http://mmg.tversu.ru ISSN 2311-1275

MMG

Mathematical Modelling and Geometry

Том 8, No 3, стр. 1 – 14 (2020) doi:10.26456/mmg/2020-831

Формализм базиса Паули в квантовых вычислениях

В. В. Никонов[a] **and А. Н. Цирулёв**[b]

Факультет математики, Тверской государственный университет, Садовый пер. 35, Тверь, Россия

e-mail: [a] nikonov.vv@tversu.ru [b] tsirulev.an@tversu.ru

Получено 1 декабря 2020, в окончательной форме 28 декабря. Опубликовано 30 декабря 2020.

Abstract. Эта статья посвящена квантовым вычислениям в базисе Паули, элементы которого обычно отождествляются со строками Паули. Этот подход позволяет представлять квантовые состояния, наблюдаемые величины и унитарные операторы в единой форме линейной комбинации строк Паули, так что все операции могут быть сведены к композициям строк. Тем не менее, формальное обоснование использования базиса Паули для квантовых вычислений должно основываться на сильных результатах комплексной линейной алгебры и теории гильбертовых пространств. Мы кратко рассматриваем основные особенности строк Паули для квантовых состояний и унитарных операторов, а также ключевые операции с ними, включая алгоритм для композиций строк и алгоритм преобразования из стандартного базиса в базис Паули.

Keywords: квантовые вычисления, базис Паули

MSC numbers: 81P16, 81P68

1. Введение

Теория квантовых вычислений остается в центре внимания на протяжении последних двух десятилетий. Различные типы и подтипы квантовых вычислений адаптированы для различных технологий и архитектур аппаратного обеспечения, но их математические структуры построены с использованием одних и тех же основных понятий гильбертова пространства, квантовой наблюдаемой величины, унитарного оператора и квантового состояния. В этой статье мы рассматриваем взаимодействующую составную квантовую систему, состоящую из n идентичных двухуровневых подсистем (кубитов), так что размерность соответствующего гильбертова пространства равна 2^n. Квантовое вычисление в чистом состоянии с числом вентилей, которое полиномиально зависит от числа кубитов, может быть эффективно смоделировано классически. Поскольку универсальный квантовый компьютер, демонстрирующий квантовое превосходство, должен иметь большое количество кубитов, скажем, $n \geq 1000$, число базисных состояний составляет $2^n > 10^{300}$. Квантовые компьютеры с малым числом кубитов ($n \sim 100$), которые будут доступны в ближайшее время, должны использоваться вместе с классическим компьютером. В обоих случаях многокубитные квантовые вычисления очень чувствительны к выбору вычислительного базиса [1, 2, 3].

Существует два общих варианта выбора базиса, и какой из них более эффективен, зависит как от данного алгоритма, так и от конкретного типа квантового компьютера. Во-первых, мы можем использовать стандартный ортонормированный базис в гильбертовом пространстве и затем построить подходящий базис в алгебре линейных операторов. Однако этот подход оказывается неудобным и неестественным при рассмотрении задач, связанных со смешанными состояниями, графовыми состояниями [4], коррекцией ошибок [3, 5, 6], тензорными сетями [7, 8, 9] и более общими вопросами, где измерения не являются проективными [10, 11, 12]. Второй вариант напрямую работает с базисом в алгебре операторов, и в этом случае элементы базиса обычно не могут быть разложены в тензорное произведение некоторых кет и бра векторов; базис Паули считается наилучшим выбором, поскольку он эрмитов, ортонормирован (по отношению к внутреннему произведению Гильберта-Шмидта) и составляет ортонормированный базис в алгебре Ли соответствующей унитарной группы. Группа Клиффорда, имеющая многочисленные применения в квантовых вычислениях, наиболее просто описывается в терминах базиса Паули [10, 14].

Основная цель этой статьи — дать систематический алгебраический обзор многокубитных систем в базисе Паули. Статья организована следующим образом. Раздел 2 содержит некоторые необходимые математические предварительные сведения. В разделе 3 мы даем краткое описание квантовых состояний для n-кубитовой квантовой системы в базисе Паули. Раздел 4 посвящен изучению некоторых вычислительных свойств строк Паули. В разделе 5 мы рассматриваем алгоритмы вычислений, предназначенные для перехода от стандартного

базиса к базису Паули.

На протяжении всей статьи мы используем естественные единицы с $\hbar = c = 1$. Для удобочитаемости некоторые обозначения сделаны контекстно-зависимыми: строчные латинские буквы в двоичных строках (например, в символах бра и кет) принимают значения 0 и 1, тогда как в строках Паули и индексах они принимают значения от 0 до 3.

2. Основные особенности базиса Паули

Мы будем рассматривать квантовую систему из n различимых кубитов, где кубит ассоциируется с двумерным гильбертовым пространством $\mathcal{H}$ и его двойственным (эрмитово сопряженным) пространством $\mathcal{H}^\dagger$. Пусть $\mathcal{H}_n = \mathcal{H}^{\otimes n}$ и $\mathcal{H}_n^\dagger = \left(\mathcal{H}^\dagger\right)^{\otimes n}$ — гильбертово пространство системы и его двойственное пространство соответственно, и пусть $L(\mathcal{H}_n) = \mathcal{H}_n \otimes \mathcal{H}_n^\dagger$ — пространство линейных операторов, действующих на $\mathcal{H}$ и $\mathcal{H}^\dagger$ слева и справа соответственно. Тогда

$$\dim_{\mathbb{C}} \mathcal{H}_n = \dim_{\mathbb{C}} \mathcal{H}_n^\dagger = 2^n, \quad \dim_{\mathbb{C}} L(\mathcal{H}_n) = 2^{2n}.$$

Мы также будем предполагать, что пространство $L(\mathcal{H}_n)$ оснащено внутренним произведением Гильберта-Шмидта,

$$\langle \hat{A}, \hat{B} \rangle = \operatorname{tr}(\hat{A}^\dagger \hat{B}), \quad \hat{A}, \hat{B} \in L(\mathcal{H}_n), \tag{1}$$

которое является естественным расширением внутреннего произведения в $\mathcal{H}_n$. Реальное линейное пространство эрмитовых операторов обозначается далее как $H(\mathcal{H}_n)$.

Пусть $\{|0\rangle, |1\rangle\}$ — ортонормированный базис в некотором одномерном кубитовом пространстве $\mathcal{H}$. Единичная матрица и матрицы Паули,

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

определяют четыре оператора Паули

$$\hat{\sigma}_0 = |0\rangle\langle 0| + |1\rangle\langle 1|, \qquad \hat{\sigma}_1 = |0\rangle\langle 1| + |1\rangle\langle 0|,$$
$$\hat{\sigma}_2 = -i|0\rangle\langle 1| + i|1\rangle\langle 0|, \quad \hat{\sigma}_3 = |0\rangle\langle 0| - |1\rangle\langle 1|,$$

которые являются эрмитовыми и унитарными одновременно и которые образуют базис в $L(\mathcal{H})$. Обратное преобразование задается

$$|0\rangle\langle 0| = \frac{\hat{\sigma}_0 + \hat{\sigma}_3}{2}, \quad |0\rangle\langle 1| = \frac{\hat{\sigma}_1 + i\hat{\sigma}_2}{2}, \quad |1\rangle\langle 0| = \frac{\hat{\sigma}_1 - i\hat{\sigma}_2}{2}, \quad |1\rangle\langle 1| = \frac{\hat{\sigma}_0 - \hat{\sigma}_3}{2}.$$

Напомним, что для $k, l, m \in \{1, 2, 3\}$ имеем $\operatorname{tr} \hat{\sigma}_k = 0$, $\hat{\sigma}_k^2 = \hat{\sigma}_0$, и

$$\hat{\sigma}_k \hat{\sigma}_l = -\hat{\sigma}_l \hat{\sigma}_k, \quad \hat{\sigma}_k \hat{\sigma}_l = i \operatorname{sign}(\pi) \hat{\sigma}_m, \ (klm) = \pi(123), \tag{2}$$

где $\pi(123)$ — это перестановка множества $\{1, 2, 3\}$.

Существует *стандартный*[1] двоичный базис в $\mathcal{H}_n$, который генерируется ортонормированными базисами $\{|0\rangle, |1\rangle\}$ в соответствующих одномерных кубитовых пространствах. Математически позиция в тензорном произведении различает кубиты друг от друга. Поэтому для фиксированного n удобно записывать элемент этого базиса и соответствующий элемент двойственного базиса в виде

$$|k\rangle = |k_1 \dots k_n\rangle = |k_1\rangle \otimes \dots \otimes |k_n\rangle, \quad \langle k| = \langle k_1 \dots k_n| = \langle k_1| \otimes \dots \otimes \langle k_n|,$$

рассматривая строки $k_1 \dots k_n$ ($k_1, \dots, k_n \in \{0, 1\}$) как двоичное число и обозначая его десятичным представлением k. Например, $|101\rangle = |5\rangle$ и $|00110\rangle = |6\rangle$

В стандартном базисе,

$$|u\rangle = \sum_{k=0}^{2^n-1} u_k |k\rangle, \quad \hat{A} = \sum_{k,l=0}^{2^n-1} a_{kl} |k\rangle\langle l|,$$

где $|u\rangle \in \mathcal{H}_n$ и $\hat{A} \in L(\mathcal{H}_n)$.

Базис Паули $P(\mathcal{H}_n)$ в $L(\mathcal{H}_n)$ определяется как

$$\left\{\hat{\sigma}_{k_1 \dots k_n}\right\}_{k_1,\dots,k_n \in \{0,1,2,3\}}, \qquad \hat{\sigma}_{k_1 \dots k_n} = \hat{\sigma}_{k_1} \otimes \dots \otimes \hat{\sigma}_{k_n}, \tag{3}$$

где $\hat{\sigma}_{0\dots0}$ — единичный оператор. Очевидно, что $P(\mathcal{H}_n)$ состоит из 4^n элементов. Мы будем использовать компактные обозначения, такие как

$$\hat{\sigma}_K = \hat{\sigma}_{k_1 \dots k_n},$$

обозначая *строку Паули* $k_1 \dots k_n$, где $k_1, \dots, k_n \in \{0, 1, 2, 3\}$, соответствующей заглавной буквой K. При этом мы будем часто рассматривать K как число, то есть как десятичное представление строки; очевидно, что $0 \leqslant K \leqslant 4^n - 1$. Заметим, что строка Паули K и элемент $\hat{\sigma}_K$ базиса Паули полностью определяют друг друга и, следовательно, могут быть отождествлены. Например, элементы стандартного базиса выражаются через элементы базиса Паули в Приложении А1 на странице 13.

Полезно сравнить $P(\mathcal{H}_n)$ со стандартным базисом. Мы имеем

$$\hat{\sigma}_{k_1 \dots k_n} \hat{\sigma}_{k_1 \dots k_n} = \hat{\sigma}_{0\dots0}, \quad \operatorname{tr} \hat{\sigma}_{0\dots0} = 2^n, \quad \operatorname{tr} \hat{\sigma}_{k_1 \dots k_n}\big|_{k_1 \dots k_n \neq 0\dots0} = 0. \tag{4}$$

Базис Паули является эрмитовым, унитарным и ортогональным по отношению к внутреннему произведению (1). Заметим, что оператор $|k\rangle\langle l|$ стандартного базиса не является унитарным и не является эрмитовым, если $k \neq l$. Стандартный

[1] Мы не используем обычный термин "вычислительный так как он может привести к путанице. Базис Паули и стандартный базис вычислительны в одном и том же смысле.

базис не содержит единичного оператора, который имеет вид

$$\sum_{k=0}^{2^n-1} |k\rangle\langle k|$$

в этом базисе. В базисе Паули любой оператор $\hat{U}$ из унитарной группы $U(\mathcal{H}_n)$ (то есть $\hat{U}^\dagger\hat{U} = \hat{\sigma}_{0\ldots0}$) имеет разложение в виде

$$\hat{U} = \sum_{i_1,\ldots,i_n\in\{0,1,2,3\}} U_{i_1\ldots i_n}\hat{\sigma}_{i_1\ldots i_n}, \quad \hat{U}^\dagger = \sum_{i_1,\ldots,i_n\in\{0,1,2,3\}} \overline{U}_{i_1\ldots i_n}\hat{\sigma}_{i_1\ldots i_n},$$

где

$$\sum_{i_1,\ldots,i_n\in\{0,1,2,3\}} \overline{U}_{i_1\ldots i_n}U_{i_1\ldots i_n} = 1, \qquad \sum_{\substack{i_1,\ldots,i_n,\,j_1,\ldots,j_n\in\{0,1,2,3\}\\(i_1,\ldots,i_n)\neq(j_1,\ldots,j_n)}} \overline{U}_{i_1\ldots i_n}U_{j_1\ldots j_n} = 0.$$

Заметим, что последнее условие может быть очевидно разложено на $2^{2n-1}\big(2^n - 1\big)$ независимых условий.

3. Квантовые состояния в базисе Паули

Квантовое состояние (оператор плотности) — это эрмитов, положительно полуопределённый (или просто положительный) оператор вида

$$\hat{\rho} = \frac{1}{2^n} \sum_{k_1,\ldots,k_n\,\in\,\{0,1,2,3\}} a_{k_1\ldots k_n}\hat{\sigma}_{k_1\ldots k_n} \equiv \frac{1}{2^n}\sum_{K=0}^{4^n-1} a_K\hat{\sigma}_K, \tag{5}$$

где $a_{k_1\ldots k_n} \in \mathbb{R}$ и

$$a_{0\ldots0} = 1\,, \quad |a_{k_1\ldots k_n}| \leqslant 1, \qquad \sum_{k_1,\ldots,k_n\,\in\,\{0,1,2,3\}} (a_{k_1\ldots k_n})^2 \leqslant 2^n. \tag{6}$$

Условия (6) гарантируют, что $\hat{\rho}^\dagger = \hat{\rho}$, $\operatorname{tr}\hat{\rho} = 1$, и $\operatorname{tr}\hat{\rho}^2 \leqslant 1$. Для квантовых вычислений важно, что все коэффициенты в состоянии (5) являются действительными, и каждый из них, кроме $a_{0\ldots0}$, точно является результатом местного измерения с одним из базисных операторов (3), $a_K \equiv a_{k_1\ldots k_n} = \operatorname{tr}\big(\hat{\rho}\hat{\sigma}_{k_1\ldots k_n}\big)$. Все квантовые (чистые и смешанные) состояния образуют выпуклое множество (замкнутый многообразие, поскольку оно является прообразом 1 при отображении $\operatorname{tr} : H(\mathcal{H}_n) \to \mathbb{R}$) реальной размерности $4^n - 1$ в реальном линейном многообразии $\mathcal{S}_n \subset \operatorname{Span}\{P(\mathcal{H}_n)\} = H(\mathcal{H}_n)$, в то время как чистые состояния располагаются на границе $\mathcal{S}_n$ и составляют реальное подмногообразие размерности $2^{n+1} - 2$.

Каждый элемент $P(\mathcal{H}_n)$ является идемпотентом ($\hat{\sigma}_K\hat{\sigma}_K = \hat{\sigma}_{0\ldots0}$), так что операторы

$$\hat{P}_K^{\pm} = \frac{\hat{\sigma}_{0\ldots0} \pm \hat{\sigma}_K}{2}$$

являются проекторами. Таким образом, наблюдаемая величина $\hat{\sigma}_K = \hat{P}^+ - \hat{P}^-$ $\hat{\sigma}_K$ естественно сводится к проективным измерениям. Используя операторы $\hat{P}_K^{\pm}$, мы теперь можем доказать следующее практически важное утверждение, которое, по-видимому, не было рассмотрено в, по крайней мере, текущей литературе.

Proposition 1. *Условие* $|a_{k_1\ldots k_n}| \leqslant 1$ *в* (6) *следует из положительности оператора плотности* (5) *и первого условия в* (6).

Заметим, что эрмитовы проекторы $\hat{P}_K^{\pm} = \hat{P}_K^{\pm}\hat{P}_K^{\pm} = \big(\hat{P}_K^{\pm}\big)^{\dagger}\hat{P}_K^{\pm}$ являются положительными операторами, так как очевидны неравенства

$$\langle u|\hat{P}_K^{\pm}\,|u\rangle = \langle u|\big(\hat{P}_K^{\pm}\big)^{\dagger}\hat{P}_K^{\pm}\,|u\rangle \geqslant 0.$$

В общем случае эрмитов оператор $\hat{A} \in L(\mathcal{H}_n)$ является положительным тогда и только тогда, когда существует некоторый оператор $\hat{B} \in L(\mathcal{H}_n)$ такой, что $\hat{A} = \hat{B}\hat{B}^{\dagger}$; более того, $\hat{B}$ может быть выбрано эрмитовым [15]. Это, в свою очередь, подразумевает, что ($\hat{A}$ и $\hat{\rho}$ положительны)

$$\mathrm{tr}\big(\hat{A}\hat{\rho}\big) = \mathrm{tr}\big(\hat{B}\hat{B}^{\dagger}\hat{\rho}\big) = \mathrm{tr}\big(\hat{B}^{\dagger}\hat{\rho}\hat{B}\big) \geqslant 0,$$

так как $\hat{B}^{\dagger}\hat{\rho}\hat{B}$, очевидно, положителен. Таким образом,

$$\mathrm{tr}\big(\hat{P}_K^{\pm}\hat{\rho}\big) = \frac{1 \pm a_K}{2} \geqslant 0, \tag{7}$$

так что $-1 \leqslant a_K \leqslant 1$. Доказательство завершено. □

В качестве примера запишем одно из практически полезных состояний в стандартном базисе и в базисе Паули, а именно трехкубитное состояние Гринбергера-Хорна-Зейлингера. Используя оператор $CNOT$ и оператор Адамара $\hat{U}_2^+$, которые определены соотношениями (13) и (14) в Приложении А2, мы можем записать унитарное преобразование начального состояния $|000\rangle$ в состояние GHZ_3 в виде

$$\hat{U}_{\mathrm{GHZ}_3} = \big(\hat{\sigma}_0 \otimes CNOT\big)\circ\big(CNOT \otimes \hat{\sigma}_0\big)\circ\big(\hat{U}_2^+ \otimes \hat{\sigma}_{00}\big),$$

из которого легко найти

$$\begin{aligned}\hat{\rho}_{\mathrm{GHZ}_3} = = \frac{1}{2}\big(&|000\rangle\langle 000| + |000\rangle\langle 111| + |111\rangle\langle 000| + |111\rangle\langle 111|\big)\\ &= \frac{1}{8}\big(\hat{\sigma}_{000} + \hat{\sigma}_{111} - \hat{\sigma}_{122} - \hat{\sigma}_{212} - \hat{\sigma}_{221} + \hat{\sigma}_{033} + \hat{\sigma}_{303} + \hat{\sigma}_{330}\big).\end{aligned}$$

4. Операции со строками Паули

Нам понадобится несколько фактов и определений, связанных с базисом Паули и множеством строк Паули длины n,

$$\mathrm{Str}_n = \{K = k_1 \dots k_n\}_{k_1,\dots,k_n \in \{0,1,2,3\}}.$$

Во-первых, рассмотрим множество $\mathbb{F}_4 = \{0,1,2,3\}$ как группу Клейна с правилами умножения

$$0{*}k = k, \quad k{*}k = 0, \quad k{*}l = m,$$

где $k,l,m \in \{1,2,3\}$ и klm — любая перестановка 123. Во-вторых, пусть функция $s : \mathbb{F}_4 \times \mathbb{F}_4 \to \{1, i, -i\}$ определяется своими значениями

$$s(0,0) = s(0,k) = s(k,0) = s(k,k) = 1, \quad k = 1,2,3,$$

$$s(1,2) = s(2,3) = s(3,1) = i, \quad s(2,1) = s(3,2) = s(1,3) = -i.$$

Далее, пусть функция $S : \mathrm{Str}_n \times \mathrm{Str}_n \to \{1,-1,i,-i\}$, $(K,L) \mapsto S_{KL}$, определяется как произведение

$$S_{KL} = s(k_1,l_1)s(k_2,l_2)\dots s(k_n,l_n), \quad K = k_1k_2\dots k_n, \quad L = l_1l_2\dots l_n.$$

Функция S симметрична или антисимметрична в зависимости от количества пар (k_r,l_r) (r — позиция в строках K и L) таких, что $k_r,l_r \in \{1,2,3\}$ и $k_r \neq l_r$, а также в зависимости от их взаимного порядка. Пусть w^+_{KL} и w^-_{KL} обозначают количество пар видов $(1,2),(2,3),(3,1)$ и видов $(2,1),(3,2),(1,3)$ соответственно, а $w_{KL} = w^+_{KL} + w^-_{KL}$. Тогда

$$S_{KL} = (i)^{w_{KL}}(-1)^{w^-_{KL}}, \quad S_{(KL)} = \frac{S_{KL}}{2}\big(1+(-1)^{w_{KL}}\big), \quad S_{[KL]} = \frac{S_{KL}}{2}\big(1-(-1)^{w_{KL}}\big), \quad (8)$$

где круглые и квадратные скобки обозначают симметризацию и антисимметризацию, соответственно. Значения S_{KL}, $S_{(KL)}$, и $S_{[KL]}$ приведены в Таблице 2.

$w_{KL} \bmod 4$	0	2	0	2	1	3	1	3
$w^-_{KL} \bmod 2$	0	1	1	0	0	1	1	0
S_{KL}	1	1	−1	−1	i	i	$-i$	$-i$
$S_{(KL)}$	1	1	−1	−1	0	0	0	0
$S_{[KL]}$	0	0	0	0	i	i	$-i$	$-i$

Таблица 1: Коэффициенты перед $\hat\sigma_M$ в (9) для $\hat\sigma_K\hat\sigma_L$, $\{\hat\sigma_K,\hat\sigma_L\}$ и $[i\hat\sigma_K, i\hat\sigma_L]$.

Теперь композицию двух элементов базиса Паули и их антикоммутатор и коммутатор можно записать в виде компактных выражений, удобных для программирования на классическом компьютере:

$$\hat\sigma_K\hat\sigma_L = S_{KL}\hat\sigma_M, \quad \{\hat\sigma_K,\hat\sigma_L\} = S_{(KL)}\hat\sigma_M, \quad [i\hat\sigma_K, i\hat\sigma_L] = -S_{[KL]}\hat\sigma_M, \qquad (9)$$

где

$$\hat{\sigma}_M = \hat{\sigma}_{m_1 \dots m_n}, \quad m_1 = k_1 * l_1, \ \dots \ , m_n = k_n * l_n. \tag{10}$$

Заметим, что две строки Паули длины n могут коммутировать, даже если у них есть различные ненулевые элементы в некоторых одинаковых позициях. Например, три оператора $\hat{\sigma}_{11}$, $\hat{\sigma}_{22}$ и $\hat{\sigma}_{33}$ взаимно коммутируют. Также легко заметить, что унитарная матрица перехода, преобразующая стандартный базис $\big\{|i_1 \dots i_n\rangle\langle j_1 \dots j_n|\big\}$ в базис Паули, состоит только из элементов 0, ± 1 и $\pm i$. В частности,

$$|00\dots0\rangle\langle 00\dots0| \to \frac{1}{2^n} \sum_{i_1,\dots,i_n \in \{0,3\}} \hat{\sigma}_{i_1 \dots i_n}.$$

Более общо, стандартные ортогональные проекторы могут быть выражены как

$$|i_1 \dots i_n\rangle\langle i_1 \dots i_n|_{i_1,\dots,i_n \in \{0,1\}} = \frac{1}{2^n} \sum_{k_1,\dots,k_n \in \{0,3\}} \chi^{i_1}_{k_1} \cdots \chi^{i_n}_{k_n} \, \hat{\sigma}_{k_1 \dots k_n},$$

где

$$\chi^0_0 = \chi^0_3 = \chi^1_0 = 1, \quad \chi^1_3 = -1.$$

Некоторые важные операторы в базисе Паули приведены в Приложении А2 на странице 15.

Выражения (9) показывают, во-первых, что множество $\{i\hat{\sigma}_K\}_{K=0}^{4^n-1}$ образует ортонормированный базис в $\mathfrak{su}(n)$. И, во-вторых, множество

$$\widetilde{P}(\mathcal{H}_n) = \big\{\epsilon\hat{\sigma}_K \,|\, K \in \mathrm{Str}_n, \ \epsilon \in \{\pm 1, \pm i\}\big\},$$

состоящее из 4^{n+1} элементов, является группой; она называется Паули-группой (n-кубитовой). Нормализатор Паули-группы,

$$\mathcal{C}(\mathcal{H}_n) = \big\{\hat{U} \in U(\mathcal{H}_n) \mid \hat{U}\hat{\sigma}_K\hat{U}^\dagger \in \widetilde{P}(\mathcal{H}_n), \ \hat{\sigma}_K \in \widetilde{P}(\mathcal{H}_n)\big\},$$

называется группой Клиффорда. Из 2, 4, и 10 имеем следующее утверждение:

Proposition 2. *Взаимные унитарные преобразования операторов базиса Паули подчиняются соотношениям* $\hat{\sigma}_{i_1 \dots i_n}\hat{\sigma}_{k_1 \dots k_n}\hat{\sigma}_{i_1 \dots i_n} = \pm\hat{\sigma}_{i_1 \dots i_n}$, *где плюс берется только в том случае, если число троек* $(i_m k_m i_m)_{m \in \{1,\dots,n\}}$, *удовлетворяющих условиям* $i_m \neq k_m$, $i_m \neq 0$, *и* $k_m \neq 0$, *четно.*

5. Алгоритмы перехода к базису Паули

В стандартном базисе и в базисе Паули оператор $\hat{A} \in L(\mathcal{H}_n)$ (например, унитарное преобразование, наблюдаемая величина или оператор плотности) можно

выразить как

$$\hat{A} = \sum_{i_0,\ldots,i_{n-1},j_0,\ldots,j_{n-1}\in\{0,1\}} a_{i_{n-1}\ldots i_0 j_{n-1}\ldots j_0} |i_{n-1}\ldots i_0\rangle\langle j_{n-1}\ldots j_0| = \frac{1}{2^n} \sum_{i_0,\ldots,i_{n-1}\in\{0,1,2,3\}} s_{i_{n-1}\ldots i_0} \hat{\sigma}_{i_{n-1}\ldots i_0},$$

или, коротко,

$$\hat{A} \;=\; \sum_{i=0}^{2^n-1}\sum_{j=0}^{2^n-1} a_{ij}|i\rangle\langle j| \;=\; \frac{1}{2^n}\sum_{I=0}^{4^n-1} S_I\hat{\sigma}_I. \tag{11}$$

Таким образом, мы имеем дело с задачей вычисления коэффициентов S_I, когда заданы коэффициенты a_i; такой алгоритм недавно был предложен [13]. Наш подход основан на следующем наблюдении: все коэффициенты a_{ij} с двоичными строками $i = i_{n-1}\ldots i_0$ и $j = j_{n-1}\ldots j_0$, которые имеют одну и ту же сумму

$$k \;=\; (k_{n-1}\ldots k_0)_2 \;=\; (i_{n-1}\ldots i_0)_2 \oplus (j_{n-1}\ldots j_0)_2\,,$$

дают ненулевые вклады только в термины вида $S_l^{(i\oplus j)}\hat{\sigma}_l$, где l — двоичная строка $l_{n-1}\ldots i_0$, $0 \leqslant l \leqslant 2^n-1$, и операторы $\hat{\sigma}_l$ должны быть пересчитаны в форме (11). Прямолинейно (но громоздко) доказать, что строки $I = I(k,l) = \bigl[I_0^{(k)},\ldots,I_{2^n-1}^{(k)}\bigr]_4$, $k = i\oplus j$, в $\hat{\sigma}_I$ определяются

$$I = \bar{l}\wedge k + 2\bigl(l\wedge k\bigr) + 3\bigl(l\wedge\bar{k}\bigr), \tag{12}$$

где черта над буквой обозначает инверсию $0 \leftrightarrow 1$ для каждого символа соответствующей двоичной строки, а $\wedge$ обозначает логическую операцию И. На правой стороне в (12) мы рассматриваем результирующие двоичные строки как числа в четверичной системе. Для заданных двоичных строк i и j псевдокод этой процедуры приведен в Алгоритме 1.

Например, слагаемые

$$a_{010,001}|010\rangle\langle 001| = \frac{a_{21}}{2^3}\bigl(\hat{\sigma}_{011} + i\hat{\sigma}_{012} - i\hat{\sigma}_{021} + \hat{\sigma}_{022} + \hat{\sigma}_{311} + i\hat{\sigma}_{312} - i\hat{\sigma}_{321} + \hat{\sigma}_{322}\bigr),$$

$$a_{001,010}|001\rangle\langle 010| = \frac{a_{12}}{2^3}\bigl(\hat{\sigma}_{011} - i\hat{\sigma}_{012} + i\hat{\sigma}_{021} + \hat{\sigma}_{022} + \hat{\sigma}_{311} - i\hat{\sigma}_{312} + i\hat{\sigma}_{321} + \hat{\sigma}_{322}\bigr),$$

$$a_{101,110}|101\rangle\langle 110| = \frac{a_{56}}{2^3}\bigl(\hat{\sigma}_{011} - i\hat{\sigma}_{012} + i\hat{\sigma}_{021} + \hat{\sigma}_{022} - \hat{\sigma}_{311} + i\hat{\sigma}_{312} - i\hat{\sigma}_{321} - \hat{\sigma}_{322}\bigr),$$

$$a_{111,100}|111\rangle\langle 100| = \frac{a_{74}}{2^3}\bigl(\hat{\sigma}_{011} - i\hat{\sigma}_{012} - i\hat{\sigma}_{021} - \hat{\sigma}_{022} - \hat{\sigma}_{311} + i\hat{\sigma}_{312} + i\hat{\sigma}_{321} + \hat{\sigma}_{322}\bigr)$$

внесут вклад в линейную комбинацию $\hat{\sigma}_{011}$, $\hat{\sigma}_{012}$, $\hat{\sigma}_{021}$, $\hat{\sigma}_{022}$, $\hat{\sigma}_{311}$, $\hat{\sigma}_{312}$, $\hat{\sigma}_{321}$, и $\hat{\sigma}_{322}$ с

$$k = 010 \oplus 001 = 001 \oplus 010 = 101 \oplus 110 = 111 \oplus 100 = \mathbf{011}.$$

Элементы базиса Паули, возникающие в (12) из этих слагаемых, показаны в Таблице 2. Например, если $l = 5 = (101)_2$, то, в соответствии с (12),

$$I^{(3)}[5] = \big[(010)_2 \wedge (011)_2\big]_4 + 2\big[(101)_2 \wedge (011)_2\big]_4 + 3\big[(101)_2 \wedge (100)_2\big]_4 \\ = \big[010\big]_4 + 2\big[001\big]_4 + 3\big[100\big]_4 = 312.$$

Далее, в качестве примера, слагаемое $a_{101,110}|101\rangle\langle 110| = a_{56}|5\rangle\langle 6|$ вносит $ia_{56}/2^3$ в $S^{(3)}[5]$, так как существуют тройки $(l_0 i_0 j_0) = (110)_2$, $(l_1 i_1 j_1) = (001)_2$, и $(l_2 i_2 j_2) = (111)_2$ в Алгоритме 1 (строки 17 – 26); поэтому $sign = 1$, $c = 1$.

l	0	1	2	3	4	5	6	7
$l_2 l_1 l_0$	000	001	010	011	100	101	110	111
$k_2 k_1 k_0$	011	011	011	011	011	011	011	011
$\bar{l} \wedge k$	011	010	001	000	011	010	001	000
$l \wedge k$	000	001	010	011	000	001	010	011
$l \wedge \bar{k}$	000	000	000	000	100	100	100	100
$\hat{\sigma}_I$	$\hat{\sigma}_{011}$	$\hat{\sigma}_{012}$	$\hat{\sigma}_{021}$	$\hat{\sigma}_{022}$	$\hat{\sigma}_{311}$	$\hat{\sigma}_{312}$	$\hat{\sigma}_{321}$	$\hat{\sigma}_{322}$

Таблица 2: Элементы базиса Паули, возникающие для $k = 011$.

Algorithm 1 Преобразование в базис Паули.

Ввод количество кубитов n
Ввод строки $i = i_{n-1} \dots i_0$ и $j = j_{n-1} \dots j_0$, $i_s, j_s \in \{0, 1\}$
Ввод комплексное число a_{ij} — коэффициент в $a_{ij}|i\rangle\langle j|$
//Составить номер строки $k = i \oplus j$
Инициализация строки $k = \text{null}$
for $i_s = i_0, \dots, i_{n-1}$ **do**
    for $j_s = j_0, \dots, j_{n-1}$ **do**
        $k_s = i_s \oplus j_s$
    end for
end for
Преобразовать $(k_{n-1} \dots k_0)_2$ в int $(k)_{10}$
//Для числа k *заполнить два ряда*
Инициализация $S^{(k)}$ нулевым вектором длины 2^n с комплексным типом данных
Инициализация $I^{(k)}$ нулевой строковой матрицей длиной 2^n
Инициализация int $cntr$ и $sign \in \{1, -1, i, -i\}$ произвольными значениями
for $l = 0$ **до** $2^n - 1$ **do**
    Преобразовать $(l)_{10}$ в $(l_{n-1} \dots l_0)_2$
    $cntr = 0$ и $sign = 1$
    for $l_s = l_0, \dots, l_{n-1}$ **do**
        if $l_s == 1$ **then**
            если $(i_s, j_s) == (1, 1)$ **тогда** $sign = -sign$
            если $(i_s, j_s) == (0, 1)$ **тогда** $cntr = cntr + 1$
            если $(i_s, j_s) == (1, 0)$ **тогда** $sign = -sign, \quad cntr = cntr + 1$
        end if
    end for
    $I^{(k)}[l] = \bar{l} \wedge k + 2\big(l \wedge k\big) + 3\big(l \wedge \bar{k}\big)$
    int $c = cntr\,(mod 4)$, $S^{(k)}[l] \mathrel{+}= i^c \cdot sign \cdot a_{ij}$
end for
Возврат строки $S^{(k)}$ и $I^{(k)}$.

6. Заключение

В этой статье мы описали основную технику работы с базисом Паули. Показано, что эта техника может сделать более удобными и алгоритмичными некоторые манипуляции с математическими выражениями, связанными с квантовыми схемами с большим числом кубитов. Мы представили новый эффективный

алгоритм с полиномиальной сложностью для перехода от стандартного базиса к базису Паули.

Список литературы

[1] B. Dirkse, M. Pompili, R. Hanson, M. Walter, S. Wehner *Witnessing Entanglement in Experiments with Arbitrary Noise* Quantum Science and Technology **5**, 035007, 2020 (arXiv:1909.09119)

[2] I. Hamamura and T. Imamichi *Efficient evaluation of quantum observables using entangled measurements* npj Quantum Information **6**, 56, 2020 (arXiv:1909.09119)

[3] O. Crawford, B. van Straaten, D. Wang, T. Parks, E. Campbell, S. Brierley *Efficient quantum measurement of Pauli operators in the presence of finite sampling error* Quantum **5**, 385–404, 2021 (arXiv:1908.06942)

[4] W. Klobus et al. *Higher dimensional entanglement without correlations.* Eur. Phys. J. D **73**, 29, 2019 (arXiv:1808.10201)

[5] T.J. O'Connor, Y. Yu, B. Helou, R. Laflamme *The robustness of magic state distillation against errors in Clifford gates* Quantum Information & Computation **13**, 361–378, 2013 (arXiv:1205.6715)

[6] C.A. Riofrio, D. Gross, S.T. Flammia, T. Monz, D. Nigg, R. Blatt, J. Eisert *Experimental quantum compressed sensing for a seven-qubit system* Nature Comm. **8**, 15305, 2017 (arXiv:1608.02263)

[7] S.S. Jahromi, R. Orus *A universal tensor network algorithm for any infinite lattice* Phys. Rev. D **99**, 195105, 2019 (arXiv:1808.00680)

[8] A.N. Tsirulev *A geometric view on quantum tensor networks* Europ. Phys. J. Web of Conferences **226**, No 4, 2020 (https://doi.org/10.1051/epjconf/202022602022)

[9] I.M. Potashov, A.N. Tsirulev *Computational Algorithm for Covariant Series Expansions in General Relativity* Europ. Phys. J. Web of Conferences **173**, 03021, 2018 (https://doi.org/10.1051/epjconf/201817303021)

[10] S. Bravyi and A. Kitaev *Universal quantum computation with ideal Clifford gates and noisy ancillas* Phys. Rev. A **71**, 022316, 2005 (arXiv:quant-ph/0403025)

[11] V. Danos and E. Kashefi *Determinism in the one-way model* Phys. Rev. A. **74**, 052310, 2006 (arXiv:quant-ph/0506062)

[12] V. Danos and E. Kashefi *Pauli measurements are universal* Electronic Notes in Theoretical Computer Science **170**, 95–100, 2007 (https://doi.org/10.1016/j.entcs.2006.12.013)

[13] D. Gunlycke, M.C. Palenik, and S.A. Fischer *Efficient algorithm for generating Pauli coordinates for an arbitrary linear operator* 2020 (arXiv:2011.08942)

[14] S. Bravyi and D. Maslov *Hadamard-free circuits expose the structure of the Clifford group.* 2020 (arXiv: 2003.09412)

[15] I. Bengtsson, K. Zyczkowski *Geometry of Quantum States: An Introduction to Quantum Entanglement.* Cambridge University Press, Cambridge, 2006

[16] V.V. Shende, I.L. Markov, and S.S. Bullock *Minimal universal twoqubit controlled-NOT-based circuits* Phys. Rev. A, **69**, 062321, 2004 (arXiv:quant-ph/0308033)

Приложение

A1. Базис Паули для $n = 2$

Для справки мы приведем здесь выражения элементов стандартного базиса в $\mathcal{H}_2$ в терминах элементов базиса Паули. Напомним, что такие выражения в $\mathcal{H}_1$ имеют вид

$$|0\rangle\langle 0| = \frac{\hat{\sigma}_0 + \hat{\sigma}_3}{2}\,, \quad |0\rangle\langle 1| = \frac{\hat{\sigma}_1 + i\hat{\sigma}_2}{2}\,, \quad |1\rangle\langle 0| = \frac{\hat{\sigma}_1 - i\hat{\sigma}_2}{2}\,, \quad |1\rangle\langle 1| = \frac{\hat{\sigma}_0 - \hat{\sigma}_3}{2}\,.$$

$$|00\rangle\langle 00| = \frac{\hat{\sigma}_{00} + \hat{\sigma}_{03} + \hat{\sigma}_{30} + \hat{\sigma}_{33}}{4}\,, \qquad |01\rangle\langle 00| = \frac{\hat{\sigma}_{01} - i\hat{\sigma}_{02} + \hat{\sigma}_{31} - i\hat{\sigma}_{32}}{4}\,,$$

$$|10\rangle\langle 00| = \frac{\hat{\sigma}_{10} + \hat{\sigma}_{13} - i\hat{\sigma}_{20} - i\hat{\sigma}_{23}}{4}\,, \qquad |11\rangle\langle 00| = \frac{\hat{\sigma}_{11} - i\hat{\sigma}_{12} - i\hat{\sigma}_{21} - \hat{\sigma}_{22}}{4}\,,$$

$$|00\rangle\langle 01| = \frac{\hat{\sigma}_{01} + i\hat{\sigma}_{02} + \hat{\sigma}_{31} + i\hat{\sigma}_{32}}{4}\,, \qquad |01\rangle\langle 01| = \frac{\hat{\sigma}_{00} - \hat{\sigma}_{03} + \hat{\sigma}_{30} - \hat{\sigma}_{33}}{4}\,,$$

$$|10\rangle\langle 01| = \frac{\hat{\sigma}_{11} + i\hat{\sigma}_{12} - i\hat{\sigma}_{21} + \hat{\sigma}_{22}}{4}\,, \qquad |11\rangle\langle 01| = \frac{\hat{\sigma}_{10} - \hat{\sigma}_{13} - i\hat{\sigma}_{20} + i\hat{\sigma}_{23}}{4}\,,$$

$$|00\rangle\langle 10| = \frac{\hat\sigma_{10} + \hat\sigma_{13} + i\hat\sigma_{20} + i\hat\sigma_{23}}{4}, \qquad |01\rangle\langle 10| = \frac{\hat\sigma_{11} - i\hat\sigma_{12} + i\hat\sigma_{21} + \hat\sigma_{22}}{4},$$
$$|10\rangle\langle 10| = \frac{\hat\sigma_{00} + \hat\sigma_{03} - \hat\sigma_{30} - \hat\sigma_{33}}{4}, \qquad |11\rangle\langle 10| = \frac{\hat\sigma_{01} - i\hat\sigma_{02} - \hat\sigma_{31} + i\hat\sigma_{32}}{4},$$

$$|00\rangle\langle 11| = \frac{\hat\sigma_{11} + i\hat\sigma_{12} + i\hat\sigma_{21} - \hat\sigma_{22}}{4}, \qquad |01\rangle\langle 11| = \frac{\hat\sigma_{10} - \hat\sigma_{13} + i\hat\sigma_{20} - i\hat\sigma_{23}}{4},$$
$$|10\rangle\langle 11| = \frac{\hat\sigma_{01} + i\hat\sigma_{02} - \hat\sigma_{31} - i\hat\sigma_{32}}{4}, \qquad |11\rangle\langle 11| = \frac{\hat\sigma_{00} - \hat\sigma_{03} - \hat\sigma_{30} + \hat\sigma_{33}}{4}.$$

A2. Некоторые унитарные операторы в базисе Паули

Оператор CNOT:

$$CNOT = \frac{\hat\sigma_{00} + \hat\sigma_{01} + \hat\sigma_{30} - \hat\sigma_{31}}{2} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|, \quad (13)$$

Контролируемый фазовый оператор:

$$CZ = \frac{\hat\sigma_{00} + \hat\sigma_{03} + \hat\sigma_{30} - \hat\sigma_{33}}{2} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|.$$

Известно, что $CNOT$ и CZ принадлежат группе Клиффорда $\mathcal{C}(\mathcal{H}_2)$. Также известны некоторые множества генераторов и канонические формы для операторов группы $\mathcal{C}(\mathcal{H}_n)$ (см., например, [14]), но количество элементов в этих группах растет экспоненциально (фактически немного быстрее) с ростом n: например, $\mathcal{C}(\mathcal{H}_1)$ порядка 24, а $\mathcal{C}(\mathcal{H}_2)$ порядка 11520. Поэтому возникает проблема нахождения практически подходящего [16] набора унитарных операторов для построения групп Клиффорда и соответствующего формализма стабилизаторов. Здесь мы вводим однокубитовый оператор Адамара $\hat U_2^+$ и псевдо-Адамаровы операторы $\hat U_2^-$, $\hat U_1^\pm$ и $\hat U_3^\pm$, подчиняющиеся соотношениям $\left(\hat U_1^\pm\right)^2 = \left(\hat U_2^\pm\right)^2 = \left(\hat U_3^\pm\right)^2 = \hat\sigma_0$. Они унитарны и эрмитовы и определяются

$$\begin{aligned}
\hat U_1^\pm &= \frac{\hat\sigma_2 \pm \hat\sigma_3}{\sqrt{2}} = \frac{1}{\sqrt{2}}\big(\pm|0\rangle\langle 0| - i|0\rangle\langle 1| + i|1\rangle\langle 0| \mp |1\rangle\langle 1|\big),\\
\hat U_2^\pm &= \frac{\hat\sigma_1 \pm \hat\sigma_3}{\sqrt{2}} = \frac{1}{\sqrt{2}}\big(\pm|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| \mp |1\rangle\langle 1|\big), \qquad (14)\\
\hat U_3^\pm &= \frac{\hat\sigma_1 \pm \hat\sigma_2}{\sqrt{2}} = \mathrm{e}^{\mp i\pi/4}|0\rangle\langle 1| \pm \mathrm{e}^{\pm i\pi/4}|1\rangle\langle 0|.
\end{aligned}$$

Они могут быть использованы для построения унитарных преобразований $\hat\sigma_i \leftrightarrow \pm\hat\sigma_j$ $(i \neq j)$ и $\hat\sigma_i \to -\hat\sigma_i$ $(i = 1, 2, 3)$:

$$\hat U_k^\pm \hat\sigma_i \hat U_k^\pm = \pm\hat\sigma_j, \quad \hat U_k^\pm \hat\sigma_k \hat U_k^\pm = -\hat\sigma_k, \quad i \neq j \neq k, \;\; i, j, k \in \{1, 2, 3\},$$

или, более подробно,

$$\hat{U}_1^{\pm}\hat{\sigma}_2\hat{U}_1^{\pm} = \pm\hat{\sigma}_3, \quad \hat{U}_1^{\pm}\hat{\sigma}_3\hat{U}_1^{\pm} = \pm\hat{\sigma}_2, \quad \hat{U}_1^{\pm}\hat{\sigma}_1\hat{U}_1^{\pm} = -\hat{\sigma}_1,$$

$$\hat{U}_2^{\pm}\hat{\sigma}_1\hat{U}_2^{\pm} = \pm\hat{\sigma}_3, \quad \hat{U}_2^{\pm}\hat{\sigma}_3\hat{U}_2^{\pm} = \pm\hat{\sigma}_1, \quad \hat{U}_2^{\pm}\hat{\sigma}_2\hat{U}_2^{\pm} = -\hat{\sigma}_2,$$

$$\hat{U}_3^{\pm}\hat{\sigma}_1\hat{U}_3^{\pm} = \pm\hat{\sigma}_2, \quad \hat{U}_3^{\pm}\hat{\sigma}_2\hat{U}_3^{\pm} = \pm\hat{\sigma}_1, \quad \hat{U}_3^{\pm}\hat{\sigma}_3\hat{U}_3^{\pm} = -\hat{\sigma}_3.$$

Далее, для однородности, обозначим $\hat{\sigma}_0$ как $\hat{U}_0$. Таким образом, например, мы можем выбрать полный набор генераторов для $\mathcal{C}(\mathcal{H}_1)$ в виде ($\hat{U}_i \equiv \hat{U}_i^{+}$, $i = 1, 2, 3$)

$$\{\hat{U}_0, \hat{U}_1, \hat{U}_2, \hat{U}_3\}.$$

В общем случае $\widetilde{P}(\mathcal{H}_n)$, полный набор генераторов для группы $\mathcal{C}(\mathcal{H}_n)$ составляют операторы вида

$$\{\hat{U}_{i_1\ldots i_n} = \hat{U}_{i_1} \otimes \cdots \otimes \hat{U}_{i_n}\}_{i_1,\ldots,i_n \in \{0,1,2,3\}}.$$