

НЕКЛАССИЧЕСКИЕ ЛОГИЧЕСКИЕ ЭЛЕМЕНТЫ И КВАНТОВЫЕ КОМПЬЮТЕРЫ

Керп А.С., Лукоткин А.С.

Научный руководитель д-р физ.-мат. наук Цих А.К., аспирант кафедры ТФ СФУ

Куликов В.Р.

Сибирский федеральный университет

ВВЕДЕНИЕ

Квантовая информатика — новый раздел науки, возникший на стыке квантовой механики, алгоритмов и теории информации. В квантовой информатике изучаются общие принципы и законы, управляющие динамикой сложных квантовых систем. Квантовый компьютер — вычислительное устройство, работающее на основе принципов квантовой механики.

Идея построения квантового компьютера была предложена в 1980 году советским математиком Ю. И. Маниным. Эту идею поддержали физики, в частности, П. Бениоф и Нобелевский лауреат Р. Фейнман.

Необходимость в квантовом компьютере возникает тогда, когда мы пытаемся исследовать методами физики сложные многочастичные системы, подобные биологическим.

На данное устройство возлагаются большие надежды, поэтому ведется активная деятельность по его созданию. После открытия квантовой физики человеку потребовался новый инструмент для исследований. И именно квантовый компьютер стал современным устройством, позволяющим изучать различные явления и вычислять необходимые данные. Пока удалось построить только ограниченный компьютер, но этого хватило, чтобы убедиться в необходимости полноценного квантового компьютера.

Квантовый компьютер использует для вычисления неклассические алгоритмы, которые реализуются посредством неклассических логических элементов.

Логический элемент — устройство ЭВМ, выполняющее одну определенную операцию над входными сигналами согласно правилам алгебры логики (восходящим к Аристотелю). Например, логический элемент, отражающий переход к отрицанию, изображается следующей схемой:

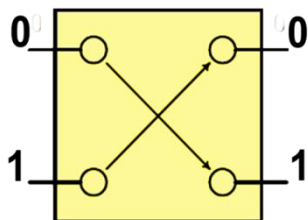


Рис. 1

Поскольку в логике отрицание высказывания образуется с помощью частицы НЕ, изображенный элемент будем обозначать символом НЕ.

В рамках действительного анализа нельзя построить логический элемент \sqrt{NE} , т.е. такой, для которого $\sqrt{NE} \times \sqrt{NE} = NE$, где под умножением подразумевается последовательное применения элемента. Иными словами, даже в рамках многозначной логики, основанной на классической теории вероятности, уравнение $X \times X = NE$ не разрешимо. Докажем это.

Отражающая это уравнение техническая схема такая:

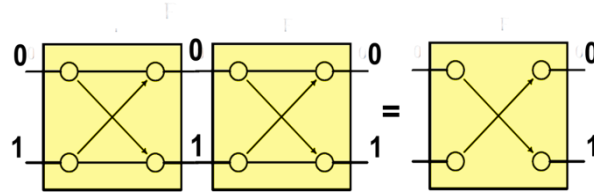


Рис. 2

Здесь слева подразумеваются две копии одного (неизвестного) логического элемента X .

Предполагается, что переходы $0 \rightarrow 0, 0 \rightarrow 1, 1 \rightarrow 0, 1 \rightarrow 1$ происходят с вероятностями $P_{00}, P_{01}, P_{10}, P_{11}$ (см. Рис.3).

Для элемента «NE» имеем:

$$P_{00}=P_{11}=0; P_{01}=P_{10}=1$$

Следовательно, для удовлетворения равенства $X \times X = NE$ получаем систему уравнений:

$$P_{00}P_{00}+P_{01}P_{10}=0;$$

$$P_{00}P_{01}+P_{01}P_{11}=1;$$

$$P_{10}P_{00}+P_{11}P_{10}=1;$$

$$P_{11}P_{11}+P_{10}P_{01}=0.$$

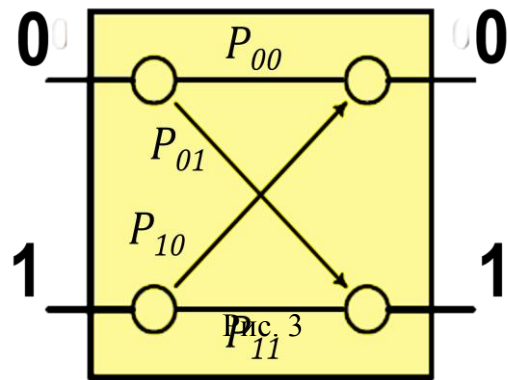


Рис. 3

Поскольку $P_{ij} \geq 0$, получаем $P_{00}=P_{11}=0$, тем самым $P_{00}P_{01}+P_{01}P_{11}=1$ или $P_{10}P_{00}+P_{11}P_{10}=1$ сводится к $0=1$. Таким образом, данная схема нереализуема для вещественных неотрицательных значений вероятностей P_{ij} .

Путь к реализации равенства подсказывает квантовая механика, в которой под амплитудой вероятности перехода $i \rightarrow j$ подразумевает комплексное число c_{ij} , для которого $P_{ij} = |c_{ij}|^2$. Таким образом, если в приведенной системе уравнений заменить P_{ij} на комплексные числа c_{ij} , то тогда следует рассмотреть уравнения

$$P(0 \rightarrow 0) = |c_{00}c_{00} + c_{01}c_{10}|^2$$

$$P(0 \rightarrow 1) = |c_{00}c_{01} + c_{01}c_{11}|^2$$

$$P(1 \rightarrow 0) = |c_{10}c_{00} + c_{11}c_{10}|^2$$

$$P(1 \rightarrow 1) = |c_{11}c_{11} + c_{10}c_{01}|^2$$

Теперь рассмотрим систему уравнений:

$$\begin{cases} 0 = |c_{00}c_{00} + c_{01}c_{10}|^2 \\ 1 = |c_{00}c_{01} + c_{01}c_{11}|^2 \\ 1 = |c_{10}c_{00} + c_{11}c_{10}|^2 \\ 0 = |c_{11}c_{11} + c_{10}c_{01}|^2 \end{cases} \quad (*)$$

Некоторые примеры корней данной системы уравнений были представлены в книге Гуца[2]:

$$c_{00} = c_{11} = i/\sqrt{2}; \quad c_{01} = e^{-i\alpha}/\sqrt{2}; \quad c_{10} = e^{i\alpha}/\sqrt{2}.$$

Ранее нами была доказана теорема о полном решении системы (*):

Теорема 1. Все комплексные решения системы (*) параметризуются в следующем виде через 2 параметра $\alpha, \beta \in [0; 2\pi]$: $c_{00} = c_{11} = e^{i\alpha}/\sqrt{2}$, $c_{01} = e^{i\beta}/\sqrt{2}$, $c_{10} = e^{i(\pi+2\alpha-\beta)}/\sqrt{2}$

Цель данной работы состоит в обобщении **Теоремы 1**, то есть в описании новых неклассических логических элементов.

В соответствии с поставленной целью, естественно были рассмотрены следующие задачи:

1. Найти математический язык для реализации последовательных применений неклассического элемента X , то есть X^2, X^3, \dots
2. Найти $\sqrt[n]{\text{НЕ}}, n \in \mathbb{N}$, то есть указать решения логического уравнения $X^n = \text{НЕ}$.
3. Выяснить вопрос о всех решениях уравнения $X^n = \text{НЕ}$ для $n \in \mathbb{N}$.

По сути, задача о поиске логического элемента $\sqrt{\text{НЕ}}$ свелась к нахождению матрицы, квадрат которой равен $\text{НЕ} = \begin{pmatrix} 0 & e^{i(\alpha-\beta)} \\ e^{i(\alpha+\beta)} & 0 \end{pmatrix}$, где $\alpha, \beta \in \mathbb{R}$. Такой способ представления матрицы НЕ позволит нам записать равенство $X^2 = \text{НЕ}$ в виде матричного уравнения.

$$\begin{pmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{pmatrix}^2 = \begin{pmatrix} c_{00}c_{00} + c_{01}c_{10} & c_{00}c_{01} + c_{01}c_{11} \\ c_{10}c_{00} + c_{11}c_{10} & c_{11}c_{11} + c_{10}c_{01} \end{pmatrix} = \begin{pmatrix} 0 & e^{i(\alpha-\beta)} \\ e^{i(\alpha+\beta)} & 0 \end{pmatrix}$$

Первое утверждение нашего исследования составляет

Лемма 1. Последовательное применение n раз неклассического элемента X соответствует возведению в n -ю степень комплексной матрицы $C = \begin{pmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{pmatrix}$, то есть X^n соответствует C^n .

Основным результатом данной работы является

Теорема 2. Решениями матричного уравнения $X^n = \text{НЕ}$ являются следующие матрицы:

$$X_{g,p} = \begin{pmatrix} \frac{1}{2} e^{i\frac{\alpha+\pi(2g+p)}{n}} (1 + e^{i\frac{\pi}{n}}) & \frac{1}{2} e^{i(\frac{\alpha+\pi(2g+p)}{n}-\beta-\pi p)} (1 - e^{i\frac{\pi}{n}}) \\ \frac{1}{2} e^{i(\frac{\alpha+\pi(2g+p)}{n}+\beta+\pi p)} (1 - e^{i\frac{\pi}{n}}) & \frac{1}{2} e^{i\frac{\alpha+\pi(2g+p)}{n}} (1 + e^{i\frac{\pi}{n}}) \end{pmatrix},$$

где $g = 0, \dots, n-1$; $p = 0, 1$.

При нечетных n появляется дополнительный набор решений:

$$X'_{g,p} = \begin{pmatrix} 0 & e^{i(\frac{\alpha+2\pi(2g+p)}{n}-\beta-\pi p)} \\ e^{i(\frac{\alpha+\pi(2g+p)}{n}+\beta+\pi p)} & 0 \end{pmatrix}.$$

Для доказательства Теоремы 2 мы задействуем следующие утверждения:

Лемма 2. Матрица $X = \begin{pmatrix} \frac{1}{2} e^{i\frac{\alpha}{n}} (e^{i\frac{\pi}{n}} + 1) & \frac{1}{2} e^{i(\frac{\alpha}{n}-\beta)} (1 - e^{i\frac{\pi}{n}}) \\ \frac{1}{2} e^{i(\frac{\alpha}{n}+\beta)} (1 - e^{i\frac{\pi}{n}}) & \frac{1}{2} e^{i\frac{\alpha}{n}} (e^{i\frac{\pi}{n}} + 1) \end{pmatrix}$ удовлетворяет

матричному уравнению $X^n = \text{HE}$.

Лемма 3. Матрица $X' = \begin{pmatrix} 0 & e^{i(\frac{\alpha}{n}-\beta)} \\ e^{i(\frac{\alpha}{n}+\beta)} & 0 \end{pmatrix}$ удовлетворяет матричному уравнению $X^n = \text{HE}$, при нечетных $n=2l+1$.

Доказательство лемм 2 и 3 основано на принципе математической индукции по степеням матриц X и X' .

Кроме того, если прибавить к показателям элементов матрицы HE числа, кратные $2\pi i$, то матрица HE не изменится. Однако подобный сдвиг изменит матрицы X и X' . Всевозможные сдвиги породят $2n$ различных матриц. Обозначим их $X_{g,p}$ и $X'_{g,p}$, где $g = 0, \dots, n-1$; $p = 0, 1$.

Полный текст доказательств лемм 1-3 мы здесь опускаем, однако можем сделать важный комментарий.

В случае $n = 2, 3, 4$ Теорема 2 предоставляет полный список решений логического уравнения $X^n = \text{HE}$. На основании этого наблюдения нами сформулирована

Гипотеза: Теорема 2 предоставляет полный список решений логического уравнения $X^n = \text{HE}$.

СПИСОК ЛИТЕРАТУРЫ

1. Мальцев А.И. Основы линейной алгебры / А.И. Мальцев – М.: Государственное издательство технико-теоретической литературы, 1956.
2. Гуц А.К. Комплексный анализ и информатика: учебное пособие / А.К. Гуц – Омск: Министерство образования Российской Федерации, Омский Государственный Университет Кафедра Информационной Безопасности, 2002. – 115с.