A decoding procedure for codes over semigroups

Tariq Shah, Amanullah, Antonio A. Andrade
Department of Mathematics, Quaid-i-Azam University
Islamabad, Pakistan
E-mail: stariqshah@gmail.com, amanullahphulpoto@gmail.com, andrade@ibilce.unesp.br.

Abstract: Corresponding to \( C_0 \), a binary cyclic code \([n, n-r]\) generated by a primitive irreducible polynomial \( p(X) \in \mathbb{F}_2[X] \) of degree \( r = 2b \), where \( b \in \mathbb{Z}^+ \) we can constitute a binary cyclic code \( C, [(n+1)^{3^k} - 1, (n+1)^{3^k} - 3^kr] \), which is generated by primitive irreducible (generalized) polynomial \( p(X^{3^k}) \in \mathbb{F}_2[X; \frac{1}{3^k} \mathbb{Z}_0] \) with degree \( 3^kr \), where \( k \in \mathbb{Z}^+ \). This new code \( C \) improves code rate and have error corrections capability higher than \( C_0 \). The purpose of this study is to establish a decoding procedure for \( C_0 \) by using \( C \) in such a way that one can obtain an improved code rate and error corrections capabilities for \( C_0 \).

Key-words: Semigroup ring, binary cyclic code, binary Hamming code, decoding principle, code rate, error correction.

1 Introduction

Principal ideals in a finite commutative ring are very indispensable in applications of finite algebraic structures. The coding for error control has rudimentary part in the design of recent communication systems and high rate data conversion in digital computers. Most of the conventional error-correcting codes are ideals in finite commutative rings, mainly in quotient rings of Euclidean domains of polynomials and group rings, that is cyclic codes are principal ideals in the quotient ring \( \mathbb{F}_q[X]/(X^n - 1) \).

Cazaran and Kelarev [1] give necessary and sufficient conditions for an ideal to have a single generator and also described all finite commutative principal ideal rings \( \mathbb{Z}_m[X_1, \cdots, X_n]/J \), where \( J \) is an ideal generated by uni-variate polynomials. Nevertheless, in [2] they obtained conditions for the certain rings to be finite commutative principal ideal rings. The extension of a BCH code embedded in a semigroup ring is considered by Cazaran et. all [3]. A lot of information linking to diverse ring constructions and regarding polynomial codes is given by Kelarev [4]. In [4] Sections 9.1 and 9.2 are devoted to error-correcting codes in ring constructions closely related to semigroup rings. Particularly Section 9.1 deals error-correcting cyclic codes of length \( n \) which are in fact the ideals in the group ring \( F[G] \), where \( G \) is a finite torsion group of order \( n \). However, in [5] and [6] Kelarev talked about extensions of BCH codes in various ring constructions, where the outcomes can also be considered as the special cases of semigroup rings of precise nature.

Andrade and Palazzo [7] constructed cyclic, BCH, alternant, Goppa and Srivastava codes via the parity check matrix having units entries of a Galois ring extension of a finite local ring. In [8], [9] and [10] the construction techniques of codes introduced in [7] are improved through semigroup rings instead of a polynomial ring in such a way that instead of conciliative torsion
free additive monoid $\mathbb{Z}_0$, the conciliative torsion free additive monoids $\frac{1}{2}\mathbb{Z}_0$, $\frac{1}{3}\mathbb{Z}_0$, and $\frac{1}{32}\mathbb{Z}_0$ are considered which convert whole construction of a finite quotient ring of a polynomial ring into the finite quotient ring of a semigroup ring. In [8] and [9], $A$ is taken as a finite local commutative ring with identity for the followings quotient rings $A[X; \frac{1}{2}\mathbb{Z}_0]/(X^{2^n} - 1)$, $A[X; \frac{1}{3}\mathbb{Z}_0]/(X^{2^n} - 1)$, $A[X; \frac{1}{32}\mathbb{Z}_0]/(X^{32^n} - 1)$ and $A[X; \frac{1}{32}\mathbb{Z}_0]/(X^{32^n} - 1)$, respectively.

For a binary cyclic code $(n, n - r)$, $C_0$, which is generated by a primitive irreducible polynomial $p(X) \in \mathbb{F}_2[X]$ of degree $r = 2k$, where $b \in \mathbb{Z}^+$, in [11] it is established that there is a binary cyclic code $C$, $((n + 1)^3k - 1, (n + 1)^3k - 1 - 3^kr)$, generated by a primitive irreducible (generalized) polynomial $p(X^k) \in \mathbb{F}_2[X; \frac{1}{32}\mathbb{Z}_0]$ with degree $3^kr$, where $k \in \mathbb{Z}^+$. This new code $C$ improves code rate and have error corrections capability higher than $C_0$. For this we use the decoding procedure for binary cyclic codes. However, in [12] Andrade et al describe the decoding principle based on modified Berlekamp-Massey algorithm for BCH, Alternant and Goppa codes constructed through monoid rings $R[X; \frac{1}{2}\mathbb{Z}_0]$. Whereas [9] Andrade and Shah describe the decoding principle for Goppa codes constructed via $B[X; \frac{1}{32}\mathbb{Z}_0]$. Work [9] and [12] are one of the motivation for this study.

## 2 Preliminaries

Let $T$ be the set of all finitely nonzero functions from a semigroup $(S, \ast)$ into an associative ring $(A, +, \cdot)$. The set $T$ is a ring with respect to binary operations addition and multiplication defined as $(f + g)(s) = f(s) + g(s)$ and $(fg)(s) = \sum_{t \ast u = s} f(t)g(u)$, where the symbol $\sum_{t \ast u = s}$ indicates that the sum is taken over all pairs $(t, u)$ of elements of $S$ such that $t \ast u = s$ and it is understood that in the situation where $s$ is not expressible in the form $t \ast u$ for any $t, u \in S$, then $(fg)(s) = 0$. The ring $T$ is known as a semigroup ring of $S$ over $A$. If $S$ is a monoid, then $T$ is called monoid ring. This ring $T$ is represented as $A[S]$ whenever $S$ is a multiplicative semigroup and an element of $T$ has the typical representation $\sum_{s \in S} f(s)s$ or $\sum_{i = 1}^{n} f(s_i)s_i$. The representation of $T$ will be $A[X; S]$ whenever $S$ is an additive semigroup. As there is an isomorphism between additive semigroup $S$ and multiplicative semigroup $\{X^s : s \in S\}$, so a nonzero element $f$ of $A[X; S]$ is uniquely represented in the canonical form $\sum_{i = 1}^{n} f(s_i)X^{s_i} = \sum_{i = 1}^{n} f_iX^{s_i}$, where $f_i \neq 0$ and $s_i \neq s_j$ for $i \neq j$.

The concept of degree is not generally defined in semigroup rings. But if we consider $S$ to be a totally ordered semigroup, one can define the degree and order of an element of semigroup ring $A[X; S]$ in the following manner; if $f = \sum_{i = 1}^{n} f_iX^{s_i}$ is the canonical form of the nonzero element $f \in A[X; S]$, where $s_1 < s_2 < \cdots < s_n$, then $s_n$ is called the degree of $f$ (i.e. $\deg(f) = s_n$) and similarly the order of $f$ is written as $\text{ord}(f) = s_1$. Now, if $A$ is an integral domain, then for $f, g \in A[X; S]$, it follows that $\deg(fg) = \deg(f) + \deg(g)$.

If $S$ is $\mathbb{Z}_0$ and $A$ is an associative ring, then the semigroup ring $T$ is simply the polynomial ring $A[X]$. Obviously, for any integer $k \geq 1$, $A[X] \subset A[X; \frac{1}{k}\mathbb{Z}_0]$. The degree of an element in $A[X; \frac{1}{k}\mathbb{Z}_0]$ is definable because $\frac{1}{k}\mathbb{Z}_0$ is ordered monoid.

We initiate this study by an observation that, for a field $F$ and an integer $k \geq 0$, the structures of a polynomial ring $F[X]$ and a semigroup ring $F[X; \frac{1}{k}\mathbb{Z}_0]$ have many commonalities, for instance; for a torsion free cancellative monoid $S$, the monoid ring $F[X, S]$ is an Euclidean domain if $F$ is a field and $S \cong \mathbb{Z}$ or $S \cong \mathbb{Z}_0$ (cf. [13, Theorem 8.4]). Of course here $\mathbb{Z}_0$ is torsion free cancellative and $\frac{1}{k}\mathbb{Z}_0 \cong \mathbb{Z}_0$.

For any given (generalized) polynomial $f(X^{\frac{1}{k}}) \in F[X; \frac{1}{k}\mathbb{Z}_0]$ such that $f((X^{\frac{1}{k}})^{3^k}) = f(X) \in F[X]$, whereas the degree of $f(X^{\frac{1}{k}})$ is $3^k$ times the degree of $f(X)$, we can con-
construct the quotient ring \( \frac{F[X; \frac{1}{3\mathbb{Z}}]}{(f(X^{\frac{1}{3}}))} \), where \( (f(X^{\frac{1}{3}})) \) denotes the principal ideal in \( F[X; \frac{1}{3\mathbb{Z}}] \), generated by \( f(X^{\frac{1}{3}}) \). The elements of the quotient ring \( \frac{F[X; \frac{1}{3\mathbb{Z}}]}{(f(X^{\frac{1}{3}}))} \) are the cosets of the ideal \( (f(X^{\frac{1}{3}})) \). The quotient ring is a field if and only if \( f(X^{\frac{1}{3}}) \) is irreducible over \( F \). Furthermore, if \( f(X^{\frac{1}{3}}) = (X^{\frac{1}{3}})^{3k} - 1 \) corresponding to \( f(X) = X^n - 1 \), then

\[
\frac{F[X; \frac{1}{3\mathbb{Z}}]}{(X^{\frac{1}{3}})^{3k} - 1}) = \{ a_0 + a_1 \frac{1}{3} \alpha + a_2 \frac{1}{3^2} \alpha^2 + \cdots + a_{3^{k-1}} \frac{1}{3^{k-1}} \alpha^{3^{k-1}} : a_0, a_1, \frac{1}{3}, \alpha, \cdots, a_{3^{k-1}} \in F \},
\]

where \( \alpha \) denotes the coset \( X^{\frac{1}{3}} + (f(X^{\frac{1}{3}})) \), so \( f(\alpha) = 0 \), where \( \alpha \) satisfies the relation \( \alpha^{3^n} - 1 = 0 \). Of course this quotient ring is not a field because \( (X^{\frac{1}{3}})^{3k} - 1 \) is reducible over \( F \).

Let us now make a change in notation and write \( X \) in place of \( \alpha \). Thus the ring \( \frac{F[X; \frac{1}{3\mathbb{Z}}]}{(X^{\frac{1}{3}})^{3k} - 1}) \)
becomes \( F[X; \frac{1}{3\mathbb{Z}}]/(X^{\frac{1}{3}})^{3n} \), in which the relation \( (X^{\frac{1}{3}})^{3n} - 1 = 0 \) holds, that is \( (X^{\frac{1}{3}})^{3n} = 1 \). So \( F[X; \frac{1}{3\mathbb{Z}}]/(X^{\frac{1}{3}})^{3n} \) is an algebra over \( F \). The multiplication \(* \) in the ring \( F[X; \frac{1}{3\mathbb{Z}}]/(X^{\frac{1}{3}})^{3n} \) is modulo \((X^{\frac{1}{3}})^{3n} - 1)\). So, given \( a(X^{\frac{1}{3}}), b(X^{\frac{1}{3}}) \in F[X; \frac{1}{3\mathbb{Z}}]/(X^{\frac{1}{3}})^{3n} \), we write \( a(X^{\frac{1}{3}}) \ast b(X^{\frac{1}{3}}) \) to denote their product in the ring \( F[X; \frac{1}{3\mathbb{Z}}]/(X^{\frac{1}{3}})^{3n} \), and \( a(X^{\frac{1}{3}})b(X^{\frac{1}{3}}) \) to denote their product in the ring \( F[X; \frac{1}{3\mathbb{Z}}]/(X^{\frac{1}{3}})^{3n} \). If \( \deg a(X^{\frac{1}{3}}) + \deg b(X^{\frac{1}{3}}) < 3^n \), then \( a(X^{\frac{1}{3}}) \ast b(X^{\frac{1}{3}}) = a(X^{\frac{1}{3}})b(X^{\frac{1}{3}}) \).

Otherwise, \( a(X^{\frac{1}{3}}) \ast b(X^{\frac{1}{3}}) \) is the remainder left on dividing \( a(X^{\frac{1}{3}})b(X^{\frac{1}{3}}) \) by \((X^{\frac{1}{3}})^{3n} - 1)\).

In other words, if \( a(X^{\frac{1}{3}}) \ast b(X^{\frac{1}{3}}) = r(X^{\frac{1}{3}}) \), then \( a(X^{\frac{1}{3}})b(X^{\frac{1}{3}}) = r(X^{\frac{1}{3}}) + (X^{\frac{1}{3}})^{3n} - 1)q(X^{\frac{1}{3}}) \) for some generalized polynomial \( q(X^{\frac{1}{3}}) \). In practice, to obtain \( a(X^{\frac{1}{3}}) \ast b(X^{\frac{1}{3}}) \), we simply compute the ordinary product \( a(X^{\frac{1}{3}})b(X^{\frac{1}{3}}) \) and then put \( X^{3n} = 1, X^{3n+1} = X^{\frac{1}{3}}, \) and so on.

In particular, consider the product \( X^{\frac{1}{3}} \ast a(X^{\frac{1}{3}}) \). In the polynomial ring \( F[X] \),

\[
Xa(X) = X(a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}) = a_0 X + a_1 X^2 + \cdots + a_{n-1} X^n, \]

and in the ring \( F[X]/n \),

\[
Xa(X) = a_{n-1} + a_0 X + a_1 X^2 + \cdots + a_{n-2} X^{n-1}. \tag{1}
\]

But in the ring \( F[X; \frac{1}{3\mathbb{Z}}]/(X^{\frac{1}{3}})^{3n} \),

\[
X^{\frac{1}{3}} \ast a(X^{\frac{1}{3}}) = X^{\frac{1}{3}} \ast (a_0 + a_1 \frac{1}{3} X^{\frac{1}{3}} + \cdots + a_{3^{k-2}} \frac{1}{3^k} X^{3^{k-2}} + a_{3^{k-1}} \frac{1}{3^{k-1}} X^{3^{k-1}})^{3^n} - 1) \ast a(X^{\frac{1}{3}}) = \frac{1}{3} a_{3^{k-2}} + a_0 X^{\frac{1}{3}} + a_1 (X^{\frac{1}{3}})^2 + \cdots + a_{3^{k-2}} (X^{\frac{1}{3}})^{3^{k-2}}. \tag{2}
\]

Multiplication of \( X \) with \( a(X) \) (Equation (1)), gives one shift and if we multiply \( X \) with \( a(X^{\frac{1}{3}}) \) (Equation (2)), we get \( 3^n \) shifts. Hence \( a \mapsto a(X^{\frac{1}{3}}) \) establishes an isomorphism between the vector spaces \( F^{3^n} \) and \( F[X; \frac{1}{3\mathbb{Z}}]/(X^{\frac{1}{3}})^{3n} \) over the field \( F \). Thus we see that multiplication by \( X^{\frac{1}{3}} \) in the ring \( F[X; \frac{1}{3\mathbb{Z}}]/(X^{\frac{1}{3}})^{3n} \) corresponds to cyclic shift \( \sigma \) in \( F^{3^n} \), that is, \( X^{\frac{1}{3}} \ast a(X^{\frac{1}{3}}) = \sigma(a)(X^{\frac{1}{3}}) \).

Let \( C \subset F^{3^n} \) be a linear code. As already agreed, we identify every vector \( a \) in \( F^{3^n} \) with the polynomial \( a(X^{\frac{1}{3}}) \) in \( F[X; \frac{1}{3\mathbb{Z}}]/(X^{\frac{1}{3}})^{3n} \), so \( C \subset F[X; \frac{1}{3\mathbb{Z}}]/(X^{\frac{1}{3}})^{3n} \). The elements of the code \( C \) are now referred to as code words or code (generalized) polynomials.

**Theorem 1** Let \( C \) be a linear code over \( F \). Then \( C \) is cyclic if and only if \( X^{\frac{1}{3}} \ast a(X^{\frac{1}{3}}) \in C \) for every \( a(X^{\frac{1}{3}}) \in C \).
Theorem 2 A subset \( C \) of \( F[X; \frac{1}{3^k}Z_0]_{3^k} \) is a cyclic code if and only if \( C \) is an ideal of the ring \( F[X; \frac{1}{3^k}Z_0]_{3^k} \).

Theorem 3 Let \( C \) be a nonzero ideal in the ring \( F[X; \frac{1}{3^k}Z_0]_{3^k} \), \( r = 2b \), \( b \in \mathbb{Z}^+ \) and \( k \geq 0 \) is an integer.

1) There exists a unique monic polynomial \( g(X^{\frac{1}{3^k}}) \) of least degree in \( C \).
2) \( g(X^{\frac{1}{3^k}}) \) divides \( (X^{\frac{1}{3^k}})^{3^kn} - 1 \) in \( F[X; \frac{1}{3^k}Z_0]_{3^k} \).
3) For all \( a(X^{\frac{1}{3^k}}) \in C \), \( g(X^{\frac{1}{3^k}}) \) divides \( a(X^{\frac{1}{3^k}}) \) in \( F[X; \frac{1}{3^k}Z_0]_{3^k} \).
4) \( C = (g(X^{\frac{1}{3^k}})) \).

Conversely, suppose \( C \) is an ideal generated by \( p(X^{\frac{1}{3^k}}) \in F[X; \frac{1}{3^k}Z_0]_{3^k} \). Then \( p(X^{\frac{1}{3^k}}) \) is a polynomial of least degree in \( C \) if and only if \( p(X^{\frac{1}{3^k}}) \) divides \( (X^{\frac{1}{3^k}})^{3^kn} - 1 \) in \( F[X; \frac{1}{3^k}Z_0]_{3^k} \).

If \( p(X^{\frac{1}{3^k}}) \) does not divide \( (X^{\frac{1}{3^k}})^{3^kn} - 1 \), \( p(X^{\frac{1}{3^k}}) \) cannot be of least degree in the ideal \( (p(X^{\frac{1}{3^k}})) \). Let \( C \) be a nonzero ideal in \( F[X; \frac{1}{3^k}Z_0]_{3^k} \) and let \( g(X^{\frac{1}{3^k}}) \) be the unique monic (generalized) polynomial of least degree in \( C \). Then \( g(X^{\frac{1}{3^k}}) \) is called the generator (generalized) polynomial of the cyclic code \( C \).

3 Improvements in the code rate and error correction

For a given positive integer \( r \geq 2 \), Ham\((r, 2)\) stands for a class of equivalent binary Hamming codes defined by an \( r \times (2^r - 1) \) parity check matrix \( H \) whose columns are the nonzero vectors in \( F_2 \). By a suitable ordering of the columns of \( H \) one can obtain a cyclic Hamming code.

Since there are \( 3^k r \) number of terms in generator polynomial \( p(X^{\frac{1}{3^k}}) = p_0 + p_1 X^{\frac{1}{3^k}} + \cdots + p_{3^kr-2} X^{\frac{1}{3^k}} + p_{3^kr-3} X^{\frac{1}{3^k}} \), so the binary bits. This means Ham\((\frac{3^k r - 1}{3^k}, 2)\) is equivalent to Ham\((3^k r, 2)\), which stands for a class of equivalent codes defined by a \( 3^k r \times (2^{3^k r} - 1) \) parity check matrix \( H \) whose columns are the nonzero vectors in \( F_2^{3^k r} \), \( r = 2b \), \( b \in \mathbb{Z}^+ \) and \( k \geq 0 \) is an integer.

Recall that, an irreducible polynomial \( p(X) \in F_2[X] \) of degree \( r \) is said to be primitive if the smallest positive integer \( n \) for which \( p(X) \) divides \( X^n + 1 \), where \( n = 2^r - 1 \).

The following theorems are from [11].

Theorem 4 Let \( p(X) \in F_2[X] \) be a primitive irreducible polynomial of degree \( r = 2b \), \( b \in \mathbb{Z}^+ \) and \( k \geq 0 \) is an integer, over \( F_2 \). Then corresponding (generalized) polynomial \( p(X^{\frac{1}{3^k}}) \) with degree \( 3^k r \) in the ring \( F_2[X; \frac{1}{3^k}Z_0] \) is also primitive irreducible.

The following establishes a relationship among Ham\((r, 2)\) and Ham\((3^k r, 2)\) if \( r = 2b \), where \( b \in \mathbb{Z}^+ \).

Theorem 5 Let \( p(X) \in F_2[X] \) be a primitive irreducible polynomial of degree \( r = 2b \), \( b \in \mathbb{Z}^+ \) and \( k \geq 0 \) is an integer, and \( (n + 1)^{3^k} - 1 = 2^{3^k r} - 1 \) be a positive integer. Then the cyclic code with the generator polynomial \( p(X^{\frac{1}{3^k}}) \) in the ring \( F_2[X; \frac{1}{3^k}Z_0]_{3^k} \) is Ham\((3^k r, 2)\).

Theorem 6 For \( r = 2b \), \( b \in \mathbb{Z}^+ \) and \( k \geq 0 \) is an integer, let \( C \subset F_2[X; \frac{1}{3^k}Z_0]_{3^k} \) be a cyclic code with generator polynomial

\[
g(X^{\frac{1}{3^k}}) = g_0 + g_1 X^{\frac{1}{3^k}} + g_2 (X^{\frac{1}{3^k}})^2 + \cdots + g_{3^kr-3} (X^{\frac{1}{3^k}})^{3^k r - 3} + g_r (X^{\frac{1}{3^k}})^{3^k r}, \text{ where } g_r = 1.
\]
Then $C$ is of dimension $(n+1)^3 - 1 - 3kr$. Moreover, the $(n+1)^3 - 1 - 3kr \times (n+1)^3 - 1$ matrix

$$G = \begin{bmatrix}
g_0 & g_{\frac{1}{3^k}} & \cdots & \cdots & g_{\frac{r}{3^k} - 1} & g_r & 0 & \cdots & 0 \\
g_0 & g_{\frac{1}{3^k}} & \cdots & \cdots & g_{\frac{r}{3^k} - 1} & g_r & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & g_0 & g_{\frac{1}{3^k}} & g_{\frac{2}{3^k}} & \cdots & g_r
\end{bmatrix}$$

is a generator matrix of $C$.

4 Decoding Procedure

Let $g(X^{\frac{1}{3^k}})$ be the generator (generalized) polynomial of the corresponding cyclic code $C \subset F_2[X; \frac{1}{3^k}Z_0]_{(n+1)^3 - 1}$, $r = 2b$, $b \in Z^+$ and $k \geq 0$ is an integer. Then we call the (generalized) polynomial $h(X^{\frac{1}{3^k}})$, the check polynomial of $C$, whereas $(X^{\frac{1}{3^k}})^{(n+1)^3 - 1} = g(X^{\frac{1}{3^k}})h(X^{\frac{1}{3^k}})$.

**Theorem 7** Let $C \subset F_2[X; \frac{1}{3^k}Z_0]_{3^k}$, $r = 2b$, $b \in Z^+$ and $k \geq 0$ is an integer, be a cyclic code with check polynomial $h(X^{\frac{1}{3^k}})$. Let $a(X^{\frac{1}{3^k}}) \in F_2[X; \frac{1}{3^k}Z_0]_{3^k}$. Then $a(X^{\frac{1}{3^k}}) \in C$ if and only if $a(X^{\frac{1}{3^k}})*h(X^{\frac{1}{3^k}}) = 0$.

**Theorem 8** For $r = 2b$, $b \in Z^+$ and an integer $k \geq 0$, let $C$ be a cyclic $((n+1)^3 - 1, (n+1)^3 - 1 - 3kr)$-code with check polynomial $h(X^{\frac{1}{3^k}}) = h_0 + h_{\frac{1}{3^k}}X^{\frac{1}{3^k}} + \cdots + h_{\frac{r}{3^k} - 1}(X^{\frac{1}{3^k}})^{l-1}$, with $1 \leq l \leq 3^k((n+1)^3 - 1 - 3kr)$, where $h_{\frac{l}{3^k}} = 1$. Then

a) The $3^kr \times ((n+1)^3 - 1)$ matrix

$$H = \begin{bmatrix}h_{\frac{l}{3^k}} & h_{\frac{l-2}{3^k}} & \cdots & \cdots & h_0 & 0 & 0 & 0 & 0 \\
0 & h_{\frac{l}{3^k}} & \cdots & \cdots & h_{\frac{1}{3^k}} & h_0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & h_{\frac{l}{3^k}} & h_{\frac{l-2}{3^k}} & \cdots & \cdots & \cdots & h_0
\end{bmatrix}$$

is a parity-check matrix for $C$.

b) The dual code $C^\perp$ is cyclic and generated by the polynomial

$$\overline{h}(X^{\frac{1}{3^k}}) = h_{\frac{l}{3^k}} + h_{\frac{l-2}{3^k}}X^{\frac{1}{3^k}} + \cdots + h_0(X^{\frac{1}{3^k}})^l.$$

**Theorem 9** Let $g(x^{\frac{1}{3^k}})$ be the generator polynomial of a cyclic $[3^kn, k]$-code $C$ over $F$. Let $A$ be a $k \times (3^kn - k)$ matrix whose $i$-th row is $g(x^{\frac{1}{3^k}})((x^{\frac{1}{3^k}})^{3^kn-K+i-1})$, where $i = 1, 2, \ldots, k$, then the canonical generator and parity-check matrices of $C$ are respectively $G = [I_k : -A]$ and $H = [A^T : I_{3^kn-k}]$.

Let $C_o$ be a cyclic $[n, m]$-code with check polynomial

$$h(x) = h_0 + h_1x + \cdots + h_mx^m$$

where $h_m = 1$. Then the $(n-m) \times n$ matrix

$$H_0 = \begin{bmatrix}h_m & h_{m-1} & \cdots & \cdots & h_0 & 0 & 0 & 0 & 0 \\
0 & h_m & \cdots & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & h_m & h_{m-1} & \cdots & \cdots & \cdots & h_0
\end{bmatrix}$$
is a parity-check matrix for $C$. Since $C \subset F[X; \frac{1}{3^k}Z_0]n$ is a cyclic code with check polynomial

$$h(X^{\frac{1}{3^k}}) = h_0 + \frac{1}{3^k}X^{\frac{1}{3^k}} + \cdots + h_{l-1}(X^{\frac{1}{3^k}})^{l-1},$$

with $1 \leq l \leq 3^k((n+1)^{3^k} - 1 - 3^kr)$, where $h_{l-1} \frac{1}{3^k} = 1$. Then $C$ is of dimension $(3^kr \times (n+1)^{3^k} - 1)$. Moreover, the $3^kr \times ((n+1)^{3^k} - 1)$ matrix $H$ is given by

$$H = \begin{bmatrix}
    h_{l-1} & h_{l-2} & \cdots & \cdots & \cdots & h_0 & 0 & 0 & 0 \\
    0 & h_{l-1} & \cdots & \cdots & \cdots & h_{l-2} & h_0 & 0 & \cdots & 0 \\
    \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\
    0 & 0 & 0 & h_{l-1} & h_{l-2} & \cdots & \cdots & \cdots & \cdots & h_0
\end{bmatrix}$$

is a parity-check matrix for $C$.

It is observed that matrix $H_0$ is a block in the matrix $H$, by interchanging the suitable columns, i.e.,

$$H = \begin{bmatrix}
    H_0 & A_1 \\
    A_2 & A_3
\end{bmatrix},$$

where the blocks $H_0, A_1, A_2$ and $A_3$ are the partitions of the matrix $H$.

Let us illustrate above claim by interchanging suitable columns by the following example. For $k = 1$ and $r = 2$, there is a parity-check matrix of order $6 \times 63$. That is

$$H = \begin{bmatrix}
    H_0(2 \times 3) & A_1(2 \times 60) \\
    A_2(4 \times 3) & A_3(4 \times 60)
\end{bmatrix}.$$ 

It is clear that in $H$, the block matrix $H_0$ is $2 \times 3$ matrix. We know that, if $C$ is a linear code with parity-check matrix $H$, then a received word $u \in F_2^{(n+1)^{3^k} - 1} = F_2^{3^k(3+1)^{3^k} - 1} = F_2^{63}$ decoded as $uH^t$ or $Hu^t$, that is, $C = \{u \in F_2^{63} : uH^t = 0 = Hu^t\}$. Let the corresponding received word $u$ be the $1 \times 63$ row matrix $[u_{0(1 \times 3)} : u_{1(1 \times 60)}]$ from $F_2^{63}$ in which the $u_{0(1 \times 3)} = [g_0 \ g_1 \ 0]$ is the initial received word from $F_2^{3}$ and $u_{1(1 \times 60)}$ is $1 \times 60$ zero row matrix. The transpose of the matrix $u$ is

$$u^t = \begin{bmatrix}
    u_{0(3 \times 1)}^t \\
    \vdots \\
    u_{1(60 \times 1)}^t
\end{bmatrix}$$

and

$$Hu^t = \begin{bmatrix}
    H_{0(2 \times 3)}u_{0(3 \times 1)}^t + A_{1(2 \times 60)}u_{1(60 \times 1)}^t \\
    \vdots \\
    A_{2(4 \times 3)}u_{0(3 \times 1)}^t + A_{3(4 \times 60)}u_{1(60 \times 1)}^t
\end{bmatrix}.$$ 

Thus received word $u$ is decoded as $Hu^t$. Thus $H_{0(2 \times 3)}u_{0(3 \times 1)}^t$ is the required decoding of initial received word $u_{0(1 \times 3)}^t$.

5 Conclusion

For a given primitive irreducible polynomial $p(X) \in F_2[X]$ of degree $r = 2b$, where $b \in Z^+$, there is a primitive irreducible (generalized) polynomial $p(X^{\frac{1}{3^k}}) \in F_2[X; \frac{1}{3^k}Z_0]$ with degree $3^kr$. Consequently corresponding to the binary Hamming code $\text{Ham}(r, 2)$ there exist a binary Hamming code $\text{Ham}(3^kr, 2)$ and hence for a given binary cyclic code $[n, n - r]$ with minimum distance $\leq r + 1$, there exist a binary cyclic code $[(n+1)^{3^k} - 1, (n+1)^{3^k} - 1 - 3^kr]$ with minimum
distance $\leq 3^k r + 1$. Thus corresponding code in $\mathbb{F}_2[X; \frac{1}{3^k} Z_0]_{(n+1)^{3k}-1}$ has capability to detect up to $3^k r$ errors in any transmitted codeword and can correct $e = \left\lfloor \frac{d - 1}{2} \right\rfloor = \left\lfloor \frac{3^k r + 1 - 1}{2} \right\rfloor = \left\lfloor \frac{3^k r}{2} \right\rfloor$ errors, while cyclic codes in $\mathbb{F}_2[X]_n$, can detect up to $r$ errors in any transmitted codeword, and can correct $e = \left\lfloor \frac{d - 1}{2} \right\rfloor = \left\lfloor \frac{r + 1}{2} \right\rfloor = \left\lfloor \frac{r}{2} \right\rfloor$ errors. Furthermore, in corresponding codes the code rate is improved.

The parity-check matrix $H_0$ of the cyclic code $[n, n - r]$ is a block of parity-check matrix $H$ of its corresponding binary cyclic code $[(n + 1)^{3k} - 1, (n + 1)^{3k} - 1 - 3^k r]$. This gives two advantages; 1) if we decode an $n$ length received word through $H$ instead of $H_0$, then there will be a more capability in error corrections, 2) if $n - r$ message transmitted under the security of binary cyclic code $[(n + 1)^{3k} - 1, (n + 1)^{3k} - 1 - 3^k r]$, then we obtain high speed data transfer as this corresponding code has high code rate than initial one.

Referências


