

## ОБ ОДНОЙ КОМБИНАТОРНОЙ ЗАДАЧЕ ИЗ ТЕОРИИ СРАВНЕНИЙ

АЛЕКСАНДЕР РОСА (ALEXANDER ROSA), ШТЕФАН ЗНАМ (ŠTEFAN ZNÁM),  
Братислава

Профессору Йозефу Кауцкому к 70-летию со дня рождения

С задачами, решаемыми в этой работе, мы встретились на семинаре по теории графов при решении проблематики т. наз. циклических разложений полных графов с  $m = 2n + 1$  вершинами на окружности с  $n$  ребрами.

Пусть задано натуральное число  $n$ . Обозначим  $m = 2n + 1$ .

Будем говорить, что множество  $X = \{x_1, x_2, \dots, x_N\} \subset \{1, 2, \dots, 2n\}$ ,  $N \leq n$ , является множеством типа (\*), если выполняется

$$(1) \quad \sum_{i=1}^N x_i \equiv 0 \pmod{m},$$

$$(2) \quad x_i + x_j \not\equiv 0 \pmod{m} \quad \text{для всех } i, j \neq 1, \dots, N.$$

Пустое множество будем считать множеством типа (\*).

I. Обозначим  $i' = m - i$ . Очевидно, имеют место следующие утверждения:

- (а) Если  $X = \{x_1, \dots, x_N\}$  — множество типа (\*), то и  $X' = \{x'_1, \dots, x'_N\}$  — множество типа (\*);
- (б) Если  $X, Y$  — множества типа (\*),  $X \subset Y$ , то и  $Y - X$  является множеством типа (\*);
- (в) Если  $X = \{x_1, \dots, x_n\}$  — множество типа (\*), то в  $X$  содержится одно и только одно из чисел  $i, i'$  ( $1 \leq i \leq 2n$ ).

**Лемма.** Если  $A = \{a_1, \dots, a_n\}$ ,  $B = \{b_1, \dots, b_n\}$  — множества типа (\*), то и  $C = A \cap B$  — множество типа (\*).

**Доказательство.** Если  $C = \emptyset$  (очевидно, тогда  $B = A'$ ), то утверждение леммы выполнено. Пусть теперь  $C = \{c_1, c_2, \dots, c_p\}$ ,  $p \leq n$ .

Обозначим  $A - C = \{a_{i_1}, a_{i_2}, \dots, a_{i_k}\}$ ,  $\{i_1, i_2, \dots, i_k\} \subset \{1, 2, \dots, n\}$ . Согласно (в) имеем  $B - C = \{a'_{i_1}, a'_{i_2}, \dots, a'_{i_k}\}$ .

Так как по условию леммы  $A, B$  — множества типа (\*), то получим

$$(3) \quad \sum_{i=1}^p c_i + \sum_{v=1}^k a_{i_v} \equiv 0 \pmod{m},$$

$$(4) \quad \sum_{i=1}^p c_i + \sum_{v=1}^k a'_{i_v} \equiv 0 \pmod{m}.$$

После сложения (3) и (4) получим

$$2 \sum_{i=1}^p c_i + \sum_{v=1}^k (a_{i_v} + a'_{i_v}) \equiv 0 \pmod{m},$$

откуда

$$\sum_{i=1}^p c_i \equiv 0 \pmod{m},$$

что и требовалось доказать.

Пусть  $A = \{a_1, \dots, a_n\}$  — множество типа (\*). Обозначим через  $p_3^{(A)}, \dots, p_{n-3}^{(A)}$  число всех отличных друг от друга подмножеств типа (\*), множества  $A$  соответственно с тремя, четырьмя, ...,  $(n-3)$ -мя элементами.

Образуем сумму

$$\sum_{i=3}^{n-3} p_i^{(A)} = p_3^{(A)} + p_4^{(A)} + \dots + p_{n-4}^{(A)} + p_{n-3}^{(A)} = k(A).$$

Из (а) следует, что  $k(A) = k(A')$ .

**Теорема.** Пусть  $A = \{a_1, \dots, a_n\}$ ,  $B = \{b_1, \dots, b_n\}$  — множества типа (\*). Тогда имеет место:  $k(A) = k(B)$ .

**Доказательство.** Обозначим  $C = A \cap B$ . Если  $C = \emptyset$ , то  $B = A$  и утверждение теоремы выполнено. Пусть  $C = \{c_1, \dots, c_p\}$   $p < n$ . Обозначим

$$A - C = D = \{d_1, \dots, d_r\},$$

и согласно (в) будет

$$B - C = D' = \{d'_1, \dots, d'_r\}.$$

В новом обозначении будем иметь

$$A = \{c_1, \dots, c_p, d_1, \dots, d_r\},$$

$$B = \{c_1, \dots, c_p, d'_1, \dots, d'_r\}.$$

Покажем теперь, что каждому подмножеству типа (\*) множества  $A$  соответствует (хотя бы) одно подмножество типа (\*) множества  $B$ , причем двум разным таким подмножествам множества  $A$  соответствуют две разные такие подмножества множества  $B$ . Так как множества  $A, B$  можно поменять местами, то тем самым наша теорема будет доказана.

Подмножества типа (\*) множества  $A$  могут быть одного из четырех следующих видов:

- I.  $X_A = \{c_1, \dots, c_s\}$ ,  $1 \leq s \leq p$ ;  $\{i_1, i_2, \dots, i_s\} \subset \{1, 2, \dots, p\}$ ;
- II.  $X_A = \{d_1, \dots, d_t\}$ ,  $1 \leq t \leq r$ ;  $\{i_1, i_2, \dots, i_t\} \subset \{1, 2, \dots, r\}$ ;
- III.  $X_A = \{c_1, \dots, c_s, d_1, \dots, d_r\}$ ,  $1 \leq s < p$ ;  $\{i_1, \dots, i_s\} \subset \{1, 2, \dots, p\}$ ;
- IV.  $X_A = \{c_1, \dots, c_s, d_{j_1}, \dots, d_{j_t}\}$ ,  $1 \leq s \leq p$ ,  $1 \leq t < r$ ;  
 $\{i_1, i_2, \dots, i_s\} \subset \{1, 2, \dots, p\}$ ,  
 $\{j_1, j_2, \dots, j_t\} \subset \{1, 2, \dots, r\}$ .

Соответствующие подмножества множества  $B$  будут иметь в отдельных случаях следующий вид:

- I.  $X_B = \{c_1, \dots, c_s\}$ ;
- II.  $X_B = \{d'_1, \dots, d'_t\}$ ;
- III.  $X_B = \{c_1, \dots, c_s, d'_1, \dots, d'_r\}$ ;
- IV.  $X_B = \{c_1, \dots, c_s, d'_{j_1}, \dots, d'_{j_t}\}$ ,

$$\{j_{t+1}, \dots, j_r\} = \{1, 2, \dots, r\} - \{j_1, j_2, \dots, j_t\},$$

т.е. двум разным подмножествам типа (\*) множества  $A$  в самом деле соответствуют два разных подмножества множества  $B$ . Из (а) вытекает, что в случаях I., II., III. множество  $X_B$  — типа (\*). Покажем, что и в случае IV. множество  $X_B$  — типа (\*).

Очевидно, имеет место (ввиду (б) и ввиду леммы):

$$(5) \quad \sum_{i=1}^r d'_i \equiv 0 \pmod{m}.$$

Поскольку  $X_A = \{c_1, \dots, c_s, d_{j_1}, \dots, d_{j_t}\}$  — типа (\*), то

$$(6) \quad \sum_{\nu=1}^s c_{i_\nu} + \sum_{\nu=1}^t d_{j_\nu} \equiv 0 \pmod{m}.$$

После сложения (5) и (6) получим

$$(7) \quad \sum_{\nu=1}^s c_{i_\nu} + \sum_{\nu=1}^t (d_{j_\nu} + d'_{j_\nu}) + \sum_{\nu=t+1}^r d'_{j_\nu} \equiv 0 \pmod{m},$$

где

$$\{j_{t+1}, \dots, j_r\} = \{1, 2, \dots, r\} - \{j_1, j_2, \dots, j_t\}.$$

Из (7) следует

$$\sum_{\nu=1}^s c_{i_\nu} + \sum_{\nu=t+1}^r d'_{j_\nu} \equiv 0 \pmod{m},$$

т.е.  $X_B = \{c_1, \dots, c_s, d'_{j_1}, \dots, d'_{j_t}\}$  — типа (\*), ч. и т.д.

Доказанная теорема показывает, что сумма  $\sum_{i=3}^{n-3} p_i^{(A)} = k(n)$  зависит только от  $n$  и не зависит от выбранного множества  $A$ .

Примечание 1. Если отказаться от условия (2), т.е. если не требовать, чтобы выполнялось

$$x_i + x_j \not\equiv 0 \pmod{m},$$

то ни лемма, ни утверждение, аналогичное теореме, не будут справедливыми.

Выведем теперь двумя путями формулы для определения числа  $Q$  разных множеств типа (\*) с  $n$  элементами.

II. Обозначим через  $p_r(s)$  количество разбиений числа  $r$  на отличные друг от друга числа, не превосходящие  $s$ . Каждое из этих разбиений отнесем к одному из двух классов. В первый класс включим разбиения, не содержащие число  $s$ ; их количество равно, очевидно,  $p_r(s-1)$ . В второй класс включим разбиения, содержащие число  $s$ ; их количество равно количеству разбиений числа  $r-s$  на отличные друг от друга числа, не превосходящие  $s-1$ . Следовательно, для  $p_r(s)$  получаем следующее рекуррентное соотношение:

$$p_r(s) = p_r(s-1) + p_{r-s}(s-1),$$

$$\text{где } p_0(s) \stackrel{\text{def}}{=} 1, \quad p_r(s) \stackrel{\text{def}}{=} 0 \quad \text{для } r < 0.$$

Легко выводятся формулы, облегчающие вычисление  $p_r(s)$ :

$$p_r(s) = p_r(r) \quad \text{для } s > r,$$

$$(8) \quad p_{\frac{1}{2}(s+1)-r}(s) = p_r(s).$$

С помощью этих соотношений построена таблица 1.

Производящая функция для  $p_r(s)$  (см. [1]) будет

$$(1+x)(1+x^2) \dots (1+x^s) = \sum_{r=0}^{\frac{1}{2}(s+1)} p_r(s) x^r.$$

Пусть  $A = \{a_1, \dots, a_n\}$  — типа (\*). Сумму всех  $a_i$ , не превосходящих  $n$ , обозначим через  $a$ . Для  $a_i > n$  мы можем писать  $a_i = m - b_i$ , где  $b_i \leq n$ . Сумму всех  $b_i$  обозначим через  $b$ . Так как  $A$  — типа (\*), то получаем соотношения:

$$a \equiv b \pmod{m},$$

$$a + b = \frac{1}{2} n (n + 1).$$

Значит,

(9)  $2a \equiv \frac{1}{2}n(n+1) \pmod{m}$ .

При этом  $a$  должно удовлетворять условию

(10)  $0 < a \leq \frac{1}{2}n(n+1)$ .

Таблица 1

$r \backslash s$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2		1	1	1	1	1	1	1	1	1	1	1	1	1	1
3			1	2	2	2	2	2	2	2	2	2	2	2	2
4				1	2	2	2	2	2	2	2	2	2	2	2
5					1	2	3	3	3	3	3	3	3	3	3
6						1	2	3	4	4	4	4	4	4	4
7							1	2	3	4	5	5	5	5	5
8								1	2	3	4	5	6	6	6
9									1	2	3	4	5	6	7
10										1	2	3	4	5	6
11											1	2	3	4	5
12												1	2	3	4
13													1	2	3
14														1	2
15															1
16															
17															
18															
19															
20															
21															
22															
23															
24															
25															
26															
27															
28															
29															
30															
31															
32															
33															
34															
35															

Легко доказать и обратное:  $a_i$  удовлетворяют (2), (9), (10), то они удовлетворяют и (1).

Пусть  $a$  удовлетворяет (9), (10). Пусть  $x_1 + x_2 + \dots + x_k = a$ ,  $k \leq n$ , — некоторое разбиение  $a$  на отличные друг от друга числа, не превосходящие  $n$ . Каждому такому разбиению соответствует одно множество типа (\*) с  $n$  элементами, причем разбиениям отличных друг от друга чисел  $a$  или же разным разбиениям одного и того же  $a$  соответствуют отличные друг от друга множества.

Следовательно, для  $Q(n)$  получаем формулу

$$(11) \quad Q(n) = \sum p_a(n),$$

где  $a$  пробегает все решения сравнения (9), удовлетворяющие неравенству (10).

Примечание 2. Соотношение (8) может быть использовано для упрощения вычислений  $Q(n)$ , а именно, в (11) следует  $p_a(n)$  для  $a > \frac{1}{4}n(n+1)$  заменить на  $p_{\frac{1}{2}n(n+1)-a}(n)$ .

III. Обозначим через  $P_r(s)$  количество разных разбиений числа  $r$  на отличные друг от друга нечетные числа, не превосходящие  $s$  ( $s$  — нечетное). Покажем, что для  $P_r(s)$  имеет место рекуррентное соотношение

$$P_r(s) = P_r(s-2) + P_{r-s}(s-2)$$

(при этом  $P_0(s) \stackrel{\text{def}}{=} 1$ ).

Каждое из разбиений числа  $r$  на отличные друг от друга нечетные числа, не превосходящие  $s$ , отнесем к одному из двух классов. В первый класс включим разбиения, в которых не фигурирует число  $s$ ; таких разбиений  $P_r(s-2)$ . Во второй класс включим разбиения, в которых содержится число  $s$ ; таких разбиений имеется ровно столько, сколько имеется разбиений числа  $r-s$  на нечетные числа, не превосходящие  $s-2$ , т.е.  $P_{r-s}(s-2)$ .

Для составления таблицы чисел  $P_r(s)$  используем еще следующие соотношения, справедливость которых легко проверяется:

$$P_r(s) = 0 \quad \text{для} \quad r > \left(\frac{s+1}{2}\right)^2,$$

$$P_r(s) = P_r(r) \quad \text{для} \quad s > r, r - \text{нечетное},$$

$$P_r(s) = P_r(r-1) \quad \text{для} \quad s > r, r - \text{четное},$$

$$(12) \quad P_r(s) = P_{\left(\frac{s+1}{2}\right)^2 - r}(s).$$

В таблице 2 приведены первые значения  $P_r(s)$ .  
 Производящая функция для  $P_r(s)$  будет

$$(1+x)(1+x^3)\dots(1+x^s) = \sum_{r=0}^{\left(\frac{s+1}{2}\right)} P_r(s)x^r \quad (s - \text{нечетное}).$$

Таблица 2

$P_r(s)$ $r \backslash s$	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2		0	0	0	0	0	0	0	0	0	0	0	0	0	0
3		1	1	1	1	1	1	1	1	1	1	1	1	1	1
4		1	1	1	1	1	1	1	1	1	1	1	1	1	1
5			1	1	1	1	1	1	1	1	1	1	1	1	1
6			1	1	1	1	1	1	1	1	1	1	1	1	1
7			0	1	1	1	1	1	1	1	1	1	1	1	1
8			1	2	2	2	2	2	2	2	2	2	2	2	2
9			1	1	2	2	2	2	2	2	2	2	2	2	2
10				1	2	2	2	2	2	2	2	2	2	2	2
11				1	1	2	2	2	2	2	2	2	2	2	2
12				1	2	3	3	3	3	3	3	3	3	3	3
13				1	2	2	3	3	3	3	3	3	3	3	3
14				0	1	2	3	3	3	3	3	3	3	3	3
15				1	2	3	3	4	4	4	4	4	4	4	4
16				1	2	3	4	5	5	5	5	5	5	5	5
17					2	3	4	4	5	5	5	5	5	5	5
18					1	2	3	4	5	5	5	5	5	5	5
19					1	3	4	5	5	6	6	6	6	6	6
20					1	3	4	5	6	7	7	7	7	7	7
21					1	3	5	6	7	7	8	8	8	8	8
22					1	2	4	5	6	7	8	8	8	8	8
23					0	2	4	6	7	8	8	9	9	9	9
24					1	3	5	7	8	9	10	11	11	11	11
25					1	2	5	7	9	10	11	11	12	12	12
26						2	4	6	8	9	10	11	12	12	12
27						2	4	7	9	11	12	13	13	14	14
28						2	5	8	10	12	13	14	15	16	16
29						1	4	7	10	12	14	15	16	16	17
30						1	4	7	10	12	14	15	16	17	18
31						1	3	7	10	13	15	17	18	19	19
32						1	4	8	12	15	17	19	20	21	22
33						1	4	7	12	15	18	20	22	23	24
34						0	3	7	11	15	18	20	22	23	24
35						1	3	7	11	16	19	22	24	26	27

Вычислим теперь  $Q(n)$  с помощью чисел  $P_r(s)$ .

Для множества  $A = \{a_1, \dots, a_n\}$  типа (\*) имеет место:

$$\binom{n+1}{2} \leq \sum_{i=1}^n a_i \leq \frac{1}{3} (3n+1),$$

$$\sum_{i=1}^n a_i = k \cdot m,$$

где

$$\frac{\binom{n+1}{2}}{m} \leq k \leq \frac{\binom{3n+1}{2}}{3m}.$$

Если рассматривать теперь все отличные друг от друга множества типа (\*) с  $n$  элементами, то  $k$  будет принимать значения от  $q_0 = [\frac{1}{4}n] + 1$  до  $q_1 = [\frac{1}{4}(3n-1)]$ :

$$k_1 = q_0; \quad k_2 = q_0 + 1; \quad \dots; \quad k_q = q_1; \quad q = q_1 - q_0 + 1.$$

Легко проверяется, что при этом

$$(13) \quad k_i + k_{q-i+1} = n.$$

Образует таблицу, в первой строке которой будут находиться числа от 1 до  $n$ , во второй — числа от  $n+1$  до  $2n$ , записанные в обратном порядке, а в третьей — разности между числом во второй строке и лежащим над ним числом в первой строке:

$$\begin{array}{cccccccc} 1, & 2, & 3, & \dots, & n-2, & n-1, & n & \\ 2n, & 2n-1, & 2n-2, & \dots, & n+3, & n+2, & n+1 & \\ 2n-1, & 2n-3, & 2n-5, & \dots, & 5, & 3, & 1 & \end{array}$$

Сумма чисел в первой строке равна  $\binom{n+1}{2}$ .

Обозначим  $v_i = m \cdot k_i - \binom{n+1}{2}$ , где  $i = 1, \dots, q$ .

Если теперь заменить некоторые числа первой строки соответствующими (т.е. лежащими под ними) числами второй строки так, чтобы сумма чисел первой строке увеличилась на  $v_i$ , то элементы первой строки будут образовывать множество типа (\*). Если это сделать всевозможными способами (и для всех  $i = 1, \dots, q$ ), то получим все отличные друг от друга множества типа (\*) с  $n$  элементами. Поскольку в третьей строке фигурируют только нечетные числа, не превосходящие  $2n-1$ , то таких способов



будет ровно столько, сколько имеется разных разбиений чисел  $v_i$  ( $i = 1, \dots, q$ ) на отличные друг от друга нечетные числа, не превосходящие  $2n - 1$ :

$$(14) \quad Q(n) = \sum_{i=1}^q P_{v_i}(2n - 1).$$

Примечание 3. С помощью соотношений (12), (13) вычисления по формуле (14) могут быть упрощены так, что числа  $P_{v_i}(2n - 1)$  для  $i > \frac{1}{2}q$  заменяются числами  $P_{v_{q-i+1}}(2n - 1)$ .

IV. Приведем еще один способ нахождения числа  $Q(n)$ .

В части I. было доказано, что значение  $k(n)$  зависит только от  $n$  и не зависит от выбранного множества  $A$ .

Выберем произвольное множество  $A = \{a_1, \dots, a_n\}$  типа (\*). Из этого множества мы можем образовать  $k(n)$  новых множеств типа (\*) с  $n$  элементами следующим образом: Пусть  $\{a_{i_1}, \dots, a_{i_k}\}$  — одно из  $k(n)$  подмножеств типа (\*) множества  $A$ . Если в исходном множестве  $A$  заменить элементы этого подмножества элементами подмножества  $\{a'_{i_1}, \dots, a'_{i_k}\}$ , где  $a'_{i_j} = m - a_{i_j}$ , и остальные элементы оставить неизменными, то получим новое множество  $A^+$ , которое будет (согласно I.) также множеством типа (\*). Если этот прием проделать для всех  $k(n)$  подмножеств типа (\*) множества  $A$ , то получим систему  $k(n)$  новых множеств типа (\*) с  $n$  элементами. Присоединим еще к этой системе исходное множество  $A$  и множество  $A' = \{a'_1, \dots, a'_n\}$ . Мы получим систему  $\mathfrak{N}$  всех отличных друг от друга множеств типа (\*) с  $n$  элементами.

Докажем последнее утверждение. Очевидно, все множества системы  $\mathfrak{N}$  отличны друг от друга. Предположим, что существует множество  $\bar{A}$  типа (\*) с  $n$  элементами, не принадлежащее системе  $\mathfrak{N}$ . Образует пересечение  $A \cap \bar{A}$ . Если  $A \cap \bar{A} = \emptyset$ , то  $\bar{A} = A'$ , что противоречит предположению о том, что  $\bar{A}$  не принадлежит  $\mathfrak{N}$ . Если же  $A \cap \bar{A} = A_1 = \{a_{i_1}, \dots, a_{i_k}\}$ , то  $A_1$  является одним из  $k(n)$  подмножеств типа (\*) множества  $A$ . Но это означает, что мы получили множество  $\bar{A}$  описанным выше образом из подмножества  $A - A_1$ , которое является (согласно части I.) также одним из  $k(n)$  подмножеств типа (\*) множества  $A$ . Мы получили противоречие, так как предполагали, что  $\bar{A}$  не принадлежит  $\mathfrak{N}$ . Утверждение доказано.

Тем самым мы вывели соотношение

$$Q(n) = k(n) + 2,$$

исходя из которого мы можем записать формулу для вычисления  $k(n)$ :

$$(15) \quad k(n) = \sum p_a(n) - 2$$

или

$$(16) \quad k(n) = \sum_{i=1}^n P_{v_i}(2n-1) - 2.$$

В таблице 3 приведено несколько первых значений  $Q(n)$  и  $k(n)$ .

Таблица 3

$n$	3	4	5	6	7	8	9	10	11	12	13	14	15
$Q(n)$	2	2	2	4	8	16	26	48	90	164	302	564	1058
$k(n)$	0	0	0	1, 2	6	14	24	46	88	162	300	562	1056

ЛИТЕРАТУРА

[1] Hardy G. H., Wright E. M., *An introduction to the theory of numbers*, Oxford 1938.

2703 ✓ Поступило 26. 2. 1964.

ČSAV, Kabinet matematiky  
Slovenskej akadémie vied,  
Bratislava

Katedra matematiky a deskriptívnej geometrie  
Chemickej fakulty  
Slovenskej vysokej školy technickej,  
Bratislava

A COMBINATORIAL PROBLEM OF THE THEORY OF CONGRUENCES

Alexander Rosa, Štefan Znám

Summary

Let  $n$  be a natural number,  $m = 2n + 1$ . The set  $X = \{x_1, \dots, x_n\} \subset \{1, \dots, 2n\}$   $N \leq n$  is said to be of the type (\*), if (1) holds and if (2) holds for all  $i, j = 1, \dots, N$ .

If  $A = \{a_1, \dots, a_n\}$  is of the type (\*), then  $p_i^{(A)}$  denotes the number of subsets of the type (\*) with  $i$  elements, of the set  $A$ .

In part I the following theorem is proved:

The sum  $\sum_{i=3}^{n-3} p_i^{(A)}$  does not depend on the choice of the set  $A$ , but only on the number of its elements (this sum is denoted by  $k(n)$ ).

In part II  $Q(n)$ , the number of different sets of the type (\*) with  $n$  elements is determined, with the help of the numbers  $p(s)$ , where  $p(s)$  denotes the number of partitions of the number  $r$  into mutually different numbers not exceeding  $s$  (formula (11)).

In part III  $Q(n)$  is determined with the help of the numbers  $P_r(s)$ , where  $P_r(s)$  denotes the number of partitions of  $r$  into mutually different odd numbers not exceeding  $s$  (formula (14)).

In part IV the relation

$$Q(n) = k(n) + 2$$

is derived.

This problem has arisen from the problem of cyclic decompositions of the complete graph with  $m = 2n + 1$  vertices into circuits with  $n$  edges each.