Improving the error-correcting code used in 3-G communication

Tahseen Rabbani

University of Virginia
twr7bm@virginia.edu

Advisor: Prof. James Davis

University of Richmond
jdavis@richmond.edu

Abstract

In 2011, Samsung Electronics Co. filed a complaint against Apple Inc. for alleged infringement of patents described in US 7706348, which details several embodiments of a TFCI (Transport Format Combination Indicator) encoder for mobile communication systems. One of the primary embodiments in question was a $[30, 10, 10]$ non-cyclic code which was implemented in all devices communicating on the 3-G network, including many Apple products. In this paper, the explicit construction of a $[30, 10, 10]$ idempotent code and a novel construction of an improved [30,10,11] non-cyclic code is detailed using methods described by F.J. MacWilliams and N.J.A. Sloane in their well-known text, "The Theory of Error-Correcting Codes."

1 Introduction

Error-correcting codes have a rich history dating back to the 1950's and now find their use in most devices capable of wireless communication and data storage. Among the more notable uses of an error-correcting code was to transmit encoded images of Mars taken by the Mariner 9 space probe. The reader is encouraged to see [3, p. 419] for further details. In the context of mobile communications, error-correcting codes are used to encode the TFCI (Transport Format Combination Indicator), which informs the receiver how to decode, de-multiplex, and deliver received messages over specified channels.

Consider a binary string of length k, representable as a vector $m \in \mathcal{F}_2^k$, sent through a noisy channel with an undesirable amount of interference. It is possible for the string to incur errors, i.e., various bits to be flipped. **Error-correcting codes** encode messages in such a way that the recipient is able to correct bit errors up to a certain threshold.

Seeing their wide usage in telecommunications, several patented codes have been the subject of litigation over possible infringement by competing developers. One such complaint [4], filed by Samsung Electronics Co. on June 28, 2011 against Apple Inc. covered a host of alleged patent infrigements. In one of the disputed patents were several versions (referred to as "embodiments" in the patent documentation) of a TFCI encoder described in US 7706348 [2]. The primary embodiment in question was a "$[30, 10, 10]$" error-correcting code. This paper details the construction and optimization of a code with the same essential properties as the $[30, 10, 10]$ embodiment, although not in same manner employed by Samsung.

We begin with a general survey of linear error-correcting codes, with a particular focus on the notions of length, dimension, and distance. An exploration of a particular family of codes, known as cyclic codes, is then presented in an effort to develop a theorem relating to a class of cyclic codes known as idempotent codes. The construction of an indempotent code with the same properties as the $[30, 10, 10]$ Samsung encoder is then given, along with an optimization which allows for stronger error-correction.

2 Properties of Error-Correcting Codes

A basic familiarity of linear algebra and abstract algebra is assumed, especially the notions of vector spaces and Galois (finite) fields. Although general properties of error-correcting codes are covered, only a certain class of codes, cyclic codes, are looked at in finer detail. For an extended treatment of cyclic codes and other families of error-correcting codes, the reader is encouraged to see [3], from which a bulk of the theoretical machinery in the paper is derived.

2.1 Linear Codes

Definition 2.1 *Let $q \in \mathbb{N}$ such that $q = p^n$ where p is prime. Consider $\mathcal{F}_q$, the field containing q elements. A* ***linear code*** *$\mathcal{C}$ of length n is a k-dimensional subspace of the vector space $\mathcal{F}_q^n$ where $0 \leq k \leq n$. Each vector in the subspace is referred to as a* ***codeword****.*

Henceforth, the reader may assume "code" to mean "linear code." Binary codes will eventually be the primary subject of discussion, which are codes over $\mathcal{F}_2 = \{0, 1\}$.

If $\{v_1, v_2, \dots, v_k\}$ form a basis of a code $\mathcal{C}$ over $\mathcal{F}_q$, we may also represent the code as the row space (over $\mathcal{F}_q$) of a **generator matrix** $\mathcal{G}$, where

$$\mathcal{G} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}.$$

Definition 2.2 *The* ***Hamming weight*** *of a binary string x, denoted by $wt(x)$, is the number of coordinates (entries) with value 1. The* ***Hamming distance*** *between two binary strings x and y, denoted by $dist(x, y)$, is the number of coordinates between which x and y differ.*

Since $0 + 0 = 0$ and $1 + 1 = 0$ over $\mathcal{F}_2$, if a coordinate differs between two strings, the resulting sum between both will yield a 1 at that coordinate. Hence,

$$dist(x, y) = wt(x + y).$$

An important property of a code is the minimum of all distances between its codewords, which is denoted by d.

Lemma 2.3 $wt_{min}(\mathcal{C}) = d$.

Proof. Consider two codewords $c_1, c_2 \in \mathcal{C}$ between which distance is minimized. $wt(c_1 + c_2) = wt(c_3) = d$, where $c_3 \in \mathcal{C}$ since any linear combination of two codewords is contained within the code. ∎

2.2 Encoding and Decoding

A binary code $\mathcal{C}$ of dimension k encodes a message $v \in \mathcal{F}_2^k$ simply by multiplying v with the generator matrix $\mathcal{G}$, that is, $v\mathcal{G}$. We will denote the encoded message as m. Clearly, m is a codeword. The sender delivers m and what the target receives will be denoted as m', which may or may not be equal to m depending on whether any errors were incurred.

To decode m', the recipient adopts a **maximum likelihood** strategy and assumes the message to be the codeword c such that $dist(m', \mathcal{C})_{min} = dist(m', c)$. Lastly, the recipient solves for $x\mathcal{G} = m'$ for which the solution is the original message v, assuming m' is similar enough to m. This threshold of similarity may now be established.

Theorem 2.4 *A linear code $\mathcal{C}$ with minimum distance $d \geq 2t + 1$ for $t \geq 0$ and decoding procedure obeying maximum likelihood can correct up to t errors.*

Proof. Let $\mathcal{C}$ be a linear code with minimum distance $d \geq 2t + 1$ where $t \geq 0$. Suppose a message v is encoded as $m = v\mathcal{G}$, delivered, and received as m'. Suppose m' has at most t errors. Then, $dist(m, m') \leq t$ and $dist(m, u) \geq d$ for any $u \in \mathcal{C}$ not equal to m. Then by the triangle inequality[1],

$$dist(m, u) \leq dist(m, m') + dist(m', u).$$

[1]The Hamming distance is a metric on binary vector spaces meaning it satisfies, among other properties, the triangle inequality.

Hence,

$$dist(m', u) \geq dist(m, u) - dist(m, m') \geq d - t \geq t + 1.$$

This indicates that under maximum likelihood, m' will be closer in Hamming distance to m than any other codeword. ∎

The length n, dimension k, and minimum distance d, are among the most important properties of a code and are often notated as $[n, k, d]$. The dimension of the code will affect the number of values assignable via codewords, greater minimum distance ensures stronger error-correcting capabilities, and shorter lengths require less memory capacity.

3 Cyclic Codes

The [30,10,10] code which is constructed in this paper is within a family of error-correcting codes known as cyclic codes.

3.1 Properties

Definition 3.1 *A linear code $\mathcal{C}$ of length n is a **cyclic code** if and only if*

$$c = (a_0, a_1, a_2, \dots, a_{n-1}) \in \mathcal{C},$$

then

$$c^* = (a_{n-1}, a_0, a_1, \dots, a_{n-2}) \in \mathcal{C}.$$

We refer to such a rightward shift as a **cyclic shift**. It is useful to associate codewords with polynomials. For a code $\mathcal{C}$ over $\mathcal{F}_q^n$ and

$$c = (a_0, a_1, a_3, \dots, a_{n-1}) \in \mathcal{C},$$

we associate it with the polynomial

$$c(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} \in \mathcal{F}_q[x]/(x^n - 1).$$

By $F_q[x]/(x^n - 1)$, we mean the set of congruence classes of $\mathcal{F}_q[x]$ modulo $(x^n - 1)$. We may represent n cyclic shifts of a codeword c as $x^n c(x)$. Since we will frequently switch between codewords and their associated polynomials, we will allow either representation to denote the other where it is convenient, i.e., the use of code polynomial in a matrix is intended to denote a string with the coefficients of the polynomial.

Theorem 3.2 *A cyclic code of length n is an ideal of $\mathcal{F}_q[x]/(x^n - 1)$.*

Proof. This follows immediately from the definition of an ideal, allowing the additive subgroup to be the code itself. ∎

We have that $\mathcal{F}_q[x]/(x^n-1)$ is a principal ideal domain so, from basic abstract algebra, this implies that for every cyclic code $\mathcal{C}$ there exists a unique monic polyonomial $g(x)$ of minimal degree such that $\langle g(x)\rangle = \mathcal{C}$. The polynomial $g(x)$ is referred to as the **generator polynomial** of $\mathcal{C}$. The generator polynomial may be used to construct a generator matrix for the code.

Theorem 3.3 *Let $\mathcal{C}$ be a cyclic code of length n over $\mathcal{F}_q[x]/(x^n-1)$ and $g(x)$ its generator polynomial. If $g(x)=\sum_{i=0}^{r} g_i x^i$ where r is the degree, then*

$$\mathcal{G} = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_r & \cdots & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{r-1} & g_r & \cdots & 0 & \cdots & 0 \\ & & & & \cdots & \cdots & & & & \\ & & & & \cdots & \cdots & & & & \\ 0 & \cdots & g_0 & g_1 & \cdots & \cdots & & & & g_r \end{pmatrix} = \begin{pmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ \vdots \\ x^{n-r-1} g(x) \end{pmatrix}$$

is a generator matrix of $\mathcal{C}$ with n columns and $n-r$ rows.

Proof. See [3, p. 190]. ■

Corollary 3.4 *Let $g(x)$ be the generator of a cyclic code $\mathcal{C} \in \mathcal{F}_q[x]/(x^n-1)$. If $g(x)$ is of degree r, then for any codeword $c(x)=h(x)g(x)$ where $h(x) \in \mathcal{F}_q[x]/(x^n-1)$, any $n-r$ cyclic shifts of $c(x)$ form a basis of $\mathcal{C}$.*

Proof. $$\mathcal{G}' = \begin{pmatrix} x^j h(x)g(x) \\ x^{j+1}h(x)g(x) \\ x^{j+2}h(x)g(x) \\ \vdots \\ x^{j+n-r-1}h(x)g(x) \end{pmatrix} = x^j h(x) \begin{pmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ \vdots \\ x^{n-r-1} g(x) \end{pmatrix} = x^j h(x)\mathcal{G}.$$

Since the row space of $\mathcal{G}$ (which is $\mathcal{C}$) is an ideal by Theorem 3.2, the result follows. ■

3.2 Idempotents

In this section, we only consider cyclic codes over $\mathcal{F}_2/(x^n-1)$ where n is odd, unless stated otherwise.

Definition 3.5 *A polynomial $I(x) \in \mathcal{F}_2/(x^n-1)$ is an **idempotent** if*

$$I(x) = I(x)^2 = I(x^2).$$

Idempotents are closed under addition. If $I_1(x)$ and $I_2(x)$ are idempotents, then

$$(I_1(x)+I_2(x))^2 = I_1(x)^2 + 2I_1(x)I_2(x) + I_2(x)^2 = I_1(x)^2 + I_2(x)^2 = I_1(x) + I_2(x)$$

Definition 3.6 *A **cyclotomic coset** mod n over $\mathcal{F}_q$ where $gcd(n,q)=1$ is any set*

$$\mathcal{C}_{s\in\mathbb{Z}} = \{s, qs, q^2 s, \ldots, q^{j-1}s\},$$

where j is the smallest positive integer such that $q^j s \equiv s \mod n$.

Definition 3.7 *If $f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$, define*

$$f^*(x) = a_0 + a_{n-1}x + \ldots + a_1 x^{n-1}$$

*to be the **reversion** of f.*

Although not explicitly proven here, the exponents of the nonzero terms are a union of cyclotomic cosets over $\mathcal{F}_2$, which we denote as $\sum_s \sum_{j\in C_s} x^j$.

Lemma 3.8 *If $I(x)$ is an idempotent, then so is $I^*(x)$.*

Proof. This simple argument comes from [3, p. 219]. If

$$I(x) = \sum_s \sum_{j\in C_s} x^j$$

then

$$I^*(x) = \sum_s \sum_{j\in C_{-s}} x^j$$

■

As an example, we list the cyclotomic cosets mod 31 over $\mathcal{F}_2$, which will play an important role in the construction of the $[30, 10, 10]$ code:

$$\begin{aligned}
\mathcal{C}_0 &= \{0\}\\
\mathcal{C}_1 &= \{1, 2, 4, 8, 16\}\\
\mathcal{C}_3 &= \{3, 6, 12, 24, 17\}\\
\mathcal{C}_5 &= \{5, 10, 20, 9, 18\}\\
\mathcal{C}_7 &= \{7, 14, 28, 25, 19\}\\
\mathcal{C}_{11} &= \{11, 22, 13, 26, 21\}\\
\mathcal{C}_{15} &= \{15, 30, 29, 27, 23\}
\end{aligned}$$

For $j \in \mathcal{C}_s$, we have that $\mathcal{C}_j = \mathcal{C}_s$, so we have listed all the distinct cosets.

Theorem 3.9 *Any ideal or cylic code $\mathcal{C}$ contains a unique idempotent $E(x)$ such that $\mathcal{C} = \langle E(x)\rangle$. We refer to such a generator as the idempotent of $\mathcal{C}$.*

Proof. See [3, p. 217]. ■

Definition 3.10 *If $\mathcal{C}$ is a minimal ideal, that is, not containing any smaller nonzero ideals, then the idempotent of C is referred to as a **primitive idempotent**. The cyclic code generated by this ideal is called an **irreducible code**.*

Let $\mathcal{C}$ be cyclic code over $\mathcal{F}_q$ of length n relatively prime to q. This implies there is a smallest natural number m such that $n \mid q^m - 1$. We may accept without proof that the roots of $x^n - 1$ lie in $\mathcal{F}_{q^m}$ and in no smaller field. These zeros are called the n^{th} **roots of unity** and there are, in fact, n of them, hence $\mathcal{F}_{q^m}$ is a splitting field of $x^n - 1$. Furthermore, the roots of unity form a cyclic subgroup and we refer to the generator α as the **primitive root of unity**.

Let $\mathcal{M}_s$ be a minimal ideal such that the nonzeros of its generator consists of $\{\alpha^i : i \in \mathcal{C}_s\}$. By Theorem 3.9, $\mathcal{M}_s$ has an idempotent generator, which we will refer to as $\theta_s(x)$. Using these theta polynomials, we arrive at a theorem which will produce a preliminary [31,11,11] code.

Theorem 3.11 *Let $m = 2t + 1$ where $t \geq 0$, and let d be any integer in the range $1 \leq d \leq t$. Then the binary ideal of length $2^m - 1$ with idempotent*

$$\theta_0 + \theta_1^* + \sum_{j=d}^{t} \theta_{l_j}^*$$

where $l_j = 2^j + 1$ forms a $[2^m - 1, m(t - d + 2) + 1, 2^{m-1} - 2^{m-d-1}]$ cyclic code.

Proof. See [3, p. 455]. ∎

3.3 The [30,10,10] Code

The first embodiment of the Samsung encoder (see Appendix A) is a noncyclic [32,10,12] code. The motivation behind shortening to a length 30 code is not entirely clear, beyond saving memory, but encoding with 10 information bits (the number of basis vectors, and thus the length of messages which may be encoded) is the TFCI standard in current coding schemes. The construction of the encoder's basis is rather complicated, so it will not be covered, but the reader is encouraged to see [1] for an explanation. The second embodiment, a [30, 10, 10] encoder,

$$S_{[30,10,10]} = \begin{pmatrix} 101010101010101101010101010101 \\ 011001100110011011001100110011 \\ 000111100001111000111100001111 \\ 000000011111111000000011111111 \\ 000000000000000111111111111111 \\ 111111111111111111111111111111 \\ 010100001100011111000001110111 \\ 000000111001101110110111000111 \\ 000101011111001001101100101011 \\ 001110000110111010111101010001 \end{pmatrix}$$

is created by puncturing the 1st and 17th coordinate from every basis vector.

By Theorem 3.11, if we set $m = 5$, $t = 2$, and $d = 2$, then the binary ideal in $\mathcal{F}_2/(x^{31} - 1)$ with idempotent $g(x) = \theta_0 + \theta_1^* + \theta_5^*$ is a [31,11,11] cyclic code. We have that

$$\begin{aligned} \theta_0 &= 1111111111111111111111111111111 \\ \theta_1^* &= 1001011001111100011011101010000 \\ \theta_5^* &= 1110100010010101100001110011011. \end{aligned}$$

By Corollary 3.4, 11 consecutive shifts of $\theta_0 + \theta_1^* + \theta_5^*$ will form a basis for this code (see appendix B). Rather than taking this construction at face value, we will algebraically prove that this basis has a mininmum distance of at least 11. First notice that over $\mathcal{F}_{32} = \mathcal{F}_2(\alpha)$ where $\alpha^5 + \alpha^2 + 1 = 0$,

$$\begin{aligned} \theta_0 + \theta_1^* + \theta_5^* &= 1000000100010110000101100110100 \\ &= 1 + x^7 + x^{11} + x^{13} + x^{14} + x^{19} + x^{21} + x^{22} + x^{25} + x^{26} + x^{28} \end{aligned}$$

has 10 consecutive roots: $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{10}$. Since every codeword $c(x) = h(x)g(x)$ where $h(x) \in \mathcal{F}_2[x]/(x^{31} - 1)$, then

$$c(\alpha) = c(\alpha^2) = \ldots = c(\alpha^{10}) = 0.$$

Thus, if $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{30}x^{30}$, we have

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{30} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{29} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{28} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{10} & \alpha^{20} & \cdots & \alpha^{31} \end{pmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_3 \\ \vdots \\ \vdots \\ c_{30} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix}.$$

Any 10 columns of the left matrix, the collection of which we will denote as the matrix $\mathcal{A}$, are linearly independent. To see this, notice that

$$det(\mathcal{A}) = \begin{vmatrix} \alpha^{j_1} & \alpha^{j_2} & \cdots & \alpha^{j_{10}} \\ \alpha^{2j_1} & \alpha^{2j_2} & \cdots & \alpha^{2j_{10}} \\ \alpha^{3j_1} & \alpha^{3j_2} & \cdots & \alpha^{3j_{10}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{10j_1} & \alpha^{10j_2} & \cdots & \alpha^{10j_{10}} \end{vmatrix} = \alpha^{(j_1+\cdots+j_{10})} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \cdots & \alpha^{j_{10}} \\ \alpha^{2j_1} & \alpha^{2j_2} & \cdots & \alpha^{2j_{10}} \\ \vdots & \vdots & \ddots & \alpha^{2j_{10}} \\ \alpha^{9j_1} & \alpha^{9j_2} & \cdots & \alpha^{9j_{10}} \end{vmatrix}$$

after factoring out j_i from every ith column, which is a standard property of determinants. The right-hand determinant is equivalent to that of a Vandermonde matrix, for which the value is $\prod_{k \neq l}(\alpha^{j_k} - \alpha^{j_l})$. Thus,

$$det(\mathcal{A}) = \alpha^{(j_1+\cdots+j_{10})} \prod_{k \neq l}(\alpha^{j_k} - \alpha^{j_l}) \neq 0$$

which establishes the linear independence of any 10 columns of $\mathcal{A}$. Thus, $c(x)$ must have at least 11 nonzero coefficients, establishing a lower bound on the minimum distance. Once again, this calculation is only illustrative and by Theorem 3.11, we know the cyclic code generated by $\theta_0 + \theta_1^* + \theta_5^*$ has a minimum distance of exactly 11.

To create a [30,10,10] code, simply delete any of the basis vectors and puncture any coordinate. A variation, shown in Appendix C, is created by deleting the last basis vector and puncturing the first coordinate.

3.4 The [30,10,11] Code

A third embodiment of the Samsung encoder, which was not actively pursued for alleged infrigement was a noncyclic [30,7-10,11] encoder. By Theorem 2.4, in 10 information bits, this is superior to a [30,10,10] encoder as it will correct up to 5 errors, while the $[30, 10, 10]$ encoder will correct up to 4 errors. A simple manipulation of $G_{[31,11,11]}$ (see Appendix B), which is generated by cyclic shifts of the idempotent $g(x) = \theta_0 + \theta_1^* + \theta_5^*$, produces a noncyclic [30,10,11] code. First, the second basis vector $xg(x)$ is replaced with $x^{12}g(x)$, producing the matrix:

$$G^*_{[31,11,11]} = \begin{pmatrix} 1000000100010110000101100110100 \\ 1011001101001000000100010110000 \\ 0010000001000101100001011001101 \\ 1001000000100010110000101100110 \\ 0100100000010001011000010110011 \\ 1010010000001000101100001011001 \\ 1101001000000100010110000101100 \\ 0110100100000010001011000010110 \\ 0011010010000001000101100001011 \\ 1001101001000000100010110000101 \\ 1100110100100000010001011000010 \end{pmatrix}$$

The rows are linearly independent as $x^{12}g(x) = xg(x) + x^3g(x) + x^8g(x) + x^9g(x) + x^{10}g(x)$, and we have removed the row corresponding to $xg(x)$. This matrix generates a [31,10,11] code.[2] The 9th column contains only a single 1 which corresponds to $x^8g(x)$, so deleting this basis vector will not affect the minimum distance and produces a column with all zeros –which is precisely the coordinate we puncture.

The [30,10,11] generator matrix:

$$G_{[30,10,11]} = \begin{pmatrix} 100000010010110000101100110100 \\ 101100111001000000100010110000 \\ 001000001000101100001011001101 \\ 100100000100010110000101100110 \\ 010010000010001011000010110011 \\ 101001000001000101100001011001 \\ 110100100000100010110000101100 \\ 011010010000010001011000010110 \\ 100110101000000100010110000101 \\ 110011010100000010001011000010 \end{pmatrix}$$

Acknowledgements

A great deal of gratitude is due towards Dr. James Davis of the University of Richmond for his invaluable insight, feedback, and technical expertise on the Samsung v. Apple lawsuit. I would also like to thank Sung-Min Park and Apollo Jain for their development of programs which allowed me to verify certain properties of the codes I was interested in. Finally, I thank my family and Mark Davis for their moral support.

[2]The minimum distance was verified using two independently developed programs.

References

[1] A.E. BROUWER, The [32,10,12] TFCI code, Jan, 19, 2012.
Available @ `http://www.win.tue.nl/~aeb/codes/tfci/tfci.pdf`.

[2] J.Y. KIM, H.W. KANG, Apparatus and method for encoding/decoding transport format combination indicator in CDMA mobile communication system, U.S. Patent 7706348 B2, Apr. 27, 2010.

[3] F. J. MACWILLIAMS, N.J.A. SLOANE, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[4] UNITED STATES INTERNATIONAL TRADE COMMISSION, Notice of Insitution of Investigation, Inv. No. 337-TA-794, July 27, 2011.

Appendix

A [32,10,12] Samsung Code

$$
S_{[32,10,12]} = \begin{pmatrix}
01010101010101010101010101010101 \\
00110011001100110011001100110011 \\
00001111000011110000111100001111 \\
00000000111111110000000011111111 \\
00000000000000001111111111111111 \\
11111111111111111111111111111111 \\
00101000011000111111000001110111 \\
00000001110011010110110111000111 \\
00001010111110010001101100101011 \\
00011100001101110010111101010001
\end{pmatrix}
$$

B [31,11,11] Idempotent Code

$$
G_{[31,11,11]} = \begin{pmatrix}
1000000100010110000101100110100 \\
0100000010001011000010110011010 \\
0010000001000101100001011001101 \\
1001000000100010110000101100110 \\
0100100000010001011000010110011 \\
1010010000001000101100001011001 \\
1101001000000100010110000101100 \\
0110100100000010001011000010110 \\
0011010010000001000101100001011 \\
1001101001000000100010110000101 \\
1100110100100000010001011000010
\end{pmatrix}
$$

C [30,10,10] Idempotent Code

$$
G_{[30,10,10]} = \begin{pmatrix}
000000100010110000101100110100 \\
100000010001011000010110011010 \\
010000001000101100001011001101 \\
001000000100010110000101100110 \\
100100000010001011000010110011 \\
010010000001000101100001011001 \\
101001000000100010110000101100 \\
110100100000010001011000010110 \\
011010010000001000101100001011 \\
001101001000000100010110000101
\end{pmatrix}
$$