

М. В. Будревич, А. Э. Гутерман, К. А. Таранин

**К ТЕОРЕМЕ КРОЙТЕРА–СЕЙФТЕРА О
ДЕЛИМОСТИ ПЕРМАНЕНТОВ**

§1. ВВЕДЕНИЕ

Пусть A – квадратная матрица порядка n . Перманентом A называется функция

$$\text{per}(A) = \sum_{\sigma \in S_n} a_{1\sigma(1)} \cdot \dots \cdot a_{n\sigma(n)},$$

где S_n – группа перестановок порядка n .

Функция перманента важна как в теоретических задачах, так и в приложениях. Например, она вычисляет число паросочетаний в двудольном графе, если A – матрица смежности рассматриваемого двудольного графа, см. [4], и, тем самым, отвечает за решение проблемы Холла о системах различных представителей, см. [8]. В частности, если функция перманента отлична от 0, то вопрос о существовании системы различных представителей решается положительно. Задача нахождения перманента даже для $(0, 1)$ -матрицы является $\#P$ -сложной [12], что вычислительно эквивалентно проблеме Кука $P \neq NP$ [2, 7, 9]. Учитывая сложность вычисления перманента, становится важным определять, отличается ли он от 0, не вычисляя.

Класс матриц смежности отвечает $(0, 1)$ -матрицам, однако в комбинаторике и ее приложениях также очень актуальны и другие матричные классы, в частности, класс $(1, -1)$ -матриц. Например, в этом классе находится очень важный и широко известный подкласс матриц Адамара, т.е. $(1, -1)$ -матриц H порядка n , удовлетворяющих уравнению $HH^t = nE_n = H^tH$, где E_n – единичная матрица и X^t обозначает транспонированную матрицу для матрицы X . Стоит отметить, что даже существование матриц Адамара для некоторых значений n является открытой проблемой. Вопрос отличия от 0 перманента для матриц из этого класса также является актуальной открытой проблемой. Один из подходов к ее решению состоит в доказательстве того, что перманент не делится на некоторые простые числа. В настоящей

Ключевые слова: перманент, делимость.

Работа выполнена при финансовой поддержке РФФ, грант No. 17-11-01124.

работе исследуется свойство делимости функции перманента $(1, -1)$ -матриц на степени двойки.

В работе Кройтера и Сейфтера [10] были получены некоторые результаты, связанные с делимостью перманента.

Лемма 1.1 ([10, лемма 5 и предложение 4]). *Пусть $n = 2^t - 1$, $t \in \mathbb{N}$, и $A \in M_n(\pm 1)$. Тогда*

$$\text{per}(A) \vdots 2^{n - \lfloor \log_2 n \rfloor - 1}.$$

Лемма 1.2 ([10, лемма 5]). *Пусть $n = 2^t - 1$ для некоторого $t \in \mathbb{N}$, тогда для любой матрицы $A \in M_n(\pm 1)$ выполнено*

$$\text{per}(A) \not\vdots 2^{n - \lfloor \log_2 n \rfloor}.$$

Лемма 1.3 ([10, предложение 5]).

Пусть $n \neq 2^t - 1$ для любого $t \in \mathbb{N}$, тогда для любой матрицы $A \in M_n(\pm 1)$ выполнено

$$\text{per}(A) \vdots 2^{n - \lfloor \log_2 n \rfloor}.$$

В работе [1] был предложен новый метод для вычисления перманента $A \in M_n(\pm 1)$, с помощью которого были получены простые доказательства лемм 1.1-1.3. В настоящей работе мы развиваем предложенный в [1] метод и показываем, что для любого n существуют $n \times n$ матрицы с коэффициентами -1 и 1 , перманент которых не делится на $2^{n - \lfloor \log_2 n \rfloor + 1}$, т.е. в общем случае оценка Кройтера и Сейфтера не улучшаема.

§2. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

В этой работе мы следуем терминологии работы [1].

Определение 2.1. *Обобщенная диагональ квадратной матрицы $A \in M_n$ – это множество пар индексов*

$$\{(1, \sigma(1)), \dots, (n, \sigma(n))\},$$

где $\sigma \in S_n$.

Определение 2.2. *Частичная обобщенная диагональ длины j квадратной матрицы $A \in M_n$ – это подмножество из j элементов какой-то обобщенной диагонали A .*

Обозначение 2.3. Частичную обобщенную диагональ матрицы

$$A \in M_n(\pm 1),$$

все элементы которой равны -1 , мы называем отрицательной.

Обозначение 2.4. Через k_j , $j \in \{1, \dots, n\}$, обозначим число различных отрицательных частичных обобщенных диагоналей длины j . По определению положим $k_0 = 1$.

В работе [1] предложен метод для нахождения перманента $(1, -1)$ -матрицы, удобный для исследования делимости перманента матрицы.

Лемма 2.5 ([1, лемма 2.3]). *Пусть $A \in M_n(\pm 1)$. Тогда*

$$\text{per}(A) = \sum_{j=0}^n (-2)^j \cdot k_j \cdot (n-j)!. \quad (2.1)$$

Определение 2.6. *Пусть $p \in \mathbb{N} \setminus \{1\}$, $x \in \mathbb{Z} \setminus \{0\}$. Положим*

$$\nu_p(x) = \max\{k \in \mathbb{Z} \mid \frac{x}{p^k} \in \mathbb{Z}\}.$$

Замечание 2.7. Заметим, что если p – простое число, то

$$\nu_p(xy) = \nu_p(x) + \nu_p(y).$$

Будем считать далее, что сумма, верхний предел которой меньше нижнего, а также сумма по пустому множеству обе равны нулю.

Лемма 2.8. *Для любого $n \in \mathbb{N}$ и $m \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ таких, что $m < n$, имеем:*

$$\nu_2(2^m \cdot (n-m)!) = n-1 - \left\{ \frac{n-m}{2^{\lfloor \log_2(n-m) \rfloor}} \right\} - \sum_{k=1}^{\lfloor \log_2(n-m) \rfloor} \left\{ \frac{n-m}{2^k} \right\}. \quad (2.2)$$

Доказательство. 1. Рассмотрим левую часть равенства (2.2):

$$\Lambda := \nu_2(2^m \cdot (n-m)!) = \nu_2(2^m) + \nu_2((n-m)!) = m + \sum_{k=1}^{\lfloor \log_2(n-m) \rfloor} \left\lfloor \frac{n-m}{2^k} \right\rfloor.$$

Применяя тождество $[a] = a - \{a\}$ к слагаемым вида $\lfloor \frac{n-m}{2^k} \rfloor$ и вынося общий множитель, имеем:

$$\Lambda = m + (n - m) \cdot \left(\sum_{k=1}^{\lfloor \log_2(n-m) \rfloor} \frac{1}{2^k} \right) - \sum_{k=1}^{\lfloor \log_2(n-m) \rfloor} \left\{ \frac{n-m}{2^k} \right\}.$$

Применяя тождество $\sum_{k=1}^t \frac{1}{2^k} = 1 - \frac{1}{2^t}$ ко второму слагаемому, получаем:

$$\Lambda = m + (n - m) \left(1 - \frac{1}{2^{\lfloor \log_2(n-m) \rfloor}} \right) - \sum_{k=1}^{\lfloor \log_2(n-m) \rfloor} \left\{ \frac{n-m}{2^k} \right\}.$$

Теперь раскроем круглые скобки и применим $a = [a] + \{a\}$:

$$\Lambda = n - \left\lfloor \frac{n-m}{2^{\lfloor \log_2(n-m) \rfloor}} \right\rfloor - \left\{ \frac{n-m}{2^{\lfloor \log_2(n-m) \rfloor}} \right\} - \sum_{k=1}^{\lfloor \log_2(n-m) \rfloor} \left\{ \frac{n-m}{2^k} \right\}.$$

Заметим, что, согласно [1, лемма 3.1], второе слагаемое в Λ тождественно равно (-1) . Поэтому

$$\Lambda = n - 1 - \left\{ \frac{n-m}{2^{\lfloor \log_2(n-m) \rfloor}} \right\} - \sum_{k=1}^{\lfloor \log_2(n-m) \rfloor} \left\{ \frac{n-m}{2^k} \right\}. \quad \square$$

Далее потребуется следующий, видимо, известный факт, доказательство которого нам, однако, найти не удалось, поэтому приводим его полностью.

Лемма 2.9. Пусть $n \in \mathbb{N}$ и s равняется количеству единиц в двоичном представлении числа n . Тогда $\nu_2(n!) = n - s$.

Доказательство. 1. Без ограничения общности считаем, что

$$2^{t-1} \leq n \leq 2^t - 1.$$

Тогда $\lfloor \log_2 n \rfloor = t - 1$. В этом случае, согласно лемме 2.8,

$$\nu_2(n!) = n - 1 - \left\{ \frac{n}{2^{\lfloor \log_2 n \rfloor}} \right\} - \sum_{k=1}^{\lfloor \log_2 n \rfloor} \left\{ \frac{n}{2^k} \right\}. \quad (2.3)$$

2. Пусть $\overline{a_{t-1}a_{t-2}\dots a_1a_0}$ — двоичное представление n :

$$n = \sum_{k=0}^{t-1} a_k 2^k,$$

где $a_{t-1} = 1$. Тогда для любого $j \in \mathbb{N}$, $0 \leq j \leq t-1$, имеем:

$$\left\{ \frac{n}{2^j} \right\} = \left\{ \sum_{k=0}^{t-1} a_k 2^{k-j} \right\} = \sum_{0 \leq k < j} a_k 2^{k-j}. \quad (2.4)$$

Числа (дробные части) $\left\{ \frac{n}{2^j} \right\}$ и $\left\{ \frac{n}{2^{j+1}} \right\}$ соотносятся следующим образом:

$$\begin{aligned} \frac{1}{2} \left\{ \frac{n}{2^j} \right\} &\stackrel{(2.4)}{=} \frac{1}{2} \sum_{0 \leq k < j} a_k 2^{k-j} \\ &= \frac{1}{2} \sum_{0 \leq k < j} a_k 2^{k-j} + \left(\frac{1}{2} a_j - \frac{1}{2} a_j \right) \\ &= \frac{1}{2} \sum_{0 \leq k \leq j} a_k 2^{k-j} - \frac{1}{2} a_j \\ &= \sum_{0 \leq k < j+1} a_k 2^{k-j-1} - \frac{1}{2} a_j \stackrel{(2.4)}{=} \left\{ \frac{n}{2^{j+1}} \right\} - \frac{1}{2} a_j, \end{aligned}$$

то есть

$$2 \left\{ \frac{n}{2^{j+1}} \right\} = \left\{ \frac{n}{2^j} \right\} + a_j. \quad (2.5)$$

3. Для каждого целого j , $1 \leq j \leq t-1$, рассмотрим следующую сумму:

$$\mathfrak{S}_j := \sum_{k=1}^j \left\{ \frac{n}{2^k} \right\} + \left\{ \frac{n}{2^j} \right\}. \quad (2.6)$$

Из равенства (2.5) вытекает, что для всех рассматриваемых j верно соотношение

$$\mathfrak{S}_j = \mathfrak{S}_{j-1} + a_{j-1},$$

где $\mathfrak{S}_0 := 0$. Следовательно, выполнено равенство

$$\mathfrak{S}_{t-1} = \mathfrak{S}_0 + \sum_{k=0}^{t-2} a_k = s - 1. \quad (2.7)$$

4. Применяя равенства (2.6) и (2.7) к (2.3), получаем:

$$\begin{aligned} \nu_2(n!) &\stackrel{(2.3)}{=} n - 1 - \left\{ \frac{n}{2^{t-1}} \right\} - \sum_{k=1}^{t-1} \left\{ \frac{n}{2^k} \right\} \\ &\stackrel{(2.6)}{=} n - 1 - \mathfrak{S}_{t-1} \stackrel{(2.7)}{=} n - 1 - (s - 1) = n - s. \quad \square \end{aligned}$$

Следствие 2.10. Для любых $n \in \mathbb{N}$ и $m \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ таких, что $m \leq n$, имеет место равенство

$$\nu_2(2^m \cdot (n - m)!) = n - s, \quad (2.8)$$

где s – число единиц в двоичном представлении числа $n - m$.

Отметим, что лемма 2.9 и следствие 2.10 могут быть использованы для тех же целей, что и леммы 3.5–3.7 в работе [1], существенно упрощая доказательство основных результатов работы [1].

Оказывается, что имея информацию лишь о некоторых из k_m , можно делать выводы о делимости перманента матрицы $A \in M_n(\pm 1)$ на степени двойки.

Определение 2.11. Пусть $n \in \mathbb{N}$ таково, что $2^{t-1} \leq n \leq 2^t - 1$. Через $\mathfrak{M} = \mathfrak{M}(n)$ обозначим множество таких положительных целых чисел m , меньших n , что в двоичном представлении числа $n - m$ имеется в точности $t - 1$ единица.

§3. ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Лемма 3.1. Пусть $n \in \mathbb{N}$, где $2^{t-1} \leq n < 2^t - 1$, и $\mathfrak{M} = \mathfrak{M}(n)$. Для любой матрицы $A \in M_n(\pm 1)$

$$\text{per}(A) \dot{\vdots} 2^{n-t+2} \quad \text{тогда и только тогда, когда} \quad \sum_{m \in \mathfrak{M}} k_m \dot{\vdots} 2.$$

Доказательство. Так как $2^{t-1} \leq n < 2^t - 1$, то двоичное представление числа n содержит не более $t - 1$ единицы. Воспользуемся разложением из леммы 2.5 и разобьем слагаемые на две группы в зависимости от количества единиц в двоичном разложении индекса суммирования:

$$\begin{aligned} \text{per}(A) &\stackrel{(2.1)}{=} \sum_{j=0}^n (-2)^j \cdot k_j \cdot (n - j)! \\ &= \sum_{\substack{m \notin \mathfrak{M} \\ 0 \leq m \leq n}} (-2)^m \cdot k_m \cdot (n - m)! + \sum_{m \in \mathfrak{M}} (-2)^m \cdot k_m \cdot (n - m)! \\ &=: \Sigma_1 + \Sigma_2, \end{aligned}$$

Рассмотрим Σ_1 . По следствию 2.10, для любого $(n - m) \in \mathbb{N}$ имеет место равенство

$$\nu_2(2^m (n - m)!) = n - s_{n-m}, \quad (3.1)$$

где s_{n-m} – количество единиц в двоичном представлении числа $n - m$. Если $s_{n-m} \leq t - 2$, то из (3.1) следует, что неравенство

$$\nu_2(2^m(n-m)!) \geq n - t + 2$$

выполняется для каждого слагаемого в Σ_1 . Следовательно, $\Sigma_1 \dot{\vdots} 2^{n-t+2}$.

Рассмотрим Σ_2 . Из определения \mathfrak{M} и следствия 2.10 получаем, что для любого $m \in \mathfrak{M}$ имеет место равенство

$$\nu_2(2^m(n-m)!) = n - t + 1.$$

Обозначая $(n-m)! \cdot (-2)^{m-(n-t+1)}$ через α_m , где α_m не делится на 2 по следствию 2.10, получаем равенство

$$\Sigma_2 = 2^{n-t+1} \left(\sum_{\substack{m \in \mathfrak{M} \\ 2 \mid k_m}} k_m \alpha_m + \sum_{\substack{m \in \mathfrak{M} \\ 2 \nmid k_m}} k_m \alpha_m \right) =: 2^{n-t+1} (\Sigma_{21} + \Sigma_{22}),$$

где $\Sigma_{21} \dot{\vdots} 2$, и все слагаемые в Σ_{22} нечетны.

Таким образом, $\text{per}(A) \dot{\vdots} 2^{n-t+2}$ тогда и только тогда, когда количество нечетных слагаемых в Σ_{22} четно. Это равносильно тому, что количество нечетных k_m , где $m \in \mathfrak{M}$, четно. Последнее эквивалентно условию

$$\sum_{m \in \mathfrak{M}} k_m \dot{\vdots} 2. \quad \square$$

Замечание 3.2. Заметим, что в условиях леммы 3.1 в двоичном разложении числа n не более t знаков, а значит, мощность множества \mathfrak{M} не превосходит $\binom{t}{1} = t$.

Следствие 3.3. Для любого $n \in \mathbb{N}$ существует такая матрица $A \in M_n(\pm 1)$, что

$$\text{per}(A) \not\dot{\vdots} 2^{n - \lfloor \log_2 n \rfloor + 1}.$$

Доказательство. 1. Пусть $n = 2^t - 1$ для некоторого $t \in \mathbb{N}$. Утверждение следует из леммы 1.2. Далее, без ограничения общности будем считать, что $n \neq 2^t - 1$ для любого $t \in \mathbb{N}$.

2. Рассмотрим множество $\mathfrak{M}(n)$. В двоичном представлении

$$n - m_1 = 2^{\lfloor \log_2 n \rfloor} - 1$$

содержится ровно $\lfloor \log_2 n \rfloor$ единиц. Следовательно, $m_1 = n - 2^{\lfloor \log_2 n \rfloor} + 1 \in \mathfrak{M}(n)$, и множество $\mathfrak{M}(n)$ непусто. Выберем минимальное $m_0 \in \mathfrak{M}$.

3. Рассмотрим матрицу $A \in M_n(\pm 1)$ с m_0 отрицательными элементами на главной диагонали такую, что все остальные элементы матрицы положительны. Так как $k_j = 0$ для любого $j > m_0$, то в формуле (2.1) для вычисления $\text{per} A$ всего $m_0 + 1$ ненулевых слагаемых. Заметим, что в A имеется единственная отрицательная частичная обобщенная диагональ длины m_0 , следовательно, $k_{m_0} = 1$.

4. Из определения m_0 следует, что в (2.1) все слагаемые, кроме последнего, делятся на $2^{n - \lfloor \log_2 n \rfloor + 1}$. Последнее слагаемое, равное $(-2)^{m_0} \cdot (n - m_0)!$, на $2^{n - \lfloor \log_2 n \rfloor + 1}$ не делится. Следовательно, $\text{per} A$ не делится на $2^{n - \lfloor \log_2 n \rfloor + 1}$. \square

В качестве примера использования полученного результата докажем, что перманент матриц определенного вида не делится на $2^{n - \lfloor \log_2 n \rfloor + 1}$. Для этого нам понадобится следующая лемма.

Лемма 3.4 ([6]). Пусть $n = \overline{a_{t-1}a_{t-2}\dots a_1a_0}$ и $k = \overline{b_{q-1}b_{q-2}\dots b_1b_0}$, $t \geq q$, — двоичные представления натуральных чисел n и k соответственно, где $n \geq k$. Тогда

$$\binom{n}{k} \text{ нечетно} \iff b_i \leq a_i \text{ для всех } i \in \{0, 1, 2, \dots, q-1\}.$$

Лемма 3.5. Пусть $2^{t-1} \leq n < 2^{t-1} + 2^{t-2} - 1$ и $A \in M_n(\pm 1)$. Имеют место следующие утверждения.

- (1) Если количество отрицательных частичных обобщенных диагоналей длины $n - 2^{t-1} + 1$ нечетно, то

$$\text{per}(A) \not\mid 2^{n-t+2}.$$

- (2) Если из матрицы A можно перестановкой строк и столбцов получить матрицу, у которой все отрицательные элементы расположены на главной диагонали, то её перманент не делится на 2^{n-t+2} тогда и только тогда, когда значение каждого разряда в двоичном разложении количества отрицательных элементов A не меньше, чем значение того же разряда в двоичном разложении $n - 2^{t-1} + 1$.

Доказательство. 1. По лемме 3.1, $\text{per}(A) \dot{\vdash} 2^{n-t+2}$ тогда и только тогда, когда $\sum_{m \in \mathfrak{M}} k_m \dot{\vdash} 2$. По определению множества \mathfrak{M} , любое число $m \in \mathfrak{M}$ представимо в виде $m = n + 2^j - \sum_{i=0}^{t-1} 2^i$, где $j \in \{0, 1, 2, \dots, t-1\}$. Таким образом, для рассматриваемого n множество $\mathfrak{M}(n)$ состоит из одного элемента $m_0 = n + 2^{t-1} - \sum_{i=0}^{t-1} 2^i = n - \sum_{i=0}^{t-2} 2^i$. Других элементов в \mathfrak{M} нет, так как если $j < t-1$, то

$$n - m = -2^j + \sum_{i=0}^{t-1} 2^i > 2^{t-1} + 2^{t-2} - 1 = n.$$

Таким образом, условие $\sum_{m \in \mathfrak{M}} k_m \dot{\vdash} 2$ эквивалентно тому, что количество отрицательных частичных обобщённых диагоналей длины $m_0 = n - 2^{t-1} + 1$ нечётно.

2. Если матрица A имеет упомянутый в условии вид, то все её отрицательные частичные обобщённые диагонали длины $n - 2^{t-1} + 1$ содержатся в самой длинной отрицательной частичной обобщённой диагонали. Обозначим её длину через L . Тогда количество отрицательных частичных обобщённых диагоналей длины $n - 2^{t-1} + 1$ равно $\binom{L}{n-2^{t-1}+1}$. Значит, согласно доказанному в пункте 1, $\text{per}(A)$ не делится на 2^{n-t+2} тогда и только тогда, когда число $\binom{L}{n-2^{t-1}+1}$ нечётно, а это, согласно лемме 3.4, эквивалентно условию, сформулированному в пункте 2. \square

Проиллюстрируем последнюю лемму следующим конкретным примером.

Пример 3.6. Пусть $n = 32$ (или $33, 34, \dots, 45, 46$ соответственно) и $A \in \Omega_n$.

$$\text{per}(A) \dot{\vdash} 2^{n-\lfloor \log_2 n \rfloor + 1} \text{ тогда и только тогда, когда}$$

число отрицательных частичных обобщённых диагоналей длины 1 (или $2, 3, \dots, 14, 15$ соответственно) в матрице A нечётно. (Заметим, что число отрицательных частичных обобщённых диагоналей длины

8. Ph. Hall, *On representatives of subsets*. — J. London Math. Soc. **10**, No. 1 (1935), 26–30.
9. R. M. Karp, *Reducibility among combinatorial problems*. — In: Complexity of Computer Computations, Plenum Press, New-York, 1972, pp. 85–104.
10. A. R. Kräuter, N. Seifter, *On some questions concerning permanents of $(1, -1)$ -matrices*. — Israel J. Math. **45**, No. 1 (1983), 53–62.
11. H. Perfect, *Positive diagonals of ± 1 -matrices*. — Monatsh. Math. **77** (1973), 225–240.
12. L. G. Valiant, *The complexity of computing the permanent*. — Theor. Comput. Sci. **8** (1979), 189–201.
13. E. T. H. Wang, *On permanents of $(1, -1)$ -matrices*. — Israel J. Math. **18** (1974), 353–361.

Budrevich M. V., Guterman A. E., Taranin K. A. On the Kräuter–Seifter theorem on permanent divisibility.

The paper investigates the divisibility of the permanent function of $(1, -1)$ -matrices by different powers of 2. It is shown that the Kräuter–Seifter bound is the best possible for generic $(1, -1)$ -matrices.

Московский государственный
университет
имени М.В. Ломоносова,
Ленинские горы, д. 1, 119991,
Москва, Россия, ГСП-1

E-mail: MBudrevich@yandex.ru

E-mail: guterman@list.ru

E-mail: cataranin@gmail.com

Поступило 2 ноября 2017 г.