ITC — Lecture 2 of week 10

The two main goals are:

(1) describe the isomorphisms $\mathbb{F}_{q^m} \xrightarrow{\cong} \mathbb{F}_q^m$ (already used in decoding concatenate codes).

(2) use those isomorphisms (and Reed-Solomons codes) to decode Reed-Muller codes — we'll only do the low degree case and binary case, as in last lecture.

Recomended reading: parts of appendix D and parts of section 3 of chapter 13 in the book.

More on Finite Fields (continuation of the notes of week 7)

Let q be a power of a prime number p. Let $\mathbb{F}_q$ be a field with q elements. $\mathbb{F}$ will denote any field, finite or not. We define the characteristic of a field $\mathbb{F}$ by

$$\operatorname{char} \mathbb{F} \stackrel{\text{def}}{=} \begin{cases} \min\{ n \in \mathbb{N}_1 \mid \underbrace{\sum_{i=1}^{n} 1}_{\text{operations done in } \mathbb{F} \text{ where } 1 \in \mathbb{F} \text{ is the identity}} = 0 \} & \text{if the minimum exists} \\ 0 & \text{otherwise} \end{cases}$$

(the 0 in the set is this is the zero $0 \in \mathbb{F}$)

i.e. we are considering the map $\varphi : \mathbb{Z} \to \mathbb{F}$ s.t. $\varphi(0) = 0$, $\varphi(1) = 1$, and preserves $+$ and $\cdot$. So we must have

$$n = \underbrace{\sum_{i=1}^{n} 1}_{\text{in } \mathbb{Z}} \longmapsto^{\varphi} \underbrace{\sum_{i=1}^{n} 1}_{\text{in } \mathbb{F}}$$

The $\operatorname{char}(\mathbb{F})$ is the smallest positive integer n such that $\varphi(n) = 0$ (if such n exists), 0 otherwise.

Example
- $\mathbb{R}$ and $\mathbb{C}$ have characteristic 0
- $\mathbb{Z}_p$ has characteristic p.

Exercise: Show that, if $\mathbb{F}$ is a <u>finite</u> field, then

(1) the minimum in the definition of characteristic exists and is a prime number p

(2) the map $\varphi: \mathbb{Z} \longrightarrow \mathbb{F}$ defined above induces an <u>injective</u> map $\tilde{\varphi}: \mathbb{Z}_p \longrightarrow \mathbb{F}$ s.t. $\tilde{\varphi}$ preserves the field structure.

The image $\tilde{\varphi}(\mathbb{Z}_p)$ is the unique copy of $\mathbb{Z}_p$ inside $\mathbb{F}$. I'll simply write $\mathbb{Z}_p \subseteq \mathbb{F}$ (or $\mathbb{F}_p \subseteq \mathbb{F}$) without refering to φ or $\tilde{\varphi}$.

The map φ also gives a meaning to $n\alpha$, where $n \in \mathbb{Z}$ and $\alpha \in \mathbb{F}$, that is, we define $n\alpha \overset{\text{def}}{=} \varphi(n)\alpha$ (product in $\mathbb{Z}$ or $\mathbb{F}$? — product in $\mathbb{F}$)

Prop 1 For every $x, y \in \mathbb{F}_q$, we have:

(1) $(x+y)^p = x^p + y^p$

(2) $(x+y)^{p^i} = x^{p^i} + y^{p^i}$, $\forall\, i \geqslant 1$

In particular, we also have $(x+y)^{q^i} = x^{q^i} + y^{q^i}$ for all $x, y \in \mathbb{F}_q$ and $i \geqslant 1$, because q is a power of p.

Pf: (1) $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$ (*) ($\binom{p}{i} \in \mathbb{N}$, $x, y \in \mathbb{F}_q$ and operations done in $\mathbb{F}_q$)

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p \times (p-1)!}{i!\,(p-i)!}$$

If $0 < i < p$, then all factors of $i!$ and $(p-i)!$ are $< p$ so none of them is a factor $\neq 1$ of p (because p is prime) and so

$$\binom{p}{i} = p \times \underbrace{\frac{(p-1)!}{i!\,(p-i)!}}_{\in \mathbb{Z}} \equiv 0 \pmod{p}$$

and the only non-zero coefficients in (*) are $\binom{p}{0} = 1$ and $\binom{p}{p} = 1$.

(2) Exercise: use induction on i and part (1)

∎

Prop 2 For any $x \in \mathbb{F}_q$, $x^q = x$.

Pf by cases

$x=0$: trivial

$x \neq 0$: want to show that $x^{q-1} = 1$.

Let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} = \{y_1, y_2, \dots, y_{q-1}\}$ ⊛

Since $x \neq 0$, multiplying by x still gives $xy_i \neq 0$, and $xy_i \neq xy_j$ if $i \neq j$. So

$$\mathbb{F}_q^* = \{xy_1, xy_2, \dots, xy_{q-1}\} \quad ⊛⊛$$

⊛ and ⊛⊛ $\Rightarrow (xy_1)(xy_2)\cdots(xy_{q-1}) = y_1 y_2 \cdots y_{q-1}$

$\Leftrightarrow x^{q-1} \underbrace{y_1 y_2 \cdots y_{q-1}}_{\in \mathbb{F}_q^*} = y_1 y_2 \cdots y_{q-1}$

$\Leftrightarrow x^{q-1} = 1$

∎

Prop 2 says that any element of $\mathbb{F}_q$ is a root of the polynomial $X^q - X \in \mathbb{F}_q[X]$, i.e., this polynomial of degree q has at least q roots, therefore

$$X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha). \quad ⊛_3$$

The coefficients of $X^q - X$ are 1 and -1 (elements of any field!) so we can also regard $X^q - X$ as a polynomial in $\mathbb{F}_{q^m}[X]$ and ⊛$_3$ tells us how to find the unique copy of $\mathbb{F}_q$ inside $\mathbb{F}_{q^m}$ (for any $m \geq 1$):

> The elements of $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ are the roots of $X^q - X \in \mathbb{F}_{q^m}[X]$

Or, equivalently, given $\alpha \in \mathbb{F}_{q^m}$, we test if $\alpha \in \mathbb{F}_q (\subseteq \mathbb{F}_{q^m})$ by checking if α is a root of $X^q - X$, i.e., by checking if $\alpha^q = \alpha$.

Recall that $\mathbb{F}_{q^m}$ (with its $+, \cdot$ operations) has a natural structure of vector space over $\mathbb{F}_q$ (because $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^m}$). We will now give a description of the linear functions $\mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ over $\mathbb{F}_q$, i.e., regarding both $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$ as vector spaces over $\mathbb{F}_q$.

Given $x \in \mathbb{F}_{q^m}$, define the trace of x by

$$\boxed{Tr(x) \stackrel{\text{def}}{=} x + x^q + x^{q^2} + \cdots + x^{q^{m-1}} = \sum_{i=0}^{m-1} x^{q^i}}$$

using the operations in $\mathbb{F}_{q^m}$ (where x belongs).

Prop 3 For any $x, y \in \mathbb{F}_{q^m}$ and $\alpha \in \mathbb{F}_q$ we have

(1) $Tr(x) \in \mathbb{F}_q$ (not just $\mathbb{F}_{q^m}$!)

(2) $Tr(x+y) = Tr(x) + Tr(y)$

(3) $Tr(\alpha x) = \alpha\, Tr(x)$

(4) $\exists\, x \in \mathbb{F}_{q^m}$ s.t. $Tr(x) \neq 0$

As a consequence, the trace function $Tr: \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ is

- well-defined (by (1)),
- linear over $\mathbb{F}_q$ (by (2) and (3)), and
- surjective and $|Tr(\alpha)^{-1}| = q^{m-1}$ $\forall \alpha \in \mathbb{F}_q$ (by linearity and (4))

$Tr: \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ $\mathbb{F}_q$-linear

$\Rightarrow$ $Im(Tr)$ is a $\mathbb{F}_q$-subspace of $\mathbb{F}_q$

$\Rightarrow$ $Im(Tr) = \{0\}$ or $Im(Tr) = \mathbb{F}_q$

(4) $\Rightarrow$ $Im(Tr) \neq \{0\}$ so it must be $Im(Tr) = \mathbb{F}_q$

therefore Tr is surjective. Also, because Tr is linear and surjective, $|Tr(\alpha)^{-1}| = |\ker(Tr)| = q^{m-1}$ $\forall \alpha \in \mathbb{F}_q$.

Example $\mathbb{F}_4 = \mathbb{F}_2[X]/\langle X^2+X+1\rangle = \{a_0 + a_1\alpha : a_0, a_1 \in \mathbb{F}_2\} = \{0, 1, \alpha, 1+\alpha\}$
where $\alpha \in \mathbb{F}_4$ is a root of X^2+X+1, i.e., $\alpha^2 = \alpha+1$.

$Tr : \mathbb{F}_4 \longrightarrow \mathbb{F}_2$, $Tr(x) = x + x^2$ by definition.

- $Tr(1) = 1 + 1^2 = 0$ (both $\mathbb{F}_4$ and $\mathbb{F}_2$ have characteristic 2)
- $Tr(\alpha) = \alpha + \alpha^2 = 1$ ← $\alpha^2 = \alpha + 1$
- $Tr(1+\alpha) = Tr(1) + Tr(\alpha) = 0 + 1 = 1$ ⊛
  ↑ linearity over $\mathbb{F}_2$

Note that it's NOT true that $Tr(\alpha) \overset{\checkmark}{=} Tr(\alpha \cdot 1) \overset{\times}{=} \alpha\, Tr(1)$
($\alpha \in \mathbb{F}_4$ but $\alpha \notin \mathbb{F}_2$ and Tr is linear over $\mathbb{F}_2$ not $\mathbb{F}_4$)
From $\mathbb{F}_4 = \{a_0 + a_1\alpha : a_0, a_1 \in \mathbb{F}_2\}$ we can see that $\{1, \alpha\}$ is a basis of $\mathbb{F}_4$ as a $\mathbb{F}_2$-vector space, and the trace function can be computed knowing only $Tr(1)$ and $Tr(\alpha)$ as it was done in ⊛. (This observation is more relevant for larger $\mathbb{F}_{q^m}$.)
For a generic $\mathbb{F}_2$-linear map $L : \mathbb{F}_4 \longrightarrow \mathbb{F}_2$, we can do the same: $L(a_0 + a_1\alpha) = a_0 L(1) + a_1 L(\alpha) = \begin{bmatrix} L(1) & L(\alpha) \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$ ⊛⊛
↑ $\mathbb{F}_2$-linearity

Different choices for $(L(1), L(\alpha)) \in \mathbb{F}_2 \times \mathbb{F}_2$ define different linear maps $\mathbb{F}_4 \longrightarrow \mathbb{F}_2$ (exercise), thus there are 4 linear maps over $\mathbb{F}_2$, including the zero map.

Exercise: Generalize for $\mathbb{F}_q$-linear maps $L : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ and conclude that the set

$$\mathcal{L} = \{ L : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q \mid L \text{ is } \mathbb{F}_q\text{-linear} \}$$

contains exactly q^m elements.

$\mathbb{F}_{q^m} = \mathbb{F}_q[X]/P(X)$ where $P(X) \in \mathbb{F}_q[X]$ is an irreducible polynomial of degree m. Let $\alpha \in \mathbb{F}_{q^m}$ be a root of $P(X)$. Then $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a basis for $\mathbb{F}_{q^m}$ (or choose any other basis) and we can define a linear map $L \in \mathcal{L}$ as in ⊛⊛

Proof of Prop 3:

(1) By definition, $Tr(x) \in \mathbb{F}_{q^m}$.

An element $y \in \mathbb{F}_{q^m}$ is in $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ iff y is a root of the polynomial $X^q - X$. So we need to check that $(Tr(x))^q = Tr(x)$.

$$(Tr(x))^q = \left(\sum_{i=0}^{m-1} x^{q^i}\right)^q = \sum_{i=0}^{m-1} \left(x^{q^i}\right)^q = x^q + x^{q^2} + \cdots + x^{q^{m-1}} + x^{q^m}$$

(def of $Tr(x)$ ↑, Prop 1 ↑)

$$= x^q + x^{q^2} + \cdots + x^{q^{m-1}} + 1 = Tr(x)$$

($x \in \mathbb{F}_{q^m} \Rightarrow x^{q^m} = x$ by Prop 2)

(2) $$Tr(x+y) = \sum_{i=0}^{m-1} (x+y)^{q^i} = \sum_{i=0}^{m-1} \left(x^{q^i} + y^{q^i}\right) = \sum_{i=0}^{m-1} x^{q^i} + \sum_{i=0}^{m-1} y^{q^i}$$

(def of Tr ↑, Prop 1 ↑)

$$= Tr(x) + Tr(y)$$

(3) $$Tr(\alpha x) = \sum_{i=0}^{m-1} (\alpha x)^{q^i} = \sum_{i=0}^{m-1} \alpha^{q^i} x^{q^i} = \sum_{i=0}^{m-1} \alpha x^{q^i}$$

(Prop 2 ↓: $\alpha \in \mathbb{F}_q \Rightarrow \alpha^q = \alpha \Rightarrow \alpha^{q^i} = \alpha \quad \forall i \geq 0$, ↑)

$$= \alpha \sum_{i=0}^{m-1} x^{q^i} = \alpha\, Tr(x)$$

(4) By definition $Tr(x)$ is a polynomial on x of degree q^{m-1}, so it has at most q^{m-1} roots.

$\ker(Tr) = \{x \in \mathbb{F}_{q^m} \mid Tr(x) = 0\} = \{\text{roots of } Tr\}$

$\Rightarrow |\ker(Tr)| \leq q^{m-1} < q^m = |\mathbb{F}_{q^m}|$

$\Rightarrow \exists\, x \in \mathbb{F}_{q^m}$ s.t. $x \notin \ker(Tr)$.

∎

Prop 4 A map $L: \mathbb{F}_q^m \longrightarrow \mathbb{F}_q$ is linear over $\mathbb{F}_q$ iff there is $\lambda \in \mathbb{F}_q^m$ s.t. $L(x) = Tr(\lambda x)$ for any $x \in \mathbb{F}_q^m$.

Pf: ($\Leftarrow$) We need to show that $x \longmapsto Tr(\lambda x)$ is linear over $\mathbb{F}_q$ for any (fixed) $\lambda \in \mathbb{F}_q^m$, i.e., we need to show that

(i) $Tr(\lambda(x+y)) = Tr(\lambda x) + Tr(\lambda y) \quad \forall x, y \in \mathbb{F}_q^m$

and

(ii) $Tr(\lambda(\alpha x)) = \alpha\, Tr(\lambda x) \quad \forall x \in \mathbb{F}_q^m$ and $\forall \alpha \in \mathbb{F}_q$

But (i) and (ii) are just a consequence of the $\mathbb{F}_q$-linearity of the trace function.

($\Rightarrow$) Let $f_\lambda(x) = Tr(\lambda x)$. Then $f_\lambda: \mathbb{F}_q^m \longrightarrow \mathbb{F}_q$ is an $\mathbb{F}_q$-linear function and, as a polynomial in x, it has degree q^{m-1} if $\lambda \neq 0$. So $f_\lambda \neq 0$ for any $\lambda \in \mathbb{F}_q^{m\,*}$. Also, if $\lambda \neq \zeta$, then $f_\lambda \neq f_\zeta$ by a similar argument:

$$(f_\lambda - f_\zeta)(x) = Tr(\lambda x) - Tr(\zeta x) \underset{\text{linearity of } Tr}{=} Tr(\lambda x - \zeta x) = f_{\lambda-\zeta}(x)$$

$$\lambda \neq \zeta \Rightarrow f_{\lambda-\zeta} \not\equiv 0$$

$\therefore$ We have q^m distinct linear functions $f_\lambda: \mathbb{F}_q^m \longrightarrow \mathbb{F}_q$ (*)

By a previous exercise,

$$|\mathcal{L}| = |\{ L: \mathbb{F}_q^m \longrightarrow \mathbb{F}_q \mid L \text{ is } \mathbb{F}_q\text{-linear} \}| = q^m \quad (**)$$

(*) and (**) $\Rightarrow \mathcal{L} = \{ f_\lambda \mid \lambda \in \mathbb{F}_q^m \}$

∎

Note: In the above proof, we only need the inequality $|\mathcal{L}| \leq |\mathbb{F}_q^m|$ in (**).

Next we will use this nice characterization of $\mathbb{F}_q$-linear functions given by Prop. 4 to describe the isomorphisms $\mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q^m$ of $\mathbb{F}_q$-vector spaces.

Any $\mathbb{F}_q$-linear function $\Phi : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q^m$ can be viewed as $\Phi(x) = (\Phi_1(x), \dots, \Phi_m(x))$ where $\Phi_i : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ is an $\mathbb{F}_q$-linear function, for each $1 \le i \le m$.

Prop 5 An $\mathbb{F}_q$-linear function $\Phi : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q^m$ is an isomorphism iff $\Phi = (\Phi_1, \dots, \Phi_m)$ where, for each $1 \le i \le m$, there is $\lambda_i \in \mathbb{F}_{q^m}$ s.t. $\Phi_i(x) = \mathrm{Tr}(\lambda_i x)$ and $\lambda_1, \dots, \lambda_m$ are linearly independent over $\mathbb{F}_q$.

Pf: By proposition 4, a function $\Phi : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q^m$ is linear iff $\Phi = (\Phi_1, \dots, \Phi_m)$ where $\Phi_i(x) = \mathrm{Tr}(\lambda_i x)$, for $1 \le i \le m$. We need to prove that the linear function Φ is bijective iff $\lambda_1, \dots, \lambda_m$ are linearly independent over $\mathbb{F}_q$.

Recall that $\mathrm{Im}\,\Phi = \{\Phi(x) \mid x \in \mathbb{F}_{q^m}\}$ is a subspace of $\mathbb{F}_q^m$. Recall also that $\dim S^\perp = m - \dim S$ for any subspace $S \subseteq \mathbb{F}_q^m$, and so Φ is surjective iff $(\mathrm{Im}\,\Phi)^\perp = \{0\}$.

Let $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{F}_q^m$. Let $\boxed{\tau = \alpha_1 \lambda_1 + \cdots + \alpha_m \lambda_m}$

For any $x \in \mathbb{F}_{q^m}$ we have:

$$\mathrm{Tr}(\tau x) = \mathrm{Tr}\left(\sum_{i=1}^m \alpha_i \lambda_i x\right) = \sum_{i=1}^m \alpha_i \mathrm{Tr}(\lambda_i x) = \sum_{i=1}^m \alpha_i \Phi_i(x) \quad (*)$$

$$= \langle \alpha, \Phi(x) \rangle$$

($\uparrow$ Tr is $\mathbb{F}_q$-linear and $\alpha_i \in \mathbb{F}_q$)

So

$\lambda_1, \dots, \lambda_m$ are <u>not</u> linearly independent

$\Leftrightarrow$ there is $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{F}_q^m \setminus \{0\}$ s.t. $0 = \alpha_1\lambda_1 + \dots + \alpha_m\lambda_m = 0$

$\Leftrightarrow$ $\mathrm{Tr}(\alpha x) = 0 \quad \forall x \in \mathbb{F}_{q^m}$

↑ as in proof of Prop 4

$\Leftrightarrow$ $\langle \alpha, \Phi(x) \rangle = 0 \quad \forall x \in \mathbb{F}_q^m \Leftrightarrow \alpha \in (\mathrm{Im}\,\Phi)^\perp \neq \{0\}$

↑ by $\circledast$ ↑ by definition of $(\mathrm{Im}\,\Phi)^\perp$

$\Leftrightarrow$ Φ is <u>not</u> surjective $\Leftrightarrow$ Φ is <u>not</u> bijective ∎

↑ $|\text{domain}| = |\mathbb{F}_q^m| = q^m = |\mathbb{F}_q^m| = |\text{range}|$

<u>Example</u> $\mathbb{F}_4 = \{a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{F}_2\}$ with $\alpha^2 = \alpha + 1$

Given this description of $\mathbb{F}_4$, the "obvious" isomorphism of $\mathbb{F}_2$-vector spaces between $\mathbb{F}_4$ and $\mathbb{F}_2 \times \mathbb{F}_2$ is

$$\Phi : \mathbb{F}_4 \longrightarrow \mathbb{F}_2^2, \quad \Phi(a_0 + a_1\alpha) = (a_0, a_1) \qquad \circledast$$

which amonts to sending the elements in the basis $\{1, \alpha\}$ of $\mathbb{F}_4$ to the elements of the basis $\{(1,0), (0,1)\}$ of $\mathbb{F}_2^2$.

To compute $\Phi(x)$ for an arbitrary $x \in \mathbb{F}_{2^2}$ ($x \in \mathbb{F}_{q^m}$ in a general case) using $\circledast$, first we need to write x as a linear combination of $1, \alpha$ (easy in $\mathbb{F}_4$, maybe not so easy in a larger $\mathbb{F}_{q^m}$). Using prop 5 (or even just prop 4 for each of the Φ_i), we get a "closed form" for Φ in terms of the trace function and fixed $\lambda_1, \lambda_2 \in \mathbb{F}_4$.

For the function Φ in $\circledast$ we get, for any $x \in \mathbb{F}_4$,

$$\Phi_1(x) = \mathrm{Tr}(\alpha^2 x) = \alpha^2 x + \alpha x^2$$

$$\Phi_2(x) = \mathrm{Tr}(x) = x + x^2$$

↑ Exercise

$\rightsquigarrow$ $\lambda_1 = \alpha^2$ and $\lambda_2 = 1$, which are l. ind. as we were expecting (by prop 5)

Back to Reed-Muller and Reed Solomon Codes

Example Consider the Reed-Muller code (separate degrees ≤ 1)

$$RM(\underset{q}{2},\underset{m}{3},\underset{r}{1}) = \{ f \in \mathbb{F}_2[X_1, X_2, X_3] \mid \deg f \leq 1 \}$$

with parameters $[2^m, \sum_{i=0}^{m} \binom{m}{i}, 2^{m-r}]_2 = [8, 4, 4]_2$.

A generic $f \in RM(2,3,1)$ is of the form

$$f(X_1, X_2, X_3) = f_0 + f_1 X_1 + f_2 X_2 + f_3 X_3, \text{ with } f_i \in \mathbb{F}_2$$

$\mathbb{F}_{2^m} = \mathbb{F}_8 = \mathbb{F}_2[X] / X^3 + X + 1$ and let $\alpha \in \mathbb{F}_8$ be a root of $X^3 + X + 1$, i.e. $\alpha^3 = \alpha + 1$

$\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{F}_8$ as a vector space over $\mathbb{F}_2$.

By prop 5, $\Phi(z) = (Tr(z), Tr(\alpha z), Tr(\alpha^2 z))$ defines an isomorphism $\Phi : \mathbb{F}_8 \longrightarrow \mathbb{F}_2^3$ over $\mathbb{F}_2$.

Note that each of the functions $Tr(z)$, $Tr(\alpha z)$ and $Tr(\alpha^2 z)$ are polynomials of degree $2^{m-1} = 4$ in z

If we take the composite $f \circ \Phi$ we also get a polynomial of degree at most 4 and coefficients in $\mathbb{F}_8$.

$$f \circ \Phi(z) = f_0 + f_1 Tr(z) + f_2 Tr(\alpha z) + f_3 Tr(\alpha^2 z)$$

$$\equiv f_0 + (f_1 + \alpha f_2 + \alpha^2 f_3) z + (f_1 + \alpha^2 f_2 + \alpha^4 f_3) z^2 + (f_1 + \alpha^4 f_2 + \alpha f_3) z^4$$

$Tr(z) = z + z^2 + z^4$
$Tr(\alpha z) = \alpha z + \alpha^2 z^2 + \alpha^4 z^4$
$Tr(\alpha^2 z) = \alpha^2 z + \alpha^4 z^2 + \alpha z^4$

I.e., $f \circ \Phi \in \mathbb{F}_8[z]$ with $\deg(f \circ \Phi) \leq 4$. If we evaluate $P \overset{def}{=} f \circ \Phi$ at all points of $\mathbb{F}_8$, we get a codeword of a Reed-Solomon code over $\mathbb{F}_8$ with dimension $k = 4 + 1$ and block length 8, i.e. a RS code with parameter $[8, 5, 4]_8$, and we can use the decoding algorithm for the RS code to decode our initial RM code.

In the previous example, it's a case of low degree polynomials in the RM code $(r=1<q=2)$. In general, it's not easy to determine the maximum possible degree of $f\circ\Phi$ (which will give the dimension of the RS code) since, for higher degree polynomials, we need to reduce modulo $z^{q^m}-z$ because, when evaluating $P(z)\in\mathbb{F}_{q^m}[z]$ at a point $\alpha\in\mathbb{F}_{q^m}$, all terms α^N in $P(\alpha)$ with $N\geq q^m$ become terms α^N with $N<q^m$ because

$$\boxed{x^{q^m}=x \quad \forall\ x\in\mathbb{F}_{q^m}}$$

Example Consider the code $RM(\overset{q}{2},\overset{m}{3},\overset{r}{2})$ and

$$f(X_1,X_2,X_3)=X_1X_2 \in \mathbb{F}_2[X_1,X_2,X_3]$$

$\deg f=2=r$ and $\deg_{X_i} f\leq 1=q-1$ ✓

Consider the same isomorphism $\Phi:\mathbb{F}_8\longrightarrow\mathbb{F}_2^3$ from the previous example and take the composite $f\circ\Phi$:

$$\begin{aligned}P(z)=f\circ\Phi(z)&=\mathrm{Tr}(z)\,\mathrm{Tr}(\alpha z)\\&=(z+z^2+z^4)(\alpha z+\alpha^2 z^2+\alpha^4 z^4)\\&=\alpha z^2+\cdots+(\alpha^4+\alpha^2)z^6+z^8\\&=1+\alpha z^2+\cdots+(\alpha^4+\alpha^2)z^6 \quad \bmod z^8-z\end{aligned}$$

because $z^8=z$ if $z\in\mathbb{F}_8$

The $f\in RM$ with $\deg f=2$ becomes a $P\in RS$ with $\deg P=6\neq 8=(\deg f)\times\deg(\mathrm{Tr})$.

Note that $(P(x))_{x\in\mathbb{F}_8}$ is a codeword of a RS code with parameters $[z^m,K,D]_{2^m}=[8,K,D]_8$ so we must have $\deg P\leq K-1<8$. Note also that if $K=N=8$ then $D=1\rightsquigarrow$ no error correction or error detection capabilities!

We want the smallest possible K so that D is larger.

So we want an upper bound on $\deg(f\circ\Phi \bmod z^{q^m}-z)$.

The general setting:

Def Given a prime power q, non-negative integers m and r, define $\boxed{R_{q,m}(r)}$ to be the maximum of $\deg(f \circ \Phi)$ over all polynomial functions $f: \mathbb{F}_q^m \to \mathbb{F}_q$ with $\deg(f) \leq r$ and over all $\mathbb{F}_q$-linear isomorphisms $\Phi: \mathbb{F}_{q^m} \to \mathbb{F}_q^m$

Note: $f: \mathbb{F}_q^m \to \mathbb{F}_q$ and $\Phi: \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ give $f \circ \Phi: \mathbb{F}_{q^m} \to \mathbb{F}_q$, but $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$, so also get a function $\mathbb{F}_{q^m} \xrightarrow{\Phi} \mathbb{F}_q^m \xrightarrow{f} \mathbb{F}_q \xrightarrow{\text{inclusion}} \mathbb{F}_{q^m}$ which we also denote by $f \circ \Phi$. The degree of these functions $\mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ is the degree of the polynomial $P \in \mathbb{F}_{q^m}[z]$ with $\deg(P) < q^m$ s.t. $P(x) = f \circ \Phi(x)$ $\forall x \in \mathbb{F}_{q^m}$ That's why we were reducing modulo $z^{q^m} - z$ in the previous example.

Consider a Reed-Muller code

$$RM(m,q,r) = \{f: \mathbb{F}_q^m \to \mathbb{F}_q \mid \deg f \leq r, \text{ separate degree} \leq q-1\}$$

Let $\Phi: \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ be an $\mathbb{F}_q$-linear isomorphism.
For the same m, q, r, consider the Reed-Solomon code over $\mathbb{F}_{q^m}$ with evaluation points $\mathbb{F}_{q^m}$:

$$\mathcal{C} = \{(P(x))_{x \in \mathbb{F}_{q^m}} \mid P \in \mathbb{F}_{q^m}[z], \deg P \leq R_{q,m}(r)\}$$

$\mathcal{C}$ is a $[q^m, R_{q,m}(r)+1, q^m - R_{q,m}(r)]_{q^m}$ code and, in particular, $\mathcal{C}$ and $RM(m,q,r)$ have the same block length.

We will now determine $R_{m,q}(r)$ for the cases we have already computed the parameters of $RM(m,q,r)$.

The low-degree case ($r < q$)

Prop If $r < q$, then $R_{q,m}(r) = r \cdot q^{m-1}$.

Pf Let $f \in \mathbb{F}_q[X_1, \ldots, X_m]$ with $\deg(f) \leq r$ and let $\underline{\Phi} = (\Phi_1, \ldots, \Phi_m)$ be an $\mathbb{F}_q$-linear isomorphism. Since each Φ_i is a polynomial degree q^{m-1} (by prop 5), then $\deg(f \circ \underline{\Phi}) \leq r \cdot q^{m-1} < q^m$ and reduction modulo $z^{q^m} - z$ gives the same degree.

$\therefore R_{q,m}(r) \leq r \cdot q^{m-1}$.

Now we need to show that $R_{q,m}(r) \geq r \cdot q^{m-1}$.

To do that consider $f(X_1, \ldots, X_m) = \prod_{a \in S} (X_1 - a)$, where $S \subseteq \mathbb{F}_q$ is a set containing $|S| = r < q$ elements. Then $P(z) = f \circ \underline{\Phi} = \prod_{a \in S} (\Phi_1(z) - a)$ where $\Phi_1(z) = \mathrm{Tr}(\lambda_1 z)$.

To get a lower bound on the degree of a polynomial $P \in \mathbb{F}_{q^m}[z]$ we count its roots:

$x \in \mathbb{F}_{q^m}$ is a root of $P(z)$ iff $\prod_{a \in S} (\mathrm{Tr}(\lambda_1 x) - a) = 0$

iff $\mathrm{Tr}(\lambda_1 x) = a$ for some $a \in S$

this equation (with $a \in S$ fixed) has q^{m-1} different solutions by Prop 3

there are $|S| = r$ different a's

$\Rightarrow P(z)$ has $r \times q^{m-1}$ roots $\Rightarrow R_{q,m}(r) \geq \deg P \geq r q^{m-1}$ ∎

Recall that, if $r < q$, $RM(q,m,r)$ is a $\left[q^m, \binom{m+r}{r}, q^m\left(1 - \frac{r}{q}\right)\right]_q$ code. By this proposition, $\mathcal{C}$ is a $\left[q^m, r q^{m-1} + 1, q^m\left(1 - \frac{r}{q}\right)\right]_{q^m}$. They have the same minimum distance!

So we can use a decoder for $\mathcal{C}$ which corrects up to $\frac{1}{2} d_H(\mathcal{C})$ many errors to decode $RM(q,m,r)$ up to $\frac{1}{2}$ of its minimum distance.

The binary case ($q=2$)

Consider a $RM(2,m,r)$ code (with $r \le m$).

If $f \in \mathbb{F}_2[X_1,\dots,X_m]$ has $\deg(f) \le r$ and $\deg_{X_i}(f) \le 1 \ (= q-1)$ then

$$f(X_1,\dots,X_m) = \sum_{\substack{S \subseteq \{1,\dots,m\} \\ |S| \le r}} f_S X_S \quad \text{where } f_S \in \mathbb{F}_2 \text{ and } X_S = \prod_{i \in S} X_i$$

Let $\Phi = (\Phi_1,\dots,\Phi_m) : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_2^m$ be an $\mathbb{F}_2$-linear isomorphism.

To get the degree of $f \circ \Phi$ (modulo $z^{2^m} - z$) we can analyze separately what happens to each of the monomials X_S after composing with Φ. W.l.o.g., assume $S = \{1,\dots,s\}$, where $s \le r$, that is, assume $X_S = X_1 X_2 \cdots X_s$, with $s \le r$, and let $f = X_S$.

For the case $s=2$:

$$f \circ \Phi(z) = \Phi_1(z)\,\Phi_2(z) = \mathrm{Tr}(\lambda_1 z)\,\mathrm{Tr}(\lambda_2 z) \overset{\text{def of trace function}}{=}$$

$$= \left(\sum_{i=0}^{m-1} \lambda_1^{2^i} z^{2^i}\right)\left(\sum_{j=0}^{m-1} \lambda_2^{2^j} z^{2^j}\right)$$

$$= \sum_{i,j=0}^{m-1} \left(\lambda_1^{q^i} \lambda_2^{q^j} z^{2^i + 2^j}\right) \quad (*)$$

If $i=j$, then $z^{2^i+2^i} = z^{2^{i+1}}$ has degree 2^{i+1}. If $2^{i+1} \ge 2^m$, it will be reduced modulo $2^m - 1$ to some degree $< 2^m$.

If $i \ne j$, then $z^{2^i+2^j}$ has degree $2^i + 2^j \le 2^{m-2} + 2^{m-1} < 2^m$ and reduction modulo $2^m - 1$ does nothing.

So, what's the highest possible degree in z we can get in $(*)$ after reducing modulo $z^{2^m} - z$?

Since the degree of the monomials in z are sums of powers of 2 with at most two summands, the answer is $2^{m-2} + 2^{m-1}$

Now we want to generalize for $2 \leq s \leq r$. One way of doing it is to consider the degrees d written in base 2:

$$d = \sum_{i \geq 0} d_i 2^i \quad (d_i \in \{0,1\}) \longrightarrow \cdots d_i \cdots d_1 d_0 \text{ in base 2}$$

($\sum_{i \geq 0} d_i 2^i$: a sum of powers of 2 as in $\circledast$)

Since $d < 2^m$ (after reducing the polynomial modulo $z^{2^m} - z$), or since $d \leq 2^m - 1 = 1 + 2 + 2^2 + \cdots + 2^{m-1}$, we want d written in base 2 with m bits $d_i \in \{0,1\}$ with at most r bits 1. The largest possible d corresponds to

$$\underbrace{1 \cdots 1}_{r} \underbrace{0 \cdots 0}_{m-r} \text{ in base 2}$$

$$\Rightarrow d = 2^{m-1} + 2^{m-2} + \cdots + 2^{m-r} = 2^{m-r}\left(\sum_{i=0}^{r-1} 2^i\right) =$$

$$= 2^{m-r} \times (2^r - 1) = 2^m - 2^{m-r}.$$

This suggests that $R_{2,m}(r) \leq 2^m - 2^{m-r}$.

To show that $R_{2,m}(r) \geq 2^m - 2^{m-r}$, we do as in the low-degree case choosing just one specific f and count its roots. Let $f(X_1, \ldots, X_m) = X_1 \cdots X_r$ (recall that $r \leq m$). Then $a = (a_1, \ldots, a_m) \in \mathbb{F}_2^m$ is a "non-root" of $f: \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$ iff

$$f(a_1, \ldots, a_m) = 1 \iff a_1 \cdots a_r = 1$$

$$\iff \begin{cases} a_1 = \cdots = a_r = 1 \\ \text{and } a_{r+1}, \ldots, a_m \in \mathbb{F}_2 \end{cases}$$

(2^{m-r} total choices)

So f has $2^m - 2^{m-r}$ roots. Since Φ is bijective and $x \in \mathbb{F}_{2^m}$ is a root of $f \circ \Phi$ iff $\Phi(x) \in \mathbb{F}_2^m$ is a root of f, $f \circ \Phi$ also has $2^m - 2^{m-r}$ roots.

$$\Rightarrow R_{2,m}(r) \geq \deg(f \circ \Phi) \geq 2^m - 2^{m-r}.$$

Prof $R_{2,m}(r) = 2^m - 2^{m-r}$

(For a rigorous proof, read section 13.3.2 in the book.)

$RM(2,m,r)$ is a $\left[2^m, \sum_{i=0}^{r}\binom{m}{i}, 2^{m-r}\right]_2$ code

The "best" RS code which contains all $f \circ \Phi$ for $f \in RM(2,m,r)$ (and $\Phi: \mathbb{F}_{2^m} \xrightarrow{\cong} \mathbb{F}_2^m$ fixed) is the code $\mathcal{C}$ with parameters

$$\left[2^m, R_{2,m}(r)+1, 2^m - R_{2,m}(r)\right]_{2^m} = \left[2^m, 2^m - 2^{m-r}+1, 2^{m-r}\right]_{2^m}$$

(by prop.)

The same minimum distance!

As in the low degree case, we can use $\mathcal{C}$ to decode $RM(2,m,r)$ up to $\frac{1}{2} \times 2^{m-r}$ many errors.