$\mathcal{R}$**??**
$F_q q q = 2 F = \{0,1\}$ *xor and*
$F n F^n$**??**
$n F_2 F_2^n \mathbf{v} = (1,0,1,1,0,1,0,1) \in F_2^8 \mathbf{v} 10110101$
xor $+ \oplus F_2$
$[n,k,d] C$ *codewords* n
$\mathbf{uv}$ *Hamming Distance*

$$wt(x) = d(x,0) = \{ {1 if x \neq 0 \atop 0 if x = 0} \tag{1}$$

$d(x,y) = wt(x-y) wt(x+y) = wt(x) + wt(y) - 2wt(x*y) x*y = (x_1y_1, x_2y_2, \ldots, x_ny_n)$
$(x_1, x_2, \ldots, x_m) \in F^m \mathbf{x} \equiv (x_1, x_2, \ldots, x_m) f f : F^{2^m} \to \{0,1\} f(\mathbf{x}) = f(x_1, x_2, \ldots, x_m) m 0 1$
$\mathbf{x} 2^m \mathbf{x} f(\mathbf{x})$ *truth-table* $x_1, x_2, x_3 f(x_1, x_2, x_3)$

$x_1 00001111$
$x_2 00110011$
$x_3 01010101$
$f\ 00011000$

$(x_1, x_2, \ldots, x_m) 2^m \mathbf{f} n = 2^m F_2 2^{2m} 2^{2m} 2^m$
$f f x_1, x_2, \ldots, x_m f = x_1 \vee x_2 \vee x_3 \ldots$**?** $f =$
${}_1, x_2, {}^m$
F_2
1

$$1 + a_1 x_1 + a_{2x} 2 + \ldots + a_n x_n \tag{2}$$

m mr

$$\mathcal{R}(r,m) = \{\mathbf{f} : degree(f(x_1, \ldots, x_m)) = r\} \tag{3}$$

$m r r_1, v_2, \ldots, v_m, v_1v_2, v_1v_3, \ldots, v_1v_m, ldots, v_1v_2..v_m{}^m$
$0 2^m - 1$
$f m - ary 2^m \mathbf{f} 2^m \mathbf{f} x_1, x_2, ldots, x_m 2^m$
?
$n = 2^m d = 2^{m-r} k = 1 + ..$
$[n,k] k/n n k k$
$\mathcal{R}(1,m) u_0 1 + \sum_{i=1}^m u_i \mathbf{v_i} u_i = 0 1$ *orthogonal code* $\prime_m [2m, m, 2m1] \sum_{i=1}^m u_i \mathbf{v_i} \mathcal{R}(1,m)_m (\mathbf{1} + \mathcal{O}_m)$
$[2^m, m+1, 2^m]$**?**
?

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

This is known as the concatenation construction of codes, with $|$ denoting the concatenation. We use the boolean logic definition of the codewords. Let $\mathbf{f} \in \mathcal{R}(r+1,m+1)$. $\mathbf{f}$ can be written as $f(v_1, v_2, \ldots, v_{m+1}) = g(v_1, v_2, \ldots, v_m) + v_{m+1} h((v_1, v_2, \ldots, v_m)$ Where $\mathbf{g} \in \mathcal{R}(r+1,m)$ and $\mathbf{h} \in \mathcal{R}(r,m)$. Consider the associated vectors $\mathbf{f}, \mathbf{g}', \mathbf{h}'$ as polynomials over $v_1, \ldots, v_{m+1}$. Then, $\mathbf{g}' = (\mathbf{g}|\mathbf{g})$ and $\mathbf{h}' = (\mathbf{0}|\mathbf{h})$. [Problem7, [0].] Thus **f = g—g + 0—h**

$$G(r+1, m+1) = (\, G \,)\, (r+1,m) G(r+1,m) 0 G(r,m) \tag{4}$$

$$G(1, m+1) = (\, G \,)\, (1,m) G(1,m) 0 1 \tag{5}$$

Theorem 2 *Minimum distance, $d = 2^{m-r}$ Proof:...*
$\mathcal{R}(0,m) \mathcal{R}(m,m) m$
${}_1 = (\,1\,)\, 1$
00
10
01
$R_{n+1} = (\, R \,)_n\, R_n$
$R_n neg R_n$

Theorem 3 $\mathcal{R}(r,m) \subset \mathcal{R}(t,m) if 0 \leq r \leq t \leq m$

*By Induction. Trivially true for $m = 1$. Let $\mathcal{R}(k, m-1) \subset \mathcal{R}(l, m-1)$ for all $0 \leq k \leq l < m$. Let $0 < i \leq j < m$. By the recursive definition, we get: $\mathcal{R}(i,m)$=$\{$(**u**,**u**+**v** — **u** $\in \mathcal{R}(i, m-1), \mathbf{v} \in \mathcal{R}(i-1, m-1)\}$ Induction hypothesis gives :*
$\subset \{(\mathbf{u}, \mathbf{u}+\mathbf{v} | \mathbf{u} \in \mathcal{R}(j, m-1), \mathbf{v} \in \mathcal{R}(j-1, m-1)\} = \mathcal{R}(j,m)$

$$dim(\mathcal{R}(r,m)) = dim(\mathcal{R}(r,m-1)) + dim(\mathcal{R}(r-1,m-1)) \tag{6}$$

Theorem 4

(7)

Theorem 5 $\mathcal{R}(m-r-1, m)$ *is the dual code of* $\mathcal{R}(r,m)$
We induct on r. Let $0 \leq i \leq r$. Inductively, assume that $\mathcal{R}(i, m-1)^{\perp} = \mathcal{R}(m-i-2, m-1)$

Theorem 6 $\mathcal{R}(m-2, m)$ *is the extended binary hamming code*

Theorem 7 *Let C_i be an $[n, k_i, d_i]$ code. Then the concatenated code defined by*
*$C = \{$(**u**,**u**+**v**) — **u** $\in C_1, \mathbf{v} \in C_2\}$*
has the parameters $[2n, k_1 + k_2, min 2d_1, d_2]$ linear code. Length: *Clearly, since length of C_1 and C_2 is n each, concatenating produces vectors of length $2n$.*

Dimension: *The number of words in C is product of number of words in C_1 and C_2. because $(c_1, c_2) \to (c_1, c_1 + c_2)$ is a bijection. Thus, the dimension is $k = k_1 + k_2$*

Distance: *We can split this into cases, depending on whether $c_1 = \mathbf{0}$ or $c_2 = \mathbf{0}$.*
Case: $\mathbf{c_2} = \mathbf{0}$ $wt((c_1, c_1 + c_2)) = wt(c_1, c_1) = 2wt(c_1) = 2d_1$
Case: $\mathbf{c_2} \neq \mathbf{0} wt((c_1, c_1 + c_2)) = wt(c_1) + wt(c_1 + c_2) \geq wt(c_1) + wt(c_2) - wt(c_1) = wt(c_2) = d_2$

Thus, the minimum distance of the code, which is equal to the weight of the minimum weight vector is $min 2d_1, d_2$

Lemma 1 *Every codeword in $\mathcal{R}(1,m)$ (except $\mathbf{1}, \mathbf{0}$) has weight 2^{m-1} This can also be proved by using the randomization lemma for boolean functions as done in [0]. However, if we notice that $\mathcal{R}(1,m) = \{(u,u) : u \in \mathcal{R}(1, m-1)\} \cup \{(u, \vec{1}+u) : u \in \mathcal{R}(1, m-1)\}$. We use induction on m and are done.*

$i - tha_i l$

$$l + a_i \geq d'$$

$_i + a_j \geq d'(9)$
$\sum_{i=1}^{J} a_i \leq n - l \geq Jd'$
$\geq J2d' \leq 2n/d' - 1$
$\mathcal{R}(r,m) m_{i_1,i_2,\ldots,i_k} correspondingtothebasisvectors v_{i_1} v_{i_2} \ldots v_{ik}$
$STS j_1 j_{2m-k} = 1, 2, ldots, m - i_1, i_2, \ldots, i_k.T$
Translate
$m_{bb} = \sum_{P \in U_i} x_P i = 1, 2, \ldots, 2^{m-r}$
??
$of abinary vector \mathbf{V} isavector with replaced by and by.$

Lemma 2 *The Orthogonal code* $\mathcal{O}_m$ *with real vectors is equivalent to the Hadamard matrix* H_m. *Let the elements of this real-vectorized orthogonal code be* v.

Claim 1 $v_i, v_j \in \mathcal{R}(1,m) v_i \cdot v_j = 0$ *The systematic choice of the basis vectors helps. We use the recursive definition of the Generator matrix.*
This is the definition of the hadamard matrix too.

$$\mathcal{R}(1,m) = (\ H\ )_m - H_m \tag{10}$$

$FH_m \mathbf{v} n O(n^2)$*Fast Hadamard Transform* $O(nlogn)$
Green Machine
$C\mathbf{u} \in F_q^n e > 0 v C(u,v) \leq eT$**?**
????$\mathcal{R}(1,m) n(\frac{1}{2} - \epsilon) O(n\epsilon^3) \frac{n}{4}$**??**$O(nlogn)$
$\mathbf{y} L_\epsilon(y) = \{f \in \mathcal{R}(1,m) : d(\mathbf{y}, \mathbf{f}) \leq n(\frac{1}{2} - \epsilon)\} i L_\epsilon^i(y) i f(x1, ..., xm) = f0 + f1x1 + ... + fmxmL(y)$
$c(i)(x1, ..., xm) = c1x1 + ... + cixiim$
$Cd \geq (1/2 - \epsilon)$

$$\forall u \in F_q^n |\{v \in C : \Delta(u,v) \leq (1/2 - \sqrt{\epsilon})\}| leq 1/\epsilon$$

?
?$\mathcal{R}(1,m)$
?
?
?