СИНТЕЗ LDPC И ПОЛЯРНЫХ КОДОВ НА ОСНОВЕ ТОРЦЕВОГО ПРОИЗВЕДЕНИЯ МАТРИЦ.

Слюсар В.И.
Центральный научно-исследовательский институт вооружения и военной техники Вооруженных Сил Украины, д.т.н., профессор, ORCID 0000-0002-2912-3149

Особенностью стандарта сотовой связи 5G NR является применение для передачи данных кодов LDPC [1, 2], доказавших свою эффективность по сравнению с турбо-кодами. Вместе с тем, такой выбор не означает, что проблема кодирования данных окончательно решена. Начало работ над технологиями сотовой связи 6G стимулировало поиск новых решений, направленных на совершенствование известных подходов к кодированию данных. Подтверждением тому, помимо развития методов LDPC, являются продолжающиеся исследования полярных кодов [3], которые в свое время рассматривались как альтернатива LDPC при разработке стандарта 5G NR.

Как известно, описывая идею синтеза LDPC кодов большой размерности, их автор Галлагер [1] предложил формировать исходную проверочную матрицу небольшой размерности с последующим увеличением её формата путем повтора исходной матрицы в сочетании с перестановкой строк и столбцов для исключения повторяющихся циклов.

В этой связи, предлагается усовершенствовать подход Галлагера путем формирования проверочных и генерирующих матриц большой размерности на основе торцевого произведения их исходных вариантов [4 - 6]. Такой метод является более общим случаем использованного Галлагером приема, состоящего в тиражировании одной и той же проверочной матрицы. При этом вариант Галлагера получается путем торцевого умножения слева матрицы единиц на исходную проверочную матрицу с тем же количеством строк, с учетом того, что количество столбцов в матрице единиц равняется требуемому количеству повторений проверочной матрицы:

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

где $\square$ – символ торцевого произведения матриц.

С другой стороны следует также отметить, что переход к торцевому произведению является развитием использованной в [2] идеи расщепления проверочной матрицы по строкам, поскольку аналогичная концепция лежит и в основе торцевого произведения, в котором декомпозиция матриц осуществляется построчно.

В контексте предлагаемого подхода существенным является свойство ортогональности торцевых произведений. Суть его стоит в том, что, если произведение двух разреженных матриц A и B с элементами 0 и 1 является ортогональным по модулю 2, то есть AB=0 (mod 2), то ортогональным будет и результат умножения по модулю 2 кратных торцевых произведений этих матриц, то есть:

$$(A\square A\square A\square\ldots\square A)(B\square B\square B\square\ldots\square B)=0 \pmod 2. \qquad (1)$$

Применительно к LDPC кодам в качестве примера, подтверждающего справедливость данного свойства, можно рассмотреть проверку ортогональности генерирующей матрицы G и транспонированной проверочной матрицы H:

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

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

Это же свойство выполняется для произведений матриц и векторов, то есть в случае ортогональности матрицы H и вектора c (Hc=0 (mod 2)) будет справедливо:

$$(H\square H\square H\square\ldots\square H)(c^T\square c^T\square c^T\square\ldots\square c^T)^T=0 \pmod 2. \quad (2)$$

В общем случае для LDCP возможна комбинация M разных проверочных матриц с одинаковым количеством строк и соответствующих им кодов:

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

В качестве примера рассмотрим проверочные матрицы и кодовые последовательности, используемые в литературе по LDPC:

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

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

Сформируем новую проверочную матрицу путем торцевого произведения:

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

и соответствующий ей новый вектор кода:

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

В результате умножения матрицы H на вектор c получим:

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

то есть их перемножение по модулю 2 порождает нулевой вектор, что является индикатором ортогональности.

Поскольку результат транспонирования торцевого произведения векторов в (2) совпадает с их кронекеровским произведением [5], данное выражение можно переписать в виде:

$$(H\square H\square H\square\ldots\square H)(c^T\square c^T\square c^T\square\ldots\square c^T)^T = (H\square H\square H\square\ldots\square H)(c\otimes c\otimes c\otimes\ldots\otimes c)=$$
$$=(Hc)\circ(Hc)\circ(Hc)\circ\ldots\circ(Hc) = (Hc)^n=0 \pmod 2, \quad (8)$$

где $\otimes$ - символ кронекеровского произведения, $\circ$ – символ поэлементного произведения Адамара.

Аналогично, для выражения (3) получим:

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

Таким образом, результат умножения торцевого произведения проверочных матриц на торцевое произведение кодовых векторов расщепляется на кратное произведение Адамара. Это позволяет заменить проверку ортогональности матриц большой размерности и соответствующих кодов на параллельное выполнение нескольких таких тестов с матрицами и векторами малой размерности. С другой стороны, из выражения (9) следует, что для ортогональности результирующей проверочной матрицы и кодовой последовательности, полученной с помощью торцевых произведений, необходимо и достаточно наличие лишь одной ортогональной пары исходных комбинаций проверочной матрицы и векторного кода. Это означает, что если не принимать во внимание проверку на четность, то увеличение длины проверочной матрицы существенно расширяет множество кодов, ей ортогональных. Другими словами, отдельно взятый кодовый вектор может подходить не каждой проверочной матрице, но, если для всей совокупности проверочных матриц ортогональным является хотя бы один из кодовых векторов, то результирующие торцевые произведения будут ортогональны. Кроме того, если использовать в кратном торцевом произведении одну и ту же проверочную матрицу в качестве сомножителей, то в торцевом произведении вектор-строк достаточно задействовать только один вектор, ортогональный с исходной поверочной матрицей, тогда как остальные векторы могут быть произвольными.

Соотношение, аналогичное (9), можно получить и в случае ортогональности торцевых произведений, образованных совокупностью произвольных генерирующих матриц и транспонированным торцевым произведением множества проверочных матриц.

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

$$=(G_1 \square G_2 \square G_3 \square \ldots \square G_M)(H_1^T \blacksquare H_2^T \blacksquare H_3^T \blacksquare \ldots \blacksquare H_M^T)=G_1H_1^T \circ G_2H_2^T \circ G_3H_3^T \circ \ldots \circ G_MH_M^T,$$

где $\blacksquare$ - символ произведения Хатри-Рао [4 - 6].

Ключевым при этом является свойство торцевого произведения [5]:

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

В рассмотренных примерах переход к торцевому произведению сопровождался деструктуризацией результирующей генерирующей матрицы. В тех случаях, когда сохранение её структурованности является обязательным условием, синтез генерирующей и соответствующей ей проверочной матриц может выполняться согласно выражениям:

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

где $\mathbf{1}$ и $\mathbf{1_H}$ – единичные матрицы соответствующей размерности, P_m – матрица кодов.

Что касается полярных кодов, то их особенностью при синтезе кодов большой размерности является применение для формирования генерирующих матриц G кратного кронекеровского произведения поляризационных матриц кодирования F [3]:

$$G=B(F\otimes F\otimes F\otimes \ldots \otimes F),$$ где B – перестановочная матрица.

В этой связи предлагается модифицировать данный подход путем полной либо частичной замены кронекеровского произведения поляризационных матриц их торцевым произведением, например: $G=B(F\square F\square F\square \ldots \square F)$ или $G=B((F\otimes F)\square(F\otimes F)\square \ldots \square(F\otimes F))$ и т.п.

Кроме того, возможно применение для формирования генерирующей матрицы G_N кратного торцевого произведения нескольких исходных генерирующих матриц G, сформированных традиционным для полярных кодов методом: $G_N= G\square G\square G\square \ldots \square G$.

Такое решение позволит сократить объем вычислительных затрат при синтезе кодовых последовательностей и их обработке на приёме, по сравнению с привычным использованием операции кронекеровского умножения. Как следствие, с помощью торцевого произведения может быть построена новая парадигма кодирования с использованием комбинированного подхода на основе кодов LDPC и полярных кодов.

Список литературы

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. Слюсар В.И. Торцевые произведения матриц в радиолокационных приложениях// Изв. высш. учебн. заведений. Радиоэлектроника.- 1998. - Том 41, № 3.- С. 71 - 75.
5. Слюсар В.И. Семейство торцевых произведений матриц и его свойства. // Кибернетика и системный анализ. – 1999. - Том 35; № 3.- С. 379-384.- DOI: 10.1007/BF02733426.
6. Основы военно-технических исследований. Теория и приложения. Том. 2. Синтез средств информационного обеспечения вооружения и военной техники. / А.И. Миночкин, В.И. Рудаков, В.И. Слюсар. – Киев: Гранмна, 2012. – С. 7 – 98; 354 – 521.