INFORMATICA CUANTICĂ

Acad. AȘM, Profesor univ. Sidorenko Anatolie

Institutul de Inginerie Electronica
și Nanotehnologii al UTM

E-mail: sidorenko.anatoli@gmail.com
anatolie.sidorenko@mib.utm.md
Tel./viber *+37369513294*

Тема 6. Квантовые алгоритмы

6.1. Квантовые алгоритмы факторизации чисел и поиска в базе данных

К настоящему времени открыты и подробно исследованы три класса квантовых алгоритмов:

1) алгоритмы с квантовыми скрытыми подгруппами преобразований абелевых групп (к ним относится алгоритм Шора факторизации чисел);
2) алгоритмы с усилением амплитуд (их представителем является алгоритм Гровера поиска

объекта в неструктурированной базе данных);

3) алгоритмы для моделирования квантовых систем на квантовом компьютере.

Алгоритмы классов 1) и 3) предусматривают применение дискретного Фурье-преобразования. При выполнении Фурье-преобразования на классическом компьютере требуется экспоненциально большое число операций. На квантовом компьютере Фурье-преобразование выполняется

за полиномиальное число (n^2) операций, поэтому квантовые алгоритмы классов 1) и 3) демонстрируют экспоненциальное ускорение решения задачи по сравнению с алгоритмами, выполняемыми на классических компьютерах.

6.1. Квантовые алгоритмы факторизации чисел и поиска в базе данных

Принцип алгоритма Гровера

— это алгоритм усиления амплитуды состояния, соответствующего искомому объекту. Пусть целое число x_s является индексом искомого объекта.

Поставим ему в соответствие базисное состояние $|x_s\rangle$ в векторе состояния $|\psi\rangle = \sum_x c_x |x\rangle$ квантового регистра. Итерационный процесс при выполнении алгоритма Гровера построен так, что интерференция амплитуд увеличивает амплитуду c_{xs}; остальные амплитуды $c_x \neq x_s$ уменьшаются. После $\sqrt{N}$ итераций (*N*— число объектов в базе данных) амплитуда c_{x_s} достигает значения $|c_{x_s}| \leq 1$.

Измерение состояния регистра после $\sqrt{N}$ итераций с вероятностью $|c_{x_s}| \simeq 1$ определяет индекс x_s искомого объекта. Поиск объекта в классическом случае требует *N* операций (перебор всех объектов). Таким образом, в квантовом алгоритме Гровера достигается квадратичное ускорение решения задачи поиска по сравнению с поиском на классическом компьютере.

Чем больше будет найдено эффективных квантовых алгоритмов, тем больше будет стимулов к реализации идеи квантовых компьютеров и квантовой информатики.

6.2. Алгоритм телепортации неизвестного квантового состояния

Поучительным примером малоразмерного алгоритма является протокол квантовой телепортации неизвестного квантового состояния. Схема протокола телепортации представлена на рис. 9. В начальный момент три участвующих в протоколе кубита находятся в точке *A*, их состояние не запутано:

$$|\psi_{in}\rangle = |a_1\rangle|0_2\rangle|0_3\rangle$$

Здесь $|a_1\rangle = \alpha|0_1\rangle + \beta|1_1\rangle$ – неизвестное состояние кубита 1. Именно оно должно быть телепортировано в точку пространства ***B***. События, происходящие в точках ***A*** и ***B***, заключены на рис. 9 в соответствующие рамки:

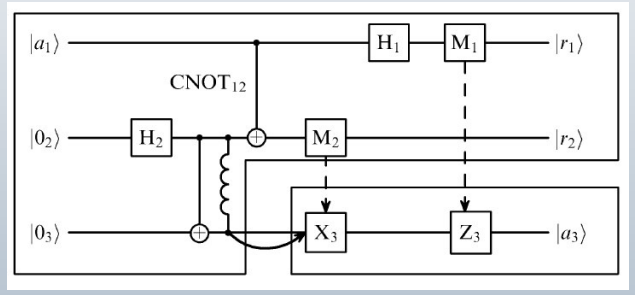

Рис. 9. Схема протокола телепортации неизвестного состояния */a1* из точки ***A*** в точку ***B***. В процессе телепортации создается запутанность, которая затем уничтожается в ходе измерений состояния кубитов. Кроме того, один из кубитов запутанной пары транспортируется из точки ***A*** в точку ***B***.

В первой операции создается запутанность кубитов 2 и 3. Операция выполняется в два этапа: над состоянием кубита 2 выполняется преобразование Адамара H, затем – CNOT

$$|0_2\rangle|0_3\rangle \xrightarrow{H_2} \frac{1}{\sqrt{2}}(|0_2\rangle + |1_2\rangle)|0_3\rangle \xrightarrow{\mathrm{CNOT}_{23}} \frac{1}{\sqrt{2}}(|0_2 0_3\rangle + |1_2 1_3\rangle). \qquad (59)$$

Запутанность кубитов 2 и 3 показана на схеме спиральной связью между линиями эволюции во времени. После генерации запутанности кубитов 2 и 3 кубит 3 транспортиру-ется в точку ***B***, удаленное от точки ***A*** на сколь угодно большое расстояние.

Дальнейшие операции локального типа (LOCC) совершаются над кубитами 1 и 2 в точке ***A***, над кубитом 3 — в точке ***B***. Штриховыми линиями показана передача в точку ***B*** классической информации о результате измерения состояния кубита в точке ***A***. Эта информация используется для выполнения операций (X_3 или Z_3) над кубитом 3 в точке ***B***.

Во второй операции запутанность кубитов 2 и 3 преобразуется в запутанность кубитов 1 и 3 с участием всех трех кубитов:

$$\frac{1}{\sqrt{2}}(\alpha|0_1\rangle + \beta|1_1\rangle)(|0_2 0_3\rangle + |1_2 1_3\rangle) \xrightarrow{\mathrm{CNOT}_{12}} (\alpha|0_1 0_2 0_3\rangle + \alpha|0_1 1_2 1_3\rangle + \beta|1_1 1_2 0_3\rangle + \beta|1_1 0_2 1_3\rangle) \xrightarrow{M_2(|0_2\rangle)} (\alpha|0_1 0_3\rangle + \beta|1_1 1_3\rangle)|0_2\rangle. \qquad (60)$$

6.2. Алгоритм телепортации неизвестного квантового состояния

. Конечным ссостоянием трех кубитов будет

$$|\psi_f\rangle = (\alpha|0_3\rangle + \beta|1_3\rangle)|r_1\rangle|r_2\rangle. \qquad (62)$$

Каков результат всех операций? Неизвестное состояние $|a_1\rangle = \alpha|0_1\rangle + \beta|1_1\rangle$ принадлежавшее вначале кубиту 1 в точке A, теперь принадлежит кубиту 3 в точке B — телепортация неизвестного состояния свершилась. Кубит 1 лишился состояния $|a_1\rangle$: сохранение его у кубита 1 означало бы клонирование неизвестного состояния, что запрещено no-cloning-теоремой. Конечное состояние трех кубитов не запутано. Запутанность, созданная в начале операции, израсходована на выполнение телепортации. Из формулы (62) следует, что **запутанность есть расходуемый ресурс квантовой информатики !**

”Чудом” здесь является телепортация именно неизвестного квантового состояния.

6.3. Моделирование квантовых систем на квантовом компьютере

Рассмотрим задачу о моделировании на квантовом компьютере квантовой системы, заданной гамильтонианом

$$H = \frac{p^2}{2mm} + V(x).$$

Статическая задача заключается в определении собственных значений E энергии и собственных функций $|u\rangle$ системы согласно уравнению:

$$H|u\rangle = E|u\rangle.$$

Динамическая задача заключается в изучении динамики системы согласно уравнению Шрёдингера

$$\mathrm{i}\frac{\partial}{\partial \mathrm{t}}|\psi\rangle = H|\psi\rangle$$

(постоянная $\hbar$ включена в гамильтониан H). Используя оператор эволюции и $\mathrm{U}(t) = \exp(-\mathrm{i}Ht)$, уравнение динамики можно свести к преобразованию вектора состояния системы:

$$|\psi(x,t)\rangle = \mathrm{U}(\mathrm{t})|\psi(x,0)\rangle. \qquad (63)$$