Difference Sets in 2-Groups and their Codes

JJ Hoo
Advised by Dr. Ken Smith and Dr. Jim Davis

Graduate Algebra Symposium
Texas A&M
October 2019

Our Research

Research Agenda

This project aims to utilize difference sets to achieve and derive information and properties related to Reed-Muller Codes and Bent Functions, providing results that have potential uses in quantum cryptography.

- Motivations
- Difference Sets
- Reed-Muller Codes and Bent Functions
- Results
- Future Work

Our Research

Research Agenda

This project aims to utilize difference sets to achieve and derive information and properties related to Reed-Muller Codes and Bent Functions, providing results that have potential uses in quantum cryptography.

- Motivations
- Difference Sets
- Reed-Muller Codes and Bent Functions
- Results
- Future Work

Our Research

Research Agenda

This project aims to utilize difference sets to achieve and derive information and properties related to Reed-Muller Codes and Bent Functions, providing results that have potential uses in quantum cryptography.

- Motivations
- Difference Sets
- Reed-Muller Codes and Bent Functions
- Results
- Future Work

Our Research

Research Agenda

This project aims to utilize difference sets to achieve and derive information and properties related to Reed-Muller Codes and Bent Functions, providing results that have potential uses in quantum cryptography.

- Motivations
- Difference Sets
- Reed-Muller Codes and Bent Functions
- Results
- Future Work

Our Research

Research Agenda

This project aims to utilize difference sets to achieve and derive information and properties related to Reed-Muller Codes and Bent Functions, providing results that have potential uses in quantum cryptography.

- Motivations
- Difference Sets
- Reed-Muller Codes and Bent Functions
- Results
- Future Work

Difference Sets

Definition

A (v, k, λ) **difference set** is a specific subset of $\mathbb{Z}_v$ labeled D such that the multiset $\{d_i - d_j | d_i d_j \in D\}$ covers each non-zero element λ times.

Example

The set $\{1, 2, 4\} \subseteq \mathbb{Z}_7$ is a $(7, 3, 1)$ difference set.

Difference Sets

Definition

A (v, k, λ) **difference set** is a specific subset of $\mathbb{Z}_v$ labeled D such that the multiset $\{d_i - d_j | d_i d_j \in D\}$ covers each non-zero element λ times.

Example

The set $\{1, 2, 4\} \subseteq \mathbb{Z}_7$ is a $(7, 3, 1)$ difference set.

Difference Set Example

$$Z_7 = \{0,1,2,3,4,5,6\}, D = \{1,2,4\}$$

$d_i - d_j$	1	2	4
1	0		
2		0	
4			0

Difference Set Example

$$Z_7 = \{0,1,2,3,4,5,6\}, D = \{1,2,4\}$$

$d_i - d_j$	1	2	4
1	0	-1 $=$ 6	
2	1	0	
4			0

Difference Set Example

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}, D = \{1, 2, 4\}$

$d_i - d_j$	1	2	4
1	0	6	-3 = 4
2	1	0	
4	3		0

Difference Set Example

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}, D = \{1, 2, 4\}$

$d_i - d_j$	1	2	4
1	0	6	4
2	1	0	-2 = 5
4	3	2	0

Difference Set Example

$$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}, D = \{1, 2, 4\}$$

$d_i - d_j$	1	2	4
1	0	6	4
2	1	0	5
4	3	2	0

Multiplicative Version

Remark

We can represent these difference sets as polynomials by using a multiplicative form for the multisets as $\{d_i d_j^{-1} | d_i, d_j \in D\}$. Thus, taking $C_7 := \langle x | x^7 = 1 \rangle$, we have, as in our previous example:

$$D = \{x, x^2, x^4\}$$

Definition

We define the **incidence matrix** of a difference set to be as follows:
Given a group G with a difference set D, we consider a pseudo-Cayley Table of G, where instead of composing elements of G with themselves, we compose elements of G with their respective inverses. If the resulting product is an element of D, we assign a value of 1 to that product, and 0 otherwise. This gives as a matrix over $\mathbb{Z}_2$.

Incidence Matrix Example

$$G = C_7 \qquad D = \{x, x^2, x^4\}$$

$G_i G_j^{-1}$	1	x^6	x^5	x^4	x^3	x^2	x
1	1	x^6	x^5	x^4	x^3	x^2	x
x	x	1	x^6	x^5	x^4	x^3	x^2
x^2	x^2	x	1	x^6	x^5	x^4	x^3
x^3	x^3	x^2	x	1	x^6	x^5	x^4
x^4	x^4	x^3	x^2	x	1	x^6	x^5
x^5	x^5	x^4	x^3	x^2	x	1	x^6
x^6	x^6	x^5	x^4	x^3	x^2	x	1

Incidence Matrix Example

$G = C_7 \qquad D = \{x, x^2, x^4\}$

$G_i G_j^{-1}$	1	x^6	x^5	x^4	x^3	x^2	x
1	1	x^6	x^5	x^4	x^3	x^2	x
x	x	1	x^6	x^5	x^4	x^3	x^2
x^2	x^2	x	1	x^6	x^5	x^4	x^3
x^3	x^3	x^2	x	1	x^6	x^5	x^4
x^4	x^4	x^3	x^2	x	1	x^6	x^5
x^5	x^5	x^4	x^3	x^2	x	1	x^6
x^6	x^6	x^5	x^4	x^3	x^2	x	1

Incidence Matrix Example

$$G = C_7 \qquad D = \{x, x^2, x^4\}$$

$G_i G_j^{-1}$	1	x^6	x^5	x^4	x^3	x^2	x
1	0	0	0	1	0	1	1
x	1	0	0	0	1	0	1
x^2	1	1	0	0	0	1	0
x^3	0	1	1	0	0	0	1
x^4	1	0	1	1	0	0	0
x^5	0	1	0	1	1	0	0
x^6	0	0	1	0	1	1	0

Bent Functions

Definition

A **Bent Function** is a function that maps an input from $\mathbb{Z}_2^n$ for some $n \in \mathbb{N}$ to $\mathbb{Z}_2$.

Remark

For our sake, we can consider bent functions to be polynomials formed from a set of variables, each in $\mathbb{Z}_2$, that provide an output of 0 or 1. For instance, in $\mathbb{Z}_2^4$, a particular difference set can be expressed as the set of vectors of length 4 such that $x_1x_2 + x_3x_4 = 1$, where each x_i is an element of $\mathbb{Z}_2$.

Bent Function Example

$$G = \mathbb{Z}_2^4 \qquad D = \{0011, 0111, 1011, 1100, 1101, 1110\}$$

Remark

We can write the elements of Z_2^4 in lexicographical order, and represent D as a vector in $\mathbb{Z}_{16}$ such that at each position in the vector, a 1 indicates that that indexed element is included in D. In this case, D can be represented as 0001000100011110.

Reed-Muller Code

Definition

We define a **Reed-Muller Code** to be a set of binary codewords $RM(n,k)$, interpreted as the n^{th} order k-variable code, where each codeword is a linear combination of k variables and the $\mathbf{1}$ vector. As a result, each codeword consists of 2^k bits due to binary coding.

Remark

In our example, we examine $RM(1,4)$, and see that there exist 32 codewords in $RM(1,4)$ - $2^4 = 16$ linear combinations and their complements.

Reed-Muller Code Example

Example

$$RM(1,2) = \{0000, 0011, 0101, 0110, 1010, 1001, 1111, 1100\}$$

Example

$$\begin{aligned} RM(1,3) = \{&00000000, 00001111, 00110011, 00111100,\\ &01010101, 01011010, 01100110, 01101001,\\ &10101010, 10100101, 10011001, 10010110,\\ &11111111, 11110000, 11001100, 11000011\} \end{aligned}$$

Reed-Muller Code Example

Example

$$RM(1,2) = \{0000, 0011, 0101, 0110, 1010, 1001, 1111, 1100\}$$

Example

$$\begin{aligned} RM(1,3) = \{&00000000, 00001111, 00110011, 00111100,\\ &01010101, 01011010, 01100110, 01101001,\\ &10101010, 10100101, 10011001, 10010110,\\ &11111111, 11110000, 11001100, 11000011\} \end{aligned}$$

Bent Function Example

$G = \mathbb{Z}_2^4$ $\qquad D = \{0011, 0111, 1011, 1100, 1101, 1110\}$

Remark

This specific choice of D recalls our previous example of a bent function such that $x_1x_2 + x_3x_4 = 1$. Note that this representation has 6 1's and 10 0's. Thus, this bent function has a **distance** of either 6 or 10 from each of the 32 Reed-Muller codewords.

Definition

The **distance** between a function and a codeword is defined as the number of places in which the vectors differ.

Results

Lemma

- *Every row of the incidence matrix corresponding to a given difference set of the form $\mathbb{Z}_2^n$ is a bent function.*
- *The sum of any two rows of the incidence matrix of a difference set is a Reed-Muller codeword.*
- *The sum of a Bent Function and a Reed-Muller codeword is itself a bent function.*
- *Each Reed-Muller codeword is a linear combination of rows of the incidence matrix of a difference set.*

Incidence Matrix of $Z_8 \times Z_2$

$$G = \langle x, y | x^8 = y^2 = 1, xy = yx \rangle$$

Remark

We can construct a difference set by taking a union of the cosets of subgroups. In other words, we have a $(16, 6, 2)$ difference set comprised of a union of cosets of:

$$H_1 = \langle x^4 \rangle$$

$$H_2 = \langle y \rangle$$

$$H_3 = \langle x^4 y \rangle$$

Incidence Matrix of $Z_8 \times Z_2$

Example

Consider the difference set using the previously shown construction of:

$$D = x\langle y\rangle \cup x^2\langle x^4\rangle \cup x^3\langle x^4 y\rangle$$

Each separate subgroup H_i admits an incidence submatrix $\mathcal{H}_i$.

$$\mathcal{H}_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \mathcal{H}_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \mathcal{H}_3 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Remark

We can construct the overall incidence matrix of $Z_8 \times Z_2$ as submatrices corresponding to the $\mathcal{H}_i$ subblocks, resulting in an anti-symmetric block matrix with $\mathbf{0}$ matrices on the diagonal:

$$Incidence_D = \begin{pmatrix} 0 & \mathcal{H}_2 & \mathcal{H}_1 & \mathcal{H}_3 \\ \overline{\mathcal{H}_3} & 0 & \mathcal{H}_2 & \mathcal{H}_1 \\ \mathcal{H}_1 & \overline{\mathcal{H}_3} & 0 & \mathcal{H}_2 \\ \overline{\mathcal{H}_2} & \mathcal{H}_1 & \overline{\mathcal{H}_3} & 0 \end{pmatrix}$$

Schur Product

Definition

We define the **Schur Product** to be a matrix where each row is a entry-wise product of unique pairwise products of rows of the previously defined incidence matrix. As such, the size of the Schur matrix associated with a difference set is $\binom{k}{2} \times k$, where k is the size of the difference set. The rank of this matrix is then defined as the **Schur Rank**.

Summary of Results

Lemma

When taking the so-called Schur ranks of incidence matrices, the minimal such Schur rank is $\binom{n}{2}$, *where n is the rank of the incidence matrix itself.*

Lemma

Given a difference set generated by the bent function $x_1x_2 + x_3x_4 + \cdots + x_{2n-1}x_{2n}$, *we have the result that the sum of any three rows of the associated incidence matrix will return either a row or row-complement of the same incidence matrix. This originates from each sum of the bent function and a codeword from* $RM(1, 2n)$ *being itself a bent function.*

Acknowledgements

- Dr. Ken Smith, Sam Houston State University
- Dr. Jim Davis, University of Richmond
- The Davis Group from the University of Richmond:
  - Calvin Reedy
  - Connor Kissane
  - Scarlett Sun
  - Kartikey Sharma
  - Jackman Liu

Thank You