

Decoding of Concatenated Codes with Interleaved Outer Codes

Jørn Justesen

COM

The Technical University of Denmark

Bldg.343

DK-2800 Kgs.Lyngby, Denmark

e-mail: jju@com.dtu.dk

Christian Thommesen

Department of Mathematical Sciences

Aalborg University

Frederik Bajersvej 7G

DK-9220 Aalborg Ø

e-mail: cthom@math.auc.dk

Tom Høholdt

Department of Mathematics.

The Technical University of Denmark

Bldg.303

DK-2800 Kgs.Lyngby,Denmark

e-mail: T.Hoeholdt@mat.dtu.dk

Abstract — Recently Bleichenbacher et al. proposed a decoding algorithm for interleaved (N, K) Reed-Solomon codes, which allows close to $N - K$ errors to be corrected in many cases. We discuss the application of this decoding algorithm to concatenated codes.

I. INTRODUCTION

Recently Bleichenbacher, Kiayias, and Yung [1] proposed a decoding algorithm for interleaved (N, K) Reed-Solomon codes over \mathbb{F}_q , $q = 2^m$, which allows close to $N - K$ errors to be corrected in many cases. The assumptions are that for interleaving degree I and $T < \frac{(N-K)I}{I+1}$, at most T errors occur in each codeword and the errors occur in the same set of positions in each code.

In [1] some form of randomization is suggested to make the error values in position j of the I words independent, but no motivation is given. Interleaving may be seen as a method of spreading the errors that occur in bursts, and a related algorithm for burst correction has recently been proposed in [2]. However, the most important application of interleaved RS codes is concatenated codes.

Following [1] we initially state the encoding of the RS codes as evaluations of I information polynomials, and the decoding is performed by solving an interpolation problem. However, the decoding can be implemented and analyzed more efficiently by considering the equivalent syndrome formulation.

We assume that the inner binary code is decoded Maximum Likelihood since the code is short relative to the total block length which is chosen to be so long that T becomes large. In most practical systems the inner code is a convolutional code, and the interleaving degree is chosen to make most error events shorter than mI bits. In [3] the relation of the interleaving degree to the distance distribution of the convolutional code was discussed. We can get an inner block code with similar performance and decoding complexity by tail-biting the convolutional code for each set of I symbols.

II. DECODING OF INTERLEAVED OUTER CODES

If the symbol error probability of the inner code is $p(e)$, the average number of errors that must be corrected by the outer codes is slightly more than $p(e)NI$. If the outer codes are decoded independently, a total of $\frac{I(N-K)}{2}$ errors can be corrected, but the decoding error probability depends on the way the errors are distributed. If one or more of the outer codes can be decoded, iteration between inner and outer codes can improve performance.

In the BKY algorithm, decoding of several interleaved words is combined to allow close to $N - K$ errors to be corrected. The idea is to express the codewords as evaluations of the information polynomials $f_1(x), f_2(x), \dots, f_I(x)$ in all

powers of a primitive element α of \mathbb{F}_q , and to let the error positions be characterized by a single error locator polynomial $Q(x)$. We define

$$m_i(x) = f_i(x)Q(x)$$

so if the received words are

$$r_i(x) = f_i(x) + e_i(x) \text{ we get } r_i(x)Q(x) - e_i(x)q(x) = m_i(x)$$

and hence

$$r_i(\alpha^j)Q(\alpha^j) = m_i(\alpha^j), \quad j = 0, 1, \dots, q-2 \quad (1)$$

since $e_i(\alpha^j)Q(\alpha^j) = 0, \quad j = 0, 1, \dots, q-2$

The system (1) gives IN equations in $I(K+T) + T$ unknowns, so if this has maximal rank we can correct close to $T = \frac{I(N-K)}{I+1}$ inner codewords or about $I(N-K)$ symbol errors.

A comparison of the two approaches shows that the BKY algorithm can provide an improved performance for realistic concatenated codes.

III. SYNDROME DECODING

The system (1) can be transformed into a smaller homogeneous system by eliminating $m_i(x)$ [4]. Thus only the error locator $Q(x)$ is found in this step and the coefficient matrix consists of syndromes. This is the standard approach to decoding RS codes, but it also provides a practical approach to BKY decoding with about the same complexity as the RS algorithm. When the algorithm is presented in this way the degree of $Q(x)$ can be increased because several syndrome sequences must satisfy the same recursion.

Clearly the syndrome matrix is singular in some cases. The transform approach shows that the syndrome matrix can be factored into the product of a matrix of monomials in the error positions and the error values and a Vandermonde matrix. For a fixed set of error positions this matrix is linear in the error values. Thus the probability of a singular syndrome matrix is in the order $\frac{1}{q}$.

REFERENCES

- [1] D. Bleichenbacher, A. Kiayias, and M. Yung "Decoding of Interleaved Reed Solomon Codes over Noisy Data," *Springer Lecture Notes In Computer Science*, vol. 2719/2003, pp. 97-108, January 2003.
- [2] V.Y. Krachkovsky "Reed-Solomon Codes for Correcting Phased Error Bursts" *IEEE Trans.Inform.Theory* vol. 49, pp.2975-2984, November 2003.
- [3] J. Justesen, C. Thommesen, and V.V. Zyablov "Concatenated codes with convolutional inner codes" *IEEE Trans.Inform.Theory* vol. IT-34, pp.1217-1225, September 1988.
- [4] J. Justesen and T. Høholdt *A Course in Error Correcting Codes* Chapter 5, EMS Textbooks in Mathematics. Zürich. 2004.