Week 11

Reed-Muller codes

Version 2023-12-03. To accessible online version of this chapter

Synopsis. *The minimum distance of a perfect code cannot exceed 7 unless the code is a repetition code. This is disappointingly low. In this final part of the course, we construct Reed-Muller codes, a family of codes with large minimum distance. Unfortunately, they are not perfect. The construction is based on Boolean functions, which arise in elementary logic as columns of truth tables and are used in cicruit design.*

Boolean functions

Fix $m \geq 1$. Denote by V^m the set of all binary words of length m. (It is the same as $\mathbb{F}_2^m$ but viewed without any vector space structure).

For example, V^3 is the set $\{000, 001, 010, 011, 100, 101, 110, 111\}$.

Definition: Boolean functions

A **Boolean function** is a (set-theoretical) function $f\colon V^m \to \mathbb{F}_2$.

Remark: the number of Boolean functions

The total number of all Boolean functions on V^m is $|\mathbb{F}_2|^{|V_m|} = 2^{2^m}$.

Remark: Boolean functions as rows of a truth table. One has certainly met Boolean functions when constructing truth tables for statements in basic logic. To give an illustration, let $m = 3$. Consider statements which involve variables x_1, x_2, x_3, each of which can take values 0 ($\textsc{false}$) or 1 ($\textsc{true}$).

We will represent a logical statement by a *row* (not column) in a truth table. (We use rows because it is common in Coding Theory to think of codevectors as of row vectors; and in

Reed-Muller codes, codevectors arise from functions.) In our example ($m = 3$), the table will have 8 columns:

x_1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1
$(x_1$ and $x_2) \implies x_3$	1	1	1	0	1	1	1	1
$\mathbf{0}$	0	0	0	0	0	0	0	0
$\mathbf{1}$	1	1	1	1	1	1	1	1
v_2v_3	0	0	0	0	0	0	1	1

In this table, $(x_1$ and $x_2) \implies x_3$ is a statement whose truth value depends on the values of x_1, x_2 and x_3. Therefore, it can be viewed as a Boolean function: its value at the binary word 000 is 1, at the word 100 the value is 1, and so on. The only binary word where this function takes the value 0 is the word 110: indeed, if x_1 and x_2 are TRUE, then x_1 and x_2 is TRUE, but x_3 is FALSE, and the value of the implication "TRUE $\implies$ FALSE" is FALSE.

(The other rows in the table will be explained below.)

The Boolean algebra

Because Boolean functions take values in $\mathbb{F}_2 = \{0, 1\}$ which is a field, Boolean functions can be added and multiplied pointwise: if $f, g \colon V^m \to \mathbb{F}_2$, one has the functions

$$f + g, fg \colon V^m \to \mathbb{F}_2; \quad (f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x), \quad \forall x \in V^m.$$

Also, there are constant functions $\mathbf{0}$ and $\mathbf{1}$. (They are shown in the 2nd, respectively 3rd, row of the truth table above.) The Boolean function $\mathbf{1}$ is often called *the tautological truth*.

Definition: Boolean algebra

The vector space of Boolean functions $f \colon V^m \to \mathbb{F}_2$, together with the operation of multiplication of functions, is the **Boolean algebra** on V^m.

The traditional logical operations can be written in terms of the Boolean algebra operations $+$ and $\times$. Clearly, multiplication is the same as AND:

$$fg = f \text{ and } g.$$

The addition obeys the rule $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, $1 + 1 = 0$. The logical operation which corresponds to addition is called the *exclusive OR*:

$$f + g = f \text{ xor } g = ((f \text{ or } g) \text{ and } \text{not}(f \text{ and } g))\,.$$

How to write elements of the Boolean algebra as row vectors?

To write elements of the Boolean algebra on V^m as binary vectors, so that we can define the weight, the Hamming distance etc, we need to order all binary words of length m as $b_0, \ldots, b_{2^m-1}$.

The standard ordering is obtained by interpreting the word $x_1 x_2 \ldots x_m$ as a number written in base 2, i.e., the number $2^{m-1}x_1 + \ldots + 2x_{m-1} + x_m$. Thus, the binary words of length 3 appear in the following order: 000, 001, 010, 011, 100, 101, 110, 111. However, the exact choice of the order is not important, as we will see.

Definition: value vector of a Boolean function

Let $f\colon V^m \to \mathbb{F}_2$ be a Boolean function. The **value vector** of f is the binary vector $\underline{f} = (f(b_0), \ldots, f(b_{2^m-1}))$ of length 2^m, where $b_0, \ldots, b_{2^m-1}$ is the chosen ordering of V^m.

The next notion does not at all depend on the chosen ordering of words in V^m:

Definition: weight of a Boolean function

The **weight** of the Boolean function f is defined as the weight of the value vector $\underline{f}$. The weight does not depend on the ordering of the binary words, because

$$w(f) = \#\{b \in V^m : f(b) = 1\}.$$

The monomial basis of the Boolean algebra

We will now introduce two special kinds of elements of the Boolean algebra: coordinate functions and, more generally, monomial functions.

Definition: coordinate function

The Boolean function $v_i\colon V^m \to \mathbb{F}_2$ defined by $v_i(x_1, x_2, \ldots, x_m) = x_i$ is called the ith **coordinate function**.

Definition: monomial, polynomial, degree

To each subset $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, m\}$ there corresponds the **monomial function** (or **monomial**) $v_{i_1} \ldots v_{i_r}$, of **degree** r.
Also, $\mathbf{1}$ is the monomial function corresponding to the set $\varnothing$, of degree 0.
A linear combination of monomials is a **polynomial**. The degree of a polynomial f is the highest degree of a monomial which appears in f.

Remark: properties of monomials.

- Observation: because the values of any Boolean function are 0 and 1, one has $v_i = v_i^2 = v_i^3 = \dots$. This is the reason why there are no higher powers of the v_i in the definition of a monomial.
- The above also implies that the product of monomials is again a monomial, and the product of polynomials is a polynomial.
- There are 2^m monomials in the Boolean algebra on V^m (because there are 2^m subsets of $\{1,\dots,m\}$).
- The weight of a monomial is calculated in the following result.

Lemma 11.1: weight of a monomial

A monomial $v_{i_1}v_{i_2}\dots v_{i_r}$ in the Boolean algebra on V^m has weight 2^{m-r}. That is,

$$w(v) = 2^{m-\deg v} \quad \text{if } v \text{ is a monomial.}$$

Proof. If $b = x_1x_2\dots x_m$ is a binary word, $v_{i_1}v_{i_2}\dots v_{i_r}(b) = 1$ if and only if $x_{i_1} = x_{i_2} = \dots = x_{i_r} = 1$. Hence the number of binary words in V^m where this monomial has value 1 is equal to the number of ways to choose the bits x_j where $j \notin \{i_1,\dots,i_r\}$. There are 2 choices (0 or 1) for each one of those $m-r$ bits, hence the total number of such binary words is 2^{m-r}, and $w(v_{i_1}\dots v_{i_r}) = \#\{b \in V^m : v_{i_1}\dots v_{i_r}(b) = 1\} = 2^{m-r}$. □

Theorem 11.2: monomial basis

Monomials form a basis of the Boolean algebra.

Proof. First, we prove by contradiction that monomials are *linearly independent*.

Assume for contradiction that a non-empty linear combination (i.e., a sum, as we are working over $\mathbb{F}_2$) of monomials equals the zero Boolean function:

$$v_{S_1} + v_{S_2} + \dots + v_{S_k} = 0, \qquad k \geq 1,$$

where $S_1, \dots S_k$ are some subsets of the index set $\{1,\dots,m\}$. Without the loss of generality, assume that v_{S_k} has the highest degree:

$$\deg v_{S_i} \leq \deg v_{S_k}, \quad \text{i.e.,} \quad \#S_i \leq \#S_k \quad \text{for all } i = 1,\dots,k-1.$$

Note that if $S, T \subseteq \{1, \ldots, m\}$ then $v_S v_T = v_{S \cup T}$. Let now $T = \{1, \ldots, m\} \setminus S_k$, the complement of the set S_k. Multiplying both sides by v_T, we obtain

$$v_{S_1 \cup T} + v_{S_2 \cup T} + \cdots + v_{S_k \cup T} = 0. \tag{$*$}$$

We have $S_k \cup T = \{1, \ldots, m\}$. If $i < k$ then the set S_i cannot contain S_k, and so $S_i \cup T \neq \{1, \ldots, m\}$ and $\deg v_{S_i \cup T} < m$. Rewrite $(*)$ as

$$v_{S_1 \cup T} + v_{S_2 \cup T} + \cdots + v_{S_{k-1} \cup T} = v_1 v_2 \ldots v_m.$$

The left-hand side is a sum of monomials of degree less than m. By Lemma 11.1, these monomials have value vectors of even weight. A sum of vectors of even weight is a vector of even weight: we know that the binary even weight code is linear. But the right-hand side is the monomial $v_1 \ldots v_m$ which by Lemma 11.1 has weight 1, which is odd. This contradiction proves that monomials are linearly independent.

It remains to show that the monomials are a *spanning set* in the Boolean algebra. There are 2^m monomials, so we can form $2^{(2^m)}$ linear combinations of monomials by putting a coefficient of 0 or 1 in front of each monomial. All these linear combinations are distinct, by linear independence. On the other hand, there are $2^{(2^m)}$ Boolean functions on V^m. Hence every Boolean function is a linear combination of monomials.

A *basis* is a set which is linearly independent and spanning, so the Theorem is proved. □

Corollary 11.3: Boolean functions are polynomials

Each Boolean function on V^m is uniquely written as a Boolean polynomial in the coordinate functions $v_1, \ldots, v_m$.

Remark: algebraic normal form. A representation of a Boolean function $f \colon V^m \to \mathbb{F}_2$ as a Boolean polynomial is sometimes referred to as the *algebraic normal form* of f. This can be compared to *disjunctive* and *conjunctive* normal forms of a Boolean function used for other purposes. Interested readers may find the details in the literature.

The Reed-Muller code

We now know that every element of the Boolean algebra on V^m is a polynomial, i.e., a sum of several monomials (squarefree products of coordinate functions). Recall also that the degree of a polynomial is the top degree of a monomial in that polynomial, which does not exceed m.

Definition: Reed-Muller code

Let $0 \le r \le m$. The **rth order Reed-Muller code on V^m**, denoted $R(r,m)$, is the space of value vectors of polynomials of degree *at most* r in the Boolean algebra on V^m.

Observe that $R(r,m)$ is spanned by the value vectors of all monomials of degree at most r.

Example: work out $R(0,m)$

Find the parameters and write down all codevectors of the Reed-Muller code $R(0,m)$.

Solution. The code $R(0,m)$ consists of value vectors of Boolean polynomials on V^m of degree ≤ 0. There are only two such polynomials, $\mathbf{0}$ and $\mathbf{1}$, hence

$$R(0,m) = \{00\ldots0, 11\ldots1\} = \mathrm{Rep}(2^m, \mathbb{F}_2)$$

is the repetition code. The length is $2^m = \#V^m$. The dimension is 1. The minimum distance equals the length. A $[2^m, 1, 2^m]_2$-code.

Example: $R(m,m)$

Show that $R(m,m) = \mathbb{F}_2^{2^m}$, the trivial binary code of length 2^m.

Solution. $R(m,m)$ consists of value vectors of polynomials on V^m of degree $\le m$. All Boolean polynomials have degree at most m, and, by Corollary 11.3, every possible binary vector of length 2^m is a value vector of some polynomial. Hence $R(m,m)$ consists of all possible binary vectors of length 2^m, i.e., is the trivial code.

The key result on Reed-Muller codes is the following theorem, which gives the parameters of these codes.

Theorem 11.4: parameters of a Reed-Muller code

$R(r,m)$ has length 2^m, dimension $\binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r}$ and minimum distance 2^{m-r}.

Proof. **Length** $= 2^m$ by construction: a value vector is made up of 2^m bits obtained by evaluating the given function on the 2^m binary words in V^m.

Value vectors of monomials of degree $0, 1, \ldots, r$ span $R(r,m)$ by definition of $R(r,m)$, and are linearly independent by Theorem 11.2, hence form a basis of $R(r,m)$. The number of monomials of degree d is the same as the number of d-element subsets of $\{1, \ldots, m\}$, which is $\binom{m}{d}$, so the total number of monomials in the basis of $R(r,m)$ — i.e., the **dimension** of $R(r,m)$ — is as stated.

Minimum distance: the code $R(r,m)$ contains monomials of degree r, for example, $v_1v_2\dots v_r$. By Lemma 11.1, these have weight 2^{m-r}. Hence $d(R(r,m)) = w(R(r,m))$ is at most 2^{m-r}.

It remains to show that $w(R(r,m)) \geq 2^{m-r}$. We do this by **induction in m.**

Base case $m=1$. According to the Examples above, the two possible codes are $R(0,1) = \mathrm{Rep}(2,\mathbb{F}_2)$ of weight $2 = 2^{1-0}$ and $R(1,1) = \mathbb{F}_2^{2^m}$ of weight $1 = 2^{1-1}$. So the inequality $w(R(r,m)) \geq 2^{m-r}$ is satisfied when $m=1$.

Inductive step. Assume $w(R(r,m-1)) \geq 2^{m-1-r}$ for all $r = 0,\dots,m-1$. This means that the weight of any non-zero polynomial of degree $\leq r$ in $v_1,\dots,v_{m-1}$ is at least 2^{m-1-r}:

$$h \neq 0,\ \deg h \leq r \quad \Longrightarrow \quad \#\{y \in V^{m-1} : h(y) = 1\} \geq 2^{m-1-r}. \qquad (\dagger)$$

The set V^m of binary words of length m splits into two subsets,

$$V^{m-1}0 = \{x_1 \dots x_m : x_m = 0\} \quad \text{and} \quad V^{m-1}1 = \{x_1 \dots x_m : x_m = 1\}$$

of words that end in 0 and words that end in 1, respectively. We need to take a polynomial $0 \neq f \colon V^m \to \mathbb{F}_2$ of degree $\leq r$ and prove that $w(f) \geq 2^{m-r}$. We have

$$w(f) = \#\{b \in V^{m-1}0 : f(b) = 1\} + \#\{b \in V^{m-1}1 : f(b) = 1\}. \qquad (\ddagger)$$

Each monomial in f contains a copy of v_m or none, so we can write

$$f = g + hv_m,$$

where g, h are polynomials in $v_1,\dots,v_{m-1}$.

The case $h = 0$. Here g is a non-zero polynomial of degree $\leq r$ in $v_1,\dots,v_{m-1}$, and so $r \leq m-1$. By ($\dagger$), there are at least 2^{m-1-r} words $y \in V^{m-1}$ where $g(y) = 1$. For each such word y we have $y0 \in V^{m-1}0$, $y1 \in V^{m-1}1$ and $f(y0) = f(y1) = 1$, and so y contributes twice when counting the weight of f in ($\ddagger$). Hence $w(f) = 2w(g)$ and so $w(f) \geq 2 \times 2^{m-1-r} = 2^{m-r}$.

The case $h \neq 0$. We note that the values of f on $V^{m-1}0$ are the same as the values of g on V^{m-1}, because $hv_m|_{V^{m-1}0} = 0$. Furthermore, the values of f on $V^{m-1}1$ are the same as the values of $g+h$ on V^{m-1}, because on $V^{m-1}1$ we have $v_m = 1$. Hence ($\ddagger$) gives $w(f) = w(g) + w(g+h)$.

By the triangle inequality, $w(\underline{a} + \underline{b}) \leq w(\underline{a}) + w(\underline{b})$ for any vectors $\underline{a}, \underline{b}$. Hence $w(g) + w(g+h) \geq w(g + (g+h)) = w(h)$. Here $\deg h \leq r-1$ because $\deg hv_m \leq r$, so the inductive hypothesis ($\dagger$) applies and gives $w(h) \geq 2^{m-1-(r-1)} = 2^{m-r}$. We proved that $w(f) \geq 2^{m-r}$, as required.

To conclude, by induction $w(R(r,m)) \geq 2^{m-r}$ for all m and all $r \leq m$. □

The key duality between Reed-Muller codes

We finish the chapter by identifying the dual code of $R(r, m)$, which happens to be another Reed-Muller code.

Theorem 11.5: duality between Reed-Muller codes

For all $m \geq 1$ and for all r such that $0 \leq r \leq m-1$,

$$R(m-1-r, m) = R(r, m)^{\perp}.$$

Proof. If $f, g \colon V^m \to \mathbb{F}_2$ are Boolean functions, the definition of inner product means that

$$\underline{f} \cdot \underline{g} = \sum_{b \in V^m} f(b)g(b) = \sum_{b \in V^m} (fg)(b).$$

If f is a monomial of degree $\leq r$ and g is a monomial of degree $\leq m-1-r$, then fg is a monomial of degree $\leq m-1$. By Lemma 11.1, there are exactly $2^{m-\deg fg}$ words $b \in V^m$ such that $(fg)(b) = 1$. Since $m - \deg fg \geq 1$, $2^{m-\deg fg}$ is an even number, and so the sum $\sum_{b \in V^m}(fg)(b)$ is zero in $\mathbb{F}_2$. This shows that f is orthogonal to g.

Since monomials f of degree $\leq r$ span $R(r, m)$, this shows that $g \in R(r, m)^{\perp}$. Thus, $R(m-1-r, m)$ is spanned by elements of $R(r, m)^{\perp}$, so $R(m-1-r, m) \subseteq R(r, m)^{\perp}$.

We will now compare the dimensions. We have $\dim R(m-1-r, m) = \binom{m}{0} + \cdots + \binom{m}{m-1-r}$. Using the relation $\binom{m}{i} = \binom{m}{m-i}$, we rewrite this as $\binom{m}{m} + \binom{m}{m-1} + \cdots + \binom{m}{r+1}$. Finally, $\dim R(m-1-r, m) + \dim R(r, m) = \sum_{i=0}^{m} \binom{m}{i} = 2^m$, the length of the Reed-Muller codes. Hence $\dim R(m-1-r, m) = 2^m - \dim R(r, m) = \dim R(r, m)^{\perp}$.

Thus, $R(r, m)^{\perp}$ contains subspace $R(m-1-r, m)$ of the same dimension as $R(r, m)^{\perp}$, hence a subset $R(m-1-r, m)$ of the same cardinality as $R(r, m)^{\perp}$. We conclude that $R(r, m)^{\perp} = R(m-1-r, m)$. □

Exercise. The code $R(m, m)$ is excluded from Theorem 11.5. How would you define "$R(-1, m)$" which should be the dual of $R(m, m)$?

Theorem 11.5 can be used to identify particular Reed-Muller codes and to deduce their further properties. Examples of this are in the exercises to this chapter.