Systematic MDS Erasure Codes Based on Vandermonde Matrices

Jérôme Lacan and Jérôme Fimes

***Abstract*—An increasing number of applications in computer communications uses erasure codes to cope with packet losses. Systematic maximum-distance separable (MDS) codes are often the best adapted codes. This letter introduces new systematic MDS erasure codes constructed from two Vandermonde matrices. These codes have lower coding and decoding complexities than the others systematic MDS erasure codes.**

***Index Terms*—Packet erasure channel, systematic MDS code, Vandermonde matrices.**

I. Introduction

THE recent past has shown a wide use of error-correcting codes in several kinds of computer communications like real-time [1], [2], multicast ones [3], [4] or distributed storage systems [5]. In these contexts, sending proactive redundant packets instead of using automatic request (ARQ) retransmissions to cope with data packet losses appears to be more efficient. In all these applications, packets are considered to be either error-free, or lost. Error-correcting codes used in this channel are called erasure codes.

In order to protect k transmitted packets, $n-k$ additional redundant packets are also sent. This aims at recovering the k initial packets even if some of the sent packets were lost. A class of erasure codes can recover the k initial packets provided *any* k packets among the n transmitted ones are received. These codes, featuring an optimal correction capability, are called maximum-distance separable (MDS) codes [6].

In computer communications, erasure codes are classically used in systematic form, i.e. the information data is a part of the encoded data. In practical applications, the construction of systematic erasure codes is based on $k \times (n-k)$-matrices with the property that any square submatrix is nonsingular. Vandermonde and Cauchy matrices are used in this context.

This letter focuses on Vandermonde matrices based codes. Indeed, they feature fast algorithms as regards inversion and matrix-vector multiplication [7]. However, Section II points out that these matrices, when defined over a finite field, can contain singular square submatrices and therefore, a systematic erasure code built from a single Vandermonde matrix cannot recover the k original packets from any configurations of k received packets. To cope with this problem, Section III introduces a new construction of systematic MDS erasure codes based on two Vandermonde matrices. It is shown that these codes have lower coding and decoding complexities than any other systematic MDS erasure codes.

Manuscript received January 14, 2004. The associate editor coordinating the review of this letter and approving it for publication was Prof. C. Chao. This letter has appeared in part in the *Proceedings of the Seventh International Conference on Finite Fields and Applications*, Toulouse, France, May 2003.

The authors are with the Department of Applied Mathematics and Information Technology of the ENSICA, 30156 Toulouse, France, and also with the Cooperative Laboratory in Telecommunications for Space and Aeronautics (TéSA), 31053 Toulouse, France (e-mail: jerome.lacan@ensica.fr).

Digital Object Identifier 10.1109/LCOMM.2004.833807

II. Classical Constructions of Systematic MDS Erasure Codes for the Packet Erasure Channel

In computer communications, the erasure code protecting k information packets with $n-k$ redundant packets is usually chosen as a $[n,k]$-linear code over a finite field $\mathbb{F}_q$ (where $q=2^m$), and the data are interleaved with a depth of sz, where sz is the number of elements of m bits contained in the packets. In other words, with this structure, for any $i \leq n$, the i^{th} packet contains the i^{th} coefficient of each codeword.

For the packet erasure channel, the construction of the systematic MDS codes is based on the following theorem:

Theorem 1 ([6, p. 321]): A $[n,k,d]$ code C with generator matrix $G=[I|A]$, where A is a $k \times (n-k)$-matrix, is MDS if and only if every square submatrix (formed from any i rows and any i columns, for any $i=1,\ldots,min\{k,n-k\}$) of A is nonsingular.

The encoding of a message of k elements $i=(i_1,\ldots,i_k)$ of $\mathbb{F}_q$ is processed by multiplying the latter by the generator matrix as follows:

$$(i_1,\ldots,i_k) \times G = (c_1,\ldots,c_n).$$

Clearly, since G is systematic, $c_j = i_j$ for $j=1,\ldots,k$.

For the decoding, let us consider the reception of the vector $(c_{u_1},c_{u_2},\ldots,c_{u_k})$, where $1 \leq u_1 < u_2 < \ldots < u_k \leq n$. Let $G_{u_1,\ldots,u_k}$ be the $k \times k$-matrix composed of the columns $u_1,\ldots,u_k$ of G. We have:

$$(i_1,\ldots,i_k) \times (G_{u_1,\ldots,u_k}) = (c_{u_1},c_{u_2},\ldots,c_{u_k}).$$

Since the code is supposed to be MDS, then necessarily, $G_{u_1,u_2,\ldots,u_k}$ is nonsingular (see [6, Cor. 3, p. 319]). Then, the decoding consists in computing the inverse of $G_{u_1,\ldots,u_k}$ and in processing the product:

$$(i_1,\ldots,i_k) = (c_{u_1},c_{u_2},\ldots,c_{u_k}) \times (G_{u_1,\ldots,u_k})^{-1}.$$

Note that the interleaved structure of the codewords implies that the packet losses produce the same erasure pattern for each of the interleaved codewords. Therefore, only one matrix inversion is necessary for the decoding of the set of the interleaved codewords. The running time of this operation can be neglected compared to the sz matrix-vector multiplications needed to decode the sz interleaved codewords (see [2]).

Consequently, constructing a MDS code is equivalent to finding a $k \times (n-k)$-matrix A such that any square matrix built from l columns of I_k and $k-l$ columns of A is nonsingular, for $l \leq k$. This problem is equivalent to finding a $k \times (n-k)$-matrix A such that any $l \times l$-submatrix of A is nonsingular, for $l \leq k$.

In practical applications, the redundancy is computed from two classes of matrices: Cauchy or Vandermonde ones.

First, Cauchy matrices are defined from two vectors $(a_i)_{i=1}^{r}$, and $(b_j)_{j=1}^{r}$, such that $a_i + b_j \neq 0$ as follows:

$$C = \left(\frac{1}{a_i + b_j}\right)_{i,j=1}^{r}.$$

Since there exists efficient algorithms for Cauchy matrices to perform the inversion and the multiplication with a vector, the Cauchy matrices are mainly used for building systematic MDS codes.

Then, Vandermonde matrices are defined from a vector of r distinct elements $(a_1, \ldots, a_r)$ of $(\mathbb{F}_q)^r$ as

$$V = \left(a_i^{j-1}\right)_{i,j=1}^{r}.$$

The determinant of such a matrix is $\det(V) = \prod_{1 \leq i < j \leq r}(a_j - a_i)$ and then, this matrix is nonsingular if and only if all the a_i are distinct.

Systematic erasure codes using a Vandermonde matrix as redundant part of the generator matrix are used in numerous commercial and free applications (see e.g. [4]). However, it has been stated in [6, p. 323, problem 7] that a Vandermonde matrix defined over a finite field can contain singular square submatrices. Consequently, such a systematic erasure code is not MDS, i.e. it is not able to recover the information from any set of k symbols of a codeword.

An upper bound of the number of singular square submatrices of a Vandermonde matrix is given in [8]. Considering a $m \times (q-1)$-Vandermonde matrix whose columns are the $q-1$ consecutive powers of the elements $a_1, \ldots, a_m$, the number of singular $m \times m$-submatrices of this matrix is bounded by $3(m-1)(q-1)^m T^{-1/(m-1)}$ with $T = min_{1 \leq i \leq m, 1 \leq j \leq m,\, j \neq i}(order(a_i/a_j))$ [8].

According to the author [8], this bound does not seem to be very tight, following some statistical measurement campaigns [9] and the accuracy of the inequalities. This bound, however shows the general evolution of the number of singular generalized Vandermonde matrices. To obtain an accurate estimation of this bound, some statistical observations [9] have been conducted showing that the proportion of nonrecoverable configurations of k received packets of a systematic Vandermonde-based erasure code can reach 0.5% for parameters corresponding to practical applications (e.g. for $q = 256$, $k = 16$ and $n = 32$).

However, despite this property, Vandermonde matrices class is an excellent candidate to build systematic MDS codes principally since matrix-vector multiplications can be performed very efficiently [7], especially when fast Fourier transform (FFT) can be used. This point motivated the introduction of a construction of systematic MDS erasure codes based on Vandermonde matrices in the next Section.

III. A New Construction of MDS Systematic Erasure Codes

A. New Construction of Matrices With No Singular Square Matrices

Theorem 2: Let us denote by $V(a_1, \ldots, a_r)$ the Vandermonde matrix $(a_i^{j-1})_{i,j=1}^{r}$. For any vectors $(a_1, \ldots, a_r)$ and $(b_1, \ldots, b_r)$ of $(\mathbb{F}_q)^r$ such that the a_i, b_j are $2r$ distinct elements, then the matrix

$$V(a_1, \ldots, a_r)^{-1} \times V(b_1, \ldots, b_r)$$

is such that any of its square submatrix is nonsingular.

Proof: Let us denote by U the $r \times 2r$-matrix $[V(a_1, \ldots, a_r)|V(b_1, \ldots, b_r)]$. Let us consider the product $W = V(a_1, \ldots, a_r)^{-1} \times U$. It is clear that W is of the form $[I|R]$ where $R = V(a_1, \ldots, a_r)^{-1} \times V(b_1, \ldots, b_r)$. We have to prove that R does not contain any singular submatrix.

It is clear that every $r \times r$-submatrix of U is nonsingular since it is a Vandermonde matrix built from a vector of r distinct elements. Then, any $r \times r$ submatrix of W is nonsingular for it is the product of $V(a_1, \ldots, a_r)^{-1}$ and the corresponding nonsingular $r \times r$-submatrix of U. As the code defined by the generator matrix $[I|R]$ is of systematic form and therefore MDS (any $r \times r$ submatrix is nonsingular), by Theorem 1, every square submatrix of R is nonsingular. ∎

B. Application of This Construction to Build Fast Erasure Codes

The construction presented in the last Section used square matrices, but it can be generalized in order to build generator matrices of systematic MDS codes of variable length.

Theorem 3: Let $V(a_1, \ldots, a_k)$ be a nonsingular $k \times k$-Vandermonde matrix and let $V(b_1, \ldots, b_{n-k})$ be a $k \times (n-k)$ matrix $(b_i^{j-1})_{i=1,\ldots,n-k}^{j=1,\ldots,k}$. Then, the code defined by the generator matrix

$$G = \left[I_k | V(a_1, \ldots, a_k)^{-1} \times V(b_1, \ldots, b_{n-k})\right]$$

is MDS if and only if the a_i, b_j are n distinct elements.

Proof: $\Rightarrow$) Assume that the code defined by G is MDS. Then the code defined by $G' = V(a_1, \ldots, a_k) \times G$ is MDS since $V(a_1, \ldots, a_k)$ is nonsingular. As G' is of the form $[V(a_1, \ldots, a_k)|V(b_1, \ldots, b_{n-k})]$, if two elements in the set $\{a_1, \ldots, a_k, b_1 \ldots, b_{n-k}\}$ are equal, then two columns of G' are equal and then there exists a $k \times k$-singular submatrix of G'. This is not possible because the code defined by G' is MDS. Therefore, all the elements a_i, b_j are pairwise distinct.

$\Leftarrow$) Assume now that the a_i, b_j are n distinct elements. Then the matrix $[V(a_1, \ldots, a_k)|V(b_1, \ldots, b_{n-k})]$, denoted by G', is such that any $k \times k$-submatrix is nonsingular because any $k \times k$-submatrix is necessarily a Vandermonde matrix defined from a set of k distinct elements. It is clear that the matrix $V(a_1, \ldots, a_k)^{-1} \times G' = G$ also verifies this property. Therefore, the code defined by G is MDS. This concludes the proof. ∎

Let us now describe the coding and the decoding algorithms of such a code. Since the code is systematic, the encoding consists in generating the redundant symbols, i.e, in multiplying the

information symbols by the redundant part of the generator matrix equal to $V(a_1,\ldots,a_k)^{-1} \times V(b_1,\ldots,b_{n-k})$. Since Vandermonde and inverse of Vandermonde matrix-vector multiplications are more efficient than generic ones, multiplying the data by the two matrices (i.e. $V^{-1}(a_i)$ and $V(b_i)$) rather than directly by the product is better in complexity.

For the decoding, the first step consists in considering the $k \times k$-submatrix of G corresponding to the k received symbols. This matrix is equal to the product of $V(a_1,\ldots,a_k)^{-1}$ by a $k \times k$-Vandermonde matrices (which is a submatrix of $[V(a_1,\ldots,a_k)|V(b_1,\ldots,b_{n-k})]$). Let us denote this Vandermonde matrix by V_R. The last step of the decoding is done by multiplying the received symbols by V_R^{-1} then by $V(a_1,\ldots,a_k)$. Note that the inversion of V_R is not compulsory with the choice of correct algorithms.

Then the encoding and the decoding only use operations (matrix-vector multiplications) on Vandermonde and on inverse of Vandermonde matrices. It must be noted that all these operations have lower complexities with Vandermonde matrices than with Cauchy matrices as shown below.

Moreover, the complexity of the encoding/decoding can be improved considering the case when k is a divisor of $q-1$. Under this assumption, taking the vector $(a_1,\ldots,a_k)$ equal to $(1,\alpha,\ldots,\alpha^{k-1})$, where α is an element of $\mathbb{F}_q$ of order k is an efficient choice. The corresponding Vandermonde matrix is then denoted by $V(\alpha)$. This choice has two objectives. First, the inversion of $V(\alpha)$ is direct since $V(\alpha)^{-1} = (1/k) \times V(\alpha^{-1})$. Then, the matrix-vector multiplication with $V(\alpha)$ (and $V(\alpha^{-1})$) can be performed in $O(k \log k)$ operations by using Fast Fourier Transform (FFT). Note that, in this case, the entries of the product $\Pi = V(\alpha)^{-1} \times V(b_1,\ldots,b_{n-k})$ can be expressed as $\pi_{i,j} = k^{-1} \times (1-b_j^k)/(1-b_j/\alpha^i)$.

The complexity study will be done thanks to the work provided by [7]. The following complexities will be used.

- $\epsilon(n) \leq O(n \log^2(n))$ is the complexity of the evaluation algorithm.
- $\iota(n) \leq O(n \log^2(n))$ is the complexity of the interpolation algorithm.
- $\phi(n) \leq O(n \log(n))$ is the complexity of the fast fourrier transform algorithm.

The complexity of the encoding can be evaluated as follows. The multiplication of the information vector by the first matrix has a complexity of $\phi(k)$ with FFT or $\iota(k)$ without. The complexity of the second matrix-vector multiplication can be estimated as $\epsilon(\max(k,n-k))$. The encoding of one vector has the resulting complexity of $\phi(k)+\epsilon(\max(k,n-k))$ with FFT or $\iota(k)+\epsilon(\max(k,n-k))$ without. This complexity is to be compared to $2\iota(\max(k,n-k))+3\epsilon(\max(k,n-k))+O(\max(k,n-k))$ required for Cauchy encoding.

The operations processed by the decoding are quite similar to the encoding since the decoding does not require any formal matrix inversion with the use of the interpolation algorithm (see [7] for more details). The decoding complexity of one vector is $\phi(k)+\iota(k)$ with FFT or $\epsilon(k)+\iota(k)$ without. This complexity is to be compared to $2\iota(k)+3\epsilon(k)+O(k)$ required for Cauchy decoding.

IV. Conclusion

In this letter, a new construction of systematic MDS erasure codes based on two Vandermonde matrices has been presented. For the packet erasure channel, these codes have lower encoding and decoding complexities than any other systematic MDS erasure codes.

References

[1] J.-C. Bolot, S. Fosse-Parisis, and D. Towsley, "Adaptive FEC-based error control for Internet telephony," in *Proc. Infocom '99*, New York, Mar. 1999.

[2] J. Bloemer, M. Kalfane, M. Karpinski, R. Karp, M. Luby, and D. Zuckerman, "An XOR-based erasure-resilient coding scheme," in *ICSI TR-95-048*, Aug. 1995.

[3] M. Luby, L. Vicisano, J. Gemmell, L. Rizzo, M. Handley, and J. Crowcroft, The use of forward error correction (FEC) in reliable multicast.

[4] L. Rizzo, "Effective erasure codes for reliable computer communication protocols," *ACM Comput. Commun. Rev.*, Apr. 1997.

[5] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," *J. Assoc. Comput. Mach.*, vol. 38, no. 335, 1989-00-00.

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

[7] I. Gohberg and V. Olshevsky, "Fast algorithms with preprocessing for matrix-vector multipication problems," *J. Complexity*, vol. 10, 1994.

[8] I. Shparlinski, "On singularity of generalized Vandermonde matrices over finite fields,", preprint, 2000.

[9] J. Fimes and J. Lacan, "Estimation of the number of singular square submatrices of Vandermonde matrices defined over a finite field," Tech. Rep. ENSICA, no. RE-2003-01.