Improved power decoding of interleaved one-point Hermitian codes

Puchinger, Sven; Rosenkilde, Johan; Bouw, Irene

Published in:
Designs, Codes, and Cryptography

Link to article, DOI:
10.1007/s10623-018-0577-z

Publication date:
2019

Document Version
Peer reviewed version

Noname manuscript No.
(will be inserted by the editor)

Improved Power Decoding of Interleaved One-Point Hermitian Codes

Sven Puchinger · Johan Rosenkilde · Irene Bouw

Received: date / Accepted: date

Abstract We propose a new partial decoding algorithm for h-interleaved one-point Hermitian codes that can decode—under certain assumptions—an error of relative weight up to $1-(\frac{k+g}{n})^{\frac{h}{h+1}}$, where k is the dimension, n the length, and g the genus of the code. Simulation results for various parameters indicate that the new decoder achieves this maximal decoding radius with high probability. The algorithm is based on a recent generalization of Rosenkilde's improved power decoder to interleaved Reed–Solomon codes, does not require an expensive root-finding step, and improves upon the previous best decoding radius by Kampf at all rates. In the special case $h=1$, we obtain an adaption of the improved power decoding algorithm to one-point Hermitian codes, which for all simulated parameters achieves a similar observed failure probability as the Guruswami–Sudan decoder above the latter's guaranteed decoding radius.

Keywords Interleaved One-Point Hermitian Codes · Power Decoding · Collaborative Decoding · 94B35 · 14G50

1 Introduction

One-point Hermitian (1-H) codes are algebraic geometry codes that can be decoded beyond half the minimum Goppa distance. Most of their decoders are conceptually similar to their Reed–Solomon (RS) code analogs, such as the *Guruswami–Sudan* (GS)

Sven Puchinger
Institute of Communications Engineering, Ulm University, Germany
E-mail: sven.puchinger@uni-ulm.de

Johan Rosenkilde
Department of Applied Mathematics and Computer Science, Technical University of Denmark
E-mail: jsrn@jsrn.dk

Irene Bouw
Institute of Pure Mathematics, Ulm University, Germany
E-mail: irene.bouw@uni-ulm.de

algorithm [1] and *power decoding* (PD) [2–4]. For both RS and 1-H codes, PD is only able to correct as many errors as the Sudan algorithm, which is a special case of the GS algorithm. Recently [5], PD for RS codes was improved to correct as many errors as the GS algorithm.

An h-interleaved 1-H code is a direct sum of h many 1-H codes. By assuming that errors occur at the same positions in the constituent codewords (burst errors), it is possible to decode far beyond half the minimum distance [6], which is inspired by decoding methods for interleaved RS codes [2,7]. In the RS case, there have been many improvements on the decoding radius in the last two decades [2,7–12], which have not all been adapted to 1-H codes. The currently best-known decoding radius for interleaved RS codes is achieved by both the interpolation-based technique in [8,10] and the method based on improved PD in [12], where the latter has a smaller complexity since it does not rely on an expensive root-finding step.

In this paper, we adapt the decoder in [12], which is based on improved PD, to h-interleaved 1-H codes using the description of PD for 1-H as in [4]. Similar to the RS case, we derive a larger system of non-linear key equations (cf. Section 3) and reduce the decoding problem to a linear problem whose solution—under certain assumptions—agrees with the solution of the system of key equations (cf. Section 4).

Using a linear-algebraic argument, we derive an upper bound on the maximum number of errors which can yield a unique solution of the linear problem (cf. Section 5). This decoding radius improves upon the previous best, [6], at all rates. In Section 6, we present simulation results for various code and decoder parameters which indicate that the new algorithm achieves the maximal decoding radius with high probability. The complexity of solving the linear problem is shown to be sub-quadratic in the code length in Section 7. Finally, we compare the decoding radii of RS, interleaved RS and interleaved 1-H codes for the same overall field size and length in Section 8.

In the special case $h = 1$, we obtain an 1-H analogue of the improved PD for RS codes [5]. This improves the decoding radius of the 1-H PD decoder of [4] at a similar cost, sub-quadratic in the code length, and similar to the best known cost of the 1-H GS algorithm [4]. Simulation results suggest that the decoder has a similar failure probability as the GS algorithm for the same parameters when the decoding radius is beyond the guaranteed radius of the GS algorithm (cf. Section 6).

The decoder is described for codes of full length $n = q^3$; the approach works for any $n < q^3$, but to obtain the good complexities, certain restrictions to how the evaluation points are chosen should be kept. For notational convenience, we restrict ourselves to homogeneous interleaved 1-H codes, i.e., where the constituent codes have the same rate. The generalization to inhomogeneous codes is straightforward.

The results of this article were partly presented at the International Workshop on Coding and Cryptography, Saint-Petersburg, Russia, 2017, where we only considered the case $h = 1$ [13]. While writing this extension, we discovered some slightly improved key equations, which are presented here. In the previous paper we sought Λ^s where Λ is a usual notion of error-locator; now we instead define and seek Λ_s, which is an "error-locator of multiplicity s".

2 Preliminaries

Let q be a prime power. We follow the notation of [4]. The *Hermitian curve* $\mathcal{H}/\mathbb{F}_{q^2}$ is the smooth projective plane curve defined by the affine equation $Y^q + Y = X^{q+1}$. The curve $\mathcal{H}(\mathbb{F}_{q^2})$ has genus $g = \frac{1}{2}q(q-1)$ and q^3+1 many $\mathbb{F}_{q^2}$-rational points $\mathcal{P} = \{P_1, \ldots, P_{q^3}, P_\infty\}$, where P_∞ denotes the point at infinity. We define $\mathcal{R} := \cup_{m_\mathrm{H} \geq 0} \mathcal{L}(m_\mathrm{H} P_\infty) = \mathbb{F}_{q^2}[X,Y]/(Y^q + Y - X^{q+1})$, which has an $\mathbb{F}_{q^2}$-basis of the form $\{X^i Y^j : 0 \leq i, 0 \leq j < q\}$. The order function $\deg_\mathcal{H} : \mathcal{R} \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}, f \mapsto -v_{P_\infty}(f)$ is defined by the valuation v_{P_∞} at P_∞. As a result, we have $\deg_\mathcal{H}(X^i Y^j) = iq + j(q+1)$. We will think often operate with elements of $\mathcal{R}$ as bivariate polynomials in X and Y, represented as $\mathbb{F}_{q^2}$-linear combinations of the aforementioned basis. In this paper, when we say "degree" of an element in $\mathcal{R}$, we mean its $\deg_\mathcal{H}$. A non-zero element of $\mathcal{R}$ is called monic if its monomial of largest $\deg_\mathcal{H}$ has coefficient 1.

Let $n = q^3$ and $m_\mathrm{H} \in \mathbb{N}$ with $2(g-1) < m_\mathrm{H} < n$. The *one-point Hermitian code* of length n and parameter m_H over $\mathbb{F}_{q^2}$ is defined by

$$\mathcal{C}_\mathcal{H}(n, m_\mathrm{H}) = \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(m_\mathrm{H} P_\infty)\}.$$

The dimension of $\mathcal{C}_\mathcal{H}$ is given by $k = m_\mathrm{H} - g + 1$ and the minimum distance d is lower-bounded by the *designed minimum distance* $d^* := n - m_\mathrm{H}$.

The *(homogeneous) h-interleaved one-point Hermitian code* of length n and parameter m_H over $\mathbb{F}_{q^2}$ is the direct sum of h one-point Hermitian codes $\mathcal{C}_\mathcal{H}(n, m_\mathrm{H})$, i.e.,

$$\mathcal{C}_\mathcal{H}(n, m_\mathrm{H}; h) = \left\{ \begin{bmatrix} \boldsymbol{c}_1 \\ \vdots \\ \boldsymbol{c}_h \end{bmatrix} \in \mathbb{F}_{q^2}^{h \times n} \,:\, \boldsymbol{c}_i \in \mathcal{C}_\mathcal{H}(n, m_\mathrm{H}) \right\}.$$

As a metric for errors, we consider *burst errors*: If $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e} \in \mathbb{F}_{q^2}^{h \times n}$ is received for a codeword $\boldsymbol{c} \in \mathcal{C}_\mathcal{H}(n, m_\mathrm{H}; h)$, then the *error positions* $\mathcal{E} \subseteq \{1, \ldots, n\}$ are given by the non-zero columns of $\boldsymbol{e}$, i.e.,

$$\mathcal{E} := \bigcup_{j=1}^h \left\{ i \,:\, e_{j,i} \neq 0 \right\}.$$

For a vector $\boldsymbol{i} = [i_1, \ldots, i_m] \in \mathbb{Z}_{\geq 0}^h$, we define its *size* as $|\boldsymbol{i}| := \sum_\mu i_\mu$. We denote by $\preceq$ the product partial order on $\mathbb{Z}_{\geq 0}^h$, i.e. $\boldsymbol{i} \preceq \boldsymbol{j}$ if $i_\mu \leq j_\mu$ for all μ. The number of vectors $\in \mathbb{Z}_{\geq 0}^m$ of size $|\boldsymbol{i}| = \mu$ is given by $\binom{h+\mu-1}{\mu}$. We use the following relations, which follow from properties of the binomial coefficient.

Lemma 1 *Let $m, t \in \mathbb{Z}_{>0}$. Then,*

$$\textstyle\sum_{\mu=0}^t \binom{m+\mu-1}{\mu} = \binom{m+t}{m}, \text{ and } \sum_{\mu=0}^{t-1} \mu \binom{m+\mu-1}{\mu} = t\binom{m+t-1}{m+1}.$$

Note that the Lemma 1 means e.g.

$$\sum_{\boldsymbol{i} \in \mathbb{Z}_{\geq 0}^h, |\boldsymbol{i}| < t} |\boldsymbol{i}| = t\binom{h+t-1}{h+1}.$$

We also introduce the following notational short-hands:

Definition 1 For $\boldsymbol{a} \in \mathcal{R}^h$, and $\boldsymbol{i}, \boldsymbol{j} \in \mathbb{Z}_{\geq 0}^h$, we define

$$\boldsymbol{a}^{\boldsymbol{i}} := \prod_{\mu=1}^{h} a_\mu^{i_\mu}, \quad \binom{\boldsymbol{j}}{\boldsymbol{i}} := \prod_{\mu=1}^{m} \binom{j_\mu}{i_\mu}.$$

By extending the binomial theorem to this notation, we obtain the following lemma.

Lemma 2 *Let $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{R}^h$, and $\boldsymbol{j} \in \mathbb{Z}_{\geq 0}^m$. Then,*

$$(\boldsymbol{a} + \boldsymbol{b})^{\boldsymbol{j}} = \sum_{\boldsymbol{i} \preceq \boldsymbol{j}} \binom{\boldsymbol{j}}{\boldsymbol{i}} \boldsymbol{a}^{\boldsymbol{i}} \boldsymbol{b}^{\boldsymbol{j}-\boldsymbol{i}}.$$

For computational complexities, we use the soft-O notation $O^\sim$, which omits log factors.

3 System of Key Equations

In this section, we derive the system of key equations that we need for decoding, using the same trick as [12] for interleaved Reed–Solomon codes. We use the description of power decoding for one-point Hermitian codes as in [4]. Suppose that the received word is $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e} \in \mathbb{F}_{q^2}^{h \times n}$, consisting of an error $\boldsymbol{e}$ with corresponding (burst) error positions $\mathcal{E}$ and a codeword $\boldsymbol{c} \in \mathcal{C}_{\mathcal{H}}(n, m_{\mathrm{H}}; h)$, which is obtained from the *message polynomials* $\boldsymbol{f} = [f_1, \ldots, f_h] \in \mathcal{L}(mP_\infty)^h$.

In the following sections we show how to retrieve the message polynomials $\boldsymbol{f}$ from the received word $\boldsymbol{r}$ if the *number of errors* $|\mathcal{E}|$ does not exceed a certain decoding radius, which depends on the parameters of the decoding algorithm. Similar to [4], we define the following polynomials.

Definition 2 Let $s \in \mathbb{N}$. The *error locator polynomial Λ_s of multiplicity s* is the element in $\mathcal{L}\left(-\sum_{i \in \mathcal{E}} sP_i + \infty P_\infty\right)$ of minimal degree that is monic.

Theorem 1 *The error locator polynomial of multiplicity s is unique and has degree*

$$s|\mathcal{E}| \leq \deg_{\mathcal{H}} \Lambda_s \leq s|\mathcal{E}| + g.$$

Proof: The proof is similar to [4, Lemma 23]. Uniqueness is clear since if there were two such polynomials, their difference would also be in $\mathcal{L}\left(-\sum_{i \in \mathcal{E}} sP_i + \infty P_\infty\right)$, but of smaller $\deg_{\mathcal{H}}$. Being in $\mathcal{L}\left(-\sum_{i \in \mathcal{E}} sP_i + \infty P_\infty\right)$ specifies $s|\mathcal{E}|$ homogeneous linear equations in the coefficients of Λ_s, since for any $i \in \mathcal{E}$, we can expand Λ_s into a power series $\sum_{j \geq s} \gamma_{i,j} \phi_i^j$ for a local parameter ϕ_i of P_i (e.g., take $\phi_i = X - \alpha_i$ if $P_i = (\alpha_i, \beta_i)$). By requiring $\deg_{\mathcal{H}} \Lambda_s \leq s|\mathcal{E}| + g$, we have more variables than equations, so there is a non-zero Λ_s of the sought form with degree at most $s|\mathcal{E}| + g$. The lower bound works exactly as in [4, Lemma 23]. ∎

Lemma 3 *For each $i = 1, \ldots, h$, there is a polynomial $R_i \in \mathcal{R}$ with $\deg_{\mathcal{H}}(R_i) < n + 2g$ that satisfies $R(P_j) = r_{i,j}$ for all $P_j \in \mathcal{P}^*$. Each R_i can be computed in $O^\sim(n)$ operations over $\mathbb{F}_{q^2}$.*

Proof: Apply [4, Lemma 6] to each row of the received word. ■

In the following, let $\boldsymbol{R} = [R_1, \ldots, R_h] \in \mathcal{R}^h$ be as in Lemma 3 and $G \in \mathcal{R}$ be defined as

$$G = \prod_{\alpha \in \mathbb{F}_{q^2}} (X - \alpha) = X^{q^2} - X.$$

Lemma 4 *For each $\boldsymbol{i} \in \mathbb{Z}_{\geq 0}$ with $|\boldsymbol{i}| \leq s$, there is a unique $\Omega_{s,\boldsymbol{i}} \in \mathcal{R}$ of degree $\deg_{\mathcal{H}} \Omega_{s,\boldsymbol{i}} \leq \deg_{\mathcal{H}} \Lambda_s + |\boldsymbol{i}|(2g-1)$ such that*

$$\Lambda_s(\boldsymbol{f} - \boldsymbol{R})^{\boldsymbol{i}} = G^{|\boldsymbol{i}|} \Omega_{s,\boldsymbol{i}}.$$

Proof: Consider $v_{P_j}(\Lambda_s(\boldsymbol{f} - \boldsymbol{R})^{\boldsymbol{i}})$ for $j = 1, \ldots, n$: if $j \in \mathcal{E}$ then $v_{P_j}(\Lambda_s(\boldsymbol{f} - \boldsymbol{R})^{\boldsymbol{i}}) = v_{P_j}(\Lambda_s) \geq s \geq |\boldsymbol{i}|$. If $j \notin \mathcal{E}$ then $v_{P_j}(\Lambda_s(\boldsymbol{f} - \boldsymbol{R})^{\boldsymbol{i}}) \geq v_{P_j}((\boldsymbol{f} - \boldsymbol{R})^{\boldsymbol{i}}) \geq |\boldsymbol{i}|$. We conclude

$$\Lambda_s(\boldsymbol{f} - \boldsymbol{R})^{\boldsymbol{i}} \in \mathcal{L}\Big(- |\boldsymbol{i}| \sum_{j=1}^{n} P_j + \infty P_\infty \Big).$$

Since the divisor in that $\mathcal{L}$-space is exactly $\operatorname{div}(G^{|\boldsymbol{i}|}) + \infty P_\infty$, then $\Lambda_s(\boldsymbol{f} - \boldsymbol{R})^{\boldsymbol{i}}$ must be divisible by $G^{|\boldsymbol{i}|}$ (see e.g., [4, Lemma 3]) with quotient in $\mathcal{R}$. The degree is given by taking $\deg_{\mathcal{H}}$ on both sides and using $\deg_{\mathcal{H}}(R_i) < n + 2g - 1$. ■

The following theorem states the system of key equations that we will use for decoding in the next sections. Note that the formulation is similar to its interleaved Reed–Solomon analog [12], with the difference that all involved polynomials are elements of the ring $\mathcal{R}$.

Theorem 2 (System of Key Equations) *Let $\ell, s \in \mathbb{Z}_{>0}$ be such that $s \leq \ell$ and Λ_s, $\boldsymbol{f}$, $\boldsymbol{R}$, G, and $\Omega_{s,\boldsymbol{i}}$ as above. Then, for all $\boldsymbol{j} \in \mathbb{Z}_{\geq 0}^h$ of size $1 \leq |\boldsymbol{j}| \leq \ell$, we have*

$$\Lambda_s \boldsymbol{f}^{\boldsymbol{j}} = \sum_{\boldsymbol{i} \preceq \boldsymbol{j}} \Omega_{s,\boldsymbol{i}} \left[\binom{\boldsymbol{j}}{\boldsymbol{i}} \boldsymbol{R}^{\boldsymbol{j}-\boldsymbol{i}} G^{|\boldsymbol{i}|} \right], \qquad 1 \leq |\boldsymbol{j}| < s \tag{1}$$

$$\Lambda_s \boldsymbol{f}^{\boldsymbol{j}} \equiv \sum_{\substack{\boldsymbol{i} \preceq \boldsymbol{j} \\ |\boldsymbol{i}| < s}} \Omega_{s,\boldsymbol{i}} \left[\binom{\boldsymbol{j}}{\boldsymbol{i}} \boldsymbol{R}^{\boldsymbol{j}-\boldsymbol{i}} G^{|\boldsymbol{i}|} \right] \mod G^s, \qquad s \leq |\boldsymbol{j}| \leq \ell, \tag{2}$$

as congruences over $\mathcal{R}$.

Proof: Using Lemma 2, we obtain

$$\Lambda_s \boldsymbol{f}^{\boldsymbol{j}} = \Lambda_s \left(\boldsymbol{R} + (\boldsymbol{f} - \boldsymbol{R}) \right)^{\boldsymbol{j}} = \textstyle\sum_{\boldsymbol{i} \preceq \boldsymbol{j}} \binom{\boldsymbol{j}}{\boldsymbol{i}} \Lambda_s \left(\boldsymbol{f} - \boldsymbol{R} \right)^{\boldsymbol{i}} \boldsymbol{R}^{\boldsymbol{j}-\boldsymbol{i}}. \tag{3}$$

In all summands with $|\boldsymbol{i}| < s$, we can rewrite, using Lemma 4,

$$\Lambda_s \left(\boldsymbol{f} - \boldsymbol{R} \right)^{\boldsymbol{i}} = G^{|\boldsymbol{i}|} \Omega_{s,\boldsymbol{i}}. \tag{4}$$

If $|\boldsymbol{i}| \geq s$, we can write $\boldsymbol{i} = \boldsymbol{i}' + \boldsymbol{i}''$, for some $\boldsymbol{i}', \boldsymbol{i}'' \in \mathbb{Z}_{\geq 0}$ with $|\boldsymbol{i}'| = s$, and

$$\Lambda_s \left(\boldsymbol{f} - \boldsymbol{R} \right)^{\boldsymbol{i}} = \Lambda_s (\boldsymbol{f} - \boldsymbol{R})^{\boldsymbol{i}'} (\boldsymbol{f} - \boldsymbol{R})^{\boldsymbol{i}''} = G^s \Omega_{s,\boldsymbol{i}'} (\boldsymbol{f} - \boldsymbol{R})^{\boldsymbol{i}''},$$

so all those terms are divisible by G^s. For $|\boldsymbol{j}| < s$, all summands of (3) have $|\boldsymbol{i}| \leq |\boldsymbol{j}| < s$ and are of the form (4). We therefore obtain (1). For $|\boldsymbol{j}| \geq s$, all summands of (3) with $|\boldsymbol{i}| \geq s$ are divisible by G^s, so we get (2). ■

4 Solving the System of Key Equations

The key equations in Theorem 2 are non-linear relations between the unknown polynomials Λ_s, $\boldsymbol{f}$, and $\boldsymbol{\Omega}$. We therefore relax them into—at the first glance much weaker—linear problem and hope that their solutions agree. The resulting problem is a heavy generalisation of multi-sequence linear shift register synthesis [14, 15], which is very related to simultaneous Hermite Padé approximations [16].

Problem 1 Consider a code $\mathcal{C} = \mathcal{C}_{\mathcal{H}}(n, m_{\mathrm{H}}; h)$ and a decoding instance with received word $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e} \in \mathbb{F}_{q^2}^{h\times n}$, where $\boldsymbol{c} \in \mathcal{C}$ is unknown and is obtained from the unknown message polynomials $\boldsymbol{f} \in \mathcal{L}(mP_\infty)^h$. Let $\boldsymbol{R}$ and G be as in Section 3. Given positive integers $s \le \ell$, let

$$A_{\boldsymbol{i},\boldsymbol{j}} = \tbinom{\boldsymbol{j}}{\boldsymbol{i}} \boldsymbol{R}^{\boldsymbol{j}-\boldsymbol{i}} G^{|\boldsymbol{i}|} \in \mathcal{R}$$

for all $\boldsymbol{i} \in \mathcal{I} := \{\boldsymbol{i} \in \mathbb{N}_0^h : 0 \le |\boldsymbol{i}| < s\}$ and $\boldsymbol{j} \in \mathcal{J} := \{\boldsymbol{j} \in \mathbb{N}_0^h : 1 \le |\boldsymbol{j}| \le \ell\}$. Find $\lambda_{\boldsymbol{i}}, \psi_{\boldsymbol{j}} \in \mathcal{R}$ for $\boldsymbol{i} \in \mathcal{I}$ and $\boldsymbol{j} \in \mathcal{J}$ with monic $\lambda_{\boldsymbol{0}}$, such that

$$\psi_{\boldsymbol{j}} = \sum_{\boldsymbol{i}\in\mathcal{I}} \lambda_{\boldsymbol{i}} A_{\boldsymbol{i},\boldsymbol{j}} \qquad \boldsymbol{j} \in \mathcal{J} \text{ and } |\boldsymbol{j}| < s, \tag{5}$$

$$\psi_{\boldsymbol{j}} \equiv \sum_{\boldsymbol{i}\in\mathcal{I}} \lambda_{\boldsymbol{i}} A_{\boldsymbol{i},\boldsymbol{j}} \mod G^s \qquad \boldsymbol{j} \in \mathcal{J} \text{ and } |\boldsymbol{j}| \ge s, \tag{6}$$

$$\deg_{\mathcal{H}} \lambda_{\boldsymbol{0}} \ge \deg_{\mathcal{H}} \lambda_{\boldsymbol{i}} - |\boldsymbol{i}|(2g-1) \qquad \boldsymbol{i} \in \mathcal{I}, \tag{7}$$

$$\deg_{\mathcal{H}} \lambda_{\boldsymbol{0}} \ge \deg_{\mathcal{H}} \psi_{\boldsymbol{j}} - |\boldsymbol{j}| m_{\mathrm{H}} \qquad \boldsymbol{j} \in \mathcal{J}. \tag{8}$$

Definition 3 Consider an instance of Problem 1. We say that a solution $(\lambda_{\boldsymbol{i}})_{i\in\mathcal{I}}, (\psi_{\boldsymbol{j}})_{\boldsymbol{j}\in\mathcal{J}}$, has *degree* $\tau \in \mathbb{Z}_{\ge 0}$ if $\deg_{\mathcal{H}} \lambda_{\boldsymbol{0}} = \tau$. Furthermore, we call a solution *minimal* if its degree is minimal among all solutions.

Problem 1 is connected to the key equations through the following statement.

Theorem 3 *Consider an instance of Problem 1. Then,*

$$\lambda_{\boldsymbol{i}} = \Lambda_{\boldsymbol{i}} := \Omega_{s,\boldsymbol{i}}, \qquad \boldsymbol{i} \in \mathcal{I},$$
$$\psi_{\boldsymbol{j}} = \Psi_{\boldsymbol{j}} := \Lambda_s \boldsymbol{f}^{\boldsymbol{j}}, \qquad \boldsymbol{j} \in \mathcal{J},$$

is a solution to the problem of degree $\tau = \deg_{\mathcal{H}} \Lambda_s$*, where* $s \cdot |\mathcal{E}| \le \tau \le s \cdot |\mathcal{E}| + g$.

Proof: Note $\Omega_{s,\boldsymbol{0}} = \Lambda_s$. The equalities and congruences are now clear from the key equations. As for the degree restrictions, we have

$$\deg_{\mathcal{H}} \Lambda_{\boldsymbol{i}} \le \deg_{\mathcal{H}} \Lambda_{\boldsymbol{0}} + |\boldsymbol{i}|(2g-1),$$
$$\deg_{\mathcal{H}} \Psi_{\boldsymbol{j}} = \deg_{\mathcal{H}}(\Lambda_s) + \deg_{\mathcal{H}}(\boldsymbol{f}^{\boldsymbol{j}}) \le \deg_{\mathcal{H}} \Lambda_{\boldsymbol{0}} + |\boldsymbol{j}| m_{\mathrm{H}},$$

which proves the claim. ∎

Remark 1 Most received words will satisfy $\deg_{\mathcal{H}} R_i = n + 2g - 1$ for all $i = 1, \ldots, h$. In such a case, the solution of Problem 1 given in Theorem 3 fulfills all degree restrictions of the problem with equality. These relative upper bounds on the degrees of $\lambda_{\boldsymbol{i}}$ and $\psi_{\boldsymbol{j}}$ are therefore the minimal choice among all such bounds for which Theorem 3 holds.

Theorem 3 motivates a decoding strategy, which is outlined in Algorithm 1: To every codeword $\boldsymbol{c}' \in \mathcal{C}_{\mathcal{H}}(n, m_{\mathrm{H}}; h)$ corresponds a solution to Problem 1 whose degree is roughly $s \cdot |\mathcal{E}'|$, where $|\mathcal{E}'|$ is the number of errors (i.e., non-zero columns) of $\boldsymbol{r} - \boldsymbol{c}'$. Among those solutions, we want to find the one of smallest degree, i.e., the one for the closest codeword. There will also be other solutions to Problem 1, which do not correspond to codewords, but the idea is that in most cases, and when the number of errors is not too large, the minimal solution *will* correspond to the closest codeword.

Algorithm 1: Improved Power Decoder for h-Interleaved 1-Point Hermitian Codes

Input: Received word $\boldsymbol{r} \in \mathbb{F}_{q^m}^{h \times n}$ and positive integers $s \leq \ell$

Output: $\boldsymbol{f} \in \mathcal{L}(m_{\mathrm{H}} P_\infty)^h$ such that $\boldsymbol{c}_i = [f_i(P_1), \ldots, f_i(P_n)]$ for all $i = 1, \ldots, h$ is the codeword with a corresponding minimal $\deg_{\mathcal{H}} \Lambda_s$; or "decoding failure".

Compute $\boldsymbol{R}$ and G as in Section 3

$A_{\boldsymbol{i},\boldsymbol{j}} \leftarrow \binom{\boldsymbol{j}}{\boldsymbol{i}} \boldsymbol{R}^{\boldsymbol{j}-\boldsymbol{i}} G^{|\boldsymbol{i}|}$ for all $\boldsymbol{i} \preceq \boldsymbol{j}$

$\lambda_{\boldsymbol{i}}, \psi_{\boldsymbol{j}} \leftarrow$ Minimal solution to Problem 1 with input s, ℓ, $A_{\boldsymbol{i},\boldsymbol{j}}$, and G

if $\lambda_{\boldsymbol{0}}$ *divides all* $\psi_{\boldsymbol{u}_i}$ *over* $\mathcal{R}$ *for* $i = 1, \ldots, h$, *where* $\boldsymbol{u}_i$ *is the* i^{th} *unit vector* **then**

  $\boldsymbol{f} \leftarrow [\psi_{\boldsymbol{u}_1}/\lambda_{\boldsymbol{0}}, \ldots, \psi_{\boldsymbol{u}_h}/\lambda_{\boldsymbol{0}}]$

  $\mathcal{E} \leftarrow$ Error set corresponding to $\boldsymbol{e}_i = \boldsymbol{r}_i - [f_i(\alpha_1), \ldots, f_i(\alpha_n)]$ for $i = 1, \ldots, h$

  if $\lambda_{\boldsymbol{0}} \in \mathcal{L}\left(-\sum_{i \in \mathcal{E}} sP_i + \infty P_\infty\right)$ **and** $s \cdot |\mathcal{E}| \leq \deg_{\mathcal{H}} \lambda_{\boldsymbol{0}} \leq s(|\mathcal{E}| + g)$ **then**

    return $\boldsymbol{f}$

return *"decoding failure"*

In the cases for which this does not happen, the decoder will fail; we will return to this in Section 5. If the algorithm finds a solution that corresponds to a codeword, then we have $\lambda_{\boldsymbol{0}} = \Lambda_s$ and $\psi_{\boldsymbol{u}_i} = \Lambda_s f_i$ for $i = 1, \ldots, h$, where $\boldsymbol{u}_i = [0, \ldots, 1, \ldots, 0]$ is the ith unit vector. Hence, we obtain the ith message polynomial f_i by division of $\psi_{\boldsymbol{u}_i}$ by $\lambda_{\boldsymbol{0}}$.

Note that Algorithm 1 does not exactly promise to find the closest codeword: it finds the codewords whose corresponding Λ_s has minimal $\deg_{\mathcal{H}}$. When the number of errors is very small, we will often or always have $\deg_{\mathcal{H}} \Lambda_s < s|\mathcal{E}| + g$; but in this case all other codewords are much farther away from $\boldsymbol{r}$. On the other hand, when the number of errors is large, most error vectors will satisfy $\deg_{\mathcal{H}} \Lambda_s = s|\mathcal{E}| + g$. In both these cases Algorithm 1 will find the closest codewords. It seems reasonable to expect, however, that there exist some rare received words for which a farther codeword will have an associated Λ_s of lower $\deg_{\mathcal{H}}$ than the closest codeword.

We will see in Section 7 that we can find a minimal solution of Problem 1 efficiently.

5 Decoding Radius and Failure Behavior

In this section, we derive an upper bound on the maximal degree of the error locator polynomial Λ_s for which there can be a unique minimal solution of Problem 1. Since the degree of Λ_s is related to the number of errors, this implies an estimate of the maximal decoding radius of our decoder. We also briefly discuss in which cases the decoder fails below this bound.

Lemma 5 *Let $\tau, \ell, s \in \mathbb{N}$ such that $s \leq \ell$ and $\tau + \ell m_{\mathrm{H}} < sn$. All polynomials $\lambda_{\boldsymbol{i}}, \psi_{\boldsymbol{j}} \in \mathcal{R}$ for $\boldsymbol{i} \in \mathcal{I}$ and $\boldsymbol{j} \in \mathcal{J}$ that fulfill (5), (6), and the absolute degree restrictions*

$$\deg_{\mathcal{H}} \lambda_{\boldsymbol{i}} - |\boldsymbol{i}|(2g-1) \leq \tau, \tag{9}$$

$$\deg_{\mathcal{H}} \psi_{\boldsymbol{j}} - |\boldsymbol{j}| m_{\mathrm{H}} \leq \tau, \tag{10}$$

can be computed by a homogeneous linear system of equations over $\mathbb{F}_{q^2}$ with at least

$$\delta(\tau) = (\tau+1)\tbinom{h+\ell}{h} - n\left[h\tbinom{h+s-1}{h+1} + s\tbinom{h+\ell}{h} - s\tbinom{h+s-1}{h}\right] + m_{\mathrm{H}} h \tbinom{h+\ell}{h+1} - g\tbinom{h+\ell}{h}$$

more variables than equations, whenever $\delta(\tau) \geq 0$. If $\tau \geq 2g-1$, there are received words for which the difference is exactly $\delta(\tau)$.

Proof: We have $\deg_{\mathcal{H}} A_{i,j} \leq (n+2g-1)|\boldsymbol{j}| - (2g-1)|\boldsymbol{i}|$, so we get

$$\deg_{\mathcal{H}} \Big(\sum_{\boldsymbol{i} \in \mathcal{I}} \lambda_{\boldsymbol{i}} A_{\boldsymbol{i},\boldsymbol{j}} \Big) \leq \tau + |\boldsymbol{j}|(n+2g-1) \quad \forall \boldsymbol{j} \in \mathcal{J}.$$

Thus, for most $\boldsymbol{j}$ the polynomial $\psi_{\boldsymbol{j}}$ has lower degree than the terms in $\sum_{\boldsymbol{i} \in \mathcal{I}} \lambda_{\boldsymbol{i}} A_{\boldsymbol{i},\boldsymbol{j}}$ in the case $|\boldsymbol{j}| < s$ and less than the degree of the modulus G^s in the other case. Consider functions in $\mathcal{R}$ over the basis $\{X^i Y^j\}$ over $\mathbb{F}_{q^2}$. Since the $\mathbb{F}_{q^2}$-coefficients of $\sum_{\boldsymbol{i} \in \mathcal{I}} \lambda_{\boldsymbol{i}} A_{\boldsymbol{i},\boldsymbol{j}}$ and $(\sum_{\boldsymbol{i} \in \mathcal{I}} \lambda_{\boldsymbol{i}} A_{\boldsymbol{i},\boldsymbol{j}} \bmod G^s)$ are known linear combinations of the unknown coefficients of the $\lambda_{\boldsymbol{i}}$, the restrictions of the lemma on the degrees of $\psi_{\boldsymbol{j}} \in \mathcal{R}$ can be described by an $\mathbb{F}_{q^2}$ homogeneous linear system of equations that specify that the top coefficients of $\psi_{\boldsymbol{j}}$ be zero ($\tau + |\boldsymbol{j}| m_{\mathrm{H}} + 1$ and higher).

For non-negative integers a and b, there are between $b-a-g$ and $b-a$ many monomials $x^i y^j \in \mathcal{R}$ with $j < q$ of degree at least a and less than b. The lower bound is due to the Riemann–Roch theorem and the upper bound follows from the injectivity of $\deg_{\mathcal{H}}$ on the set of monomials.

Due to the degrees of the involved polynomials, the number of $\mathbb{F}_{q^2}$-linear restrictions for each $|\boldsymbol{j}| < s$ becomes

$$N_{\boldsymbol{j}} = (\tau + |\boldsymbol{j}|(n+2g-1)) - (\tau + |\boldsymbol{j}| m_{\mathrm{H}}) = |\boldsymbol{j}|(n+2g-1-m_{\mathrm{H}}).$$

For $|\boldsymbol{j}| \geq s$, the analysis is a bit more involved: Since G is a polynomial only in X with $\deg_X(G^s) = sq^2$, the congruence modulo G^s reduces the X-degree of all monomials below sq^2, i.e., the polynomial $(\sum_{\boldsymbol{i} \in \mathcal{I}} \lambda_{\boldsymbol{i}} A_{\boldsymbol{i},\boldsymbol{j}} \bmod G^s)$ can be written as

$$\left(\sum_{\boldsymbol{i} \in \mathcal{I}} \lambda_{\boldsymbol{i}} A_{\boldsymbol{i},\boldsymbol{j}} \bmod G^s \right) = \sum_{j=0}^{q-1} \sum_{i=0}^{sq^2-1} a_{ij} X^i Y^j,$$

where $a_{ij} \in \mathbb{F}_{q^2}$ are linear expressions of the coefficients of the $\lambda_{\boldsymbol{i}}$. By the degree restriction of $\psi_{\boldsymbol{j}}$, we must have that the coefficients a_{ij} with $\deg_{\mathcal{H}}(X^iY^j) > \tau + |\boldsymbol{j}|m_{\mathrm{H}}$ are zero. Thus, we get at most

$$\begin{aligned} N_{\boldsymbol{j}} &= \left(\sum_{j=0}^{q-1} sq^2\right) - \underbrace{|\{(i,j) \,:\, qi + (q+1)j \leq \tau + |\boldsymbol{j}|m_{\mathrm{H}}\}|}_{=\tau+|\boldsymbol{j}|m_{\mathrm{H}}-g+1} \\ &= sn - \tau - |\boldsymbol{j}|m_{\mathrm{H}} + g - 1 \end{aligned}$$

linear equations. Note that the condition $\tau + \ell m_{\mathrm{H}} < sn$ guarantees that there is no monomial X^iY^j of $\deg_{\mathcal{H}}(X^iY^j) > \tau + |\boldsymbol{j}|m_{\mathrm{H}}$ with $\deg_X \geq sq^2$. In total, and using Lemma 1 repeatedly:

$$\begin{aligned} \mathrm{NE} = \sum_{\boldsymbol{j}\in\mathcal{J}} N_{\boldsymbol{j}} &= \sum_{1\leq|\boldsymbol{j}|<s} |\boldsymbol{j}|(n+2g-1-m_{\mathrm{H}}) + \sum_{s\leq|\boldsymbol{j}|\leq\ell} \big(sn - \tau - |\boldsymbol{j}|m_{\mathrm{H}} + g - 1\big) \\ &= (n+2g-1)h\tbinom{h+s-1}{h+1} + (sn-\tau-1+g)\left(\tbinom{h+\ell}{h} - \tbinom{h+s-1}{h}\right) - m_{\mathrm{H}}h\tbinom{h+\ell}{h+1}. \end{aligned}$$

The number of variables, i.e., the number of $\mathbb{F}_{q^2}$-coefficients of the $\lambda_{\boldsymbol{i}}$ is at least

$$\mathrm{NV} = \Big(\sum_{\boldsymbol{i}\in\mathcal{I}} (\tau + |\boldsymbol{i}|(2g-1) + 1 - g)\Big) = (\tau+1-g)\tbinom{h+s-1}{h} + (2g-1)h\tbinom{h+s-1}{h+1}.$$

The claim follows by subtracting NV − NE.

In the case $\tau \geq 2g-1$, all Weierstraß gaps are below the degree bounds of the $\lambda_{\boldsymbol{i}}$ and $\psi_{\boldsymbol{j}}$. Hence, the number of variables and equations is equal to the derived NE and NV, respectively, as long as the maximal possible degree of $\deg_{\mathcal{H}}\left(\sum_{\boldsymbol{i}\in\mathcal{I}} \lambda_{\boldsymbol{i}} A_{\boldsymbol{i},\boldsymbol{j}}\right)$, i.e., for some choice of the $\lambda_{\boldsymbol{i}}$, is equal to $\tau + |\boldsymbol{j}|(n+2g-1)$. There are received words for which $\deg_{\mathcal{H}} R_i = n+2g-1$ for all i. In these cases, we can have $\deg_{\mathcal{H}}\left(\sum_{\boldsymbol{i}\in\mathcal{I}} \lambda_{\boldsymbol{i}} A_{\boldsymbol{i},\boldsymbol{j}}\right) = \tau + |\boldsymbol{j}|(n+2g-1)$ for some values of $\lambda_{\boldsymbol{i}}$, so (if $\tau \geq 2g-1$), the number of variables minus the number of equations is exactly $\delta(\tau)$. ■

Lemma 6 *If Problem 1 has a solution of degree τ, it has at least $(q^2)^{\delta(\tau)-1}$ many such solutions.*

Proof: Solutions of degree τ of Problem 1 are exactly the solutions of the homogeneous linear system in Lemma 5 with $\deg_{\mathcal{H}} \lambda_{\boldsymbol{0}} = \tau$ and monic $\lambda_{\boldsymbol{0}}$. Thus, we set the τth coefficient of $\lambda_{\boldsymbol{0}}$ to 1 and obtain an inhomogeneous linear system of equations with at least $\delta(\tau) - 1$ more variables than equations. If Problem 1 has a solution of degree τ, then this system has at least $(q^2)^{\ker(\boldsymbol{A})}$ solutions, where $\boldsymbol{A}$ is the system's matrix. The claim follows by $\dim(\ker(\boldsymbol{A})) \geq \delta(\tau) - 1$. ■

Lemma 6 implies the following statement.

Theorem 4 *Let $\tau = \deg_{\mathcal{H}} \Lambda_s$ and $s, \ell \in \mathbb{N}$ such that $s \leq \ell$ and $\tau + \ell m_{\mathrm{H}} < sn$ and*

$$\tau > \tau_{\max} := sn\left(1 - \frac{s\binom{h+s-1}{h} - h\binom{h+s-1}{h+1}}{s\binom{h+\ell}{h}}\right) - \frac{h}{h+1}\ell m_{\mathrm{H}} + \left(\frac{1}{\binom{h+\ell}{h}} - 1\right) + g. \tag{11}$$

Then, Problem 1 has at least two solutions of degree τ.

Proof: Condition (11) is fulfilled if and only if $\delta(\tau) > 1$. Due to $\tau = \deg_{\mathcal{H}} \Lambda_s$, Problem 1 has a solution of degree τ and the claim follows by Lemma 6. ∎

Theorem 4 can be interpreted as follows: If $\deg_{\mathcal{H}} \Lambda_s > \tau_{\max}$, then either Λ_s does not correspond to a minimal solution of Problem 1, or it is a minimal solution but there are many other minimal solutions as well. There is no reason to think that our solver for Problem 1 will find Λ_s among all those solutions, so decoding will likely fail.

Since we have $|\mathcal{E}| \leq \deg_{\mathcal{H}} \Lambda_s \leq s|\mathcal{E}| + g$, and often $\deg_{\mathcal{H}} \Lambda_s = s|\mathcal{E}| + g$, we usually have no unique solution whenever $s|\mathcal{E}| + g > \tau_{\max}$, i.e.,

$$|\mathcal{E}| > \tfrac{\tau_{\max} - g}{s}$$

and for sure if $|\mathcal{E}| > \frac{\tau_{\max}}{s}$. We therefore call

$$t_{\text{new}} = \tfrac{\tau_{\max} - g}{s} = n\left(1 - \frac{s\binom{h+s-1}{h} - h\binom{h+s-1}{h+1}}{s\binom{h+\ell}{h}}\right) - \frac{h}{h+1}\frac{\ell}{s}m_{\text{H}} + \frac{1}{s}\left(\frac{1}{\binom{h+\ell}{h}} - 1\right) \tag{12}$$

the *decoding radius* of Algorithm 1.

Remark 2 For $\tau \geq 2g - 1$, by Lemma 5, there are received words (in fact most of them) such that the difference of numbers of variables and equations of the inhomogeneous system for computing all degree-τ solutions of Problem 1 is exactly $\delta(\tau) - 1$. Thus, if there are sufficiently many linearly independent equations[1], there is no other solution of the problem, besides the error locator, of degree τ whenever $\delta(\tau) < 0$.

For $\tau < 2g - 1$, the degree bounds of $\lambda_{\mathbf{0}}$ and $\psi_{\mathbf{0}}$ are smaller than $2g - 1$, but those of all other $\lambda_{\boldsymbol{i}}$ and $\psi_{\boldsymbol{j}}$ are bigger (note that $m_{\text{H}} \geq 2g - 1$). Thus, there can be up to g fewer equations and up to g more variables than predicted by $\delta(\tau)$ for any received word. The value of $\tau_{\max}$ as in Theorem 4 can in this case therefore be smaller by a value up to

$$\tau'_{\max} = \tau_{\max} - 2g\frac{1}{\binom{h+\ell}{h}},$$

which reduces the decoding radius by at most $2g/[s\binom{h+\ell}{h}]$.

In the case $\tau + \ell m_{\text{H}} \geq sn$, the number of equations is also smaller than predicted by $\tau_{\max}$. However, we will see in Section 5.1 that the best choice of s for a given ℓ yields $\tau + \ell m_{\text{H}} < sn$ for $\tau \leq \tau_{\max}$.

Since we cannot guarantee that the linear equations of the system in Lemma 5 are linearly independent for $\tau \leq \deg_{\mathcal{H}} \Lambda_s$, Algorithm 1 can fail to return the sent codeword $\boldsymbol{c}$ for some errors of weight less than the maximal decoding radius. In these cases, we have one of the following.

- There is a solution of Problem 1 of degree $< \deg_{\mathcal{H}} \Lambda_s$.
- There is more than one solution of Problem 1 of degree $= \deg_{\mathcal{H}} \Lambda_s$ and the decoder picks the wrong one.

[1] This linear-algebraic condition resembles, but seems weaker than, the "(non-linear) algebraic independence assumption" in [10] for decoding interleaved RS codes.

However, the simulation results for various code and decoder parameters, presented in the following section, indicate that the new decoder is able to decode most error patterns up to the derived decoding radius t_{new}. Sometimes, decoding succeeds even beyond t_{new}. In these cases, we usually have $\deg_{\mathcal{H}}(\Lambda_s) < s|\mathcal{E}| + g$.

In all previous power decoding algorithms for Reed–Solomon [2,5], one-point Hermitian [4,6], and interleaved Reed–Solomon codes [12], simulation results indicate that the failure probability for a number of errors below the maximal decoding radius is small and decreases exponentially in the difference of maximal decoding radius and number of errors.

As for these other variants, except for a few parameters of theirs (e.g., $\ell \leq 3$ and $s \leq 2$ for a single Reed–Solomon code in [5]), it remains an open problem to prove an analytic upper bound on the failure probability of Algorithm 1.

5.1 Asymptotic Analysis and Parameter Choice

We study the asymptotic behavior of the decoding radius $\tau_{\max}$ and give explicit parameters to achieve the given limit. The analysis is based on the following lemma.

Lemma 7 ([12, Lemma 14]) *Let $\gamma \in (0,1)$ and $h \in \mathbb{N}$ be fixed. Then, we have*

$$\frac{\binom{h+\lfloor \gamma i \rfloor}{h}}{\binom{h+i}{h}} = \gamma^h + O\left(\tfrac{1}{i}\right) \quad \textit{for } (i \to \infty).$$

Theorem 5 *Let $(\ell_i, s_i) = (i, \lfloor \gamma i \rfloor + 1)$ for $i \in \mathbb{N}$, where $\gamma = \sqrt[h+1]{\frac{m_{\text{H}}}{n}}$. Then,*

$$t_{\text{new}}(\ell_i, s_i) = n\left(1 - \left(\tfrac{m_{\text{H}}}{n}\right)^{\frac{h}{h+1}} - O\left(\tfrac{1}{i}\right)\right) \quad \textit{for } (i \to \infty).$$

Proof: We have

$$\begin{aligned}\frac{t_{\text{new}}}{n} &= 1 - \Bigg[1 + \underbrace{\left(1 - \tfrac{1}{s_i}\right)}_{=1-O\left(\frac{1}{i}\right)} \tfrac{h}{h+1}\Bigg] \underbrace{\frac{\binom{h+\lfloor \gamma i \rfloor}{h}}{\binom{h+i}{h}}}_{=\gamma^h + O\left(\frac{1}{i}\right)} - \frac{h}{h+1} \underbrace{\frac{\ell_i}{s_i}}_{\substack{=\gamma^{-1} \\ +O\left(\frac{1}{i}\right)}} \frac{m_{\text{H}}}{n} + \underbrace{\frac{1}{s_i}}_{=O\left(\frac{1}{i}\right)} \underbrace{\left[\frac{1}{\binom{h+\ell_i}{h}} - 1\right]}_{=-1+O\left(\frac{1}{i}\right)} \\ &= 1 + \frac{m}{m+1} \underbrace{\left(\gamma^h - \gamma^{-1}\frac{m_{\text{H}}}{n}\right)}_{=0} - \gamma^h - O\left(\tfrac{1}{i}\right) = 1 - \left(\tfrac{m_{\text{H}}}{n}\right)^{\frac{h}{h+1}} - O\left(\tfrac{1}{i}\right),\end{aligned}$$

which proves the claim. ■

Note that the choice of ℓ_i and s_i in Theorem 5 ensures that $\tau + \ell_i m_{\text{H}} < s_i n$ for all $\tau \leq s \cdot t_{\text{new}}(\ell_i, s_i)$.

6 Numerical Results

In this section, we present simulation results. We have conducted Monte-Carlo simulations for estimating the failure probability of the new decoding algorithm in a channel that randomly adds $t = |\mathcal{E}|$ errors, using $N \in \{10^3, 10^4\}$ samples. The decoder was implemented in SageMath v7.5 [17], based on the power decoder implementation of [4].

All simulated examples fulfill $\deg_{\mathcal{H}} \Lambda_s \geq st \geq 2g - 1$. If this condition is not fulfilled, the simulation results might differ from the expected decoding radius, cf. Remark 2.

6.1 Case $h = 1$

We first compare the new improved power ($\hat{\mathrm{P}}_{\mathrm{fail,IPD}}$) with the Guruswami–Sudan ($\hat{\mathrm{P}}_{\mathrm{fail,GS}}$) decoder. The used implementation of the Guruswami–Sudan decoder is the publicly available one from [4]. Table 1 presents the simulation results for various code (q, m, n, k, d^*), decoder (ℓ, s), and channel (t) parameters.

Table 1 Observed failure rate of the improved power ($\hat{\mathrm{P}}_{\mathrm{fail,IPD}}$) and Guruswami–Sudan ($\hat{\mathrm{P}}_{\mathrm{fail,GS}}$) decoder for $h = 1$. Code parameters q, m, n, k, d^*. Decoder parameters ℓ, s. Number of errors t ($^+t = t_{\mathrm{new}}$ decoding radius as in (12)). Number of experiments N.

q	m	n	k	d^*	ℓ	s	t	$\hat{\mathrm{P}}_{\mathrm{fail,IPD}}$	$\hat{\mathrm{P}}_{\mathrm{fail,GS}}$	N
4	15	64	10	49	4	2	28	0	0	10^4
							29^+	0	$3.30 \cdot 10^{-3}$	10^4
							30	$9.93 \cdot 10^{-1}$	$9.39 \cdot 10^{-1}$	10^4
5	55	125	46	70	3	2	35	0	0	10^4
							36^+	0	$4.00 \cdot 10^{-4}$	10^4
							37	$9.57 \cdot 10^{-1}$	$9.60 \cdot 10^{-1}$	10^4
5	20	125	11	105	5	2	67	0	0	10^3
							68^+	0	$7.00 \cdot 10^{-3}$	10^3
							69	$9.91 \cdot 10^{-1}$	$9.60 \cdot 10^{-1}$	10^3
7	70	343	50	273	3	2	160	0	0	10^3
							161^+	0	0	10^3
							162	$9.78 \cdot 10^{-1}$	$9.86 \cdot 10^{-1}$	10^3
7	70	343	50	273	4	2	168	0	0	10^3
							169^+	0	0	10^3
							170	$9.79 \cdot 10^{-1}$	$2.2 \cdot 10^{-2}$	10^3
7	55	343	35	288	4	2	183	0	0	10^3
							184^+	0	0	10^3
							185	$9.82 \cdot 10^{-1}$	$1.9 \cdot 10^{-2}$	10^3

It can be observed that both algorithms can almost always correct t_{new} many errors, improving upon classical power decoding. Also, neither of the two algorithms is generally superior in terms of failure probability.

When comparing the two algorithms, one has to keep in mind that the GS algorithm is guaranteed to work only up to $n[1 - \frac{s+1}{2(\ell+1)}] - \frac{\ell}{2s} m_{\mathrm{H}} - \frac{g}{s} = t_{\mathrm{new}} - \frac{g}{s} + \frac{\ell}{s(\ell+1)}$ errors.

6.2 General Case

We now turn to the general case of $h > 1$, where the previous best relative decoding radius is $t_{\mathrm{K}} = \frac{h}{h+1}(n - m_{\mathrm{H}})$ [6]. The simulations results for various code and decoder parameters are given in Table 2.

Table 2 Observed failure rate of Algorithm 1 ($\hat{\mathrm{P}}_{\mathrm{fail,IPD}}$) for $h > 1$. Code parameters $q, m_{\mathrm{H}}, n, k, d^*, h$. Decoder parameters ℓ, s. Number of errors t ($^+t = t_{\mathrm{new}}$ decoding radius as in (12)). Number of experiments N. Previous best decoding radius t_{K} [6].

q	m_{H}	n	k	d^*	h	ℓ	s	t	$\hat{\mathrm{P}}_{\mathrm{fail,IPD}}$	N	t_{K}
4	15	64	10	49	2	3	2	35^+	0	10^5	32
								36	$9.18 \cdot 10^{-1}$	10^3	32
4	15	64	10	49	2	5	3	36^+	0	10^3	32
								37	$9.31 \cdot 10^{-1}$	10^3	32
4	15	64	10	49	3	3	2	38^+	0	10^5	36
								39	$9.42 \cdot 10^{-1}$	10^3	36
4	15	64	10	49	3	4	3	39^+	0	10^2	36
								40	1	10^2	36
4	22	64	17	42	2	4	3	29^+	0	10^3	28
								30	$9.44 \cdot 10^{-1}$	10^3	28
5	20	125	11	105	2	3	2	79^+	0	10^5	70
								80	$9.37 \cdot 10^{-1}$	10^3	70
5	20	125	11	105	2	4	2	81^+	0	10^3	70
								82	$9.93 \cdot 10^{-1}$	10^3	70
5	20	125	11	105	3	3	2	86^+	0	10^3	78
								87	$9.94 \cdot 10^{-1}$	10^3	78
5	55	125	46	70	2	4	3	48^+	0	10^3	46
								49	$9.86 \cdot 10^{-1}$	10^3	46
7	90	343	70	253	2	3	2	183^+	0	10^3	168
								184	$9.72 \cdot 10^{-1}$	10^3	168
8	128	512	101	384	2	3	2	281^+	0	10^2	256
								282	1	10^2	256

In all tested cases, Algorithm 1 corrected all decoding trials up to t_{new} many errors and failed with large observed probability one error beyond this radius.

7 Efficiently Finding a Minimal Solution of Problem 1

We use the $\mathbb{F}_{q^2}[X]$-vector representation of an element of $\mathcal{R}$ (cf. [4]) to reformulate Problem 1 over $\mathbb{F}_{q^2}[X]$. Recall that for $a \in \mathcal{R}$, we can write $a = \sum_{i=0}^{q-1} a_i Y^i \in \mathcal{R}$ with unique $a_i \in \mathbb{F}_{q^2}[X]$. Then, the *vector representation* [4] of a is defined by $\boldsymbol{\nu}(a) = (a_0, \ldots, a_{q-1}) \in \mathbb{F}_{q^2}[X]^q$. Note that $q \deg(a_i) + i(q+1) \leq \deg_{\mathcal{H}}(a)$. For $a, b \in \mathcal{R}$ it can be shown that

$$\boldsymbol{\nu}(a+b) = \boldsymbol{\nu}(a) + \boldsymbol{\nu}(b), \qquad \boldsymbol{\nu}(ab) = \boldsymbol{\nu}(a)\boldsymbol{\mu}(b)\boldsymbol{\Xi},$$

where $\boldsymbol{\mu}(b) \in \mathbb{F}_{q^2}[X]^{q\times(2q-1)}$ and $\boldsymbol{\Xi} \in \mathbb{F}_{q^2}[X]^{(2q-1)\times q}$ are defined by

$$\boldsymbol{\mu}(b) := \begin{bmatrix} b_0 & b_1 & b_2 & \dots & b_{q-1} & & & \\ & b_0 & b_1 & \dots & b_{q-2} & b_{q-1} & & \\ & & \ddots & \ddots & \dots & \ddots & \ddots & \\ & & & b_0 & b_1 & \dots & b_{q-2} & b_{q-1} \end{bmatrix}, \quad \boldsymbol{\Xi} := \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & & 1 \\ X^{q+1} & -1 & & & \\ & X^{q+1} & -1 & & \\ & & \ddots & \ddots & \\ & & & X^{q+1} & -1 \end{bmatrix}.$$

Note further that for $c \in \mathbb{F}_{q^2}[X]$ we have simply $\boldsymbol{\mu}(ac) = \boldsymbol{\mu}(a)c$. Using the notation above, we can reformulate Problem 1 into the following problem over $\mathbb{F}_{q^2}[X]$. In the following, let $[q)$ denote $\{0, \dots, q-1\}$.

Problem 2 Given positive integers $s \le \ell$, $\boldsymbol{R}$ and G as in Section 3, and

$$\boldsymbol{A}^{(\boldsymbol{i},\boldsymbol{j})} := \boldsymbol{\mu}(A_{\boldsymbol{i},\boldsymbol{j}})\boldsymbol{\Xi} = \boldsymbol{\mu}\left(\tbinom{\boldsymbol{j}}{\boldsymbol{i}}\boldsymbol{R}^{\boldsymbol{j}-\boldsymbol{i}}G^{|\boldsymbol{i}|}\right)\boldsymbol{\Xi} \in \mathbb{F}_{q^2}[X]^{q\times q}$$

for all $\boldsymbol{i} \in \mathcal{I} := \{\boldsymbol{i} \in \mathbb{N}_0^h : 0 \le |\boldsymbol{i}| < s\}$ and $\boldsymbol{j} \in \mathcal{J} := \{\boldsymbol{j} \in \mathbb{N}_0^h : 1 \le |\boldsymbol{j}| \le \ell\}$. Find $\lambda_{\boldsymbol{i},\iota}, \psi_{\boldsymbol{j},\kappa} \in \mathbb{F}_{q^2}[X]$ for $\boldsymbol{i} \in \mathcal{I}$, $\boldsymbol{j} \in \mathcal{J}$, $\iota, \kappa \in [q)$, not all zero, such that

$$\begin{aligned} \psi_{\boldsymbol{j},\kappa} &= \sum_{\boldsymbol{i}\in\mathcal{I}} \sum_{\iota=0}^{q-1} \lambda_{\boldsymbol{i},\iota} A_{\iota,\kappa}^{(\boldsymbol{i},\boldsymbol{j})} && 1 \le |\boldsymbol{j}| < s, \\ \psi_{\boldsymbol{j},\kappa} &\equiv \sum_{\boldsymbol{i}\in\mathcal{I}} \sum_{\iota=0}^{q-1} \lambda_{\boldsymbol{i},\iota} A_{\iota,\kappa}^{(\boldsymbol{i},\boldsymbol{j})} \mod G^s && 1 \le |\boldsymbol{j}| < s, \\ \max_{\iota\in[q)} \left\{q \deg \lambda_{\boldsymbol{0},\iota} + \iota(q+1)\right\} &\le q \deg \lambda_{\boldsymbol{i},\iota} + \iota(q+1) - |\boldsymbol{i}|(2g-1) && 0 \le |\boldsymbol{i}| < s,\ \iota \in [q) \\ \max_{\iota\in[q)} \left\{q \deg \lambda_{\boldsymbol{0},\iota} + \iota(q+1)\right\} &\le q \deg \psi_{\boldsymbol{j},\kappa} + \kappa(q+1) - |\boldsymbol{j}| m_{\mathrm{H}} && 1 \le |\boldsymbol{j}| \le \ell,\ \kappa \in [q) \end{aligned}$$

Similar to its $\mathcal{R}$-equivalent, we define the degree of a solution of the above problem to be $\max_{\iota\in[q)} \left\{q \deg \lambda_{\boldsymbol{0},\iota} + \iota(q+1)\right\}$ and call the solution monic if the leading coefficient of the $\lambda_{\boldsymbol{0},\iota}$ that maximizes $\max_{\iota\in[q)} \left\{q \deg \lambda_{\boldsymbol{0},\iota} + \iota(q+1)\right\}$ is 1. The following statement establishes the connection between Problem 1 and Problem 2.

Theorem 6 *Let $\tau \in \mathbb{Z}_{\ge 0}$. Then, $\lambda_{\boldsymbol{i}}, \psi_{\boldsymbol{j}} \in \mathcal{R}$ for $\boldsymbol{i} \in \mathcal{I}$ and $\boldsymbol{j} \in \mathcal{J}$ is a solution of degree τ of Problem 1 if and only if*

$$\begin{aligned} [\lambda_{\boldsymbol{i},0}, \dots, \lambda_{\boldsymbol{i},q-1}] &:= \boldsymbol{\nu}(\lambda_{\boldsymbol{i}}) \\ [\psi_{\boldsymbol{j},0}, \dots, \psi_{\boldsymbol{j},q-1}] &:= \boldsymbol{\nu}(\psi_{\boldsymbol{j}}) \end{aligned}$$

is monic solution of degree τ of Problem 2.

Proof: If $\lambda_{\boldsymbol{i}}$ and $\psi_{\boldsymbol{j}}$ forms a solution to Problem 1 this means for $|\boldsymbol{j}| \geq s$ that there is some $u_{\boldsymbol{j}} \in \mathcal{R}$ such that:

$$\begin{aligned} \psi_{\boldsymbol{j}} &= \sum_{\substack{\boldsymbol{i} \preceq \boldsymbol{j} \\ |\boldsymbol{i}|<s}} \lambda_{\boldsymbol{i}} A_{\boldsymbol{i},\boldsymbol{j}} + u_{\boldsymbol{j}} G^s && \iff \\ \boldsymbol{\nu}(\psi_{\boldsymbol{j}}) &= \sum_{\substack{\boldsymbol{i} \preceq \boldsymbol{j} \\ |\boldsymbol{i}|<s}} \boldsymbol{\nu}(\lambda_{\boldsymbol{i}}) \boldsymbol{\mu}(A_{\boldsymbol{i},\boldsymbol{j}}) \boldsymbol{\Xi} + \boldsymbol{\mu}(u_{\boldsymbol{j}}) G^s \ . \end{aligned}$$

since $G^s \in \mathbb{F}_{q^2}[X]$. This implies element-wise the congruence of Problem 2. The opposite direction is analogous, as is the case $|\boldsymbol{j}| < s$. The degree restrictions follow immediately from $\deg_{\mathcal{H}}(a) = \max_{\iota \in [q]}\{q \deg a_\iota + \iota(q+1)\}$ for any $a \in \mathcal{R}$ and $\boldsymbol{\nu}(a) = (a_1, \ldots, a_{q-1})$. ■

Problem 2 is of the same instance as the problem discussed in [4, Section V.B],[2] which can be solved by transforming an $\mathbb{F}_{q^2}[X]$-module basis that depends on the entries of $\boldsymbol{A}^{(\boldsymbol{i},\boldsymbol{j})}$ and the relative degree bounds in Problem 2, into a reduced polynomial matrix form (weak Popov form). Using this approach, finding a minimal solution of Problem 1 can be implemented in

$$O^{\sim}\left(\tbinom{h+\ell}{h}^{\omega} s n^{\frac{\omega+2}{3}}\right) \subseteq O^{\sim}\left(\ell^{h\omega} s n^{\frac{\omega+2}{3}}\right)$$

operations over $\mathbb{F}_{q^2}$, where $2 \leq \omega \leq 3$ is the matrix multiplication exponent. In [5], a similar kind of problem was reduced to finding solution bases of so-called Padé approximation problems. In this way, the complexity can be slightly reduced to

$$O^{\sim}\left(\tbinom{h+s-1}{h}\tbinom{h+\ell}{h}^{\omega-1} s n^{\frac{\omega+2}{3}}\right) \subseteq O^{\sim}\left(\ell^{h(\omega-1)} s^{h+1} n^{\frac{\omega+2}{3}}\right)$$

operations over $\mathbb{F}_{q^2}$. In order to achieve the asymptotic decoding radius, the code parameters must be chosen as in Section 5.1. In this case, the two asymptotic complexity statements above coincide and we get the following result.

Theorem 7 *For a fixed code of rate $R = \frac{k}{n}$ and any constant $\varepsilon > 0$, we can choose $s, \ell \in O(1/\varepsilon)$ such that $t_{\text{new}} \geq n(1 - (R + \frac{g-1}{n})^{\frac{h}{h+1}} - \varepsilon)$. In this case, Algorithm 1 costs $O^{\sim}((1/\varepsilon)^{h\omega+1} n^{\frac{\omega+2}{3}})$.*

Proof: The first statement directly follows from Theorem 5. The pre- and post-computations in Algorithm 1 are negligible compared to Line 3 by similar arguments as in [4]. The complexity thus follows by the arguments above. ■

[2] Using this approach, it is necessary to reformulate the equations for $1 \leq |\boldsymbol{j}| < s$ into congruences modulo x^{ξ}, where ξ is greater than the largest possible degree of the $\lambda_{\boldsymbol{i},\iota} A_{\iota,\kappa}^{(\boldsymbol{i},\boldsymbol{j})}$ for the maximal number of errors that we expect to corrected.

8 Comparison to Interleaved Reed–Solomon Codes

An h-interleaved code over some field $\mathbb{F}_Q$ over the burst error channel can equivalently be considered as a code over $\mathbb{F}_{Q^h}$ considered over the Q^h-ary channel. This allows comparing the decoding capability of interleaved 1-H codes with other constructions of short codes over large fields, most notably RS codes and interleaved RS codes, see Figure 1 for the case $Q^h = q^6$.

More precisely, for any $h \in \mathbb{Z}_{>0}$, we have several ways of obtaining $[n, k]$ codes over $\mathbb{F}_{q^{6h}}$ for $n = q^3$ and some dimension $k < n$. We will compare the following relative decoding radii:

t_{RS}: an RS code over $\mathbb{F}_{q^{6h}}$ decoding up to the Johnson radius using one of [1, 5, 18].[3]

t_{IRS}: $2h$-interleaved RS code over $\mathbb{F}_{q^3}$ using one of [10, 12].

t_{1H}: $3h$-interleaved 1-H code over $\mathbb{F}_{q^2}$ using the proposed algorithm.

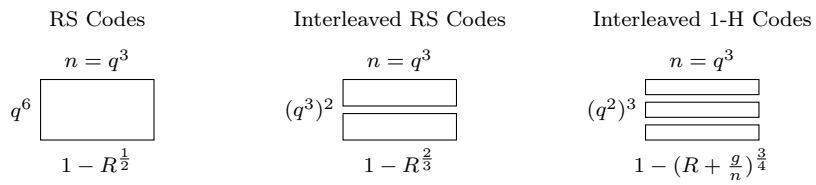

Fig. 1 Example: Comparison of interleaved Reed–Solomon and one-point Hermitian codes of length $n = q^3$ over an overall field size of q^6.

These values are as follows:

$$t_{\mathrm{RS}} = 1 - \left(\tfrac{k-1}{n}\right)^{\frac{1}{2}} \qquad t_{\mathrm{IRS}} = 1 - \left(\tfrac{k-1}{n}\right)^{\frac{2h}{2h+1}}, \qquad t_{\mathrm{IH}} = 1 - \left(\tfrac{k-1}{n} - \tfrac{g}{n}\right)^{\frac{3h}{3h+1}},$$

The asymptotics are already clear: since $\frac{g}{n} \to 0$ for $n \to \infty$, we can asymptotically achieve larger decoding radii with interleaved 1-H codes than with interleaved RS codes, when considering comparable overall field size. Below follows some concrete parameter examples.

$q = 13$ is the smallest prime power for which $t_{\mathrm{IH}} > t_{\mathrm{IRS}}$ for rate $1/2$, i.e. both interleaved codes can be considered as $[2197, 1098]$ codes over $\mathbb{F}_{13^6}$, and the decoding radii are $t_{\mathrm{RS}} = 644$, $t_{\mathrm{IRS}} = 814$ and $t_{\mathrm{IH}} = 823$. A list of decoding radii of rate $1/2$ codes with even q is given in Table 3.

9 Conclusion

We have presented a new decoding algorithm for h-interleaved one-point Hermitian codes based on the improved power decoder for Reed–Solomon codes in [5], its generalization

[3] As pointed out in [19], an RS code over $\mathbb{F}_{q^{6h}}$ whose evaluation points all lie in $\mathbb{F}_{q^3}$ are equivalent to a $2h$-interleaved RS codes over $\mathbb{F}_{q^3}$, i.e. can be decoded up to t_{IRS}. In our comparison here we therefore consider RS codes with arbitrary evaluation points for which this equivalence doesn't hold.

Table 3 Examples for t_{IH} and t_{IRS} for rate 1/2 codes of several lengths for $h_{\mathrm{RS}} = 2$ and $h_{\mathrm{H}} = 3$.

q	$n = q^3$	$k = \frac{n}{2}$	t_{RS}	t_{IRS}	t_{IH}	$t_{\mathrm{IH}}/t_{\mathrm{RS}} \approx$	$t_{\mathrm{IH}}/t_{\mathrm{IRS}} \approx$
2^3	512	256	150	190	183	1.22	0.96
2^4	4096	2048	1200	1516	1555	1.30	1.03
2^5	32768	16384	9598	12126	12844	1.34	1.06
2^6	262144	131072	76780	97004	104478	1.36	1.08
2^7	2097152	1048576	614242	776029	842936	1.37	1.09

to h-interleaved Reed–Solomon codes in [12], and the power decoder for one-point Hermitian codes in [4, 6].

The maximal decoding radius of the new algorithm is $n(1 - (R + \frac{g-1}{n})^{\frac{h}{h+1}} - \varepsilon)$ at a cost of $O^{\sim}((1/\varepsilon)^{h\omega+1} n^{\frac{\omega+2}{3}})$ operations over $\mathbb{F}_{q^2}$, where $2 \leq \omega \leq 3$ is the matrix multiplication exponent, and improves upon previous best decoding radii at all rates. Experimental results indicate that the algorithm achieves this maximal decoding radius with large probability.

For large n, interleaved one-point Hermitian codes achieve larger maximal decoding radii than interleaved Reed–Solomon codes when compared for the same length and overall field size.

In the case $h = 1$, we obtain a one-point Hermitian codes equivalent of the improved power decoder for Reed–Solomon codes in [5], which achieves a similar decoding radius as the Guruswami–Sudan list decoder. Simulation results indicate that the new decoder has a similar failure probability for numbers of errors beyond the latter's guaranteed decoding radius.

As for any other power decoding algorithm, both for Reed–Solomon and one-point Hermitian codes, deriving analytic bounds on the failure probability remains an open problem. So far, the only parameters for which such an expression is known are $h = 1$, $\ell \leq 3$, and $s \leq 2$, cf. [2, 5].

References

1. V. Guruswami and M. Sudan, "Improved Decoding of Reed–Solomon and Algebraic-Geometric Codes," in *IEEE Annual Symposium on Foundations of Computer Science*, 1998, pp. 28–37.
2. G. Schmidt, V. R. Sidorenko, and M. Bossert, "Syndrome Decoding of Reed–Solomon Codes Beyond Half the Minimum Distance Based on Shift-Register Synthesis," *IEEE Transactions on Information Theory*, vol. 56, no. 10, pp. 5245–5252, 2010.
3. S. Kampf, "Decoding Hermitian Codes - An Engineering Approach," Ph.D. dissertation, Universität Ulm, 2012.
4. J. S. R. Nielsen and P. Beelen, "Sub-Quadratic Decoding of One-Point Hermitian Codes," *IEEE Transactions on Information Theory*, vol. 61, no. 6, pp. 3225–3240, 2015.
5. J. Rosenkilde, "Power Decoding Reed–Solomon Codes up to the Johnson Radius," *Accepted for: Advances in Mathematics of Communications*, (2018), arXiv preprint arXiv:1505.02111.
6. S. Kampf, "Bounds on Collaborative Decoding of Interleaved Hermitian Codes and Virtual Extension," *Designs, codes and cryptography*, vol. 70, no. 1-2, pp. 9–25, 2014.
7. V. Y. Krachkovsky and Y. X. Lee, "Decoding for Iterative Reed–Solomon Coding Schemes," *IEEE Trans. Magn.*, vol. 33, no. 5, pp. 2740–2742, 1997.

8. F. Parvaresh and A. Vardy, "Multivariate Interpolation Decoding Beyond the Guruswami–Sudan Radius," in *Proceedings of the 42nd Allerton Conference on Communication, Control and Computing*, 2004.
9. G. Schmidt, V. Sidorenko, and M. Bossert, "Enhancing the Correcting Radius of Interleaved Reed-Solomon Decoding using Syndrome Extension Techniques," in *IEEE ISIT*, 2007, pp. 1341–1345.
10. H. Cohn and N. Heninger, "Approximate Common Divisors via Lattices," *The Open Book Series*, vol. 1, no. 1, pp. 271–293, 2013.
11. A. Wachter-Zeh, A. Zeh, and M. Bossert, "Decoding Interleaved Reed–Solomon Codes Beyond Their Joint Error-Correcting Capability," *Designs, Codes and Cryptography*, vol. 71, no. 2, pp. 261–281, 2014.
12. S. Puchinger and J. Rosenkilde né Nielsen, "Decoding of Interleaved Reed-Solomon Codes Using Improved Power Decoding," *IEEE International Symposium on Information Theory*, 2017.
13. S. Puchinger, I. Bouw, and J. Rosenkilde né Nielsen, "Improved Power Decoding of One-Point Hermitian Codes," in *International Workshop on Coding and Cryptography*, 2017, arXiv:1703.07982.
14. G.-L. Feng and K. K. Tzeng, "A Generalized Euclidean Algorithm for Multisequence Shift-Register Synthesis," *IEEE Transactions on Information Theory*, vol. 35, no. 3, pp. 584–594, 1989.
15. J. S. R. Nielsen, "Generalised Multi-sequence Shift-Register Synthesis using Module Minimisation," in *IEEE International Symposium on Information Theory*, 2013, pp. 882–886. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6620353
16. B. Beckermann and G. Labahn, "A Uniform Approach for the Fast Computation of Matrix-Type Padé Approximants," *SIAM Journal on Matrix Analysis and Applications*, vol. 15, no. 3, pp. 804–823, Jul. 1994. [Online]. Available: http://epubs.siam.org/doi/abs/10.1137/S0895479892230031
17. W. A. Stein *et al.*, "SageMath Software," http://www.sagemath.org.
18. Y. Wu, "New List Decoding Algorithms for Reed-Solomon and BCH Codes," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3611–3630, 2008.
19. V. Sidorenko, G. Schmidt, and M. Bossert, "Decoding Punctured Reed–Solomon Codes up to the Singleton Bound," in *International ITG Conference on Source and Channel Coding*, 2008, pp. 1–6.