E. Gorog

Some New Classes of Cyclic Codes Used for Burst-Error Correction

Abstract: A general theory of cyclic codes correcting a set of given types of errors is presented. Codes published by Abramson, Fire, Melas and others are accounted for in this theory, which also offers several new classes of codes. These new codes are competitive with existing ones. In burst-error correction, for certain message lengths they may be better since they may need fewer parity check bits.

Introduction

A class of error-correcting codes is defined by a relationship existing among the symbols of a message. When this relationship can be expressed as a part of a mathematical theory the specific class of code becomes of direct interest.

For a cyclic code the relationship may be represented in a purely algebraic form. The main purpose of this paper is to study this model and the useful applications which can be derived from it.

We shall first give some definitions, particularly on cyclic codes correcting different given types of error. A *type of error* is an error pattern which may occur anywhere inside the message.

The construction of such codes rests essentially on the cyclic structure of their generator polynomials. Therefore a *theorem* relates the cyclic structure of any polynomial to the correction properties of the corresponding cyclic code.

Many new classes of codes, then, can be constructed. These have good burst-error correction properties when certain specific conditions are satisfied. Each new class of codes presented is described by means of an example. Applications to codes which correct several separated errors or several bursts inside the message are not included here.

The table of the best cyclic codes which correct given bursts in given message lengths for limited values of these parameters is presented elsewhere.[1] The present paper, however, is an exposition of mathematical research leading to the development of some new efficient classes of codes.

Definitions

- *Representation of a cyclic code*

A linear (L, K) *code* may be defined by means of a parity-check (L, K) matrix of rank K (L columns, K rows). The message length is L. There are K check bits and $L - K$ information bits.[2]

Cyclic codes are systematically constructed by feedback shift registers.[3-4]

If x^i represents the state of a K-element shift register at the instant i, the parity-check matrix of the corresponding code will be represented[5] by $\lambda = (x^0\ x^1\ x^2 \cdots x^{L-1})$.

λ is formed by the L terms x^i which satisfy $F(x) = 0$.

λ is therefore defined as *modulo* $F(x)$. We may write

$$\lambda \equiv (x^0 x^1 x^2 \cdots x^{L-1}) \qquad [F(x)].$$

$F(x)$ and L completely define the cyclic code. We shall often denote this cyclic code simply by $F(x)$. Note that $F(x)$ is such that $F(0) = 1$ and its degree, K, is equal to the number of check bits within the message. The cyclic code $F(x)$ *corrects* always $2^K - 1$ different error-patterns.

If it corrects α different types of error in a message of length L such that: $\alpha L = 2^K - 1$ this code will be, by definition, a *perfect cyclic code in correction of error types.*

The period of any polynomial $F(x)$, with coefficients in $GF(2)$, is the least integer N such that

$$x^{t+N} \equiv x^t \qquad [F(x)].$$

- *Structure of a polynomial* $F(x)$

Every polynomial with coefficients in $GF(2)$ is equivalent, modulo $F(x)$, to an element of a finite set S which has 2^K elements:

$$E_1(x)E_2(x) \cdots E_{2^K}(x).$$

Let us realize a partition of S into subclasses such that if $E_e(x)$ is an element of any subclass and $E_f(x)$ is an element of any other subclass, the following inequivalence is always verified:

$$x^h E_e(x) \not\equiv x^i E_f(x) \qquad [F(x)].$$

The values i and h are any integers.

This partition will give, for instance,

a first subset of n_1 elements
a second subset of n_2 elements
•
•
•
a b^{th} subset of n_b elements and no other subset.

We obtain b values n_j $1 \leq j \leq b$ and there are 2^K elements in S: $\sum_j n_j = 2^K$.

Let us arrange these values in nonascending order:

$$n_j \geq n_{j+1} \qquad 1 \leq j \leq b$$

and denote by $B_j(x)$ any element of the j^{th} subclass. We have

$$j \neq l \qquad B_j(x) \not\equiv x^i B_l(x) \qquad [F(x)]$$

$$B_j(x) \equiv x^{n_j} B_j(x) \qquad [F(x)],$$

where n_j divides N.

For any specific $B_j(x)$ there corresponds one and only one cycle.

By definition we shall call this $B_j(x)$ which may characterize its cycle *the j^{th} characteristic* of $F(x)$, and n_j *the order* of $B_j(x)$.

Two "different characteristics" will generate two different cycles.

• *Definition of structure of $F(x)$*

The cyclic structure of a polynomial $F(x)$, defined only if $F(0) = 1$, will be the sequence of the b values n_j and of b corresponding characteristics. We shall denote this sequence by

$$\{n_j, B_j(x)\} \qquad 1 \leq j \leq b$$

with $n_j \geq n_{j+1}$.

Remark

The work of B. Elspas[6] is concerned only with the length n_j of each cycle (or cycle set). Our definition of a polynomial structure includes the knowledge of the cycle length n_j as well as of one element $B_j(x)$ which characterizes its cycle. The choice of this element will be specified later; it is a polynomial taken in one of the n_j classes defined as *modulo $F(x)$*.

Fundamental theorem on error-correction properties of any cyclic code

Let us consider the structure $F(x)$:

$$\{n_j, B_j(x)\} \qquad 1 \leq j \leq b.$$

In this ensemble the value of n_j may be repeated c_j times. We shall define a new index r_j by

$$n_{r_j} = n_j$$

for every j which satisfies

$$r_j - c_j + 1 \leq j \leq r_j,$$

$$n_{r_j} > n_{r_{j'}}, \qquad \text{for} \quad r_{j'} > r_j.$$

The index r_j is the largest value of j among equal n_j's.

Theorem

1) *The cyclic code $F(x)$ corrects necessarily* at least r_j *different types of error if the message length is n_j. Each corrected type of error is any characteristic of each of the first r_j cycles.*

2) *If the message length is n_j, we shall have, for any $n_t > n_j$,*

$$n_t = d_t n_j + y_t \qquad \textit{with} \qquad 1 \leq t \leq r_j \qquad y_t < n_j.$$

The cyclic code $F(x)$ never corrects more than $\sum_t d_t$ *different types of error, and is a shortened cyclic code if $d_t > 1$.*

We shall now apply the theory to cyclic codes correcting one burst of errors.

• *Demonstration*

According to the definition of r_j, the $r_j{}^{\text{th}}$ cycle, in the structure of $F(x)$, is the last cycle of length equal to n_j. The length of the $(r_j + 1)^{\text{th}}$ cycle is shorter than n_j. $B_j(x)$ is the characteristic of the j^{th} cycle.

1) Let us form the r_j sequences $x^0\, B_j(x)\, x^1\, B_j(x) \cdots x^{L-1}\, B_j(x)$ corresponding to the first r_j characteristic with $L = n_j$. By construction, each element of each sequence appears only one time: the code $F(x)$ corrects at least r_j different types of error if the message length is n_j.

2) Let us consider now the t^{th} cycle of length n_t with $1 \leq t \leq r_j$. We may form d_t sequences of length $L = n_j$ from this cycle if

$$n_t = d_t n_j + y_t \qquad y_t < n_j.$$

The characteristics of these sequences are

$$B_t(x),\ x^{n_j} B_t(x),\ \cdots,\ x^{(d_t-1)n_j} B_t(x),$$

and each element of each sequence appears only one time. Then d_t is the maximum number of sequences which are obtained from the t^{th} cycle, and the code $F(x)$ never corrects more than $\sum_t d_t$ different types of error.

Burst-error correction codes

A burst of d errors, or fewer than d errors defined for $d > 1$ is a type of error $T(x)$ of the following form:

$$T(x) = 1 + a_1 x + \cdots + a_i x^i + a_{d-1} x^{d-1}.$$

There exist 2^{d-1} different polynomials $T(x)$.

A code which corrects any burst of d errors in a certain message is a code which corrects necessarily the 2^{d-1} different possible types of error $T(x)$ in this message.

This definition of a burst of d errors includes bursts of fewer than d errors. If we consider a real burst of d errors,

that is, $1 + a^i x + \cdots + a_{d-2} x^{d-2} + x^{d-1}$ (the width is d), we shall always specify this.

Group *S*: Systematic codes

• *Proposition 1*

Let $P_1(x)$ be a polynomial of period N_1 and degree K_1 with a structure such that:

1) the 2^{d-1} polynomials $T(x)$ form different characteristics.

2) L is the length of the shortest cycle.

($P_1(x)$ may represent a cyclic code which corrects a burst of d errors in a message of length L).

Let $P_2(x)$ be a primitive polynomial of degree K_2 which does not divide $P_1(x)$:

If K_2 is superior or equal to d and if $2^{K_2} - 1$ is relatively prime to N_1, the cyclic code represented by $P_1(x)P_2(x)$ corrects any burst of d errors in a message of length $(2^{K_2} - 1)\, L$.

The above is applicable even if L is less than K_1. Melas and Gorog[7] consider the case where L is greater than the degree of $P_1(x)$.

Demonstration

To prove this proposition we need to apply Lemma 3(c) of the Appendix.

The order of any characteristic $T(x)$ of $P_1(x)$ is $n \geq L$.

$T(x)$ is relatively prime to $P_2(x)$: the degree of $P_2(x)$, which is irreducible, is greater than the degree of $T(x)$.

n is relatively prime to $2^{K_2} - 1$ since n divides N_1, and N_1 is relatively prime to $2^{K_2} - 1$. The least common multiple of n and $2^{K_2} - 1$ is $n(2^{K_2} - 1)$. $T(x)$ is therefore a characteristic of $P_1(x)P_2(x)$ and its order is $n(2^{K_2} - 1)$ with $n \geq L$.

Let us apply now the fundamental theorem: the shortest cycle is $L(2^{K_2} - 1)$ and the code $P_1(x)P_2(x)$ corrects any burst of d errors in a message of length $L(2^{K_2} - 1)$.

• *Proposition 2*

We shall give now some simple polynomials $F(x)$, $G(x)$, $H(x)$, $I(x)$, $J(x)$, $K(x)$, $A(x)$ which have the properties of $P_1(x)$.

In their structures the 2^{d-1} polynomials $T(x)$ form different characteristics. We shall denote the length of the shortest cycle for each structure by L_F, L_G, L_H, L_I, L_J, L_K, L_A.

The results are:

$$F(x) = x^{2d-1} + 1 \qquad L_F = 2d - 1$$

$$G(x) = x^{2d-2} + 1 \qquad L_G = d - 1$$

$$H(x) = x^{2d-1} + x^{2d-2} + \cdots + x + 1 \qquad L_H = d$$

$$I(x) = x^{2d} + x^d + 1 \qquad L_I = 3d$$

$$J(x) = x^{2d} + x^{2d-1} + \cdots + x + 1 \qquad L_J = 2d + 1$$

$$K(x) = x^{2d} + x^{2d-2} + \cdots + x^2 + 1 \begin{cases} L_K = 2d + 2 & \text{if } d \text{ is even} \\ L_K = d + 1 & \text{if not.} \end{cases}$$

$$A(x) = x + 1 \qquad L_A = 1.$$

The last polynomial $A(x)$ is a special case for $d = 2$.

Demonstration

Any element of the finite set S, defined by $P_1(x) \equiv 0$, may be represented by

$$E(x) = 1 + \sum_h \alpha_h x^h$$

with $1 \leq h \leq K_1$

$$x^i T(x) \equiv 1 + \sum_h \alpha_h(i) x^h. \qquad [P_1(x)].$$

Every selected polynomial is shown such that there always exists, for any $T(x)$, when i varies from 0 to $L - 1$, at least one nonzero $\alpha_h(i)$ with $d \leq h \leq K_1$.

Then two different types $T(x)$ are never in the same cycle. The structure of $G(x) - 1 + x^6$, for instance, is:

$\underline{(6, 1)}$ $\underline{(6, 1 + x)}$ $\underline{(6, 1 + x^2)}$ $\underline{(6, 1 + x + x^2)}$

$\underline{(6, 1 + x + x^3)}$ $\underline{(6, 1 + x^2 + x^3)}$

$\underline{(6, 1 + x + x^2 + x^3)}$ $\underline{(6, 1 + x + x^2 + x^4)}$

$\underline{(6, 1 + x + x^2 + x^3 + x^4)}$ $\underline{(3, 1 + x^3)}$

$(3, 1 + x + x^3 + x^4)$ $(2, 1 + x^2 + x^4)$

$(1, 1 + x + x^2 + x^3 + x^4 + x^5)$ $(1, 1 + x^6)$.

The 2^3 underlined polynomials form different characteristics: (burst of 4) $L_G = 3$.

For any polynomial $P_1(x)$ of degree K_1, corresponding values of d and L exist, but it appears that for simple generator polynomials the most interesting ones are constructed as follows.

Let a be a divisor of K_1 $\quad ar = K_1$

$$P_1(x) = 1 + \sum_k x^{ka} \quad \text{with} \quad 1 \leq k \leq r.$$

• *Consequence*

Proposition 1 may be applied *systematically* to these different polynomials in the correction of a burst of d errors.

We may call them *systematic burst-error correction codes* and they will be denoted by S:

$S_F, S_G, S_H, S_I, S_J, S_K, S_A$ (See Example 1).

The following conclusions can be drawn:

1) If we select the best code, with minimum redundancy, for any message length, S_F and S_G are, in general, better than the others.

2) For some message lengths we might choose among

several systematic codes which are equivalent and take the simplest implementation.

3) If we accept correction of any burst of $d-1$ errors (or fewer) and any real burst of d errors except one S_G and S_H are better than the others. In these cases $L_G = 2(d-1)$ $L_H = 2d$.

4) There exist other cyclic systematic codes.

Remark

The first class S_F was found by Philip Fire[8] and the last one by Norman Abramson.[9] The other classes are new, and these codes which are able to correct large bursts of errors have a good efficiency if the messages are very long.

From practical point of view, it seems interesting to develop codes correcting relatively long bursts in shorter message lengths with a high coding efficiency. Such codes are presented in the next group.

Group *P*: "Perfect codes"

"Perfect codes" which correct the maximum number of types of error in messages of length N, if N is the period of $F(x)$, may be used in burst-error correction. (Their generating polynomials are given by irreducible polynomials of same period).

Let us suppose that there are s cycles of length N: $sN = 2^K - 1$.

The code $F(x)$ will correct a burst of d errors in a message of length N if:

1) $s > 2^{d-1}$;

2) the 2^{d-1} types $T(x)$ form different characteristics of $F(x)$.

The best "perfect codes" which correct a burst of d errors satisfy: $2^{d-1} < s < 2^d$. We shall denote them by P_A.

Remark

The class of code which is generated simply by a nonprimitive polynomial *was found independently by Zetterberg.*[10]

- *Class* P_B

Most interesting codes will be given by the product of different irreducible nonprimitive polynomials of same period. (See Example 2).

- *Class* P_C

"Perfect codes" which correct any burst of d errors in a message of length N may correct any burst of $d+1$ errors in a message shorter than N.

If two bursts of $d+1$ errors are in the same cycle, we have necessarily $L \leq (N-1)/2$. (See Example 3.)

The Reiger code[11] is in the class P_C. In this case, $F(x)$ is given simply by one primitive polynomial.

- *Class* P_D

Good codes may be constructed as follows. Take a perfect cyclic code which corrects many different types of errors in a message of length, N_1, multiply the corresponding polynomial by a new primitive polynomial of period N_2 relatively prime to N_1 (the different types are still corrected in N_1N_2) and shorten the message such that bursts are corrected. (See Example 4).

Group *E*: Some efficacious codes

- *Proposition* 3

Let $P_1(x)$ be a polynomial of degree K_1, period N_1 with the structure

$$\{n_j, B_j(x)\} \qquad 1 \leq j \leq b.$$

Let $P_2(x)$ be a polynomial of degree K_2, period N_2 with the structure

$$\{m_l, C_l(x)\} \qquad 1 \leq l \leq c, \text{ and}$$

$$m_l = N_2 \quad \text{for} \quad 1 \leq l \leq t < c.$$

We shall denote by S_{jl} the intersection of the j^{th} cycle of $P_1(x)$ and the l^{th} cycle of $P_2(x)$ and by $E(x)$ any element of S_{jl}.

$$E(x) \equiv x^i B_j(x) \qquad [P_1(x)]$$

$$E(x) \equiv x^k C_l(x) \qquad [P_2(x)].$$

The cyclic code $P_1(x)$ $P_2(x)$ corrects any burst of $K_1 + 1$ errors in a message of length N_2 if the following conditions are satisfied:

(α) N_1 divides N_2.

(β) For $l \leq t$ in every subset S_{jl} the value $k - i$ modulo n_j is different for each element $E(x)$.

(γ) For $l > t$, every subset S_{jl} is either empty or contains only one element of order N_2.

(δ) $P_1(x)$ and $P_2(x)$ are relatively prime.

Demonstration

Conditions (α) and (δ) state that there are at least $s2^{K_1}$ cycles of length N_2. [See Lemma 4(b)].

Each burst $T(x)$ of $K_1 + 1$ errors may be in a different cycle $s2^{K_1} \geq 2^{K_1}$.

Conditions (β) and (γ) state that any two different bursts $T(x)$ are two different characteristics of order N_2 in the structure of $F(x)$.

If two different types $T(x)$ are in the same cycle they belong to the same subset S_{jl}.

When two types $E_1(x)$ and $E_2(x)$ belong to different subsets they are already in different cycles with respect to at least one of the two structures of $P_1(x)$ and $P_2(x)$.

If two different types $E_1(x)$ and $E_2(x)$ are in the same cycle we have

$$k_1 - i_1 \equiv k_2 - i_2 \qquad [n_j].$$

k_1, i_1, k_2, i_2 are defined by

$$E_1(x) \equiv x^{i_1}B_i(x), \qquad E_2(x) \equiv x^{i_2}B_i(x) \qquad [P_1(x)]$$

$$E_1(x) \equiv x^{k_1}C_l(x), \qquad E_2(x) \equiv x^{k_2}C_l(x) \qquad [P_2(x)].$$

The proof is in the demonstration of Lemma 1.

$$q_{il} = n_i \qquad \text{for} \quad l \leq t.$$

In the case of $l > t$, if S_{il} contains only one element, this element is a characteristic of its independent cycle, but Proposition 3 is true if and only if the length of this cycle is N_2.

We shall denote these general classes of codes by E. (See Example 5.)

• *Class E_O*

When $P_2(x)$ is primitive, with $K_2 > K_1$ the precedent conditions become:

(α) N_1 divides N_2.
(β) In every subset S_i, the value $k - i$ modulo n_i is different for each element $E(x)$.

If conditions (α) and (β) are both satisfied, the code $P_1(x)\ P_2(x)$ is in the class E_O.

The structure of these codes is such that:

1) There are 2^{K_1} cycles of length N_2.

2) The length of the other cycles is less than N_2.

Remark

1) The Melas code[12] is in the class E_O.

2) This class corresponds to the *codes presented independently by Elspas and Short.*[13]

Table 1 **Codes for $d = 5$.**

Check bits (K)	*Cyclic code*					*Message length (L)*
	S_F	S_G	S_H	S_I	S_J	
13		x				≤ 124
14	x	x	x			≤ 155
	x	x				≤ 252
	x					≤ 279
15		x		x	x	≤ 315
		x		x	x	≤ 341
		x		x		≤ 465
		x				≤ 508
16	x	x	x		x	≤ 615
	x	x			x	≤ 693

• *Classes E_P E_Q E_R*

These classes are relative to cyclic codes of the form $P_1(x)\ P_2(x)$, with $P_2(x)$ primitive where conditions (α) and (β) are not both satisfied. These codes are new.

(*a*) *Condition (α) is satisfied and (β) is not.*

1) It may happen that this code corrects a burst of K_1 errors, instead of $K_1 + 1$, in a message of length N_2. *Class E_P.* (See Example 6.)

2) The code always corrects any burst of $K_1 + 1$ errors but in a message shorter than N_2. *Class E_Q.* (See Example 7.)

(*b*) *Condition (β) is satisfied and (α) is not.*

It is still possible for the cyclic code $P_1(x)\ P_2(x)$ to correct any burst of $K_1 + 1$ errors in a message shorter than N_2. *Class E_R.* (See Example 8.)

This particular example is, in fact, a description of a very efficacious code with an odd number of check bits, correcting a burst of three errors.

Example 1

In Table 1 the systematic codes presented correct a burst of five errors. If the message length is 330, for instance, we need 15 check bits and we may use S_G, S_I, or even S_J. However, the most interesting one is S_G, which is valid for a message length of 508.

In the left half of Table 2 we selected the polynomials of least degree codes with minimum redundancy as a function of message length.

An interesting case is the correction of a burst of eight

Table 2 **Best codes for $d = 5$ and $d = 8$ as functions of message length.**

$d = 5$			$d = 8$		
Check bits (K)	*Cyclic codes*	*Message length (L)*	*Check bits (K)*	*Cyclic codes*	*Message length (L)*
13	S_G	$\leq$ 124	22	S_G	$\leq$ 1785
14	S_F	$\leq$ 279	23	S_H	$\leq$ 2040
15	S_G	$\leq$ 508	24	S_F	$\leq$ 7665
16	S_F	$\leq$ 1143	25	S_G	$\leq$ 14323
17	S_G	$\leq$ 2044	26	S_F	$\leq$ 30705
18	S_F	$\leq$ 4533	27	S_G	$\leq$ 57337
19	S_G	$\leq$ 8188	28	S_F	$\leq$122865
20	S_F	$\leq$18423	29	S_I	$\leq$136584

errors (right half of Table 2) where, for different message lengths, the best cyclic systematic codes are first S_G, then S_H, then S_F and even S_I. This is due to the fact that, when one of the values $L_F, L_G, L_H, L_I \cdots$ is not relatively prime to $2^{K_2} - 1$, the corresponding class is eliminated.

Example 2

Class of cyclic code	P_B	*Number of check bits* (K)	16
Burst corrected (d)	7	*Message length* (L)	51

Codes with minimum possible check bits, taken in the class P_B, are given by polynomials of degree 16. They are the product of two different polynomials of degree 8 taken in one of the following sets (the conjugate polynomials belong also to these sets.) Peterson[3] gives a table of irreducible polynomials.

$x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$
$x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$
$x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$
$x^8 + x^7 + x^3 + x + 1$
} with period 85

$x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$
$x^8 + x^4 + x^3 + x + 1$
} with period 51

$x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$
$x^8 + x^5 + x^4 + x^3 + 1$
} with period 17.

The code is given, in this example, by the product of the two irreducible nonprimitive polynomials of period 51: $F(x) = P_1(x)\, P_2(x)$, where

$$P_1(x) = (1 + x + x^4 + x^5 + x^6 + x^7 + x^8)$$
$$P_2(x) = (1 + x + x^3 + x^4 + x^8).$$

Their structures are:

$(51, 1)\ (51, 1+x)\ (51, 1+x^2)\ (51, 1+x+x^2+x^3)$
$(51, 1 + x^4)\ (1, P_1(x))$ and
$(51, 1)\ (51, 1 + x)\ (51, 1 + x^2)\ (51, 1 + x + x^2)$
$(51, 1 + x^3)\ (1, P_2(x))$.

If we apply Lemma 1 of the Appendix to find the structure of $F(x)$, we see that the 2^6 polynomials $T(x)$, form different characteristics $H_{il}{}^k(x)$.

Remark

The greatest burst of errors which could be corrected by 16 check bits correspond to $d = 8$.

Example 3

Class of cyclic code	P_C	*Number of check bits* (K)	9
Burst corrected (d)	4	*Message length* (L)	23

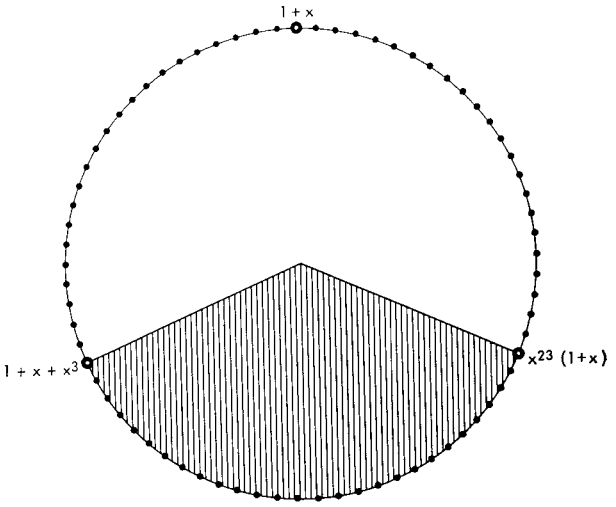
The code is given, in this example, by $F(x) = 1 + x + x^2 + x^4 + x^9$, which is a nonprimitive irreducible polynomial. Its period is 73.

The complete structure is:

$(73, 1)\ (73, 1 + x)\ (73, 1 + x^2)\ (73, 1 + x + x^2)$
$(73, 1 + x^3)\ (73, 1 + x^2 + x^3)$
$(73, 1 + x + x^2 + x^3)\ (1, F(x))$.

The code $F(x)$ corrects in a message of length 73 any burst of four except one: $1 + x + x^3$, which is in the cycle of $1 + x$.

This cycle may be represented by the illustration.



$$1 + x + x^3 \equiv x^{50}(1 + x) \qquad [F(x)]$$
$$1 + x \equiv x^{23}(1 + x + x^3) \qquad [F(x)].$$

If the message length is $L = \min(50, 73 - 50) = 23$ the two error patterns $1 + x$ and $1 + x + x^3$ are both corrected $F(x)$ corrects a burst of four in a message of length 23. The cross-hatched area corresponds to error patterns which are not used. In this cycle $(50 - 23)$, 27 elements are lost instead of 50 in the others $(73 - 23)$.

Example 4

Class of cyclic code	P_D	*Number of check bits* (K)	14
Burst corrected (d)	4	*Message length* (L)	1045

The code is given, in this example, by the product

$$F(x) = P_1(x) \cdot P_2(x),$$

where

$$P_1(x) = 1 + x + x^2 + x^4 + x^9$$

$$P_2(x) = 1 + x^2 + x^5.$$

$P_1(x)$ corrects any burst of three in a message of length 73, $N_1 = 73$. (See Example 3.)

$P_2(x)$ is a primitive polynomial $N_2 = 31$.

$F(x)$ corrects any burst of three in a message of length $N_1N_2 = 73 \times 31 = 2263$. (See Proposition 3.)

In the structures of $P_1(x)$ and $P_2(x)$ we have, respectively,

$$\left.\begin{array}{ll} 1 + x + x^3 \equiv x^{50}(1 + x) & [P_1(x)] \\ 1 + x + x^3 \equiv x^9\,(1 + x) & [P_2(x)] \end{array}\right\} \text{(I)}$$

(I) implies (II) and (III)

$1 + x$ and $1 + x + x^3$ will belong still to the same cycle, in the structure of $F(x)$:

$$1 + x + x^3 \equiv x^t(1 + x) \qquad [F(x)] \qquad \text{(II)}$$

$$\left.\begin{array}{l} t \equiv 50\ [73] \\ t \equiv 9\ \ [31] \end{array}\right\} \qquad \text{(III)}$$

The solution of t is given by $t \equiv 1218$. [2263].

We may apply now the same method as in the Example 3 to correct a burst of four errors.

$$L = \min\,(1218,\ 2263 - 1218) = 1045.$$

$F(x)$ of degree 14 corrects a burst of four in a message of length 1045.

Example 5

Class of cyclic code	E	*Number of check bits* (K)	10
Burst corrected (d)	5	*Message length* (L)	15

The code is given, in this example, by the product:

$$F(x) = P_1(x)\ P_2(x),$$

where

$P_1(x) = 1 + x + x^2 + x^3 + x^4$; $K_1 = 4$ and $N_1 = 5$.

$P_2(x) = 1 + x + x^2 + x^3 + x^6$; $K_2 = 6$ and $N_2 = 15$

Their structures are:

$1 \leq j \leq 4$

$(5, 1)$ $(5, 1 + x)$ $(5, 1 + x^2)$ $(1, P_1(x))$

and $1 \leq l \leq 6$

$(15, 1)$ $(15, 1 + x)$ $(15, 1 + x^2)$ $(15, 1 + x + x^2)$

$(3, 1 + x^3 + x^4)$ $(1, P_2(x))$ $\qquad t = 4.$

All the conditions are verified:

(α) 5 divides 15.

(β) In each set S_{jl} which contains more than one element the values $k - i$ modulo n_j are different for $1 \leq l \leq 4$. For instance, S_{11} contains two elements: 1 and $1 + x + x^2 + x^3$. As a matter of fact in this case (the simplest one) we have: $B(x) = 1$ and $C(x) = 1$

$$\left.\begin{array}{ll} 1 \equiv x^0(1) & [P_1(x)] \\ 1 \equiv x^0(1) & [P_2(x)] \end{array}\right\} k - i = 0 - 0 = 0$$

$$\left.\begin{array}{ll} 1+x+x^2+x^3 \equiv x^4(1) & [P_1(x)] \\ 1+x+x^2+x^3 \equiv x^6(1) & [P_2(x)] \end{array}\right\} k - i = 6 - 4 = 2$$

and $\quad 2 \neq 0 \qquad [5].$

(γ) S_{j5} is empty except S_{25} which contains $1 + x^3 + x^4$ but the order of $1 + x^3 + x^4$ is $3 \times 5 = 15$. S_{j6} is empty.

(δ) $P_1(x)$ and $P_2(x)$ are relatively prime. The decomposition of P_2 gives: $(1 + x + x^2)\,(1 + x^3 + x^4)$.

Example 6

Class of cyclic code	E_P	*Number of check bits* (K)	12
Burst corrected (d)	4	*Message length* (L)	255

$F(x) = P_1(x)\ P_2(x)$, where

$$P_1(x) = 1 + x + x^2 + x^3 + x^4$$

$$P_2(x) = 1 + x + x^5 + x^6 + x^8.$$

Their structures are: $(5, 1)$ $(5, 1 + x)$ $(5, 1 + x^2)$ $(1, P_1)$

and $(255, 1)$ $(1, P_2)$.

(α) $5 \mid 255$

(β):

	$E(x)$	$k - i$ [5]
	1	0
	$1 + x + x^2 + x^3$	2
S_{11}	$1 + x + x^3\,x + x^4$	0
	$1 + x^2 + x^3 + x^4$	3
	$1 + x + x^2 + x^4$	1
	$1 + x$	2
	$1 + x + x^2$	0
S_{21}	$1 + x + x^4$	1
	$1 + x^3 + x^4$	1
	$1 + x^4$	4
	$1 + x^2$	4
	$1 + x^3$	2
S_{31}	$1 + x + x^3$	0
	$1 + x^2 + x^3$	3
	$1 + x^2 + x^4$	0

In each set S_{i1} the values $k - i$ modulo 5 are not all different but, if we consider only polynomials of degree 3 or less, the corresponding values are different.

$F(x)$ does not correct a burst of 5 but a burst of 4 in a message of length 255.

Example 7

Class of cyclic code	E_Q	*Number of check bits* (K)	9
Burst corrected (d)	4	*Message length* (L)	26

The code is given, in this example, by the product $F(x) = P_1(x)P_2(x)$ where

$P_1(x) = 1 + x + x^3$

$P_2(x) = 1 + x + x^6$.

Their structures are:

(7, 1) (1, $P_1(x)$) and (63, 1) (1, $P_2(x)$)

(α) 7 | 63

(β):

$E(x)$	$1 + x + x^6$	$1 + x + x^3$	$k - i$ [7]
1	x^0	x^0	0
$1 + x + x^2$	x^{26}	x^5	0
$1 + x$	x^6	x^3	3
$1 + x^3$	x^{32}	x^1	3
$1 + x^2$	x^{12}	x^6	6
$1 + x^2 + x^3$	x^{48}	x^4	2
$1 + x + x^2 + x^3$	x^{18}	x^2	2

The condition (β) is not satisfied.

The types 1 and $1 + x + x^2$, are in the same cycle (same value of $k - i$ modulo 7) as well as $1 + x$ and $1 + x^3$, $1 + x^2 + x^3$ and $1 + x + x^2 + x^3$. All these patterns will be corrected by $F(x)$ if the message length is $L = \min(26, 63 - 26, 32 - 6, 63 - 32 + 6, 48 - 18, 63 - 48 + 18)$. $L = 26$.

Example 8

Class of cyclic code		E_R	
Burst corrected (d)		3	
Number of check bits (K)	7	9	15
Message length (L)	25	119	8177

The code is given, in this example, by the product $F(x) = P_1(x)P_2(x)$, where

$P_1(x) = 1 + x^2 \qquad N_1 = 2$

$P_2(x) = \sum_{l=0}^{l=K_2} x^l - x \qquad N_2 = 2^{K_2} - 1 \qquad K_2$ is odd.

The properties of the polynomials, which are easy to be verified, are

$1 + x + x^2 \equiv x^1(1) \qquad [P_1(x)]$

$1 + x + x^2 \equiv x^{K_2+1}(1) \qquad [P_2(x)]$.

$1 + x + x^2$ and 1 are in the same cycle for each of the two structures

(α) 2 does not divide $2^{K_2} - 1$.

(β) in S_{11}

Table 1

$E(x)$	$P_2(x)$	$P_1(x)$	$k - i$ [2]
1	x^0	x^0	0
$1 + x + x^2$	$x^{K_2} + 1$	x^1	1

In Table 1 the 2 values of $k - i$ modulo 2 are different.

Since (α) is not satisfied, the problem is to find the values of j such that Table 2 be valid (Table 1 is not sufficient).

Table 2

$E'(x)$	$k - i$ [2]
$x^j(1)$	0
$x^j(1 + x + x^2)$	1

The first value of j which does not satisfy Table 2 is:

$j = 2^{K_2} - K_2 - 2$.

As a matter of fact, for this value of j

$x^j(1 + x + x^2) \equiv x^0 \qquad [P_1(x)]$

$x^j(1 + x + x^2) \equiv x^0 \qquad [P_2(x)]$.

Furthermore, Table 2 will not be valid for $2^{K_2} - K_2 - 2 \leq j \leq 2^{K_2} - 2$ since, having regard to polynomials $x^j(1 + x + x^2)$, $k - i$ is equivalent to zero modulo 2. (The error pattern $1 + x + x^2$ which occurs on the $(2^{K_2} - K_2 - 2)^{\text{th}}$ bit of the message is confounded with the error pattern 1 which occurs on the 1^{st} bit of the message).

Table 2 being valid only for $0 \leq j \leq 2^{K_2} - K_2 - 1$, the message length L is: $L = 2^{K_2} - K_2 - 2$

Remark

1) If $K_2 = 9$ for instance, it appears that the polynomial

$P_2(x)$ is not primitive: $N_2 \neq 2^{K_2} - 1$.

In this case we shall take for $P_2(x)$ a primitive polynomial which has not the precedent form but such that

$$1 + x + x^2 \equiv x^h \qquad [P_2(x)],$$

where h is the smallest possible value.

The message length will be then $L = 2^{K_2} - 1 - h$.

Example: $P_2(x) = 1 + x^4 + x^5 + x^8 + x^9$

$$h = 26 \qquad L = 511 - 26 = 485.$$

2) The particular codes of E_R presented in this example are very efficient.

These codes are, in fact, optimum in the sense that, if the message length is $L = 2^{K_2} - K_2 - 2$, and if a burst of three errors has to be corrected, the minimum possible number of check bits is $K_2 + 2$ for $K_2 > 3$.

If it were possible to correct a burst of three errors, (i.e., four different types of errors) in a message of length $2^{K_2} - K_2 - 2$ with $K_2 + 1$ check bits, the following inequality would be valid: $2^{K_2+1} - 1 > 4(2^{K_2} - K_2 - 2)$.

This is not the case for K_2 superior to three or for message lengths greater than five.

The following table compares these new codes of E_R with Melas codes of E_O which correct both bursts of three.

Number check bits (K)	*Classes Cyclic codes*		*Message length* (L)
	E_O	E_R	
6	x		≤ 15
7		x	≤ 25
8	x		≤ 63
9		x	≤ 119
10	x		≤ 255
11		x	≤ 485

Conclusion

The *efficiency of a code* is usually defined by its redundancy. Since we desire to compare the different classes of burst-error-correction codes presented, we shall give a sharper definition of the efficiency of a cyclic code.

Let n_1 be the number of error patterns consisting of bursts of d or fewer errors which are effectively corrected by the code $F(x)$ in a certain message of length L: $n_1 = 2^{d-1} L$.

Let n_2 be the number of error patterns which can be corrected by this code in this message. If K is the degree of $F(x)$, then $n_2 = 2^K - 1$.

The efficiency e will be $e = n_1/n_2$.

1) The optimal structure does not exist: e cannot be equal to 1: $\quad 0 < e < 1 \quad$ (n_1 is even and n_2 is odd).

2) If we compare the efficiency of the different systematic codes presented we find immediately that

$$e(S_H) < e(S_J) < e(S_I) < e(S_G) < e(S_F).$$

3) If we would like to have a general efficiency comparison, we may compare only those codes with fixed message length L. It is easy to verify that for codes S, P_A, E_O, E_P we obtain:

$$\frac{d}{2^d}\left(1 - \frac{d}{L+d}\right) < e(S) < \frac{d}{2^{d-1}}$$

$$\tfrac{1}{2} < e(P_A) < 1$$

$$1 - \frac{1}{L} < e(E_O) < 1$$

$$\frac{1}{2}\left(1 - \frac{1}{L}\right) < e(E_P) < \tfrac{1}{2}.$$

The final general result for these codes is:

$$e(S) < e(E_P) < e(P_A) < e(E_O) \qquad \text{if } d > 4.$$

The class E_O is optimal but it is often empty. If this is the case and if there exist codes in the class P_A, then P_A becomes the best class, et cetera.

4) This notion of optimality in burst-error correction codes rests essentially on the size of the burst d and on certain appropriate message lengths L given by the codes themselves.

These lengths do not coincide generally with practical message lengths, so that any cyclic code, taken in one of the different classes presented here, may be chosen for its best "practical efficiency."

5) The following table gives the different efficiencies corresponding to the described examples.

Burst corrected (d)	*New class*	*Example*	*Efficiency* (e)
3	E_R	8	.78 .93 .99
4	P_D	4	.51
	E_P	6	.49
	E_Q	7	.40
	P_C	3	.36
5	S_G	1	.24
	E	5	.23
7	P_B	2	.05
8	S_G	1	.054
	S_I	1	.032
	S_H	1	.031

One has to be careful in the interpretation of this table because other values of e may be found with other codes (that is, other examples) taken in each of the new classes S_G, S_H, S_I, P_B, P_C, P_D, E_P, E_Q, E_R.

6) In the same way we could construct other classes of codes in studying the structure of other families of generating polynomials, but the most interesting burst-error-correction codes seem to be in groups S, P and E.

Appendix

In this Appendix we give the four lemmas to which we refer in the text. These are useful not only for constructing the above mentioned classes of codes but also for other burst-error-correction codes as well as for codes correcting other error types.

They are concerned with the structure of $F(x) = P_1(x) \cdot P_2(x)$ when:

1. The respective structures of $P_1(x)$ and $P_2(x)$ are known.
2. The polynomials $P_1(x)$ of degree K_1 and period N_1, and $P_2(x)$ of degree K_2 and period N_2 are relatively prime.

Let $\{n_j, B_j(x)\}\ 1 \leq j \leq b$ be the structure of $P_1(x)$

and $\{m_l, C_l(x)\}\ 1 \leq l \leq c$ be the structure of $P_2(x)$.

p_{jl} will be the least common multiple of n_j and m_l; q_{jl} will be the greatest common divisor of n_j and m_l.

The structure of $F(x)$ is:

$$p_{jl},\ H_{jl}^k(x) \qquad \begin{matrix} 1 \leq j \leq b \\ 1 \leq l \leq c \\ 1 \leq k \leq q_{jl}, \end{matrix}$$

where k is an index which varies between 1 and q_{jl}
q_{jl} is defined for each pair (j, l).

There are q_{jl} different characteristics H_{jl} of same order p_{jl}.

Lemma 1

Let $G_1(x)$ and $G_2(x)$ satisfy:

$$P_2(x) \cdot G_2(x) \equiv 1 \qquad [P_1(x)]$$

$$P_1(x) \cdot G_1(x) \equiv 1 \qquad [P_2(x)].$$

Then each characteristic $H_{jl}{}^k(x)$ is given by

$$H_{jl}^k(x) \equiv P_2(x)G_2(x)B_j(x) + P_1(x)G_1(x)x^{k-1}C_l(x) \qquad [F(x)].$$

Remark

In the computation of the different characteristics $H_{jl}{}^k(x)$ the polynomials $G_1(x)$ and $G_2(x)$ need to be calculated only once. The structure will be compatible with the definition if we arrange this sequence such that the p_{jl} appear in descending order.

Lemma 2

Among the q_{jl} cycles of p_{jl} elements each, one cycle may be generated by $B_j(x)\ C_l(x)$ if and only if $B_j(x)$ is relatively prime to $P_2(x)$ and $C_l(x)$ is relatively prime to $P_1(x)$.

Lemma 3

(a) If the two following conditions are satisfied,

1. N_1 and N_2 are relatively prime, and
2. $B_j(x)$ and $C_l(x)$ are relatively prime to $P_2(x)$ and $P_1(x)$ respectively, whatever the characteristics $B_j(x)$ of $P_1(x)$ and $C'(x)$ of $P_2(x)$ may be,

then all possible products $B_j(x)\ C'(x)$ form all the characteristics of $F(x)$, providing that all these $B_j(x)\ C_l(x)$ are different.

(b) In the structure of $F(x)$, $B_j(x)$ is a characteristic of a cycle of p_{jl} elements if and only if $B_j(x)$ is relatively prime to $P_2(x)$.

(c) If N_1 and N_2 are relatively prime, and if $B_j(x)$ and $P_2(x)$ are relatively prime, then $B_j(x)$, the characteristic of a cycle of $P_1(x)$ with n_j elements is a characteristic of a cycle of $F(x)$ with n_jN_2 elements.

Lemma 4

(a) If N_1 divides N_2, there are necessarily, in the structure of $F(x)$, 2^{K_1} cycles of length N_2.

(b) If N_1 divides N_2 and if, in the structure of $P_2(x)$, there are s cycles of N_2 elements, there are necessarily, in the structure of $F(x)$, $s2^{K_1}$ cycles of length N_2.

References

1. F. Corr and E. Gorog, "Les codes capables d'assurer une sécurité contre les erreurs dans la transmission de données," to be published in *Onde Électrique*.
2. D. Slepian, "A Class of Binary Signaling Alphabets," *Bell System Tech. J.*, **35,** 203 (1956).
3. W. Peterson, *Error Correcting and Error Detecting Codes,* Technology Press, 1961.
4. J. Meggitt, "Error Correcting Codes for Correcting Bursts of Errors," *IBM Journal,* **4,** 329 (1960).
5. E. Gorog, "Les codes cycliques détecteurs et correcteurs," communication to 2 ème Congrès de l'AFCALTI à Paris, October, 1961.
6. B. Elspas, "The Theory of Autonomous Linear Sequential Networks," *IRE Trans. on Circuit Theory,* **CT-6,** 45 (1959). See Section V-C.
7. M. Melas and E. Gorog, "A Note on Extending Certain Codes to Correct Error Bursts in Longer Messages," *IBM Journal,* this issue, p. 151.
8. P. Fire, "A Class of Multiple-Error-Correcting Binary Codes for Non-Independent Errors," Stanford Electronics Laboratories, Technical Report No. 55, April 24, 1959.
9. N. Abramson, "A Class of Systematic Codes for Non-Independent Errors," *IRE Trans. on Information Theory,* **IT-5,** 150 (1959).
10. L. H. Zetterberg, "Cyclic Codes from Irreducible Polynomials for Correction of Multiple Errors," *IRE Trans. on Information Theory,* **IT-8,** 13 (1962).
11. S. H. Reiger, "Codes for the Correction of 'Clustered' Errors," *IRE Trans. on Information Theory,* **IT-6,** 16 (1960).
12. M. Melas, "A New Group of Codes for Correction of Dependent Errors in Data Transmission," *IBM Journal,* **4,** 58 (1960).
13. B. Elspas and R. A. Short, "A Note on Optimum Burst-Error-Correcting Codes," *IRE Trans. on Information Theory,* **IT-8,** 39 (1962).

Received July 3, 1962