The concept of synthesis of LDPC and Polar Codes on the basis of Face-Splitting product of matrices

Vadym Slyusar

January 3, 2021

Vadym Slyusar

The concept of synthesis of LDPC and Polar Codes on the basis of Face-Splitting product of matrices.

A feature of the 5G NR cellular communication standard is the use of LDPC codes for data transmission [1, 2], which have proven their effectiveness in comparison with turbo codes. However, such a choice does not mean that the problem of data coding is finally solved. The beginning of work on 6G cellular technologies has stimulated the search for new solutions aimed at improving the known approaches to data encoding. In addition to the development of LDPC methods, this is confirmed by the ongoing studies of polar codes [3], which at one time were considered as an alternative to LDPC when developing the 5G NR standard.

As known, describing the idea of synthesizing LDPC codes of large dimension, their author Gallagher [1] proposed to form an initial check matrix of small dimension with subsequent increase in its format by repeating the original matrix in combination with permutation of rows and columns for the elimination of repetitive cycles.

In this regard, it is proposed to improve the Gallager approach by forming high-dimensional checking and generating matrices based on the face-splitting product of their original versions [4 - 6]. This method is a more general case of the technique used by Gallagher, which consists in replicating the same check matrix. In this case, the Gallager version is obtained by row-by-row multiplication on the left of the matrix of ones by the original check matrix with the same number of rows, taking into account that the number of columns in the matrix of ones is equal to the required number of repetitions of the check matrix:

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \square \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} = \left[\begin{array}{cccccc:cccccc:cccccc} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{array}\right],$$

where □ – symbol of face-splitting matrix product.

On the other hand, it should also be noted that the transition to the face-splitting product is a development of the idea of splitting the check matrix by rows used in [2], since a similar concept lies at the heart of the face-splitting product, in which matrix decomposition is performed row by row.

In the context of the proposed approach, the orthogonality property of face-splitting products is essential. Its essence is that if the product of two sparse matrices A and B with elements 0 and 1 is orthogonal modulo 2, that is, AB = 0 (mod 2), then the results of multiplication modulo 2 of multiple face-splitting products of these matrices will be orthogonal as well, that is:

$$(A\square A\square A\square\ldots\square A)(B\square B\square B\square\ldots\square B)=0 \pmod 2. \tag{1}$$

As applied to LDPC codes, as an example confirming the validity of this property, we can consider checking the orthogonality of the generating matrix G and the transposed parity check matrix H:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix},\ H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix},\ GH^T = \begin{bmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{bmatrix} \underset{(\mathrm{mod}\,2)}{=} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

$$(G\square G\square G)(H\square H\square H)^T = \begin{bmatrix} 8 & 8 & 8 \\ 8 & 8 & 8 \\ 8 & 8 & 8 \end{bmatrix} \underset{(\mathrm{mod}\,2)}{=} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

The same property holds for products of matrices and vectors, that is, in the case of orthogonality of the matrix H and the vector c (Hc = 0 (mod 2)), it will be true:

$$(H\square H\square H\square\ldots\square H)(c^T\square c^T\square c^T\square\ldots\square c^T)^T=0 \pmod 2. \tag{2}$$

In general, for LDCP, a combination of M different parity check matrices with the same number of rows and the corresponding codes is possible:

$$(H_1\square\, H_2\square H_3\square\ldots\square H_M)(c_1^T\square c_2^T\square c_3^T\square\ldots\square c_M^T)^T=0 \ (\mathrm{mod}\ 2). \qquad (3)$$

As an example, consider the parity check matrices and code sequences used in the LDPC literature:

$$H_1=\begin{bmatrix}1&1&1&1&0&0\\0&0&1&1&0&1\\1&0&0&1&1&0\end{bmatrix},\ c_1^T=[1\ 0\ 1\ 0\ 1\ 1], \qquad (4)$$

$$H_2=\begin{bmatrix}1&0&1&0&1&0\\0&1&0&1&0&1\\1&1&0&0&0&1\end{bmatrix},\ c_2^T=[0\ 1\ 0\ 0\ 0\ 1]. \qquad (5)$$

Let's form a new parity check matrix by the face-splitting product:

$$H=H_1\square H_2, \qquad (6)$$

and the corresponding new vector of code:

$$c=(c_1^T\square c_2^T)^T.$$

As a result of multiplying the matrix H by the vector c, we get:

$$Hc=\begin{bmatrix}0\\4\\4\end{bmatrix}\underset{(\mathrm{mod}\,2)}{=}\begin{bmatrix}0\\0\\0\end{bmatrix}, \qquad (7)$$

that is, their multiplication modulo 2 generates a zero vector, which is an indicator of orthogonally.

Since the result of transposition of the face-splitting product of vectors in (2) coincides with their Kronecker product [5], this expression can be rewritten as:

$$(H\square H\square H\square\ldots\square H)(c^T\square c^T\square c^T\square\ldots\square c^T)^T = (H\square H\square H\square\ldots\square H)(c\otimes c\otimes c\otimes\ldots\otimes c)=$$
$$=(Hc)\circ(Hc)\circ(Hc)\circ\ldots\circ(Hc) = (Hc)^n=0 \ (\mathrm{mod}\ 2), \qquad (8)$$

where □ is the symbol of the Kronecker product, ○ is the symbol of the Hadamard element-wise product.

Similarly, for expression (3) we get:

$$(H_1\square\, H_2\square H_3\square\ldots\square H_M)(c_1^T\square c_2^T\square c_3^T\square\ldots\square c_M^T)^T=$$
$$=(H_1\square\, H_2\square H_3\square\ldots\square H_M)(c_1\otimes c_2\otimes c_3\otimes\ldots\otimes c_M)=(H_1c_1)\circ(H_2c_2)\circ(H_3c_3)\circ\ldots\circ(H_4c_M). \qquad (9)$$

Thus, the result of multiplying the face-splitting product of parity-check matrices by the face-splittung product of code vectors is split into a multiple Hadamard product. This makes it possible to replace the orthogonality check of high-dimensional matrices and corresponding codes with the parallel execution of several such tests with low-dimension matrices and vectors. On the other hand, it follows from expression (9) that for the orthogonality of the resulting parity check matrix and the code sequence obtained with the face-splitting products, it is necessary and sufficient to have only one orthogonal pair of initial combinations of the parity check matrix and the vector code. This means that if the parity check is not taken into account, then increasing the length of the parity matrix significantly expands the set of codes orthogonal to it. In other words, a single code vector may not be suitable for every parity check matrix, but if at least one of the code vectors is orthogonal for the entire set of parity check matrices, then the resulting face-splitting products will be orthogonal. In addition, if you use the same check matrix as factors in the multiple face-splitting product, then in the face-splitting product of the row vectors it is sufficient to use only one vector orthogonal with the original check matrix, while the other vectors can be arbitrary.

A relation similar to (9) can also be obtained in the case of orthogonality of the face-splitting products formed by a set of arbitrary generating matrices and the transposed face-splitting product of the set of parity check matrices.

$$(G_1\square\, G_2\square G_3\square\ldots\square G_M)(H_1\square H_2\square H_3\square\ldots\square H_M)^T=$$

$=(G_1 \square G_2 \square G_3 \square \ldots \square G_M)(H_1^T \blacksquare H_2^T \blacksquare H_3^T \blacksquare \ldots \blacksquare H_M^T)=G_1H_1^T \circ G_2H_2^T \circ G_3H_3^T \circ \ldots \circ G_MH_M^T$,
where $\blacksquare$ – symbol of Khatry-Rao product [4 - 6].

The key here is the property of the face-splitting product [5]:

$$(A \square B)(A^T \blacksquare B^T)= AA^T \circ BB^T.$$

In the examples considered, the transition to the face-splitting product was accompanied by the destructuring of the resulting generating matrix. In cases where the preservation of its structuredness is a prerequisite, the synthesis of the generating and corresponding check matrices can be performed according to the expressions:

$$G=[\ \mathbf{1} \mid P_1 \square P_2 \square P_3 \square \ldots \square P_M];\ H=[(P_1 \square P_2 \square P_3 \square \ldots \square P_M)^{\mathbf{T}} \mid \mathbf{1_H}\ ],$$

where $\mathbf{1}$ and $\mathbf{1_H}$ are identity matrices of the corresponding dimension, P_m is the matrix of codes.

As for polar codes, their feature in the synthesis of high-dimensional codes is the use of a multiple Kronecker product of polarization coding matrices F [3] to generate generating matrices G:

$$G=B(F\otimes F\otimes F\otimes \ldots \otimes F),$$

where B is a permutation matrix.

In this regard, it is proposed to modify this approach by completely or partially replacing the Kronecker product of the polarization matrices with their face-splitting product, for example:

$$G=B(F\square F\square F\square \ldots \square F) \text{ или } G=B((F\otimes F)\square(F\otimes F)\square \ldots \square(F\otimes F)) \text{ etc.}$$

In addition, it is possible to use a multiple face-splitting product for building the generating matrix G_N of several initial generating matrices G formed by the method traditional for polar codes:

$$G_N= G\square G\square G\square \ldots \square G.$$

This solution will reduce the amount of computational costs in the synthesis of code sequences and their processing at the reception, in comparison with the usual use of the Kronecker multiplication operation. As a consequence, with the face-splitting product, a new coding paradigm can be constructed using a combined approach based on LDPC and polar codes.

References

1. R. G. Gallager. Low density parity-check codes. // IRE Trans. Inf. Theory, vol. 8, no. 1, pp. 21-28, Jan. 1962. - DOI: 10.1109/TIT.1962.1057683.

2. Yu Kou, Shu Lin, and Marc P. C. Low-Density Parity-Check Codes Based on Finite Geometries: A Rediscovery and New Results.// IEEE transactions on information theory, Vol. 47, No. 7, November 2001. – Pp. 2711 – 2736.

3. E. Arıkan. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels.// IEEETrans. Inf. Theory, vol. 55, no. 7, pp. 3051 – 3073, Jul. 2009.

4. Slyusar, V. I. End products in matrices in radar applications// Radioelectronics and Communications Systems.– 1998, Vol. 41; Number 3, pages 50 - 53.

5. Slyusar, V. I. A Family of Face Products of Matrices and its Properties// Cybernetics and Systems Analysis c/c of Kibernetika i Sistemnyi Analiz. – 1999, Vol. 35; Part 3, pages 379 - 384. - DOI: 10.1007/BF02733426.

6. Osnovy voenno-tehniceskih issledovanij. Teoria i prilozenia. Tom 2. Sintez sredstv informacionnogo obespecenia vooruzenia i voennoj tehniki. (Eng.: Fundamentals of military-technical research. Theory and applications. Tom. 2. Synthesis of means of information support of weapons and military equipment.) / A.I. Minochkin, V.I. Rudakov, V.I. Slyusar. – Kiev: Granmna, 2012. – Pp. 7 – 98; 354 – 521. (In Russian).