Aalborg Universitet

AALBORG UNIVERSITY
DENMARK

On the Feng-Rao bound for generalized Hamming weights

Geil, Olav; Thommesen, Christian

Publication date:
2005

Document Version
Publisher's PDF, also known as Version of record

Link to publication from Aalborg University

Citation for published version (APA):
Geil, O., & Thommesen, C. (2005). *On the Feng-Rao bound for generalized Hamming weights*. Research Report Series No. R-2005-33

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

Take down policy
If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from vbn.aau.dk on: April 19, 2024

AALBORG UNIVERSITY

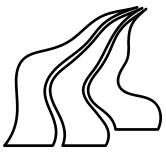
On the Feng-Rao bound for generalized Hamming weights

by

Olav Geil and Christian Thommesen

R-2005-33 November 2005

Department of Mathematical Sciences
Aalborg University
Fredrik Bajers Vej 7 G ▪ DK - 9220 Aalborg Øst ▪ Denmark
Phone: +45 96 35 80 80 ▪ Telefax: +45 98 15 81 29
URL: http://www.math.aau.dk



ISSN 1399–2503 ▪ On-line version ISSN 1601–7811

On the Feng-Rao Bound for Generalized Hamming Weights

Olav Geil and Christian Thommesen

Aalborg University, 9220 Aalborg Øst, Denmark,
olav@math.aau.dk and cthom@math.aau.dk

Abstract. The Feng-Rao bound gives good estimates of the minimum distance of a large class of codes. In this work we are concerned with the problem of how to extend the Feng-Rao bound so that it deals with all the generalized Hamming weights. The problem was solved by Heijnen and Pellikaan in [7] for a large family of codes that includes the duals of one-point geometric Goppa codes and the q-ary Reed-Muller codes, but not the Feng-Rao improved such ones. We show that Heijnen and Pellikaan's results holds for the more general class of codes for which the traditional Feng-Rao bound can be applied. We also establish the connection to the Shibuya-Sakaniwa bound for generalized Hamming weights ([15], [16], [17], [18], [19] and [20]). More precisely we show that the Shibuya-Sakaniwa bound is a consequence of the extended Feng-Rao bound. In particular the extended Feng-Rao bound gives always at least as good estimates as does the Shibuya-Sakaniwa bound.

1 Introduction

In [3] and [4] Feng and Rao showed how to estimate the minimum distance of a large class of algebraically defined codes by considering certain relations between the rows in the corresponding parity check matrices. This result is known today as the Feng-Rao bound. Using the bound Feng and Rao were able to improve a large class of well-known codes by leaving out certain rows in the corresponding parity check matrices. Since the emergence of the Feng-Rao bound quite a lot of research has been done on the subject. In the present paper we will present a new point of view on how to extend the Feng-Rao bound so that it also deals with generalized Hamming weights. This in particular will allow us to establish the connection between various results in the literature.

The literature gives several interpretations of the Feng-Rao bound. In [14] and [9] Kirfel and Pellikaan introduced the concept of an error-correcting array. Using this concept they reformulated the Feng-Rao bound for a large class of codes that includes the duals of one-point geometric Goppa codes, the q-ary Reed-Muller codes and the cyclic codes. Another interpretation was given by Høholdt, van Lint and Pellikaan in [8]. Here they introduced the concept of an order function acting on what is known today as an order domain ([6]). They reformulated some of the most important results by Feng and Rao into this new setting. The code

constructions described by Høholdt et al. includes the set of duals of one-point geometric Goppa codes, the set of Feng-Rao improved such ones, the set of q-ary Reed-Muller codes and the set of Feng-Rao improved such ones (the hyperbolic codes). In the PhD thesis [11] and the papers [12] and [13] Miura independently took on more or less the same point of view as done by Høholdt et. al. Furthermore Miura showed how to interpret the Feng-Rao bound into the setting of any linear code over $\mathbb{F}_q$ defined by means of its paritycheck matrix. This point of view was taken a little further by Matsumoto and Miura in [10]. The work by Matsumoto and Miura is very much related to the work by Kirfel and Pellikaan. Matsumoto and Miura's formulation of the Feng-Rao bound is the most general version of all previous proposed interpretations.

In [7] Heijnen and Pellikaan showed how to derive the generalized Hamming weights of a family of codes related to order domains. This family of codes consists of the duals of one-point geometric Goppa codes, the q-ary Reed-Muller codes and a large class of codes defined from order domains of transcendence degree more than one. However, it was not described in [7] how to deal with the Feng-Rao improved codes. In the series of papers [15], [16], [17], [18], [19], [20], Shibuya, Sakaniwa et. al derived a bound on the generalized Hamming weights of linear codes defined by means of their parity check matrices. We will refer to this bound as the *Shibuya-Sakaniwa bound*. In the first paper they consider only affine variety codes, but in the later papers their results are generalized into the setting of any linear codes using the concepts introduced by Miura in [11] and [12] and using to some extend the concepts introduced by Matsumoto and Miura in [10]. The very fact that Shibuya, Sakaniwa et. al use the concept introduced by Matsumoto and Miura indicates that there should be a strong connection between the Shibuya-Sakaniwa bound and the Feng-Rao bound. This connection is to some extent investigated in the work by Shibuya, Sakaniwa et. al, but it is left as an open problem to establish the precise and general connection ([18, p. 1094], [20, p. 3141]). In the present paper we suggest an extension of the Feng-Rao bound so that it deals with the generalized Hamming weights of any linear codes defined by means of their paritycheck matrices. From our bound it is clear what is the connection between the work by Heijnen, Pellikaan by Matsumoto, Miura and by Shibuya, Sakaniwa et. al. Our bound can be viewed as a generalization and to some extend improvement of all the above bounds.

2 The new bound

Generalized Hamming weights were introduced by Wei in [21] for cryptographically purposes. We start this section by reminding the reader of their definition. Recall that the support of a set S, $S \subseteq \mathbb{F}_q^n$ is defined by

$$\mathrm{Supp}(S) := \{i \mid c_i \neq 0 \ \text{ for some } \ \boldsymbol{c} = (c_1, \ldots, c_n) \in S\}.$$

The tth generalized Hamming weight of a code C is defined by

$$d_t(C) := \min\{\#Supp(S) \mid S \text{ is a linear subcode of } \ C \ \text{ of dimension } \ t\}.$$

Clearly $d_1(C)$ is just the well-known minimum distance. Consider the following definition of a linear code.

Definition 1. *Let $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ be a basis for $\mathbb{F}_q^n$ and let $G \subseteq B$. We define the $\#G$ dimensional code $C(B,G)$ by $C(B,G) := span_{\mathbb{F}_q}\{\boldsymbol{b} \mid \boldsymbol{b} \in G\}$. The dual code (of dimension $n - \#G$) is denoted $C^{\perp}(B,G)$. If $\mathbb{F}_{q'}$ is a subfield of $\mathbb{F}_q$ then the corresponding subfield-subcode of $C^{\perp}(B,G)$ is denoted $C_{q'}^{\perp}(B,G)$*

We next introduce a number of concepts that play a central role in the following.

Definition 2. *For $\boldsymbol{u} = (u_1, \ldots, u_n), \boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ define the componentwise (or Schur or Hadamard) product $\boldsymbol{u} * \boldsymbol{v} := (u_1 v_1, \ldots, u_n v_n)$. Consider the basis $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ for $\mathbb{F}_q^n$ and define $\boldsymbol{b}_0 := \boldsymbol{0} \in \mathbb{F}_q^n$. Define $L_{-1} := \emptyset$ and $L_l := span_{\mathbb{F}_q}\{\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_l\}$ for $l = 0, \ldots, n$.*

We have a chain of spaces $L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_{n-1} \subsetneq L_n = \mathbb{F}_q^n$ and $\dim(L_i) = i$ holds for $i = 0, 1, \ldots, n$. Hence, the following definition makes sense.

Definition 3. *Define $\bar{\rho} : \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$ by $\bar{\rho}(\boldsymbol{v}) = l$ if $\boldsymbol{v} \in L_l \backslash L_{l-1}$.*

The concept of a well-behaving ordered pair plays a central role in this paper. We recall this concept and introduce a new concept called *one-way well-behaving*.

Definition 4. *Consider two bases $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ and $B' = \{\boldsymbol{b}'_1, \ldots \boldsymbol{b}'_n\}$ for $\mathbb{F}_q^n$ (we may or may not have $B = B'$). Let $I := \{1, 2, \ldots, n\}$. An ordered pair $(i,j) \in I^2$ is said to be well-behaving (WB) if $\bar{\rho}(\boldsymbol{b}_u * \boldsymbol{b}'_v) < \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}'_j)$ for all u and v with $1 \leq u \leq i, 1 \leq v \leq j$ and $(u,v) \neq (i,j)$. Less restrictive an ordered pair $(i,j) \in I^2$ is said to be one-way well-behaving (OWB) if $\bar{\rho}(\boldsymbol{b}_u * \boldsymbol{b}'_j) < \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}'_j)$ for $u < i$.*

In the literature (e.g. [10] and [9]) one also finds the concept of weakly well-behaving (WWB). This concept can be interpreted as follows. An ordered pair (i,j) is said to be WWB if both (i,j) and (j,i) are OWB. Clearly, WB implies OWB and also WWB implies OWB. The results in the present paper are all stated using the concept of OWB. As a consequence of the above observations all results holds if OWB is replaced by either WB or WWB.

Definition 5. *Given bases B, B' as above consider for $l = 1, 2, \ldots, n$ the following sets*

$$V_l := \{i \in I \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}'_j) = l \text{ for some } \boldsymbol{b}'_j \in B' \text{ with } (i,j) \text{ OWB } \} \quad (1)$$

$$\Lambda_i := \{l \in I \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}'_j) = l \text{ for some } \boldsymbol{b}'_j \in B' \text{ with } (i,j) \text{ OWB}\} \quad (2)$$

Definition 6. *For $\{l_1, \ldots, l_t\} \subseteq I$ and $\{i_1, \ldots, i_t\} \subseteq I$ define*

$$\bar{\mu}(l_1, \ldots l_t) := \#\left((\cup_{s=1,\ldots,t} V_{l_s}) \cup \{l_1, \ldots, l_t\}\right) \quad (3)$$

$$\bar{\sigma}(i_1, \ldots i_t) := \#\left((\cup_{s=1,\ldots,t} \Lambda_{i_s}) \cup \{i_1, \ldots, i_t\}\right) \quad (4)$$

Our main result is (5) below.

Theorem 1. *Let $G \subseteq B$ be fixed. For $1 \leq t \leq \#G$ respectively $1 \leq t \leq n - \#G$ we have*

$$\begin{aligned} &d_t(C(B,G)) \geq \min\{\bar{\sigma}(a_1,\ldots,a_t) \mid a_i \neq a_j \text{ for } i \neq j \text{ and } \{\boldsymbol{b}_{a_1},\ldots,\boldsymbol{b}_{a_t}\} \subseteq G\} \\ &d_t(C^{\perp}(B,G)) \geq \\ &\qquad \min\{\bar{\mu}(a_1,\ldots,a_t) \mid a_i \neq a_j \text{ for } i \neq j \text{ and } \{\boldsymbol{b}_{a_1},\ldots,\boldsymbol{b}_{a_t}\} \subseteq B\backslash G\}. \end{aligned} \tag{5}$$

Given a subfield $\mathbb{F}_{q'}$ of $\mathbb{F}_q$ the bound (5) also holds if for t, $1 \leq t \leq \dim\left(C_{q'}^{\perp}(B,G)\right)$ one replaces $d_t(C^{\perp}(B,G))$ with $d_t(C_{q'}^{\perp}(B,G))$.

The result concerning $C(B,G)$ is from [1]. The results concerning the codes $C^{\perp}(B,G))$ and $C_{q'}^{\perp}(B,G)$ are new, but are very much related to the Shibuya-Sakaniwa bound. We postpone a discussion of these connections to the next section. Obviously the result concerning the code $C_{q'}^{\perp}(B,G)$ follows immediately from (5). For the proof of (5) we will need the following definition and a lemma.

Definition 7. *For any $\boldsymbol{c} \in \mathbb{F}_q^n\backslash\{\boldsymbol{0}\}$ we define $m(\boldsymbol{c})$ to be the unique number m such that $\boldsymbol{c} \in L_{m-1}^{\perp}$ but $\boldsymbol{c} \notin L_m^{\perp}$. In other words*

$$m(\boldsymbol{c}) = \min\{m \mid \boldsymbol{c}\cdot\boldsymbol{b}_m \neq 0, \boldsymbol{c}\cdot\boldsymbol{b}_1 = \cdots = \boldsymbol{c}\cdot\boldsymbol{b}_{m-1} = 0\}.$$

Lemma 1. *Consider $G = \{\boldsymbol{b}_{i_1},\ldots,\boldsymbol{b}_{i_s}\} \subseteq B$. Let S, $S \subseteq C^{\perp}(B,G)$ be a linear space of dimension t. There exist a basis $\{\boldsymbol{c}_1,\ldots,\boldsymbol{c}_t\}$ for S with*

$$m(\boldsymbol{c}_1) < \cdots < m(\boldsymbol{c}_t). \tag{6}$$

We have

$$m(\boldsymbol{c}_i) \in I\backslash\{i_1,\ldots,i_s\}, i = 1,\ldots,t. \tag{7}$$

Proof. We first observe that by the very definition of the function m for any $\boldsymbol{c} \in C^{\perp}(B,G)\backslash\{\boldsymbol{0}\}$ we have $m(\boldsymbol{c}) \in \{1,2,\ldots,n\}\backslash\{i_1,\ldots,i_s\}$. Hence, if a basis exists that satisfies (6) then it will certainly also satisfy (7). Let $\{\boldsymbol{c}_1,\ldots,\boldsymbol{c}_t\}$ be a basis for S. If $m(\boldsymbol{c}_1),\ldots,m(\boldsymbol{c}_t)$ are pairwise different we are through. Assume $m(\boldsymbol{c}_u) = m(\boldsymbol{c}_v) =: m$ for some u, v with $1 \leq u < v \leq t$. Define $\beta_u := \boldsymbol{c}_u\cdot\boldsymbol{b}_m \neq 0$, $\beta_v := \boldsymbol{c}_v\cdot\boldsymbol{b}_m \neq 0$. Consider $\boldsymbol{c}'_v := \beta_v\boldsymbol{c}_u - \beta_u\boldsymbol{c}_v$. As $\boldsymbol{c}'_v\cdot\boldsymbol{r} = \beta_v(\boldsymbol{c}_u\cdot\boldsymbol{r}) - \beta_u(\boldsymbol{c}_v\cdot\boldsymbol{r})$ for any $\boldsymbol{r}$ we conclude that $\boldsymbol{c}'_v\cdot\boldsymbol{b}_i = 0$ for $i = 1,2,\ldots,m$. If we replace $\boldsymbol{c}_v$ with $\boldsymbol{c}'_v$ in the basis $\{\boldsymbol{c}_1,\ldots,\boldsymbol{c}_t\}$ we get a new basis. In particular $\boldsymbol{c}'_v \neq \boldsymbol{0}$ and therefore $m(\boldsymbol{c}'_v)$ is well defined. We therefore have $m(\boldsymbol{c}'_v) > m$. The lemma now follows by induction.

Proof of (5). Let S, $S \subseteq C^{\perp}(B,G)$ be a space of dimension t. Let $\{\boldsymbol{c}_1,\ldots,\boldsymbol{c}_t\}$ be a basis for S as in Lemma 1. Denote $m_1 := m(\boldsymbol{c}_1),\ldots,m_t := m(\boldsymbol{c}_t)$. Denote $\gamma := \bar{\mu}(m_1,\ldots,m_t)$ and write

$$\begin{aligned} &\{i_1,\ldots,i_\gamma\} = \\ &\cup_{s=1,\ldots,t}\left(\{i \in I \mid \exists \boldsymbol{b}'_j \in B' \text{ with } \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}'_j) = m_s \text{ and } (i,j) \text{ OWB }\} \cup \{m_s\}\right). \end{aligned}$$

We may assume $i_1 < \ldots < i_\gamma$. Let $1 \leq h \leq \gamma$ and consider any vector

$$\boldsymbol{r}_h = \sum_{v=1}^{h} \alpha_v \boldsymbol{b}_{i_v},\ \alpha_v \in \mathbb{F}_q,\ \alpha_h \neq 0.$$

If $i_h \in \{m_1, \ldots, m_t\}$ then it follows from the definition of the function m (Definition 7) that $\boldsymbol{r}_h \cdot \boldsymbol{c}_h \neq 0$ and in particular that $\boldsymbol{r}_h * \boldsymbol{c}_h \neq \boldsymbol{0}$. If $i_h \notin \{m_1, \ldots, m_t\}$ then it is because there exists a j and an m_u, $u \in \{1, \ldots, t\}$ such that $\bar{\rho}(\boldsymbol{b}_{i_h} * \boldsymbol{b}'_j) = m_u$ with (i_h, j) OWB. From the definition of the function m and from the OWB property of (i_h, j) we know that $(\boldsymbol{r}_h * \boldsymbol{b}'_j) \cdot \boldsymbol{c_u} \neq 0$. But then $\boldsymbol{r}_h * \boldsymbol{c_u} \neq \boldsymbol{0}$ holds again. All together for every $\boldsymbol{r}_h$ there exist a $\boldsymbol{c} \in S$ with $\boldsymbol{r}_h * \boldsymbol{c} \neq \boldsymbol{0}$.
This contradicts that $\#\mathrm{Supp}(S) < \gamma$, $\mathrm{Supp}(S) \subseteq \{1, \ldots, \gamma - 1\}$ say, which is seen by selecting $\boldsymbol{r} = \sum_{v=1}^{\gamma} \beta_v \boldsymbol{b}_{i_v}$, $(\beta_1, \ldots, \beta_\gamma) \in \mathbb{F}_q^\gamma \backslash \{\boldsymbol{0}\}$ such that $\mathrm{Supp}(\{\boldsymbol{r}\}) \subseteq \{\gamma, \gamma + 1, \ldots, n\}$ and observe that $\boldsymbol{r} * \boldsymbol{c} = \boldsymbol{0}$ for all $\boldsymbol{c} \in S$. The proof of (5) is complete.

Clearly, Theorem 1 holds in particular for the special case $B = B'$. More or less all known code constructions for which the Feng-Rao bound is known to be interesting corresponds to the case $B = B'$. As an exception, to deal with the cyclic codes we will need two different bases B, B' (see [9, Ex. 2.4] and [20, Sec. 4]). The results in Theorem 1 concerning the codes $C^\perp(B, G)$ and $C_{q'}^\perp(B, G)$ can be generalized to deal not only with two, but with many different bases for $\mathbb{F}_q^n$. In this way one can in particular extend the traditional Feng-Rao bound as stated by Matsumoto and Miura in [10] so that it also deals with generalized Hamming weights. Actually, by the following remark one can generalize even further.

Remark 1. From the proof of (5) it is clear that it is of no significance that B' is a basis for $\mathbb{F}_q^n$ and therefore B' can be any indexed subset of $\mathbb{F}_q^n$.

The use of the OWB concept prior to the WWB concept is already justified by the above remark. We further note that it is possible to give examples where OWB gives better estimates than WWB does.

3 The connection to the work by Shibuya, Sakaniwa et al.

In [19] Shibuya and Sakaniwa considered the set-up with only one basis B (that is, the setup in Theorem 1 with $B = B'$). In [19] they were concerned with the WWB property. In [20] Shibuya and Sakaniwa considered the set-up with two bases B, B' but were only concerned with the WB property. As we will show below our bound is at least as good as their bound even if we replace their WB as well as their WWB with OWB.

In the following let B and B' be bases as in the previous section. Assume $G \subseteq B$ and denote $G = \{\boldsymbol{b}_{i_1}, \ldots, \boldsymbol{b}_{i_s}\}$. The Shibuya-Sakaniwa bound from [19] and [20] can be interpreted as follows (we have replaced their WB respectively WWB with OWB).

Definition 8. *For $T \subseteq \{i_1, \ldots, i_s\}$ let*

$$\Lambda_T := \cup_{i \in T} \Lambda_i \qquad \Lambda_T^* := (I \backslash \{i_1, \ldots, i_s\}) \setminus \Lambda_T$$
$$\eta_t := s - \max\{\#T \mid T \subseteq \{i_1, \ldots, i_s\} \ \textit{such that} \ \#\Lambda_T^* \geq t\}.$$

Theorem 2. *For $t = 1, \ldots, n - \#G$ we have*

$$d_t\left(C^{\perp}(B,G)\right) \geq \eta_t + t \tag{8}$$

Given a subfield $\mathbb{F}_{q'}$ of $\mathbb{F}_q$ the bound (8) also holds if for t, $1 \leq t \leq \dim\left(C_{q'}^{\perp}(B,G)\right)$ one replaces $d_t(C^{\perp}(B,G))$ with $d_t(C_{q'}^{\perp}(B,G))$.

The connection to the theory in the present paper is easily read of the proof of the following proposition.

Proposition 1. *The bound (5) in Theorem 1 is at least as tight as the Shibuya-Sakaniwa bound (8).*

Proof. From Definition 6 we have

$$\begin{aligned}
&\min_{\substack{a_1 < \cdots < a_t \\ a_i \in I \backslash \{i_1, \ldots, i_s\}}} \{\bar{\mu}(a_1, \ldots, a_t)\} \\
&= \min_{\substack{a_1 < \cdots < a_t \\ a_i \in I \backslash \{i_1, \ldots, i_s\}}} \big\{\#[\cup_{s=1}^{t} \{i \in I \mid \\
&\qquad \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}'_j) = a_s \text{ for some } \boldsymbol{b}'_j \in B' \text{ with } (i,j) \text{ OWB}\} \cup \{a_1, \ldots, a_t\}]\big\} \\
&\geq \min_{\substack{a_1 < \cdots < a_t \\ a_i \in I \backslash \{i_1, \ldots, i_s\}}} \big\{\# \cup_{s=1}^{t} \{i \in \{i_1, \ldots, i_s\} \mid \\
&\qquad \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}'_j) = a_s \text{ for some } \boldsymbol{b}'_j \in B' \text{ with } (i,j) \text{ OWB}\}\big\} + t \\
&= s - \max\{\#T \mid T \subseteq \{i_1, \ldots, i_s\} \text{ such that } \#\Lambda_T^* \geq t\} + t = \eta_t + t
\end{aligned}$$

This concludes the proof of Proposition 1

In Section 5 below we demonstrate that the bound (5) in Theorem 1 can actually be sharper than the bound (8) in Theorem 2.

Next we will be concerned with the complexity of calculating the two bounds (5) and (8). By k we will denote the dimension of $C^{\perp}(B,G)$. That is, $\#G = n - k$. The bound (8) can be calculated with a worst case complexity of

$$O\left(ki \sum_{i=1}^{n-k} \binom{n-k}{i}\right).$$

At a first glance it seems as if the worst case complexity of the bound (5) is

$$O\left(nt \binom{k}{t}\right). \tag{9}$$

However, due to the generalized Singleton bound $d_t \leq n-k+t$ one need in (5) only consider the a_i's with $\bar{\mu}(a_i) \leq n-k+t$. The number of such a_i's are in general much smaller than k. So the value k in (9) should be replaced with a much smaller value. Hence, for large t combined with small dimensions the new bound (5) is by far the fastest. Whereas, for large t combined with large dimensions the picture is not so clear. For small values of t the estimation of d_t will be fastest by using the bound (5). Fortunately we may sometimes do without the above calculations. Recall, that a code is called tth rank MDS if the tth generalized Hamming weight attains the generalized Singleton bound. In [20] Shibuya and Sakaniwa gave an easily calculate-able criterion under which the code $C^{\perp}(B,G)$ is guaranteed to be tth rank MDS.

Theorem 3. *Let $G = \{\boldsymbol{b}_{i_1}, \ldots, \boldsymbol{b}_{i_s}\}$ and $I = \{1, 2, \ldots, n\}$ and define*

$$g(B,G) := \max_{i \in \{i_1,\ldots,i_s\}} \{\#\left(I \backslash (\Lambda_i \cup \{i_1, \ldots, i_s\})\right)\}. \tag{10}$$

For t with $g(B,G)+1 \leq t \leq n-s$ the code $C^{\perp}(B,G)$ is tth rank MDS.

In [20, Sec. 4] Shibuya and Sakaniwa presented a BCH type bound for the generalized Hamming weights of cyclic codes. To establish this bound they considered two bases B and B'. The proof in [20] is not very complicated, however with the bound (5) in hand the proof gets even shorter.

4 Codes from order domains

In [7] Heijnen and Pellikaan showed how to estimate the generalized Hamming weights of a family of codes related to order domains. This family consists of the duals of one-point geometric Goppa codes and their generalizations to order domains of transcendence degree more than one, including the q-ary Reed-Muller codes. Heijnen and Pellikaan did not describe how to deal with the Feng-Rao improved codes. In this section we will apply the bound (5) to the case of codes defined from order domains. We will see that Heijnen and Pellikaan's bound can be viewed as a consequence of (5) and as a special case of our new bound. In our presentation we will consider only order functions that are also weight functions. These seems to be the only order functions that are relevant for coding theoretical purposes. From[6] we have the following definition and theorem.

Definition 9. *Let R be an $\mathbb{F}_q$-algebra, let Γ be a subsemigroup of $\mathbb{N}_0^r$ for some r and let $\prec$ be a monomial ordering on $\mathbb{N}_0^r$. A surjective map $\rho : R \to \Gamma_{-\infty} := \Gamma \cup \{-\infty\}$ that satisfies the following five conditions is said to be a weight function over the order domain R*

- (*W*.0) *$\rho(f) = -\infty$ if and only if $f = 0$*
- (*W*.1) *$\rho(af) = \rho(f)$ for all nonzero $a \in \mathbb{F}_q$*
- (*W*.2) *$\rho(f+g) \preceq \max\{\rho(f), \rho(g)\}$ and equality holds when $\rho(f) \prec \rho(g)$*
- (*W*.4) *If f and g are nonzero and $\rho(f) = \rho(g)$, then there exists a nonzero $a \in \mathbb{F}_q$ such that $\rho(f - ag) \prec \rho(g)$*
- (*W*.5) *If f and g are nonzero then $\rho(fg) = \rho(f) + \rho(g)$.*

Theorem 4. *Given a weight function then any set $\mathcal{B} = \{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma\in\Gamma}$ constitutes a basis for R as a vector space over $\mathbb{F}_q$. In particular $\{f_\lambda \in \mathcal{B} \mid \lambda \preceq \gamma\}$ constitutes a basis for $R_\gamma := \{f \in R \mid \rho(f) \preceq \gamma\}$.*

In the following we will assume that a basis $\mathcal{B}$ as above has been chosen.

Definition 10. *Let R be an $\mathbb{F}_q$-algebra. A surjective map $\varphi : R \to \mathbb{F}_q^n$ is called a morphism of $\mathbb{F}_q$-algebras if φ is $\mathbb{F}_q$-linear and $\varphi(fg) = \varphi(f) * \varphi(g)$ for all $f, g \in R$.*

From [1] we have the following definition.

Definition 11. *Let $\alpha(1) := 0$ and define for $i = 2, 3, \ldots, n$ recursively $\alpha(i)$ to be the smallest element in Γ that is greater than $\alpha(1), \alpha(2), \ldots, \alpha(i-1)$ and satisfies $\varphi(R_\gamma) \subsetneq \varphi(R_{\alpha(i)})$ for all $\gamma < \alpha(i)$. Write $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$.*

We are now in the position that we can describe bases $B = B'$ for $\mathbb{F}_q^n$ for which the bound (5) is very much applicable. From [1] we have.

Theorem 5. *Let $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ be as in Definition 11. The set*

$$B := \{\boldsymbol{b}_1 := \varphi(f_{\alpha(1)}), \ldots, \boldsymbol{b}_n := \varphi(f_{\alpha(n)})\} \tag{11}$$

constitutes a basis for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. For any $\boldsymbol{c} \in \mathbb{F}_q^n$ there exists a unique ordered set $(\beta_1, \ldots, \beta_n)$, $\beta_i \in \mathbb{F}_q$ such that $\boldsymbol{c} = \varphi\left(\sum_{i=1}^n \beta_i f_{\alpha(i)}\right)$. The function $\bar{\rho} : \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$ corresponding to B is given by

$$\bar{\rho}(\boldsymbol{c}) = \begin{cases} 0 & \text{if } \boldsymbol{c} = 0 \\ \max\{i \mid \beta_i \neq 0\} & \text{otherwise} \end{cases}$$

The following proposition from [1] helps us dealing with the concept of WB.

Proposition 2. *Let $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ be the basis in (11). If $\alpha(i), \alpha(j)$, $\alpha(l) \in \Delta(R, \rho, \varphi)$ are such that $\rho(f_{\alpha(i)} f_{\alpha(j)}) = \alpha(l)$ then $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l$ and $(i, j) \in I^2$ is WB. Consider $\alpha(l) \in \Delta(R, \rho, \varphi)$ and assume $\beta_1, \beta_2 \in \Gamma$ satisfies $\rho(f_{\beta_1} f_{\beta_2}) = \alpha(l)$. Then $\beta_1, \beta_2 \in \Delta(R, \rho, \varphi)$ holds.*

We have motivated the following definition.

Definition 12. *For $\lambda \in \Gamma$ define $N(\lambda) := \{\alpha \in \Gamma \mid \lambda - \alpha \in \Gamma\}$ and $\mu(\lambda) := \#N(\lambda)$ if $N(\lambda)$ is finite and $\mu(\lambda) := \infty$ if not. In larger generality consider $\{\lambda_1, \ldots, \lambda_t\} \subseteq \Gamma$ and define $N(\lambda_1, \ldots, \lambda_t) := \cup_{s=1}^t N(\lambda_s)$. Define $\mu(\lambda_1, \ldots, \lambda_t) := \#N(\lambda_1, \ldots, \lambda_t)$ if $N(\lambda_1, \ldots, \lambda_t)$ is finite and $\mu(\lambda_1, \ldots, \lambda_t) := \infty$ if not.*

As an immediate consequence of Proposition 2 we have.

Proposition 3. *Consider the set $\Delta(R, \rho, \varphi) = \{\alpha(1), \ldots \alpha(n)\}$ and the basis $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ from Definition 5. Let $\alpha(s) \in \Delta(R, \rho, \varphi)$. For $i = 1, \ldots, n$ we have $\bar{\mu}(i) \geq \mu(\alpha(i))$. In larger generality for $\{a_1, \ldots, a_t\} \subseteq I$ we have $\bar{\mu}(a_1, \ldots, a_t) \geq \mu(\alpha(a_1), \ldots, \alpha(a_t))$.*

The results concerning the generalized Hamming weights in (5) are now easily translated into the setting of codes from order domains. We consider only two particular choices of subsets G of B.

Definition 13. *Given a basis $\mathcal{B}$ as in Theorem 4 and a morphism φ let*

$$C(\lambda) := \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \varphi(f_\gamma) = 0 \text{ for all } \gamma \preceq \lambda\}$$
$$\tilde{C}(\delta) := \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \varphi(f_{\alpha(i)}) = 0 \text{ for all } \alpha(i) \in \Delta(R, \rho, \varphi) \text{ with } \mu(\alpha(i)) < \delta\}$$

For the case of order domains of transcendence degree 1 the set of codes $C(\lambda)$ are the set of duals to one-point geometric Goppa codes. For larger transcendence degree the set of codes $C(\lambda)$ includes the q-ary Reed-Muller codes but also many other codes. The codes $\tilde{C}(\delta)$ are examples of Feng-Rao improved codes. The theorem below is an immediate consequence of (5) and the above discussion.

Theorem 6. *For $1 \leq t \leq \dim(C(\lambda))$ respectively $1 \leq t \leq \dim(\tilde{C}(\delta))$ we have*

$$d_t(C(\lambda)) \geq \min\{\mu(\eta_1, \ldots, \eta_t) \mid \{\eta_1, \ldots, \eta_t\} \subseteq \Delta(R, \rho, \varphi), \lambda \prec \eta_s \text{ for } s = 1, \ldots, t\} \tag{12}$$

$$d_t(\tilde{C}(\delta)) \geq \min\{\mu(\eta_1, \ldots, \eta_t) \mid \{\eta_1, \ldots, \eta_t\} \subseteq \Delta(R, \rho, \varphi), \mu(\eta_s) \geq \delta \text{ for } s = 1, \ldots, t\} \tag{13}$$

The bound (12) for the codes $C(\lambda)$ is identical to the bound given by Heijnen and Pellikaan in [7, Th. 3.14]. It is known that (12) gives the actual values of the t generalized Hamming weights of the q-ary Reed-Muller codes (see [7]). It is also known that (12) gives the actual values of the tth generalized Hamming weights of the Hermitian codes (see [2]). For the case of hyperbolic codes (improved q-ary Reed-Muller codes) (13) gives exactly the same estimates as was found in [5]. We note that the result concerning the condition for tth rank MDS from the previous section is easily translated into the setting of the present section. Also we note that one can show that applying the Shibuya-Sakaniwa bound (8) to the codes of this section would produce the same estimates as is found by using(12) and(13).

5 Examples

The following two examples deals with codes coming from the Hermitian curve.

Example 1. Consider the factorring $R = \mathbb{F}_{q^2}[X, Y]/I$ where $I := \langle X^{q+1} - Y^q - Y \rangle$ means the ideal generated by $X^{q+1} - Y^q - Y$. The set $\mathcal{B} = \{X^a Y^b + I \mid 0 \leq a, 0 \leq b < q\}$ constitutes a basis for R as a vectorspace over $\mathbb{F}_{q^2}$. Consider the map $\rho : \mathcal{B} \to \mathbb{N}_0$, $\rho(X^a Y^b + I) = qa + (q+1)b$. This map is easily extended to a weight function ρ on R by applying the rules (W.0), (W.1) and (W.2) from Definition 9. With this weight function, the basis $\mathcal{B}$ can be indexed to be of the form described in Theorem 4. The polynomial $X^{q+1} - Y^q - Y$ has

q^3 zeros $P_1, \ldots, P_{q^3}$ which give rise to the following morphism $\varphi : R \to \mathbb{F}_{q^2}^{q^3}$ $\varphi(G(X,Y)+I) = (G(P_1), \ldots, G(P_{q^3}))$. We get

$$\Delta(R,\rho,\varphi) = \{\alpha(1), \ldots, \alpha(q^3)\} = \{qa + (q+1)b \mid 0 \le a < q^2, 0 \le b < q\}.$$

The basis B that we should use for the code construction is $B = \{\boldsymbol{b}_i \mid i = 1, \ldots, q^3\}$ where $\boldsymbol{b}_i := \varphi(X^aY^b + I)$ with $0 \le a < q^2$, $0 \le b < q$ and $qa + (q+1)b = \alpha(i)$. Using (12) and (13) we calculate the following parameters for some Hermitian codes and improved such ones (recall that we noted above that the bound (12) is sharp for the non-improved Hermitian codes). The codes in the first two arrays are defined over $\mathbb{F}_{16}$ and are of length $n = 64$. The codes in the last two arrays are defined over $\mathbb{F}_{64}$ and are of length $n = 512$. A bolded number means that the generalized Singleton bound is attained. We note that Theorem 3 predicts exactly the bolded numbers.

	k	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	d_9
$\tilde{C}(6)$	55	6	8	9	11	12	14	15	16	**18**
$C(14)$	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
$\tilde{C}(9)$	51	9	12	14	15	17	18	19	**21**
$C(18)$	51	8	12	13	16	17	18	**20**	**21**
$C(19)$	50	9	13	14	17	18	19	**21**	**22**

	k	d_1	d_2	d_3	d_4	d_5	d_6	d_7
$\tilde{C}(18)$	476	18	21	24	26	27	30	32
$C(63)$	476	9	17	18	25	26	27	33
$C(72)$	467	18	26	27	34	35	36	42

	k	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	d_9
$\tilde{C}(5)$	504	5	6	7	8	9	12	13	14	15
$C(25)$	504	4	5	6	7	8	11	12	13	14
$C(27)$	502	5	6	7	8	9	13	14	15	16

We take a closer look at the code $\tilde{C}(6)$ and $C(14)$ over $\mathbb{F}_{16}$. These codes are of the same dimension $k = 55$ and $\tilde{C}(6)$ is indeed an improved code as $d(\tilde{C}(6)) \ge 6 > 4 = d(C(14))$ holds. Nevertheless we observe that the estimated value of d_7 respectively d_8 of $\tilde{C}(6)$ are smaller than $d_7(C(14))$ respectively $d_8(C(14))$. A similar phenomenon occurs for the the codes $\tilde{C}(9)$ and $C(18)$ over $\mathbb{F}_{16}$.

In the next example we consider not only one, but two different bases B and B' related to the Hermitian curve. This will allow us to demonstrate that the bound (5) can actually be better than the Shibuya-Sakaniwa bound (8).

Example 2. Consider $R = \mathbb{F}_4[X,Y]/I$ where $I = \langle X^3 + Y^2 + Y \rangle$. Let φ be as in the previous example and consider the following two bases for $\mathbb{F}_4^8$.

$$\begin{aligned} B = \{&\boldsymbol{b}_1 = \varphi(1+I), \boldsymbol{b}_2 = \varphi(X+I), \boldsymbol{b}_3 = \varphi(Y+I), \boldsymbol{b}_4 = \varphi(X^2+I),\\ &\boldsymbol{b}_5 = \varphi(XY+I), \boldsymbol{b}_6 = \varphi(X^3+I), \boldsymbol{b}_7 = \varphi(X^2Y+I), \boldsymbol{b}_8 = \varphi(X^3Y+I)\}\\ B' = \{&\boldsymbol{b}'_1 = \varphi(1+I), \boldsymbol{b}'_2 = \varphi(X+I), \boldsymbol{b}'_3 = \varphi(XY+X^2+Y+I),\\ &\boldsymbol{b}'_4 = \varphi(XY+X^2+I), \boldsymbol{b}'_5 = \varphi(XY+I), \boldsymbol{b}'_6 = \varphi(X^2Y+X^3+I),\\ &\boldsymbol{b}'_7 = \varphi(X^2Y+I), \boldsymbol{b}'_8 = \varphi(X^3Y+I)\} \end{aligned}$$

Given a monomial X^aY^b we define the weight of X^aY^b to be $w(X^aY^b) := 2a+3b$. The following observations will play an important role to us:

$$\left.\begin{aligned} &w(X^aY^b) = 0 \Rightarrow \varphi(X^aY^b + I) \in L_1\\ &w(X^aY^b) = s \Rightarrow \varphi(X^aY^b + I) \in L_s \backslash L_{s-1} \quad \text{for} \quad s = 2,3,4,5,6,7\\ &w(X^aY^b) = 9 \Rightarrow \varphi(X^aY^b + I) \in L_8 \backslash L_7 \end{aligned}\right\} \qquad (14)$$

Consider the Hermitian code $C(3)$ (made from B). Clearly, this code has parameters $[n,k,d] = [8,5,3]$. We now show that for the particular choice of B' our new bound (5) will give us at least $d(C(3)) \geq 2$ whereas the Shibuya-Sakaniwa bound will only give $d(C(3)) \geq 1$.
The bound (5) calls for an estimation of the values $\bar{\mu}(4), \ldots, \bar{\mu}(8)$. By use of (14) we get the following estimates: $\bar{\mu}(4) \geq 2$ as $\boldsymbol{b}_2 * \boldsymbol{b}'_2, \boldsymbol{b}_4 * \boldsymbol{b}'_1 \in L_4 \backslash L_3$ and $(2,2),(4,1)$ are OWB. $\bar{\mu}(5) \geq 3$ as $\boldsymbol{b}_1 * \boldsymbol{b}'_3, \boldsymbol{b}_3 * \boldsymbol{b}'_2, \boldsymbol{b}_5 * \boldsymbol{b}'_1 \in L_5 \backslash L_4$ and $(1,3),(3,2),(5,1)$ are OWB. $\bar{\mu}(6) \geq 2$ as $\boldsymbol{b}_4 * \boldsymbol{b}'_2, \boldsymbol{b}_6 * \boldsymbol{b}'_1 \in L_6 \backslash L_5$ and $(4,2),(6,1)$ are OWB. $\bar{\mu}(7) \geq 4$ as $\boldsymbol{b}_1 * \boldsymbol{b}'_6, \boldsymbol{b}_2 * \boldsymbol{b}'_3, \boldsymbol{b}_5 * \boldsymbol{b}'_2, \boldsymbol{b}_7 * \boldsymbol{b}'_1 \in L_7 \backslash L_6$ and $(1,6),(2,3),(5,2),(7,1)$ are all OWB. $\bar{\mu}(8) \geq 5$ as $\boldsymbol{b}_1 * \boldsymbol{b}'_8, \boldsymbol{b}_2 * \boldsymbol{b}'_6, \boldsymbol{b}_4 * \boldsymbol{b}'_3, \boldsymbol{b}_7 * \boldsymbol{b}'_2, \boldsymbol{b}_8 * \boldsymbol{b}'_1 \in L_8 \backslash L_7$ and $(1,8),(2,6),(4,3),(7,2),(8,1)$ are all OWB. Hence, from (5) we get $d(C(3)) \geq 2$.
We next apply Definition 8 and (8) in Theorem 2. We will show that for $T = \{1,2,3\}$ we have $\{6\} \subseteq \Lambda_T^*$. From this we can conclude that $\eta_1 = 3 - 3 = 0$ and therefore (8) becomes $d(C(3)) \geq 0 + 1 = 1$. To establish $\{6\} \subseteq \Lambda_T^*$ we will in the following show that there is no pair (i,j), $i \in \{1,2,3\}$, $j \in \{1,\ldots,8\}$ such that $\boldsymbol{b}_i * \boldsymbol{b}'_j \in L_6 \backslash L_5$. By use of (14) we get $\boldsymbol{b}_1 * \boldsymbol{b}'_1 \in L_1$, $\boldsymbol{b}_1 * \boldsymbol{b}'_2 \in L_2$, $\boldsymbol{b}_1 * \boldsymbol{b}'_3, \boldsymbol{b}_1 * \boldsymbol{b}'_4, \boldsymbol{b}_1 * \boldsymbol{b}'_5 \in L_5$, $\boldsymbol{b}_1 * \boldsymbol{b}'_6, \boldsymbol{b}_1 * \boldsymbol{b}'_7 \in L_7 \backslash L_6$, $\boldsymbol{b}_1 * \boldsymbol{b}'_8 \in L_8 \backslash L_7$, $\boldsymbol{b}_2 * \boldsymbol{b}'_1 \in L_2$, $\boldsymbol{b}_2 * \boldsymbol{b}'_2 \in L_4$, $\boldsymbol{b}_2 * \boldsymbol{b}'_3, \boldsymbol{b}_2 * \boldsymbol{b}'_4, \boldsymbol{b}_2 * \boldsymbol{b}'_5 \in L_7 \backslash L_6$, $\boldsymbol{b}_2 * \boldsymbol{b}'_6, \boldsymbol{b}_2 * \boldsymbol{b}'_7 \in L_8 \backslash L_7$, $\boldsymbol{b}_3 * \boldsymbol{b}'_1 \in L_3$, $\boldsymbol{b}_3 * \boldsymbol{b}'_2 \in L_5$.
It remains to study the incidents (i,j), $i \in \{1,2,3\}$ for which (14) does not immediately apply. We get

$$\boldsymbol{b}_2 * \boldsymbol{b}'_8 = \varphi(X^4Y + I) = \varphi(XY + I) \in L_5$$
$$\boldsymbol{b}_3 * \boldsymbol{b}'_3 = \varphi(XY^2 + X^2Y + Y^2 + I) = \varphi(X + XY + X^2Y + X^3 + Y + I) \in L_7 \backslash L_6$$
$$\boldsymbol{b}_3 * \boldsymbol{b}'_4 = \varphi(XY^2 + X^2Y + I) = \varphi(X + XY + X^2Y + I) \in L_7 \backslash L_6$$
$$\boldsymbol{b}_3 * \boldsymbol{b}'_5 = \varphi(XY^2 + I) = \varphi(X + XY + I) \in L_5$$
$$\boldsymbol{b}_3 * \boldsymbol{b}'_6 = \varphi(X^2Y^2 + X^3Y + I) = \varphi(X^2 + X^2Y + X^3Y + I) \in L_8 \backslash L_7$$
$$\boldsymbol{b}_3 * \boldsymbol{b}'_7 = \varphi(X^2Y^2 + I) = \varphi(X^2 + X^2Y + I) \in L_7 \backslash L_6$$
$$\boldsymbol{b}_3 * \boldsymbol{b}'_8 = \varphi(X^3Y^2 + I) = \varphi(X^3 + X^3Y + I) \in L_8 \backslash L_7.$$

We have shown that there is no pair (i,j), $i \in \{1,2,3\}$, $j \in \{1,\ldots,8\}$ such that $\boldsymbol{b}_i * \boldsymbol{b}'_j \in L_6 \backslash L_5$ and therefore by the above discussion (8) becomes $d(C(3)) \geq 1$.

6 Acknowledgments

The authors wish to thank the anonymous referees for their valuable remarks.

References

1. H. E. Andersen, O. Geil, The Missing Evaluation Codes from Order Domain Theory, (2004), submitted.
2. A. I. Barbero, C. Munuera, The Weight Hierarchy of Hermitian Codes, *Siam J. Discrete Math.,* **13** (2000), 79–104.

3. G.-L. Feng and T.R.N. Rao, Decoding of algebraic geometric codes up to the designed minimum distance, *IEEE Trans. Inf. Theory*, **39**, (1993) 37-46.
4. G.-L. Feng and T.R.N. Rao, Improved Geometric Goppa Codes, Part I:Basic theory, *IEEE Trans. Inf. Theory*, **41**, (1995), 1678-1693.
5. O. Geil and T. Høholdt, On Hyperbolic Codes, Proc. AAECC-14, *Lecture Notes in Comput. Sci. 2227*, Springer, Berlin, 2001, 159-171.
6. O. Geil and R. Pellikaan, On the Structure of Order Domains, *Finite Fields and their Applications*, **8**, (2002), 369-396.
7. P. Heijnen, R. Pellikaan, Generalized Hamming weights of q-ary Reed-Muller codes, *IEEE Trans. Inf. Theory*, **44**, (1998), 181-196.
8. T. Høholdt, J. van Lint and R. Pellikaan, Algebraic Geometry Codes, Chapter 10 in "Handbook of Coding Theory," (V.S. Pless and W.C. Huffman, Eds.), vol. 1, Elsevier, Amsterdam, 1998, 871-961.
9. C. Kirfel and R. Pellikaan, The minimum distance of codes in an array coming from telescopic semigroups, *IEEE Trans. Inf. theory*, **41**, (1995), 1720-1732.
10. R. Matsumoto and S. Miura, On the Feng-Rao Bound for the $\mathcal{L}$-Construction of Algebraic Geometry Codes, *IEICE Trans. Fund.,* **E83-A**, no. 5 (2000), 923-927.
11. S. Miura, On error correcting codes based on algebraic geometry, Ph.D. thesis, Univ. Tokyo, May 1997, (in Japanese).
12. S. Miura, Linear Codes on Affine Algebraic Varieties, *Trans. IEICE*, **J81-A**, no. 10 (1998), 1386-1397 (in Japanese).
13. S. Miura, Linear Codes on Affine Algebraic Curves, *Trans. IEICE*, **J81-A**, no. 10 (1998), 1398-1421 (in Japanese).
14. R. Pellikaan, On the efficient decoding of algebraic-geometric codes, *Eurocode 92*, edited by P. Camion, P. Charpin and S. Harari, Udine, CISM Courses and Lectures, **339**, Springer-Verlag, (1993), 231-253.
15. T. Shibuya, J. Mizutani, K. Sakaniwa, On generalized Hamming Weights of codes constructed on Affine algebraic sets, Proc. AAECC-12, *Lecture Notes in Computer Science*, **vol. 1255**, Springer-Verlag, (1997), 311-320.
16. T. Shibuya, J. Mizutani, K. Sakaniwa, On generalized Hamming Weights of codes constructed on Affine algebraic sets, *IEICE Trans. Fund.*, **E81-A** (1998), 1979–1989.
17. T.Shibuya and K. Sakaniwa, Lower bound on generalized Hamming weights in terms of a notion af well-behaving, Proc. ISIT 1998, Cambridge, USA, (1998), 96.
18. T. Shibuya, R. Hasagawa, K. Sakaniwa, A Lower Bound for Generalized Hamming Weights and a Condition for t-th Rank MDS, *IEICE Trans. Fund.*, **E82-A**, (1999), 1090-1101.
19. T. Shibuya and K. Sakaniwa, A Dual of Well-Behaving Type Designed Minimum Distance, *IEICE Trans. Fund.*, **E84-A**, (2001), 647–652.
20. T. Shibuya and K. Sakaniwa, A note on a Lower Bound for General Hamming Weights, *IEICE Trans. Fund.*, **E84-A**, (2001), 3138–3145.
21. V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inf. Theory*, **37**, (1991), 1412-1418.