Информационные процессы, Том 4, № 3, 2004, стр. 284–290.

Some Results and some Problems Related to Concatenated Codes

J. Justesen

COM, Technical University of Denmark, Lyngby, Denmark

Received November 22, 2004

Abstract—Some results of the cooperation between IPPI and the coding group in Denmark are reviewed. From this starting point several new developments and open problems in concatenated codes are discussed.

1. INTRODUCTION

In this presentation, I mention some classical results on concatenated codes, and in particular I touch upon some results of the long cooperation between the laboratory of Victor Zyablov at IPPI and the coding group at DTU. However, the aim is not to give an account of the history of the topic, but to use these results as a starting point for discussing some recent developments and some open problems.

Concatenated codes have been at the focus of the research in both groups for more than three decades. The reason is that not only has this technique become increasingly important in applications, but it has also maintained its position as an essential method in theoretical analysis, and it has absorbed several new developments in coding theory.

2. REED-SOLOMON CODES

A discussion of concatenated codes necessarily involves some details of Reed-Solomon codes as an essential component of these constructions. Reed-Solomon codes were some of the first codes to appear in the literature, and I prefer to take them as the starting point for developing algebraic coding theory. Their properties can be explained in very simple terms:

Let the data be a sequence of K symbols, interpreted as coefficients of a polynomial $U(x)$. The transmitted codeword is then a sequence of $N > K$ values attained by this polynomial in N district points:

$$c = [U(x_0), U(x_1), \ldots, U(x_{N-1})] \tag{1}$$

Two distinct codewords can agree in at most $K - 1$ points, since the difference polynomial can have at most $K - 1$ roots.

Assume that T of the received values are in error. Decoding may be seen as an interpolation; the receiver should find a polynomial which passes through as many of the received points as possible. The positions of the errors are found by determining the coefficients of a polynomial $E(x)$ of degree T with the error positions as roots. If the received values are y_j, we have

$$M(x) = U(x)E(x)$$

$$M(x_j) = y_j E(x_j) \tag{2}$$

since either

$$U(x_j) = y_j$$

or both sides are zero. If $T \leq (N-K)/2$, there are enough linear equations to find the coefficients of M and E.

The description of the coding problem in such basic terms has allowed new results in fundamental computer science to be applied in our area.

3. CONCATENATED CODES

In Forney's thesis [1], it was proved that concatenated codes using a combination of RS (outer) codes and binary codes for each RS symbol (inner codes) could be used to reach the channel capacity with a favorable combination of error probability and computational complexity. However, in reality this goal appeared out of reach at the time.

Several results in the early 70s changed this perspective. A specific combination of inner and outer codes was suggested as a practical way of obtaining good performance on deep-space channels. The space telemetry standard is specified in detail in the Blue Book of the Consultative Committee for Space Data Systems [2], an organization that has the American NASA, the European ESA, and the Russian Space Agency among its members.

While in [1] concatenation was seen almost as a way of avoiding the construction of long codes, it was found that the process could also be seen as a way of constructing a single long code with fairly good parameters [3, 4]. Here a codeword is seen as a binary array where column j is a binary codeword in the inner code representing the symbol $c_j = U(x_j)$. Thus a solution was found to the problem of constructing long codes with good distances. This point of view led to algorithms that correct all errors within half the designed minimum distance. It follows immediately from the two-level construction that the distance of the concatenated code is at least the product of the distances of the component codes. This bound is often referred to as the Zyablov bound.

Unfortunately the results on the performance on the Binary Symmetric Channel (or the Gaussian Channel) and the results on the distance properties are not clearly related. The exact distance of the standard code is not known, and probably of little importance in applications. On the other hand algorithms that guarantee correction of a certain number of errors are usually not effective with a random distribution of errors.

The separation between the results related to performance and to distances is further amplified by the use of convolutional inner codes in most applications. There has been relatively little research in the properties of concatenated codes with convolutional inner codes, although we established some of the fundamental properties in [5]. Recently there has been some interest in so-called tail-biting codes as a bridge between convolutional codes and block codes [6]. In a tail-biting code the encoding is done by a linear system as in convolutional codes, but the encoding process circles through a limited number of information bits to produce a block code. This approach would make the decoding of each column of symbols in a concatenated code independent of the rest of the code, providing some benefits both for the implementation and the analysis. With a suitable choice of parameters the performance would not change much, but it is unknown whether it can actually be improved by the right choice of parameters.

By considering averages of codes with random inner codes, it has been proved that concatenated codes can have the same properties as general average codes with the same parameters [7, 8]. However, in this case the parameters of the component codes have to be chosen in a way that appears to rule out separate decoding of the inner and outer codes. There are several known cases where the binary images of RS codes are very good binary codes. A recently reported example is the (160, 80, 24) codes [9]. For low-rate concatenated codes with good short inner codes, the Zyablov bound is sufficient to prove that the binary codes have good distances. Codes of length 85 can serve as a small example, but no specific good code with a non-trivial inner code and distance above the Zyablov bound has been reported.

4. APPLICATIONS IN COMMUNICATION SYSTEMS

In 1985/86 the concatenated coding standard was used in two spectacular space missions. In NASA's Voyager the code was used to send back images and telemetry from the planet Uranus, and Voyager has since continued to transmit data from the outer parts of the Solar system. ESA's GIOTTO probe made a close encounter with Halley's comet producing closeup images and measurements of the environment of the active comet. In this case the communication problem was not related to the distance, but to the unknown hazards of the encounter. Actually the probe survived the flyby, but the signal level started varying periodically when dust particles made the probe oscillate around its proper alignment.

Our work on the GIOTTO decoder produced an important feedback from the realities of communication systems. In particular it demonstrated that the interaction of the error-correcting code with other parts of the communication system is more complicated than we expected, and that building the decoders was a less complicated task. The activities since then have further emphasized these points.

In addition to a growing number of applications in communication systems, concatenated codes are now also commonly used in digital storage media [10].

A long concatenated code is, at least in this context, part of the structure of a block of data commonly referred to as a frame. In addition to the user data, the frame contains a synchronization pattern and some header information like a serial number and an address. The decoding of the RS code requires that the beginning of the frame is correctly identified, and even in the presence of errors this decision can usually be made with sufficient reliability. But the interaction of error-correction and synchronization is not adequately described in the literature. The header information must usually be available without complete decoding of the frame. In storage systems that can lead to problems with false sequence numbers, whereas in networks the addresses are a particular concern. This is an area that has frequently been marred by design errors, and network models in particular do not have a consistent way of treating error-correcting codes.

The implementation of decoders for concatenated codes shows that RS codes are well suited for modern digital technology in spite of their apparent complexity. At low data rates, a suitable program for a microprocessor may be the choice, but usually faster solutions are required. At present decoders are often implemented in Field Programmable Gate Arrays (FPGA). In this way the circuit is actually configured by downloading a program, and it is even possible to make changes later by modifying the software. Standard decoding methods (syndrome calculation, solution for the error locator polynomial by Euclid's algorithm, etc.) can be efficiently converted to parallel versions and used in such systems. Such algorithms are still commonly used, but there is a long line of research in faster methods based on fast transforms, probably starting with Afanasyev's paper [11]. The fast algorithms allow a significant speed-up of parallel decoders, and the use of RS codes in optical communication systems may eventually make such decoders a reality. However, while there is some work done on the details of the implementations in the industry [12, 13], the theoretical work on complexity does not seem to have produced results on space/time bounds for parallel algorithms.

5. ALGEBRAIC GEOMETRY CODES AS OUTER CODES

One of the spectacular advances in coding theory in the '80s was the development of long codes over large alphabets using methods from Algebraic Geometry. Such codes are generalizations of RS codes in the sense that codewords are obtained by evaluating an information polynomial as in (1), but

$$x_j = (v_j, w_j)$$

is a point of an algebraic curve, usually a point in the plane satisfying some defining equation

$$F(v, w) = 0$$

In this way it is possible to keep the alphabet fixed and let the length of the code increase. Decoding of such codes can be seen as a generalization of decoding RS codes as described in [14], which is in part based

on work I did while visiting IPPI. However, a version of the algorithm that exploits fast transforms has not yet been described in a satisfying form.

While algebraic geometry so far has not produced good direct constructions of binary codes, long binary codes have been obtained by concatenation [15]. We can also fix the inner code in a concatenated code and consider outer codes of increasing length with a randomized mapping of the symbols [16].

6. DECODING MORE ERRORS

If the decoding of the inner code leads to more than $(N-K)/2$ errors, the result of decoding the RS code is usually a decoding failure. Even though it is easy to construct examples where additional errors cause decoding to a wrong codeword, such cases are extremely rare, and in principle more errors can be corrected. Efforts to modify the decoding methods had very limited success until Sudan's work on interpolation was applied to the problem [17]. Sudan's idea was to rewrite (2) as

$$Q(x_j, z_j) = y_j$$

and factor the two-variable interpolating polynomial Q. In this way one will in general find a list of factors of the form

$$z - U_i(x)$$

which represent different possible codewords. Usually there is only one factor, and the major improvement is that, at least for low rates, some additional errors can be corrected.

For concatenated codes, more efficient decoding would be possible if the inner decoder produced a short list of possible codewords rather than a single result. This approach was first discussed in Pinsker and Zyablov's paper [7], where the authors proved that decoding of the inner code within a suitable sphere would always produce a very small number of results. In [7] this result was combined with a complex approach to the decoding of the outer codes. Recently there has been some work on using a list input in a generalized version of Sudan's algorithm [18]. However, the gains for concatenated codes so far appear to be limited.

It may be useful to note that if the input list is very small and there are no errors, the RS code can be decoded by solving a system of linear equations: Let the symbols in some subsets of the positions $j \in J$ have two possible values. Choose one of the values arbitrarily, and calculate the syndrome of the received word, s. For each position find the change that the other choice of the symbol would add to the syndrome, and solve the binary equations

$$\sum_{j \in J} a_j s_j$$

where $a_j = 1$ indicates that the symbol in position j should be changed. However, no way of combining this approach with error correction is known.

A more recent variant of the interpolation approach allows more errors to be corrected when several codewords are interleaved (as it is common usage), and the errors in all codewords are confined to a common set of positions [19]. Thus (2) becomes

$$M_i(x) = U_i(x)E(x)$$
$$M_i(x_j) = y_{ij}E(x_j)$$

and by comparing the number of equations and the number of unknown coefficients one finds that as many as

$$(N-K)I/(I+1)$$

errors can be corrected where I is the number of outer codes. Clearly this is not always possible. However, as indicated in [20] there is actually a high probability of successful decoding. The method appears very well suited for decoding of concatenated codes, but more work is needed to establish the choice of parameters and details of the decoding algorithm that will give a real gain.

7. CONCATENATED CODES FROM GRAPHS

Recently a generalized form of concatenated codes has been described as codes defined on bipartite expander graphs [21]. A special case is studied in more details in [22], and here the connection to the usual concatenated codes is also made more explicit.

Let M be a cyclic incidence matrix for a projective plane with S lines and points. Thus each row has n 1s. The largest eigenvalue is n, and all remaining eigenvalues have modulus$\lambda = \sqrt{n-1}$. A bipartite graph consisting of two sets of S nodes of order n is described by the connection matrix

$$A = \begin{pmatrix} 0 & M \\ M^t & 0 \end{pmatrix}$$

This matrix may be seen as a simple expander graph: Starting from a node in the right set, n nodes in the left set can be reached in one transition, and the remaining nodes in the right set can be reached from these nodes. We have

$$S = n(n-1) + 1$$

The graph can be used to define a code by associating a symbol with each branch and letting all branches that meet in a node satisfy the parity checks of an (n, k, d) code. Thus the length of the code is

$$N = Sn$$

If the rate of the code associated with the nodes is r, the total rate is

$$R \geq 2r - 1$$

For our purpose we will choose codes on both sides of the graph as extended RS codes over the field of $q = n - 1$ symbols, since in this way the same field is used in constructing the projective plane. But we will refer to the codes on the right as the inner codes, since the symbols are converted to binary vectors, and the right side is decoded as binary codes.

In order to obtain a lower bound on the minimum distance, we want to determine the smallest size of sets of nodes in each of the two parts of the graph, s, such that the subgraph consisting of these nodes and the branches connecting them has degree at least d. Clearly in this case sd is a lower bound on the minimum distance. It follows from the expansion property of the graph that the minimum distance satisfies the product bound if $d >> \sqrt{n}$.

The decoding can make use of the graph structure of the code. First decode the binary images of the right side codes. For each $F(q)$ symbol in a given position, propagate a message along the branch in the graph indicating the minimum number of binary errors corrected in the first stage of decoding. Using these messages, decode the left codes as RS codes. Pass the result to the right side, and consider these codes as RS codes. Each code on the right side is now the root of a tree code consisting of all codes on the right side, a small subset of codes on the left side, and all symbols in the total code. To get a complete decoding, the results from several of these trees must be reconciled.

8. CONCLUDING REMARKS

This presentation mentions only a small part of the research on concatenated codes. The topics discussed here reflect my personal interests, and they were chosen to illustrate some of the interactions between coding

theory and related subjects and between different areas of coding theory. I consider it a privilege to have been involved with this line of research, both on the scientific side and in applications over many years. During this entire period, many of the essential inputs have come from working with colleagues at Institut Problem Peredachi Informatsii.

9. REFERENCES

1. Forney G.D., Jr., *Concatenated Codes*, MIT Press, 1966.

2. Consultative Committee for Space Data Systems, www.ccsds.org /CCSDS /documents /101x0b6.pdf

3. Zyablov V.V., Estimate of the Complexity of Constructing Binary Linear Concatenated Codes, *Prob. Peredachi Inform.*, 1971, No. 1, pp. 5-13.

4. Justesen J., A Class of Constructive Asymptotically Good Algebraic Codes, *IEEE Trans. Info. Theory*, 1972, vol. IT-18, pp 652-656.

5. Justesen J., Thommesen C., and Zyablov V.V., Concatenated Codes with Convolutional Inner Codes, *IEEE Trans. Info. Theory*, 1088, vol. IT-34, pp. 1217 - 1225.

6. Stahl P., Anderson J.B., and Johannesson R., Optimal and Near-Optimal Encoders for Short and Moderate-Length Tail-Biting Trellises, *IEEE Trans. Info. Theory*, 1999, vol. IT-45, pp. 2562 - 2571.

7. Zyablov V.V., Pinsker M.S., List Cascade Decoding, *Probl. Pered. Inform.*, 1981, vol. 17, no. 4, pp. 29 - 34.

8. Thommesen C., The Existence of Binary Linear Concatenated Codes with Reed-Solomon Outer Codes which Asymptotically Meet the Gilbert-Varshamov Bound, *IEEE Trans. Inform. Theory*, 1983, vol. IT-29, pp. 850-853.

9. v.Dijk M., Egner S., Greferath M., and Wassermann A., On Binary Linear [160,80,24] codes, Proceedings *ISIT 2003*, Yokohama, 2003, p. 162.

10. Immink K.A.S., *Coding Techniques for Digital Recorders*, Prentice Hall, 2001.

11. Afanasyev V.B., Fast Encoding and Detection of Errors in Reed-Solomon Codes, Abstracts of Papers, *3rd Int. Symp. Inf. Th.*, Tallin, 1973, pp. 13-15.

12. www.altera.com /products /ip /dsp /error_ detection_ correction /ipm-index.jsp

13. www.xilinx.com /ipcenter /catalog /logicore /docs /reed_ solomon_ dec.pdf

14. Justesen J., Larsen K.J., Jensen H.E., Havemose A., and Hfiholdt T., Construction and Decoding of a Class of Algebraic Geometry Codes, *IEEE Trans. Info. Theory*, 1989, vol. IT-35, pp. 811 - 821.

15. Shum K.W., Aleshnikov I., Kumar P.V., Stichtenoth H, and Deolalikar V., A Low-Complexity Algorithm for the Construction of Algebraic-Geometric Codes Better than the Gilbert-Varshamov Bound, *IEEE Trans. Info. Theory*, 2001, vol. IT-47, pp. 2225 - 2241.

16. Barg A., Justesen J., and Thommesen C., Concatenated Codes with Fixed Inner Code and Random Outer Code, *IEEE Trans. Info. Theory*, 2001, vol. IT-47, pp. 361 - 365.

17. Guruswami V., and Sudan M., Improved Decoding of Reed-Solomon and Algebraic-Geometry codes, *IEEE Trans. Info. Theory*, 1999, vol. IT-45, pp. 1757 - 1767.

18. Koetter R, and Vardy A., Algebraic Soft-Decision Decoding of Reed Solomon Codes, *IEEE Trans. Inform. Theory*, 2003, vol. IT-49, pp. 2809 - 2825.

19. Bleichenbacher D., Kiayias A., and Yung M., Decoding of Interleaved Reed Solomon Codes over Noisy Data, *Lecture notes in Computer Science*, Vol. 2719/2003, pp. 97-108, Springer-Verlag, 2003.

20. Justesen J., Thommesen C., and Hfiholdt T., Decoding of Concatenated Codes with Interleaved Outer Codes, Proceedings, *ISIT 2004*, Chicago, 2004, p. 329.

21. Barg A., Zemor G., Error Exponents of Expander Codes, *IEEE Trans. Inform. Theory*, 2002, vol. IT-48, pp. 1725-29.

22. Justesen J., Hfiholdt T., From Concatenated Codes to Graph Codes, Proceedings, *IEEE Workshop on Information Theory*, San Antonio, Texas, 2004.