Использование нормальной формы Смита для квазициклических LDPC кодов с проверочной матрицей неполного ранга

Д. В. Алексеев (МГУ им. М. В. Ломоносова, Москва)

Коды с малой плотностью проверок на четность (LDPC) были впервые предложены Р. Галлагером в [1], позднее они были переоткрыты Д. МакКеем и Р. Нилом ([2]). Они демонстрируют возможности по исправлению ошибок, близкие к пределу Шеннона. Кроме того они позволяют реализацию кодека с высокой степенью параллелизма, что означает возможность эффективной программной и аппаратной реализации. Поэтому LDPC коды используются во многих областях: жестких дисках, беспроводных коммуникациях и т. д. В данной работе предлагается эффективный алгоритм кодирования для случая проверочной матрицы определенного вида, обладающей неполным рангом. В работе [3] предложен другой эффективный алгоритм, основанный на китайской теореме об остатках.

Ключевые слова: кодирование, коды НППЧ, квазициклические коды, нормальная форма Смита.

1. Основные определения и постановка задачи

LDPC код задается проверочной матрицей H. Кодовыми словами являются те и только те векторы x, для которых $H \cdot x = 0$.

Определение 1. Матрица называется циркулянтной (или циркулянтом), если каждый ее ряд получается циклическим сдвигом предыдущего. То есть, циклическая матрица однозначно определяется своим первым рядом:

$$\mathcal{C}(a_1, \ldots, a_n) = \begin{bmatrix} a_1 & a_2 & \ldots & a_{n-1} & a_n \\ a_n & a_1 & \ldots & a_{n-2} & a_{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_2 & a_3 & \ldots & a_n & a_1 \end{bmatrix}$$

В данной работе подразумевается, что все a_i принадлежат $\mathbb{F}_2$, хотя, вообще говоря, рассуждения остаются верны для любого поля характеристики 2.

Определение 2. Матрица называется квазициклической, если она образована $M \times N$ блоками, каждый из которых является циркулянтном. Указанные блоки называются циркулянтами.

Определение 3. Циркулянт называется простейшим, если в каждой строке содержится ровно одна единица. Простейший циркулянт представляет собой единичную матрицу, столбцы которой сдвинуты вправо на некоторую величину.

Определение 4. Матрица называется простейшей квазициклической, если каждая циркулянт является либо простейшим циркулянтом, либо нулевой матрицей.

Простейшие квазициклические матрицы часто используются как проверочные в LDPC-кодах, поскольку любая такая матрица может быть задана набором сдвигов, соответствующих каждому циркулянту. Кроме того, умножение на такую матрицу представляет собой просто набор сдвигов, что обеспечивает эффективную аппаратную реализацию.

2. Кольцо циркулянтов матриц и нормальная форма Смита

Несложно показать, что циклические матрицы образуют коммутативное кольцо с единицей, в роли которой выступает единичная матрица.

Циркулянты можно также представить в полиномиальном виде. Если поставить в соответствие $\mathcal{C}(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \mapsto \sum_{i=0}^{n-1} \alpha_i \cdot x^i$, то умножению циркулянтных матриц будет соответствовать умножение многочленов по модулю $p(x) = x^n + 1$. Также, удобно рассматривать замену $Z = x + 1$, которая позволяет рассматривать умножение многочленов по модулю $P(Z) = z^n$.

Определение 5. ([2]) Матрица H с элементами из кольца полиномов $\mathbb{Z}[x]/x^n + 1$ называется унимодулярной, если $det(H) = 1$.

Унимодулярные матрицы всегда обратимы, то есть существует H^{-1} с элементами из того же кольца.

Определение 6. Нормальная форма Смита ([2]). Пусть задана матрица $H = (h_i j)_{i,j=1 \div n}$, элементы которой принадлежат некоторому коль-

цу $\mathbb{K}$ элементарных делителей (например, кольцу многочленов). Тогда можно выбрать матрицы-единицы L и R так, что $L \times H \times R = diag(g_1, g_2, \ldots, g_p, 0, \ldots, 0)$, причём g_{i+1} делится на g_i при $i = 1, \ldots, p-1$ (здесь подразумевается, что диагональная матрица дополнена до прямоугольной матрицы нулями).

В [3] показано, что в кольцо циркулянтов тоже является кольцом элементарных делителей.

3. Стандартный алгоритм кодирования

Будем рассматривать простейшие квазициклические матрицы, которые путем перестановки циркулянтов можно привести к следующему виду

$$H = \begin{pmatrix} I^{(1)} & \mathbb{O} & \mathbb{O} & Hu_1^{(1)} \\ \mathbb{O} & I^{(2)} & Hp_{1,2} & Hu_1^{(2)} \\ Hp_{21}^{(1)} & Hp_{21}^{(2)} & Hp_{2,2} & Hu_2 \end{pmatrix}.$$

Здесь $I^{(1)}$ и $I^{(2)}$ — единичные матрицы размера $m_1^{(1)} \cdot C$ и $m_1^{(2)} \cdot C$, соответственно.

Информационная часть (то есть биты, соответствующие пользовательскому сообщению) помечена буквой u, проверочная часть (которую надо вычислить) помечена буквой p.

Таким образом, проверочная часть разбивается на 3 части: $p = (p_1^{(1)}, p_1^{(2)}, p_2)$.

Проверочные уравнения будут записаны в следующем виде:

$$\begin{cases} p_1^{(1)} + Hu_1^{(1)} \times u & = 0 \\ p_1^{(2)} + Hp_1^{(2)} \times p_2 + Hu_1^{(2)} \times u & = 0 \\ Hp_{21}^{(1)} \times p_1^{(1)} + Hp_{21}^{(2)} \times p_1^{(2)} + Hp_{22} \times p_2 + Hu_2 \times u & = 0 \end{cases}$$

Преобразуем эту систему методом Гаусса к виду

$$\begin{cases} p_1^{(1)} + Hu_1^{(1)} \times u & = 0; \\ p_1^{(2)} + Hp_{12} \times p_2 + Hu_1^{(1)} \times u & = 0; \\ \tilde{H}p_2 \times p_2 + \tilde{H}u \times u & = 0, \end{cases} \tag{1}$$

где $\tilde{H}p = Hp_{21}^{(1)} \times Hp_{12} + Hp_{22}^{(1)}$ и $\tilde{H}u = Hp_{21}^{(1)} \times Hu_1^{(1)} + Hp_{21}^{(1)} \times Hu_1^{(2)} + Hu_2$.

Заметим, что часть проверочных битов — $p_1^{(1)}$ — может быть вычислена независимо от остальных, из первого уравнения в **??**. Следующая часть — $p_1^{(2)}$ — может быть получена из второго уравнения: $p_1^{(2)}{=}Hp_{12}{\times}p_2 + Hu_1^{(1)}{\times}u$, но для этого сначала необходимо найти p_2.

В классическом случае, то есть когда исходная матрица H обладает полным рангом, матрица $\tilde{H}p$ является обратимой и, следовательно, p_2 может быть получена из последнего уравнения как $p_2 = \left(\tilde{H}p\right)^{-1}{\times}\tilde{H}u{\times}u$.

4. Алгоритм кодирования для матриц неполного ранга

В данной работе рассматривается случай, когда матрица H неполного ранга, то есть матрица $\tilde{H}p$ является необратимой. Кроме того, предполагается, что циркулянты переставлены в таком порядке, что

$$rank\begin{pmatrix} I^{(1)} & \mathbb{O} & \mathbb{O} \\ \mathbb{O} & I^{(2)} & Hp_{1,2} \\ Hp_{21}^{(1)} & Hp_{21}^{(2)} & Hp_{2,2} \end{pmatrix} = rank\begin{pmatrix} I^{(1)} & \mathbb{O} & \mathbb{O} & Hu_1^{(1)} \\ \mathbb{O} & I^{(2)} & Hp_{1,2} & Hu_1^{(2)} \\ Hp_{21}^{(1)} & Hp_{21}^{(2)} & Hp_{2,2} & Hu_2 \end{pmatrix}$$

Таким образом, необходимо эффективно решать уравнения вида

$$\tilde{H}p \times p_2 = q, \tag{2}$$

где $q = \tilde{H}u \times u$ может быть получено обычным способом.

Представим $\tilde{H}p$ в виде матрицы составленной из многочленов в кольце $\mathbb{Z}_2[x]/z^n$: $\hat{H} = \begin{pmatrix} h_{11}(z) & \dots & h_{1N}(z) \\ \dots & \dots & \dots \\ h_{M1}(z) & \dots & h_{MN}(z) \end{pmatrix}$. В дальнейшем будем использовать обозначение $\hat{A}$ для матрицы, элементы которой — многочлены, соответствующие циркулянтам квазициклической матрицы A.

Существует представление этой матрицы в нормальной форме Смита $\hat{L} \times \hat{H} \times \hat{R} = \hat{D}$, где $\hat{L}$ и $\hat{R}$ — матрицы-единицы, а $\hat{D}$ — диагональная. Подставив в (**??**), получим: $L^{-1}\cdot D\cdot R^{-1}\cdot p_2 = q$, откуда $p_2 = R\cdot\tilde{D}^{-1}\cdot L\cdot q$. Здесь матрицы L и R — квазициклические, а $\tilde{D}^{-1}$ — псевдообратная к D, блочно-диагональная матрица. Поскольку матрица D необратима, то $\tilde{D}^{-1}$ не будет, вообще говоря, квазициклической.

Интересным с точки зрения приложений является случай, когда ранг проверочной матрицы на 1 меньше максимального ранга, то есть

$rank(H) = M \cdot n - 1$. В этом случае матрица $\hat{D}$ имеет вид $D = diag(1, 1, \ldots, 1, Z + 1)$. Тогда псевдообратная матрица является блочно-диагональной: $\tilde{D}^{-1} = Diag(I, I, \ldots, I, Q)$, где матрица Q имеет вид:

$$Q = \begin{pmatrix} 1 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 1 & 1 & \ldots & 0 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 \end{pmatrix}.$$

В итоге алгоритм кодирования выглядит следующим образом:

1. $p_1^{(1)} = Hu_1^{(1)} \times u$;
2. $q = \tilde{H}u \times u$;
3. $q_1 = L \times q$;
4. $q_2 = \tilde{D}^{-1} \times q_1$;
5. $p_2 = R \times q_2$;
6. $q_3 = Hp_{12} \times p_2$;
7. $q_4 = Hu_1^{(2)} \times u$;
8. $p_1^{(2)} = q_3 + q_4$.

В пунктах **??**, **??**, **??**, **??** происходит умножение на разреженные, а в пунктах **??**, **??** — на плотные квазициклические матрицы. В пункте **??** происходит умножение на матрицу общего вида, размер которой совпадает с размером циркулянта. Все матрицы, используемые в алгоритме вычисляются заранее и хранятся в памяти.

Автор выражает благодарность П. А. Пантелееву за плодотворные дискуссии, в ходе которых возникла идея данной статьи.

Список литературы

[1] Gallager R. Low-density parity-check codes // IRE Transactions on Information Theory. — Vol. 8, no. 1. — Jan. 1962. — P. 21–28.

[2] MacKay D. J. C., Neal R. M. Near Shannon limit performance of low density parity check codes // Electronics Letters. — Vol. 33, no. 6. — Mar. 1997. — P. 457–458.

[3] Panteleev P. A. Fast systematic encoding of quasi-cyclic codes using the Chinese remainder theorem // Information Theory (ISIT) — 2015 IEEE International Symposium. — P. 1916–1920.

[4] Прасолов В. В. Задачи и теоремы линейной алгебры — М.: Наука, Физматлит, 1996. — С. 229–231.

[5] Alekseev D. V., Panteleev P. A., Gasanov E. E., Sokolov A. P., Shutkin Y. S. Systems and Methods for Rank Deficient Encoding / US Patent #20150229333, 2015-08-13.