



MIT Open Access Articles

New Constructions of Codes for Asymmetric Channels via Concatenation

The MIT Faculty has made this article openly available. **Please share** how this access benefits you. Your story matters.

Citation	Grassl, Markus et al. "New Constructions of Codes for Asymmetric Channels via Concatenation." IEEE Transactions on Information Theory 61, 4 (April 2015): 1879–1886 © 2015 IEEE
As Published	http://dx.doi.org/10.1109/TIT.2015.2401567
Publisher	Institute of Electrical and Electronics Engineers (IEEE)
Version	Original manuscript
Citable link	http://hdl.handle.net/1721.1/115987
Terms of Use	Creative Commons Attribution-Noncommercial-Share Alike
Detailed Terms	http://creativecommons.org/licenses/by-nc-sa/4.0/

New Constructions of Codes for Asymmetric Channels via Concatenation

Markus Grassl, *Member, IEEE*, Peter Shor, Graeme Smith, John Smolin, and Bei Zeng

Abstract—We present new constructions of codes for asymmetric channels for both binary and nonbinary alphabets, based on methods of generalized code concatenation. For the binary asymmetric channel, our methods construct nonlinear single-error-correcting codes from ternary outer codes. We show that some of the Varshamov-Tenengol'ts-Constantin-Rao codes, a class of binary nonlinear codes for this channel, have a nice structure when viewed as ternary codes. In many cases, our ternary construction yields even better codes. For the nonbinary asymmetric channel, our methods construct linear codes for many lengths and distances which are superior to the linear codes of the same length capable of correcting the same number of symmetric errors.

In the binary case, Varshamov [2] has shown that almost all good linear codes for the asymmetric channel are also good for the symmetric channel. Our results indicate that Varshamov's argument does not extend to the nonbinary case, i.e., one can find better linear codes for asymmetric channels than for symmetric ones.

I. INTRODUCTION

In communication systems, the signal transmitted is conventionally represented as a finite sequence of elements from an alphabet A , which we assume to be finite. In general, we may take $A = \{0, 1, \dots, q-1\}$, and if needed, some additional structure is assumed, e.g., $A = \mathbb{Z}_q$ or $A = \mathbb{F}_q$. The most commonly discussed channel model is the uniform symmetric channel, that is, an error $a \rightarrow b$ happens with equal probability for any $a, b \in A$ and $a \neq b$. Error-correcting codes for these channels are extensively studied, see, for instance, [3].

However, in other systems, such as some data storing systems including flash memories [4], [5] and optical communication [6], the probability of the error $a \rightarrow b$ is no longer independent of a and b and might vary a lot. If some errors of low probability are neglected, some of those channels can be modeled as 'asymmetric channels.'

G. Smith and J. Smolin acknowledge support from the DARPA QUEST program under contract number HR0011-09-C-0047. B. Zeng is supported by NSERC and CIFAR. The Centre for Quantum Technologies is a Research Centre of Excellence funded by the Ministry of Education and the National Research Foundation of Singapore.

M. Grassl is with the Centre for Quantum Technologies, National University of Singapore, Singapore 117543, Republic of Singapore (e-mail: Markus.Grassl@nus.edu.sg).

P. W. Shor is with the Department of Mathematics, Massachusetts Institute of Technology, Cambridge MA 02139, USA.

G. Smith and J. Smolin are with the IBM T. J. Watson Research Center, Yorktown Heights, NY 10598, USA.

B. Zeng is with the Department of Mathematics & Statistics, University of Guelph, Guelph, ON, N1G 2W1, Canada and with the Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada.

Part of this work has been presented [1] at the 2012 IEEE International Symposium on Information (ISIT 2012) in Cambridge, MA, USA.

More precisely, let the alphabet be $A = \{0, 1, \dots, q-1\} \subset \mathbb{Z}$ with the ordering $0 < 1 < 2 < \dots < q-1$. A channel is called asymmetric if any transmitted symbol a is received as $b \leq a$. For example, for $q = 2$, the symbol 0 is always received correctly while 1 may be received as 0 or 1. The corresponding channel is called \mathcal{Z} -channel, see Fig. 1. For $q > 2$, one can have different types of asymmetric channels [7].

Coding problems for asymmetric channels were discussed by Varshamov in 1965 [2]. For the characterization of codes for these channels, we need the following.

Definition 1.1 (see [2], [8], [9]): For $\mathbf{x}, \mathbf{y} \in A^n$, where $\mathbf{x} = (x_1, x_2, \dots, x_n)$ and $\mathbf{y} = (y_1, y_2, \dots, y_n)$, let

- (i) $w(\mathbf{x}) := \sum_{i=1}^n x_i$,
- (ii) $N(\mathbf{x}, \mathbf{y}) := \sum_{i=1}^n \max\{y_i - x_i, 0\}$, and
- (iii) $\Delta(\mathbf{x}, \mathbf{y}) := \max\{N(\mathbf{x}, \mathbf{y}), N(\mathbf{y}, \mathbf{x})\}$.

Here $w(\mathbf{x})$ is the weight of \mathbf{x} , and $\Delta(\mathbf{x}, \mathbf{y})$ is called the asymmetric distance between \mathbf{x} and \mathbf{y} . If \mathbf{x} is sent and \mathbf{y} is received, we say that $w(\mathbf{x} - \mathbf{y})$ errors have occurred. Note that $w(\mathbf{x} - \mathbf{y}) \geq 0$ for asymmetric channels.

In this model, a code correcting t -errors is called a t -code [9]. The following theorem naturally follows.

Theorem 1.2 (see [9]): A set $C \subset A^n$ is a t -code if and only if $\Delta(\mathbf{x}, \mathbf{y}) > t$ for all $\mathbf{x}, \mathbf{y} \in C$, $\mathbf{x} \neq \mathbf{y}$.

Apparently, any code which can correct t errors on a symmetric channel will also be capable of correcting t asymmetric errors, but the converse is not true in general. However, Varshamov showed that almost all linear binary codes which are able to correct t errors for the \mathcal{Z} -channel are also able to correct t symmetric errors [2]. Therefore, in order to construct good codes for the \mathcal{Z} -channel, nonlinear constructions are needed. Varshamov and Tenengol'ts [10], followed by Constantin and Rao [11], constructed families of 1-codes for the \mathcal{Z} -channel with size $\geq \frac{2^n}{n+1}$. These codes are constructed based on an Abelian group G for which the group operation is denoted by '+' and the identity of G is denoted by 0_G or just 0.

Definition 1.3 (Constantin-Rao (CR) codes): Let G be an Abelian group of order $n+1$ and identity 0_G . For fixed $g \in G$, the CR code \mathcal{C}_g is given by

$$\mathcal{C}_g = (\{(x_1, x_2, \dots, x_n) \mid \sum_{i=1}^n x_i g_i = g\}), \quad (1)$$

where g_1, g_2, \dots, g_n are the non-identity elements of G , $x_i \in \{0, 1\}$, and the product $x_i g_i$ is defined in the canonical way $1g_i = g_i$ and $0g_i = 0_G$.

If the group G is a cyclic group of order $n+1$, then the corresponding codes are Varshamov-Tenengol'ts (VT) codes

[10] (denoted by \mathcal{V}_g). It is known that the largest Constantin-Rao code of length n is the code \mathcal{C}_0 based on the group $G = \bigoplus_{p|(n+1)} \bigoplus_{i=1}^{n_p} \mathbb{Z}_{p_i}$, where $n+1 = \prod_{p|(n+1)} p^{n_p}$ is the prime factorization of $n+1$ and \bigoplus denotes the direct product of groups (see [9]). These VT-CR codes have better rates than the corresponding single-error-correcting codes for the binary symmetric channel for all lengths n apart from $n = 2^r - 1$. In this case, the code \mathcal{C}_0 for the group $G = \mathbb{Z}_2^r$ is the linear binary Hamming code.

These VT-CR codes have a direct generalization to the nonbinary case. The modification of Definition 1.3 is to let $x_i \in A = \{0, 1, \dots, q-1\}$ and require that the order of g_i is at least q . The resulting nonlinear codes have cardinality $|\mathcal{C}_g| \geq \frac{q^n}{q^{n+1}}$. Note that by the Hamming bound, we have $|\mathcal{C}_{\text{sym}}| \leq \frac{q^n}{(q-1)^{n+1}}$ for a symmetric single-error-correcting code. Hence for $q > 2$ and all lengths n , the VT-CR codes have more codewords than the best single-error-correcting symmetric codes of the same length. The construction can also be generalized to the case of t -codes with $t > 1$, for both binary and nonbinary alphabets [9].

Some other constructions for designing single-error-correcting codes for the \mathcal{Z} -channel have also been introduced. In particular the partition method, together with some heuristic search give good lower bounds for small length codes with $n \leq 25$ [12]–[15]. Nevertheless, the VT-CR construction remains the best systematic construction of binary 1-codes to date, and the situation is similar for the nonbinary case. For a survey of classical results on codes for the \mathcal{Z} -channel, see [9].

In this paper, we present new constructions of codes for asymmetric channels for both binary and nonbinary alphabets, based on methods of generalized code concatenation. For the binary asymmetric channel, our methods construct nonlinear 1-codes from ternary outer codes which are better than the VT-CR codes. For nonbinary asymmetric channels, our methods yield linear codes for many lengths and distances, which outperform the linear codes of the same lengths capable of correcting the same number of symmetric errors. For certain lengths, our construction gives linear codes with equal cardinality as the nonlinear VT-CR codes. Our results indicate that Varshamov's argument does not extend to the nonbinary case, i.e., one can find better linear codes for asymmetric channels than for symmetric ones. We will also apply our nonbinary linear codes to correct asymmetric limited magnitude errors [16], which models the asymmetric errors in multilevel flash memories in a more detailed manner.

II. BINARY ASYMMETRIC CODES FROM TERNARY OUTER CODES

To discuss our new construction for asymmetric codes based on the generalized concatenation method, we start with the binary case, building 1-codes for the \mathcal{Z} -channel. We know that in this case, good codes would have to be nonlinear, so our method returns nonlinear codes.

To construct 1-codes for the \mathcal{Z} -channel, we first partition all two-bit strings $\{00, 01, 10, 11\}$ into three 1-codes, which are $\mathcal{C}_0 = \{00, 11\}$, $\mathcal{C}_1 = \{01\}$, $\mathcal{C}_2 = \{10\}$. Then we further find some outer codes over the alphabet $\{0, 1, 2\}$ (i.e. ternary

outer codes). Each code symbol is encoded into each of the 1-codes by $i \mapsto C_i$. To be more precise, define a binary to ternary map $\tilde{\mathfrak{S}}$, which maps two bits to one trit.

Definition 2.1: The map $\tilde{\mathfrak{S}}: \mathbb{F}_2^2 \rightarrow \mathbb{F}_3$ is defined by

$$\tilde{\mathfrak{S}}: 00 \mapsto 0, 11 \mapsto 0, 01 \mapsto 1, 10 \mapsto 2. \quad (2)$$

The encoding $i \rightarrow C_i$ is then given by the inverse map of $\tilde{\mathfrak{S}}$. Note that $\tilde{\mathfrak{S}}$ is not one-to-one. So for the ternary symbol 0 the inverse map gives the two binary codewords 00 and 11, while for 1 and 2 we get the unique codewords 01 and 10, respectively.

Definition 2.2: The map $\mathfrak{S}: \mathbb{F}_3 \rightarrow \mathcal{P}(\mathbb{F}_2^2)$ is defined by

$$\mathfrak{S}: 0 \mapsto \{00, 11\}, 1 \mapsto \{01\}, 2 \mapsto \{10\}. \quad (3)$$

Note that for a binary code of length $n = 2m$, by choosing a pairing of coordinates, the map $\tilde{\mathfrak{S}}^m: \mathbb{F}_2^{2m} \rightarrow \mathbb{F}_3^m$ takes a given binary code of length $2m$ to a ternary code of length m . On the other hand, Definition 2.2 can be naturally extended as well, i.e., the map \mathfrak{S}^m takes a given ternary code of length m to a binary code of length $2m$. The map \mathfrak{S}^m hence specifies the encoding of an outer ternary code into the inner codes C_i .

We remark that our method is indeed a two-level concatenation as discussed in [17]. In the language of [17], we have an inner code $B_0 = \{00, 01, 10, 11\}$ which is partitioned into three codes $B_{1,1} = \{00, 11\}$, $B_{1,2} = \{01\}$ and $B_{1,3} = \{10\}$. We also have two outer codes, one is a ternary code A_0 of length m , and the other is the trivial ternary code of length 1, i.e. $A_1 = \{0, 1, 2\}$. The two-level concatenated code is then a binary code with length $2m$.

For a better understanding of the maps $\tilde{\mathfrak{S}}^m$ and \mathfrak{S}^m , we look at some examples.

Example 2.3: The optimal 1-code $\mathcal{C}^{(4)}$ of length $n = 4$ and cardinality 4 has four codewords 0000, 1100, 0011, 1111. By pairing coordinates 1, 2 and 3, 4, the ternary image under $\tilde{\mathfrak{S}}^2$ is then 00.

Example 2.4: By starting from the ternary outer code of length $n = 3$ with the codewords 000, 111, 122, 212, 221, the map \mathfrak{S}^3 yields the binary code $\mathcal{C}^{(6)}$ with the 12 codewords

$$\begin{aligned} &000000, 000011, 001100, 001111, 110000, 110011, \\ &111100, 111111, 010101, 011010, 100110, 101001. \end{aligned} \quad (4)$$

The code $\mathcal{C}^{(6)}$ has asymmetric distance 2, hence correcting one asymmetric error. This is known to be an optimal 1-code for $n = 6$ [9].

Example 2.5: By starting from the linear ternary code $[4, 2, 3]_3$ with generators 0111, 1012, the map \mathfrak{S}^4 yields the binary code $\mathcal{C}^{(8)}$ with 32 codewords

$$\begin{aligned} &00000000, 00000011, 00001100, 00001111, \\ &00110000, 00110011, 00111100, 00111111, \\ &11000000, 11000011, 11001100, 11001111, \\ &11110000, 11110011, 11111100, 11111111, \\ &00010101, 00101010, 11010101, 11101010, \\ &01000110, 10001001, 01110110, 10111001, \\ &01011000, 10100100, 01011011, 10100111, \\ &10010001, 01100010, 10011101, 01101110. \end{aligned} \quad (5)$$

$\mathcal{C}^{(8)}$ has asymmetric distance 2, hence correcting one asymmetric error. We observe that $\mathcal{C}^{(8)}$ is exactly the CR code \mathcal{C}_0

of length $n = 8$ constructed from the group $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, which hints some relationship between the ternary construction and CR codes. We will discuss this in more detail in Sec. IV.

Example 2.5 indicates that good 1-codes can be obtained from some ternary codes under the map \mathfrak{S}^m . Now the question is what is the general condition under which a ternary code gives a 1-code via the map \mathfrak{S}^m . To address this question, by combining the action of the channel $\mathcal{Z} \times \mathcal{Z}$ and the map \mathfrak{S} , we obtain the ternary channel \mathcal{T} as shown in middle of Fig. 1. Note that \mathcal{T} is different from the ternary symmetric channel \mathcal{R}_3 , which is also shown in Fig. 1.

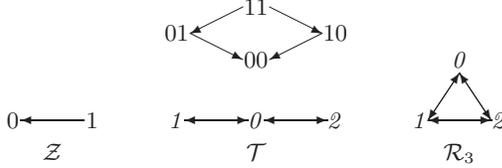


Fig. 1. The binary asymmetric channel \mathcal{Z} , the ternary channel \mathcal{T} derived from $\mathcal{Z} \times \mathcal{Z}$ and \mathfrak{S} , and the ternary symmetric channel \mathcal{R}_3 . The arrows indicate the possible transitions between symbols.

Now we come to the main result of this section, which states that any single-error-correcting code for the ternary channel \mathcal{T} gives a 1-code under the map \mathfrak{S}^m .

Theorem 2.6: If \mathcal{C}' is a single-error-correcting ternary code of length m for the channel \mathcal{T} , then $\mathcal{C} = \mathfrak{S}^m(\mathcal{C}')$ is a 1-code of length $2m$.

Proof: For any two codewords $\mathbf{c}'_1, \mathbf{c}'_2 \in \mathcal{C}'$, we have to show that the asymmetric distance between $\mathfrak{S}^m(\mathbf{c}'_1)$ and $\mathfrak{S}^m(\mathbf{c}'_2)$ is at least two.

First assume that the Hamming distance between \mathbf{c}'_1 and \mathbf{c}'_2 is at least three. Then the Hamming distance between $\mathfrak{S}^m(\mathbf{c}'_1)$ and $\mathfrak{S}^m(\mathbf{c}'_2)$ is also at least three, which implies that the asymmetric distance between $\mathfrak{S}^m(\mathbf{c}'_1)$ and $\mathfrak{S}^m(\mathbf{c}'_2)$ is at least two.

If the Hamming distance between \mathbf{c}'_1 and \mathbf{c}'_2 is less than three, it suffices to consider ternary words of length two. It turns out that the following ten pairs of such ternary words can be uniquely decoded if a single error happens in the channel $\mathcal{T} \times \mathcal{T}$:

$$\begin{array}{cccccc} 01, 22 & 10, 22 & 01, 12 & 10, 21 & 02, 11, & \\ 20, 11 & 02, 21 & 20, 12 & 11, 22 & 12, 21. & \end{array} \quad (6)$$

The asymmetric distance between the images of each pair under \mathfrak{S}^2 is at least two. ■

The following corollary is straightforward.

Corollary 2.7: If \mathcal{C}' is an $(m, K, 3)_3$ code, then $\mathfrak{S}^m(\mathcal{C}')$ is a 1-code of length $2m$.

The size of the binary code can be computed as follows.

Theorem 2.8: Let \mathcal{C}' be a ternary code of length m with homogeneous weight enumerator

$$W_{\mathcal{C}'}(X, Y) = \sum_{\mathbf{c}' \in \mathcal{C}'} X^{m-\text{wgt}(\mathbf{c}')} Y^{\text{wgt}(\mathbf{c}')}, \quad (7)$$

where $\text{wgt}(\mathbf{c}')$ denotes the Hamming weight of \mathbf{c}' . Then $\mathcal{C} = \mathfrak{S}^m(\mathcal{C}')$ has cardinality $|\mathcal{C}| = W_{\mathcal{C}'}(2, 1)$.

Proof: By Definition 2.2, for every zero in the codeword \mathbf{c}' the corresponding pair in the binary codeword can take two

different values, while the non-zero elements are mapped to a unique binary string. Hence $|\mathfrak{S}^m(\mathcal{C}')| = 2^{m-\text{wgt}(\mathcal{C}')}$. ■

Theorem 2.6 only works for designing 1-codes of even length. So we generalize this construction to odd length, starting from ‘adding a bit’ to the ternary code.

Theorem 2.9: If \mathcal{C}' is a single-error-correcting code of length $m + 1$ for the channel $\mathcal{Z} \times \mathcal{T}^m$, then $\mathcal{C} = \mathfrak{S}^m(\mathcal{C}')$ is a 1-code of length $2m + 1$, where \mathfrak{S}^m acts on the last m coordinates of \mathcal{C}' .

Proof: First note that the combined channel $\mathcal{Z} \times \mathcal{T}^m$ has a mixed input alphabet. Hence the first coordinate in \mathcal{C} is binary while the others are ternary. For any two codewords $\mathbf{c}'_1, \mathbf{c}'_2 \in \mathcal{C}'$, we have to show that the asymmetric distance between $\mathfrak{S}^m(\mathbf{c}'_1)$ and $\mathfrak{S}^m(\mathbf{c}'_2)$ is at least two.

First assume that the Hamming distance between \mathbf{c}'_1 and \mathbf{c}'_2 is at least three. Then the Hamming distance between $\mathfrak{S}^m(\mathbf{c}'_1)$ and $\mathfrak{S}^m(\mathbf{c}'_2)$ is also at least three, implying that the asymmetric distance between $\mathfrak{S}^m(\mathbf{c}'_1)$ and $\mathfrak{S}^m(\mathbf{c}'_2)$ is at least two.

If the Hamming distance between \mathbf{c}'_1 and \mathbf{c}'_2 is less than three, the case that the positions where they differ does not involve the first coordinate has already been covered in the proof of Theorem 2.6. So assume that the first coordinate is a bit and the second is a trit. There are exactly two pairs $01, 12$ and $12, 11$ for which a single error on $\mathcal{Z} \times \mathcal{T}$ can be corrected. The corresponding images of each pair under \mathfrak{S}^m give binary codewords of asymmetric distance two. ■

To illustrate this construction for odd length codes, we look at the following example.

Example 2.10: Consider the code $0000, 0111, 0222, 1012, 1120, 1201$ for the channel $\mathcal{Z} \times \mathcal{T}^3$. The image under the map \mathfrak{S}^3 is the binary code

$$\begin{array}{cccc} 0000000, & 0000011, & 0001100, & 0001111, \\ 0110000, & 0110011, & 0111100, & 0111111, \\ 0010101, & 0101010, & 1000110, & 1110110, \\ 1011000, & 1011011, & 1100001, & 1101101. \end{array} \quad (8)$$

This is a code of length 7, cardinality 16, with asymmetric distance two, hence correcting one asymmetric error.

The following corollary is straightforward, but gives the most general situation of the ternary construction.

Corollary 2.11: If \mathcal{C}' is a ternary single error correcting code of channel $\mathcal{Z}^{m_1} \times \mathcal{T}^{m_2}$ of length $m_1 + m_2$, then $\mathcal{C} = \mathfrak{S}^{m_2}(\mathcal{C}')$ is a 1-code of length $m_1 + 2m_2$, where \mathfrak{S}^{m_2} acts on the last n coordinate of \mathcal{C}' .

III. NEW BINARY ASYMMETRIC CODES WITH STRUCTURE

In the following, we compare nonlinear binary codes for the \mathcal{Z} -channel which are the image of ternary linear codes (“ \mathbb{F}_3 -linear codes”), and linear binary codes. For this, we compare the rate of 1-codes for various length. The ratio of the rates is given by $s = \log_2 |T| / \log_2 |B|$, where $|T|$ and $|B|$ are the cardinalities of the nonlinear binary 1-code from a linear ternary code T of Hamming distance three, and a linear binary code B of Hamming distance three, respectively.

From Table I we see that for certain lengths, the 1-codes obtained from ternary linear codes indeed encode more bits than the corresponding linear binary codes. In particular, for

TABLE I

RATIO s OF THE RATES OF \mathbb{F}_3 -LINEAR CODES AND LINEAR BINARY CODES

n	6	8	10	12	14	16	18
s	1.107	1.250	1.000	0.940	0.936	1.026	1.020
n	20	22	24	26	28	30	32
s	1.017	1.014	1.013	1.012	0.967	0.946	0.987
n	34	36	38	40	42	44	46
s	0.988	0.988	0.989	0.990	0.990	0.991	0.991
n	48	50	52	54	56	58	60
s	0.992	0.992	0.992	0.993	0.993	0.993	0.994
n	62	64	66	68	70	72	74
s	0.994	1.012	1.011	1.011	1.010	1.010	1.010
n	76	78	80	82	84	86	88
s	1.010	1.009	1.009	0.987	0.988	0.988	0.988

$n = 8$ the 1-code of cardinality 32 encodes one bit more than the linear binary code of size 16. This should be related to the fact that the ternary Hamming code of length $8/2 = 4$ is ‘good.’ On the other hand, binary linear codes of distance three are ‘bad’ for length 8, 16, 32, 64. Also, the 1-codes of length 64 through 80 outperform the corresponding linear binary code, i.e. $s > 1$. A general understanding of the condition under which $s > 1$ for those \mathbb{F}_3 -linear codes for the \mathcal{Z} -channel is still lacking. For instance, we do not know why $s < 1$ for $n = 32$, despite the fact that the binary linear code of distance three is ‘bad’ at length 32.

Recall that Example 2.4 starts from a single-error-correcting ternary cyclic code of length 3, and results in a 1-code of length 6 achieving the upper bound given in [9] via the map \mathfrak{S}^3 . Note that by the ternary construction, ternary cyclic codes give binary quasi-cyclic codes. It turns out that we can find more good 1-codes from cyclic ternary codes of length m .

For $m = 4$, we have found a ternary cyclic code with codewords 0000, 0112, 1222, 1111, and their cyclic shifts, which leads to a 1-code with parameters (8,29). For $m = 5$, we have found a unique ternary cyclic code which lead to a 1-code with parameters (10,98). For $m = 6, 7, 8$, we have found ternary cyclic codes which lead to 1-codes with parameters (12,336), (14,1200), and (16,3952), respectively. The generators of the cyclic codes for $m = 4, \dots, 8$ are given in Table II.

From Table IV below we see that the 1-codes from cyclic ternary codes are not as good as the codes (8,32) (given in Example 2.5) and (10,105), (12,351) which are obtained via random numerical search based on the ternary construction. However, with growing length imposing the cyclic structure reduces the search complexity. The codes (14,1200) and (16,3952) listed in Table IV, for example, are obtained from ternary cyclic codes of length $m = 7$ and $m = 8$, respectively, while non-exhaustive randomized search did not yield anything better as the search space is too large.

For odd length, we can use the following construction of extended ternary codes.

Lemma 3.1: Let C' be a ternary code of length m which can be decomposed into two subcode C'_0 and C'_1 such that each code C'_i can correct a single error for the channel \mathcal{T} and for any pair of codewords $c'_0 \in C'_0$ and $c'_1 \in C'_1$, the distance with respect to the channel \mathcal{T} is at least two. Then the image

TABLE II

GENERATORS OF TERNARY CYCLIC CODES WHICH YIELD GOOD BINARY 1-CODES.

m	generators
4	0000, 0112, 1222, 1111
5	00000, 10012, 20110, 12210, 11202, 11111, 22122
6	000000, 100021, 122000, 010101, 120102, 101101, 201102, 101202, 102012, 222102, 202020, 112011, 220220
7	0000000, 0000121, 1100022, 0022020, 1110100, 1020100, 1002001, 0021021, 2001011, 1200211, 2021200, 0201220, 1022200, 1221010, 1012020, 1021201, 1022121, 2221020, 0112122, 1111121, 1112221, 1122112, 2121211, 2221212, 2222222
8	00000201, 00010112, 00011010, 00021200, 00101210, 00110011, 00121111, 00222110, 01011102, 01212210, 02021002, 02112201, 02211101, 02211210, 02211222, 10001122, 10010210, 10122021, 10122111, 10202002, 11021220, 11100200, 11111111, 11111210, 11120002, 11222011, 12001200, 12100120, 12102200, 12111211, 12112022, 12121212, 20010200, 20102201, 20121212, 20210101, 20222011, 20222200, 21100210, 21120111, 21120120, 21200221, 21212110, 22000012, 22000100, 22020201, 22022000, 22101102, 22101222, 22102210, 22120110, 22221221, 22222222

of $C'' = 0C'_0 \cup 1C'_1$ under \mathfrak{S}^m is a 1-code of length $2m + 1$ for the asymmetric binary channel.

Proof: We only have to consider codewords of C'' which differ in the first position, i.e., $c''_0 = 0c'_0$ and $c''_1 = 1c'_1$. If the Hamming distance between c'_0 and c'_1 is only one, then without loss of generality, we can assume $c'_0 = 1v$ and $c'_1 = 2v$, as only the symbols 1 and 2 have distance two with respect to the channel \mathcal{T} . Then the images of c''_i under \mathfrak{S}^m are $c_0 = 001\mathfrak{S}^{m-1}(v)$ and $c_1 = 110\mathfrak{S}^{m-1}(v)$. Similarly, if c'_0 and c'_1 differ in at least two positions, the images of c''_i under \mathfrak{S}^m will have asymmetric distance greater than one. ■

Generators for extended cyclic codes based on Lemma 3.1 are given in Table III.

Example 3.2: For $m = 3$, consider the cyclic codes $C'_0 = \{000, 111, 222\}$, and $C'_1 = \{210, 021, 102\}$. The image of $0C'_0 \cup 1C'_1$ under \mathfrak{S}^3 is

0000000, 0000011, 0001100, 0001111,
0110000, 0110011, 0111100, 0111111,
0010101, 0101010,
1100100, 1100111, 1001001, 1111001, 1010010, 1011110.

We finally note that we use nonlinear cyclic codes. This makes it more complicated to find a systematic generalized construction for larger length.

IV. THE BINARY VT-CR CODES VIEWED AS TERNARY CODES

In this section we clarify the relationship between the ternary construction and the VT-CR codes, by showing that certain VT-CR codes are a special case of the ternary construction. We start from the following.

Definition 4.1: A binary code C of even length $n = 2m$ is called ternary if $\mathfrak{S}^m(\mathfrak{S}^m(C)) = C$.

Based on this definition, if a binary code C of even length is ternary, then it can be constructed from some ternary code

TABLE III
GENERATORS OF EXTENDED TERNARY CYCLIC CODES WHICH YIELD
GOOD BINARY 1-CODES.

m	generators
3	0000, 0111, 0222, 1210
4	00000, 00221, 01211, 02222, 11010, 12020, 11220
5	000000, 010021, 012102, 020111, 022201, 011111, 022222, 102210, 101020, 101212
6	0100021, 0122000, 0100100, 0200200, 0010101, 0222010, 0110201, 0101202, 0202020, 0111111, 0221211, 0212211, 0222222, 1022100, 1112000, 1001002, 1120102, 1101101, 1012111, 1102012, 1220220, 1122202, 1211112, 1211222, 1121212
7	01100002, 00200100, 01200010, 00202200, 00112200, 01002120, 01001011, 01210020, 01222100, 00022202, 01221200, 00101121, 00210201, 01102220, 01020111, 01012211, 02021210, 00122221, 01112021, 01202221, 01111111, 01122112, 02222222, 10221000, 10102000, 10001101, 12000120, 12101100, 11100120, 11002202, 11200220, 11200211, 10012112, 11021210, 12201022, 11110220, 10112111, 11212210, 10202122, 10211212, 12202212, 11221221

via the map \mathfrak{S} . The following theorem shows that certain VT-CR codes are a special case of asymmetric codes constructed from some ternary codes.

Theorem 4.2: For n even, the VT code \mathcal{V}_g and the CR code \mathcal{C}_g are ternary for any g .

Proof: Let $\mathcal{C} = \mathcal{V}_g$ or $\mathcal{C} = \mathcal{C}_g$. We only need to prove that there exists a pairing of the coordinates of \mathcal{C} such that for any codeword $v \in \mathcal{C}$ the following holds: if for a pair α of coordinates the code symbols of v are 00, denoted by $v|_\alpha = 00$, then there exists another codeword $v' \in \mathcal{C}$ with $v'|_\alpha = 11$ and $v'|_{\bar{\alpha}} = v|_{\bar{\alpha}}$. Here $\bar{\alpha}$ denotes all coordinates except the pair α .

Both the VT code \mathcal{V}_g and the CR code \mathcal{C}_g are defined by a group G of odd order $n+1$, and the coordinates of the codewords correspond to the non-identity group elements. As the group order is odd, the only group element that is its own inverse is identity. Hence we can pair every non-identity element $h \in G$ with its inverse $-h$. If neither h nor $-h$ are contained in the sum in Eq. (1), then the sum clearly does not change when including both h and $-h$. ■

We look at some examples.

Example 4.3: For $n = 6$, the VT code \mathcal{V}_0 is given by

$$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 = 0 \pmod{7}, \quad (9)$$

where $x_i \in \{0, 1\}$. Then one can use the pairing

$$\{x_1x_6, x_2x_5, x_3x_4\}. \quad (10)$$

The cardinality of the code is 10. The image of this code under \mathfrak{S}^6 is a linear code $[3, 1, 3]_3$.

Example 4.4: For $n = 8$, the VT code \mathcal{V}_0 is given by

$$\sum_{i=1}^8 ix_i = 0 \pmod{9}, \quad (11)$$

where $x_i \in \{0, 1\}$. Then one can use the pairing

$$\{x_1x_8, x_2x_7, x_3x_6, x_4x_5\}. \quad (12)$$

The cardinality of the code is 30.

Example 4.5: For $n = 8$, the CR code \mathcal{C}_0 of largest cardinality, which is associated with the group $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, is given by

$$x_1(0, 1) + x_2(0, 2) + x_3(1, 0) + x_4(1, 1) \\ + x_5(1, 2) + x_6(2, 0) + x_7(2, 1) + x_8(2, 2) = \pmod{3, 3}, \quad (13)$$

where $x_i \in \{0, 1\}$. Then one can use the pairing

$$\{x_1x_2, x_3x_6, x_4x_8, x_5x_7\}. \quad (14)$$

The cardinality of the code is 32, which is however nonlinear. The image of this code under \mathfrak{S}^8 is a linear code $[4, 2, 3]_3$, which is the one given in Example 2.5.

Example 4.6: Consider $n = 10$. For the VT code \mathcal{V}_0 is then given by

$$\sum_{i=1}^{10} ix_i = 0 \pmod{11}, \quad (15)$$

where $x_i \in \{0, 1\}$. Then one can use the pairing

$$\{x_1x_{10}, x_2x_9, x_3x_8, x_4x_7, x_5x_6\}. \quad (16)$$

The cardinality of the code is 94, and the image of this code under \mathfrak{S}^{10} is equivalent to a cyclic ternary code with $m = 5$. Note that there exists a 1-code $(10, 98)$ which is obtained from a cyclic ternary code (see Sec. III).

Now we consider the case of odd length.

Definition 4.7: A binary code \mathcal{C} of odd length $n = 2m + 1$ is called *generalized ternary* if $\mathfrak{S}^m(\tilde{\mathfrak{S}}^m(\mathcal{C})) = \mathcal{C}$, where $\tilde{\mathfrak{S}}^m$ acts on the last $2m$ coordinates of \mathcal{C} .

Based on this definition, if a binary code \mathcal{C} of odd length $2m + 1$ is generalized ternary, then it can be constructed from some single-error-correcting code for the channel $\mathcal{Z} \times \mathcal{T}^m$ via the map \mathfrak{S} .

Theorem 4.8: For n odd, the VT code \mathcal{V}_g is generalized ternary for any g .

Proof: We only need to prove that there exists a pairing which leaves a single coordinate as a bit, such that for any codeword $v \in \mathcal{V}_g$, if v restricted to a chosen pair α is 00, then there exist another codeword $v' \in \mathcal{V}_g$ such that $v'|_\alpha = 11$ and $v'|_{\bar{\alpha}} = v|_{\bar{\alpha}}$.

For a VT code \mathcal{V}_g of odd length, choose the pairing $\{i, n + 1 - i\}_{i=1}^{n/2}$ and leave the coordinate $(n+1)/2$ as a bit. Then the above condition is satisfied. ■

We discuss an example.

Example 4.9: For $n = 7$, the VT code \mathcal{V}_0 is given by

$$\sum_{i=1}^7 ix_i = 0 \pmod{8}, \quad (17)$$

where $x_i \in \{0, 1\}$. Then one can use the pairing

$$\{x_1x_7, x_2x_6, x_3x_5\}, \quad (18)$$

and treat x_4 as a bit. The size of the code is 16, and it is equivalent to the code given in Example 2.10.

In Table IV, the cardinality of codes found by the (generalized) ternary method is compared to the size of the corresponding VT-CR codes. One can see that the (generalized) ternary construction indeed outperforms the VT-CR construction, in particular for larger n .

TABLE IV

SIZE OF 1-CODES FROM TERNARY CONSTRUCTION VIA NUMERICAL SEARCH, COMPARED TO CR CODES, CODES OBTAINED BY THE PARTITION METHOD, AND THE KNOWN BOUNDS FROM [9], [14], [18]. FOR ODD n , ‘CYCLIC TERNARY’ REFERS TO EXTENDED CYCLIC CODES.

n	CR	cyclic ternary	ternary	partition	known bounds
6	10	12	12	*	12
7	16	16	16	*	18
8	32	29	32	*	36
9	52	53	55	*	62
10	94	98	105	104 ^(a)	112–117
11	172	154	180	180 ^(b)	198–210
12	316	336	351	336 ^(b)	379–410
13	586	612	612	652 ^(b)	699–786
14	1096	1200	1200	1228 ^(b)	1273–1500
15	2048	2144	2144	2288 ^(b)	2288–2828
16	3856	3952	3952	4280 ^(b)	4280–5486

The column in Table IV labeled ‘partition’ is obtained from the partition method in Ref. [12]. The code (a) is found from the partition of constant weight codes of length 6 and asymmetric codes of length 4. Codes (b) are from Ref. [12]. For $n = 10, 11, 12$, the ternary construction yields codes of equal size or even more codewords compared to the partition method. However, the best codes are obtained by heuristic methods, which, e.g., give (10, 112) [14] and (12, 379) [15]. This is not surprising as both the ternary construction and the partition method assume some additional structure of the binary 1-codes.

V. NONBINARY ASYMMETRIC-ERROR-CORRECTING CODES

In this section, we consider the construction of 1-codes for nonbinary asymmetric channels. Recall that the characteristic properties of codes for this channel model are given by Definition 1.1 and Theorem 1.2. Our construction will again be based on concatenation, generalizing the map \mathcal{G}^m .

For a given q , choose the outer code as some code over the alphabet $A = \{0, 1, \dots, q-1\}$, which encodes to some inner codes $\{C_0, C_1, \dots, C_{q-1}\}$ via $i \mapsto C_i$. Now choose the q inner codes as the double-repetition code $C_0 = \{00, 11, \dots, (q-1)(q-1)\}$ and all its $q-1$ cosets $C_i = C_0 + (0i)$, i.e., we have the rule that $(0i) \in C_i$. It is straightforward to check that each C_i is a 1-code, i.e., has asymmetric distance 2. Note that a single asymmetric error will only drive transitions between i, j for $i = j \pm 1$. For instance, for $q = 3, 4, 5$, the induced channels $\mathcal{R}_3, \mathcal{R}_4, \mathcal{R}_5$ are shown in Fig. 2. In general, we will write the induced channel as \mathcal{R}_q for outer codes over the alphabet $A = \{0, 1, \dots, q-1\}$.

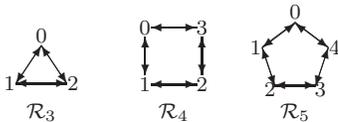


Fig. 2. The induced channel \mathcal{R}_3 for $q = 3$ (which is just the ternary symmetric channel), the induced channel \mathcal{R}_4 for $q = 4$, and the induced channel \mathcal{R}_5 for $q = 5$. The arrows indicate the possible transitions between symbols.

Similar to Theorems 2.6 and 2.9, we have the following

Theorem 5.1: For n even, an outer $(n/2, K)_q$ code correcting a single error for the channel \mathcal{R}_q leads to an $(n, q^{n/2}K)_q$

1-code \mathcal{C} , for $q > 2$. For n odd, an outer $((n+1)/2, K)_q$ code correcting a single error for the channel \mathcal{R}_q leads to an $(n, q^{(n-1)/2}K)_q$ 1-code \mathcal{C} , for $q > 2$.

If the outer code is linear, then our construction gives linear codes for the asymmetric channel. We state this result as a corollary below.

Corollary 5.2: An outer $[m, k]_q$ linear code correcting a single error for the channel \mathcal{R}_q leads to a $[2m, m+k]_q$ 1-code and a $[2m-1, m+k-1]_q$ 1-code, for $q > 2$.

It turns out that in many cases, our construction gives linear codes with larger cardinality than the distance-three symmetric codes of equal length. We first discuss the case of $q = 3$. In this case, \mathcal{R}_3 is the ternary symmetric channel, so we will just use outer codes of Hamming distance 3. We consider some examples.

Example 5.3: Consider $q = 3$ and take the outer code as $[3, 1, 3]_3$, with codewords $000, 111, 222$. This will give a $[5, 3]_3$ 1-code with codewords

$$\begin{array}{cccccc}
 00000, & 00011, & 00022, & 01100, & 01111, \\
 01122, & 02200, & 02211, & 02222, & \\
 10101, & 10112, & 10120, & 11201, & 11212, \\
 11220, & 12001, & 12012, & 12020, & \\
 21010, & 21021, & 21002, & 22110, & 22121, \\
 22102, & 20210, & 20221, & 20202, &
 \end{array} \tag{19}$$

while the best linear single-symmetric-error-correcting code is $[5, 2, 3]_3$. The $[3, 1, 3]_3$ outer code also yields a $[6, 4]_3$ 1-code, while the best linear single-symmetric-error-correcting code is $[6, 3, 3]_3$. Now take the outer code as $[4, 2, 3]_3$. This will give a $[7, 5]_3$ 1-code, while the best linear single-symmetric-error-correcting code is $[7, 4, 3]_3$. We can also construct a $[8, 6]_3$ 1-code, while the best linear single-symmetric-error-correcting code is $[8, 5, 3]_3$.

This example can be directly generalized to other lengths. Furthermore, the constructions extend trivially to $q > 3$, as any code of Hamming distance 3 corrects a single error for the channel \mathcal{R}_q . Note that Hamming codes over \mathbb{F}_q have length $n_r = (q^r - 1)/(q - 1)$. For a given n_r , our construction then allows to construct asymmetric 1-codes of all length $[n_r + 1, 2n_r]$ for n_r odd or all lengths $[n_r + 2, 2n_r]$ for n_r even. The sequence of lengths n_r is a geometric series, and hence our method can construct asymmetric codes for approximately $\frac{1}{q}$ of all lengths, outperforming the best single-symmetric-error-correcting linear codes.

Now consider the case $q > 3$ in more detail. The channel \mathcal{R}_q (see Fig. 2) is no longer a symmetric channel, so outer codes of Hamming distance 3 are no longer expected to give the best 1-codes. It turns out, however, that single-error-correcting codes for the channel \mathcal{R}_q are equivalent to single-symmetric-error correcting codes with respect to Lee metric [19] (see also [20]), for which optimal linear codes are known. When q is odd, let H be the parity check matrix whose columns are all vectors in \mathbb{Z}_q^r whose first non-zero element is in the $\{1, 2, \dots, \frac{q-1}{2}\}$ (where r is the number of rows in H), then the corresponding code can correct a single error for the channel \mathcal{R}_q .

We consider an example.

Example 5.4: For $q = 5$ consider the parity check matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 \\ 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 \end{pmatrix},$$

which gives a $[10, 8]_5$ code correcting a single error for the channel \mathcal{R}_5 , and hence a $[20, 18]_5$ 1-code. Note that the best linear single-symmetric-error-correcting code for $n = 20$ is $[20, 17, 3]_5$.

Our new linear codes for asymmetric channels for $q > 2$ show that Varshamov's argument that for the binary case, there is almost no hope to find good linear codes for the asymmetric channel, does not hold for the nonbinary case. There is indeed room for constructing good linear codes adapted to the asymmetric channel.

Note that contrary to the binary case, the nonlinear VT-CR codes can no longer be viewed as a special case of our construction. However, for lengths $n_r = q^r - 1$, our construction gives codes of the same cardinality as the VT-CR codes, while our codes are linear, but the VT-CR codes are not.

Finally, we briefly discuss the extension of our concatenation method to construct t -asymmetric-error-correcting codes for $t > 1$. We look at some examples.

Example 5.5: Consider the case of $q = 3$. Take the outer code as the $[5, 3]_3$ 1-code constructed in Example 5.3, which has asymmetric distance 2. Now take the encoding to the inner code as $0 \mapsto 00$, $1 \mapsto 11$, $2 \mapsto 22$. Then the concatenated code has asymmetric distance 4, which gives a $[10, 3]_3$ 3-code, while the best linear triple-error-correcting code is $[10, 2, 7]_3$. Similarly, take the outer code as the $[6, 4]_3$ 1-code, then the concatenated code is a $[12, 4]_3$ 3-code, while the best 3-error-correcting linear code is $[12, 3, 7]_3$.

VI. CODES FOR ASYMMETRIC LIMITED-MAGNITUDE ERRORS

In this section, we discuss the application of these nonbinary linear codes constructed in Sec. V to correct asymmetric limited-magnitude errors with wrap around. This new 'asymmetric limited-magnitude error' model, is introduced recently in [16], which models the asymmetric errors in multilevel flash memories in a more detailed manner. This model is parameterized by two integer parameters: \tilde{t} is the maximum number of symbol errors within a codeword, and ℓ the maximal magnitude of an error. The definition of asymmetric limited-magnitude errors is the following [16].

Definition 6.1: A vector of integers $\mathbf{e} = (e_1, \dots, e_i)$ is called a \tilde{t} asymmetric ℓ -limited-magnitude error word if $|\{i : e_i \neq 0\}| \leq \tilde{t}$, and for all i , $0 \leq e_i \leq \ell$.

Here by 'asymmetric' it still means that if any transmitted symbol a is received as $b \leq a$. For a codeword $\mathbf{x} \in A^n$, then a \tilde{t} asymmetric ℓ -limited-magnitude channel outputs a vector $\mathbf{y} \in A^n$ such that $\mathbf{y} = \mathbf{x} - \mathbf{e}$, where \mathbf{e} is a \tilde{t} asymmetric ℓ -limited-magnitude error word.

Coding problems for these channels have an intimate relation to coding problems for asymmetric channels. Indeed, when $t = \tilde{t}\ell$, any t -code for the asymmetric channel trivially corrects \tilde{t} asymmetric ℓ -limited-magnitude errors. Of course, the reverse is not true.

A generalization of Definition 6.1 is when we allow asymmetric errors to wrap around from 0 back to $q-1$. That is, we interpret '-' in $\mathbf{y} = \mathbf{x} - \mathbf{e}$ as subtraction mod q . This error model is then called the asymmetric ℓ -limited-magnitude channels with wrap around.

Similar as the asymmetric distance $\Delta(\mathbf{x}, \mathbf{y})$, we can define a distance d_ℓ for this error model, as below.

Definition 6.2: For $\mathbf{x}, \mathbf{y} \in A^n$, define $M(\mathbf{x}, \mathbf{y}) = |\{i : x_i > y_i\}|$. The distance d_ℓ between the words \mathbf{x}, \mathbf{y} is then defined as

$$d_\ell(\mathbf{x}, \mathbf{y}) = \begin{cases} n+1 & \text{if } \max_i \{|x_i - y_i|\} > \ell \\ \max\{M(\mathbf{x}, \mathbf{y}), M(\mathbf{y}, \mathbf{x})\} & \text{otherwise} \end{cases}$$

Similar as Theorem 1.2, the proposition below directly follows [16].

Proposition 6.3: A code \mathcal{C} corrects \tilde{t} asymmetric ℓ -limited-magnitude errors if and only if $d_\ell(\mathbf{x}, \mathbf{y}) \geq \tilde{t} + 1$ for all distinct $\mathbf{x}, \mathbf{y} \in \mathcal{C}$.

And one can readily interpret d_ℓ for asymmetric ℓ -limited-magnitude channels with wrap around (interpret '-' in as subtraction mod q), such that Proposition 6.3 still holds. Apparently, in general a t -code for the asymmetric channel can no longer be used to correct errors for asymmetric ℓ -limited-magnitude channel with wrap around. There is a sphere packing bound which naturally follows.

Theorem 6.4: [16] If \mathcal{C} is a \tilde{t} asymmetric ℓ -limited-magnitude (with wrap-around) error-correcting code, of length n over an alphabet of size q , then

$$|\mathcal{C}| \sum_{i=0}^{\tilde{t}} \binom{n}{i} \ell^i \leq q^n. \quad (20)$$

An asymmetric ℓ -limited-magnitude code is called perfect in a sense that it attains this sphere-packing bound.

Code designs for correcting asymmetric ℓ -limited-magnitude errors, with or without wrap around, are discussed in [16], [20]. Here we show that the linear codes constructed in Sec. V can be used to correct asymmetric ℓ -limited-magnitude errors and then further discuss their optimality using the sphere-packing bound.

Recall the construction in Sec. V, where for a given q , we choose the q inner codes C_0, C_1, \dots, C_{q-1} as $\{00, 11, \dots, (q-1)(q-1)\}$ and all its $q-1$ cosets. It is straightforward to check that each C_i has $d_\ell = 2$, for the asymmetric ℓ -limited-magnitude channel with wrap around, for $\ell = 1$, according to Definition 6.2. Indeed, this asymmetric ℓ -limited-magnitude channel with wrap around, for $\ell = 1$ has transitions

$$(q-1) \rightarrow (q-2) \rightarrow (q-3) \dots \rightarrow 1 \rightarrow 0 \rightarrow (q-1). \quad (21)$$

We illustrate these asymmetric 1-limited-magnitude channels \mathcal{L}_n for $n = 3, 4, 5$ bits in Fig. 3.

Now choose the outer code as some distance 3 code over the alphabet $A = \{0, 1, \dots, q-1\}$, which encodes to the inner codes $\{C_0, C_1, \dots, C_{q-1}\}$ via $i \rightarrow C_i$, then the following results readily hold according to Proposition 6.3.

Proposition 6.5: The codes based on the constructions given by Theorem 5.1 and Corollary 5.2 in Sec. V correct

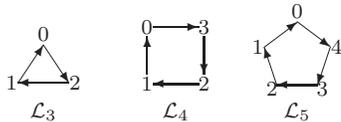


Fig. 3. The asymmetric 1-limited-magnitude channels \mathcal{L}_n for $n = 3, 4, 5$ bits. The arrows indicate the possible transitions between symbols.

a single asymmetric ℓ -limited-magnitude error with wrap around, for $\ell = 1$.

For $\ell = 1$, the sphere-packing bound of Eq. (20) for correcting a single error becomes

$$|\mathcal{C}| \leq \frac{q^n}{n+1}. \quad (22)$$

Recall that for a given n_r , the construction in Sec. V gives linear codes of all lengths $[n_r + 1, 2n_r]$ for n_r odd or all lengths $[n_r + 2, 2n_r]$ for n_r even, which outperform the best single-symmetric-error-correcting linear codes. Here $n_r = \frac{1}{q}(q^r - 1)$, and q is a prime power that \mathbb{F}_q is a field. The sphere-packing bound given in Eq. (22) then shows that all these linear codes are indeed optimal linear codes, for correcting a single asymmetric ℓ -limited-magnitude error with wrap around, for $\ell = 1$. For $n = q^r - 1$, we have perfect linear codes. As an example, the $[8, 6]_3$ code constructed in Example 5.3 is a perfect linear code. Note that perfect linear codes of length $n = q^r - 1$ for correcting a single asymmetric ℓ -limited-magnitude error with wrap around, for $\ell = 1$, are also obtained in [20], but from different constructions.

Indeed, those linear t -codes constructed in Sec. V can also be used to correct \tilde{t} asymmetric ℓ -limited-magnitude errors for $t = \tilde{t}\ell$. However, the sphere-packing bound no longer tells us whether these linear codes are optimal.

VII. DISCUSSION

We present new methods of constructing codes for asymmetric channels, based on modified code concatenation. Our methods apply to both binary and nonbinary case, for constructing both single- and multi-asymmetric-error-correcting codes.

For the binary case, our construction gives nonlinear 1-codes for the \mathcal{Z} channel, based on ternary outer codes. Some good 1-codes with structure, such as codes from ternary linear codes and ternary cyclic codes are constructed. We also show that the VT-CR code, which are the best known systematic construction of 1-codes, possess some nice structure while viewed in the (generalized) ternary construction, and they are suboptimal under the (generalized) ternary construction. Indeed, this ternary construction is originally inspired by constructing high performance quantum codes adapted to asymmetric channels, see [21].

For the nonbinary case, our construction gives linear 1-codes, which for many lengths outperforms the best single-symmetric-error-correcting codes of the same lengths. Our method can also be applied to construct good linear t -codes. To our knowledge, our method gives the first systematic construction of good linear codes for nonbinary asymmetric channels, which indicates that Varshamov's argument of no

good linear codes for asymmetric channels does not extend to the nonbinary case.

Our t -codes also apply to correct \tilde{t} asymmetric ℓ -limited-magnitude errors with wrap around, for $t = \tilde{t}\ell$. These channels model the errors in multilevel flash memory in a more detailed manner than Varshamov's asymmetric channel given in Definition 1.1. In case of $\ell = 1$, our single-error-correcting codes are shown to be optimal linear codes by the sphere-packing bound. For lengths $n = q^r - 1$, these codes are perfect linear codes.

We hope our methods shed light on further study of asymmetric codes, particularly, on systematic construction of these codes. These initial results on good linear t -codes with $t > 1$ and $q > 2$ are rather promising as they might find application in the context of flash memories.

REFERENCES

- [1] M. Grassl, P. Shor, G. Smith, J. Smolin, and B. Zeng, "New constructions of codes for asymmetric channels via concatenation," in *Proceedings of the 2012 IEEE International Symposium on Information Theory*, Cambridge, MA, Jul. 2012, pp. 751–755.
- [2] R. R. Varshamov, "Some Features of Linear Codes that Correct Asymmetric Errors," *Soviet Physics Doklady*, vol. 9, pp. 538–540, Jan. 1965.
- [3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland Publishing Company, 1977.
- [4] S. D. Constantin and T. R. M. Rao, "Concatenated group theoretic codes for binary asymmetric channels," *AFIPS Conf. Proc.*, vol. 46, pp. 837–842, 1979.
- [5] P. Cappelletti, C. Golla, P. Olivo, and E. Zanoni, *Flash Memories*. Boston: Kluwer Academic, 1999.
- [6] R. J. McEliece and E. R. Rodemich, "The Constantin-Rao construction for binary asymmetric error-correcting-codes," *Information and Control*, vol. 44, pp. 187–196, 1980.
- [7] T. Kløve, *Codes for error detection*. Singapore: World Scientific, 2007.
- [8] R. Varshamov, "A class of codes for asymmetric channels and a problem from the additive theory of numbers," *IEEE Transactions on Information Theory*, vol. 19, no. 1, pp. 92–95, 1973.
- [9] T. Kløve, "Error correcting codes for the asymmetric channel," *Report 18-09-07-81, Department of Informatics, University of Bergen*, 1981.
- [10] R. R. Varshamov and G. M. Tenengolts, "Correcting code for single asymmetric errors," *Avtomatika i Telemekhanika (in Russian)*, vol. 26, no. 2, pp. 228–292, 1965.
- [11] S. D. Constantin and T. R. M. Rao, "On the theory of binary asymmetric error correcting codes," *Information and Control*, vol. 40, pp. 20–36, 1979.
- [12] T. Etzion, "New lower bounds for asymmetric and unidirectional codes," *IEEE Transactions on Information Theory*, vol. 37, no. 6, pp. 1696–1704, 1991.
- [13] B. Al-Bassam, "New single asymmetric error-correcting codes," *IEEE Transactions on Information Theory*, vol. 43, no. 5, pp. 1619–1623, 1997.
- [14] T. Etzion and P. R. J. Östergård, "Greedy and heuristic algorithms for codes and colorings," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 382–338, 1998.
- [15] V. P. Shilo, "New lower bounds of the size of error-correcting codes for the \mathcal{Z} -channel," *Cybernetics and Systems Analysis*, vol. 38, no. 1, pp. 13–16, 2002.
- [16] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, "Codes for asymmetric limited-magnitude errors with application to multilevel flash memories," *IEEE Transactions on Information Theory*, vol. 56, no. 4, pp. 1582–1595, 2010.
- [17] I. Dumer, "Concatenated codes and their multilevel generalizations," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam: Elsevier Science, 1998, pp. 1911–1988.
- [18] N. J. A. Sloane, "Challenge problems: Independent sets in graphs," <http://www2.research.att.com/~njas/doc/graphs.html>, accessed on 2012-02-02.
- [19] E. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

- [20] T. Kløve, B. Bose, and N. Elarief, "Systematic, single limited magnitude error correcting codes for flash memories," *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4477–4487, 2011.
- [21] P. W. Shor, G. Smith, J. A. Smolin, and B. Zeng, "High performance single-error-correcting quantum codes for amplitude damping," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 7180–7188, 2011.