ASYMPTOTICALLY DENSE NONBINARY CODES CORRECTING A CONSTANT NUMBER OF LOCALIZED ERRORS

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

Abstract

The binary case was studied in [1], but the method used there doesn't give the tight answer for nonbinary cases and we presented in [2] another method for the corresponding result. Here we formulate the main theorem and prove the auxiliary statements used in [2].

During the transmission of q–ary words of length n over the channel at most t errors occur, and the encoder knows the set E of t positions, where these errors are possible. The decoder doesn't know anything about these positions. Let $\mathcal{E}_t = \{E \mid E \subseteq \{1,2,\ldots,n\}, |E| = t\}$ be the set of all subsets from $\{1,2,\ldots,n\}$ of size t and let $\mathcal{M}$ be a set of messages $(|\mathcal{M}| = M)$. A code word $x(m,E)$ depends not only on the message $m \in \mathcal{M}$ but also on the configuration of possible errors E. So there exists the natural correspondence between the message $m \in \mathcal{M}$ and the list of code words $\bigcup_{E\in\mathcal{E}_t}\{x(m,E)\}$, which we use for the transmission of this message. Thus the code X for the set of messages $\mathcal{M}$ represents a collection of M lists $\{\bigcup_{E\in\mathcal{E}_t}\{x(m,E)\}, m \in \mathcal{M}\}$. Sinde we can use the same word for different configurations, the size of a list can be essentially smaller than the size of the set $\mathcal{E}_t$ $\left(|\mathcal{E}_t| = \binom{n}{t}\right)$. Let us define the cylinder $C(a,A)$ with the base $a = (a,\ldots,a_n)$ and the support $A\big(A \subseteq \{1,2,\ldots,n\}\big)$ as the set of words $(y_1,\ldots,y_n)$ with $y_i = a_i$, if $i \notin A$. It is clear that the size of the cylinder $C(a,A)$ is equal to $q^{|A|}$ and the number of different cylinders with the same support A is equal to $q^{n-|A|}$.

As a result of the transmission of the codeword $x(m,E)$ every word of $C\big(x(m,E),E\big)$ can appear as output of the channel. The code X corrects t localized errors, if the decoder can correctly recover every message $m \in \mathcal{M}$. The following condition is necessary and sufficient for it:

$$C\big(x(m,E),E\big) \cap C\big(x(m',E'),E'\big) = \varnothing \text{ for all } E,E' \in \mathcal{E}_t, m,m' \in \mathcal{M}, m \neq m'. \quad (1)$$

The maximal number of messages, which we can transmit by a code correcting t localized errors, is denoted by $L_q(n,t)$.

Proposition 1:

$$L_q(n,t) \le \frac{q^n}{S_t}$$

where $S_t = \sum_{i=0}^{t}(q-1)^i C_n^i$ is the size of a sphere of radius t in the Hamming n–space.

A proof of this bound in the q–ary case can be given as for the binary case in [3] or [4]. The key inequality there has the following generalization.

Lemma 1. *Let $C(a_i, A_i), \ldots, C(a_T, A_T)$ be cylinders with pairwise different supports $A_i \ne A_j, i \ne j$. Then for the size of the union of the cylinders*

$$\left| \bigcup_{i=1}^{T} C(a_i, A_i) \right| \ge \sum_{i=1}^{T} (q-1)^{|A_i|}.$$

Proof: We proceed by an induction on n . For $n = 1$ the statement is obvious. Let $C(a_1, A_1), \ldots, C(a_T, A_T)$ satisfy the condition of the Lemma. We consider now the new family $\mathbb{C}$ of cylinders:

a) if $n \notin A_i$, then $C(a_i, A_i) \in \mathbb{C}$

b) if $n \in A_i$, then $C(a_i^{(k)}, A_i \setminus n) \in \mathbb{C}$ for all $k (k = 0, 1, \ldots, q-1)$, where $a_i^{(k)} = (a_{i1}, \ldots, a_{in-1}, k)$.

We have

$$\mathbb{C} = \bigcup_{k=0}^{q-1} \mathbb{C}^{(k)}$$

where $\mathbb{C}^{(k)}$ – all cylinders from $\mathbb{C}$ whose last coordinate is equal to $k (k = 0, 1, \ldots, q-1)$. It is easy to show that

$$\left| \bigcup_{C \in \mathbb{C}} C \right| = \sum_{k=o}^{q-1} \left| \bigcup_{C \in \mathbb{C}^{(k)}} C \right| .$$

If follows from the condition of the Lemma that the support $A_i \setminus n$ of q cylinders $C(a_i^{(k)}, A_i \setminus n), k = 0, 1, \ldots, q-1$ differs from the support of other cylinders at least for $q-1$ subfamilies $\mathbb{C}^k$, $k = 0, 1, \ldots, q-1$. Thus one proves the Lemma using the induction step to estimate $| \bigcup_{C \in \mathbb{C}^{(k)}} C |$. It is easy to obtain Proposition 1 from Lemma 1. In fact for every union of cylinders $\bigcup_{E \in \mathcal{E}_t} C(\cdot, E)$ there exists some union of cylinders $\bigcup_{E \in \bigcup_{i=0}^{t} \mathcal{E}_i} C(\cdot, E)$ such that

$$\bigcup_{E \in \mathcal{E}_t} C(\cdot, E) = \bigcup_{E \in \bigcup_{i=1}^{t} \mathcal{E}_i} C(\cdot, E)$$