Further improvements on the Feng-Rao bound for dual codes

Olav Geil, Stefano Martin
Aalborg University

Mathematics of Information-Theoretic Cryptography
Lorentz Center, May 2013

The Feng-Rao bound for the minimum distance and generalized Hamming weights of dual codes:

- Linear code level.
- Level with supporting algebra:
  - Affine variety.
  - Order domain.
  - Algebraic function field (arbitrary transcendence degree). For one-point AG codes an improvement to the Goppa bound.

This talk:

- Illustrative examples at affine variety code level.
- Enhancements and improvements at linear code level.

The Feng-Rao bound for the minimum distance and generalized Hamming weights of dual codes:

- Linear code level.
- Level with supporting algebra:
  - Affine variety.
  - Order domain.
  - Algebraic function field (arbitrary transcendence degree). For one-point AG codes an improvement to the Goppa bound.

This talk:

- Illustrative examples at affine variety code level.
- Enhancements and improvements at linear code level.

Order of improvements

- The Feng-Rao bound with WB.
- The Feng-Rao bound with WWB.
- The Feng-Rao bound with OWB.
- The advisory bound (Salazar, Dunn, Graham, 2006).
- New improvement.

We also lift the advisory bound as well as our bound to deal with generalized Hamming weights.

Order of improvements

- The Feng-Rao bound with WB.
- The Feng-Rao bound with WWB.
- The Feng-Rao bound with OWB.
- The advisory bound (Salazar, Dunn, Graham, 2006).
- New improvement.

We also lift the advisory bound as well as our bound to deal with generalized Hamming weights.

Generalized Hamming weights

Definition: Let $D \subseteq \mathbb{F}_q^n$. The support-size of D is the number of entries for which some word in D is non-zero.

Example: $D = \{(01001), (00011)\}$. The support-size is 3.

Definition: Let C be a linear code. The minimum distance is the minimum of the support-size of D, when $D \subseteq C$ runs through all possible subspaces of dimension 1.

Definition: The tth generalized Hamming weight is the minimum of the support-size of D, when $D \subseteq C$ runs through all possible subspaces of dimension t.

Applications: Wiretap channel of type II (Wei), and secret sharing schemes (Kurihara, Uyematsu, Matsumoto).

Generalized Hamming weights

Definition: Let $D \subseteq \mathbb{F}_q^n$. The support-size of D is the number of entries for which some word in D is non-zero.

Example: $D = \{(01001), (00011)\}$. The support-size is 3.

Definition: Let C be a linear code. The minimum distance is the minimum of the support-size of D, when $D \subseteq C$ runs through all possible subspaces of dimension 1.

Definition: The tth generalized Hamming weight is the minimum of the support-size of D, when $D \subseteq C$ runs through all possible subspaces of dimension t.

Applications: Wiretap channel of type II (Wei), and secret sharing schemes (Kurihara, Uyematsu, Matsumoto).

Generalized Hamming weights

Definition: Let $D \subseteq \mathbb{F}_q^n$. The support-size of D is the number of entries for which some word in D is non-zero.

Example: $D = \{(01001), (00011)\}$. The support-size is 3.

Definition: Let C be a linear code. The minimum distance is the minimum of the support-size of D, when $D \subseteq C$ runs through all possible subspaces of dimension 1.

Definition: The tth generalized Hamming weight is the minimum of the support-size of D, when $D \subseteq C$ runs through all possible subspaces of dimension t.

Applications: Wiretap channel of type II (Wei), and secret sharing schemes (Kurihara, Uyematsu, Matsumoto).

Example 1

$$I_8 = \langle X^4 + X^2 + X - Y^6 - Y^5 - Y^3, X^8 - X, Y^8 - Y \rangle \subseteq \mathbb{F}_8[X, Y].$$

$$\mathbb{V}_{\mathbb{F}_8}(I_8) = \{P_1, \ldots, P_{32}\}.$$

$\mathrm{ev} : \mathbb{F}_8[X, Y]/I_8 \to \mathbb{F}_8^{32}$
$\mathrm{ev}(F + I_8) = (F(P_1), \ldots, F(P_{32}))$.

From a monomial basis $\{M_1 + I_8, \ldots, M_{32} + I_8\}$ for $\mathbb{F}_8[X, Y]/I_8$ we produce a basis $\{\vec{b}_1, \ldots, \vec{b}_{32}\}$ for $\mathbb{F}_8^{32}$.

Example 1

$$I_8 = \langle X^4 + X^2 + X - Y^6 - Y^5 - Y^3, X^8 - X, Y^8 - Y \rangle \subseteq \mathbb{F}_8[X, Y].$$

$$\mathbb{V}_{\mathbb{F}_8}(I_8) = \{P_1, \ldots, P_{32}\}.$$

$\mathrm{ev} : \mathbb{F}_8[X, Y]/I_8 \to \mathbb{F}_8^{32}$
$\mathrm{ev}(F + I_8) = (F(P_1), \ldots, F(P_{32})).$

From a monomial basis $\{M_1 + I_8, \ldots, M_{32} + I_8\}$ for $\mathbb{F}_8[X, Y]/I_8$ we produce a basis $\{\vec{b}_1, \ldots, \vec{b}_{32}\}$ for $\mathbb{F}_8^{32}$.

Example 1

$$I_8 = \langle X^4 + X^2 + X - Y^6 - Y^5 - Y^3, X^8 - X, Y^8 - Y \rangle \subseteq \mathbb{F}_8[X, Y].$$

$\mathbb{V}_{\mathbb{F}_8}(I_8) = \{P_1, \ldots, P_{32}\}.$

ev : $\mathbb{F}_8[X, Y]/I_8 \rightarrow \mathbb{F}_8^{32}$
$\mathrm{ev}(F + I_8) = (F(P_1), \ldots, F(P_{32})).$

From a monomial basis $\{M_1 + I_8, \ldots, M_{32} + I_8\}$ for $\mathbb{F}_8[X, Y]/I_8$ we produce a basis $\{\vec{b}_1, \ldots, \vec{b}_{32}\}$ for $\mathbb{F}_8^{32}$.

Example 1 - cont.

Weighted degree lexicographic ordering with $w(X) = 3$ and $w(Y) = 2$.

Y^7	XY^7	X^2Y^7	X^3Y^7
Y^6	XY^6	X^2Y^6	X^3Y^6
Y^5	XY^5	X^2Y^5	X^3Y^5
Y^4	XY^4	X^2Y^4	X^3Y^4
Y^3	XY^3	X^2Y^3	X^3Y^3
Y^2	XY^2	X^2Y^2	X^3Y^2
Y	XY	X^2Y	X^3Y
1	X	X^2	X^3

14^{21}	17^{26}	20^{30}	23^{32}
12^{17}	15^{23}	18^{28}	21^{31}
10^{13}	13^{19}	16^{25}	19^{29}
8^{9}	11^{15}	14^{22}	17^{27}
6^{6}	9^{11}	12^{18}	15^{24}
4^{4}	7^{8}	10^{14}	13^{20}
2^{2}	5^{5}	8^{10}	11^{16}
0^{1}	3^{3}	6^{7}	9^{12}

Monomials $\{M_1, \ldots, M_{32}\}$ from which we produce $\{\vec{b}_1, \ldots, \vec{b}_{32}\}$.

z^a means: weight is z and index is a

$C(s) = \{\vec{c} \in \mathbb{F}_8^{32} \mid \vec{c} \cdot \vec{b}_1 = \cdots = \vec{c} \cdot \vec{b}_s = 0\}$.

Example 1 - cont.

Weighted degree lexicographic ordering with $w(X) = 3$ and $w(Y) = 2$.

$$\begin{array}{cccc}
Y^7 & XY^7 & X^2Y^7 & X^3Y^7 \\
Y^6 & XY^6 & X^2Y^6 & X^3Y^6 \\
Y^5 & XY^5 & X^2Y^5 & X^3Y^5 \\
Y^4 & XY^4 & X^2Y^4 & X^3Y^4 \\
Y^3 & XY^3 & X^2Y^3 & X^3Y^3 \\
Y^2 & XY^2 & X^2Y^2 & X^3Y^2 \\
Y & XY & X^2Y & X^3Y \\
1 & X & X^2 & X^3
\end{array}
\qquad
\begin{array}{rrrr}
14^{21} & 17^{26} & 20^{30} & 23^{32} \\
12^{17} & 15^{23} & 18^{28} & 21^{31} \\
10^{13} & 13^{19} & 16^{25} & 19^{29} \\
8^{9} & 11^{15} & 14^{22} & 17^{27} \\
6^{6} & 9^{11} & 12^{18} & 15^{24} \\
4^{4} & 7^{8} & 10^{14} & 13^{20} \\
2^{2} & 5^{5} & 8^{10} & 11^{16} \\
0^{1} & 3^{3} & 6^{7} & 9^{12}
\end{array}$$

Monomials $\{M_1, \ldots, M_{32}\}$ from which we produce $\{\vec{b}_1, \ldots, \vec{b}_{32}\}$.

z^a means: weight is z and index is a

$C(s) = \{\vec{c} \in \mathbb{F}_8^{32} \mid \vec{c} \cdot \vec{b}_1 = \cdots = \vec{c} \cdot \vec{b}_s = 0\}.$

Example 1 - cont.

	Feng-Rao WB	Feng-Rao WWB	Feng-Rao OWB	Advisory bound	New bound
d_1	7	7	8	9	10
d_2	8	8	10	12	13

Tabel: Estimates on first and second generalized Hamming weight of the code $C(16)$. Dimension is $32 - 16 = 16$.

dimension

Y^7	12	7	3	1
Y^6	16	10	5	2
Y^5	20	14	8	4
Y^4	24	18	11	6
Y^3	27	22	15	9
Y^2	29	25	19	13
Y	31	28	23	17
1	32	30	26	21
	1	X	X^2	X^3

d_1

Y^7	13^5	16^1	26^2	32^1
Y^6	10^5	14^1	22^2	28^1
Y^5	6^1	12^4	16^1	24^1
Y^4	4^1	8^3	14^1	20^1
Y^3	3^1	4^1	12^4	16^1
Y^2	3^1	4^1	8^3	12^4
Y	2^1	3^1	4^1	8^3
1	1^1	2^1	3^1	4^1
	1	X	X^2	X^3

d_2

Y^7	15^1	24^2	31^1	—
Y^6	13^5	16^1	26^2	32^1
Y^5	9^4	14^1	22^2	28^1
Y^4	6^1	12^4	16^1	24^1
Y^3	4^1	8^3	14^1	20^1
Y^2	4^1	6^1	11^4	15^1
Y	3^1	4^1	7^1	12^4
1	2^1	3^1	4^1	8^3
	1	X	X^2	X^3

d_3

Y^7	16^1	26^2	32^1	—
Y^6	14^1	22^2	28^1	—
Y^5	12^4	15^1	24^2	31^1
Y^4	8^3	13^1	20^1	27^1
Y^3	6^1	10^3	15^1	23^1
Y^2	5^1	8^3	12^1	16^1
Y	4^1	6^1	8^1	14^1
1	3^1	4^1	7^1	10^3
	1	X	X^2	X^3

d_4

Y^7	21^1	28^1	—	—
Y^6	15^1	24^2	31^1	—
Y^5	13^1	16^1	26^2	32^1
Y^4	10^3	14^1	22^2	28^1
Y^3	8^3	12^3	16^1	24^1
Y^2	6^1	10^3	14^1	20^1
Y	5^1	7^1	11^1	15^1
1	4^1	6^1	8^1	12^3
	1	X	X^2	X^3

d_5

Y^7	22^1	30^1	—	—
Y^6	16^1	26^1	32^1	—
Y^5	14^1	21^1	28^1	—
Y^4	12^3	15^1	24^1	31^1
Y^3	9^3	13^1	20^1	27^1
Y^2	8^3	11^1	20^1	22^1
Y	6^1	8^1	12^1	16^1
1	5^1	7^1	10^1	14^1
	1	X	X^2	X^3

Comparison with a class of AG codes

Important observation: For one-point AG codes the same weight does not appear more than once among the basis vectors.

This gives better results when the Feng-Rao bound is used.

Fair to compare our codes with norm-trace codes. We consider improved code construction.

NT	32	28	24	22	21	20	18	18	16	15	14
Ex. 1	32	28	26	24	22	20	18	16	16	15	14
NT	12	12	12	11	10	9	8	8	7	6	6
Ex. 1	13	12	12	12	10	10	9	8	8	6	6
NT	6	5	4	4	4	3	3	2	2	1	
Ex. 1	6	5	4	4	4	3	3	2	2	1	

Example 2

Similar example, but now over $\mathbb{F}_{27}$. Codes are of length $n = 243$.

	Feng-Rao WB	Feng-Rao WWB	Feng-Rao OWB	Advisory bound	New bound
$d_1(C(75))$	15	15	21	29	33
$d_2(C(75))$	16	16	24	34	38
$d_1(C(76))$	15	15	21	33	36
$d_2(C(76))$	16	16	24	38	39
$d_1(C(83))$	16	16	24	34	38
$d_2(C(83))$	17	17	27	39	41

Tabel: Estimates of minimum distance and second generalized Hamming weight. Codes are of dimension 168, 167, and 160, respectively.

dimension

	1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8
Y^{26}	54	43	33	24	17	11	6	3	1
Y^{25}	63	51	40	30	22	15	9	5	2
Y^{24}	72	60	48	37	28	20	13	8	4
Y^{23}	81	69	57	45	35	26	18	12	7
Y^{22}	90	78	66	53	42	32	23	16	10
Y^{21}	99	87	75	62	50	39	29	21	14
Y^{20}	108	96	84	71	59	47	36	27	19
Y^{19}	117	105	93	80	68	56	44	34	25
Y^{18}	126	114	102	89	77	65	52	41	31
Y^{17}	135	123	111	98	86	74	61	49	38
Y^{16}	144	132	120	107	95	83	70	58	46
Y^{15}	153	141	129	116	104	92	79	67	55
Y^{14}	162	150	138	125	113	101	88	76	64
Y^{13}	171	159	147	134	122	110	97	85	73
Y^{12}	180	168	156	143	131	119	106	94	82
Y^{11}	189	177	165	152	140	128	115	103	91
Y^{10}	198	186	174	161	149	137	124	112	100
Y^{9}	206	195	183	170	158	146	133	121	109
Y^{8}	213	203	192	179	167	155	142	130	118
Y^{7}	219	210	200	188	176	164	151	139	127
Y^{6}	225	217	208	197	185	173	160	148	136
Y^{5}	230	223	215	205	194	182	169	157	145
Y^{4}	234	228	221	212	202	191	178	166	154
Y^{3}	237	232	226	218	209	199	187	175	163
Y^{2}	240	236	231	224	216	207	196	184	172
Y	242	239	235	229	222	214	204	193	181
1	243	241	238	233	227	220	211	201	190

d_1

	1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8
Y^{26}	73^4	77^4	81^1	138^3	150^3	162^1	219^2	231^2	243^1
Y^{25}	70^4	74^4	78^1	132^3	144^3	156^1	210^2	222^2	234^1
Y^{24}	67^4	71^4	75^4	81^1	138^3	150^3	162^1	213^2	225
Y^{23}	64^4	68^4	72^4	77^4	81^1	138^3	150^3	162^1	216
Y^{22}	61^4	65^4	69^4	74^4	78^1	132^3	144^3	156^3	207^2
Y^{21}	58^4	62^4	66^4	71^4	75^4	81^1	138^3	150^3	162^1
Y^{20}	55^4	59^4	63^4	68^4	72^4	77^4	81^1	138^3	150^3
Y^{19}	52^4	56^4	60^4	65^4	69^4	73^4	77^4	81^1	138^3
Y^{18}	49^4	53^4	57^4	62^4	66^4	70^4	74^4	78^1	132^3
Y^{17}	46^4	50^4	54^4	59^4	63^4	67^4	71^4	75^4	81^1
Y^{16}	43^4	47^4	51^4	56^4	60^4	64^4	68^4	72^4	77^4
Y^{15}	40^5	44^4	48^4	53^4	57^4	61^4	65^4	69^4	73^4
Y^{14}	37^5	41^5	45^4	50^4	54^4	58^4	62^4	66^4	70^4
Y^{13}	30^5	38^5	42^4	47^4	51^4	55^4	59^4	63^4	67^4
Y^{12}	21^5	33^5	39^4	44^4	48^4	52^4	56^4	60^4	64^4
Y^{11}	12^1	24^4	36^5	41^5	45^4	49^4	53^4	57^4	61^4
Y^{10}	9^1	18^4	27^5	38^5	42^4	46^4	50^4	54^4	58^4
Y^{9}	8^1	9^1	18^4	33^5	39^4	43^4	47^4	51^4	55^4
Y^{8}	7^1	8^1	9^1	24^4	36^5	40^5	44^4	48^4	52^4
Y^{7}	7^1	8^1	9^1	18^4	27^5	36^5	41^5	45^4	49^4
Y^{6}	6^1	7^1	8^1	9^1	18^4	27^5	38^5	42^4	46^4
Y^{5}	5^1	6^1	7^1	8^1	9^1	18^4	33^5	39^5	43^4
Y^{4}	4^1	5^1	6^1	7^1	8^1	9^1	24^4	36^5	40^5
Y^{3}	4^1	5^1	6^1	7^1	8^1	9^1	18^4	27^5	36^5
Y^{2}	3^1	4^1	5^1	6^1	7^1	8^1	9^1	18^4	27^5
Y	2^1	3^1	4^1	5^1	6^1	7^1	8^1	9^1	18^4
1	1^1	2^1	3^1	4^1	5^1	6^1	7^1	8^1	9^1

Figur: Dimension and minimum distance of the codes $C(s)$ over $\mathbb{F}_{27}$.

Example 2 - cont.

d_2

Y^{26}	76	80^1	135^3	149^3	161^1	216^2	230^2	242^1	—
Y^{25}	73^4	77^4	81^1	138^3	150^3	162^1	219^2	231^2	243^1
Y^{24}	70^4	74^4	78^1	132^3	144^3	156^1	210^2	222^2	234^1
Y^{23}	67^4	71^4	75^4	80^1	135^3	149^3	161^1	213^2	225^2
Y^{22}	64^4	68^4	72^4	77^4	81^1	138^3	150^3	162^1	216^2
Y^{21}	61^4	65^4	69^4	74^4	78^1	132^3	144^3	156^1	207^2
Y^{20}	58^4	62^4	66^4	71^4	75^4	80^1	135^3	149^3	161^1
Y^{19}	55^4	59^4	63^4	68^4	72^4	76^4	80^1	135^3	149^3
Y^{18}	52^4	56^4	60^4	65^4	69^4	73^4	77^4	81^1	138^3
Y^{17}	49^4	53^4	57^4	62^4	66^4	70^4	74^4	78^1	132^3
Y^{16}	46^4	50^4	54^4	59^4	63^4	67^4	71^4	75^4	80^1
Y^{15}	43^4	47^4	51^4	56^4	60^4	64^4	68^4	72^4	76^4
Y^{14}	40^5	44	48^4	53^4	57^4	61^4	65^4	69^4	73^4
Y^{13}	37^5	41^5	45^4	50^4	54^4	58^4	62^4	66^4	70^4
Y^{12}	30^5	38^5	42^4	47^4	51^4	55^4	59^4	63^4	67^4
Y^{11}	21^5	33^5	39^5	44^4	48^4	52^4	56^4	60^4	64^4
Y^{10}	12^1	24^4	36^5	41^5	45^4	49^4	53^4	57^4	61^4
Y^{9}	9^1	17^4	27^5	38^5	42^4	46^4	50^4	54^4	58^4
Y^{8}	8^1	9^1	18^4	33^5	39^5	43^4	47^4	51^4	55^4
Y^{7}	8^1	9^1	12^1	24^4	35^5	40^5	44^4	48^4	52^4
Y^{6}	7^1	8^1	9^1	17^4	26^4	36^5	41^5	45^4	49^4
Y^{5}	6^1	7^1	8^1	9^1	17^4	27^5	38^5	42^4	46^4
Y^{4}	5^1	6^1	7^1	8^1	9^1	18^4	33^5	39^5	43^4
Y^{3}	5^1	6^1	7^1	8^1	9^1	12^1	24^4	35^5	40^5
Y^{2}	4^1	5^1	6^1	7^1	8^1	9^1	17^4	26^4	36^5
Y	3^1	4^1	5^1	6^1	7^1	8^1	9^1	17^4	27^5
1	2^1	3^1	4^1	5^1	6^1	7^1	8^1	9^1	18^4
	1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8

Figur: Second generalized Hamming weight of the codes $C(s)$ over $\mathbb{F}_{27}$.

Notation by example

$\mathbb{F}_q = \{P_1, \ldots, P_{n=q}\}$.

$\vec{c} = \mathrm{ev}(F) = (F(P_1), \ldots, F(P_n))$.

$\vec{b}_1 = \mathrm{ev}(1), \vec{b}_2 = \mathrm{ev}(X), \ldots, \vec{b}_n = \mathrm{ev}(X^{n-1})$.

$\rho(\vec{c}) = i$ if $\vec{c} \in \mathrm{span}\{\vec{b}_1, \ldots, \vec{b}_i\} \backslash \mathrm{span}\{\vec{b}_1, \ldots, \vec{b}_{i-1}\}$. That is, if $\deg(F \bmod X^n - X) = i - 1$.

Component wise product: $\vec{u} * \vec{v} = (u_1 v_1, \ldots, u_n v_n)$.

(i, j) is OWB if $\rho(\vec{b}_{i'} * \vec{b}_j < \rho(\vec{b}_i * \vec{b}_j$ for all $i' < i$.

Example: Assume $(i-1) + (j-1) < n$. Then $\vec{b}_i * \vec{b}_j = \vec{b}_{i+j-1}$ and $\vec{b}_{i'} * \vec{b}_j = \vec{b}_{i'+j-1}$ for all $i' < i$. Hence, (i, j) is OWB.

Notation by example

$\mathbb{F}_q = \{P_1, \ldots, P_{n=q}\}$.

$\vec{c} = \mathrm{ev}(F) = (F(P_1), \ldots, F(P_n))$.

$\vec{b}_1 = \mathrm{ev}(1), \vec{b}_2 = \mathrm{ev}(X), \ldots, \vec{b}_n = \mathrm{ev}(X^{n-1})$.

$\rho(\vec{c}) = i$ if $\vec{c} \in \mathrm{span}\{\vec{b}_1, \ldots, \vec{b}_i\} \backslash \mathrm{span}\{\vec{b}_1, \ldots, \vec{b}_{i-1}\}$. That is, if $\deg(F \bmod X^n - X) = i - 1$.

Component wise product: $\vec{u} * \vec{v} = (u_1 v_1, \ldots, u_n v_n)$.

(i, j) is OWB if $\rho(\vec{b}_{i'} * \vec{b}_j < \rho(\vec{b}_i * \vec{b}_j$ for all $i' < i$.

Example: Assume $(i-1) + (j-1) < n$. Then $\vec{b}_i * \vec{b}_j = \vec{b}_{i+j-1}$ and $\vec{b}_{i'} * \vec{b}_j = \vec{b}_{i'+j-1}$ for all $i' < i$. Hence, (i, j) is OWB.

Notation by example

$\mathbb{F}_q = \{P_1, \ldots, P_{n=q}\}$.

$\vec{c} = \mathrm{ev}(F) = (F(P_1), \ldots, F(P_n))$.

$\vec{b}_1 = \mathrm{ev}(1), \vec{b}_2 = \mathrm{ev}(X), \ldots, \vec{b}_n = \mathrm{ev}(X^{n-1})$.

$\rho(\vec{c}) = i$ if $\vec{c} \in \mathrm{span}\{\vec{b}_1, \ldots, \vec{b}_i\} \backslash \mathrm{span}\{\vec{b}_1, \ldots, \vec{b}_{i-1}\}$. That is, if $\deg(F \bmod X^n - X) = i - 1$.

Component wise product: $\vec{u} * \vec{v} = (u_1 v_1, \ldots, u_n v_n)$.

(i, j) is OWB if $\rho(\vec{b}_{i'} * \vec{b}_j < \rho(\vec{b}_i * \vec{b}_j$ for all $i' < i$.

Example: Assume $(i-1) + (j-1) < n$. Then $\vec{b}_i * \vec{b}_j = \vec{b}_{i+j-1}$ and $\vec{b}_{i'} * \vec{b}_j = \vec{b}_{i'+j-1}$ for all $i' < i$. Hence, (i, j) is OWB.

Notation by example

$\mathbb{F}_q = \{P_1, \ldots, P_{n=q}\}$.

$\vec{c} = \mathrm{ev}(F) = (F(P_1), \ldots, F(P_n))$.

$\vec{b}_1 = \mathrm{ev}(1), \vec{b}_2 = \mathrm{ev}(X), \ldots, \vec{b}_n = \mathrm{ev}(X^{n-1})$.

$\rho(\vec{c}) = i$ if $\vec{c} \in \mathrm{span}\{\vec{b}_1, \ldots, \vec{b}_i\} \backslash \mathrm{span}\{\vec{b}_1, \ldots, \vec{b}_{i-1}\}$. That is, if $\deg(F \bmod X^n - X) = i - 1$.

Component wise product: $\vec{u} * \vec{v} = (u_1 v_1, \ldots, u_n v_n)$.

(i, j) is OWB if $\rho(\vec{b}_{i'} * \vec{b}_j < \rho(\vec{b}_i * \vec{b}_j$ for all $i' < i$.

Example: Assume $(i-1) + (j-1) < n$. Then $\vec{b}_i * \vec{b}_j = \vec{b}_{i+j-1}$ and $\vec{b}_{i'} * \vec{b}_j = \vec{b}_{i'+j-1}$ for all $i' < i$. Hence, (i, j) is OWB.

The theory

$\{\vec{b}_1, \ldots, \vec{b}_n\}$ a basis for $\mathbb{F}_q^n$.

- $\rho(\vec{c}) = i$ if i is the smallest index such that $\vec{c} \in \mathrm{Span}_{\mathbb{F}_q}\{\vec{b}_1, \ldots \vec{b}_i\}$.
- $m(\vec{c}) = l$ if l is the smallest index such that $\vec{c} \notin \left(\mathrm{Span}_{\mathbb{F}_q}\{\vec{b}_1, \ldots \vec{b}_l\}\right)^{\perp}$.

$(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ is OWB if for all $i' < i$ it holds that $\rho(\vec{b}_{i'} * \vec{b}_j) < \rho(\vec{b}_i * \vec{b}_j)$ (here, $*$ is the component-wise product).

$\mu(l) = \#\{i \mid \text{ for some } j, (i, j) \text{ is OWB and } \rho(\vec{b}_i * \vec{b}_j) = l\}$.

The Feng-Rao bound: $w_H(\vec{c}) \geq \mu(m(\vec{c}))$.

The theory

$\{\vec{b}_1, \ldots, \vec{b}_n\}$ a basis for $\mathbb{F}_q^n$.

- $\rho(\vec{c}) = i$ if i is the smallest index such that $\vec{c} \in \mathrm{Span}_{\mathbb{F}_q}\{\vec{b}_1, \ldots \vec{b}_i\}$.
- $m(\vec{c}) = l$ if l is the smallest index such that $\vec{c} \notin \left(\mathrm{Span}_{\mathbb{F}_q}\{\vec{b}_1, \ldots \vec{b}_l\}\right)^{\perp}$.

$(i,j) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ is OWB if for all $i' < i$ it holds that $\rho(\vec{b}_{i'} * \vec{b}_j) < \rho(\vec{b}_i * \vec{b}_j)$ (here, $*$ is the component-wise product).

$\mu(l) = \#\{i \mid \text{ for some } j, (i,j) \text{ is OWB and } \rho(\vec{b}_i * \vec{b}_j) = l\}$.

The Feng-Rao bound: $w_H(\vec{c}) \geq \mu(m(\vec{c}))$.

The theory

$\{\vec{b}_1, \ldots, \vec{b}_n\}$ a basis for $\mathbb{F}_q^n$.

- $\rho(\vec{c}) = i$ if i is the smallest index such that $\vec{c} \in \mathrm{Span}_{\mathbb{F}_q}\{\vec{b}_1, \ldots \vec{b}_i\}$.
- $m(\vec{c}) = l$ if l is the smallest index such that $\vec{c} \notin \left(\mathrm{Span}_{\mathbb{F}_q}\{\vec{b}_1, \ldots \vec{b}_l\}\right)^{\perp}$.

$(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ is OWB if for all $i' < i$ it holds that $\rho(\vec{b}_{i'} * \vec{b}_j) < \rho(\vec{b}_i * \vec{b}_j)$ (here, $*$ is the component-wise product).

$\mu(l) = \#\{i \mid \text{ for some } j, (i, j) \text{ is OWB and } \rho(\vec{b}_i * \vec{b}_j) = l\}$.

The Feng-Rao bound: $w_H(\vec{c}) \geq \mu(m(\vec{c}))$.

The advisory bound

Uses the following relaxation:

Let $\mathcal{I}' \subseteq \{1, \ldots, n\}$.

$(i, j) \in \mathcal{I}' \times \{1, \ldots, n\}$ is OWB with respect to $\mathcal{I}'$ if for all $i' < i, i' \in \mathcal{I}'$ it holds that $\rho(\vec{b}_{i'} * \vec{b}_j) < \rho(\vec{b}_i * \vec{b}_j)$

Our method

- Relax OWB further. Technical definition – but manageable.
- Take into account not only $m(\vec{c}) = l$, but also $l+1, \ldots, l+v$.
  - Consider $v+1$ different cases corresponding to if the numbers $\vec{c} \cdot \vec{b}_{l+1}, \cdots, \vec{c} \cdot \vec{b}_{l+v}$ are zero or non-zero.
  - Bound comes from worst-case consideration.

The definition that should NOT go into the presentation

Definition:
Consider the numbers $1 \leq l, l+1, \ldots, l+g \leq n$. A set $\mathcal{I}' \subseteq \mathcal{I}$ is said to have the μ-property with respect to l with exception $\{l+1, \ldots, l+g\}$ if for all $i \in \mathcal{I}'$ a $j \in \mathcal{I}$ exists such that

(1a) $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l$, and

(1b) for all $i' \in \mathcal{I}'$ with $i' < i$ either $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < l$ or $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) \in \{l+1, \ldots, l+g\}$ holds.

Assume next that $l+g+1 \leq n$. The set $\mathcal{I}'$ is said to have the relaxed μ-property with respect to $(l, l+g+1)$ with exception $\{l+1, \ldots, l+g\}$ if for all $i \in \mathcal{I}'$ a $j \in \mathcal{I}$ exists such that either conditions $(1a)$ and $(1b)$ above hold or

(2a) $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l+g+1$, and

(2b) (i, j) is OWB with respect to $\mathcal{I}'$, and

(2c) no $i' \in \mathcal{I}'$ with $i' < i$ satisfies $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) = l$.

The theorem that should NEITHER find its way to the talk

Theorem:
Consider a non-zero codeword $\vec{c}$ and let $l = m(\vec{c})$. Choose a non-negative integer v such that $l + v \leq n$. Assume that for some indexes $x \in \{l+1, \ldots, l+v\}$ we know *a priori* that $\vec{c} \cdot \vec{w}_x = 0$. Let $l'_1 < \cdots l'_s$ be the remaining indexes from $\{l+1, \ldots, l+v\}$. Consider the sets $\mathcal{I}'_0, \mathcal{I}'_1, \ldots, \mathcal{I}'_s$ such that:

- $\mathcal{I}'_0$ has the μ-property with respect to l with exception $\{l+1, \ldots, l+v\}$.
- For $i = 1, \ldots, s$, $\mathcal{I}'_i$ has the relaxed μ-property with respect to (l, l'_i) with exception $\{l+1, \ldots, l'_i - 1\}$.

We have

$$w_H(\vec{c}) \geq \min\{\#\mathcal{I}'_0, \#\mathcal{I}'_1, \ldots, \#\mathcal{I}'_s\}. \quad (1)$$

To establish a lower bound on the minimum distance of a code C we repeat the above process for each $l \in m(C)$. For each such l we choose a corresponding v, we determine sets $\mathcal{I}'_i$ as above and we calculate the right side of (1). The smallest value found constitutes a lower bound on the minimum distance.

The proposition that should in NO WAY being displayed

Proposition:
Let the notation be as above. Consider a subspace $D \subseteq C$ of dimension 2, say $m(D) = \{a, b\}$. Let v_a be the v corresponding to $l = a$. Let $a'_1 < \cdots < a'_{s_a}$ be the numbers $l'_1 < \cdots < l'_s$ corresponding to $l = a$. Analogously for the case b. Referring to the definition above, for $\alpha = 1, \ldots, s_a$ and $\beta = 1, \ldots, s_b$ we define subsets of $\mathcal{I}$ as follows:

- $\mathcal{I}''_{0,0}$ is a set such that for all $i \in \mathcal{I}''_{0,0}$ for an $l \in \{a, b\}$ a j exists such that (1a) and (1b) hold with $g = v_a$ if $l = a$, and $g = v_b$ if $l = b$.
- $\mathcal{I}''_{\alpha,0}$ is a set such that for all $i \in \mathcal{I}''_{\alpha,0}$ a j exists such that one of the following two conditions holds:
  - Either (1a), (1b) or (2a), (2b), (2c) hold with $l = a$ and $g + 1 = a'_\alpha$.
  - (1a) and (1b) hold with $l = b$ and $g = v_b$.
- $\mathcal{I}''_{0,\beta}$ is defined similarly to $\mathcal{I}''_{\alpha,0}$.
- $\mathcal{I}''_{\alpha,\beta}$ is a set such that for all $i \in \mathcal{I}''_{\alpha,\beta}$ an $l \in \{a, b\}$ and a $j \in \mathcal{I}$ exist such that either (1a), (1b) or (2a), (2b), (2c) hold. Here, $g + 1 = a'_\alpha$ if $l = a$, and $g + 1 = b'_\beta$ if $l = b$.

The support of D is of size at least equal to the smallest cardinality of the above sets. To establish a lower bound on the second generalized Hamming weight of a code C we repeat the above process for each $(a, b) \in m(C) \times m(C)$ with $a < b$. The smallest value found constitutes a lower bound on the second generalized Hamming weight.

Concluding remarks

- The advisory bound and our new bound are tailored for affine variety codes. Do the bounds have implications for algebraic geometric codes? If they do, it might be via the equations $X_i^q - X_i$.
- The usual Feng-Rao bound suggests that affine variety codes do not have very good parameters. Is it the Feng-Rao bound or the affine variety code construction that is the problem?