

Впервые матрицы Адамара были применены французским математиком Жаком Адамаром. Их часто используют для организации хранения и передачи информации.

Квадратная матрица H порядка m состоящая из единичных по модулю элементов называется матрицей Адамара, если выполняется следующее условие:

$$H_m H_m^T = m E_m$$

Матрицу Адамара порядка $2m$ можно получить следующим образом:

$$H_{2m} = \begin{pmatrix} H_m & H_m \\ H_m & -H_m \end{pmatrix}$$

Таким образом мы можем сгенерировать матрицу любого порядка m вида $m=t \cdot 2^k$, где t — порядок исходной матрицы Адамара. Проблема состоит в том что можно получить только одну матрицу порядка m из одной матрицы Адамара меньшего порядка, а для небольшого порядка t существует не так много матриц Адамара.

Цель данной работы в реализации алгоритма способного эффективно генерировать все матрицы Адамара заданной размерности, для последующего порождения матриц высоких порядков и их изучения.

В основу лег алгоритм подбора множества взаимноортогональных векторов заданной длины состоящих из единичных по модулю элементов.

Исходно имеется M_0 множество из 2^m векторов. На i итерации фиксируется вектор v_i из множества M_{i-1} , затем составляется множество векторов M_i , в которое войдут все вектора из M_{i-1} ортогональные v_i .

На m -ой итерации процесс останавливается вектора $v_1 \dots v_m$ и будут составлять матрицу Адамара, после получения очередной матрицы Адамара или, когда после i -ой итерации полученное множество M_i пусто, алгоритм возвращается на предыдущую итерацию, выбирается другой вектор v_i .

Так продолжается до тех пор пока на первой итерации не будут перебраны все вектора из множества M_0 .

Простейшая реализация данного алгоритма показывает что такой перебор имеет недопустимую сложность выполнения, грубая оценка получения одной матрицы: $O(2^n \cdot n^2)$. Если посчитать, что за 1 секунду выполняется 10^9 операций, то мы получим что для получения одной матрицы 28 порядка необходимо 3,5 минуты.

Вывод: реализация нуждается в оптимизации, а так же в применении параллельных вычислений.