Zero-error codes for the noisy-typewriter channel

Francisco J. R. Ruiz
University Carlos III in Madrid
Email: franrruiz87@tsc.uc3m.es

Fernando Pérez-Cruz
University Carlos III in Madrid
Email: fernando@tsc.uc3m.es

***Abstract*—In this paper, we propose nontrivial codes that achieve a non-zero zero-error rate for several odd-letter noisy-typewriter channels. Some of these codes (specifically, those which are defined for a number of letters of the channel of the form $2^n + 1$) achieve the best-known lower bound on the zero-error capacity. We build the codes using linear codes over rings, as we do not require the multiplicative inverse to build the codes.**

I. Introduction

Zero-error information theory, or error-free information theory, is a branch of information theory in which no errors can be tolerated. It was recently discussed in [1], where classic and new results and its applications to information theory were shown. In this paper, we focus on the channel coding results of this broader theory. For the channel-coding problem, Shannon defined in 1956 the zero-error capacity C_0 of a noisy channel [2] as: "the least upper bound of rates at which it is possible to transmit information with zero probability of error". In that paper, Shannon showed that zero capacity is zero if there is a non-zero probability of error for any pair of input symbols (i.e., at least one input symbol can be mistaken for any other input symbol), but it could be non-zero otherwise. Shannon also defined the adjacency between the input symbols, in which we "say that two input symbols are adjacent if there is an output letter which can be caused by either of these two". Shannon constructed an *adjacency matrix*, in which the entry (i, j) is one if the letters i and j are adjacent and 0 otherwise. From this matrix, he proposed a linear graph in which the vertices represented the letters and any two letters were connected if the corresponding entry in the adjacency matrix is one. Shannon used this matrix and its graphical interpretation to obtain or lower-bound the zero-error capacity for several channels.

In this work, we concentrate on the M-letter noisy-typewriter channel, as defined in [3], and its zero-error capacity (see Fig. 1a). From the point of view of the graph that represents this channel, it corresponds to a M-vertices cycle (as shown in Fig. 1b).

For M being an even number, the problem of getting C_0 for this channel is trivially solved by transmitting only one out of every two input letters (e.g., transmitting only the letters $0, 2, \ldots, M-2$). Doing so yields the result $C_0 = \log_2 \frac{M}{2}$, which in this case equals the channel capacity. For an odd value of M, trivial bounds on the zero-error capacity can be found. Since the behavior must be at least as good as a noisy-typewriter channel with $M-1$ letters, C_0 is lower-bounded by the quantity $\log_2 \frac{M-1}{2}$. Since for any given channel, C_0 cannot exceed the ordinary capacity, given in [3], the upper bound is $\log_2 \frac{M}{2}$. Thus, for M being an odd number, we have:

$$\log_2\left(\frac{M-1}{2}\right) \leq C_0 \leq \log_2\left(\frac{M}{2}\right) \tag{1}$$

The main contribution of this paper is the construction of codes that achieve larger rates than the trivial lower bounds given by (1).

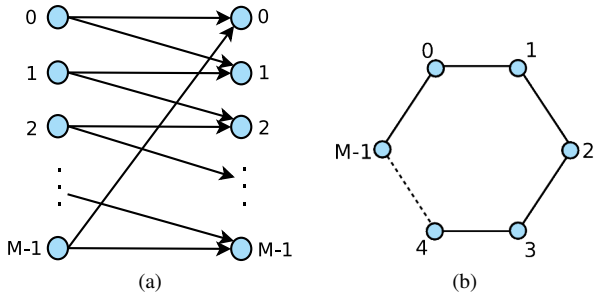

Fig. 1. The M-letter noisy-typewriter channel, and its associated graph.

A. Previous work on the zero-error capacity

Several methods have been studied in order to find the precise value of C_0. For $M = 3$, Shannon proved that $C_0 = 0$, i.e., transmission with zero probability of error is not possible over this channel, since all letters are adjacent. Shannon also found a code for $M = 5$ that achieved the zero-error rate of $\frac{1}{2}\log_2 5$ (simply by constructing the following dictionary of codewords: 00, 12, 24, 31 and 43) [2].

Later on, in 1979, Lovász cleverly proposed a method to upper-bound the zero-error capacity of any arbitrary channel [4]. When applied to the M-vertices cycle graph, whith odd M, it yields the lowest upper bound on the zero-error capacity for this channel:

$$N_0 = 2^{C_0} \leq \frac{M\cos(\pi/M)}{1+\cos(\pi/M)} \tag{2}$$

When applied for $M = 5$, it can be seen that the zero-capacity for this channel is achieved by Shannon's 1956 code.

For $M \geq 7$, the zero-error capacity is still unknown. In particular, for $M = 7$, the best known lower bound on C_0 is given in Vesel and Zerovnik's 2002 work: $N_0 \geq \sqrt[4]{108}$ [5]. For greater odd values of M, several lower bounds have been proposed. Baumert *et al.* [6] proved that:

$$N_0 \geq \sqrt[n]{k(k2^n+1)^{n-1}}, \qquad \text{for } M = k2^n + 1 \tag{3}$$

$$N_0 \geq \sqrt[n]{\frac{k(k2^n+3)^n+1}{k2^n+1}}, \qquad \text{for } M = k2^n + 3 \tag{4}$$

Bohman also established some results concerning on the zero-error capacity of the channel represented by a M-vertices cycle graph. In [7], he proved that for $M = k2^n + 2^{n-1} + 1$, the value of N_0 is lower-bounded by:

$$N_0 \geq \sqrt[n]{kM^{n-1} + \left(\frac{M-1}{2}\right) M^{n-2}} \tag{5}$$

However, whereas these bounds are widely known, no codes have been proposed in order to achieve the corresponding zero-error rates, apart from Shannon's 1956 code. In this paper, we propose new achievable codes that present larger rates than those given by the trivial lower bound for several odd values of $M \geq 7$.

The paper is organized as follows. We show the achievability results in Section II, we present some other examples of codes in Section III and we conclude the paper in Section IV.

II. Codes over rings

In order to construct the achievable codes, instead of working with the adjacency matrix and the graphs proposed by Shannon, we resort to standard linear codes that are defined over rings. For the M-letter noisy-typewriter channel, we can define the channel by the linear operation:

$$y = (x + e) \mod M, \tag{6}$$

where e can either take the value 0 or 1, depending on whether the channel has flipped a letter or it has not, while x and $y \in \{0, 1, \ldots, M-1\}$. As the error can only take the values 0 or 1, we do not need the property that every element of the set has a multiplicative inverse, and hence we can work with rings instead of finite fields, which allows finding a linear code for any M, not only those that are prime or power of a prime.

The codes we propose allow us not only to show a way of achieving a zero-error rate, but also to give an alternative proof of the lower bound that C_0 must satisfy. In particular, for values of M of the form $M = 2^n + 1$, we find the same zero-error rate than the lower bound given in (3).

Also, it is known that, as M grows, $N_0 \to \frac{M}{2}$, which implies that zero-error capacity can be achieved with linear block codes over rings as M tends to infinity.

We start by emphasizing that Shannon's code for $M = 5$ is actually a linear block code with generator matrix $\mathbf{G} = [1\ 2]$, operating under modulo 5 addition and multiplication. It is straightforward to check that the alternative matrix $\mathbf{G} = [1\ 3]$, under identical operations, also yields a zero-error code (in which the full dictionary would be composed by the codewords: 00, 13, 21, 34 and 42). In that case, the corresponding parity-check matrix would be given by $\mathbf{H} = [1\ 2]$. Note that, since each of the elements of the error vector $\mathbf{e}$ can either take the value 0 or 1, the operations implemented at the decoder in order to compute the (scalar) syndrome are indeed a binary to base-5 conversion.

In addition, for $M = 7$ letters, the same parity-check matrix can be used to generate a code with zero error probability, although the rate would fall below $\log_2(3)$. For $M \geq 8$, one can do better by setting $\mathbf{H} = [1\ 2\ 4]$ and operating under modulo M addition and multiplication.

In general, for a noisy-typewriter channel of M letters, we can construct a (n, k) M-ary code with $n \leq \log_2 M$, $k = n-1$ and a parity-check matrix $\mathbf{H}$ of the form:

$$\mathbf{H} = \begin{bmatrix} 1 & 2 & 2^2 & \cdots & 2^{n-1} \end{bmatrix}, \tag{7}$$

which can be identified with a cyclic linear code with a generator polynomial $g(x) = 1 - 2x$.

As every element of the error vector $\mathbf{e}$ is binary, the binary to base-M conversion implemented at the decoder in order to obtain the syndrome yields an integer strictly lesser than M. That is, the maximum value of the syndrome is given by:

$$s_{\max} = \sum_{i=0}^{n-1} 2^i = 2^n - 1 < 2^n \leq M$$

Since this quantity is always less than M and every possible error vector produces a different value of the syndrome, there are exactly 2^n different achievable syndromes, so all error vectors can be correctly identified at the decoder with probability one. Hence, it follows that there is no need to compute any multiplicative inverse elements, and the code can be defined to operate over a ring (instead of a Galois field, as usual [8], [9]). This result yields the following lower bound on C_0:

$$C_0 \geq \frac{n-1}{n} \log_2 M, \qquad n \leq \log_2 M \tag{8}$$

For values of M of the form $M = 2^n$, all the possible syndromes are achievable and the code is a perfect code. Note that, if M can be written as $M = 2^n + 1$, then equations (8) and (3) yield the same rate, which means that we have provided codes that achieve the best-known lower-bound on zero-error capacity for these precise values of M.

For $M = 2^n$, we know that the best code is a nonlinear code that uses one out of two letters, but the code defined by the parity check matrix in (7) also achieves the same rate and, hence, capacity. Additionally, we cad add for these codes the label of *perfect codes*. They are not perfect in the sphere packing sense, but in the sense that every syndrome defines an error and every error is mapped to a single syndrome. Therefore, for those $M = 2^n$, a higher rate code cannot be found (something that we already knew).

III. Other Codes

Apart from the already exposed, we have tried several other linear codes over rings, leading to better results than the previous ones for certain values of M. Since there exist no procedure to construct linear codes over rings, we have

obtained them through a random search. We have focus on codes of rate $(n-2)/n$ for odd n that yield possible codes for $M \geq 2^{n-5} + 2^{n-4} + 1$.

For instance, it is possible to construct a $(5, 3)$ code for the 7-letter channel using the following parity-check matrix:

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 3 & 5 & 3 \\ 0 & 1 & 1 & 2 & 3 \end{bmatrix} \tag{9}$$

For $M = 13$, a $(7, 5)$ code can be defined, yielding zero error probability. The corresponding parity-check matrix needed to achieve this result is given by:

$$\mathbf{H} = \begin{bmatrix} 8 & 4 & 5 & 5 & 10 & 3 & 3 \\ 5 & 0 & 9 & 10 & 7 & 10 & 1 \end{bmatrix} \tag{10}$$

We have also found similar codes for $M = 25$ and 49, with rates $7/9$ and $9/11$ respectively, given by the following parity-check matrices:

$$\mathbf{H} = \begin{bmatrix} 24 & 19 & 0 & 0 & 13 & 5 & 24 & 22 & 0 \\ 21 & 13 & 1 & 2 & 13 & 4 & 0 & 7 & 12 \end{bmatrix} \tag{11}$$

$$\mathbf{H} = \begin{bmatrix} 19 & 19 & 4 & 11 & 16 & 22 & 44 & 35 & 6 & 38 & 16 \\ 0 & 1 & 45 & 0 & 2 & 0 & 0 & 4 & 4 & 12 & 24 \end{bmatrix} \tag{12}$$

It is still unclear if there is a way to construct these codes systematically and how can we achieve other rates.

See Figs. 2 and 3 for details on the achievable rates that have been found. Note that none of the proposed codes achieves a higher rate than the previously known lower bounds, although the codes defined for $M = 2^n + 1$ achieve those bounds.

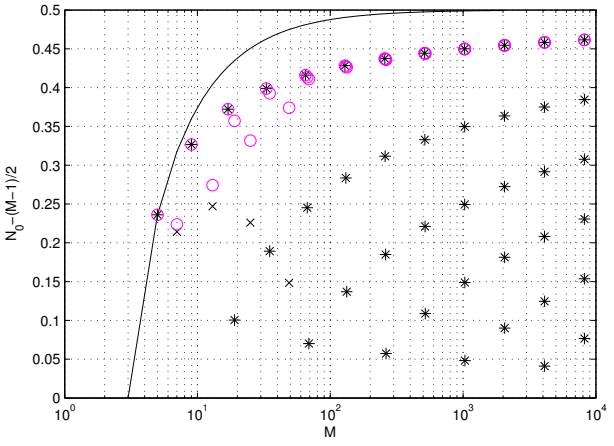

Fig. 2. Lower bounds on C_0 as a function of M. The vertical axis has been chosen so that the trivial bounds given by (1) correspond to horizontal lines at 0 and $1/2$. Stars and crosses show the values attained by the proposed codes (from equation (7) in section II and (9)-(12) in section III, respectively), whereas circles show the previously known lower bounds (from equations (3)-(5) and Theorem 3.1 in [7]). The continuous line shows the upper bound given by Lovász (it is only valid for odd values of M).

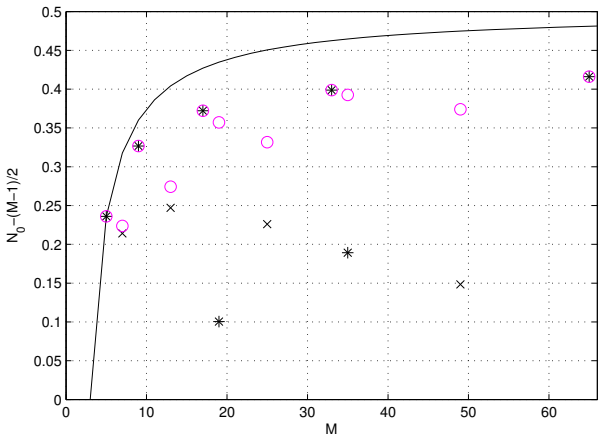

Fig. 3. Zoom on Fig. 2 for small values of M. This figure is included to clarify the performance of the codes from section III. Black crosses correspond, from left to right, to the codes defined by equations (9), (10), (11) and (12).

IV. Conclusion

To sum up, we have given a way to construct zero-error rate codes for the noisy-typewriter channel of an odd number of letters M. The rates of these codes do not improve the previously known lower bounds on the zero-error capacity, but they provide the same values when M can be written on the form $M = 2^n + 1$, so the codes can be seen as an alternative proof of the achievability results.

The peculiarity of these codes lies on the fact that they are based on linear codes defined over rings instead of Galois fields, as usual.

References

[1] J. Korner and A. Orlitsky, "Zero-Error Information Theory," *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2207−2229, Oct. 1998.

[2] C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inform. Theory*, vol. IT-2, no. 3, pp. 8−19, Sept. 1956.

[3] T. M. Cover and J. A. Thomas, *Elements of Information Theory,* Wiley-Interscience, New York, 1991.

[4] L. Lovász, "On the Shannon capacity of a graph," *IEEE Trans. Inform. Theory*, vol. IT-25, no. 1, pp. 1-7, Jan. 1979.

[5] A. Vesel and J. Zerovnik, "Improved lower bound on the Shannon capacity of C7," *Inform. Processing Lett.*, vol. 81, no. 5, pp. 277-282, 2002.

[6] L. Baumert *et al.*, "A combinatorial packing problem," *Computers in Algebra and Number Theory*, Providence, American Mathematical Society, pp. 97-108, 1971.

[7] T. Bohman, "A limit theorem for the Shannon capacities of odd cycles. II," *Proceedings of the American Mathematical Society*, vol. 133, no. 2, pp. 537-543, 2005.

[8] S. B. Wicker, *Error control systems for digital communication and storage,* Prentice-Hall, New Jersey, 1995.

[9] S. Lin and D. J. Costello, *Error control coding: Fundamentals and applications,* Prentice-Hall, 1983.