Discrete Mathematics 112 (1993) 245–248
North-Holland

Communication

On the concatenated structures of a [49, 18, 12] binary abelian code

Hervé Chabanne and Nicolas Sendrier

INRIA, projet CODES, Domaine de Voluceau, Rocquencourt, B.P. 105, 78153 Le Chesnay Cedex, France

Communicated by P. Camion
Received 14 October 1992

Abstract

Chabanne, H. and N. Sendrier, On the concatenated structures of a [49, 18, 12] binary abelian code, Discrete Mathematics 112 (1993) 245–248.

We here introduce a new formalism for describing concatenated codes. Using this formalism, we show how any generalized concatenated code can be viewed as a first order concatenated code. Finally, we give an illustrative example: using Jensen's result (1985) which shows that any abelian code has a generalized concatenated structure, we first give the representation of the [49, 18, 12] abelian code introduced by Camion (1971) as a second order concatenated code; then using our description, we show that this code is also equal to the first order concatenation of two linear cyclic codes.

1. Definition of generalized concatenated codes

We will recall here the definition of a generalized concatenated code [1, 4]. We denote by $\mathscr{A}(K;\, n, M, d)$ or $\mathscr{B}(K;\, n, M, d)$ a code over the alphabet K of length n, cardinality M and minimum distance d.

Given s codes $\mathscr{A}^{(i)}(k_a^{(i)}; n_a, M_a^{(i)}, d_a^{(i)})$ we first construct all the matrices

$$\begin{pmatrix} a_1^{(1)} & \cdots & a_1^{(s)} \\ \vdots & \ddots & \vdots \\ a_{n_a}^{(1)} & \cdots & a_{n_a}^{(s)} \end{pmatrix}$$

Correspondence to: Hervé Chabanne, INRIA, projet CODES, Domaine de Voluceau, Rocquencourt, B.P. 105, 78153 Le Chesnay Cedex, France.

where the ith column

$$\begin{pmatrix} a_1^{(i)} \\ \vdots \\ a_{n_a}^{(i)} \end{pmatrix}$$

is a codeword of $\mathscr{A}^{(i)}, i=1,\ldots,s$.

An sth order partition of a code $\mathscr{B}^{(1)}(k_b; n_b, M_b^{(1)}, d_b^{(1)})$ is an iteration of partitions

$$\mathscr{B}^{(1)} = \bigcup_{i_1=1}^{|k_a^{(1)}|} \mathscr{B}_{i_1}^{(2)}, \quad \forall i_1, \qquad \mathscr{B}_{i_1}^{(2)} = \bigcup_{i_2=1}^{|k_a^{(2)}|} \mathscr{B}_{i_1,i_2}^{(3)}, \ldots, \quad \forall i_1,\ldots,i_{s-2},$$

$$\mathscr{B}_{i_1,\ldots,i_{s-2}}^{(s-1)} = \bigcup_{i_{s-1}=1}^{|k_a^{(s-1)}|} \mathscr{B}_{i_1,\ldots,i_{s-1}}^{(s)},$$

with, for all $i_1,\ldots,i_{s-1}, |\mathscr{B}_{i_1,\ldots,i_{s-1}}^{(s)}| = |k_a^{(s)}|$, in such a way that if we number the elements $a^{(i)} \in k_a^{(i)}, i=1,\ldots,s$ then any vector $(a^{(1)},\ldots,a^{(s)})$ determines a unique codeword in $\mathscr{B}^{(1)} - a^{(1)}$ enumerates the subcodes of $\mathscr{B}^{(1)},\ldots,a^{(s-1)}$ enumerates the subcodes of $\mathscr{B}_{i_1,\ldots,i_{s-2}}^{(s-1)}$; and finally, $a^{(s)}$ determines a codeword in $\mathscr{B}_{i_1,\ldots,i_{s-1}}^{(s)}$.

Any row $(a_j^{(1)},\ldots,a_j^{(s)})$ of the matrix above determines a unique codeword $(c_{j,1},\ldots,c_{j,n_b})$ in $\mathscr{B}^{(1)}$ according to a given suitable sth order partition. And the Generalized Concatenated (GC) code of outers codes $\mathscr{A}^{(i)}$ and inner code $\mathscr{B}^{(1)}$ with the above sth order partition consists of all the following $n_a \times n_b$ matrices:

$$\begin{pmatrix} c_{1,1} & \cdots & c_{1,n_b} \\ \vdots & \ddots & \vdots \\ c_{n_a,1} & \cdots & c_{n_a,n_b} \end{pmatrix}$$

Note that when $s=1$ this definition of GC code reduces to the usual definition of concatenated code. For this reason, we will call the code obtained by substituting any symbol of a word of $\mathscr{A}^{(1)}$ with a word of $\mathscr{B}^{(1)}$ a *first order concatenated code* and denote it by $\mathscr{A}^{(1)} \square \mathscr{B}^{(1)}$.

We introduce now a new formalism using mapping rather than partition. This give us an equivalent definition of GC codes that suits our purposes.

Remark 1. The knowledge of $\mathscr{B}^{(1)} \subset k_b^{n_b}$ and its sth order partition suitable to the outer codes $\mathscr{A}^{(i)}(k_a^{(i)}; n_a, M_a^{(i)}, d_a^{(i)})$, $1 \leqslant i \leqslant s$ is equivalent to the knowledge of a bijection θ between the product of the alphabets $k_a^{(1)} \times \cdots \times k_a^{(s)}$ and the inner code $\mathscr{B}^{(1)}$. If we denote by Θ the mapping

$$\Theta: \mathscr{A}^{(1)} \times \cdots \times \mathscr{A}^{(s)} \to \mathscr{B}^{(1)n_a} \subset k_b^{n_a n_b}$$

$$\left(\begin{pmatrix} a_1^{(1)} \\ \vdots \\ a_{n_a}^{(1)} \end{pmatrix}, \ldots, \begin{pmatrix} a_1^{(s)} \\ \vdots \\ a_{n_a}^{(s)} \end{pmatrix} \right) \mapsto \begin{pmatrix} \theta(a_1^{(1)},\ldots,a_1^{(s)}) \\ \vdots \\ \theta(a_{n_a}^{(1)},\ldots,a_{n_a}^{(s)}) \end{pmatrix}$$

then the GC code of $\mathscr{A}^{(i)}$, $1 \leqslant i \leqslant s$ and θ is equal to $\Theta(\mathscr{A}^{(1)} \times \cdots \times \mathscr{A}^{(s)})$.

For instance, a first order concatenated code is entirely defined by the knowledge of its outer code, its inner code and a bijection between the alphabet of the outer code and the inner code. Thus the usual notation $A \,\square\, B$ may be ambiguous if the bijection is not clearly defined.

This leads us to the the following remark which states that GC codes are a sub-class of first order concatenated codes. In other words, GC codes are a specialization rather than a generalization of concatenated codes.

Remark 2. Any generalized concatenated code can be viewed as a first order concatenated code.

This can be justified as follows. Let $\mathscr{C}$ be the sth order GC code with outer codes $\mathscr{A}^{(i)}(k_a^{(i)}; n_a, M_a^{(i)}, d_a^{(i)})$, $1 \leqslant i \leqslant s$ and inner code $\mathscr{B}^{(1)}$ partitioned in a way suitable to the outer codes. Let θ and Θ be the mappings defined in the first remark. Thus $\mathscr{C} = \Theta(\mathscr{A}^{(1)} \times \cdots \times \mathscr{A}^{(s)})$.

Let K be an alphabet of size $|K| = \prod_{i=1}^{s} |k_a^{(i)}|$, and let φ be a bijective mapping between $k_a^{(1)} \times \cdots \times k_a^{(s)}$ and K. Using φ, we build the mapping

$$\Phi:\ \mathscr{A}^{(1)} \times \cdots \times \mathscr{A}^{(s)} \to K^{n_a}$$

$$\left(\begin{pmatrix} a_1^{(1)} \\ \vdots \\ a_{n_a}^{(1)} \end{pmatrix}, \ldots, \begin{pmatrix} a_1^{(s)} \\ \vdots \\ a_{n_a}^{(s)} \end{pmatrix} \right) \mapsto \begin{pmatrix} \varphi(a_1^{(1)}, \ldots, a_1^{(s)}) \\ \vdots \\ \varphi(a_{n_a}^{(1)}, \ldots, a_{n_a}^{(s)}) \end{pmatrix} \tag{1}$$

Let $\mathscr{A} = \Phi(\mathscr{A}^{(1)} \times \cdots \times \mathscr{A}^{(s)})$. Then $\mathscr{A}$ is a code of length n_a over K.

Let's consider the first order concatenated code of $\mathscr{A}$ and $\mathscr{B}^{(1)}$ with the bijection $\theta \circ \varphi^{-1}$ from K to $\mathscr{B}^{(1)}$. We have $\mathscr{A} \,\square\, \mathscr{B}^{(1)} = \Theta \circ \Phi^{-1}(\mathscr{A}^{(1)} \times \cdots \times \mathscr{A}^{(s)}) = \mathscr{C}$.

2. First order concatenated structure of a [49, 18, 12] binary abelian code

In [2] Camion exhibits a [49, 18, 12] binary abelian code which is not equivalent to any product code. The set of its nonzeroes is

$$\{(\alpha,\alpha^6), (\alpha^2,\alpha^5), (\alpha^4,\alpha^3), (\alpha,\alpha^3), (\alpha^2,\alpha^6), (\alpha^4,\alpha^5), (\alpha,\alpha^5), (\alpha^2,\alpha^3), (\alpha^4,\alpha^6),$$
$$(\alpha^6,\alpha), (\alpha^5,\alpha^2), (\alpha^3,\alpha^4), (\alpha^3,\alpha), (\alpha^6,\alpha^2), (\alpha^5,\alpha^4), (\alpha^5,\alpha), (\alpha^3,\alpha^2), (\alpha^6,\alpha^4)\}$$

where α is a primitive seventh root of unity over $\mathbb{F}_2$ which satisfies $\alpha^3 + \alpha + 1 = 0$.

Using Jensen's factorisation of any abelian code as a GC code [3] we can describe Camion's code as a second order GC code:

- the two outer codes are both the cyclic code of length 7 over $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ whose nonzeroes are $\{\alpha^3, \alpha^5, \alpha^6\}$,
- the inner code $\mathscr{B}^{(1)}(\mathbb{F}_2;\ 7, 64, 2)$ is the even weight code,
- to partition $\mathscr{B}^{(1)}$ we use the simplex code $\mathscr{B}^{(2)}(\mathbb{F}_2;\ 7, 8, 4)$ of nonzeroes $\{\alpha^3, \alpha^5, \alpha^6\}$: $\mathscr{B}^{(1)} = \bigcup_{i=1}^{8} \mathscr{B}_i^{(2)}$ where the $\mathscr{B}_i^{(2)}$ are the eight cosets of $\mathscr{B}^{(2)}$ composing $\mathscr{B}^{(1)}$.

Note that the outer codes were defined by Jensen in a slightly different way: the first outer code was the cyclic code of length 7 over $\mathbb{F}_2(\alpha)$ with nonzeroes $\{\alpha^3, \alpha^5, \alpha^6\}$ and the second, the cyclic code of same length, but over $\mathbb{F}_2(\alpha^3)$ and with nonzeroes $\{\alpha, \alpha^2, \alpha^4\}$.

Now, let $\mathbb{F}_{16} = \mathbb{F}_8[X]/(X^2 + X + 1)$ and let φ be the $\mathbb{F}_8$-vector space isormorphism between $\mathbb{F}_8 \times \mathbb{F}_8$ and $\mathbb{F}_{16}$ defined by $\varphi(f_1, f_2) = f_1 + X f_2$. Let Φ be the mapping and $\mathscr{A}$ be the code defined from φ and the outer codes as previously in (1). Then $\mathscr{A}$ is the cyclic code of length 7 over $\mathbb{F}_{16}$ whose nonzeroes are $\{\alpha^3, \alpha^5, \alpha^6\}$. And Camion's code can also be viewed as the first order concatenated code of $\mathscr{A}$ and $\mathscr{B}^{(1)}$.

Note that from Remark 2 a similar result holds for any GC code, but in general the unique outer code of the first order concatenated structure is not linear.

Acknowledgement

The authors wish to thank Thomas Ericson for some helpful advice.

References

[1] M. Bossert, Decoding of generalized concatenated codes, in: T. Mora, ed., AAECC-6, number 357 in LNCS (Springer, Berlin 1988) 89–98.

[2] P. Camion, Abelian codes, Technical Summary Report 1059, MRC, University of Wisconsin, December 1971.

[3] J.M. Jensen, The concatenated structure of cyclic and abelian codes, IEEE Trans. Inform. Theory 31 (1985) 783–793.

[4] V. Zinoviev, Generalized concatenated codes, Problemy Peredachi Informatsii 12 (1976) 5–15.