XII семинар Д.Н. Клышко. Квантовая оптика

Распараллеливание квантовых алгоритмов с помощью квантовой телепортации

С.С. Сысоев[1, *]

[1] *Международный математический институт им. Леонарда Эйлера*
Россия, 199178, Санкт-Петербург, 14-я линия В.О. д. 29Б

(Поступила в редакцию 13.12.2024; после доработки 20.02.2025; подписана в печать 24.02.2025)

В работе предложен метод распараллеливания квантовых алгоритмов в схемной модели, основанный на технике телепортации квантовых гейтов. Получаемое таким образом параллельное представление алгоритма имеет меньшую глубину схемы и, следовательно, большую вероятность корректного исполнения в условиях растущей со временем декогеренции квантового состояния. Сокращение длины схемы достигается за счет увеличения ее ширины — количества одновременно используемых в вычислениях кубитов.

PACS: 03.67.Ac УДК: 519.6
Ключевые слова: квантовая телепортация, квантовые алгоритмы, параллельные вычисления.

DOI: 10.55959/MSU0579-9392.80.2530406

ВВЕДЕНИЕ

Универсальные квантовые вычисления в схемной модели, впервые предложенные Д. Дойчем [1] и получившие дальнейшее развитие, например в [2–5], позволяют разрабатывать квантовые алгоритмы в парадигме, привычной для специалистов по классическим вычислениям. Схема квантового алгоритма (рис. 1) представляет собой последовательное выполнение элементарных операций (квантовых гейтов) над регистрами, состоящими из квантовых битов (кубитов). Каждый кубит является квантовой системой с двумерным пространством состояний, поэтому вектор состояния регистра из n кубитов имеет размерность 2^n. Алгоритмы математически представляют собой унитарные преобразования в этом пространстве. В [6] показано, что для любого унитарного преобразования существует его аппроксимация в виде произведения элементарных преобразований из конечного набора. Такой набор является аналогом универсального набора элементарных логических операций в классических вычислениях. В качестве примера универсального набора квантовых гейтов можно привести множество $\{R_x(\theta), R_y(\theta), R_z(\theta), CX\}$, где $R_p(\theta) = e^{i\frac{\theta}{2}P}$, $P \in \{X, Y, Z\}$ — однокубитные повороты вокруг соответствующих осей на сфере Блоха на произвольный угол θ, а $CX = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$ — единственная двухкубитная операция (X, Y, Z здесь и далее — операторы Паули).

Для схемной модели разработаны алгоритмы, демонстрирующие ее преимущество над известными классическими алгоритмами. Среди наиболее известных примеров можно назвать алгоритм Шора [5], предназначенный для поиска периода функции, и алгоритм Гровера [7], осуществляющий поиск прообраза некоторого значения для функции, необратимой на практике. Алгоритм Шора дает экспоненциальное ускорение по сравнению с известными классическими алгоритмами за счет эффективной декомпозиции квантового аналога преобразования Фурье. Алгоритм Гровера дает квадратичное ускорение по числу вычислений анализируемой функции. Для демонстрации преимущества этих алгоритмов на реальных практических задачах необходимы квантовые компьютеры, работающие в схемной модели. Масштабирование задач в схемной модели подразумевает рост двух параметров схемы — ее ширины (количества одновременно используемых кубитов) и глубины — количества последовательных операций, выполняемых над кубитами до существенной декогеренции квантового состояния. Современные квантовые компьютеры имеют достаточную ширину для демонстрации квантового превосходства, но глубина на них достигает лишь нескольких десятков операций, что на несколько порядков ниже требуемых значений. Это справедливо для вычислителей, реализованных, например, на трансмонах, где верность двухкубитного преобразования уже достигает 99.9% [8, 9], а скорость декогеренции кубитов очень высока [10]. Для фотонных кубитов ситуация противоположна — фотоны значительно проще защитить от взаимодействия с окружением, но двухкубитные преобразования выполняются на них с низкой вероятностью, что усложняет масштабирование схем как в ширину, так и в глубину.

Традиционным подходом к увеличению точности квантовых вычислений за счет увеличения количества используемых кубитов являются коды коррекции ошибок [11, 12]. Основной идеей этого подхода является кодирование одного кубита при помощи нескольких, с помощью комбинаций, устойчивых к ошибкам разного рода. При этом, помимо уве-

* E-mail:s.s.sysoev@spbu.ru

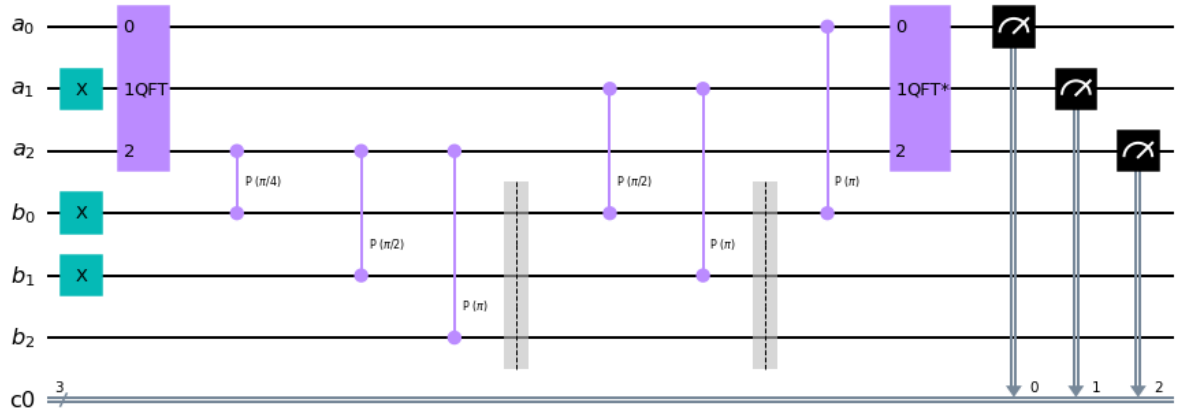

Рис. 1. Пример квантового алгоритма сложения двух чисел. Горизонтальные линии соответствуют кубитам. Однокубитные гейты располагаются на кубитах в порядке их применения. Двухкубитные гейты представлены вертикальными линиями, с точками на кубитах, к которым они применяются. Блоки QFT и QFT^* инкапсулируют в себе алгоритмы прямого и обратного квантового преобразования Фурье. Черные квадраты обозначают измерение состояния кубита, на котором они расположены, с записью измеренного значения в классический бит

личения количества кубитов, усложняется и схема алгоритма, в которую включаются блоки обнаружения и исправления ошибки. Масштабируемость процедуры коррекции также ограничена общим временем жизни квантового состояния, так как время исполнения алгоритма не уменьшается.

Одним из подходов к сокращению времени выполнения алгоритма в классической теории вычислений является его распараллеливание. Прямолинейный подход к распараллеливанию алгоритма Гровера подразумевает разделение пространства поиска на два подпространства, например по значению одного из битов аргумента функции, и запуск алгоритма на двух системах с меньшей размерностью. При этом квадратичное ускорение, обеспечиваемое алгоритмом Гровера, оказывается не на нашей стороне, поскольку время выполнения алгоритма уменьшается также квадратично (в $\sqrt{2}$ вместо 2 раз).

В настоящей работе предложен метод, позволяющий ускорять квантовые алгоритмы за счет использования телепортации квантовых гейтов. Работа организована следующим образом: в разделе 2 описывается методика телепортации квантовых гейтов. Раздел 3 посвящен описанию алгоритма Гровера в виде, удобном для демонстрации предлагаемого метода. В разделе 4 представлена общая схема алгоритма Гровера, ускоренного в 2 раза за счет трехкратного увеличения ширины схемы. В заключении приводятся общие соображения относительно универсальности предлагаемого метода.

1. ТЕЛЕПОРТАЦИЯ КВАНТОВЫХ ГЕЙТОВ

Общая схема телепортации однокубитного квантового состояния, предложенная в [13], представлена на рис. 2. Верхний кубит несет состояние $|\phi\rangle$, которое будет телепортировано в нижний кубит. Кубиты b_0 и b_1 первоначально инициализированы состоянием $|0\rangle$. На первом шаге происходит подготовка в них запутанного ресурса — состояния Белла $B_{00} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. На втором шаге алгоритма кубиты $|\phi\rangle$ и b_0 переводятся в базис Белла, после чего на третьем шаге происходит их измерение. По результатам этого измерения к кубиту b_1 применяются корректирующие преобразования (Z, управляемое результатом в кубите b_0, и X, управляемое результатом в верхнем кубите). В результате этой процедуры состояние в верхнем кубите разрушается измерением, а в кубите b_1 оказывается состояние $|\phi\rangle$.

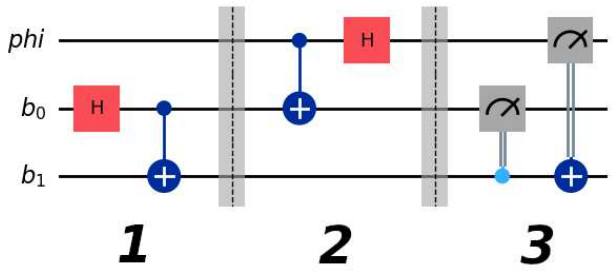

Рис. 2. Алгоритм квантовой телепортации однокубитного состояния. Шаг 1 — подготовка ресурсного состояния Белла. Шаг 2 — переход в базис Белла. Шаг 3 — измерение в базисе Белла и корректировка результирующего состояния по результатам измерения

В работе [14] представлена схема телепортации, в результате которой вместо первоначального состояния $|\phi\rangle$ в кубите b_1 оказывается состояние $U|\phi\rangle$. Эта схема позволяет реализовать вычисления над однокубитным состоянием $|\phi\rangle$, не применяя к нему

оператор U непосредственно. Вместо этого оператор U применяется параллельно к одному из кубитов запутанного ресурса — поэтому такой подход называется телепортацией квантовых гейтов. Схема для случая $U = H$ представлена на рис. 3. Здесь и далее H — преобразование Адамара:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1}$$

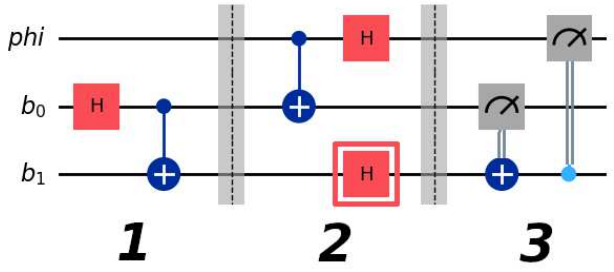

Рис. 3. Алгоритм квантовой телепортации гейта H. Гейт H применяется на втором шаге алгоритма к ресурсному состоянию b_1. Процедура коррекции на шаге 3 изменена (гейты коррекции поменялись местами). В результате в кубите b_1 получается состояние $H|\phi\rangle$

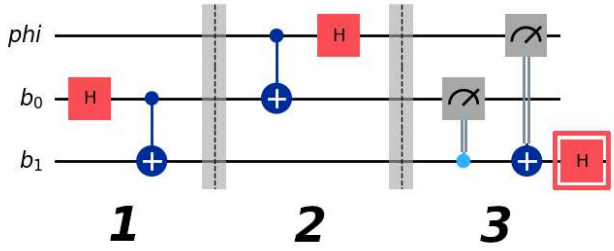

Рис. 4. Алгоритм вычисления $H|\phi\rangle$ без телепортации гейта. Гейт H применяется к $|\phi\rangle$ после завершения процедуры телепортации

На ней гейт H применяется к кубиту приемнику состояния — b_1, до момента коррекции по результатам измерения. Из-за этого процедура коррекции должна быть изменена, поскольку гейт H не коммутирует с гейтами X и Z, участвующими в коррекции:

$$HZ = XH, \tag{2}$$

$$HX = ZH. \tag{3}$$

Схема телепортации гейта H с рис. 3 может быть получена из схемы на рис. 4 переносом гейта H справа налево через корректирующие гейты X и Z с учетом соотношений (2) и (3).

Для двухкубитных гейтов в [14] предложена схема телепортации гейта CX, представленная на рис. 5, что делает репертуар вычислений с телепортацией универсальным. На первом шаге подготавливаются два ресурсных состояния Белла. На втором шаге происходит переход в базис Белла для информационных состояний — контрольного $|\psi\rangle$ и контролируемого $|\phi\rangle$ с одним кубитом из пары ресурсных состояний, после чего на шаге 3 происходит измерение и коррекция состояния. Результат $CX|\psi\phi\rangle$ оказывается в кубитах $b1_1$ и $b2_0$.

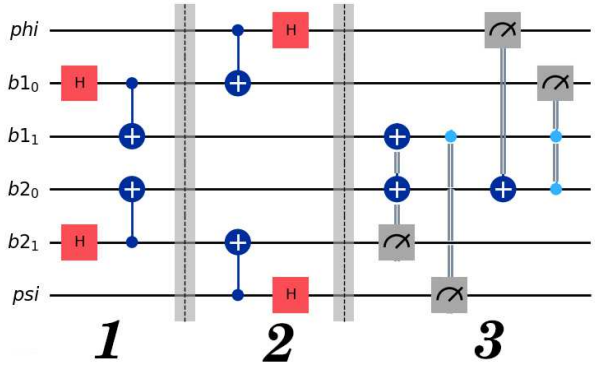

Рис. 5. Алгоритм телепортации гейта CX

2. АЛГОРИТМ ГРОВЕРА

Алгоритм Гровера [7] представляет собой обобщенный алгоритм для решения задач из класса NP. NP — класс сложности, включающий в себя все поисковые задачи, для которых проверка решения может быть осуществлена алгоритмом, работающим за полиномиальное время от размера входных данных. Гровер формализует этот алгоритм проверки в виде функции f_ω, принимающей на вход n-битные числа и возвращающей 1 бит:

$$f_\omega : \{0,1\}^n \to \{0,1\}, \tag{4}$$

$$f_\omega(x) = \delta_{x\omega}. \tag{5}$$

Функция f_ω является индикаторной функцией для единственного значения ω из области определения, которое требуется найти (5), здесь и далее δ_{ij} — символ Кронекера. Для того, чтобы формализовать понятие функции, необратимой на практике, Гровер определяет f_ω как функцию-оракул, алгоритм для которой неизвестен, но допустимо вычисление ее значения от любого аргумента. Количество вызовов функции оракула определяет меру сложности алгоритма поиска.

Для квантового поискового алгоритма определяется оператор $U_f : |x\rangle|-\rangle \to (-1)^{f(x)}|x\rangle|-\rangle$, который на подпространстве аргумента $|x\rangle$ действует как оператор отражения U_ω относительно гиперплоскости, ортогональной вектору, кодируемому значением ω:

$$U_\omega = \mathbb{I} - 2|\omega\rangle\langle\omega|. \tag{6}$$

Каждое обращение к оператору U_ω в алгоритме считается за итерацию и увеличивает сложность алгоритма на 1. Гровер так же вводит вспомогательный

оператор U_s:

$$|s\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle \tag{7}$$

$$U_s = 2|s\rangle\langle s| - \mathbb{I}. \tag{8}$$

Оператор U_s определяется только на подпространстве аргумента и отражает проекцию вектора состояния системы на этом подпространстве относительно равновзвешенной суммы всех векторов пространства. Итерация Гровера состоит из последовательного применения операторов U_ω и U_s. Полный алгоритм представляет собой применение к начальному состоянию итерации Гровера T раз, где $T = \frac{\pi}{4}2^{n/2}$, а начальное состояние задается как равновзвешенная сумма всех векторов пространства аргумента $|s\rangle$, и вектор $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ в кубите результата:

$$U_{Grov} = (U_s U_\omega)^T \frac{1}{\sqrt{2}} |s\rangle(|0\rangle - |1\rangle). \tag{9}$$

В результате применения описанного алгоритма вектор состояния системы приближается к искомому вектору $|\omega\rangle|-\rangle$ (рис. 6).

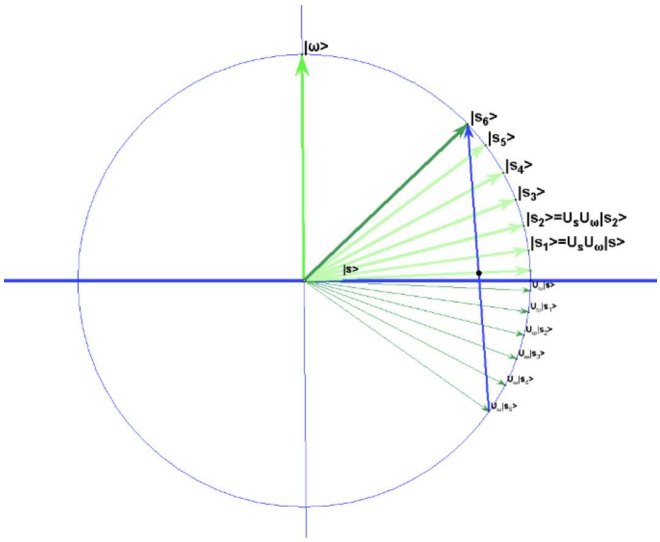

Рис. 6. Действие 6-и итераций алгоритма Гровера в 8-кубитном пространстве

Для реализации алгоритма в виде последовательности квантовых гейтов требуется получить такое представление для операторов U_ω и U_s. Реализация U_ω зависит от реализации функции оракула f_ω, которая считается нам неизвестной по постановке задачи. Алгоритм выполнения оператора U_s изображен на рис. 7.

На основе идеи алгоритма для U_s можно предложить модификацию алгоритма Гровера, в которой вектор $|0\rangle^{\oplus n}$ попадает в вектор $|\omega\rangle$ за одно отражение вокруг вектора $|s\rangle_{T/2}$, получаемого после выполнения половины итераций Гровера. Оператор такого отражения можно представить в следующем

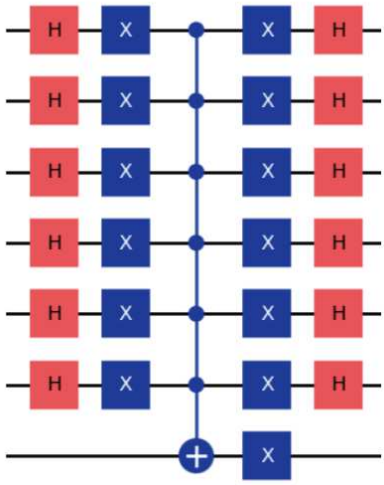

Рис. 7. Реализация оператора U_s. Сначала выполняется переход в базис Адамара, в котором вектор $|s\rangle$ кодируется строкой нулей $|0\rangle^{\oplus n}$. Операторы X превращают строку нулей в строку единиц $|1\rangle^{\oplus n}$, которая используется для выполнения условного оператора X на кубите результата, содержащем значение $|-\rangle$. Эта процедура умножает вектор $|1\rangle^{\oplus n}$ на -1, а последующий за ней безусловный гейт X домножает на -1 все пространство, возвращая вектор $|1\rangle^{\oplus n}$ на место. После обратной смены базиса получается отражение всего пространства вокруг вектора $|s\rangle$

виде:

$$Grov^{T/2} H Rot_0 H Grov^{-T/2} |0\rangle^{\oplus n}. \tag{10}$$

Аналогично реализации оператора U_s здесь также происходит смена базиса таким образом, чтобы вектор $|s\rangle_{T/2}$ представлялся в виде $|0\rangle^{\oplus n}$. Для этого приходится выполнить T итераций Гровера $Grov$ — половину в прямом и половину в обратном направлении. Оператор Rot_0 выполняет отражение пространства вокруг вектора $|0\rangle^{\oplus n}$ аналогично тому, как это делается в реализации U_s. Схема работы измененного таким образом алгоритма представлена на рис. 8. Важно отметить, что общее количество вызовов оракула остается прежним, но теперь они разделены на два класса: вызовы в прямую и в обратную стороны, которые мы можем выполнить параллельно.

3. ПАРАЛЛЕЛЬНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА

На рис. 9 представлена схема алгоритма Гровера, основанная на его декомпозиции из предыдущего раздела. В ней используются n кубитов для начального состояния $|0\rangle^{\oplus n}$ и $2n$ попарно запутанных кубитов, представляющих собой ресурс для телепортации.

Итерации Гровера в обратную сторону ($Grov^{-1}$) выполняются на кубитах начального состояния. Там же выполняется переход в базис Адамара

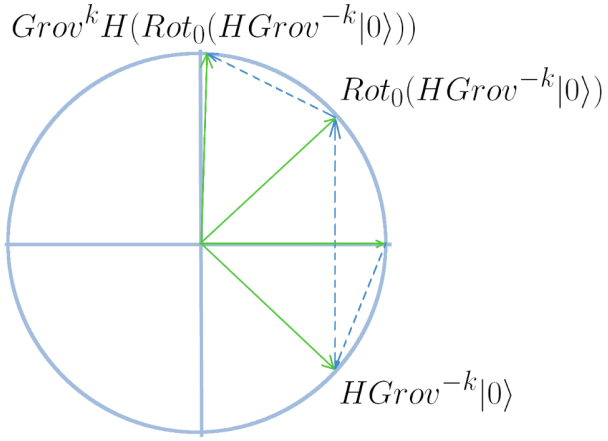

Рис. 8. Альтернативная реализация итераций Гровера ($k = T/2$)

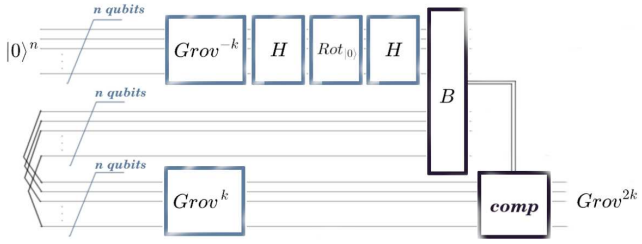

Рис. 9. Параллельная реализация итераций Гровера

и поворот вокруг $|0\rangle^{\oplus n}$. Вторая половина итераций ($Grov$) выполняется параллельно с ними на половине кубитов ресурса. После выполнения всех итераций осуществляется телепортация вычислений из верхней части схемы в нижнюю и коррекция состояния по результатам измерений в базисе Белла. Таким образом достигается двукратное ускорение алгоритма за счет трехкратного увеличения ширины схемы.

ЗАКЛЮЧЕНИЕ

Продемонстрированный в настоящей работе подход может быть использован для распараллеливания любых алгоритмов, в которых необходимо сократить глубину схемы при доступном ресурсе ее ширины (свободных кубитах).

В работе [7] Гровер показал, что количество вызовов оракула не может быть меньше, чем $2^{n/2-1}$, но это не означает, что эти вызовы нельзя делать одновременно, ускоряя таким образом работу алгоритма.

При этом результата, говорящего о том, что такое ускорение требует не менее чем трехкратного увеличения количества кубитов, нет. Дальнейшие исследования в этой области могут снизить эту оценку или доказать, что она минимальна.

Процедуру распараллеливания вычислений можно применить рекурсивно к частям, представленным на рис. 9. В общем, при ускорении в 2^k раз исполнение алгоритма можно представить в виде бинарного дерева с 2^k листьями. В каждом узле дерева используется дополнительно n кубитов ресурса, поэтому общее количество кубитов получается $n(2^{k+1} - 1)$, по n кубитов на каждый узел дерева, включая листья.

Работа выполнена при поддержке Министерства науки и высшего образования Российской Федерации, соглашение № 075–15–2022–287.

[1] *Deutsch D.* // Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences. **400** (1818), 97 (1985).
[2] *Deutsch D., Jozsa R.* // Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences. **439**, 1907. 553 (1992).
[3] *Bernstein E., Vazirani U.* // Proceedings of the twenty-fifth annual ACM symposium on Theory of computing.: 11-20 (1993).
[4] *Simon D.R.* // SIAM journal on computing. **26**(5). 1474 (1997).
[5] *Shor P.W.* // SIAM Review. **41** (2). 303 (1999).
[6] *Barenco A., Bennett C.H., Cleve R., DiVincenzo D.P.* et al. // Phys. Rev. A. **52**(5). 3457 (1995).
[7] *Grover L.K.* Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 212 (1996).
[8] *Kandala A.* et al. // Phys. Rev. A. **127**(13). 130501 (2021).
[9] *AbuGhanem M.* // arXiv preprint arXiv:2410.00916 (2024).
[10] *Mandelbaum R.* et al. // // IBM Blog (2023).
[11] *Gottesman D.* // Quantum information science and its contributions to mathematics, Proceedings of Symposia in Applied Mathematics. Vol. 68. (2010).
[12] *Roffe J.* // Contemporary Physics **60**, N 3 226 (2019)
[13] *Bennett C.H., Brassard G.* et al. // Phys. Rev. Lett. **70**(13). 1895 (1993).
[14] *Gottesman D., Chuang I.L.* // arXiv preprint quant-ph/9908010. (1999).

Quantum algorithms parallelization with quantum teleportation

S. S. Sysoev

Leonard Euler International Mathematical Institute at Saint Petersburg (SPB LEIMI)
St. Petersburg, 199178, Russia

E-mail: *s.s.sysoev@spbu.ru*

In this work, a method for parallelizing quantum algorithms in the circuit model is proposed, based on the technique of quantum gate teleportation. The parallel representation of the algorithm obtained in this way has a reduced circuit depth and, consequently, a higher probability of correct execution under conditions of quantum state decoherence that increases over time. The reduction of the circuit length is achieved by increasing its width—the number of qubits used simultaneously in computations.

PACS: 03.67.Ac
Keywords: quantum algorithms, quantum teleportation, parallelization.
Received 13 December 2024.
English version: *Moscow University Physics Bulletin*. 2025. **80**, No. . Pp. .

Сведения об авторе
Сысоев Сергей Сергеевич — канд. физ.-мат. наук, науч. сотрудник; e-mail: s.s.sysoev@spbu.ru.