Footprints or Generalized Bezout's Theorem

Olav Geil[1], *Student Member, IEEE* ,
and Tom Høholdt[2] *Senior Member, IEEE.*

June 16, 2000

[1]Olav Geil is with Department of Mathematical Sciences, Aalborg University, Frederik Bajersvej 7E, DK-9220 Aalborg Ø, Denmark (email: geil@math.auc.dk).

[2]Tom Høholdt is with Department of Mathematics, Technical University of Denmark, Bldg 303, DK-2800 Lyngby, Denmark (email: tom@mat.dtu.dk)

Abstract

In two recent papers the first by Feng, Rao, Berg and Zhu and the second by Feng, Zhu, Shi and Rao, the authors use a generalization of Bezout's theorem to estimate the minimum distance and generalized Hamming weights for a class of error correcting codes obtained by evaluation of polynomials in points of an algebraic curve. The main aim of this note is to show that instead of using this rather complex method the same results and some improvements can be obtained by using the so-called footprint from Gröbner basis theory. We also develop the theory further such that the minimum distance and the generalized Hamming weights can not only be estimated but can actually be determined.

Keywords

Evaluation Codes, generalized Hamming weights, minimum distance.

II.16.1 Introduction

In this paper we study the generalized Hamming weights for linear codes and for duals of evaluation codes in particular. The material is a natural continuation of the material presented in [2], [3] and [4].
The idea of generalized Hamming weights for a linear code is to generalize the concept of the minimum distance. We have the following definition. Given

$$U = \{\boldsymbol{u_1} = (u_{11}, \ldots, u_{1n}), \ldots, \boldsymbol{u_s} = (u_{s1}, \ldots, u_{sn})\} \subseteq \mathbb{F}_q^n$$

define the support of U to be

$$\mathrm{Supp}(U) := \{i \mid \exists \boldsymbol{u_j} \in U \text{ with } u_{ji} \neq 0\}.$$

Consider a linear code C of dimension k. For $h = 1, \ldots, k$, the h.th generalized Hamming weight is defined to be

$$d_h := \min\{\#\mathrm{Supp}(U) \mid U \text{ is a linear subcode of } C \text{ of dimension } h\}.$$

The set $\{d_1, \ldots, d_k\}$ is called the weight hierarchy for C.
In this paper we first state a method to determine/estimate the generalized Hamming weights of any linear code with known parity check matrix. In the case of a dual code to an evaluation code this method involves the estimation of the size of certain varieties. The so-called footprint bound that is a very suitable tool for this kind of estimations is used in various cases. Finally we estimate the generalized Hamming weights for the codes presented in [2], comment on the codes presented in [3], and discuss the relation between the method presented in [6] and the method presented in this paper.

II.16.2 Basic results

Let a parity check matrix $H := [\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}]^T$ be given. Define

$$[\boldsymbol{h_i}] := \{\boldsymbol{h_i} + \sum_{j=1}^{i-1} \alpha_j \boldsymbol{h_j} \mid \alpha_j \in \mathbb{F}_q\},$$

for $i = 1, \ldots, r$.

$$D_{\{[\boldsymbol{h_{i_1}}], \ldots, [\boldsymbol{h_{i_s}}]\}} := \max\{n - \#\mathrm{Supp}(\boldsymbol{h'_{i_1}}, \ldots, \boldsymbol{h'_{i_s}}) \mid \boldsymbol{h'_{i_t}} \in [\boldsymbol{h_{i_t}}], t = 1, \ldots, s\}$$

for $1 \leq i_1 < \cdots < i_s \leq r$. And

$$D_s := \max\left\{D_{\{[\boldsymbol{h_{i_1}}], \ldots, [\boldsymbol{h_{i_s}}]\}} \mid 1 \leq i_1 < \cdots < i_s \leq r\right\}$$

for $s = 1, \ldots, r$. There is a strong relation between the numbers D_s and the generalized Hamming weights for the code with parity check matrix H. To prove this relation we will need the following fact originally noted in [8].

Proposition II.16.1
Let C be a code with parity check matrix H. Then $d_h = d^*$ if and only if d^* is the largest number such that any $d^* - 1$ columns of H constitutes a matrix of rank at least $d^* - h$.

The above mentioned relation is.

Theorem II.16.2
Let C be a code of length n with parity check matrix $H = [\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}]^T$ (not necessarily of full rank). For any $d^* \leq r + h$, $h \leq k$, $d^* \leq n$ the following biimplications hold

(i) $d_h \geq d^* \Leftrightarrow D_{r-d^*+h+1} \leq d^* - 2$

(ii) $d_h \leq d^* \Leftrightarrow D_{r-d^*+h} \geq d^*$.

Proof:
(i): From [2] we have the following proof of the $\Leftarrow$ part. Assume $d_h < d^*$. By proposition II.16.1 there exists an $r \times (d^* - 1)$ submatrix $M = [\boldsymbol{m_1}, \ldots, \boldsymbol{m_r}]^T$ of H of rank at most $d^* - h - 1$. Now there are at least $r - (d^* - h - 1)$ rows $\boldsymbol{m_i}$, such that $\boldsymbol{m_i}$ is linearly dependent on $\{\boldsymbol{m_1}, \ldots, \boldsymbol{m_{i-1}}\}$. But then

$D_{r-d^*+h+1} \geq d^* - 1$. We next prove the $\Rightarrow$ part. Assume $D_{r-d^*+h+1} \geq d^* - 1$. But then there exists an $r \times (d^* - 1)$ submatrix M of rank at most

$$r - (r - d^* + h + 1) = d^* - h - 1,$$

and by proposition II.16.1 we must have $d_h < d^*$. *(ii)*: To show the $\Rightarrow$ part assume $D_{r-d^*+h} < d^*$. Then $D_{r-(d^*+1)+h+1} \leq (d^* + 1) - 2$ and from *(i)* we conclude that $d_h \geq d^* + 1$. To show the $\Leftarrow$ part assume $d_h \geq d^* + 1$. By *(i)* we must have $D_{r-(d^*+1)+h+1} \leq d^* - 1$. □

The by far most important part of theorem II.16.2, namely the $\Leftarrow$ part of *(i)* was originally stated in [2] in the special case of duals of evaluation codes.

II.16.3 Duals of evaluation codes

Let $V = \{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q^m$ be a variety, say $V = \mathcal{V}_{\mathbb{F}_q}(I)$ where

$$\begin{aligned} I &= \langle G_1(X_1, \ldots, X_m), \ldots, G_g(X_1, \ldots, X_m) \rangle \\ &\subseteq \mathbb{F}_q[X_1, \ldots, X_m]. \end{aligned}$$

For $F \in \mathbb{F}_q[X_1, \ldots, X_m]$ we denote $\boldsymbol{f} := (F(P_1), \ldots, F(P_n))$. Consider the code with parity check matrix $H := [\boldsymbol{f_1}, \ldots, \boldsymbol{f_r}]^T$. We define

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

for $i = 1, \ldots, r$. And

$$\begin{aligned} D_{\{[F_{i_1}], \ldots, [F_{i_s}]\}} &:= \max\{\#\{P_j \in V \mid F'_{i_1}(P_j) = \cdots = F'_{i_s}(P_j) = 0\} \mid \\ &\qquad F'_{i_t} \in [F_{i_t}],\ t = 1, \ldots, s\} \\ &= \max\{\#\{Q \in \mathbb{F}_q^m \mid F'_{i_1}(Q) = \cdots = F'_{i_s}(Q) = \\ &\qquad G_1(Q) = \cdots = G_g(Q) = 0\} \mid \\ &\qquad F'_{i_t} \in [F_{i_t}],\ t = 1, \ldots, s\} \end{aligned}$$

for $1 \leq i_1 < \cdots < i_s \leq r$. Now the crucial observation is that

$$D_{\{[\boldsymbol{f_{i_1}}], \ldots, [\boldsymbol{f_{i_s}}]\}} = D_{\{[F_{i_1}], \ldots, [F_{i_s}]\}},$$

and in particular that

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

By theorem II.16.2 the problem of estimating the generalized Hamming weights is translated to the problem of estimating the number of common solutions to certain sets of polynomial equations. Or in other words to the problem of estimating the size of certain varieties.
One might get the idea that equality in $D_{r-d^*+h+1} \leq d^* - 2$ implies $d_h = d^*$. The following example shows that this is certainly not the case.

Example II.16.3
Let $V := \mathbb{F}_2^2$ *and consider the code over* $\mathbb{F}_2$ *with parity check matrix* $H := [\mathbf{1}, \boldsymbol{x}, \boldsymbol{y}]^T$. *Clearly* $D_3 = 0$, $D_2 = 1$, $D_1 = 2$. *Now equality holds in both* $D_3 \leq 2 - 2$, $D_2 \leq 3 - 2$ *and in* $D_1 \leq 4 - 2$.

II.16.4 The footprint bound

Given an ideal $I \subseteq k[X_1, \ldots, X_m]$ then the size of the variety $\mathcal{V}_{\bar{k}}(I)$ ($\bar{k}$ denotes the algebraic closure of k) is bounded by the footprint bound. To state this bound we will need some definitions. Let a monomial ordering $\prec$ on $k[X_1, \ldots, X_m]$ be given (see [1, p. 53] for a definition of monomial orderings). The footprint of I with respect to $\prec$ is

$$\begin{aligned}\Delta_\prec(I) \quad := \quad & \{M \text{ a monomial in } k[X_1, \ldots, X_m] \mid M \text{ is not} \\ & \text{a leading monomial of any polynomial in } I\}.\end{aligned}$$

When the monomial ordering is clear from the context we will use the abbreviated notation $\Delta(I)$. Varying the monomial ordering will in general change the related footprint. However whenever the size (of one of them) is finite this will be independent of the choice of $\prec$. Given a finite set of generators of I then we can use Buchberger's algorithm to determine the footprint $\Delta(I)$ exact. In this paper however the generators will not be completely specified, implying that we can only use some parts of Buchberger's algorithm. The following theorem known as the footprint bound can be found in various textbooks on Gröbner basis theory, e.g. in [1, §5.3]. See also [5].

Theorem II.16.4
Let $I \subseteq k[X_1, \ldots, X_m]$ *be an ideal. If* $\Delta_\prec(I)$ *is finite then* $\#\mathcal{V}_{\bar{k}}(I) \leq \#\Delta_\prec(I)$. *Equality holds whenever* I *is a radical ideal.*

Recall that we want to estimate the number of common solutions in $\mathbb{F}_q^m$ to an equation set

$$E : \begin{cases} F_1(X_1, \ldots, X_m) &= 0 \\ &\vdots \\ F_s(X_1, \ldots, X_m) &= 0. \end{cases} \tag{II.16.1}$$

Now we are not interested in the ideal $I := \langle F_1, \ldots, F_s \rangle \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ but in the corresponding variety. So we can replace I by any other ideal with the same variety. In particular we can replace I with

$$\langle F_1, \ldots, F_s, X_1^q - X_1, \ldots, X_m^q - X_m \rangle.$$

In this way we are sure always to get finite footprints.
This adding new defining polynomials of course corresponds to adding new equations to the equation set E. Now let E be any equation set of the form (II.16.1). Given a monomial ordering $\prec$ on $\mathbb{F}_q[X_1, \ldots, X_m]$ we define the ideal $I_{lead} := \langle \mathrm{lm}(F_1), \ldots, \mathrm{lm}(F_s) \rangle$. It is clear that $\Delta_\prec(I) \subseteq \Delta_\prec(I_{lead})$ giving us the immediate bound that the number of solutions to (II.16.1) is at most $\#\Delta_\prec(I_{lead})$. Note that I_{lead} depends on the choice of representation of I and on the choice of monomial ordering as well. One of the most important tools in the calculations in the remaining part of this paper will be to add more equations to (II.16.1) to lower the value $\#\Delta(I_{lead})$.
Note that an important advantage of theorem II.16.4 in comparison with the generalized Bezout's theorem for more than two polynomials is that we do not need to check whether these have components in common.

II.16.5 Estimating the number of common zeros - examples

All the propositions in this section but the last one are more or less generalized versions of results stated in [3] and [4]. To demonstrate the strength of the footprint theory we include new proofs that are in general more simple than the original ones that are based on the generalized Bezout's theorem. Also the footprint theory suggests some generalizations and two important corollaries.

Proposition II.16.5
Let natural numbers i_s and j_s be given where $i_1 > i_2 > \cdots > i_n = 0$ and

$0 = j_1 < j_2 < \cdots < j_n$. *Consider*

$$\begin{aligned} G_1(X,Y) &= F_{10}(Y)X^{i_1} + F_{11}(Y)X^{i_1-1} + \cdots + F_{1i_1}(Y) \\ G_2(X,Y) &= F_{20}(Y)X^{i_2} + F_{21}(Y)X^{i_2-1} + \cdots + F_{2i_2}(Y) \\ &\vdots \\ G_n(X,Y) &= F_{n0}(Y)X^{i_n} + F_{n1}(Y)X^{i_n-1} + \cdots + F_{ni_n}(Y) \end{aligned}$$

where $F_{i0}(Y)$, $i = 1, \ldots, n$ *is a polynomial of degree* j_i. *The equation set* $G_1(X,Y) = G_2(X,Y) = \cdots = G_n(X,Y) = 0$ *has at most* $j_2(i_1 - i_2) + j_3(i_2 - i_3) + \cdots + j_n i_{n-1}$ *solutions.*

Proof:
Consider the pure lexicographic ordering $\prec_{plex}$ on $k[X,Y]$ where $X^{\alpha_1}Y^{\beta_1} \prec_{plex} X^{\alpha_2}Y^{\beta_2}$ whenever either $\alpha_1 < \alpha_2$ or $\alpha_1 = \alpha_2$ and $\beta_1 < \beta_2$. The leading monomial of G_s, $s = 1, \ldots, n$ is $\mathrm{lm}(G_s) = X^{i_s}Y^{j_s}$. In particular $\mathrm{lm}(G_1) = X^{i_1}$ and $\mathrm{lm}(G_n) = Y^{j_n}$. Define

$$I := \langle G_1(X,Y), \ldots, G_n(X,Y) \rangle \subseteq k[X,Y]$$

and let I_{lead} be given as in the previous section. We have

$$\Delta(I_{lead}) = \{X^iY^j \mid \text{not both } i \geq i_s \text{ and } j \geq j_s, \text{ for any } s = 1, \ldots, n\}$$

The number of monomials in $\Delta(I_{lead})$ is

$$\begin{aligned} & i_1 j_n - (i_1 - i_2)(j_n - j_2) - (i_2 - i_3)(j_n - j_3) \\ & - \cdots - (i_{n-2} - i_{n-1})(j_n - j_{n-1}) \\ = \; & j_2(i_1 - i_2) + j_3(i_2 - i_3) + \cdots + j_n i_{n-1}. \end{aligned}$$

□

The footprint technique suggests a sharpening of [4, Th. 3.2].

Proposition II.16.6
Consider

$$\begin{aligned} G_1(X,Y,Z) &= X^{i_1} + F_{11}(Y,Z)X^{i_1-1} + \cdots + F_{1i_1}(Y,Z) \\ G_2(X,Y,Z) &= Y^{j_2} + F_{21}(Z)Y^{j_2-1} + \cdots + F_{2j_2}(Z) \\ G_3(X,Y,Z) &= Z^{k_3} + F_{31}Z^{k_3-1} + \cdots + F_{3k_3} \\ H_4(X,Y,Z) &= F_{40}(Y,Z)X^{i_4} + F_{41}(Y,Z)X^{i_4-1} + \cdots + F_{4i_4}(Y,Z). \end{aligned}$$

Let $Y^{j_4}Y^{k_4}$ be the leading monomial of $F_{40}(Y,Z)$ with respect to the pure lexicographic ordering where $Z \prec_{plex} Y \prec_{plex} X$. The number of solutions to the equation set

$$\begin{aligned} &G_1(X,Y,Z) = G_2(X,Y,Z) \\ &= G_3(X,Y,Z) = H_4(X,Y,Z) = 0 \end{aligned} \tag{II.16.2}$$

is at most $i_1j_2k_3 - (i_1 - i_4)(j_2 - j_4)(k_3 - k_4)$ whenever $i_1 \geq i_4$, $j_2 \geq j_4$, $k_3 \geq k_4$ and is at most equal to $i_1j_2k_3$ when not.

Proof:
Let I be the ideal generated by $G_1(X,Y,Z), \ldots, H_4(X,Y,Z)$. Define $j_1 = k_1 = i_2 = k_2 = i_3 = j_3 = 0$. Using the monomial ordering from the proposition we get

$$\Delta(I_{lead}) = \{X^iY^jZ^k \mid \text{not all } i \geq i_s, j \geq j_s, k \geq k_s \text{ for any } s = 1, \ldots, 4\}.$$

□

Remark II.16.7
Let a monomial ordering be specified on the polynomial ring $k[\boldsymbol{X}]$. Let two equation sets $E^{(1)}$ with corresponding ideals $I^{(1)}, I^{(1)}_{lead} \subseteq k[\boldsymbol{X}]$ and $E^{(2)}$ with corresponding ideals $I^{(2)}, I^{(2)}_{lead} \subseteq k[\boldsymbol{X}]$ be given. It is clear that the number of elements that are a solution to the equation set $E : E^{(1)}, E^{(2)}$ is bounded above by

$$\#\left(\Delta\left(I^{(1)}_{lead}\right) \cap \Delta\left(I^{(2)}_{lead}\right)\right) \tag{II.16.3}$$

in the case of this being finite. Actually the argument of (II.16.3) is the ideal I_{lead} corresponding to E.

From remark II.16.7 it is clear how one should handle the situation where an extra equation

$$F_{50}(Y,Z)X^{i_5} + F_{51}(Y,Z)X^{i_5-1} + \cdots + F_{5i_5}(Y,Z) = 0$$

is added to (II.16.2). This is preciously the case in [4, Th. 3.3] meaning that we have an easy proof of this theorem also.
In [4] it is implicit assumed that $j < b$ in the following proposition. We do not need this assumption.

Proposition II.16.8
Define a weighted degree function on $k[X,Y]$ by weights $w(X) = b$ and $w(Y) = a$. Consider

$$\begin{aligned} F(X,Y) &= X^a + \alpha Y^b + F'(X,Y) \\ G(X,Y) &= X^i Y^j + G'(X,Y) \end{aligned}$$

where α is nonzero 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.

Proof:
Consider the weighted degree lexicographic ordering on $k[X,Y]$ given by the weighted degree function from the proposition in combination with the lexicographic ordering $X \prec_{lex} Y$. Now $\mathrm{lm}(F) = Y^b$ and $\mathrm{lm}(G) = X^i Y^j$. If $j \geq b$ then we replace $X^i Y^j$ in $G(X,Y)$ by $\alpha^{-1} X^i Y^{j-b}(-X^a - F'(X,Y))$. The leading monomial of the polynomial derived in this way is $X^{i+a} Y^{j-b}$. We continue the process un till we finally get a polynomial $\tilde{G}(X,Y)$ with leading monomial $X^{\tilde{i}} Y^{\tilde{j}}$ such that $\tilde{j} < b$. Note that $w(X^i Y^j) = w(X^{\tilde{i}} Y^{\tilde{j}})$ and note that $\tilde{G}(X,Y)$ lies in the ideal $I := \langle F(X,Y), G(X,Y) \rangle$. Another polynomial in I is the S-polynomial

$$S(F, \tilde{G}) = X^{\tilde{i}} F(X,Y) - \alpha Y^{b-\tilde{j}} \tilde{G}(X,Y)$$

with leading monomial $X^{a+\tilde{i}}$. Now

$$\Delta(I) \subseteq \{X^\alpha Y^\beta \mid \alpha < a + \tilde{i}, \beta < b, \text{ not both } \alpha \geq \tilde{i} \text{ and } \beta \geq \tilde{j}\}.$$

The last being of size equal to

$$\begin{aligned} & (a + \tilde{i})b - (a + \tilde{i} - \tilde{i})(b - \tilde{j}) \\ = \; & w(X^{\tilde{i}} Y^{\tilde{j}}) = w(X^i Y^j) = bi + aj. \end{aligned}$$

□

The following two corollaries are new.

Corollary II.16.9
Define a weighted degree function by $w(X) = c$, $w(Y) = a + b$. Consider

$$\begin{aligned} F(X,Y) &= X^i Y^j + \alpha X^a + F'(X,Y) \\ G(X,Y) &= X^{i+b} Y^j + \beta Y^c + G'(X,Y) \end{aligned}$$

where α, β are nonzero and where $ci + (a+b)j > ac > \mathrm{wdeg}(F')$ and $\mathrm{wdeg}(G') < ac + bc$. The equation set $F(X,Y) = G(X,Y) = 0$ has at most $(a+b)j + ci$ solutions.

Proof:
Consider the S-polynomial

$$\begin{aligned} H(X,Y) &:= X^b F(X,Y) - G(X,Y) \\ &= \alpha X^{a+b} - \beta Y^c + H'(X,Y) \end{aligned}$$

where $\mathrm{wdeg}(H') < w(X^{a+b}) = w(Y^c)$. By proposition II.16.8 we get at most

$$(a+b)j + ci$$

solutions to $F(X,Y) = H(X,Y) = 0$. □

The generality of the following corollary is seen from the proof of proposition II.16.8.

Corollary II.16.10
Define a weighted degree function as in proposition II.16.8. Consider

$$\begin{aligned} F(X,Y) &= X^a + \alpha Y^b + F'(X,Y) \\ G(X,Y) &= X^i Y^j + G'(X,Y) \end{aligned}$$

where α is nonzero $a, b > 0$, $j \leq b$, $w(G') < bi + aj$, $w(F') \leq ab$ and any monomial in F' of weight ab is neither X^a, Y^b nor $X^s Y^t$ where $t < j$. The equation set $F(X,Y) = G(X,Y) = 0$ has at most $bi + aj$ solutions.

Proof:
The last assumption ensures that $S(F,G)$ can be reduced modulo G to a polynomial with leading monomial X^{a+i}. □

From remark II.16.7 and the proof of proposition II.16.8 it is clear how one should handle the equation set

$$\begin{aligned} X^a + \alpha Y^b + F'(X,Y) &= 0 \\ X^{i_1} Y^{j_1} + G'_1(X,Y) &= 0 \\ X^{i_2} Y^{j_2} + G'_2(X,Y) &= 0 \\ &\vdots \\ X^{i_n} Y^{j_n} + G'_n(X,Y) &= 0. \end{aligned}$$

This observation replace a rather long proof from [4] of their theorem 4.2. Finally the footprint technique suggest a sharpening of [4, Th. 4.3].

Proposition II.16.11
Define a weighted degree function on $k[X,Y,Z]$ *by* $w(X) = b^2$, $w(Y) = ab$ *and* $w(Z) = a^2$. *Consider*

$$\begin{aligned} G_1(X,Y,Z) &= X^a + \alpha Y^b + G_1'(X,Y,Z) \\ G_2(X,Y,Z) &= Y^a + \beta Z^b + G_2'(X,Y,Z) \\ G_3(X,Y,Z) &= X^i Y^j Z^k + G_3'(X,Y,Z) \end{aligned}$$

where α, β *are nonzero and where* $\mathrm{wdeg}(G_1') < ab^2$, $\mathrm{wdeg}(G_2') < a^2 b$, $\mathrm{wdeg}(G_3') < ib^2 + jab + ka^2$. *The equation set* $G_1(X,Y,Z) = G_2(X,Y,Z) = G_3(X,Y,Z) = 0$ *has at most* $\mathrm{wdeg}(G_3) = ib^2 + jab + ka^2$ *solutions.*

Proof:
Wlog. we assume $\alpha = \beta = 1$. Consider the weighted degree lexicographic ordering on $k[X,Y,Z]$ given by the weighted degree function from the proposition in combination with the lexicographic ordering $Z \prec_{lex} Y \prec_{lex} X$. We will wlog. assume that $a \geq b$. Now G_3 can be reduced modulo $\{G_1, G_2\}$ to a polynomial with leading monomial $X^{\tilde{i}} Y^{\tilde{j}} Z^{\tilde{k}}$ where $\tilde{i}, \tilde{j} < a$. Clearly $w(X^{\tilde{i}} Y^{\tilde{j}} Z^{\tilde{k}}) = w(G_3)$. To ease the notation we assume in the following wlog. that G_3 is of this form from the beginning. There are two cases to consider.
Case I $a < b + j$:
The S-polynomial $S(G_1, G_3) = Y^{b+j} Z^k + \cdots$ is reduced modulo G_2 to

$$G_4 := Y^{b+j-a} Z^{b+k} + \cdots .$$

Further let

$$\begin{aligned} G_5 &:= S(G_2, G_4) = Z^{2b+k} + \cdots \\ G_6 &:= S(G_2, G_3) = X^i Z^{b+k} + \cdots . \end{aligned}$$

All together we can detect the following leading monomials from $\langle G_1, G_2, G_3 \rangle$, namely

$$\{X^a, Y^a, Z^{2b+k}, X^i Y^j Z^k, Y^{b+j-a} Z^{b+k}, X^i Z^{b+k}\}$$

and the bound follows.
Case II $a \geq b + j$:
We get the following S-polynomials

$$\begin{aligned} G_4 &:= S(G_1, G_3) = Y^{j+b} Z^k + \cdots \\ G_5 &:= S(G_2, G_4) = Z^{b+k} + \cdots \end{aligned}$$

and the bound follows. □

Inspired by some examples in [2] we state the following proposition.

Proposition II.16.12
Consider

$$\begin{aligned} F(X,Y) &= Y + \alpha X + \beta \\ G(X,Y) &= G_1(X,Y) + G_2(X,Y) \end{aligned}$$

where G_1 is irreducible and homogeneous of multidegree $m > 1$, and where G_2 is of multidegree less than m. The equation set $F(X,Y) = G(X,Y) = 0$ has at most m solutions.

Proof:
Substitute $Y + \alpha X + \beta$ in $G(X,Y)$ to get a polynomial $H(X)$ of degree at most m. If $H(X)$ is not the zero polynomial then the proposition follows at once. It remains to show that $H(X)$ can not be the zero polynomial. The coefficient to X^m in $H(X)$ is $G_1(1,\alpha)$. Now $G_1(1,\alpha) = 0$ would imply $G_1(1,T) = (T-\alpha)L(T)$ giving us $G_1(X,Y) = X^n G_1(1,Y/X) = (Y-\alpha)L'(X,Y)$, a contradiction to our assumptions. □

II.16.6 The weight hierarchies

In the following we will estimate and in one case find the weight hierarchy for the codes treated in [2]. The minimum distances of these codes were estimated in [2] by use of the generalized Bezout's theorem. We will estimate the generalized Hamming weights using the footprint technique and the classical Bezout's theorem. We will often specify a weighted degree lexicographic ordering $\prec_w$ with respect to which we will estimate the footprint $\Delta(I_{lead})$. We will choose linearly dependent weights but in a way such that the choice of lexicographic part of $\prec_w$ is insignificant to our purpose. Therefore we will only specify the values $w(X)$ and $w(Y)$.

II.16.6.1 Improved Klein codes

Let V be the 22 points on the Klein curve $X^3Y + Y^3 + X = 0$ over $\mathbb{F}_8$. Consider the code over $\mathbb{F}_8$ with parity check matrix

$$H := [\mathbf{1}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}^2, \boldsymbol{xy}, \boldsymbol{x}^3, \boldsymbol{y}^2]^T.$$

We will find the values D_1, D_2 and estimate the value D_3.
We first determine D_1. $D\{[1]\} = 0$ is obvious. $D_{\{[X]\}} \leq 3$ is seen as follows.

We want to estimate the maximal number of solutions in $\mathbb{F}_8^2$ to the equation set

$$\begin{aligned} X + a &= 0 \\ X^3Y + Y^3 + X &= 0 \end{aligned}$$

whenever $a \in \mathbb{F}_8$. We insert $X = a$ in $X^3Y + Y^3 + X$ to get a nonzero polynomial in Y of degree at most 3. $D_{\{[Y]\}} \leq 4$ is seen as follows. We want to solve

$$\begin{aligned} Y + aX + b &= 0 \\ X^3Y + Y^3 + X &= 0. \end{aligned}$$

If $a = 0$ then we proceed as above and get a most 3 solutions. If $a \neq 0$ then we use proposition II.16.8 and get at most 4 solutions. $D_{\{[X^2]\}} \leq 6$ is seen as follows. We want to solve

$$\begin{aligned} X^2 + aY + bX + c &= 0 \\ X^3Y + Y^3 + X &= 0. \end{aligned}$$

By choosing $w(X) = 1$ and $w(Y) = 1.6$ we get

$$\Delta(I_{lead}) = \{1, X, Y, Y^2, XY, XY^2\}.$$

$D_{\{[XY]\}} \leq 7$ is seen in the following way. We study the equation set

$$\begin{aligned} XY + aX^2 + bY + cX + d &= 0 \\ X^3Y + Y^3 + X &= 0. \end{aligned}$$

If $a \neq 0$ then by corollary II.16.9 we get at most 7 solutions. If $a = 0$ then the resultant with respect to X is

$$\begin{vmatrix} c+Y & bY+d & 0 & 0 \\ 0 & c+Y & bY+d & 0 \\ 0 & 0 & c+Y & bY+d \\ Y & 0 & 1 & Y^3 \end{vmatrix}$$

that is a polynomial in Y of degree 6. So by Bezout's theorem there are at most 6 solutions when $a = 0$. $D_{\{[X^3]\}} \leq 9$ is seen by choosing $w(X) = 1, w(Y) = 1.6$. $D_{\{[Y^2]\}} \leq 9$ is seen in the following way. We study the equation set

$$\begin{aligned} Y^2 + aX^3 + bXY + cX^2 + dY + eX + f &= 0 \\ X^3Y + Y^3 + X &= 0. \end{aligned}$$

If $a \neq 0$ then by proposition II.16.8 we have at most 9 solutions. If $a = 0$ but $c \neq 0$ then by corollary II.16.10 there is at most 8 solutions. Assume now $a = c = 0$. The resultant with respect to X is

$$\begin{vmatrix} bY+e & Y^2+dY+f & 0 & 0 \\ 0 & bY+e & Y^2+dY+f & 0 \\ 0 & 0 & bY+e & Y^2+dY+f \\ Y & 0 & 1 & Y^3 \end{vmatrix}$$

that is a polynomial of degree 7. So by Bezout's theorem we have at most 7 solutions. All together $D_1 \leq 9$. By inspection the equation set

$$\begin{aligned} X^3+XY+X^2+Y+X+1 &= 0 \\ X^3Y+Y^3+X &= 0. \end{aligned}$$

has the 9 solutions $(1,\alpha)$, $(1,\alpha^2)$, $(1,\alpha^4)$, (α,α^6), (α^2,α^5), (α^3,α^2), (α^4,α^3), (α^5,α) and (α^6,α^4) where α is a root in T^3+T+1. So $D_{\{[X^3]\}} \geq 9$ and we conclude $D_1 = 9$.

Next we determine D_2. $D_{\{[1],*\}} = 0$, $D_{\{[X],*\}} \leq 3$, $D_{\{[Y],*\}} \leq 4$ and $D_{\{[X^2],*\}} \leq 6$ follows from above. $D_{\{[XY],[X^3]\}} \leq 5$ is seen in the following way. We study the equation set

$$\begin{aligned} XY+aX^2+bY+cX+d &= 0 \\ X^3+eX^2+fY+gX+h &= 0 \\ X^3Y+Y^3+X &= 0. \end{aligned}$$

If $f \neq 0$ then we use proposition II.16.8 on the first two equations to give at most 4 solutions. If $f = 0$ then we solve the second equation to get at most 3 solutions. The ones that are different from b are inserted in the first equation to give unique corresponding Y values. If eventually b is a solution to the second equation, then we insert $X = b$ in the third equation to get at most 3 corresponding Y values. All together we get at most 5 solutions. $D_{\{[XY],[Y^2]\}} \leq 5$ is seen as follows. We study the equation set

$$\begin{aligned} XY+aX^2+bY+cX+d &= 0 \\ Y^2+eX^3+fX^2+gY+hX+i &= 0 \\ X^3Y+Y^3+X &= 0. \end{aligned}$$

If $e \neq 0$ then by proposition II.16.8 we get at most 5 solutions. If $e = 0$ but $a \neq 0$ then we consider

$$\begin{aligned} & S(F_1,F_2) \\ = \; & X^2(XY+aX^2+bY+cX+d)+X^3Y+Y^3+X \\ = \; & aX^4+Y^3+bX^2Y+cX^3+dX^2+X. \end{aligned}$$

Choose $w(X) = 1, w(Y) = 1.1$ to get $\Delta(I_{lead}) = \{1, Y, X, X^2, X^3\}$. If $e = a = 0$ and not both $f = 0$ and $h = 0$ then we use proposition II.16.8 on the first two equations to get at most 4 respectively 3 solutions. Finally if $e = a = f = h = 0$ then we solve the second equation and insert the solutions into the first respectively the third equation to get at most 5 solutions. $D_{\{[X^3],[Y^2]\}} \leq 6$ is obvious. All together $D_2 \leq 6$. By inspection the equation set

$$\begin{aligned} X^2 + Y + 1 &= 0 \\ X^3 + XY + X^2 + Y + X + 1 &= 0 \\ X^3Y + Y^3 + X &= 0 \end{aligned}$$

has the solutions (α, α^6), (α^2, α^5), (α^3, α^2), (α^4, α^3), (α^5, α) and (α^6, α^4). So $D_{\{[X^2],[X^3]\}} \geq 6$ and we conclude $D_2 = 6$.
Next we estimate D_3. $D_{\{[1],*,*\}} = 0$, $D_{\{[X],*,*\}} \leq 3$, $D_{\{[Y],*,*\}} \leq 4$ follows from above. $D_{\{[X^2],*,[Y^2]\}} \leq 4$ follows by choosing $w(X) = 1, w(Y) = 1.6$. $D_{\{[XY],[X^3],[Y^2]\}} \leq 4$ and $D_{\{[X^2],[XY],[X^3]\}} \leq 4$ follows in exactly the same way. All together $D_3 \leq 4$.
Now to the parameters of the code. Obviously $n = 22$. We next determine the weight hierarchy. We get $d_1 = 6$ as $D_{7-6+1+1} = D_3 \leq 4$ but $D_2 \geq 6$. We get $d_2 = 8$ as $D_{7-8+2+1} = D_2 \leq 6$ but $D_1 \geq 8$. And we get $d_3 = 9$ as $D_{7-10+3+1} = D_1 \not\leq 10-2 = 8$. Now on the one hand $d_i \geq i+7$ for $i = 4, \ldots, k$ as $D_{\{7-(i+7)+i+1\}} = D_1 \leq 9$. And on the other hand the Singleton type bound implies $d_i \leq i + (n-k)$ for any $i \leq k$. Now $n-k$ can not exceed the number of rows in H. So we conclude $n - k = 7$ and $k = 15$. And we conclude $d_i = i + 7$ for $i = 4, \ldots, 15$. Note that the consideration concerning the weight hierarchy gave us a proof that the row vectors in H are linearly independent.

Now let V be unchanged but consider the code with parity check matrix

$$H := [\mathbf{1}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}^2, \boldsymbol{xy}, \boldsymbol{x}^3 + \boldsymbol{y}^2]^T.$$

From [2] we know that $D_3 \leq 3$. We now estimate the values D_1 and D_2. We first consider D_1. $D_{\{[1]\}} = 0$ is obvious. $D_{\{[X]\}} \leq 3$ respectively $D_{\{[Y]\}} \leq 3$ is found by inserting $X = a$ respectively $Y = aX + b$ in $X^3Y + Y^3 + X$ to get a nonzero polynomial in Y of degree at most 3. $D_{\{[X^2]\}} \leq 6$ follows by choosing $w(X) = 1, w(Y) = 1.6$. $D_{\{[XY]\}} \leq 7$ is seen in the following way. We study the equation set

$$\begin{aligned} XY + aX^2 + bY + cX + d &= 0 \\ X^3Y + Y^3 + X &= 0. \end{aligned}$$

If $a \neq 0$ then by corollary II.16.9 there are at most 7 solutions. If $a = 0$ then Bezout's theorem gives at most 6 solutions. $D_{\{[X^3+Y^2]\}} \leq 8$ is seen in the following way. We study the equation set

$$\begin{aligned} X^3 + Y^2 + aXY + bX^2 + cY + dX + e &= 0 \\ X^3Y + Y^3 + X &= 0. \end{aligned}$$

Consider $aXY^2+bX^2Y+cY^2+dXY+eY+X = 0$. If $a \neq 0$ or $b \neq 0$ then we use proposition II.16.8 on the first and third equation to give at most 8 solutions. If $a = b = 0$ but $c \neq 0$ then we choose $w(X) = 1, w(Y) = 1.1$ to give at most 6 solutions. If $a = b = c = 0$ but $d \neq 0$ then we use proposition II.16.8 to give at most 5 solutions. And finally when $a = b = c = d = 0$ we substitute $X = eY$ in $X^3Y + Y^3 + X = 0$ to give at most 3 solutions. All together $D_1 \leq 8$.
We next consider D_2. $D_{\{[X^2],[XY]\}} \leq 4$ and $D_{\{[X^2],[X^3+Y^2]\}} \leq 4$ follows by choosing $w(X) = 1, w(Y) = 1.6$. $D_{\{[XY],[X^3+Y^2]\}} \leq 5$ follows from proposition II.16.8. We conclude $D_2 \leq 5$.
Now to the parameters of the code. Again obviously $n = 22$. And $d_1 \geq 5$, $d_2 \geq 7$, $d_3 \geq 8$, $d_i \geq i + 6$ for $i = 4, \ldots, k$ follows from $D_3 \leq 3$, $D_2 \leq 5$ and $D_1 \leq 8$. The Singleton type bound states that $d_i \leq i + (n - k)$ for any $i \leq k$. Using the fact that $n - k$ can not exceed the number of rows in H we get $k = 16$ and $d_i = i + 6$ for $i = 4, \ldots, 16$.

II.16.6.2 Improved Hermitian code

Let V be the 64 points on the Hermitian curve $X^5 + Y^4 + Y = 0$ over $\mathbb{F}_{16}$. Consider the code over $\mathbb{F}_{16}$ with parity check matrix

$$H := [\mathbf{1}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}^2, \boldsymbol{xy}, \boldsymbol{y}^2, \boldsymbol{x}^3, \boldsymbol{y}^3 + \boldsymbol{x}^4]^T.$$

$D_4 \leq 4$ is shown in [2]. In the following we estimate D_1, D_2 and D_3.
We first consider D_1. $D_{\{[1]\}} = 0$ is obvious. $D_{\{[X]\}} \leq 4$ and $D_{\{[Y]\}} \leq 5$ are seen as in the previous section. $D_{\{[X^2]\}} \leq 8$ follows when $w(X) = 1, w(Y) = 1.3$ is chosen. $D_{\{[XY]\}} \leq 9$ is a consequence of proposition II.16.8. $D_{\{[Y^2]\}} \leq 10$ follows by choosing $w(X) = 1, w(Y) = 1.1$. $D_{\{[X^3]\}} \leq 12$ follows by choosing $w(X) = 1, w(Y) = 1.3$. $D_{\{[Y^3+X^4]\}} \leq 16$ follows by choosing $w(X) = 1, w(Y) = 1.3$. We conclude $D_1 \leq 16$.
We next consider D_2. $D_{\{[1],*\}} = 0$, $D_{\{[X],*\}} \leq 4$, $D_{\{[Y],*\}} \leq 5$ and $D_{\{[X^2],*\}} \leq 8$ follows from above. $D_{\{[XY],[Y^2]\}} \leq 6$ by choosing $w(X) = 1, w(Y) = 1.1$. $D_{\{[XY],[X^3]\}} \leq 6$ follows by choosing $w(X) = 1, w(Y) = 1.3$. $D_{\{[XY],[Y^3+X^4]\}} \leq 7$ follows from proposition II.16.8. $D_{\{[Y^2],[X^3]\}} \leq 6$ and $D_{\{[Y^2],[Y^3+X^4]\}} \leq 8$ follows by choosing $w(X) = 1, w(Y) = 1.1$. We conclude $D_2 \leq 8$.

We next consider D_3. $D_{\{[1],*,*\}} = 0$, $D_{\{[X],*,*\}} \leq 4$ and $D_{\{[Y],*,*\}} \leq 5$ follows from above. $D_{\{[X^2],[Y^2],*\}} \leq 4$ follows by choosing $w(X) = 1, w(Y) = 1.1$. $D_{\{[X^2],[XY],*\}} \leq 5$ by choosing $w(X) = 1, w(Y) = 1.3$. $D_{\{[XY],[Y^2],[X^3]\}} \leq 4$ follows by choosing $w(X) = 1, w(Y) = 1.1$. $D_{\{[XY],[Y^2],[Y^3+X^4]\}} \leq 5$ follows by choosing $w(X) = 1, w(Y) = 1.1$. $D_{\{[XY],[X^3],[Y^3+X^4]\}} \leq 6$ follows by choosing $w(X) = 1, w(Y) = 1.4$. $D_{\{[X^2],[X^3],[Y^3+X^4]\}} \leq 6$ follows by choosing $w(X) = 1, w(Y) = 1.4$. All together $D_3 \leq 6$. From [2] we get as mentioned $D_4 \leq 4$. We note that to show $D_4 \leq 4$ we need only use the Hermitian equation in one case, namely when we consider $D_{\{[X],*,*,*\}}$. We conclude that we could replace the Hermitian polynomial with any polynomial $F(X, Y)$ for which $F(a, Y)$ is a nonzero polynomial of degree at most 4 for any $a \in \mathbb{F}_{16}$. For instance $F(X, Y) = Y^4 + Y + 1$ has 64 zeros also and would give a $[64, 56, \geq 6]$ code.
Now to the parameters of the code from the Hermitian curve. Clearly $n = 64$. Further $d_1 \geq 6$, $d_2 \geq 8$, $d_i \geq i+7$ for $i = 3, \ldots, 9$, $d_i \geq i+8$ for $i = 10, \ldots, k$ follows from $D_1 \leq 16$, $D_2 \leq 8$, $D_3 \leq 6$ and $D_4 \leq 4$. Similar to the previous considered codes we investigate the Singleton type bound and the number of rows in H. We conclude $k = 56$ and $d_i = i + 8$ for $i = 10, \ldots, 56$.
Finally we compare the above code with the conventional Hermitian codes. The Weierstrass semigroup related to the point Q at infinity is $\langle 4, 5\rangle$. Denote by $C(m)$ the image of the usual evaluation map $ev : \mathcal{L}(mQ) \to \mathbb{F}_{16}^{64}$. The dual code with dimension $k = 56$ is $C(13)^{\perp}$. From [10] we get $C(m)^{\perp} = C(n - 2g - 2 - m)$ where g is the genus. So $C(13)^{\perp} = C(61)$. By [10, Th. 6.2] the first six generalized Hamming weights of $C(61)$ are $d_1 = 4$, $d_2 = 7$, $d_3 = 8$, $d_4 = 11$, $d_5 = 12$, $d_6 = 13$. We conclude that not only the minimum distance is improved for the Hermitian code.

II.16.6.3 A family of codes

Let V be $\mathbb{F}_q^2$, where $q > 2$. Let $F(X, Y)$ be any homogeneous irreducible polynomial of degree i, $2 \leq i < q$. Define

$$S := \{M \text{ a monomial in } \mathbb{F}_q[X, Y] \mid \deg_M < i\} \cup \{F(X, Y)\}.$$

Let $\prec$ be the graded lexicographic ordering on $k[X, Y]$ where $X \prec_{lex} Y$ ($w(X) = w(Y)$ in this case). Define

$$r := \#S = 1 + \sum_{j=1}^{i} j = \frac{(i+1)i}{2} + 1,$$

and enumerate the elements in S by $S = \{H_1, \ldots, H_r\}$ such that $H_i \prec H_{i+1}$ for $i = 1, \ldots, r-1$. Consider the code C with parity check matrix

$$H = [\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}]^T.$$

Clearly $n = q^2$. It is well known that

$$\{\boldsymbol{m} \mid M \text{ a monomial in } \mathbb{F}_q[X,Y] \text{ and } \deg_X M, \deg_Y M < q\}$$

is a basis for $\mathbb{F}_q^2$. So H is of full rank and the dimension of C is $k = n - r$. We next estimate the value of D_{r-i}. $D_{\{[1],*,\ldots,*\}} = 0$ as usual. $D_{\{[X],*,\ldots,*\}} \leq i$ as at least one of the $*$'s will be equal to $[Y^a]$ for some a or be equal to $[F(X,Y)]$ (note that $F(X,Y)$ contains the monomial Y^i). $D_{\{[Y],*,\ldots,*\}} \leq i$ is seen in the following way. If $[F(X,Y)]$ is one of the $*$'s then by proposition II.16.12 we have at most i solutions. If $[F(X,Y)]$ is not one of the $*$'s then is at least one of the $[X^a]$'s. $D_{\{*,\ldots,*\}} \leq i$ whenever no of the $*$'s are $[1], [X], [Y]$ is seen as follows. First note that this situation of course only occurs when $i > 2$. Then note that at least one of the $*$'s is of the form $[X^a]$ and also at least one is either $[F(X,Y)]$ or an element of the form $[Y^b]$. Now assume that $\{*, \ldots, *\}$ is chosen such that $D_{\{*,\ldots,*\}}$ is maximal. We observe that if $[X^s Y^t]$ is not one of the $*$'s then will neither $[X^{s'} Y^{t'}]$ where $X^{s'} Y^{t'} | X^s Y^t$ be one of the $*$'s. Combining this with the above observation that there exist $a < i$ and $b \leq i$ such that $X^a, Y^b \in \Delta(I_{lead})$ shows $D_{\{*,\ldots,*\}} \leq i$. We conclude that C is a $[q^2, q^2 - \frac{(i+1)i}{2} - 1, i+2]$ code.
The family of codes presented above is a generalization of the following two codes from [2]. Namely the code over $\mathbb{F}_{2^m}$ with parity check matrix

$$H := [\boldsymbol{1}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}^2 + \beta \boldsymbol{xy} + \boldsymbol{y}^2]^T$$

where β is any element with $tr(\beta^{-1}) = 1$. And the code over $\mathbb{F}_{2^m}$ with parity check matrix

$$H := [\boldsymbol{1}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}^2, \boldsymbol{xy}, \boldsymbol{y}^2, \boldsymbol{x}^3 + \gamma \boldsymbol{x}^2 \boldsymbol{y} + \beta \boldsymbol{xy}^2 + \boldsymbol{y}^3]^T$$

where $X^3 + \gamma X^2 Y + \beta X Y^2 + Y^3$ is irreducible.

II.16.6.4 Codes from $k[X,Y,Z]$

In [3] two examples of codes are given. In the first example a code over $\mathbb{F}_4$ is constructed by

$$V := \mathcal{V}_{\mathbb{F}_4}\left(\langle X^3 + Y^2 + Y, Y^3 + Z^2 + Z \rangle\right)$$

and

$$H := [\mathbf{1}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x^2}, \boldsymbol{z}, \boldsymbol{xy}, \boldsymbol{xz} + \boldsymbol{yz}]^T .$$

It is claimed that the minimum distance is at least 5. However the following observation shows that this is not the case. Consider $D_{\{[Y],[X^2],[XY],[XZ+YZ]\}}$. The equation set

$$\begin{aligned} Y + X + 1 = X^2 + X + 1 = XY + 1 = XZ + YZ + Z \\ = X^3 + Y^2 + Y = Y^3 + Z^2 + Z = 0 \end{aligned}$$

has the solutions $(\alpha, \alpha^2, \alpha)$, $(\alpha, \alpha^2, \alpha^2)$, $(\alpha^2, \alpha, \alpha)$ and $(\alpha^2, \alpha, \alpha^2)$ where α is a zero of $T^2 + T + 1$. It follows that $D_4 \geq 4$ and in particular that $d < 5$. One can very easily show that $D_5 \leq 2$. So the true value of the minimum distance is $d = 4$.

II.16.6.5 Codes constructed from footprints

Consider an affine variety $V = \{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q^m$. Let $\{G_1, \ldots, G_s\} \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ be a Gröbner basis for $I := \mathcal{I}(V)$ wrt. some monomial ordering $\prec$ on the set of monomials in $X_1, \ldots, X_m$. Let $\Delta(I) = \{F_1, \ldots, F_n\}$, where $F_i \prec F_{i+1}$, $i = 1, \ldots, n-1$, be the corresponding footprint (note that $\#V = \#\Delta(I)$ follows from the last part of theorem II.16.4 as $I = \mathcal{I}(V)$ is a radical ideal). Consider the $\mathbb{F}_q$-linear code $C_r^\perp$ (C_r respectively) with parity check matrix (generator matrix respectively)

$$H = [\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}]^T \tag{II.16.6}$$

where $\boldsymbol{h_i} = (F_i(P_1), \ldots, F_i(P_n))$. It is well-known that whenever $I \subseteq k[\boldsymbol{X}]$ is an ideal and $\Delta(I)$ is a footprint, then $\{M + I \mid M \in \Delta(I)\}$ constitutes a basis for $k[\boldsymbol{X}]/I$ as a vector space over k (see [1]). In the present case therefore $\{\boldsymbol{h_1}, \ldots, \boldsymbol{h_n}\}$ constitutes a basis for $\mathbb{F}_q^n$. And in particular $\boldsymbol{h_1}, \ldots, \boldsymbol{h_n}$ are linearly independent, giving $C_r^\perp$ the dimension $k := n - r$ and C_r the dimension r.

In the following we will show how one can derive lower bounds on the generalized Hamming weights of $C_r^\perp$ in a

direct way.
We start by investigating D_1. For a fixed F_i the number of solutions P to

$$F_i(P) + \sum_{j=1}^{i-1} a_j F_j(P) = G_1(P) = \cdots = G_s(P) = 0$$

is bounded by the size of

$$\Delta(\langle F_i + \sum_{j=1}^{i-1} a_j F_j, G_1, \ldots, G_s \rangle).$$

However

$$\Delta(\langle F_i + \sum_{j=1}^{i-1} a_j F_j, G_1, \ldots, G_s \rangle) \subseteq \Delta(I_{lead})$$

where

$$\begin{aligned} I_{lead} &:= \langle \mathrm{lm}(F_i + \textstyle\sum \cdots), \mathrm{lm}(G_1), \ldots, \mathrm{lm}(G_s) \rangle \\ &= \langle F_i, \mathrm{lm}(G_1), \ldots, \mathrm{lm}(G_s) \rangle \\ &= \{ \boldsymbol{X}^{\boldsymbol{\alpha}} \in \Delta(I) \mid F_i \text{ does not divide } \boldsymbol{X}^{\boldsymbol{\alpha}} \}. \end{aligned}$$

Define now

$$\begin{aligned} \Lambda_{\{i\}} &:= \{ \boldsymbol{X}^{\boldsymbol{\alpha}} \mid F_i \text{ divides } \boldsymbol{X}^{\boldsymbol{\alpha}} \} \\ S_1 &:= \min\{ \#(\Lambda_{\{i\}} \cap \Delta(I)) \mid i = 1, \ldots, r \}. \end{aligned}$$

And D_1 is bounded by $D_1 \leq n - S_1$.
To estimate D_j for arbitrary j, $1 \leq j \leq r$, we generalize the above terminology. Define

$$\begin{aligned} \Lambda_{\{i_1,\ldots,i_j\}} &:= \cup_{t=1}^{j} \Lambda_{\{i_t\}} \\ S_j &:= \min\{ \#(\Lambda_{\{i_1,\ldots,i_j\}} \cap \Delta(I)) \mid 1 \leq i_1 < i_2 < \cdots < i_j \leq r \}. \end{aligned}$$

We get that D_j is bounded by $D_j \leq n - S_j$.

Theorem II.16.13
Consider the code $C_r^{\perp}$ over $\mathbb{F}_q$ with parity check matrix given by (II.16.6). Let h, i be integers with $1 \leq h \leq n - r$, $1 \leq i \leq r$. If $r + h - 1 - i \geq n - S_i$ then $d_h \geq n - S_i + 2$.

Proof:
Given h, i where $1 \leq h \leq n-r$, $1 \leq i \leq r$, define $d^* := r+h+1-i$. Assume $r+h-1-i \geq n-S_i$ that is assume $d^* \geq n-S_i+2$. We have

$$D_{r-d^*+h+1} = D_i \leq n - S_i \leq d^* - 2,$$

which by theorem II.16.2 implies $d_h \geq d^*$. But $d^* \geq n-S_i+2$ and the theorem follows. □

II.16.7 Conclusion

We have demonstrated that working with the footprint instead of the generalized Bezout's theorem is easier and also allows one to give more general results. It seems fair to mention that probably Feng et. al are also aware of this fact now. See [9].

Bibliography of part II

[1] David Cox, John Little and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Second Edition. Springer, 1997.

[2] Gui-Liang Feng, T.R.N. Rao, Gene A. Berg, J. Zhu. *Generalized Bezout's Theorem in Its Applications in Coding Theory*. IEEE Trans. Inf. Theory, vol. 43, pp. 1799-1810, nov.1997.

[3] Gui-Liang Feng, Junmei Zhu. Xiaofa Shi and T,R,N. Rao. *The Applications of Generalized Bezout's Theorem to the Codes from the Curves in High Dimensional Spaces.* Proceedings of the 35th Allerton Conference on Communication, Control and Computing, pp.205-214 , 1997.

[4] Gui-Liang Feng, Junmei Zhu, Xinwen Wu and T.R.N. Rao. *High Dimensional Generalized Bezout's Theorem.* Preprint University of Southwestern Lousiana april 1998.

[5] Tom Høholdt. *On (or in) Dick Blahut's "footprint".* In Codes, Curves and Signals (A. Vardy ed.), pp. 3-9 , Kluwer 1998.

[6] Tomoharu Shibuya, Jiro Mizutani and Kohichi Sakaniwa. *On Generalized Hamming Weights of Codes Constructed on Affine Algebraic Sets.* AAECC-12, Lect. Notes Comp. Sc., vol.1255, pp. 311-320, 1997.

[7] Michael A. Tsfasman and Serge G. Vladut. *Geometric Approach to Higher Weights.* IEEE Trans. Inf. Theory, vol.41, pp. 1564-1588, nov.1995.

[8] V. K. Wei. *Generalized Hamming weights for linear codes.* IEEE Trans. Inf. Theory, vol.37, pp. 1412-1418, sept.1991.

[9] Xin-Wen Wu, Gui-Liang Feng, T.R.N. Rao. *Designing a class of Efficient Codes Via Estimating the Number of Zeros of Polynomials.* Preprint University of Southwestern Lousiana april 1999.

[10] A.I. Barbero, C. Munuera. *The weight hierarchy of Hermitian codes.* Preprint University of Valladolid, june 1998.