Subspace Subcodes of Reed–Solomon Codes

Masayuki Hattori, *Member, IEEE,* Robert J. McEliece, *Fellow, IEEE,* and Gustave Solomon, *Fellow, IEEE*

***Abstract*— In this paper we introduce a class of nonlinear cyclic error-correcting codes, which we call *subspace subcodes of Reed–Solomon* (SSRS) codes. An SSRS code is a subset of a parent Reed–Solomon (RS) code consisting of the RS codewords whose components all lie in a fixed ν-dimensional vector subspace $\mathcal{S}$ of GF (2^m). SSRS codes are constructed using properties of the Galois field GF (2^m). They are not linear over the field GF (2^ν), which does not come into play, but rather are Abelian group codes over $\mathcal{S}$. However, they are linear over GF (2), and the symbol-wise cyclic shift of any codeword is also a codeword.**

Our main result is an explicit but complicated formula for the dimension of an SSRS code. It implies a simple lower bound, which gives the true value of the dimension for most, though not all, subspaces. We also prove several important duality properties. We present some numerical examples, which show, among other things, that 1) SSRS codes can have a higher dimension than comparable subfield subcodes of RS codes, so that even if GF (2^ν) is a subfield of GF (2^m), it may not be the best ν-dimensional subspace for constructing SSRS codes; and 2) many high-rate SSRS codes have larger dimension than any previously known code with the same values of n, d, and q, including algebraic-geometry codes. These examples suggest that high-rate SSRS codes are promising candidates to replace Reed–Solomon codes in high-performance transmission and storage systems.

***Index Terms*—Error-correcting codes, nonbinary codes, Reed–Solomon codes.**

I. Introduction

In this paper, we will introduce a new class of codes, which we call subspace subcodes of Reed–Solomon (SSRS) codes. Given an (n, k_0, d_0) Reed–Solomon (RS) code $\mathbb{C}$ over GF (2^m), and a ν-dimensional subspace $\mathcal{S}$ $(0 \leq \nu \leq m)$ of GF (2^m), the SSRS code $\mathbb{C}_\mathcal{S}$ is defined to be the set of codewords from $\mathbb{C}$ whose components all lie in $\mathcal{S}$. SSRS codes are constructed using properties of the Galois field GF (2^m). The field GF (2^ν) does not come into play in the construction, and so SSRS codes are not necessarily linear over the symbol field GF (2^ν). However, SSRS codes are Abelian group codes over the elementary Abelian group of order 2^ν, and are linear codes over GF (2), and the (symbol-wise) cyclic shift of any codeword is also a codeword.

SSRS codes can be viewed as a generalization of both subfield subcodes of RS codes [17], and trace-shortened RS codes [18]. Although the extension from subfield subcodes to subspace subcodes is quite natural, the only previous work on this subject we are aware of other than the preliminary work that led to this paper [9], [12], [18], [25]–[27], is the 1988 patent by Weng [28], the 1995 paper by Jensen [13], and the 1997 paper by Edel and Biebrauer [5].[1]

In [26] and [27], Solomon introduced a special class of SSRS codes. Several examples were given and a way of computing the binary dimension was illustrated. However, the construction was quite limited both by a required clever choice of polynomial which defines a primitive root for the underlying field, and by the choice of subspace. Thus a method of counting codewords was available only for some cases and an explicit formula was not given.

Soon afterwards, McEliece and Solomon extended the results of [26] and [27] to the class of "trace-shortened Reed–Solomon (TSRS) codes" [18]. A formula for the binary dimension of TSRS codes was given. TSRS codes are also a special class of SSRS codes. But again, the class of TSRS codes was restricted to a special classes of subspaces. With hindsight, we now see that it is much more natural to consider projecting a RS code onto an arbitrary subspace, rather than to one of a select few. However, there are a huge number of subspaces to choose from. Which ones are best? And how do SSRS codes compare to codes already known? We will attempt to answer these questions in this paper.

II. Overview

We begin in Section III by introducing a simple example which is essentially the same as the original construction given in [26]. Then, we will formally define an SSRS code as the set of codewords from a parent RS code whose symbols all lie in a particular vector subspace of the defining field. We will introduce some prerequisites and notation. Finally, we will give some immediate consequences of the definition of SSRS codes and list the problems we will solve.

In Section IV, we will give our main result, a dimension formula for SSRS codes (Theorem 4.4). We will give several

Manuscript received November 11, 1996; revised March 2, 1998. The work of M. Hattori was supported by the Sony Corporation and the California Institute of Technology. A portion of the work of R. McEliece was performed at the Jet Propulsion Laboratory, California Institute of Technology, under Contract to the National Aeronautics and Space Administration. This work was also supported by NSF under Grant NCR-9505975, and in part by the Sony Corporation. The work of G. Solomon was carried out in part at the Jet Propulsion Laboratory, California Institute of Technology, under Contract to the National Aeronautics and Space Administration. G. Solomon died on January 31, 1996, after the research in this paper had been completed. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Trondheim, Norway, 1994.

M. Hattori was with the Department of Electrical Engineering and the Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA 91125 USA. He is now with Sony Corporation Research Center, 6-7-35 Kitashinagawa, Shinagawa-ku, Tokyo 141, Japan.

R. J. McEliece is with the Department of Electrical Engineering and the Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA 91125 USA.

G. Solomon (deceased) was with the Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA 91125 USA.

Publisher Item Identifier S 0018-9448(98)04743-9.

[1] After this paper was completed, Philippe Piret pointed out to us that a result equivalent to our Corollary 4.9, below, appeared as Theorem 3.1 in the 1984 paper of Couvreur and Piret [4].

examples illustrating the theorem. We will see that, in some cases, there exists an SSRS code which has a larger number of codewords than the subfield subcode derived from the same parent code. We will also show that our formula implies a lower bound for the dimension of SSRS codes and, moreover, the TSRS codes proposed in [18], achieve this lower bound in all cases.

In Section V, we will derive some "elementary" bounds on the dimension of SSRS codes, and compare them to our main result (Theorem 4.4), and to a recent result of Jensen [13].

In Section VI, we discuss a "duality" among subspaces. We will start with a discussion of the relationship between our dimension formula for SSRS codes and a generator (parity-check) matrix for maximum-disstance separable (MDS) codes. We will see that, among all ν-dimensional subspaces, most are *ordinary*, meaning that the corresponding SSRS codes always achieve the lower bound on the dimension regardless of the choice of the parent code. However, we shall also see that there exist a few *exceptional* subspaces, which can produce SSRS codes whose dimension exceeds the lower bound.

Then we will focus on the relationship between the dimension of an SSRS code and subspace duality. Trace-dual subspaces are closely related to each other, and the dimension of the corresponding SSRS codes are also related. We will prove this relationship using a curious result we call the "*defect theorem*."

In Section VII, we discuss the performance of SSRS codes in terms of codelength, dimension, and designed minimum distance. We will give several specific examples. Then, we will compare the performance of SSRS codes to that of algebraic-geometry (AG) codes. We will see that, in some cases, SSRS codes are preferable to AG codes. Finally, we will exhibit an infinite sequence of SSRS codes which provides counterexamples to a conjecture about optimal quasi-MDS codes.

III. Construction

In this section, we will give the formal definition for subspace subcodes of Reed–Solomon (SSRS) codes. This definition generalizes both the nonlinear nonbinary codes [26] and the trace-shortened Reed–Solomon (TSRS) codes [18]. We start with a simple example, which illustrates the underlying idea, originated by Solomon [26], and leads to the general construction.

A. Illustrative Example

Let $\mathbb{C}$ be the $(15, 9, 7)$ RS code over $\mathbb{F} = \mathrm{GF}(2^4)$ with parity-check polynomial

$$h(x) = \prod_{i=1}^{9}(x - \alpha^i) \tag{1}$$

where α is a primitive root of $\mathbb{F}$ satisfying $\alpha^4 = \alpha + 1$. Let $\boldsymbol{C} = (C_0, C_1, \cdots, C_{14})$ be a codeword from $\mathbb{C}$. Suppose we expand each component of $\boldsymbol{C}$ into a binary 4-vector with respect to the basis $\{1, \alpha, \alpha^2, \alpha^3\}$. Consider now the set of codewords from $\mathbb{C}$ with the property that the fourth binary component of each C_i, i.e., the component corresponding to the basis element α^3, is zero, for all $i = 0, 1, \cdots, 14$. Alternatively, this is the set of codewords for which each C_i lies in the subspace S of $\mathrm{GF}(16)$ spanned by $\{1, \alpha, \alpha^2\}$. We call this subset of codewords from $\mathbb{C}$ a *subspace subcode* and denote it by $\mathbb{C}_{\mathcal{S}}$.

If we use this code in practice, we do not need to transmit the fourth binary component of each C_i, since these are guaranteed to be zero. So we can regard $\mathbb{C}_{\mathcal{S}}$ as a code of length 15 over the set of binary 3-tuples.

This construction is similar to the construction of a subfield subcode of a parent RS code. However, the essential difference is that the vector space spanned by $\{1, \alpha, \alpha^2\}$ is not a subfield. Indeed, since $\mathrm{GF}(2^3)$ is not a subfield of $\mathrm{GF}(2^4)$, there is no corresponding subfield subcode in this case. The minimum distance of $\mathbb{C}_{\mathcal{S}}$ is at least 7, because the minimum distance of the subcode cannot be less than its parent RS code. We say that the *designed* minimum distance is 7. Therefore, this construction gives us a nonlinear cyclic code of length 15 over 3-tuples with distance 7^+, where the notation 7^+ means that the designed minimum distance is 7. In general, the true minimum distance can be greater than the designed minimum distance, but an ordinary decoder can only decode up to designed minimum distance, and in any case at present we know very little about the true minimum distance.[2]

For us, the key question is, how many codewords are contained in $\mathbb{C}_{\mathcal{S}}$? We will see from Theorem 4.4, below, that there are 2^{22} codewords in $\mathbb{C}_{\mathcal{S}}$. If we define the "pseudo dimension" as $\log_{|\mathcal{S}|} |\mathbb{C}_{\mathcal{S}}|$, we find that this code has pseudo-dimension $22/3 = 7\frac{1}{3}$. So, this SSRS code is a $(15, 7\frac{1}{3}, 7^+)$ code over the set of binary triples. We have paid a price—the dimension has been reduced by $1\frac{2}{3}$ in order to reduce the symbol set size from 16 to 8.[3]

Another possible construction for a code of length 15 over binary 3-tuples, is a shortened subfield subcode. In fact, there is a $(63, 52, 7)$ subfield subcode over $\mathrm{GF}(2^3)$, so by the general shortening argument, we obtain a $(15, 4, 7^+)$ code, which has only $2^{4\cdot 3} = 2^{12}$ codewords. On the other hand, $\mathbb{C}_{\mathcal{S}}$ contains 2^{22} codewords. So, if we need a code of length 15 over binary 3-tuples, a shortened subfield subcode is not nearly as attractive as the SSRS code.

As another comparison, we consider an algebraic-geometry (AG) code. We do not go into details, but there is an elliptic curve of genus 1, which produces a $(14, 7, 7)$ code over $\mathrm{GF}(2^3)$. But $\mathbb{C}_{\mathcal{S}}$ contains twice as many codewords and is one symbol longer.

B. Formal Definition

We start from a field $\mathbb{F} = \mathrm{GF}(2^m)$, a positive integer n which is a divisor of $2^m - 1$, and a primitive nth root of unity in $\mathbb{F}$, say α. Let J be a set of k_0 integers whose elements, chosen from $\{0, 1, \cdots, n-1\}$, form an arithmetic progression[4] modulo n whose increment is relatively prime to n.

[2] In fact, for our example, the true minimum distance is 7.

[3] We shall see below (Section VII-A) that there is in fact an SSRS code over an 8-symbol alphabet with parameters $(15, 7\frac{2}{3}, 7^+)$, obtained by starting with the nonstandard parity-check polynomial $h(x) = \Pi_{i=2}^{10}(x - \alpha^i)$.

[4] Our discussion can easily be extended to an arbitrary integer set J. However, we focus on the consecutive integer sets, i.e., Reed–Solomon codes, because in the more general case, we have no estimate of the minimum distance, and no good decoding algorithm for the parent code.

We then define the code $\mathbb{C}(J)$ to be an (n, k_0, d_0) cyclic RS code over $\mathbb{F}$, where $d_0 = n - k_0 + 1$, with parity-check polynomial $h(x)$ and generator polynomial $g(x)$ as follows:

$$h(x) = \prod_{j \in J} (x - \alpha^j) \tag{2}$$

$$g(x) = \prod_{j \in \overline{J}} (x - \alpha^j). \tag{3}$$

Equivalently, using a Mattson–Solomon polynomial $P(x)$, $\mathbb{C}$ consists of all vectors $\boldsymbol{C} = (C_0, C_1, \cdots, C_{n-1})$ of the form

$$C_i = P(\alpha^i), \qquad i = 0, 1, \cdots, n-1 \tag{4}$$

$$P(x) = \sum_{j \in J} c_j x^j, \qquad \text{for all } p_j \in \mathbb{F} \tag{5}$$

where (c_j), $j \in J$ is an arbitrary set of elements from $\mathbb{F}$, indexed by J.

Since $\mathbb{C}$ is an RS code, the minimum distance of $\mathbb{C}$ is $d_0 = n - k_0 + 1$. Here is the formal definition.

3.1. Definition: Let $\mathbb{C}$ be an (n, k_0, d_0) cyclic RS code over $\mathrm{GF}(2^m)$. Let $\mathcal{S}$ be a ν-dimensional vector subspace of $\mathrm{GF}(2^m)$, where $0 \leq \nu \leq m$. The *subspace subcode* $\mathbb{C}_\mathcal{S}$ associated with $\mathbb{C}$ and $\mathcal{S}$ is defined to be the set of codewords from $\mathbb{C}$ whose components all lie in $\mathcal{S}$. □

Thus an SSRS code $\mathbb{C}_\mathcal{S}$ is a code of length n over the 2^ν-letter alphabet $\mathcal{S}$. The alphabet $\mathcal{S}$ is a vector space, but not necessarily a field. However, $\mathcal{S}$ is an *elementary Abelian group* [23] under addition, and the sum of any two codewords is also a codeword for $\mathbb{C}_\mathcal{S}$. Moreover, since the parent code $\mathbb{C}$ is cyclic, any symbol-wise cyclic shift of a codeword is also a codeword. Therefore, an SSRS code $\mathbb{C}_\mathcal{S}$ is a cyclic group code over the elementary Abelian group $\mathcal{S}$.

Note that if $\nu | m$ the parent field $\mathrm{GF}(2^m)$ contains a subfield $\mathrm{GF}(2^\nu)$, which is a ν-dimensional subspace. Thus the class of SSRS codes includes subfield subcodes as a special case.

Moreover, "trace-shortened" Reed–Solomon (TSRS) codes [18] are also a special case of SSRS codes, in which the subspace $\mathcal{S}$ is the trace-dual of a subspace with a basis of the form

$$\mathfrak{G}_\mathcal{S} = \{1, \gamma, \gamma^2, \cdots, \gamma^{\mu-1}\} \tag{6}$$

where γ is a primitive root of $\mathrm{GF}(2^m)$.

We denote the symbol-wise minimum distance of the code $\mathbb{C}_\mathcal{S}$ by $d_\mathcal{S}$. Since every codeword in $\mathbb{C}_\mathcal{S}$ is also a codeword in the parent code $\mathbb{C}$, and since $\mathbb{C}$ is an RS code, for which the true minimum distance is $d_0 = n - k_0 + 1$, it follows that the true minimum distance $d_\mathcal{S}$ of $\mathbb{C}_\mathcal{S}$ satisfies

$$d_\mathcal{S} \geq d_0. \tag{7}$$

We call d_0 the *designed* minimum distance for the SSRS code $\mathbb{C}_\mathcal{S}$.

An SSRS code over the ν-dimensional subspace $\mathcal{S}$ is a subgroup of the group $\mathcal{S}^n$, and thus the order of the code need not be a power of 2^ν. However, since the sum of any two codewords from $\mathbb{C}_\mathcal{S}$ is another codeword, $\mathbb{C}_\mathcal{S}$ a linear code over $\mathrm{GF}(2)$, and so the order must be a power of 2. Let us denote the $\mathrm{GF}(2)$-dimension of $\mathbb{C}_\mathcal{S}$ by $K(\mathbb{C}, \mathcal{S})$. If $|\mathbb{C}_\mathcal{S}|$ denotes the number of codewords in $\mathbb{C}_\mathcal{S}$, then

$$|\mathbb{C}_\mathcal{S}| = 2^{K(\mathbb{C}, \mathcal{S})}. \tag{8}$$

We call $K(\mathbb{C}, \mathcal{S})$ the *binary* dimension of $\mathbb{C}_\mathcal{S}$. Similarly, we define the *pseudo-dimension* (*over* S) for $\mathbb{C}_\mathcal{S}$ as

$$k(\mathbb{C}, \mathcal{S}) = \frac{1}{\nu} K(\mathbb{C}, \mathcal{S}) = \log_{|\mathcal{S}|} |\mathbb{C}_\mathcal{S}|. \tag{9}$$

Note that $k(\mathbb{C}, \mathcal{S})$ need not to be an integer. The most important theoretical problem addressed in this paper is the calculation of the exact dimension of $\mathbb{C}_\mathcal{S}$, which is equivalent to counting the number of codewords in $\mathbb{C}_\mathcal{S}$. We give the solution to this problem in the next section.

Decoding SSRS codes is quite easy. Since $\mathbb{C}_\mathcal{S}$ is a subcode of the parent RS code, we can use the existing sophisticated algorithms for RS codes to decode SSRS codes up to the designed minimum distance. The computational complexity of the most efficient decoding algorithm for RS codes is, according to Blahut [3], "greater than $O(n \log n)$ by the thinnest of margins."

On the other hand, the encoding of SSRS codes is not as easy as that of RS codes. Of course, since an SSRS code $\mathbb{C}_\mathcal{S}$ is a binary linear code, one can always find a systematic binary generator matrix, and use it for encoding.[5] However, such an encoding is not entirely satisfactory, since $\mathbb{C}_\mathcal{S}$ is most naturally viewed as a code over the nonbinary alphabet $\mathcal{S}$, not as a binary code. What is wanted, ideally, is a systematic encoder that works directly with symbols from $\mathcal{S}$. However, as Solomon showed in [26], a systematic encoding is not always possible, even when the pseudodimension is an integer. In a forthcoming paper [11], we will discuss the conditions under which a systematic encoder for an SSRS code can be constructed. The encoding problem for SSRS codes is also discussed in [12], [13], and [15].

IV. Dimension

In this section, we will derive an explicit formula for the dimension of a subspace subcode of a Reed–Solomon code. Moreover, we will show that, in some cases, there exists an SSRS code, whose dimension is higher than the subfield subcode with the same codelength n, designed distance d_0, and symbol size $q = 2^\nu$. We will begin by briefly reviewing some known facts about finite fields. Then we will state and prove the dimension theorem using some lemmas which were first introduced and proved in [18]. The main theorem is followed by a corollary which gives a simple lower bound on the dimension of SSRS codes, which is attained by the TSRS codes introduced in [18], and many others. Finally, we will give several examples which shed light on the importance of SSRS codes.

[5] Indeed, since the number of rows in such a matrix is the binary dimension of the SSRS code, this is also one way to compute the binary dimension of an arbitrary SSRS code. Under some circumstances, this approach could be computationally superior to our main result, Theorem 4.4, though it provides no general insight.

A. Preparation

We begin by introducing the *trace* operation (e.g., [19]), and the trace-dual subspace associated with a subspace $\mathcal{S}$ of $\mathrm{GF}(2^m)$.

Let ξ be an element from $\mathrm{GF}(2^m)$. We denote by $\mathrm{Tr}_1^m(\xi)$, the trace of ξ from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2^1)$, i.e., the $\mathrm{GF}(2)$-linear mapping from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2^1)$, given by

$$\mathrm{Tr}_1^m(\xi) = \xi + \xi^2 + \xi^4 + \cdots + \xi^{2^{m-1}}. \tag{10}$$

Similarly, if d is a divisor of m, $\mathrm{Tr}_d^m(\xi)$ denotes the trace of ξ from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2^d)$, i.e., the $\mathrm{GF}(2^d)$-linear mapping from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2^d)$, given by

$$\mathrm{Tr}_d^m(\xi) = \xi + \xi^{2^d} + \xi^{2^{2d}} + \cdots + \xi^{2^{(f-1)d}} \tag{11}$$

where $f = m/d$.

Next, we define a *basis* for $\mathrm{GF}(2^m)$ to be a set of m linearly independent elements from $\mathrm{GF}(2^m)$ which spans whole space. Let us denote a typical basis by

$$\mathfrak{S} = \{\sigma_0, \sigma_1, \cdots, \sigma_{m-1}\}.$$

A *dual basis* $\mathfrak{T}$ for $\mathfrak{S}$ is defined to be a set of linearly independent elements which are orthogonal to $\mathfrak{S}$, with respect to the trace operator, i.e.,

$$\mathfrak{T} = \{\tau_0, \tau_1, \cdots, \tau_{m-1}\},$$
$$\mathrm{Tr}_1^m(\sigma_i \tau_j) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j. \end{cases} \tag{12}$$

It is known (e.g., [16], [19]) that a dual basis always exists and is unique.

Note also that if an element ζ from $\mathrm{GF}(2^m)$ is expanded with respect to the basis $\mathfrak{S}$ as

$$\zeta = \sum_{j=0}^{m-1} z_j \sigma_j, \qquad z_j \in \mathrm{GF}(2) \tag{13}$$

then, by (12), its binary components (z_j), $j = 0, 1, \cdots, m-1$ are given by

$$z_j = \mathrm{Tr}_1^m(\zeta \tau_j), \qquad \text{for } j = 0, 1, \cdots, m-1. \tag{14}$$

Now, we consider a ν-dimensional vector subspace $\mathcal{S}$ of $\mathrm{GF}(2^m)$, where $0 \leq \nu \leq m$. Suppose $\mathcal{S}$ is spanned by basis

$$\mathfrak{B}_{\mathcal{S}} = \{\sigma_0, \sigma_1, \cdots, \sigma_{\nu-1}\} \tag{15}$$

consisting of ν linearly independent elements. The *trace dual* subspace $\mathcal{S}^{\perp}$ associated with $\mathcal{S}$ is defined to be the μ-dimensional subspace of $\mathrm{GF}(2^m)$ with $\mu = m - \nu$ satisfying

$$\mathrm{Tr}_1^m(xy) = 0 \quad \begin{cases} \text{for all } x \in \mathcal{S} \\ \text{for all } y \in \mathcal{S}^{\perp}. \end{cases} \tag{16}$$

It follows from the fact that a dual basis of a complete basis always exists, that a trace-dual subspace of any subspace also exists. However, it is not unique in general.

B. Main Theorem

First, we define the *modulo n cyclotomic cosets*. Let n be an odd positive integer, and let m be the least integer such that n divides $2^m - 1$. If i and j are integers in the range $0 \leq i \leq n-1$, and if $2^s i \equiv j \pmod n$ for some integer s, we say that i and j are *conjugate modulo n*. It is easy to see that conjugation modulo n is an equivalence relation on the set $\{0, 1, \cdots, n-1\}$, which is therefore partitioned into a number of disjoint equivalent classes, which are called the *modulo n cyclotomic cosets*. Alternatively, the cyclotomic coset containing j, which we will denote by Ω_j, can be described explicitly as the set $\{j, 2j, \cdots, 2^{d-1}j\}$, where d is the least positive integer such that $2^d j \equiv j \pmod n$. The integer d is called the *degree* of j, written $d = \deg(j)$. In what follows, we will denote the cardinality of Ω_j by d_j. It is easy to see that every element of Ω_j has degree d_j, and that d_j is a divisor of m. We therefore define $f_j = m/d_j$. Finally, we denote by I_n the set consisting of the smallest integers in each cyclotomic coset.

4.1. Example: Let $n = 15$. A short calculation shows that there are five cyclotomic cosets modulo 15; indeed, we have $I_{15} = \{0, 1, 3, 5, 7\}$, and

$$\begin{array}{lll} \Omega_0 = (0) & d_0 = 1 & f_0 = 4 \\ \Omega_1 = (1, 2, 4, 8) & d_1 = 4 & f_1 = 1 \\ \Omega_3 = (3, 6, 12, 9) & d_3 = 4 & f_3 = 1 \\ \Omega_5 = (5, 10) & d_5 = 2 & f_5 = 2 \\ \Omega_7 = (7, 14, 13, 11) & d_7 = 4 & f_7 = 1. \end{array}$$

□

We next define the *modulo n cyclotomic array*. The cyclotomic array is the $|I_n| \times m$ array of integers whose jth row corresponds to the jth cyclotomic coset. However, the integers in a cyclotomic coset whose degree d_j is not equal to m are *repeated* $m/d_j = f_j$ times. More precisely, the nth *cyclotomic array* is the $|I_n| \times m$ matrix of integers in $\{0, 1, \cdots, n-1\}$, whose (j, i)th entry is $j2^i \pmod n$. Here $j \in I_n$ and $i \in \{0, 1, \cdots, m-1\}$, where m is the least integer such that $2^m \equiv 1 \pmod n$.

4.2. Example: Let $n = 15$, as in Example 4.1. Then the corresponding cyclotomic array is as follows:

	index i				
	0	1	2	3	
$j = 0$	0	0	0	0	$d_0 = 1$ $f_0 = 4$
$j = 1$	1	2	4	8	$d_1 = 4$ $f_1 = 1$
$j = 3$	3	6	12	9	$d_3 = 4$ $f_3 = 1$
$j = 5$	5	10	5	10	$d_5 = 2$ $f_5 = 2$
$j = 7$	7	14	13	11	$d_7 = 4$ $f_7 = 1$

□

As a final preparation for stating our formula for the exact binary dimension for an SSRS code, we define a family of *cyclotomic matrices* $\Gamma_j(\mathbb{C}_{\mathcal{S}})$, for $j \in J$, where J is the subset of $\{0, \cdots, n-1\}$ which defines the parent code $\mathcal{C}$ (see (2)–(5)).

	index i								
	0	1	2	3					
$j=0$	**0**	**0**	**0**	**0**	$d_0=1$	$f_0=4$	$e_0=1$	$A_0=\{0,1,2,3\}$	$a_0=4$
$j=1$	**1**	**2**	**4**	**8**	$d_1=4$	$f_1=1$	$e_1=4$	$A_1=\{0,1,2,3\}$	$a_1=4$
$j=3$	**3**	**6**	12	**9**	$d_3=4$	$f_3=1$	$e_3=3$	$A_3=\{0,1,3\}$	$a_3=3$
$j=5$	**5**	10	**5**	10	$d_5=2$	$f_5=2$	$e_5=1$	$A_5=\{0,2\}$	$a_5=2$
$j=7$	**7**	14	13	11	$d_7=4$	$f_7=1$	$e_7=1$	$A_7=\{0\}$	$a_7=1$

Given the set J, for each $j \in I_n$, we define $J_j = J \cap \Omega_j$. Let $e_j = |J_j|$ be the number integers in J_j. We define the index set A_j to be the set of integers i, which satisfy $0 \le i \le m-1$ and $(j \cdot 2^i \bmod n) \in J_j$. With this definition, it is apparent that $|A_j| = a_j = e_j f_j$. For convenience, we order the elements in A_j and denote it as follows:

$$A_j = \{i_0, i_1, \cdots, i_{a_j-1}\}, \qquad i_0 < i_1 < \cdots < i_{a_j-1}. \quad (17)$$

The jth cyclotomic matrix Γ_j is defined as the following $\mu \times a_j$ matrix:

$$\Gamma_j = \begin{bmatrix} \gamma_0^{2^{m-i_0}} & \gamma_0^{2^{m-i_1}} & \cdots & \gamma_0^{2^{m-i_{a_j-1}}} \\ \gamma_1^{2^{m-i_0}} & \gamma_1^{2^{m-i_1}} & \cdots & \gamma_1^{2^{m-i_{a_j-1}}} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_{\mu-1}^{2^{m-i_0}} & \gamma_{\mu-1}^{2^{m-i_1}} & \cdots & \gamma_{\mu-1}^{2^{m-i_{a_j-1}}} \end{bmatrix}. \quad (18)$$

In (18), $\{\gamma_0, \gamma_1, \cdots, \gamma_{\mu-1}\}$ is a trace-dual basis for $\mathcal{S}$, where $\mu = n - \nu$.

4.3. Example: Let $n = 15, m = 4$, and $J = \{0,1,2,3,4,5,6,7,8,9\}$. Since $I_{15} = \{0,1,3,5,7\}$, the cyclotomic array is as shown at the top of this page.

Suppose $\nu = 2$, so that $\mu = m - \nu = 2$. Let the basis of $\mathcal{S}^\perp$ be $\{\gamma_0, \gamma_1\}$. Since $A_0 = \{0,1,2,3\}$, Γ_0 is the following 2×4 matrix:

$$\Gamma_0 = \begin{bmatrix} \gamma_0^{2^0} & \gamma_0^{2^3} & \gamma_0^{2^2} & \gamma_0^{2^1} \\ \gamma_1^{2^0} & \gamma_1^{2^3} & \gamma_1^{2^2} & \gamma_1^{2^1} \end{bmatrix}.$$

Similarly, we see that $\Gamma_1 = \Gamma_0$. The cyclotomic matrices for $j = 3, 5, 7$ are as follows:

$$\Gamma_3 = \begin{bmatrix} \gamma_0^{2^0} & \gamma_0^{2^3} & \gamma_0^{2^1} \\ \gamma_1^{2^0} & \gamma_1^{2^3} & \gamma_1^{2^1} \end{bmatrix}$$

$$\Gamma_5 = \begin{bmatrix} \gamma_0^{2^0} & \gamma_0^{2^2} \\ \gamma_1^{2^0} & \gamma_1^{2^2} \end{bmatrix}$$

$$\Gamma_7 = \begin{bmatrix} \gamma_0^{2^0} \\ \gamma_1^{2^0} \end{bmatrix}. \qquad \square$$

Now we are prepared to state our main theorem, which gives a method for computing the exact binary dimension of the SSRS code $\mathbb{C}_\mathcal{S}$ derived from the (n, k_0) RS code $\mathbb{C}$ over GF(2^m).[6]

[6] Berlekamp [2, Ch. 12] has made a deep study of the dimension of Bose–Chaudhuri–Hocquengham (BCH) codes, which are SSRS codes with $\nu = 1$. The results in this paper, however, when specialized to the case $\nu = 1$, are merely equivalent to Berlekamp's relatively trivial starting point, [2, Lemma 12.11].

4.4. Theorem (Dimensions of SSRS Codes): Given an (n, k_0) parent cyclic RS code $\mathbb{C}$ over GF(2^m) with $n | 2^m - 1$ defined by the integer set J. Let $\mathcal{S}$ be a ν-dimensional subspace of GF(2^m) spanned by the basis $\{\beta_0, \beta_1, \cdots, \beta_{\nu-1}\}$. Let $\mathcal{S}^\perp$ be the μ-dimensional trace-dual subspace of $\mathcal{S}$ spanned by the basis $\{\gamma_0, \gamma_1, \cdots, \gamma_{\mu-1}\}$, where $\mu = m - \nu$. Further, let r_j be the rank of jth cyclotomic matrix Γ_j. The binary dimension $K(\mathbb{C}, \mathcal{S})$ of SSRS code $\mathbb{C}_\mathcal{S}$ is given by the following formula:

$$K(\mathbb{C}, \mathcal{S}) = \sum_{j \in I_n} d_j (a_j - r_j) \quad (19)$$

$$= \sum_{j \in I_n} (m e_j - r_j d_j). \quad (20)$$

C. Proof of Dimension Theorem

In order to prove Theorem 4.4, we will need three lemmas that were first presented in [18]. We will state these results here without proof.

Let $P(x)$ be a polynomial over GF(2^m) of degree $n-1$, where $n | 2^m - 1$:

$$P(x) = \sum_{j=0}^{n-1} P_j x^j, \qquad P_j \in \text{GF}(2^m). \quad (21)$$

Now we define the polynomial $\mathcal{P}(x)$ as follows:

$$\mathcal{P}(x) = P(x) + P(x)^2 + \cdots + P(x)^{2^{m-1}} \pmod{x^n - 1} \quad (22)$$

$$= \sum_{j=0}^{n-1} \mathcal{P}_j x^j. \quad (23)$$

4.5. Lemma: Let $P(x)$ be as defined in (21), $\mathcal{P}(x)$ as defined in (22) and (23), and let α be a primitive nth root of unity in GF(2^m). Then $\text{Tr}_1^m(P(x)) = 0$ for all $x \in \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ if and only if $\mathcal{P}_j = 0$ for all $j = 0, 1, \cdots, n-1$. $\square$

4.6. Lemma: For $j \in \{0, 1, 2, \cdots, n-1\}$, if $d = \deg(j)$, then

$$\mathcal{P}_j = \sum_{i=0}^{m-1} P_{j \cdot 2^i}^{2^{m-i}} \quad (24)$$

where all subscripts and superscripts are modulo n. $\square$

4.7. Lemma: If j_1 and j_2 are conjugate modulo n, then $\mathcal{P}_{j_1}$ and $\mathcal{P}_{j_2}$ are conjugates in GF(2^m). More precisely, if j has degree d, and if $s \in \{0, 1, \cdots, d-1\}$, then

$$\mathcal{P}_{j\cdot 2^s} = \mathcal{P}_j^{2^s} \tag{25}$$

where all superscripts and subscripts are modulo n. □

If $S = \{\beta_0, \cdots, \beta_{\nu-1}\}$, it is always possible to find a basis for GF(2^m) of the form

$$\mathfrak{B} = \{\beta_0, \beta_1, \cdots, \beta_{\nu-1}, \beta_\nu, \cdots, \beta_{m-1}\}.$$

If we consider the binary expansion of the codeword $\mathbb{C}$ into m-tuples with respect to this complete basis, Definition 3.1 for SSRS codes amounts to saying that the SSRS code is the set of codewords from $\mathbb{C}$ whose binary components corresponding to $\{\beta_\nu, \cdots, \beta_{m-1}\}$ are all zero. So, if we denote a trace-dual basis for $\mathfrak{B}_\mathcal{S}$ by $\mathfrak{G}_\mathcal{S}$ and use (14), we can restate the definition of $\mathbb{C}_\mathcal{S}$ as follows. The SSRS code is the set of codewords $\boldsymbol{C} = (C_0, C_1, \cdots, C_{n-1})$ from $\mathbb{C}$ satisfying

$$\mathrm{Tr}_1^m(\gamma_h C_i) = 0, \qquad \begin{cases} \text{for all } h = \nu, \nu+1, \cdots, m-1 \\ \text{for all } i = 0, 1, \cdots, n-1. \end{cases} \tag{26}$$

If we combine this restatement of the definition with the MS polynomials defined in (5), we obtain the following equivalent condition:

$$\mathrm{Tr}_1^m\left(\sum_{j\in J}(\gamma_h c_j x^j)\right) = 0, \qquad \begin{cases} \text{for all } h = 0, 1, 2, \cdots, \mu-1 \\ \text{for all } x \in \{1, \alpha^{-1}, \alpha^{-2}, \cdots, \alpha^{-(n-1)}\}. \end{cases} \tag{27}$$

Next, we define the polynomial $P_h(x)$ for $h = 0, 1, \cdots, \mu-1$ as

$$P_h(x) = \sum_{j\in J} \gamma_h c_j x^j. \tag{28}$$

Then, as in (22), we define the polynomial $\mathcal{P}_h(x)$ as

$$\mathcal{P}_h(x) = \mathrm{Tr}_1^m(P_h(x)) \pmod{x^n - 1}. \tag{29}$$

Thus condition (27) holds if and only if

$$\mathcal{P}_h(x) = 0, \qquad \text{for all } x \in \{1, \alpha, \cdots, \alpha^{n-1}\}. \tag{30}$$

By Lemma 4.5, this is true if and only if

$$\mathcal{P}_{h,j} = 0, \qquad \begin{cases} \text{for all } h = 0, 1, \cdots, \mu-1 \\ \text{for all } j \in J \end{cases} \tag{31}$$

where $\mathcal{P}_{h,j}$ is the coefficient of x^j in the polynomial $\mathcal{P}(x)$. By Lemma 4.6, the coefficient $\mathcal{P}_{h,j}$ is given by the formula

$$\mathcal{P}_{h,j} = \sum_{i\in A_j} \gamma_h^{2^{m-i}} c_{j\cdot 2^i}^{2^{m-i}} \tag{32}$$

where A_j is the index set of $J_j = \Omega_j \cap J$ defined in Section IV-B.

In summary, a set $(c_j), j \in J$ of elements from GF(2^m) corresponds to a codeword in $\mathbb{C}_\mathcal{S}$ if and only if $\mathcal{P}_{h,j} = 0$, for all $h = 0, 1, \cdots, \mu-1$ and all $j \in J$. However, by Lemma 4.7, if $j_1, j_2 \in J$ are conjugates, i.e., both lie in the same cyclotomic coset, $\mathcal{P}_{h,j_1}$ and $\mathcal{P}_{h,j_2}$ are also conjugates. So, if $\mathcal{P}_{h,j} = 0$ for one element j of a given cyclotomic coset, then the coefficients of all other elements of the same coset must be zero. Therefore, when we count the number of coefficient sets (c_j) such that $\mathcal{P}_{h,j} = 0$ for all j, it is sufficient to restrict j to lie in the set I_n, consisting of the least element of each cyclotomic coset.

Therefore, counting the number of sets $(c_j), j \in J$ corresponding to codewords in the SSRS code $\mathbb{C}_\mathcal{S}$ is equivalent to counting the number of solutions to the set of equations of the form

$$\sum_{i\in A_j} \gamma_h^{2^{m-i}} c_{j\cdot 2^i}^{2^{m-i}} = 0, \qquad \text{for } h = 0, 1, \cdots, \mu-1 \tag{33}$$

for each $j \in I_n$. Let N_j denote the number of solutions to the set of equations defined by (33). Since the set of equations in (33) involves only variables c_l's, where all l's are in the jth cyclotomic coset, we can compute the number of solutions to the set of equations corresponding to each cyclotomic coset independently. It follows that $N_\mathcal{S}$, the total number of codewords in the code $\mathbb{C}_\mathcal{S}$, is given by

$$N_\mathcal{S} = \prod_{j\in I_n} N_j. \tag{34}$$

Theorem 4.4 will be proven if we can show that N_j, the number of solutions to the set of equations (33) for the jth cyclotomic coset, is exactly

$$N_j = 2^{me_j - r_j d_j} = 2^{d_j(a_j - r_j)}. \tag{35}$$

Once (35) is proved, it immediately follows that the binary dimension of $\mathbb{C}_\mathcal{S}$ is

$$K(\mathbb{C}, \mathcal{S}) = \sum_{j\in I_n} K_j \tag{36}$$

where $K_j = me_j - r_j d_j$.

It is easy to see that the set of equations (33) can be written in matrix form by using the jth cyclotomic matrix, defined in (18), as follows:

$$\Gamma_j \boldsymbol{c}^T = \mathbf{0}^T \tag{37}$$

where

$$\boldsymbol{c} = \left[c_{j\cdot 2^{i_0}}^{2^{m-i_0}}, c_{j\cdot 2^{i_1}}^{2^{m-i_1}}, \cdots, c_{j\cdot 2^{i_{a_j-1}}}^{2^{m-i_{a_j-1}}}\right]. \tag{38}$$

We recall that the matrix Γ_j is a $\mu \times a_j$ matrix whose (h, l)th entry is $\gamma_h^{m-i_l}$. There are e_j distinct variables in the vector $\boldsymbol{c}$, so each variable appears exactly f_j times as a component of $\boldsymbol{c}$, if $d \neq m$.

To complete the proof, we consider the cases $d = m$ and $d \neq m$ separately. We begin with the easier case $d = m$. In the rest of the proof, we will omit the subscript j and simplify the notation by using a, d, e, f, and r instead of a_j, d_j, e_j, f_j, and r_j, respectively. Since we will focus only on the jth cyclotomic coset, no confusion should occur.

Case I. $d = m$*:* In (38), all components $c_{j\cdot 2^i}^{2^{m-i}}$ $(i \in A_j)$ are distinct. We now define the variable x_l as

$$x_l = c_{j\cdot 2^{i_l}}^{2^{m-i_l}}, \qquad l = 0, 1, \cdots, e-1. \tag{39}$$

Since the mapping $\xi \to \xi^{2^{m-i_l}}$ is one-to-one, the $c_{j\cdot 2^{i_l}}$'s can be uniquely recovered from the x_l's. Thus the binary dimension K_j is the GF(2)-dimension of the solution space of the set of equations

$$\Gamma_j \boldsymbol{x}^T = \boldsymbol{0}^T \tag{40}$$

where

$$\boldsymbol{x} = [x_0, x_1, \cdots, x_{e-1}]. \tag{41}$$

It is apparent that the set of solutions to (40) is a vector space over GF(2^m). But since (40) represents a set of simultaneous linear equations, the GF(2^m)-dimension of the set of solutions to (40) is the nullity of the matrix Γ_j, i.e., $e-r$, where e is the number of variables and r is the rank of Γ_j. Thus the number of solutions to (40) is $(2^m)^{e-r} = 2^{me-dr} = 2^{d(a-r)}$. In other words, the contribution of this cyclotomic coset to the binary dimension of $\mathbb{C}_{\mathcal{S}}$ is exactly $me - dr = d(a-r)$.

Case II. $d \neq m$*:* In this case, there are only e distinct coefficients in $\boldsymbol{c}$ and each coefficient appears exactly f times, raised to different powers. This is because if the index i is in A_j, then $i+d, i+2d, \cdots, i+(f-1)d$ are also in A_j. Therefore, (37) is no longer a set of simultaneous linear equations, and so we cannot derive the number of solutions directly from (37). However, since we have assumed that the indices $i_l, l = 0, 1, \cdots, a-1$ in (17) are in increasing order, it follows that the first e components of $\boldsymbol{c}$ are distinct from each other and then repeated f times in the same order, as follows:

$$\begin{aligned}\boldsymbol{c} = [&\overbrace{c_{j\cdot 2^{i_0}}^{2^{m-i_0}}, c_{j\cdot 2^{i_1}}^{2^{m-i_1}}, \cdots, c_{j\cdot 2^{i_{e-1}}}^{2^{m-i_{e-1}}}}^{e}, \\ &\overbrace{c_{j\cdot 2^{i_0}}^{2^{m-i_0-d}}, c_{j\cdot 2^{i_1}}^{2^{m-i_1-d}}, \cdots, c_{j\cdot 2^{i_{e-1}}}^{2^{m-i_{e-1}-d}}}^{e}, \cdots, \\ &\overbrace{c_{j\cdot 2^{i_0}}^{2^{m-i_0-(f-1)d}}, c_{j\cdot 2^{i_1}}^{2^{m-i_1-(f-1)d}}, \cdots, c_{j\cdot 2^{i_{e-1}}}^{2^{m-i_{e-1}-(f-1)d}}}^{e}].\end{aligned} \tag{42}$$

We note that if α is a primitive root of GF(2^m), then the elements $(1, \alpha, \cdots, \alpha^{f-1})$ are linearly independent over GF(2^d), where $d = m/f$, so that any element $x \in$ GF(2^m) can be written uniquely as

$$x = \sum_{i=0}^{f-1} x_i \alpha^i$$

where $x_i \in$ GF(2^d). So, we can decompose each coefficient $c_{j\cdot 2^i}^{2^{m-i}} \in$ GF(2^m) as

$$c_{j\cdot 2^{i_g}}^{2^{m-i_g}} = \sum_{l=0}^{f-1} x_{g,l} \alpha^l, \qquad \text{for } g = 0, 1, \cdots, e-1 \tag{43}$$

where $x_{g,l} \in$ GF(2^d) for all $l = 0, 1, \cdots, f-1$.

Next, we will decompose each component of $\boldsymbol{c}$ into f variables in the subfield GF(2^d). Note that if $c_{i_g}^{2^{m-i_g}}$ appears in $\boldsymbol{c}$, then

$$c_{i_g}^{2^{m-i_g-d}}, c_{i_g}^{2^{m-i_g-2d}}, \cdots, c_{i_g}^{2^{m-i_g-(f-1)d}}$$

also appear in $\boldsymbol{c}$. We expand each such term in terms of the variables $x_{g,l}$. Using (43), we get

$$c_{j\cdot 2^{i_g}}^{2^{m-i_g-ud}} = \left[\sum_{l=0}^{f-1} x_{g,l}\alpha^l\right]^{2^{-ud}} \tag{44}$$

$$= \sum_{l=0}^{f-1} [x_{g,l}\alpha^l]^{2^{-ud}} \tag{45}$$

$$= \sum_{l=0}^{f-1} x_{g,l}^{2^{-ud}} \alpha^{l2^{-ud}}. \tag{46}$$

In (44)–(46), all superscripts and subscripts are modulo n. Now, since $x_{g,l} \in$ GF(2^d), it follows that $x_{g,l}^{2^{-ud}} = x_{g,l}$. So, (46) becomes

$$c_{j\cdot 2^{i_g}}^{2^{i_g-ud}} = \sum_{l=0}^{f-1} x_{g,l}\alpha^{l2^{-ud}}, \qquad \text{for } u = 0, 1, \cdots, f-1. \tag{47}$$

If we now define two length f vectors, $\boldsymbol{c}_g$ and $\boldsymbol{x}_g$, as follows:

$$\boldsymbol{c}_g = \left[c_{j\cdot 2^{i_g}}^{2^{m-i_g}}, c_{j\cdot 2^{i_g}}^{2^{m-i_g-d}}, \cdots, c_{j\cdot 2^{i_g}}^{2^{m-i_g-(f-1)d}}\right] \tag{48}$$

$$\boldsymbol{x}_g = [x_{g,0}, x_{g,1}, \cdots, x_{g,f-1}]. \tag{49}$$

Then we can rewrite (47) in the vector form

$$\boldsymbol{c}_g^T = V \boldsymbol{x}_g^T, \tag{50}$$

where V is the $f \times f$ Vandermonde matrix given by

$$V = \begin{bmatrix} 1 & \alpha^1 & \alpha^2 & \cdots & \alpha^{(f-1)} \\ 1 & \alpha^{1\cdot 2^{-d}} & \alpha^{2\cdot 2^{-d}} & \cdots & \alpha^{(f-1)\cdot 2^{-d}} \\ 1 & \alpha^{1\cdot 2^{-2d}} & \alpha^{2\cdot 2^{-2d}} & \cdots & \alpha^{(f-1)\cdot 2^{-2d}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{1\cdot 2^{-(f-1)d}} & \alpha^{2\cdot 2^{-(f-1)d}} & \cdots & \alpha^{(f-1)\cdot 2^{-(f-1)d}} \end{bmatrix}. \tag{51}$$

The set of elements in the second column of V, i.e., $\alpha, \alpha^{2^{-d}}, \alpha^{2^{-2d}}, \cdots, \alpha^{2^{-(f-1)d}}$ are all distinct, since $m = df$ and α is a primitive root of GF(2^m), and so V is nonsingular.

Finally, we define two more vectors, $\boldsymbol{c}'$ and $\boldsymbol{x}$ as follows:

$$\boldsymbol{c}' = [\boldsymbol{c}_0, \boldsymbol{c}_1, \cdots, \boldsymbol{c}_{e-1}] \tag{52}$$

$$\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \cdots, \boldsymbol{x}_{e-1}]. \tag{53}$$

Since the matrix V in (51) does not depend on g, we can express the relationship between $\boldsymbol{c}'$ and $\boldsymbol{x}$ as

$$\boldsymbol{c}'^T = W \boldsymbol{x}^T \tag{54}$$

where W is the $a \times a$ matrix

$$W = \begin{bmatrix} V & 0 & \cdots & 0 \\ 0 & V & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & V \end{bmatrix}. \tag{55}$$

The vector $\boldsymbol{c}$ defined in (38) and the vector $\boldsymbol{c}'$ defined in (52) have the same dimension, viz., a, and the same components with a different order. In other words, $\boldsymbol{c}$ and $\boldsymbol{c}'$ are permutations of each other. So, since any permutation of a vector can be represented by left multiplication by a nonsingular permutation matrix, say Q, we have

$$\boldsymbol{c}^T = Q\boldsymbol{c}'^T. \tag{56}$$

Finally, by inserting (54) and (56) into (37), we get

$$\Gamma_j Q W \boldsymbol{x}^T = \boldsymbol{0}^T. \tag{57}$$

Thus the number of solutions to the set of equations (37) is equal to the number of solutions to (57), since a nonsingular linear transformation does not change the dimension of the solution space. But the set of equations (57) is a set of μ simultaneous linear equations in a variables which lie in the subfield GF(2^d). So, the number of solutions must be a power of 2^d and the GF(2^d)-dimension of the solution space is equal to the nullity of Γ_j, i.e., $a-r$, so the total number of solutions to (57) is $2^{d(a-r)}$. Thus the binary dimension of the solution set is $d(a-r) = mc-dr$. This completes the proof of Theorem 4.4. □

D. A Simple Lower Bound

From Theorem 4.4, it is apparent that $K(\mathbb{C},\mathcal{S})$, the dimension of SSRS code $\mathbb{C}_{\mathcal{S}}$, is minimized if all the cyclotomic matrices Γ_j are of full rank. So, we immediately get the following.

4.8. Corollary (Lower Bound): With the same setup as Theorem 4.4

$$\begin{aligned} K(\mathbb{C},\mathcal{S}) &\geq \sum_j \max(d_j(a_j-\mu),0) \\ &= \sum_j \max(me_j - \mu d_j, 0). \end{aligned} \tag{58}$$

Proof: Since Γ_j is a $\mu \times a_j$ matrix, its rank r_j satisfies

$$r_j \leq \min(a_j,\mu). \tag{59}$$

Therefore,

$$\begin{aligned} K(\mathbb{C},\mathcal{S}) &= \sum_{j\in I_n} d_j(a_j - r_j) \\ &\geq \sum_{j\in I_n} d_j(a_j - \min(a_j,\mu)) \\ &= \sum_{j\in I_n} \max(d_j(a_j-\mu),0). \end{aligned} \tag{60}$$

□

The bound of Corollary 4.8 is the same as the formula for the dimension of "TSRS" codes which is proved in [18]. Indeed, the TSRS codes of [18] are exactly the special case of SSRS codes in which the subspace $\mathcal{S}$ is spanned by the dual of polynomial basis $\{1,\alpha,\alpha^2,\cdots,\alpha^{\mu-1}\}$. (Similarly, the codes of [26] are SSRS codes for which the subspace $\mathcal{S}$ is spanned by a polynomial basis $\{1,\alpha,\alpha^2,\cdots,\alpha^{\mu-1}\}$.) The theorem for the dimension of TSRS codes [18, Theorem 3.1] thus guarantees that there exist many SSRS codes whose dimension satisfy Corollary 4.8 with equality. We can generalize this result, slightly, as follows.

TABLE I
$E(m,\nu)$: THE FRACTION OF EXCEPTIONAL ν-DIMENSIONAL SUBSPACES OF GF(2^m)

ν	m					
	2	3	4	5	6	7
1	0	0	0	0	0	0
2		0	1/7	0	1/31	0
3			0	0	36/155	2/93
4				0	1/31	2/93
5					0	0
6						0

4.9. Corollary: The lower bound of Corollary 4.8 is met with equality if $\mathcal{S}$ is spanned by the dual of the polynomial basis $\{1,\xi,\xi^2,\cdots,\xi^{\mu-1}\}$, where ξ is an arbitrary element in GF(2^m) whose minimal polynomial has degree m.

Proof: From the definition,

$$\Gamma_j = \begin{bmatrix} \gamma_0^{2^{m-i_0}} & \gamma_0^{2^{m-i_1}} & \cdots & \gamma_0^{2^{m-i_{a_j-1}}} \\ \gamma_1^{2^{m-i_0}} & \gamma_1^{2^{m-i_1}} & \cdots & \gamma_1^{2^{m-i_{a_j-1}}} \\ \vdots & & \ddots & \vdots \\ \gamma_{\mu-1}^{2^{m-i_0}} & \gamma_{\mu-1}^{2^{m-i_1}} & \cdots & \gamma_{\mu-1}^{2^{m-i_{a_j-1}}} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \xi^{2^{m-i_0}} & \xi^{2^{m-i_1}} & \cdots & \xi^{2^{m-i_{a_j-1}}} \\ (\xi^{2^{m-i_0}})^2 & (\xi^{2^{m-i_1}})^2 & \cdots & (\xi^{2^{m-i_{a_j-1}}})^2 \\ \vdots & & \ddots & \vdots \\ (\xi^{2^{m-i_0}})^{\mu-1} & (\xi^{2^{m-i_1}})^{\mu-1} & \cdots & (\xi^{2^{m-i_{a_j-1}}})^{\mu-1} \end{bmatrix}. \tag{61}$$

Although the matrix in (61) is not a square matrix, it is a submatrix of a "parent" Vandermonde matrix. Since we are assuming that $\deg(\xi) = m$ and $a_j = e_j f_j \leq d_j f_j = m$, all the elements in the second row of Γ_j are distinct from each other. So, the parent Vandermonde matrix is nonsingular and we can conclude that the rank of Γ_j is $\min(a_j,\mu)$. □

Corollary 4.9 identifies a number of subspaces for which $K(\mathbb{C},\mathcal{S})$ is a minimum, for a given $\mathbb{C}$ and $\nu = \dim(\mathcal{S})$. Surprisingly, perhaps, experimental work indicates that the lower bound of Corollary 4.9 is achieved for most subspaces. For this reason, we call subspaces for which the lower bound of Corollary 4.9 is *not* achieved for all $\mathbb{C}$ *exceptional*. If we denote by $E(m,\nu)$ the fraction of ν-dimensional subspaces of GF(2^m) that are exceptional, Table I gives the values of $E(m,\nu)$ for $m = 2,\cdots,7$ and $\nu = 1,\cdots,m-1$.

The above table suggests that all all subspaces of dimension $\nu = 1$ or codimension $\mu = 1$ are ordinary. The following Corollary shows that this is in fact true.

4.10. Corollary: The lower bound of Corollary 4.8 is attained for all subspaces of dimension $\nu = 1$ $(\mu = m-1)$ or $\nu = m-1$ $(\mu = 1)$.

Proof: In the case $\nu = 1$ this follows immediately from Corollary 4.9, since every basis for a subspace of dimension 1 is a polynomial basis.

In the case of $\mu = 1$, all Γ_j's are $1 \times a_j$ matrices, so if $e_j \neq 0$, Γ_j is always full rank, regardless of the choice of subspace $\mathcal{S}$, i.e., $r_j = 1$. Therefore, the bound of Corollary 4.8 gives the exact binary dimension of all the SSRS codes for $\mu = 1$. □

We will discuss exceptional and ordinary subspaces further in Section VI.

E. Examples

In this section, we give several numerical examples of SSRS codes. In one of these examples (Example 4.12), we will see an SSRS code whose dimension is higher than that of the corresponding subfield subcode.

4.11. Example: Let $m = 4, n = 15, k_0 = 9, \nu = 2$ ($\mu = 2$), and $J = \{1, 2, \cdots, 9\}$. We start from an ordinary $(15, 9, 7)$ RS code. Let α be a primitive root of GF(2^4) defined by $\alpha^4 = \alpha + 1$. We form the cyclotomic matrix (at the bottom of this page), using the same cyclotomic array as Example 4.2, with $I_{15} = \{0, 1, 3, 5, 7\}$. Consider the subspace $\mathcal{S}_1$ which is spanned by the basis $\{1, \alpha^1\}$. It is easily seen that $\mathcal{S}_1$ is a self-dual subspace, so $\mathcal{S}_1^{\perp} = \mathcal{S}_1$. Using the same procedure as in Example 4.3, we get the following.

$$\Gamma_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \alpha & \alpha^8 & \alpha^4 & \alpha^2 \end{bmatrix}$$

$$\Gamma_3 = \begin{bmatrix} 1 & 1 & 1 \\ \alpha & \alpha^8 & \alpha^2 \end{bmatrix}$$

$$\Gamma_5 = \begin{bmatrix} 1 & 1 \\ \alpha & \alpha^4 \end{bmatrix}$$

$$\Gamma_7 = \begin{bmatrix} 1 \\ \alpha \end{bmatrix}.$$

The ranks of these matrices are given by

$$r_1 = r_3 = r_5 = 2, \qquad r_7 = 1.$$

By Theorem 4.4, the dimension of $\mathbb{C}_{\mathcal{S}_1}$ is

$$\begin{aligned} K(\mathbb{C}, \mathcal{S}_1) &= \sum_{j \in I_{15}} d_j (a_j - r_j) \\ &= 4 \cdot (4-2) + 4 \cdot (3-2) + 2 \cdot (2-2) \\ &\quad + 4 \cdot (1-1) \\ &= 12. \end{aligned}$$

Thus we obtain a $(15, 6, 7)$ SSRS code over the alphabet $\mathcal{S}_1$, i.e., the vector space of binary 2-tuples. In this case, all cyclotomic matrices have full rank, so the dimension of $\mathbb{C}_{\mathcal{S}_1}$ is equal to the lower bound in Corollary 4.8. In fact, since the basis of $\mathcal{S}^{\perp}$, i.e., $\{1, \alpha\}$, is a polynomial basis and $\deg(\alpha) = 4$, $\mathbb{C}_{\mathcal{S}_1}$ is a TSRS code as originally defined in [18]. Next, let $\mathcal{S}_2$ be the two-dimensional subspace spanned by $\{1, \alpha^5\}$. We can see that $\mathcal{S}_2$ is also a self-dual subspace, so the basis of $\mathcal{S}_2{}^{\perp}$ can be taken as $\{1, \alpha^5\}$. We now form the cyclotomic matrix for each $j \in I_{15}$ and compute the corresponding rank.

$$\Gamma_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \alpha^5 & \alpha^{10} & \alpha^5 & \alpha^{10} \end{bmatrix}$$

$$\Gamma_3 = \begin{bmatrix} 1 & 1 & 1 \\ \alpha^5 & \alpha^{10} & \alpha^{10} \end{bmatrix}$$

$$\Gamma_5 = \begin{bmatrix} 1 & 1 \\ \alpha^5 & \alpha^5 \end{bmatrix}$$

$$\Gamma_7 = \begin{bmatrix} 1 \\ \alpha^5 \end{bmatrix}$$

$$r_1 = r_3 = 2, \qquad r_5 = r_7 = 1.$$

Using these results, we can compute the dimension of $\mathbb{C}_{\mathcal{S}_2}$ as

$$\begin{aligned} K(\mathbb{C}, \mathcal{S}_2) &= \sum_{j \in I_{15}} d_j (a_j - r_j) \\ &= 4 \cdot (4-2) + 4 \cdot (3-2) + 2 \cdot (2-1) \\ &\quad + 4 \cdot (1-1) \\ &= 14. \end{aligned}$$

In this case, we get a $(15, 7, 7)$ SSRS code over the alphabet $\mathcal{S}_2$. This example demonstrates that the dimension of the SSRS code derived from a given parent code may depend on the choice of subspace, since $K(\mathbb{C}, \mathcal{S}_2) > K(\mathbb{C}, \mathcal{S}_1)$. Note that the elements $\{1, \alpha^5\}$ both lie in the subfield GF(4) of the parent symbol field GF(16). So, $\mathcal{S}_2$ is, in fact, the subfield GF(4) itself. It follows that $\mathbb{C}_{\mathcal{S}_2}$ is a subfield subcode over GF(4). □

4.12. Example: Let $m = 6, n = 63, k_0 = 53, \nu = 2$ ($\mu = 4$), and $J = \{1, 2, \cdots, 53\}$. We start from a parent $(63, 53, 11)$ RS code. Let α be a primitive root of GF(2^6) defined by $\alpha^6 = \alpha + 1$. Now we consider the two subspaces $\mathcal{S}_1$ and $\mathcal{S}_2$, spanned by the bases $\{1, \alpha^9\}$ and $\{1, \alpha^{21}\}$, respectively. A short computation produces bases for the trace dual subspaces as given below. Note that $\mathcal{S}_2$ is the subfield

index i

	0	1	2	3					
$j=0$	**0**	**0**	**0**	**0**	$d_0=1$	$f_0=4$	$e_0=0$	$A_0=\emptyset$	$a_0=0$
$j=1$	**1**	**2**	**4**	**8**	$d_1=4$	$f_1=1$	$e_1=4$	$A_1=\{0,1,2,3\}$	$a_1=4$
$j=3$	**3**	**6**	12	**9**	$d_3=4$	$f_3=1$	$e_3=3$	$A_3=\{0,1,3\}$	$a_3=3$
$j=5$	**5**	10	**5**	10	$d_5=2$	$f_5=2$	$e_5=1$	$A_5=\{0,2\}$	$a_5=2$
$j=7$	**7**	14	13	11	$d_7=4$	$f_7=1$	$e_7=1$	$A_7=\{0\}$	$a_7=1$

GF (2^2).

$$\{1, \alpha^9\} \perp \{1, \alpha^3, \alpha^4, \alpha^7\}$$
$$\{1, \alpha^{21}\} \perp \{\alpha^3, \alpha^6, \alpha^7, \alpha^{24}\}.$$

Now we compute the dimensions of $\mathbb{C}_{\mathcal{S}_1}$ and $\mathbb{C}_{\mathcal{S}_2}$, using Theorem 4.4, as follows (details omitted):

$$\begin{aligned} K(\mathbb{C}, \mathcal{S}_1) &= \sum_{j \in I_{63}} d_j(a_j - r_j) \\ &= 85 \\ K(\mathbb{C}, \mathcal{S}_2) &= \sum_{j \in I_{63}} d_j(a_j - r_j) \\ &= 82. \end{aligned}$$

In this case, $\mathbb{C}_{\mathcal{S}_2}$ is a subfield subcode over GF (2^2) and its dimension is 41. But $\mathbb{C}_{\mathcal{S}_1}$ has pseudo dimension 42.5. Thus in this case, the dimension of an SSRS code exceeds that of the corresponding subfield subcode. □

V. Elementary Bounds on Dimension

In this section, we will develop estimates for the dimension of SSRS codes from "elementary" arguments. In a recent paper, Jensen [13] has obtained results on SSRS codes which follow from general results on "subgroup subcodes." In particular, he has derived some interesting estimates for the dimension of subgroup subcodes. We will review his results and give an alternative proof of them.[7]

Let $\mathbb{C}$ be a parent (n, k_0, d_0) RS code over GF (2^m) with $n = 2^m - 1$ and $d_0 = n - k_0 + 1$. Let $\mathcal{S}$ be a ν-dimensional subspace of GF (2^m). We consider the SSRS code $\mathbb{C}_{\mathcal{S}}$. In Theorem 4.4, we have derived a formula for the *exact* dimension of $\mathbb{C}_{\mathcal{S}}$, which requires detailed matrix rank computations. But now, we consider a rough *estimate* for the dimension of $\mathbb{C}_{\mathcal{S}}$.

First, we consider the binary expansion of $\mathbb{C}$. If we expand the components of the codewords in $\mathbb{C}$ into binary m-tuples, then we obtain an (mn, mk_0) code over GF (2). Therefore, since $\mathbb{C}_{\mathcal{S}}$ is obtained by requiring $n(m-\nu)$ binary coordinates of the binary code to be zero, from the argument for general shortened codes, we have the elementary estimate

$$\dim(\mathbb{C}_{\mathcal{S}}) \geq mk_0 - n(m - \nu). \tag{62}$$

But we can improve the bound in (62), in many cases.

Suppose, for example, that the parent code $\mathbb{C}$ satisfies an overall parity check, i.e., each codeword

$$\boldsymbol{C} = (C_0, C_1, \cdots, C_{n-1})$$

from $\mathbb{C}$ satisfies

$$C_0 + C_1 + \cdots + C_{n-1} = 0. \tag{63}$$

In this case, all codewords from $\mathbb{C}$ have an even number of 1's in every binary component, and so do the codewords from $\mathbb{C}_{\mathcal{S}}$. Therefore, if we require $m-\nu$ binary components in each of the first $n-1$ coordinates to be zero, then the last (nth) coordinate is automatically forced to be zero in these same coordinates, because of the overall parity check. Thus we can improve the estimate (62) as follows:

$$\dim(\mathbb{C}_{\mathcal{S}}) \geq mk_0 - (n-1)(m-\nu). \tag{64}$$

This argument can be generalized as follows. Suppose that GF (2^d) is a subfield of $F = \text{GF}(2^m)$, and that $\mathbb{C}$ satisfies a set of t linearly independent parity checks over GF (2^d), e.g.,

$$\begin{aligned} a_{0,0}C_0 + a_{0,1}C_1 + a_{0,2}C_2 + \cdots + a_{0,n-1}C_{n-1} &= 0 \\ a_{1,0}C_0 + a_{1,1}C_1 + a_{1,2}C_2 + \cdots + a_{1,n-1}C_{n-1} &= 0 \\ \vdots & \\ a_{t-1,0}C_0 + a_{t-1,1}C_1 + a_{t-1,2}C_2 + \cdots + a_{t-1,n-1}C_{n-1} &= 0 \end{aligned} \tag{65}$$

where $a_{i,j} \in$ GF (2^d). Then the estimate (64) can be improved, as follows:

$$\dim(\mathbb{C}_{\mathcal{S}}) \geq mk_0 - d(n-t)(m-\nu). \tag{66}$$

But how many linearly independent equations of the form (65) are satisfied by $\mathbb{C}$? Each vector $(a_{i,0}, a_{i,1}, \cdots, a_{i,n-1})$ is orthogonal to $\mathbb{C}$, so it is a codeword from $\mathbb{C}^{\perp}$. But $a_{i,j} \in$ GF (2^d). Therefore, the set of vectors of the form $(a_{i,0}, a_{i,1}, \cdots, a_{i,n-1})$ satisfying (65) is the GF (2^d) subfield subcode of $\mathbb{C}^{\perp}$. Therefore,

$$t = \dim(\mathbb{C}^{\perp}_{\text{GF}(2^d)}). \tag{67}$$

The estimate (66), where t is given in (67), gives a tight bound in some cases. In fact, Jensen [13] shows that the estimate is sharp when $d = 1$ and $\nu = m-1$. (We have already noted, in Corollary 4.10, that for $\nu = m-1$, the dimension of an SSRS code is always given by Corollary 4.8.) Thus there is an exact relationship between (66) and (67), and Corollary 4.8 in the case $\nu = m-1$. On the other hand, Jensen's estimate does not distinguish between different subspaces of the same dimension, and so it cannot be exact in all cases.

VI. Duality

In this section, we will study the relationship between an SSRS code associated with a given subspace $\mathcal{S}$, and that associated with its trace-dual subspace $\mathcal{S}^{\perp}$. We will start with a discussion of a convenient way to identify an "*interesting*" subspace. Then we discuss a relationship between interesting subspaces and MDS codes. Next, we will focus on the relationship between the dimension of SSRS code and trace-duality. We will show that the dimension of an SSRS code can be computed from that of its complementary trace-dual SSRS code, without the need for matrix rank computation. We will show this using a fundamental fact that we call the "*defect theorem*."

[7] The bounds we derive in this section are bounds on the binary dimension, whereas the bounds in Jensen's paper are bounds on the pseudodimension, i.e., they are divided by the parameter that we call ν.

A. Ordinary Subspaces

We showed in Section IV that the dimension of an SSRS code is determined by the ranks of the appropriate cyclotomic matrices. On the other hand, the lower bound on the dimension given by Corollary 4.8 does not depend on rank computations. Many subspaces which achieve this lower bound are exhibited by Corollary 4.9, which says that, if the subspace is spanned by a basis of the form $\{1, \xi, \xi^2, \cdots, \xi^{\mu-1}\}$, where ξ is an arbitrary element in $\mathrm{GF}(2^m)$ with $\deg(\xi) = m$, i.e., a polynomial basis, then the corresponding cyclotomic matrices Γ_j's are always full rank for any choice of integers from cyclotomic cosets.

But even if the subspace is not spanned by a polynomial basis, it is still possible that the subspace will achieve the lower bound for any parent code. This leads us to the following definition.

6.1. Definition: A subspace is said to be "*ordinary*" if the dimension of the corresponding SSRS code achieves the lower bound given by Corollary 4.8 for all parent codes. A subspace is called "*exceptional*" if it is not ordinary, i.e., if the subspace gives a higher dimension for at least one parent code. □

This definition does not give a practical way to determine "ordinariness." In order to clarify the definition, we now give an equivalent condition in terms of the cyclotomic matrices.

Let $\mathcal{S}$ be a ν-dimensional subspace of $\mathrm{GF}(2^m)$ spanned by the basis $\{\beta_0, \beta_1, \cdots, \beta_{\nu-1}\}$. We have defined the $\nu \times m$ cyclotomic matrix $G(\mathcal{S})$ as follows.[8]

$$G(\mathcal{S}) = \begin{bmatrix} \beta_0 & \beta_0^2 & \cdots & \beta_0^{2^{m-1}} \\ \beta_1 & \beta_1^2 & \cdots & \beta_1^{2^{m-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{\nu-1} & \beta_{\nu-1}^2 & \cdots & \beta_{\nu-1}^{2^{m-1}} \end{bmatrix}. \tag{68}$$

Thus a subspace $\mathcal{S}$ is ordinary if and only if every $\nu \times h$ submatrix of the corresponding cyclotomic matrix $G(\mathcal{S})$ has full rank, where $0 < h < m$.

But from an elementary property of matrices (e.g., [8]), "every $\nu \times h$ submatrix" can be replaced by "every $\nu \times \nu$ submatrix." Moreover, if we view $G(\mathcal{S})$ as the generator matrix of a code, we can restate Definition 6.1 in a more convenient manner.

6.2. Theorem: A subspace $\mathcal{S}$ is ordinary if and only if every $\nu \times \nu$ submatrix of the cyclotomic matrix $G(\mathcal{S})$ is nonsingular. Equivalently, a subspace $\mathcal{S}$ is ordinary if and only if the cyclotomic matrix $G(\mathcal{S})$ in (68) generates an (m, ν) MDS code over $\mathrm{GF}(2^m)$.

Theorem 6.2 gives us an opportunity to utilize known theorems about MDS codes.

6.3. Theorem: Let $\mathcal{S}$ be a ν-dimensional subspace of $\mathrm{GF}(2^m)$ and let $\mathcal{S}^\perp$ be the trace-dual subspace of $\mathcal{S}$. The subspace $\mathcal{S}$ is ordinary if and only if $\mathcal{S}^\perp$ is ordinary.

[8] In Section IV, the indices are in reversed order. But here we will make the indices simpler since it does not materially affect the discussion.

Proof: Let $\{\gamma_0, \gamma_1, \cdots, \gamma_{\mu-1}\}$ be a basis for $\mathcal{S}^\perp$. Then by definition

$$\mathrm{Tr}_1^m(\gamma_i \beta_j) = 0, \qquad \begin{cases} i = 0, 1, \cdots, \mu - 1 \\ j = 0, 1, \cdots, \nu - 1. \end{cases} \tag{69}$$

Thus if we define the $\mu \times m$ matrix

$$H = \begin{bmatrix} \gamma_0 & \gamma_0^2 & \cdots & \gamma_0^{2^{m-1}} \\ \gamma_1 & \gamma_0^2 & \cdots & \gamma_0^{2^{m-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_{\mu-1} & \gamma_{\mu-1}^2 & \cdots & \gamma_{\mu-1}^{2^{m-1}} \end{bmatrix} \tag{70}$$

then $HG^T = 0$, since the inner product of the ith row of H and the jth row of G is

$$\beta_i \gamma_j + \beta_i^2 \gamma_j^2 + \cdots + \beta_i^{2^{m-1}} \gamma_j^{2^{m-1}} = \mathrm{Tr}_1^m(\beta_i \gamma_j) = 0. \tag{71}$$

It follows that if an (m, ν) code $\mathbb{C}$ is defined by the generator matrix G, then the dual code $\mathbb{C}^\perp$ of $\mathbb{C}$ is generated by the matrix H. But since $\mathcal{S}$ is ordinary, $\mathbb{C}$ is an MDS code. But since the dual code of an MDS code is also an MDS code [17, Sec. XI, Theorem 2], $\mathbb{C}^\perp$ is also an MDS code. It follows that $\mathcal{S}^\perp$ is ordinary as well. □

B. Shortened and Punctured Codes

Here we give a brief general discussion of shortening and puncturing of linear codes over any field. Although shortening and puncturing are commonly used techniques in coding theory, this formal kind of discussion seems to have first appeared in [7], [13], and [20]. The proofs of Theorems 6.4–6.6 which are omitted here, can be found in those references.

Let $\mathbb{C}$ be an (n, k) linear code over a field $\mathbb{F}$. First, we number each coordinate of $\mathbb{C}$ from 1 to n, and let S be an arbitrary coordinate subset defined as

$$S \subseteq \{1, 2, \cdots, n\} \tag{72}$$

$$= \{i_1, i_2, \cdots, i_s\} \tag{73}$$

where $s = |S|$; and let $\overline{S}$ be the complementary subset of S. Further, we define the projection map Π_S: $\mathbb{F}^n \to \mathbb{F}^s$ by

$$\Pi_S(v_1, v_2, \cdots, v_n) \to (v_{i_1}, v_{i_2}, \cdots, v_{i_s}) \tag{74}$$

where $v_i \in \mathbb{F}$. Now we apply the mapping Π_S to the code $\mathbb{C}$. We denote the *image* of the mapping by $\Omega^S(\mathbb{C})$, and the *kernel* by $\Omega'_S(\mathbb{C})$, i.e.,

$$\Omega^S(\mathbb{C}) = \{\Pi_S(\boldsymbol{c}) | \boldsymbol{c} \in \mathbb{C}\} \tag{75}$$

$$\Omega'_S(\mathbb{C}) = \{\boldsymbol{c} \in \mathbb{C} | \Pi_S(\boldsymbol{c}) = \boldsymbol{0}\}. \tag{76}$$

We call $\Omega^S(\mathbb{C})$ the $\overline{S}$-*punctured* version of $\mathbb{C}$. Each $\boldsymbol{c} \in \Omega'_S(\mathbb{C})$ is identically zero on the coordinates indexed by S. If we delete these zero coordinates, we obtain what is called the S-*shortened* version of $\mathbb{C}$, and denoted by $\Omega_S(\mathbb{C})$

$$\Omega_S(\mathbb{C}) = \{\Pi_{\overline{S}}(\boldsymbol{c}) | \boldsymbol{c} \in \Omega'_S(\mathbb{C})\}. \tag{77}$$

The following theorem follows immediately from the fact that the dimension of the image plus the dimension of the kernel of any linear transformation is the dimension of the whole space.

6.4. Theorem:

$$\dim(\Omega_S(\mathbb{C})) + \dim(\Omega^S(\mathbb{C})) = \dim(\mathbb{C}). \tag{78}$$

Now, let G and H be a generator matrix and a parity-check matrix for $\mathbb{C}$, respectively. Thus G is a $k \times n$ matrix and H is an $r \times n$ matrix, where $r = n - k$. By definition, we have

$$GH^T = \mathbf{0}. \tag{79}$$

Further, let G_S be the $k \times s$ matrix obtained from G by deleting the columns whose indices lie in $\overline{S}$ and similarly let $H_{\overline{S}}$ be the $r \times t$ matrix obtained from H by deleting the columns whose indices lie in S, where $t = n - s$.

6.5. Theorem: $H_{\overline{S}}$ is a parity-check matrix for $\Omega_S(\mathbb{C})$, and G_S is a generator matrix for $\Omega^S(\mathbb{C})$.

Next we investigate the relationship between shortened and punctured codes and their duals. Let $\mathbb{C}^\perp$ be the dual code of $\mathbb{C}$. Then $\mathbb{C}^\perp$ is an (n, r) linear code whose generator matrix and parity-check matrix are H and G, respectively.

6.6. Theorem: (This is similar to [13, Theorem 4].)

$$\Omega_S(\mathbb{C})^\perp = \Omega^{\overline{S}}(\mathbb{C}^\perp) \tag{80}$$

$$\Omega^S(\mathbb{C})^\perp = \Omega_{\overline{S}}(\mathbb{C}^\perp). \tag{81}$$

Now we move to the Defect Theorem. Let M be an arbitrary $i \times j$ matrix. The rank of M can be written as $\operatorname{rank}(M) = \min(i, j) - d(M)$, where $d(M)$ is a nonnegative integer in the range $0 \le d(M) \le \min(i, j)$. We shall call $d(M)$ the "*defect*" of the matrix M:

$$d(M) = \min(i, j) - \operatorname{rank}(M). \tag{82}$$

Note that $d(M) = 0$ if and only if the matrix is *full rank*. Here is our main result.

6.7. Theorem (Defect Theorem): If G is a generator matrix, and H is a parity-check matrix, for the code $\mathbb{C}$, and if S is any coordinate subset, then

$$d(H_S) = d(G_{\overline{S}}). \tag{83}$$

Proof: Recall that H_S is the $r \times s$ matrix obtained from H by deleting the columns with indices in $\overline{S}$, and, similarly, $G_{\overline{S}}$ is the $k \times t$ matrix obtained from G by deleting all columns indexed by S. Therefore, the ranks of H_S and $G_{\overline{S}}$ can be written as follows:

$$\operatorname{rank}(H_S) = \min(r, s) - d(H_S) \tag{84}$$

$$\operatorname{rank}(G_{\overline{S}}) = \min(k, t) - d(G_{\overline{S}}) \tag{85}$$

where $d(H_S)$ and $d(G_{\overline{S}})$ are nonnegative integers in the range

$$0 \le d(H_S) \le \min(r, s) \tag{86}$$

$$0 \le d(G_{\overline{S}}) \le \min(k, t). \tag{87}$$

From Theorem 6.5, we see that H_S is a parity-check matrix for $\Omega_{\overline{S}}(\mathbb{C})$ and $G_{\overline{S}}$ is a generator matrix for $\Omega^{\overline{S}}(\mathbb{C})$. It then follows from Theorem 6.6 that $G_{\overline{S}}$ is also a parity-check matrix for $\Omega^{\overline{S}}(\mathbb{C})^\perp = \Omega_S(\mathbb{C}^\perp)$.

Now from Theorem 6.4, we have

$$\dim(\mathbb{C}) = \dim(\Omega_{\overline{S}}(\mathbb{C})) + \dim(\Omega^{\overline{S}}(\mathbb{C})). \tag{88}$$

However, from Theorem 6.6, we get

$$\Omega^{\overline{S}}(\mathbb{C}) = \Omega_{\mathcal{S}}(\mathbb{C}^\perp)^\perp. \tag{89}$$

This says that $\Omega^{\overline{S}}(\mathbb{C})$ and $\Omega_S(\mathbb{C}^\perp)$ are dual to each other, and therefore the codelengths of $\Omega^{\overline{S}}(\mathbb{C})$ and $\Omega_S(\mathbb{C}^\perp)$ are the same. The codelength of $\Omega^{\overline{S}}(\mathbb{C})$ is $t = n - s$, since the code $\Omega^{\overline{S}}(\mathbb{C})$ is the S-punctured code obtained from $\mathbb{C}$. Now, from the fact that the sum of the dimensions of two codes which are dual to each other is equal to the length of the code, we get

$$\dim(\Omega^{\overline{S}}(\mathbb{C})) + \dim(\Omega_S(\mathbb{C})) = t. \tag{90}$$

Eliminating $\dim(\Omega^{\overline{S}}(\mathbb{C}))$ from (88) by inserting (90), and using the fact that $\dim(\mathbb{C}) = k$, we get

$$\begin{aligned} k &= \dim(\Omega_{\overline{S}}(\mathbb{C})) + (t - \dim(\Omega_S(\mathbb{C}^\perp))) \\ \dim(\Omega_S(\mathbb{C}^\perp)) &- \dim(\Omega_{\overline{S}}(\mathbb{C})) = t - k. \end{aligned} \tag{91}$$

Since any linear code is, by definition, the null space of its parity-check matrix, we have the following:

$$\dim(\Omega_{\overline{S}}(\mathbb{C})) = s - \operatorname{rank}(H_S) \tag{92}$$

$$\dim(\Omega_S(\mathbb{C}^\perp)) = t - \operatorname{rank}(G_{\overline{S}}). \tag{93}$$

By inserting (92) and (93) into (91), we have

$$\begin{aligned} (t - \operatorname{rank}(G_{\overline{S}})) - (s - \operatorname{rank}(H_S)) &= t - k \\ \operatorname{rank}(H_S) - \operatorname{rank}(G_{\overline{S}}) &= s - k. \end{aligned} \tag{94}$$

Finally, we insert (84) and (85) into (94), obtaining

$$\begin{aligned} (\min(r, s) - d(H_S)) - (\min(k, t) - d(G_{\overline{S}})) &= s - k \\ d(G_{\overline{S}}) - d(H_S) &= \min(k, t) - \min(r, s) + s - k. \end{aligned} \tag{95}$$

Since $k + r = n$ and $s + t = n$, there are only eight possibilities for the relationships between k, r, s, and t. We evaluate the right-hand side of (95) for each of these cases, as follows:

	inequality	$\min(k,t) - \min(r,s) + s - k$
1	$k \le s \le t \le r$	$k - s + s - k = 0$
2	$r \le s \le t \le k$	$t - s + s - k = 0$
3	$k \le t \le s \le r$	$k - s + s - k = 0$
4	$r \le t \le s \le k$	$t - r + s - k = 0$
5	$s \le k \le r \le t$	$k - s + s - k = 0$
6	$t \le k \le r \le s$	$t - r + s - k = 0$
7	$s \le r \le k \le t$	$l = s + s - k = 0$
8	$t \le r \le k \le s$	$t - r + s - k = 0$

Therefore, we can conclude

$$d(G_{\overline{S}}) - d(H_S) = 0 \tag{96}$$

and Theorem 6.7 follows. □

C. Application to SSRS Codes

In this section, we apply Theorem 6.7 to the problem of computing the dimension of SSRS codes. Let us consider two parent RS codes $\mathbb{C}(J)$ and $\mathbb{C}(\overline{J})$, where $\overline{J}$ is a set of integers complementary to J. We will call these codes "*complementary*."

We recall that J defines an (n, k_0) RS code $\mathbb{C}(J)$, where $n = 2^m - 1$ and $k_0 = |J|$ with parity-check polynomial

$$h(x) = \prod_{j \in J} (x - \alpha^j). \tag{97}$$

It follows that $\overline{J}$ defines an $(n, n - k_0)$ RS code with parity-check polynomial

$$\overline{h}(x) = \prod_{j \in \overline{J}} (x - \alpha^j). \tag{98}$$

Next, let $\mathcal{S}$ be a ν-dimensional subspace of GF(2^m) and let $\mathcal{S}^\perp$ be its trace-dual subspace, with dimension $\mu = m - \nu$. If we consider the two SSRS codes $\mathbb{C}_{\mathcal{S}}(J)$ and $\mathbb{C}_{\mathcal{S}^\perp}(\overline{J})$, we get the following theorem.

6.8. Theorem: With the setup described above

$$\begin{aligned} K(\mathbb{C}(J), \mathcal{S}) - K_{LB}(\mathbb{C}(J), \nu) \\ = K(\mathbb{C}(\overline{J}), \mathcal{S}^\perp) - K_{LB}(\mathbb{C}(\overline{J}), \mu) \end{aligned} \tag{99}$$

where $K_{LB}(\mathbb{C}(J), \nu)$ represents the lower bound on the binary dimension of SSRS codes given by Corollary 4.8 in Section IV.

Theorem 6.8 says that the "excess" of the SSRS dimension over the lower bound given by Corollary 4.8, is the same for $\mathbb{C}_{\mathcal{S}}(J)$ and $\mathbb{C}_{\mathcal{S}^\perp}(\overline{J})$. Since the computation of the lower bound on the dimension does not require the knowledge of the rank of any matrices, Theorem 6.8 says that once we know one of these dimensions, we can immediately compute the other.

Proof: We recall that the dimension of SSRS code is determined by the ranks of the cyclotomic matrices corresponding to the cyclotomic cosets. Let $G(\mathcal{S})$ and $G(\mathcal{S}^\perp)$ be the full cyclotomic matrices associated with the trace-dual subspaces $\mathcal{S}$ and $\mathcal{S}^\perp$. Let $\{\beta_0, \beta_1, \cdots, \beta_{\nu-1}\}$ and $\{\gamma_0, \gamma_1, \cdots, \gamma_{\mu-1}\}$ be bases for $\mathcal{S}$ and $\mathcal{S}^\perp$, respectively. Then, as in the proof of Theorem 6.3, we have

$$G(\mathcal{S}) = \begin{bmatrix} \gamma_0 & \gamma_0^2 & \gamma_0^{2^2} & \cdots & \gamma_0^{2^{m-1}} \\ \gamma_1 & \gamma_1^2 & \gamma_1^{2^2} & \cdots & \gamma_1^{2^{m-1}} \\ \vdots & \vdots & & \ddots & \vdots \\ \gamma_{\mu-1} & \gamma_{\mu-1}^2 & \gamma_{\mu-1}^{2^2} & \cdots & \gamma_{\mu-1}^{2^{m-1}} \end{bmatrix} \tag{100}$$

$$G(\mathcal{S}^\perp) = \begin{bmatrix} \beta_0 & \beta_0^2 & \beta_0^{2^2} & \cdots & \beta_0^{2^{m-1}} \\ \beta_1 & \beta_1^2 & \beta_1^{2^2} & \cdots & \beta_1^{2^{m-1}} \\ \vdots & \vdots & & \ddots & \vdots \\ \beta_{\nu-1} & \beta_{\nu-1}^2 & \beta_{\nu-1}^{2^2} & \cdots & \beta_{\nu-1}^{2^{m-1}} \end{bmatrix} \tag{101}$$

$$G(\mathcal{S}) G(\mathcal{S}^\perp)^T = \mathbf{0}. \tag{102}$$

To compute the dimension of the corresponding SSRS code, we need to compute the ranks of certain submatrices of these cyclotomic matrices. Let Ω_j be the jth cyclotomic coset. Then, the coordinate set A_j for $\mathbb{C}_{\mathcal{S}}(J)$ is

$$A_j = \Omega_j \cap J. \tag{103}$$

Similarly, the corresponding set for $\mathbb{C}_{\mathcal{S}^\perp}(\overline{J})$ is its complement

$$\overline{A}_j = \Omega_j \cap \overline{J}. \tag{104}$$

Therefore, by Theorem 6.7,

$$d(G(\mathcal{S})_{A_j}) = d(G(\mathcal{S}^\perp)_{\overline{A}_j}). \tag{105}$$

From (20) in Section IV-B, we see that the dimension excess is the sum of the products of the degree d_j and the defect of the jth cyclotomic matrix. But by (105), for every cyclotomic coset, the defect of the corresponding submatrices are always the same, so the theorem is proved. □

6.9. Example: Let $m = 6$ and $\nu = 4$. Let us choose the parameters for $\mathbb{C}$ as $k_0 = 20$ and let $J = \{1, \cdots, 20\}$. We pick the subspace $\mathcal{S}$ spanned by the basis

$$\mathfrak{B} = \{1, \alpha, \alpha^8, \alpha^{21}\}.$$

It is easy to check

$$\begin{aligned} K(\mathbb{C}(J), \mathcal{S}) &= 48 \\ K_{LB}(\mathbb{C}(J), 2) &= 42 \\ K(\mathbb{C}(J), \mathcal{S}) - K_{LB}(\mathbb{C}(J), 2) &= 6. \end{aligned}$$

On the other hand, consider $\mathbb{C}(\overline{J})$ with $k_0 = 63 - 20 = 43$ and $\overline{J} = \{21, \cdots, 62, 0\}$. Here $\mathcal{S}^\perp$ is a $\nu = 2$-dimensional subspace spanned by the basis

$$\mathfrak{B}^\perp = \{1, \alpha^{21}\}.$$

If we compute the dimension for the SSRS code $\mathbb{C}(\overline{J})_{\mathcal{S}}$ using Theorem 4.4, we can verify that the excess dimension is the same as above

$$\begin{aligned} K(\mathbb{C}(\overline{J}), \mathcal{S}^\perp) &= 54 \\ K_{LB}(\mathbb{C}(\overline{J}), 4) &= 48 \\ K(\mathbb{C}(\overline{J}), \mathcal{S}^\perp) - K_{LB}(\mathbb{C}(\overline{J}), 4) &= 6. \end{aligned}$$ □

If we combine our two duality Theorems 6.3 and 6.8, we can avoid the rank computation for the computation of the dimension of an SSRS code, provided we know the dimension of its dual code. This is very helpful if we fix the dimension of the parent code k_0 and search for the best possible SSRS code by changing both the integer set J and the subspace $\mathcal{S}$, since Theorem 6.8 guarantees that if an integer set J and a subspace $\mathcal{S}$ gives an optimal SSRS code for a ν-dimensional subspace, then the integer set $\overline{J}$ and the subspace $\mathcal{S}^\perp$ also gives an optimal code.

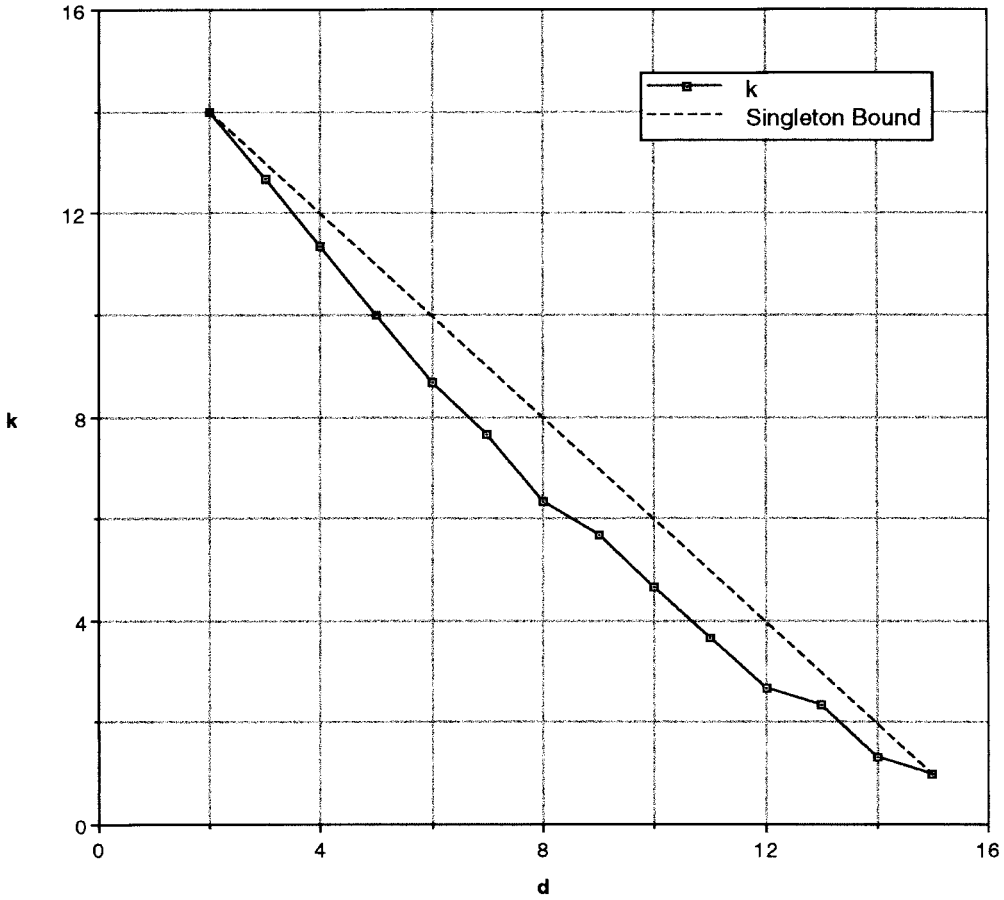

Fig. 1. The best SSRS codes for $m = 4, n = 15, \nu = 3, q = 8$.

VII. The (n, k, d) Parameters

In this section, we discuss the performance of SSRS codes in terms of codelength n, pseudo-dimension k, designed minimum distance d, and symbol size $q = 2^{\nu}$. First, we will present graphs illustrating the parameters (n, k, d) and q in some specific cases. Then, we will attempt to compare SSRS codes to algebraic-geometry (AG) codes. We will see that in some cases, SSRS codes are superior to AG codes. Finally, we will exhibit some infinite sequences of SSRS codes, which provide counterexamples to a conjecture about optimal "quasi-MDS" codes.

A. Examples

In this subsection, we give several numerical examples, viz., $(m, \nu) = (4, 3), (6, 4), (6, 2)$. Extensive tables of the best SSRS codes are given in [12].

7.1. Example: Consider the case $m = 4$ and $\nu = 3$. If we start with a parent $(15, k_0, d_0)$ RS code over GF(2^4), we obtain a $(15, k, d_0^+)$ SSRS code over an eight-letter alphabet. Fig. 1 gives the relationship between d_0, the designed minimum distance, and k, the symbol-wise pseudo-dimension. The plot is almost a straight line and is very close to that of optimal MDS codes (Singleton bound). Note that the maximum codelength of a cyclic RS code over GF(2^3) is 7. SSRS codes enable us to double the codelength n with little penalty in d.

(In Fig. 1, at the abscissa $d = 7$, we see that there is a $(15, 7\frac{2}{3}, 7^+)$ SSRS code over an eight-letter alphabet, which is slightly superior to the $(15, 7\frac{1}{3}, 7^+)$ code that we constructed in our introductory Section III-A. The difference is that in our introductory example we started with the "natural" parity-check polynomial $h(x) = \Pi_{i=1}^{9}(x - \alpha^i)$, whereas a computer search revealed that the optimum dimension is obtained with $h(x) = \Pi_{i=2}^{10}(x - \alpha^i)$.)

7.2. Example: Next we consider $m = 6$ and $\nu = 4$. We choose four representative subspaces,[9] as shown in the table below. (Recall that a subspace is ordinary if it invariably produces SSRS codes whose dimension meets the lower bound of Corollary 4.8, and exceptional, otherwise.)

category	basis	
$\mathbb{G}_0$	$\{1, \alpha, \alpha^2, \alpha^3\}$	ordinary
$\mathbb{G}_1$	$\{1, \alpha, \alpha^2, \alpha^9\}$	ordinary
$\mathbb{G}_2$	$\{1, \alpha, \alpha^4, \alpha^{15}\}$	exceptional
$\mathbb{G}_3$	$\{1, \alpha, \alpha^8, \alpha^{21}\}$	exceptional

From Fig. 2, we can see for any d_0, the maximum dimension is always achieved by either $\mathbb{G}_2$ or $\mathbb{G}_3$.

[9] In fact, in the table, $\mathbb{G}_0, \mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_3$ represent *categories*, of equivalent subspaces. Subspaces in the same category are guaranteed to produce the same pseudodimension for SSRS codes. We explain subspace equivalence in [10] and [12].

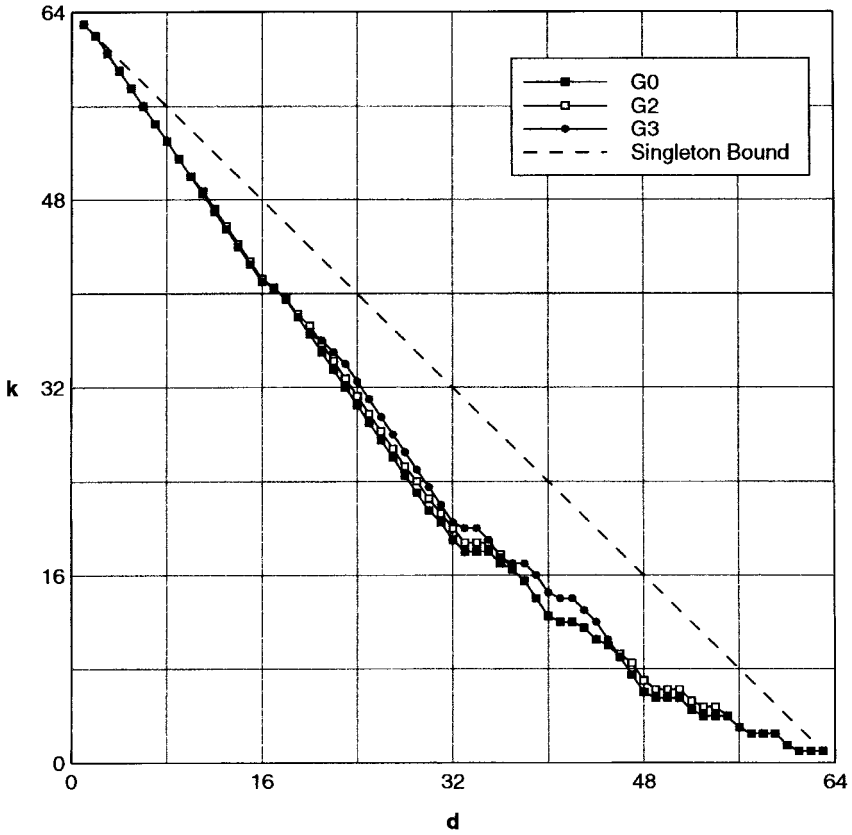

Fig. 2. The best SSRS codes for $m = 6, n = 63, \nu = 4, q = 16$.

7.3. Example: Finally, we consider $m = 6, \nu = 2$. This case is dual to the $(6, 4)$ case discussed in Example 7.2, and so there are again four categories of subspace:

$\mathbb{G}_0$	$\mathfrak{B}_0 = \{1, \alpha\}$	ordinary
$\mathbb{G}_1$	$\mathfrak{B}_1 = \{1, \alpha^7\}$	ordinary
$\mathbb{G}_2$	$\mathfrak{B}_2 = \{1, \alpha^9\}$	exceptional
$\mathbb{G}_3$	$\mathfrak{B}_3 = \{1, \alpha^{21}\}$	exceptional (subfield)

In Fig. 3, we see again that the subspace which gives the maximum dimension depends on the parameter d. In particular, the subspace $\mathbb{G}_3$, although it is a subfield, does not always give the maximum dimension. Once again we see that the best SSRS code need not be a subfield subcode.

B. Application to Concatenated Codes

We believe SSRS codes may provide an attractive alternative to RS codes in certain applications. For example, SSRS codes appear to be suitable as outer codes in concatenated coding schemes with inner convolutional codes.

Concatenated coding systems using an inner convolutional code and an outer RS code, are one of the most efficient schemes, currently known, for reliable digital communication over the additive white Gaussian noise (AWGN) channels [29]. In concatenated coding systems, a soft-input Viterbi decoder for the convolutional code is essential for channels with low signal-to-noise ratio, while a full algebraic decoder for the RS code is needed to correct burst errors from the Viterbi decoder, since a typical error from the Viterbi decoder is a long burst. RS codes can correct such long bursts if an interleaver is introduced. The famous "NASA standard" concatenated coding system used routinely in deep-space communication has an inner convolutional code with rate $1/2$, constraint length 7, and a $(255, 223, 33)$ outer RS code over GF(2^8).

However, for such systems, an RS code may not be the best choice for the outer code. Once we fix the constraint length of the inner convolutional code, we may obtain better performance by extending the length of the outer code while keeping the alphabet size fixed.

We now compare the performance of the standard NASA concatenated system to two others, obtained by replacing the outer RS code by two SSRS codes with the same alphabet size. For $m = 9$ and $\nu = 8$, there are SSRS codes over a 256-symbol alphabet with parameters $(511, 478, 30)$ and $(511, 465, 42)$. If we replace the NASA standard RS code by these SSRS codes, we can obtain better performance. Fig. 4 gives the decoded bit-error rate (BER) versus the bit signal-to-noise ratio E_b/N_0 for an AWGN channel. We see, for example, that the $(511, 478)$ SSRS code outperforms the standard $(255, 223)$ RS code in the concatenated system by 0.35 dB at BER $= 10^{-5}$.

Since SSRS codes enable us to extend the codelength while keeping the alphabet size fixed, there may be SSRS codes which outperform RS code still further. Thus a search for the "best" SSRS outer code is indicated.

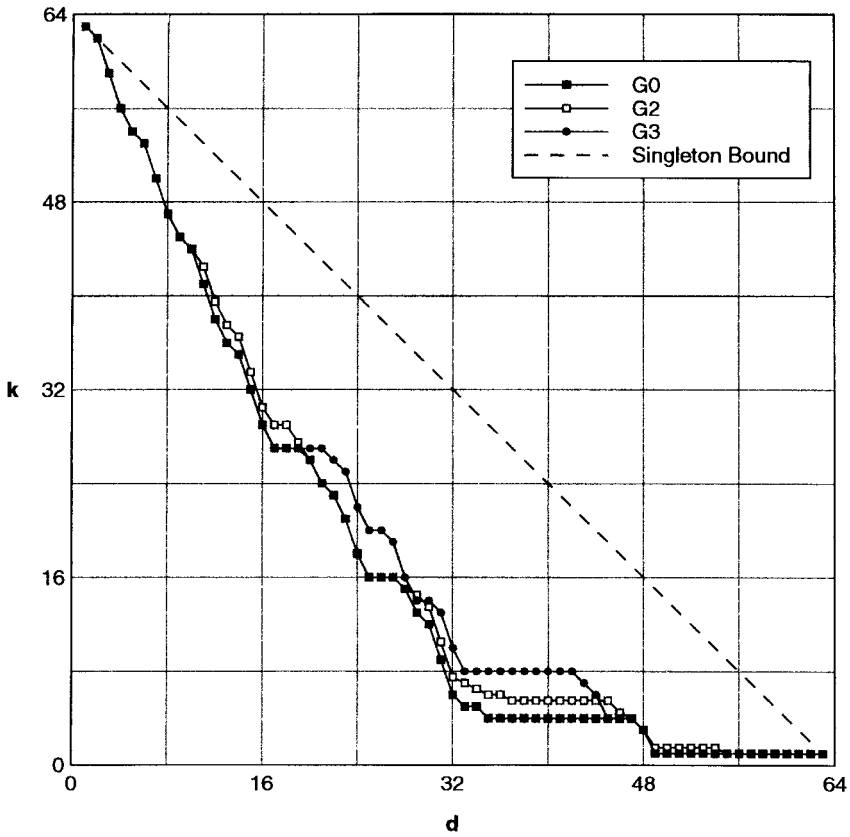

Fig. 3. The best SSRS codes for $m = 6, n = 63, \nu = 2, q = 4$.

C. Comparison to Algebraic-Geometry Codes

SSRS codes occupy a relatively uninhabited part of coding theory, in that they typically have codelengths much longer than RS codes with the same alphabet size. The only class of codes with parameters comparable to SSRS codes, that we are aware of, are the algebraic-geometry (AG) codes, and in this section we will briefly attempt to compare the two classes.

First, we briefly review the general construction for AG codes [21], [22]. However, it is not our purpose to go into detail, or to be self-contained.

Let X be a nonsingular projective curve of genus g over $K = \mathbb{F}_q$. Assume $P_1, \cdots, P_n$ are K-rational points on the curve X and let $D = P_1 + \cdots + P_n$. Assume G is a divisor on X with support consisting of only k-rational points and disjoint from D. For the range $2g-2 < \deg(G) < n$, the corresponding AG code has parameters (n, k, d) with

$$n = \deg(D) \tag{106}$$

$$k = \deg(G) - g + 1 \tag{107}$$

$$d \geq d^* = n - \deg(G) = (n - k + 1) - g. \tag{108}$$

Thus the codelength n is governed by the number of rational points on the curve X, and the dimension k of the AG code is smaller than that of MDS code with the same n and k, by an amount equal to the genus g of X. If $\deg(G)$ is not in the range $2g - 2 < \deg(G) < n$, the dimension k may be higher than the value given by (107) [30].

In order to obtain good AG codes, one should find curves with as many rational points as possible. However, for a given genus g and symbol size q, the number of rational points is upper-bounded by the Hasse–Weil bound [1] as follows:

$$n_{\mathrm{AG}} \leq q + 1 + \lfloor 2g\sqrt{q} \rfloor. \tag{109}$$

Only a few classes of curves which reach the Hasse–Weil bound are known. These include the elliptic curves and Hermitian curves. For comparison with SSRS codes, we will first study AG codes constructed from Hermitian curves.

The AG codes over GF(q^2) derived from a Hermitian curve have the following parameters:

$$n = q^3 \tag{110}$$

$$d \geq d^* = (n - k + 1) - (q^2 - q)/2 \tag{111}$$

for k in the range $q^2 - q - 2 < k < n$.

For example, with symbol alphabet size $q^2 = 4^2 = 16$, there exists a family of Hermitian codes of length $n = 4^3 = 64$ and genus $g = (4^2 - 4)/2 = 6$, i.e., these Hermitian codes have parameters $(64, k, 59 - k)$ in the range $10 < k < 64$. If k is not in the specified range, i.e., for high and low rates, the true minimum distance can be higher than the designed minimum distance. Fortunately, the true minimum distance of Hermitian codes has been exactly determined in [30]. It is also known that, with the recent decoding algorithm of Feng and Rao [6], we can decode Hermitian codes up to the true minimum distance [14]. Therefore, for a fair comparison to SSRS codes, we use the true minimum distance of Hermitian codes from [30]. Let us try to compare the family of Hermitian codes of length 64 over GF(16) to their SSRS counterparts.

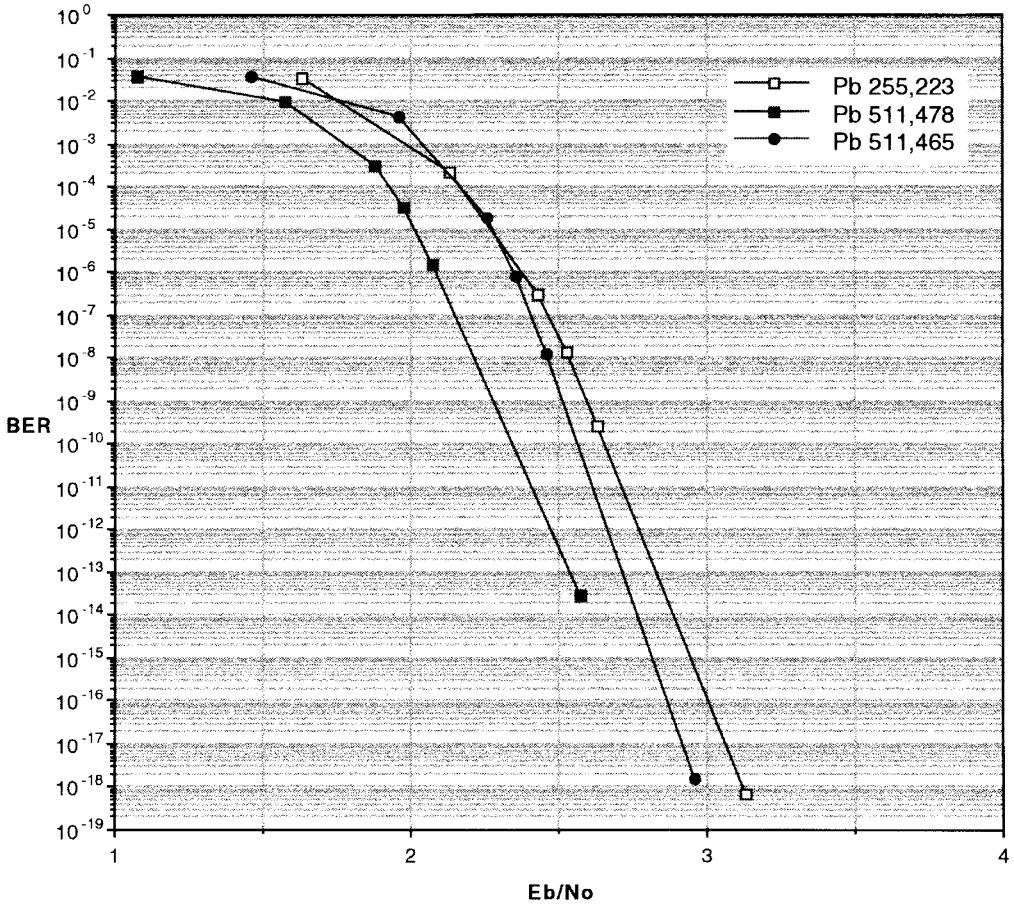

Fig. 4. Bit-error rate versus signal-to-noise ratio E_b/N_0 in a concatenated coding scheme with the $R = 1/2, M = 7$ NASA standard convolutional code. Two SSRS codes, and an RS code are compared (fixed symbol size $q = 256$). (This figure is based on simulation results of Dr. Fabrizio Pollara at the Jet Propulsion Laboratory, Pasadena, CA.)

For $m = 6$, the "natural" codelength of SSRS codes is 63, not 64. In order obtain length-64 SSRS codes, we extend the codes by appending an overall parity-check. In general, this transforms an (n, k, d) SSRS code into an $(n+1, k, d+1)$ extended SSRS code. Here d is the *designed* minimum distance, which is appropriate for comparison to AG codes, since we cannot decode SSRS codes out to the true minimum distance.

Fig. 5 shows the dimensions of Hermitian codes and SSRS codes versus the minimum distance for $n = 64$ and $q = 16$. We see that the two are very close and, even at rate $1/2$, where the Hermitian codes are best, SSRS codes are closely competitive.

Fig. 6 shows a "zoomed" plot in the high rate area, which is important for many applications. We see that, for $d \leq 14$, SSRS codes are consistently superior to Hermitian codes.

The Hasse–Weil bound says, for $q = 16$, that $n = 64$ (or possibly $n = 65$) is the maximum achievable codelength for AG codes from curves of genus 6. To go further, one needs a curve of genus $g > 6$ which also achieves the Hasse–Weil bound. Unfortunately, no such curves are known. In contrast, there is virtually no limitation on extending the codelength for SSRS codes with a fixed symbol alphabet size. For example, for $q = 16$, if we start from a parent RS code with $m = 7$, SSRS codes of length 127 over a 16-letter alphabet can easily be found.

As the alphabet size increases, Hermitian codes become increasingly superior to SSRS codes *for the values of n, q, and g available for Hermitian codes*. However, it is important to note that SSRS codes are available for may sets of parameters for which there are no comparable AG codes.

We should also compare the decoding complexities of these codes. The most efficient decoding algorithm of AG codes, up to designed minimum distance, currently known, is the Sakata *et al.* algorithm [24], whose complexity is $\mathcal{O}(n^{7/3})$. The decoding of SSRS codes is much easier, however, since the well-developed decoding algorithms for RS codes can be applied directly. The decoding complexity of RS codes is, according to Blahut [3], "greater than $O(n \log n)$ by the thinnest of margins."

In conclusion: for given values of n and q, high-rate SSRS codes are often superior to AG codes, and if we consider not only the code parameters but also the decoding complexity of the codes, SSRS codes become more attractive. Furthermore, SSRS codes are available for a much larger range of parameters than are the AG codes.

D. An Interesting Family of SSRS Codes

In this section, we derive an infinite family of SSRS codes using the dimension formula provided by Theorem 4.4, and make some remarks on a recent conjecture about quasi-MDS codes made in [21].

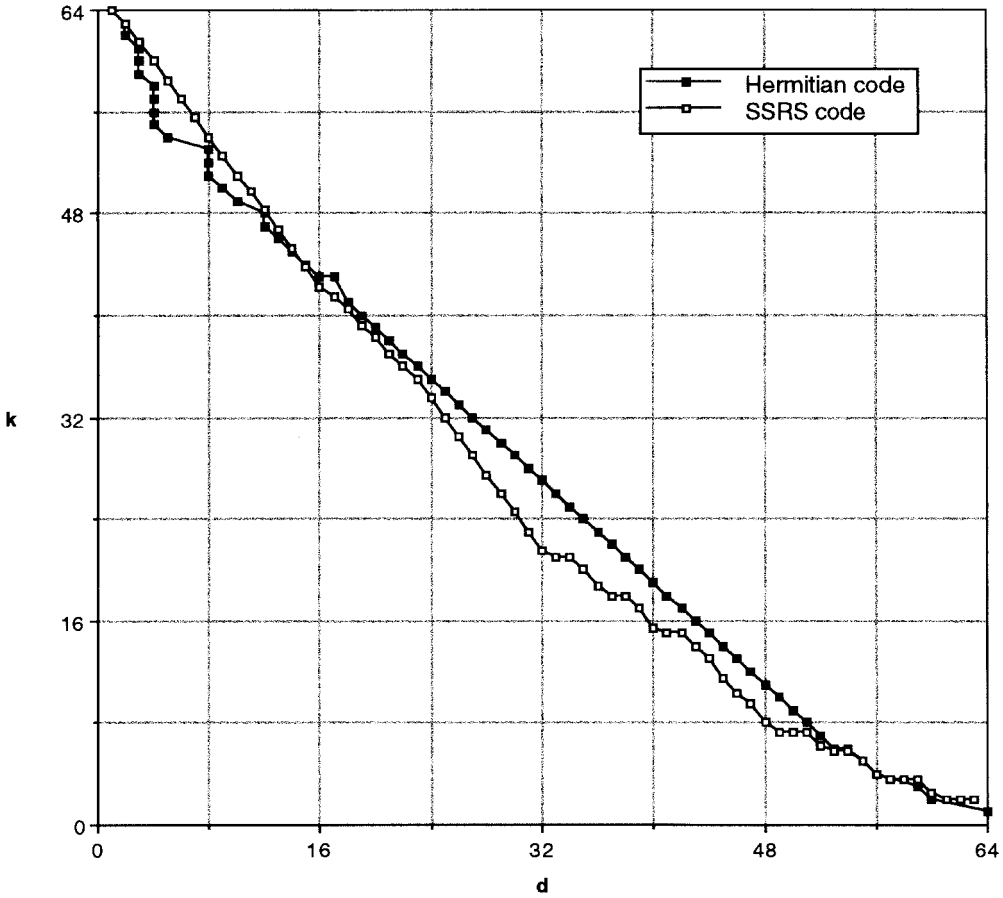

Fig. 5. Dimension and minimum distance of SSRS codes and Hermitian codes for $q^2 = 16$, $n = 64$, $g = 6$.

We begin with an RS code with $J = \{1, \cdots, k_0\}$ and construct an SSRS code with $\mu = 1$, i.e., $\nu = m - 1$. For $\mu = 1$, the binary dimension of the SSRS code is always equal to the lower bound of Corollary 4.8. We restrict the dimension of the parent code to be $k_0 \geq 2^{m-1} - 1$, which ensures that every cyclotomic coset except for the zero coset, is occupied. The binary dimension of such SSRS codes is given by

$$\begin{aligned} K(\mathbb{C}, \mathcal{S}) &= mk_0 - \sum_{\substack{j \in I_n \\ j \neq I_0}} d_j \\ &= mk_0 - (2^m - 2). \end{aligned} \tag{112}$$

For convenience, we want this binary dimension to be a multiple of $\nu = m - 1$, so that the pseudodimension $k = K/(m-1)$ will be an integer. This requires

$$mk_0 - 2^m + 2 \equiv 0 \pmod{m-1} \tag{113}$$

$$k_0 - 2^m + 2 \equiv 0 \pmod{m-1}. \tag{114}$$

In terms of the redundancy $r = 2^m - 1 - k_0$, (114) becomes

$$r \equiv 1 \pmod{m-1} \tag{115}$$

where $r \leq 2^{m-1}$ since $k_0 \geq 2^{m-1} - 1$. Thus we have the family given in Table II.

In Table II, g^* denotes the penalty which is paid to extend the codelength. A penalty $g^* = 0$ corresponds to an MDS code. We shall call the number g^* the *pseudogenus* of the code, in view of (108). For example, for the family with $r = m$, we get the sequence of codes, all with pseudogenus equal to 1, in Table III. (A code with pseudogenus equal to 1 is sometimes called a *quasi-MDS* code.)

TABLE II
SOME FAMILIES OF SSRS CODES WITH SMALL PSEUDOGENUS

r	k_0	k	d	g^*
1	$2^m - 2$	$2^m - 2$	2	0
m	$2^m - m - 1$	$2^m - m - 2$	$m + 1$	1
$2m - 1$	$2^m - 2m$	$2^m - 2m - 2$	$2m$	2
$3m - 2$	$2^m - 3m + 1$	$2^m - 3m - 2$	$3m - 1$	3
$4m - 3$	$2^m - 4m + 2$	$2^m - 4m - 2$	$4m - 2$	4
$5m - 4$	$2^m - 5m + 3$	$2^m - 5m - 2$	$5m - 3$	5

Similarly, for the family with $r = 2m - 1$, i.e., pseudogenus $g^* = 2$, we get the sequence of codes, in Table IV.

In [21], several research problems are presented about the optimality of AG codes which meet the Hasse–Weil bound. Here is one of them.

7.4. Conjecture ([21, Research Problem 10.5]): Given an (n, k, d) code over the q symbol alphabet from an algebraic curve that achieves the Hasse-Weil bound, it is impossible to have a code which has parameters $(n, k, \hat{d})$ with $\hat{d} > d$.

Examining Tables III and IV, we see that the family of SSRS codes includes infinitely many codes whose length exceeds the best possible AG code with the same values of q and

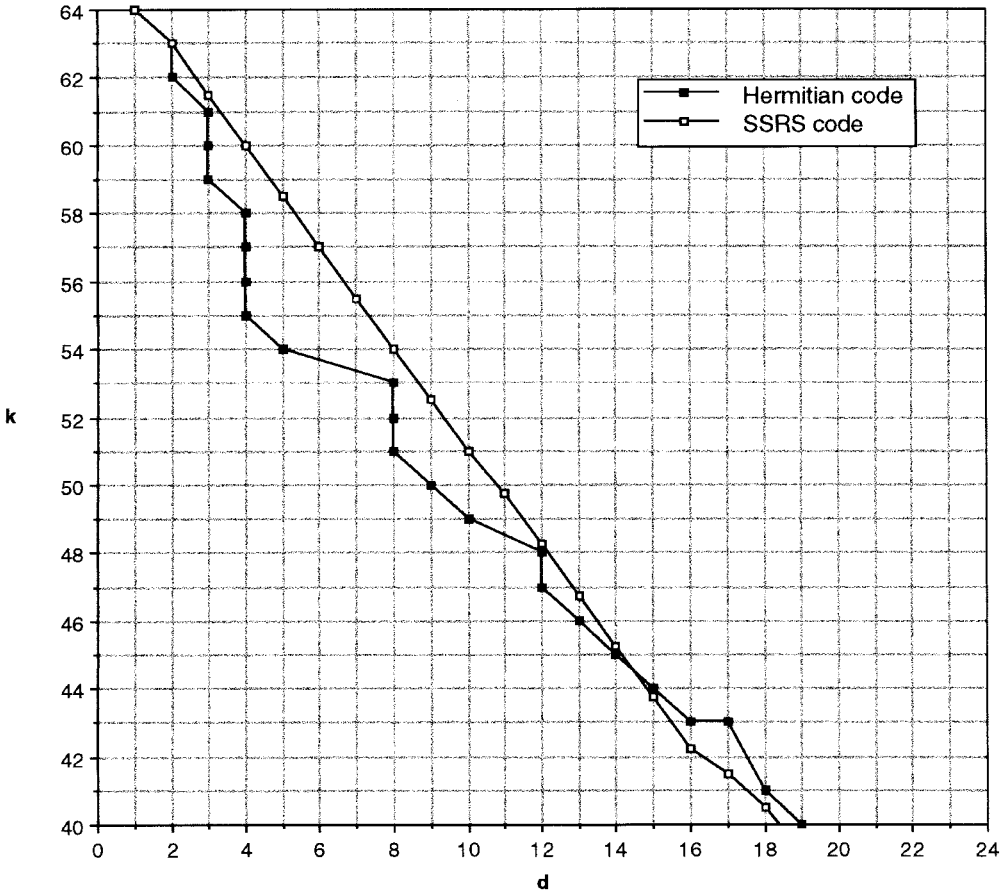

Fig. 6. High-rate Hermitian codes and SSRS codes for $q^2 = 16$, $n = 64$.

TABLE III
A FAMILY OF SSRS CODES OF PSEUDOGENUS 1.
(HERE n_{AG} DENOTES THE HASSE–WEIL UPPER BOUND (109) ON n FOR AG CODES WITH THE SAME VALUES OF q AND g)

m	q	(n,k,d)	n_{AG}
3	4	$(7,3,4)$	9
4	8	$(15,10,5)$	14
5	16	$(31,25,6)$	21
6	32	$(63,56,7)$	44
7	64	$(127,119,8)$	81

TABLE IV
A FAMILY OF SSRS CODES OF PSEUDOGENUS 2.
(HERE n_{AG} DENOTES THE HASSE–WEIL UPPER BOUND (109) ON n FOR AG CODES WITH THE SAME VALUES OF q AND g)

m	q	(n,k,d)	n_{AG}
3	4	$(7,3,4)$	13
4	8	$(15,6,8)$	20
5	16	$(31,20,10)$	33
6	32	$(63,50,12)$	55
7	64	$(127,112,14)$	97

g. What this tells us about Conjecture 7.4 depends on how one interprets it. Superficially, it appears that SSRS codes provide counterexamples to the conjecture. However, if one interprets the conjecture as a question about the existence of certain *linear* codes over GF(q), SSRS codes, being nonlinear in general, are not counterexamples. But in that case, either the conjecture is false, or else there are infinitely many SSRS codes with parameters superior to any comparable linear code. Thus however one interprets the conjecture, SSRS codes provide food for thought.

VIII. CONCLUSIONS AND OPEN PROBLEMS

Although SSRS codes are promising in many ways, there are many unsolved problems related to them. We conclude with a list of such problems.

- How can one find the true minimum distance of an SSRS code?
- Is it possible to reduce the decoding complexity for SSRS codes by taking advantage of the fact that the SSRS code has a smaller symbol alphabet than the parent RS code? (For example, in the special case $\nu = 1$, SSRS codes are just binary BCH codes, and it is known that these codes are somewhat easier to decode than RS codes [3].)
- How can one find the "best" subspace of GF(2^m) for constructing an SSRS code?
- We have investigated SSRS codes only in the case of RS codes over the field GF(2^m). It would be interesting to generalize this work, especially Theorem 4.4, to GF(q^m).
- If, instead of RS codes, we begin with *generalized RS* codes [17], what new codes result?

- In our definition of SSRS codes, we have insisted that each codeword coordinate belong to the same ν-dimensional subspace. Is there anything to be gained by specifying different subspaces for the different coordinate positions?
- As mentioned above, our main result, Theorem 4.4, can be viewed as a generalization of Berlekamp's elementary lemma [2, Lemma 12.11] on the dimension of binary BCH codes. Is is possible to begin with our Theorem 4.4 and go on to generalize some or all of the rest of Berlekamp's work?

REFERENCES

[1] A. M. Barg, G. L. Katsman, and M. A. Tsfasman, "Algebraic-geometric codes from curves of small genus," *Probl. Pered. Inform.*, vol. 23, pp. 42–46, Jan.–Mar. 1987.

[2] E. R. Berlekamp, *Algebraic Coding Theory, Revised 1984 Edition*. Laguna Hills, CA: Aegean Park, 1984.

[3] R. E. Blahut, *Theory and Practice of Error-Control Codes*. Reading, MA: Addison-Wesley, 1983.

[4] C. Couvreur and P. Piret, "Codes between BCH and RS codes," *Philips J. Res.*, vol. 39, pp. 195–205, 1984.

[5] Y. Edel and J. Biebrauer, "Twisted BCH codes," *IEEE Trans. Inform. Theory*, to be published.

[6] G. L. Feng and T. R. N. Rao, "Decoding algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 39, pp. 37–45, Jan. 1993.

[7] G. D. Forney, Jr., "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1741–1752, Nov. 1994.

[8] J. N. Franklin, *Matrix Theory*. Englewood Cliffs, NJ: Prentice-Hall, 1968.

[9] M. Hattori, R. J. McEliece, and W. Lin, "Subspace subcodes of Reed-Solomon codes," in *Proc. 1994 IEEE Int. Symp. Information Theory* (Trondheim, Norway, 1994), p. 430.

[10] M. Hattori and R. J. McEliece, "Classification of vector spaces over finite fields," in preparation.

[11] M. Hattori, R. J. McEliece, and G. Solomon, "On the encoding of shortened linear codes," in preparation.

[12] M. Hattori, "Subspace subcodes of Reed-Solomon codes," Ph.D. dissertation, Calif. Inst. Technol., Pasadena, May 1995.

[13] J. M. Jensen, "Subgroup subcodes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 781–785, May 1995.

[14] C. Kirfel and R. Pellikaan, "The minimum distance of codes in an array coming from telescopic semigroups," informal publication, May 7, 1993.

[15] C. Le Dantec and P. Piret, "An encoder to match Reed-Solomon codes over GF(q) to a subalphabet of GF(q)." submitted to *IEEE Trans. Inform. Theory.*

[16] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications*. Reading, MA: Addison-Wesley, 1983.

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: Elsevier, North-Holland, 1977.

[18] R. J. McEliece and G. Solomon, "Trace-shortened Reed-Solomon codes," in *Proc. 2nd Int. Symp. Communication Theory and Applications* (Ambleside, UK, July 1993).

[19] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Boston, MA: Kluwer, 1987.

[20] ———, "On the BCJR trellis for linear block codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1072–1092, July 1996.

[21] A. J. Menezes, Ed., *Applications of Finite Fields*. Boston, MA: Kluwer, 1993.

[22] O. Pretzel, *Error-Correcting Codes and Finite Fields*. Oxford, U.K.: Oxford Univ. Press, 1992.

[23] J. J. Rotman, *An Introduction to the Theory of Groups*, 4th ed. New York: Springer-Verlag, 1995.

[24] S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen, and T. Hoholdt, "Fast decoding of algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 41, pp. 46–51, Sept. 1995.

[25] G. Solomon, "A note on alphabet codes and fields of computation," *Inform. Contr.*, vol. 25, pp. 395–398, 1974.

[26] ———, "Nonlinear, nonbinary cyclic group codes," JPL TDA Progr. Rept., vol. 43, pp. 84–95, Feb. 1992.

[27] ———, "Nonlinear, non-binary cyclic group codes," in *Proc. 1993 IEEE Int. Symp. Information Theory*, 1993, p. 192.

[28] L.-J. Weng, "Reed-Solomon error correction code encoder," European patent 0 290 349, 1988.

[29] S. B. Wicker and V. K. Bhargava, Eds., *Reed-Solomon Codes and Their Applications*. Piscataway, NJ: IEEE, 1994.

[30] K. Yang and P. V. Kumar, "On the true minimum distance of Hermitian codes," in *Coding Theory and Algebraic Geometry, Lecture Notes in Mathematics 1518*, H. Stichtenoth and M. A. Tsfasman, Eds. Berlin, Germany: Springer-Verlag, 1992, pp. 99–107.