А.Г.Дьячков

Теория информации

§ 4. Модель статического поиска А. Реньи

Содержание

4.1 Определения, обозначения, постановка задачи

Пусть $X = \Big(\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(M)\Big) = \|x_n(m)\|,\ n = \overline{1,N},\ m = \overline{1,M},$ — двоичный код объема M, длины N. Зафиксируем целое число $k,\ 1 \le k \le M/2$. Обозначим через

$$\mathbf{x}(m) = \Big(x_1(m), \ldots, x_N(m)\Big), \quad m = \overline{1,M},$$

столбцы (кодовые слова), а через

$$\mathbf{x}_n = \Big(x_n(1), x_n(2), \ldots, x_n(M)\Big), \quad n = \overline{1,N},$$

строки этого кода. Пусть символы

$$|\mathbf{x}(m)| \triangleq \sum_{n=1}^{N} x_n(m), \quad m = \overline{1,M}, \quad \text{и} \quad |\mathbf{x}_n| \triangleq \sum_{m=1}^{M} x_n(m), \quad n = \overline{1,N}$$

обозначают число единиц (вес) m-ого кодового слова и n-ой строки.

Определение 1. Код X называется (M,k)*–планом* (или *разделяющим планом статического поиска в модели А.Реньи*), если для любого $n = \overline{1,N}$ вес строки $|\mathbf{x}_n| = k$, а все столбцы $\mathbf{x}(m),\ m = \overline{1,M}$ отличны друг от друга.

Определение 2. Если строки X удовлетворяют условию: $|\mathbf{x}_n| \le k,\ \ n = \overline{1,N}$, а все столбцы $\mathbf{x}(m),\ m = \overline{1,M}$ отличны друг от друга, то код X называется $(M, \le k)$*–планом.*

Обозначим через $N(M,k)$ или через $N(M, \le k)$ минимально возможное число строк в соответствующем разделяющем плане. Наша цель — построение границ и исследование асимптотики этих характеристик. Имеет место

Лемма 1. *Если* $1 \le k \le M/2$, *то* $N(M,k) = N(M, \le k)$.

Доказательство. Пусть $k' \le k$ и

$$\mathbf{x}_n = \Big(\underbrace{11\ldots1}_{k'}, \overbrace{\underbrace{00\ldots0}_{k-k'}, 00\ldots0}^{M-k'}\Big)$$

произвольная строка $(M, \leq k)$–плана, в которой k' единиц, $k' < k$. Достаточно доказать, что в строке $\mathbf{x}_n$ найдется $k - k'$ нулевых позиций, которые можно заменить на единичные и при этом сохранится свойство различия столбцов. Заметим, что при замене *двух* нулевых позиций строки $\mathbf{x}_n$ на единичные *вновь получившиеся два столбца не совпадают между собой,* а потому не могут совпасть с одним и тем же из k' столбцов, которые имеют в $\mathbf{x}_n$ единицу. Поэтому число нулевых позиций $\mathbf{x}_n$, которые нельзя заменять на единичные без потери свойства различия, заведомо $\leq k'$. Следовательно, число "хороших"нулевых позиций, которые можно заменять на единичные без потери свойства различия заведомо $\geq M - k' - k' = M - 2k' \geq k - k'$, где последнее неравенство верно, если $k + k' \leq M$. Поскольку при $k' < k \leq M/2$ имеем $k + k' \leq M$, то лемма 1 доказана.

В дальнейшем, не нарушая общности, мы будем рассматривать лишь величину $N(M,k)$ и соответствующие конструкции оптимальных (M,k)-планов при $1 \leq k \leq M/2$.

Задача 4.1. Докажите, что при $1 \leq k \leq M/2$ величина

$$N(M,k) \geq \lceil \log_2 M \rceil,$$

где при $k = \lfloor M/2 \rfloor$ достигается знак равенства.

Указание. При $2^{N-1} < M \leq 2^N$ для доказательства достижения границы $\lceil \log_2 M \rceil = N$ рассмотрите код $X = \Big(\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(2^N)\Big)$ объема 2^N, длины N, где кодовое слово $\mathbf{x}(m)$ является двоичным разложением числа $m - 1$, $m = \overline{1, 2^N}$. Докажите, что код $X' = \Big(\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(M)\Big)$ будет $(M, \leq \lfloor M/2 \rfloor)$–планом длины $N = \lceil \log_2 M \rceil$.

4.2 Обратная теорема Шеннона

Символом $h(u) \triangleq -u \log_2 u - (1-u)\log_2(1-u)$, $0 \leq u \leq 1$, будем обозначать двоичную энтропию. Имеет место

Лемма 2. *Пусть $1 \leq k \leq M/2$ и существует (M,k)–план X длины N. Тогда справедливо неравенство*

$$N \cdot h\left(\frac{k}{M}\right) \geq \log_2 M, \quad \text{т.е.} \quad N(M,k) \geq \frac{\log_2 M}{h(k/M)}.$$

Пусть $k \triangleq \lceil Mp \rceil$, где $0 < p < 1/2$. Тогда

$$\frac{k}{M} = \frac{\lceil Mp \rceil}{M} \leq p + \frac{1}{M}, \quad \text{т.е.} \quad h\left(\frac{k}{M}\right) \leq h\left(p + \frac{1}{M}\right),$$

и лемма 2 означает, что справедлива

Теорема 1. (Обратная теорема Шеннона). *Для любого фиксированного p, $0 < p < 1/2$, и $M \to \infty$, число*

$$N(M, \lceil Mp \rceil)) \geq \frac{\log_2 M}{h(p)}\,(1 + o(1)),$$

что равносильно асимптотическому неравенству

$$\frac{\log_2 M}{N(M, \lceil Mp \rceil))} \leq h(p)(1 + o(1)).$$

Доказательство леммы 2. Обозначим через ξ случайную величину с равномерным распределением на множестве $[M] \triangleq \{1, 2, \ldots, M\}$, т.е.

$$\Pr\{\xi = m\} \triangleq M^{-1}, \quad m = \overline{1, M}.$$

Пусть $X = (\mathbf{x}(1), \ldots, \mathbf{x}(M))$ — произвольный (M, k)–план длины N. Для энтропии Шеннона векторной случайной величины $\mathbf{x}(\xi) \triangleq (x_1(\xi), x_2(\xi), \ldots, x_N(\xi))$ имеем

$$H(\mathbf{x}(\xi)) \triangleq -\sum_{m=1}^{M} \Pr\{\mathbf{x}(\xi) = \mathbf{x}(m)\} \log_2 \Pr\{\mathbf{x}(\xi) = \mathbf{x}(m)\} = \log_2 M.$$

С другой стороны, по свойству субаддитивности энтропии Шеннона (см.**§5**)

$$\log_2 M = H(\mathbf{x}(\xi)) \le \sum_{n=1}^{N} H(x_n(\xi)) = \sum_{n=1}^{N} h\left(\frac{|\mathbf{x}_n|}{M}\right),$$

где учли, что двоичная случайная величина $x_n(\xi)$ принимает значения 0, 1 с вероятностями

$$x_n(\xi) = \begin{pmatrix} 0 & 1 \\ \frac{M - |\mathbf{x}_n|}{M} & \frac{|\mathbf{x}_n|}{M} \end{pmatrix}.$$

По определению (M, k)-плана X вес его n-ой строки $|\mathbf{x}_n| = k$ для любого $n = \overline{1, N}$. Поэтому

$$\log_2 M = H(\mathbf{x}(\xi)) \le Nh\left(\frac{k}{M}\right).$$

Лемма 2 доказана.

4.3 Прямая теорема Шеннона

Пусть $1 \le w \le t - 1$ – произвольные целые числа.

Лемма 3. *Существует (M, k)-план X длины N с параметрами*

$$N = t, \quad M = \binom{t}{w}, \quad k = \binom{t-1}{w-1}.$$

Доказательство леммы 3. Искомый код X строится как двоичная $N \times M$-матрица, имеющая $N = t$ строк $\mathbf{x}_n$ и состоящая из всех $M = \binom{t}{w}$ столбцов (кодовых слов) $\mathbf{x}(m)$ длины t и веса $|\mathbf{x}(m)| = w$. Все строки $\mathbf{x}_n$ этой матрицы имеют один и тот же вес $|\mathbf{x}_n| = \binom{t-1}{w-1}$, равный числу кодовых слов кода X, содержащих в фиксированной позиции единичный символ.

Лемма 3 доказана.

Задача 4.2. Докажите, что при $N \to \infty$ и произвольном фиксированном p, $0 < p < 1/2$, справедливы асимптотические равенства

$$\frac{\log_2 M}{N} = \frac{\log_2 \binom{N}{\lceil Np \rceil}}{N} = h(p)(1 + o(1)), \qquad \frac{k}{M} = \binom{N-1}{\lceil Np \rceil - 1} \Big/ \binom{N}{\lceil Np \rceil} = p(1 + o(1)).$$

Из результата задачи 4.2 вытекает

Теорема 2. (Прямая теорема Шеннона). *Для любого фиксированного p, $0 < p < 1/2$, и $M \to \infty$, отношение*

$$\frac{\log_2 M}{N(M, \lceil Mp \rceil))} \geq h(p)(1 + o(1)),$$

что равносильно асимптотическому неравенству

$$N(M, \lceil Mp \rceil)) \leq \frac{\log_2 M}{h(p)} \, (1 + o(1)).$$

Из теорем 1 и 2 получаем

Следствие. *Для любого фиксированного p, $0 < p < 1/2$, и $M \to \infty$ справедливо асимптотическому равенство*

$$N(M, \lceil Mp \rceil)) \; = \; \frac{\log_2 M}{h(p)} \, (1 + o(1)).$$

4.4 Построение (M, k)-планов

В данном разделе будут описаны некоторые конструкции оптимальных (M, k)-планов.

Задача 4.3 Докажите, что при фиксированном $k = 1, 2, \ldots$ и $M \to \infty$ справедиво асимптотическое равенство

$$h\left(\frac{k}{M}\right) = k \, \frac{\log_2 M}{M} \, \left(1 + o(1)\right).$$

Это означает, что в данных условиях нижняя граница леммы 2 для $N(M, k)$ равносильна асимптотическому неравенству

$$N(M, k) \geq \frac{M}{k} \left(1 + o(1)\right).$$

Следующий результат показывает, что в условиях $k \ll M$ границу леммы 2 можно *уточнить примерно в два раза.*

Теорема 3. *Для любого* $1 \leq k < M$ *число*

$$N(M, k) \geq \left\lceil \frac{2(M-1)}{k+1} \right\rceil. \tag{1}$$

Доказательство теоремы 3. Рассмотрим произвольный (M, k)-план X длины N. Пусть $n = \overline{0, N}$, а C_n обозначает число столбцов X, которые имеют вес n. Тогда

$$C_0 \leq 1; \quad C_1 \leq N; \quad \sum_{n=2}^{N} C_n = M - C_0 - C_1. \tag{2}$$

Далее, в силу (2), имеем

$$\begin{aligned} Nk = \sum_{n=0}^{N} nC_n = C_1 + \sum_{n=2}^{N} nC_n \geq C_1 + 2\sum_{n=2}^{N} C_n = C_1 + 2(M - C_0 - C_1) = \\ = 2(M - C_0) - C_1 \geq 2(M-1) - N. \end{aligned}$$

Следовательно, $N(k+1) \geq 2(M-1)$.

Теорема 3 доказана.

Обозначим через $M(N,k)$ *максимально возможное* число кодовых слов кода X длины N, у которого все столбцы различны, а вес каждой строки равен k. Из вывода теоремы 3 следует, что

$$M(N,k) \leq \left\lfloor \frac{1}{2} N(k+1) \right\rfloor + 1, \quad M(2n,k) \leq n(k+1) + 1, \tag{3}$$

где оптимальный (M,k)-план X, на котором в (1) и (3) достигается знак равенства, должен иметь параметры

$$C_0 = 1; \quad C_1 = N; \quad C_n = 0, \quad n = \overline{3, N}.$$

Это означает, что справедлива

Лемма 4. *В оптимальном, т.е. достигающем границ* (1) *и* (3), (M,k)*-плане* X *длины* N *должен быть один нулевой столбец,* N *различных столбцов, содержащих по одной единице, попарно различные столбцы веса* 2 *и не должно содержаться столбцов веса* ≥ 3.

4.4.1 Конструкции оптимальных (M,k)-планов, основанные на q-ных однородных разделяющих матрицах

Имеет место

Лемма 5. *Зафиксируем произвольное целое число* $k = 2, 3, \ldots$. *Для любого целого числа* $q \geq k-1$ *существует* (M,k)*-план* X *длины* N, *параметры которого задаются соотношениями*

$$N = 2q, \quad M = 1 + 2q + q(k-1) = 1 + q(k+1), \quad q = k-1, k, k+1, \ldots.$$

Из леммы 5 и теоремы 3 вытекает

Теорема 4. *Для любого целого числа* $q \geq k-1$ *величина*

$$M(2q,k) = 1 + q(k+1).$$

Доказательство леммы 5. В силу леммы 4, для вывода леммы 5 достаточно построить двоичную $(2q \times q(k-1))$-матрицу, все $q(k-1)$ столбцов которой различны и имеют вес 2, а каждая из $2q$ строк содержит ровно $k-1$ единицу.

Введем q-ный алфавит $\mathbf{A} \triangleq \{1, 2, \ldots, q\}$. Будем говорить, что q-ная $(2 \times q(k-1))$-матрица $B = \|b_j(u)\|$, $b_j(u) \in \mathbf{A}$, состоящая из двух строк и $q(k-1)$ столбцов

$$\mathbf{b}_j \triangleq (b_j(1), b_j(2), \ldots, b_j(q(k-1))),\ j = 1, 2, \qquad \mathbf{b}(u) \triangleq (b_1(u), b_2(u)),\ u = 1, 2, \ldots, q(k-1).$$

является *однородной*, если каждый q-ный символ $a \in \mathbf{A}$ встречается ровно $k-1$ раз в каждой из ее двух строк. Матрицу B назовем *разделяющей*, если все ее $q(k-1)$ столбцов отличны друг от друга.

Каждый q-ный элемент $a \in \mathbf{A}$ матрицы B заменим на двоичный столбец длины q, который содержит единицу на a-ой позиции и нули на остальных $q-a$ позициях, т.е.

$$a \quad \Longleftrightarrow \quad (\underbrace{0,0,\ldots,0}_{(a-1)\text{ раз}},1,\underbrace{0,0,\ldots,0}_{(q-a)\text{ раз}}).$$

Нетрудно понять, что в результате такого преобразования из однородной разделяющей матрицы B получается искомая двоичная $(2q\times q(k-1))$-матрица, все $q(k-1)$ столбцов которой различны и имеют вес 2, а каждая из $2q$ строк содержит ровно $k-1$ единицу.

Для построения однородной разделяющей матрицы B мы воспользуемся двоичной характеристической $(q\times q)$-матрицей $C=\|c_i(j)\|$, $i=1,2,\ldots q$, $j=1,2,\ldots q$, которая взаимно - однозначно связана с q-ной разделяющей матрицей $B=(\mathbf{b}(1),\mathbf{b}(2),\ldots,\mathbf{b}(q(k-1))$ следующим образом

$$c_i(j) \triangleq \begin{cases} 1, & \text{если в } B \text{ существует столбец } \mathbf{b}(u)=(i,j),\\ 0, & \text{противном случае.}\end{cases}$$

Очевидно, что матрица B является однородной и разделяющей тогда и только тогда, когда в ее характеристической матрице вес каждой строки $\mathbf{c}_i \triangleq (c_i(1),c_i(2),\ldots,c_i(q))$ и вес каждого столбца $\mathbf{c}(j) \triangleq (c_1(j),c_2(j),\ldots,c_q(j))$ совпадают и равны $k-1$. Нетрудно понять, что такому условию удовлетворяют *циркулянтные* матрицы, определяемые следующим образом:

- первая строка $\mathbf{c}_1=(c_1(1),c_1(2),\ldots,c_1(q))$ циркулянтной матрицы C является произвольной двоичной последовательностью длины q и веса $k-1\le q$,

- i-ая $i=2,3,\ldots,q$ строка $\mathbf{c}_i \triangleq (c_i(1),c_i(2),\ldots,c_i(q))$ является *циклическим сдвигом* $(i-1)$-ой строки $\mathbf{c}_{i-1} \triangleq (c_{i-1}(1),c_{i-1}(2),\ldots,c_{i-1}(q))$, т.е.

$$c_i(j) \triangleq \begin{cases} c_{i-1}(q), & \text{если } j=1,\\ c_{i-1}(j-1), & \text{если } j=2,3,\ldots,q.\end{cases}$$

Лемма 5 доказана.

Следующий пример иллюстрирует метод построения (M,k)-плана X, основанный на методе доказательства леммы 5.

Пример. Пусть $k \triangleq 3$, $q \triangleq 3 \ge k-1=2$. Тогда

$$q(k-1)=6, \quad N=2q=6, \quad M=1+2q+q(k-1)=13.$$

Выберем циркулянтную (3×3)-матрицу C в виде

$$C \triangleq \begin{pmatrix} 1 & 1 & 0\\ 0 & 1 & 1\\ 1 & 0 & 1\end{pmatrix}.$$

Этой характеристической двоичной матрице соответствует троичная однородная разделяющая (2×6)-матрица

$$B = \begin{pmatrix} 1 & 1 & 2 & 2 & 3 & 3 \\ 1 & 2 & 2 & 3 & 1 & 3 \end{pmatrix},$$

которая задает $(13, 3)$-план X длины 6:

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

4.4.2 Конструкции оптимальных (M, k)-планов, основанные на непересекающихся разбиениях конечного множества

Имеет место следующая комбинаторная

Лемма 6. *Все $\binom{2n}{2} = n(2n-1)$ различных 2-подмножеств $2n$-множества можно разбить на $2n-1$ групп, где каждая группа содержит n попарно непересекающихся 2-подмножеств, образующих разбиение $2n$-множества. Другими словами, среди всех $(2n-1)!! = (2n-1)(2n-3) \cdot \ldots \cdot 3 \cdot 1$ разбиений $2n$-множества на 2-подмножества можно выделить максимально возможное число $2n-1$ непересекающихся разбиений.*

Каждое 2-подмножество $2n$-множества можно идентифицировать соответствующим двоичным столбцом (словом) длины $2n$, имеющим вес 2. Всего таких столбцов $C_{2n}^2 = n(2n-1)$. Каждое разбиение $2n$-множества на n 2-подмножеств идентифицируется соответствующей $(2n \times n)$ -матрицей A из 0 и 1, все $2n$ строк которой имеют вес 1, а все n столбцов — вес 2. Пусть $A_1, A_2, \ldots, A_{2n-1}$ — матрицы, идентифицирующие попарно непересекающиеся разбиения, которые можно выделить согласно лемме 6. Утверждение леммы 6 означает, что множество D_{2n} всех $n(2n-1)$ двоичных столбцов длины $2n$ веса 2 можно записать в виде

$$D_N = D_{2n} = (A_1, A_2, \ldots, A_{2n-1}) = (A_1, A_2, \ldots, A_{N-1})$$

Доказательство леммы 6. Мы ограничимся построением представления

$$D_{2n} = (A_1, A_2, \ldots, A_{2n-1})$$

когда $2n = 2^m, \ m = 1, 2, \ldots$. При рекуррентной процедуре этого построения используется следующая операция циклического сдвига столбцов матрицы $X \Rightarrow X'$:

$$X = (\mathbf{x}(1), \ldots, \mathbf{x}(t)) \Rightarrow X' \triangleq (\mathbf{x}(t), \mathbf{x}(1), \ldots, \mathbf{x}(t-1))$$

Различные t циклических сдвигов обозначим символами $X^{(i)}, \ i = \overline{1,t}; \quad X^{(1)} \triangleq X; \quad X(i) = \left(X^{(i-1)}\right)', \ i = \overline{2,t}$. Будем использовать также символ $E_n = \|e_i(j)\|, \ i = \overline{1,n}, \ j = \overline{1,n}$ для обозначения единичной $(n \times n)$-матрицы, т.е. $e_{ij} = 0, \ i \neq j; \quad e_{ij} = 1, \ i = j$.

Пусть построено представление

$$D_{2^m} = (A_1, A_2, \ldots, A_{2^m-1}) \sim \left(2^m \times 2^{m-1}(2^m - 1)\right),$$

где A_i — $(2^m \times 2^{m-1})$-матрицы, со столбцами веса 2 и строками веса 1, и для $i \neq j$ матрицы A_i и A_j не имеют общих столбцов.

Рекуррентный переход:

$$D_{2^m} \Rightarrow D_{2^{m+1}} = (\widetilde{A}_1, \widetilde{A}_2, \ldots, \widetilde{A}_{2^m}; B_1, B_2, \ldots, B_{2^m-1});$$

$$\widetilde{A}_i = \begin{pmatrix} E_{2^m} \\ E_{2^m}^{(i)} \end{pmatrix}; \quad B_i = \begin{pmatrix} A_i & 0 \\ 0 & A_i \end{pmatrix} \sim \left(2^{m+1} \times 2^m\right); \quad i = \overline{1, 2^m - 1}$$

Начало: $m = 1 \Rightarrow D_2 = A_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

Первый шаг: $m = 2 \Rightarrow D_4 =$

$$= \left(\begin{array}{cc|cc|cc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{c|c|cc} E_2 & E_2 & A_1 & 0 \\ E_2 & E_2^{(2)} & 0 & A_1 \end{array}\right) = \left(\begin{array}{c|c|c} \widetilde{A}_1 & \widetilde{A}_2 & B_1 \end{array}\right).$$

Второй шаг: $m = 3 \Rightarrow D_8 =$

$$= \left(\begin{array}{c|c|c|c|cc|cc|cc} E_4 & E_4 & E_4 & E_4 & \widetilde{A}_1 & 0 & \widetilde{A}_2 & 0 & B_1 & 0 \\ E_4 & E_4^{(2)} & E_4^{(3)} & E_4^{(4)} & 0 & \widetilde{A}_1 & 0 & \widetilde{A}_2 & 0 & B_1 \end{array}\right).$$

Лемма 6 доказана.

Замечание. Пример способа построения представления D_{2n}, когда $2n \neq 2^m$, покажем для частного случая $n = 3, \quad N = 2n = 6, \quad 2n - 1 = 5$:

$$D_6 = \begin{array}{|ccc|ccc|ccc|ccc|ccc|} \hline 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ \hline \end{array}$$

Общее решение задачи построения оптимальных (M, k)-планов дано в работе: *Лузгин В.Н.* "Разделяющие системы разбиений конечного множества". Комбинаторный анализ. М.: Изд-во МГУ, 1980. Вып. 5, с. 39-45.

Из свойств матриц $A_i, \ i = \overline{1, 2n - 1}$, вытекает

Лемма 7. *Пусть $n = 1, 2, \ldots$. Если $N = 2n$ и $k \leq 2n = N$, то матрица*

$$X = (\mathbf{0}\ E_{2n}\ A_1\ A_2\ \ldots\ A_{k-1})$$

является (M, k)-планом длины $N = 2n$ и объема

$$M = 1 + 2n + (k - 1)n = 1 + n(k + 1) = 1 + \frac{N}{2}(k + 1). \tag{4}$$

Сравнение границ (3) и (4) показывает, что справедлива

Теорема 5. *Если $k \leq 2n$, то $M(2n, k) = n(k + 1) + 1$.*

Эта теорема существенно расширяет класс конструкций оптимальных (M, k)-планов из теоремы 4, основанных на q-ных однородных разделяющих матрицах.