ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 2**

УДК 621.391.15 : 519.725

© 2020 г. **А.В. Харин, К.Н. Заверткин, А.А. Овинников**

ОБНАРУЖЕНИЕ ЦИКЛОВ ДЛИНЫ 8 В ГРАФЕ ТАННЕРА КВАЗИЦИКЛИЧЕСКОГО МПП-КОДА ПО РЕЗУЛЬТАТАМ АНАЛИЗА ПРОТОГРАФА[1]

Предложена процедура идентификации циклов длины 8 в графе Таннера, основанная на анализе маршрутов в протографе. Сформулирован и доказан ряд теорем, которые вводят правила идентификации циклов и ограничивают число анализируемых подграфов. Для их различения предложен набор параметров, однозначно определяющих группу анализируемых маршрутов в протографе.

Ключевые слова: граф Таннера, протограф, расширенный граф, объединение циклов, базовое уравнение, метрика связанности цикла, МПП-код.

DOI: 10.31857/S0555292320020035

§ 1. Введение

В настоящее время широкое распространение в технике передачи и хранения данных получили коды с малой плотностью проверок (МПП-коды). Среди них особое место занимает подкласс квазициклических (КЦ) МПП-кодов, которые были предложены в работах [1–3]. Максимальную популярность в современных спецификациях получили нерегулярные КЦ МПП-коды из-за их высокой энергетической эффективности [4] и наличию относительно быстрых алгоритмов кодирования и декодирования [5, 6]. Структура КЦ проверочных матриц обеспечивает компактность хранения в памяти и упрощает процедуру кодирования МПП-кода. Однако с точки зрения синтеза таких кодов еще остается ряд нерешенных задач. Первой из них является оптимизация весовых распределений ненулевых элементов по строкам и столбцам проверочной матрицы в заданном канале связи с учетом ограниченной длины кода и размера циркулянта. Вторая задача состоит в получении кодов с заданным обхватом графа Таннера и распределением метрик связанности циклов (МСЦ) [7] в нем. Представленное здесь исследование может выступать как теоретическая основа для решения последней задачи.

Величина обхвата графа Таннера считается [8] важной метрикой в оценке эффективности итеративного декодирования МПП-кодов. В работе [2] была предложена формула, отражающая необходимое и достаточное условие существования цикла в графе Таннера, определяемое по протографу. Там же было показано, что для полносвязанных графов обхват ограничен значением $g_0 = 12$. Впервые концепция объединений циклов в протографе была введена в публикации [9]. Авторами [9] было обнаружено, что процедура преобразования циклов в процессе расширения базового графа КЦ МПП-кода является достаточно сложной и предложили необходимые условия для получения $g_0 = 10$. Однако ими была допущена ошибка при рассмотрении вариантов пар объединений циклов с длинами 4, один из них был пропущен,

[1] Работа выполнена за счет гранта Российского научного фонда (проект № 17-79-20302).

о чем подробнее будет рассказано далее. Кроме того, ничего не сказано про необходимые условия для достижения в графе Таннера обхвата, равного 12. Логическим завершением работ [2, 9] стал разработанный в [10] метод синтеза КЦ МПП-кодов, основанный на двух теоремах, описывающих необходимые и достаточные условия существования циклов в расширенных двудольных графах по обозначенным конфигурациям объединенных циклов в протографе. Авторами [10] была выдвинута гипотеза о существовании необнаруживаемого алгоритмом PEG [11] цикла в расширенном графе, состоящая в том, что объединение циклов в базовом графе должно содержать как минимум одно общее ребро. Полученные нами результаты, а также исходное описание алгоритма PEG [11] говорят об ошибочности такого предположения. Однако даже в рамках рассматриваемых множеств объединений авторы [10] упустили ряд важных конфигураций.

Первые предпосылки к полученным в настоящей статье результатам были обозначены в [12], где сформулированы и доказаны две теоремы о преобразовании одиночного цикла протографа при его расширении в граф Таннера. Кроме того, в работе [12] введены необходимые понятия для описания параметров объединенных циклов и получен первичный набор правил для их идентификации в базовом графе. В то же время было упущено несколько важных исключений и дополнений, которые не позволят достичь поставленной в работе [12] задачи для произвольных размеров циркулянтов КЦ МПП-кодов. Таким образом, до настоящего времени не было получено исчерпывающего описания процесса топологического расширения базового графа с точки зрения преобразования коротких циклов длины до 8 включительно. Настоящая статья решает эту задачу как в части анализа соответствующих маршрутов в протографе, так и в рамках расчета МСЦ [7], чему посвящены последующие параграфы.

§ 2. Общие теоретические сведения

Ненаправленный двудольный граф $G = (V, C, E)$ определяется множествами кодовых V и проверочных C вершин, таких что $V \cap C = \varnothing$, а также подмножеством пар $\{(v, c),\ v \in V,\ c \in C\}$, соответствующих ребрам $e = (v, c) \in E$. Степени кодовых и проверочных вершин обозначаются через d_v, $v \in V$, и d_c, $c \in C$. В силу того, что в дальнейшем интерес будут представлять только значения d_v, можно ввести упрощенное обозначение вида $d_{v_i} = d_i$. Маршрут w^g длины g в графе G представляется последовательностью вершин вида $v_0, c_0, v_1, c_1, \ldots, v_{g-1}, c_{g-1}, v_g$. При этом если $v_0 = v_g$, то маршрут называется замкнутым. Маршрут не содержит обратных проходов, если любая тройка вершин имеет вид v_i, c_j, v_k или c_i, v_j, c_k, $i \neq k$. В дальнейшем будем рассматривать только замкнутые маршруты без обратных проходов и будем называть их просто маршрутами. Циклом s^g длины g называется такой маршрут, в котором все промежуточные вершины за исключением $v_0 = v_g$ отличаются друг от друга. Обхватом графа G считается длина g_0 кратчайшего цикла s_0. В классе двудольных графов g_0 не может быть меньше $g_{\min} = 4$. Общее количество кодовых и проверочных вершин определяется формулами $n = |V|$, $m = |C|$. В статье рассматриваются только такие двудольные графы, для которых отсутствуют кратные ребра.

Рассмотрим следующую конструкцию. Пусть C_q – циклическая подгруппа симметричной группы S_q над множеством целых чисел $Z_q = \{0, 1, \ldots, q-1\}$ мощности q с единственной операцией – циклической перестановкой. Элементы S_q – это перестановки на множестве из q элементов. Рассмотрим циркулянт p_a в C_q, который соответствует циклическому сдвигу на a элементов вправо, где a – величина сдвига циркулянта.

Пусть G_b и G – топологически связные двудольные графы, причем второй получается из первого следующим образом: копируем q раз каждую кодовую и проверочную вершину в G_b, где $v_b \in V_b$, $c_b \in C_b$. Полученные q копий $v = \{v_b^0, v_b^1, \ldots, v_b^{q-1}\} \in$

$\in V$ и $c = \{c_b^0, c_b^1, \ldots, c_b^{q-1}\} \in C$ подвергаются циклической перестановке $p_a \in C_q$ для каждой копии e_b в e. Далее граф G_b будет называться базовым, или протографом, а G – расширенным графом. Число вершин в G определяется соотношениями $m = m_b q$ и $n = n_b q$.

Известно [2], что представленное топологическое преобразование графов приводит к тому, что интегральный сдвиг для маршрута в G_b определяется согласно формуле

$$P^{g_b} = \sum_{k=0}^{g_b/2-1} (a_{i_k,j_k} - a_{i_{k+1},j_k}) \mod q. \tag{1}$$

Для пояснения этого выражения рассмотрим базовую матрицу регулярного МПП-кода, элементы которой соответствуют величинам сдвига циркулянтов $p_{a_{i,j}}$. Любой маршрут в связанном с ней протографе можно записать в виде последовательности элементов, например, $a_{0,0}, a_{0,1}, a_{1,1}, a_{1,0}, a_{0,0}$. Согласно [2] сумма попарных разностей значений базовой матрицы, принадлежащих одному столбцу j_k, позволяет получить так называемый интегральный сдвиг, обладающий рядом чрезвычайно важных свойств, которые рассмотрены далее,

$$H_b = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,d_c-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,d_c-1} \\ \cdots & \cdots & \cdots & \cdots \\ a_{d_v-1,0} & a_{d_v-1,1} & \cdots & a_{d_v-1,d_c-1} \end{bmatrix}. \tag{2}$$

Формулу (1) и величину P^{g_b} назовем базовым уравнением (БУ) и его решением (РБУ) соответственно. Важно отметить, что изменение направления обхода маршрута на противоположный приводит к изменению знака РБУ с плюса на минус или наоборот. Следующая теорема описывает необходимое и достаточное условие существования циклов в расширенном графе [9].

Теорема 1. *Маршрут w^{g_b} длины g_b в базовом графе отображается в набор циклов длины $g = g_b$ в расширенном графе тогда и только тогда, когда $P^{g_b} = 0$ и w^{g_b} не содержит в себе маршрутов w_{inc}, для которых $P_{\text{inc}} = 0$. Здесь P^{g_b} и P_{inc} рассчитываются согласно* (1), *а индекс* inc *обозначает вложенность маршрута.*

Данная теорема описывает возможные преобразования как одиночного цикла, так и маршрута при расширении графа. Однако согласно [9, 10] объединения циклов также могут быть подвержены изменениям. Циклы s_i и s_j образуют объединение в протографе тогда и только тогда, когда они содержат хотя бы одну общую вершину. Такая пара циклов в G_b описывается следующим набором параметров:

- g_i и g_j – длины пересекающихся циклов;
- n_{cv} – число общих вершин между s_i и s_j;
- n_{ce} – число общих ребер между s_i и s_j;
- n_{cr} – взаимное направление обхода, которое принимает значение, равное нулю, при совпадении обходов циклов по общему ребру (общим ребрам), а в противном случае $n_{\text{cr}} = 1$.

В работе [7] рассмотрена мера, описывающая число ребер, связывающих кодовые вершины цикла с внешними по отношению к нему проверочными вершинами. Для определения числа таких связей используется формула (см. [7])

$$\gamma = \sum_{k=0}^{g/2-1} (d_k - 2). \tag{3}$$

Определим параметр γ как метрику связанности цикла (МСЦ) s с графом G.

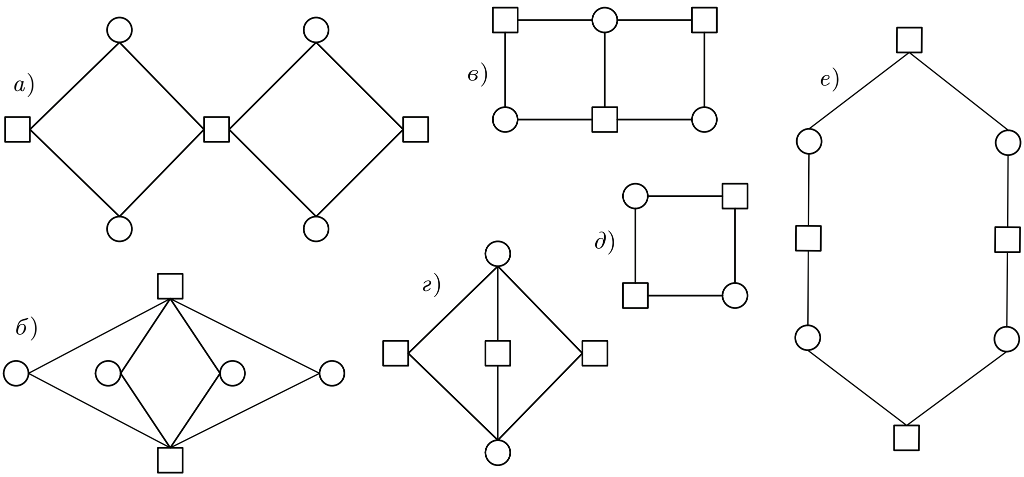

Рис. 1. Конфигурации подграфов, в которых возможно существование маршрутов длины g_x

В последующих параграфах рассмотрены маршруты целевой длины $g_x = 8$ и образующие их подграфы – элементы протографов, состоящие из объединений циклов минимальной длины, а также аналитика изменения значений МСЦ при расширении базового графа.

§ 3. Условия образования циклов

Теорема 2. *Циклы s^{g_x} в расширенном графе G образуются из маршрутов w^{g_x} в базовом графе G_b, таких что определяемые ими подграфы изоморфны одному из шести графов, представленных на рис.* 1.

Доказательство. Пусть цикл имеет вид $s^{g_x} = (u_1, u_2, \ldots, u_{g_x}, u_1)$, где $u \in C \cup V$. Тогда маршрут в протографе, из которого образовался цикл, имеет вид $w^{g_x} = (f(u_1), f(u_2), \ldots, f(u_{g_x}), f(u_1))$, где $f(v_b^i) = v_b$, $f(c_b^j) = c_b$ для всех $v_b \in V_b$, $c_b \in C_b$, $i, j \in [0, q-1]$.

Тогда маршрут w^{g_x} определяет в графе G_b подграф T с множеством вершин $\{f(u_1), f(u_2), \ldots, f(u_{g_x})\}$ и множеством ребер

$$\{(f(u_1), f(u_2)), (f(u_2), f(u_3)), \ldots, (f(u_{g_x}), f(u_1))\}.$$

Теперь можно сформулировать следующие предложения.

Предложение 1. *Подграф T изоморфен факторграфу графа S по разбиению P, а именно $T \cong S/P$, где S – цикл с вершинами $\{u_1, u_2, \ldots, u_{g_x}\}$ и ребрами $\{(u_1, u_2), (u_2, u_3), \ldots, (u_{g_x}, u_1)\}$, а $P = \{i, j \in I \mid f(u_j) = f(u_i)\}$, $I = \{1, 2, \ldots, g_x\}$.*

Предложение 2. *Для всяких $J \in P$, $u_i, u_j \in J$ разность $i - j$ четна, но отлична от двух.*

Для $g_x = 8$ из предложения 2 следует, что J либо одноэлементно, либо является одной из пар (u_1, u_5), (u_2, u_6), (u_3, u_7), (u_4, u_8).

Пусть $\mathcal{P}$ – множество всех разбиений множества J, указанного в предложении 2. Назовем $P, Q \in \mathcal{P}$ эквивалентными, $P \sim Q$, если $Q = \{\{a(u_j) \mid u_j \in J\} \mid J \in P\}$, где a – автоморфизм цикла S. Тогда справедливо следующее

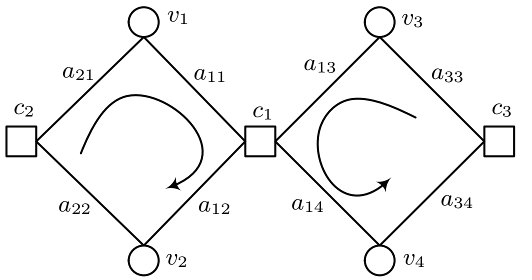

Рис. 2. Графическое изображение подграфа а)

П р е д л о ж е н и е 3. *Если $P \sim Q$, $P, Q \in \mathcal{P}$, то $S/P \cong S/Q$. Если P эквивалентно Q, то факторграф графа S по разбиению P изоморфен факторграфу графа S по разбиению Q.*

Учитывая возможные значения J и предложение 3, существует шесть вариантов для P:

$$\begin{aligned}
&\{u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8\},\\
&\{(u_1, u_5), u_2, u_3, u_4, u_6, u_7, u_8\},\\
&\{(u_1, u_5), (u_2, u_6), u_3, u_4, u_7, u_8\},\\
&\{(u_1, u_5), (u_3, u_7), u_2, u_4, u_6, u_8\},\\
&\{(u_1, u_5), (u_2, u_6), (u_3, u_7), u_4, u_8\},\\
&\{(u_1, u_5), (u_2, u_6), (u_3, u_7), (u_4, u_8)\}.
\end{aligned} \tag{4}$$

Тогда S/P для этих вариантов P будет соответствовать подграфам е), а), в), б), г) и д). ▲

В силу того, что подграф е) является одиночным циклом в базовом графе, его учет является относительно тривиальной задачей и может быть выполнен на основе любого алгоритма нумерации циклов.

Т е о р е м а 3. *Базовое уравнение для любого маршрута w^{g_x} в протографе может быть выражено через БУ пары циклов $s^{g_{\min}}$, покрывающих все вершины маршрута w^{g_x}.*

Д о к а з а т е л ь с т в о. В соответствии с теоремой 2 маршруты длины g_x могут образовываться в одном из шести возможных подграфов, исключая из рассмотрения случай е). Рассмотрим первый из них (рис. 2).

В данном подграфе возможно существование двух маршрутов длины g_x:

$$\begin{aligned}
&w_1^{g_x} = v_1, c_1, v_4, c_3, v_3, c_1, v_2, c_2, v_1,\\
&w_2^{g_x} = v_1, c_1, v_3, c_3, v_4, c_1, v_2, c_2, v_1.
\end{aligned}$$

Запишем БУ для этих маршрутов:

$$P_1^{g_x} = (a_{3,4} - a_{1,4}) + (a_{1,1} - a_{2,1}) + (a_{2,2} - a_{1,2}) + (a_{1,3} - a_{3,3}), \tag{5}$$
$$P_2^{g_x} = (a_{1,4} - a_{3,4}) + (a_{3,3} - a_{1,3}) + (a_{1,1} - a_{2,1}) + (a_{2,2} - a_{1,2}). \tag{6}$$

Уравнение для $P_1^{g_x}$ может быть представлено в виде следующих двух сумм: $P_1^{g_{\min}} = (a_{1,1} - a_{2,1}) + (a_{2,2} - a_{1,2})$ и $P_2^{g_{\min}} = (a_{3,4} - a_{1,4}) + (a_{1,3} - a_{3,3})$. При этом первая из них является записью БУ для цикла $s_1^{g_{\min}} = v_1, c_1, v_2, c_2, v_1$, а вторая – для цикла $s_2^{g_{\min}} = v_3, c_1, v_4, c_3, v_3$. Таким образом, БУ для маршрута $w_1^{g_x}$ может быть выражено

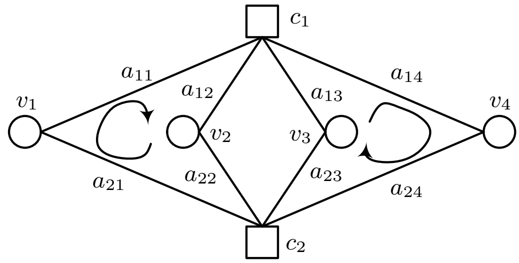

Рис. 3. Графическое изображение подграфа б)

как сумма БУ циклов $s_1^{g_{\min}}$ и $s_2^{g_{\min}}$:

$$P_1^{g_x} = P_1^{g_{\min}} + P_2^{g_{\min}}. \tag{7}$$

Аналогично, уравнение для $P_2^{g_x}$ можно разбить на следующие две суммы: $P_1^{g_{\min}} = (a_{1,1} - a_{2,1}) + (a_{2,2} - a_{1,2})$ и $P_2'^{g_{\min}} = (a_{1,4} - a_{3,4}) + (a_{3,3} - a_{1,3})$, где $P_2'^{g_{\min}} = -P_2^{g_{\min}}$. Таким образом, БУ для маршрута $w_2^{g_x}$ может быть выражено через БУ тех же циклов, что и БУ для маршрута $w_1^{g_x}$:

$$P_2^{g_x} = P_1^{g_{\min}} - P_2^{g_{\min}}. \tag{8}$$

В итоге БУ для обоих маршрутов длины g_x, существующих в подграфе а), могут быть выражены через БУ циклов длины $g_{\min}$.

Далее рассмотрим второй из возможных подграфов (рис. 3). В нем возможно существование шести маршрутов длины g_x:

$$\begin{aligned} &w_1^{g_x} = v_1, c_1, v_2, c_2, v_3, c_1, v_4, c_2, v_1, \quad && w_2^{g_x} = v_1, c_1, v_2, c_2, v_4, c_1, v_3, c_2, v_1,\\ &w_3^{g_x} = v_1, c_1, v_3, c_2, v_2, c_1, v_4, c_2, v_1, && w_4^{g_x} = v_1, c_1, v_3, c_2, v_4, c_1, v_2, c_2, v_1,\\ &w_5^{g_x} = v_1, c_1, v_4, c_2, v_2, c_1, v_3, c_2, v_1, && w_6^{g_x} = v_1, c_1, v_4, c_2, v_3, c_1, v_2, c_2, v_1. \end{aligned}$$

Записав БУ для каждого из маршрутов, можно показать, что все они могут быть выражены суммой или разностью БУ пары циклов длины $g_{\min}$:

$$\left.\begin{aligned} P_i^{g_x} &= P_i^{g_{\min}} + P_{i+1}^{g_{\min}},\\ P_{i+1}^{g_x} &= P_i^{g_{\min}} - P_{i+1}^{g_{\min}}, \end{aligned}\right. \qquad i = 1, 3, 5.$$

Здесь $P_j^{g_{\min}}$, $j \in [1, 6]$, – БУ для циклов длины $g_{\min}$: $s_1^{g_{\min}} = v_1, c_1, v_2, c_2, v_1$, $s_2^{g_{\min}} = v_3, c_1, v_4, c_2, v_3$, $s_3^{g_{\min}} = v_1, c_1, v_3, c_2, v_1$, $s_4^{g_{\min}} = v_2, c_1, v_4, c_2, v_2$, $s_5^{g_{\min}} = v_1, c_1, v_4, c_2, v_1$ и $s_6^{g_{\min}} = v_2, c_1, v_3, c_2, v_2$.

Таким образом, БУ для всех маршрутов длины g_x, существующих в подграфе б), могут быть выражены через БУ циклов длины $g_{\min}$.

Далее рассмотрим третий из возможных подграфов (рис. 4). В нем возможно существование одного маршрута длины g_x:

$$w_1^{g_x} = v_1, c_1, v_3, c_2, v_1, c_1, v_2, c_3, v_1.$$

Записав БУ для этого маршрута, можно показать, что оно может быть выражено суммой БУ пары циклов длины $g_{\min}$:

$$P_1^{g_x} = P_1^{g_{\min}} + P_2^{g_{\min}}, \tag{9}$$

где $P_1^{g_{\min}}$ и $P_2^{g_{\min}}$ – БУ для циклов длины $g_{\min}$: $s_1^{g_{\min}} = v_1, c_1, v_3, c_2, v_1$ и $s_2^{g_{\min}} = v_1, c_1, v_2, c_3, v_1$.

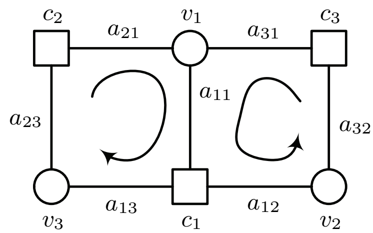

Рис. 4. Графическое изображение подграфа в)

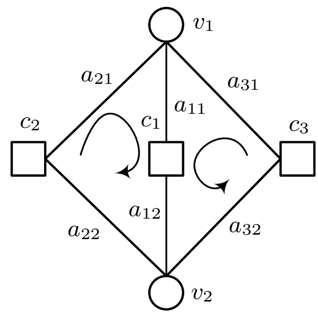

Рис. 5. Графическое изображение подграфа г)

Таким образом, БУ для маршрута длины g_x, существующего в подграфе в), может быть выражено через БУ циклов длины $g_{\min}$.

Далее рассмотрим четвертый из возможных подграфов (рис. 5). В нем возможно существование одного маршрута длины g_x:

$$w_1^{g_x} = v_1, c_1, v_2, c_2, v_1, c_1, v_2, c_3, v_1.$$

Записав БУ для этого маршрута, можно показать, что оно может быть выражено суммой БУ пары циклов длины $g_{\min}$:

$$P_1^{g_x} = P_1^{g_{\min}} + P_2^{g_{\min}}, \tag{10}$$

где $P_1^{g_{\min}}$ и $P_2^{g_{\min}}$ – БУ для циклов длины $g_{\min}$: $s_1^{g_{\min}} = v_1, c_1, v_2, c_2, v_1$ и $s_2^{g_{\min}} = v_1, c_1, v_2, c_3, v_1$.

Таким образом, БУ для маршрута длины g_x, существующего в подграфе г), может быть выражено через БУ циклов длины $g_{\min}$.

Наконец, рассмотрим пятый из возможных подграфов (рис. 6). В нем возможно существование одного маршрута длины g_x:

$$w_1^{g_x} = v_1, c_1, v_2, c_2, v_1, c_1, v_2, c_2, v_1.$$

Записав БУ для этого маршрута, можно показать, что оно может быть выражено удвоенным БУ цикла длины $g_{\min}$:

$$P_1^{g_x} = P_1^{g_{\min}} + P_1^{g_{\min}}, \tag{11}$$

где $P_1^{g_{\min}}$ – БУ для цикла длины $g_{\min}$: $s_1^{g_{\min}} = v_1, c_1, v_2, c_2, v_1$.

Таким образом, БУ для маршрута длины g_x, существующего в подграфе д), может быть выражено через БУ цикла длины $g_{\min}$.

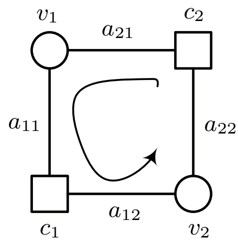

Рис. 6. Графическое изображение подграфа д)

Из всего вышесказанного следует, что БУ любого маршрута длины g_x может быть выражено через БУ циклов длины $g_{\min}$, которые существуют в подграфе, формируемом маршрутом, и покрывают всего его вершины. ▲

Теорема 4. *Условие образования цикла длины g_x в расширенном графе из маршрута в протографе может быть выражено через базовые уравнения циклов длины $g_{\min}$.*

Доказательство. В соответствии с теоремой 1 маршрут в базовом графе будет преобразован в цикл в расширенном графе, если решение БУ для маршрута равно нулю, а решения БУ для всех более коротких маршрутов, входящих в рассматриваемый, будут отличны от нуля.

Рассмотрим пару маршрутов длины g_x, образующихся в подграфе а). В соответствии с теоремой 3 БУ для каждого из них может быть выражено через БУ циклов длины $g_{\min}$. Также, обратившись к записи маршрутов, легко заметить, что они содержат более короткие маршруты, являющиеся циклами длины $g_{\min}$, через БУ которых выражается БУ маршрутов. Далее такие короткие циклы будем называть компонентными циклами.

Таким образом, преобразование маршрутов в протографе в цикл при расширении графа происходит при выполнении системы условий вида

$$\begin{cases} (P_1^{g_{\min}} \pm P_2^{g_{\min}}) \mod q = 0, \\ P_1^{g_{\min}} \mod q \neq 0, \\ P_2^{g_{\min}} \mod q \neq 0. \end{cases}$$

Аналогичные системы условий можно составить для маршрутов, существующих в подграфах в) и д):

$$\begin{cases} (P_1^{g_{\min}} + P_2^{g_{\min}}) \mod q = 0, \\ P_1^{g_{\min}} \mod q \neq 0, \\ P_2^{g_{\min}} \mod q \neq 0. \end{cases}$$

Для подграфа г) количество дополнительных условий сводится к одному согласно теореме 3, что позволяет составить следующую систему условий:

$$\begin{cases} (P_1^{g_{\min}} + P_1^{g_{\min}}) \mod q = 0, \\ P_1^{g_{\min}} \mod q \neq 0. \end{cases}$$

Маршруты, образующиеся в подграфе б), отличаются от рассмотренных выше тем, что каждый из них содержит по четыре дополнительных цикла. Используя нумерацию циклов из описания подграфа б) в теореме 3, можно показать, что

$$
\begin{aligned}
&w_1^{g_x} \supset s_1^{g_{\min}}, s_2^{g_{\min}}, s_5^{g_{\min}}, s_6^{g_{\min}}, \quad && w_2^{g_x} \supset s_1^{g_{\min}}, s_2^{g_{\min}}, s_3^{g_{\min}}, s_4^{g_{\min}},\\
&w_3^{g_x} \supset s_3^{g_{\min}}, s_4^{g_{\min}}, s_5^{g_{\min}}, s_6^{g_{\min}}, \quad && w_4^{g_x} \supset s_3^{g_{\min}}, s_4^{g_{\min}}, s_1^{g_{\min}}, s_2^{g_{\min}},\\
&w_5^{g_x} \supset s_5^{g_{\min}}, s_6^{g_{\min}}, s_3^{g_{\min}}, s_4^{g_{\min}}, \quad && w_6^{g_x} \supset s_5^{g_{\min}}, s_6^{g_{\min}}, s_1^{g_{\min}}, s_2^{g_{\min}}.
\end{aligned}
$$

В таком случае происходит преобразование маршрута w^{g_x} в равновеликий цикл при расширении протографа, если выполняется система условий

$$
\begin{cases}
(P_i^{g_{\min}} + P_{i+1}^{g_{\min}}) \mod q = 0,\\
P_i^{g_{\min}} \mod q \neq 0,\\
P_{i+1}^{g_{\min}} \mod q \neq 0,\\
P_k^{g_{\min}} \mod q \neq 0,\\
P_\ell^{g_{\min}} \mod q \neq 0,
\end{cases}
\qquad i = 1,3,5, \quad k = 5,5,3, \quad \ell = 6,6,2,
$$

или

$$
\begin{cases}
(P_i^{g_{\min}} - P_{i+1}^{g_{\min}}) \mod q = 0,\\
P_i^{g_{\min}} \mod q \neq 0,\\
P_{i+1}^{g_{\min}} \mod q \neq 0,\\
P_k^{g_{\min}} \mod q \neq 0,\\
P_{k+1}^{g_{\min}} \mod q \neq 0,
\end{cases}
\qquad i = 1,3,5, \quad k = 3,1,1.
$$

Таким образом, утверждение, указанное в формулировке теоремы, является верным для всех существующих маршрутов. ▲

Т е о р е м а 5. *Значение МСЦ для циклов s^{g_x} в расширенном графе определяется суммой метрик связанности циклов, через которые выражено БУ маршрута.*

Д о к а з а т е л ь с т в о. В соответствии с теоремой 3 БУ любого маршрута длины g_x может быть описано суммой БУ циклов длины $g_{\min}$.

В случае подграфа а) МСЦ циклов длины g_x, образованных соответствующими им маршрутами, равны и вычисляются согласно выражению

$$\gamma^{g_x} = (d_1 - 2) + (d_2 - 2) + (d_3 - 2) + (d_4 - 2). \tag{12}$$

При этом МСЦ компонентных циклов длины $g_{\min}$ равны

$$
\begin{aligned}
\gamma_1^{g_{\min}} &= (d_1 - 2) + (d_2 - 2),\\
\gamma_2^{g_{\min}} &= (d_3 - 2) + (d_4 - 2).
\end{aligned} \tag{13}
$$

Объединяя (12) и (13), получим

$$\gamma^{g_x} = \gamma_1^{g_{\min}} + \gamma_2^{g_{\min}}.$$

Если в подграфе а) все кодовые вершины заменить проверочными и наоборот, то выражения для вычисления МСЦ изменятся, однако соотношение между ними сохранится:

$$
\begin{aligned}
\gamma^{g_x} &= 2(d_1 - 2) + (d_2 - 2) + (d_3 - 2),\\
\gamma_1^{g_{\min}} &= (d_1 - 2) + (d_2 - 2),\\
\gamma_2^{g_{\min}} &= (d_1 - 2) + (d_3 - 2),\\
\gamma^{g_x} &= \gamma_1^{g_{\min}} + \gamma_2^{g_{\min}}.
\end{aligned}
$$

В случае подграфа б) МСЦ для циклов длины g_x, образующихся из всех шести возможных маршрутов, одинакова:

$$\gamma^{g_x} = (d_1 - 2) + (d_2 - 2) + (d_3 - 2) + (d_4 - 2),$$

а МСЦ компонентных циклов выражаются следующим образом:

$$\begin{aligned} &\gamma_1^{g_{\min}} = (d_1 - 2) + (d_2 - 2), \quad &&\gamma_2^{g_{\min}} = (d_3 - 2) + (d_4 - 2),\\ &\gamma_3^{g_{\min}} = (d_1 - 2) + (d_3 - 2), \quad &&\gamma_4^{g_{\min}} = (d_2 - 2) + (d_4 - 2),\\ &\gamma_5^{g_{\min}} = (d_1 - 2) + (d_4 - 2), \quad &&\gamma_6^{g_{\min}} = (d_2 - 2) + (d_3 - 2), \end{aligned}$$

и тогда МСЦ для циклов длины g_x может быть выражено одной из трех сумм:

$$\gamma^{g_x} = \gamma_1^{g_{\min}} + \gamma_2^{g_{\min}} = \gamma_3^{g_{\min}} + \gamma_4^{g_{\min}} = \gamma_5^{g_{\min}} + \gamma_6^{g_{\min}}. \tag{14}$$

Если в подграфе б) все кодовые вершины заменить проверочными и наоборот, то выражения для МСЦ циклов изменятся:

$$\begin{aligned} &\gamma^{g_x} = 2(d_1 - 2) + 2(d_2 - 2),\\ &\gamma_1^{g_{\min}} = \gamma_2^{g_{\min}} = \gamma_3^{g_{\min}} = \gamma_4^{g_{\min}} = \gamma_5^{g_{\min}} = \gamma_6^{g_{\min}} = (d_1 - 2) + (d_2 - 2), \end{aligned}$$

а формула (14) останется верной.

Запишем выражение для МСЦ циклов, образующихся из подграфа в):

$$\gamma^{g_x} = 2(d_1 - 2) + (d_2 - 2) + (d_3 - 2).$$

Эту же метрику для компонентных циклов выразим уравнениями

$$\begin{aligned} &\gamma_1^{g_{\min}} = (d_1 - 2) + (d_2 - 2),\\ &\gamma_2^{g_{\min}} = (d_1 - 2) + (d_3 - 2). \end{aligned}$$

Объединяя приведенные выше выражения, получим

$$\gamma^{g_x} = \gamma_1^{g_{\min}} + \gamma_2^{g_{\min}}.$$

Если в подграфе заменить типы вершин на противоположные, то выражения для вычисления МСЦ не изменятся.

Формула для вычисления МСЦ циклов, образующихся из подграфа г), имеет вид

$$\gamma^{g_x} = 2(d_1 - 2) + 2(d_2 - 2),$$

причем компонентные циклы характеризуются следующей метрикой связанности:

$$\begin{aligned} &\gamma_1^{g_{\min}} = (d_1 - 2) + (d_2 - 2),\\ &\gamma_2^{g_{\min}} = (d_1 - 2) + (d_2 - 2). \end{aligned}$$

Объединяя приведенные выше выражения, получим

$$\gamma^{g_x} = \gamma_1^{g_{\min}} + \gamma_2^{g_{\min}}.$$

Если в подграфе г) все кодовые вершины заменить проверочными и наоборот, то выражения для вычисления МСЦ изменятся, однако соотношение между ними

Таблица 1

Параметры n_{cv} и n_{ce} для подграфов

Подграф	а)	б)	в)	г)	д)
n_{cv}	1	2	2	3	4
n_{ce}	0	0	1	2	4

сохранится:

$$\gamma^{g_x} = 2(d_1 - 2) + (d_2 - 2) + (d_3 - 2),$$
$$\gamma_1^{g_{\min}} = (d_1 - 2) + (d_2 - 2),$$
$$\gamma_2^{g_{\min}} = (d_1 - 2) + (d_3 - 2),$$
$$\gamma^{g_x} = \gamma_1^{g_{\min}} + \gamma_2^{g_{\min}}.$$

И наконец, для подграфа д) МСЦ образующихся циклов вычисляется в соответствии со следующим выражением:

$$\gamma^{g_x} = 2(d_1 - 2) + 2(d_2 - 2).$$

При этом МСЦ цикла длины $g_{\min}$, БУ которого используется для выражения БУ маршрута, равна

$$\gamma_1^{g_{\min}} = (d_1 - 2) + (d_2 - 2).$$

В этом случае

$$\gamma^{g_x} = \gamma_1^{g_{\min}} + \gamma_1^{g_{\min}}.$$

Замена типа вершин в подграфе на противоположные не изменяет выражений для вычисления МСЦ.

Таким образом, утверждение, указанное в формулировке теоремы, является верным для всех типов подграфов при целевой длине цикла, равной g_x. ▲

§ 4. Процедура определения наличия циклов длины g_x в расширенном графе путем анализа протографа

Полученные выше условия позволяют построить процедуру определения наличия циклов длины g_x в расширенном графе путем анализа циклов, существующих в протографе.

Сравнение алгоритмов обнаружения коротких циклов с прямым поиском маршрутов по вычислительной сложности говорит не в пользу последнего. Поэтому целесообразно взять за основу именно первый вариант. Любой из пяти возможных подграфов, в котором существуют маршруты длины g_x, может быть представлен как объединение двух циклов длины $g_{\min}$ с некоторым количеством общих вершин n_{cv} и ребер n_{ce}. В табл. 1 приведено соответствие между подграфами, в которых существуют маршруты длины g_x, и параметрами n_{cv} и n_{ce} объединения двух циклов длины $g_{\min}$.

Таким образом, сравнив записи двух циклов длины $g_{\min}$ и определив наличие общих вершин и ребер, мы можем однозначно определить наличие и тип подграфа согласно теореме 2. Также можно заметить, что для описания протографа и выражения БУ маршрута используется одна и та же пара циклов. Все это позволяет нам предложить процедуру определения наличия циклов длины g_x в расширенном графе, который включает в себя следующие шаги:

1. Выполнить поиск одиночных циклов длины g_x и $g_{\min}$;
2. Составить и решить БУ для одиночных циклов длины g_x, найденных в п. 1. Если хотя бы одно связанное с циклом РБУ равно нулю, то процедура завершается, иначе переходим к следующему шагу;
3. Попарно сравнить все циклы длины $g_{\min}$ и обнаружить их объединения;
4. Определить тип подграфа по табл. 1 для каждого из обнаруженных объединений;
5. Составить и решить систему условий по всем объектам из п. 4;
6. Цикл длины g_x считается обнаруженным, если хотя бы одна из систем условий выполнена, иначе циклы целевой длины отсутствуют.

С помощью предложенной процедуры мы можем обнаружить циклы длины g_x без выполнения затратной процедуры расширения протографа.

§ 5. Заключение

В рамках проделанной работы предложена процедура определения наличия цикла длины g_x в графе Таннера КЦ МПП-кода путем анализа соответствующих маршрутов в протографе. Сформулирован и доказан набор теорем 2–5, которые лежат в основе представленной процедуры. Они служат для определения множества подграфов в базовом графе, образованных объединением одиночных циклов длины $g_{\min}$ и позволяющих выявить факт существования циклов длины g_x в расширенном графе с универсальной формулой расчета МСЦ. Таким образом, описан процесс топологического расширения двудольного графа без параллельных ветвей в плоскости изменения структуры циклов длины g_x. В дальнейшем планируется продолжить работу в направлении увеличения длины анализируемого цикла в расширенном графе без кратных ребер, а также разработать алгоритм, максимизирующий обхват графа Таннера КЦ МПП-кода с $g_0 \leqslant 12$ на основе предлагаемого подхода.

Авторы выражают особую благодарность А.Н. Воропаеву за помощь в доказательстве теоремы 2, а также рецензенту за внимательное прочтение рукописи и ценные замечания, позволившие улучшить качество итоговой работы.

СПИСОК ЛИТЕРАТУРЫ

1. *Tanner R.M.* On Quasi-cyclic Repeat-Accumulate Codes // Proc. 37th Allerton Conf. on Communication, Control and Computing. Monticello, IL, USA. Sept. 22–24, 1999. P. 249–259.
2. *Fossorier M.P.C.* Quasi-cyclic Low-Density Parity-Check Codes from Circulant Permutation Matrices // IEEE Trans. Inform. Theory. 2004. V. 50. № 8. P. 1788–1793.
3. *Fan J.L.* Array Codes as Low-Density Parity-Check Codes // Proc. 2nd Int. Symp. on Turbo Codes and Related Topics. Brest, France. Sept. 4–7, 2000. P. 543–546.
4. *Richardson T.J., Shokrollahi M.A., Urbanke R.L.* Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes // IEEE Trans. Inform. Theory. 2001. V. 47. № 2. P. 619–637.
5. *Li Z., Chen L., Zeng L., Lin S., Fong W.H.* Efficient Encoding of Quasi-cyclic Low-Density Parity-Check Codes // IEEE Trans. Commun. 2006. V. 54. № 1. P. 71–81.
6. *Kschischang F.R., Frey B.J., Loeliger H.-A.* Factor Graphs and the Sum-Product Algorithm // IEEE Trans. Inform. Theory. 2001. V. 47. № 2. P. 498–519.
7. *Tian T., Jones C.R., Villasenor J.D., Wesel R.D.* Selective Avoidance of Cycles in Irregular LDPC Code Construction // IEEE Trans. Commun. 2004. V. 52. № 8. P. 1242–1247.
8. *Mao Y., Banihashemi A.H.* A Heuristic Search for Good Low-Density Parity-Check Codes at Short Block Lengths // Proc. 2001 IEEE Int. Conf. on Communications (ICC'2001). Helsinki, Finland. June 11–14, 2001. V. 1. P. 41–44.
9. *Karimi M., Banihashemi A.H.* On the Girth of Quasi Cyclic Protograph LDPC Codes // IEEE Trans. Inform. Theory. 2013. V. 59. № 7. P. 4542–4552.

10. *Diouf M., Declercq D., Fossorier M., Quya S., Vasić B.* Improved PEG Construction of Large Girth QC-LDPC Codes // Proc. 9th Int. Symp. on Turbo Codes & Iterative Information Processing (ISTC'2016). Brest, France. Sept. 5–9, 2016. P. 146–150.
11. *Hu X.-Y., Eleftheriou E., Arnold D.M.* Regular and Irregular Progressive Edge-Growth Tanner Graphs // IEEE Trans. Inform. Theory. 2005. V. 51. № 1. P. 386–398.
12. *Овинников А.А.* Способ идентификации циклов в графах Таннера LDPC кодов на основе пересечения коротких замкнутых структур в протографах // Цифровая обработка сигналов. 2016. № 4. С. 26–30.

Харин Алексей Владимирович
Заверткин Константин Николаевич
Овинников Алексей Анатольевич
Рязанский государственный радиотехнический университет им. В.Ф. Уткина,
факультет радиотехники и телекоммуникаций,
кафедра телекоммуникаций и основ радиотехники
kharin.a.v@tor.rsreu.ru
zavertkin.k.n@tor.rsreu.ru
ovinnikov.a.a@tor.rsreu.ru

Поступила в редакцию
05.07.2019
После доработки
08.05.2020
Принята к публикации
12.05.2020