Subspace Subcodes of Reed-Solomon Codes[1]

Masayuki Hattori Robert J. McEliece Wei Lin
California Institute of Technology
Pasadena, California 91125, USA

Abstract — **A subspace subcode of a Reed-Solomon (SSRS) code over $GF(2^m)$ is the set of RS codewords, whose components all lie in a particular $GF(2)$-subspace of $GF(2^m)$. SSRS codes include both generalized BCH codes and "trace-shortened" RS codes [2][3] as special cases. In this paper we present an explicit formula for the dimension of an arbitrary RS subspace subcode. Using this formula, we find that in many cases, SSRS codes are competetive with algebraic geometry codes, and that in some cases, the dimension of the best subspace subcode is larger than that of the corresponding GBCH code.**

I. Introduction. Definition of SSRS Codes.

Let $\mathcal{C}$ be the (n, k_0, d_0) RS code over $GF(2^m)$ defined by the parity-check polynomial $h(x) = \prod_{j=1}^{k_0}(x - \alpha^j)$, where α is a primitive nth root of unity in $GF(2^m)$, and $d_0 = n - k_0 + 1$. Let $\mathcal{S}$ be a ν-dimensional $GF(2)$-subspace of $GF(2^m)$. We define the subspace subcode $\mathcal{C}_\mathcal{S}$ to be the set of all codewords from $\mathcal{C}$, whose components all lie in $\mathcal{S}$. The code $\mathcal{C}_\mathcal{S}$ is thus a cyclic group code of length n over the Abelian group $\mathcal{S}$ of size 2^ν, with minimum distance at least d_0. For example, if $\mathcal{S} = GF(2^\nu)$, where $\nu | m$, the corresponding SSRS code is a generalized BCH code. Also, if we consider subspaces $\mathcal{S}$ which have dual bases of the form $\{1, \alpha, \alpha^2, \ldots, \alpha^{\mu-1}\}$, we obtain the class of "TSRS" codes [3], which are in turn a generalization of the codes introduced by Solomon [2].

II. Main Result. Dimension Formula.

Suppose $\mathcal{S}$ has basis $\{\beta_0, \ldots, \beta_{\nu-1}\}$ and "trace-dual" basis $\{\gamma_0, \ldots, \gamma_{\mu-1}\}$, where $\mu = m - \nu$ and $\mathrm{Tr}_1^m(\beta_i \gamma_j) = 0$ for all i, j. Let $\{j2^i : i = 0 \ldots, d_j - 1\}$ be the jth cyclotomic coset modulo n, where d_j is the degree of j mod n. Let $J = \{1, 2, \ldots, k_0\}$. We define the jth index set A_j for the SSRS code $\mathcal{C}_\mathcal{S}$ as $A_j = \{i : 0 \le i \le m - 1 \text{ and } j \cdot 2^i \bmod n \in J\}$, with $|A_j| = a_j$. We define the jth cyclotomic matrix for $\mathcal{C}_\mathcal{S}$ to be the $\mu \times a_j$ matrix Γ_j whose (h, i)th entry is $\gamma_h^{2^i}$ where $h = 0, \ldots, \mu - 1$ and $i \in A_j$. The rank of Γ_j is denoted by r_j.

Theorem 1. *The binary dimension of the SSRS code as defined above is given by the formula*

$$K(\mathcal{C}, \mathcal{S}) = \sum_{j \in I_n} d_j (a_j - r_j), \tag{1}$$

where I_n denotes a complete set of representatives of the modulo n cyclotomic cosets. Thus $\mathcal{C}_\mathcal{S}$ is an (n, k, d_0^+) cyclic group code over $\mathcal{S}$, where $k = K(\mathcal{C}, \mathcal{S})/\nu$. (The notation d_0^+ means that the true minimum distance of the code is at least d_0.)

Since Γ_j is a $\mu \times a_j$ matrix, it follows that $r_j \le \min(\mu, a_j)$, and so we have the following Corollary.

Corollary 1. *With the same hypotheses as Theorem 1, we have the lower bound*

$$K(\mathcal{C}, \mathcal{S}) \ge \sum_{j \in I_n} \max(d_j(a_j - \mu), 0). \tag{2}$$

It is possible to show that if $\mathcal{S}$ has a dual basis of the form $\{1, \beta, \ldots, \beta^{\mu-1}\}$, where β is an element of degree m in $GF(2^m)$, then the lower bound of Corollary 1 is exact, for all parent RS codes $\mathcal{C}$. (This result is a small generalization of the main result proved in [3].) In fact, extensive numerical experimentation indicates that "most" subspaces $\mathcal{S}$ have this property, although we do not have a fully satisfactory theoretical explanation of this phenomenon.

III. Examples and Conclusion.

Example 1. Let $m = 4$, $n = 15$, $k_0 = 9$ and $\nu = 2$. Suppose $\mathcal{S}_0$ and $\mathcal{S}_1$ are spanned by $\{1, \alpha\}$ and $\{1, \alpha^5\}$, respectively. Starting from a parent $(15, 9, 7)$ RS code $\mathcal{C}$, and using Theorem 1, we find that $\mathcal{C}_{\mathcal{S}_0}$ is a $(15, 6, 7^+)$ code over $\mathcal{S}_0$ and $\mathcal{C}_{\mathcal{S}_1}$ is a $(15, 7, 7^+)$ code over $\mathcal{S}_1$. $\mathcal{C}_{\mathcal{S}_0}$ is equivalent to a TSRS code given in [3]. On the other hand, since $\mathcal{S}_1 = GF(4)$, $\mathcal{C}_{\mathcal{S}_1}$ is a GBCH code.

Example 2. Let $m = 6$, $n = 63$, $k_0 = 53$ and $\nu = 2$. Suppose $\mathcal{S}_0$ and $\mathcal{S}_1$ are spanned by $\{1, \alpha^9\}$ and $\{1, \alpha^{21}\}$, respectively. (Thus $\mathcal{S}_1 = GF(4)$.) Starting from a parent $(63, 53, 11)$ RS code, and using Theorem 1, we find that $\mathcal{C}_{\mathcal{S}_0}$ is a $(63, 42.5, 11^+)$ code over $\mathcal{S}_0$, and $\mathcal{C}_{\mathcal{S}_1}$ is a $(63, 41, 11^+)$ GBCH code over $GF(4)$. Note that the dimension of $\mathcal{C}_{\mathcal{S}_0}$ is higher than that of the GBCH code $\mathcal{C}_{\mathcal{S}_1}$.

The only codes with parameters comparable to subspace subcodes that we are aware of are the algebraic geometry (AG) codes, e.g., [1]. For a given length n and alphabet size q, high-rate subspace subcodes are often superior to AG codes. Furthermore, decoding a subspace subcode up to the designed distance d_0 is almost the same as for the parent RS codes, which of course is quite easy. Thus subspace subcodes may provide an attractive alternative to AG codes in certain practical applications, such as outer codes in concatenated coding schemes.

[1] Wei Lin's contribution, and a portion of Robert McEliece's contribution, was supported by AFOSR grant no. F49620-94-1-005. A portion of McEliece's contribution was done at the Jet Propulsion Laboratory, California Institute of Technology, under contract to the National Aeronautics and Space Administration. Masayuki Hattori's contribution was sponsored by the Sony Corporation.

References

[1] A. M. Barg, G. L. Katsman and M. A. Tsfasman, "Algebraic-Geometric Codes from Curves of Small Genus." Problemy Peredachi Informatsii, Vol. 23, No. 1, (January–March 1987) pp. 42–46.

[2] Gustave Solomon, "Nonlinear, Nonbinary Cyclic Group Codes." JPL TDA Progress Report vol. 43–108 (February 1992), pp. 84–95. *See also* Proc. ISIT 93, p. 192.

[3] R. J. McEliece and G. Solomon, "Trace-Shortened Reed-Solomon Codes." Proc. 2nd International Symposium on Communication Theory and Applications, Ambleside, UK, July 1993.

0 - 7803-2015-8/94/$4.00 ©1994 IEEE