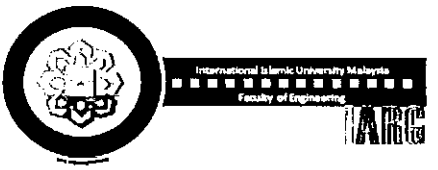
Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM PRESS
2011



Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM Press
2011

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Mohammad Umar Siddiqi, Sigit Puspito Wigati Jarot and Othman Omran Khalifa: Topics in Coding, Cryptography and Information Security

ISBN: 978-967-418-169-7

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

Topics in Coding, Cryptography and Information Security

Contents

Chapter 4

Reed-Muller Codes: An overview

Othman O. Khalifa

4.1. Introduction

Reed-Muller codes are amongst the oldest and most well known of codes. They were discovered and proposed by D. E. Muller and I. S. Reed in 1954. 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 that are worth examination; they form an infinite family of codes, and larger Reed-Muller codes can be constructed from smaller ones. This particular observation leads us to show that Reed-Muller codes can be defined recursively. Unfortunately, Reed-Muller codes become weaker as their length increases. However, they are often used as building blocks in other codes. One of the major advantages of Reed-Muller codes is their relative simplicity to encode messages and decode received transmissions. We examine encoding using *generator matrices* and decoding using one form of a process known as *Hadamard transform*. Reed-Muller codes, like many other codes, have tight links to design theory; we briefly investigate this link between Reed-Muller codes and the designs resulting from affine geometries.

4.2. Coding theory of reed-muller codes and the parameters

Reed-Muller can be defined as follow: r rank RM code $R(r,m)$ is the code we get when the true table of a m elements Boolean function whose order is not larger than r is treated. In other words, an r^{th} order of Reed-Muller Code $R(r, m)$ is the set of all binary string (vectors) of length $n = 2^m$. RM codes consist of three theorems that could be deduced from the definition above[2].

Theorem 1: If check matrix of Hamming Code is H and its column vectors equal to the correspondent column serial number, then the dual code of increased Hamming code is:

$$H_s = \begin{bmatrix} 1 & 1 & L & 1 \\ 0 & & & \\ M & & H & \\ 0 & & & \end{bmatrix}$$