Weighted Reed-Muller codes revisited

Olav Geil
(joint with Casper Thomsen)

Aalborg University
Denmark

CAACT , EPFL 2011

A class of affine variety codes

Pointensemble:

$$T = S_1 \times \cdots \times S_m = \{P_1, \ldots, P_{|T|}\}, \qquad S_1, \ldots, S_m \subseteq \mathbb{F}_q.$$

Monomials:

$$\mathcal{M} \subseteq \{X_1^{i_1} \cdots X_m^{i_m} \mid i_1 < |S_1|, \ldots, i_m < |S_m|\}$$

Code:

$$E(\mathcal{M}, T) = \mathrm{Span}_{\mathbb{F}_q}\{\big(M(P_1), \ldots, M(P_{|T|})\big) \mid M \in \mathcal{M}\}$$

Parameters:
Dimension equals $|\mathcal{M}|$. Minimum distance: apply footprint bound.

q-ary Reed-Muller codes

Pointensemble:

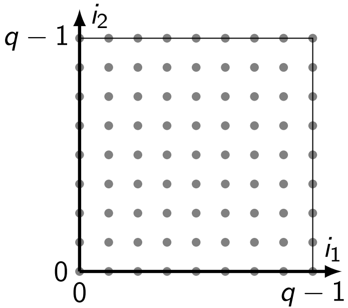
$$T = \mathbb{F}_q \times \cdots \times \mathbb{F}_q$$

Monomials:

$$\mathcal{M} = \{X_1^{i_1} \cdots X_m^{i_m} \mid i_1, \ldots, i_m < q, i_1 + \cdots + i_m \leq s\}$$

Code:

$$E(\mathcal{M}, T) = \mathrm{RM}_q(s, m)$$



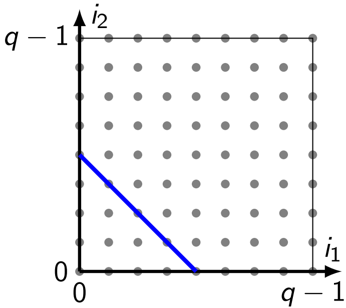
q-ary Reed-Muller codes

Pointensemble:

$$T = \mathbb{F}_q \times \cdots \times \mathbb{F}_q$$

Monomials:

$$\mathcal{M} = \{X_1^{i_1} \cdots X_m^{i_m} \mid i_1, \ldots, i_m < q, i_1 + \cdots + i_m \leq s\}$$



Code:

$$E(\mathcal{M}, T) = \mathrm{RM}_q(s, m)$$

q-ary Reed-Muller codes

Pointensemble:

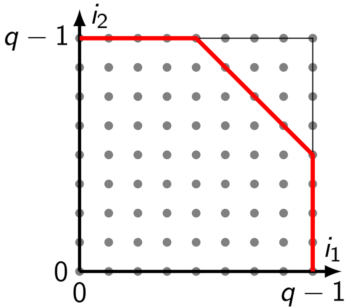
$$T = \mathbb{F}_q \times \cdots \times \mathbb{F}_q$$

Monomials:

$$\mathcal{M} = \{X_1^{i_1} \cdots X_m^{i_m} \mid i_1, \ldots, i_m < q, i_1 + \cdots + i_m \leq s\}$$

Code:

$$E(\mathcal{M}, T) = \mathrm{RM}_q(s, m)$$



Minimum distance of q-ary RM-code

$$I = \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$$

$$\vec{c} = \big(F(P_1), \ldots, F(P_n)\big)$$

$$J = I + \langle F(X_1, \ldots, X_m) \rangle$$

$$\Delta_{\prec}(J) = \{M \text{ a monomial} \mid M \text{ is not leading of any polynomial in } J\}$$

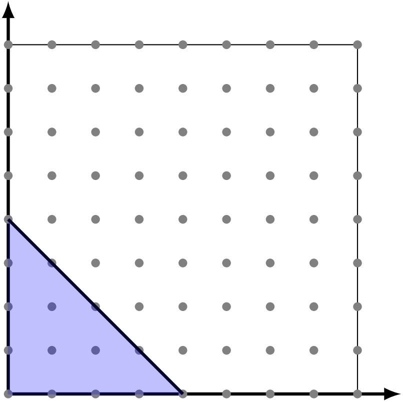
Footprintbound: $w_H(\vec{c}) = n - \#\Delta_{\prec}(J)$

Use: $X_1^{i_1} \cdots X_m^{i_m} F(X_1, \ldots, X_m) \in J$

Minimum distance of q-ary RM-code

Parameters of $\mathrm{RM}_9(4, 2)$:

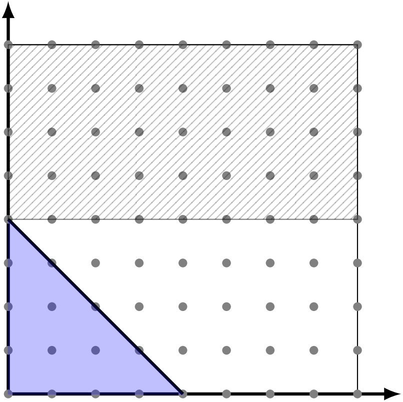
- $k = 15$
- $d = 45$



Minimum distance of q-ary RM-code

Parameters of $RM_9(4, 2)$:

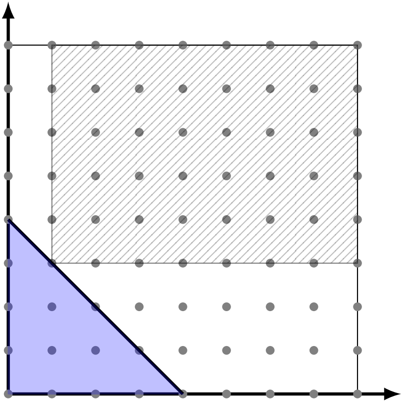
- $k = 15$
- $d = 45$



Minimum distance of q-ary RM-code

Parameters of $RM_9(4,2)$:

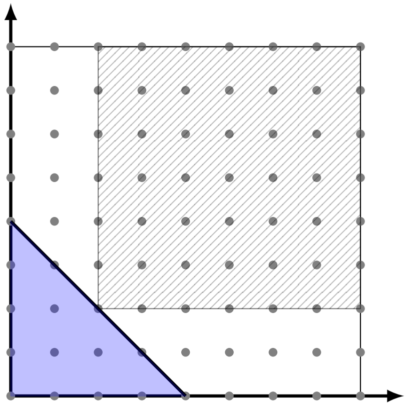
- $k = 15$
- $d = 45$



Minimum distance of q-ary RM-code

Parameters of $\mathrm{RM}_9(4,2)$:

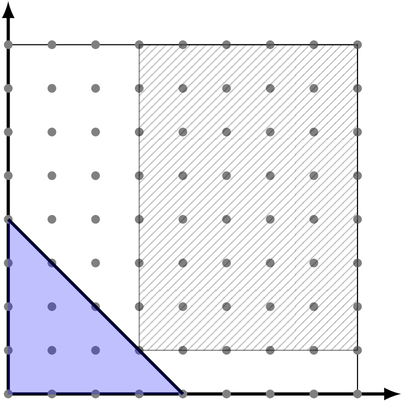
- $k = 15$
- $d = 45$



Minimum distance of q-ary RM-code

Parameters of $RM_9(4,2)$:

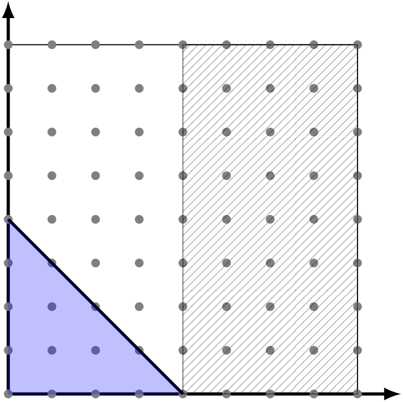
- $k = 15$
- $d = 45$



Minimum distance of q-ary RM-code

Parameters of $\mathrm{RM}_9(4,2)$:

- $k = 15$
- $d = 45$



Shorter codes - Strategy I

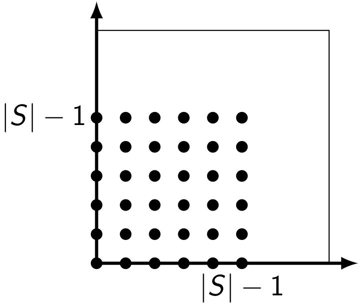
$S = \{\alpha_1, \ldots, \alpha_{|S|}\} \subsetneq \mathbb{F}_q$

$T = S \times \cdots \times S$

$I = \langle \prod_{j=1}^{|S|}(X_i - \alpha_j), i = 1, \ldots, m \rangle$

$\mathcal{M} = \{X_1^{i_1} \cdots X_m^{i_m} \mid i_k < |S|, \deg(M) \leq s\}$

$E(\mathcal{M}, T) = \mathrm{RM}_T(s, m)$



Shorter codes - Strategy I

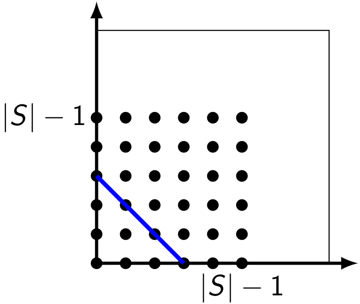
$S = \{\alpha_1, \dots, \alpha_{|S|}\} \subsetneq \mathbb{F}_q$

$T = S \times \cdots \times S$

$I = \langle \prod_{j=1}^{|S|} (X_i - \alpha_j), i = 1, \dots, m \rangle$

$\mathcal{M} = \{X_1^{i_1} \cdots X_m^{i_m} \mid i_k < |S|, \deg(M) \leq s\}$

$E(\mathcal{M}, T) = \mathrm{RM}_T(s, m)$



Shorter codes - Strategy I

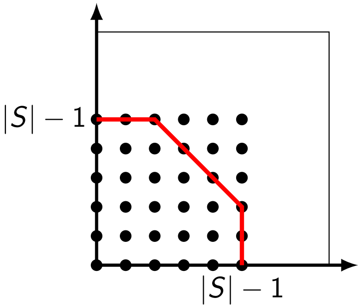
$S = \{\alpha_1, \ldots, \alpha_{|S|}\} \subsetneq \mathbb{F}_q$

$T = S \times \cdots \times S$

$I = \langle \prod_{j=1}^{|S|} (X_i - \alpha_j), i = 1, \ldots, m \rangle$

$\mathcal{M} = \{X_1^{i_1} \cdots X_m^{i_m} \mid i_k < |S|, \deg(M) \leq s\}$

$E(\mathcal{M}, T) = \mathrm{RM}_T(s, m)$



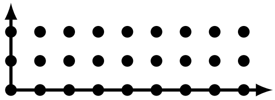
Shorter codes - strategy II

Add curve equation(s)

Example:

$$I = \langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle$$

- The extra relation lowers the size of footprint.
- Basis is no longer quadratic.

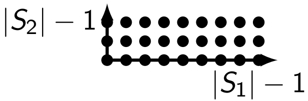


Shorter codes - strategy III

Good curves are difficult to find.

Question:

What can be said from the shape of the basis alone?



$$S_1 = \{\alpha_1, \ldots, \alpha_{|S_1|}\}$$

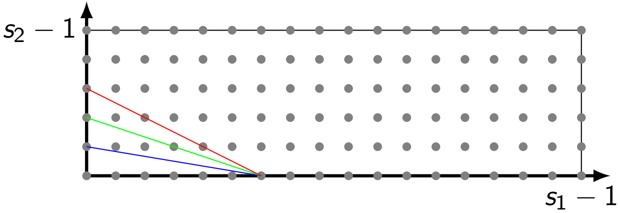
$$S_2 = \{\alpha_1, \ldots, \alpha_{|S_2|}\}$$

$$I = \left\langle \prod_{i=1}^{|S_1|}(X-\alpha_i), \prod_{j=1}^{|S_2|}(Y-\alpha_j) \right\rangle$$

Weighted Reed-Muller codes

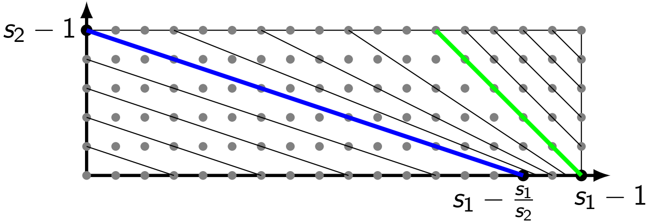
$$T = S_1 \times \cdots \times S_m$$

$$\mathcal{M} = \{X_1^{i_1} \cdots X_m^{i_m} \mid i_1 < |S_1|, \ldots, i_m < |S_m|, \\ w_1 i_1 + \cdots + w_m i_m \leq s\}$$



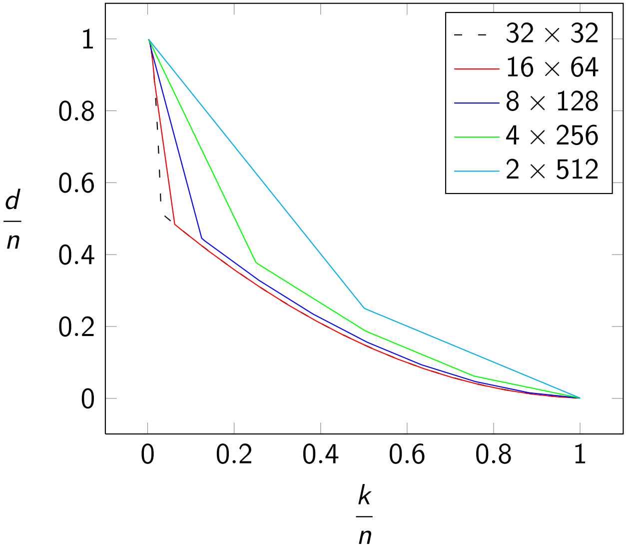
Optimal weighted Reed-Muller codes

For the case of two variables, the situation falls in three regions.



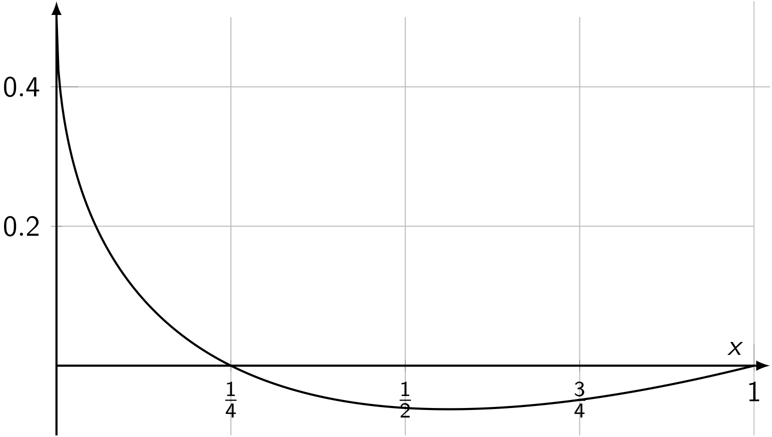
Optimal choices of weights are such that $\mathcal{M}$ is as in figure.

The effect of flattening



Region I

Relative improvement of k/n when d/n is fixed. A function in $x = |S_2|/|S_1|$.



Decoding of $E(\mathcal{M}, T)$

- Strategy A: Subfield subcode decoding following approach by Pellikaan-Wu and Santhi.
- Strategy B: Direct implementation of Guruswami-Sudan decoding with a preperation step.

Subfield subcode decoding

$t = \max\{\deg(M) \mid M \in \mathcal{M}\}$

Decoding radius: $\lceil n(1 - \sqrt{\frac{tq^{m-1}+1}{n}})\rceil$.

Example: Joyner code. $T = \mathbb{F}_8^* \times \mathbb{F}_8^*$.
$\mathcal{M} = \{1\} \cup \{X^iY^j \mid 1 \leq i,j \ \text{ and } \ i+j \leq 5\}$

Parameters: $[49, 11, 28]$.

Subfield subcode decoding with a trick can correct as follows

m	1	2	3	4	5	6
errors	12	20	24	27	29	31

Guruswami-Sudan decoding of RS-codes

$T = \{x_1, \ldots, x_n\} \subseteq \mathbb{F}_q$, $\mathcal{M} = \{1, X, \ldots, X^{k-1}\}$.

Received word $\vec{r} = (r_1, \ldots, r_n)$.

To correct E errors:

Find $Q(X,Y) = Q_0(X) + Q_1(X)Y + \cdots + Q_s(X)Y^s$ such that

- All (x_i, r_i) are zeros of multiplicity $\geq r$.
- $Q(X, F(X))$ cannot have $n - E$ zeros of multiplicity $\geq r$ for any $F(X) \in \mathrm{Span}_{\mathbb{F}_q}(\mathcal{M})$.

List decoding of $E(\mathcal{M}, T)$

$T = S_1 \times \cdots \times S_m = \{P_1, \ldots, P_n\}$. $\mathcal{M}$ is any specified set of monomials.

Find nonzero $Q(X_1, \ldots, X_m, Y)$ such that

- Any (P_i, r_i) is a zero of multiplicity $\geq r$.
- $Q(X_1, \ldots, X_m, F(X_1, \ldots, X_m))$ cannot have $n - E$ zeros of multiplicity $\geq r$ for any $F(X_1, \ldots, X_m) \in \mathrm{Span}_{\mathbb{F}_q}(\mathcal{M})$.

Using only information on total degree

Monomials are allowed in the support of $Q_i(X_1, \ldots, X_m)$ if of degree lower than some value.

- Pellikaan Wu: $\mathrm{RM}_q(s, m)$. Tool: generalized footprintbound.
- Augot et al.: $\mathrm{RM}_T(s, m)$ (improved) and Reed-Solomon product codes. Tool: Schwartz-Zippel bound with multiplicity.

Using full information on monomial

Bounds in terms of $(i_1, \ldots, i_m)$ rather than in terms of deg.

G-Matsumoto used this approach for order domain codes, but could not deal with multiplicity.

Order domain codes includes one-point geometric Goppa codes, Weighted Reed-Muller codes and many more.

A closer analysis of Dvir, Kopparty, Saraf and Sudan's proof of the Schwartz-Zippel bound with muliplicity allows for improved information...and thereby improved decoding of $E(\mathcal{M}, T)$

However, strongly non-linear and not even symmetric. A recursive function D. Closed formula estimates for two variables.

Therefore, at preperation step is needed to find optimal E and corresponding monomials that are allowed in $Q_0, \ldots, Q_s$.

Table 1: Maximal improvements relative to q^m; truncated.

m		2				3				4	
r		2	3	4	5	2	3	4	5	2	3
	2	0.25	0.25	0.25	0.25	0.25	0.375	0.375	0.375	0.312	0.375
	3	0.222	0.222	0.222	0.222	0.296	0.296	0.296	0.296	0.296	0.333
	4	0.187	0.187	0.187	0.187	0.281	0.25	0.25	0.265	0.316	0.289
q	5	0.24	0.16	0.16	0.2	0.256	0.256	0.232	0.24	0.307	0.288
	6	0.222	0.194	0.166	0.166	0.277	0.25	0.231	0.212	0.293	0.287
	7	0.204	0.204	0.163	0.142	0.279	0.244	0.227	0.209	0.299	0.276
	8	0.234	0.203	0.171	0.140	0.275	0.25	0.214	0.203	0.299	0.275

Table 1: The mean value of relative improvements; truncated.

m		2				3				4	
r		2	3	4	5	2	3	4	5	2	3
	2	0.363	0.273	0.337	0.291	0.301	0.300	0.342	0.307	0.248	0.260
	3	0.217	0.286	0.228	0.236	0.194	0.224	0.213	0.214	0.158	0.177
	4	0.191	0.197	0.232	0.195	0.158	0.169	0.180	0.172	0.125	0.135
q	5	0.155	0.167	0.174	0.197	0.139	0.145	0.148	0.153	0.110	0.116
	6	0.148	0.160	0.156	0.154	0.128	0.132	0.132	0.131	0.100	0.105
	7	0.128	0.137	0.138	0.138	0.119	0.122	0.121	0.119	0.093	0.098
	8	0.126	0.127	0.134	0.126	0.114	0.115	0.113	0.111	0.089	0.093

Table 1: Error correction abilities of weighted Reed-Muller codes and hyperbolic codes when $s_1 = 8$ and $s_2 = 64$.

	s/d	3	488	4	480	7	456	15	392	16	384	20	352
r	Bound	W	H	W	H	W	H	W	H	W	H	W	H
2	S	267		243		191		103	95	95	87	67	59
	C	286		266		219		131	128	122	119	97	94
	D	298		277		228		135	131	121	119	99	95
3	S	287		263		213		130	122	122	117	95	90
	C	301		279		234		149	145	138	135	113	109
	D	319		298		255		177	175	161	160	139	135
4	S	295		273		225		145	139	139	131	111	105
	C	307		286		242		159	155	147	145	123	118
	D	328		311		269		196	195	181	181	160	159
9	S	312		292		247		173	166	166	159	140	134
	C	318		299		255		178	173	169	166	144	139
20	S	320		301		258		185	178	178	171	153	147
	C	323		304		262		188	182	180	175	155	149
	Sub	198		149		33		0		0		0	
	$\lfloor \frac{d-1}{2} \rfloor$	243		239		227		195		191		175	
	Dim	4		5		8		24	25	27	28	39	41

Table 1: Error correction abilities of weighted Reed-Muller codes and hyperbolic codes when $s_1 = 16$ and $s_2 = 256$.

	s/d	5	4016	8	3968	15	3856	31	3600	36	3620	55	3216
r	Bound	W	H	W	H	W	H	W	H	W	H	W	H
2	S	2591		2335		1927		1359	1335	1231	1207	839	791
	C	2680		2456		2112		1565	1557	1392	1391	1022	1003
	D	2729		2504		2153		1589	1583	1411	1408	1035	1015
3	S	2714		2479		2106		1578	1551	1455	1434	1082	1034
	C	2790		2579		2240		1695	1684	1552	1547	1190	1167
	D	2861		2651		2326		1859	1855	1707	1706	1359	1351
4	S	2779		2555		2195		1691	1667	1575	1551	1211	1163
	C	2843		2635		2305		1782	1767	1638	1632	1284	1260
9	S	2894		2689		2362		1895	1871	1784	1763	1443	1367
	C	2928		2730		2415		1935	1919	1811	1804	1469	1442
20	S	2947		2751		2439		1988	1966	1882	1862	1551	1506
	C	2964		2772		2464		2007	1989	1894	1884	1562	1529
	Sub	1806		1199		130		0		0		0	
	$\lfloor \frac{d-1}{2} \rfloor$	2007		1983		1927		1799		1759		1607	
	Dim	4		5		8		24	25	27	28	39	41