Инженерный вестник Дона, №3(2023)
ivdon.ru/ru/magazine/archive/n3y2023/8265

Матрицы Адамара как источник тестов квантовых компьютеров

С.Т. Хвощ

АО «Электронная компания «Элкус», Санкт-Петербург

Аннотация: Рассматривается вопрос вычисления симметричных матриц Адамара конструкции Балонина-Себерри. Для получения таких матриц требуется большое количество случайных двоичных последовательностей для выбора из них трех, которые связаны требованиями дизайна матриц. Такие последовательности являются первыми строками трех циклических блоков матриц Адамара. Рассматривается предыстория возникновения квантовых вычислений и преимущество квантовой генерации двоичных последовательностей для последующего отбора. Предлагается вычисление матриц Адамара как тестовая задача для квантовых компьютеров, позволяющая показать квантовое превосходство.

Ключевые слова: квантовые компьютеры, кубиты, генераторы случайных чисел, ортогональные матрицы, матрицы Мерсенна, кронекерово произведение.

Введение

Матрицы Адамара **H** порядка n с элементами ±1 являются классическими матрицами, содержащими в столбцах ортогональные последовательности [1]. Они используются для построения помехоустойчивых кодов и решения некоторых прикладных задач криптографии [2, 3]. Эти матрицы естественным образом вписываются в технологию квантовых вычислений. Более того, хорошо известная опорная матрица Адамара **H** порядка 2 описывает так называемый вентиль Адамара **U** [4] – это ортогональная **U**(α), или, в более общем случае, унитарная матица линейного оператора, описывающего поворот двумерного вектора в виде:

$$\mathbf{H}=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\ \mathbf{U}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\ \mathbf{U}(\alpha)=\begin{pmatrix}\cos(\alpha) & \sin(\alpha)\\ \sin(\alpha) & -\cos(\alpha)\end{pmatrix}.$$

Цепочки ортогональных преобразований, описываемых синусно-косинусной матрицей, зависящей от угла вращения, ввел еще Эйлер. С помощью углов можно выразить поворот орта в любую заданную позицию трехмерного пространства $\mathbf{R}=\mathbf{U}_1\mathbf{U}_2\mathbf{U}_3$. В семимерном пространстве, казалось бы, нужно 7 таких поворотов. Однако это не верно: количество матриц вращения зависит от порядка задачи n как $n(n–1)/2$ и требуется,

соответственно, 21 поворот. Эти соображения хорошо раскрывают особенность квантовых компьютеров. Их «процессор» отличается от арифметического устройства обычных компьютеров тем, что он в качестве элементарной операции рассматривает не сложение или умножение двоичного кода, с помощью которых вычисляются, в том числе, и матрицы Эйлера, а непосредственно унитарное преобразование **U**, которое не может быть любым. Это своего рода «мозаичная арифметика», поскольку нет возможности плавно осуществить поворот, но можно осуществить его очень быстро [5].

Общим местом теории матриц Адамара является правило Сильвестра $\begin{pmatrix} \mathbf{H} & \mathbf{H} \\ \mathbf{H} & -\mathbf{H} \end{pmatrix}$, согласно которому любую такую матрицу порядка n можно удвоить и, следовательно, порядки 2^k, где k = 1, 2, 3, 4,…, являются легко осваиваемыми на квантовых компьютерах. Эквивалентными преобразованиями (перегруппировкой столбцов) матрица Адамара отмеченного порядка сводится к так называемому виду Уолша, когда первый столбец не осциллирует совсем, он является аналогом постоянного сигнала, а последний – осциллирует с максимальной частотой, переключаясь между 1 и –1. Следовательно, столбцам матрицы можно приписать возрастающую частоту, то есть, использовать их в качестве спектральных матриц. Результат умножения вектора сигнала на такую матрицу есть вектор его спектра.

В максимально общем случае этот аппарат способствует вычислению как обычных, так и комплексных матриц так называемого быстрого преобразования Фурье (БПФ). БПФ - это основа цифровой обработки данных в трактах устройств, связанных с кодированием, маскированием, сжатием и другой обработкой информации, что повышает интерес к квантовым вычислениям.

Разумеется, поиск матриц Адамара для любого порядка $4t$, где t – натуральное число, а не только для сильвестровых порядков 2^k – это почти идеальная задача для проверки положения о квантовом превосходстве. Если квантовый компьютер вычислит симметричную матрицу Адамара порядка 428 или любую матрицу Адамара порядка 668, он гарантированно превзойдет все существующие на данный момент компьютеры, поскольку хорошо известно, что на обычных компьютерах такая задача еще не была решена.

Впервые на это обстоятельство обратило внимание исследование, освещающее практику использования квантовых компьютеров [6], и содержащее новые неизвестные ранее симметричные матрицы Адамара конструкции Пропус [7].

Цель настоящей статьи состоит в том, чтобы обратить внимание специалистов в области квантовых вычислений на матрицы Адамара как на источник тестов для оценки производительности квантовых компьютеров.

Необходимые термины и определения

Для удобства следует привести из работы [7] некоторые необходимые сведения.

Определение. Квазиортогональная матрица $\mathbf{A}$ порядка n – это квадратная матрица, удовлетворяющая уравнению $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \omega(n)\mathbf{I}$, где $\omega(n) = n–k$, при целом k, некоторая весовая функция, определяющая тип матрицы. $\mathbf{I}$ – единичная матрица $\mathrm{diag}\{1,1,1,\ldots 1\}$.

При $k = 0$ это матрицы Адамара, при $k = 1$ – матрицы Белевича, широко известные как конференц-матрицы [7].

При $k \geq 1$ матрицы рассматриваются как обобщение матриц Адамара и называются взвешенным матрицам $\mathbf{W}(n, n–k)$. Если значения $\omega(n)$ являются иррациональными, то для них принято обозначение $\mathbf{W}(n, \omega(n))$. Иными словами, квазиортогональная матрица является взвешенной матрицей с элементами $\{a=1, –b\}$ – вещественными числами.

Элементы матрицы с третьим значением d находятся обычно на ее диагонали $\{d, a=1, -b\}$ $(d \le b \le 1)$, а элемент s на ее кайме $\{a=1, -b, s\}$ $(b \le s \le 1)$. В работах [1, 7] такие матрицы названы критскими, что призвано подчеркнуть нецелочисленность значений их элементов.

Кронекерово умножение двух матриц **A** и **B** с элементами $\{1, -1\}$ в виде **C** = **A**⊗**B** реализуется вставкой матрицы **B** по месту элементов матрицы **A** с сохранением знака замещаемого элемента в виде:

$$\mathbf{A}\times\mathbf{B}=\begin{pmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B} & \ldots & a_{2n}\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}\mathbf{B} & a_{n2}\mathbf{B} & \ldots & a_{nn}\mathbf{B} \end{pmatrix}.$$

В результате кронекерова умножения двух матриц Адамара порядков n и m будет матрица Адамара порядка nm.

Таковы, кратко, основы теории, которая описывает ортогональные матрицы и дает почти все известные ныне ортогональные массивы. Слово *почти* тут основное. После основополагающих работ создателей базовых образцов ортогональных матриц было выяснено, что ни правило Сильвестра, ни обобщающее его правило Кронекера, ни некоторые другие похожие на них правила, не дают образцов матриц Адамара размера 92, 116, 156, 172 и многих других. Нетрудно заметить, что именно на эти порядки нацелена работа [6], где приводятся впервые найденные с помощью современных технологий симметричные матрицы Адамара отмеченных порядков, за исключением матрицы порядка 156.

Невозможно, например, посчитать Фурье спектры бинарных последовательностей произвольной длины. Всплески спектральных кривых свидетельствуют о наличии в последовательностях некоторых регулярных составляющих, следовательно, до 99% генерируемого для поиска матриц Адамара бесполезных последовательностей можно было бы отсеивать

пороговыми Фурье-фильтрами [8]. Сказанное не означает, что надо прекращать попытки нахождения матриц Адамара на отмеченных тестовых порядках, поскольку технологии совершенствуются не сразу.

Обозначения Дирака и квантовые вычисления

Поль Дирак, работая с вероятностями в диапазоне от 0 до 1, предложил вектор состояний вентиля [1,0] или [0,1] обозначать индексом (номером) позиции, где находится 1: начиная чертой |0> или |1>.

У реле это физически различимые положения контактов. Электрона мы не видим, где он, но подозреваем, что таковой есть. Понятие состояния суперпозиции родилось из предположения Шредингера о том, что электрон размазан по орбите, как «тесто». Тогда перед номером его позиции логично писать плотность, сколько теста пришлось на тот или иной «контакт». Борна смутило это «тесто», и он предложил считать цифру не плотностью, а вероятностью встретить электрон p1|0> или p2|1>.

Само собой, p1 + p2 = 1, ибо более в этой модели электрон нигде не бывает.

Помимо вероятностей можно писать комплексные числа, полагая, что квадрат модуля их характеризует вероятность, а сумма превращается в уравнение круга. Если использовать для характеристики кубита (элемента квантового компьютера) модули комплексных чисел и добавить в описание разности их фаз, получим параметры вектора, размещенного в сфере.

Вероятностный характер фиксируемого состояния кубитов наследует открытие Беккерелем феномена излучения радиевых лучей радиоактивного распада, также носящего вероятностный характер.

Несмотря на наличие в Интернет-источниках обзоров и научно-просветительских книг, квантовые компьютеры настолько сложно понимаемы, что выходят статьи, сомневающиеся в их существовании. Возможно это происходит потому, что в первой позитивной литературе

авторы увлекаются вероятностной интерпретацией квантового устройства Мира, а расчет вероятностей сложнее себе представить, чем работу реле, породившего обычный компьютер.

Таким образом, квантовый компьютер одновременно занят всеми возможными треками, каждый из которых отвечает своему расчету. Остается их разделить. Если вероятность выше, то результаты регистрации следуют чаще, и не могут отвечать слишком длинным траекториям.

В работе [6] отмечается, что квантовые технологии пока еще далеки от совершенства. Они встречаются с серьезными трудностями реализации вычислений на цепочках кубитов, удержания их в рабочем состоянии когерентности и т.п.

Однако наиболее распространенным сегодня применением кубитов является создание квантовых генераторов случайных чисел (ГСЧ). На компьютере как детерминированной системе может быть реализован только генератор псевдослучайных чисел (ГПСЧ), поскольку с использованием программы получить последовательность истинно случайных чисел невозможно. В контексте настоящей статьи этот факт определяет важное значение ГСЧ для вычисления матриц Адамара высоких порядков.

Генераторы псевдослучайных чисел и матицы Адамара

Матрицы Адамара сегодня плотно вошли в нашу жизнь. Их вычисление на больших порядках вызывает большие трудности, связанные с необходимостью генерации случайных последовательностей как основы их построения. Известен вихрь Мерсенна – алгоритм реализации генератора псевдослучайных чисел, позволяющий получать коды для построения матриц Мерсенна – основы построения матриц Адамара конструкции «ядро+кайма» [7].

На рис.1 приведен портрет циклической матрицы Мерсенна порядка $7 = 2^3 - 1$, взятый из статьи [7].

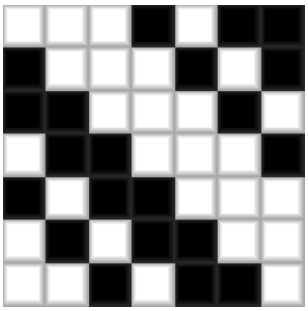

Рис. 1. Портрет циклической матрицы Мерсенна порядка 7 [7]

Эта квазиортогональная матрица с элементами $\{a=1, -b\}$, где $b=\frac{t}{t+\sqrt{t}}$ для $n=4t-1$. Она строится по определенным правилам, а ее базовыми порядками являются числа Мерсенна $p=2^k-1$, большинство из которых простые, что и дает ее простой вид.

Матрица Мерсенна, например, порядка $15=3\times5$ – циклическая, но не кососимметричная матрица. Из ее вектор-столбцов длины k образуются псевдослучайные коды вихря Мерсенна. Они обладают настолько серьезными преимуществами, что популярный генератор случайных чисел на C++ строится на основе именно этой матицы.

Каков же недостаток вихря Мерсенна для поиска матриц Адамара порядков 92, 116, 156, 172?

Матрицы Мерсенна с добавлением каймы образуют матрицы Адамара порядков 2^k, которые особенно просто строятся. Случайные последовательности 1 и –1, полученные на их основе, являются базовыми для их фильтрации фильтрами Фурье промежуточных для сильвестровых матриц порядков. Как видно, подобное строится подобным. Но это подобное, оно не совсем такое, какое нужно. ГПСЧ в силу детерминированности и ограниченности вычислительного ресурса при больших объемах генерации начинает выдавать повторяющиеся последовательности.

Выход из этого положения напрашивается почти очевидный. Потоки данных с квантовых ГСЧ можно направлять на фильтры Фурье [9],

построенные с помощью чипов, не квантовых. Получается чрезвычайно перспективная схема комбинированного компьютера, не квантового только, но и не совсем обычного.

Симметричные матрицы Адамара

Для синтеза симметричной матрицы Адамара необходимо найти не одну (как у матриц Мерсенна), не две (как у них же, но в двухблочной конфигурации), а три бинарные связанные последовательности. Это сокращает потребные длины последовательностей в 4 раза, например, для конструкции Пропус матриц Адамара. Это специфичная конструкция, у которой ради достижения симметрии из четырех циклических блоков **A**, **B**, **C**, **D** два равны **B** = **C**.

Кососимметичная **G** и симметричная **P** матицы Адамара с четырьмя блоками ищутся (сходными с массивом Вильямсона) в формах массива Себерри [1] и массива Балонина-Себерри [7]:

$$\mathbf{G}=\begin{pmatrix} \mathbf{A} & \mathbf{BR} & \mathbf{CR} & \mathbf{DR} \\ -\mathbf{BR} & \mathbf{A} & \mathbf{RD} & -\mathbf{RC} \\ -\mathbf{CR} & -\mathbf{RD} & \mathbf{A} & \mathbf{RB} \\ -\mathbf{DR} & \mathbf{RC} & -\mathbf{RB} & \mathbf{A} \end{pmatrix},\ \mathbf{P}=\begin{pmatrix} \mathbf{A} & \mathbf{BR}=\mathbf{CR} & \mathbf{CR}=\mathbf{BR} & \mathbf{DR} \\ \mathbf{CR} & \mathbf{RD} & -\mathbf{A} & -\mathbf{RB} \\ \mathbf{BR} & -\mathbf{A} & -\mathbf{RD} & \mathbf{RC} \\ \mathbf{DR} & -\mathbf{RC} & \mathbf{RB} & -\mathbf{A} \end{pmatrix},$$

где **R** – обратная единичная матрица с единицами вдоль второй не главной диагонали. Она служит для реверса и циклического смещения на такт первой строки для сохранения ортогональности массива в целом. Еще более общий массив Гетхальса-Зейделя не пользуется упрощением вида $\mathbf{B}^{\mathrm{T}}\mathbf{R}=\mathbf{RB}$, характерным для циклических блоков.

Алгоритм Сильвестра, с которого начинается знакомство с матицами Адамара, связан с порядками матриц, кратных 2^k, и не покрывает все возможные для таких ортогональных матриц порядки. Оказывается, что симметричные матицы Адамара, которые состоят из трех сопряженных определенным образом

последовательностей, удобны тем, что существуют без какого-либо ограничения на любом выделенном для матриц порядке. Чем удобны такие матрицы и почему суперкомьютеры могут использовать их как тесты?

Разложение матицы на блоки опирается не на теорему Лагранжа о разложении любого числа на сумму не более чем четырех чисел, а на теорему Гаусса.

Теорема Гаусса, одна из основных теорем алгебры чисел, свидетельствует о том, что любое число, независимо от того, простое оно или нет, разложимо на сумму трех треугольных чисел $T_a+T_b+T_d$ [10]. Дополнение Лиувилля говорит о том, что сумма может быть взвешенной $T_a+2T_b+T_d$. Оказывается, что троица T_a, $2T_b$ и T_d содержит орнаментальные инварианты блоков **A**, **B** и **D**. Следовательно, длины последовательностей сокращаются в четыре раза, а самих последовательностей нужно только три. Причем, так как начальный блок **A** разделяет симметрию матрицы в целом, первая последовательность оказывается еще и симметричной.

Заключение

Квантовые компьютеры – претенденты на практическую проверку гипотезы Адамара о существовании всех матриц порядков, кратных 4. Это следует из теорем Гаусса-Лиувилля. Однако нужны не только гипотезы, но и практически вычисленные матрицы. Порог производительности обычных компьютеров не позволяет получить матицу Адамара уже порядка 668, а в первой тысяче чисел наблюдается еще три таких порядка [2].

Аргументация, изложенная в работе [6], является весьма полезной, поскольку симметричные матрицы Адамара получены относительно недавно, и освещены в узкоспециализированной и известной не многим литературе.

Длина кода, генерируемого цепочкой из L кубитов, растет как 2^L. Матрицы Адамара в симметричной форме требуют меньшее количество кубитов для их вычисления, чем матрицы в каких-либо иных формах.

Литература

1. Jennifer S., Yamada M. Hadamard Matrices: Constructions using number theory and linear algebra. Wiley, 2020. 384 p.

2. Colbourn C.J., Dinitz J. H. Handbook of Combinatorial Designs, Second Edition. Chapman and Hall/CRC, 2007. 967 p.

3. Horadam K.J. Hadamard matrices and their applications. Princeton University Press, 2007. 263 p.

4. Бетеров И.И. Квантовые компьютеры на основе холодных атомов // Автометрия. 2020. Т. 56, № 4. С. 3-11.

5. Магомадов В.С. Квантовые вычисления, квантовая теория и искусственный интеллект // Инженерный вестник Дона. 2018. № 4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5424

6. Olivia Di Matteo. Methods for parallel quantum circuit synthesis, fault-tolerant quantum RAM, and quantum state tomography. A thesis for the degree of PhD in Physics-Quantum Information, Waterloo, Ontario, Canada, 2019. URL: uwspace.uwaterloo.ca/bitstream/handle/10012/14371/DiMatteo_Olivia.pdf?sequence=3&isAllowed=y

7. Балонин Н. А., Сергеев М. Б. Специальные матрицы: псевдообратные, ортогональные, адамаровы и критские. СПб.: Политехника, 2019. 196 с.

8. Balonin N. A., Balonin Y. N., Djokovic D. Z., Karbovskiy D. A., Sergeev M. B. Construction of symmetric Hadamard matrices // Информационно-управляющие системы. 2017. № 5. С. 2–11.

9. Fletcher R.J., Gysin M., and Seberry J. Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices // Australasian Journal of Combinatorics. 2001. Vol. 23. P. 75–86.

10. Деза Е. И. Специальные числа натурального ряда. – М.: Книжный дом «ЛИБРОКОМ», 2011. 240 с.

References

1. Jennifer S., Yamada M. Hadamard Matrices: Constructions using number theory and linear algebra. Wiley, 2020. 384 p.

2. Colbourn C.J., Dinitz J. H. Handbook of Combinatorial Designs, Second Edition. Chapman and Hall/CRC, 2007. 967 p.

3. Horadam K.J. Hadamard matrices and their applications. Princeton University Press, 2007. 263 p.

4. Beterov I.I. Avtometriya. 2020. Vol. 56, № 4. pp. 3-11.

5. Magomedov V.S. Inzhenernyj vestnik Dona. 2018. № 4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5424

6. Olivia Di Matteo. Methods for parallel quantum circuit synthesis, fault-tolerant quantum RAM, and quantum state tomography. A thesis for the degree of PhD in Physics-Quantum Information, Waterloo, Ontario, Canada, 2019. URL: uwspace.uwaterloo.ca/bitstream/handle/10012/14371/DiMatteo_Olivia.pdf?sequence=3&isAllowed=y

7. Balonin N.A., Sergeev M.B. Special'nye matricy: psevdoobratnye, ortogonal'nye, adamarovy i kritskie [Special matrices: pseudo-inverse, orthogonal, Hadamard and Cretan]. St. Peterburg: Polytechnic, 2019. 196 p.

8. Balonin N.A., Balonin Y.N., Djokovic D.Z., Karbovskiy D.A., Sergeev M.B. Informatsionno-Upravliaiushchie Sistemy. 2017. № 5. pp. 2–11.

9. Fletcher R.J., Gysin M., Seberry J. Australasian Journal of Combinatorics. 2001. Vol. 23. pp. 75–86.

10. Deza E. I. Special'nye chisla natural'nogo ryada [Special numbers of the natural series]. M.: Book house "LIBROCOM", 2011. 240 p.