NONBINARY CODES CORRECTING LOCALIZED ERRORS

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

Abstract

A recursive construction yields for all alphabets asymptotically dense codes correcting a constant number of localized errors.

1. Introduction and main result

The authors of the paper [1], where codes correcting localized errors were introduced, noticed that an extension of results to nonbinary alphabets causes difficulties. In particular this is the case with the asymptotical Hamming bound, when the number of errors $t = \tau n$ increases linearly with the length n of the code. Up to now we proved it only in a small fixed interval $[0, \tau_o]$, although we believe that Hamming's bound is the true bound in the intervall $[0, \frac{1}{2}]$ (if $\tau \geq \frac{1}{2}$, then the rate of transmission is equal to 0 because it is impossible to transmit even two messages, when $t \geq \frac{n}{2}$). However our joint efforts bore fruit for other, rather accurate, asymptotical estimates on the code size, when the number of errors t is constant. The binary case was studied in [2], but the method used there doesn't give the tight answer for nonbinary cases. Here we present another method.

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 $\left\{\bigcup_{E \in \mathcal{E}_t} \{x(m, E)\}, m \in \mathcal{M}\right\}$. Since we can use the same word for different configurations, the size of a list can be essentially smaller than the size of the set $\mathcal{E}_t (|\mathcal{E}_t| = \binom{n}{t})$.

Let us define the cylinder $\mathcal{C}(\mathfrak{a}, A)$ with the base $\mathfrak{a} = (a_1, \ldots, a_n)$ and the support A ($A \subseteq \{1, 2, \ldots, n\}$) 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 $\mathcal{C}(\mathfrak{a}, A)$ 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 $\mathcal{C}(x(m, E), E)$ 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:

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

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.

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

where $S_t = \sum_{i=0}^{t} (q-1)^i \binom{n}{i}$ 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 [1] or [3]. The key inequality there has the following generalization.

Lemma 1. *Let* $\mathcal{C}(\mathfrak{a}_1, A_1), \ldots, \mathcal{C}(\mathfrak{a}_T, A_T)$ *be cylinders with pairwise different supports* $A_i \neq A_j, i \neq j$. *Then for the size of the union of the cylinders*

$$\Big|\bigcup_{i=1}^{T} \mathcal{C}(\mathfrak{a}_i, A_i)\Big| \geq \sum_{i=1}^{T} (q-1)^{|A_i|}.$$

The proof of this lemma can be made by an induction on n as in [1] or [3] (for other proofs see [4]).

It yields immediately

$$\Big|\bigcup_{E \in \mathcal{E}_t} \mathcal{C}\big(x(m, E), E\big)\Big| \geq \binom{n}{t} (q-1)^t.$$

However, it can be used more efficiently. Choose any monotone map $f : \bigcup_{i=1}^{t} \mathcal{E}_i \to \mathcal{E}_t$ with the property $F \subset f(F)$ for all $F \in \bigcup_{i=1}^{t} \mathcal{E}_i$. Then we can write

$$\mathcal{C}\big(x(m, E), E\big) = \bigcup_{F \subset E} \mathcal{C}\big(x(m, f(F)), F\big).$$

Thus by Lemma 1

$$\Big|\bigcup_{E\in\mathcal{E}_t}\mathcal{C}\big(x(m,E),E\big)\Big| = \Big|\bigcup_{F\in\bigcup_{i=0}^t\mathcal{E}_i}\mathcal{C}\big(x(m,f(F)),F\big)\Big| \geq \sum_{i=0}^t\binom{n}{i}(q-1)^i \tag{1}$$

and Proposition 1 follows.

The following lower bound can be easily deduced by the standard greedy algorithm (maximal coding).

Proposition 2.

$$L_q(n,t) \geq \frac{q^n}{q^{2t}\binom{n}{t}}.$$

Already Propositions 1 and 2 imply the asymptotic equivalence within a constant

$$L_q(n,t) \asymp \frac{q^n}{n^t}, \quad \text{when } t \text{ is fixed and } n\to\infty.$$

We draw attention to the fact that this equivalence is known for nonbinary error–correcting codes except $t=1$ only for $t=2$ and $q=3,4$ [5].

The purpose of our work is to find the precise constant in the equivalence. We construct asymptotically dense codes.

Theorem. *For every constant* t

$$L_q(n,t) = \frac{q^n}{S_t}(1+o(1)) = \frac{t!}{(q-1)^t}\cdot\frac{q^n}{n^t}(1+o(1))$$

where $o(1)\to 0$ *as* $n\to\infty$ *(* $o(1)$ *depends certainly on* t *and* q *).*

2. Proof of Theorem: the induction step

We proceed by induction on t. The induction beginning $t=1$ is established at the end of the proof in Section 4. The induction step to t goes through the following scheme.

We divide the interval of transmission of length n into $b+1$ successive intervals: the first interval shall be of length r and all the other b intervals shall be of length $k=\frac{n-r}{b}$ (more precisely, when $n-r$ isn't divisible by b, these intervals have the length $\lfloor\frac{n-r}{b}\rfloor$ or $\lceil\frac{n-r}{b}\rceil$). Now, for fixed E let us denote by $t_0,t_1,\dots,t_b$ the number of possible errors in the i–th interval $(i=0,1,\dots,b)$ $(t_0+t_1+\dots+t_b=t)$.

At first we guarantee that the decoder always knows whether $t_0=0$ or $t_0>0$. This we achieve by using in the first r positions always at least $t+1$ 1's, if $t_0=0$, and always r 0's, if $t_0>0$.

Now we distinguish three cases.

Case 1. $t_0 > 0$

We use a code correcting $t-1$ localized errors on the last $n-r$ positions.

Case 2. $t_0 = 0$ and $t_i < t$ for all $i, i = 1, \dots, b$.

In the first r positions we transmit the values of $t_1, \dots, t_b$, and we use for this transmission words of weight at least $t+1$ with the additional restriction that in the first r_1 of the r positions there is at least one 0 . Since the number of solutions of the equality $t_1 + \dots + t_b = t$ with $t_i < t, i = 1, \dots, b$, is equal to $\binom{b+t-1}{t} - b$, we can do this, if numbers satisfy

$$\binom{b+t-1}{t} - b \le q^r - \sum_{i=0}^{t} \binom{r}{i} (q-1)^i - (q-1)^{r_1} q^{r-r_1}. \tag{2}$$

Having transmitted the values of $t_i, i = 1, \dots, b$, we use in the i–th interval $(i = 1, \dots, b)$ a code correcting t_i localized errors.

Case 3. $t_0 = 0$ and $t_j = t, t_i = 0, i \ne j$

We transmit in the first r_1 from r positions ones only in order to distinguish this and the previous case, in the next $\lceil \log_q b \rceil$ positions we transmit the number $j (j = 1, 2, \dots, b)$, and in the next $r - r_1 - \lceil \log_q b \rceil$ positions and in all intervals, except for the j–th , we transmit all possible sequences, and, finally, we use in the j–th interval a code correcting t localized errors with parameters guaranteed by Proposition 2.

After this description of the code count how many messages can be transmitted in everyone of the three cases. Of course this counting makes use of the induction hypothesis for $t' < t$.

Case 1: We can transmit at least

$$L_q(n-r, t-1) = \frac{q^{n-r}}{(q-1)^{t-1} \binom{n-r}{t-1}} \big(1 + o(1)\big) \ge \frac{q^{n-r}}{(q-1)^t \binom{n}{t}} \cdot \frac{(q-1)n}{t} \big[1 + o(1)\big] \tag{3}$$

messages, where $o(1) \to 0$ as $n - r \to \infty$. The inequality is based on the relations $\binom{n-r}{t-1} \le \binom{n-1}{t-1} = \binom{n}{t} \frac{t}{n}$.

Case 2: We can transmit at least

$$\prod_{i=1}^{b} \cdot L_q(k, t_i) \ge \frac{q^{n-r}}{(q-1)^t k^t} \big(1 + o(1)\big) \tag{4}$$

messages, where $o(1) \to 0$ as $k \to \infty$.

Case 3: We can transmit at least

$$L_q(k,t)\cdot q^{n-k-r_1-\lceil\log_q b\rceil} \ge \frac{q^{n-r_1-\lceil\log_2 b\rceil-2t}}{\binom{k}{t}} \ge \frac{q^{n-r}}{\binom{k}{t}} \ge \frac{q^{n-r}}{k^t} \tag{5}$$

messages, provided that

$$r - r_1 \ge \lceil\log_q b\rceil + 2t. \tag{6}$$

Therefore, if (2) and (6) hold, then

$$L_q(n,t) \ge \min\left\{\frac{(q-1)n}{tq^r}, \frac{\binom{n}{t}}{k^t q^r}\right\}\cdot\frac{q^n}{S_t}\big(1+o(1)\big), \text{ where } o(1)\to 0 \text{ as } k\to\infty \text{ and } n-r\to\infty. \tag{7}$$

Under the conditions

$$q^r \le \frac{(q-1)n}{t} \tag{8}$$

and

$$q^r \le \frac{\binom{n}{t}}{k^t}\big[1+o(1)\big], \text{ where } o(1)\to 0 \text{ as } b\to\infty, \tag{9}$$

we have from (7)

$$L_q(n,t) \ge \frac{q^n}{S_t}\big(1+o(1)\big), \tag{10}$$

where $o(1)\to 0$, if $k\to\infty, b\to\infty$.

Finally, we have to choose the parameters r , r_1 and b in a suitable way:

$$\begin{aligned} r &= \lfloor\log_q \frac{(q-1)n}{t}\rfloor \\ r_1 &= r - \lceil\log_q b\rceil - 2t \\ b &= \text{ maximal number such that (2) holds.} \end{aligned} \tag{11}$$

Clearly with these parameters (2), (6) and (8) hold by definitions and it remains only to verify (9). But the definition of b , (11) and (2) imply

$$q^r \le \binom{b}{t}\big(1+o(1)\big), \text{ where } o(1)\to 0 \text{ as } b\to\infty.$$

Since

$$\binom{b}{t} \le \frac{\binom{n}{t}}{k^t},$$

(9) holds.

3. An auxiliary result for perfect codes with one localized error

Recently Kabatyansky [6] constructed codes for one localized error of length $D = \frac{q^d-1}{q-1} (d = 1, 2, \dots)$, which are perfect and thus

$$L_q(D,1) = \frac{q^D}{(q-1)D+1} = \frac{q^D}{S_1}(1+o(1)). \tag{12}$$

From his construction it follows also that

$$L_q(D-1,1) \geq \frac{q^{D-1}}{(q-1)D+1}. \tag{13}$$

Subsequently we established in [7] the following recurrence relation of independent interest. We repeat the proof, because it is brief.

Lemma 2. *If* $N \leq (q-1)T+1$ *, then*

$$L_q(N+T,1) \geq q^{N-1} L_q(T,1).$$

Proof. On the first N positions we always transmit a parity check ($\bmod q$) code of the size q^{N-1} . The last T positions we reserve for the code, which allows us to transmit $L_q(T,1)$ messages and to correct a single localized error. The method of transmission depends on the position of the localized error in the following way:

a) The error is on the last T positions. We use our code as a code, correcting a single localized error.

b) The error is in the first N positions. We use our code for the transmission of both, the message and the number of the position, where the error can occur. According to (1) at least $(q-1)T+1$ different words in the output of the channel of length T corresponds to everyone of $L_q(T,1)$ messages and therefore we can make the successful transmission, if

$$N \leq (q-1)T+1.$$

The proof is complete.

We derive now (12) and (13) and thus make our paper independent of work, which did not yet appear.

Clearly, for $d=1$ we have $D=1$ and (12) holds, because obviously $L_q(1,1)=1$. We proceed now inductively from d to $d+1$. We set $D' = \frac{q^{d+1}-1}{q-1}$ and observe that for $N=(q-1)D+1$ we have $D' = q^d + q^{d-1} + \cdots + 1 = qD+1 = D+N$. By Lemma 2

$$L_q(D',1) \geq q^{(q-1)D} L_q(D,1)$$

and by the induction hypothesis

$$L_q(D',1) \geq q^{(q-1)D} \frac{q^D}{(q-1)D+1} = \frac{q^{qD}}{(q-1)D+1} = \frac{q^{d'}}{q(q-1)D+q} = \frac{q^{D'}}{(q-1)D'+1}.$$

Finally, we verify (13). With the choices $T = \frac{q^{d-1}-1}{q-1}$ and $N = (q-1)T$ we have by Lemma 2 and (12)

$$\begin{aligned} L_q(D-1,1) = L_q(N+T,1) &\geq q^{(q-1)T-1} \frac{q^T}{(q-1)T+1} \\ &= \frac{q^{D-1}}{(q-1)T+1} \geq \frac{q^{D-1}}{(q-1)D+1} \quad \text{(because } D \geq T\text{)}. \end{aligned}$$

Remark. When q is a prime power then the maximal size of a code of length n, correcting a *single* (not necessarily localized) error, already equals $\frac{q^n}{S_1}(1+o(1))$, where $o(1) \to o$ as $n \to \infty$ ([8]). Such a strong result is not available for general q. However, next we establish the asymptotic Hamming bound for general q in case of a localized error $(t=1)$.

4. Proof of Theorem: the induction beginning

For the value $t = 1$ only the cases 1 and 3 occur. This simplifies matters, because there is now no need to inform the decoder whether case 2 or case 3 occured. On the other hand, since $\binom{n}{1}$ is linear in n, rather accurate estimates are needed and in particular the inequality in Proposition 2 is to crude for the present purposes. Instead we use (12) and (13), consequences of Lemma 2.

For general n we devide the interval of transmission of length n into $b+1$ successive blocks such that the 0–th block has length $r \triangleq \lfloor \log_q (q-1)n \rfloor$ and all others have length D or $D-1$ (and so $\left\lfloor \frac{n-r}{D} \right\rfloor \leq b \leq \left\lceil \frac{n-r}{D-1} \right\rceil$).

Case 1. The one error can only be in the 0–th block, where we send (as previously) 0's. In the other blocks all sequences can be send. Therefore we can transmit q^{n-r} messages, where

$$q^{n-r} = q^{n - \lfloor \log_q (q-1)n \rfloor} \geq \frac{q^n}{(q-1)n+1} = \frac{q^n}{S_1}.$$

Case 3. Let the position of a possible error be in the j–th block.

In the 0–th block we use only sequences with at most $r-2$ 0's (to distinguish for the decoder this case from case 1) and we also encode that an error may occur in the j–th block. We cannot waste even one position! This we achieve by partitioning the $q^r - r(q-1) - 1$ sequences with at most $r-2$ 0's into b sets $P_1, \dots, P_b$ such that

$$\left| |P_i| - \frac{q^r - r(q-1) - 1}{b} \right| \leq 1$$

for $i = 1, 2, \dots, b$.

Words in P_j inform the decoder that an error may occur in the j–th block. There the sender uses a code meeting the bounds in (12) or (13) and in the remaining blocks all sequences can be used.

Therefore we can transmit at least

$$\left\lfloor \frac{q^r - r(q-1) - 1}{b} \right\rfloor \frac{q^{n-r}}{(q-1)D+1} \geq \frac{q^n}{S_1}(1 + o(1))$$

messages, where $o(1) \to o$ as $D \to \infty$ and $b \to \infty$.

The proof is complete.

References

1. L.A. Bassalygo, S.I. Gelfand, M.S. Pinsker, Coding for channels with localized errors, Proc. 4–th Soviet–Swedish Workshop in Information Theory, Gotland, Sweden, 1989, 95–99.

2. L.A. Bassalygo, S.I. Gelfand, M.S. Pinsker, Coding for channels with partially localized errors, IEEE Inf. Theory, vol. 37, no. 3, May 1991, 880–884.

3. L.A. Bassalygo, S.I. Gelfand, M.S. Pinsker, Simple methods of deduction of lower bounds in coding theory, Probl. Peredaci Inform., vol. 27, no. 4, 1991, 3–8.

4. R. Ahlswede, Coding for channels with localized errors: the non–binary cases, Preprint 89–020 of SFB 343, Universität Bielefeld.

5. I.I. Dumer, V.A. Zinovyev, New maximum codes over GF(4), Probl. Peredaci Inform., vol. 14, 1978, no. 3, 24–34.

6. G.A. Kabatyansky, The construction of code correcting single localized error. Proc. III International Workshop "Algebraic and Combinatorial Coding Theory", 22–28 June, 1992, Tyrnovo, Bulgaria, in print.

7. R. Ahlswede, L.A. Bassalygo, M.S. Pinsker, Asymptotically dense nonbinary codes correcting a constant number of localized errors, Proc. III International Workshop "Algebraic and Combinatorial Coding Theory, 22–28 June, 1992, Tyrnovo, Bulgaria, in print.

8. G.A. Kabatyansky, V.I. Panchenko, Packings and coverings of Hamming spaces with unit spheres, Probl. Peredaci Inform., vol. 24, 1988, no. 4, 3–16.