Е. Е. Маренич, Сравнения по простому модулю для числа $(0,1)$-матриц,
Дискрет. матем., 1990, том 2, выпуск 3, 153–157

https://www.mathnet.ru/dm879

Дискретная математика

том 2 выпуск 3 * 1990

УДК 519.1

СРАВНЕНИЯ ПО ПРОСТОМУ МОДУЛЮ ДЛЯ ЧИСЛА (0, 1)-МАТРИЦ

Маренич Е. Е.

Пусть B — такое множество (0, 1)-матриц порядка $n\times n$, что если $M\in B$ и M' получена из M произвольной перестановкой строк и столбцов, то $M'\in B$. В работе для простых p найдены сравнения для $|B|$, где $|B|$ — число элементов в B. Рассмотрены применения полученного результата в случаях, когда B есть: 1) множество матриц с перманентом равным r, $r\in \mathbf{N}_0=\{0, 1, 2, \ldots\}$; 2) множество матриц с заданными строчечными и столбцовыми суммами.

1. Основная лемма. Пусть n, $q\in \mathbf{N}=\{1, 2, 3, \ldots\}$, $q>1$, q-ичное разложение n имеет вид

$$n=a_0q^k+a_1q^{k-1}+\ldots+a_{k-1}q+a_k, \tag{1.1}$$

где $a_0, a_1, \ldots, a_k\in\{0, 1, \ldots, q-1\}$, $a_0\neq 0$, $k\in \mathbf{N}$.

Пусть M — произвольная $(n\times n)$-матрица. Определим, исходя из (1.1), разбиение M на подматрицы. Разобьем столбцы M слева направо, в соответствии с (1.1), на группы столбцов: 1) первые a_0 группы столбцов содержат по q^k столбцов; 2) следующие a_1 группы столбцов содержат по q^{k-1} столбцов; и т. д.; $k+1$) последние a_k групп столбцов содержат по одному столбцу. Аналогично, в соответствии с (1.1), разобьем строки M сверху вниз на группы строк: 1) первые a_0 группы строк содержат по q^k строк; 2) следующие a_1 группы строк содержат по q^{k-1} строк; и т. д.; последние a_k групп строк содержат по одной строке. Указанные выше разбиения строк и столбцов матрицы M порождают разбиение M на подматрицы. На рис. 1 приведены разбиения M на подматрицы: *а* — для $n=15$, $q=2$; *б* — $n=15$, $q=3$; *в* — $n=15$, $q=5$. Получившиеся подматрицы матрицы M будем нумеровать буквами M_{ij}, где i — номер «строки», j — номер «столбца», где расположена M_{ij}. На рис. 1, *а* — *г* показано, как производится нумерация подматриц матрицы M. Будем считать, что для каждой подматрицы M_{ij} все ее элементы равны 0 или все равны 1, т. е. элементами M_{ij} не могут быть одновременно 0 и 1. Пишем $M_{ij}=(0)$, если все элементы M_{ij} равны 0. Аналогично, $M_{ij}=(1)$, если все элементы M_{ij} равны 1. Описанное выше разбиение M и последнее условие порождают множество (0, 1)-матриц порядка $n\times n$, которое мы обозначим $A(n, q)$. Обозначим $A(n)$ множество всех (0, 1)-матриц порядка $n\times n$.

Лемма 1.1. *Пусть $n\in\mathbf{N}$, p простое. Тогда*

$$|B|\equiv|B\cap A(n, p)|\,(\mathrm{mod}\,p).$$

Доказательство. Пусть $M \in B$, $q = p$. Будем рассматривать в матрице M элементы первой строки, расположенные в первых p^k столбцах (остальные элементы первой строки будем считать фиксированными). Обозначим T_r число матриц M, у которых первыми p^k элементами первой строки являются $(1, \ldots, 1, 0, \ldots, 0)$, где единиц r штук, нулей $p^k - r$ штук, $r = 0, 1, \ldots, p^k$. Тогда

$$|B| = \sum_{r=0}^{p^k} C_{p^k}^r T_r \equiv T_0 + T_{p^k} \pmod p,$$

т. е. по $\operatorname{mod} p$ число $|B|$ сравнимо с числом (0, 1)-матриц $M \in B$, у которых все первые p^k элементов первой строки равны 0 или все равны 1.

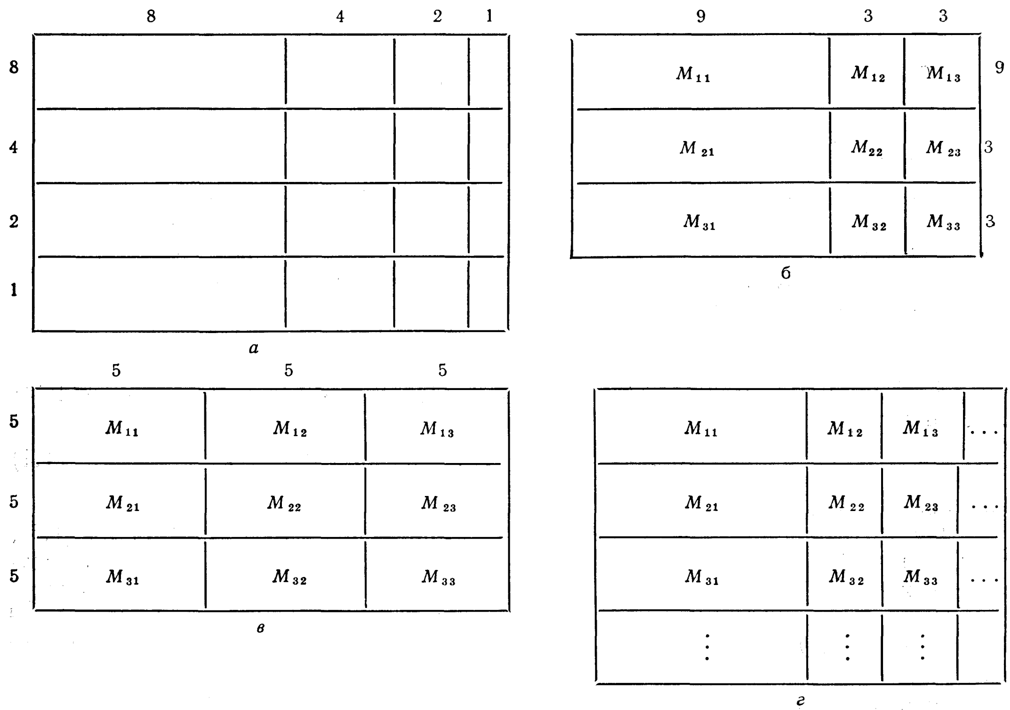

Рис. 1

Если $a_0 > 1$, то повторяем это рассуждение для следующих p^k элементов первой строки, и т. д. После того, как мы проведем это рассуждение для первых a_0 групп элементов первой строки, мы проводим это рассуждение для следующих a_1 групп элементов первой строки и т. д. Получим, что по $\operatorname{mod} p$ число $|B|$ сравнимо с числом (0, 1)-матриц $M \in B$, у которых элементы первой строки разбиты слева направо на a_0 групп по p^k элементов, на a_1 групп по p^{k-1} элементов, и т. д., на a_k групп по одному элементу, и каждая группа элементов состоит только из нулей или только из единиц, (0 и 1 не могут быть вместе в одной группе).

Повторив проведенные выше рассуждения для оставшихся строк, а затем для всех столбцов, получим утверждение леммы.

2. Сравнения по простому модулю для числа (0, 1)-матриц порядка $n \times n$, перманент которых равен 0. Пусть M — (0, 1)-матрица порядка $n \times n$ такая, что $\operatorname{per} M = 0$. Хорошо известен следующий критерий [2]: $\operatorname{per} M = 0$ тогда и только тогда, когда в M существует подматрица из нулей порядка $s \times t$, где $s + t > n$. Подматрицы из нулей порядка $s \times t$, где $s + t > n$, будем называть определяющими для $n \times n$-матрицы M.

Пусть Z_n обозначает число (0, 1)-матриц порядка $n\times n$, перманент которых равен 0. О числах Z_n, по-видимому, мало что известно. В [1] определена асимптотика Z_n, $Z_n \sim n2^{n^2-n+1}$. Можно проверить, что $Z_1=1$, $Z_2=9$, $Z_3=265$, $Z_4=27713$. Через $\mathcal{U}_n$ обозначим число (0, 1)-матриц порядка $n\times n$, перманент которых не равен нулю.

Теорема 2.1. *Для* $n\in\mathbf{N}$ $Z_n\equiv 1 \pmod 2$, $\mathcal{U}_n\equiv 1 \pmod 2$.

Доказательство. Из леммы 1.1 следует, что

$$Z_n\equiv |B\cap A(n,\ 2)| \pmod 2, \tag{2.1}$$

где B — множество (0, 1)-матриц порядка $n\times n$, перманент которых равен 0. Из (2.1) находим, что

$$Z_n\equiv |C| \pmod 2, \tag{2.2}$$

где $C=\{M\,|\,M\in A(n,\ 2),\ M \text{ симметрическая, } \operatorname{per} M=0\}$. Рассмотрим множество $C^1=\{M\,|\,M\in C,\ M_{11}=(0)\}$. Для $M\in C^1$ матрица M_{11} является определяющей, поэтому матрицы M_{ij}, $(j,\ i)\neq(1,\ 1)$ могут заполняться произвольным образом. Отсюда следует, что $|C^1|\equiv 0 \pmod 2$ и

$$Z_n\equiv |C_1| \pmod 2, \tag{2.3}$$

где $C_1=\{M\,|\,M\in C,\ M_{11}=(1)\}$.

Рассмотрим множество $C_1^1=\{M\,|\,M\in C_1,\ M_{12}=(1)\}$. Для $M\in C_1^1$ определяющие матрицы не содержат матрицу M_{22}, так как наибольшая подматрица M, состоящая из нулей и содержащая M_{22}, имеет порядок $s\times t$, где $s+t<n$. Поэтому подматрица M_{22} может заполняться произвольным образом и $|C_1^1|\equiv 0 \pmod 2$. Рассмотрим множество $C_1^2=\{M\,|\,M\in C_1,\ M_{12}=(0),\ M_{22}=(0)\}$. Для $M\in C_1^2$ матрица $\begin{pmatrix}M_{12}\\ M_{22}\end{pmatrix}$ является определяющей, поэтому матрицы M_{ji}, $(i,\ j)\neq(1,\ 1),\ (1,\ 2),\ (2,\ 2)$ могут заполняться произвольным образом. Отсюда следует, что $|C_1^2|\equiv 0 \pmod 2$ и

$$Z_n\equiv |C_2| \pmod 2, \tag{2.4}$$

где $C_2=\{M\,|\,M\in C_1,\ M_{12}=(0),\ M_{22}=(1)\}$.

Рассмотрим множество $C_2^1=\{M\,|\,M\in C_2,\ M_{13}=(1)\}$. Для $M\in C_2^1$ определяющие матрицы не содержат M_{23}, M_{33}, M_{32}, так как наибольшая подматрица M, состоящая из нулей и содержащая M_{23} и M_{33} (или M_{32} и M_{33}), имеет порядок $s\times t$, где $s+t<n$. Поэтому подматрицы M_{23}, M_{33}, M_{32} могут заполняться произвольным образом и $|C_2^1|\equiv 0 \pmod 2$. Рассмотрим множество $C_2^2=\{M\,|\,M\in C_2,\ M_{13}=(0),\ M_{23}=(1)\}$. Для $M\in C_2^2$ определяющие матрицы не содержат M_{33}, так как наибольшая подматрица M, состоящая из нулей и содержащая M_{33}, имеет порядок $s\times t$, где $s+t<n$. Поэтому подматрица M_{33} может заполняться произвольным образом и $|C_2^2|\equiv 0 \pmod 2$. Рассмотрим множество $C_2^3=\{M\,|\,M\in C_2,\ M_{13}=(0),\ M_{23}=(0),\ M_{33}=(0)\}$. Для $M\in C_2^3$ матрица $\begin{pmatrix}M_{13}\\ M_{23}\\ M_{33}\end{pmatrix}$ является определяющей, поэтому матрицы M_{ij} $((i,\ j)\neq$ $\neq(1,\ 1),\ (1,\ 2),\ (1,\ 3),\ (2,\ 3),\ (3,\ 3))$ могут заполняться произвольным образом. Отсюда следует, что $|C_2^3|\equiv 0 \pmod 2$ и

$$Z_n\equiv |C_3| \pmod 2, \tag{2.5}$$

где $C_3=\{M\,|\,M\in C_2,\ M_{13}=(0),\ M_{23}=(0),\ M_{33}=(1)\}$.

Продолжая таким образом, мы получим, что $Z_n\equiv |C_n| \pmod 2$, где C_n — множество (0, 1)-матриц M таких, что $M_{ii}=(1)$ для $i=1,\ 2,\ \ldots,\ a_0+a_1+\ldots$ $\ldots+a_k-1$, $M_{ii}=(0)$ для $i=a_0+a_1+\ldots+a_k$, $M_{ij}=(0)$ для всех $i\neq j$. Так как $|C_n|=1$, то $Z_n\equiv 1 \pmod 2$. Сравнения $\mathcal{U}_n\equiv 1 \pmod 2$ являются следствием $Z_n\equiv 1 \pmod 2$. Теорема доказана.

Обозначим $B(n,\ q,\ r)=\{M\,|\,M\in A(n,\ q),\ \operatorname{per} M=r\}$, $B(n,\ q)=B(n,\ q,\ 0)$. В теореме 2.2 собрано несколько применений леммы 1.1.

Теорема 2.2. *Для $k\in\mathbf{N}$ и простых p справедливы сравнения:*

1) *если $n=a_0p^k$, где $a_0\in\{1, 2, \ldots, p-1\}$, то $Z_n\equiv Z_{a_0}\pmod p$;*

2) *если $n=p^k$, то $Z_n\equiv 1\pmod p$;*

3) *если $n=2p^k$, $p>2$, то $Z_n\equiv 9\pmod p$;*

4) *если $n=3p^k$, $p>3$, то $Z_n\equiv 265\pmod p$;*

5) *если $n\equiv 0\pmod p$, то $Z_n\equiv Z_{n/p}\pmod p$;*

6) *если каноническое разложение n на простые множители имеет вид $n=p_1^{b_1}p_2^{b_2}\ldots p_r^{b_r}$, то $Z_n\equiv Z_{n/p_i^{b_i}}\pmod{p_i}$ для $i=1, \ldots, r$;*

7) *если $n=p^k+1$, то $Z_n\equiv 11\pmod p$;*

8) *если $n=p^k+2$, $p>2$, то $Z_n\equiv 359\pmod p$;*

9) *если $n=2p^k+1$, $p>2$, то $Z_n\equiv 345\pmod p$;*

10) *если $n=p^k+p+1$, $k\geqslant 2$, то $Z_n\equiv 389\pmod p$.*

Доказательство. Из леммы 1.1 следует, что $Z_n\equiv|B(n, p)|\pmod p$.

1) Если $M\in B(n, p)$, то M разбита на a_0^2 квадратных матриц M_{ij} порядка p^k. Поставим в соответствие матрице M квадратную матрицу $M'=(M'_{ij})$ порядка a_0 такую, что $M'_{ij}=(0)$ тогда и только тогда, когда $M_{ij}=(0)$. Применяя критерий равенства перманента нулю, нетрудно убедиться, что построенное соответствие — биекция $B(n, p)$ на множестве (0, 1)-матриц порядка $a_0\times a_0$, перманент которых равен 0.

Утверждения 2) — 4) следуют из 1).

5) Если $M\in B(n, p)$, то M разбита на матрицы M_{ij}, причем если $s\times t$ — порядок M_{ij}, то $p|s$ и $p|t$. Поставим в соответствие матрице M матрицу $M'\in B(n/p, p)$ такую, что для всех i, j $M_{ij}=(0)$ тогда и только тогда, когда $M'_{ij}=(0)$. Применяя критерий равенства перманента нулю, нетрудно убедиться, что построенное соответствие — биекция $B(n, p)$ на $B(n/p, p)$.

Утверждение 6) следует из 5).

В случаях 8) — 10) матрицы $M\in B(n, p)$ раскладываются на небольшое число матриц M_{ij}. Непосредственным вычислением проверяем справедливость 8) — 10). Теорема доказана.

3. Сравнения по простому модулю для числа (0, 1)-матриц порядка $n\times n$, перманент которых равен r. Обозначим $Z_n(r)$ число (0, 1)-матриц порядка $n\times n$, перманент которых равен r.

Теорема 3.1. *Для $k\in\mathbf{N}$ и простых p справедливы утверждения:*

1) *для $n=p^k$ если $Z_n(r)\not\equiv 0\pmod p$, то $r\in\{0, n!\}$;*

2) *для $n=2p^k$ $p>2$, если $Z_n(r)\not\equiv 0\pmod p$, то $r\in\left\{0, \left(\frac{n}{2}!\right)^2, n!\right\}$;*

3) *для $n=p^k+1$ если $Z_n(r)\not\equiv 0\pmod p$, то $r\in\{0, (n-1)!, n!-(n-1)!, n!\}$.*

Доказательство. 1) По лемме 1.1, $Z_n(r)\equiv|B(n, p, r)|\pmod p$. Если $M\in B(n, p, r)$, то M состоит из одной матрицы M_{11}. Отсюда следует нужное утверждение.

Утверждения 2), 3) получаются аналогично.

4. Сравнения по простому модулю для числа (0, 1)-матриц порядка $n\times n$ с данными строчечными и столбцовыми суммами. Обозначим $\mathcal{U}_n(R, S)$ множество (0, 1)-матриц M порядка $n\times n$ таких, что $R=\{r_1, \ldots, r_n\}$ — мультимножество строчечных сумм M, а $S=\{s_1, \ldots, s_n\}$ — мультимножество столбцовых сумм M. Если некоторое мультимножество T состоит из элементов t_i таких, что t_i имеет кратность a_i, $i=1, \ldots, l$, то будем писать $T=\{t_1\}^{a_1}\ldots\{t_l\}^{a_l}$. О числах $|\mathcal{U}_n(R, S)|$ мало что известно. В [2], [3] отмечалась сложность чисел $|\mathcal{U}_n(R, S)|$, как функций R и S.

Теорема 4.1. *Для $k\in\mathbf{N}$ и простых p справедливы утверждения:*

1) *для $n=p^k$, если $|\mathcal{U}_n(R, S)|\not\equiv 0\pmod p$, то $R=S=\{0\}^n$ или $R=S=\{n\}^n$;*

2) *для $n=2p^k$, если $|\mathcal{U}_n(R, S)|\not\equiv 0\pmod p$, то выполнено одно из условий:*

а) $R=S=\{n/2\}^{n/2}\{0\}^{n/2}$;

б) $R=\{n\}^{n/2}\{0\}^{n/2}$, $S=\{n/2\}^{n}$;
в) $R=\{n/2\}^{n}$, $S=\{n\}^{n/2}\{0\}^{n/2}$;
г) $R=S=\{n/2\}^{n}$;
д) $R=S=\{n/2\}^{n/2}\{n\}^{n/2}$;
е) $R=S=\{n\}^{n}$;
ж) $R=S=\{0\}^{n}$.

Доказательство теоремы 4.1 проводится аналогично доказательству теоремы 3.1.

СПИСОК ЛИТЕРАТУРЫ

1. Everett C. J., Stein P. R. The asymptotic number of matrices with zero permanent // Discrete Mathematics.— 1973.— № 6.— P. 29—34.
2. Тараканов В. Е. Комбинаторные задачи и (0, 1)-матрицы.— М.: Наука, 1985.
3. Райзер Н.. Комбинаторная математика.— М.: Мир, 1966.

Статья поступила 23.06.89