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

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

Theorem 2 If \( \Delta_{\prec}(I) \) is finite then \( \# \varnothing_k(I) \leq \#\Delta_{\prec}(I) \) holds.
Generalized Hamming Weights

\[ D = \{(1, 1, 0, 0, 1, 0), (1, 0, 1, 0, 0, 0), (0, 0, 1, 0, 1, 0)\} \]

\[ \text{Supp}(D) = \{1, 2, 3, 5\} \]

\[ d_t(C) := \min\{\#\text{Supp}(D) \mid D \text{ is a subcode of } C \text{ of dimension } t\} \]

\[ d_1(C) = d(C) \]
Reed-Muller codes over $\mathbb{F}_4$

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

\[
\begin{array}{cccc}
Y^3 & XY^3 & X^2Y^3 & X^3Y^3 \\
Y^2 & XY^2 & X^2Y^2 & X^3Y^2 \\
Y & XY & X^2Y & X^3Y \\
1 & X & X^2 & X^3 \\
\end{array}
\]

$C = \text{RM}_q(3, 2)$

[16, 10, 4]

A basis for a subspace $D \subseteq C$ can be assumed to “consist” of polynomials with different leading leading monomials.
**d₂-calculations**: We look for worst case of

\[ \#\Delta_<(\langle X^{i_1} Y^{j_1}, X^{i_2} Y^{j_2}, X^4, Y^4 \rangle) \]

An incident is

\[ \#\Delta_<(\langle X^3, X^2 Y, X^4, Y^4 \rangle) = 9 \]

So \( d_2 \geq 16 - 9 = 7 \).

**d₃-calculations**: We look for worst case of

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

An incident is

\[ \#\Delta_<(\langle X^3, X^2 Y, X_2, X^4, Y^4 \rangle) = 8 \]

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

\[(1) \quad w(X_1^{i_1} \cdots X_m^{i_m}) < w(X_1^{j_1} \cdots X_m^{j_m}) \]
\[(2) \quad w(X_1^{i_1} \cdots X_m^{i_m}) = w(X_1^{j_1} \cdots X_m^{j_m}) \]

and \( X_1^{i_1} \cdots X_m^{i_m} \prec_{lex} X_1^{j_1} \cdots X_m^{j_m} \)
Hermitian codes over $\mathbb{F}_{16}$

$\forall_{\mathbb{F}_{16}}(\langle X^5 + Y^4 + Y \rangle) = 64$, $ev : \mathbb{F}_{16}[X, Y] \rightarrow \mathbb{F}_{16}^{64}$.

Let $w(X) = 5$, $w(Y) = 4$ and lexicographic ordering be $X \prec_{lex} Y$.

$ev(\Delta_{w}(\langle X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y \rangle))$ basis for $\mathbb{F}_{16}^{64}$.

\[
\begin{array}{cccccccccccc}
Y^3 & XY^3 & X^2Y^3 & X^3Y^3 & \ldots & X^{11}Y^3 & X^{12}Y^3 & X^{13}Y^3 & X^{14}Y^3 & X^{15}Y^3 \\
Y^2 & XY^2 & X^2Y^2 & X^3Y^2 & \ldots & X^{11}Y^2 & X^{12}Y^2 & X^{13}Y^2 & X^{14}Y^2 & X^{15}Y^2 \\
Y & XY & X^2Y & X^3Y & \ldots & X^{11}Y & X^{12}Y & X^{13}Y & X^{14}Y & X^{15}Y \\
1 & X & X^2 & X^3 & \ldots & X^{11} & X^{12} & X^{13} & X^{14} & X^{15}
\end{array}
\]
For all $X^i Y^j$ “in basis” we list the values of
\[
\# \left( \Delta_{\prec_w}(\langle X^i Y^j, X^5 + Y^4 \rangle) \cap \Delta_{\prec_w}(\langle X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y \rangle) \right)
\]
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 \(\Delta\)-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

\[
\begin{align*}
n - \#(\Delta \triangleleft w(\langle X^{i_1} Y^{j_1}, X^{i_2} Y^{j_2}, X^5 + Y^4 \rangle)) \
\cap \Delta \triangleleft w(\langle X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y \rangle))
\end{align*}
\]

= “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($X^i Y^j$) with $w(X^i Y^j) \leq s$.
Improved codes corresponds to linear span of all ev($X^i Y^j$) with $\Delta$-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

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

= “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 $d_3$, . . .
<table>
<thead>
<tr>
<th></th>
<th>k</th>
<th>$d_1$</th>
<th>$d_2$</th>
<th>$d_3$</th>
<th>$d_4$</th>
<th>$d_5$</th>
<th>$d_6$</th>
<th>$d_7$</th>
<th>$d_8$</th>
<th>$d_9$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved</td>
<td>55</td>
<td>6</td>
<td>8</td>
<td>9</td>
<td>11</td>
<td>12</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td><strong>18</strong></td>
</tr>
<tr>
<td>Traditional</td>
<td>55</td>
<td>4</td>
<td>8</td>
<td>9</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td><strong>16</strong></td>
<td><strong>17</strong></td>
<td><strong>18</strong></td>
</tr>
<tr>
<td></td>
<td>k</td>
<td>$d_1$</td>
<td>$d_2$</td>
<td>$d_3$</td>
<td>$d_4$</td>
<td>$d_5$</td>
<td>$d_6$</td>
<td>$d_7$</td>
<td>$d_8$</td>
<td></td>
</tr>
<tr>
<td>Improved</td>
<td>51</td>
<td>9</td>
<td>12</td>
<td>14</td>
<td>15</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td><strong>21</strong></td>
<td></td>
</tr>
<tr>
<td>Traditional</td>
<td>51</td>
<td>8</td>
<td>12</td>
<td>13</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td><strong>20</strong></td>
<td><strong>21</strong></td>
<td></td>
</tr>
<tr>
<td>Traditional</td>
<td>50</td>
<td>9</td>
<td>13</td>
<td>14</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td><strong>21</strong></td>
<td><strong>22</strong></td>
<td></td>
</tr>
</tbody>
</table>

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

\[ V = \{ P_1, \ldots, P_n \} = \mathbb{V}_{F_q}(\langle G_1, \ldots G_g \rangle), \]
\[ \text{ev}(F) = (F(P_1), \ldots, F(P_n)). \]

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

\[ [F_i] = \{ F_i + \sum_{j=1}^{i-1} \alpha_j F_j \mid \alpha_j \in F_q \} \]

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

\[ D_s = \max\{ D\{[F_{i_1}], \ldots, [F_{i_s}]\} \mid 1 \leq i_1 < \cdots < i_s \leq r \}. \]
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

$$d_t \geq d^* \iff D_{a-d^*+t+1} \leq d^* - 2$$
$$d_t \leq d^* \iff D_{a-d^*+t} \geq d^*$$
Let $V$ be the 64 points on the Hermitian curve $X^5 + Y^4 + Y$ over $\mathbb{F}_{16}$. Let parity check matrix be

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

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.