ЖЭТФ, 2020, том 157, вып. 5, стр. 771–776

ПРИМЕНЕНИЕ АЛГОРИТМА КВАНТОВОГО ПЕРЕЧИСЛЕНИЯ ДЛЯ ОЦЕНКИ ВЕСА БУЛЕВЫХ ФУНКЦИЙ В КВАНТОВОМ СИМУЛЯТОРЕ QUIPPER

*Д. В. Денисенко**

Московский государственный технический университет им. Н. Э. Баумана
105005, Москва, Россия

Поступила в редакцию 26 октября 2019 г.,
после переработки 3 декабря 2019 г.
Принята к публикации 10 декабря 2019 г.

Квантовое перечисление — одна из известных задач, в которых проявляется ускорение вычислений за счет использования квантового параллелизма. В различных работах можно найти разные оценки вероятности успеха алгоритма квантового перечисления. Кроме того, в одних источниках в алгоритме квантового перечисления используют прямое квантовое преобразование Фурье, в других — обратное квантовое преобразование Фурье. В данной работе представлены результаты математического моделирования применения алгоритма квантового перечисления для оценки веса некоторых булевых функций, зависящих от шести переменных, в квантовом симуляторе Quipper с целью проверки известных оценок вероятности успеха алгоритма квантового перечисления.

DOI: 10.31857/S0044451020050016

1. ВВЕДЕНИЕ

Квантовые вычисления — одно из направлений квантовых технологий, стремительно развивающихся с конца XX века. В настоящее время фундаментальные исследования в области квантовых вычислений направлены на создание квантовых симуляторов и квантовых процессоров: в 2017 г. группа физиков заявила о создании программируемого 51-кубитного квантового симулятора [1], разработан 53-кубитный симулятор, основанный на ионах в оптических ловушках [2]. В компании IBM успешно испытан прототип 50-кубитного квантового процессора [3], а в декабре 2017 г. опубликована статья [4], согласно которой представлен проект масштабируемого кремниевого квантового процессора, представляющего собой массив из $24 \times 20 = 480$ кубитов. В январе 2018 г. компания Intel сообщила о создании 49-кубитного сверхпроводящего квантового чипа «Tangle Lake». В марте 2018 г. компания Google объявила о создании 72-кубитного квантового процессора «Bristlecone», с помощью которого компания надеялась продемонстрировать «квантовое превосходство» [5, 6]. Осенью 2019 г. опубликована работа [7], согласно которой с помощью 54-кубитного процессора «Sycamore» продемонстрировано существенное ускорение в решении одной специальной задачи: вычисление 1 млн раз 53-кубитной квантовой схемы на квантовом процессоре «Sycamore» занимает около 200 с, в то время как решение аналогичной задачи на классическом суперкомпьютере, по оценкам авторов, займет не менее 10000 лет.

Одной из задач, в которых проявляется ускорение вычислений за счет использования квантового параллелизма, является задача квантового перечисления [8–10]. Задача квантового перечисления может быть использована в различных областях науки, в том числе и в информационной безопасности (см. [11]). Проблема в том, что в работе [8] вероятность успеха алгоритма квантового перечисления оценена снизу величиной $8/\pi^2$, в работе [9] та же самая вероятность успеха оценивается снизу величиной $2/3$, в [12] вероятность успеха квантового алгоритма определения собственного числа, на котором основан алгоритм квантового перечисления, оценивается снизу величиной $4/\pi^2$, причем в [10, 12] указано, что если в регистре управления $m = t + [\log_2(2 + 1/2\epsilon)]$ кубитов, то вероятность успеха алгоритма определения собственного числа, а значит и квантового перечисления, будет не менее $1 - \epsilon$.

* E-mail: DenisenkoDV@bmstu.ru

Таким образом, в источниках информации можно найти различные оценки вероятности успеха алгоритма квантового перечисления, из-за чего результаты практического применения квантового перечисления могут отличаться от ожидаемых теоретических результатов. Кроме того, в оригинальной работе [8] в алгоритме квантового перечисления используется прямое квантовое преобразование Фурье, а в [9,10] используется обратное преобразование Фурье.

В настоящей работе представлены результаты математического моделирования применения алгоритма квантового перечисления для оценки веса некоторых булевых функций, зависящих от 6 переменных, в квантовом симуляторе Quipper [13–15] с целью проверки оценок вероятности успеха алгоритма квантового перечисления. Результаты представлены на рис. 2–9, их можно рассматривать как результаты экспериментов с идеальным 12-кубитным квантовым компьютером и использовать при тестировании физических реализаций квантовых вычислительных систем по аналогии с тестами [16]. Кроме того, проведены эксперименты по моделированию квантового перечисления с использованием как прямого, так и обратного квантового преобразования Фурье. Получен вывод о том, что в алгоритме квантового перечисления можно использовать как прямое, так и обратное квантовое преобразование Фурье (результаты выполненных экспериментов получились одинаковыми).

2. КВАНТОВОЕ ПЕРЕЧИСЛЕНИЕ

Задача квантового перечисления рассмотрена в работах [8–10]. Пусть имеется проиндексированное множество из $N = 2^n$ элементов. В задаче поиска с помощью квантового алгоритма Гровера [17] требуется найти индекс элемента, удовлетворяющего некоторому критерию поиска, задаваемому булевой функцией $f : V_n \to V_1$, причем предполагается, что всего существует M таких элементов. Если с помощью квантового алгоритма Гровера можно найти какое-то одно решение рассматриваемой задачи, то с помощью квантового алгоритма перечисления — оценку общего количества решений в рассматриваемой задаче поиска.

Задача квантового перечисления: дана случайная булева функция $f : V_n \to V_1$, требуется оценить количество $M = |f^{-1}(1)|$ аргументов, на которых рассматриваемая булева функция принимает значение 1.

Следуя [10], обозначим

$$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_{x_{bad}} |x\rangle, \quad |\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_{x_{good}} |x\rangle,$$

тогда состояние равновероятной суперпозиции «входов» рассматриваемой булевой функции f можно записать в виде

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle.$$

Обозначим $\cos(\theta/2) = \sqrt{(N-M)/N}$, тогда $|\psi\rangle = \cos(\theta/2)|\alpha\rangle + \sin(\theta/2)|\beta\rangle$, вероятность получить в результате измерения кубитов какое-либо одно из M возможных решений равна $\sin^2(\theta/2)$. В базисе, состоящем из $|\alpha\rangle$ и $|\beta\rangle$, итерацию Гровера можно записать следующим образом (см. [10]):

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \tag{1}$$

где $0 \le \theta \le \pi/2$ (для случая $M \le N/2$), $\sin\theta = 2\sqrt{M(N-M)}/N$.

После k итераций Гровера получим состояние

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle.$$

После $k = \left[\pi/4\sqrt{N/M}\right]$ итераций Гровера и измерения кубитов с высокой вероятностью $\sin^2((2k+1)/2\theta)$ получим одно из M возможных решений.

Квантовое перечисление — это применение процедуры нахождения собственного числа итерации Гровера G, позволяющее определить количество решений M задачи поиска.

Пусть $|a\rangle$ и $|b\rangle$ — два собственных вектора итерации Гровера в пространстве, натянутом на векторы $|\alpha\rangle$ и $|\beta\rangle$, а θ — угол поворота, определяемый итерацией Гровера. Квантовый алгоритм, решающий рассматриваемую задачу квантового перечисления, имеет два параметра: булева функция f и количество кубитов m, которое определяет точность, с которой мы оцениваем величину M, и влияет на время выполнения всего алгоритма. Квантовый алгоритм перечисления основан на двух унитарных преобразованиях:

$$G^x : \ |x\rangle \otimes |\Psi\rangle \to |x\rangle \otimes G_f^x|\Psi\rangle,$$

$$QFT_m^{-1} \ : \ |x\rangle \to \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} \exp\left(-\frac{2\pi ixj}{2^m}\right)|j\rangle,$$

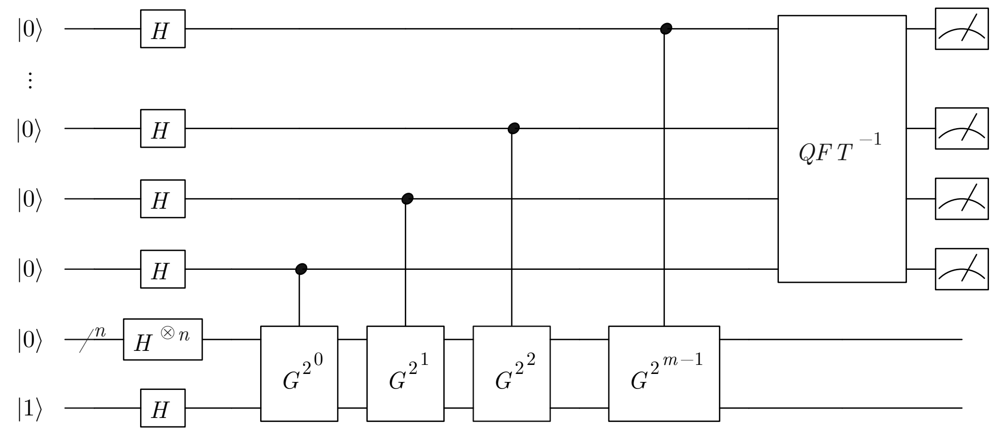

Рис. 1. Квантовая схема для алгоритма определения угла поворота θ итерации Гровера G. Регистр управления содержит m кубитов

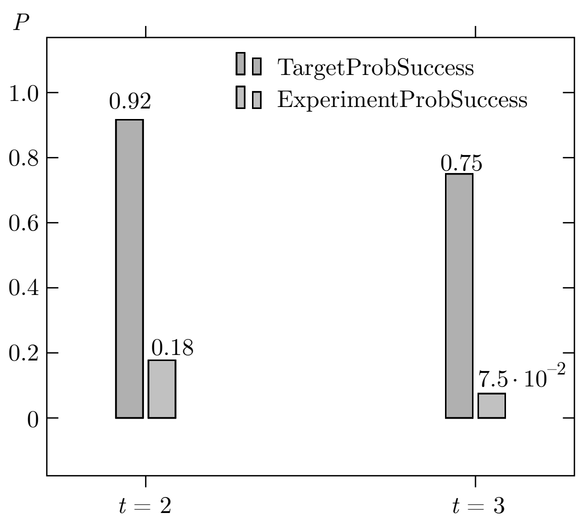

Рис. 2. $f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1x_2x_3x_4x_5x_6$, $M = 1$, $N = 2^6$, $\theta = 2\arcsin\sqrt{M/N} = 0.250656$. В регистре управления 5 кубитов, т. е. $m = 5$. Поскольку $m = t + [\log_2(2+1/2\epsilon)]$, рассмотрим два варианта: 1) $t = 2$, тогда $\epsilon = 1/12$ и согласно теории $|\Delta\theta| < 0.25$, $|\Delta M| < 3$, теоретическая вероятность успеха $1-\epsilon = 0.916667$; 2) $t = 3$, тогда $\epsilon = 1/4$ и согласно теории $|\Delta\theta| < 0.125$, $|\Delta M| < 1.25$, теоретическая вероятность успеха $1 - \epsilon = 0.75$. Экспериментальная вероятность успеха определяется как сумма вероятностей тех исходов, на которых $|\theta - \widetilde{\theta}| < 0.25$ при $t = 2$ либо $|\theta - \widetilde{\theta}| < 0.125$ при $t = 3$

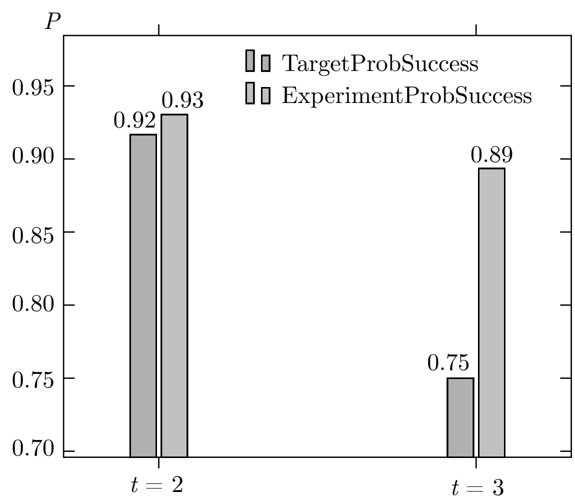

Рис. 3. $f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1x_2x_3x_4x_5$, $M = 2$, $N = 2^6$, $\theta = 2\arcsin\sqrt{M/N} = 0.355421$. $P_{t=2}(|\Delta\theta| < 0.25) = 0.93$, $P_{t=3}(|\Delta\theta| < 0.125) = 0.89$

где $i = \sqrt{-1}$, оператор G_f^x — композиция x итераций Гровера относительно булевой функции f, m — количество кубитов для оценки величины угла поворота θ итерации Гровера. Собственные числа оператора G равны $\exp(i\theta)$ и $\exp(i(2\pi - \theta))$ (см. [10], разд. 6.3).

Схема определения собственного числа, используемая для квантового перечисления представлена на рис. 1.

Согласно [10], для того чтобы полученная оценка θ с вероятностью не менее $1 - \epsilon$ имела погрешность не более 2^{-t}, $t \in \mathbb{N}$, в первом регистре должно быть $m \equiv t + [\log_2(2 + 1/2\epsilon)]$ кубитов, во втором регистре должно быть $n+1$ логических кубитов (считаем, что итерации Гровера G могут быть эффективно реализованы без вспомогательных кубитов).

Состояние второго регистра с помощью преобразования Адамара $H^{\otimes n}$ переводится в суперпозицию всех возможных входных значений булевой функции f с равными амплитудами вероятностей, т. е. в

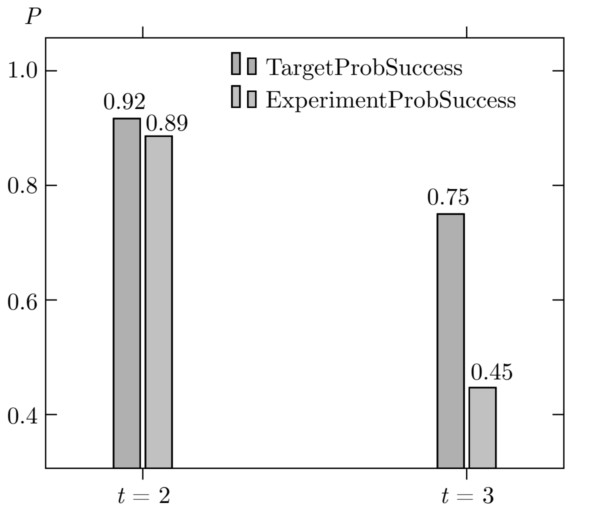

Рис. 4. $f(x_1,x_2,x_3,x_4,x_5,x_6) = x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4x_6 \oplus$ $\oplus x_1x_2x_3x_4x_5x_6$, $M = 3$, $N = 2^6$, $\theta = $ $= 2\arcsin\sqrt{M/N} = 0.436469$. $P_{t=2}(|\Delta\theta| < 0.25) = 0.89$, $P_{t=3}(|\Delta\theta| < 0.125) = 0.45$

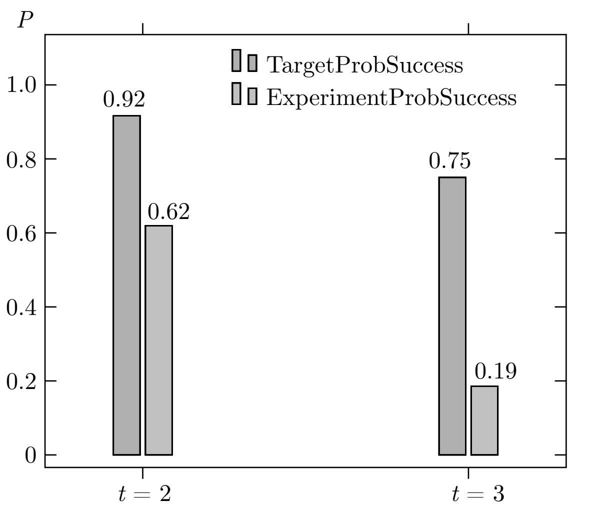

Рис. 5. $f(x_1,x_2,x_3,x_4,x_5,x_6) = x_1x_2x_3x_4$, $M = 4$, $\theta = $ $= 2\arcsin\sqrt{M/N} = 0.505361$. $P_{t=2}(|\Delta\theta| < 0.25) = 0.62$, $P_{t=3}(|\Delta\theta| < 0.125) = 0.19$

состояние суперпозиции собственных состояний $|\alpha\rangle$ и $|\beta\rangle$ (так как $G|\alpha\rangle = e^{i(2\pi-\theta)}|\alpha\rangle$, $G|\beta\rangle = e^{i\theta}|\beta\rangle$). Квантовая схема на рис. 1 дает ответ θ или $2\pi - \theta$ с точностью $|\Delta\theta| \le 2^{-t}$ при вероятности не менее $1-\epsilon$. Более того, ответ $2\pi-\theta$ эквивалентен ответу θ с той же точностью, поэтому в действительности процедура определения собственного числа определяет значение θ с точностью 2^{-t} и вероятностью успеха $1-\epsilon$.

Используя уравнение $\sin^2(\theta/2) = M/N$ и оценку для величины θ, можно оценить величину ошибки ΔM для количества решений M:

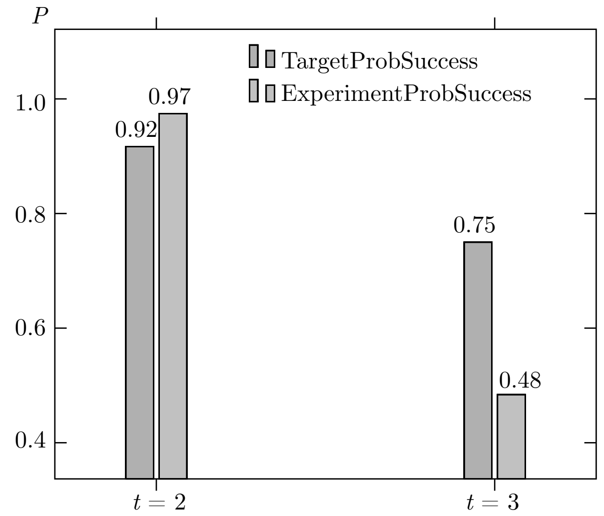

Рис. 6. $f(x_1,x_2,x_3,x_4,x_5,x_6) = x_1x_2x_3x_4 \oplus x_1x_2x_3x_5x_6 \oplus$ $\oplus x_1x_2x_3x_4x_5x_6$, $M = 5$, $\theta = 2\arcsin\sqrt{M/N} = 0.566564$. $P_{t=2}(|\Delta\theta| < 0.25) = 0.97$, $P_{t=3}(|\Delta\theta| < 0.125) = 0.48$

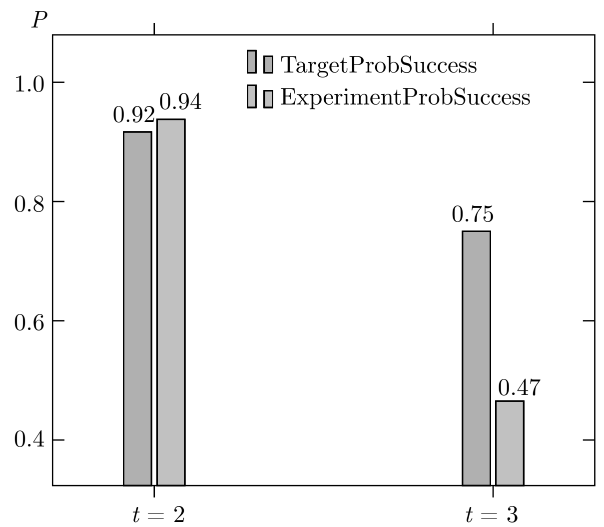

Рис. 7. $f(x_1,x_2,x_3,x_4,x_5,x_6) = x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus$ $\oplus x_1x_2x_3x_4x_5$, $M = 6$, $\theta = 2\arcsin\sqrt{M/N} = 0.622368$. $P_{t=2}(|\Delta\theta| < 0.25) = 0.94$, $P_{t=3}(|\Delta\theta| < 0.125) = 0.47$

$$\left|\frac{M+\Delta M}{N} - \frac{M}{N}\right| = \left|\sin^2\frac{\theta+\Delta\theta}{2} - \sin^2\frac{\theta}{2}\right| = \\ = \left(\sin\frac{\theta+\Delta\theta}{2} + \sin\frac{\theta}{2}\right)\left|\sin\frac{\theta+\Delta\theta}{2} - \sin\frac{\theta}{2}\right|.$$

К первому множителю применимо тригонометрическое неравенство:

$$\left|\sin\frac{\theta+\Delta\theta}{2}\right| < \sin\frac{\theta}{2} + \frac{|\Delta\theta|}{2},$$

ко второму множителю —

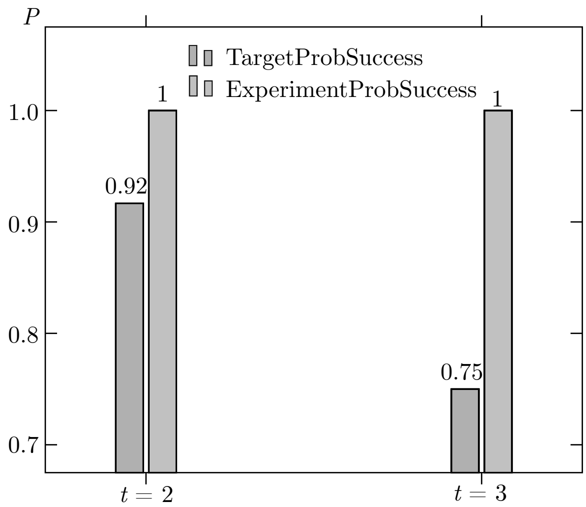

Рис. 8. $f(x_1, x_2, x_3, x_4, x_5, x_6) = 0$, $M = 0$, $\theta = 2\arcsin\sqrt{M/N} = 0$. $P(\widetilde{\theta} = 0.03125) \approx 1$

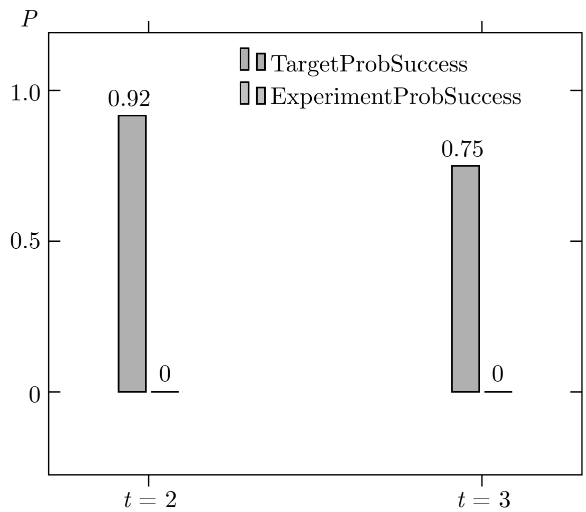

Рис. 9. $f(x_1, x_2, x_3, x_4, x_5, x_6) = 1$, $M = 64$, условие $M < N/2$ не выполнено, но мы посмотрели, что получится в результате применения алгоритма квантового перечисления в таком случае: $P(\widetilde{\theta} = 0) \approx 1$

$$\left|\sin\frac{\theta+\Delta\theta}{2} - \sin\frac{\theta}{2}\right| \le \frac{|\Delta\theta|}{2},$$

таким образом получаем оценку

$$\frac{|\Delta M|}{N} < \left(2\sin\frac{\theta}{2} + \frac{|\Delta\theta|}{2}\right)\frac{|\Delta\theta|}{2}.$$

Подставив сюда $\sin(\theta/2) = \sqrt{M/N}$, полагая, что $|\Delta\theta| \le 2^{-t}$, получим окончательную оценку для ошибки $|\Delta M|$:

$$|\Delta M| < N\left(2\sqrt{\frac{M}{N}} + \frac{1}{2^{t+1}}\right)\frac{1}{2^{t+1}},$$

$$|\Delta M| < \frac{\sqrt{MN}}{2^t} + \frac{N}{2^{2(t+1)}}.$$

При выборе $t = n/2$, $m = [n/2] + 3$ получим оценку M, используя $2^{n/2+3}$ итераций Гровера, т. е. всего за $2^{n/2+3}$ обращений к функции f, а не за 2^n при полном переборе аргументов f в классическом случае. При этом вероятность того, что будет получен заданный уровень погрешности $\Delta\theta$ и ΔM (вероятность успеха алгоритма квантового перечисления), составляет $1-1/12 = 0.916667$. Таким образом, получено квадратичное ускорение по сравнению с классическим алгоритмом полного перебора «входов» f для оценки мощности прообраза $|f^{-1}(1)|$.

Далее рассмотрим результаты математического моделирования применения квантового алгоритма перечисления.

3. РЕЗУЛЬТАТЫ ПРИМЕНЕНИЯ АЛГОРИТМА КВАНТОВОГО ПЕРЕЧИСЛЕНИЯ ДЛЯ ОЦЕНКИ ВЕСА БУЛЕВОЙ ФУНКЦИИ В КВАНТОВОМ СИМУЛЯТОРЕ QUIPPER

Задача квантового перечисления рассмотрена относительно некоторых булевых функций $f : V_6 \to V_1$ веса $M = 1, 2, \ldots, 6$. Общий вид квантовой схемы, использующейся для решения задачи квантового перечисления, представлен на рис. 1:

1) пять кубитов в верхнем регистре управления;

2) шесть кубитов соответствуют переменным булевой функции;

3) еще один кубит требуется для реализации «итерации Гровера» относительно рассматриваемых булевых функций f.

Получена квантовая схема на 12 кубитах. Результат измерения первого регистра, верхние пять кубитов, обозначим $|x\rangle$. После процедуры измерения $|x\rangle$ получим оценку $2^5\widetilde{\theta}$, т. е. для того, чтобы получить $\widetilde{\theta}$, необходимо разделить целое число x на 2^5.

Отметим, что стандартные квантовые схемы, реализующие прямое и обратное квантовые преобразования Фурье, инвертируют порядок записи кубитов, т. е. старшие кубиты и младшие кубиты меняются местами. Для того чтобы вернуть исходный порядок записи, требуется применять SWAP-гейты, которые обычно не указывают (см. [10], рис. 5.1, с. 219). В квантовом симуляторе Quipper обратное преобразование Фурье выполняется с помощью композиции функций «reverse_generic_endo» и «qft_big_endian», в результате чего старшие и младшие кубиты меняются местами.

Результаты применения квантового алгоритма перечисления для оценки веса $||f(x_1, x_2, x_3, x_4, x_5, x_6)||$ представлены на рис. 2–9. Программную реализацию можно найти в [18].

4. ЗАКЛЮЧЕНИЕ

В целом, за исключением случаев, проиллюстрированных на рис. 2 и 5, при выборе $t = n/2$, $m = [n/2] + 3$ с вероятностью не менее $4/\pi^2 = 0.405285$ полученные оценки M за $2^{n/2+3}$ итераций Гровера имеют заданный уровень погрешности ΔM, т. е. за $2^{n/2+3}$ обращений к функции f можно получить оценку $|f^{-1}(1)|$, однако вероятность успеха алгоритма квантового перечисления может существенно отличаться от теоретической оценки $1 - \epsilon$ при $m = t + [\log_2(2 + 1/2\epsilon)]$ из [10].

Таким образом, с помощью алгоритма квантового перечисления, вероятность успеха которого обычно составляет не менее $4/\pi^2 = 0.405285$, может быть получено квадратичное ускорение по сравнению с классическим алгоритмом полного перебора «входов» f для оценки мощности прообраза $|f^{-1}(1)|$.

ЛИТЕРАТУРА

1. H. Bernien, S. Schwartz, A. Keesling, H. Levine, and A. Omran, Nature **551**, 579 (2017), DOI:10.1038/nature24622; arXiv:1707.04344.

2. J. Zhang, G. Pagano, P. W. Hess, A. Kyprianidis, and P. Becker, Nature **551**, 601 (2017), DOI:10.1038/nature24654; arXiv:1708.01044.

3. https://www.ibm.com/blogs/research/2017/11/the-future-is-quantum.

4. M. Veldhorst, H. G. J. Eenink, C. H. Yang, and A. S. Dzurak, Nature Comm. **8**, 1766 (2017), DOI:10.1038/s41467-017-01905-6; https://doi.org/10.1038/s41467-017-01905-6.

5. C. S. Calude and E. Calude, arXiv:1712.01356v1.

6. J. Kelly, *A Preview of Bristlecone, Google's New Quantum Processor*, Quantum AI Lab, 05.03.2018, https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html.

7. F. Arute, K. Arya, J. M. Martinis et al., Nature **574**, 505 (2019), https://doi.org/10.1038/s41586-019-1666-5.

8. G. Brassard, P. Hoyer, and A. Tapp, http://arxiv.org/abs/quant-ph/9805082v1.

9. M. Mosca, in *Proceedings of Randomized Algorithms, Workshop of Mathematical Foundations of Computer Science* (1998), pp. 90–100.

10. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, New York (2010), pp. 261–263.

11. Q. Zhou, S. Lu, A. Zhang, and J. Sun, https://arxiv.org/abs/1811.09931.

12. G. Benenti, G. Casati, and G. Strini, *Principles of Quantum Computation and Information*, World Sci. (2004), https://doi.org/10.1142/5528.

13. *Квантовый симулятор Quipper*, http://www.mathstat.dal.ca/selinger/quipper/.

14. A. S. Green, P. L. Lumsdaine, N. J. Ross, P. Selinger, and B. Valiron, arXiv:1304.5485v1.

15. S. Siddiqui, M. J. Islam, and O. Shehab, arXiv:1406.4481v2[quant-ph].

16. P. Murali, M. Martanosi et al., arXiv:1905.11349v2 [quant-ph].

17. L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

18. https://github.com/DenisenkoDV/Quipper-QuantumCounting.git.