Two applications of the footprint bound

Estimation of generalized Hamming weights

O. G. - from joint works with T. Høholdt and joint work with H. E. Andersen

Special Semester on Gröbner Bases and Related Methods 2006

Generator matrix case: a continuation of yesterdays talk

Parity check matrix case: another point of view

The footprint bound

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

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

Theorem 2 If $\Delta_\prec(I)$ is finite then $\#\mathbb{V}_{\bar{k}}(I) \leq \#\Delta_\prec(I)$ holds.

Generalized Hamming Weights

$$\begin{aligned} D = \; & \{(1,1,0,0,1,0) \\ & \;(1,0,1,0,0,0) \\ & \;(0,0,1,0,1,0)\} \end{aligned}$$

$$\mathrm{Supp}(D) = \{1,2,3,5\}$$

$$\begin{aligned} d_t(C) \; &:= \; \min\{\#\mathrm{Supp}(D) \mid D \text{ is a subcode of } C \\ & \qquad\qquad\qquad\qquad\qquad\qquad \text{of dimension } t\} \\ d_1(C) \; &= \; d(C) \end{aligned}$$

Reed-Muller codes over $\mathbb{F}_4$

$X^4 - X, Y^4 - Y$

$$\begin{array}{cccc} \underline{Y^3} & XY^3 & X^2Y^3 & X^3Y^3 \\ \underline{Y^2} & \underline{XY^2} & X^2Y^2 & X^3Y^2 \\ \underline{Y} & \underline{XY} & \underline{X^2Y} & X^3Y \\ \underline{1} & \underline{X} & \underline{X^2} & \underline{X^3} \end{array} \qquad C = \mathrm{RM}_q(3, 2)$$

$$[16, 10, 4]$$

A basis for a subspace $D \subseteq C$ can be assumed to “consist” of polynomials with different leading monomials.

d_2-calculations: We look for worst case of

$$\#\Delta_{\prec}(\langle X^{i_1}Y^{j_1}, X^{i_2}Y^{j_2}, X^4, Y^4\rangle)$$

An incident is

$$\#\Delta_{\prec}(\langle X^3, X^2Y, X^4, Y^4\rangle) = 9$$

So $d_2 \geq 16 - 9 = 7$.

d_3-calculations: We look for worst case of

$$\#\Delta_{\prec}(\langle X^{i_1}Y^{j_1}, X^{i_2}Y^{j_2}, X^{i_3}Y^{j_3}, X^4, Y^4\rangle)$$

An incident is

$$\#\Delta_{\prec}(\langle X^3, X^2Y, X_2, X^4, Y^4\rangle) = 8$$

So $d_3 \geq 16 - 8 = 8$.

Definition 7 $w(X_1), \ldots, w(X_m) \in \mathbb{R}_+$, $X_1^{i_1} \cdots X_m^{i_m} \prec_w X_1^{j_1} \cdots X_m^{j_m}$ if (1) or (2) holds

$$\begin{array}{ll} (1) & w(X_1^{i_1} \cdots X_m^{i_m}) < w(X_1^{j_1} \cdots X_m^{j_m}) \\ (2) & w(X_1^{i_1} \cdots X_m^{i_m}) = w(X_1^{j_1} \cdots X_m^{j_m}) \\ & \quad \text{and } X_1^{i_1} \cdots X_m^{i_m} \prec_{lex} X_1^{j_1} \cdots X_m^{j_m} \end{array}$$

Hermitian codes over $\mathbb{F}_{16}$

$\mathbb{V}_{\mathbb{F}_{16}}(\langle X^5 + Y^4 + Y \rangle) = 64$, ev : $\mathbb{F}_{16}[X, Y] \to \mathbb{F}_{16}^{64}$.
Let $w(X) = 5$, $w(Y) = 4$ and lexicographic ordering be $X \prec_{lex} Y$.
ev($\Delta_{\prec_w}(\langle X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y \rangle)$) basis for $\mathbb{F}_{16}^{64}$.

$$\begin{array}{cccccccccc}
Y^3 & XY^3 & X^2Y^3 & X^3Y^3 & \cdots & X^{11}Y^3 & X^{12}Y^3 & X^{13}Y^3 & X^{14}Y^3 & X^{15}Y^3 \\
Y^2 & XY^2 & X^2Y^2 & X^3Y^2 & \cdots & X^{11}Y^2 & X^{12}Y^2 & X^{13}Y^2 & X^{14}Y^2 & X^{15}Y^2 \\
Y & XY & X^2Y & X^3Y & \cdots & X^{11}Y & X^{12}Y & X^{13}Y & X^{14}Y & X^{15}Y \\
1 & X & X^2 & X^3 & \cdots & X^{11} & X^{12} & X^{13} & X^{14} & X^{15}
\end{array}$$

15	19	23	27	31	35	39	43	47	51	55	59	63	67	71
10	14	18	22	26	30	34	38	42	46	50	54	58	62	66
5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
0	4	8	12	16	20	24	28	32	36	40	44	48	52	56

For all X^iY^j "in basis" we list the values of

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

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

Traditional codes corresponds to linear span of all $\mathrm{ev}(X^iY^j)$ with $w(X^iY^j) \leq s$.
Improved codes corresponds to linear span of all $\mathrm{ev}(X^iY^j)$ with Δ-size at most some chosen number.

<u>d_2-calculations:</u> Consider all pairs $X^{i_1}Y^{j_1}, X^{i_2}Y^{j_2}$ (from code basis). Calculate

$$n - \#(\Delta_{\prec_w}(\langle X^{i_1}Y^{j_1}, X^{i_2}Y^{j_2}, X^5+Y^4\rangle) \cap \Delta_{\prec_w}(\langle X^5+Y^4+Y, X^{16}+X, Y^{16}+Y\rangle))$$

$=$ “what can be hit by either $w(X^{i_1}Y^{j_1})$ or/and $w(X^{i_2}Y^{j_2})$.“

Choose worstcase. Repeat process for $d_3, \ldots$.

Traditional codes corresponds to linear span of all ev(X^iY^j) with $w(X^iY^j) \leq s$.
Improved codes corresponds to linear span of all ev(X^iY^j) with Δ-size at most some chosen number.

d_2-calculations: Consider all pairs $X^{i_1}Y^{j_1}, X^{i_2}Y^{j_2}$ (from code basis). Calculate

$$n - \#(\Delta_{\prec_w}(\langle X^{i_1}Y^{j_1}, X^{i_2}Y^{j_2}, X^5+Y^4\rangle) \\ \cap \Delta_{\prec_w}(\langle X^5+Y^4+Y, X^{16}+X, Y^{16}+Y\rangle))$$

$=$ “what can be hit by either $w(X^{i_1}Y^{j_1})$ or/and $w(X^{i_2}Y^{j_2})$.“

Choose worstcase. Repeat process for $d_3, \ldots$.

	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.

Some notation

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

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

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

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

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

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

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

Improved Hermitian codes - parity check matrix

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

$$\begin{bmatrix} \mathrm{ev}(1) \\ \mathrm{ev}(X) \\ \mathrm{ev}(Y) \\ \mathrm{ev}(X^2) \\ \mathrm{ev}(XY) \\ \mathrm{ev}(Y^2) \\ \mathrm{ev}(X^3) \\ \mathrm{ev}(Y^3 + X^4) \end{bmatrix}$$

$D_{\{[XY],[Y^3+X^4]\}} \leq 7$ chose $w(X) = 3, w(Y) = 4$
$D_{\{[Y^2],[Y^3+X^4]\}} \leq 8$ choose $w(X) = 1$ and $w(Y) = 1.1$
$D_{\{[X^2],[X^3],[Y^3+X^4]\}} \leq 6$ choose $w(X) = 1$ and $w(Y) = 1.4$

ABOVE WEIGHTS KEEP THE ORDERING OF ROWS. 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 $i = 3, \ldots, 9$ and $d_i = i + 8$ for $i = 10, \ldots, 56$. Not only minimum distance is improved.