УДК 004.415.2, 004.588

ГЕНЕТИЧЕСКИЕ И КВАНТОВЫЕ АЛГОРИТМЫ. Ч. 1: ИННОВАЦИОННЫЕ МОДЕЛИ В ОБУЧЕНИИ

Ульянов Сергей Викторович[1], Добрынин Владимир Николаевич[2], Нефёдов Никита Юрьевич[3], Петров Сергей Павлович[4], Полунин Алексей Сергеевич[5], Решетников Андрей Геннадиевич[6]

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

[3]Студент;
ГОУ ВПО Международный Университет природы, общества и человека «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: nefnukem@gmail.com.

[4]Студент;
ГОУ ВПО Международный Университет природы, общества и человека «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: bloodthirsty_89@mail.ru.

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

[6]Студент;
ГОУ ВПО Международный университет природы, общества и человека «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: reshet@sunhe.jinr.ru.

Рассмотрены фундаментальные принципы, физическая и алгоритмическая интерпретации основных квантовых и эволюционных эффектов, используемых в квантовых и генетических алгоритмах. Данные эффекты применяются при поиске эффективных решений задач глобальной оптимизации и интеллектуального управления слабо формализованными системами в условиях непредвиденных ситуаций и риска.

Ключевые слова: квантовые генетические алгоритмы, программный инструментарий, глобальная оптимизация, интеллектуальное управление, образование.

GENETIC AND QUANTUM ALGORITHMS. PT I: INNOVATION MODELS IN EDUCATION

Ulyanov Sergey[1], Dobrynin Vladimir[2], Nefedov Nikita[3], Petrov Sergey[4], Polunin Aleksey[5], Reshetnikov Andrey[6]

[1]*Doctor of 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]*Candidate of Science in Engineering, professor of Institute of system analysis and management;*
Dubna International University of Nature, Society and Man,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: arbatsolo@yandex.ru.

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

[4]*Student;*
Dubna International University of Nature, Society and Man,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: bloodthirsty_89@mail.ru.

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

[6]*Student;*
Dubna International University of Nature, Society and Man,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: reshet@sunhe.jinr.ru.

Main fundamental principles, physical and algorithmic interpretation of quantum and evolution effects of quantum and genetic algorithms are discussed. These effects effective in solutions of global optimization problems and in intelligent control of ill-defined systems are used.

Keywords: quantum and genetic algorithms, global optimization, intelligent control, education.

Введение

Поиск решения задач глобальной (многокритериальной в общем случае) оптимизации является типичной проблемой для системного анализа, принятия оптимальных решений и управления сложными системами в условиях неопределенности информации и риска, и развивается многие годы по разным направлениям [1]. В последние годы решение данной задачи успешно решается новыми видами интеллектуальных вычислений. В общем виде к таким вычислениям относятся следующие виды и типы [2]: (1) эволюционное и квантовое программирование; (2) алгоритмы оптимизации типа иммунных алгоритмов; (3) алгоритмы оптимизации на основе поведенческих реакций и обмена информацией активных агентов (самоорганизация целенаправленного и оптимального поведения людей в тоннеле, колоний муравьев, стай птиц и рыб, животных и т.п. – swarm intelligence, active agents opti-

mization); (4) квантовые и/или генетические алгоритмы; (5) квантовые нейронные сети обучения; (6) квантовые и/или классические алгоритмы отжига (quantum annealing algorithms); и мн. др.

Анализ различных подходов дан в [2].

Модели генетических алгоритмов (ГА) оказались наиболее применяемыми в практике решения задач глобальной оптимизации системного анализа и управления и уже нашли достаточно широкое отражение в университетских программах дисциплин. Модели квантовых алгоритмов (КА) разрабатываются в последнее десятилетие, результаты нашли эффективное практическое инженерное применение в последние годы, но мало известны широкому кругу исследователей и тем более студенческой аудитории. В результате университетские программы соответствующих дисциплин и бакалаврские/магистерские диссертации слабо затрагивают данное направление исследований. Однако существует определенная глубокая аналогия между структурами ГА и КА.

Поэтому возник определенный разрыв в программах дисциплин и методологии учебных процессов при освещении вопросов структурной реализации ГА и КА на доступном (для инженерных специальностей) уровне (особенно при изучении вопросов решения задач глобальной векторной многокритериальной оптимизации в задачах интеллектуального управления).

Цель работы

В Части I данной статьи сделана попытка освещения разработанных методологических вопросов, необходимых для студентов (соответствующих специальностей), математического описания структур ГА и КА, используя накопленный опыт одного из авторов (Ульянов С.В.) при чтении соответствующих курсов лекций в Международном университете природа, общество и человек «Дубна», University of Electro-Communications (Tokyo) и Universita di Milano. При этом используется также практический опыт применения ГА и КА в реальных Международных проектах между Yamaha Motor Co., Ltd (Japan) и ST Microelectronics (Italy) и создания совместно с компанией KMOB (USA, CA) патентов на трудно патентуемые объекты интеллектуальной собственности (ОИС), такие как алгоритмический и программный инструментарий интеллектуальных вычислений.

Решаемая задача

Обсуждаются инновационные подходы к построению учебных материалов для разъяснения таких трудных вопросов как алгоритмическое описание и разработка программного интеллектуального инструментария для реализации операторов и структур указанных алгоритмов при моделировании на классических компьютерах.

Сочетание теоретических результатов по разработке новых моделей КА и ГА, и практических реализаций в проектах бакалаврских/магистерских дает мощный стимул инновационного развития инженерных коммерчески привлекательных интеллектуальных инструментариев в малых инновационных предприятиях при университетах и стимулирует финансовую политику инвесторов и венчурных фондов.

Ниже дано краткое описание генетических и квантовых операторов, структур алгоритмов, их взаимоотношений и свойств, часто используемых в решении задач глобальной оптимизации.

Данные сведения позволяют более полно и глубоко понять на практике решение следующей трудной и принципиально важной для теории и систем управления проблемы: *определение роли и влияния квантовых эффектов на повышение уровня робастности проектируемых интеллектуальных процессов управления* за счет извлечения дополнительной квантовой информации, скрытой (и только частично доступной) в корреляционных классических состояниях законов управления, и спроектированных только на основе классических методов технологии мягких вычислений.

Особую роль играет выбор метода исследования, физическая и математическая корректность описания моделей объекта управления на основе интеллектуальных вычислений. Данные вопросы исследуется в Части II данной статьи. Дополнительные сведения и подробное изложение данных вопросов с математическим доказательством требуемых утверждений можно найти в [3].

1. Структура ГА

ГА являются процедурами поиска глобального оптимума (максимума или минимума) некоторой целевой функции, основанными на принципах естественной эволюции. В них сгенерированная случайным образом начальная популяция решений подвергается воздействию генетических операций, таких как *селекция*, *скрещивани*е и *мутация*. В результате получается новая популяция решений, с улучшенными основными свойствами (значениями целевой функции). Целевая функция называется функцией пригодности и в задачах теории оптимального управления является многокритериальным функционалом качества оптимального управления. Данный процесс продолжается итеративно до достижения глобального оптимума.

ГА использует информацию только о значениях функции и не требует информации о производных исследуемой функции. Это свойство ГА дает огромное преимущество перед классическими градиентными алгоритмами. Сам ГА реализует принцип параллельных вычислений. ГА, имеющий хромосому, может быть в принципе любым из известных ГА, имеющих хромосому фиксированной длины. В данной работе для простоты изложения выбран ГА «элитного» типа, с двухточечными операциями скрещивания и мутации. В качестве системы кодирования была выбрана бинарная система с числом бит для кодирования каждого параметра, достаточным для покрытия соответствующего диапазона изменения. Для более компактного размещения, гены представлены символьными типами данных (16 бит на символ), при этом были использованы операции прямого копирования содержимого памяти для реализации операций скрещивания и мутации.

Рассмотрим более подробно структуру ГА.

Математическая модель ГА может быть представлена следующим упорядоченным набором:

$$\left\langle C, F, P^0, \mu, \Omega, \Gamma(p^\Gamma), \Delta(p^\Delta), \Psi \right\rangle,$$

где C – система кодирования (Coding system); F – функция пригодности (Fitness function); P^0 – начальная популяция (Initial population); μ – размер начальной популяции (Population size); Ω – операция селекции (Selection operation); $\Gamma(p^\Gamma)$ – операция скрещивания (Crossover operation), p^Γ – вероятность скрещивания (Probability of crossover); $\Delta(p^\Delta)$ – операция мутации (Mutation operation), p^Δ – вероятность мутации (Probability of mutation); Ψ – условие остановки (Termination condition).

Структура ГА показана на рис.1. Система кодирования C является унитарной операцией, определяющей отображение пространства решений в некоторое *пространство*, на котором определены генетические операции. Простым примером кодирования является двоичное кодирование, отображающее пространство вещественных чисел в пространство бинарных строк заданной длины: $A \overset{C}{\leftrightarrow} B : A \in R^n, B \in B^l = \{0,1\}^l$, где R^n – пространство вещественных векторов размерности n; B^l – пространство двоичных строк длины l. В большинстве программных реализаций ГА предпочтение отдается двоичному кодированию. Во многом это связано с простотой реализации генетических операций над двоичными строками.

Такая кодировка гарантирует также *максимальную энтропию* внутри популяции. Начальная популяция P^0 есть набор равномерно распределенных в пространстве кодирования элементов. В случае двоичного кодирования – набор различных двоичных строк длины l. Размер популяции μ есть число индивидуумов (хромосом), входящих в популяцию.

Функция пригодности F является критерием, определяющим качество данного индивидуума. Обычно функция пригодности оценивает отклик некоторой внешней функции или динамической системы на параметры, закодированные в данной хромосоме.

В случае сложных нелинейных задач оптимизации, вычисление значения функции F является наиболее трудоемкой процедурой, требующей большег**о** машинного времени, по сравнению с ос-

тальными генетическими операциями. Процесс ускорения вычисления функции пригодности ГА освещен подробно в [4].

Как правило, ГА не использует непосредственные значения функции пригодности. Обычно осуществляется нормализация значений и вычисляется так называемый относительный критерий качества, распределяющий вес каждой из хромосом в текущей популяции.

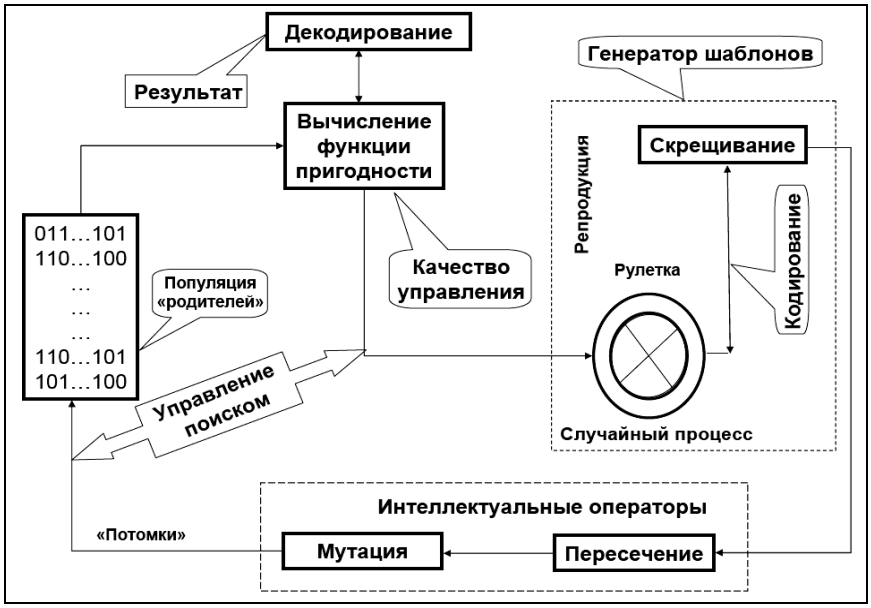

Рис. 1. Структура ГА

На рис. 2, представлена блок-схема операций кодирования и вычисления значения функции пригодности.

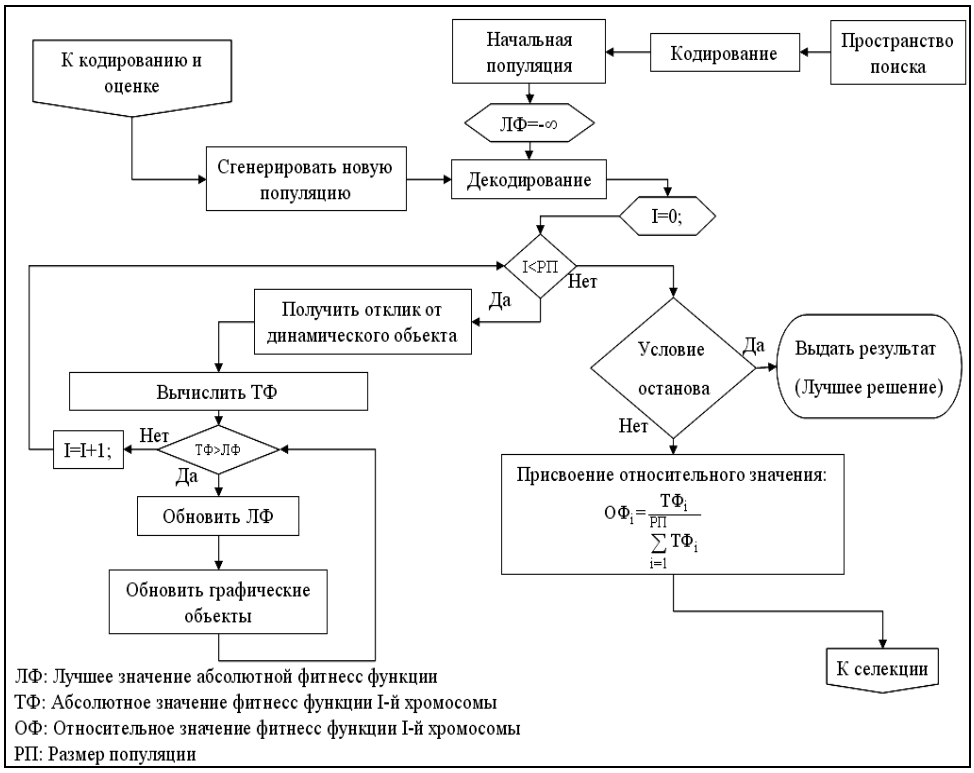

Рис. 2. Операции кодирования и вычисления объектных функций ГА

Оператор селекции Ω (Selection) является вероятностной операцией, определенной для воспроизведения большего числа хромосом с большим значением функции пригодности в следующем по-

колении. В частности, в некоторых реализациях ГА, оператор селекции выбирает набор хромосом в промежуточную популяцию, к которой в дальнейшем могут быть применены операции скрещивания и мутации.

Блок-схема реализации оператора селекции представлена на рис. 3.

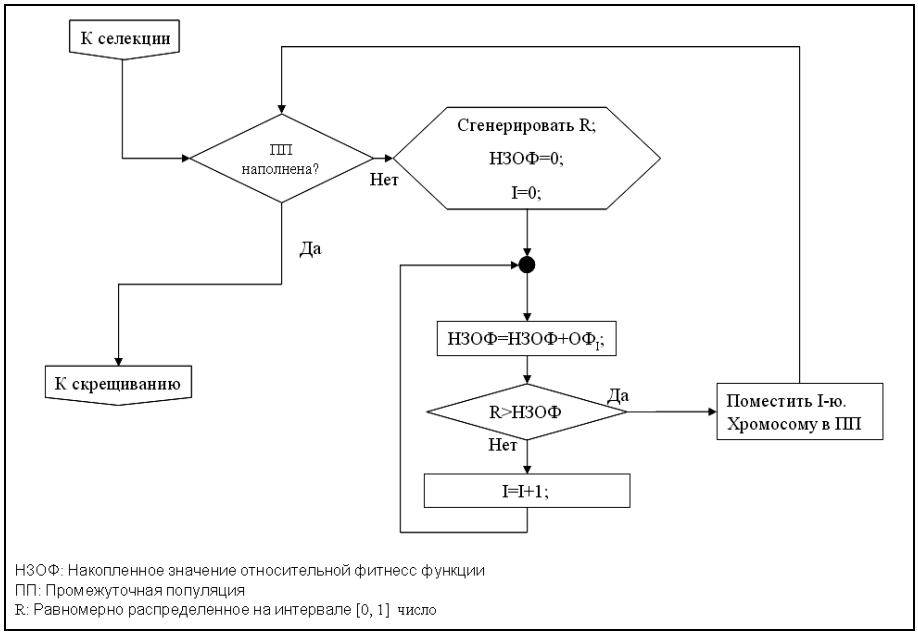

Рис. 3. Блок-схема реализации операции селекции методом рулетки

Оператор селекции работает по принципу рулетки. При этом индивидуумам с большим значением функции пригодности выделяется больший сектор рулетки. Таким образом, после вращения рулетки, вероятность выбора индивидуумов с большим значением функции пригодности увеличивается.

Операция скрещивания Γ является вероятностной операцией, предназначенной для обмена генетической информацией между индивидуумами, входящими в данную популяцию. Вероятность данной операции p^{Γ} обычно задается пользователем и меняется в зависимости от типа решаемой задачи. Входом операции скрещивания является промежуточная популяция, получаемая после операции селекции Ω.

Операция скрещивания (на примере бинарного кодирования B^l) выполняется следующим образом:

1. Выбрать два индивидуума из промежуточной популяции.
2. Сгенерировать случайное число, равномерно распределенное на интервале [0, 1] и если полученное число меньше p^{Γ}, выполнить операцию скрещивания, если нет, перейти к шагу 5.
3. Сгенерировать точку скрещивания, равномерно распределенное случайное число на интервале [0, l].
4. Поменять местами части выбранных индивидуумов, правее точки скрещивания.
5. Поместить выбранные хромосомы в новую популяцию.
6. Повторить шаги 1 – 5 до заполнения новой популяции.

Блок схема операции скрещивания представлена на рис. 4.

В некоторых реализациях ГА, операция скрещивания применяется несколько раз для одних и тех же хромосом. В таком случае говорят о двухточечном скрещивании (two-point crossover). Выбор числа применений операции скрещивания зависит от конкретной задачи, а также связан со значениями основных параметров ГА.

Теоретически операции селекции и скрещивания позволяют находить экстремумы выпуклых функций, или достигать локальных экстремумов при многоэкстремальной оптимизации. По своей структуре данные операции «стерильны». ГА, построенный только на операциях селекции и скрещивания, как правило, не справляется с решением задачи нахождения глобального оптимума многоэкстремальной целевой функции.

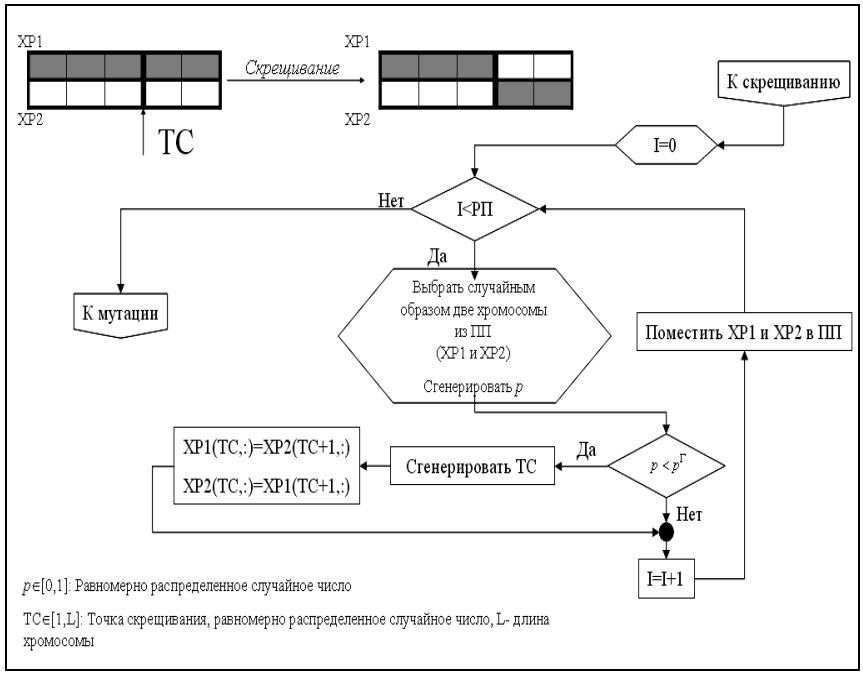

Рис. 4. Блок-схема реализации операции скрещивания

Для его достижения алгоритму необходима операция мутации. Операция мутации $\Delta(p^{\Delta})$ является унитарной вероятностной операцией, предназначенной для внесения новой информации в данную популяцию.

Операция мутации позволяет ГА избегать локальных экстремумов, т.к. генерирует хромосомы, находящиеся на достаточном удалении от оригинала.

Алгоритм мутации реализуется следующими шагами:

1. Выбрать случайным образом индивидуум из промежуточной популяции.
2. Сгенерировать случайное число, равномерно распределенное на интервале [0, 1]. Если полученное число меньше p^{Δ}, выполнить операцию мутации. В противном случае перейти к шагу 5.
3. Сгенерировать точку мутации (mutation point) – случайное число, равномерно распределенное на интервале [0, l].
4. Инвертировать бит, находящийся в точке мутации.
5. Поместить выбранную хромосому в новую популяцию.
6. Повторить шаги 1 – 5 до заполнения популяции.

Блок-схема реализации операции мутации представлена на рис. 5.

Как и в случае с операцией скрещивания, операцию мутации можно применять несколько раз к одной и той же хромосоме. В таком случае говорят о многоточечной мутации [4]. Таким образом, структура ГА имеет простой вид и легко реализуется программным инструментарием.

При использовании ГА, однако, часто возникают проблемы поиска решения.

Так, например, в задачах интеллектуального робастного управления при существенном изменении или непредвиденных ситуациях управления, спроектированные законы управления, не всегда сохраняют свойство робастности [3]. Данный эффект определяется функциональной структурой ГА,

в которой (по определению) пространство поиска решений фиксировано и задается экспертом, а также выбором функции пригодности, которая рассматривается как критерий оптимальности управления.

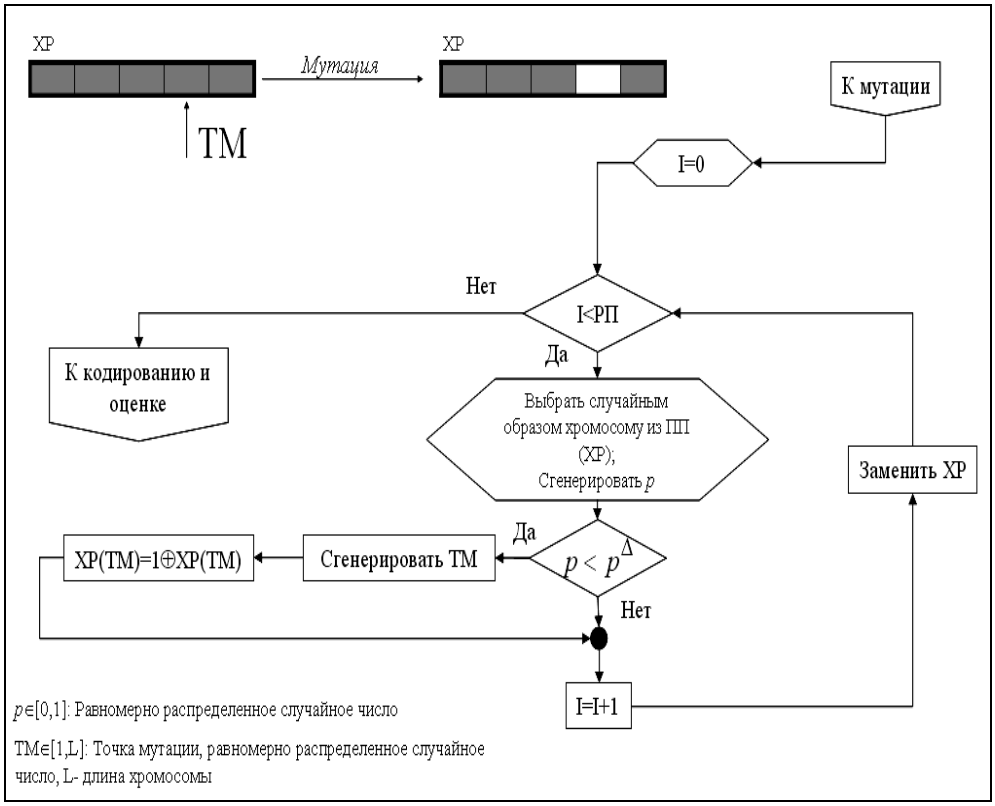

Рис. 5. Блок-схема реализации операции мутации

Знания эксперта проявляются в общем случае в его опыте корректного задания пространства поиска ГА и знании вида функции пригодности. Следовательно, решение, найденное оптимальное решение при помощи технологии мягких вычислений (на основе ГА) соответствует заданной ситуации управления, содержит (в неявном виде) субъективность исходной информации, а при неправильном определении пространства поиска и функции пригодности решение может неадекватно соответствовать ситуации управления.

На рис. 6 показан результат поиска глобальных экстремумов многокритериальной функции.

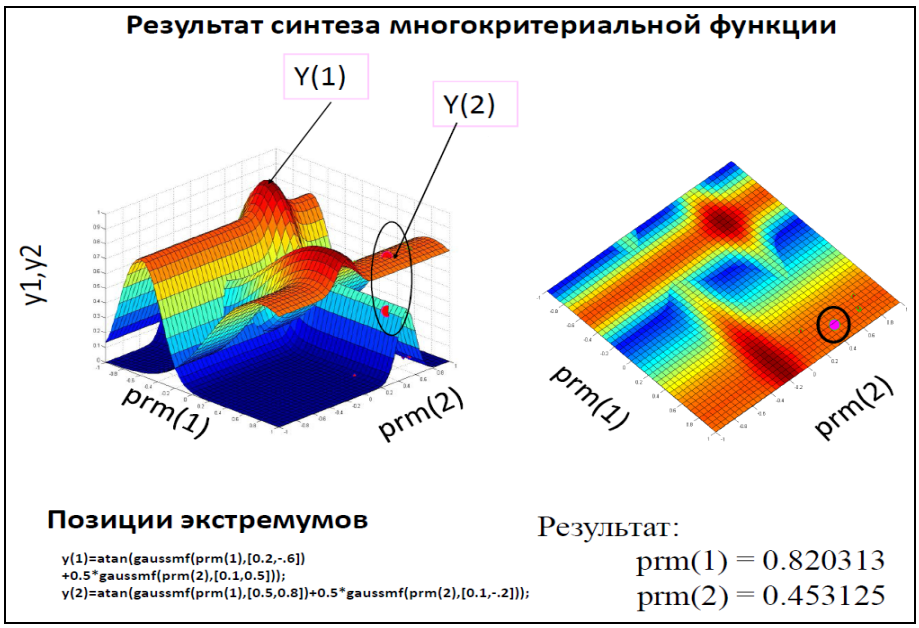

Рис. 6. Результат поиска ГА экстремумов многокритериальной функции

Операторы ГА достаточно хорошо известны и имеют четкую физическую интерпретацию по аналогии с биологическими механизмами эволюции естественного отбора Дарвина. Операторы КА менее известны в инженерных приложениях и требуют более детального рассмотрения физической интерпретации и математической формализации квантовых вычислений [2, 5].

2. Структура квантовых вычислений и КА

В теории квантовых вычислений можно выделить два направления исследований:

- задано множество точек функционала $S = \{(x, y)\}$, необходимо найти вид такого оператора U, чтобы выполнялось условие $y = U \cdot x$;
- задана проблема (КА), необходимо найти вид квантовой схемы – квантовой алгоритмической ячейки (КАЯ), решающей заданную проблему (реализующей данный КА).

Алгоритмы решения данных задач могут быть реализованы как на аппаратных средствах в виде КАЯ, так и на программном уровне с помощью соответствующего программного инструментария (toolkit) с реализацией на классическом компьютере [6].

В [6 – 8] показана возможность эффективного моделирования КА на классическом компьютере и используется в данной статье для моделирования КА. Фундаментальный результат теории квантовых вычислений заключается в том, что все операции (подобно классическому случаю) могут быть реализованы на схеме, состоящей из универсальных базисных элементов.

В отличие от классического аналога, КАЯ могут быть выполнены на различных классах универсальных элементов в зависимости от используемого вычислительного базиса [9]. КАЯ (с фиксированными вычислительным и измерительным базисами) обеспечивают описание эволюции некоторого унитарного оператора U, которому соответствует квантовый вычислительный процесс: $|\psi_{fin}\rangle = U|\psi_{in}\rangle$, где вектор (волновая функция) $|\psi_{in}\rangle$ задает начальные условия вычислений (решаемой проблемы), а $|\psi_{fin}\rangle$ отражает результат вычислений за счёт действия оператора U на начальное состояние $|\psi_{in}\rangle$.

На рис. 7 показана типовая структура КА.

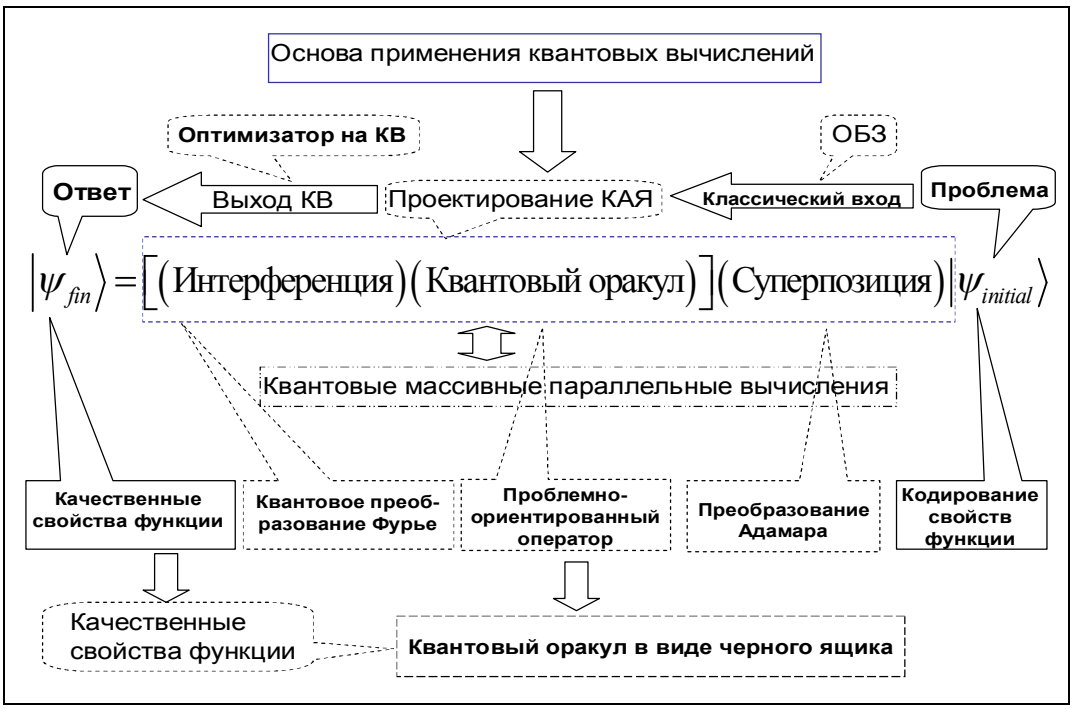

Рис. 7. Обобщенная структура КА

Выбирая различный вид оператора U (в частности, Гамильтониан), можно сформировать различные модели квантовых вычислений.

В общем виде модель квантовых вычислений [9] состоит из пяти этапов:

- подготовка начального (классического или квантового) состояния $|\psi_{in}\rangle$;
- выполнение преобразования Адамара H для начального состояния с целью подготовки состояния суперпозиции;
- применение запутанного оператора или оператора квантовой корреляции (квантового оракула) к суперпозиционному состоянию;
- применение оператора интерференции;
- использование оператора измерения для результата квантовых вычислений $|\psi_{fin}\rangle$.

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 не разрешимых на классическом уровне проблем, т.е. эффективно решаемые с помощью применения КА, для которых не существует ни одного классического (рандомизированного) алгоритма.

На рис. 8 приведено сравнение операторов ГА и КА.

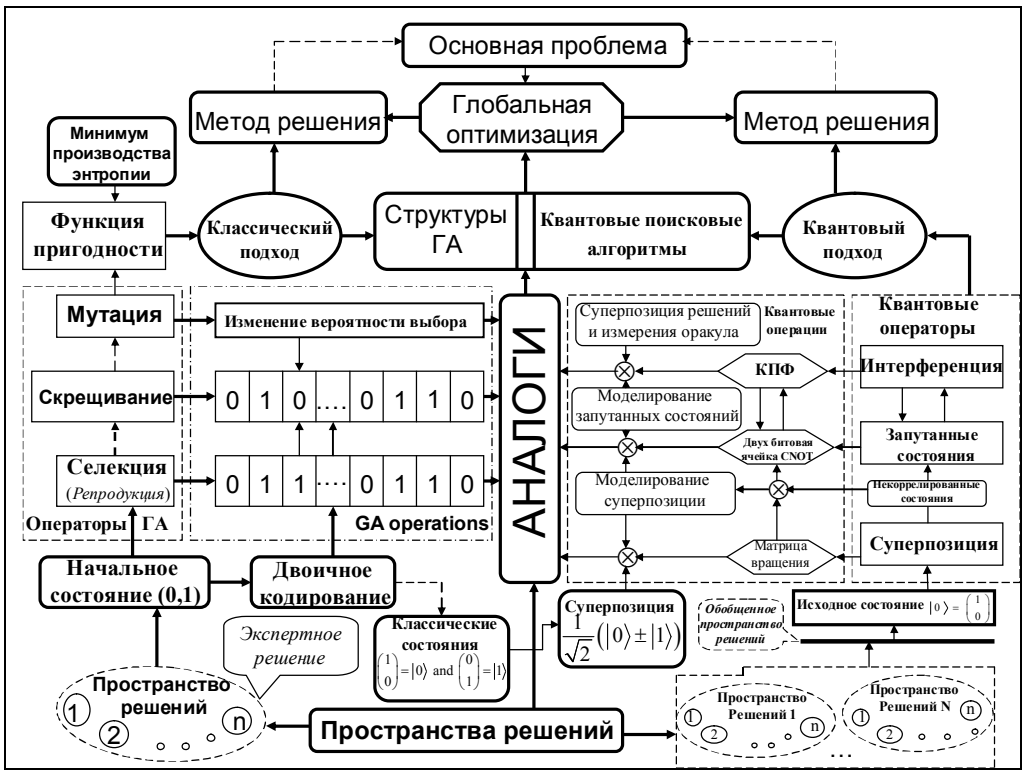

Рис. 8. Сравнение структур ГА и КА

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).

Аналоги мягких вычислений и квантовых вычислений приведены на рис. 9.

Рис. 9. Аналоги мягких и квантовых вычислений

Дополнительно к отмеченным вычислительным ресурсам, квантовая корреляция рассматривается как новый физический вычислительный ресурс, позволяющий резко увеличить успешный поиск решений проблем ранее не рассматриваемых в классической области вычислений.

К таким проблемам относятся: телепортация, сверхплотное кодирование, передача данных по квантовым каналам связи с повышенным уровнем секретности и защиты (от несанкционированного доступа или подслушивания), коррекция квантовых кодов с заданным уровнем толерантности и др. [10].

Таким образом, КА основаны на физических законах теории квантовых вычислений [4, 9], а именно в вычислениях участвуют унитарные, обратимые квантовые операторы. В общем виде КА состоит из трёх основных унитарных операций: суперпозиция; квантовая корреляция (квантовый оракул или запутанные операторы) и интерференция. Четвёртый оператор, оператор измерения результатов квантовых вычислений, является необратимым (классическим).

Квантовые вычисления, основанные на перечисленных типах операторов, относятся к новому виду интеллектуальных вычислений [2].

Классификация КА и их применение в задачах управления отражены рис. 10.

С точки зрения функциональных возможностей КА классифицируются (рис. 10) на две группы: алгоритмы принятия решений и поисковые алгоритмы.

В квантовых вычислениях в первую очередь интересуются качественными свойствами функции, кодируя их в начальных квантовых состояниях. Для поиска решения с помощью КА целенаправленно изменяют исходную суперпозицию начальных состояний, применяя последовательно перечисленные типы квантовых операторов.

В этом случае может быть использован алгебраический формализм, который поддерживается абстрагированием логического вывода относительно квантовых эффектов и отображает важнейшие квантовые эффекты на программном уровне, устраняя трудность аппаратной реализации, такую как декогерентность.

Поэтому в квантовых вычислениях и моделях КА особую роль играет выбор квантовых операторов.

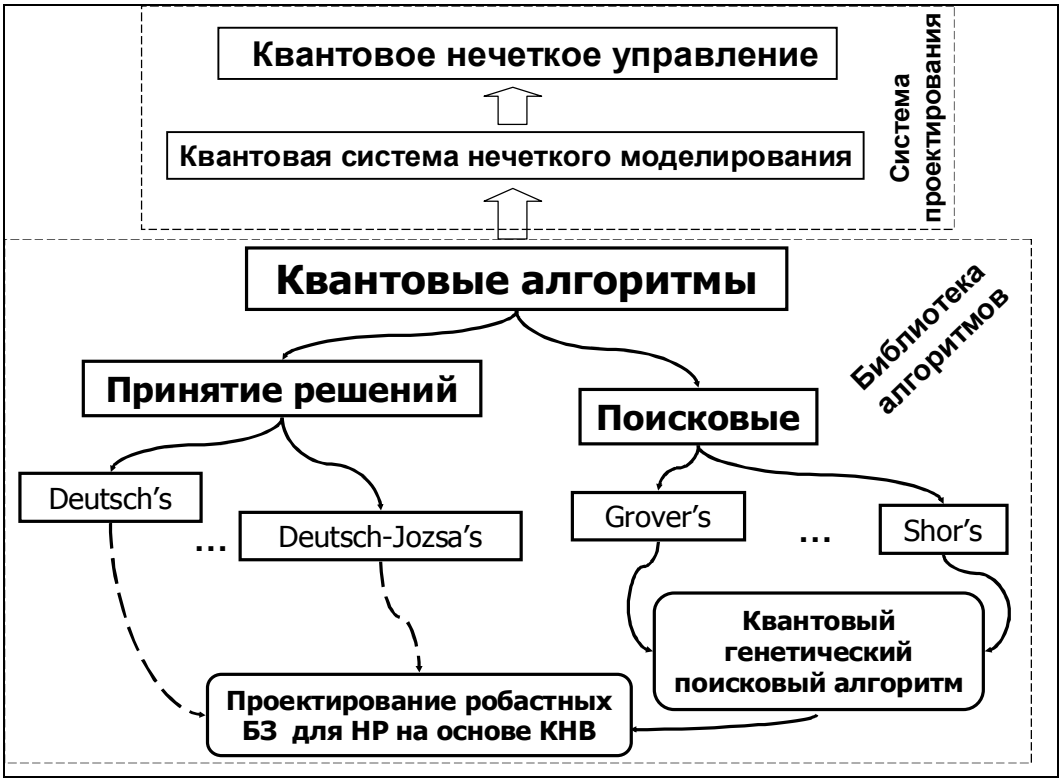

Рис. 10. Классификация КА

Рассмотрим кратко некоторые особенности квантовых операторов, составляющих основу КА, а также физическую интерпретацию результата действия от применения квантовых операторов.

3. Квантовые вычисления: примеры и свойства основных операторов

В качестве примера рассмотрим традиционный математический формализм описания моделей основных квантовых операторов с точки зрения второй (отмеченной выше) квантовой проблемы описания. Данный формализм может быть выражен на языке квантовых состояний или преобразований, но мы интересуемся также возможностью адекватного описания квантовых состояний и эффектов на языке логического вывода: применение традиционного формализма, его мощности и выразительности как квантовой системы нечёткого логического вывода [2, 10].

Пример 1: Квантовый бит

Классический бит может находиться в одном из двух состояний: 0 или 1. Таким образом, его физическое состояние можно представить как $b = a_1 0 + a_2 1$, которое имеет одну из форм: или $a_1 = 1$ и $a_2 = 0$, тогда $b = 0$, или $a_1 = 0$ и $a_2 = 1$, и тогда $b = 1$. В противоположность состояние квантового бита $|\psi\rangle$ задается вектором в двухмерном комплексном векторном пространстве. Здесь вектор имеет две компоненты, и его проекции на базисы векторного пространства являются комплексными числами. Квантовый бит ψ представляется (в обозначениях Дирака в виде кет-вектора) как $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ или в векторном обозначении $|\psi\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}$, $\langle\psi| = [\alpha\ \beta]^T$ (бра-вектор). Если $|\psi\rangle = |0\rangle$, то $|0\rangle = \begin{bmatrix}1\\ 0\end{bmatrix}$. Амплитуды α и β – комплексные числа, для которых выполнено следующее условие: $\alpha\alpha^* + \beta\beta^* = 1$, где «*» операция комплексного сопряжения; $|0\rangle$ и $|1\rangle$ образует пару ортонормальных базисных векторов, называемых состоянием вычислительного базиса. Если α или β принимают нулевые значения, то ψ определяет классическое, чистое состояние. В противном случае говорят, что ψ находится в состоянии суперпозиции двух классических базисных состояний. Геометрически квантовый бит находится в непрерывном состоянии между $|0\rangle$ и $|1\rangle$, пока не производятся измерения его состояния. Понятие амплитуды вероятностей квантового состояния является комбинацией концепции состояния и фазы. В этом случае геометрическое представление кубита имеет более общий вид:

$$|\varphi\rangle = e^{j\gamma}\left[\cos\left(\frac{\alpha}{2}\right)|0\rangle + e^{j\beta}\sin\left(\frac{\alpha}{2}\right)|1\rangle\right],$$

где $\gamma, \alpha, \beta \in R$. Рис. 11 показывает геометрическую природу кубита на сфере Блоха.

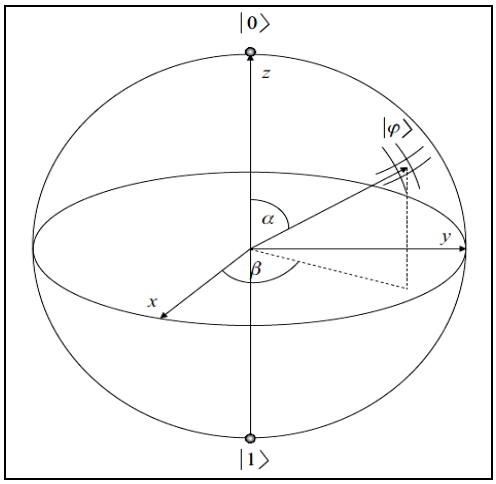

Рис. 11. Сфера Блоха

В случае, когда система состоит из двух квантовых битов, она описывается как тензорное произведение. Например, в обозначениях Дирака двухквантовая бит-система задается, как:

$$\left|\psi_1\psi_2\right\rangle = \alpha\gamma\left|00\right\rangle + \alpha\delta\left|01\right\rangle + \beta\gamma\left|10\right\rangle + \beta\delta\left|11\right\rangle.$$

Число возможных состояний комбинированной системы возрастает экспоненциально при добавлении квантового бита. Это приводит к проблеме оценки квантовой корреляции, которая присутствует между квантовыми битами в составной систем.

Примечание. С точки зрения теории информации, в квантовом бите содержится точно такое же количество информации, как и в классическом бите, несмотря на бесконечное множество виртуальных состояний квантового бита. Квантовый бит может быть описан бесконечным числом суперпозиций классических состояний, но из-за необратимого характера процесса измерения можно извлечь только простой классический бит информации из одного среди возможных состояний. При этом остальные виртуальные состояния разрушаются, и происходит потеря информации. Основанием для данного утверждения (в квантовом бите содержится не больше количества информации, чем в классическом бите) является тот факт, что информация извлекается в результате физического процесса измерений. За счёт измерения квантового бита происходит изменение его состояния и в результате он переходит в одно из возможных базисных состояний. Каждый квантовый бит существует в двухмерном пространстве, его измерение ассоциируется с соответствующим базисом и выражает результат только в одном из двух состояний, т.е. один из базисных векторов ассоциирован с данным измерительным прибором.

Таким образом, как и в классическом случае, при измерении квантового бита существует только два возможных результата. Поскольку измерение изменяет состояние квантового бита, то невозможно осуществить одновременно регистрацию состояния в двух различных базисах. При моделировании классической динамической системы, её состояние можно измерить на первом этапе в одном базисе, затем – на втором этапе в другом базисе. В истинно квантовой системе подобное невозможно, так как при измерении происходит разрушение волновой функции, описывающей состояние квантового бита.

Более того, квантовые состояния в истинно квантовой системе невозможно клонировать, т.е. существуют объективные физические ограничения, в силу которых не удаётся проводить измерение двумя разными путями, используя, например, копирование квантового бита и его регистрацию в различных базисах [4]. В отличие от квантового бита состояние классического бита можно копировать и осуществлять измерение в различных вычислительных базисах. Неизвестный квантовый бит нельзя «расщепить» на взаимно дополняющие части [10], т.е. содержащаяся в неизвестном состоянии квантового бита информация неразделима.

Таким образом, в квантовой механике допустимы операции, невозможные в классической механике. И, наоборот, в классической механике существуют операторы решения задач, недопустимые в квантовой механике.

Пример 2: Формирование состояния суперпозиции с помощью оператора Адамара (Уолша-Адамара)

Существование состояния суперпозиции и эффекта измерения квантового состояния физически означает, что присутствует *скрытая от наблюдателя информация*, которая содержится в замкнутой квантовой системе (до момента ее возбуждения от внешнего возмущения) в виде наблюдения квантового состояния. Система остается замкнутой до взаимодействия с внешней средой (т.е. до действия наблюдения системы).

Важнейшим в этом случае является следующий вопрос: как эффективно использовать скрытую в суперпозиции информацию?

В традиционном формализме квантовых вычислений квантовые операторы описываются в эквивалентной матричной форме. Умножение матрицы оператора на вектор состояния означает действие операции на исследуемую систему.

Например, действие матрицы Адамара (H) на систему $|\psi\rangle = |0\rangle$ может быть представлено как

$$H|\psi\rangle = H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\ 0\end{bmatrix} + \begin{bmatrix}0\\ 1\end{bmatrix}\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right).$$

Аналогично, $H|\psi\rangle = H|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix} = \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\ 0\end{bmatrix} + \begin{bmatrix}0\\ -1\end{bmatrix}\right) = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$, т.е. преобразование Адамара порождает состояние квантового бита в виде суперпозиции двух классических состояний. Формирование суперпозиции с эквивалентными амплитудами вероятностей – важный шаг для многих КА.

Применяя $H^{\otimes n}$ на соответствующих базисных состояниях $|x\rangle \in \mathrm{H}_n$, $x \in \{0,1\}^n$, получим в результате эквивалентную форму преобразования Адамара:

$$H|x\rangle = \frac{1}{\sqrt{2}}\sum_{z=0,1}(-1)^{x\cdot z}|z\rangle, \text{ где } x\cdot z = x_1z_1 + \ldots + x_nz_n \text{ для } x=0 \text{ и } x=1.$$

Таким образом, суперпозицию с эквивалентными амплитудами вероятностей $\frac{1}{\sqrt{2^n}}$ для каждого базисного состояния получают применением оператора $H^{\otimes n}$ к состоянию $|0\rangle$. Значение состояния суперпозиции для теории вычислительных процессов становится более понятным, если интерпретировать результирующее суперпозиционное состояние как набор 2^n классических траекторий (путей) вычислений с эквивалентными весами, по которым квантовый компьютер физически проводит вычисления параллельно. Более того, тензорное произведение является обобщением билинейной операции произведения матриц: $A\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}A\times a & A\times b\\ A\times c & A\times d\end{pmatrix}$ и имеет следующие свойства:

$(a)\ Ранг(A\otimes B) = Ранг(A) + Ранг(B)$;

$(b)\ Размерность(A\otimes B) = Размерность(A)\times Размерность(B)$.

Таким образом, с помощью тензорного произведения можно экспоненциально расширить рабочее пространство вычислений и сформировать *базис для параллельных вычислений*. В этом смысле суперпозиция выступает как первый этап на пути организации *квантового параллелизма.*

Рассмотрим пример классической логической операции, содержащей (или состоящей) из *внутренних* квантовых операций.

4. Эффективное моделирование КА на классических компьютерах

Запутанные состояния в квантовых вычислениях рассматриваются как дополнительный физический ресурс, позволяющий существенно увеличить расчетную мощность по сравнению с классическими моделями вычислений. Число параметров, необходимых для описания незапутанных (чистых) состояний в заданном Гильбертовом пространстве H_n (представленных как тензорное произведение квантовых битов), возрастает только линейно с увеличением числа n квантовых битов. Однако для описания общего вида состояния (незапутанного или запутанного) требуется экспоненциальное число $\left(2^n\right)$ векторных коэффициентов.

Поэтому вопрос о физическом ресурсе квантовых вычислений не имеет простого ответа.

Данная проблема проанализирована в деталях с общих позиций теории квантовых вычислений в [10]. Было отмечено, в частности, что для КА (оперирующих чистыми состояниями) для повышения эффективности по сравнению с классическими аналогами с увеличением размерности входных квантовых битов требуется неограниченное число перепутанных состояний. Более того, эффективно КА можно моделировать классическим инструментарием (классическими алгоритмами) только при наличии малого количества квантовой корреляции и фиксированном уровне толерантности вычислительных операций в КА. Было показано, как можно эффективно классическими алгоритмами моделировать КА со сравнительно слабой квантовой корреляцией. Вычислительная стоимость возрастает линейно с числом входных квантовых бит и экспоненциально – с увеличением требуемого количества квантовой корреляции. Независимое обобщение такого подхода приведено в [6, 8] и разработано соответствующее программно-аппаратное обеспечение для эффективного моделирования КА на классических компьютерах.

Изложенные аргументы и результаты свидетельствуют о предпочтительной роли квантовой корреляции как движущей силы квантовых вычислений (на чистых состояниях эволюции квантовой динамики).

Пример 3: Моделирование квантовой интерференции с помощью квантового преобразования Фурье (КПФ)

С целью повышения вероятности измерения и извлечения искомого (маркированного) решения основной единой идеей в процессах проектирования различных моделей КА служит использование явления конструктивной/деструктивной интерференции в качестве инструментария извлечения результатов эффективных вычислений КА. Для увеличения вероятности извлечения «успешного» решения применяется конструктивная интерференция, а для редукции «плохих» решений – деструктивная интерференция. Конструктивный (деструктивный) эффект можно проиллюстрировать наглядно на примере применения преобразования Адамара к состояниям $\{|0\rangle,|1\rangle\},\left\{|\pm\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle\pm|1\rangle\right)\right\}$. Очевидно, что $H|0\rangle=|+\rangle$ è $H|1\rangle=|-\rangle$, т.е. воспроизводится состояние суперпозиции классических состояний в виде квантовых бит. При этом применение преобразований Адамара к состояниям $|0\rangle$ и $|1\rangle$ порождает состояния с одинаковым распределением вероятностей. Поскольку состояние $|+\rangle$ является суперпозицией обоих классических состояний $|0\rangle$ и $|1\rangle$, то при повторном применении преобразовании Адамара к $|+\rangle$ классическая модель логического вывода (модель Колмогорова) предполагает одинаковую вероятность результирующего классического состояния (принцип сохранения вероятности). Однако вследствие оперирования в квантовых вычислениях с понятием амплитуды вероятностей применение преобразования Адамара к состоянию $|+\rangle$ дает следующий результат:

$$H|+\rangle=\frac{1}{\sqrt{2}}\left(|+\rangle+|-\rangle\right)=|0\rangle.$$

Таким образом, проявился эффект интерференции между вероятностями обоих классических состояний. С одной стороны, интерференция (в силу своего физического характера) усилила амплитуду вероятности одного ($|0\rangle$) классического состояния (конструктивная интерференция) и ослабила существенно (до нуля) амплитуду вероятности другого ($|1\rangle$) классического состояния (деструктивная интерференция). Действуя на суперпозицию возможных решений, интерференция реализует процесс формирования финальной фазы квантовых вычислений и является (так же, как и квантовая корреляция) физическим ресурсом усиления квантовых вычислений. Например, применяя преобразование $H^{\otimes n}$ к состоянию $|\psi'\rangle$, получим в результате квантовое состояние вида $\frac{1}{2^n}\sum_{z\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot z+f(x)}|z\rangle$, служащее основой для проектирования КАЯ, например, при решении проблемы Deutsch-Jozsa.

В модели КА Шора при факторизации произведения на простые числа интерференцию обеспечивает оператор КПФ: оператор $QFT_n \otimes I_n$ действует на каждый базисный вектор, принадлежащий линейной комбинации исходного вектора $|\psi\rangle$. Это означает, что любой вектор в такой комбинации воспроизводит суперпозицию базисных векторов. Комплексные весовые коэффициенты базисных векторов равны по модулю (т.е. амплитуды вероятностей равны), но имеют различные фазы. Каждый базисный вектор является взвешенной суммой амплитуд вероятностей, полученных из разных последовательностей базисных векторов. Данная сумма может увеличивать или уменьшать результирующую амплитуду вероятностей. Так как этот эффект подобен эффекту интерференции классических волн, то говорят, что оператор:

$$\left[QFT_n\right]_{ij}=\frac{1}{\sqrt{2^n}}\exp\left\{2\pi J\left[\frac{(i-1)(j-1)}{2^n}\right]\right\}$$

играет роль оператора интерференции. С математической точки зрения, когда оператор $QFT_n \otimes I_n$ действует на состояние, то все столбцы результирующей матрицы задействованы при вычислении и интерференция осуществляется между весовыми коэффициентами из разных последовательностей базисных векторов [10].

Пример 4: Квантовый массивный параллелизм и модели вычислений с квантовым оракулом

Рассматриваемый эффект является одним из важнейших в квантовых вычислениях и используется (так же как и суперпозиция) во многих моделях КА. Он особенно широко применяется в различных моделях «чёрного ящика» или «квантового оракула» при проектировании разного класса КА [4], например, для вычислений функций следующего вида: $g:\{0,1\}^n\to\{0,1\}^m$. Поскольку отображение $x\to(x,g(x)),\ x\in\{0,1\}^n$ обратимо, то существует унитарное преобразование U_g, эффективно моделируемое классическими вычислениями $(x,g(x))$ так, что $|x,y\rangle\to|x,y\oplus g(y)\rangle$ для некоторого $y\in\{0,1\}^m$, где $\oplus$ – операция сложения по модулю 2. При этом дополнительные квантовые биты, необходимые для реализации обратимых схемных преобразований, здесь не рассматриваются. Преобразование U_f, описывающее «чёрный ящик» (как частный случай U_g), представляет унитарное преобразование в виде Булевой функции $f:\{0,1\}^n\to\{0,1\}$. Если $|y\rangle$ – начальное состояние $|0\rangle$, то после применения преобразования U_f выход преобразования $f(x)$ будет $|x,f(x)\rangle$.

Физический смысл *квантового массивного параллелизма* заключается в наличии эффекта параллелизма вычислений после использования преобразования U_f для суперпозиционного состояния, представляющего различные значения x. Так, применяя U_f к состоянию $|x,y\rangle=|\psi,0\rangle$,

$|\psi\rangle = H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z\rangle$, имеем в результате $U_f|\psi,0\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z, f(z)\rangle$, т.е. суперпозицию всех возможных значений вычисляемой функции.

Таким образом, применение *только одного* шага для оценки значений функции $f(x)$ является достаточным для вычисления параллельно значений $f(x)$ от всех возможных входных аргументов x. Данный эффект эквивалентен применению свойств «чёрного ящика» (одноразовое применение внутренней квантовой схемы). Однако в действительности только одно значение функции $f(x)$ доступно при измерении результата вычисления $f(x)$ в суперпозиции возможных состояний, так как из-за эффекта разрушения состояний в суперпозиции доступно только одно случайно измеренное состояние дано ниже.

С математической точки зрения, объединённые квантовые состояния формируются с помощью тензорного (кронекерского) произведения на гильбертовых пространствах базисных состояний. Результатом такой операции выступает квантовый регистр. Включение в вычислительный процесс квантовой корреляции приводит к увеличению скорости и достоверности поиска решений на основе соответствующего КА, а благодаря наличию данного физического вычислительного ресурса многие вычислительные операции можно выполнять параллельно.

Поэтому квантовая корреляция в этом смысле демонстрирует новый специальный физический ресурс квантовых вычислений.

Квантовая алгебра позволяет формализовать некоторые важные свойства квантовых эффектов путем включения их описания в определенные программные атрибуты. Тогда программный инструментарий включает механизм компактного описания программных атрибутов и эффективного логического вывода на большом количестве квантовых битов и базисных состояний с высоким уровнем квантовой корреляции, а также обладает дескриптивным представлением физических свойств описываемых квантовых операторов [10].

Данный подход является аппаратно независимым и может быть использован в качестве модели квантовых вычислений или базиса языка квантового программирования.

На рис. 12 показаны типовые свойства и проблемы КА и квантовой информации.

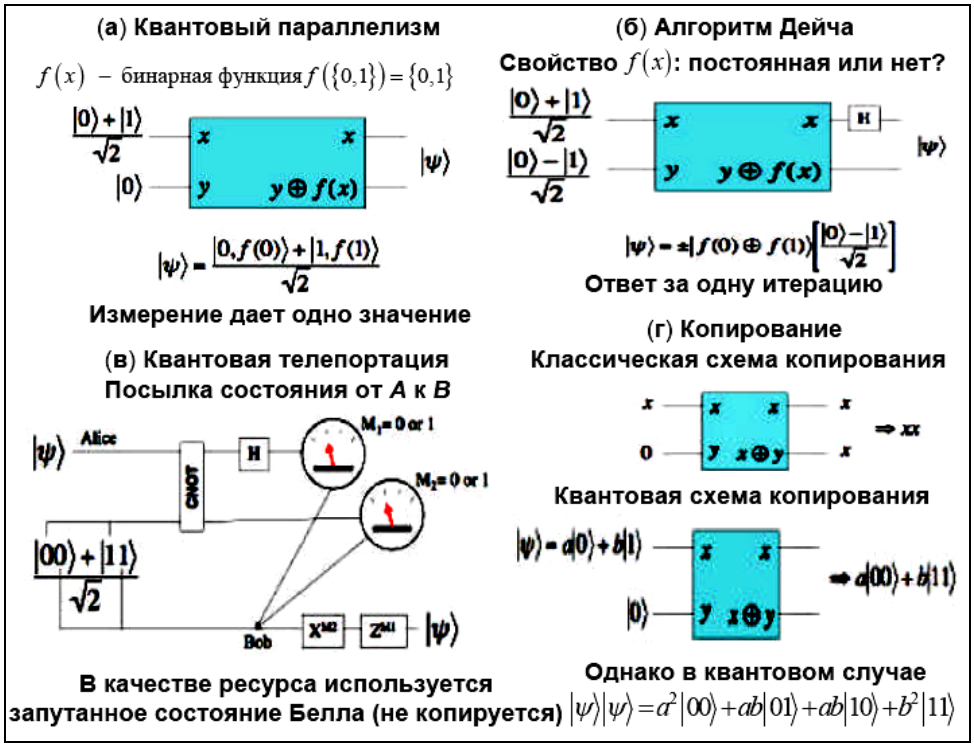

Рис. 12. Типовые свойства и проблемы КА и квантовой информации

Выше рассмотрены примеры, иллюстрирующие основные квантовые операторы и их свойства. Поэтапное применение КАЯ и измерение результатов вычислений после применения квантовых операторов в КАЯ позволяет реализовать КА на классическом компьютере.

5. Общая структура квантовых алгоритмов и КАЯ

Проблемы, решаемые при помощи квантовых алгоритмов, могут быть представлены в следующей форме:

Вход	Функция $f:\{0,1\}^n \to \{0,1\}^m$
Задача	Найти определенное качественное свойство функции f

Основой квантовых вычислений, как отмечалось выше, являются три оператора, действующих на квантовые когерентные состояния: суперпозиция, запутывание (смешивание состояний) и интерференция.

Оператором суперпозиции является тензорное произведение *n* операторов Адамара *H* и *m* операторов тождественного преобразования *I*. Полученный таким образом оператор действует на первый регистр (на первые *n* кубитов), создавая их суперпозицию, и действует тождественно на второй регистр (последние *m* кубитов), оставляя его без изменений.

Оператором запутывания является оператор U_F, полученный в результате работы блока кодирования. Как уже отмечалось выше, его вид зависит от свойств исходной функции f.

Оператор интерференции зависит от рассматриваемого алгоритма. Оператором интерференции могут выступать, например, квантовое преобразование Фурье (алгоритм Шора) или также оператор Адамара и др.

Система моделирования квантовых вычислений основана на методе КАЯ. Процесс проектирования КАЯ включает в себя матричную форму представления трех отмеченных выше операторов: суперпозицию (Sup), квантовую корреляцию – запутанные состояния (U_F), и интерференцию (Int). В общем виде структура КАЯ можно представить в виде

$$\hat{E}\grave{A}\beta = \left[\left(Int \otimes {}^n I\right)\cdot U_F\right]^{h+1}\cdot\left[{}^n H \otimes {}^m S\right], \qquad (1)$$

где I – идентичный оператор; символ $\otimes$ означает тензорное произведение; *S* эквивалентно *I* или *H* и зависит от описания проблемы. Одной из особенностей процесса проектирования в (1) является выбор проблемно-зависимого оператора запутанных состояний U_F, физически описывающего качественные особенности функции f.

На рис. 13 показана структура КАЯ, соответствующая выражению (1).

Входом КА всегда является бинарная функция f. Эта функция представляется в качестве отображения, определяющего изображение каждой входной бинарной строки. На первом этапе, функция f кодируется в виде унитарного матричного оператора U_F, зависящего от свойств функции f. Полученный матричный оператор U_F включается в структуру квантовой ячейки G, унитарной матрицы, чья структура зависит от матрицы U_F и от проблемы, которую алгоритм должен решить. Квантовая ячейка является основой КА. В любом КА, квантовая ячейка действует на начальный канонический базисный вектор (мы можем всегда выбирать одинаковый) с целью создания комплексной линейной комбинации (суперпозиции) базисных векторов в качестве выхода.

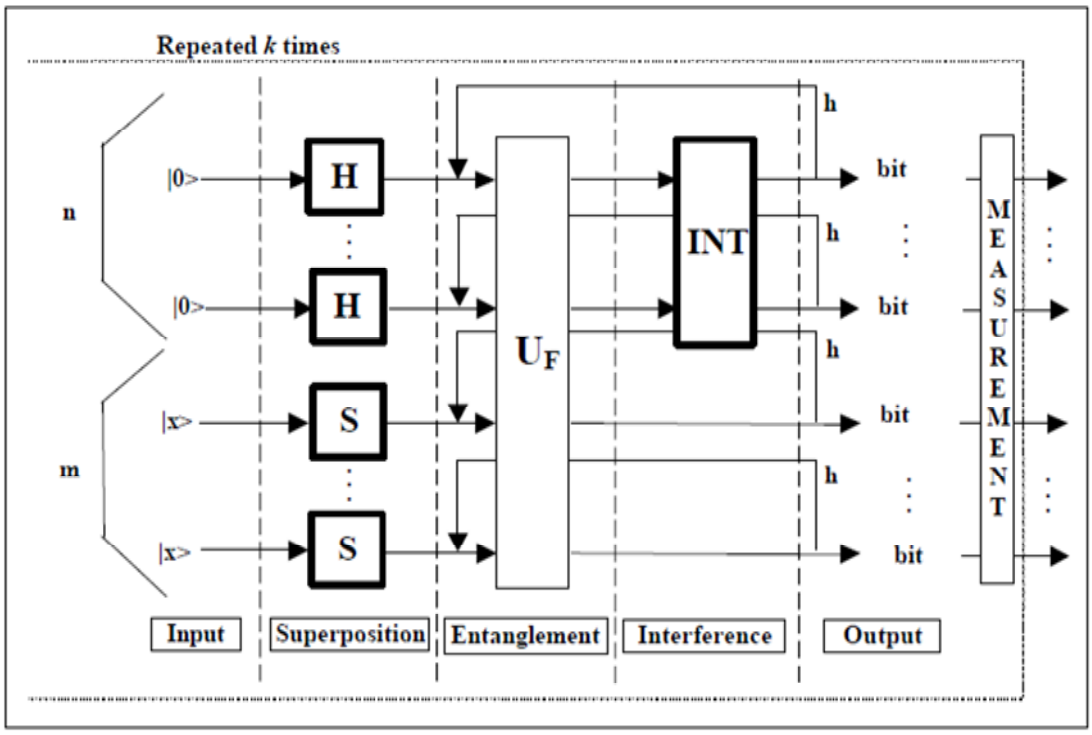

Рис. 13. Структура обобщенной КАЯ

На рис. 14 изображена общая схема моделирования КА на классическом компьютере.

Данная суперпозиция будет содержать *всю информацию*, необходимую для ответа на начальную проблему. После создания суперпозиции, проводится операция измерения с целью извлечения информации о решении проблемы. Вероятность любого из базисных векторов быть измеренным зависит от его комплексного коэффициента (амплитуды вероятности) с каким он входит в суперпозицию. Поочередное применение квантового оператора и измерение результата образуют квантовый блок. Квантовый блок выполняется k раз с целью получения набора базисных векторов. Так как измерение не является детерминированной операцией, то полученные базисные векторы необязательно будут одинаковы, и каждый из них будет содержать лишь часть информации, необходимой для решения проблемы.

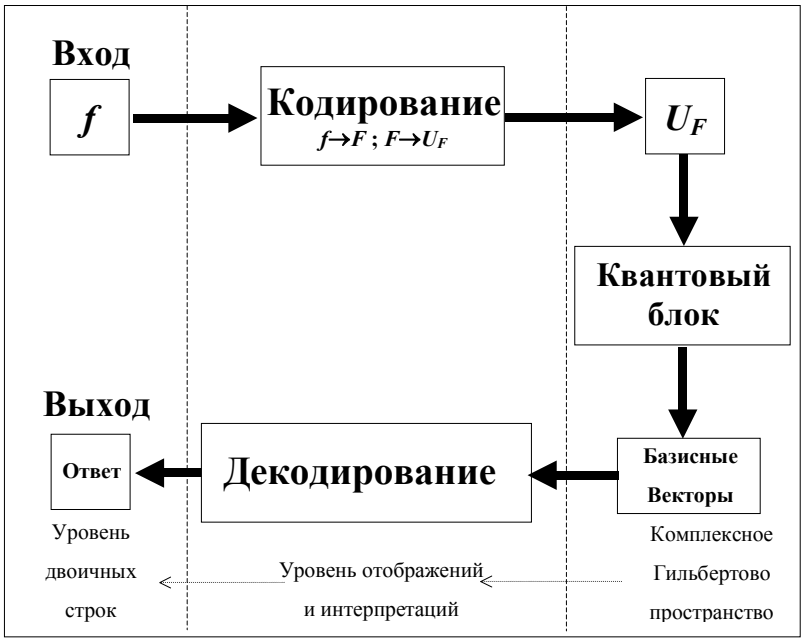

Рис. 14. Схематическая диаграмма КА

Завершающей фазой КА является интерпретация набора полученных базисных векторов с целью получения правильного ответа на начальную задачу с определенной долей вероятности.

Рассмотрим более подробно основные шаги КА.

Кодирование

Диаграмма работы блока кодирования представлена на рис. 15.

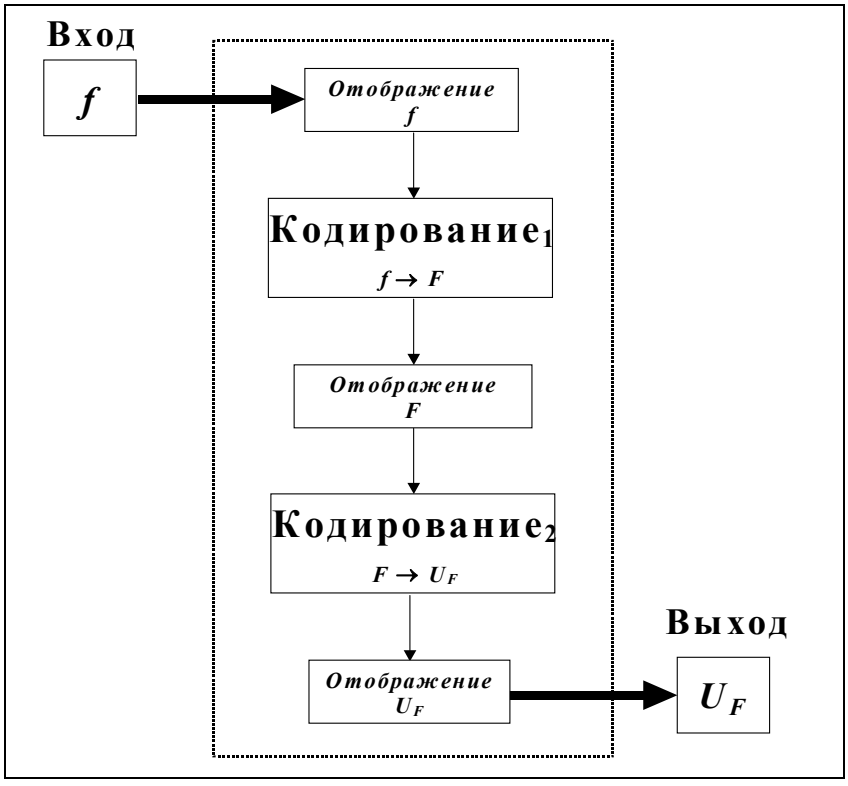

Рис. 15. Диаграмма блока кодирования

Шаг 1. Таблица отображения функции $f:\{0,1\}^n \to \{0,1\}^m$ преобразуется в таблицу отображения унитарной функции $F:\{0,1\}^{n+m} \to \{0,1\}^{n+m}$, такой что:

$$F(x_0,...,x_{n-1},y_0,...,y_{m-1}) = (x_0,...,x_{n-1},f(x_0,...,x_{n-1}) \oplus (y_0,...,y_{m-1})).$$

Необходимость данного преобразования связана с требованием унитарности оператора U_F. Оператор U_F является обратимым, следовательно, он не может отображать два разных входа в одинаковые выходные значения. Так как данный оператор является матричным представлением функции F, функция F должна быть обратимой функцией. Если мы опустим создание функции F и напрямую создадим матричный оператор U_f, то он не будет являться унитарным, так как функция f необязательно обратима. Таким образом, обратимость выполняется за счет увеличения числа бит и рассмотрением функции F вместо функции f. В любом случае, функция f может быть всегда получена из F вычислением последних m значений при $(y_0,...,y_{m-1}) = (0,...,0)$.

Шаг 2. Отображение функции F преобразуется в отображение U_F, согласно следующим ограничениям:

$$\forall s \in \{0,1\}^{n+m} : U_F[\tau(s)] = \tau[F(s)]$$

Таблица кодирования $\tau:\{0,1\}^{n+m} \to C^{2n+m}$, где C^{2n+m} есть результирующее Гильбертово пространство, определяется как:

$$\tau(0) = \begin{pmatrix}1\\0\end{pmatrix} = |0\rangle \quad \tau(1) = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle; \quad \tau(x_0,...,x_{n+m-1}) = \tau(x_0) \otimes ... \otimes \tau(x_{n+m-1}) = |x_0...x_{n+m-1}\rangle.$$

Шаг 3. Отображение U_F преобразуется в матричный оператор U_F, следуя следующему правилу:

$$\lfloor U_{F_{ij}} \rfloor = 1 \Leftrightarrow U_F|i\rangle = |j\rangle.$$

Данное правило легко понять, если рассмотреть $|i\rangle$ и $|j\rangle$ как вектор столбцы. Распределяя эти вектор столбцы по каноническому базису, U_F определяет перестановку рядов матрицы идентичности.

В общем виде, ряд $|j\rangle$ отображается в ряд $|i\rangle$.

Квантовый блок

Основой квантового блока является квантовая ячейка, зависящая от свойств матрицы оператора U_F. Матричный оператор U_F, являющийся выходом блока кодирования, в данной структуре является входом квантового блока рис. 16.

На первом этапе оператор U_F включается в более сложный оператор, квантовую ячейку G. Унитарная матрица G применяется k раз к начальному каноническому вектору $|i\rangle$ размерности 2^{n+m}. Результирующая комплексная линейная комбинация базисных векторов измеряется, производя один базисный вектор $|x_i\rangle$ как результат. Все измеренные базисные векторы $\{x_l,..,x_k\}$ собираются вместе. Полученный набор является выходом квантового блока.

Основной проблемой построения подобных алгоритмов является построение квантовых ячеек таким образом, чтобы они были способны извлекать требуемые свойства функции f и хранить их в наборе выходных векторов.

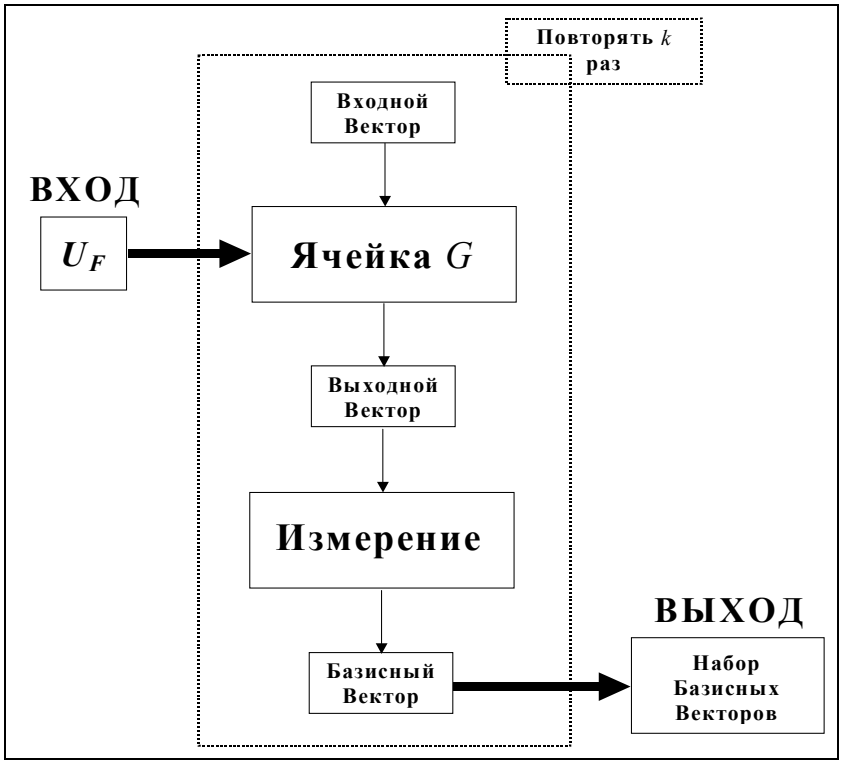

Рис. 16. Структура квантового блока, изображенного на рис. 14

Для представления квантовых ячеек будут использованы специальные диаграммы – «квантовые схемы», представленной на рис. 17.

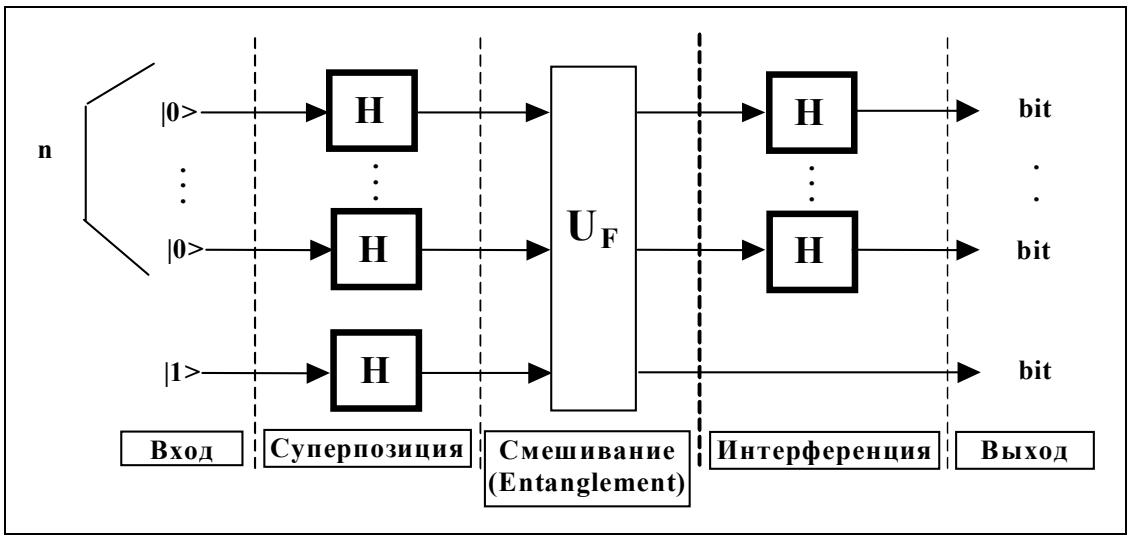

Рис. 17. Пример квантовой схемы

Каждый прямоугольник данной схемы ассоциируется с матрицей размерности $2^n \times 2^n$, где n – число линий, входящих и выходящих из прямоугольника. Например, прямоугольник обозначенный U_F, ассоциируется с матрицей U_F.

Квантовые схемы позволяют дать высокоуровневое представление квантовых ячеек. Используя правила преобразования, квантовые схемы можно преобразовывать в матричные операторы.

Одно из правил преобразования представлено рис. 18.

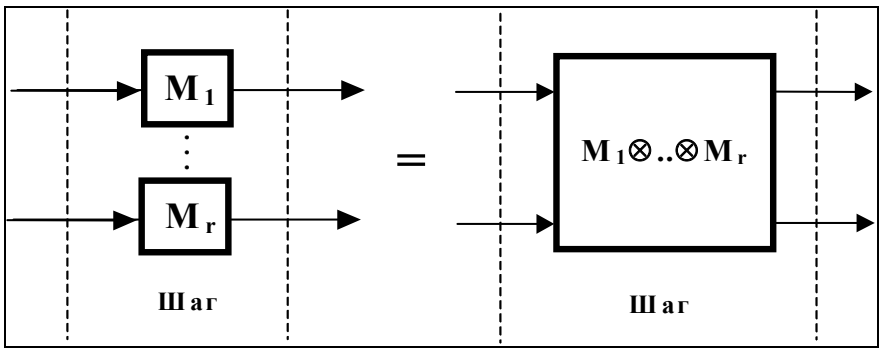

Рис. 18. Преобразование тензорного произведения

Декодирование результата

Блок декодера имеет функцию интерпретации базисных векторов, полученных после выполнения квантового блока. Декодирование базисных векторов заключается в их преобразовании в бинарные строки с последующим использованием этих строк в качестве коэффициентов некоторого уравнения, либо в случае прямого кодирования решения задачи, для извлечения ответа. Структура блока декодирования значительно зависит от характера решаемой задачи, и по существу является тем или иным классическим алгоритмом. Квантовый блок повторяет итеративно k раз квантовые операции с целью воспроизводства набора k базисных векторов, содержащих искомое решение.

Поскольку измерение является в общем случае недетерминированной операцией, то полученные в наборе базисные векторы не идентичны, и каждый из них кодирует часть информации, необходимой для решения исследуемой проблемы.

Последняя часть КА содержит блок интерпретации набора базисных векторов, позволяющий выделить конечное содержательное решение исследуемой проблемы с определенной вероятностью.

5.1. Особенности разработки моделей КА на основе КАЯ

Как отмечалось, фундаментальный результат теории квантовых вычислений заключается в установленной возможности погружать все КА в квантовые ячейки, реализуемые на универсальных типовых элементных схемах (типа «И», «ИЛИ», «НЕТ», «контролируемое НЕТ» и т.п.), которые используются в структуре классического компьютера. Данные ячейки описываются математически унитарными операторами, отражающими эволюцию вычислительного процесса. В теории квантовых вычислений показано также, что возможна реализация квантовых вычислений на основе классически эффективного симулятора.

Таким образом, метод проектирования КАЯ, разработанный в [10], можно применять для моделирования, например, процессов глобальной оптимизации БЗ в робастных структурах ИСУ, используя технологию квантовых вычислений, которая содержит такие инструментальные программные средства, как квантовый генетический поисковый алгоритм или квантовые обучающие процессы оптимизации (см. рис. 9).

Примечание. Задача оценки роли квантовых эффектов в КА и разработка самих моделей КА относится к классу проблем повышенной сложности. В квантовых вычислениях есть много технических трудностей, связанных с необходимостью манипуляции нетрадиционными свойствами квантовой информации. К ним относятся невозможность копировать квантовую информацию о неизвестном квантовом состоянии; разрушение ценной информации, содержащейся в суперпозиции, при измерении результата вычислений; оперирование с такими нестандартными для классической теории вычислений понятиями, как квантовая корреляция, относительная фаза или суперпозиция. Суперпозиция и квантовая корреляция (запутанные состояния) не имеют классических аналогов и составляют, как отмечалось выше, базис мощности квантовых вычислений. Фаза имеет традиционную интерпретацию непрерывной величины, но в квантовых вычислениях базовая единица фазы играет дополнительную роль различения квантовых состояний промежуточных вычислений без возможности копирования. При этом описательное представление квантовых операторов указывает на необходимость

включения искомых, качественных свойств функций в процесс приготовления исходной суперпозиции начальных квантовых состояний как потенциальных решений.

Многие из наиболее популярных моделей квантовых вычислений являются прямыми квантовыми обобщениями соответствующих конструкций классических вычислений. К ним относятся квантовая машина Тьюринга, квантовые ячейки и случайные блуждания. Данные модели основаны на унитарной эволюции (как базисного механизма информационных процессов). Только в конце вычислений проводятся конечные измерения, в результате чего квантовая информация отображается в классическую информацию (для считывания результата вычислений в классическом виде).

При этом рассматриваются две основные идеи. Первая из них связана с усилением амплитуд вероятностей искомого решения, вторая утверждает, что классические вычисления можно моделировать на квантовом компьютере. Таким образом, вместо описания КА можно оперировать соответствующим классическим алгоритмом, который дает решение с заданной вероятностью ошибки. Затем классический алгоритм трансформируется в КА и применяется процедура усиления амплитуды вероятности искомого решения в КА.

Другие модели квантовых вычислений основаны на применении только необратимых измерений (one-way quantum computing), на теории скрытых параметров (hidden variable), адиабатические КА (adiabatic quantum computing). Существует также модель квантовых вычислений на «дуальном» квантовом компьютере, использующая корпускулярные и интерференционные свойства квантовых систем (duality quantum computer) и т.п.

Данные модели исследованы в [2] с точки зрения квантовой теории оптимальных процессов управления.

5.2. Особенности практической реализации КА на классическом компьютере

Одной из основных задач практического применения разработанной информационной технологии проектирования КА на основе КАЯ является использование функциональных возможностей (существующих или перспективных) классических персональных компьютеров с последующей коммерциализацией интеллектуального продукта (в частности, объединение с фирмами-разработчиками в области программно-аппаратной поддержки квантовых мягких вычислений). Возможность моделирования на классическом персональном компьютере КА открывает большие перспективы коммерциализации разработанного наукоёмкого интеллектуального продукта и расширяет области инженерного менеджмента основанного на знаниях в реализации стандартной программно-аппаратной поддержки.

Сложность создания такого наукоёмкого интеллектуального продукта заключалась в существовании в теории квантовых вычислений обобщенного тезиса Черча-Тьюринга. Следствие данного тезиса утверждает, что для решения квантовых проблем классического компьютера последовательного действия (с архитектурой фон Неймана) недостаточно и необходим квантовый компьютер для реализации квантовых параллельных массивных вычислений (на основе введения принципа суперпозиции, т.е. новых операторов, отсутствующие в классическом компьютере). Более того, Р. Фейнман в 1982г. показал, что при решении квантовых задач сложность решения на классическом компьютере возрастает экспоненциально в зависимости от входных переменных, т.е. практически решить задачу невозможно и необходимо применять квантовый компьютер.

Проблема казалась ясной, и применению классических компьютеров оставлялась классическая область вычислительных задач. Однако разработанный авторами данной работы алгоритмический подход [3] только на первый взгляд приводил к противоречию с обобщенным тезисом Черча-Тьюринга и выводами Манина-Фейнмана. Для доказательства данного утверждения необходимо было провести дополнительный анализ структуры КА и его составляющих операторов с целью разработки нового алгоритма моделирования самих квантовых алгоритмов, позволяющего преодолеть «проклятие размерности» и ускорить моделирование исходного квантового алгоритма на персональном компьютере [6, 7]. В этом случае следствие и обобщенный тезис Черча-Тьюринга не нарушаются. В результате создана возможность решать практические задачи ограниченной размерности (зависящей от объема памяти персонального компьютера), не дожидаясь появления квантового компьютера [8].

Ниже отметим некоторые основные подходы в эффективном моделировании КА, которые будут рассмотрены в последующих частях данной статьи. Эффективное применение разработанного программного продукта моделирования квантовых алгоритмов на классическом компьютере можно найти в [6].

5.3. Основные подходы моделирования КА

Сложность моделирования КА на классическом компьютере состоит в том, что ядром КА являются квантовые ячейки и унитарные операторы. В практическом представлении квантовая ячейка является унитарной матрицей с особой структурой. Размерность, которой возрастает экспоненциально с линейным увеличением размерности квантовой системы. Таким образом, смоделировать квантовый алгоритм, использующий более чем 30-35 кубитов, представляется практически не возможным [6].

Известны следующие подходы, позволяющие эффективно моделировать КА:

- матричный подход;
- алгоритмический подход, когда элементы матриц вычисляются «по требованию»;
- проблемно-ориентированный подход;
- подход, использующий упрощенные квантовые операторы.

В таблице 1 приведены сводные результаты разных подходов и различных технологий моделирования квантовых алгоритмов на классическом компьютере [7].

Таблица 1. Результаты разных подходов моделирования КА

Подходы	Аппаратные характеристики	Максимальное количество кубитов	Время выполнения одного шага, с
Матричный подход, основанный на распределенных вычислениях	*Sun Enterprise* 4500, 8 процессоров 400 МГц, 10 Гб ОЗУ, 64-разрядная ОС	30	395,81
Программный подход, основанный на каскадном соединении матриц	PIV 1,7 ГГц, 1 Гб ОЗУ, *Linux*, *Matlab*	23	44,6
QuIDD-подход[1]	*Dual AthlonMP* 1,2 ГГц, 1 Гб ОЗУ, C++	20	< 1
Аппаратный подход	Аналоговые цепи	3	<< 1
Аппаратный подход	Аналоговые цепи, устройства внешнего монтирования	6	<< 1
Программный подход, основанный на матричных операторах	PIII, 800 МГц, 512 Мб ОЗУ, *Matlab*, *Windows* 2000	11	1500
Программный подход, основанный на векторизованных алгоритмах	PIII, 1 ГГц, 512 Мб ОЗУ, *Matlab*, *Windows* 2000	24	50

[1] *QuIDD – Quantum Information Decision Diagram* – квантово-информационная схема принятия решения.

Первый подход (матричный) основан на представлении матричных квантовых операторов. Этот подход является более стабильным и точным, но требует много памяти компьютера для расположения матричных операторов. Поскольку размер операторов растет в геометрической прогрессии, то возможно моделировать алгоритмы с небольшим числом кубитов.

Второй подход не требует выделения памяти компьютера для квантовых операторов, он вычисляет каждый компонент, когда он требуется. Этот подход позволяет использовать немного больший размер входных данных, но также имеет свои недостатки. Во-первых, так как с увеличением числа кубитов экспоненциально возрастает количество элементов и операций с ними, соответственно, возрастает и время вычислений. К тому же вектор состояний по-прежнему должен оставаться в памяти компьютера. Во-вторых, этот подход требует дополнительного изучения структуры операторов.

Третий подход – проблемно-ориентированный. Подход основан на глубоком изучении структуры конкретного квантового алгоритма, характера поведения вектора состояния. Например, для алгоритма Гровера характерно, что вектор состояния имеет только два различных значения (соответствующие различной амплитуде вероятностей). Используя эту закономерность, на классическом компьютере можно запускать этот алгоритм с входными данными размеров более чем 64 кубита.

Четвертый подход применим лишь к некоторым КА, позволяющие получать решение исходной задачи, используя свою редуцированную версию, в которой отсутствует один или два базовых квантовых оператора [7, 8].

В дальнейшем мы будем рассматривать метод моделирования КА, в первую очередь, основанный на представлении квантовых матричных операторов, включающий в себя универсальный способ построения квантового оператора (который мы будем в дальнейшем называть квантовой ячейкой), применение которого будет достаточно для реализации «квантовой» части любого квантового алгоритма.

Выводы

Рассмотрены фундаментальные принципы, физическая и алгоритмическая интерпретации основных квантовых и эволюционных эффектов, используемые в квантовых и генетических алгоритмах. Данные эффекты применяются при поиске эффективных решений задач глобальной оптимизации в системном анализе и интеллектуального управления слабо формализованными системами в условиях непредвиденных ситуаций и риска. Сделана попытка освещения разработанных методологических вопросов математического описания структур ГА и КА необходимых для студентов (соответствующих специальностей). Инновации в изложении позволяют усовершенствовать программы дисциплин для бакалавров и магистров соответствующих специальностей. Методология учебных процессов при освещении вопросов структурной реализации ГА и КА на доступном (для инженерных специальностей) уровне используется на практике (особенно при изучении вопросов решения задач глобальной векторной многокритериальной оптимизации в задачах интеллектуального управления).

Список литературы

1. Ulyanov S.V., Litvintseva L.V., Ulyanov S.S. Quantum information and quantum computational intelligence: Quantum optimal control and quantum filtering – Stability, robustness, and self-organization models in nanotechnologies. – Milan: Note del Polo (Ricerca), Universita degli Studia di Milano. – 2005. – Vol. 82.
2. Ulyanov S.V., Litvintseva L.V., Ulyanov S.S. Quantum information and quantum computational intelligence: Applied quantum soft computing in AI, quantum language and programming in computer science, quantum knowledge self-organization and intelligent wise robust control (4rd edit.). – Milan: Note del Polo (Ricerca), Universita degli Studia di Milano. – 2010. – Vol. 86.
3. Ulyanov S.V., System and method for control using quantum soft computing // US patent. – № 6,578,018 B1. – 2003.
4. Ohwi J., Ulyanov S.V., Yamafuji K. GA in continuous space and fuzzy classifier system for opening a door with a manipulator of mobile robot: New Benchmark of evolutionary intelligent computing // J. of Robotics and Mechatronics, 1996. – Vol.8. – № 3. – Pp. 297-301.

5. Имре Ш., Балаж Ф. Квантовые вычисления и связь: Инженерный подход. – М.: ФИЗМАТЛИТ, 2008.

6. Ulyanov S.V. Efficient simulation system of quantum algorithm gates on classical computer based on fast algorithm // US patent. – № US20060224547 A1. – 2006.

7. Ulyanov S.V., Litvintseva L.V., Takahashi K. Fast algorithm for efficient simulation of quantum algorithm gates on classical computer // Systemics, Cybernetics and Informatics. – 2004. – Vol. 2. – №3. – Pp. 63-68.

8. Ulyanov S.V. Method and device for performing a quantum algorithm for simulate a genetic algorithm // US patent. – № 20080140749 A1. – 2008.

9. Ulyanov S.V., Litvintseva L.V., Ulyanov S.S. Quantum Information and Quantum Computational Intelligence: Design & Classical Simulation of Quantum Algorithm Gates. – Milan: Note del Polo (Ricerca), Universita degli Studia di Milano. – 2000. – Vol. 80.

10. 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. – Milan: Note del Polo (Ricerca), Universita degli Studia di Milano. – 2003. – Vol. 80.