Further Improvements on the Feng-Rao Bound for Dual Codes

Olav Geil, Stefano Martin
Aalborg University (Denmark)

stefano@math.aau.dk

Abstract

The famous Feng-Rao bound for the minimum distance of dual codes was born using a language close to that of affine variety codes. Afterwards it was generalized to the level of general linear codes. The first generalized version of the Feng-Rao bound used one basis for $\mathbb{F}_q^n$ and the well-behaving (WB) property. Later formulations use two or three bases of $\mathbb{F}_q^n$, the weakly well-behaving (WWB) property or, even, the one-way well-behaving (OWB) property. It is trivial to prove that the Feng-Rao bound obtained with OWB property is at least as sharp as the one obtained with WWB property which in turn is at least as sharp as the one with WB. Whereas it is known that WWB produces sometimes strictly better results than WB, until now no examples have been known for which OWB produces better results than WWB.
In 2006 Salazar, Dunn and Graham proposed the advisory bound based on the WWB property and the analysis of the syndromes of the dual code. This bound was a new improvement of the Feng-Rao bound for the minimum distance, but they still used a language connected with affine variety codes.

We give several contributions.

- We show that the advisory bound can be generalized for general linear code and that this bound is a consequence of a lemma from which further improvements of Feng-Rao bound can be derived using the OWB property.
- We introduce a new bound for the minimum distance of dual codes which is sometimes strictly sharper than the advisory bound and always at least as good. To obtain our result we use a relaxation of the concept of OWB property.
- We show how to obtain new bounds for generalized Hamming weights of dual codes using the advisory bound and the new bound proposed in our work. We remind the reader that generalized Hamming weight is relevant for the analysis of wiretap channels of type II, secret sharing schemes based on error correcting codes and the computation of the trellis complexity of a linear code.
- We compare these bounds to each other in illustrative examples. These examples are obtained by analyzing the codes over optimal generalized C_{ab} curves over $\mathbb{F}_q$ (C_{ab} curves with no assumptions on $\gcd(a, b)$ and with aq roots). Furthermore they demonstrate for the first time in the literature that the Feng-Rao bound with OWB can sometimes be strictly sharper than the one equipped with WWB.

In our examples we generate several tables comparing the performances of the bounds.

Example:
Consider $X^4-Y^6+X^2+X-Y^5-Y^3 \in \mathbb{F}_8[X,Y]$ and the corresponding variety $\{P_1,\ldots,P_{32}\}$. Let $\prec_w$ be the weighted degree lexicographic ordering with $w(X)=3$, $w(Y)=2$ and $X \succ_{\text{Lex}} Y$. Consider the footprint
$\Delta_{\prec_w}\left(\left\langle X^4-Y^6+X^2+X-Y^5-Y^3, X^8-X, Y^8-Y\right\rangle\right)=\{N_1,\ldots,N_{32}\}$; enumerated with respect to $\prec_w$. Write $\vec{w}_i=(N_i(P_1),\ldots,N_i(P_n))$ for $i=1,\ldots,32$ and define the dual code $C(s)=\{\vec{c}\in\mathbb{F}_8^{32} \mid \vec{c}\cdot\vec{w}_1=\ldots=\vec{c}\cdot\vec{w}_s=0\}$. We derive the results in Figure 1.

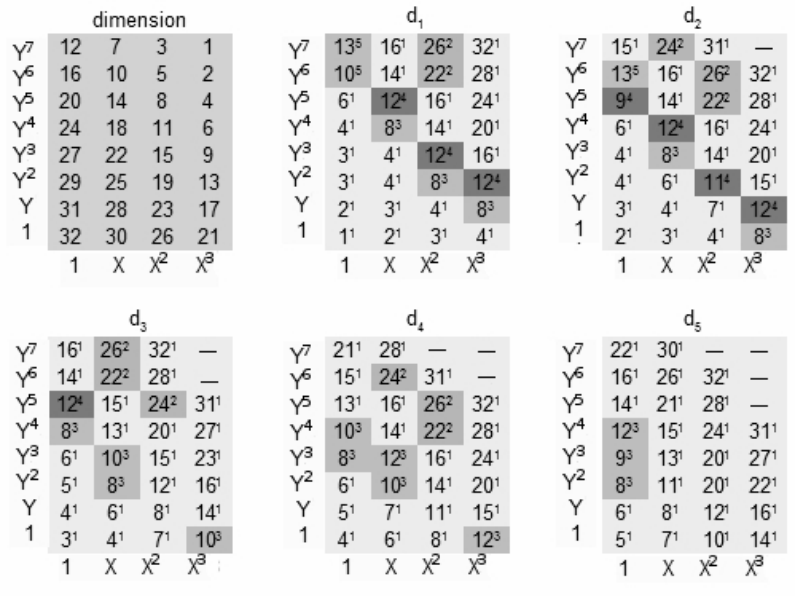

Figure 1: The figure lists the dimensions of codes $C(s)$ over $\mathbb{F}_8$ and corresponding estimates on the generalized Hamming weights $d_1,\ldots,d_5$. Information about $C(s)$ is placed in position $\vec{w}_{s+1}$. An entry z^1 means that the value z was obtained from the Feng-Rao bound with WB, z^2 indicates that the same bound with WWB was used, and finally z^3 the same bound with OWB. With z^4 we indicate that the value z was obtained from the advisory bound and by z^5 that the bound proposed in our work was used.

Keywords
Coding Theory, Feng-Rao Bound, Generalized Hamming Weight