MDS Array Codes with Independent Parity Symbols

Mario Blaum
IBM Almaden Research Center
650 Harry Rd., San Jose, CA 95120
blaum@almaden.ibm.com

Jehoshua Bruck*
California Institute of Technology
Pasadena, CA 91125
bruck@systems.caltech.edu

Alexander Vardy**
Coordinated Science Laboratory
University of Illinois, Urbana, IL 61801
vardy@golay.csl.uiuc.edu

Abstract — **A new family of MDS array codes is presented. The code arrays contain p information columns and r independent parity columns, where p is a prime. We give necessary and sufficient conditions for our codes to be MDS, and then prove that if p belongs to a certain class of primes these conditions are satisfied up to $r \leq 8$. We also develop efficient decoding procedures for the case of two and three column errors, and any number of column erasures. Finally, we present upper and lower bounds on the average number of parity bits which have to be updated in an MDS code over GF(2^m), following an update in a single information bit. We show that the upper bound obtained from our codes is close to the lower bound and does not depend on the size of the code symbols.**

I. Introduction

This work is concerned with maximum distance separable (MDS) codes. The Reed-Solomon (RS) codes are a well-known example of MDS codes. However, with Reed-Solomon codes, (a) the encoding and decoding procedures are performed as operations over a finite field, and (b) an update in a single information bit requires an update in all the parity symbols and affects a number of bits in each symbol. These two properties of RS codes are quite undesirable for certain channels. Firstly, the fact that encoding/decoding is performed in a finite field makes it unfeasible to use large symbols, since the size of the field grows exponentially with the symbol size. Secondly, the fact that an update in a single information bit requires to re-compute most of the parity bits is particularly undesirable in storage applications where the stored data has to be frequently updated in real-time. In this work, we present a new family of MDS codes having the following two properties: encoding and decoding may be accomplished with simple cyclic shifts and XOR operations on the code symbols, without finite field operations; and an update in an information bit affects a minimal number of parity bits.

II. The New MDS Array Codes

Our new codes are based on recent work in array codes [1, 3]. We assume that the information is presented as a two-dimensional array of bits. Henceforth we will identify the symbols of an MDS code with the columns of such an array. Thus the errors that can occur are column errors.

A trivial example of an MDS array code of this type is a simple parity code. This code is defined by requiring that the last column in the array is a parity column, given by the exclusive-OR of the other columns. The first nontrivial generalization of the parity code is the EVENODD code introduced in [1]. The EVENODD code has columns of size $p-1$ for some prime p, and requires two parity symbols. It can correct one error or two erasures.

In this paper, we generalize the construction of the EVENODD code to a family of codes with p information columns and r parity columns, for $r \geq 1$. We assume that p is prime number, and let $M_p(x) = 1 + x + \cdots + x^{p-1}$ with $M_p(x) \in \mathbb{F}_2[x]$. Consider the code C whose entries are in the ring of polynomials modulo $M_p(x)$, defined by the parity-check matrix:

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 & 1 & 0 & \dots & 0 \\ 1 & \alpha & \dots & \alpha^{p-1} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{r-1} & \dots & \alpha^{(r-1)(p-1)} & 0 & 0 & \dots & 1 \end{pmatrix}$$

It is not difficult to show that this code is MDS for all p when $r = 2$ or $r = 3$. However, this is no longer true when $r \geq 4$. We give necessary and sufficient conditions for the code to be MDS when $r \geq 4$. Although we determined completely the primes $p \leq 100$ for which this code is MDS when $r \leq 8$, checking the necessary and sufficient conditions in the general case may be very complex. Our solution to this problem is related to certain generalizations of Vandermonde determinants called alternants. Using alternants, we have been able to show that if 2 is primitive in $\mathbb{F}_p$, then our codes are MDS up to $r = 5$ for all $p \neq 3$, and up to $r = 8$ for all $p \notin \{3, 5, 11, 13, 19, 29\}$.

III. Decoding and Information Updates

We present a decoding algorithm for the case of two symbol errors, that is for $r = 4$. Notably, this algorithm does not require finite field operations. This extends the algorithms of [3], applicable only for the case of a single symbol error.

Finally, we present lower and upper bounds on the average number $\eta(C)$ of parity bits affected by an update in a single information bit. In particular, we investigate the behavior of $\eta(C)$ for MDS codes over GF(2^m). It is shown that for our codes $\eta(C)$ *does not depend* on the size of the code symbols. In contrast, we also show that for Reed-Solomon codes, as well as for the MDS codes of Blaum and Roth [3], $\eta(C)$ increases linearly with the symbol size.

All these properties of the new MDS array codes make them very well suited for applications where the size of the code symbols is required to be large. We refer the reader to [2] for further details.

*Supported by the NSF Young Investigator Award CCR-9457811, by the Sloan Research Fellowship, and by grants from the IBM Almaden Research Center and the AT&T Foundation.

**Research supported in part by a grant from the Joint Services Electronics Program.

References

[1] M. Blaum, J. Brady, J. Bruck and J. Menon, "EVENODD: an optimal scheme for tolerating double disk failures in RAID architectures," *IEEE Trans. Computers*, vol. 44, pp. 192–202, 1995.

[2] M. Blaum, J. Bruck and A. Vardy, "MDS array codes with independent parity symbols," IBM Research Report, RJ 9887 (87267), September 1994.

[3] M. Blaum and R.M. Roth, "New array codes for multiple phased burst correction," *IEEE Trans. on Information Theory*, vol. 39, pp. 66–77, 1993.