ПСЕВДОАДАМАРОВЫ МАТРИЦЫ

@ Р.А. Шарипов

r-sharipov@mail.ru

УДК 519.101

DOI: 10.33184/mnkuomsh2t-2021-10-06.100.

В докладе даётся определение псевдоадамаровых матриц первого и последующих поколений. В случае псевдоадамаровых матриц первого поколения приводятся некоторые доказанные результаты о строении этих матриц и формулируются гипотезы, проверенные численным счётом до размера $m = 22$.

Ключевые слова: адамаровы матрицы, псевдоадамаровы матрицы.

Pseudo-Hadamard matrices

In the report pseudo-Hadamard matrices of the first and the further generations are defined. In the case of pseudo-Hadamard matrices of the first generation some proved results are given and some conjectures are formulated which are tested for the sizes up to $m = 22$.

Keywords: Hadamard matrices, pseudo-Hadamard matrices.

Стандартные матрицы Адамара определяются как целочисленные ортогональные матрицы $n \times n$ с элементами 1 и -1 (см. [1]). Имеется процедура преобразования таких матриц к матрицам с элементами 0 и 1 с понижением размера на единицу (см. [2]). Полученные матрицы называются адамаровыми матрицами в представлении $\{0, 1\}$. Класс таких матриц инвариантен относительно перестановок строк и столбцов в них. При помощи таких перестановок каждая адамарова матрица приводится к виду

$$H = \left\| \begin{array}{cccccc} 1 & \dots & 1 & 0 & \dots & 0 \\ \vdots & & & & & \\ 1 & & & & & \\ 0 & & \{0, 1\} & & & \\ \vdots & & & & & \\ 0 & & & & & \end{array} \right\|. \quad (1)$$

Определение. Псевдоадамаровой матрицей первого поколения называется обведённый рамкой правый нижний диагональный блок в некоторой адамаровой матрице, приведённой к виду (1). Псевдоадамаровы

Шарипов Руслан Абдулович, к.ф.-м.н., доцент, БашГУ (Уфа, Россия); Ruslan Sharipov (Bashkir State University, Ufa, Russia)

матрицы каждого следующего поколения получаются из матриц предыдущего поколения понижением размера при помощи процедуры, аналогичной (1).

Пусть $m = 4q - 2$, где $q \in \mathbb{N}$, и пусть $a = (m+2)/4 = q$, $b = (m+2)/2 = 2q$, $\tilde{a} = a - 1$, $\tilde{b} = b - 1$. Рассмотрим матрицу

$$G = \begin{pmatrix} \overbrace{\tilde{b} \dots \tilde{a}}^{2q-1} & \overbrace{a \dots a}^{2q-1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \tilde{a} & \dots & \tilde{b} & a & \dots & a \\ a & \dots & a & b & \dots & a \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a & \dots & a & a & \dots & b \end{pmatrix}. \quad (2)$$

Теорема 1. *Квадратная матрица $m \times m$ с элементами 0 и 1 является псевдоадмаровой матрицей первого поколения в том и только в том случае, когда $m = 4q - 2$ для некоторого $q \in \mathbb{N}$ и когда её столбцы и её строки, рассматриваемые как вектора в $\mathbb{R}^m$, порождают матрицы Грама вида (2) с $a = (m+2)/4 = q$, $b = (m+2)/2 = 2q$, $\tilde{a} = a - 1$ и $\tilde{b} = b - 1$ относительно стандартного скалярного произведения в $\mathbb{R}^m$.*

Вероятно теорема 1 может быть усилена. Однако, соответствующее утверждение ещё не доказано и оно формулируется в виде гипотезы.

Гипотеза 1. *Пусть $\tilde{H}$ — квадратная $m \times m$ матрица, где $m = 4q - 2$ для некоторого $q \in \mathbb{N}$, с элементами 0 и 1, строки которой, рассматриваемые как вектора в $\mathbb{R}^m$, порождают матрицу Грама вида (2) с $a = (m+2)/4 = q$, $b = (m+2)/2 = 2q$, $\tilde{a} = a - 1$ и $\tilde{b} = b - 1$ относительно стандартного скалярного произведения в $\mathbb{R}^m$. Тогда матрица $\tilde{H}$ совпадает с некоторой псевдоадмаровой матрицей первого поколения после некоторой перестановки её столбцов.*

Другая гипотеза, назовём её **гипотезой 2**, получается из гипотезы 1 путём замены в её формулировке строк на столбцы и столбцов на строки. В [3] гипотезы 1 и 2 были проверены и подтверждены численным счётом на псевдоадмаровых матрицах первого поколения размером до $m = 22$. Общее число матриц, для которых они проверены и подтверждены, превышает 31 тысячу.

Стандартные адамаровы матрицы связаны с проблемой Адамара о максимальности детерминанта матрицы с элементами 1 и -1 (см. [4] и [5]). Упрощённая версия этой проблемы предложена в [6]. Однако, как сама проблема Адамара, так и её упрощённая версия остаются нерешёнными математическими задачами.

Стандартные матрицы Адамара находят применение в криптографии. Такого же применения следует ожидать и для псевдоадамаровых матриц.

Литература

1. *Hadamard matrix* // Wikipedia, Wikimedia Foundation Inc., San Francisco, USA.
2. *Sharipov R.A.* Hadamard matrices in $\{0,1\}$ presentation and an algorithm for generating them // e-print arXiv:2105.01485 (2021).
3. *Sharipov R.A.* Pseudo-Hadamard matrices of the first generation and an algorithm for producing them // e-print arXiv:2105.08974 (2021).
4. *Hadamard's maximal determinant problem* // Wikipedia, Wikimedia Foundation Inc., San Francisco, USA.
5. *Hadamard J.* Résolution d'une question relative aux déterminants // Bulletin des Sciences Mathématiques, 1893, V. 17, P. 240–246.
6. *Sharipov R.A.* On a simplified version of Hadamard's maximal determinant problem // e-print arXiv:2104.01749 (2021).