Lecture 4
Evaluation Codes

4.1. Definition

Suppose that M is a set of "functions" which acts on a set $S = \{P_1, \ldots, P_n\}$, in the following sense: each $\phi \in M$ maps each element P_i of P to an element of $\mathbb{F}_q$. Moreover, we assume that M carries the structure of an $\mathbb{F}_q$-vector space compatible with the evaluation map, i.e., we can form linear combinations $a\phi + b\psi$ for $a, b \in \mathbb{F}_q$ and $\phi, \psi \in M$, such a combination belongs to M, and its effect on a point P_i is $a\phi(P_i) + b\psi(P_i)$.

In such a situation, we are able to construct a q-ary code of length n, which we call an *evaluation code via* $(M, S, \mathbb{F}_q)$. The exact definition is as follows: we map M to $\mathbb{F}_q^n$ via

$$\iota \colon M \to \mathbb{F}_q^n, \qquad \phi \mapsto (\phi(P_1), \ldots, \phi(P_n)). \tag{4.1}$$

The evaluation code in question is the image of this map.

Despite their appearance, evaluation codes are not peculiar, as the following simple result suggests:

Proposition 4.1. *Any linear code is an evaluation code.*

Proof. Consider a generator matrix G of an $[n, k, d]_q$-code. In this case, the vector space M will be the dual space $(\mathbb{F}_q^k)^*$ of $\mathbb{F}_q^k$, i.e., the $\mathbb{F}_q$-space of all linear forms on $\mathbb{F}_q^k$, and the set S will be the set of columns of G. The encoding of an element v of $\mathbb{F}_q^k$ is given as $v \cdot G$. Denoting by ϕ the linear form corresponding to v, the encoding of v equals $(\phi(c_1), \ldots, \phi(c_n))$. □

What can we say about the dimension and minimum distance of such a code? The answer is: essentially nothing meaningful, if we don't have an "interpretation" for M and for S. But at least we can rephrase the problem.

Proposition 4.2. *Let C be an evaluation code via $(M, S, \mathbb{F}_q)$.*

(1) *the dimension of C is $\dim_{\mathbb{F}_q}(M) - \dim_{\mathbb{F}_q}(T)$, where T is the subspace of M for which all the function disappear on all the points of S.*

(2) *Suppose that all $\phi \in M$ which do not identically disappear on S have the property that they have at most t zeros on S. Then the minimum distance of C is at least $n - t$.*

Proof. The kernel of ι from (4.1) is exactly equal to T, so the assertion on the dimension follows. The assertion on the minimum distance is trivial. □

Construction of "good" codes amounts to finding M and S such that M has many elements, points of S separate elements of M, and elements of M don't have too many zeros on S. What M and S are is anybody's best guess. A good method often uses interpretations for M and S so that the evaluation problem becomes some well-studied problem within that interpretation.

For example, remember the Hadamard codes we mentioned in one of the earlier lectures. This code is an evaluation code via $(M, S, \mathbb{F}_2)$, where M is the dual space of $\mathbb{F}_2^k$, and S is the set of all nonzero elements of $\mathbb{F}_2^k$. Any linear code

Lecture and scribes by Amin Shokrollahi

(0,	0,	0,	0,	0,	0,	0,	0)
(0,	0,	0,	1,	0,	0,	1,	1)
(0,	0,	1,	0,	0,	1,	1,	0)
(0,	1,	0,	0,	1,	1,	0,	1)
(1,	0,	0,	1,	1,	0,	1,	0)
(0,	0,	1,	1,	0,	1,	0,	1)
(0,	1,	1,	0,	1,	0,	1,	1)
(1,	1,	0,	1,	0,	1,	1,	1)
(1,	0,	1,	0,	1,	1,	1,	1)
(0,	1,	0,	1,	1,	1,	1,	0)
(1,	0,	1,	1,	1,	1,	0,	0)
(0,	1,	1,	1,	1,	0,	0,	0)
(1,	1,	1,	1,	0,	0,	0,	1)
(1,	1,	1,	0,	0,	0,	1,	0)
(1,	1,	0,	0,	0,	1,	0,	0)
(1,	0,	0,	0,	1,	0,	0,	1)

(a)

(0,	0,	0,	0,	0,	0,	0,	0)
(0,	0,	0,	1,	1,	0,	0,	1)
(0,	0,	1,	1,	0,	0,	1,	0)
(0,	0,	1,	0,	1,	0,	1,	1)
(0,	1,	1,	0,	0,	1,	0,	0)
(0,	1,	1,	1,	1,	1,	0,	1)
(0,	1,	0,	1,	0,	1,	1,	0)
(0,	1,	0,	0,	1,	1,	1,	1)
(1,	1,	0,	0,	1,	0,	0,	0)
(1,	1,	0,	1,	0,	0,	0,	1)
(1,	1,	1,	1,	1,	0,	1,	0)
(1,	1,	1,	0,	0,	0,	1,	1)
(1,	0,	1,	0,	1,	1,	0,	0)
(1,	0,	1,	1,	0,	1,	0,	1)
(1,	0,	0,	1,	1,	1,	1,	0)
(1,	0,	0,	0,	0,	1,	1,	1)

(b)

Figure 4.1: (a) The codewords of the evaluation code of Example 4.5, and (b) the codewords of the dual code

of dimension k is equivalent to a punctured version of this code. The dimension of the code is k, since a nonzero linear form cannot vanish on all elements of $\mathbb{F}_2^k$. The minimum distance of the code is 2^{k-1}, since a linear form has exactly $2^{k-1}-1$ zeros among the nonzero elements of $\mathbb{F}_2^k$.

In the next few lectures we will give ample examples of evaluation codes.

4.2. Cyclic Codes

4.2.1. Simple Evaluation Codes

In our first construction we consider M as the dual space of $\mathbb{F}_2^k$, and S as $\{1, \omega, \ldots, \omega^{n-1}\}$ in $\mathbb{F}_q$, where $q = 2^k$. If S does not contain a basis of $\mathbb{F}_q/\mathbb{F}_2$, then there will be a linear form vanishing on all the points of S, an event we would like to exclude. If S contains a basis, and $n = k$, then the evaluation code is equal to $\mathbb{F}_2^k$, hence trivial. We therefore assume that the elements of S generate $\mathbb{F}_q$ as an $\mathbb{F}_2$-space, and that $n > k$.

It is more convenient to consider the dual code of this particular evaluation code. Consider the space of all "binary relations" on S. These are the set of all binary $(a_0, \ldots, a_{n-1})$ such that $\sum_i a_i\omega^i = 0$. This vector space is the dual space of the evaluation code we are considering. In fact, if $\sum_i a_i\varphi(\omega^i) = 0$ for all linear forms φ, then by linearity $\sum_i a_i\omega^i = 0$, and vice versa.

Lemma 4.3. *Let C be the evaluation code via $(M, S, \mathbb{F}_2)$ as described above. Then $C^\perp$ is the set (of coefficients) of all binary polynomials f of degree $< n$ such that $f(\omega) = 0$. Moreover, any such polynomial is a multiple of the minimal polynomial g of ω over $\mathbb{F}_2$.*

If $\mathcal{I}$ denotes the ideal $g(x)\mathbb{F}_2[x]$, and $\mathcal{I}_{<n}$ denotes the space of polynomials in $\mathcal{I}$ of degree less than n, then this space is exactly the dual of the evaluation code. The dimension of this space is $n - \deg(g)$ (why?), so that the dimension of the evaluation code is $\deg(g)$.

As for the minimum distance, we can prove the following.

Lemma 4.4. *Suppose that any subset of S of size $n - d + 1$ contains a basis of $\mathbb{F}_q/\mathbb{F}_2$. Then the minimum distance of the evaluation code is at least d.*

Proof. Suppose that there is a nonzero word of weight $d-1$ or less. This word has at least $n - d + 1$ zeros, so there is a nonzero linear form that vanishes on a subset of S of size at least $n - d + 1$. But such a subset contains a basis, and a nonzero linear form cannot vanish on every element of a basis. This yields the desired contradiction. □

Example 4.5. Let $q = 16$, $\mathbb{F}_q = \mathbb{F}_2[x]/(f)$ with $f(x) = x^4 + x + 1$, and $\omega := x \bmod f$. The minimal polynomial of ω is by definition $x^4 + x + 1$, and hence $\mathcal{I}$ is generatd by this polynomial. The codewords of this code and the codewords of the dual code are given in Figure 4.1 As can be seen, the code and its dual are both $[8, 4, 3]_2$-codes.

4.2.2. Cyclic Codes

Suppose now that ω is an nth root of unity, i.e., $\omega^n = 1$. Then the minimal polynomial of ω is a divisor of $x^n - 1$. Let $\mathbb{F}_\ell = \mathbb{F}_2(\omega)$ be the smallest extension of $\mathbb{F}_2$ containing ω. We would like to study the evaluation code via $(M_\omega, S, \mathbb{F}_2)$, where $M_\omega = (\mathbb{F}_\ell)^*$. In this case, the evaluation map is injective, since S contains a basis of $\mathbb{F}_\ell$ (by construction).

Such evaluation codes are *cyclic*, i.e., $(c_0, \ldots, c_{n-1})$ is in the code iff $(c_{n-1}, c_0, \ldots, c_{n-2})$ is. To see this, note that if $(a_0, \ldots, a_{n-1})$ is in the dual code, then $\sum_i a_i\omega^i = 0$, so

$$0 = \omega \sum_i a_i\omega^i = \sum_i a_i\omega^{i+1} = a_{n-1} + a_0\omega + \cdots + a_{n-2}\omega^{n-1}.$$

Hence $(a_0, \ldots, a_{n-1})$ is in the dual code iff its cyclic shift is. A moment's thought reveals that therefore the original code is cyclic as well.

The evaluation codes given above are sometimes called *irreducible cyclic codes*. This means that they are cyclic, and there is no subspace of them that is cyclic (this needs a proof, of course). Moreover, it turns out that *any* cyclic code is a direct sum of such simple evaluation codes (or irreducible cyclic codes). All these facts are naturally embedded in the representation theory of finite groups (in this case: cyclic groups), but we do not have the time to touch upon this very interesting tangent.

We will now proceed by proving some useful facts about cyclic codes.

Theorem 4.6. *Let C be a cyclic code of length n. Then there is a unique monic divisor $g(x)$ of $x^n - 1$ in $\mathbb{F}_2[x]$ such that C is the set of (coefficients of) polynomials of the form $f(x)g(x) \bmod x^n - 1$.*

Conversely, for any polynomial $g(x)$ the set of polynomials $f(x)g(x) \bmod x^n - 1$ forms a cyclic code.

Proof. Identify a vector $(a_0, a_1, \ldots, a_{n-1})$ in $\mathbb{F}_2^n$ with the polynomial $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. Since C is cyclic, $a(x) \in C$ iff $xa(x) \bmod x^n - 1$ is in C. Let $g(x)$ be a monic polynomial of lowest degree in C. Then $g(x)$ divides any $a(x)$ in C: otherwise, there is $0 \neq r(x)$ of degree lower than $\deg(g)$ such that $a(x) = g(x)q(x) + r(x)$ for some polynomial $q(x)$, and hence $r(x) \in C$ since $a(x)$ and $g(x)q(x)$ are. This also shows that $g(x)$ is unique (otherwise it divides another monic polynomial of same degree, which cannot be).

The polynomial $g(x)$ also divides $x^n - 1$, since otherwise $x^n - 1 = u(x)g(x) + v(x)$ for some nonzero $u(x)$, and some $v(x)$ of degree less than $g(x)$, and hence $v(x) \in C$, contradicting the minimality of $g(x)$.

Conversely, if $C = \{f(x)g(x) \bmod x^n - 1 \bmod f(x) \in \mathbb{F}_2[x]\}$, then with any $h(x) \in C$ also $xh(x) \bmod x^n - 1$ is in C, and the code is cyclic. □

The polynomial $g(x)$ from the previous theorem is called *the generator polynomial* of the code C. Obviously, all polynomials in the code are of the form $g(x)f(x)$ with $\deg(f)$ strictly less than $n - \deg(g)$ and all such polynomials are distinct. Hence, we have

Corollary 4.7. *If C is a cyclic code with generator polynomial $g(x)$ and length n, then* $\dim(C) = n - \deg(g)$.

4.2.3. Minimum Distance of Cyclic Codes

How about the minimum distance of a cyclic code? Suppose that n is odd. Then there exists a *primitive* nth root of unity ω over $\mathbb{F}_2$. This means that $\omega^i = 1$ iff $i \equiv 0 \bmod n$. (Why?) The following theorem gives a lower bound on the minimum distance of a cyclic code given by its generator polynomial.

Theorem 4.8. *Suppose that the generator polynomial g of a cyclic code satisfies $g(\omega^i) = \cdots = g(\omega^{i+d-2}) = 0$, for some i and d. Then the minimum distance of the code is at least d.*

Proof. For simplicity we will assume that $i = 0$. The reader can verify that trivial modifications make the proof work for the case of arbitrary i. Consider the matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-2} & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-2)} & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \omega^{d-2} & \omega^{2(d-2)} & \cdots & \omega^{(d-2)(n-2)} & \omega^{(d-2)(n-1)} \end{pmatrix}.$$

Because g is the generator polynomial of C, if $x = (x_0, \ldots, x_{n-1})$ is in C, then

$$H \cdot x^\top = 0,$$

which means that the code C' (over $\mathbb{F}_q = \mathbb{F}_2(\omega)$) which has H as a check matrix contains C. Note that any $d-1$ columns of H are independent, since they form a Vandermonde matrix. Hence, the minimum distance of C' is at least d, which implies that the minimum distance of C is at least d. □

Example 4.9. (1) [Repetition code] Let n be an integer (not necessarily odd), and $g = x^{n-1} + x^{n-2} + \cdots + x + 1$. The corresponding code has dimension 1, and contains only the all-one and the all-zero codewords. It is the repetition code of length n, with minimum distance n.

(2) [Parity code] Let n be an integer, and $g = x - 1$. The corresponding code has dimension $n-1$. Any codeword is a multiple of $x-1$, and hence vanishes at 1, when considered as a polynomial. This means that the sum of all coordinates of any codeword is zero, and the code is the parity code of minimum distance 2.

(3) [Hamming code] Let $n = 7$, and $g(x) = x^3 + x + 1$. If ω is a root of g, then ω is a primitive 7th root of unity, and the other roots of g are ω^2 and ω^4. This code has dimension 4. By the previous theorem, the minimum distance of this code is at least 3. In fact, the minimum distance is exactly 3 (why?), and the code is equivalent to the $[7,4,3]_2$-Hamming code, i.e., after a possible one-time permutation of the codewords, we obtain the $[7,4,3]_2$-Hamming code.

(4) (Optimal 2-error correcting code of length 15) Let $n = 15$. The polynomial $x^{15} - 1$ has the factorization

$$x^{15} - 1 = (x-1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1).$$

Let $g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$. Let ω be a root of $x^4 + x + 1$. Then ω is a primitive 15th root of unity, and the other roots of this polynomial are ω^2, ω^4, and ω^8. The roots of $x^4 + x^3 + x^2 + x + 1$ are $\omega^3, \omega^6, \omega^9$, and ω^{12}. Hence, $g(x)$ has $\omega, \omega^2, \omega^3, \omega^4$ as its roots, so that the minimum distance of C is at least 5 (so C is 2-error correcting). The dimension of C is $15 - 8 = 7$, so C is a $[15, 7, \geq 5]_2$-code.

One can check that the minimum distance of this code is indeed 5, and that the code is optimal, in the sense that it is not possible to find a binary linear code of shorter length and same dimension and minimum distance.

4.2.4. BCH Codes

Suppose that we are given an odd length n, and a designed minimum distance d, and we are asked to construct a cyclic code of length n and minimum distance at least d. The following procedure would construct such a code using Theorem 4.8. The code obtained this way is called a BCH-code, named after its inventors Bose, Ray-Chaudhuri, and Hocquenghem.

To construct the code, we first factor the polynomial $x^n - 1$ over $\mathbb{F}_2$. Let ω denote a primitive nth root of unity over $\mathbb{F}_2$. Then each of these factors has a set of zeros of the form $\{\omega^{i_1}, \ldots, \omega^{i_t}\}$, if the factor is of degree t. Next, we multiply factors together so that the resulting product has a "consecutive" set of roots, i.e., a subset of roots of the form $\{\omega^i, \omega^{i+1}, \ldots, \omega^{i+d-2}\}$. Then Theorem 4.8 implies that the minimum distance of the code is at least d. Of course, while combining the factors of $x^n - 1$, we need to ensure that we combine a minimum number of such factors so as to obtain the consecutive set of zeros. This can be at times challenging, with the problems compounded by the fact that the root of unity ω can be replaced by any other primitive nth root of unity, thereby adding to the challenge of checking whether a particular combination of factors is good.

We will learn how to decode such BCH codes in the next lecture.

4.3. Weight Distribution of Irreducible Cyclic Codes

The weight distribution of irreducible cyclic codes has astonishing relationships to other areas of mathematics, most notably, algebraic geometry. In this section, we will describe one such connection. We will only sketch the proofs, and leave the detailed presentation to the exercises. To fix the notation, we let ω be a primitive nth root of unity over $\mathbb{F}_2$, and let $\mathbb{F}_{2^k} = \mathbb{F}_2(\omega)$. Throughout this section, we denote by C_n the simple evaluation code via $(M, S, \mathbb{F}_2)$, where M is the dual space of $\mathbb{F}_{2^k}$, and $S = \{1, \ldots, \omega^{n-1}\}$.

Starting point of our journey is the trace map. Recall that the trace of $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$ of an element $\alpha \in \mathbb{F}_{2^k}$ is $\mathrm{Tr}(\alpha) = \alpha + \alpha^2 + \cdots + \alpha^{2^{k-1}}$.

Lemma 4.10. *Let φ be a linear form of $\mathbb{F}_{2^k}$ as an $\mathbb{F}_2$-space. Then there is an $\alpha \in \mathbb{F}_{2^k}$ such that for all $x \in \mathbb{F}_{2^k}$, we have $\varphi(x) = \mathrm{Tr}(\alpha x)$.*

Proof. (Sketch) It is easy to show that $\mathrm{Tr}(\alpha x)$ and $\mathrm{Tr}(\beta x)$ are different linear forms on $\mathbb{F}_{2^k}$ if α and β are different. Hence, the set of all $\mathrm{Tr}(\alpha x)$ coincides with the set of all linear forms of $\mathbb{F}_{2^k}$. □

Lemma 4.11. *If an element $\alpha \in \mathbb{F}_{2^k}$ has trace zero, then there exists $\beta \in \mathbb{F}_{2^k}$ such that $\alpha = \beta^2 - \beta$.*

Proof. (Sketch) The map $\beta \mapsto \beta^2 - \beta$ is a linear map of $\mathbb{F}_{2^k}$. Moreover, its image is clearly contained in the space of elements of trace 0. Being a quadratic polynomial over a field, it is at most 2-to-1, so its image has at least 2^{k-1} elements. Hence, its image is the set of elements of trace 0. □

Lemma 4.12.

$$C_n = \{(\mathrm{Tr}(\alpha), \mathrm{Tr}(\alpha\omega), \ldots, \mathrm{Tr}(\alpha\omega^{n-1})) \mid \alpha \in \mathbb{F}_{2^k}\}.$$

Proof. Follows from the two previous lemmas. □

Proposition 4.13. *Notations being as in the previous lemma, let $m = (2^k - 1)/n$, and let N_α denote the number of $\mathbb{F}_{2^k}$-solutions of the equation $\alpha x^m = y^2 - y$ for which $x \neq 0$. Then the weight distribution of C_n is*

$$\sum_{\alpha \in \mathbb{F}_{2^k}} x^{n - N_\alpha/2m} y^{N_\alpha/2m}.$$

Proof. The number of zeros of the vector $(\mathrm{Tr}(\alpha), \mathrm{Tr}(\alpha\omega), \ldots, \mathrm{Tr}(\alpha\omega^{n-1}))$ is the number of times $\mathrm{Tr}(\alpha\omega^i)$ is zero, i.e., the number of i such that there exists y with $\alpha\omega^i = y^2 - y$, or equivalently, the number of i such that there exists y with $\alpha(\tau^i)^m = y^2 - y$, where τ is a primitive element of $\mathbb{F}_{2^k}$. □

The equation $\alpha x^m = y^2 - y$ describes a *curve* over the field $\mathbb{F}_{2^k}$. There is an area of algebraic geometry which studies the number of points of curves over finite fields. We will briefly touch upon this area later in the class.

Example 4.14. (1) (Hadamard codes) Let k be a positive integer, and $n = 2^k - 1$. Then $m = 1$, and we need to look at the solution of the equation $\alpha x = y^2 - y$. For any nonzero α, the number of solutions of this equation with $x \neq 0$ is $2 \cdot (2^{k-1} - 1)$. Hence, the weight of the corresponding codeword is 2^{k-1}. The code in question is nothing but the Hadamard code.

(2) (Lower bounds from elliptic cuves) Let $n = 21$. Then $k = 6$, i.e., the smallest extension of $\mathbb{F}_2$ containing a primitive 21st root of unity is $\mathbb{F}_{2^6} = \mathbb{F}_{64}$. In this case $m = (2^k - 1)/n = 3$, and the weight distribution of the irreducible cyclic code C_{21} is associated with the number of points of the curve $\alpha x^3 = y^2 - y$, for which $\neq 0$. The case $x = 0$ gives two points, so we need to subtract 2 from the total number of points. This curve is called an *elliptic curve* if $\alpha \neq 0$. By a general theorem from algebraic geometry, the number of points of such a curve cannot exceed $63 + 2 \cdot 8 = 79$. As a result, a nonzero codeword in C_{21} has at least $21 - 77/6$ nonzero positions, which means that the weight of a nonzero codeword in C_{21} has weight at least 8. This makes the code a $[21, 6, \geq 8]_2$-code. Using the Griesmer bound (or checking Andries Brouwer's tables) shows that this code is optimal. (This result also could have been obtained differently, for example using Theorem 4.8.) On the other hand, the number of points of an elliptic curve over $\mathbb{F}_{64}$ cannot be less than $63 - 2 \cdot 8 = 47$, so a codeword in C_{21} cannot have weight more than $21 - 47/6$, i.e., more than 13. In fact, an inspection yields that this code has only weights 0,8, and 12.

4.4. Reed-Muller Codes

In this case M consists of m-variate polynomial functions with total degree $\leq r$, and S consists of $\mathbb{F}_2^m$. This means that we can assume the local degree of the polynomials in M in each of the variables to be at most 1. The action of the polynomials on the elements of $\mathbb{F}_2^m$ is through evaluation. This code is called a *Reed-Muller code of order* r, denoted $\mathcal{R}(r, m)$. Obviously we can assume that $r \leq m$.

Whyshould this give a reasonable code? This is because polynomials of bounded degree tend to have few zeros. More precisely, we have the following:

Lemma 4.15. *A nonzero m-variate polynomial in $\mathbb{F}_2[X_1, \ldots, X_m]$ of total degree $\leq r \leq m$ has at most $2^m - 2^{m-r}$ zeros. In particular, the minimum distance of $\mathcal{R}(r, m)$ is 2^{m-r}.*

Proof. The proof proceeds by induction on m. For $m = 1$ the assertion is obvious. Let us prove the assertion for $m + 1$, assuming its correctness for m.

Let f denote the polynomial in question, and let r denote its degree. We have

$$f(x_1, \ldots, x_{m+1}) = \sum_{\ell=0}^{r} x_{m+1}^\ell Q_\ell(x_1, \ldots, x_m).$$

The evaluation of f is equal to the sum of the evaluations of the $x_{m+1}^{\ell} Q_\ell(x_1, \ldots, x_m)$. If $\ell > 0$, then this polynomial vanishes on all points with $x_{m+1} = 0$, and its evaluation is equal to that of Q_ℓ on the complementary set of points. The evaluation of Q_0 on both these sets is the same. Hence, the evaluation of f can be written as $(u|u+v)$, where u is the evaluation of an m-variate polynomial of degree $\leq r$ and v is the evaluation of an m-variate polynomial of degree $< r$. The induction hypothesis applies to both u and v, and implies that the weight of u is at least 2^{m-r} if u is nonzero, and the weight of v is at least 2^{m-r+1} if v is nonzero. If $u = 0$ and $v \neq 0$, the weight of $(u|u+v)$ is thus at least 2^{m-r+1}. If $u \neq 0$ and $u + v = 0$, then $u = v$ and the weight of $(u|u+v)$ is at least 2^{m-r+1}. If $u \neq 0$ and $u + v \neq 0$, then the weights of u and $u + v$ are at least 2^{m-r} each, and hence the weight of $(u|u+v)$ is at least 2^{m-r+1}.

The second part of the theorem follows, since the polynomial $x_1 \cdots x_r$ has only 2^{m-r} nonzero evaluations (take $x_1 = \cdots = x_r = 1$, and the other x_i arbitrary). □

What about the dimension of $\mathcal{R}(r, m)$? An m-variate polynomial that vanishes on all the points of the $\mathbb{F}_2^m$ must be the zero polynomial (proof?) Hence, the dimension of $\mathcal{R}(r, m)$ is the dimension of the space of polynomials of degree $\leq r$, which is

$$\sum_{i=0}^{r} \binom{m}{i}.$$

How about asymptotic properties of these codes? It is easily seen that the rate is (for large r and m)

$$R \sim 2^{m(h(r/m)-1)},$$

and the relative distance (i.e., minimum distance dvided by the length) is 2^{-r}. The relative distance goes to zero if we let r go to infinity. If we let m go to infinity, and keep r fixed, then the relative distance is bounded from below, but the dimension will be polynomial in m, while the length is exponential in m, so that the rate goes to zero as $\log(N)^c/N$, where N is the block length, and c is some constant (depending on r).

Hence, asymptotically, these codes are not very good.