

168487

YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

REED-MULLER KODLARI

Matematikçi Seza ERMAN

FBE Matematik Anabilim Dalında
Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Yrd.Doç.Dr.Nilgün AYGÖR

Yrd. Doç. Dr. Nilgün AYGÖR 

Prof. Dr. Mustafa Sivri 

Prof. Dr. Göksel Ağargün 

İSTANBUL, 2005

İÇİNDEKİLER

	Sayfa
SİMGE LİSTESİ	iii
KISALTMA LİSTESİ	iv
ÖNSÖZ	v
ÖZET	vi
ABSTRACT	vii
1 TEMEL TANIMLAR.....	1
2 REED-MULLER KODLARI	7
2.1 Basit Tanım.....	7
2.2 Tekrarlamalı Tanım	9
2.3 Alternatif Tanım	13
2.4 Kodlama.....	15
3 KOD ÇÖZME.....	16
3.1 Majority Logic ile Kod Çözme.....	16
3.2 RM(1, m) için Kod Çözme	22
4 REED-MULLER KODLARININ UYGULAMALARI	29
4.1 Üreteç Matrisin Hesaplanması.....	29
4.2 Kodlama.....	31
4.3 Kod Çözme	32
KAYNAKLAR.....	36
ÖZGEÇMİŞ.....	37

SİMGE LİSTESİ

$RM(r, m)$	m değişkenli, r. mertebeden Reed-Muller kodu
$G_{RM(r, m)}$	Üreteç Matris
$C^\perp$	C kodunun duali
$d(C)$	C kodunun uzaklığı
$w(x)$	x vektörünün ağırlığı



KISALTMA LİSTESİ

MIT Massachusetts Institute of Technology



ÖNSÖZ

Bu tezi hazırlamamda bana her konuda yardımcı olan, sayın hocam Yrd. Doç. Dr. Nilgün Aygör'e teşekkürlerimi sunarım.



ÖZET

Reed-Muller kodları, en eski ve en iyi bilinen kodlardan biridir. 1954 yılında, D.E.Muller ve I.S.Reed tarafından keşfedilmiştir. 1972’de bir Reed-Muller kodu, Mariner 9 uydusu tarafından, Mars’ın siyah-beyaz fotoğraflarını gönderebilmek için kullanılmıştır.

Reed-Muller kodlarının ilginç bir özelliği kodların sonsuz bir ailesi şeklinde oluşmalarıdır. Geniş Reed-Muller kodları, küçük olanlardan oluşturulur. Fakat uzunluklarının artması Reed-Muller kodlarını daha zayıf yapar.

Reed-Muller kodlarının önemli avantajlarından biri de mesajların kodlanması ve alınan iletilerin çözülmesinde önemli kolaylıklar getirmesidir.

Bu tezde amaç, Reed-Muller kodlarını anlayabilmek için gerekli bilgileri vermektir. Reed-Muller kodlarının tanımı üç farklı biçimde yapılmıştır. Her tanım ayrı ayrı incelenmiş ve örneklerle açıklanmıştır. Farklı üreteç matrisler tanımlanmıştır. Mesajları kodlayabilmek için basit bir yöntem gösterilmiştir. Kodların çözümünde ise farklı metodlar ele alınmış ve algoritmaları verilmiştir. Özel durumdaki kodların hata içeren mesajlarını çözebilmek için, farklı yöntemler gösterilmiştir. Son olarak, MATLAB programı ile yazılmış, üreteç matris hesaplama, kodlama ve kod çözme programları ve örnekleri verilmiştir.

Anahtar kelimeler: Reed-Muller Kodları, Kodlama Teorisi, Kod Çözme, Üreteç Matris, Majority Logic

ABSTRACT

Reed-Muller codes are some of the oldest and most well-known error correcting codes. They were invented in 1954 by D.E.Muller and I.S.Reed. In 1972, a Reed-Muller code was used by Mariner 9 to transmit black and white photographs of Mars.

Reed-Muller codes have many interesting properties. They form an infinite family of codes and larger Reed-Muller codes can be constructed from smaller ones. But, they become weaker as their length increases.

One of the major advantages of Reed-Muller codes is their relative simplicity to encode messages and decode received transmissions.

The aim of this thesis is to give the necessary informations in order to understand Reed-Muller codes. There are three different definitions for Reed-Muller codes. Each definition has been explained by giving examples. Different generator matrices have been defined. A simple method has been given to encode the messages. In decoding, different methods and algorithm have been given. Also, we can decode easily the error messages in the codes which are in special situations. Finally, generator matrix, encoding and decoding have been calculated by MATLAB.

Keywords: Reed-Muller Codes, Coding Theory, Encoding, Generator Matrix, Decoding, Majority Logic.

1. TEMEL TANIMLAR

1.1 Tanım

$a_i \in F_q$ olmak üzere $a_1, a_2, \dots, a_n$ şeklindeki tüm sıralı n 'lilerin kümesi F_q^n ile gösterilir. F_q^n 'in elemanlarına kod sözcükleri denir.

F_q^n cismi üzerinde bir x vektörü alalım. x vektörü n uzunluktadır ve elemanları $\bar{q}$ kümesinin elemanlarıdır. Örneğin; $v = (1,0,1,1,0,1,0)$ vektörü $v = 1011010$ şeklinde yazılabilir ve $v \in F_2^7$ 'dir.

$x, y \in F_2^n$ ve $a \in F_2$ olacak şekilde, $x = (x_1, x_2, \dots, x_n)$ ve $y = (y_1, y_2, \dots, y_n)$ vektörleri için,

$x + y = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$ toplama

$a + x = (a + x_1, a + x_2, \dots, a + x_n)$ skalerle toplama

$\bar{x} = 1 + x = (1 + x_1, 1 + x_2, \dots, 1 + x_n)$ tümleyen vektör

$x * y = (x_1 * y_1, x_2 * y_2, \dots, x_n * y_n)$ çarpma

$a \cdot x = (a \cdot x_1, a \cdot x_2, \dots, a \cdot x_n)$ skalerle çarpma

olarak tanımlanır.

Ayrıca, $1+1=0, 0+1=1, 1+0=1, 0+0=0$ ve $1*1=1, 0*1=0, 1*0=0, 0*0=0$ dır.

$x \cdot y = x_1 * y_1 + x_2 * y_2 + \dots + x_n * y_n$ nokta çarpım olarak tanımlanır.

Bu özelliklerden $(F_2^n, +, *)$ 'nin bir değişmeli halka yapısında olduğu da görülebilir.

F_2 cismi üzerinde vektör uzayı olan $F_2^{2^m}$ 'i düşünelim. R_m halkası $R_m = F_2[x_0, x_1, \dots, x_{m-1}]$ olacak şekilde R_m ve $F_2^{2^m}$ 'in elemanları arasında birebir ve örten bir eşleme vardır. Diğer bir deyişle $(R_m, +, *)$ ve $(F_2^{2^m}, +, *)$ arasında bir halka izomorfizması vardır.

1.2 Tanım

$p \in R_m$ elemanı, $r_i \in \mathbb{N}$ ve $i \in \{0, 1, \dots, m-1\}$ için $p = x_0^{r_0} x_1^{r_1} \dots x_{m-1}^{r_{m-1}}$ şeklinde olsun. Bir Boole polinomu, p elemanları ile F_2 'deki elemanların lineer kombinasyonu ile oluşur. R_m deki herhangi bir eleman bir boole polinomu şeklinde düşünülebilir.

1.3 Tanım

$p \in R_m$, Tanım (1.2)'de olduğu gibi $p = x_0^{r_0} x_1^{r_1} \dots x_{m-1}^{r_{m-1}}$ şeklinde tanımlı olsun. Eğer aşağıdaki

özellikler sağlanıyorsa p 'ye indirgenmiş formdadır denir:

$$\begin{aligned} x_i x_j &= x_j x_i \\ x_i^2 &= x_i \end{aligned} \quad (1.1)$$

Ayrıca bir Boole polinomu, indirgenmiş formdaki p elemanları ve $\mathbb{F}_2$ 'deki elemanların lineer kombinasyonu şeklinde oluşmuş ise indirgenmiş formdadır. Örneğin; bir Boole polinomu

$$p = 1 + x_1 + x_0^5 x_2^2 + x_0 x_1^4 x_2^{101} \in R_3 \text{ olsun.}$$

p polinomunun indirgenmiş formu $p' = 1 + x_1 + x_0 x_2 + x_0 x_1 x_2$ olur.

1.4 Tanım

$\psi: R_m \rightarrow \mathbb{F}_2^{2^m}$ fonksiyonu aşağıdaki gibi tanımlanmış olsun:

$$\begin{aligned} \psi(0) &= \underbrace{00\dots0}_{2^m} \\ \psi(1) &= \underbrace{11\dots1}_{2^m} \\ \psi(x_0) &= \underbrace{11\dots1}_{2^{m-1}} \underbrace{00\dots0}_{2^{m-1}} \\ \psi(x_1) &= \underbrace{11\dots1}_{2^{m-2}} \underbrace{00\dots0}_{2^{m-2}} \underbrace{011\dots1}_{2^{m-2}} \underbrace{100\dots0}_{2^{m-2}} \\ \psi(x_2) &= \underbrace{11\dots1}_{2^{m-3}} \underbrace{00\dots0}_{2^{m-3}} \underbrace{011\dots1}_{2^{m-3}} \underbrace{100\dots0}_{2^{m-3}} \underbrace{011\dots1}_{2^{m-3}} \underbrace{100\dots0}_{2^{m-3}} \underbrace{011\dots1}_{2^{m-3}} \underbrace{100\dots0}_{2^{m-3}} \\ &\vdots \\ \psi(x_i) &= \underbrace{11\dots1}_{2^{m-(i+1)}} \underbrace{00\dots0}_{2^{m-(i+1)}} \dots \\ &\vdots \end{aligned}$$

Tanım (1.2)'deki gibi tanımlanmış herhangi $p \in R_m$ için $\psi(p)$ 'yi hesaplamak isteyelim.

Öncelikle indirgenmiş forma getirelim. $p' = x_{i_1} x_{i_2} \dots x_{i_r}$ olsun. ($i_j \in \mathbb{Z}_m$ için, $i_j = i_k$ ise $j = k$, ve $0 \leq r \leq m$).

$\psi(p) = \psi(x_{i_1}) * \psi(x_{i_2}) * \dots * \psi(x_{i_r})$ şeklindedir.

m_i 'ler Tanım (1.2)'deki gibi tanımlanmak üzere, herhangi $q \in R_m$ polinomu

$q = m_1 + m_2 + \dots + m_r$ şeklinde olur. ($m_i = m_j$ ise $i = j$, ve $0 \leq r \leq 2^m$).

$$\psi(q) = \psi(m_1) + \psi(m_2) + \dots + \psi(m_r) \quad (1.2)$$

1.5 Örnek

$p = 1 + x_1 + x_0^5 x_2^2 + x_0 x_1^4 x_2^{101} \in R_3$ polinomunu alalım.

p 'nin indirgenmiş formu $p' = 1 + x_1 + x_0 x_2 + x_0 x_1 x_2$ olur.

$$\psi(p) = \psi(p')$$

$$= \psi(1) + \psi(x_1) + \psi(x_0 x_2) + \psi(x_0 x_1 x_2)$$

$$= \psi(1) + \psi(x_1) + \psi(x_0) * \psi(x_2) + \psi(x_0) * \psi(x_1) * \psi(x_2)$$

$$= 11111111 + 11001100 + 11110000 * 10101010 + 11110000 * 11001100 * 10101010$$

$$= 00010011 \text{ bulunur.}$$

1.6 Tanım

Bir C kodunun minimum uzaklığı $d(C)$ ile gösterilir ve bu farklı kod sözcükleri arasındaki minimum uzaklığa eşittir. x ve y kod sözcükleri olmak üzere, $d(C) = \min \{d(x, y) | x \neq y\}$ dir.

1.7 Tanım

Bir C kodunun duali $C^\perp$ ile gösterilir ve $C^\perp = \{v \in V(n, q) | u \cdot v = 0, \forall u \in C \text{ için}\}$ 'dir.

1.8 Tanım

F_2^n 'deki bir x vektörünün ağırlığı; x vektörünün bileşenlerindeki 1'lerin sayısıdır ve $w(x)$ ile gösterilir.

1.9 Teorem

x ve y bir lineer kodun, herhangi iki kod sözcüğü olsun. Buna göre $d(x, y) = w(x - y)$ dir.

İspat: $x - y$ vektöründeki 0'dan farklı semboller x ve y 'nin farklı sembol taşıdığı konumlarda bulunur. Buradan eşitlik görünür.

1.10 Teorem

$w(C)$, bir C lineer kodunun 0'dan farklı kod sözcüklerinin ağırlıklarının en küçüğü olsun. Bu durumda $d(C) = w(C)$ dir.

İspat: $x, y \in C$ için $d(C) = d(x, y)$ olsun.

$$d(C) = d(x, y) = w(x - y) \geq w(C) \quad (1)$$

$$x \in C \text{ alalım. } w(C) = w(x) = d(x, 0) \geq d(C) \quad (2)$$

(1) ve (2)'den $d(C) = w(C)$ elde edilir.

1.11 Tanım

Lineer bir $[n, k]$ kodun, bir bazındaki vektörleri satırlara yazarak elde edilen bir $k \times n$ matris, bir lineer kodun üreteç matrisi adını alır.

1.12 Örnek

F_2^5 'te üreteç matrisi $G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$ olan lineer C kodunun kod sözcüklerini

listeleyelim.

$$C = \begin{cases} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & x_1 \\ 0 & 0 & 1 & 1 & 1 & x_2 \\ 1 & 1 & 0 & 0 & 0 & x_1 + x_2 \end{cases}$$

1.13 Örnek

F_3^4 'te üreteç matrisi $G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$ olan lineer C kodunun kod sözcüklerini listeleyelim.

$$C = \begin{cases} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & x_1 \\ 0 & 1 & 1 & 2 & x_2 \\ 2 & 0 & 2 & 2 & 2x_1 \\ 0 & 2 & 2 & 1 & 2x_2 \\ 1 & 1 & 2 & 0 & x_1 + x_2 \\ 2 & 2 & 1 & 0 & 2x_1 + 2x_2 \\ 1 & 2 & 0 & 2 & x_1 + 2x_2 \\ 2 & 1 & 0 & 1 & 2x_1 + x_2 \end{cases}$$

1.14 Tanım

A ve B matrisleri için $A \times B = [a_{ij}B]$ şeklinde tanımlanan çarpıma Kronecker çarpımı denir.

Burada, A matrisinde a_{ij} ler, $a_{ij}B$ ile yer değiştirir.

1.15 Örnek

$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ ve $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ matrislerini alalım.

$$I_2 \times H = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \text{ ve } H \times I_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \text{ olur.}$$

Şimdi $i = 1, 2, \dots, m$ için $H_m^i = I_{2^{m-i}} \times H \times I_{2^{i-1}}$ şeklindeki matrisleri düşünelim.

1.16 Örnek

$m = 2$ olsun. Buna göre;

$$H_2^1 = I_2 \times H \times I_1 = I_2 \times H$$

$$H_2^2 = I_1 \times H \times I_2 = H \times I_2 \text{ dir.}$$

1.17 Örnek

$m = 3$ olsun. Buna göre;

$$H_3^1 = I_4 \times H \times I_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

$$H_3^2 = I_2 \times H \times I_2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}$$

$$H_3^3 = H \times I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix} \text{ elde edilir.}$$



2. REED-MULLER KODLARI

2.1 Basit Tanım ve Kodlama

2.1.1 Tanım

R_m halkasında en çok r dereceli polinomların kümesine r . mertebeden Reed-Muller kodu denir ve $RM(r, m)$ ile gösterilir. Başka bir deyişle, ψ izomorfizmasını düşündüğümüzde, Reed-Muller kodu, $\mathbb{F}_2^{2^m}$ 'in bir alt uzayıdır.

0. mertebeden Reed-Muller kodu, $RM(0, m)$ 'dir ve aşağıdaki vektörlerden oluşur:

$$\left\{ \underbrace{00\dots 0}_{2^m}, \underbrace{11\dots 1}_{2^m} \right\}$$

Böylece $RM(0, m)$ kodu, 2^m uzunlukta sıfır ya da birlerden oluşan bir tekrarlı koddur.

m . mertebeden Reed-Muller kodu $RM(m, m)$ 'dir ve $RM(m, m) = R_m \cong \mathbb{F}_2^{2^m}$ dir.

2.1.2 Tanım

Bir $RM(r, m)$ Reed-Muller kodu için üreteç matris aşağıdaki gibi tanımlanır:

$$G_{RM(r,m)} = \begin{bmatrix} \Psi(1) \\ \Psi(x_0) \\ \Psi(x_1) \\ \vdots \\ \Psi(x_{m-1}) \\ \Psi(x_0x_1) \\ \Psi(x_0x_2) \\ \vdots \\ \Psi(x_{m-2}x_{m-1}) \\ \Psi(x_0x_1x_2) \\ \vdots \\ \Psi(x_{m-r}x_{m-r+1}\dots x_{m-1}) \end{bmatrix} \quad (2.1)$$

2.1.3 Örnek

$RM(1, 3)$ kodunun üreteç matrisi aşağıdaki gibidir:

$$G_{RM(1,3)} = \begin{bmatrix} \Psi(1) \\ \Psi(x_0) \\ \Psi(x_1) \\ \Psi(x_2) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

2.1.4 Örnek

RM(2, 3) kodunun üreteç matrisi aşağıdaki gibidir:

$$G_{RM(2,3)} = \begin{bmatrix} \Psi(1) \\ \Psi(x_0) \\ \Psi(x_1) \\ \Psi(x_2) \\ \Psi(x_0x_1) \\ \Psi(x_0x_2) \\ \Psi(x_1x_2) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

2.1.5 Örnek

RM(2, 4) kodunun üreteç matrisi aşağıdaki gibidir:

$$G_{RM(2,4)} = \begin{bmatrix} \Psi(1) \\ \Psi(x_0) \\ \Psi(x_1) \\ \Psi(x_2) \\ \Psi(x_3) \\ \Psi(x_0x_1) \\ \Psi(x_0x_2) \\ \Psi(x_0x_3) \\ \Psi(x_1x_2) \\ \Psi(x_1x_3) \\ \Psi(x_2x_3) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

2.1.6 Teorem

$G_{RM(r,m)}$ matrisi, $k = \sum_{i=0}^r \binom{m}{i}$ ve $n = 2^m$ olacak şekilde, $k \times n$ boyutludur. Böylece kodun boyutu da k olur.

İspat: Matrisin satırlarını, her satıra ait polinomun derecesine göre parçalayalım. Derecesi 0

olan satırlar $\binom{m}{0}$, derecesi 1 olanlar $(x_0, x_1, \dots, x_{m-1}) \binom{m}{1}$, derecesi 2 olanlar $\binom{m}{2}$, ..., derecesi r olanlar $\binom{m}{r}$ tanedir. Bu durumda toplamda;

$\binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{r} = \sum_{i=0}^r \binom{m}{i}$ tane satır vardır. Böylece kodun boyutu da k olur. ψ 'nin tanımından sütunların sayısının 2^m olduğu da kolayca görülebilir.

2.2 Tekrarlamalı Tanım

Bu bölümde ψ izomorfizması kullanılarak yapılan tanıma ek olarak Reed-Muller kodlarının yeni bir tanımını inceleyeceğiz. Ayrıca ψ kullanılmadan yeni bir üreteç matris tanımı yapacağız.

2.2.1 Tanım

Aşağıdaki özellikleri sağlayan $RM(r, m)$ kodu bir Reed-Muller koddur:

- (i) $RM(0, m) = \{\underbrace{00\dots 0}_{2^m}, \underbrace{11\dots 1}_{2^m}\}$
- (ii) $RM(m, m) = F_2^{2^m}$
- (iii) $RM(r, m) = \{(x, x+y) \mid x \in RM(r, m-1), y \in RM(r-1, m-1)\}, 0 < r < m$

Bu tanımdan $RM(m, m)$ kodunun, uzunluğu 2^m olan tüm kod sözcükleri olduğu görülebilir.

2.2.2 Örnek

$$RM(0, 0) = \{0, 1\}$$

$$RM(0, 1) = \{00, 11\}$$

$$RM(0, 2) = \{0000, 1111\}$$

$$RM(1, 1) = F_2^2 = \{00, 01, 10, 11\}$$

$$RM(2, 2) = F_2^{2^2}$$

$$\begin{aligned} RM(1, 2) &= \{(x, x+y) \mid x \in RM(1, 1), y \in RM(0, 1)\} \\ &= \{(x, x+y) \mid x \in \{00, 01, 10, 11\}, y \in \{00, 11\}\} \\ &= \{0000, 0011, 0101, 0110, 1010, 1001, 1111, 1100\} \end{aligned}$$

2.2.3 Tanım

Reed-Muller kodlarının tekrarlamalı tanımında, üreteç matris aşağıdaki şekilde tanımlanır:

$$G_{RM(r, m)} = \begin{bmatrix} G_{RM(r, m-1)} & G_{RM(r, m-1)} \\ 0 & G_{RM(r-1, m-1)} \end{bmatrix} \quad (2.2)$$

$r = 0$ için,

$$G_{RM(0, m)} = [\underbrace{11\dots 1}_{2^m}] \text{ ve} \quad (2.3)$$

$r = m$ için,

$$G_{RM(m, m)} = \begin{bmatrix} G_{RM(m-1, m)} \\ \underbrace{00\dots 01}_{2^{m-1}} \end{bmatrix} \text{ şeklindedir.} \quad (2.4)$$

2.2.4 Örnek

$RM(0, 1)$ ve $RM(1, 1)$ kodlarının üreteç matrisleri:

$$G_{RM(0, 1)} = [1 \ 1] \text{ ve } G_{RM(1, 1)} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ şeklindedir.}$$

2.2.5 Örnek

$m = 2$ ve $r = 1, 2$ için, (2.2) ve (2.4) eşitliklerinden;

$$G_{RM(1, 2)} = \begin{bmatrix} G_{RM(1, 1)} & G_{RM(1, 1)} \\ 0 & G_{RM(0, 1)} \end{bmatrix} \text{ ve } G_{RM(2, 2)} = \begin{bmatrix} G_{RM(1, 2)} \\ 0001 \end{bmatrix} \text{ dir.}$$

Örnek (2.2.4)'ten yararlanarak;

$$G_{RM(1, 2)} = \begin{bmatrix} 1111 \\ 0101 \\ 0011 \end{bmatrix} \text{ ve } G_{RM(2, 2)} = \begin{bmatrix} 1111 \\ 0101 \\ 0011 \\ 0001 \end{bmatrix} \text{ bulunur.}$$

2.2.6 Örnek

$m = 3$ ve $r = 0, 1, 2$ için;

$$G_{RM(0, 3)} = [11111111]$$

$$G_{RM(1, 3)} = \begin{bmatrix} G_{RM(1, 2)} & G_{RM(1, 2)} \\ 0 & G_{RM(0, 2)} \end{bmatrix}$$

Örnek (2.2.5)'ten yararlanarak;

$$G_{RM(1,3)} = \begin{bmatrix} 11111111 \\ 01010101 \\ 00110011 \\ 00001111 \end{bmatrix} \text{ bulunur.}$$

$$G_{RM(2,3)} = \begin{bmatrix} G_{RM(2,2)} & G_{RM(2,2)} \\ 0 & G_{RM(1,2)} \end{bmatrix}$$

Örnek (2.2.5)'ten yararlanarak;

$$\begin{aligned} G_{RM(2,3)} &= \begin{bmatrix} G_{RM(2,2)} & G_{RM(2,2)} \\ 0 & G_{RM(1,2)} \end{bmatrix} \\ &= \begin{bmatrix} G_{RM(1,2)} & & G_{RM(1,2)} & & & & & \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & G_{RM(1,1)} & G_{RM(1,1)} & & \\ 0 & 0 & 0 & 0 & 0 & 0 & G_{RM(0,1)} & \end{bmatrix} \\ &= \begin{bmatrix} G_{RM(1,1)} & G_{RM(1,1)} & G_{RM(1,1)} & G_{RM(1,1)} & & & & \\ 0 & 0 & G_{RM(0,1)} & 0 & 0 & G_{RM(0,1)} & & \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & G_{RM(1,1)} & G_{RM(1,1)} & & \\ 0 & 0 & 0 & 0 & 0 & 0 & G_{RM(0,1)} & \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \text{ elde edilir.} \end{aligned}$$

2.2.7 Teorem

r. mertebeden Reed-Muller kodu $RM(r, m)$ için aşağıdaki özellikler sağlanır:

- (i) Uzunluk $n = 2^m$ dir.
- (ii) $RM(r-1, m) \subseteq RM(r, m)$, $r > 0$ dir.
- (iii) Uzaklığı $d = 2^{m-r}$ dir.

(iv) Boyut $k = \sum_{i=0}^r \binom{m}{i}$ dır.

(v) Dual kod $RM(m-1-r, m)$, $r < m$ dir.

İspat: $r = 0$ ve $r = m$ için yukarıdaki özelliklerin sağlandığı açıktır. r 'nin diğer değerleri için bu özellikleri sağladığını gösterelim.

(i) Tanımdan bir $RM(r, m)$ kodunun uzunluğunun $n = 2^m$ olduğu görülebilir.

(ii) Şimdi $RM(r-1, m) \subseteq RM(r, m)$ 'in sağlandığını gösterelim. (2.2) eşitliğinden;

$$G_{RM(1, m)} = \begin{bmatrix} G_{RM(1, m-1)} & G_{RM(1, m-1)} \\ 0 & G_{RM(0, m-1)} \end{bmatrix} \text{ dir.}$$

$G_{RM(1, m-1)}$ matrisinin ilk satırı 1'lerden oluşan vektör olduğundan, $(G_{RM(1, m-1)}, G_{RM(1, m-1)})$ matrisinin ilk satırı da tekrarlı 1 vektördür ([11...1]). Böylece $RM(0, m) = \{0, 1\}$ kodu $RM(1, m)$ kodunun içerisinde.

$G_{RM(r-1, m-1)}$ matrisi $G_{RM(r, m-1)}$ matrisinin altmatrisi olduğundan, $G_{RM(r-2, m-1)}$ matrisi de $G_{RM(r-1, m-1)}$ matrisinin altmatrisi olur.

Bu durumda açıkça $G_{RM(r-1, m)} = \begin{bmatrix} G_{RM(r-1, m-1)} & G_{RM(r-1, m-1)} \\ 0 & G_{RM(r-2, m-1)} \end{bmatrix}$ matrisi $G_{RM(r, m)}$ 'in altmatrisidir ve

böylece $RM(r-1, m)$ kodu $RM(r, m)$ 'in bir altkodu olur.

(iii) İspatı van Lint, (1982) tarafından gösterilmiştir.

(iv) $G_{RM(r, m)}$ 'in tanımından;

$\text{boy}RM(r, m) = \text{boy}RM(r, m-1) + \text{boy}RM(r-1, m-1)$ olduğu açıktır. Teorem (2.1.6)'dan,

$$\begin{aligned} \text{boy}RM(r, m) &= \sum_{i=0}^r \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i} \\ &= \sum_{i=1}^r \left(\binom{m-1}{i} + \binom{m-1}{i-1} \right) + \binom{m-1}{0} \end{aligned}$$

$$\binom{m}{i} = \binom{m-1}{i} + \binom{m-1}{i-1} \text{ ve } \binom{m-1}{0} = 1 = \binom{m}{0} \text{ olduğundan,}$$

$$\text{boy}RM(r, m) = \sum_{i=0}^r \binom{m}{i} \text{ bulunur.}$$

(v) $RM(r, m) = \{(x, x+y) \mid x \in RM(r, m-1), y \in RM(r-1, m-1)\}$ ve

$RM(m-r-1, m) = \{(x', x' + y') \mid x' \in RM(m-r-1, m-1), y' \in RM(m-r-2, m-1)\}$ olsun.

Hipotezden, $RM(r, m-1)$ 'in duali $RM(m-r-2, m-1)$ ve $RM(r-1, m-1)$ 'in duali $RM(m-r-1, m-1)$ dir. Böylece $x \cdot y' = 0$ ve $x' \cdot y = 0$ dır.

Ayrıca $RM(r-1, m-1) \subseteq RM(r, m-1)$ olduğundan $y \cdot y' = 0$ dır.

$$\begin{aligned} \text{Böylece } (x, x+y) \cdot (x', x'+y') &= (x+y) \cdot (x'+y') + x \cdot x' \\ &= 2(x \cdot x') + x \cdot y' + y \cdot x' + y \cdot y' \\ &= 0 \text{ olur.} \end{aligned}$$

$RM(r, m)$ 'deki her vektörün $RM(m-r-1, m)$ 'deki her vektöre dik olduğunu da görebiliriz.

$$\begin{aligned} \text{boy}RM(r, m) + \text{boy}RM(m-r-1, m) &= \sum_{i=0}^r \binom{m}{i} + \sum_{i=0}^{m-r-1} \binom{m}{i} \\ &= \sum_{i=0}^r \binom{m}{m-i} + \sum_{j=0}^{m-r-1} \binom{m}{j} \\ &= \sum_{j=0}^m \binom{m}{j} = 2^m \text{ olduğundan,} \end{aligned}$$

$RM(m-r-1, m)$ kodu $RM(r, m)$ kodunun dualidir.

2.3 Alternatif Tanım

Bu bölümde, (2.1) tanımındaki ψ izomorfizmasını kullanarak farklı bir yöntemle Reed-Muller kodlarını oluşturacağız. R_m halkasını ve $\mathbb{F}_2^m$ vektör uzayını düşünelim. $\mathbb{F}_2^m$ 'deki vektörler standart bir sıralamaya sahiptirler.

Tanım (1.2)'deki p elemanlarının kümesi S olsun. p 'nin indirgenmiş formu $p' = x_{i_1} x_{i_2} \dots x_{i_r}$ ($i_j \in \mathbb{Z}_m, i_j = i_k \rightarrow j = k, 0 \leq r \leq m$) şeklindedir.

$P(X)$, X 'in kuvvet kümesi olmak üzere α fonksiyonu aşağıdaki gibi tanımlansın:

$$\alpha : S \rightarrow P(\mathbb{Z}_m)$$

$$p \equiv p' = x_{i_1} x_{i_2} \dots x_{i_r} \mapsto \begin{cases} \phi & : r = 0 \text{ ise} \\ \{i_1, i_2, \dots, i_r\} & : r \neq 0 \text{ ise} \end{cases} \quad (2.5)$$

Şimdi de $T \in P(\mathbb{Z}_m)$ için aşağıdaki fonksiyonu tanımlayalım:

$$f_T : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$$

$$(x_0, x_1, \dots, x_{m-1}) \mapsto \begin{cases} \prod_{i \in T} (x_i + 1) & : T \neq \phi \text{ ise} \\ 1 & : T = \phi \text{ ise} \end{cases} \quad (2.6)$$

2.3.1 Örnek

$f_{\{0,2\}}(1001)$ ve $f_{\{0,2\}}(0101)$ 'i hesaplayalım.

Öncelikle (2.6)'daki f_T tanımından, $f_{\{0,2\}}(x_0, x_1, x_2, x_3) = (x_0 + 1).(x_2 + 1)$ elde edilir.

Buna göre, $f_{\{0,2\}}(1001) = (1 + 1).(0 + 1) = 0 . 1 = 0$ ve

$f_{\{0,2\}}(0101) = (0 + 1).(0 + 1) = 1 . 1 = 1$ bulunur.

$n_b, \mathbb{F}_2^m$ 'deki vektörlerin ikili sistemde gösterimi olmak üzere β fonksiyonu aşağıdaki gibi tanımlansın:

$$\beta : S \rightarrow \mathbb{F}_2^{2^m}$$

$$x \mapsto (f_{\alpha(x)}(0_b), f_{\alpha(x)}(1_b), f_{\alpha(x)}(2_b), \dots, f_{\alpha(x)}((2^m - 1)_b)) \quad (2.7)$$

$q \in R_m$ polinomu, $m_i \in S, m_i = m_j \rightarrow i = j, 0 \leq r \leq 2^m$ olmak üzere $q = m_1 + m_2 + \dots + m_r$ şeklinde olsun. ψ fonksiyonu aşağıdaki gibi tanımlanır:

$$\begin{aligned} \psi : R_m &\rightarrow \mathbb{F}_2^{2^m} \\ x = m_1 + m_2 + \dots + m_r &\mapsto \begin{cases} \beta(0) & : x = 0 \\ \beta(m_1) + \beta(m_2) + \dots + \beta(m_r) & : x \in R_m / \{0\} \end{cases} \end{aligned} \quad (2.8)$$

ψ 'nin bu tanımı, bölüm (2.1)'de incelenmiş olan ψ tanımından daha nettir. Şimdi bir örnekle bu tanımı inceleyelim.

2.3.2 Örnek

$G_{RM(2, 3)}$ 'ü ψ 'yi kullanarak oluşturalım. $\{1, x_0, x_1, x_2, x_0x_1, x_0x_2, x_1x_2\}$ kümesi $G_{RM(2, 3)}$ 'ün satırlarına karşılık gelir. $\mathbb{F}_2^3$ 'teki standart sıralama aşağıdaki gibidir:

(000, 001, 010, 011, 100, 101, 110, 111).

Buna göre;

$$\psi(1) = \beta(1) = (f_\phi(000), f_\phi(001), \dots, f_\phi(111)) = 11111111$$

$$\psi(x_0) = \beta(x_0) = (f_{\{0\}}(000), f_{\{0\}}(001), \dots, f_{\{0\}}(111)) = 11110000$$

$$\psi(x_1) = \beta(x_1) = (f_{\{1\}}(000), f_{\{1\}}(001), \dots, f_{\{1\}}(111)) = 11001100$$

$$\psi(x_2) = \beta(x_2) = (f_{\{2\}}(000), f_{\{2\}}(001), \dots, f_{\{2\}}(111)) = 10101010$$

$$\psi(x_0x_1) = \beta(x_0x_1) = (f_{\{0,1\}}(000), f_{\{0,1\}}(001), \dots, f_{\{0,1\}}(111)) = 11000000$$

$$\psi(x_0x_2) = \beta(x_0x_2) = (f_{\{0,2\}}(000), f_{\{0,2\}}(001), \dots, f_{\{0,2\}}(111)) = 10100000$$

$$\psi(x_1x_2) = \beta(x_1x_2) = (f_{\{1,2\}}(000), f_{\{1,2\}}(001), \dots, f_{\{1,2\}}(111)) = 10001000$$

Görüldüğü gibi $G_{RM(2,3)}$ matrisinin satırları (2.1.4) örneğindeki ile aynıdır.

2.4 Kodlama

Üreteç matris ile kodlama oldukça kolaydır. Verilen bir $m \in \mathbb{F}_2^k$ mesajı ile $m * G_{RM(r,m)}$ çarpımı uygulanarak kodlama yapılabilir.

2.4.1 Örnek

$m = 01101001010$ mesajını $RM(2,4)$ kodunu kullanarak kodlamak isteyelim:

$$c = m * G_{RM(2,4)} = [01101001010] \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$c = 101011111111010$ elde edilir.

3. KOD ÇÖZME

Reed-Muller kodlarının çözümü için çeşitli yöntemler geliştirilmiştir. Bu yöntemlere geçmeden önce, Reed-Muller kodlarını çözebilmek için gerekli, bazı temel özelliklerden bahsetmek gereklidir.

Verilen bir $RM(r, m)$ kodu için, iki kod sözcüğü arasındaki uzaklığın 2^{m-r} olduğunu biliyoruz. Bir kod sözcüğündeki e tane hatayı çözebilmek için, kod sözcükleri arasındaki uzaklığın $2e$ 'den büyük olması gerekmektedir. Böylece Reed-Muller kodlarında, uzaklık 2^{m-r} olduğundan, $\max(0, 2^{m-r-1}-1)$ hata düzeltilebilir.

3.1 Majority Logic ile Kod Çözme

Bu kod çözme tekniği ile ilgili iki farklı yöntem verilmiştir.

3.1.1 Tanım

Tanım (1.2)'deki gibi tanımlanan $p \in R_m$ elemanının indirgenmiş formu p' olsun. $\mathcal{T}$ kümesi, p' 'de olmayan değişkenler ve onların tümleyenlerinden meydana gelen küme olsun. $\mathcal{T}$ 'deki değişkenlerden oluşan ve derecesi $m-d$ olan tüm vektörlere p 'nin karakteristik vektörleri denir. Ayrıca Tanım (1.4)'teki ψ fonksiyonu için, $\overline{x_i}$, x_i 'nin tümleyeni olmak üzere, $\psi(\overline{x_i} \overline{x_i}) = \psi(x_i) * \overline{\psi(x_i)} = 0$ dır.

3.1.2 Örnek

$RM(3, 4)$ kodu için, $x_0x_1x_3$ 'ün karakteristik vektörleri $\{x_2, \overline{x_2}\}$ dir. x_0x_2 'nin karakteristik vektörleri ise $\{x_1x_3, \overline{x_1x_3}, x_1\overline{x_3}, \overline{x_1}\overline{x_3}\}$ dir.

3.1.3 Yöntem I

Algoritma

Kod çözümüne başlarken ilk olarak, $RM(r, m)$ kod için, derecesi r olan satırlar belirlenir. Her satır için 2^{m-r} tane karakteristik vektör yazılır. Daha sonra her bir karakteristik vektörün ψ 'deki görüntüsü ile alınan mesaj vektörüne nokta çarpım uygulanır. Eğer çarpım sonucu 1 ise, bu satırın sözcüğümüzün oluşumunda kullanılacağını düşünebiliriz ve alınan mesaj vektöründe bu satıra karşılık gelen bileşeni 1 yaparız. Eğer çarpım sonucu 0 ise, bu satırın sözcüğün oluşumunda kullanılmayacağını düşünerek, alınan mesaj vektöründe bu satıra karşılık gelen bileşeni 0 yaparız.

Bu tekniği derecesi r olan tüm satırlara uyguladıktan sonra, yeni meydana gelen $\begin{pmatrix} m \\ r \end{pmatrix}$ uzunluktaki vektör alınır ve $\begin{pmatrix} m \\ r \end{pmatrix}$ tane satırlı üreteç matris ile çarpılır. Böylece n uzunluğundaki s vektörü elde edilir. s ile alınan mesaj vektörü toplanır ve mesaj vektörü yerine elde edilen toplam alınarak işleme devam edilir. Daha sonra derecesi $r-1$ olan satırlara geçilerek işlem sürdürülür.

Şimdi bu algoritmayı bir örnekle açıklayalım:

3.1.4 Örnek

RM(2, 3) kodundaki $u = 00110110$ mesajını çözelim.

RM(2, 3) koduna ait üreteç matris:

$$G_{RM(2,3)} = \begin{bmatrix} \Psi(1) \\ \Psi(x_0) \\ \Psi(x_1) \\ \Psi(x_2) \\ \Psi(x_0x_1) \\ \Psi(x_0x_2) \\ \Psi(x_1x_2) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \text{ şeklindedir.}$$

İlk olarak derecesi $r = 2$ olan satırlarla başlayalım.

x_1x_2 satırının karakteristik vektörleri $x_0, \overline{x_0}$ dir.

$$\left. \begin{array}{l} u \cdot \Psi(x_0) = 0 \\ u \cdot \overline{\Psi(x_0)} = 0 \end{array} \right\} \rightarrow m = \dots\dots 0$$

x_0x_2 satırının karakteristik vektörleri $x_1, \overline{x_1}$ dir.

$$\left. \begin{array}{l} u \cdot \Psi(x_1) = 1 \\ u \cdot \overline{\Psi(x_1)} = 1 \end{array} \right\} \rightarrow m = \dots\dots 10$$

x_0x_1 satırının karakteristik vektörleri $x_2, \overline{x_2}$ dir.

$$\left. \begin{array}{l} u \cdot \Psi(x_2) = 0 \\ u \cdot \overline{\Psi(x_2)} = 0 \end{array} \right\} \rightarrow m = \dots 010$$

Derecesi $r = 2$ olan terimler tamamlandığından s 'i hesaplayabiliriz:

$$s = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$s + u = 10010110$ şeklindedir. u yerine 10010110 alarak işleme devam edebiliriz.

Şimdi aynı işlemleri $r - 1 = 2 - 1 = 1$ dereceli terimler için tekrarlamalıyız.

x_2 satırının karakteristik vektörleri $x_0x_1, \overline{x_0x_1}, \overline{x_0x_1}, \overline{x_0x_1}$ dir.

$$\begin{aligned} u.(\psi(x_0) * \psi(x_1)) &= u.(11110000 * 11001100) \\ &= 10010110 . 11000000 \\ &= 1 \end{aligned}$$

$$\begin{aligned} u.(\overline{\psi(x_0)} * \psi(x_1)) &= u.(00001111 * 11001100) \\ &= 10010110 . 00001100 \\ &= 1 \end{aligned}$$

$$\begin{aligned} u.(\psi(x_0) * \overline{\psi(x_1)}) &= u.(11110000 * 00110011) \\ &= 10010110 . 00110000 \\ &= 1 \end{aligned}$$

$$\begin{aligned} u.(\overline{\psi(x_0)} * \overline{\psi(x_1)}) &= u.(00001111 * 00110011) \\ &= 10010110 . 00000011 \\ &= 1 \end{aligned}$$

Buradan $m = \dots 1010$ olur.

x_1 satırının karakteristik vektörleri $x_0x_2, \overline{x_0x_2}, \overline{x_0x_2}, \overline{x_0x_2}$ dir.

$$\begin{aligned} u.(\psi(x_0) * \psi(x_2)) &= u.(11110000 * 10101010) \\ &= 10010110 . 10100000 \\ &= 1 \end{aligned}$$

$$\begin{aligned} u.(\overline{\psi(x_0)} * \psi(x_2)) &= u.(00001111 * 10101010) \\ &= 10010110 . 00001010 \\ &= 1 \end{aligned}$$

$$\begin{aligned}
u.(\overline{\psi(x_0)} * \overline{\psi(x_2)}) &= u.(11110000 * 01010101) \\
&= 10010110 . 01010000 \\
&= 1
\end{aligned}$$

$$\begin{aligned}
u.(\overline{\psi(x_0)} * \overline{\psi(x_2)}) &= u.(00001111 * 01010101) \\
&= 10010110 . 00000101 \\
&= 1
\end{aligned}$$

Buradan $m = \cdot\cdot 11010$ olur.

x_0 satırının karakteristik vektörleri $x_1x_2, \overline{x_1x_2}, \overline{x_1x_2}, \overline{x_1x_2}$ dir.

$$\begin{aligned}
u.(\overline{\psi(x_1)} * \overline{\psi(x_2)}) &= u.(11001100 * 10101010) \\
&= 10010110 . 10001000 \\
&= 1
\end{aligned}$$

$$\begin{aligned}
u.(\overline{\psi(x_1)} * \overline{\psi(x_2)}) &= u.(00110011 * 10101010) \\
&= 10010110 . 00100010 \\
&= 1
\end{aligned}$$

$$\begin{aligned}
u.(\overline{\psi(x_1)} * \overline{\psi(x_2)}) &= u.(11001100 * 01010101) \\
&= 10010110 . 01000100 \\
&= 1
\end{aligned}$$

$$\begin{aligned}
u.(\overline{\psi(x_1)} * \overline{\psi(x_2)}) &= u.(00110011 * 01010101) \\
&= 10010110 . 00010001 \\
&= 1
\end{aligned}$$

Buradan $m = \cdot 111010$ olur.

Derecesi $r = 1$ olan terimler tamamlandığından s 'i hesaplayabiliriz:

$$s = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

$s + u = 10010110 + 10010110 = 00000000$ şeklindedir.

$$u . 1 = 00000000 . 11111111 = 0$$

Buradan $m = 0111010$ olur.

Böylece orijinal mesaj $v = 0111010$ olarak bulunur.

Kontrol etmek istersek;

$$v \cdot G_{RM(2,3)} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$= 00110110$$

Buradan $v \cdot G_{RM(2,3)} = u$ olduğunu görürüz. Bu da bize u vektörünün hata içermediğini gösterir.

3.1.5 Yöntem II

Algoritma

1. **Adım:** $G_{RM(r,m)}$ üreteç matrisinde, en alt satırdan başlamak üzere, her bir satıra ait karakteristik vektörler yazılır. Kodlanmış mesaj vektörü ile karakteristik vektörlere nokta çarpım uygulanır.
2. **Adım:** Nokta çarpım sonuçlarından en büyük değer alınarak o satıra ait katsayı belirlenir.
3. **Adım:** 1. ve 2. adım en üst satır hariç bütün satırlara uygulandıktan sonra, belirlenen katsayılar ile o satırlara karşılık gelen üreteç matrisin satırları çarpılır ve çarpımlar toplanarak M vektörü elde edilir. Bulunan M vektörü ile mesaj vektörü toplanır. Bu toplamda 1'lerin sayısı fazla ise üst satıra ait katsayı 1, 0'ların sayısı fazla ise üst satıra ait katsayı 0 olarak belirlenir. Böylece tüm katsayılar sırasıyla yazılarak alınan mesaj vektörü bulunmuş olur. Üreteç matrisle çarpılarak orijinal mesaj elde edilir.

3.1.6 Örnek

$RM(1,3)$ kodu için $m = 10011000$ mesajı alınmış olsun.

$2^{m-r-1} - 1 = 2^{3-1-1} - 1 = 1$ hata düzeltilebilir.

$$G_{RM(1,3)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

x_2 satırının karakteristik vektörleri $x_0x_1, \overline{x_0x_1}, \overline{x_0x_1}, \overline{x_0x_1}$ dir.

$$x_0x_1 = (11000000)$$

$$\overline{x_0 x_1} = (00001100)$$

$$x_0 \overline{x_1} = (00110000)$$

$$\overline{x_0} \overline{x_1} = (00000011)$$

$$(10011000).(11000000) = 1$$

$$(10011000).(00001100) = 1$$

$$(10011000).(00110000) = 1$$

$$(10011000).(00000011) = 0$$

x_2 için 1 bulunur.

x_1 satırının karakteristik vektörleri $x_0 x_2, \overline{x_0} x_2, x_0 \overline{x_2}, \overline{x_0} \overline{x_2}$ dir.

$$x_0 x_2 = (10100000)$$

$$\overline{x_0} x_2 = (00001010)$$

$$x_0 \overline{x_2} = (01010000)$$

$$\overline{x_0} \overline{x_2} = (00000101)$$

$$(10011000).(10100000) = 1$$

$$(10011000).(00001010) = 1$$

$$(10011000).(01010000) = 1$$

$$(10011000).(00000101) = 0$$

x_1 için 1 bulunur.

x_0 satırının karakteristik vektörleri $x_1 x_2, \overline{x_1} x_2, x_1 \overline{x_2}, \overline{x_1} \overline{x_2}$ dir.

$$x_1 x_2 = (10001000)$$

$$\overline{x_1} x_2 = (00100010)$$

$$x_1 \overline{x_2} = (01000100)$$

$$\overline{x_1} \overline{x_2} = (00010001)$$

$$(10011000).(10001000) = 0$$

$$(10011000).(00100010) = 0$$

$$(10011000).(01000100) = 0$$

$$(10011000).(00010001) = 1$$

x_0 için 0 bulunur.

Şimdi bulunan değerleri üreteç matriste ait oldukları satırlarla çarpıp toplayalım.

$$1*(10101010) + 1*(11001100) + 0*(11110000) = (01100110) = M$$

$$M + m = (01100110) + (10011000) = 11111110$$

1'lerin sayısı 0'lardan fazla olduğundan ilk satıra ait bileşen 1 olur.

Alınan mesaj (1011) olarak bulunur.

$(1011) * G_{RM(1,3)} = 10011001$ elde edilir. Hata son bileşendedir.

3.2 RM(1, m) için Kod Çözme

Bu bölümde, RM(1,m) şeklindeki Reed-Muller kodlarının çözümü için, iki farklı yöntem verilmiştir.

3.2.1 Yöntem I

Algoritma

w mesajının alındığını ve RM(1, m) kodu için üreteç matrisin $G_{RM(1, m)}$ olduğunu varsayalım.

H matrisi (1.15) örneğindeki gibi olmak üzere, w mesaj vektörünü çözebilmek için;

1. w'da 0 yerine -1 yazılarak w' elde edilir.
2. $w_1 = w' H_m^1$ ve $i = 2, 3, \dots, m$ için $w_i = w_{i-1} H_m^i$ hesaplanır.
3. w_m 'de en büyük değere sahip j. konumdaki bileşen bulunur.

$v(j)$, düşük mertebe başa yazılmak üzere j'nin ikilik sistemde yazılışı olsun. Eğer w_m 'in j. bileşeni pozitif ise mesaj (1, $v(j)$) şeklindedir. Eğer negatif ise, mesaj (0, $v(j)$) şeklinde olur. (2.2) eşitliğinden yararlanarak kodlama yapılırsa, hatalı bileşen görülebilir.

3.2.2 Örnek

$$m = 3 \text{ ve } RM(1, 3) \text{ kodunun üreteç matrisi } G_{RM(1,3)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \text{ olsun.}$$

$w = 10101011$ mesajı alınsın.

$w' = (1, -1, 1, -1, 1, -1, 1, 1)$ dir.

Şimdi w_1 ve w_i leri hesaplayalım. Örnek (1.17)'den yararlanarak,

$$w_1 = w'H_3^1 = \begin{bmatrix} 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

$$= (0, 2, 0, 2, 0, 2, 2, 0)$$

$$w_2 = w_1 H_3^2 = \begin{bmatrix} 0 & 2 & 0 & 2 & 0 & 2 & 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}$$

$$= (0, 4, 0, 0, 2, 2, -2, 2)$$

$$w_3 = w_2 H_3^3 = \begin{bmatrix} 0 & 4 & 0 & 0 & 2 & 2 & -2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

$$= (2, 6, -2, 2, -2, 2, 2, -2) \text{ elde edilir.}$$

w_3 'ün en büyük değerli bileşeni $j = 1$. konumdaki 6'dır. $v(1) = 100$ ve $6 > 0$ olduğundan mesaj $m = (1100)$ bulunur. Kodlamak istersek;

$$u = \begin{bmatrix} 1 & 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} = 10101010 \text{ elde edilir. Hatanın son bileşende}$$

olduğu görülmektedir.

3.2.3 Örnek

$w = (10001111)$ mesajı alınmış olsun. $G_{RM(1,3)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$ şeklinde alınmış

olsun.

$w' = (1, -1, -1, -1, 1, 1, 1, 1)$ dir.

Örnek (1.17)'den yararlanarak;

$$w_1 = w' H_3^1 = (0, 2, -2, 0, 2, 0, 2, 0)$$

$$w_2 = w_1 H_3^2 = (-2, 2, 2, 2, 4, 0, 0, 0)$$

$$w_3 = w_2 H_3^3 = (2, 2, 2, 2, -6, 2, 2, 2) \text{ elde edilir.}$$

w_3 'ün en büyük değerli bileşeni $j = 4$. konumdaki -6 'dır. $v(4) = 001$ ve $-6 < 0$ olduğundan mesaj $m = (0001)$ bulunur.

$$u = [0 \ 0 \ 0 \ 1] \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} = 00001111 \text{ elde edilir. Hatanın ilk bileşende}$$

olduğu görülmektedir.

3.2.4 Örnek

RM(1,4) kodu için $w = 1011011001101001$ mesajı alınsın.

$$w' = (1, -1, 1, 1, -1, 1, 1, -1, -1, 1, 1, -1, 1, -1, -1, 1)$$

Şimdi Tanım (1.14) ve Örnek (1.15)'ten yararlanarak, H_4^1, H_4^2, H_4^3 ve H_4^4 matrislerini hesaplayalım:

$$H_4^3 = I_2 \times H \times I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

[illegible]

Bu matrislerden yararlanarak w_i 'leri hesaplayalım:

$$w_1 = w'H_4^1 = (0, 2, 2, 0, 0, -2, 0, 2, 0, -2, 0, 2, 0, 2, 0, -2)$$

$$\mathbf{w}_2 = \mathbf{w}_1 H_4^2 = (2, 2, -2, 2, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 4)$$

$$\mathbf{w}_3 = \mathbf{w}_2 H_4^3 = (2, 2, -2, -2, 2, 2, -2, 6, 0, 0, 0, 0, 0, 0, 0, -8)$$

$$w_4 = w_3 H_4^4 = (2, 2, -2, -2, 2, 2, -2, -2, 2, 2, -2, -2, 2, 2, -2, 14)$$

w_4 'te en büyük değerli bileşen $j = 15$. konumdaki 14'tür. $v(15) = 1111$ ve $14 > 0$ olduğundan $m = 11111$ olarak bulunur. Bu vektörü $G_{RM(1,4)}$ ile çarpalım:

$$[1 \ 1 \ 1 \ 1 \ 1] \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} = (1001011001101001)$$

Böylece kodlanmış mesaj 1001011001101001 dir. Hatanın 3. bileşende olduğu görülür.

3.2.5 Yöntem II

$G_{RM(1,m)}$ matrisinin satırları $v_1, v_2, \dots, v_{m+1}$ olsun. Buna göre herhangi bir v kod sözcüğü;

$v = a_1 v_1 + a_2 v_2 + \dots + a_{m+1} v_{m+1}$ şeklinde yazılabilir.

$v = x_1 x_2 \dots x_{2^m}$ mesajı alınmış olsun. m tane denklem sistemi yazılarak kod çözümü kod çözümü yapılır. Örneğin $m = 3$ olsun.

$$i = 1 \text{ için } 2^{m-i} = 2^{3-1} = 4$$

Buna göre her bileşene 4 ekleyerek ilk satır yazılır.

$$a_2 = x_1 + x_5 = x_2 + x_6 = x_3 + x_7 = x_4 + x_8$$

$$i = 2 \text{ için } 2^{m-i} = 2^{3-2} = 2$$

$$a_3 = x_1 + x_3 = x_2 + x_4 = x_5 + x_7 = x_6 + x_8$$

$$i = 3 \text{ için } 2^{m-i} = 2^{3-3} = 1$$

$$a_4 = x_1 + x_2 = x_3 + x_4 = x_5 + x_6 = x_7 + x_8$$

Burada dikkat edilmesi gereken kısım, her satırda her bileşenden bir tane olmasıdır.

a_2, a_3, a_4 hesaplandıktan sonra $a_2 v_2 + a_3 v_3 + a_4 v_4$ bulunur. Buradan çıkan vektör incelenerek ilk satıra ait a_1 değerinin 1 veya 0 dan hangisi olması gerektiğine karar verilir. a_1 vektörü de sonuca eklenerek orijinal mesaj elde edilir.

3.2.6 Örnek

RM(1,3) kodu için $v = 11011100$ mesajı alınsın.

$v = x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8$ diyelim.

$$i = 1 \text{ için } 2^{m-i} = 2^{3-1} = 4$$

$$a_2 : x_1 + x_5 = 0 \quad x_2 + x_6 = 0 \quad x_3 + x_7 = 0 \quad x_4 + x_8 = 1 \Rightarrow a_2 = 0$$

$$i = 2 \text{ için } 2^{m-i} = 2^{3-2} = 2$$

$$a_3 : x_1 + x_3 = 1 \quad x_2 + x_4 = 0 \quad x_5 + x_7 = 1 \quad x_6 + x_8 = 1 \Rightarrow a_3 = 1$$

$$i = 3 \text{ için } 2^{m-i} = 2^{3-3} = 1$$

$$a_4 : x_1 + x_2 = 0 \quad x_3 + x_4 = 1 \quad x_5 + x_6 = 0 \quad x_7 + x_8 = 0 \Rightarrow a_4 = 0$$

Şimdi $a_2v_2 + a_3v_3 + a_4v_4$ ü hesaplayalım:

$$0*(11110000) + 1*(11001100) + 0*(10101010) = 11001100$$

$a_1 = 1$ alırsak üreteç matrisin ilk satırı da birlerden oluşan vektör olduğundan

$$v = (11111111)*(11111111) + 11001100 = 00110011 \text{ bulunur.}$$

$a_1 = 0$ alırsak $(00000000)*(11111111) + 11001100 = 11001100$ bulunur. Buna göre $a_1 = 0$ alınmalıdır. Orijinal kod sözcüğümüz ise 11001100 olarak bulunmuş olur.

3.2.7 Örnek

RM(1,3) kodu için $m = 11000001$ mesajı alınsın.

$m = x_1x_2x_3x_4x_5x_6x_7x_8$ olsun.

$$i = 1 \text{ için } 2^{m-i} = 2^{3-1} = 4$$

$$a_2 : x_1 + x_5 = 1 \quad x_2 + x_6 = 1 \quad x_3 + x_7 = 0 \quad x_4 + x_8 = 1 \Rightarrow a_2 = 1$$

$$i = 2 \text{ için } 2^{m-i} = 2^{3-2} = 2$$

$$a_3 : x_1 + x_3 = 1 \quad x_2 + x_4 = 1 \quad x_5 + x_7 = 0 \quad x_6 + x_8 = 1 \Rightarrow a_3 = 1$$

$$i = 3 \text{ için } 2^{m-i} = 2^{3-3} = 1$$

$$a_4 : x_1 + x_2 = 0 \quad x_3 + x_4 = 0 \quad x_5 + x_6 = 0 \quad x_7 + x_8 = 1 \Rightarrow a_4 = 0$$

$$\begin{aligned} a_2v_2 + a_3v_3 + a_4v_4 &= 1*(11110000) + 1*(11001100) + 0*(10101010) \\ &= 00111100 \end{aligned}$$

$a_1 = 1$ alalım.

$$11111111 + 00111100 = 11000011 \text{ olur.}$$

Buna göre mesaj vektöründe hatanın sondan ikinci bileşende olduğu görülür. Mesaj 11000011 şeklindedir.

4. REED-MULLER KODLARININ UYGULAMALARI

Bu bölümde Reed-Muller kodlarının, MATLAB programı üzerinde çeşitli uygulamaları incelenmiştir.

4.1 Üreteç Matrisin Hesaplanması

Aşağıda $r = 1, 2$ ve $m = 2, 3, 4$ için üreteç matrisi bulan MATLAB programı yer almaktadır.

```
function GRM = uretec(r,m)
if m == 2
    if r == 1
        GRM = [1 1 1 1; 1 1 0 0; 1 0 1 0]
    end
    if r == 2
        GRM = [1 1 1 1; 1 1 0 0; 1 0 1 0; 1 0 0 0]
    end
    if r ~= 1 & r ~= 2
        display('r=1 veya r=2 olmalıdır')
    end
end
if m == 3
    G = [ones(1,8); 1 1 1 1 0 0 0 0; 1 1 0 0 1 1 0 0; 1 0 1 0 1 0 1 0];
    if r == 1
        GRM = G
    end
    if r == 2
        B = [G(2,:).*G(3,:); G(2,:).*G(4,:); G(3,:).*G(4,:)];
        GRM = [G; B]
    end
    if r ~= 1 & r ~= 2
        display('r=1 veya r=2 olmalıdır')
    end
end
if m == 4
    G = [ones(1,16); ones(1,8),zeros(1,8); ones(1,4),zeros(1,4),ones(1,4),zeros(1,4);
```

```

1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0; 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0];
if r == 1
    GRM = G
end
if r == 2
    B = [G(2,:).*G(3,:); G(2,:).*G(4,:); G(2,:).*G(5,:); G(3,:).*G(4,:);
        G(3,:).*G(5,:); G(4,:).*G(5,:);];
    GRM = [G; B]
end
if r ~= 1 & r ~= 2
    display('r=1 veya r=2 olmalıdır')
end
end
end

```

4.1.1 Örnek

MATLAB komut penceresine uretec(2,3) komutu yazılarak enter'a basıldığında aşağıdaki ekran görülecektir:

```
>> uretec(2,3)
```

```
GRM =
```

```

1  1  1  1  1  1  1  1
1  1  1  1  0  0  0  0
1  1  0  0  1  1  0  0
1  0  1  0  1  0  1  0
1  1  0  0  0  0  0  0
1  0  1  0  0  0  0  0
1  0  0  0  1  0  0  0

```

Burada RM(2, 4) kodu için üreteç matris GRM ile isimlendirilmiştir.

4.1.2 Örnek

RM(2,4) kodu için üreteç matrisi hesaplamak isteyelim. Komut satırına uretec(2,4) yazdığımızda aşağıdaki çıkış alınır:

```
>> uretec(2,4)
```

GRM =

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0
1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0
1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0

4.2 Kodlama

Aşağıda $r = 1, 2$ ve $m = 2, 3, 4$ için bulunan üreteç matristen yararlanılarak, verilen bir mesaj vektörünü kodlamaya yarayan program verilmiştir. Programa giriş verileri olarak, m mesaj vektörü ve kullanılacak üreteç matris için, `uretec(r, m)` komutu girilmelidir. İstenilirse üreteç matris programı kullanılmadan üreteç matrisin kendisi de girilebilir.

```
function kodlama(m,GRM)
```

```
B = m * GRM;
```

```
A = size(B);
```

```
C = A(:,2);
```

```
u = mod(B(:,1:C),2)
```

4.2.1 Örnek

Örnek (2.4.1)'deki kodlama işlemini, programımızı kullanarak yapalım. $m = 01101001010$ mesaj vektörünü $G_{RM(2,4)}$ yardımıyla kodlayacağız. Bunun için mesajımızı vektörel gösterimde, üreteç matrisi ise üreteç matris bulma programı yardımıyla gireceğiz.

>> `kodlama([0 1 1 0 1 0 0 1 0 1 0],uretec(2,4))` komutu girildiğine ekran görüntüsü:

GRM =

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0

```

1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0
1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0
1 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0
1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0
1 1 0 0 0 0 0 0 1 1 0 0 0 0 0 0
1 0 1 0 0 0 0 0 1 0 1 0 0 0 0 0
1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0

```

u =

```

1 0 1 0 1 1 1 1 1 1 1 1 0 1 0

```

şeklinde olur.

4.2.2 Örnek

m = 1001001 mesajını RM(2,3) kodu için kodlamak isteleyim. MATLAB komut satırına kodlama([1 0 0 1 0 0 1],uretec(2,3)) komutu girilmelidir.

```
>> kodlama([1 0 0 1 0 0 1],uretec(2,3))
```

GRM =

```

1 1 1 1 1 1 1 1
1 1 1 1 0 0 0 0
1 1 0 0 1 1 0 0
1 0 1 0 1 0 1 0
1 1 0 0 0 0 0 0
1 0 1 0 0 0 0 0
1 0 0 0 1 0 0 0

```

u =

```

1 1 0 1 1 1 0 1

```

Buna göre mesaj vektörü, u = 11011101 şeklinde kodlanmış olur.

4.3 Kod Çözme

Aşağıda RM(1,3) kodu için kod çözme uygulaması verilmiştir. Burada program verileri olarak, çözülmesi istenen u mesaj vektörü ile r ve m değerleri girilmelidir. Mesaj vektörü kodlanmamış ise öncelikle kodlama programı ile kodlanması, daha sonra kod çözme

programına veri olarak girilmesi gerekir. Ekran çıktısı olarak, önce GRM üreteç matrisini, sonrada orijinal kod sözcüğünü verir.

```
function kodcozum(u, r, m)
GRM = uretec(r,m);
if r ~= 1 | m ~= 3
    display('r=1 ve m=3 olmalıdır')
end
if r == 1 & m == 3
    C = GRM(2,:).*GRM(3,:);
    D = mod(GRM(2,:)+1,2).*GRM(3,:);
    E = GRM(2,:).*mod(GRM(3,:)+1,2);
    F = mod(GRM(2,:)+1,2).*mod(GRM(3,:)+1,2);
    S = u*C(:);  A = mod(S,2);
    S = u*D(:);  B = mod(S,2);
    S = u*E(:);  C = mod(S,2);
    S = u*F(:);  D = mod(S,2);
    x = A+B+C+D/4;
    if x == 0.25
        X2 = 0;
    else
        X2 = 1;
    end
end
C = GRM(2,:).*GRM(4,:);
D = mod(GRM(2,:)+1,2).*GRM(4,:);
E = GRM(2,:).*mod(GRM(4,:)+1,2);
F = mod(GRM(2,:)+1,2).*mod(GRM(4,:)+1,2);
S = u*C(:);  A = mod(S,2);
S = u*D(:);  B = mod(S,2);
S = u*E(:);  C = mod(S,2);
S = u*F(:);  D = mod(S,2);
x = A+B+C+D/4;
if x == 0.25
    X1 = 0;
else
```

```

    X1 = 1;
end
C = GRM(3,:).*GRM(4,:);
D = mod(GRM(3,:)+1,2).*GRM(4,:);
E = GRM(3,:).*mod(GRM(4,:)+1,2);
F = mod(GRM(3,:)+1,2).*mod(GRM(4,:)+1,2);
S = u*C(:);  A = mod(S,2);
S = u*D(:);  B = mod(S,2);
S = u*E(:);  C = mod(S,2);
S = u*F(:);  D = mod(S,2);
x = A+B+C+D/4;
if x == 0.25
    X0 = 0;
else
    X0 = 1;
end
M = mod(X2*GRM(4,:)+X1*GRM(3,:)+X0*GRM(2,:),2);
x = sum(u + M);
if m==3
    if x > 4
        row1 = 1;
    else
        row1 = 0;
    end
else
    if x > 2
        row1 = 1;
    else
        row1 = 0;
    end
end
w1 = [row1 X0 X1 X2];
w = mod(w1*GRM,2)
end

```

4.3.1 Örnek

Örnek (3.1.6)'daki $m = 10011000$ mesajını $RM(1,3)$ kodu için çözelim.

```
>> kodcozum([1 0 0 1 1 0 0 0],1,3)
```

GRM =

```
1 1 1 1 1 1 1 1
1 1 1 1 0 0 0 0
1 1 0 0 1 1 0 0
1 0 1 0 1 0 1 0
```

w =

```
1 0 0 1 1 0 0 1
```

Hatanın son bileşende olduğu görülmektedir. Orijinal mesaj $w = 10011001$ şeklindedir.

4.3.2 Örnek

Örnek (3.2.7)'deki $m = 11000001$ mesajını $RM(1,3)$ kodu için çözelim.

```
>> kodcozum([1 1 0 0 0 0 0 1],1,3)
```

GRM =

```
1 1 1 1 1 1 1 1
1 1 1 1 0 0 0 0
1 1 0 0 1 1 0 0
1 0 1 0 1 0 1 0
```

w =

```
1 1 0 0 0 0 1 1
```

Burada hata 7. bileşendedir. Orijinal mesaj $w = 11000011$ şeklindedir.

KAYNAKLAR

Cooke, Ben, (1999), "Reed-Muller Error Correcting Codes", MIT Undergraduate Journal of Mathematics

Hankerson, D.R., Hoffman, D.G., Leonard, D.A., Lindner, C.C., Phelps, K.T., Rodger, C.A., Wall, J.R., (2000), "Coding Theory and Cryptography-The Essentials", Marcel Dekker, Inc., New York

Hill, Raymond, (1986), "A First Course in Coding Theory", Oxford Press, New York

Raaphorst, Sebastian, (2003), "Reed-Muller Codes", Carleton University

Roman, Steven, (1997), "Introduction to Coding and Information Theory", Springer-Verlag, New York Inc.

Van Lint, J.H., (1982), "Introduction to Coding Theory", Springer-Verlag, New York Inc.

INTERNET KAYNAKLARI

[1] <http://citeseer.ist.psu.edu>

[2] www.sciencedirect.com

ÖZGEÇMİŞ

Doğum tarihi 17.02.1980

Doğum yeri İstanbul

Lise 1994-1996 Özel Üsküdar Fen Lisesi
1996-1997 Özel Bilfen Lisesi

Lisans 1997-2002 Yıldız Teknik Üniversitesi Fen-Edebiyat Fak.
Matematik Bölümü

Yüksek Lisans 2002-2005 Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Çalıştığı Kurum

2002-Devam ediyor Doğu Üniversitesi Fen-Edebiyat Fak.
Matematik ve Fen Bilimleri Bölümü
Araştırma Görevlisi

