УДК 004.415.2, 004.588

КВАНТОВАЯ РЕЛЯТИВИСТСКАЯ ИНФОРМАТИКА. Ч. 4: ЭЛЕМЕНТЫ КВАНТОВОЙ РЕЛЯТИВИСТСКОЙ ТЕОРИИ ИНФОРМАЦИИ И КВАНТОВОГО ПРОГРАММИРОВАНИЯ

Ульянов Сергей Викторович[1], Албу Вячеслав Андреевич[2], Бархатова Ирина Александровна[3], Решетников Андрей Геннадьевич[4], Ростовцев Виталий Александрович[5]

[1]*Доктор физико-математических наук, профессор;*
ГБОУ ВПО «Международный Университет природы, общества и человека «Дубна», Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: ulyanovsv@mail.ru.

[2]*Младший научный сотрудник;*
Институт математики и информатики АН Республики Молдова;
Молдавия, МД-2028, г. Кишинев, ул. Академией, 5;
e-mail: vaalbu@googlemail.com.

[3]*Старший преподаватель;*
ГБОУ ВПО «Международный Университет природы, общества и человека «Дубна», Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: i.a.barhatova@gmail.com.

[4]*Аспирант;*
ГБОУ ВПО «Международный Университет природы, общества и человека «Дубна», Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: reshetnikovag@pochta.ru.

[5]*Доцент;*
ГБОУ ВПО «Международный Университет природы, общества и человека «Дубна», Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: rost@jinr.ru.

Рассмотрены алгоритмические и физические особенности основных моделей квантовых операторов, применяемых при конструировании квантовых алгоритмов. Моделирование квантовых алгоритмических ячеек рассмотрено с позиции квантового программирования. Кратко описаны основные языки квантового программирования и факты квантовой релятивистской теории информации.

Ключевые слова: Квантовые операторы, квантовое программирование, квантовая релятивистская информация, квантовая релятивистская информатика.

QUANTUM RELATIVISTIC INFORMATICS. PT. 4: ELEMENTS OF QUANTUM RELATIVISTIC INFORMATION THEORY AND QUANTUM PROGRAMMING

Ulyanov Sergey[1], Albu Veaceslav[2], Barchatova Irina[3], Reshetnikov Andrey[4], Rostovtsev Vitaly[5]

[1]*Doctorof Science in Physics and Mathematics, professor;*
Dubna International University of Nature, Society, and Man,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: ulyanovsv@mail.ru.

[2]*Junior scientist;*
Institute of Mathematics and Computer Science;
Republic of Moldova, Chisinau MD 2028, Kishinev, Academiei str.5;
e-mail: vaalbu@googlemail.com.

[3]*Senior researcher;*
Dubna International University of Nature, Society and Man,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: i.a.barhatova@gmail.com.

[4]*PhD student;*
Dubna International University of Nature, Society and Man,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: reshetnikovag@pochta.ru.

[5]*Associate professor;*
Dubna International University of Nature, Society and Man,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: rost@jinr.ru.

Main algorithmic and physical peculiarities of quantum operator's models that are used in the design of quantum algorithms are considered. Modelling of quantum algorithmic gates from quantum programming viewpoint is discussed. Briefly main quantum programming languages and facts of quantum relativistic information theory are described.

Keywords: Quantum operators, quantum programming, quantum relativistic information theory, quantum relativistic informatics.

Введение: Роль квантовой релятивистской теории информации и квантового программирования как фундаментального базиса квантовой релятивистской информатики

Разработка наукоёмких ИТ затрагивает одновременно пересмотр исходных положений таких фундаментальных теорий как квантовая механика, общая теория квантовой гравитации, квантовой релятивистской термодинамики, теории неразрушающих квантовых измерений в криволинейном пространстве – времени, квантовой релятивистской теории описания поведения релятивистской частицы в римановом и нериманового пространственно-временном континууме и мн. др.

В свою очередь, существование алгоритмической неразрешимости при применении традиционных вычислительных методов и количественных подходов к поиску оптимальных решений сложных задач физики, механики, биофизики, систем управления, развитие наукоемких

компьютерных (типа квантового компьютера) и прорывных ИТ типа квантовый Интернет на основе квантовых слепых облачных вычислений (quantum blind cloud computing), квантовая криптография, квантового управления наноструктурами, формирования интеллектуальных наноматериалов, разработка ИТ нанотехнологий и мн. др. привело к необходимости поиска и развития технологий на основе новых видов интеллектуальных вычислений (ИВ) и программно-аппаратной поддержки вычислительных процессов.

Разработка подобных наукоёмких платформ элементной базы аппаратной поддержки квантовых ИТ потребовало одновременно создания и внедрения новых видов нанотехнологий изготовления материалов и технологической оснастки. Резко возросший объем перерабатываемой информации и сложность решаемых задач в науке и технике привел к необходимости создания новой элементной базы квантового компьютера, способного реализовать квантовый массивный параллелизм обработки информации, решать классические алгоритмически неразрешимые задачи с экспоненциальной скоростью, обладая огромной памятью и быстродействием.

Поэтому выбранное решение фундаментальных и прикладных проблем конкретной технологии ИВ существенно влияет на эффективность разработки и качество применения моделей наукоемких ИТ. Возрастание сложности структур современных физических объектов и логических устройств, трудности прогнозирования непредвиденных (нештатных) ситуаций управления только усиливают актуальность данной проблемы и внимание к поиску её решения.

Элементы квантовой релятивистской теории информации

В данном разделе рассмотрим кратко некоторые особенности и прикладные аспекты квантовой релятивистской теории информации с позиции системной инженерии и задач квантовой релятивистской информатики. Прежде всего, остановимся на некоторых мерах количества информации и оценки влияния квантовых и релятивистских эффектов на измерение количества информации.

Меры квантовой информации и законы квантовой теории информации

Информационная энтропия Шеннона определяется как $H\ \ p\ = -\sum_i p_i \log p_i$.

Энтропия фон Неймана имеет следующий вид: $S^{vN}\ \ \rho\ = -Tr\ \ \rho \log \rho$.

В частном случае, когда матрица ρ диагональная, наблюдается тождественное равенство энтропийных мер Шеннона и фон Неймана. Однако законы и следствия квантовой теории информации имеют ряд принципиальных отличий при квантовом обобщении классической теории информации Шеннона.

– *Меры информации Фишера / Шеннона и информационные метрики пространства – времени*

В данном разделе рассмотрим прежде всего простые примеры вывода широко применяемых мер информационной энтропии Шеннона и количества информации Фишера.

Информационная энтропия Шеннона. Напомним, что само понятие «информация» в теории Шеннона не ассоциируется с индивидуальным сообщением, а характеризует источник сообщений. Идея о статистической природе источника позволяет упростить описание пропускной способности канала передачи информации, воспроизводимой источником сообщений. Рассмотрим ансамбль $X = x_1, x_2, \ldots x_n$ алфавита x_i, появляющегося в сообщении с вероятностью $p\ x_i$. Ансамбль сообщений состоит из большого числа N . Для каждого сообщения типовая последовательность букв алфавита x_i содержит $Np\ x_i$ букв, $Np\ x_j$, из x_j и т.д.

Число таких различимых типовых последовательностей букв сообщений определяется комбинаторикой как $\frac{N!}{Np\ x_1\ !Np\ x_2\ !\ldots Np\ x_n\ !}$ и применяя формулу Стирлинга получим

аппроксимацию данного выражения в виде $2^{NH\ X}$, где $H\ X = -\sum_{i}^{n} p\ x_i\ \log p\ x_i$ является информационной энтропией Шеннона. При $N \to \infty$ вероятность появления нетипичной последовательности стремится к нулю и поэтому достаточно рассматривать типовой ансамбль $2^{NH\ X}$ типовых равновероятных типовых последовательностей сообщений.

Таким образом, ансамбль из N букв алфавита может быть сжат до $NH\ X \le N \log n$ бит (теорема о сжатии Шеннона).

Соотношение неопределенности и информация Фишера. Рассмотрим процесс измерения координаты x для упрощения в одномерном пространстве. Результат многократного измерения данной величины можно охарактеризовать средними значениями как $\langle x \rangle = \int x p\ x,t\ dx$, $\langle x^2 \rangle = \int x^2 p\ x,t\ dxp$, где интегрирование осуществляется по всему пространству значений измеряемой величины и $p\ x,t \ge 0$ при условии нормировки функции плотности распределения вероятностей $\int p\ x,t = 1$ и $\lim_{x \to \pm\infty} x^n p = 0,\ n = 0,1,2$. Проинтегрируем по частям условие нормирование функции $p\ x,t \ge 0$ и получим $xp\big|_{x=-\infty}^{+\infty} - \int x \frac{\partial p}{\partial x} dx = 1$.

Примем за нулевое значение первый член, согласно ранее принятому предположению и получим условие $\int x \frac{\partial p}{\partial x} dx = -1$. Положим теперь, что $u = x\sqrt{p}$ и $\vartheta = \frac{1}{\sqrt{p}} \frac{\partial p}{\partial x}$.

Из известного неравенства Шварца $u,u\ \ \vartheta,\vartheta \ge \left| u,\vartheta \right|^2$ $u,\vartheta\ \int u^* \vartheta dx$ получим соотношение «неопределенности» в виде $\langle x^2 \rangle I \ge 1$, где $I = \int \frac{1}{p} \left(\frac{\partial p}{\partial x} \right)^2 dx$ и называется информацией Фишера.

Соотношение между дивергенцией, информационной энтропией Шеннона и количеством информации Фишера. Допустим, что X является случайной величиной с заданной (в общем случае не гауссовской) плотностью распределения вероятностей и конечной величиной дисперсии. Пусть $X_t \overset{d}{=} X + \sqrt{t} Z$, где Z случайная величина, имеет стандартное нормальное распределение, независимое от X. Тогда имеем следующее соотношение между информационной энтропией Шеннона и количеством информации Фишера[1]:

$$H\ X = \frac{1}{2} \log\ 2\pi e - \frac{1}{2} \int_0^{\infty} \left[I\ X_t - \frac{1}{1+t} \right] dt .$$

Обозначим относительную энтропию (расхождение Кульбака-Леблера) для плотности вероятностей $p\ x$ относительно нормальной $q\ x$ с тем же средним значением и дисперсией как и у $p\ x$ в виде $S\ X = \int p\ x \log \left[\frac{p\ x}{q\ x} \right] dx$. Относительная энтропия не симметричная функция и поэтому не обладает свойством метрики (расстояния), а измеряет отклонение $p\ x$ от $q\ x$. Если среднее $E\ X = f$ и $\mathrm{var}\, X = \sigma^2$, то имеем:

[1] M. Madiman, A. Barron, Generalized entropy power inequalities and monotonicity properties of information // IEEE Transactions on Information Theory. – 2007. – Vol. 53. – № 7 (arXiv: cs / 0605047 [cs. IT]).

$$S\ X\ =\int p\ x\ \log p\ x\ dx-\int p\ x\ \log q\ x\ dx=-H\ X\ -\int p\ x\ \left[\sigma^2\frac{1}{\sqrt{2\pi\sigma^2}}-\frac{x-a\ ^2}{2\sigma^2}\right]dx=$$

$$=\frac{1}{2}\left[\log\ 2\pi\sigma^2\ +1\right]-H\ X\ .$$

Таким образом, относительная энтропия определяет отличие информационной энтропии Шеннона случайной величины X от нормального закона. При $p\ x$ равном $q\ x$ величина $S\ X$ равна нулю, т.е. нормальное распределение имеет при заданной дисперсии максимальную величину. Для случайной величины X с определенными ранее параметрами обобщенная стандартная мера количества информации Фишера определяется как:

$$\Phi\ X\ =\sigma^2\mathrm{E}\left[\frac{p'\ X}{p\ X}-\frac{q'\ X}{q\ X}\right]^2 \text{ и } S\ X\ =\frac{1}{2}\int_0^1\Phi\ \sqrt{t}X+\sqrt{1-t}Y\ dt\,.$$

Тождество de Bruijn определяет соотношение между энтропией Шеннона и количеством информации Фишера в виде: $\frac{\partial}{\partial t}h_e\ X+\sqrt{t}Z\ =\frac{1}{2}I\ X+\sqrt{t}Z$, где $h_e=-\int_{-\infty}^{+\infty}p\ x\ \ln p\ x\ dx$ означает дифференциальную энтропию Шеннона по основании e . В частном случае в пределе $t\to 0$ имеем из приведенного выражения $\frac{\partial}{\partial t}h_e\ X+\sqrt{t}Z\ \Big|_{t=0}=\frac{1}{2}I\ X\ .$

Тождество de Bruijn для дивергенции Кульбака – Леблера и относительной информации Фишера имеет вид: $\frac{d}{dt}S\ \ p|q\ =-\frac{1}{2}\Phi\ \ p|q\ $. Для меры относительной энтропии Реньи типа:

$$D_\alpha\ \ P\|Q\ =\frac{1}{1-\alpha}\log\int\left(\frac{P}{Q}\right)^{\alpha-1}dP,\ \alpha>0,\ P\ll Q$$

имеем

$$\frac{d}{d\delta}D_\alpha\ \ P\|Q\ \Big|_{\alpha=0}=-\frac{\alpha}{2}\int_{-\infty}^{+\infty}\left(\nabla\log\frac{p\ z}{q\ z}\right)^2\frac{p^\alpha\ z\ q^{1-\alpha}\ z}{\int_{-\infty}^{\infty}p^\alpha\ u\ q^{1-\alpha}\ u\ du}dz$$

при условии $\lim_{z\to\infty}\frac{d}{dz}\left[p^\alpha\ z\ q^{1-\alpha}\ z\ \right]=0$. Для более обобщенных мер типа $I_f\ \ P\|Q\ =\int f\left(\frac{dP}{dQ}\right)dQ$ имеет место соотношение[2]:

$$\frac{d}{d\delta}I_f\ \ P\|Q\ \Big|_{\delta=0}=-\frac{1}{2}\int q\ y\ f''\left(\frac{p\ y}{q\ y}\right)\left(\nabla\frac{p\ y}{q\ y}\right)^2dy\,.$$

Имеет место соотношение $\left|\frac{dS}{dt}\right|\le\gamma\sqrt{I}$, т.е., скорость производства энтропии определяется количеством информации Фишера. Для диффузионных процессов имеем $\frac{dS}{dt}=I\ge 0$ и $\frac{d^2S}{dt^2}=\frac{dI}{dt}\le 0$. Тогда имеем:

$$S\ t=0\ \le S\ t\ \le S\ t=0\ +\ t-t_0\ \ I\ t=0\ .$$

Информационная геометрия. Рассмотрим некоторые примеры:

---

[2] D. Guo, Relative entropy and score function: New information-estimation relationships through arbitrary additive perturbation // ISIT 2009, Seoul, Korea. – 2009. – Pp. 814-818.

Пример 1: Квантовые геометрические аналоги классических моделей кривизны в информационной геометрии искривленных пространственно-временных континуумов. Рассмотрим в качестве примера факты геометрии пространства квантовых состояний. Расстояние между двумя квантовыми состояниями $|\psi_1\rangle$ и $|\psi_2\rangle$ можно определить различными способами (V. V. Dodonov, O. V. Man'ko, V. I. Man'ko, A. Wunsche, Phys. Scripta 59, 81 (1999)). Например, широко применяемые меры расстояния Fubiny-Study (FS) и Wootters (W) определяются соответственно в следующем виде:

$$d^{\,\mathrm{FS}}\ |\psi_1\rangle,|\psi_2\rangle\ = \gamma\ \sqrt{1-|\langle\psi_1|\psi_2\rangle|^2}\quad \text{и}\quad d^{\,\mathrm{W}}\ |\psi_1\rangle,|\psi_2\rangle\ = \arccos\gamma|\langle\psi_1|\psi_2\rangle|,$$

где γ – постоянная величина. Несмотря на внешнее различие, данные меры расстояния эквивалентно определяют расстояние между квантовыми состояниями. Так для близких состояний, когда $|\langle\psi_1|\psi_2\rangle|^2 = 1-\delta^2$, где δ – малая величина, имеем соотношение $d^{\,\mathrm{FS}} = d^{\,\mathrm{W}} = \gamma\delta$. Аналогичным образом определяются другие меры расстояний (см., ниже). Аналогично данному результату элементы длины для семейства (множества) векторов квантовых состояний $|\psi\ \xi^1,\xi^2,\ldots,\xi^k\ \rangle$ параметризованных k параметрами $\xi^1,\xi^2,\ldots,\xi^k$, определенные на заданных метриках расстояния, эквивалентны для различных определений расстояния $ds^2 = g_{ij}d\xi^i d\xi^j$ с метрическим тензором:

$$g_{ij} = \gamma^2\mathrm{Re}\ \langle\psi_i|\psi_j\rangle - \langle\psi_i|\psi\rangle\langle\psi|\psi_j\rangle\ ,\ \text{где}\ |\psi_i\rangle = \frac{\partial}{\partial\xi^i}|\psi\ \ \xi^1,\xi^2,\ldots,\xi^k\ \rangle.$$

Приведенная форма метрики расстояния применяется на практике многими исследователями и обычно принимается $\gamma = 2$. Тогда для двумерного случая g_{ij} является метрическим тензором сферы с единичным радиусом (сфера Блоха). При рассмотрении эволюции квантового состояния, описываемой уравнением Шредингера, вводится понятие скорости квантовой эволюции

$$\vartheta = \frac{ds}{dt} = \frac{\gamma}{\hbar}\sqrt{\langle\ \Delta H\ ^2\rangle},\ \text{где}\ \Delta H = H - \langle H\rangle.$$

Рассмотрим теперь определение геодезической кривой на пространстве векторов квантовых состояний. Геодезическая линия (однопараметрическое множество векторов квантовых состояний), соединяющая два вектора состояний $|\psi_0\rangle$ и $|\psi_1\rangle$ можно определить как линейную комбинацию (аналог суперпозиции):

$$|\psi\ \ \xi\ \rangle = C\left[\ 1-\xi\ |\psi_0\rangle + \xi|\psi_1\rangle e^{i\phi}\right], \qquad (1)$$

где ξ – параметр, принимающий значения от 0 до 1.

Примечание 1. Фазовый множитель $e^{i\phi}$ выбирается следующим образом. Векторы $|\psi_0\rangle$ и $|\psi_0\rangle e^{i\phi_0}$ определяют эквивалентные квантовые состояния. Поэтому требуется выполнение условия эквивалентности геодезических линий определенных между состояниями $|\psi_0\rangle$ и $|\psi_1\rangle$, и состояниями $|\psi_0\rangle e^{i\phi_0}$ и $|\psi_1\rangle e^{i\phi_1}$. Данное условие выполняется, если выбрать $e^{i\phi} = \dfrac{\langle\psi_1|\psi_0\rangle}{|\langle\psi_1|\psi_0\rangle|}$. Условие нормализации для параметра C определяется из выражения внутреннего произведения $\langle\psi\ \ \xi\ |\psi\ \ \xi\ \rangle = 1$ и имеет следующий вид: $C = \dfrac{1}{\sqrt{1-2\xi\ \ 1-\xi\ \ \ 1-|\langle\psi_1|\psi_0\rangle|}}$. Отметим, что геодезическая линия (1) является множеством состояний и существует много способов её параметризации. В геометрии квантовых состояний показано, что длина кривой в квантовом пространстве состояний не зависит от пути её параметризации.

Для вычисления длины геодезической линии удобно представлять определяющее её уравнение в виде:

$$|\psi\ \ \xi\ \rangle = C\left[\ \sin\left(\frac{1}{2}\theta\right)|\psi_0\rangle + \cos\left(\frac{1}{2}\theta\right)|\psi_1\rangle e^{i\phi}\ \right], \qquad (2)$$

где новый параметр $0 \le \theta \le \pi$ и константа нормализации $C = \dfrac{1}{\sqrt{1+|\langle\psi_1|\psi_0\rangle|\sin\theta}}$.

Подчеркнем, что (1) и (2) адекватно описывают однопараметрическое семейство векторов квантовых состояний в виде геодезических линий.

Используя определение метрики как: $g_{ij} = \gamma^2 \mathrm{Re}\ \langle\psi_i|\psi_j\rangle - \langle\psi_i|\psi\rangle\langle\psi|\psi_j\rangle$ для однопараметрического множества состояний дает выражение $ds = \dfrac{\gamma}{2}\dfrac{\sqrt{1-|\langle\psi_1|\psi_0\rangle|^2}}{1+|\langle\psi_1|\psi_0\rangle|\sin\theta}$.

Тогда длина геодезической линии, соединяющей состояния $|\psi_0\rangle$ и $|\psi_1\rangle$, определяется в виде:

$$s = \int ds = \gamma \arccos|\langle\psi_1|\psi_0\rangle|. \quad (3)$$

Таким образом, выражение (3) для длины геодезической линии совпадает с выражением метрики Wootters расстояния между векторами квантовых состояний. Аналогично можно вычислить длину кривой (1), соединяющей состояния $|\psi_0\rangle$ и $|\psi_1\rangle$, для определенной фазы ϕ. Тогда геодезическая линия определяется как кривая минимальной длины на семействе кривых.

Минимальная длина достигается при установленном выше условии $e^{i\phi} = \dfrac{\langle\psi_1|\psi_0\rangle}{|\langle\psi_1|\psi_0\rangle|}$ и эквивалентно метрике расстояния Wootters.

Рассмотрим теперь другой геометрический фактор – кривизна пространства и его квантовый аналог в пространстве векторов квантовых состояний.

– *Кривизна*. Вектор состояния квантовой эволюции от одного параметра, такой как время t, и однопараметрического множества векторов состояний $|\psi\ t\ \rangle = \exp\ -iHt\ |\psi_0\rangle$, генерируемое гамильтонианом системы. Отклонение вектора состояний $|\psi\ t\ \rangle$ от геодезической линии, связывающей состояния $|\psi_0\rangle$ и $|\psi_1\rangle$, определяется через кривизну пространства. Для введения понятия кривизны рассмотрим случай эволюции из двух состояний $|\psi_0\rangle$ в $|\psi_1\rangle$. На первом этапе предположим, что осуществляется эволюция в течении отрезка времени Δt из начального состояния $|\psi_0\rangle$ в промежуточное состояние $|\psi'\rangle$ в виде $|\psi'\rangle = e^{-\frac{i}{\hbar}H\Delta t}|\psi_0\rangle$ и далее в течении отрезка времени $\Delta t'$ из состояния $|\psi'\rangle$ в состояние $|\psi_1\rangle = e^{-\frac{i}{\hbar}H\Delta t'}|\psi'\rangle = e^{-\frac{i}{\hbar}H\ \Delta t+\Delta t'}\ |\psi_0\rangle$, где H – не зависящий от времени гамильтониан. Без потери общности в дальнейшем принимается $\Delta t = \Delta t'$. Отклонение квантовой эволюции от геодезической линии, связывающей состояния $|\psi_0\rangle$ и $|\psi_1\rangle$, может быть охарактеризовано максимальным значением величины $|\langle\psi'|\psi\ \xi\ \rangle|^2$ параметризованной ξ. При $\max|\langle\psi'|\psi\ \xi\ \rangle|^2 = 1$ состояние $|\psi'\rangle$ принадлежит геодезической. Отклонение $|\psi'\rangle$ от геодезической увеличивается с уменьшением величины $\max|\langle\psi'|\psi\ \xi\ \rangle|^2$, соответственно. Обычно вводится следующее выражение $1-\max|\langle\psi'|\psi\ \xi\ \rangle|^2 = \min\ 1-|\langle\psi'|\psi\ \xi\ \rangle|^2$, которое эквивалентно нулю, когда отклонение равно нулю, и положительно возрастает, когда отклонение увеличивается.

Нетрудно заметить, что данное выражение эквивалентно метрики расстояния Fubiny-Study.

Пример 2. Рассмотрим теперь уравнение геодезических в рамках квантовой геометрии с обобщением понятия в квантовых системах отсчета. В этом случае рассматривается 8-мерное фазовое пространство $x^\mu\ \ q^r, p^s\ \ , q^0 = ct;\ p^0 E/c$, метрикой ds^2 типа:

$$ds^2 = dt^2 - \frac{1}{c^2}x^2 + \frac{\hbar^2}{\mu^4 c^6}\left[\frac{1}{c^2}dE^2 - dp^2\right], \quad (4)$$

где $E = mc^2 \approx m_0c^2 + \frac{1}{2}m_0c^2\frac{a^2}{A^2}$, $A = \frac{\mu^2c^2}{m_0\hbar}$ описывает пространство-время квазиклассического уровня с ограничением на максимальное собственное ускорение a для частицы в виде величины A, полученной из квантовых ограничений. Пространство-время, описываемое метрикой (9), является 8-мерным: первые четыре компоненты образуют пространство-время, описываемое 4-вектором $x^\mu \equiv t, x/c$, $\mu = 0,1,2,3$; вторая группа 4-компонент, ортогональных к первой группе x^μ , пропорциональна 4-скорости $u^\mu = \frac{cdx^\mu}{d\tau} = \left(\frac{c}{\sqrt{1-\vartheta^2/c^2}}, \frac{\vartheta}{\sqrt{1-\vartheta^2/c^2}}\right) = u^0, u$. Событие в метрике (4) описывается 8-компонентами $\xi^\mu = t, x/c; w^0, w$, $w^0 = u^0/k$, $w = u/k$, где κ – нормирующий параметр. В этом случае 8-мерный пространственно-временной континуум определяется в виде:

$$g_{\mu\nu}d\xi^\mu d\xi^\nu = dt^2 - |dx/c|^2 + |dw^0|^2 - |dw|^2. \quad (5)$$

В этом случае преобразования Лоренца для (5) принимает обобщенный вид:

$$dt' = \frac{1}{\Gamma}\left\{dt - \frac{\vartheta_0}{c^2}dx + \frac{a_0\vartheta_0}{ck_1}dw^0 - \frac{a_0}{k_1}dw^1\right\};\ dx' = \frac{1}{\Gamma}\left\{-\vartheta_0 dt + dx - \frac{a_0}{k\vartheta_0^2}cdw^0 + \frac{a_0}{k_1}\vartheta_0 dw^1\right\};$$

$$dw^{0\prime} = \frac{1}{\Gamma}\left\{\frac{\vartheta_0 a_0}{ck_1}dt - \frac{a_0}{ck_1}dx + dw^0 - \frac{\vartheta_0}{c}dw^1\right\};\ dw^{1\prime} = \frac{1}{\Gamma}\left\{-\frac{a_0}{k_1}dt + \frac{\vartheta_0 a_0}{c^2k_1}dx - \frac{\vartheta_0}{c}dw^0 + dw^1\right\}; \quad (6)$$

$$\Gamma = \sqrt{\left(1-\frac{\vartheta_0^2}{c^2}\right)\left(1-\frac{a_0^2}{c^2}\right)},\quad k_1 = k\left(1-\frac{\vartheta_0^2}{c^2}\right)^{3/2},\quad a_0 \cong \sqrt{\frac{c^7}{\hbar G}}.$$

При $\vartheta/c \ll 1$ и $c/k_1 \ll 1$ имеем $E = m_0c^2 + \frac{1}{2}m_0\vartheta^2 + \frac{1}{2}m_0c^2\frac{a^2}{k^2}$.

Уравнение геодезических (как частный случай обобщения для квантового параллельного переноса) имеет вид:

$$\ddot{x}^\alpha + \frac{i}{\hbar}F^\alpha_{\beta\nu}\dot{x}^\beta\dot{x}^\nu = 0, \quad (7)$$

где связность $\Gamma = -\frac{i}{\hbar}F$ задается в виде: $F = p_r dq^r \begin{Vmatrix}\eta & 0\\ 0 & 0\end{Vmatrix} - q^r dp_r \begin{Vmatrix}0 & 0\\ 0 & \eta\end{Vmatrix}$, $\eta = \mathrm{diag}\ 1,1,1,-1$. Уравнение (7) для $x^\mu = q^r, p^s$ при заданном F распадается на систему уравнений:

$$\ddot{q}^l + \frac{i}{\hbar}p_s\dot{q}^s\dot{q}^l = 0;\quad \ddot{p}^l - \frac{i}{\hbar}\dot{p}_s q^s\dot{p}^l = 0. \quad (8)$$

Если ввести обозначения $z = q - ip, \bar{z} = q + ip$, то из (13) при $\xi = \dot{z}^k, z^k = x^k + iy^k, \alpha_k = \gamma_k + i\omega_k$ имеем уравнение диссипативной системы:

$$\ddot{x}^k + \gamma\dot{x}^k - \omega\dot{y}^k = 0;\quad \ddot{y}^k + \gamma\dot{y}^k + \omega\dot{x}^k = 0 \quad (9)$$

в виде системы связанных осцилляторов.

Свойства количества классической и квантовой информации.

В табл. 1 приведены основные свойства классической и квантовой мер информации, применяемых в решении задач информационного анализа и проектирования квантовой эволюции.

Одними из основных проблем квантовой теории информации, решение которых важно для исследования квантовой эволюции динамических систем, являются следующие:

Таблица 1. Свойства классической и квантовой информации

Теории информации	
Классическая	**Квантовая**
Энтропия Шеннона: $H\ X\ = -\sum_x p_x \log p_x$	*Энтропия фон Неймана*: $S\ \rho\ = -Tr\ \rho \log \rho$
Различимость и доступность информации	
Знаки алфавита различимы: $N = \lvert X \rvert$	*Граница Холево - Левитина*: $H\ X:Y\ \le S\ \rho\ - \sum_x p_x S\ \rho_x\ ,\ \rho = \sum_x p_x \rho_x$
Информационно – теоретические отношения	
Неравенство Фано: $H\ p_e\ + p_e \log\ \lvert X \rvert - 1\ \ge H\ X\ \lvert Y$	*Квантовое неравенство Фано*: $H\ F\ \rho, E\ + 1 - F\ \rho, E\ \ \log\ d^2 - 1\ \ge S\ \rho, E$
Взаимная информация: $H\ X:Y\ = H\ Y\ - H\ Y\ \lvert X$	*Когерентная информация*: $I\ \rho, E\ = S\ E\ \rho\ \ - S\ \rho, E$
Неравенство цепи обработки данных: $X \to Y \to Z$ $H\ X\ \ge H\ X:Y\ \ge H\ X:Z$	*Квантовое неравенство цепи обработки данных*: $\rho \to \mathrm{E}_1\ \rho\ \to\ \mathrm{E}_2 \circ \mathrm{E}_1\ \ \rho$ $S\ \rho\ \ge I\ \rho, \mathrm{E}_1\ \ge I\ \rho, \mathrm{E}_2 \circ \mathrm{E}_1$
Кодирование канала передачи данных без шума	
Теорема Шеннона: $n_{bits} = H\ X$	*Теорема Шумахера*: $n_{qubits} = S\left(\sum_x p_x \rho_x \right)$
Пропускная способность каналов связи с шумом для классической информации	
Теорема Шеннона кодирования канала связи с шумом: $C\ \mathrm{N}\ = \max_{p\ x} H\ X:Y$	*Теорема Holevo-Schumacher-Westmoreland*: $C^{1}\ \mathrm{E}\ = \max_{p_j, \rho_j} \left[S\ \rho'\ - \sum_x p_x S\ \rho'_x\ \right],$ $\rho'_x = \mathrm{E}\ \rho_x\ ,\ \rho' = \sum_x p_x \rho'_x$

- Классическая, квантовая и полная корреляции: Взаимосвязь с мерами запутанных состояний;
- Доступная информация и информационно-теоретические модели квантовых измерений;
- Извлечение информации эффективными измерениями и границы взаимной информации.

Исследуем кратко на примерах некоторые из этих особенностей, используемые в моделях квантового нечеткого вывода (КНВ).

Пример 3. Рассмотрим особенности описания и информационного анализа запутанных состояний Белла $\left|\Psi_Q\right\rangle = \frac{\left|0_1 0_0\right\rangle - \left|1_1 1_0\right\rangle}{\sqrt{2}}$. Так как состояние Белла с оператором плотности чистое, то ρ_Q представляет чистый ансамбль. Поэтому неопределённость квантового состояния отсутствует, т.е. энтропия фон Неймана $S^{vN}\ \rho_Q\ = 0$.

Редуцированный оператор плотности ρ_0 для квантового бита $\left|0_0\right\rangle$ есть частный след над системой Q, т.е. $\rho_0 = Tr_1\ \rho_Q\ = \frac{1}{2}\ \left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|\ = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Следовательно, квантовая неопределённость в состоянии $\left|0_0\right\rangle$ определяется энтропией фон Неймана как $S^{vN}\ \rho_Q\ = 1$.

Таким образом, информационный анализ неопределенности в состоянии составной квантовой системы позволяет четко разъяснить наличие необычных (неклассических) свойств: игнорирование в

ней части информации о состоянии подсистемы приводит к увеличению квантовой неопределённости.

В результате квантовая неопределенность в «части» (подсистеме) Q_0 больше, чем в «полной» (составной) квантовой системе Q. Такой эффект отсутствует в классических системах в силу свойств меры информационной энтропии Шеннона.

Пример 4. Рассмотрим состояние Белла $|\psi\rangle = \frac{1}{\sqrt{2}}\ |00\rangle + |11\rangle$ в Гильбертовом пространстве $\mathrm{H}_{AB} = \mathrm{H}_A \otimes \mathrm{H}_B$, где $\mathrm{H}_A = \mathrm{H}_B = \mathrm{H}_2$. Матрицы плотности $\rho_{AB} = |\psi\rangle\langle\psi|$, ρ_A, $\rho_{A|B}$ определяются как:

$$\rho_A = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix},\ \rho_{A|B} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix},\ \rho_{AB} = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

Матрица условной плотности $\rho_{A|B} = \rho_{AB}(\mathrm{I}_A \otimes \rho_B)^{-1}$ (в этом случае взаимная ρ_{AB} и маргинальная $\mathrm{I}_A \otimes \rho_B$ матрицы плотности коммутируют). Из определения энтропии фон Нёймана следует $S^{vN}(A) = S^{vN}(B) = 1$. Тогда $S(AB) = S(B) + S(A|B) = 1 - 1 = 0$, так как $S(A|B) = -1$.

Следовательно, в отличие от классической теории информации Шеннона квантовая условная энтропия фон Неймана может принимать *отрицательные* значения, когда рассматриваются запутанные состояния. Этот факт непосредственно связан с квантовой неразделимостью запутанных состояний, а сами они интерпретируются как гигантски (супер) коррелированные состояния. Таким образом, отрицательность условной энтропии указывает на наличие запутанных состояний в составной квантовой системе и определяет нижнюю границу их корреляции.

Существование данного факта установлено также в квантовых поисковых алгоритмах Шора и Гровера и используется в решении проблемы эффективного останова КА.

Отметим также, что не все базовые классические соотношения и неравенства имеют квантовые аналоги. Так, например, в классическом случае $I(x:y) \le \min\ H(x), H(y)$.

Тогда как в квантовом случае верхняя граница задается неравенством:

$$S(X:Y) \le 2\min\ S(X), S(Y)\ .$$

Квантовая теория информации имеет строго обоснованные правила, как извлекать информацию из неизвестного кантового состояния. Оптимальный квантовый процесс извлечения ценной информации из индивидуальных БЗ, спроектированных для фиксированных ситуаций управления на основе мягких вычислений, основан на четырех фактах квантовой теории информации, приведенных ниже. В частности, доказано, что существует: эффективное квантовое сжатие данных; «сцепление» классической и квантовых частей информации в квантовом состоянии; полная корреляция в квантовом состоянии является «смесью» классической и квантовой корреляций; наличие скрытой (наблюдаемой) классической корреляции в квантовом состоянии. Далее кратко рассматривается физический смысл перечисленных фактов и их роль в процессах проектирования оптимальных процессов и сигналов управления на основе КНВ.

Факт 1. Эффективное квантовое сжатие данных. В классической теории информации Шеннон показал, насколько (при заданной точности) предельно можно сжать сообщение, состоящее из N независимых знаков x_a , где каждый знак появляется в сообщении с априорной вероятностью p_a, используя понятие информационной энтропии. Информационная энтропия Шеннона $H\ p_a$ определяется как $H\ p_a = -\sum_a p_a \log_2 p_a$. Было доказано следующее утверждение: блок кодов длиной NH битов достаточен для кодирования всех типовых (наиболее часто появляющихся)

последовательностей без учета способов кодирования нетипичных последовательностей сообщений. При этом вероятность ошибки кодирования (потери информации) не превосходит заданный порог ε. В квантовой теории информации знаками являются матрицы плотности. Возможны два варианта, когда матрицы плотности соответствуют ансамблю чистых состояний $|\phi_a\rangle$ или когда ансамбль формируется матрицами плотности ρ_a с вероятностью p_a. Рассмотрим ансамбль состояний для второго варианта. В этом случае матрица плотности сообщений, состоящих из *N* знаков, описывается как $\rho^N = \rho \otimes \rho \otimes \cdots \otimes \rho$, где $\rho = \sum_a p_a |\phi_a\rangle\langle\phi_a|$.

Энтропия сообщений фон Неймана $S = -Tr\ \rho \ln \rho$ имеет простое соотношение с энтропией ансамбля, $S\ \rho^N = NS\ \rho$. Известно следующее неравенство между Шенноновской информационной энтропией и энтропией фон Неймана: $H\ p \geq S\ \rho$, т.е. значение информационной энтропии Шеннона превышает значение энтропии фон Неймана. Это означает, что применение квантовой теории информации позволяет осуществить более глубокое сжатие классической информации.

Факт 2. Сцепление (разделение) информации в квантовом состоянии в виде классической и квантовых частей. Рассмотрим модель обобщённого измерения (см. разд. 2) на состоянии $A_i A_i^\dagger$, для которой матрица плотности имеет следующее определение: $\rho_B^i = \dfrac{A_i \rho_B A_i^\dagger}{Tr\ A_i \rho_B A_i^\dagger}$.

Конечное состояние подсистемы *B* будет тогда $\sum_i A_i \rho_B A_i^\dagger = \sum_i p_i \rho_B^i$. Энтропия редуцированного состояния равна $\sum_i p_i S\ \rho_B^i$. Количество классической информации, полученной на измерении i с вероятностью p_i выражается как информационная энтропия Шеннона $H\ p$. Если квантовые состояния ρ_B^i принадлежат ортогональным подпространствам, то энтропия конечного состояния (после измерения) есть сумма редуцированной квантовой энтропии, $\sum_i p_i S\ \rho_B^i$ и классической информации т.е.:

$$S\left(\sum_i p_i \rho_B^i\right) = \underbrace{H\ p}_{\text{Классическая}} + \underbrace{\sum_i p_i S\ \rho_B^i}_{\text{Квантовая}}.$$

Таким образом, количество информации, содержащейся в квантовом состоянии, может быть разделено (сцеплено в виде) на квантовую и классическую части. Поэтому при моделировании робастных структур ИСУ с помощью ОБЗ моделируется классическая часть информации, а ее *дефицит* может быть определён как:

$$\Delta I = \underbrace{S\left(\sum_i p_i \rho_B^i\right)}_{\text{Полная}} - \underbrace{\sum_i p_i S\ \rho_B^i}_{\text{Квантовая}} = \underbrace{H\ p}_{\text{Классическая}}.$$

Можно извлечь, следовательно, дополнительное количество ценной квантовой информации из индивидуальных БЗ для последующего использования при проектировании интеллектуального управления повышенного уровня. При этом применяются квантовые процедуры сжатия и редукции избыточной информации, содержащейся в классических сигналах управления (привлекая соответствующие модели квантовой корреляции в квантовом алгоритме КНВ).

Факт 3. Количества полной, классической и квантовой корреляций. Запутанные состояния или, в общем виде, квантовая корреляция являются типичными физическими ресурсами квантовых вычислений. Однако не все виды корреляций имеют чисто квантовую природу. Иными словами, полные корреляции представляют собой «смеси» классической и квантовой корреляций. Для оптимального проектирования (эффективно моделируемых на классических компьютерах) заданного класса КА важно знать тип (и вид) необходимой классической корреляции. Так, например, если

возможно определить классическую часть корреляций, то, используя оптимальные ПООЗ-меры измерения, допустимо извлечь максимальное количество информации в классической форме, содержащейся в квантовом состоянии, с минимумом возрастания энтропии. Количество полной корреляции может быть разделено на классическую и квантовую части. Данная мера эквивалентна мере максимальной классической/квантовой взаимной информации $I\ A{:}B$, сохраняя непосредственно прямую физическую интерпретацию взаимоотношений между соответствующими мерами.

Факт 4. Скрытая (наблюдаемая) классическая корреляция в квантовом состоянии. В квантовой теории информации установлен следующий неожиданный факт. Условие пропорционального увеличения количества информации $I_{Cl}\ \rho = \max\limits_{M_A \otimes M_B} I\ A{:}B$, определённого локальными измерениями $M_A \otimes M_B$ на состоянии ρ_{AB}, может быть нарушено при некоторых экстремальных ограничениях на начальное смешанное состояние ρ. Так, например, начальный объем информации в виде одного классического бита информации, посланного от A к B, может увеличиться на этапе приема на определённую величину в количественной мере $I_{Cl}\ \rho$. Этот факт объясняется с позиции феномена наблюдения классической корреляции в квантовом состоянии ρ. Так как пропорциональное увеличение количества информации $I_{Cl}\ \rho$ выполняется на классическом уровне, то феномен наблюдения корреляции является чисто квантовым эффектом, возникающим вследствие неразличимости квантовых неортогональных состояний.

Поэтому существуют квантовые двухчастичные состояния, которые содержат большое количество классической корреляции, ненаблюдаемой на классическом уровне из-за диспропорционально малого для ее наблюдения необходимого количества классической информации в канале передачи (ограниченная способность передачи информации).

Существует $2n+1$ квантовых битов, с помощью которых однобитовое сообщение вдвое увеличивает оптимальное количество классической взаимной информации как результат измерений между подсистемами. В общем случае для посланных $n/2$ битов происходит увеличение указанного количества информации до n битов. Получить указанный эффект на классическом уровне невозможно в силу законов классической физики. При этом замечателен следующий факт: состояния, поддерживающие указанный эффект, не обязательно должны быть запутанными и соответствующий классический канал обмен данными можно реализовать с помощью преобразования Адамара.

Приведенные факты составляют информационный ресурс основы КНВ, используемый при моделировании робастных БЗ для интеллектуальных НР.

– *Полная корреляция и скрытая (наблюдаемая) корреляция в квантовых состояниях.* Существует уверенность, что ожидаемая вычислительная мощность квантовых вычислений исходит из существования квантового ресурса. Запутанные состояния, или квантовая корреляция в общем случае, являются яркими тому примерами. Однако, как упоминалось в разд. 3, не все виды корреляции имеют чисто квантовую природу, т.е. полная корреляция представляет «смесь» классической и квантовой корреляций. Важным моментом является знание о том, как и где, используется классическая корреляция в КА. Например, если возможно определить и выделить классическую часть корреляции, то с помощью оптимального измерения можно извлечь некоторое дополнительное количество информации в классической форме, скрытое в квантовом состоянии, с минимальным возрастанием энтропии.

Физически перечисленные виды корреляции характеризуются количеством работы (шумом), которое необходимо совершить для устранения (разрушения) корреляций: для полной корреляции требуется количество работы до полного разрушения, для квантовой корреляции достаточно количество работы до разрушения на разделимые состояния. Однако и в случае классической корреляции максимальная корреляция разрушается после устранения квантовой корреляции. Полное количество корреляции, измеряемое минимальным производством рандомизации и эквивалентное требованию полного разрушения всех видов корреляций в состоянии ρ_{AB}, эквивалентно квантовому количеству взаимной информации.

Классическая и квантовая корреляции. Классическую взаимную информацию, содержащуюся в квантовом состоянии ρ_{AB} (до его измерения), можно оценить естественным образом как максимальную взаимную информацию, которую можно извлечь путём локальных измерений $M_A \otimes M_B$ на состоянии ρ_{AB}:

$$I_{Cl}\ \rho\ = \max_{M_A \otimes M_B} I\ A:B\ .$$

Здесь $I\ A:B\ $ – классическая взаимная информация, определяемая в виде:

$$I\ A:B\ \equiv H\ p_A\ + H\ p_B\ - H\ p_{AB}\ ,$$

где H – информационная энтропия и p_{AB}, p_A, p_B – функции плотности распределения вероятностей взаимного и индивидуального результатов, полученных локальными измерениями $M_A \otimes M_B$ на состоянии ρ.

Пример 5: *Взаимная информация и классическая корреляция*. Для понимания роли классической корреляции, а также её взаимосвязи с понятием взаимной информации, определим квантовую взаимную информацию для двухчастичного состояния ρ_{AB} квантовой системы в форме Стратоновича

$$I\ A:B\ = S\ \rho_A\ + S\ \rho_B\ - S\ \rho_{AB}\ .$$

Рассмотрим составную систему AB в состоянии ρ_{AB}, способную пребывать в состоянии ρ_A с вероятностью p и с вероятностью $1-p$ – в другом состоянии ρ_B. Для данного случая составной системы AB взаимная информация может быть вычислена в следующем виде:

$$I\ A:B\ = 2H\left(\frac{1}{2}\left[1+\sqrt{p^2+\ 1-p\ ^2}\right]\right) - H\left(\frac{1}{2}\left[1+\sqrt{1+3p^2-3p}\right]\right). \qquad (10)$$

Если ρ_{AB} – разделимое состояние, то его относительная энтропия в запутанном состоянии равна нулю. Физическая интерпретация значения $I_{Cl}\ \rho$ многозначна: $I_{Cl}\ \rho$ выступает максимальной классической корреляцией, извлекаемой чисто локальной процедурой измерения из состояния ρ; $I_{Cl}\ \rho$ соответствует классическому определению, когда состояние ρ – «классическое», т.е. диагональное в некотором (локально используемом) вычислительном базисе и отвечает классическому распределению; если ρ – чистое состояние, то $I_{Cl}\ \rho$ задает корреляцию, определённую базисом Шмидта и эквивалентную мере перепутанных чистых состояний; $I_{Cl}\ \rho\ = 0$, если и только если $\rho_{AB} = \rho_A \otimes \rho_B$.

Известно, что некоторые подходящие меры квантовой корреляции должны удовлетворять некоторым аксиоматическим свойствам: 1) квантовая корреляция является нелокальной и не может возрастать при локальных процедурах измерений (свойство монотонности); 2) полная пропорциональность; 3) приращение пропорциональности; 4) непрерывность по ρ.

Физически свойство 2) означает, что протокол состояний, составленный из некоррелированного начального состояния, использующий l квантовых битов или $2l$ классических битов (для передачи сообщений по квантовому каналу связи) и применяющий локальные операции, не может породить более чем $2l$ битов корреляции. Свойство 3) предполагает, что при передаче сообщения в количестве l квантовых битов или $2l$ классических битов корреляция в начальном состоянии не возрастает и не превышает величины $2l$ битов.

Свойства 1)-4) выполняются полностью для ряда известных мер корреляции. Эти свойства справедливы, в частности, для классической взаимной информации $I\ A:B\ $, когда передача сообщений осуществляется классическим способом. Так, например, свойства полной и приращения пропорциональности $I\ A:B\ $ для классического случая следуют из факта, что $\max\ H\ p_A\ , H\ p_B\ \le H\ p_{AB}\ \le H\ p_A\ + H\ p_B\ $, так что когда A посылает классическую систему A' к B, имеем $I_{Cl}\ \rho\ = I\ A;BA'\ \le I\ AA';B\ + H\ p_{A'}\ $.

Тогда свойство полной пропорциональности следует из свойства приращения пропорциональности. Это же выполняется для квантовой взаимной информации

$$I_Q\ A{:}B\ = S\ \rho_A\ + S\ \rho_B\ - S\ \rho_{AB}\ .$$

Неожиданным оказалось то, что свойство приращения пропорциональности нарушается для $I_{Cl}\ \rho$ экстремальным образом в случае смешанных начальных состояний ρ: простой классический бит, посланный от A к B, может в результате привести к увеличению $I_{Cl}\ \rho$ до некоторого большого значения.

Данный феномен рассматриваем как возможность наблюдения классической корреляции в квантовом состоянии ρ. Если свойство приращения пропорциональности $I_{Cl}\ \rho$ имеет место на классическом уровне, то феномен наблюдаемой классической корреляции является чисто квантовым эффектом. Этот результат непосредственно следует из неразличимости неортогональных квантовых состояний.

Пример 6. Допустим, что задано начальное состояние ρ, тип передачи сообщения и соответствующее количество передаваемой информации. Возрастание корреляции можно охарактеризовать следующими функциями:

$$I_{Cl}^{\ l} = \max_{\Lambda^{\ l}} I_{Cl}\ \ \Lambda^{\ l}\ \ \rho \quad \text{(одностороннее классическое сообщение)};$$

$$I_{Cl}^{\ l} = \max_{\Lambda^{\ l}} I_{Cl}\ \ \Lambda^{\ l}\ \ \rho \quad \text{(двухстороннее классическое сообщение)}.$$

Оператор Λ – операция над двухчастичным состоянием, которая состоит из локальных операций и содержит не более чем $2l$ классических или l квантовых битов в сообщении. Это отражено в соответствующих верхних индексах l или l. Через ρ и ρ' обозначены состояния до и после проведения операций с обменом сообщениями, $\rho' = \Lambda\ \rho$. Количество корреляции $I_{Cl}^{\ l}\ \rho$, скрытой (ненаблюдаемой) в состоянии с l квантовыми битами при одностороннем обмене сообщениями, может быть ограничено следующим условием: $I_{Cl}^{\ l}\ \rho - I_{Cl}\ \rho \le l + 2^l - 1\ I_{Cl}\ \rho$. Для малых значений $I_{Cl}\ \rho$, количество скрытой (ненаблюдаемой) корреляции при двустороннем обмене сообщениями ограничено сверху:

$$I_{Cl}^{\ l}\ \rho - I_{Cl}\ \rho \le 2l + O\ d^2 \sqrt{I_{Cl}\ \rho}\ \log I_{Cl}\ \rho\ .$$

Скрытая (наблюдаемая) классическая корреляция в квантовом состоянии. Обсудим ситуацию, в которой некоторое количество корреляции не доступно наблюдению при одностороннем обмене сообщениями. Начальное состояние определяется подсистемами A и B на соответствующих подпространствах размерностью $2d$ и d в виде:

$$\rho = \frac{1}{2d} \sum_{k=0}^{d-1} \sum_{t=0}^{1} |k\rangle\langle k| \otimes |t\rangle\langle t|\ _A \otimes\ U_t |k\rangle\langle k| U_t^{\dagger}\ _B, \qquad (11)$$

где операторы $U_0 = I$ и U_1 меняют исходный вычислительный базис на объединённый как $\left|\langle i|U_1|k\rangle\right| = \frac{1}{\sqrt{d}}\ \ \forall i,k$. Тогда B выбирает случайным образом состояние $|k\rangle$ из d состояний в двух возможных рандомизированных базисах (в зависимости от случая, когда $t = 0$ или 1 в (11)). В то же время наблюдатель A имеет полную информацию о квантовом состоянии наблюдателя B. Получив необходимое количество информации в виде $I_{Cl}^{\ l}\ \rho = \log d + 1$, A посылает значение t к B, который в свою очередь применяет оператор U_t к своему состоянию и измеряет значение k в вычислительном базисе. В результате A и B имеют измерение k и t, что даёт $I_{Cl}^{\ l}\ \rho = \log d + 1$ бит корреляции. Состояние ρ эволюционирует по следующему сценарию. Пусть $d = 2^n$. Тогда A выбирает случайным образом k длиной в n битов и посылает к B сообщение о состоянии $|k\rangle$ или $H^{\otimes n}|k\rangle$ в зависимости от случайного значения бита $t = 0$ или 1. Здесь H – преобразование Адамара;

A посылает t к B и позже наблюдает созданную корреляцию. Экспериментально установлено, что применения преобразования Адамара и измерения состояния квантовых битов достаточно, чтобы реализовать процедуру приготовления состояния ρ и затем извлечь скрытую в состоянии ρ' классическую корреляцию. Начальная корреляция является малой величиной, $I_{Cl}^{l}\ \rho = \frac{1}{2}\log d$. После полного измерения M_A при одностороннем обмене сообщениями конечное значение количества информации в квантовом состоянии определяется как $I_{Cl}\ \rho' = I_{Cl}^{l}\ \rho = \log d + 1$, т.е. количество доступной информации увеличивается.

Примечание 2. Отметим, что полное измерение M_A в базисе $|k\rangle \otimes |t\rangle$ оптимально для системы A. Выходное значение результата измерения точно даёт информацию о том, какое чистое состояние из ансамбля выбрано. Поэтому имеется возможность применить классический, локальный процесс обработки (результата измерения) для получения информации о распределении результатов других измерений. Для системы A выбор оптимального измерения позволяет для системы B извлечь из $I_{Cl}\ \rho$ *доступное* количество информации I_{Acc} об ансамбле равномерно распределённых состояний $|k\rangle,\ U_1 = H\ |k\rangle\ _{k=0,\ldots,d-1}$.

– *Доступная информация об ансамбле смешанных состояний*. В общем случае доступная информация об ансамбле смешанных состояний $\mathrm{E} = \{p_i, \eta_i\}$ определяется как максимальная взаимная информация между измеряемым состоянием с индексом i и результатом его измерения. Количество доступной информации $I_{Acc}\ \mathrm{E}$ можно охарактеризовать как максимальное значение информации, извлекаемое из квантового состояния с помощью ПООЗ-измерений (разд. 2) с элементами только ранга 1.

Допустим, что $M = \{\alpha_j |\phi_j\rangle\langle\phi_j|\}_j$ означает ПООЗ-измерение с элементами ранга 1, где каждое состояние $|\phi_j\rangle$ нормализовано и $\alpha_j > 0$. Тогда $I_{Acc}\ \mathrm{E}$ можно вычислить как:

$$I_{Acc}\ \mathrm{E} = \max_M \left[\underbrace{-\sum_i p_i \log p_i}_{\text{Классическая часть}} + \underbrace{\sum_i \sum_i p_i \alpha_j \langle\phi_j|\eta_i|\phi_j\rangle \log \frac{p_i \langle\phi_j|\eta_i|\phi_j\rangle}{\langle\phi_j|\mu|\phi_j\rangle}}_{\text{Квантовая часть}} \right], \qquad (12)$$

где $\mu = \sum_i p_i \eta_i$. Применим теперь выражение (12) к решению вышеупомянутой проблемы. Ансамбль состояний задается как $\left\{\frac{1}{2d}, U_t |k\rangle\right\}_{k,t}$ при следующих значениях $i = k,t;\ p_{k,t} = \frac{1}{2d},\ \mu = \frac{I}{2}$ и $\langle\phi_j|\mu|\phi_j\rangle = \frac{1}{d}$. Подставляя все из приведенных выражений в формулу для $I_{Acc}\ \mathrm{E}$, получим:

$$I_{Cl}\ \mathrm{E} = \max_M \left[\underbrace{\log 2d}_{\text{Классическая часть}} + \underbrace{\sum_{j,k,t} \frac{\varepsilon_j}{2d} \left|\langle\phi_j|U_t|k\rangle\right|^2 \log \frac{\left|\langle\phi_j|U_t|k\rangle\right|^2}{2}}_{\text{Квантовая часть}} \right] =$$

$$= \max_M \left[\underbrace{\log d}_{\text{Классическая часть}} + \underbrace{\sum_j \frac{\alpha_j}{d} \left(\frac{1}{2} \sum_{k,t} \left|\langle\phi_j|U_t|k\rangle\right|^2 \log \left|\langle\phi_j|U_t|k\rangle\right|^2 \right)}_{\text{Квантовая часть}} \right],$$

где использованы следующие обозначения: $\sum_j \alpha_j = d$ и $\forall j,t \ \sum_k \left|\langle \phi_j | U_t | k \rangle\right|^2 = 1$. Так как выполняется соотношение $\sum_j \frac{\alpha_j}{d} = 1,$ то второе выражение является выпуклой комбинацией и может быть ограничено сверху путём операции максимизации по первому члену в виде

$$I_{Cl}\ \mathrm{E}\ \leq \log d + \max_{|\phi\rangle} \frac{1}{2} \sum_{k,t} \left|\langle \phi | U_t | k \rangle\right|^2 \log \left|\langle \phi | U_t | k \rangle\right|^2 .$$

Отметим, что член $-\sum_{k,t} \left|\langle \phi | U_t | k \rangle\right|^2 \log \left|\langle \phi | U_t | k \rangle\right|^2$ представляет сумму энтропийных мер измеряемого состояния $|\phi\rangle$ в вычислительном и в обобщённом базисах. Такая сумма энтропий ограничена величиной $\log d$. Нижние границы подобного типа в теории квантовых измерений называются *неравенствами энтропийной неопределённости* (EUI), которые количественно определяют невозможность одновременного извлечения вектора $|\phi\rangle$ из двух обобщённых (совместных) базисов.

Из приведенных соотношений следует, что $I_{Cl}\ \rho\ \leq \frac{1}{2} \log d$. Равенство можно достигнуть, если B измеряется в вычислительном базисе

$$I_{Cl}\ \rho\ = \frac{1}{2} \log d\ , \quad I_{Cl}^{\ l}\ \rho\ - I_{Cl}\ \rho\ = 1 + \frac{1}{2} \log d\ .$$

Отметим, что свойство приращения пропорциональности выполняется для многократных копий состояния ρ. Wootters показал, что доступная информация из m независимых копий ансамбля E разделённых состояний аддитивна, $I_{Acc}\ \mathrm{E}^{\otimes m}\ = m I_{Acc}\ \mathrm{E}\ $. Отсюда следует, что для рассматриваемого случая имеем: $I_{Cl}\ \rho^{\otimes m}\ = m I_{Cl}\ \rho\ $.

Пример 7. Пусть задано двухчастичное состояние ρ_{AB}. Определим возможную меру классической корреляции между подсистемами A и B как:

$$Cor_B\ \rho_{AB}\ = \max_B \left[S\ \rho_A\ - \sum_i p_i S\ \rho_A^i\ \right], \tag{13}$$

где $\rho_A = Tr_B\ \rho_{AB}\ $ – редуцированная матрица плотности. Энтропия фон Неймана $S\ \rho\ = -Tr\ \rho \log \rho\ $. Условная матрица плотности ρ_A^i определяется через матрицы плотности состояния A после реализации измерения B_i над состоянием B в виде:

$$\rho_A^i = \frac{Tr_B\ B_i \rho_{AB}}{Tr_{AB}\ B_i \rho_{AB}} .$$

Вероятность определить A в состоянии ρ_A^i есть $p_i = Tr_{AB}\ B_i \rho_{AB}\ $. Мера корреляции (13) имеет простую физическую интерпретацию: если A и B не коррелированны, то маргинальное значение энтропии $\left[S\ \rho_A\ \right]$состояния A и взвешенное усреднённое значение энтропии A после ПООЗ-измерения $\left[\sum_i p_i S\ \rho_A^i\ \right]$ над состоянием B дает как следствие $Cor_B\ \rho_{AB}\ = 0$, так как для некоррелированной системы AB состояние A не зависит от действия ПООЗ- измерения над состоянием B. Более того, отметим, что имеет место соотношение $\rho_A = \sum_i p_i \rho_A^i$; тогда для данного ПООЗ-измерения над системой B выражение $\left[S\ \rho_A\ - \sum_i p_i S\ \rho_A^i\ \right]$ задает дефект энтропии. Следовательно, классическую корреляцию $Cor_B\ \rho_{AB}$ можно рассматривать как максимальное осреднённое возрастание энтропии системы A, когда состояние ρ_A^i (после завершения измерения B_i

над системой B) является специфически сравнимым с ситуацией, в которой известны только смешанные состояния ρ_A.

Классическая корреляция устанавливает меру силы корреляции двух подсистем без указания приоритета подсистемы, используемой для извлечения данной корреляции. Количество квантовой взаимной информации $I\ A:B$ двухчастичной составной системы AB можно декомпозировать на дефицит информации (или работы) Δ и дефицит классической информации Δ_{cl} в виде $I = \Delta_{cl} + \Delta$. Это приводит к естественной аналогии с процессом декомпозиции для случая количества взаимной информации, используемой при описании различных мер классической корреляции. Количество оцененной классической корреляции и относительной энтропии E_{REn} в запутанных состояниях также не превышает в сумме количества взаимной информации фон Неймана между двумя подсистемами, т.е. $I\ \rho_{A:B} > \left[C_B\ \rho_{AB} \right]_{opt} + E_{REn}$.

Физически это означает, что выбор неоптимального ПООЗ-измерения может разрушить полную корреляцию. Естественно, что при рассмотрении всех возможных ПООЗ-измерений для данного состояния оптимальный класс ПООЗ-измерений не может устранить полную корреляцию. Другой альтернативой, которая делает совместимыми понятия классической корреляции и взаимной информации, является возможность различных определений мер квантовых корреляций, отличных от представления последних в виде E_{REn} .

Одним из возможных кандидатов служит квантовый беспорядок.

Пример 8: *Взаимная информация и квантовый беспорядок*. В противоположность к определению классической условной энтропии квантовая условная энтропия является зависимой величиной от процедуры измерения, проводимой над исследуемой системой.

Мерой квантового беспорядка выступает: $\delta\ A:B\ = I\ A:B\ - J\ A:B\ _{\Pi_i^B}$.

Величина J задает информацию о системе B по результатам серии измерений Π_i^B

$$J\ A:B\ _{\Pi_i^B} = S\ A\ - S\ A\left|\ \Pi_i^B\right. = S\ A\ - \sum {}^{*}p_i S\ {}^{*}\rho_i^A\ ,$$

где ${}^{*}p_i$ и ${}^{*}\rho_i^A$ изначально выбраны как специальные случаи p_i и ρ_i^A, когда множества измерений формируются как ограниченные одномерные проекции Π_i^B.

Приведенное определение квантового беспорядка четко описывает неразделимую зависимость квантовой условной энтропии от процедуры измерения[3]. Мера квантового беспорядка равна нулю, если существует такое (хотя бы одно) измерение, для которого эта мера принимает нулевое значение. Поэтому минимальному значению меры квантового беспорядка сопоставляют квантовую корреляцию. При выборе соответствующего множества измерений над системой B, определённого как множество одномерных проекций, нетрудно проверить, что множество измерений, при которых минимизируется квантовый беспорядок, т.е. максимизируется величина J, эквивалентно ПООЗ - измерениям, оптимизирующим меру классических корреляций бинарных состояний. Данный результат следует из определения этих количественных мер и результата оптимизации классических корреляций при использовании только проективных измерений. Следовательно, имеем $\max\left[J\ A:B\ _{\Pi_i^B} \right] = Cor_B\ \rho_{AB}$. Поэтому, $I\ A:B\ = Cor_B + \min_{\Pi_i^B} \delta\ A:B$, т.е. для бинарных состояний классическая корреляция и квантовый беспорядок выступают составными компонентами в оценке взаимной информации. Поэтому не существует измерения, извлекающего классическую корреляцию и способного изменить значение взаимной информации между двумя подсистемами при добавлении классической корреляции к относительной энтропии. Это подтверждает утверждение, что удобнее

[3] Hosseini S., Rahimi-Keshari S., Haw J.Y. et all. Experimental verification of quantum discord in Continuous-variable states // arXiv:1310.6796v1 [quant-ph]. – 25 Oct 2013.

использовать понятие квантового беспорядка в качестве квантовой составной части для классической корреляции вместо относительной энтропии.

Моделирование квантовых алгоритмических ячеек и квантовое программирование

В настоящее время разработка теории и практики «квантовой информатики» в целом интенсивно развивается по всем направлениям, включая создание языков и систем квантового программирования. В настоящей статье приведены лишь примеры первоначальных сведений о средствах, применяемых в этой последней области. Для серьезного овладения квантовым программированием читатель может обратиться к библиографическим ссылкам [28-34] и мн. др.

Основу метода проектирования квантовых алгоритмических схем и ему подобных методов формирования новых типов КА составляет система проектирования квантовых алгоритмических ячеек (КАЯ). Как и в общей структуре КА, структура системы проектирования КАЯ основана на формализации описания трёх основных квантовых операторов (суперпозиции, квантовой корреляции (запутанных состояний) и интерференции) и измерения в виде элементарных эволюционных унитарных операторов.

В соответствии с квантовой схемой КА данные операторы собраны тензорным и прямым произведением в единый эволюционный квантовый унитарный оператор.

Система моделирования квантовых вычислений и КА реализуется на классических компьютерах с применением КАЯ. Процесс проектирования КАЯ в матричной форме заключается в проектировании трех квантовых операторов: суперпозиции (*Sup*), квантовой корреляции (запутанных состояний – entanglement U_F), и интерференции (*Int*) и составляют основу структур КА. В общем виде структура КАЯ может быть представлена в виде:

$$\text{КАЯ} = \left[\; Int \otimes {}^{n} I \; \cdot U_F \right]^{h+1} \cdot \left[{}^{n}H \otimes {}^{m} S \right], \qquad (14)$$

где I – оператор идентичности; $\otimes$ – символ тензорного произведения; S равен I или матрице Адамара и выбор зависит от описания исследуемых свойств функции.

Одной из особенностей процесса проектирования (1) является выбор типа оператора U_F, физически описывающего тип квантовой корреляции и закодированные в суперпозиции качественные свойства исследуемой функции f.

Работа квантовых операторов осуществляется в итеративном режиме в зависимости от типа КА. При этом для общего случая предполагается, что определённые вычислительные проблемы могут быть решены на квантовом компьютере более эффективно (с меньшей вычислительной сложностью, так называемая *NP* – проблема), чем на классическом компьютере. Более того, с помощью эффективного применения квантового компьютера достигаются решения алгоритмически неразрешимых (на классическом уровне) проблем.

Таким образом, существуют эффективно решаемые с помощью применения КА задачи, для которых не существует ни одного успешного классического (рандомизированного) алгоритма.

Эти наблюдения свидетельствуют о том, что КА составляют физически обоснованный базис не только техники ускорения вычислений, но и поиска решений сложных проблем, используя такие квантовые законы, как суперпозиция (для расширения пространства возможных решений), квантовый параллелизм процессов вычислений (в интересах ускорения поиска решений) и квантовая интерференция (с целью извлечения искомого решения).

Структурно КАЯ действует на начальный канонический базисный вектор и формирует комплексную линейную комбинацию состояний составляющих классических векторов (называемую суперпозицией) в виде базисных векторов как выходной результат действия оператора суперпозиции. Суперпозиция содержит в качестве одной из составляющих информацию о решении исследуемой проблемы. После процесса формирования суперпозиции в КАЯ применяются операторы квантовой корреляции, интерференции и измерения с целью извлечения информации об искомом решении. В квантовой механике процесс измерения носит необратимый характер и является

недетерминированной операцией, что приводит к измерению только одного из базисных векторов в сформированной суперпозиции. Вероятность каждого базисного вектора быть результатом измерения в составе суперпозиции при заданном вычислительном базисе зависит от комплексного коэффициента (амплитуды вероятности).

Процесс останова итерационного действия КАЯ осуществляется программным путем на основе принципа минимума информационной энтропии «интеллектуального квантового состояния», содержащего ценную информацию об искомом решении. КАЯ могут быть реализованы с помощью программно-аппаратной поддержки эволюционных квантовых вычислений.

Квантовое программирование

В квантовом программировании существует доказательство полноты описания КАЯ с помощью соответствующих программных языков повышенной семантической выразительности. По аналогии с существованием эквивалентности в теории вычислений, которая основана на классических алгоритмах, известна гипотеза об эквивалентности между представлением выражений квантовых операций на синтаксическом уровне с сохранением полноты их описания за счет включения в квантовые языки программирования семантической выразительности квантовых операторов (на функциональном уровне описания действий квантовых операторов).

Одним из естественных шагов в этом направлении является разработка принципов логического вывода и проверки истинности суждений в языках квантового программирования для устранения противоречий в получаемом следствии логического вывода. К таким языкам квантового программирования следует отнести, например язык QPL (Quantum Programming Language) и др.

Рассмотрим, как осуществляется в языке QPL непротиворечивое описание, например, определения действия оператора Адамара в следующем виде:

$$H\,x = \text{if } x \text{ then } \quad false + \ -1 \ * true \quad \text{else} \quad false + true \ .$$

Оценим полноту и истинность данного выражения, которое эквивалентно проверке истинности того, что последовательное действие операторов Адамара $H\ H\,x$ на функциональном уровне описания приводит к результату, эквивалентному x.

Для этого используем следующую модель логического вывода языка QPL:

$$\begin{aligned}
H\ \ H\,x \ = \ & \text{if} \quad \text{if } x \text{ then} \quad false + \ -1 \ * true \quad \text{else} \quad false + true \\
& \quad \text{then} \quad false + \ -1 \ * true \\
& \quad \text{else} \quad false + true \\
& \quad -- \text{ by commuting conversion for "if"} \\
& = \ \text{if } x \\
& \quad \text{then if } \left(false + \left(-1 \right) * true \right) \\
& \qquad \text{then } \left(false + \left(-1 \right) * true \right) \\
& \qquad \text{else } \left(false + true \right) \\
& \quad \text{else if } \left(false + true \right) \\
& \qquad \text{then } \left(false + \left(-1 \right) * true \right) \\
& \qquad \text{else } \left(false + true \right) \\
-- \ & \text{ by "if"}
\end{aligned}$$

$$
\begin{aligned}
&= \text{if } x \\
&\quad \text{then} \quad false - false + true + true \\
&\quad \text{else} \quad false + false + true - true \\
&\quad -- \text{ by simplification and normalisation} \\
&= \text{if } x \text{ then } true \text{ else } false \\
&\quad -- \text{ by } \eta\text{-rule for "if"} \\
&= x
\end{aligned}
$$

Элементы теории проверки полноты и истинности семантики функционального описания КА на языке функционального квантового программирования QPL описаны ниже.

– *Квантовые языки программирования.* При проектировании языка программирования одна из целей состоит в том, чтобы идентифицировать и проработать полезные понятия "высокого уровня" — абстракции или парадигмы, которые позволяют решать проблему концептуальным способом, вместо сосредоточения на деталях его выполнения. Исследование квантовых языков программирования обеспечивает урегулирование, в котором можно исследовать возможные языковые особенности и проверять их полноту и экспрессивность. Кроме того, определение прототипа языков программирования создает объединяющую формальную структуру, для рассмотрения и анализа существующего квантового алгоритма.

– *Модели виртуальных машин.* Развитие языков программирования часто вызывается наряду с другими причинами развитием методов проектирования компиляторов. В случае квантовых вычислений ситуация усложняется отсутствием (в настоящее время) пригодной к использованию квантовой вычислительной аппаратуры. Чтобы иметь возможность говорит о «реализации», необходимо определить некоторую «виртуальную» модель вычислительной машины и работать с ней. При этом следует понимать, что будущая реальная квантовая машина, возможно, будет существенно отличаться от этой виртуальной модели, но эти отличия в идеальном случае должны быть прозрачными для программиста и обрабатываться автоматически компилятором или операционной системой. Существуют несколько возможных моделей виртуальных машин, но все они эквивалентны, по крайней мере, теоретически.

Таким образом, можно подобрать модель, которая наилучшим образом соответствует вычислительной интуиции. По-видимому, наиболее популярной и понятной виртуальной моделью машины является модель квантовой цепи.

Квантовая цепь строится из квантовых ячеек точно таким же образом, как классическая логическая цепь – из логических ячеек. Отличие состоит в том, что квантовые ячейки всегда обратимы и соответствуют унитарным преобразованиям в пространстве комплексных векторов. Модель квантовой схеме в основном рассматривает унитарные преобразования как основные базовые операции. Другой базовой операцией является измерение, которое выполняется как последний шаг в процессе вычисления.

Другая модель виртуальной машины, возможно даже более подходящая для интерпретации квантовых языков программирования, – *модель QRAM, предложенная Knill.* В этой модели допускается свободное перемешивание унитарных преобразований и измерений. Квантовым устройством управляет универсальный классический компьютер. Это квантовое устройство содержит большое, но конечное число индивидуально адресуемых кубитов точно такое, как в классическом чипе памяти содержится конечное множество классических битов. Классический контроллер посылает последовательность инструкций («команд»), каждая из которых имеет вид «применить унитарное преобразование U к кубитам i и j» или «измерить кубит j». Квантовое устройство выполняет эти инструкции и выдает в качестве ответа результаты доступных измерений.

Иногда в работах по теории сложности используется третья модель виртуальной машины – квантовая машина Тьюринга. В этой модели измерение не производится, а все операции предполагаются унитарными. Машина сдержит ленту, головку и конечный набор управляющих правил перехода, аналогично классическому варианту. Хотя теоретически эта модель эквивалентна двум предыдущим, в общем случае она не рассматривается как достаточно реалистическое приближение для возможных будущих квантовых компьютеров.

– *Императивные квантовые языки программирования.* Ранее предложенные квантовые языки программирования следовали за императивной программной парадигмой. Эта линия языков была начата Knill, который определил ряд соглашений для выражения квантовых алгоритмов в псевдокоде. Несмотря на то, что предложение Knill было не очень формально, оно оказало большое влияние при проектировании более поздних императивных квантовых языков программирования. Более полные императивные языки были определены Omer, Sanders и Zuliani, Bettelli и мн. др.

Общая черта этих императивных квантовых языков программирования заключается в том, что программа рассматривается как последовательность операций, которые работают, обновляя некоторое глобальное состояние. Эти языки могут быть непосредственно скомпилированы или интерпретироваться в реальную модель аппаратных средств QRAM. Квантовые состояния в этой парадигме, как правило, реализованы как массивы кубитов, и во время выполнения необходимы средства обнаружения ошибочных условий. Кроме того, обычно эти языки не имеют формальной семантики, за исключением языка Sanders и Zuliani, который обладает операционной семантикой.

Различные языки в этой категории предлагают множество программных особенностей. Например, QCL содержит такие функции, как, автоматическое управление рабочей памятью, и богатый язык для описания пользовательских операторов. Предложено несколько операций более высокого порядка, таких как вычисление инверсии определенного пользователем оператора. Язык Bettelli и мн. др. уделяют особое внимание практичности применения. Языки задуманы, как расширение C++, и рассматриваются как квантовые операторы объектов первого порядка, которые могут быть явно построены и управляться во время выполнения. Одна из самых серьезных особенностей этого языка - непрерывная оптимизация квантовых операторов, которая производится во времени выполнении.

– *Функциональные квантовые языки программирования.* В функциональном программировании, программы работают не на обновлении глобального состояния, а на отображении конкретных входов на выходы. Типы данных, связанные с чисто функциональными языками, (такие как списки, рекурсивные типы), более поддаются анализу во время компиляции, чем их императивные аналоги (такие как массивы). Следовательно, даже в очень простых функциональных языках программирования можно избежать многих проверок во время исполнения.

В первом предложении варианта функционального квантового языка программирования введен язык QFC, который представляет программы через функциональную версию блок - схем. У языка также есть альтернативный синтаксис, основанный на текстовом представлении. И унитарные операции и измерения непосредственно встроены в язык, и обрабатываются с сохранением типов. Классические и квантовые особенности интегрированы в рамках одного формализма. Отсутствует контроль соответствия типов во время выполнения или обработки ошибок. Язык может быть откомпилирован на модель QRAM, а также обладает полной денотационной семантикой, которая может использоваться для формальных рассуждений о программах.

Основной квантовый язык блок-схем функционален, поскольку свободен от побочных эффектов. Однако, функции сами по себе не рассматриваются как данные, и, таким образом язык теряет черты более высокого порядка.

Таблица 2. Классификация языков программирования

Тип языка	**QCL**	**Q language**	**qGCL**	**(Block-)QPL**
императивный язык	+	+	+	
функциональный язык				+
прагматический подход	+	+		
теоретический подход			+	+
формальная семантика			+	+
универсальный язык	+	+	+	+

Пример. Рассмотрим некоторые свойства языков квантового программирования.

QCL (Quantum Computation Language)

Общие свойства

- фактически первый квантовый язык программирования
- (элементарный) процедурный язык
- автоматическое управление рабочим пространством
- синтаксическая обратимость определяемых пользователем квантовых операций
- синтаксис как в C / Паскаль
- универсальный язык: может осуществить и моделировать все известные квантовые алгоритмы
- отсутствует формальная семантика
- нетривиальные унитарные операции – функции (функциональный синтаксис запроса).

Далее приведен пример «*Вычисление факториала*» на языке QCL с помощью классического программирования:

```
// program example: recursive
// and non-recursive function call:

int factorialR(int x) {
      // recursive implementation
      // precondition x >= 0
      if x == 0 {
        return 1;
      }
      return
        x*factorialR(x-1);
}

int x = 5;
print x, "! = ", factorialR(x);

//---------------------------------
int factorialNR(int x) {
      // iterative implementation
      // precondition  x >= 0
      int k;
      int y = x;
      if (y == 0) or (y == 1) {
        return 1;
      }
      else { // "else" for better readability
        // here: y >= 2
        k = y;
        while y >= 3 {
              y = y - 1;
              k = k*y;
        }
        return k;
      }
}

x = 7;
print x, "! = ", factorialNR(x);
```

```
print "The End.";

/* result:
: 5 ! = 120
: 7 ! = 5040
: The End.
*/
```

Квантовые операторы и их действие

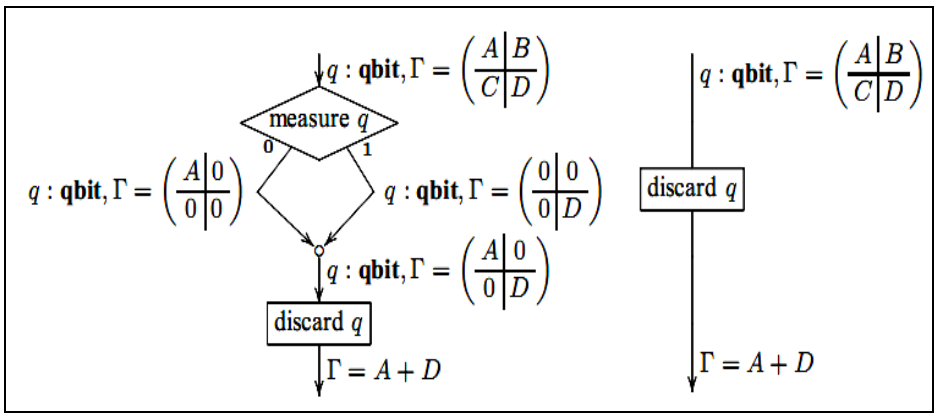
1. Оператор тождественности *Qopmy_op*
2. Встроенные квантовые операторы *Qopmy_op = QHadamard (7)*
3. Квантовые операторы Qopmyop = QFourier (7)
4. Переупорядочение строки *Qubit, Qopa_swap = QSwap (5)*
5. Операторы управления Qopa_controlled_op (U, 5)
6. Операторы для классических функций *Qopan_oracle = Qop (f, 3, 5)*
7. Оформление структуры оператора *Qopcomposed = part_1 &part_2*
8. Оператор связи Qopadj_operator =! an_op
9. Оператор перестановки Qopsplit = an_op(2, 3, SPLIT)
10. Применение оператора an_operator (a_register)

qGCL (Quantum Guarded Command Language)

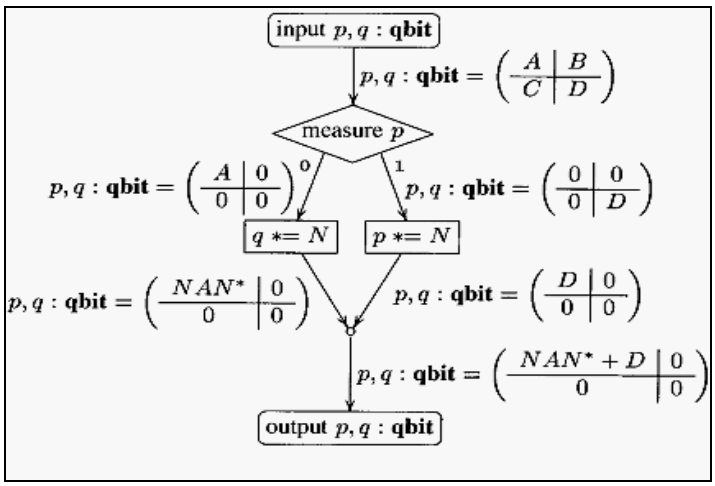
Общие свойства

- qGCL: выражается через pGCL (вероятностный командный язык)
- qGCL: императивный язык
- подходит в качестве языка спецификаций (высокий уровень математической нотации)
- механизм пошагового уточнения программы для вывода и проверки (доказательство корректности)
- формальная семантика: пред – и пост-условия распространяются на пред- и пост-ожидания
- включает в себя три квантовых примитива на высоком уровне: состояние подготовки, эволюции, наблюдения
- универсальный язык.

– *Блок-схема QPL* (Квантовая блок-схема). Квантовая блок-схема практически не отличается от классической, только в квантовой блок-схеме добавляется новый тип переменной, названный qbit, а также возникают новые операции: унитарные преобразования и измерения (см. рис. 1 а,б).



(а)



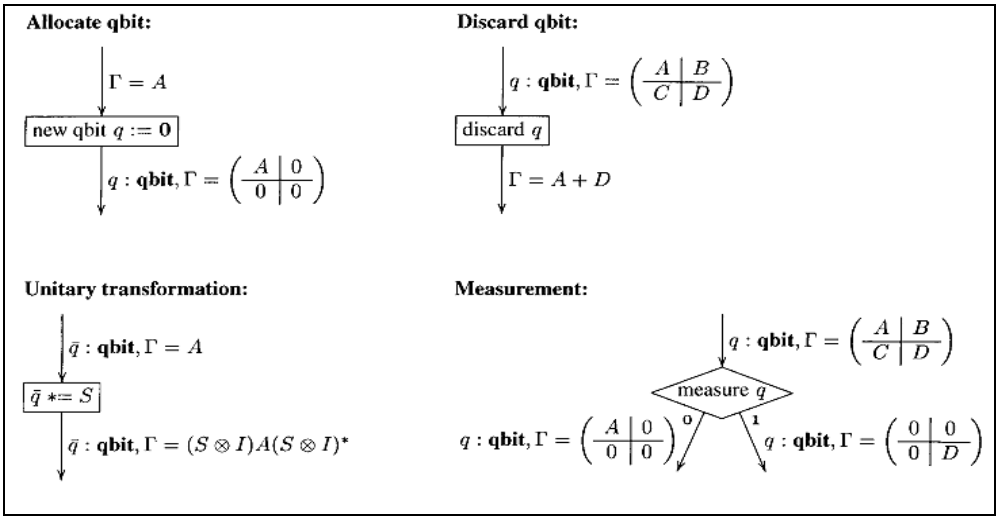
(б)

Рис. 1. Квантовая блок-схема

– Правила для квантовых блок-схем

При составлении квантовых блок-схем используются некоторые правила, представленные на рис. 2:

- выделение бита (Allocatebit),
- отменить бит (Discardbit),
- унитарное преобразование (Unitary transformation),
- слияние (Merge),
- перестановка (Permutation),
- измерение (Measurement),
- перестановка (Permutation).



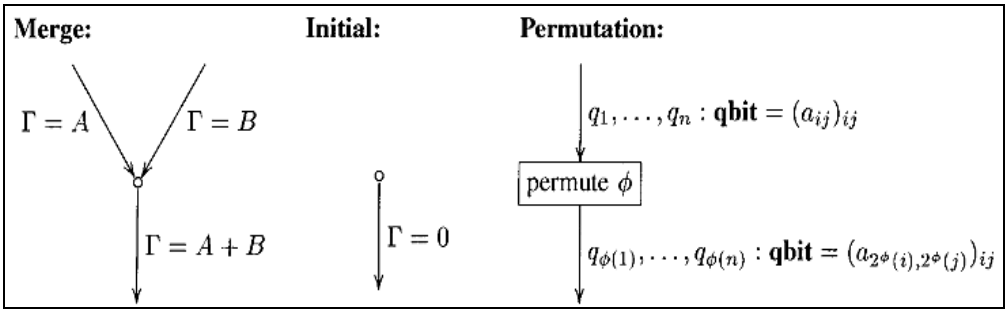
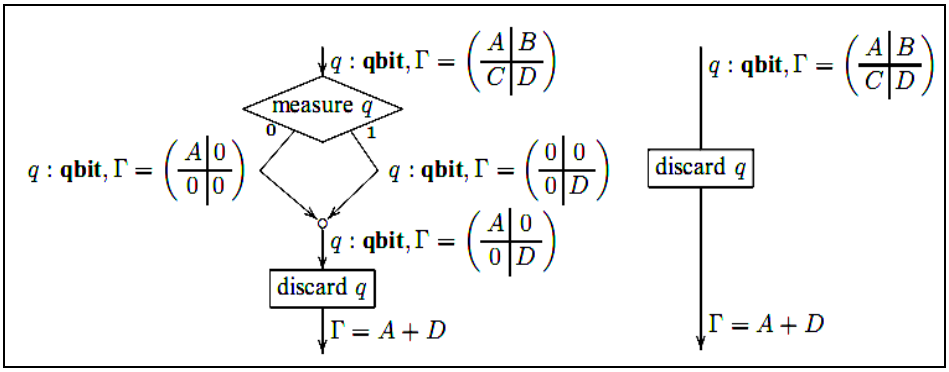


Рис. 2. Правила преобразований в квантовых блок-схемах

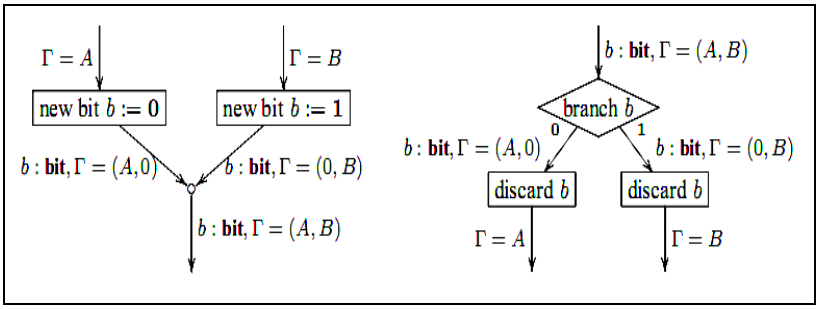
– Примеры

Первый пример показывает правильность преобразования программы: измерение, сопровождаемое перемещением.

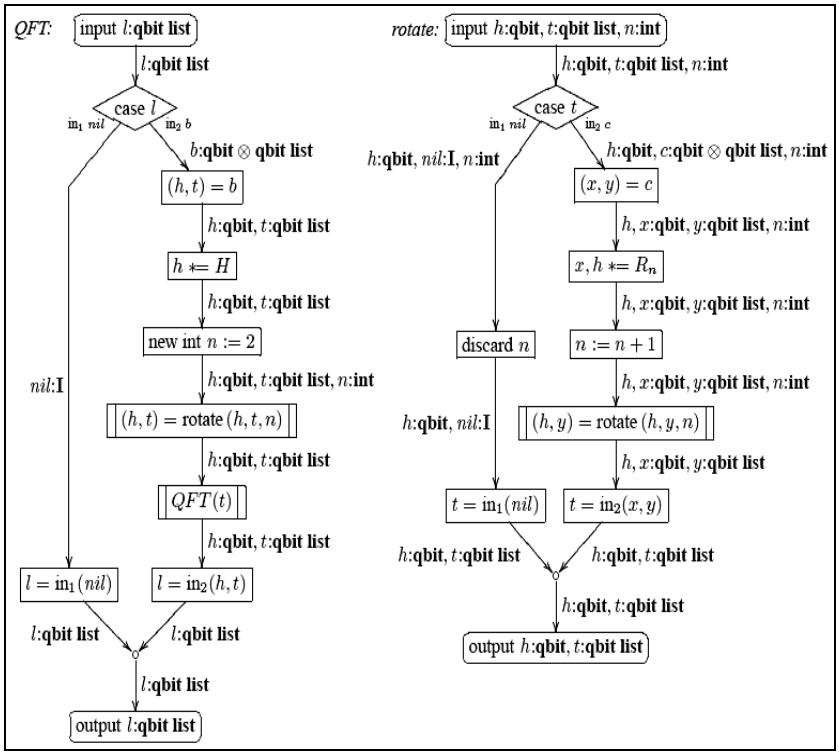


Правильность этого преобразования в программе состоит в том, что операция «отбрасывания» уже встраивает неявное измерение в программу.

Во втором примере следующие две схемы являются взаимно обратными:



В третьем примере представлена схема квантового преобразования Фурье:



Пример 9: *Квантовое лямбда-исчисление*. Рассмотрим основные определения и понятия данного вида квантового программирования (см. Приложение).

– *Термы*. Язык использует обозначения интуиционистского лямбда-исчисления[4]. Рассматриваются обозначения стандартного лямбда-исчисления с булевыми и конечными переменными. Расширение стандартного языка осуществляется за счет введения трех специальных квантовых операций типа *new, meas,* built-in unitary gates (встраиваемые унитарные ячейки). Операция *new* отображает классический бит в квантовый бит; *meas* отображает квантовый бит в классический бит посредством операции измерения и является вероятностной операцией. Предполагается, что существует множество U^n встраиваемых (built-in) унитарных ячеек для каждого n. Через U обозначим область всех множеств U^n. Тогда синтаксис языка можно представить в виде:

$$Term \quad M,N,P \ ::= \ x \left| MN \right| \lambda x.M \left| if \ M \ then \ N \ else \ P \right| 0 \left| 1 \right| meas$$
$$\left| new \right| U \left| * \right| \left\langle M,N \right\rangle \left| let \left\langle x,y \right\rangle = M \ in \ N. \right.$$

Термы идентифицируются с точностью до α – эквивалентности и используется упрощенная запись типа $\langle M_1,\ldots,M_n\rangle = \langle M_1,\langle M_2,\ldots\rangle\rangle$.

– *Программы*. Введение в язык синтаксиса постоянных квантовых состояний, таких как $\alpha|0\rangle + \beta|1\rangle$ в виде лямбда терма типа $\lambda x.\ \alpha|0\rangle + \beta|1\rangle$ в общем случае не эффективно. Рассмотрим, например, лямбда терм $\lambda y.\lambda f.fpy \quad q$, где p и q запутанные квантовые биты в состоянии $|pq\rangle = \alpha|00\rangle + \beta|11\rangle$. Такое состояние невозможно представить локально в виде произведения отдельных множителей p и q с постоянными множителями. Нелокальная природа квантовых состояний требует уровня косвенного введения представления состояния квантовых программ.

Определение 1. *Состояние программы* представляется триплетом Q,L,M, где

Q – нормализованный вектор $\otimes_{i=0}^{n-1}\mathrm{C}^2$ для некоторого $n \geq 0$;
M – лямбда терм;
L – функция отображения из W в $0,\ldots,n-1$, где $FV\ M \subseteq W \subseteq \mathrm{V}_{\mathrm{term}}$.

L называют также связывающей функцией или кубит события. Назначением данной функции является установление соответствия между свободными переменными в M с соответствующими кубитами в Q. Введение условия α-эквивалентности распространяется естественным образом на программы, например, состояния $\left[|1\rangle,\ x \mapsto 0\ ,\lambda y.x\right]$ и $\left[|1\rangle,\ z \mapsto 0\ ,\lambda y.x\right]$ эквивалентны. Множество состояний α-эквивалентных программ обозначается через S.

В дальнейшем, с целью упрощения обозначений, через p_i будем обозначать свободную переменную x так что выполняется соотношение $L\ x = i$. Программа Q,L,M обозначается как Q,M' и $M' = M\left[p_{i_n}/x_1\right]\ldots\left[p_{i_n}/x_n\right]$ где $i_k = L\ x_k$.

– *Операционная семантика*. Определим вероятностные процедуры редукции значений вызываемых переменных для квантового лямбда исчисления. Отметим, сама процедура также носит вероятностный характер, а выбор значений на каждом шаге редукции носит детерминированный характер.

Определение: *Значение* (*value*) является термом следующей формы:

$$Value \quad V,M \ ::= \ x \left| \lambda x.M \right| 0 \left| 1 \right| meas \left| new \right| U \left| * \right| \left\langle V,M \right\rangle .$$

Множество *состояний значений* обозначается как $\mathrm{V} = \ Q,V,L \ \in \mathrm{S} \left| V \in Value \right.$.

[4]Atzemoglou G.Ph. Higher-order semantics for quantum programming languages with classical control // arXiv:1311.6563v1 [cs.LO]. – 26 Nov 2013.

Правила редукции перечислены в Табл. 3, где использованы принятые ранее соглашения об обозначениях.

Таблица 3. Правила редукции квантового лямбда исчисления

$$[Q,(\lambda x.M)V] \longrightarrow_1 [Q,M[V/x]]$$

$$\frac{[Q,N] \longrightarrow_p [Q',N']}{[Q,MN] \longrightarrow_p [Q',MN']}$$

$$\frac{[Q,M] \longrightarrow_p [Q',M']}{[Q,MV] \longrightarrow_p [Q',M'V]}$$

$$\frac{[Q,M_1] \longrightarrow_p [Q',M_1']}{[Q,\langle M_1,M_2\rangle] \longrightarrow_p [Q',\langle M_1',M_2\rangle]}$$

$$\frac{[Q,M_2] \longrightarrow_p [Q',M_2']}{[Q,\langle V_1,M_2\rangle] \longrightarrow_p [Q',\langle V_1,M_2'\rangle]}$$

$$[Q,\mathit{if}\ 0\ \mathit{then}\ M\ \mathit{else}\ N] \longrightarrow_1 [Q,N]$$

$$[Q,\mathit{if}\ 1\ \mathit{then}\ M\ \mathit{else}\ N] \longrightarrow_1 [Q,M]$$

$$[Q,U\langle p_{j_1},\ldots,p_{j_n}\rangle] \longrightarrow_1 [Q',\langle p_{j_1},\ldots,p_{j_n}\rangle]$$

$$[\alpha|Q_0\rangle+\beta|Q_1\rangle,\mathit{meas}\ p_i] \longrightarrow_{|\alpha|^2} [|Q_0\rangle,0]$$

$$[\alpha|Q_0\rangle+\beta|Q_1\rangle,\mathit{meas}\ p_i] \longrightarrow_{|\beta|^2} [|Q_1\rangle,1]$$

$$[Q,\mathit{new}\ 0] \longrightarrow_1 [Q\otimes|0\rangle,p_n]$$

$$[Q,\mathit{new}\ 1] \longrightarrow_1 [Q\otimes|1\rangle,p_n]$$

$$\frac{[Q,P] \longrightarrow_p [Q',P']}{[Q,\mathit{if}\ P\ \mathit{then}\ M\ \mathit{else}\ N] \longrightarrow_p [Q',\mathit{if}\ P'\ \mathit{then}\ M\ \mathit{else}\ N]}$$

$$\frac{[Q,M] \longrightarrow_p [Q',M']}{[Q,\text{let}\ \langle x_1,x_2\rangle = M\ \text{in}\ N] \longrightarrow_p [Q',\text{let}\ \langle x_1,x_2\rangle = M'\ \text{in}\ N]}$$

$$[Q,\text{let}\ \langle x_1,x_2\rangle = \langle V_1,V_2\rangle\ \text{in}\ N] \longrightarrow_1 [Q,N[V_1/x_1,V_2/x_2]]$$

Конечное отношение определяется как $\rightharpoonup$, которое моделирует преобразования в присутствии декогеренции или неточности физических операций. Тогда $Q,M \rightharpoonup Q',M'$ определяет $Q,M \to_p Q',M'$ даже когда $p=0$, плюс дополнительная операция, если Q и Q' являются векторами одинаковой размерности: $Q,M \rightharpoonup Q',M$.

Пример 10: *Эксперимент* Белла. Два квантовых бита *A* и *B* образуют максимальное запутанное состояние $|\phi_{AB}\rangle = \frac{1}{\sqrt{2}}|0\rangle\otimes|1\rangle - |1\rangle\otimes|0\rangle$. Эти кубиты посылаются Алисе и Бобу, соответственно. Допустим, что Алиса и Боб могут независимо друг от друга выбрать один из трех базисов a,b,c для измерения своего кубита:

$$|0_a\rangle = |0\rangle,\quad |0_b\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle,\quad |0_c\rangle = \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle,$$

$$|0_a\rangle = |0\rangle,\quad |0_b\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle,\quad |0_c\rangle = \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle,$$

$$|1_a\rangle = |1\rangle,\quad |1_b\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle,\quad |1_c\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$$

Требуется вычислить вероятность получения одинакового выходного результата в случае измерения *A* и *B* относительно каждого из девяти возможных выборов пары базисов.

Можно интерпретировать данный эксперимент в контексте квантовых вычислений высокого уровня. Во-первых, приготовление состояния может рассматриваться как отображение EPR: $\bullet \to qbit \otimes qbit$. Тогда Алиса и Боб принимают свой кубит, выбирают базис, и проводит измерение: осуществляется применением функции $f : qbit \otimes trit \to bit$, где элемент $trit = 0,1,2$ является классическим триплетом. Тогда данную функцию можно представить в виде $f : qbit \to trit \to bit$.

Эксперимент Белла можно рассматривать как композицию:

$$\bullet \xrightarrow{\text{EPR}} qbit \otimes qbit \xrightarrow{f'\otimes f'} trit \to bit \ \otimes \ trit \to bit \ ,$$

которая воспроизводит терм типа $trit \to bit \otimes trit \to bit$, т.е., пару $\langle f, g \rangle$ функций запутанных состояний. Данный тип результата является по своей физической природе чисто классическим; неравенство Белла доказывает, что не существует классической вероятностной пары функций, проявляющих подобное поведение, т.е. таких что $f\ x = g\ x$ с вероятностью 1 при $x = y$, но с вероятностью ¼ при $x \neq y$.

Рассмотрим возможность применения квантовой логики для анализа квантовых программ.

Квантовая логика для анализа квантовых программ. Формализм представления подпространств в терминах языка пропозиционального исчисления включает два элемента: язык (т.е., пропозициональные термы) L и функцию интерпретации $\cdot$, которая отображает каждый терм языка в замкнутое подпространство гильбертова H. В этом случае, каждый терм $p \in \mathrm{L}$ ассоциируется с замкнутым подпространством H, обозначаемое как p . Язык L содержит две связки: отрицание $\neg$ и конъюнкцию $\wedge$, а также множество констант Ψ. Таким образом, каждая константа $p \in \Psi$ является термом (т.е., $p \in \mathrm{L}$) и задаются два терма $p, q \in \mathrm{L}$ и оба $\neg p$ и $p \wedge q$ являются также термами.

Определение функции интерпретации основано на структуре термов и соответствии между отрицанием $\neg$ и ортодополнением $\perp$ с одной стороны, и между конъюнкцией и пересечением $\bigcap$ с другой стороны. Тогда определение $\cdot$ можно задать как:

$$\forall p \in \mathrm{L}, \quad \neg p \ = \ p^{\perp}, \quad \forall p, q \in \mathrm{L}, \quad p \wedge q \ = \ p \ \bigcap \ q \ . \tag{15}$$

Определение (15) полно при интерпретации каждого атомарного высказывания. Рассмотрим частный случай, когда пространство Гильберта H имеет вид $\otimes^n \mathrm{C}^2$ и имеем атомарные высказывания z_i и x_i $1 \le i \le n$. На интуитивном уровне высказываниям можно сопоставить соответствующее направление i-го кубита. Если $n = 1$, то интерпретации можно определить с помощью выражения $z = \mathrm{C}|1\rangle \ x = \mathrm{C}|-\rangle = \mathrm{C}\ |0\rangle - |1\rangle$, и для $n > 1$ данное определение расширяется до применения тензорных произведений. Например,

$$x_i \ = \ \otimes^{i-1}\mathrm{C}^2 \ \otimes \mathrm{C}|-\rangle \otimes \ \otimes^{n-1}\mathrm{C}^2 \ . \tag{16}$$

Тогда к двум константам применимо обычные определения: истинность высказывания T проверяется непосредственно (их интерпретация T эквивалентна полному пространству Гильберта H) и абсурдное высказывание $\perp$, истинность которого невозможно проверить так, что $\perp \ = \ 0$.

Пример 11: *Описание* ЭПР *пары*. Данное логическое состояние содержит описание многих интересных состояний квантовой системы. Для иллюстрации данного свойства рассмотрим высказывание $z_1 \leftrightarrow z_2 \ \wedge \ x_1 \leftrightarrow x_2$, которое полностью описывает ЭПР пару:

$$z_1 \leftrightarrow z_2 \ = \ z_1 \leftrightarrow z_2 \ \wedge \ z_2 \leftrightarrow z_1 \ = \ z_1^{\perp} \oplus \ z_2 \ \bigcap \ z_1 \ \oplus \ z_2^{\perp} \ =$$

$$= \ \mathrm{C}|00\rangle \oplus \mathrm{C}|10\rangle \oplus \mathrm{C}|11\rangle \ \oplus \ \mathrm{C}|00\rangle \oplus \mathrm{C}|01\rangle \oplus \mathrm{C}|11\rangle \ = \mathrm{C}|00\rangle + \mathrm{C}|11\rangle.$$

$$x_1 \leftrightarrow x_2 \ = \mathrm{C}|++\rangle \oplus \mathrm{C}|--\rangle,$$

$$\left(z_1 \leftrightarrow z_2 \ \wedge \ x_1 \leftrightarrow x_2 \right) = \ z_1 \leftrightarrow z_2 \ \bigcap \ x_1 \leftrightarrow x_2 \ = \ \mathrm{C}|00\rangle \oplus \mathrm{C}|11\rangle \ \bigcap \ \mathrm{C}|++\rangle \oplus \mathrm{C}|--\rangle$$

$$= \mathrm{C}|00\rangle + \mathrm{C}|11\rangle$$

Эквивалентным образом можно использовать выражение $z_1 \oplus_2 z_2 \leftrightarrow \perp \ \wedge \ x_1 \oplus_2 x_2 \leftrightarrow \perp$ для описания ЭПР пары. В этом случае $\oplus_2$ интерпретируется как сложение по модулю 2, связка $\leftrightarrow$ означает эквивалентность и $\perp$ есть 0. Аналогично можно показать, что выражение $z_1 \oplus_2 z_2 \leftrightarrow \perp \ \wedge \ z_1 \oplus_2 z_3 \leftrightarrow \perp \ \wedge \ x_1 \oplus_2 x_2 \oplus_2 x_3 \leftrightarrow \perp$ полностью описывает запутанное GHZ состояние.

Пример 12: *Порождение* ЭПР *пары*. Традиционно Процесс генерации ЭПР пары стартует из состояния $|00\rangle$ (которое описывается логическим соотношением $\neg z_1 \wedge \neg z_2$ или эквивалентным

выражением $z_1 \leftrightarrow \bot \wedge z_2 \leftrightarrow \bot$) применением оператора Адамара H_1 и затем $\oplus_{1,2}$ к системе, представленной на схеме рис. 3.

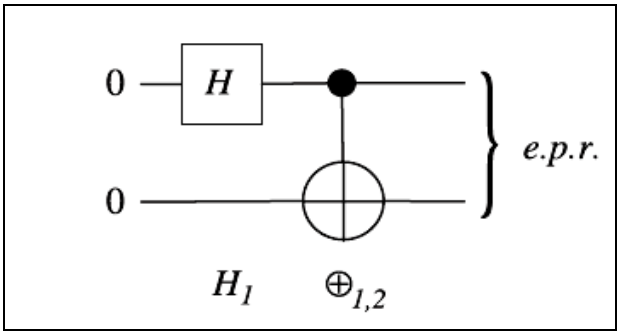


Рис. 3. Схема порождения ЭПР пары

Логически квантовая схема выполняет следующую последовательность операций:

$$H_1 \ \neg z_1 \wedge \neg z_2 \ \text{”ђ} \ H_1 \ \neg z_1 \ \wedge \ H_1 \ \neg z_2 \ \text{”ђ} \neg \ H_1 \ z_1 \ \wedge \neg \ H_1 \ z_2$$

$$\text{”ђ} \neg x_1 \wedge \neg z_2$$

$$\left[\oplus_{1,2}\right] H_1 \ \neg z_1 \wedge \neg z_2 \ \text{”ђ} \left[\oplus_{1,2}\right] \neg x_1 \wedge \neg z_2 \ \text{”ђ} \neg \left[\oplus_{1,2}\right] x_1 \ \wedge \neg \left[\oplus_{1,2}\right] z_2$$

$$\text{”ђ} \neg \ x_1 \oplus_2 x_2 \ \wedge \neg \ z_1 \oplus_2 z_2 \ \text{”ђ} \ x_1 \leftrightarrow x_2 \ \wedge \ z_1 \leftrightarrow z_2$$

Как и ожидалось, конечное высказывание $x_1 \leftrightarrow x_2 \ \wedge \ z_1 \leftrightarrow z_2$ полностью характеризует подпространство, натянутое ЭПР парами, что соответствует результатам предыдущего примера.

Программное обеспечение эмулятора квантового алгоритма

Рассмотрим кратко вопросы моделирования квантовых вычислений и квантовых алгоритмов на классических компьютерах с архитектурой фон Неймана.

Структура системы моделирования квантового алгоритма

На рис. 4 показана структура программного обеспечения системы моделирования квантового алгоритма (КА).

Программное обеспечение (ПО) системы разделено на две части. Первая часть включает в себя общие функции. Во вторую часть входят специализированные алгоритмические функции, реализующие конкретные алгоритмы.

Перечислим общие функции:
- Блок выбора суперпозиции;
- Операторы интерференции;
- Бра-Кэт функции;
- Операторы измерения;
- Операторы вычисления энтропии;
- Функции визуализации;
- Функции визуализации состояния;
- Оператор визуализации.

Специализированные алгоритмические функции включают в себя:
- Декодирование запутанных состояний (квантовая корреляция);
- Проблемный преобразователь;
- Интерпретатор результатов;
- Сценарии выполнения алгоритмов;
- Сценарий выполнения алгоритма Дойча;
- Сценарий выполнения алгоритма Дойча-Джоза;
- Сценарий выполнения алгоритма Гровера;

– Сценарий выполнения алгоритма Шора;
– Сценарий квантового алгоритма управления алгоритмами.

Функции визуализации – это функции, которые обеспечивают корректное отображение амплитуд вектора квантового состояния, а также визуализация структуры квантовых операторов.

Специализированные алгоритмические функции обеспечивают набор сценариев для выполнения КА в общей части и инструментарий для моделирования КА, включая и КА управления алгоритмами. Функции второй части подготавливают операторы для каждого из указанных алгоритмов, используя операнды из первой общей части.

Команды, используемые в КА. Пример выполнения алгоритма Гровера представлен на рис. 5-11. В частности, на рис. 5 показан алгоритм подготовки операторов суперпозиции, квантовой корреляции и интерференции для алгоритма Гровера с тремя кубитами (включая процедуру измерения кубита). Затем операторы собираются в квантовую ячейку. В приведенном примере на рис. 5 показан запуск сценария с начальным состоянием |in> = |001> и вычисление конечного состояния |out> = G|in>. В процессе выполнения данного сценария в программе Matlab осуществляется выделение памяти для оператора матриц и векторов состояния. Полученные квантовые операторы матриц представлен на рис. 7. Вектора начального и выходного состояний, а также квантовая ячейка показаны на рис. 8. Для демонстрации результатов, код функций визуализации представлен на рис. 6. На основе этих данных была построена 3D-визуализация оператора матриц (рис. 9). Здесь вертикальная ось показывает амплитуду соответствующих элементов матриц. Индексы элементов проставлены согласно нотации кэт. Визуализация квантовых состояний, начального и выходного, продемонстрирована на рис. 11. На рис. 11 вертикальная ось соответствует вероятности амплитуд компонент вектора состояния, а горизонтальная ось соответствует индексу компоненты вектора состояния, согласно нотации кэт. Другой подобный КА может быть сформулирован и выполнен с использованием аналогичных сценариев, и с помощью соответствующих уравнений, взятых из предыдущей части.

Рис. 4. Структура программного обеспечения системы моделирования КА

C:\Documents\YMC\QC\algorithms\Grover\simplegrover.m

File Edit View Text Debug Breakpoints Web Window Help

Stack: Base

```
% simplest simulation of Grover's algorithm
clear %clear memory
close all % close all figures
I=eye(2); % identity operator eye is identity matrix built in matlab
C=[0 1;1 0]; %cancellation matrix
Z=zeros(2); %2x2 matrix of zeros
H=1/sqrt(2)*hadamard(2); %W-H transformation operator, hadamard is a built in matlab operator
SP=kron(kron(H,H),H); %superposition operator, kron is a direct product, built in matlab
ENT=[...
        C Z Z Z
        Z I Z Z
        Z Z I Z
        Z Z Z I
    ];%entanglement operator
INT=kron(difusion(2),I); % interference operator

G=INT*ENT*SP; %quantum gate, matrix product is a built in matlab operator
in=ket([0 0  1]); %input vector
out=G*in; %output vector
```

Рис. 5. Пример сценария моделирования алгоритма Гровера (код алгоритма)

```
% Plot results of calculations
figure(1)
subplot(221)
plotoperator3(SP); title('SP') %plot superposition operator
subplot(222)
plotoperator3(ENT); title('ENT')  %plot entanglement operator
subplot(223)
plotoperator3(INT); title('INT') %plot interference operator
subplot(224)
plotoperator3(G); title('G=INT*ENT*SP')%plot operator

figure(2)
subplot(211)
plotsuperposition(in); %plot input superposition
title(['IN,entropy_{SH}=' num2str(entropySH(in)) ,' entropy_{VN}=' num2str(entropyVN(in*in'))])
subplot(212)
plotsuperposition(out); %plot output superposition
title(['OUT, entropy_{SH}=' num2str(entropySH(out)) ,' entropy_{VN}=' num2str(entropyVN(out*out'))])
```

Рис. 6. Пример сценария моделирования алгоритма Гровера (визуализация результата вычислений, выполнения команд)

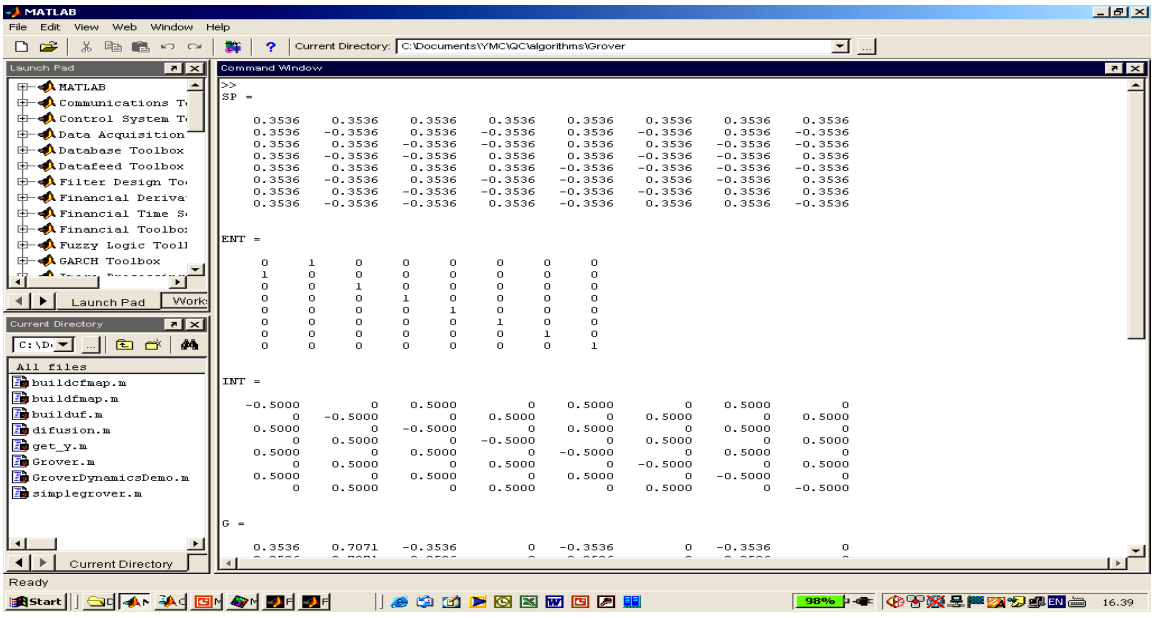


Рис. 7. Пример сценария моделирования алгоритма Гровера (операторы суперпозиции, квантовой корреляции и интерференции)

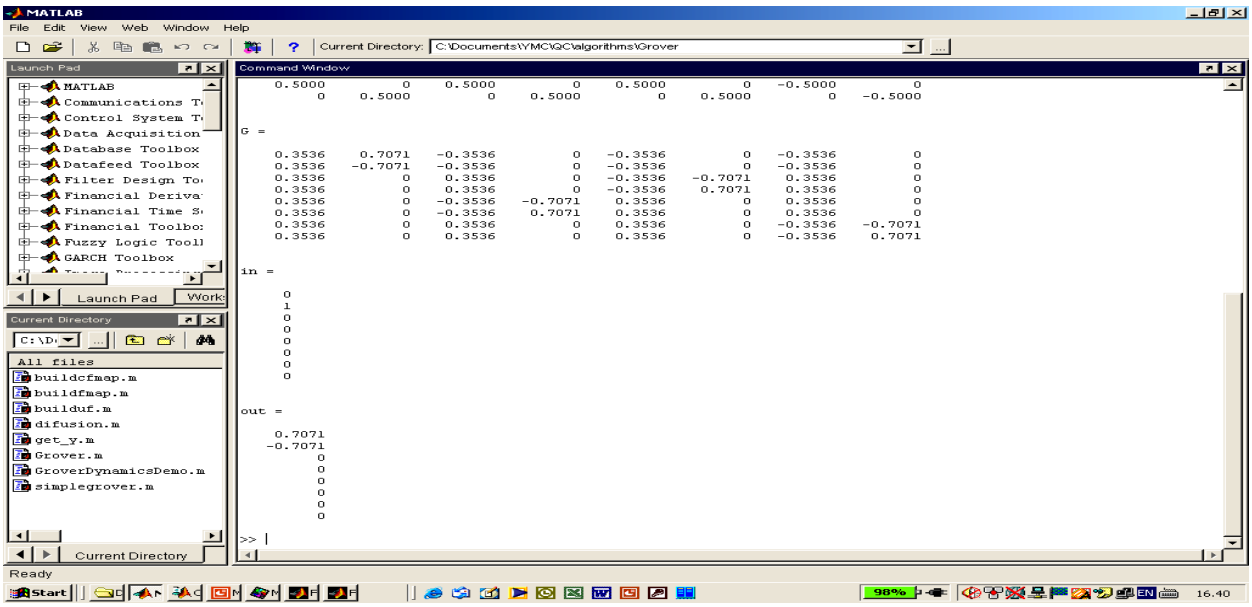


Рис. 8. Пример сценария моделирования алгоритма Гровера (квантовый вентиль, входной вектор и результат выполнения квантового вентиля)

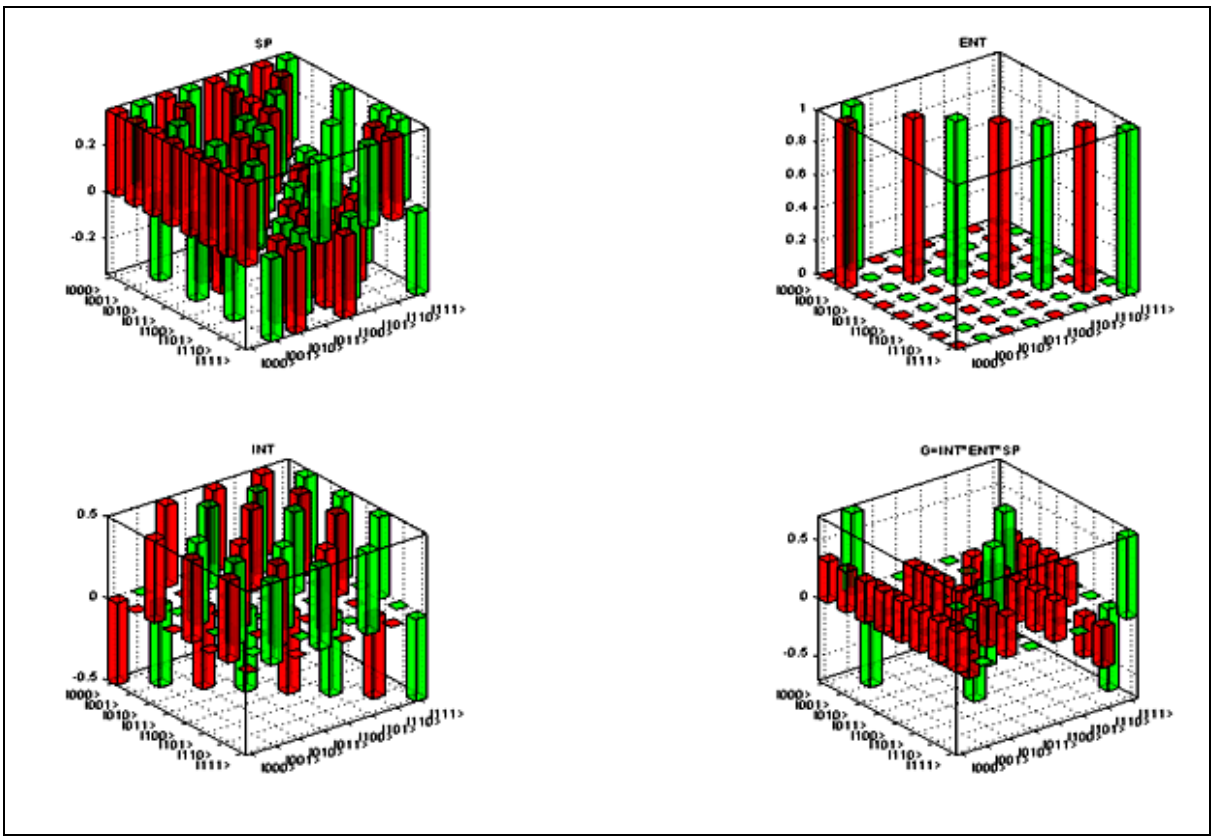


Рис. 9. Пример сценария моделирования алгоритма Гровера (визуализация квантовых операторов)

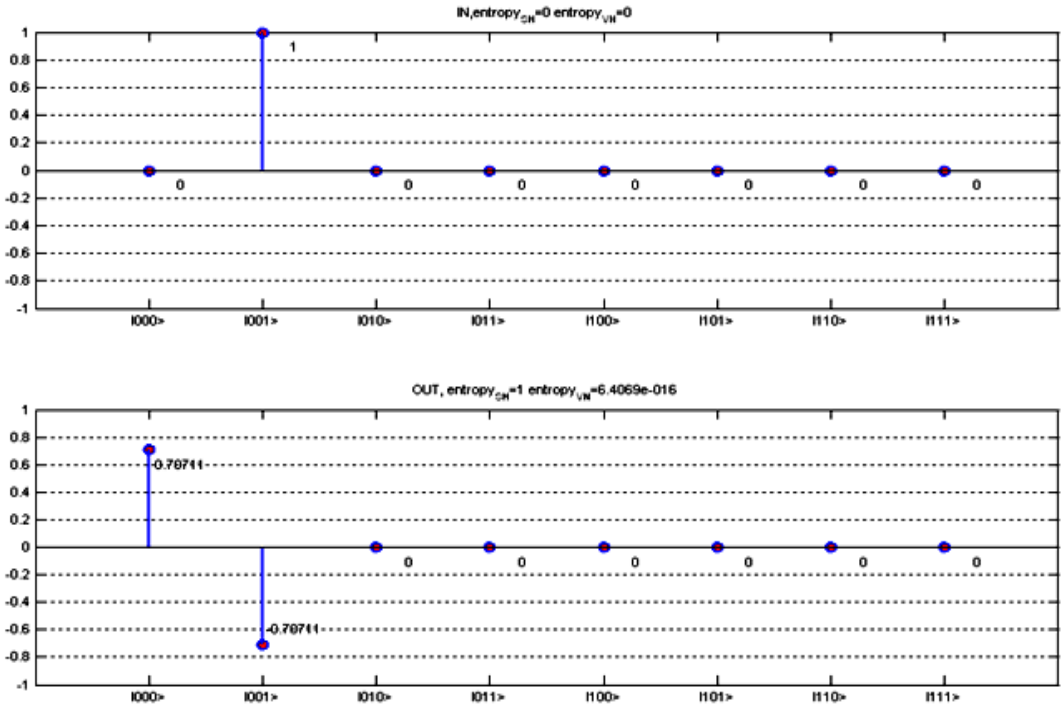


Рис. 10. Пример сценария моделирования алгоритма Гровера (визуализация квантовых состояний: входного и выходного)

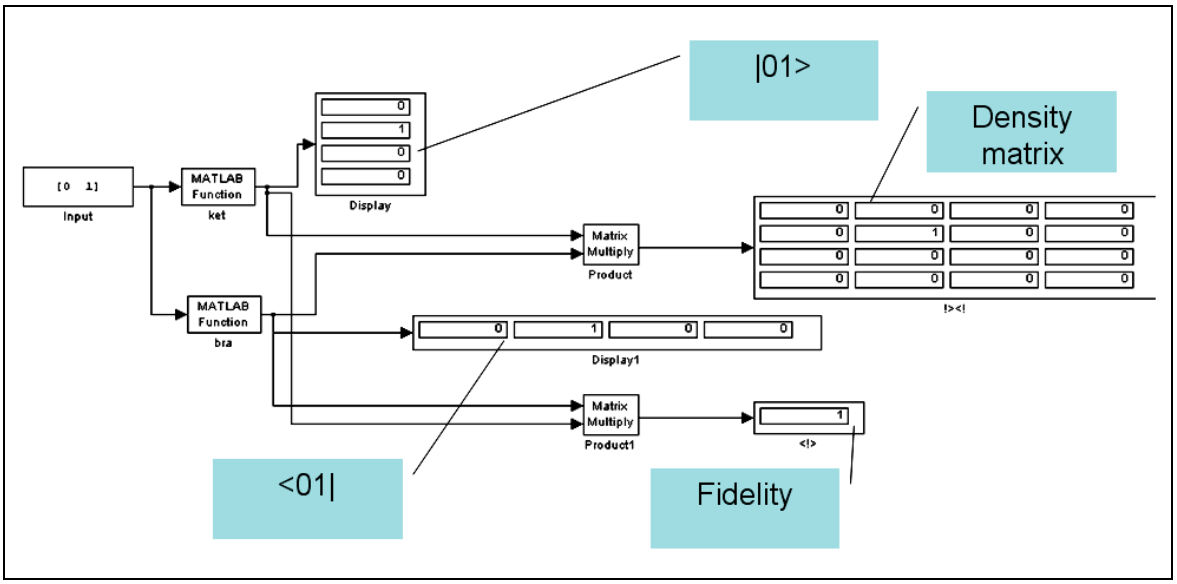


Рис. 11. Диаграмма пакета Simulink моделирования произвольного КА

Моделирование КА как динамической системы. Для того чтобы смоделировать поведение динамической системы, включающей в себя квантовые эффекты, нужно рассмотреть КА как динамическую систему в виде блок-схемы и затем имитировать его поведение во времени. На рис. 11 представлена диаграмма пакета Simulink программного продукта MatLab квантовой схемы расчетов верности <a|a> квантового состояния и вычисления матрицы плотности |a><a| квантового состояния. Функции Бра-Кэт взяты из общей библиотеки. Данный пример демонстрирует, как используются общие функции для моделирования динамики поведения КА.

На рис. 11 показано, что входное значение разделяется на вычисление кэт-функции и бра-функции. Выходное значение кэт-функции является первым входным значением матрицы мультипликатора и вторым входным значением мультипликатора. Вычисленное выходное значение функции бра используется во втором входном значении матрицы мультипликатора, а также как первый вход в матрицу мультипликатора. Результатом работы мультипликатора является расчет матрицы плотности входного состояния, а также вероятность входного квантового состояния.

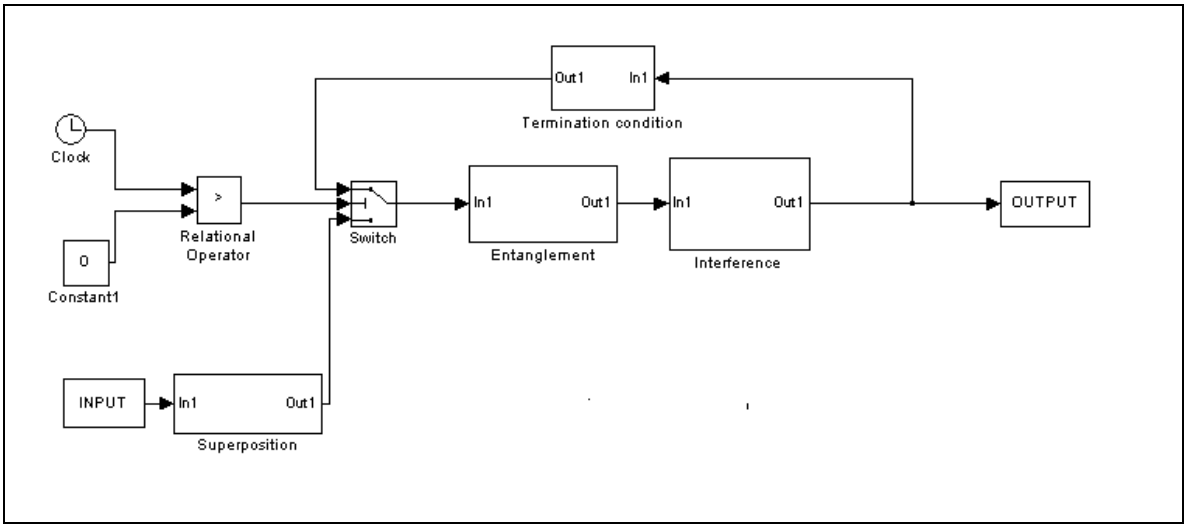


Рис. 12. Диаграмма Simulink моделирования произвольного КА

На рис. 12 показана Simulink-схема произвольного КА. Подобная схема может быть использована в моделировании ряда квантовых алгоритмов в среде Matlab/Simulink.

Эмулятор квантового алгоритма

Разработанное алгоритмическое представление КА может быть использовано для проектирования программного обеспечения (ПО) эмулятора КА. Ключевым моментом является уменьшение количества матричных операций вектора операций и последующая замена операций умножения. Это может привести к резкому увеличению производительности эмуляции, особенно в тех алгоритмах, которые не требуют комплексного числа операций, а также когда вектор квантового состояния имеет относительно простую структуру (например, такой как алгоритм поиска Гровера).

Разработанное ПО было смоделировано для 4-х квантовых алгоритмов: Дойча-Джодза, Шора, Саймона и Гровера. Система использует единый интерфейс для всех алгоритмов, с вариантами 3D-визуализации динамики векторов квантового состояния и квантовых операторов.

Стартовое окно приложения КА эмулятора представлено на рис. 13, в котором пользователь может выбрать создание новой модели КА или продолжить моделирование существующей.

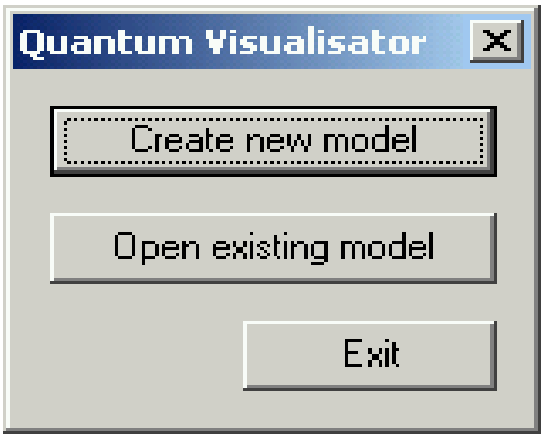


Рис. 13. Стартовое окно приложения КА эмулятора

В случае создания новой модели КА следующим шагом будет выбор алгоритма (рис. 14). На данном этапе пользователь может выбрать не только алгоритм, но и задать нужную размерность. Система предусматривает работу с 50 и более кубитами, но из-за проблем визуализации рекомендуется ограничить число кубитов до 10-11.

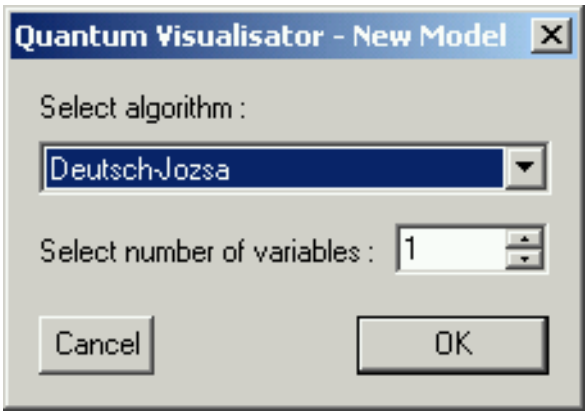


Рис. 14. Диалоговое окно режима создания модели КА приложения КА эмулятора

После того, как были заданы начальные параметры в алгоритме, система отобразит первоначальный вектор состояния и выбранную структуру алгоритма в главном окне системы (рис. 15).

Главное окно (рис. 15) содержит всю информацию о моделируемом квантовом алгоритме и реализует основные операции и осуществляет его анализ. В меню формы есть доступ к квантовым операторам (рис. 16), использовав их можно изменять входные функции (рис. 17). В системе предусмотрена возможность возврата: при нажатии на соответствующие стрелки можно сделать шаги вперед или назад по алгоритму; шаг, который применяется в настоящее время, будет выделен на схеме алгоритма.

Меню эмулятора состоит из 4-х компонент:

1. Пункт *File (Файл)* обеспечивает основные операции, такие как загрузить/сохранить проект, создание новой модели.
2. Пункт *Model (Модель)* осуществляет доступ к изменению входных функций (рис. 17).
3. Пункт *View (Вид)* обеспечивает доступ к матричному оператору визуализаторов, включая операторы суперпозиции, квантовой корреляции и интерференции. Также есть возможность просмотра 3D-визуализации алгоритма динамики квантового состояния (рис. 18).
4. Пункт *Help (Помощь)* позволяет просмотреть документацию по приложению.

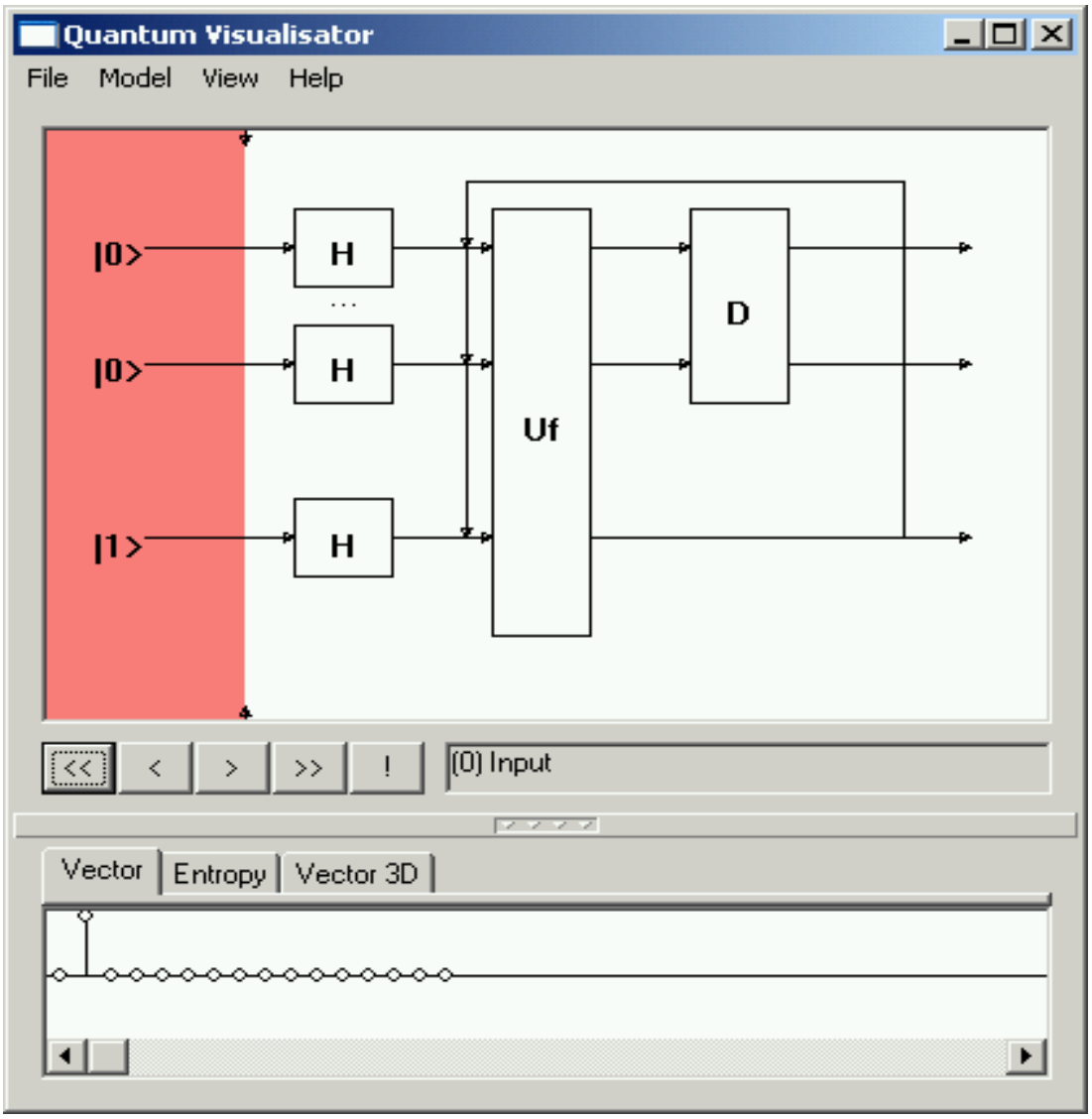


Рис. 15. Главное окно приложения КА эмулятора (поисковый алгоритм Гровера, 3 кубита).

Интерфейс с вкладками в нижней части окна позволяет просмотреть график энтропии Шеннона и 3D представление динамики вектора квантового состояния, а также в обычный, простой график квантового состояния. Размер вкладок может быть изменен путем перетаскивания разделителя между ними. Нажав на серединной точке делителя, можно скрыть интерфейс с вкладками.

При нажатии на кнопку в средней части главного окна приложения можно увидеть заданный в настоящее время КА. Как уже было сказано выше, система позволяет осуществлять шаги вперед и назад.

Если было сделано достаточное количество шагов алгоритма, нажмите на кнопку «!» для получения ответа о текущем векторе состояния (рис. 18). В зависимости от КА будет выдан соответствующий результат.

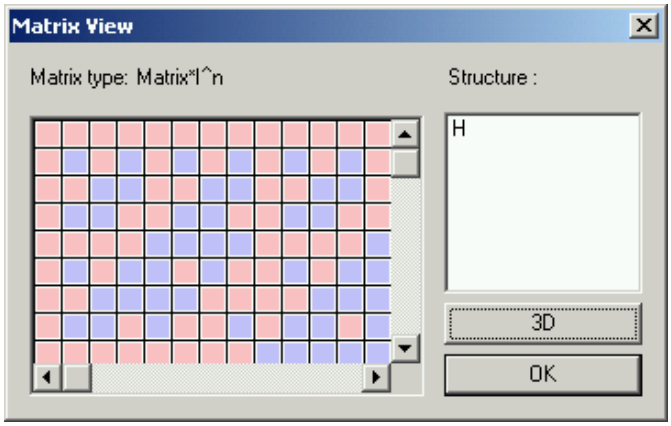


Рис. 16,а. Поле представления оператора суперпозиции

Квантовый оператор визуализации позволяет отображать структуру матриц используемых квантовых операторов в двумерном представлении (рис. 16а) и в 3D-представлении (рис. 16б). Если оператор состоит из тензорного произведения небольших операторов, то существует возможность просмотра подблоков тензорных произведений. 3D-визуализатор позволяет изменять параметры просмотра: увеличить или уменьшить изображение, а также вращать его.

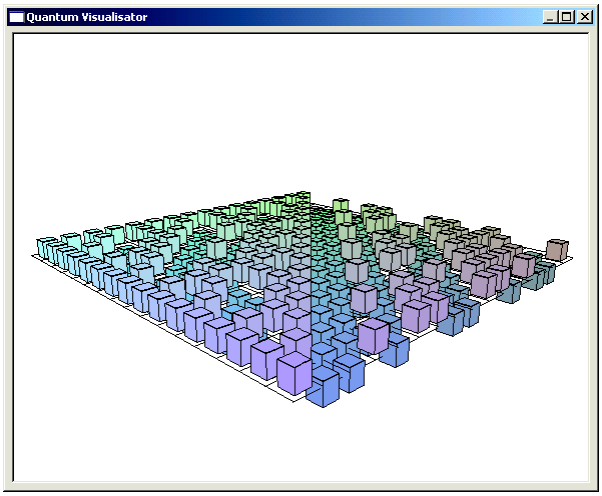


Рис. 16,б. 3D-представление оператора суперпозиции для поискового квантового алгоритма Гровера с 3 кубитами в приложении квантового эмулятора

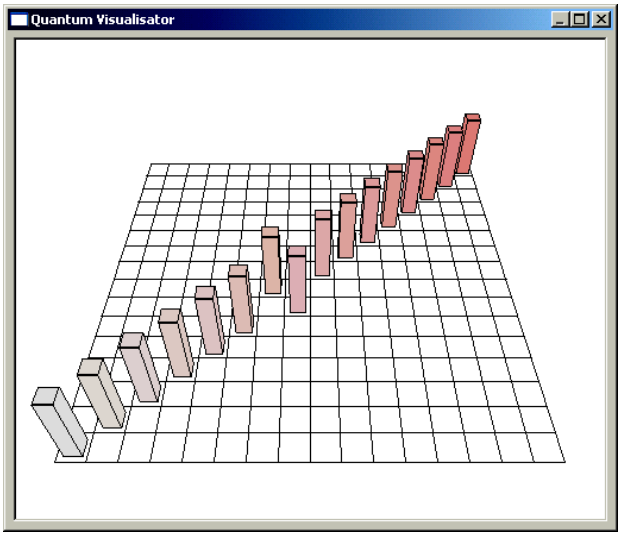


Рис. 16,в. 3D-представление оператора квантовой корреляции для поискового квантового алгоритма Гровера с 3 кубитами в приложении квантового эмулятора

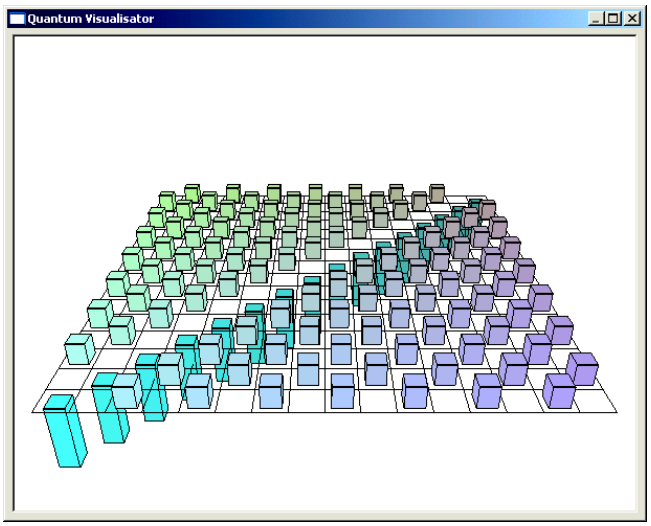


Рис. 16,г. 3D-представление оператора интерференции для поискового квантового алгоритма Гровера с 3 кубитами в приложении квантового эмулятора

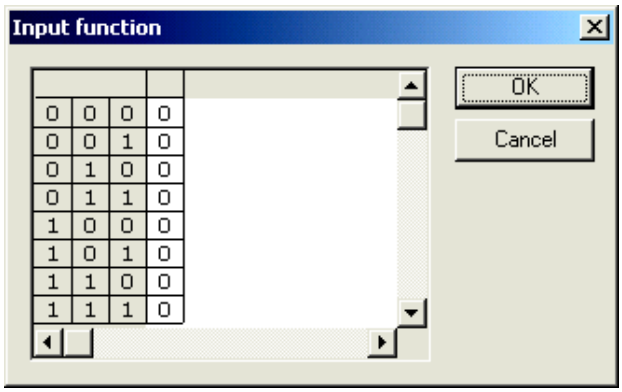


Рис. 17. Редактор входных функций приложения КА-эмулятора (поисковый квантовый алгоритм Гровера с 3 кубитами)

Редактор входных функций позволяет автоматизировать процесс кодирования оператора квантовой корреляции, как это было описано в предыдущих разделах. Для поискового квантового алгоритма Гровера можно закодировать функции, которые имеют более чем один положительный вывод.

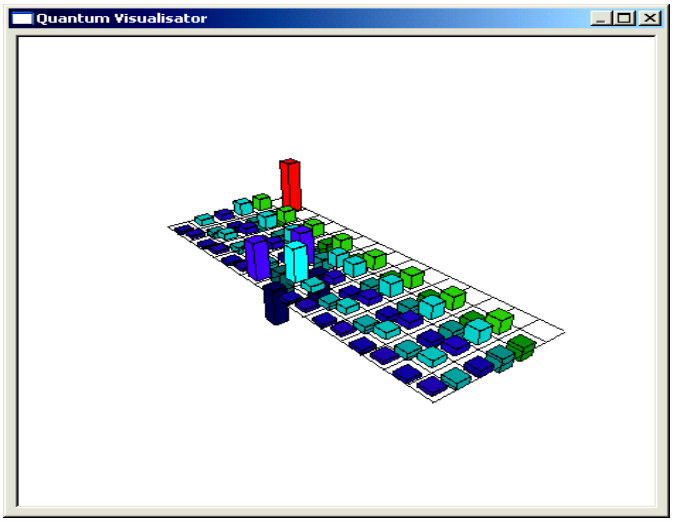


Рис. 18. 3D-график вектора состояния для поискового квантового алгоритма Гровера с 3 кубитами после выполнения 2-х итераций

Рис. 19. Окно выдачи ответа в случае, когда алгоритм Гровера выполнил достаточное количество шагов

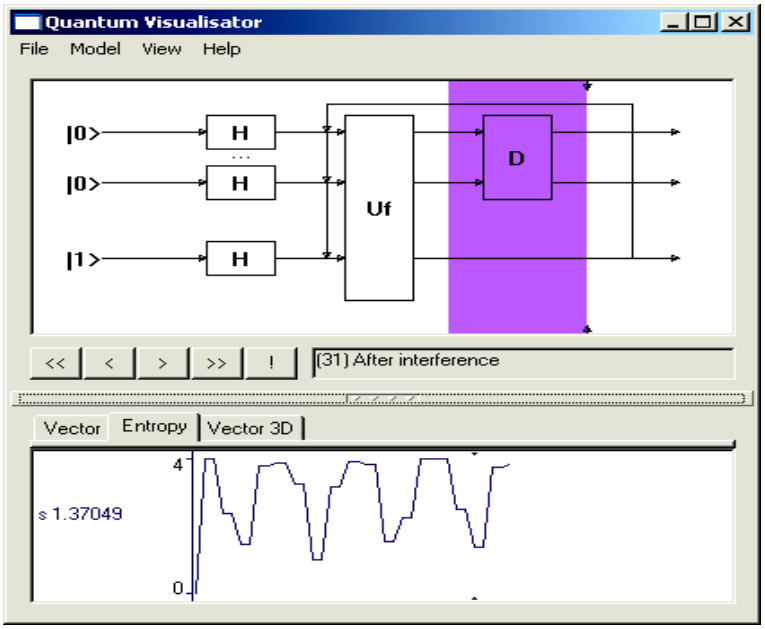
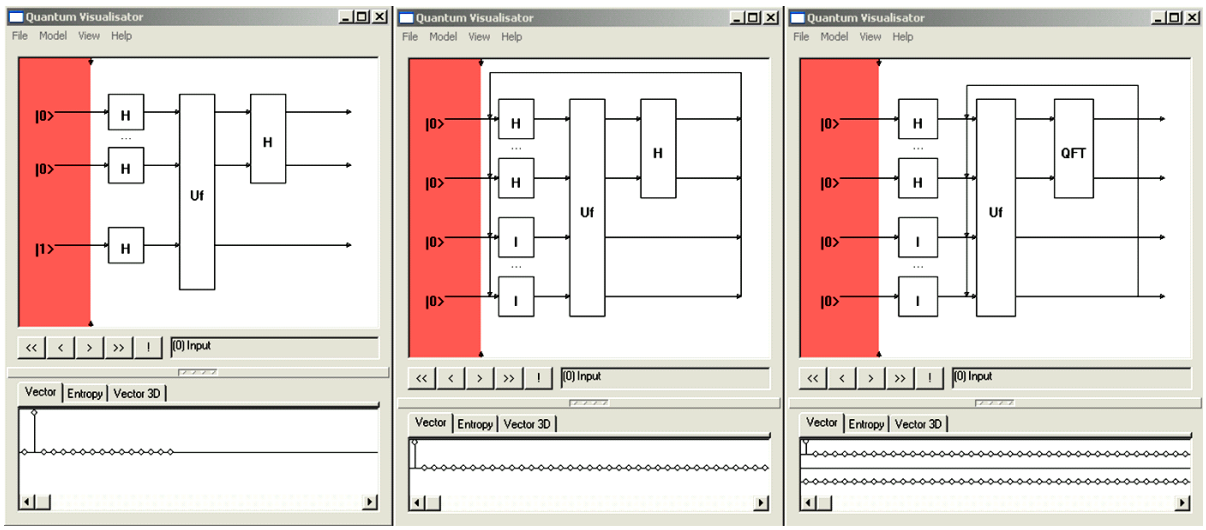


Рис. 20. Динамика энтропии Шеннона после выполнения 31-го шага поискового квантового алгоритма Гровера

Рисунки 21 и 22 показывают начальное (рис. 21) и конечное (рис. 22) квантовое состояние в случаях использования алгоритмов Дойча-Джодза, Саймона и Шора.



(a) (b) (c)

Рис. 21. Начальное состояние КА-эмулятора при моделировании алгоритмов Дойча-Джодза (a), Саймона (b) и Шора (c)

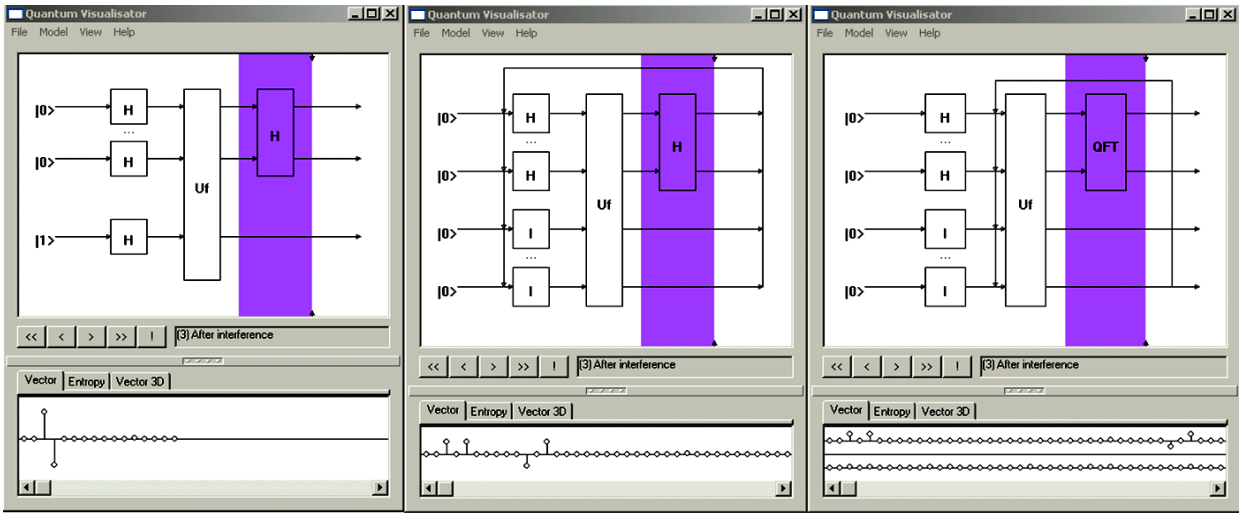


Рис. 22. Конечное состояние КА-эмулятора при моделировании алгоритмов Дойча-Джодза (a), Саймона (b) и Шора (c)

Пример кодирования входных функции и соответствующее 3D-представление оператора запутанности для алгоритмов Дойча-Джодза, Саймона и Шора представлены на рис. 23.

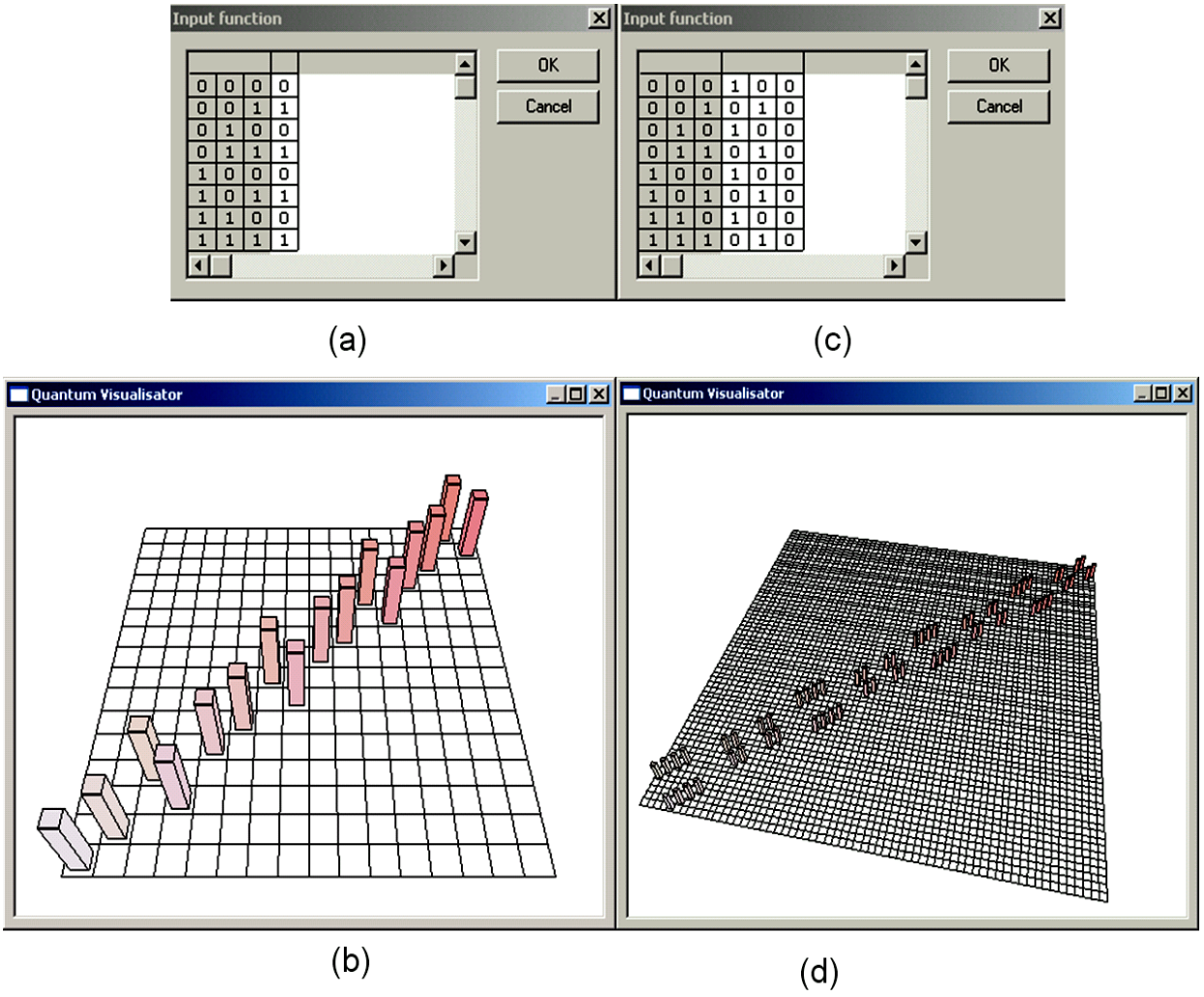
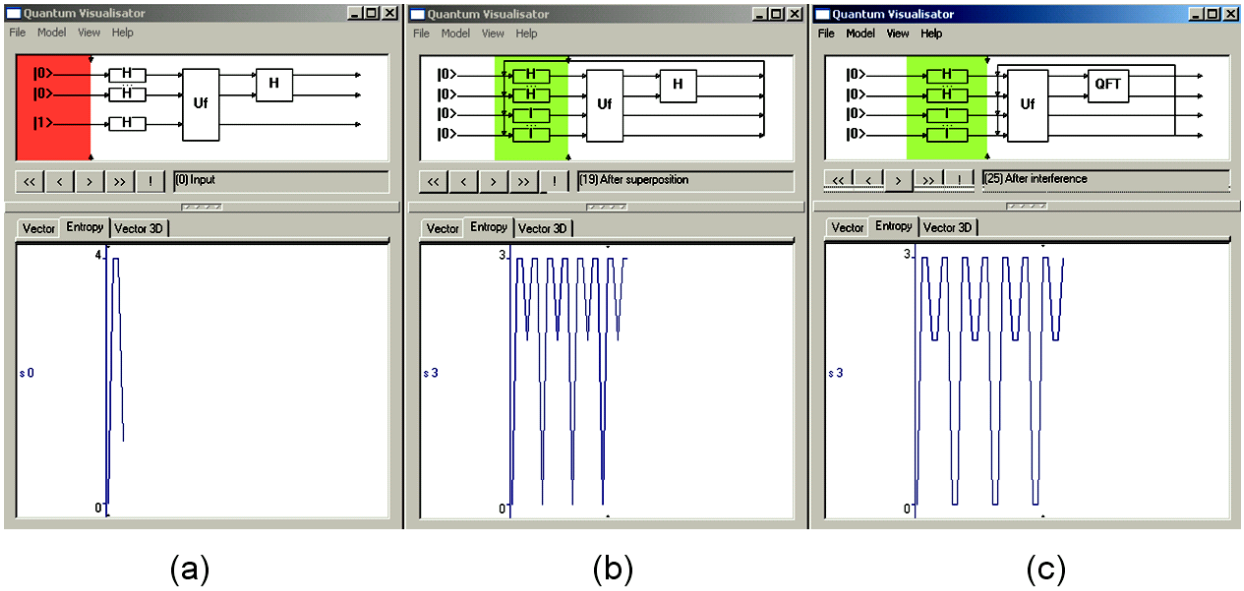


Рис. 23. Сбалансированный вход в КА Дойча-Джодза. Функция (a) и соответствующий оператор запутанности (b); вход в КА Саймона и Шора (c) и соответствующий оператор запутанности (d)

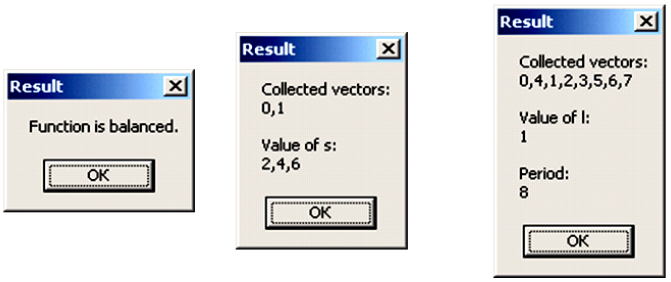
Рисунок 24 демонстрирует динамику энтропии Шеннона в моделируемых квантовых алгоритмов после нескольких итераций алгоритма. Понятно, что ее минимум достигается в состояниях с минимальной неопределенностью, независимо от алгоритма имитации.



(a) (b) (c)

Рис. 24. Динамика энтропии Шеннона: КА Дойча-Джодза (a), КА Саймона (b), КА Шора (c).

Результаты моделирования представленных КА представлены на рисунке 5.41, после работы интерпретатора.



(a) (b) (c)

Рис. 25. Результат интерпретации после выполнения соответствующего КА: КА Дойча-Джодза (a), КА Саймона (b), КА Шора (c).

Приложение. Нетиповое квантовое λ-исчисление. Краткое введение

Рассмотрим другое, нетипичное квантовое λ-исчисление (Q), основанное на квантовых измерениях и данных, а также на парадигме классического управления. Понятия Q обобщаются на основе пояснений и интерпретации терминов, а также измерения операторов.

Исчисление Q^* основано на понятии конфигурации, в виде триплета $Q, Q\nu, M$, где Q – квантовый регистр, Q, ν – конечное множество символов, которые считаются квантовыми переменными и M – не типизированный терм линейного лямбда-исчисления. Conf означает набор таких конфигураций.

Квантовые регистры – это системы n кубитов или, говоря на математическом языке, нормализованные вектора линейного Гильбертово пространства. В частности, квантовый регистр Q конфигурации $Q, Q\nu, M$ – это нормализованный вектор Гильбертова пространства $\ell^2 \quad 0,1^{Q\nu}$, обозначаемого как $H(Q\nu)$. В Гильбертовым пространством физически квантовые переменные интерпретируются как указатели кубитов в квантовом регистре.

При работе квантовым регистром возможны три вида операций:

- операция «new», ответственная за создание новых кубитов;
- унитарные операторы: каждый унитарный оператор $U_{\langle\langle q_1,\ldots,q_n\rangle\rangle}$, соответственно, выполняет квантовую операцию, действующую на кубиты $q_1,\ldots,q_n$ (математически, унитарные преобразования в Гильбертовом пространстве $H \quad q_1,\ldots,q_n \quad$);
- измерение операций одного кубита $M_{r,0}, M_{r,1}$, отвечающих за вероятностную редукцию квантового состояния и удаление ссылок на r: данный квантовый регистр $Q \in H \quad Q\nu$ и название квантовой переменной $r \in Q\nu$, позволяют измерять кубиты с именем r (но с потерей описания квантового состояния).

Другим важным компонентом конфигурации является терм. Набор термов строится на основе:

- счетного множества классических переменных $x, x_0, \ldots$;
- счетного множества квантовых переменных $r, r_0, \ldots$;
- конечного или счетного множества названий, соответствующих унитарным операциям;
- булевские константы 0, 1;
- и операторы new (создать) и meas (измерить).

В пространстве Γ – конечное (возможно пустое) множество в виде $\Lambda, !\Delta$, где Λ – (возможно пустое) множество классических и квантовых переменных, а $!\Delta$ – обозначает (возможно пустое) множество шаблонов, образов $!x_1,\ldots,!x_n$. Утверждается, что в пространстве каждая классическая переменная x встречается не более одного раза (либо как $!x$, либо как x). Суждением является выражение $\Gamma \vdash M$, где Γ – пространство и M – это терм. Будем считать, что суждение хорошо сформировано, если оно получено (выведено) на основе измерений хорошо сформулированных правил (рис. П.1).

$$\frac{}{!\Delta \vdash C}\ \text{const} \qquad \frac{}{!\Delta, r \vdash r}\ \text{qvar} \qquad \frac{}{!\Delta, x \vdash x}\ \text{cvar} \qquad \frac{}{!\Delta, !x \vdash x}\ \text{der}$$

$$\frac{!\Delta \vdash M}{!\Delta \vdash !M}\ \text{prom} \qquad \frac{\Lambda_1, !\Delta \vdash M \quad \Lambda_2, !\Delta \vdash N}{\Lambda_1, \Lambda_2, !\Delta \vdash MN}\ \text{app} \qquad \frac{\Lambda_1, !\Delta \vdash M_1 \cdots \Lambda_k, !\Delta \vdash M_k}{\Lambda_1, \ldots, \Lambda_k, !\Delta \vdash \langle M_1, \ldots, M_k \rangle}\ \text{tens}$$

$$\frac{\Gamma \vdash M}{\Gamma \vdash \mathtt{new}(M)}\ \text{new} \qquad \frac{\Gamma, x_1, \ldots, x_n \vdash M}{\Gamma \vdash \lambda\langle x_1, \ldots, x_n \rangle.M}\ \text{lam}_1 \qquad \frac{\Gamma, x \vdash M}{\Gamma \vdash \lambda x.M}\ \text{lam}_2 \qquad \frac{\Gamma, !x \vdash M}{\Gamma \vdash \lambda !x.M}\ \text{lam}_3$$

$$\frac{\Gamma \vdash M}{\Gamma \vdash \mathtt{meas}(M)}\ \text{meas} \qquad \frac{\Lambda \vdash N \quad !\Delta \vdash M_1 \quad !\Delta \vdash M_2}{\Lambda, !\Delta \vdash \ \mathtt{if}\ N\ \mathtt{then}\ M_1\ \mathtt{else}\ M_2}\ \text{if}$$

Рис. П.1. Хорошо сформулированные правила

Пример П.1: *Телепортация в λ_q-исчислении*. Рассмотрим особенности физической интерпретации алгоритма телепортации на рис. П.2 в предложенном варианте квантового программирования.

$$\begin{aligned}
&\text{teleport } q \rightarrow \ \textbf{let } (e_1, e_2) = \text{epr } \textbf{in} \\
&\qquad\qquad \textbf{let } (q', y') = \text{alice } (q, e_1) \textbf{ in} \\
&\qquad\qquad\ \text{bob } (q', y', e_2) \\
&\text{where} \\
&\text{alice } (q, e_1) \rightarrow \ \textbf{let } (q', y') = cnot\ (q, e_1) \textbf{ in} \\
&\qquad\qquad\ ((H\ q'), y') \\
&\text{bob } (q', y', e_2) \rightarrow \ \textbf{let } (y'', e_2') = cX\ (y', e_2) \textbf{ in} \\
&\qquad\qquad\qquad\ \textbf{let } (q'', e_2'') = cZ\ (q', e_2') \textbf{ in} \\
&\qquad\qquad\qquad\ (q'', y'', e_2'') \\
&\text{epr} \equiv cnot\ ((H\ 0), 0)
\end{aligned}$$

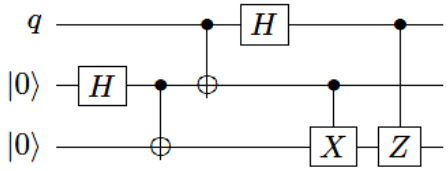


Схема алгоритма квантовой телепортации с задержкой измерения

Рис. П.2: Алгоритм телепортации в λ_q -исчислении

Неясно, если Алиса и Боб физически разделены, каким образом все каналы связи используются в квантовых каналах. Возникает очевидный вопрос: почему используется данный алгоритм, если между Алисой и Бобом работает квантовый канал? Результат измерения конечного квантового состояния логического кубита (квантовой системы), как ожидается, будет перемещен к Бобу. Проблема состоит не в оценке корректности алгоритма, а в его физической интерпретации. В теории квантового программирования данные вопросы не рассматриваются и считается по умолчанию их выполнение.

Рассмотрим как в расширенном квантовом программирование решается данная проблема. Как уже было сказано, измерение является по своей сути вероятностной операцией. Согласно Di Pierro, вероятностная замена системы определяется по λ-исчислению, семантика операций измерения показана на рис. П.3.

$M : \dfrac{q = \sum_{i=0}^{2^m-1} \alpha_i q_i}{H;\ M_I\ q\ \rightarrow p_j \sum_{i \in C_j} \dfrac{\alpha_i}{\sqrt{p_j}} q_i} \left\|I\right\| \le m$	• $q_i = !q_{1i} \otimes !q_{2i} \otimes ... \otimes !q_{mi}$, где $!q_{ki} = !\left\|0\right\rangle$ или $!\left\|1\right\rangle$ для $k = 1...m$. • $C_j = \ i\left\|bin\ \ i, j, I\ \ , i = 0,...,2^m - 1\right.$ для $j = 0,...,2^{\left\|I\right\|} - 1$, где, если $i_k = (resp.\ j_k)$ – это k – ый бит в двоичном представлении $i(j)$, то $bin(i, j, I)$ – это *истина*, при условии $i_{k_h} = j_h, \forall h = 1,...,\left\|I\right\|, k_h \in I, k_h < k_{h+\gamma}\ \forall \gamma > 0$. • $p_j = \sum_{i \in C_j} \left\|\alpha_i\right\|^2$.

Рис. П.3: Оперативная семантика измерений

На рис. П.3 индекс по стрелке – это вероятность данного перехода и I – индекс измеряемого кубита.

Используя эти правила, алгоритм телепортации может быть теперь записан как указано на рис. П. 4, сохраняя при этом корректную физическую интерпретацию.

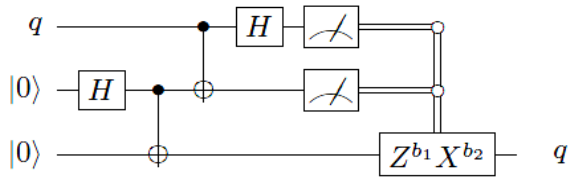
$\text{teleport}\, q \rightarrow_1\ \text{let}\, x \otimes y = epr\, \text{in}$ $\text{let}\, b_1 \otimes b_2 = M_{1,2}\ \text{alice}\ \ q, x\ \ \text{in}$ $\text{bob}\,(b_1, b_2, y)$ где $\text{alice}\,(q, x) \rightarrow_1\ \text{let}\, r \otimes w = cnot\, q \otimes x\, \text{in}$ $H\, r\ \ \otimes w$ $\text{bob}\,(b_1, b_2, y) \rightarrow_1\ (\text{zed}\, b_1)\ \ \text{ex}\, b_2\ \ y$ $\text{epr} \equiv cnot\ \ (H\ !\left\|0\right\rangle \otimes !\left\|0\right\rangle$	 Схема расширенного алгоритма квантовой телепортации

Рис. П.4: Алгоритм телепортации в расширенном λ_q - исчислении

На рис. П.4 функции ex и zed не представлены: ($\mathrm{ex}\, b_2$ представляет X^{b_2}, а $\mathrm{zed}\, b_1$ соответствует оператор Z^{b_1}).

Определение: Квантовое состояние – это набор векторов Q, L, M , где:

- Q – нормализованный вектор $\otimes_{i=1}^{n}\square^{2}$ для целых чисел $n \geq 0$. Вектор Q называется квантовым массивом;
- L – список n отдельных переменных термов, написанный как $|x_1, ..., x_n\rangle$;
- M – лямбда терм, у которого свободные переменные используются в L.

Запишем $|L| = x_1, ..., x_n$., а также $L\ x_i = i$ для позиций переменных x_i в этом списке.

Целью квантового (замыкания), процесса является создание механизма, позволяющего говорить о термах со встроенными квантовыми данными. Идея заключается в том, что переменная x_i связана с термом M числом кубитов $L\ x_i$ состояния квантовой системы Q.

Например, квантовое состояние как замкнутое описание: $\left[\frac{1}{\sqrt{2}}\ |00\rangle + |11\rangle\ ,\ |pq\rangle,\ \lambda x.xpq\right]$ означает, что терм $\lambda x.xpq$ с двумя встроенными кубитами p, q находятся в запутанном состоянии

$$|pq\rangle = \frac{1}{\sqrt{2}}\ |00\rangle + |11\rangle\ .$$

Понятие α-эквивалентности естественным образом расширяется до понятия квантового замкнутого описания состояния, например, состояния $\left[Q, |x\rangle, \lambda y.x\right]$ и $\left[Q, |z\rangle, \lambda y.z\right]$- эквивалентны.

Определим такие квантовые замкнутые состояния как эквивалентные с точностью до переименования соответствующих переменных. Рассмотрим правила сокращений, представленные в Табл. П. 1 – П.3.

Таблица П.1. Правила сокращения: классическое управление

$$Q, L, let\ x = V\ in\ M\ \rightarrow_1 \left[Q, L, M\ \ V/x\ \right]$$
$$\left[Q, L, let\ \langle x, y\rangle = \langle V, W\rangle\ in\ N\right] \rightarrow_1 \left[Q, L, N\ \ V/x, W/y\ \right]$$
$$\left[Q, L, match\ inj_l\ \ V\ \ \ with\ \ \ x \mapsto M \mid y \mapsto N\ \right] \rightarrow_1 \left[Q, L, M\ \ V/x\ \right]$$
$$\left[Q, L, match\ inj_r\ \ W\ \ \ with\ \ \ x \mapsto M \mid y \mapsto N\ \right] \rightarrow_1 \left[Q, L, N\ \ W/y\ \right]$$
$$Q, L, let\ rec\ \ f\ x = M\ in\ N\ \rightarrow_1 \left[Q, L, N\left[\lambda x.\ let\ rec\ \ f\ \ x = M\ in\ M\ \ / f\right]\right]$$

Таблица П.2. Правила сокращения: квантовые данные

$$\left[Q, |x_1 ... x_n\rangle, U\langle x_{j_1}, ..., x_{j_n}\rangle\right] \rightarrow_1 \left[Q', |x_1 ... x_n\rangle, \langle x_{j_1}, ..., x_{j_n}\rangle\right]$$
$$\left[\alpha|Q_0\rangle + \beta|Q_1\rangle, |x_1 ... x_n\rangle, meas\ x_i\right] \rightarrow_{|\alpha|^2} \left[|Q_0\rangle, |x_1 ... x_n\rangle, 0\right]$$
$$\left[\alpha|Q_0\rangle + \beta|Q_1\rangle, |x_1 ... x_n\rangle, meas\ x_i\right] \rightarrow_{|\beta|^2} \left[|Q_1\rangle, |x_1 ... x_n\rangle, 1\right]$$
$$\left[Q, |x_1 ... x_n\rangle, new\ 0\right] \rightarrow_1 \left[Q \otimes |0\rangle, |x_1 ... x_{n+1}\rangle, x_{n+1}\right]$$
$$\left[Q, |x_1 ... x_n\rangle, new\ 1\right] \rightarrow_1 \left[Q \otimes |1\rangle, |x_1 ... x_{n+1}\rangle, x_{n+1}\right]$$

Таблица П.3. Правила сокращения: сравнение правил

$$\frac{Q,L,N \ \to_p \ Q',L',N'}{Q,L,MN \ \to_p \ Q',L,MN'}$$

$$\frac{Q,L,M \ \to_p \ Q',L',M'}{Q,L,MV \ \to_p \ Q',L',M'V}$$

$$\frac{Q,L,M_2 \ \to_p \ Q',L',M_2'}{\left[Q,L,\langle M_1,M_2\rangle\right]\to_p\left[Q',L',\langle M_1,M_2'\rangle\right]}$$

$$\frac{Q,L,M_1 \ \to_p \ Q',L',M_1'}{\left[Q,L,\langle M_1,V_2\rangle\right]\to_p\left[Q',L',\langle M_1',V_2\rangle\right]}$$

$$\frac{Q,L,M \ \to_p \ Q',L',M'}{\left[Q,L,\ inj_l \ \ M\ \right]\to_p\left[Q',L',inj_l \ \ M'\ \right]}$$

$$\frac{Q,L,M \ \to_p \ Q',L',M'}{\left[Q,L,\ inj_r \ \ M\ \right]\to_p\left[Q',L',inj_r \ \ M'\ \right]}$$

$$\frac{Q,L,P \ \to_p \ Q',L',P'}{Q,L,\ match\ P\ with...\ \to_p \ Q',L',match\ P'\ with...}$$

$$\frac{Q,L,M \ \to_p \ Q',L',M'}{\left[Q,L,\ let\langle x,y\rangle = M\ \ in\ N\right]\to_p\left[Q',L',\ let\langle x,y\rangle = M'\ in\ N\right]}$$

Эволюция квантовых лямбда-термов определяется как вероятностная процедура перезаписи квантовых замкнутых состояний (КМС), используя вызов по значению стратегию сокращения.

Определение: Значение терма определяется следующим образом:

$$Value\ V,W ::= c\left|x\right|\lambda x.M\left|inj_r V\right|inj_l V\left|*\right|\langle V,W\rangle .$$

КМС Q,L,V называется значением состояния, если V имеет конкретное значение.

Определение: Правила сокращения приведены в таблицах. Запишем $Q,L,M \ \to_p \ Q',L',M'$ для пошагового сокращения КМС, которые возникают с вероятностью p. В правилах для $let,\ let\,rec, match,$ в $M\ V/x$ обозначает терм M, где свободные переменные x заменены на V (если необходимо, то переименованы связанные переменные). В правиле сокращения терм $U\langle x_{j_1},...,x_{j_n}\rangle$, U - это n -ый встроенный квантовый вентиль, $j_1,...,j_n$ попарно различные, и Q' - это квантовое состояние, полученное из Q путем применения квантового вентиля над кубитами $j_1,...,j_n$. В правилах измерения $\left|Q_0\right\rangle$ и $\left|Q_1\right\rangle$ - это нормализованные вектора состояний, имеющих вид:

$$\left|Q_0\right\rangle = \sum_j \alpha_j \left|\phi_j^0\right\rangle \otimes \left|0\right\rangle \otimes \left|\psi_j^0\right\rangle ,$$

$$\left|Q_1\right\rangle = \sum_j \beta_j \left|\phi_j^1\right\rangle \otimes \left|1\right\rangle \otimes \left|\psi_j^1\right\rangle ,$$

где ϕ_j^0 и ϕ_j^1 – это состояния i -го кубита (измеренный кубит данным образом является точкой x_i). В правиле операция new для Q – это состояние n-го кубита; таким образом $Q\otimes\left|i\right\rangle$ можно представить как $n+1$ -состояние кубита. Используем $\to$ для сокращения $\to_1$ и $\to^*$ для обозначения рефлексивного, переходного состояния $\to$.

Отметим, что только шаг вероятностного сокращения является возможным для измерения.

Пример. Для терма $M = let\,rec\ f\ x = \ if\ \ c*\ \ then\ H\ \ f\ x\ \ else\ x\ \ in\ f\ p$ можно записать :

$$P = if\,(c*)\ then\ H(f\ x)\ else\ x$$
$$R = let\ rec\ f\ x = P\ in\ P\,.$$

Получаем:

$$M \to \left[|0\rangle, |p\rangle,\ f\ p\ \ \lambda x.R\,/\,f\ \right]$$
$$\to \left[|0\rangle, |p\rangle,\ \lambda x.R\ \ p\right]$$
$$\to \left[|0\rangle, |p\rangle, let\,rec\ f\ x = P\,in\ \ if\ (\mathrm{c}*)\,then\,H(f\ p)\,else\,p\ \right]$$
$$\to \left[|0\rangle, |p\rangle,\ if\ (\mathrm{c}*)\,then\,H(f\ p)\,else\,p\ \ \lambda x.R\,/\,f\ \right]$$
$$\to \left[|0\rangle, |p\rangle, if\ (\mathrm{c}*)\,then\,H((\lambda x.R)\,p)\,else\,p\right]$$
$$\to \left[|0\rangle, |p\rangle, if\ meas(H(new0)))\,then\,H((\lambda x.R)\,p)\,else\,p\right]$$
$$\to \left[|00\rangle, |pq\rangle, if\ meas(H\,q))\,then\,H((\lambda x.R)\,p)\,else\,p\right]$$
$$\to \left[\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle), |pq\rangle,\ if\ (meas\,q)\,then\,H((\lambda x.R)\,p)\,else\,p\right]$$
$$\to \begin{cases} \left[|00\rangle, |pq\rangle,\ if\ 0\ then\,H((\lambda x.R)\,p)\,else\,p\right] \\ \left[|01\rangle, |pq\rangle,\ if\ 1\ then\,H((\lambda x.R)\,p)\,else\,p\right] \end{cases}$$
$$\to \begin{cases} \left[|00\rangle, |pq\rangle,\ p\right] \\ \left[|01\rangle, |pq\rangle, H((\lambda x.R)\,p)\right] \end{cases}$$
$$\to \begin{cases} \left[|00\rangle, |pq\rangle,\ p\right] \\ \left[|01\rangle, |pq\rangle, H(let\,rec\ f\ x = P\ in\ if\ (\mathrm{c}*)\,then\,H((\lambda x.R)\,p)\,else\,p)\right] \end{cases}$$
$$\to^{*} \begin{cases} \left[|00\rangle, |pq\rangle,\ p\right] \\ \left[\frac{1}{\sqrt{2}}(|010\rangle + |011\rangle), |pqr\rangle,\ H\ if\ (meas\,r)\,then\,H((\lambda x.R)\,p)\,else\,p\right] \end{cases}$$
$$\to \begin{cases} \left[|00\rangle, |pq\rangle,\ p\right] \\ \left[|010\rangle, |pqr\rangle, H\ if\ 0\ then\,H((\lambda x.R)\,p)\,else\,p\right] \\ \left[|011\rangle, |pqr\rangle, H\ if\ 1\ then\,H((\lambda x.R)\,p)\,else\,p\right] \end{cases}$$
$$\to \begin{cases} \left[|00\rangle, |pq\rangle,\ p\right] \\ \left[|010\rangle, |pqr\rangle, H\ p\right] \\ \left[|011\rangle, |pqr\rangle, H\,(H((\lambda x.R)\,p))\right] \end{cases}$$
$$\to^{*} \begin{cases} \left[|00\rangle, |pq\rangle,\ p\right] \\ \left[\frac{1}{\sqrt{2}}(|010\rangle + |110\rangle), |pqr\rangle, p\right] \\ \left[|0110\rangle, |pqrs\rangle, H\,(H\ p)\right] \\ \left[|0111\rangle, |pqrs\rangle, H\,(H\,(H((\lambda x.R)\,p)))\right] \end{cases}$$

$$\rightarrow^{*}\begin{cases} \left[|00\rangle,|pq\rangle,\ p\right] \\ \begin{cases} \left[\frac{1}{\sqrt{2}}(|010\rangle+|110\rangle),|pqr\rangle,p\right] \\ \begin{cases} \left[|0110\rangle,|pqrs\rangle,\ p\right] \\ \begin{cases} \frac{1}{\sqrt{2}}(|01110\rangle+|11110\rangle),|pqrst\rangle,p \\ \ldots \end{cases} \end{cases} \end{cases} \end{cases}$$

где каждый блок возникает с вероятностью $\frac{1}{2}$, а результат считывается как терм части значения квантового состояния. В среднем, терм M измеряется как $|0\rangle$ с вероятностью $\frac{1}{2}\sum_{n=0}^{\infty}\frac{1}{2^{2n}}=\frac{1}{2}\left(\frac{1}{1-\frac{1}{4}}\right)=\frac{2}{3}$ и как состояние $\frac{1}{\sqrt{2}}|0\rangle+|1\rangle$ с вероятностью $\frac{1}{3}$. Заметим, что, так как нет «мусора», квантовый массив заполняется невостребованными битами. В этом случае, возможно, определить формулы (семантику операций) удаления неиспользуемых битов.

Список литературы

1. Kitaev A.Yu., Shen A.H., Vyaly M.N. Classical and quantum computation. – N.Y.: AMS, 2002.
2. Brylinski F.K. and Chen G. (Eds). Mathematics of quantum computation. – Computational Mathematics Series. – CRC Press Co, 2002.
3. Ulyanov S.V., Litvintseva L.V., Ulyanov I.S. and Ulyanov S.S. Quantum information and quantum computational intelligence: Quantum decision making and search algorithms // Note del Polo Ricerca, Università degli Studi di Milano (Polo Didattico e di Ricerca di Crema). – Milan, 2005. – Vols. 84, 85.
4. Stenholm S. and Suominen K.-A. Quantum approach to informatics. – Wiley- Interscience. J. Wiley&Sons, Inc, 2005.
5. Marinescu D.C. and Marinescu G.M. Approaching quantum computing. – Pearson Prentice Hall, New Jersey, 2005.
6. Benenti G., Casati G., Strini G. Principles of quantum computation and information. – Singapore: World Scientific. – 2004. – Vol. I; – 2007. – Vol. II.
7. Janzing D. Computer science approach to quantum control. – Habilitation: Univ. Karlsruhe (TH) Publ. Germany. – 2006.
8. Jaeger G. Quantum Information: An overview. – N.Y.: Springer Verlag, 2007.
9. Kaye P., Laflamme R. and Mosca M. An introduction to quantum computing. – N.Y.: Oxford University Press, 2007.
10. McMahon D. Quantum computing explained. – Wiley Interscience. A J. Wiley Sons, Inc, 2008.
11. Lanzagorta M. and Uhlmann J. Quantum computer science. – Morgan & Claypool Publ. – Series: SYNTHESIS LECTURES ON QUANTUM COMPUTING (Lecture #2). – 2009.
12. Nakahara M. and Ohmi T. Quantum computing: From Linear Algebra to Physical Realizations. – Taylor & Francis, 2008.
13. Chen G., Kauffman L., and Lomonaco S. J. Mathematics of Quantum Computation and Quantum Technology. – N.Y.: Chapman Hall/CRC (Applied Mathematics and Nonlinear Science Series), 2008.

14. Chen G.,. Church D.A., Englert B.-G., Henkel C., Rohwedder B., Scully M.O. and Zubairy M.S. Quantum Computing Devices: Principles, Designs, and Analysis. – N.Y.: Chapman Hall/CRC (Applied Mathematics and Nonlinear Science Series), 2008.

15. McMahon D. Quantum computing explained. – N.J.: John Wiley & Sons, 2008.

16. Yanofsky N.S. and Mannucci M.A. Quantum Computing for Computer Scientists. – Cambridge University Press. – 2008.

17. Chen G. and Diao C. Mathematical Theory of Quantum Computation. – N.Y.: Chapman Hall/CRC (Applied Mathematics and Nonlinear Science Series), 2009.

18. Kholevo A.S. Quantum systems, channels, and information. – M.: МЦНМО. – 2010 (in Russian).

19. Batty M., Braunstein S.L., Duncan A.J. and Rees S. Quantum algorithms in group theory // http:// arXiv: quant-ph/0310133v1. – 21 Oct 2003. – P. 52.

20. Quantum Algorithms: Shor's algorithm, Grover's algorithm, Quantum logic, Quantum algorithm, Quantum Fourier transform, Deutsch-Jozsa algorithms. – Books LLC. – 2010.

21. Ulyanov S.V., Litvintseva L.V., Ulyanov I.S. et all. Quantum information and quantum computational intelligence: Applied quantum soft computing in AI, computer science, quantum games and self-organization, informatics and design of intelligent wise robust control. Note del Polo Ricerca. Milano: Universita degli Studi di Milano Publ. – 2007. – Vol. 86.

22. Ulyanov S.V., Litvintseva L.V., Ulyanov I.S. et all. Quantum information and quantum computational intelligence: Quantum feedback control models – Physical limits, information bounds, and information-disturbance trade-off. Note del Polo Ricerca. Milano: Universita degli Studi di Milano Publ. – 2006. – Vol. 81.

23. Ulyanov S.V., Litvintseva L.V., Ulyanov I.S. et all. Quantum information and quantum computational intelligence: Quantum optimal control and filtering – Stability, robustness, and self-organization models in nanotechnologies. Note del Polo Ricerca. Milano: Universita degli Studi di Milano Publ. – 2007. – Vol. 82.

24. Nielsen M.A., Chuang I.L. Quantum computation and quantum information. Cambridge: University Press, 2000.

25. Ulyanov S.V., Litvintseva L.V., Ulyanov S.S. Quantum information and quantum computational intelligence: Quantum probability, physics of quantum information and information geometry, quantum computational logic and quantum complexity. Note del Polo Ricerca. Milano: Universita degli Studi di Milano Publ. – 2005. – Vol. 83.

26. Benenti G., Casati G., Strini G. Principles of quantum computation and information. Singapore: World Scientific. – 2004. – Vol. I; 2004. – V. II.

27. Janzing D. Computer science approach to quantum control. Habilitation: Univ. Karlsruhe (TH) Publ. Germany, 2006.

28. Selinger P. Towards a quantum programming language // Math. Struct. In Comp. Science. – 2004. – Vol. 14. – Pp. 527-586.

29. Bettelli S., Calarco T., Serafini L. Toward an architecture for quantum programming // arXiv:cs/0103009v3 [cs.PL]. – 27 Mar 2003.

30. Mauerer W. Semantics and simulation of communication in quantum programming. – Diploma Thesis. – 2005. – University Erlangen Nuremberg, May 2005.

31. Tafliovich A. Predicative Quantum Programming. - A thesis submitted in conformity with the requirements for the degree of Doctor of Philosophy Graduate Department of Computer Science University of Toronto. – 2010.

32. Chakraborty A. QuECT: A new quantum programming paradigm // arXiv:1104.0497v1 [quant-ph] 4 Apr 2011.

33. Gawron P, Klamka J., Miszczak J.A., Winiarczyk R. Extending scientific computing system with structural quantum programming capabilities // BULLETIN OF THE POLISH ACADEMY OF SCIENCES TECHNICAL SCIENCES. – 2010. – Vol. 58. – №. 1.

34. Green A.S., Lumsdaine P., Rosss N.J. Quipper: A scalable quantum programming language // arXiv:1304.3390v1 [cs.PL]. – 11 Apr 2013.