect cyclic code is necessarily of Π_0-type. Hence, the cyclic Hamming codes and the cyclic Golay code found by Prange are of Π_0-type. A simple proof that $S(u^{11}+u^{10}+u^6+u^5+u^4+u^2+1)$ is perfect is presented.

5. *Extension*

Now, let C' denote the noncyclic shift operator such that $C'^l \cdot x$ or $C'^{-l} \cdot x$ is defined only when no nonzero digtis are lost by the shift operation. A code S will be called a Π'-type code if for any vector x in S, every vector that has the form $C'^l \cdot x$ is also in S. Clearly, a cyclic code is of Π'-type. Some similar theorems to those in Sections 2 and 3 hold with regard to this class of codes. For example, the following theorem is obtained.

Theorem 1′: The necessary and sufficient condition that S is of Π'-type is that there exists a polynomial $g(u)$ of degree m such that

(i) $$g(0)=1\,,$$

and (ii) a polynomial $x(u)$ in R_n is in I, if and only if

$$x(u)\equiv 0 \qquad [\text{modd } 2,\ g(u)]\,.$$

This theorem implies that every Π'-type code may be formed by omitting some leading information symbols from code vectors of a suitable cyclic code.

The Reiger codes[6], the Fire codes[3] and the codes considered by the author[7] are of Π'-type.

REFERENCES

(1) E. PRANGE: Some Cyclic Error-Correcting Codes with Simple Decoding Algorithms, AFCRC, ASTIA Document No. AD 152386; April, 1958.

E. PRANGE: The Use of Coset Equivalence in the Analysis and Decoding of Group Codes, AFCRC-TR-59-164; June, 1959.

(2) N. M. ABRAMSON: A Class of Systematic Codes for Non-Independent-Errors, Trans. IRE, PGIT-5, p. 150; December, 1959.

(5) P. FIRE: A Class of Multiple-Error Correcting Binary Codes for Non-Independent Errors, Sylvania Report RSL-E-2; 1959.

(3) C. M. MELAS: A New Group of Codes for Correction of Dependent Errors in Data Transmission, IBM J. Research Develop., **4**, p. 58; January, 1960.

(5) R. W. MARSH: Tables of Irreducible Polynomials over GF(2) Through Degree 19, NSA; October, 1957.

(6) S. H. REIGER: Codes for the Correction of Clustered Errors, Trans. IRE, PGIT-6, p. 16; March, 1960.

(7) T. KASAMI: A Systematic Code for Non-Independent Errors, J. Information Processing Soc. Japan, **1**, p. 132; November, 1960.

(8) B. ELSPAS: The Theory of Autonomous Linear Sequential Networks, Trans. IRE, PGCT-6, p. 45; March, 1959.