An introduction to coding theory

Adrish Banerjee

Department of Electrical Engineering
Indian Institute of Technology Kanpur
Kanpur, Uttar Pradesh
India

Feb. 6, 2017

Lecture #6B: Some simple linear block codes -II

Outline of the lecture

- Reed-Muller code

Outline of the lecture

- Reed-Muller code
- Decoding of Reed-Muller code

Reed-Muller code

- For any integers m and r with $0 \leq r \leq m$, there exists a binary r^{th}-order Reed Muller (RM) code, denoted by RM(r,m), with the following parameters:

  Code length : $n = 2^m$

  Dimension : $k(r, m) = 1 + \begin{pmatrix} m \\ 1 \end{pmatrix} + \begin{pmatrix} m \\ 2 \end{pmatrix} + \cdots + \begin{pmatrix} m \\ r \end{pmatrix}$,

  Minimum distance : $d_{\min} = 2^{m-r}$

  where $\begin{pmatrix} m \\ i \end{pmatrix}$ is the binomial coefficient

Reed-Muller code

- For any integers m and r with $0 \leq r \leq m$, there exists a binary r^{th}-order Reed Muller (RM) code, denoted by RM(r,m), with the following parameters:

  Code length : $n = 2^m$

  Dimension : $k(r, m) = 1 + \begin{pmatrix} m \\ 1 \end{pmatrix} + \begin{pmatrix} m \\ 2 \end{pmatrix} + \cdots + \begin{pmatrix} m \\ r \end{pmatrix}$,

  Minimum distance : $d_{\min} = 2^{m-r}$

  where $\begin{pmatrix} m \\ i \end{pmatrix}$ is the binomial coefficient

- Let $m = 4$, and $r = 2$, then $n = 16$, $k = 11$, and $d_{\min} = 4$

Reed-Muller code

- For $1 \leq i \leq m$, let $\mathbf{v}_i$ be a binary 2^m-tuple of the following form:

$$\mathbf{v}_i = \left(\underbrace{0 \cdots 0}_{2^{i-1}}, \underbrace{1 \cdots 1}_{2^{i-1}}, \underbrace{0 \cdots 0}_{2^{i-1}}, \cdots, \underbrace{1 \cdots 1}_{2^{i-1}} \right)$$

  which consists of 2^{m-i+1} alternating all-zero and all-one 2^{i-1}-tuples.

Reed-Muller code

- For $1 \leq i \leq m$, let $\mathbf{v}_i$ be a binary 2^m-tuple of the following form:

$$\mathbf{v}_i = \left(\underbrace{0 \cdots 0}_{2^{i-1}}, \underbrace{1 \cdots 1}_{2^{i-1}}, \underbrace{0 \cdots 0}_{2^{i-1}}, \cdots, \underbrace{1 \cdots 1}_{2^{i-1}} \right)$$

  which consists of 2^{m-i+1} alternating all-zero and all-one 2^{i-1}-tuples.
- For $m = 4$, we have the following four 16-tuples.

$$\begin{aligned}
\mathbf{v}_1 &= (0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1) \\
\mathbf{v}_2 &= (0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1) \\
\mathbf{v}_3 &= (0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1) \\
\mathbf{v}_4 &= (0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1)
\end{aligned}$$

Reed-Muller code

- Let $\mathbf{x} = (x_0, x_1, x_2, \cdots, x_{n-1})$ and $\mathbf{y} = (y_0, y_1, y_2, \cdots, y_{n-1})$ be two binary n-tuples, we define Boolean product of $\mathbf{x}$ and $\mathbf{y}$ as follows:

$$\mathbf{x} \cdot \mathbf{y} = (x_0 \cdot y_0, x_1 \cdot y_1, \cdots, x_{n-1} \cdot y_{n-1}),$$

where "$\cdot$" denotes the Boolean product of $\mathbf{x}$ and $\mathbf{y}$:

Reed-Muller code

- Let $\mathbf{x} = (x_0, x_1, x_2, \cdots, x_{n-1})$ and $\mathbf{y} = (y_0, y_1, y_2, \cdots, y_{n-1})$ be two binary n-tuples, we define Boolean product of $\mathbf{x}$ and $\mathbf{y}$ as follows:

$$\mathbf{x} \cdot \mathbf{y} = (x_0 \cdot y_0, x_1 \cdot y_1, \cdots, x_{n-1} \cdot y_{n-1}),$$

where "$\cdot$" denotes the Boolean product of $\mathbf{x}$ and $\mathbf{y}$:

- For example, if

$$\mathbf{v}_1 = (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1)$$

and

$$\mathbf{v}_2 = (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1)$$

then,

$$\mathbf{v}_1 \cdot \mathbf{v}_2 = (0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1)$$

Reed-Muller code

- Let $\mathbf{v}_0$ denote all one 2^m-tuple, $\mathbf{v}_0 = (1, 1, \cdots, 1)$. For $l \leq i_1 < i_2 < \cdots < i_l \leq m$, the product vector

$$\mathbf{v}_{i_1}\mathbf{v}_{i_2}\cdots\mathbf{v}_{i_l}$$

  is said to have degree l.

Reed-Muller code

- Let $\mathbf{v}_0$ denote all one 2^m-tuple, $\mathbf{v}_0 = (1, 1, \cdots, 1)$. For $l \leq i_1 < i_2 < \cdots < i_l \leq m$, the product vector

$$\mathbf{v}_{i_1}\mathbf{v}_{i_2}\cdots\mathbf{v}_{i_l}$$

  is said to have degree l.

- The weight of the product

$$\mathbf{v}_{i_1}\mathbf{v}_{i_2}\cdots\mathbf{v}_{i_l}$$

  is equal to 2^{m-l}.

Reed-Muller code

- The r^{th}-order RM code , RM(r,m), of length 2^m is generated by following set of independent vectors:

$$\begin{aligned} G_{RM}(r,m) &= \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m, \mathbf{v}_1\mathbf{v}_2, \mathbf{v}_1\mathbf{v}_3, \cdots, \mathbf{v}_{m-1}\mathbf{v}_m, \cdots \\ &, \quad \text{up to products of degree r}\}. \end{aligned}$$

Reed-Muller code

- The r^{th}-order RM code , RM(r,m), of length 2^m is generated by following set of independent vectors:

$$\begin{aligned} G_{RM}(r,m) &= \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m, \mathbf{v}_1\mathbf{v}_2, \mathbf{v}_1\mathbf{v}_3, \cdots, \mathbf{v}_{m-1}\mathbf{v}_m, \cdots \\ &, \quad \text{up to products of degree r}\}. \end{aligned}$$

- There are

$$k(r,m) = 1 + \begin{pmatrix} m \\ 1 \end{pmatrix} + \begin{pmatrix} m \\ 2 \end{pmatrix} + \cdots + \begin{pmatrix} m \\ r \end{pmatrix},$$

vectors in $G_{RM}(r,m)$

Reed-Muller code

- The r^{th}-order RM code , RM(r,m), of length 2^m is generated by following set of independent vectors:

$$G_{RM}(r,m) = \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m, \mathbf{v}_1\mathbf{v}_2, \mathbf{v}_1\mathbf{v}_3, \cdots, \mathbf{v}_{m-1}\mathbf{v}_m, \cdots , \text{up to products of degree r}\}.$$

- There are

$$k(r,m) = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r},$$

vectors in $G_{RM}(r,m)$

- If the vectors in $G_{RM}(r,m)$ are arranged as rows of a matrix, then the matrix is a generator matrix of the $RM(r,m)$ code.

Reed-Muller code

- Let $m = 4$, and $r = 2$, the second-order RM code of length $n = 16$ is generated by the following 11 vectors:

$\mathbf{v}_0$	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
$\mathbf{v}_1$	0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
$\mathbf{v}_2$	0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1
$\mathbf{v}_3$	0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1
$\mathbf{v}_4$	0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1
$\mathbf{v}_1\mathbf{v}_2$	0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1
$\mathbf{v}_1\mathbf{v}_3$	0 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1
$\mathbf{v}_1\mathbf{v}_4$	0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 1
$\mathbf{v}_2\mathbf{v}_3$	0 0 0 0 0 0 1 1 0 0 0 0 0 0 1 1
$\mathbf{v}_2\mathbf{v}_4$	0 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1
$\mathbf{v}_3\mathbf{v}_4$	0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1

Reed-Muller code

- For $1 \leq r \leq m$, we define

$$R(r,m) = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) \,|\mathbf{u} \in R(r,m-1), \mathbf{v} \in R(r-1,m-1)\}$$

Reed-Muller code

- For $1 \leq r \leq m$, we define

$$R(r,m) = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) \,|\mathbf{u} \in R(r,m-1), \mathbf{v} \in R(r-1,m-1)\}$$

- The generator matrix can be written as

$$G(r,m) = \begin{bmatrix} \text{G(r, m-1)} & \text{G(r, m-1)} \\ 0 & \text{G(r-1, m-1)} \end{bmatrix}$$

Reed-Muller code

- Minimum distance of RM(r, m) is 2^{m-r}.

Reed-Muller code

- Minimum distance of RM(r, m) is 2^{m-r}.
- **Proof:** We will prove the result by mathematical induction.

Reed-Muller code

- Minimum distance of RM(r, m) is 2^{m-r}.
- **Proof:** We will prove the result by mathematical induction.
- Let $m = 1$, then RM(0,1) is a length two repetition code. In this case the minimum distance is 2.

Reed-Muller code

- Minimum distance of RM(r, m) is 2^{m-r}.
- **Proof:** We will prove the result by mathematical induction.
- Let $m = 1$, then RM(0,1) is a length two repetition code. In this case the minimum distance is 2.
- RM(1,1) has four codewords $\{00, 01, 11, 10\}$ of length 2. Minimum distance in this case is 2.

Reed-Muller code

- Minimum distance of RM(r, m) is 2^{m-r}.
- **Proof:** We will prove the result by mathematical induction.
- Let $m = 1$, then RM(0,1) is a length two repetition code. In this case the minimum distance is 2.
- RM(1,1) has four codewords $\{00, 01, 11, 10\}$ of length 2. Minimum distance in this case is 2.
- Let us assume for upto m and for $0 \leq r \leq m$, the minimum distance is 2^{m-r}. We will show that $d_{min}$for RM$(r, m+1)$ is 2^{m-r+1}.

Reed-Muller code

- Let $\mathbf{f}, \mathbf{f}' \in$ RM(r, m) and let $\mathbf{g}, \mathbf{g}' \in$ RM$(r-1, m)$. Then vectors $\mathbf{c}_1 = (\mathbf{f}, \mathbf{f}+\mathbf{g})$ and $\mathbf{c}_2 = (\mathbf{f}', \mathbf{f}'+\mathbf{g}')$ must be in RM$(r, m+1)$.

Reed-Muller code

- Let $\mathbf{f}, \mathbf{f}' \in \mathrm{RM}(r, m)$ and let $\mathbf{g}, \mathbf{g}' \in \mathrm{RM}(r-1, m)$. Then vectors $\mathbf{c}_1 = (\mathbf{f}, \mathbf{f}+\mathbf{g})$ and $\mathbf{c}_2 = (\mathbf{f}', \mathbf{f}'+\mathbf{g}')$ must be in $\mathrm{RM}(r, m+1)$.
- if $\mathbf{g} = \mathbf{g}'$, then $d(\mathbf{c_1}, \mathbf{c_2}) = 2d(\mathbf{f}, \mathbf{f}') \geq 2 \cdot 2^{m-r}$.

Reed-Muller code

- Let $\mathbf{f}, \mathbf{f}' \in \mathrm{RM}(r, m)$ and let $\mathbf{g}, \mathbf{g}' \in \mathrm{RM}(r-1, m)$. Then vectors $\mathbf{c}_1 = (\mathbf{f}, \mathbf{f}+\mathbf{g})$ and $\mathbf{c}_2 = (\mathbf{f}', \mathbf{f}'+\mathbf{g}')$ must be in $\mathrm{RM}(r, m+1)$.
- if $\mathbf{g} = \mathbf{g}'$, then $d(\mathbf{c_1}, \mathbf{c_2}) = 2d(\mathbf{f}, \mathbf{f}') \geq 2 \cdot 2^{m-r}$.
- if $\mathbf{g} \neq \mathbf{g}'$, then $d(\mathbf{c_1}, \mathbf{c_2}) = w(\mathbf{f} - \mathbf{f}') + w(\mathbf{g} - \mathbf{g}' + \mathbf{f} - \mathbf{f}')$.

Reed-Muller code

- Let $\mathbf{f}, \mathbf{f}' \in \mathrm{RM}(r, m)$ and let $\mathbf{g}, \mathbf{g}' \in \mathrm{RM}(r-1, m)$. Then vectors $\mathbf{c}_1 = (\mathbf{f}, \mathbf{f}+\mathbf{g})$ and $\mathbf{c}_2 = (\mathbf{f}', \mathbf{f}'+\mathbf{g}')$ must be in $\mathrm{RM}(r, m+1)$.
- if $\mathbf{g} = \mathbf{g}'$, then $d(\mathbf{c_1}, \mathbf{c_2}) = 2d(\mathbf{f}, \mathbf{f}') \geq 2 \cdot 2^{m-r}$.
- if $\mathbf{g} \neq \mathbf{g}'$, then $d(\mathbf{c_1}, \mathbf{c_2}) = w(\mathbf{f} - \mathbf{f}') + w(\mathbf{g} - \mathbf{g}' + \mathbf{f} - \mathbf{f}')$.
- Since $w(\mathbf{x} + \mathbf{y}) \geq w(\mathbf{x}) - w(\mathbf{y})$, we have

$$d(\mathbf{c_1}, \mathbf{c_2}) \geq w(\mathbf{f} - \mathbf{f}') + w(\mathbf{g} - \mathbf{g}') - w(\mathbf{f} - \mathbf{f}') = w(\mathbf{g} - \mathbf{g}')$$

Reed-Muller code

- Let $\mathbf{f}, \mathbf{f}' \in \mathrm{RM}(r, m)$ and let $\mathbf{g}, \mathbf{g}' \in \mathrm{RM}(r-1, m)$. Then vectors $\mathbf{c}_1 = (\mathbf{f}, \mathbf{f}+\mathbf{g})$ and $\mathbf{c}_2 = (\mathbf{f}', \mathbf{f}'+\mathbf{g}')$ must be in $\mathrm{RM}(r, m+1)$.
- if $\mathbf{g} = \mathbf{g}'$, then $d(\mathbf{c_1}, \mathbf{c_2}) = 2d(\mathbf{f}, \mathbf{f}') \geq 2 \cdot 2^{m-r}$.
- if $\mathbf{g} \neq \mathbf{g}'$, then $d(\mathbf{c_1}, \mathbf{c_2}) = w(\mathbf{f} - \mathbf{f}') + w(\mathbf{g} - \mathbf{g}' + \mathbf{f} - \mathbf{f}')$.
- Since $w(\mathbf{x} + \mathbf{y}) \geq w(\mathbf{x}) - w(\mathbf{y})$, we have

$$d(\mathbf{c_1}, \mathbf{c_2}) \geq w(\mathbf{f} - \mathbf{f}') + w(\mathbf{g} - \mathbf{g}') - w(\mathbf{f} - \mathbf{f}') = w(\mathbf{g} - \mathbf{g}')$$

- Since $\mathbf{g} - \mathbf{g}' \in \mathrm{RM}(r-1, m)$, so that

$$w(\mathbf{g} - \mathbf{g}') \geq 2^{m-(r-1)} = 2^{m-r+1}$$

Reed-Muller code

- The $(m-r-1)^{\text{th}}$-order RM code is the dual code of r^{th}-order RM code.

Reed-Muller code

- The $(m-r-1)^{\text{th}}$-order RM code is the dual code of r^{th}-order RM code.
- **Proof:** Let us consider $a \in \text{RM}(m-r-1, m), b \in \text{RM}(r, m)$. Then $a(v_1, \ldots, v_m)$ is a polynomial of degree $\leq m-r-1$.

Reed-Muller code

- The $(m-r-1)^{\text{th}}$-order RM code is the dual code of r^{th}-order RM code.
- **Proof:** Let us consider $a \in \text{RM}(m-r-1, m), b \in \text{RM}(r, m)$. Then $a(v_1, \ldots, v_m)$ is a polynomial of degree $\leq m-r-1$.
- Similarly, $b(v_1, \ldots, v_m)$ has degree $\leq r$, and their product ab has degree $\leq m-1$.

Reed-Muller code

- The $(m-r-1)^{\text{th}}$-order RM code is the dual code of r^{th}-order RM code.
- **Proof:** Let us consider $a \in \text{RM}(m-r-1, m), b \in \text{RM}(r, m)$. Then $a(v_1, \ldots, v_m)$ is a polynomial of degree $\leq m-r-1$.
- Similarly, $b(v_1, \ldots, v_m)$ has degree $\leq r$, and their product ab has degree $\leq m-1$.
- Therefore $ab \in \text{RM}(m-1, m)$ and has even weight. Therefore the dot product $a \cdot b = 0 \bmod 2$.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to coding theory

Reed-Muller code

- The $(m-r-1)^{\text{th}}$-order RM code is the dual code of r^{th}-order RM code.
- **Proof:** Let us consider $a \in \text{RM}(m-r-1, m), b \in \text{RM}(r, m)$. Then $a(v_1, \ldots, v_m)$ is a polynomial of degree $\leq m-r-1$.
- Similarly, $b(v_1, \ldots, v_m)$ has degree $\leq r$, and their product ab has degree $\leq m-1$.
- Therefore $ab \in \text{RM}(m-1, m)$ and has even weight. Therefore the dot product $a \cdot b = 0 \bmod 2$.
- Also, $dim(\text{RM}(m-r-1, m)) + dim(\text{RM}(r, m))$

$$= 1 + \begin{pmatrix} m \\ 1 \end{pmatrix} + \cdots + \begin{pmatrix} m \\ m-r-1 \end{pmatrix} + 1 + \begin{pmatrix} m \\ 1 \end{pmatrix} + \cdots + \begin{pmatrix} m \\ r \end{pmatrix}$$

$$= 2^m$$

which implies that $\text{RM}(m-r-1, m) = \text{RM}(r, m)^{\perp}$

Reed-Muller code

- From the construction we can see that RM(r-1,m) code is a proper subcode of the RM(r,m) code. hence

$$RM(0, m) \subset RM(1, m) \subset \cdots \subset RM(r, m)$$

Reed-Muller code

- From the construction we can see that RM(r-1,m) code is a proper subcode of the RM(r,m) code. hence

$$RM(0, m) \subset RM(1, m) \subset \cdots \subset RM(r, m)$$

- The zeroth order RM code is a repetition code.

Reed-Muller code

- From the construction we can see that RM(r-1,m) code is a proper subcode of the RM(r,m) code. hence

$$RM(0, m) \subset RM(1, m) \subset \cdots \subset RM(r, m)$$

- The zeroth order RM code is a repetition code.
- The $(m-1)^{\text{th}}$-order RM code is a single parity check code.

Reed-Muller code

- From the construction we can see that RM(r-1,m) code is a proper subcode of the RM(r,m) code. hence

$$RM(0, m) \subset RM(1, m) \subset \cdots \subset RM(r, m)$$

- The zeroth order RM code is a repetition code.
- The $(m-1)^{\text{th}}$-order RM code is a single parity check code.
- The $(m-2)^{\text{th}}$-order RM code of length 2^m is distance-4 extended Hamming code obtained by adding an overall parity bit to the Hamming code of length $2^m - 1$.

Decoding of Reed-Muller code

- Consider a 2nd order Reed Muller code of length $n = 16$ generated by following 11 vectors

$\mathbf{v_0}$	1111111111111111
$\mathbf{v_4}$	0000000011111111
$\mathbf{v_3}$	0000111100001111
$\mathbf{v_2}$	0011001100110011
$\mathbf{v_1}$	0101010101010101
$\mathbf{v_3v_4}$	0000000000001111
$\mathbf{v_2v_4}$	0000000000110011
$\mathbf{v_1v_4}$	0000000001010101
$\mathbf{v_2v_3}$	0000110000000011
$\mathbf{v_1v_3}$	0000101000000101
$\mathbf{v_1v_2}$	0001000100010001

Decoding of Reed-Muller code

- The message to be encoded is given by

$$(a_0, a_4, a_3, a_2, a_1, a_{34}, a_{24}, a_{14}, a_{23}, a_{13}, a_{12})$$

- The codeword is given by

$$\begin{aligned}(b_0, b_1, b_2, \cdots, b_{15}) \quad = \quad & a_0\mathbf{v_0} + a_4\mathbf{v_4} + a_3\mathbf{v_3} + a_2\mathbf{v_2} + a_1\mathbf{v_1} \\ & + a_{34}\mathbf{v_3}\mathbf{v_4} + a_{24}\mathbf{v_2}\mathbf{v_4} + a_{14}\mathbf{v_1}\mathbf{v_4} \\ & + a_{23}\mathbf{v_2}\mathbf{v_3} + a_{13}\mathbf{v_1}\mathbf{v_3} + a_{12}\mathbf{v_1}\mathbf{v_2}\end{aligned}$$

Decoding of Reed-Muller code

- We can see that first four components of each generator vector and subsequent three groups of four consecutive components is zero except for the the vector $\mathbf{v_1}\mathbf{v_2}$.
- Thus the code bit a_{12} can be written as

$$\begin{aligned} a_{12} &= b_0 + b_1 + b_2 + b_3 \\ a_{12} &= b_4 + b_5 + b_6 + b_7 \\ a_{12} &= b_8 + b_9 + b_{10} + b_{11} \\ a_{12} &= b_{12} + b_{13} + b_{14} + b_{15} \end{aligned}$$

- RM codes uses majority logic decision rule for decoding.

Decoding of Reed-Muller code

- Consider a 2nd order Reed Muller code of length $n = 16$ generated by following 11 vectors

$\mathbf{v_0}$	1111111111111111
$\mathbf{v_4}$	0000000011111111
$\mathbf{v_3}$	0000111100001111
$\mathbf{v_2}$	0011001100110011
$\mathbf{v_1}$	0101010101010101
$\mathbf{v_3v_4}$	0000000000001111
$\mathbf{v_2v_4}$	0000000000110011
$\mathbf{v_1v_4}$	0000000001010101
$\mathbf{v_2v_3}$	0000110000000011
$\mathbf{v_1v_3}$	0000101000000101
$\mathbf{v_1v_2}$	0001000100010001

Decoding of Reed-Muller code

- Let $\mathbf{r} = (r_0, r_1, \cdots, r_{15})$ be the received vector. In decoding a_{12}, we form the following equations

$$\begin{aligned} A_1 &= r_0 + r_1 + r_2 + r_3 \\ A_2 &= r_4 + r_5 + r_6 + r_7 \\ A_3 &= r_8 + r_9 + r_{10} + r_{11} \\ A_4 &= r_{12} + r_{13} + r_{14} + r_{15} \end{aligned}$$

Decoding of Reed-Muller code

- Similarly we can decode, $a_{13}, a_{23}, a_{14}, a_{24}, a_{34}$. For example, for a_{13} we have

$$\begin{aligned} A_1 &= r_0 + r_1 + r_4 + r_5 \\ A_2 &= r_2 + r_3 + r_6 + r_7 \\ A_3 &= r_8 + r_9 + r_{12} + r_{13} \\ A_4 &= r_{10} + r_{11} + r_{14} + r_{15} \end{aligned}$$

- For a_{23} we have

$$\begin{aligned} A_1 &= r_0 + r_2 + r_4 + r_6 \\ A_2 &= r_1 + r_3 + r_5 + r_7 \\ A_3 &= r_8 + r_{10} + r_{12} + r_{14} \\ A_4 &= r_9 + r_{11} + r_{13} + r_{15} \end{aligned}$$

Decoding of Reed-Muller code

- For a_{14}

$$\begin{aligned} A_1 &= r_0 + r_1 + r_8 + r_9 \\ A_2 &= r_2 + r_3 + r_{10} + r_{11} \\ A_3 &= r_4 + r_5 + r_{12} + r_{13} \\ A_4 &= r_6 + r_7 + r_{14} + r_{15} \end{aligned}$$

- For a_{24} we have

$$\begin{aligned} A_1 &= r_0 + r_1 + r_4 + r_5 \\ A_2 &= r_2 + r_3 + r_6 + r_7 \\ A_3 &= r_8 + r_9 + r_{12} + r_{13} \\ A_4 &= r_{10} + r_{11} + r_{14} + r_{15} \end{aligned}$$

Decoding of Reed-Muller code

- For a_{34} we have

$$\begin{aligned} A_1 &= r_0 + r_4 + r_8 + r_{12} \\ A_2 &= r_1 + r_5 + r_9 + r_{13} \\ A_3 &= r_2 + r_6 + r_{10} + r_{14} \\ A_4 &= r_3 + r_7 + r_{11} + r_{15} \end{aligned}$$

- After decoding $a_{12}, a_{13}, a_{23}, a_{14}, a_{24}, a_{34}$, we form a modified received vector as

$$\begin{aligned} \mathbf{r}^{(1)} &= (r_0^{(1)}, r_1^{(1)}, \cdots, r_{15}^{(1)}) \\ &= \mathbf{r} - a_{34}\mathbf{v_3}\mathbf{v_4} - a_{24}\mathbf{v_2}\mathbf{v_4} - a_{14}\mathbf{v_1}\mathbf{v_4} - a_{23}\mathbf{v_2}\mathbf{v_3} - a_{13}\mathbf{v_1}\mathbf{v_3} - a_{12}\mathbf{v_1}\mathbf{v_2} \end{aligned}$$

Decoding of Reed-Muller code

- Consider a 2nd order Reed Muller code of length $n = 16$ generated by following 11 vectors

$\mathbf{v_0}$	1111111111111111
$\mathbf{v_4}$	0000000011111111
$\mathbf{v_3}$	0000111100001111
$\mathbf{v_2}$	0011001100110011
$\mathbf{v_1}$	0101010101010101
$\mathbf{v_3v_4}$	0000000000001111
$\mathbf{v_2v_4}$	0000000000110011
$\mathbf{v_1v_4}$	0000000001010101
$\mathbf{v_2v_3}$	0000110000000011
$\mathbf{v_1v_3}$	0000101000000101
$\mathbf{v_1v_2}$	0001000100010001

Decoding of Reed-Muller code

- In absence of errors, we can write $\mathbf{r}^{(1)}$ as following codeword

$$(b_0^{(1)}, b_1^{(1)}, \cdots, b_{15}^{(1)} = a_0\mathbf{v_0} + a_4\mathbf{v_4} + a_3\mathbf{v_3} + a_2\mathbf{v_2} + a_1\mathbf{v_1}$$

- We can see that sum of every two components of $\mathbf{v_0}, \mathbf{v_4}, \mathbf{v_3}, \mathbf{v_2}$ starting from first is zero, whereas for $\mathbf{v_1}$ it is 1.
- Therefore we can form eight independent equations for a_1, given by

$$\begin{aligned}
a_1 &= b_0^{(1)} + b_1^{(1)}, a_1 = b_8^{(1)} + b_9^{(1)} \\
a_1 &= b_2^{(1)} + b_3^{(1)}, a_1 = b_{10}^{(1)} + b_{11}^{(1)} \\
a_1 &= b_4^{(1)} + b_5^{(1)}, a_1 = b_{12}^{(1)} + b_{13}^{(1)} \\
a_1 &= b_6^{(1)} + b_7^{(1)}, a_1 = b_{14}^{(1)} + b_{15}^{(1)}
\end{aligned}$$

Decoding of Reed-Muller code

- Similarly independent determination of a_2, a_3 and a_4 can be formed.
- We can form eight independent equations for a_2, given by

$$\begin{aligned}
a_2 &= b_0^{(1)} + b_2^{(1)}, a_2 = b_8^{(1)} + b_{10}^{(1)} \\
a_2 &= b_1^{(1)} + b_3^{(1)}, a_2 = b_9^{(1)} + b_{11}^{(1)} \\
a_2 &= b_4^{(1)} + b_6^{(1)}, a_2 = b_{12}^{(1)} + b_{14}^{(1)} \\
a_2 &= b_5^{(1)} + b_7^{(1)}, a_2 = b_{13}^{(1)} + b_{15}^{(1)}
\end{aligned}$$

- We can form eight independent equations for a_3, given by

$$\begin{aligned}
a_3 &= b_0^{(1)} + b_4^{(1)}, a_3 = b_8^{(1)} + b_{12}^{(1)} \\
a_3 &= b_1^{(1)} + b_5^{(1)}, a_3 = b_9^{(1)} + b_{13}^{(1)} \\
a_3 &= b_2^{(1)} + b_6^{(1)}, a_3 = b_{10}^{(1)} + b_{14}^{(1)} \\
a_3 &= b_3^{(1)} + b_7^{(1)}, a_3 = b_{11}^{(1)} + b_{15}^{(1)}
\end{aligned}$$

Decoding of Reed-Muller code

- We can form eight independent equations for a_4, given by

$$\begin{aligned} a_4 &= b_0^{(1)} + b_8^{(1)}, a_4 = b_4^{(1)} + b_{12}^{(1)} \\ a_4 &= b_1^{(1)} + b_9^{(1)}, a_4 = b_5^{(1)} + b_{13}^{(1)} \\ a_4 &= b_2^{(1)} + b_{10}^{(1)}, a_4 = b_6^{(1)} + b_{14}^{(1)} \\ a_4 &= b_3^{(1)} + b_{11}^{(1)}, a_4 = b_7^{(1)} + b_{15}^{(1)} \end{aligned}$$

- Equations for decoding a_1 can be written as

$$\begin{aligned} A_1^{(1)} &= r_0^{(1)} + r_1^{(1)}, A_5^{(1)} = r_8^{(1)} + r_9^{(1)} \\ A_2^{(1)} &= r_2^{(1)} + r_3^{(1)}, A_6^{(1)} = r_{10}^{(1)} + r_{11}^{(1)} \\ A_3^{(1)} &= r_4^{(1)} + r_5^{(1)}, A_7^{(1)} = r_{12}^{(1)} + r_{13}^{(1)} \\ A_4^{(1)} &= r_6^{(1)} + r_7^{(1)}, A_8^{(1)} = r_{14}^{(1)} + r_{15}^{(1)} \end{aligned}$$

Decoding of Reed-Muller code

- After decoding a_1, a_2, a_3, a_4, we create a modified received vector $\mathbf{r}^{(2)}$

$$\begin{aligned} \mathbf{r}^{(2)} &= (r_0^{(2)}, r_1^{(2)}, \cdots, r_{15}^{(2)}) \\ &= \mathbf{r}^{(1)} - a_4\mathbf{v_4} - a_3\mathbf{v_3} - a_2\mathbf{v_2} - a_1\mathbf{v_1} \end{aligned}$$

- In absence of errors, we have

$$\mathbf{r}^{(2)} = a_0\mathbf{v_0} = (a_0, a_0, \cdots, a_0)$$

- a_0 is decoded to be the value of majority of the bits in $\mathbf{r}^{(2)}$.