Asymptotically optimal binary codes of polynomial complexity correcting localized errors

R. Ahlswede, L. A. Bassalygo, and M. S. Pinsker

Abstract. The asymptotically optimal transmission rate of binary codes correcting localized errors is known for the case when the number of errors grows linearly in the code length. Here we prove that this rate can be attained by codes with polynomial complexity of encoding, decoding, and code construction.

Recall that the only difference between codes correcting localized errors (see [1], [2]) and the conventional codes lies in the fact that the positions of possible errors are known to the encoder in advance. Therefore, codewords depend not only on messages but also on these positions. The asymptotically optimal transmission rate of such binary codes is known [1]. Here we prove that this rate can be attained by codes with polynomial complexity of encoding, decoding, and construction. We supply a recurrent proof in which every passage (recurrence) from the greater to the smaller length is accomplished in three steps. This proof is based on the following argument.

In the first step, we split the entire transmission segment of length n into a number, growing with n, of consecutive segments of equal length. We then choose a segment with the least possible number of errors. We call it the auxiliary segment for it will be used to transmit a certain auxiliary information rather than the message. However, its length is small compared to n and does not affect the asymptotic behavior of the transmission rate.

Having chosen the auxiliary segment, we proceed to the second step. We arrange a new partition of the entire transmission segment except the auxiliary segment into a large number of intervals whose length grows slowly in n (here we say 'interval' instead of 'segment' only in order to distinguish between the first and the second steps). The choice of the interval length is determined by the two following conditions: a) the exhaustive search encoding and decoding methods on the interval must be polynomial in n, b) we must record on the auxiliary segment the number of possible errors on every interval. These conditions suggest the following precoding method. We record on the auxiliary segment the number of possible errors on every interval while the message is encoded on the intervals themselves. Here we employ the existing asymptotically optimal codes correcting the known number of localized errors (the asymptotic optimality of the code on the full length follows from the asymptotic optimality of the code on every interval). Moreover, these codes can be taken constant-weight with certain natural restrictions on the weight, and we use precisely these codes (we need this on the third step).

If the number of the auxiliary segment were known to the decoder, there would be no need for the third step. It would be sufficient to transmit the codeword obtained on the second step and our problem would have been solved, because the encoding/decoding on the entire segment of length n would be reduced to the encoding/decoding on the auxiliary segment and to the encoding/decoding on every interval whose complexity is polynomial in n by Condition a). Applying the same procedure to the auxiliary segment (notice that the fraction of errors on it does not exceed the fraction of errors on the entire transmission segment), and so on, after a certain number of steps (growing in n) we shall arrive at the recurrent auxiliary segment of the sufficiently small length. For this segment, we can accomplish the encoding/decoding by exhaustive search, which completes our recurrent procedure.

Thus, the only thing left is to explain the way in which we communicate the number of the auxiliary segment to the decoder. Since the number of numbers is small (certainly less than n), any reasonable transmission method, at first, does not reduce the transmission rate asymptotically, and, secondly, admits the exhaustive search encoding/decoding of complexity polynomial in n. On the third step we present such a method. Here we consider the codeword constructed on the second step as *the error vector known to the encoder and construct a code that corrects known errors and localized errors at the same time.* We need an additional restriction to the decoding method, namely, the decoder must reconstruct correctly not only the message, which in our case bears the number of the auxiliary segment, but also the transmitted codeword (it is precisely this property that imposes the restriction on the weight of the known error, to which we paid attention on the second step). *By now it is clear that the transmitted codeword equals the sum of the codewords constructed on the second and third step.* When decoding, we first reconstruct the codeword constructed on the third step (and hence the auxiliary segment number) and then subtract it from the received word (add modulo 2 since we deal with binary codes only). We then arrive at the situation described above, namely, we transmit a codeword constructed on the second step and the decoder knows the auxiliary segment number.

Let us now proceed to the formal exposition of the result. Let us introduce the notation. Let B be the set of binary sequences of length n, $\mathcal{M} = \{m\}$ the message set, let $\mathcal{E}_t = \{E \subseteq \{1,2,\ldots,n\}|\ |E| = t\}$ be the set of all possible positions of errors of multiplicity t ($|\mathcal{E}_t| = \binom{n}{t}$), and let $V(E) = \{e = (e_1,\ldots,e_n) \in B|e_i = 0, \text{ if } i \notin E\}$ be the set of binary words of length n that are zero outside the positions of E ($|V(E)| = 2^t$). Since on the encoding stage, we know the possible t error positions, the codeword $x(m,E)$ depends on $m \in \mathcal{M}$ and $E \in \mathcal{E}_t$. The code $X = \{x(m,E)|m \in \mathcal{M}, E \in \mathcal{E}_t\}$ corrects t localized errors if the following condition holds:

$$x(m,E) + e \neq x(m',E') + e' \quad \text{for all } E,E' \in \mathcal{E}_t, e \in V(E), e' \in V(E'), m,m' \in \mathcal{M}, m \neq m'.$$

It is known [1] that the maximum transmission rate of such a code equals $1 - h(\tau) - o(1)$, where $t = \tau n (0 \leq \tau \leq 1/2)$ and $o(1) \to 0$ as $n \to \infty$.

Theorem 1. *Let $0 < \tau < 1/2$. Then for any $\epsilon > 0$, there exists $n(\epsilon)$ such that for $n > n(\epsilon)$, there exists a code of length n with transmission rate $1 - h(\tau) - \epsilon$ that corrects τn localized errors and has the encoding and decoding complexity not greater than cn^3, where c is a constant. The construction of this code can also be accomplished with complexity not greater than cn^3.*

In the course of the proof of Th.1 we frequently refer to Theorem 2 below, which is of independent interest. This theorem provides a natural continuation of Theorem 3 [1], pointing out auxiliary properties of codes correcting localized errors, which were unclaimed before the present paper.

Theorem 2. *There exists a t localized error-correcting binary code of length n for the transmission of M messages, where M satisfies the following inequality:*

$$M \geq \frac{2^n}{32nS_t}$$

($S_t = \sum_{i=0}^{t} \binom{n}{i}$ is the volume of the sphere of radius t). This code can be chosen so that the two following properties are satisfied:

a) *The decoding into the nearest codeword reconstructs not only the message, but also the transmitted codeword;*

b) *For any binary sequence e of length n and any message m, in the code set corresponding to m there exists a word such that its modulo 2 sum with the sequence e lies at the distance greater than t from all other codewords (including codewords of the same code set).*

REFERENCES

[1.] L. A. Bassalygo, S. I. Gelfand, and M. S. Pinsker, "Coding for channels with localized errors," in: *Proc. 4th Joint Swedish-Soviet Int. Workshop Inform. Theory*, Sweden, 95–99, 1989.

[2.] L. A. Bassalygo and M. S. Pinsker, "Binary constant-weight codes correcting localized errors," *Probl. Inform. Trans.*, **28**, 4, 103–105, 1992.