

*

Two applications of the footprint (or Δ -set) bound

Estimation of generalized Hamming weights

Olav Geil, Aalborg University
Based on joint works with T. Høholdt and H. E. Andersen

1 The Footprint (or Δ -set) bound

Definition 1 Let \prec be a monomial ordering on $\mathcal{M}(X_1, \dots, X_m)$ and k a field. Given an ideal $I \subseteq k[X_1, \dots, X_m]$ the set

$$\Delta_{\prec}(I) = \{M \in \mathcal{M}(X_1, \dots, X_m) \mid \text{there does not exist any } F \in I \text{ with } \text{Im}(F) = M\}$$

is called the footprint of I

Theorem 2 If $\Delta_{\prec}(I)$ is finite then $\#\mathbb{V}_{\bar{k}}(I) \leq \#\Delta_{\prec}(I)$ holds. Equality holds if I is radical. In particular $\#\mathbb{V}_{\mathbb{F}_q}(I) = \#\Delta_{\prec}(I \cup \langle X_1^q - X_1, \dots, X_m^q - X_m \rangle)$.

2 Generalized Hamming weights

Definition 3 The t th generalized Hamming weight of a code C is

$$d_t(C) = \min\{\#\text{Sup}(U) \mid U \text{ is a linear subcode of } C \text{ of dimension } t\}$$

Let $\{P_1, \dots, P_n\} = \mathbb{V}_{\mathbb{F}_q}(\langle G_1, \dots, G_g \rangle)$ and $\text{ev}(F) = (F(P_1), \dots, F(P_n))$.

$$A = \begin{bmatrix} \text{ev}(F_1) \\ \vdots \\ \text{ev}(F_a) \end{bmatrix}$$

$$[F_i] = \{F_i + \sum_{j=1}^{i-1} \alpha_j F_j \mid \alpha_j \in \mathbb{F}_q\}$$

$$D_{\{[F_{i_1}], \dots, [F_{i_s}]\}} = \max\{\#\{P_j \in V \mid F_{i_1}'(P_j) = \dots = F_{i_s}'(P_j) = 0\} \mid F_{i_t}' \in [F_{i_t}], t = 1, \dots, s\}$$

$$D_s = \max\{D_{\{[F_{i_1}], \dots, [F_{i_s}]\}} \mid 1 \leq i_1 < \dots < i_s \leq r\}.$$

Theorem 4 Let C be a code with parity check matrix A (not necessarily of full rank) then for $d^* \leq a+t, t \leq k, d \leq n$ we have

$$d_t \geq d^* \Leftrightarrow D_{a-d^*+t+1} \leq d^* - 2 \\ d_t \leq d^* \Leftrightarrow D_{a-d^*+t} \geq d^*$$

Theorem 5 Let C be a code with generator matrix A (assumed to be of full rank) then for $t = 1, \dots, k$ we have $d_t = n - D_t$.

Observation 6

$$D_{\{[F_{i_1}], \dots, [F_{i_s}]\}} = \max\{\#\Delta_{\prec}(\langle F_{i_1}', \dots, F_{i_s}', G_1, \dots, G_g, X_1^q - X_1, \dots, X_m^q - X_m \rangle \mid F_{i_t}' \in [F_{i_t}], t = 1, \dots, s\} \\ \leq \#\Delta_{\prec}(\langle \text{Im}(F_{i_1}), \dots, \text{Im}(F_{i_s}), G_1, \dots, G_g \rangle,$$

3 Weighted degree orderings

Definition 7 Given weights $w(X_1), \dots, w(X_m) \in \mathbb{R}_+$ define \prec_w on $\mathcal{M}(X_1, \dots, X_m)$ by $X_1^{i_1} \dots X_m^{i_m} \prec_w X_1^{j_1} \dots X_m^{j_m}$ if one of following conditions holds

- (1) $w(X_1^{i_1} \dots X_m^{i_m}) < w(X_1^{j_1} \dots X_m^{j_m})$
- (2) $w(X_1^{i_1} \dots X_m^{i_m}) = w(X_1^{j_1} \dots X_m^{j_m})$ and $X_1^{i_1} \dots X_m^{i_m} \prec_{lex} X_1^{j_1} \dots X_m^{j_m}$

Proposition 8 Define a weighted degree monomial ordering by the weights $w(X) = b$ and $w(Y) = a$ and consider

$$F(X, Y) = X^a + \alpha Y^b + F'(X, Y) \\ G(X, Y) = X^i Y^j + G'(X, Y)$$

where α is non-zero and $a, b > 0, w(F') < ab$, and $w(G') < bi + aj$. The equation set $F(X, Y) = G(X, Y) = 0$ has at most $bi + aj$ solutions

4 Parity check matrix description

Improved Hermitian codes

Let V be the 64 points on the Hermitian curve $X^5 + Y^4 + Y$ over \mathbb{F}_{16} . Let parity check matrix be

$$\begin{bmatrix} \text{ev}(1) \\ \text{ev}(X) \\ \text{ev}(Y) \\ \text{ev}(X^2) \\ \text{ev}(XY) \\ \text{ev}(Y) \\ \text{ev}(X) \\ \text{ev}(Y + X^4) \end{bmatrix}$$

$D_{\{[XY], [Y+X^4]\}} \leq 7$ follows from Proposition 8

$D_{\{[Y^2], [Y^3+X^4]\}} \leq 8$ follows by choosing $w(X) = 1$ and $w(Y) = 1.1$

$D_{\{[X], [X], [Y+X^4]\}} \leq 6$ follows by choosing $w(X) = 1$ and $w(Y) = 1.4$

Going through all combinations gives $D_1 \leq 16, D_2 \leq 8, D_3 \leq 6$ and $D_4 \leq 4$.

This implies $d_1 \geq 6, d_2 \geq 8, d_i \geq i+7$ for $i = 3, \dots, 9$ and $d_i = i+8$ for $i = 10, \dots, 56$. Not only minimum distance is improved.

5 Generator matrix description

Hermitian codes over \mathbb{F}_{16} Defining polynomial $X^5 + Y^4 + Y$ has 64 zeros which gives an evaluation map $\text{ev} : \mathbb{F}_{16}[X, Y] \rightarrow \mathbb{F}_{16}^{64}$.

Choose $w(X) = 5, w(Y) = 4$ and lexicographic ordering with $X \prec_{lex} Y$. By standard results

$$\text{ev}(\Delta_{\prec_w}(\langle X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y \rangle))$$

constitutes a basis for \mathbb{F}_{16}^{64} . Below is listed

$$\#\Delta_{\prec_w}(\langle X^i Y^j, X^5 + Y^4 \rangle) \cap \Delta_{\prec_w}(\langle X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y \rangle)$$

for all

$$X^i Y^j \in \Delta_{\prec_w}(\langle X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y \rangle)$$

15	19	23	27	31	35	39	43	47	51	55	59	60	61	62	63
10	14	18	22	26	30	34	38	42	46	50	54	56	58	60	62
5	9	13	17	21	25	29	33	37	41	45	49	52	55	58	61
0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60

Traditional codes corresponds to linear span of all $\text{ev}(X^i Y^j)$ with $w(X^i Y^j) \leq s$.

Improved codes corresponds to linear span of all $\text{ev}(X^i Y^j)$ with Δ -size at most some chosen number.

	k	d ₁	d ₂	d ₃	d ₄	d ₅	d ₆	d ₇	d ₈	d ₉
Improved	55	6	8	9	11	12	14	15	16	18
Traditional	55	4	8	9	12	13	14	16	17	18
	k	d ₁	d ₂	d ₃	d ₄	d ₅	d ₆	d ₇	d ₈	
Improved	51	9	12	14	15	17	18	19	21	
Traditional	51	8	12	13	16	17	18	20	21	
Traditional	50	9	13	14	17	18	19	21	22	

Certainly, minimum distances are improved, but higher weights need NOT be.

References

- [1] H. E. Andersen, On puncturing of codes from Norm-Trace curves, to appear in *Finite Fields and their Applications*.
- [2] A. I. Barbero and C. Munuera, The Weight Hierarchy of Hermitian Codes, *SIAM J. Discrete Math.*, **13**, 79-104.
- [3] D. Cox, J. Little and D. O'Shea, "Ideals, Varieties, and Algorithms, 2nd ed.," Springer, Berlin, 1997.
- [4] G.-L. Feng, T. R. N. Rao, G. A. Berg and J. Zhu, "Generalized Bezout's theorem in its applications in coding theory," *IEEE Trans. Inform. Theory*, **43**, 1799-1810.
- [5] O. Geil and T. Høholdt, "Footprints or Generalized Bezout's Theorem," *IEEE Trans. Inf. Theory*, **46**, 635-641.
- [6] O. Geil and T. Høholdt, On Hyperbolic Codes, Proc. AAECC-14, *Lecture Notes in Comput. Sci.* 2227, (S. Bozta, I. Sphparlinski, Eds.), Springer, Berlin, 2001, 159-171.
- [7] P. Heijnen and R. Pellikaan, Generalized Hamming Weights of q-ary Reed-Muller codes, *IEEE Trans. Inform. Theory*, **44**, (1998), 181-196