On the minimum distance of one-point geometric Goppa codes

Henning E. Andersen and Olav Geil

The Feng-Rao bound gives a lower bound on the minimum distance of codes defined by means of their parity check matrices. From this bound it is clear how to improve a large family of codes by leaving out certain rows in their parity check matrices. In our work we derive a simple bound on the minimum distance of codes defined by means of their generator matrices. From our bound it is clear how to improve a large family of codes by adding certain rows to their generator matrices. Actually our result not only deals with the minimum distance but gives lower bounds on any generalized Hamming weight. Our bound is easily interpreted into the setting of order domain theory. In particular it deals with one-point geometric Goppa codes.

In the remaining part of this extended abstract we consider only one-point geometric Goppa codes. Let $\mathbb{F}/\mathbb{F}_q$ be an algebraic function field with a single place $P_\infty$ at infinity. Let $P_1, \ldots, P_n$ be rational places, $P_i \neq P_\infty$, $i = 1, \ldots, n$. Consider

$$D := P_1 + \cdots + P_n$$
$$R := \bigcup_{m=0}^{\infty} (\mathcal{L}(mP_\infty))$$
$$ev_D : \begin{cases} R \to \mathbb{F}^n_q \\ x \mapsto (x(P_1), \ldots, x(P_n)) \end{cases}$$

Let $W = \{m_1, m_2, \ldots\}$, $0 = m_1 < m_2 < \cdots$, be the set of polenumbers of $P_\infty$. Choose a basis $\mathcal{B} = \{f_1, f_2, \ldots\}$ for $R$ as a vector space over $\mathbb{F}_q$ such that $\nu_{P_\infty}(f_i) = -m_i$, $i = 1, 2, \ldots$. Consider the one point geometric Goppa code

$$C_L(D, m_j P_\infty) := \text{span}_{\mathbb{F}_q} \{ ev_D(f_i) \mid i = 1, \ldots, j \}.$$ 

Let $1 =: i_1 < i_2 < \cdots < i_n$ be such that

$$C_L(D, m_{i_1} P_\infty) \neq C_L(D, m_{i_{i-1}} P_\infty)$$
for $s = 2, \ldots, n$. Define

$$S := \{m_{i_1}, m_{i_2}, \ldots, m_{i_n}\} \subseteq W.$$  

Consider any subset $T \subseteq S$ and the corresponding code

$$E(T) := \text{span}_{\mathbb{F}_q}\{e(v_D(f_i)) \mid m_i \in T\}.$$  

Note, that if $T$ is chosen as the smallest $k$ elements in $S$ then $E(T)$ is a one point geometric Goppa code. Define

$$\sigma: \{ \begin{array}{c} S \rightarrow \mathbb{N} \\ m_{is} \mapsto \#\{m_i \in S \mid \exists m_{iv} \in S \text{ such that } m_{is} + m_{iv} = m_i \} \end{array}$$  

**PROPOSITION**

$$d(E(T)) \geq \min\{\sigma(m_{is}) \mid m_{is} \in T\}.$$  

**COROLLARY**

$$d(C_L(D, mP_\infty)) \geq \min\{\sigma(m_{is}) \mid m_{is} \in S, m_{is} \leq m\} \geq n - \text{deg}(mP_\infty) = n - m$$  

The proof of the proposition simply relies on the following observation. Let $*$ be the componentwise multiplication. Then if

$$\vec{c} * \vec{b}_1, \ldots, \vec{c} * \vec{b}_\sigma$$  

are linearly independent we must have $w_H(\vec{c}) \geq \sigma$.

**References**