Feng-Rao decoding of primary codes☆

Olav Geil[a], Ryutaroh Matsumoto[b], Diego Ruano[a]

[a]*Department of Mathematical Sciences, Aalborg University, Denmark*
[b]*Department of Communications and Integrated Systems, Tokyo Institute of Technology, Japan*

Abstract

We show that the Feng-Rao bound for dual codes and a similar bound by Andersen and Geil [1] for primary codes are consequences of each other. This implies that the Feng-Rao decoding algorithm can be applied to decode primary codes up to half their designed minimum distance. The technique applies to any linear code for which information on well-behaving pairs is available. Consequently we are able to decode efficiently a large class of codes for which no non-trivial decoding algorithm was previously known. Among those are important families of multivariate polynomial codes. Matsumoto and Miura in [30] (See also [3]) derived from the Feng-Rao bound a bound for primary one-point algebraic geometric codes and showed how to decode up to what is guaranteed by their bound. The exposition in [30] requires the use of differentials which was not needed in [1]. Nevertheless we demonstrate a very strong connection between Matsumoto and Miura's bound and Andersen and Geil's bound when applied to primary one-point algebraic geometric codes.

Keywords: decoding, Feng-Rao bound, generalized Hamming weight, minimum distance, order domain, well-behaving pair
2010 MSC: 94B65, 94B35

1. Introduction

Originally the celebrated Feng-Rao bound was stated [9, 10, 11] in the language of affine variety codes [12]. Later Høholdt, Pellikaan, and van Lint [26]

☆Published in Finite Fields and their Applications, Volume 23, pages 35-52 (2013).

URL: http://people.math.aau.dk/~olav (Olav Geil),
http://www.rmatsumoto.org/research.html (Ryutaroh Matsumoto),
http://people.math.aau.dk/~diego (Diego Ruano)

introduced the concept of order domains and order functions to facilitate the use of the bound, and for those structures it was renamed the order bound. The success of the order bound formulation comes from the fact that order domain codes include the important family of duals of one-point algebraic geometric codes as well as the generalization of such codes to higher transcendence degree algebraic structures. A completely different point of view was to formulate the Feng-Rao bound in the setting of general linear codes [26, 30, 31, 32, 34]. In this setting having no supporting algebra, a grading of $\mathbb{F}_q^n$ is assumed. This simply corresponds to defining an indexed basis. The componentwise product then plays the role that should otherwise be played by multiplication in the supporting algebra. It should be stressed that the linear code formulation is the most general in the sense that the other formulations mentioned above can be deduced from that. So results derived in the linear code description can be easily translated into the situation where we have some kind of a supporting algebra. This of course in particular holds for the decoding method to be discussed in the present paper.

The strength of the Feng-Rao bound — besides the fact that it improves on previous bounds such as the Goppa bound — is that it enables an improved code construction [11]. Furthermore, it comes with a decoding algorithm that applies to any dual code, improved or not. This decoding algorithm can be formulated in any of the three settings: affine variety codes, order domain codes, and general linear codes.

Building on [16, 18, 35] Andersen and Geil in [1] introduced a bound on the minimum distance of primary codes. This bound was later slightly generalized and enhanced in [23], but we shall refer also this version as Andersen and Geil's bound. The bound has the same flavor as the Feng-Rao bound. In particular it also enables an improved code construction. The exposition in [1] starts by treating the general linear code set-up. It is then simply a matter of translation to reformulate the bound in the setting of order domain codes and affine variety codes [1, 17]. In particular an improvement to the Goppa bound for primary one-point algebraic geometric codes is given in [1, Th. 33 and Pr. 37]. Recent papers [27, 28] show how to decode a certain class of one-point algebraic geometric codes up to half the value of Andersen and Geil's bound. (See [19, Prop. 6] for a proof that the error-correcting capability is actually that of Andersen and Geil's bound). A generalization of the previous algorithm [28] for decoding general primary one-point algebraic geometric codes has been given in [19, 20], furthermore it can decode beyond that number.

Although the two bounds are of a similar flavor, to the best of our knowledge till now no general correspondence between the Feng-Rao bound and Andersen and Geil's bound has been established. The following is known about the correspondence: Firstly, Shibuya and Sakaniwa in [35] derive a bound on the minimum distance of primary codes. This bound relies on the Feng-Rao bound for generalized Hamming weights. As demonstrated in [1, Sec. 5] one can in a certain sense view Andersen and Geil's bound as an improvement to Shibuya and Sakaniwa's bound. Secondly, for the case of isometry-dual one-point algebraic geometric codes it was shown in [21] that the Feng-Rao bound and Andersen and Geil's bound produce the same result. This is in contrast with the general case of one-point algebraic geometric codes where the two bounds may produce completely different values [1, Ex. 51]. In the light of Section 6 below, [30, Sec. 4] constitutes another example of the two bounds producing different values. Finally, a result in a different direction was established in [21] where it was shown that for one-point algebraic geometric codes one can view Andersen and Geil's bound as a consequence of the Beelen bound [2] for more point codes and thereby also as a consequence of the Duursma-Kirov-Park bound [7, 8] for such codes. However, it seems prohibitively difficult to prove the equality between the error correction capability of [27, 28] and half the bounds in [2, 7, 8], while we proved in just a few lines [19, Prop. 6] the equality between [27, 28] and half the bound in [1]. This demonstrates that Andersen and Geil's bound [1] is much more convenient than [2, 7, 8] in some cases, though the former [1] is implied by the latter [2, 7, 8].

The translations via generalized Hamming weights and via more point codes do not seem to suggest a simple connection between the Feng-Rao bound and Andersen and Geil's bound for minimum distance. Nevertheless, we shall demonstrate that such a connection does indeed exist. As a consequence, we can see that the error correction capability of the recently proposed decoding algorithms [27, 28] is equal to the Feng-Rao decoding algorithm for primary codes [30].

The above connection is of academic interest itself. But maybe more importantly, it enables us to decode primary codes up to what is guaranteed by Andersen and Geil's bound. As shall be demonstrated in the present paper it suffices to derive a particular dual description of the codes by means of linear algebra, and then to apply the three-bases generalization of the Feng-Rao decoding algorithm in [26, Sec. 4.3] and [30, Sec. 2], while a similar generalization appeared much earlier in [34]. The technique applies to a large variety of codes for which no efficient decoding algorithms are known. This includes important families of multivariate polynomial codes often considered by theoretical computer scientists. Another implication of the above mentioned connection is that it becomes clear that Andersen and Geil's bound is in some sense a generalization of Matsumoto and Miura's bound for primary one-point algebraic geometric codes [30, Secs. 3 & 4]. This also implies that the decoding method of the present paper can be viewed as a generalization of the decoding method for primary one-point algebraic geometric codes in [30]. It should be mentioned that another generalization of Matsumoto and Miura's bound and decoding method is given by Beelen and Høholdt in [3] where more point codes $C_{\mathcal{L}}(D, G)$ are treated.

The present paper starts by treating in Sections 2 and 3 the general case of linear codes. Section 2 describes the state of the art and Section 3 establishes the connection between the two bounds. In Section 4 we briefly discuss how to use the results from Section 2 and 3 when a supporting algebra is given. A couple of examples illustrate the idea. The new decoding method for primary codes is then treated in Section 5. In Section 6 we investigate the connection between Andersen and Geil's bound when applied to primary one-point algebraic geometric codes and the bound by Matsumoto and Miura for similar codes. The correspondence in Section 3 has implications for the estimation of generalized Hamming weights. We briefly comment on this fact in Section 7.

As a consequence of our findings in the present paper we suggest that the Feng-Rao bound is in the future called "the Feng-Rao bound for dual codes" and that Andersen and Geil's bound is called "the Feng-Rao bound for primary codes". Similarly, we suggest that the order bound is in the future called "the order bound for dual codes" whereas the bound by Andersen and Geil for order domain codes is named "the order bound for primary codes". We shall stick to this naming throughout the remaining part of the paper.

2. The general linear code formulation

Let $\mathcal{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ be a basis for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. Consider a non-empty set $I \subseteq \{1, 2, \ldots, n\}$. We shall study the code

$$C(\mathcal{B}, I) = \mathrm{span}_{\mathbb{F}_q}\{\boldsymbol{b}_i \mid i \in I\}$$

and its dual, which we denote by $C^{\perp}(\mathcal{B}, I)$.
Let $L_{-1} = \emptyset$, $L_0 = \{\boldsymbol{0}\}$, and define for $l = 1, \ldots, n$, $L_l = \mathrm{span}_{\mathbb{F}_q}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_l\}$. We have

$$\emptyset = L_{-1} \subsetneq L_0 \subsetneq \cdots \subsetneq L_n = \mathbb{F}_q^n.$$

Hence, the following definition makes sense.

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

We equip $\mathbb{F}_q^n$ with a second binary operation namely the component-wise product

$$(u_1, \ldots, u_n) * (v_1, \ldots, v_n) = (u_1 v_1, \ldots, u_n v_n).$$

With the above in hand we can introduce the concept of well-behaving pairs which plays a fundamental role in the Feng-Rao bound for dual codes as well as in the Feng-Rao bound for primary codes.

Definition 2. Consider two bases $\mathcal{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ and $\mathcal{U} = \{\boldsymbol{u}_1, \ldots \boldsymbol{u}_n\}$ for $\mathbb{F}_q^n$ as vector space over $\mathbb{F}_q$ (we may or may not have $\mathcal{B} = \mathcal{U}$).
An ordered pair $(i, j) \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, n\}$ is said to be well-behaving (WB) with respect to $(\mathcal{B}, \mathcal{U})$ if

$$\bar{\rho}_{\mathcal{B}}(\boldsymbol{b}_u * \boldsymbol{u}_v) < \bar{\rho}_{\mathcal{B}}(\boldsymbol{b}_i * \boldsymbol{u}_j)$$

holds for all u and v with $1 \leq u \leq i, 1 \leq v \leq j$ and $(u, v) \neq (i, j)$.
An ordered pair $(i, j) \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, n\}$ is said to be weakly well-behaving (WWB) with respect to $(\mathcal{B}, \mathcal{U})$ if

$$\bar{\rho}_{\mathcal{B}}(\boldsymbol{b}_u * \boldsymbol{u}_j) < \bar{\rho}_{\mathcal{B}}(\boldsymbol{b}_i * \boldsymbol{u}_j),$$
$$\bar{\rho}_{\mathcal{B}}(\boldsymbol{b}_i * \boldsymbol{u}_v) < \bar{\rho}_{\mathcal{B}}(\boldsymbol{b}_i * \boldsymbol{u}_j)$$

hold for all $u < i$ and $v < j$.
Even less restrictively an ordered pair $(i, j) \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, n\}$ is said to be one-way well-behaving (OWB) with respect to $(\mathcal{B}, \mathcal{U})$ if

$$\bar{\rho}_{\mathcal{B}}(\boldsymbol{b}_u * \boldsymbol{u}_j) < \bar{\rho}_{\mathcal{B}}(\boldsymbol{b}_i * \boldsymbol{u}_j)$$

holds for $u < i$.

Remark 3. Clearly, WB implies WWB which again implies OWB.

The Feng-Rao bound for dual codes and the Feng-Rao bound for primary codes are about counting well-behaving pairs satisfying certain criteria. Assume in the following that $\mathcal{B}$ and $\mathcal{U}$ are fixed. To introduce the Feng-Rao bound for dual codes we define for $l = 1, 2, \ldots, n$

$$\begin{aligned}\bar{\mu}^{\mathrm{WB}}_{(\mathcal{B},\mathcal{U})}(l) &= \sharp\{i \in \{1, 2, \ldots, n\} \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{u}_j) = l \text{ for some } \boldsymbol{u}_j \in \mathcal{U} \\ &\qquad \text{with } (i, j) \text{ WB } \}, \\ \bar{\mu}^{\mathrm{OWB}}_{(\mathcal{B},\mathcal{U})}(l) &= \sharp\{i \in \{1, 2, \ldots, n\} \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{u}_j) = l \text{ for some } \boldsymbol{u}_j \in \mathcal{U} \\ &\qquad \text{with } (i, j) \text{ OWB } \}.\end{aligned}$$

We stress that our definition of $\overline{\mu}^{\mathrm{WB}}_{(\mathcal{B},\mathcal{U})}$ is equivalent to the following form usually found in the literature:

$$\overline{\mu}^{\mathrm{WB}}_{(\mathcal{B},\mathcal{U})}(l) = \sharp\{(i,j) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,n\} \mid \overline{\rho}(\boldsymbol{b}_i * \boldsymbol{u}_j) = l \text{ with } (i,j) \text{ WB } \}.$$

To introduce the Feng-Rao bound for primary codes we define for $i = 1,2,\ldots,n$

$$\overline{\sigma}^{\mathrm{WB}}_{(\mathcal{B},\mathcal{U})}(i) = \sharp\{l \in \{1,2,\ldots,n\} \mid \overline{\rho}(\boldsymbol{b}_i * \boldsymbol{u}_j) = l \text{ for some } \boldsymbol{u}_j \in \mathcal{U} \text{ with } (i,j) \text{ WB}\},$$

$$\overline{\sigma}^{\mathrm{OWB}}_{(\mathcal{B},\mathcal{U})}(i) = \sharp\{l \in \{1,2,\ldots,n\} \mid \overline{\rho}(\boldsymbol{b}_i * \boldsymbol{u}_j) = l \text{ for some } \boldsymbol{u}_j \in \mathcal{U} \text{ with } (i,j) \text{ OWB}\}.$$

In the next theorem the first bound is the Feng-Rao bound for dual codes. The latter is the Feng-Rao bound for primary codes.

Theorem 4. *The minimum distance of $C^{\perp}(\mathcal{B}, I)$ satisfies:*

$$d(C^{\perp}(\mathcal{B},I)) \geq \min\{\overline{\mu}^{OWB}_{(\mathcal{B},\mathcal{U})}(l) \mid l \notin I\} \quad (1)$$

$$\geq \min\{\overline{\mu}^{WB}_{(\mathcal{B},\mathcal{U})}(l) \mid l \notin I\}. \quad (2)$$

The minimum distance of $C(\mathcal{B}, I)$ satisfies:

$$d(C(\mathcal{B},I)) \geq \min\{\overline{\sigma}^{OWB}_{(\mathcal{B},\mathcal{U})}(i) \mid i \in I\} \quad (3)$$

$$\geq \min\{\overline{\sigma}^{WB}_{(\mathcal{B},\mathcal{U})}(i) \mid i \in I\}. \quad (4)$$

Proof. For proofs of the bounds (1) and (3) see [23, Th. 1]. □

The bound (3) is a slight enhancement of (4), the latter being introduced for the first time in [1]. This explains why we in Section 1 referred to both bounds as Andersen and Geil's bound. The bound (2) is a special case of the three-bases formulation [26, Sec. 4.3], [30, Sec. 2] of the original Feng-Rao bound [9, 10, 11]. The formulation in [26, 30] involves three bases rather than only the above two. We note that three bases were also used earlier in [34] for expressing the idea of Feng and Rao [9] in the general linear code formulation. The contribution of [23] is the notion of OWB as a generalization of WWB [31, 32]. If we replace OWB with WWB in (1) then we get another special case of [30].

Note, that Theorem 4 allows us to construct improved codes by choosing I cleverly according to the $\overline{\mu}$ respectively $\overline{\sigma}$ values. Remark 3 demonstrates that Theorem 4 can also be formulated in a version with WWB instead of OWB or WB (See [30]). However, the result to be shown in the next section that (1) and (3) respectively (2) and (4) are consequences of each other seemingly does not hold for WWB.

3. The two bounds are consequences of each other

In this section we consider two bases $\mathcal{G} = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n\}$ and $\mathcal{H} = \{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_n\}$ for $\mathbb{F}_q^n$. They shall both be used in replacement of the $\mathcal{B}$ from the previous section. The basis $\mathcal{U} = \{\boldsymbol{u}_1, \ldots \boldsymbol{u}_n\}$ will be fixed throughout the section. Hence, we will be concerned with WB and OWB pairs with respect to $(\mathcal{G}, \mathcal{U})$ as well as with respect to $(\mathcal{H}, \mathcal{U})$.

We shall assume the following strong relation

$$\boldsymbol{g}_i \cdot \boldsymbol{h}_j = \delta_{i,n-j+1} \tag{5}$$

where the expression on the left side is the inner product and the expression on the right side is Kronecker's delta. Clearly, if $\mathcal{G}$ is given then there is a unique choice of $\mathcal{H}$ such that (5) holds and vice versa. Let G be an $n \times n$ matrix where row i equals $\boldsymbol{g}_i$ and let H be an $n \times n$ matrix where column j equals $\boldsymbol{h}_{n-j+1}^T$. Then indeed $H = G^{-1}$.

The above correspondence gives us an alternative expression for the function $\overline{\rho}$ (Definition 1), namely that for any non-zero $\boldsymbol{v}$

$$\overline{\rho}_{\mathcal{G}}(\boldsymbol{v}) = \max\{k \mid \boldsymbol{v} \cdot \boldsymbol{h}_{n-k+1} \neq 0\},$$

$$\overline{\rho}_{\mathcal{H}}(\boldsymbol{v}) = \max\{k \mid \boldsymbol{v} \cdot \boldsymbol{g}_{n-k+1} \neq 0\}.$$

For $I \subseteq \{1, \ldots, n\}$ denote

$$\overline{I} = \{1, \ldots, n\} \backslash \{n - i + 1 \mid i \in I\}$$

and observe $\overline{\overline{I}} = I$. Equation (5) corresponds to saying

$$C(\mathcal{G}, I) \quad = \quad C^{\perp}(\mathcal{H}, \overline{I})$$

which can of course also be formulated

$$C(\mathcal{G}, \overline{I}) \quad = \quad C^{\perp}(\mathcal{H}, I).$$

We shall show that for $i = 1, \ldots, n$ it holds that

$$\begin{aligned} \overline{\mu}^{\mathrm{WB}}_{(\mathcal{H},\mathcal{U})}(n-i+1) &= \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{U})}(i), \\ \overline{\mu}^{\mathrm{OWB}}_{(\mathcal{H},\mathcal{U})}(n-i+1) &= \overline{\sigma}^{\mathrm{OWB}}_{(\mathcal{G},\mathcal{U})}(i) \end{aligned}$$

which is to say that for WB and OWB the Feng-Rao bound for dual codes and the Feng-Rao bound for primary codes are consequences of each other. The fact that a similar result seemingly does not hold for WWB might partially explain why the correspondences of the present paper has not been found before.

Lemma 5. *The following statements are equivalent:*

1. $\overline{\rho}_{\mathcal{G}}(\boldsymbol{g}_i * \boldsymbol{u}_j) = k$ *and* (i, j) *is WB with respect to* $(\mathcal{G}, \mathcal{U})$.
2. $\overline{\rho}_{\mathcal{H}}(\boldsymbol{h}_{n-k+1} * \boldsymbol{u}_j) = n - i + 1$ *and* $(n - k + 1, j)$ *is WB with respect to* $(\mathcal{H}, \mathcal{U})$.

Proof. We shall make extensive use of the correspondence

$$(\boldsymbol{v} * \boldsymbol{w}) \cdot \boldsymbol{s} = (\boldsymbol{s} * \boldsymbol{w}) \cdot \boldsymbol{v}. \tag{6}$$

Assume that statement 1 holds. That is assume $\overline{\rho}_{\mathcal{G}}(\boldsymbol{b}_i * \boldsymbol{u}_j) = k$ and (i, j) is WB with respect to $(\mathcal{G}, \mathcal{U})$. From the first half of this assumption we get

$$(\boldsymbol{g}_i * \boldsymbol{u}_j) \cdot \boldsymbol{h}_{n-k+1} \neq 0, \tag{7}$$
$$(\boldsymbol{g}_i * \boldsymbol{u}_j) \cdot \boldsymbol{h}_t = 0 \quad \text{for } t < n - k + 1, \tag{8}$$

and from the latter half

$$(\boldsymbol{g}_{i'} * \boldsymbol{u}_j) \cdot \boldsymbol{h}_t = 0 \quad \text{for } i' < i \text{ and } t \leq n - k + 1, \tag{9}$$
$$\begin{aligned} (\boldsymbol{g}_i * \boldsymbol{u}_{j'}) \cdot \boldsymbol{h}_t &= 0 \quad \text{for } j' < j \text{ and } t \leq n - k + 1, \\ (\boldsymbol{g}_{i'} * \boldsymbol{u}_{j'}) \cdot \boldsymbol{h}_t &= 0 \quad \text{for } i' < i, j' < j \text{ and } t \leq n - k + 1. \end{aligned} \tag{10}$$

Using (7), (9) in combination with (6) gives

$$(\boldsymbol{h}_{n-k+1} * \boldsymbol{u}_j) \cdot \boldsymbol{g}_i \neq 0, \tag{11}$$
$$(\boldsymbol{h}_{n-k+1} * \boldsymbol{u}_j) \cdot \boldsymbol{g}_{i'} = 0 \text{ for } i' < i. \tag{12}$$

In a similar fashion we derive at

$$(\boldsymbol{h}_t * \boldsymbol{u}_j) \cdot \boldsymbol{g}_{i'} = 0 \quad \text{for } t < n - k + 1 \text{ and } i' \leq i, \tag{13}$$
$$(\boldsymbol{h}_{n-k+1} * \boldsymbol{u}_{j'}) \cdot \boldsymbol{g}_{i'} = 0 \quad \text{for } j' < j \text{ and } i' \leq i, \tag{14}$$
$$(\boldsymbol{h}_t * \boldsymbol{u}_{j'}) \cdot \boldsymbol{g}_{i'} = 0 \quad \text{for } t < n - k + 1, j' < j, \text{ and } i' \leq i. \tag{15}$$

Expressions (11) and (12) mean that $\overline{\rho}_{\mathcal{H}}(\overline{h}_{n-k+1} * \boldsymbol{u}_j) = n - i + 1$ and (13), (14), (15) imply that $(n - k + 1, j)$ is WB with respect to $(\mathcal{H}, \mathcal{U})$. In other words statement 2 is true. That statement 2 implies statement 1 follows by symmetry. □

Lemma 6. *The following statements are equivalent*

1. $\overline{\rho}_{\mathcal{G}}(\boldsymbol{g}_i * \boldsymbol{u}_j) = k$
   and (i, j) *is OWB with respect to* $(\mathcal{G}, \mathcal{U})$.
2. $\overline{\rho}_{\mathcal{H}}(\boldsymbol{h}_{n-k+1} * \boldsymbol{u}_j) = n - i + 1$
   and $(n - k + 1, j)$ *is OWB with respect to* $(\mathcal{H}, \mathcal{U})$.

Proof. Assume that statement 1 holds. The first part implies (7) and (8) and from the latter part we get (9). Using (7), (9) in combination with (6) gives (11) and (12). Combining (8), (9) with (6) we get (13). Expressions (11) and (12) mean that $\overline{\rho}_{\mathcal{H}}(\overline{h}_{n-k+1} * \boldsymbol{u}_j) = n - i + 1$ and (13) implies that $(n - k + 1, j)$ is OWB with respect to $(\mathcal{H}, \mathcal{U})$. In other words statement 2 is true. That statement 2 implies statement 1 follows by symmetry. □

Theorem 7. *Assume that* $\mathcal{G}, \mathcal{H}$ *satisfy condition (5). Let a non-empty set* $I \subseteq \{1, 2, \ldots, n\}$ *be given. Then* $C(\mathcal{G}, I) = C^{\perp}(\mathcal{H}, \overline{I})$ *and*

$$\min\{\overline{\mu}^{OWB}_{(\mathcal{H},\mathcal{U})}(l) \mid l \neq \overline{I}\} = \min\{\overline{\sigma}^{OWB}_{(\mathcal{G},\mathcal{U})}(i) \mid i \in I\}, \quad (16)$$

$$\min\{\overline{\mu}^{WB}_{(\mathcal{H},\mathcal{U})}(l) \mid l \neq \overline{I}\} = \min\{\overline{\sigma}^{WB}_{(\mathcal{G},\mathcal{U})}(i) \mid i \in I\}. \quad (17)$$

Similar results hold with the role of I *and* $\overline{I}$ *interchanged.*

Proof. Follows from Lemma 5, Lemma 6 and the fact that $i \in I \Leftrightarrow n - i + 1 \notin \overline{I}$. □

Remark 8. Consider the following assumption which is weaker than (5):

$$\begin{cases} \boldsymbol{g}_i \cdot \boldsymbol{h}_{n-i+1} \neq 0, & \\ \boldsymbol{g}_i \cdot \boldsymbol{h}_j = 0 & \text{for } j < n - i + 1. \end{cases} \quad (18)$$

Inspecting the proofs of Lemma 5 and 6 we see that (16) and (17) still hold. However, $C(\mathcal{G}, I) = C^{\perp}(\mathcal{H}, \overline{I})$ is only guaranteed to hold when I is of the form $I = \{1, 2, \ldots, k\}$ under the assumption (18) that is weaker than (5). Therefore (18) does not allow us to translate information regarding improved primary codes $C(\mathcal{G}, I)$ and improved dual codes $C^{\perp}(\mathcal{H}, \overline{I})$.

The above remark is in the spirit of [6] where Duursma showed how to speed up the erasure decoding of algebraic geometric codes, by introducing a condition [6, Def. 4] that is implied by (5) and implies (18). After having finished the manuscript we learned that Duursma is aware of the implication (17) of (18) to the Feng-Rao bound for the case of non-improved codes, i.e. I is of the form $\{1, \ldots, k\}$.

The following example illustrates the last part of the remark.

Example 1. Let $n = 4$ and $I = \{3, 4\}$. This gives $\bar{I} = \{3, 4\}$. Assume $\mathcal{G}$ and $\mathcal{H}$ are given such that (18) is satisfied. We keep $\mathcal{H}$, leaving $C^{\perp}(\mathcal{H}, \bar{I})$ intact, but allow for redefinition of $\mathcal{G}$ by replacing for $i = 1, \ldots, 4$, $\boldsymbol{g}_i$ with any other vector of $\bar{\rho}_{\mathcal{G}}$-value equal to i. This possibly redefines $C(\mathcal{G}, I)$ but keeps the estimates of the minimum distance the same. Even allowing for the above redefinition (18) is not enough to guarantee that for any of the above choices of g_3, g_4 we arrive at $\boldsymbol{h}_i \cdot \boldsymbol{g}_j = 0$ for all $i = 3, 4$ and $j = 3, 4$. Hence, we have no guarantee that all of the resulting codes $C(\mathcal{G}, I)$ equals $C^{\perp}(\mathcal{H}, \bar{I})$.

4. Utilizing a supporting algebra

As mentioned in the introduction the results in Section 2 and 3 are universal in the sense that they can in particular be applied when given various types of supporting algebra. We now explain how to do this in the case of the supporting algebra being an order domain. We shall restrict to order functions that are weight functions. From [1, Sec. 6] we have the following couple of results.

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

- $(W.0)$ $\rho(f) = -\infty$ if and only if $f = 0$.
- $(W.1)$ $\rho(af) = \rho(f)$ for all non-zero $a \in \mathbb{F}_q$.
- $(W.2)$ $\rho(f + g) \preceq \max\{\rho(f), \rho(g)\}$ and equality holds when $\rho(f) \prec \rho(g)$.
- $(W.3)$ If $\rho(f) \prec \rho(g)$ and $h \neq 0$, then $\rho(fh) \prec \rho(gh)$.
- $(W.4)$ If f and g are non-zero and $\rho(f) = \rho(g)$, then there exists a non-zero $a \in \mathbb{F}_q$ such that $\rho(f - ag) \prec \rho(g)$.
- $(W.5)$ If f and g are non-zero then $\rho(fg) = \rho(f) + \rho(g)$.

An $\mathbb{F}_q$-algebra with a weight function is called an order domain over $\mathbb{F}_q$.

Theorem 10. *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 $R_\gamma = \{f \in R \mid \rho(f) \preceq \gamma\}$.* □

Definition 11. Let R be an $\mathbb{F}_q$-algebra. A surjective map $\varphi : R \rightarrow \mathbb{F}_q^n$ 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 $f, g \in R$.

Definition 12. Assume that φ is a morphism as in Definition 11. Let $\alpha(1) = \mathbf{0}$. For $i = 2, 3, \ldots, n$ define 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 $\gamma \prec \alpha(i)$. Write $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$.

The following theorem is a synthesis [1, Th. 25, Pro. 27, 28].

Theorem 13. *Let $\Delta(R,\rho,\varphi) = \{\alpha(1),\alpha(2),\ldots,\alpha(n)\}$ be as in Definition 12. The set*

$$\mathcal{B} = \{\boldsymbol{b}_1 = \varphi(f_{\alpha(1)}), \boldsymbol{b}_2 = \varphi(f_{\alpha(2)}), \ldots, \boldsymbol{b}_n = \varphi(f_{\alpha(n)})\} \tag{19}$$

constitutes a basis for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$.

If $\gamma, \lambda \in \Gamma$ satisfy $\gamma + \lambda = \alpha(l)$ for some $\alpha(l) \in \Delta(R,\rho,\varphi)$ then $\gamma = \alpha(i)$ and $\lambda = \alpha(j)$ for some $i, j \in \{1,\ldots,n\}$ and (i, j) is WB with respect to $(\mathcal{B},\mathcal{B})$. □

Theorem 13 in combination with (4) respectively (2) proves the order bound for primary [1] respectively dual [26] order domain codes. To formulate these bounds we will need a definition.

Definition 14. Let notation be as in Definition 12. For $\lambda \in \Delta(R,\rho,\varphi)$ we define

$$\sigma(\lambda) = \sharp\{\eta \in \Delta(R,\rho,\varphi) \mid \eta = \lambda + \gamma \text{ for some } \gamma \in \Gamma\}.$$

For $\eta \in \Delta(R,\rho,\varphi)$ define

$$\mu(\eta) = \sharp\{\lambda \in \Gamma \mid \lambda + \gamma = \eta \text{ for some } \gamma \in \Gamma\}.$$

The bounds are:

Theorem 15. *Let $\mathcal{B}$ be as in Theorem 13. The minimum distance of $C(\mathcal{B}, I)$ is at least* $\min \sigma(\alpha(i)) \mid i \in I\}$. *The minimum distance of $C^{\perp}(\mathcal{B}, I)$ is at least* $\min\{\mu(\alpha(l)) \mid l \in \{1,\ldots,n\}\backslash I\}$. □

Just as with the Feng-Rao bounds, the order bounds suggest improved code constructions by choosing I cleverly. The best-known example of an order domain is the following. Consider an algebraic function field over $\mathbb{F}_q$ of transcendence degree 1. Let $P_1,\ldots,P_n,Q$ be rational places. Then $R = \sum_{m=0}^{\infty} \mathcal{L}(mQ)$ is an order domain with a weight function $\rho(f) = -\nu_Q(f)$. Here, ν_Q is the discrete valuation corresponding to Q. Let φ be defined by $\varphi(f) = (f(P_1),\ldots,f(P_n))$. Applying the standard notation for Weierstrass semigroups we have $\Gamma = H(Q)$. The corresponding set $\Delta(R,\rho,\varphi)$ sometimes in the literature is denoted $H^*(Q)$ [21].

It is well-known [3, 30] how to decode primary codes defined from algebraic function fields of transcendence degree 1. In Section 5 we shall see how to decode primary codes coming form order domains of higher transcendence degree. Examples of order domains of higher transcendence degree can be found in

[1, 13, 14, 15, 22, 29, 33]. The most simple example of such an order domain is $R = \mathbb{F}_q[X_1, \ldots, X_m]$ with a weight function given by $\rho(X_1^{i_1} \cdots X_m^{i_m}) = (i_1, \ldots, i_m)$ and the ordering $\prec$ (Definition 9) being any fixed monomial ordering. Evaluating in all the points of $\mathbb{F}_q^m$ we get q-ary Reed-Muller codes, Massey-Costello-Justesen codes (also known as hyperbolic codes) and weighted Reed-Muller codes. Theoretical computer scientists take a special interest in the case where rather than evaluating in all of $\mathbb{F}_q^m$ one evaluates in an arbitrary Cartesian product $S_1 \times \cdots \times S_m$, where $S_1, \ldots, S_m \subseteq \mathbb{F}_q$. Such codes can have surprisingly good parameters as demonstrated in [24]. Their good parameters cannot be obtained as the punctured codes of the ordinary Reed-Muller codes. The following two examples illustrate the theory from Section 3 when $R = \mathbb{F}_q[X, Y]$ and the Cartesian product $S_1 \times S_2$ is a proper subset of $\mathbb{F}_q^2$.

Example 2. Consider $R = \mathbb{F}_5[X, Y]$, $\rho(X^iY^j) = (i, j)$ and let $\prec$ be the graded lexicographic ordering with $(1, 0) \prec (0, 1)$. Consider the point ensemble

$$\{P_1 = (1, 1), P_2 = (1, 2), P_3 = (1, 3), P_4 = (2, 1), \ldots, P_9 = (3, 3)\} \\ = \{1, 2, 3\} \times \{1, 2, 3\} \subseteq \mathbb{F}_5^2$$

and the morphism $\mathrm{ev} : \mathbb{F}_5[X.Y] \to \mathbb{F}_5^9$, given by $\mathrm{ev}(F) = (F(P_1), \ldots, F(P_9))$. The basis (19) becomes (writing $\mathcal{G}$ instead of $\mathcal{B}$ as we want to apply the theory from Section 3)

$$\begin{aligned} \mathcal{G} \;=\; \{&\boldsymbol{g}_1 = \mathrm{ev}(1), \boldsymbol{g}_2 = \mathrm{ev}(X), \boldsymbol{g}_3 = \mathrm{ev}(Y), \boldsymbol{g}_4 = \mathrm{ev}(X^2), \boldsymbol{g}_5 = \mathrm{ev}(XY), \\ &\boldsymbol{g}_6 = \mathrm{ev}(Y^2), \boldsymbol{g}_7 = \mathrm{ev}(X^2Y), \boldsymbol{g}_8 = \mathrm{ev}(XY^2), \boldsymbol{g}_9 = \mathrm{ev}(X^2Y^2)\}. \end{aligned}$$

Still using the notation from Section 3 let $\mathcal{U} = \mathcal{G}$. From Theorem 13 we immediately get information about WB pairs as described in the following array. Here a number x in entry (i, j) means that (i, j) is known to be WB and that $\bar{\rho}_{\mathcal{G}}(\boldsymbol{g}_i * \boldsymbol{g}_j) = x$.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & & 7 & 8 & & 9 & \\ 3 & 5 & 6 & 7 & 8 & & 9 & & \\ 4 & & 7 & & & 9 & & & \\ 5 & 7 & 8 & & 9 & & & & \\ 6 & 8 & & 9 & & & & & \\ 7 & & 9 & & & & & & \\ 8 & 9 & & & & & & & \\ 9 & & & & & & & & \end{bmatrix} \tag{20}$$

It is now an easy task to calculate from this array

$$\begin{array}{lll} \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(1) = 9, & \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(2) \geq 6, & \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(3) \geq 6, \\ \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(4) \geq 3, & \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(5) \geq 4, & \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(6) \geq 3, \\ \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(7) \geq 2, & \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(8) \geq 2, & \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(9) \geq 1, \end{array}$$

(actually, equality holds – also even if we replace WB with OWB – but we will not prove this fact). Using a computer we found $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_9$ and the corresponding polynomials. We have:

$$\begin{array}{rcl} \boldsymbol{h}_1 &=& \mathrm{ev}(X^2Y^2 + XY^2 + X^2Y + XY), \\ \boldsymbol{h}_2 &=& \mathrm{ev}(X^2Y^2 + 3XY^2 + X^2Y + Y^2 + 3XY + Y), \\ \boldsymbol{h}_3 &=& \mathrm{ev}(X^2Y^2 + XY^2 + 3X^2Y + 3XY + X^2 + X), \\ \boldsymbol{h}_4 &=& \mathrm{ev}(XY^2 + Y^2 + XY + Y), \\ \boldsymbol{h}_5 &=& \mathrm{ev}(X^2Y^2 + 3XY^2 + 3X^2Y + Y^2 + 4XY + X^2 + 3Y + 3X + 1), \\ \boldsymbol{h}_6 &=& \mathrm{ev}(X^2Y + XY + X^2 + X), \\ \boldsymbol{h}_7 &=& \mathrm{ev}(XY^2 + Y^2 + 3XY + 3Y + X + 1), \\ \boldsymbol{h}_8 &=& \mathrm{ev}(X^2Y + 3XY + X^2 + Y + 3X + 1), \\ \boldsymbol{h}_9 &=& \mathrm{ev}(XY + Y + X + 1). \end{array}$$

It is clearly not at all an easy task to determine by hand WB pairs with respect to $(\mathcal{H}, \mathcal{G})$ without using (20) and the correspondence in Lemma 5. A similar observation holds regarding $\overline{\rho}_{\mathcal{H}}(\boldsymbol{h}_i * \boldsymbol{g}_j)$.

Example 3. Consider $R = \mathbb{F}_4[X, Y]$ with ρ and $\prec$ as in Example 2. Write $\mathbb{F}_4 = \mathbb{F}_2[T]\backslash\langle T^2 + T + 1\rangle$ and let $\alpha = T + \langle T^2 + T + 1\rangle$. The point ensemble

$$\{P_1 = (0, 1), P_2 = (0, \alpha), P_3 = (1, 1), P_4 = (1, \alpha), P_5 = (\alpha, 1), P_6 = (\alpha, \alpha)\} \\ = \{0, 1, \alpha\} \times \{1, \alpha\} \subseteq \mathbb{F}_4^2$$

defines a morphism $\mathrm{ev} : \mathbb{F}_4[X, Y] \to \mathbb{F}_4^6$ by $\mathrm{ev}(F) = (F(P_1), \ldots, F(P_6))$. The basis (19) becomes

$$\begin{array}{rcl} \mathcal{G} &=& \{\boldsymbol{g}_1 = \mathrm{ev}(1), \boldsymbol{g}_2 = \mathrm{ev}(X), \boldsymbol{g}_3 = \mathrm{ev}(Y), \\ && \boldsymbol{g}_4 = \mathrm{ev}(X^2), \boldsymbol{g}_5 = \mathrm{ev}(XY), \boldsymbol{g}_6 = \mathrm{ev}(X^2Y)\}. \end{array}$$

Again we let $\mathcal{U} = \mathcal{G}$. Using Theorem 13 we easily derive information on $\overline{\rho}_{\mathcal{G}}$ as well as information on which pairs are WB. From this we conclude

$$\begin{array}{lll} \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(1) = 6, & \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(2) \geq 4, & \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(3) \geq 3, \\ \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(4) \geq 2, & \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(5) \geq 2, & \overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(6) = 1, \end{array}$$

(again actually equalities hold). Using a computer we found $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_6$ and the polynomials behind them. They are:

$$
\begin{aligned}
\boldsymbol{h}_1 &= \mathrm{ev}(\alpha X + 1), \\
\boldsymbol{h}_2 &= \mathrm{ev}(\alpha X^2 + \alpha + 1), \\
\boldsymbol{h}_3 &= \mathrm{ev}(\alpha XY + Y + X + \alpha + 1), \\
\boldsymbol{h}_4 &= \mathrm{ev}(X^2 + (\alpha + 1)X + \alpha), \\
\boldsymbol{h}_5 &= \mathrm{ev}(\alpha X^2 Y + X^2 + (\alpha + 1)Y + \alpha), \\
\boldsymbol{h}_6 &= \mathrm{ev}(X^2 Y + (\alpha + 1)XY + (\alpha + 1)X^2 + \alpha Y + \alpha X + 1).
\end{aligned}
$$

Some information on the values of $\overline{\mu}^{\mathrm{WB}}_{(\mathcal{H},\mathcal{G})}(1), \ldots, \overline{\mu}^{\mathrm{WB}}_{(\mathcal{H},\mathcal{G})}(6)$ can be seen directly from $\mathcal{H}$ and $\mathcal{G}$, but one does not get the complete picture without using Lemma 6 or alternatively a computer.

5. Feng-Rao decoding

We now turn to the problem of decoding primary codes up to half the Feng-Rao bound. In this section we assume that two bases $\mathcal{G}, \mathcal{U}$ are given. We consider a primary code $C(\mathcal{G}, I)$ and assume that we have information about WB pairs with respect to $(\mathcal{G}, \mathcal{U})$. To set up the decoding algorithm, the first task is to calculate the basis $\mathcal{H}$ such that the correspondence (5) holds. Using Lemma 5 we then translates the information we have on WB pairs with respect to $(\mathcal{G}, \mathcal{U})$ into information on WB pairs with respect to $(\mathcal{H}, \mathcal{U})$. Decoding $C(\mathcal{G}, I)$ up to half the Feng-Rao bound for primary codes by Theorem 7 now is the same as decoding $C^{\perp}(\mathcal{H}, \overline{I})$ up to half the Feng-Rao bound for dual codes. The contribution of the present paper regarding decoding basically is this observation. In [26] Høholdt, van Lint and Pellikaan presented a couple of decoding algorithms that correct up to half the order bound for dual codes. Of particular interest to us is the algorithm in [26, Sec. 6.3]. This algorithm uses majority voting for unknown syndromes and builds on the work by Feng and Rao [9] and Duursma [4, 5]. For this algorithm to be applicable to the situation of general codes $C^{\perp}(\mathcal{H}, \overline{I})$ a couple of modifications are needed. These modifications were described by Matsumoto and Miura in [30, Sec. 2]. Actually, the description in [30] is a little more general than we need as three bases are involved in their description in contrast to our two $\mathcal{H}, \mathcal{U}$. Obviously, the problem is solved by letting two of them being the same. By [30, Prop. 2.5] the algorithm can correct up to

$$
(\min\{\overline{\mu}^{\mathrm{WB}}_{(\mathcal{H},\mathcal{U})}(l) \mid l \notin \overline{I}\} - 1)/2
$$

errors in computational complexity $O(n^3)$.

As the description in [30, Sec. 2] is rather brief in the following we shall give an overview of how to apply the above algorithm to our problem and illustrate it with an example (we refer to [26, 30] for more details). Observe that in practice we might only have partial information on which pairs (i, j) are WB. This is for instance the case when our information comes from the study of a supporting algebra. Clearly we can derive exact information on all WB pairs (i, j) and corresponding values $\overline{\rho}_{\mathcal{H}}(\boldsymbol{h}_i * \boldsymbol{u}_j)$ in a preparation step. This can be done in $O(n^4)$ operations which is more expensive than the algorithm itself. To treat also the case where one wants to avoid such a preparation step we define

$$\widetilde{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{U})}(i) = \sharp\{l \in \{1, 2, \ldots, n\} \mid \overline{\rho}(\boldsymbol{g}_i * \boldsymbol{u}_j) = l \text{ for some } \boldsymbol{u}_j \in \mathcal{U} \text{ where } (i, j) \text{ is known to be WB}\}$$

and we define $\widetilde{\mu}^{\mathrm{WB}}_{(\mathcal{H},\mathcal{U})}(i)$ by a similar correspondence as in Lemma 5. Let $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ be received where $\boldsymbol{c} \in C(\mathcal{G}, I) = C^{\perp}(\mathcal{H}, \overline{I})$. Under the assumption

$$w_H(\boldsymbol{e}) \leq \left(\min\{\widetilde{\sigma}^{\mathrm{WB}}_{\mathcal{B}}(i) \mid i \in I\} - 1\right)/2$$

which is equivalent to

$$w_H(\boldsymbol{e}) \leq \left(\min\{\widetilde{\mu}^{\mathrm{WB}}_{\mathcal{B}}(l) \mid l \notin \overline{I}\} - 1\right)/2 \tag{21}$$

we shall determine the syndromes

$$s_1 = \boldsymbol{h}_1 \cdot \boldsymbol{e}, \ldots, s_n = \boldsymbol{h}_n \cdot \boldsymbol{e}.$$

From this we will be able to calculate

$$\boldsymbol{e}^T = H^{-1} \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}.$$

Clearly, s_i is known for all $i \in \overline{I}$ as for such indexes $\boldsymbol{h}_i \cdot \boldsymbol{e} = \boldsymbol{h}_i \cdot \boldsymbol{r}$. We next determine the missing s_i's one by one by applying the following procedure iteratively. We shall need the notation

$$s_{vw} = (\boldsymbol{h}_v * \boldsymbol{u}_w) \cdot \boldsymbol{e},\ 1 \leq v, w \leq n$$

$$S(i, j) = (s_{vw})_{\substack{1 \leq v \leq i \\ 1 \leq w \leq j}}.$$

Let l be the smallest index such that s_l is not known. Consider all known ordered WB pairs (i, j) such that $\overline{\rho}_{\mathcal{H}}(\boldsymbol{h}_i * \boldsymbol{u}_j) = l$. The WB property ensures that we know $S(i-1, j-1)$, $S(i, j-1)$ and $S(i-1, j)$. If these three matrices are of the same rank then (i, j) is called a candidate. For each candidate (i, j) we proceed as follows:

1. Determine the unique scalar s'_{ij} such that $(s_{i1}, \ldots, s_{i(j-1)}, s'_{ij})$ belongs to the row space of $S(i-1, j)$.
2. The WB property ensures that we can write s_{ij} as a linear combination of $s_1, \ldots, s_l$ with the coefficient of s_l being non-zero. Assuming $s_{ij} = s'_{ij}$ holds, calculate s_l. This is the vote of (i, j).

Assumption (21) ensures that the majority of candidates vote for the correct value of s_l. Hence, we apply majority voting and proceed to the next unknown s_l if any.

In practice we will of course compute the basis $\mathcal{H}$ only once and then use this basis for every received word. Doing so however does not affect the fact that the complexity estimate of the algorithm is still $O(n^3)$.

Example 4. This is a continuation of Example 2. In this example we found the $\overline{\sigma}^{\mathrm{WB}}_{(\mathcal{G},\mathcal{G})}(i)$ values. Regarding the $\overline{\mu}^{\mathrm{WB}}_{(\mathcal{H},\mathcal{G})}(l)$ values we only noted that they could most easily be found by using the correspondence in Lemma 5. Doing this the array of information regarding WB pairs with respect to $(\mathcal{H}, \mathcal{G})$ turns out to be exactly the same as that for WB pairs with respect to $(\mathcal{G}, \mathcal{G})$. That is, the information is described in (20). Choosing $I = \{1, 2, 3, 5\}$ we get $C(\mathcal{G}, I) = C^{\perp}(\mathcal{H}, \overline{I})$ where $\overline{I} = \{1, 2, 3, 4, 6\}$. This is a code with parameters $[n, k, d] = [9, 4, 4]$. Consider the codeword

$$\boldsymbol{c} = 4\boldsymbol{g}_1 + 3\boldsymbol{g}_2 + 2\boldsymbol{g}_3 + \boldsymbol{g}_5 = (0, 3, 1, 4, 3, 2, 3, 3, 3).$$

Let $\boldsymbol{e} = (0, \ldots, 0, 1)$ and $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$. We shall use the majority voting algorithm to detect $\boldsymbol{e}$ using the information that $\boldsymbol{c} \in C^{\perp}(\mathcal{H}, \overline{I})$. The starting point is to calculate

$$s_1 = \boldsymbol{h}_1 \cdot \boldsymbol{r} = 4, s_2 = \boldsymbol{h}_2 \cdot \boldsymbol{r} = 3, s_3 = \boldsymbol{h}_3 \cdot \boldsymbol{r} = 3, s_4 = \boldsymbol{h}_4 \cdot \boldsymbol{r} = 3, s_6 = \boldsymbol{h}_6 \cdot \boldsymbol{r} = 3.$$

We start by looking for $s_5 = \boldsymbol{h}_5 \cdot \boldsymbol{e}$. In the following array a number k in position (i, j) means that $s_{ij} = k$ is known and ? means that $\overline{\rho}_{\mathcal{H}}(\boldsymbol{h}_i * \boldsymbol{g}_j) = 5$.

$$\begin{bmatrix} 4 & 2 & 2 & 1 & ? \\ 3 & 4 & ? & & \\ 3 & ? & & & \\ 3 & & & & \\ ? & & & & \end{bmatrix}.$$

The candidates are $(3, 2)$ and $(2, 3)$. Both vote for $s_5 = 1$.
Knowing now $s_1, \ldots, s_6$ we turn to investigate s_7. In the following array again

a number k in position (i, j) means that $s_{ij} = k$ is known; but now ? means that $\overline{\rho}_{\mathcal{H}}(\boldsymbol{h}_i * \boldsymbol{g}_j) = 7$.

$$\begin{bmatrix} 4 & 2 & 2 & 1 & 1 & 1 & ? \\ 3 & 4 & 4 & 2 & ? & & \\ 3 & 4 & 4 & ? & & & \\ 3 & 4 & ? & & & & \\ 1 & ? & & & & & \\ 3 & & & & & & \\ ? & & & & & & \end{bmatrix}.$$

Candidates are $(5, 2), (4, 3), (3, 4), (2, 5)$. All vote for $s_7 = 1$.
Turning to s_8 the array is

$$\begin{bmatrix} 4 & 2 & 2 & 1 & 1 & 1 & 3 & ? \\ 3 & 4 & 4 & 2 & 2 & ? & & \\ 3 & 4 & 4 & 2 & ? & & & \\ 3 & 4 & 4 & & & & & \\ 1 & 3 & ? & & & & & \\ 3 & ? & & & & & & \\ 1 & & & & & & & \\ ? & & & & & & & \end{bmatrix}.$$

The candidates are $(6, 8)$, $(5, 3)$, $(3, 5)$,$(2, 6)$ all of which vote for $s_8 = 1$.
Turning finally to s_9 we have

$$\begin{bmatrix} 4 & 2 & 2 & 1 & 1 & 1 & 3 & 3 & ? \\ 3 & 4 & 4 & 2 & 2 & 2 & 1 & ? & \\ 3 & 4 & 4 & 2 & 2 & 2 & ? & & \\ 3 & 4 & 4 & 2 & 2 & ? & & & \\ 1 & 3 & 3 & 4 & ? & & & & \\ 3 & 4 & 4 & ? & & & & & \\ 1 & 3 & ? & & & & & & \\ 1 & ? & & & & & & & \\ ? & & & & & & & & \end{bmatrix}.$$

Candidates are $(8, 2)$, $(7, 3), \ldots, (2, 8)$. All vote for $s_9 = 1$.

Finally

$$\boldsymbol{e}^T = [\boldsymbol{g}_9 \cdots \boldsymbol{g}_1] \begin{pmatrix} 4 \\ 3 \\ 3 \\ 3 \\ 1 \\ 3 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

as expected.

6. Primary one-point algebraic geometric codes

In this section we are concerned with primary one-point algebraic geometric codes and their improvements. We shall describe in detail the connection between the order bound (Section 5) for such codes and an almost similar bound in [30].

Following [30] let

$$\{\beta(1), \ldots, \beta(n)\} = \{m \mid C_\Omega(D, mQ) \neq C_\Omega(D, (m+1)Q)\}$$

with $\beta(1) > \cdots > \beta(n)$ and choose $\omega_i \in \Omega(\beta(i)Q - D)$ such that $\nu_Q(\omega_i) = \beta(i)$, $i = 1, \ldots, n$. Let

$$\{\alpha(1), \ldots, \alpha(n)\} = \{m \mid C_{\mathcal{L}}(D, mQ) \neq C_{\mathcal{L}}(D, (m-1)Q)\}$$

with $\alpha(1) < \cdots < \alpha(n)$ and choose $f_i \in \mathcal{L}(\alpha(i)Q)\backslash\mathcal{L}((\alpha(i)-1)Q)$, $i = 1, \ldots, n$. This is consistent with the notation in Definition 12. We define

$$\boldsymbol{h}_i = (\mathrm{res}_{P_1}(\omega_i), \ldots, \mathrm{res}_{P_n}(\omega_i))$$

and $\mathcal{H} = \{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_n\}$. Similarly we define

$$\boldsymbol{g}_i = (f_i(P_1), \ldots, f_i(P_n))$$

and $\mathcal{G} = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n\}$. In this section we shall always assume that $\mathcal{H}$ and $\mathcal{G}$ are chosen as above. A standard result tells us that

$$C_{\mathcal{L}}(D, mQ) = C_\Omega(D, mQ)^\perp = C(\mathcal{G}, \overline{I}) = C^\perp(\mathcal{H}, I), \tag{22}$$

where $I = \{1, \ldots, n-k\}$ and $\overline{I} = \{1, \ldots, k\}$, for some k. Matsumoto and Miura showed how to derive information on WB pairs with respect to $(\mathcal{H}, \mathcal{G})$.

Proposition 16. *Let $(\mathcal{H}, \mathcal{G})$ be as above. If $\beta(i) - \alpha(j) = \beta(k)$ then (i, j) is WB with respect to $(\mathcal{H}, \mathcal{G})$ and $\bar{\rho}_{\mathcal{H}}(\boldsymbol{h}_i * \boldsymbol{g}_j) = k$.* □

We now derive an alternative formulation:

Proposition 17. *Let $(\mathcal{H}, \mathcal{G})$ be as above. If $\alpha(i) + \alpha(j) = \alpha(k)$ then $(n - k + 1, j)$ is WB with respect to $(\mathcal{H}, \mathcal{G})$ and $\bar{\rho}_{\mathcal{H}}(\boldsymbol{h}_{n-k+1} * \boldsymbol{g}_j) = n - i + 1$.*

Proof. We first observe that $\beta(i) = \alpha(n - i + 1) - 1$ holds. Rearranging the condition in Proposition 16 and substituting $i' = n - k + 1$ and $k' = n - i + 1$ we arrive at the proposition, except we have i' and k' where the proposition has i and k. □

Proposition 17 suggests the following equivalent formulation of Matsumoto and Miura's bound on codes from algebraic function fields of transcendence degree one [30, Secs. 3 & 4]. Observe that differentials and residues are completely removed from the proof, while such removal had been completely unimaginable to the second author.

Proposition 18. *Let $(\mathcal{H}, \mathcal{G})$ be as above, and I an arbitrarily chosen subset of $\{1, \ldots, n\}$. The minimum distance of $C^{\perp}(\mathcal{H}, I)$ is at least*

$$\min\{\sigma(\alpha(i)) \mid i \in \bar{I}\},$$

where σ is as in Definition 14. In particular the minimum distance of the one-point algebraic geometric code in (22) is at least

$$\min\{\sigma(\alpha(i)) \mid i = 1, \ldots, k\}.$$

Proof. Observe that

$$i \in \bar{I} \Leftrightarrow n - i + 1 \in \{1, \ldots, n\} \backslash I.$$

We now apply Proposition 17 and (2). □

Proposition 18 and Theorem 15 produce the same bound for the codes in (22). Note that $(\mathcal{H}, \mathcal{G})$ satisfies the condition in (18), but in general not the condition in (5). Therefore by Remark 8, $C(\mathcal{G}, \bar{I})$ is not always equal to $C^{\perp}(\mathcal{H}, I)$. However, the order bound (Theorem 15) for primary codes and Proposition 18 produce the same estimates on the minimum distances of the two codes, and their dimensions are the same.

7. Estimation of generalized Hamming weights

As explained in Section 3 the correspondences in Lemma 5 and 6 imply that the Feng-Rao estimates for the minimum distances of $C(\mathcal{G}, I)$ and $C^{\perp}(\mathcal{H}, \bar{I})$ are the same (although as demonstrated in Section 4, they may be easier to derive from one of the code descriptions than the other). This is Theorem 7. A similar result holds regarding generalized Hamming weights which will be clear once we have stated the Feng-Rao bounds for these parameters. Recall that the support of a set $S \subseteq \mathbb{F}_q^n$ 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

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

Clearly $d_1(C)$ is just the well-known minimum distance. To introduce the Feng-Rao bounds we will need the following two definitions. The latter is a slight modification of [23, Def. 6].

Definition 19. Given bases $\mathcal{B}, \mathcal{U}$ consider for $l = 1, 2, \ldots, n$ the following sets

$$\begin{aligned}
\mathrm{V}^{\mathrm{WB}}_{(\mathcal{B},\mathcal{U})}(l) &= \{i \in \{1, \ldots, n\} \mid \bar{\rho}_{\mathcal{B}}(\boldsymbol{b}_i * \boldsymbol{u}_j) = l \text{ for some } \boldsymbol{u}_j \in \mathcal{U} \text{ with } (i, j) \text{ WB }\},\\
\Lambda^{\mathrm{WB}}_{(\mathcal{B},\mathcal{U})}(i) &= \{l \in \{1, \ldots, n\} \mid \bar{\rho}_{\mathcal{B}}(\boldsymbol{b}_i * \boldsymbol{u}_j) = l \text{ for some } \boldsymbol{u}_j \in \mathcal{U} \text{ with } (i, j) \text{ WB}\}.
\end{aligned}$$

Definition 20. For $1 \leq l_1 < \cdots < l_t \leq n$ define

$$\bar{\mu}^{\mathrm{WB}}_{(\mathcal{B},\mathcal{U})}(l_1, \ldots l_t) = \sharp\left(\cup_{s=1,\ldots,t} \mathrm{V}^{\mathrm{WB}}_{(\mathcal{B},\mathcal{U})}(l_s)\right)$$

and for $1 \leq i_1 < \cdots < i_t \leq n$ define

$$\bar{\sigma}^{\mathrm{WB}}_{(\mathcal{B},\mathcal{U})}(i_1, \ldots, i_t) = \sharp\left(\cup_{s=1,\ldots,t} \Lambda^{\mathrm{WB}}_{(\mathcal{B},\mathcal{U})}(i_s)\right).$$

$\mathrm{V}^{\mathrm{OWB}}_{(\mathcal{B},\mathcal{U})}$, $\Lambda^{\mathrm{OWB}}_{(\mathcal{B},\mathcal{U})}$, $\bar{\mu}^{\mathrm{WWB}}_{(\mathcal{B},\mathcal{U})}$ and $\bar{\sigma}^{\mathrm{WWB}}_{(\mathcal{B},\mathcal{U})}$ are defined similarly, but with WB replaced with OWB. The Feng-Rao bounds for generalized Hamming weights are as follows:

Theorem 21. *Let I be fixed.*
For $1 \leq t \leq n - \sharp I$ we have

$$\begin{aligned}
&d_t(C^{\perp}(\mathcal{B}, I))\\
&\quad \geq \min\{\bar{\mu}^{OWB}_{(\mathcal{B},\mathcal{U})}(l_1, \ldots, l_t) \mid 1 \leq l_1 < \cdots < l_t \leq n \text{ and } l_1, \ldots, l_t \notin I\}\\
&\quad \geq \min\{\bar{\mu}^{WB}_{(\mathcal{B},\mathcal{U})}(l_1, \ldots, l_t) \mid 1 \leq l_1 < \cdots < l_t \leq n \text{ and } l_1, \ldots, l_t \notin I\}.
\end{aligned}$$

For $1 \leq t \leq \sharp I$ *we have*

$$d_t(C(\mathcal{B}, I))$$
$$\geq \min\{\overline{\sigma}^{OWB}_{(\mathcal{B},\mathcal{U})}(i_1, \ldots, i_t) \mid 1 \leq i_1 < \cdots < i_t \leq n \text{ and } i_1, \ldots, i_t \in I\}\}$$
$$\geq \min\{\overline{\sigma}^{WB}_{(\mathcal{B},\mathcal{U})}(i_1, \ldots, i_t) \mid 1 \leq i_1 < \cdots < i_t \leq n \text{ and } i_1, \ldots, i_t \in I\}\}.$$

Proof. See [25, Th. 3.14] and [23, Th. 1]. □

Applying Lemma 5 and 6 we get:

Theorem 22. *Assume* $\mathcal{G}, \mathcal{H}$ *satisfy condition (5) and that* $\mathcal{U}$ *is any basis. Let a non-empty set* $I \subseteq \{1, 2, \ldots, n\}$ *be given. Then* $C(\mathcal{G}, I) = C^{\perp}(\mathcal{H}, \overline{I})$ *and for* $t \leq \sharp I$ *we have*

$$\min\{\overline{\mu}^{OWB}_{(\mathcal{H},\mathcal{U})}(l_1, \ldots, l_t) \mid 1 \leq l_1 < \cdots < l_t \leq n \;\text{ and }\; l_1, \ldots, l_t \notin \overline{I}\}$$
$$= \min\{\overline{\sigma}^{OWB}_{(\mathcal{G},\mathcal{U})}(i_1, \ldots, i_t) \mid 1 \leq i_1 < \cdots < i_t \leq n \;\text{ and }\; i_1, \ldots, i_t \in I\},$$

$$\min\{\overline{\mu}^{WB}_{(\mathcal{H},\mathcal{U})}(l_1, \ldots, l_t) \mid 1 \leq l_1 < \cdots < l_t \leq n \;\text{ and }\; l_1, \ldots, l_t \notin \overline{I}\}$$
$$= \min\{\overline{\sigma}^{WB}_{(\mathcal{G},\mathcal{U})}(i_1, \ldots, i_t) \mid 1 \leq i_1 < \cdots < i_t \leq n \;\text{ and }\; i_1, \ldots, i_t \in I\}.$$

□

In other words, also in the setting of generalized Hamming weights the Feng-Rao bound for primary codes and the Feng-Rao bound for dual codes are consequences of each other.

Acknowledgments

The present work was done while Ryutaroh Matsumoto was visiting Aalborg University as a Velux Visiting Professor supported by the Villum Foundation. The authors gratefully acknowledge this support. The authors also gratefully acknowledge the support from the Danish National Research Foundation and the National Science Foundation of China (Grant No. 11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography. Furthermore the authors are thankful for the support from Spanish grant MTM2007-64704, the Spanish MINECO grant No. MTM2012-36917-C03-03, and for the MEXT Grant-in-Aid for Scientific Research (A) No. 23246071.

[1] H.E. Andersen, O. Geil, Evaluation codes from order domain theory, Finite Fields Appl. 14 (2008) 92–123. doi:10.1016/j.ffa.2006.12.004.
[2] P. Beelen, The order bound for general algebraic geometric codes, Finite Fields Appl. 13 (2007) 665–680. doi:10.1016/j.ffa.2006.09.006.
[3] P. Beelen, T. Høholdt, The decoding of algebraic geometry codes, in: E. Martínez-Moro, C. Munuera, D. Ruano (Eds.), Advances in algebraic geometry codes, volume 5 of *Coding Theory and Cryptology*, World Scientific, Singapore, 2008, pp. 49–98. doi:10.1142/9789812794017_0002.
[4] I.M. Duursma, Decoding codes from curves and cyclic codes, Ph.D. thesis, Eindhoven University of Technology, 1993. URL: http://www.math.uiuc.edu/~duursma/pub/frame.pdf.
[5] I.M. Duursma, Majority coset decoding, IEEE Trans. Inform. Theory 39 (1993) 1067–1070. doi:10.1109/18.256518.
[6] I.M. Duursma, On erasure decoding of AG-codes, in: Proc. 1994 IEEE Information Theory Workshop, Moscow, Russia, 1994. URL: http://www.math.uiuc.edu/~duursma/pub/Erasure94.pdf.
[7] I.M. Duursma, R. Kirov, An extension of the order bound for AG codes, in: M. Bras-Amorós, T. Høholdt (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, volume 5527 of *Lecture Notes in Computer Science*, Springer, 2009, pp. 11–22. doi:10.1007/978-3-642-02181-7_2.
[8] I.M. Duursma, R. Kirov, S. Park, Distance bounds for algebraic geometric codes, J. Pure Appl. Algebra 215 (2011) 1863–1878. doi:10.1016/j.jpaa.2010.10.018.
[9] G.L. Feng, T.R.N. Rao, Decoding algebraic-geometric codes up to the designed minimum distance, IEEE Trans. Inform. Theory 39 (1993) 37–45. doi:10.1109/18.179340.
[10] G.L. Feng, T.R.N. Rao, A simple approach for construction of algebraic-geometric codes from affine plane curves, IEEE Trans. Inform. Theory 40 (1994) 1003–1012. doi:10.1109/18.335972.
[11] G.L. Feng, T.R.N. Rao, Improved geometric Goppa codes part I: Basic theory, IEEE Trans. Inform. Theory 41 (1995) 1678–1693. doi:10.1109/18.476241.
[12] J. Fitzgerald, R.F. Lax, Decoding affine variety codes using Gröbner bases, Des. Codes Cryptogr. 13 (1998) 147–158. doi:10.1023/A:1008274212057.
[13] C. Galindo, F. Monserrat, δ-sequences and evaluation codes defined by plane valuations at infinity, Proc. Lond. Math. Soc. (3) 98 (2009) 714–740. doi:10.1112/plms/pdn042.
[14] C. Galindo, F. Monserrat, Evaluation codes defined by finite families of plane valuations at infinity, Des. Codes Cryptogr. (2012) 1–25. doi:10.1007/s10623-012-9738-7.
[15] C. Galindo, M. Sanchis, Evaluation codes and plane valuations, Des. Codes Cryptogr. 41 (2006) 199–219. doi:10.1007/s10623-006-9011-z.
[16] O. Geil, On codes from norm-trace curves, Finite Fields Appl. 9 (2003) 351–371. doi:10.1016/S1071-5797(03)00010-8.
[17] O. Geil, Evaluation codes from an affine variety code perspective, in: E. Martínez-Moro, C. Munuera, D. Ruano (Eds.), Advances in algebraic geometry codes, volume 5 of *Coding Theory and Cryptology*, World Scientific, Singapore, 2008, pp. 153–180. doi:10.1142/9789812794017_0004.
[18] O. Geil, T. Høholdt, On hyperbolic codes, in: S. Boztaş, I.E. Shparlinski (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, volume 2227 of *Lecture Notes in Computer Science*, Springer, 2001, pp. 159–171. doi:10.1007/3-540-45624-4_17.

[19] O. Geil, R. Matsumoto, D. Ruano, List decoding algorithm based on voting in Gröbner bases for general one-point AG codes, 2012. arXiv:1203.6127v4.

[20] O. Geil, R. Matsumoto, D. Ruano, List decoding algorithms based on Gröbner bases for general one-point AG codes, in: Proc. 2012 IEEE International Symposium on Information Theory, Cambridge, MA, USA, 2012, pp. 86–90. doi:10.1109/ISIT.2012.6284685.

[21] O. Geil, C. Munuera, D. Ruano, F. Torres, On the order bounds for one-point AG codes, Adv. Math. Commun. 5 (2011) 489–504. doi:10.3934/amc.2011.5.489.

[22] O. Geil, R. Pellikaan, On the structure of order domains, Finite Fields Appl. 8 (2002) 369–396. doi:10.1006/ffta.2001.0347.

[23] O. Geil, C. Thommesen, On the Feng-Rao bound for generalized Hamming weights, in: M.P. Fossorier, H. Imai, S. Lin, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, volume 3857 of *Lecture Notes in Computer Science*, Springer, 2006, pp. 295–306. doi:10.1007/11617983_29.

[24] O. Geil, C. Thomsen, Weighted Reed–Muller codes revisited, Des. Codes Cryptogr. (2012) 1–26. doi:10.1007/s10623-012-9680-8.

[25] P. Heijnen, R. Pellikaan, Generalized Hamming weights of q-ary Reed-Muller codes, IEEE Trans. Inform. Theory 44 (1998) 181–196. doi:10.1109/18.651015.

[26] T. Høholdt, J.H. van Lint, R. Pellikaan, Algebraic geometry codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, volume 1, Elsevier, Amsterdam, 1998, pp. 871–961.

[27] K. Lee, Unique decoding of plane AG codes revisited, 2012. arXiv:1204.0052v2.

[28] K. Lee, M. Bras-Amorós, M.E. O'Sullivan, Unique decoding of plane AG codes via interpolation, IEEE Trans. Inform. Theory 58 (2012) 3941–3950. doi:10.1109/TIT.2012.2182757.

[29] J.B. Little, The ubiquity of order domains for the construction of error control codes, Adv. Math. Commun. 1 (2007) 151–171. doi:10.3934/amc.2007.1.151.

[30] R. Matsumoto, S. Miura, On the Feng-Rao bound for the $\mathcal{L}$-construction of algebraic geometry codes, IEICE Trans. Fundamentals E83-A (2000) 926–930. URL: http://www.rmatsumoto.org/repository/e83-a_5_923.pdf.

[31] S. Miura, Study of Error-Correcting Codes based on Algebraic Geometry, Ph.D. thesis, Univ. Tokyo, 1997. (in Japanese).

[32] S. Miura, Linear codes on affine algebraic varieties, IEICE Trans. Fundamentals (Japanese Edition) J81-A (1998) 1386–1397. (in Japanese).

[33] M.E. O'Sullivan, New codes for the Berlekamp-Massey-Sakata algorithm, Finite Fields Appl. 7 (2001) 293–317. doi:10.1006/ffta.2000.0283.

[34] R. Pellikaan, On the efficient decoding of algebraic-geometric codes, in: P. Camion, P. Charpin, S. Harari (Eds.), Eurocode '92 International Symposium on Coding Theory and Applications, number 339 in CISM Courses and Lectures, CISM International Centre for Mechanical Sciences, Springer, 1993, pp. 231–253. URL: http://www.win.tue.nl/~ruudp/paper/17.pdf.

[35] T. Shibuya, K. Sakaniwa, A dual of well-behaving type designed minimum distance, IEICE Trans. Fundamentals E84-A (2001) 647–652. URL: http://www.ts-lab.net/members/tshibuya/pdf/e84-a_2_647.pdf.