SECR

Software Engineering Conference Russia

14-15 ноября, 2019. Санкт-Петербург

# Автоматизированная генерация спецификаций квантовых цепей на основе полиномов Рида-Маллера

Калмычков В.А., Матвеева И.В.

СПбГЭТУ «ЛЭТИ»

# Квантовые компьютеры и вычисления: целевое назначение

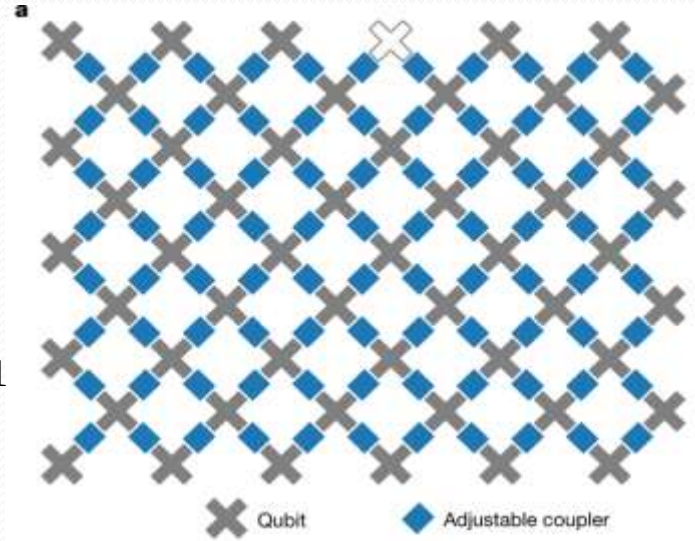
Цели применения квантового компьютера:

- решение вычислительных задач значительно быстрее компьютеров классической архитектуры (перебор/поиск, NP-задачи, многокритериальный выбор, оптимизация) – квантовое превосходство (quantum supremacy)[1]
- «одновременная» обработка набора данных на основе классических алгоритмов
- высокоскоростные эмуляторы физических и химических систем

КВАНТОВАЯ ТЕХНОЛОГИЯ (пока дорогая и не всегда доступная) – **В НАЛИЧИИ !!**

**Учимся программировать ? Физически ?**

**Можно какие-то этапы автоматизировать ?**




**a**: Компоновка процессора: прямоугольный массив из 54 кубитов (серый), каждый соединен с 4-мя ближайшими соседями (nearest neighbours) регулируемыми соединителями (синий). Выделено неработоспособное состояние кубита. **b**: Sycamore chip (Google Al Quantum) [2]

[1] 23 октября 2019, : Arute, F., Arya, K., Babbush, R. et al. Quantum supremacy using a programmable superconducting processor. *Nature* 574, pages 505–510. https://www.nature.com/articles/s41586-019-1666-5

# Квантовые вычисления: математики, физики или специалисты ВТ?

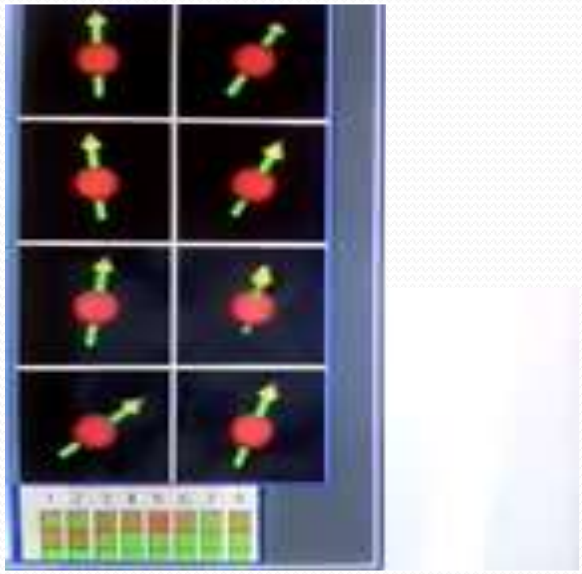
- 1980: математик Юрий Манин – идея квантовых вычислений
- 1981: физик Ричард Фейнман – базовая модель квантового компьютера (моделирование эволюции квантовой системы)
- 1981: физик(специалист ВТ) Томмазо Тоффоли – преобразователь
- 1985: физик Дэвид Дойч – квантовая машина Тьюринга
- 1994: математик Питер Шор – квантовый алгоритм факторизации
- 1995: физик Д.П. Дивинченцо (исследователь, IBM) и др. – описание элементарных квантовых преобразователей (gates)
- 1996: математик Лов Гровер – квантовый алгоритм поиска в БД
- 1997: физик Алексей Китаев – принципы топологических квантовых вычислений
- 1997: Д.Кори, А.Фахми и Т.Хавел (Н.Гершенфельд и И.Чанг) – КК на эффекте объемного спинового резонанса или тепловых ансамблей (ЯМР)
- 1997: Д.П. Дивинченцо – КК с кубитами на собственном моменте импульса отдельных электронов, находящихся в квантовых точках
- 1998: демонстрация 2-х, 3-х кубитных КК на ЯМР (ЯМР-компьютер)

# Квантовые компьютеры: препятствия при создании

- 2000: 5-ти кубитный ЯМР-компьютер (Мюнхен), 7-ми кубитный ЯМР-компьютер (Лос-Аламос)

Основные задачи (проблемы):

- обеспечение стабильного состояния на существенный временной промежуток (+ «температурное» влияние),
- физические носители и процессы,
- обнаружение и исправление квантовых ошибок при вычислениях,
- обработка результатов (измерение),
- воспроизводимость,
- обеспечение существенного числа
- кубитов (даже не сотни, а тысячи !).



# Квантовые компьютеры: основные технологии

| Технология | Логический кубит | Управление |
|---|---|---|
| Твердотельные квантовые точки на полу-проводниках | Зарядовые состояния (электрон) или направление электронного и/или ядерного спина в квантовой точке | Внешние потенциалы или лазерный импульс |
| Сверхпроводящие элементы | Присутствие/отсутствие куперовской пары в определённой точке пространства | Внешний потенциал, магнитный поток |
| Атомы в оптических ловушках (ионы) | Состояния внешнего электрона в ионе | Лазерные импульсы вдоль оси ловушки или на ионы |

Дополнительно: приготовление запутанных состояний фотонов для управления атомными ансамблями, генерация квантовых состояний света

# Общая схема организации вычислений с использованием квантового компьютера


M.A. Nielsen, and I.L. Chuang. Quantum Computation and Quantum Information, 2000. Cambridge Univ. Press, Cambridge, UK. 704 стр.

Валиев К.А., Кокин А.А. Квантовые компьютеры. Надежды и реальность, 2001. Ижевск: НИЦ «Регулярная и хаотическая динамика». 352 стр.

# Квантовая цепь – модель квантовых вычислений

- ***Квантовые вычисления*** (***quantum computing***) – одно из перспективных направлений исследований в области компьютерных технологий.
- В последней трети прошлого века работы Ландауэра и Беннетта стимулировали интерес мирового научного сообщества к обратимым вычислениям и, как следствие, проектированию квантовых цепей на основе реверсивных преобразователей.
- ***Модель квантовой цепи*** – это способ представления спецификации для реализации квантовых вычислений на основе изменения состояний кубитов. Квантовая цепь представляет способ преобразований, которые позволяют перейти от входных состояний кубитов к выходным.
- Проблема в том, что для каждой конкретной вычислительной задачи нужно использовать свой особенный **квантовый алгоритм** (**квантовую цепь**), поэтому разработка новых алгоритмов – не менее важная задача, чем разработка квантовых процессоров.
- Проектирование и оптимизация квантовых цепей играет важную роль в разработке технологии квантовых вычислений.

# Квантовая цепь: основные модельные представления

**Квантовый бит (кубит)** – единичный вектор в двумерном комплексном векторном пространстве, для которого собственный базис фиксирован как {|0>,|1>}. Кубиты могут находиться в суперпозиции базовых состояний |0> и |1>: $a|0\rangle + b|1\rangle$, где амплитуды вероятности $a$ и $b$ комплексные числа, причем $|a|^2+|b|^2=1$. $|a|^2$ и $|b|^2$ это оценка вероятности получить при измерении в качестве результата одно из состояний:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ или } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

**Квантовый регистр** – набор кубитов. В основе двухкубитовой системы находится четырехкомпонентный базис:

$$|00\rangle = |0\rangle|0\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{bmatrix} 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{bmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle = |0\rangle|1\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{bmatrix} 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{bmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle|0\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{bmatrix} 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{bmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = |1\rangle|1\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{bmatrix} 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{bmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

# Квантовая цепь: основные модельные представления

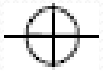
**Квантовые преобразователи**. При вычислениях квантовый регистр подвергается преобразованиям, переводящим регистр в новое состояние.

*Квантовое преобразование* (оператор) над кубитами может быть представлено матрицей U. Квантовая механика требует, чтобы преобразование было унитарным, т.е. $UU^T=I$.

***Квантовое вычисление*** **представляет из себя выполнение над входным значением регистра $|\varphi\rangle$ последовательности квантовых унитарных операторов $U_1U_2\ldots U_m$ для получения конечного состояния $U_1U_2\ldots U_m|\varphi\rangle$.**

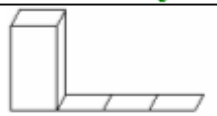
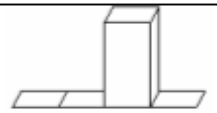
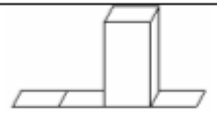
Квантовая операция над кубитом можно представлена как матрица 2 x 2.

Пример унитарной матрицы преобразователей: $NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

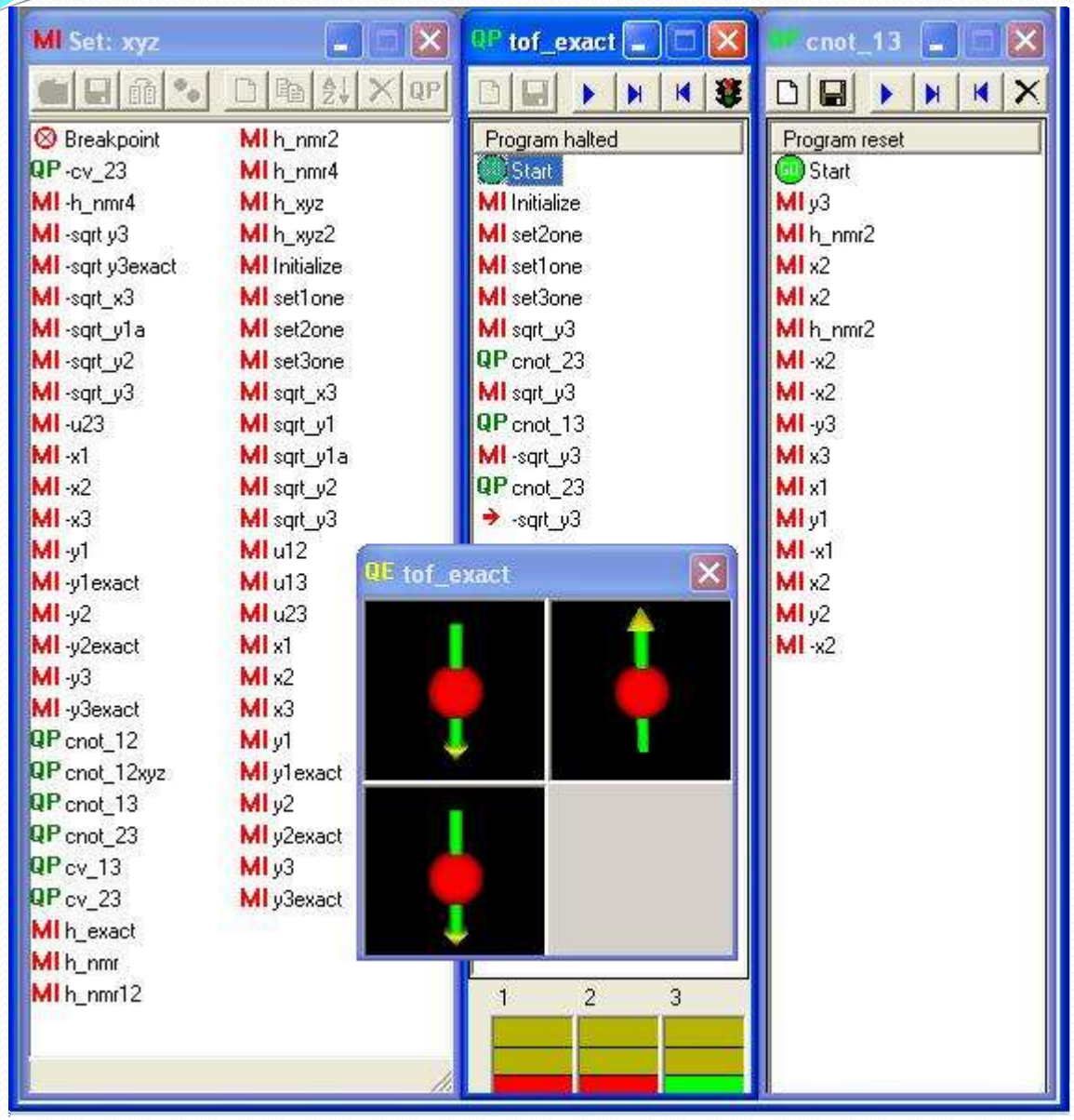
Графическая спецификация *NOT* : 

Преобразователь *NOT* выполняет преобразование |0> в |1> и |1> в |0>.

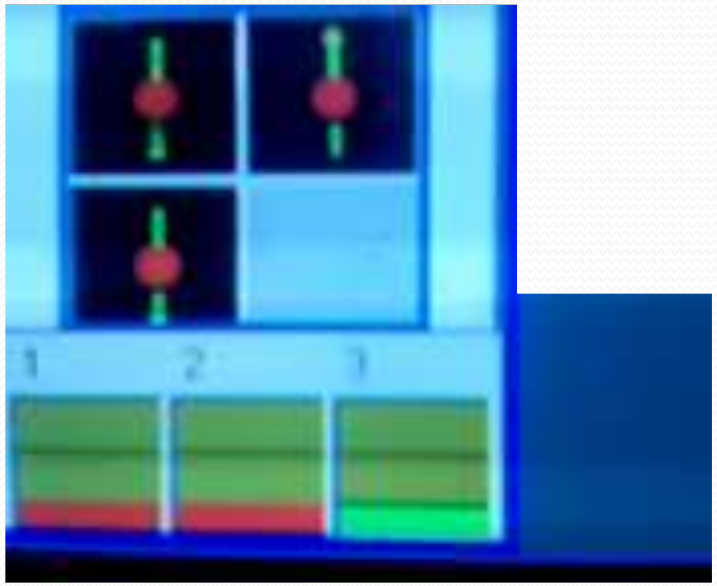
# Квантовая цепь: преобразователи (gates), нотации

| Преобразование | Состояния | Нотация | Амплитуда |
|---|---|---|---|
| $\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}$ – два одинаковых скалярных значения в двух векторах | 0 1 + 0i \|00><br>1 0 + 0i \|01><br>2 0 + 0i \|10><br>3 0 + 0i \|11> | Q1 \|0><br>Q2 \|0> |  |
| $\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}$ – два разных скалярных значения в двух векторах | 0 0 + 0i \|00><br>1 0 + 0i \|01><br>2 1 + 0i \|10><br>3 0 + 0i \|11> | Q1 \|0><br>Q2 \|1> |  |
| $\mathrm{Not}\left(\begin{bmatrix}1\\0\end{bmatrix}\right)\otimes\begin{bmatrix}1\\0\end{bmatrix}$ – смена проекций на оси (обмен осей первого вектора) | 0 0 + 0i \|00><br>1 0 + 0i \|01><br>2 1 + 0i \|10><br>3 0 + 0i \|11> | Q1 \|0><br>Q2 \|0> |  |
| $\begin{bmatrix}0\\1\end{bmatrix}\otimes\mathrm{Not}\left(\begin{bmatrix}1\\0\end{bmatrix}\right)\xrightarrow{e^{j\pi/4}\begin{bmatrix}0\\1\end{bmatrix}}$<br>$\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\\frac{1+j}{\sqrt{2}}\end{bmatrix}$ – обмен осей и зависимый поворот по одной оси | 0 0 + 0i \|00><br>1 0 + 0i \|01><br>2 0 + 0i \|10><br>3 0,70711 + 0,70711i \|11> | Q1 \|0> 45<br>Q2 \|1> |  |
| $\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}\xrightarrow{H}\begin{bmatrix}0\\1\end{bmatrix}\otimes\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$ – преобразование Адамара | 0 0 + 0i \|00><br>1 0 + 0i \|01><br>2 0,70711 + 0i \|10><br>3 0,70711 + 0i \|11> | Q1 \|0> H<br>Q2 \|1> |  |

# Преобразователи: инструкции физического уровня




Преобразователь Тоффоли:
2 управляющих кубита – слева
целевой кубит – справа



# Квантовая цепь: графическая спецификация

Для графической спецификации цепи квантовых преобразователей используется нотация, предложенная Дойчем.

Кубиты представляются как нити, на которые нанизаны преобразователи, действующие на соответствующие кубиты. Преобразователи представляются как квадратики или кружочки с соответствующими обозначениями. Время в цепи изменяется слева направо.

Управляющие преобразователи представлены как кружок или квадратик на целевом кубите, вертикальная линия управления с символами «●» (управление 1-ей) и «o» (управление 0-м) на соответствующих управляющих кубитах.

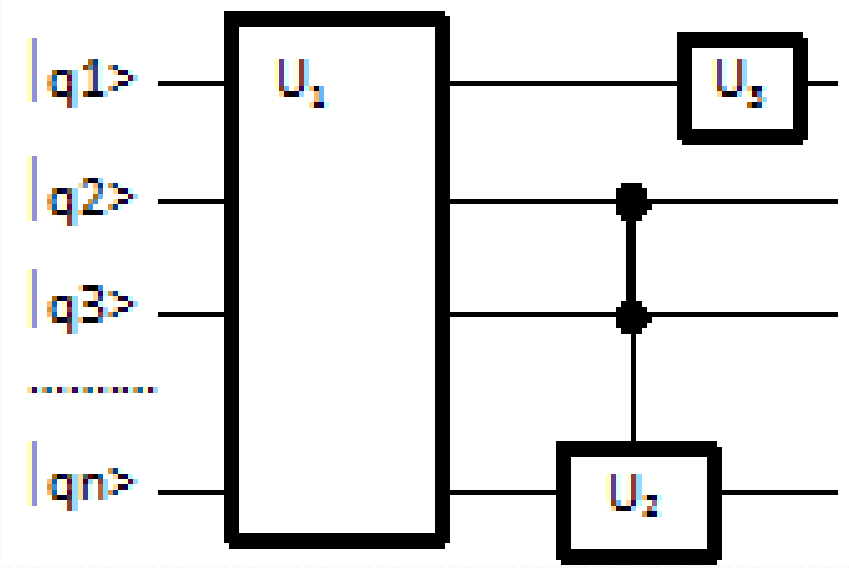
Пример произвольной квантовой цепи:

U1 – произвольный n-кубитовый квантовый преобразователь

U2 – управляющий трехкубитовый преобразователь

U3 – однокубитовый преобразователь

Слева представлен n-кубитовый квантовый регистр.



# Квантовая цепь: основные модельные представления

**Управляемые (условные) квантовые преобразователи** *C*U введены как обобщенный тип преобразователей.

Состоят из *кубитов управления* и *целевого кубита*.

Матрица U воздействует на целевой кубит, если **все** кубиты управления принимают требуемое состояние (|0> или |1>).

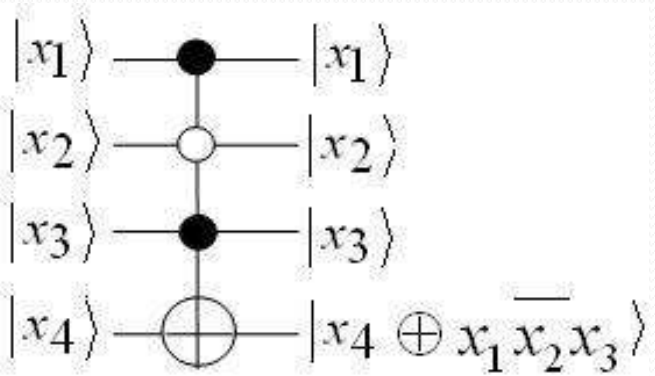
Действие универсального *n*-кубитового преобразователя $\Lambda_{n-1}(U)$ с *n*-1 управляющими кубитами $j_1, \ldots, j_{n-1}$ и одним целевым кубитом $j_0$ на векторах вычислительного базиса (квантового регистра):

$$|x_1,\ldots,x_{j_0},\ldots,x_n\rangle \to |x_1,\ldots\rangle \otimes U^{x_{j_1}\wedge\ldots\wedge x_{j_m}}|x_{j_0}\rangle \otimes |\ldots,x_n\rangle$$

Самой известной разновидностью управляемого (контролируемого) преобразования является семейство преобразователей $C^k$NOT, где *k* – целое число, определяющее количество управляющих узлов преобразователя.

$C^k$NOT(*Z*; *t*) – преобразователь, в котором целевой кубит *t* управляется набором кубитов *Z*.

Пример справа представляет графическую нотацию для $C^3\text{NOT}\left(x_1, \overline{x_2}, x_3; x_4\right)$.

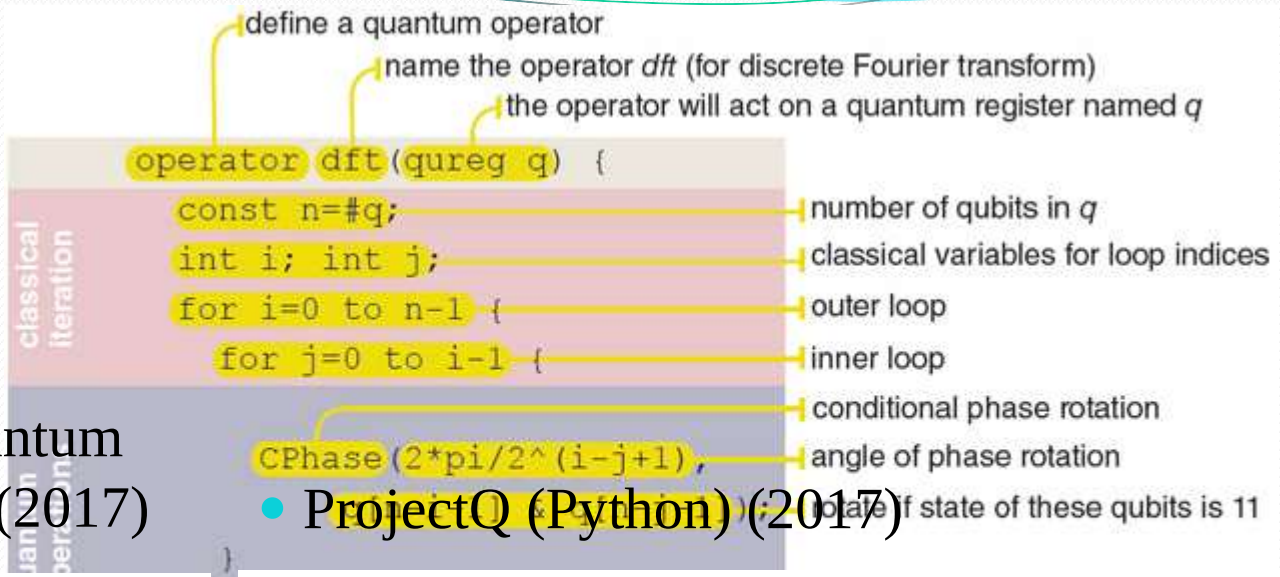


# Квантовые компьютеры: квантовое превосходство?

- D-Wave Systems: 2007: 16 и 28 кубит, 2011: 128 кубит (D-Wave One)
  2012: 512 кубит (Vesuvius ) 2015: более 1000 кубит
  2017: 2000 кубит (D-Wave 2000Q) [кластеры по 8 кубит]
- 2017: Гарвардский университет и Массачусетский технологический институт – программируемый квантовый компьютер на базе 51 кубита
- 2017: Joint Quantum Institute and Joint Center for Quantum Information and Computer Science, University of Maryland – 53-кубитный квантовый симулятор
- 2018: МГУ, Внешэкономбанк, Фонд перспективных исследований, "ВЭБ-инновации" и АНО "Цифровая экономика" подписали соглашение о создании в России 50-кубитного квантового компьютера
- 2019: Alibaba Quantum Laboratory – Alibaba Cloud Quantum Development Kit
- сентябрь 2019: Google-Sycamore chip (NASA),14-й от IBM на 53 кубита
- октябрь 2019: система из 2-х кубитов, собранная учеными МИСиС, успешно решила алгоритм Гровера (53% вероятность верного ответа)

# Квантовые языки программирования

- QCL, 1998 (Quantum Computation Language)




- QDK (Microsoft Quantum Development Kit) Q# (2017)

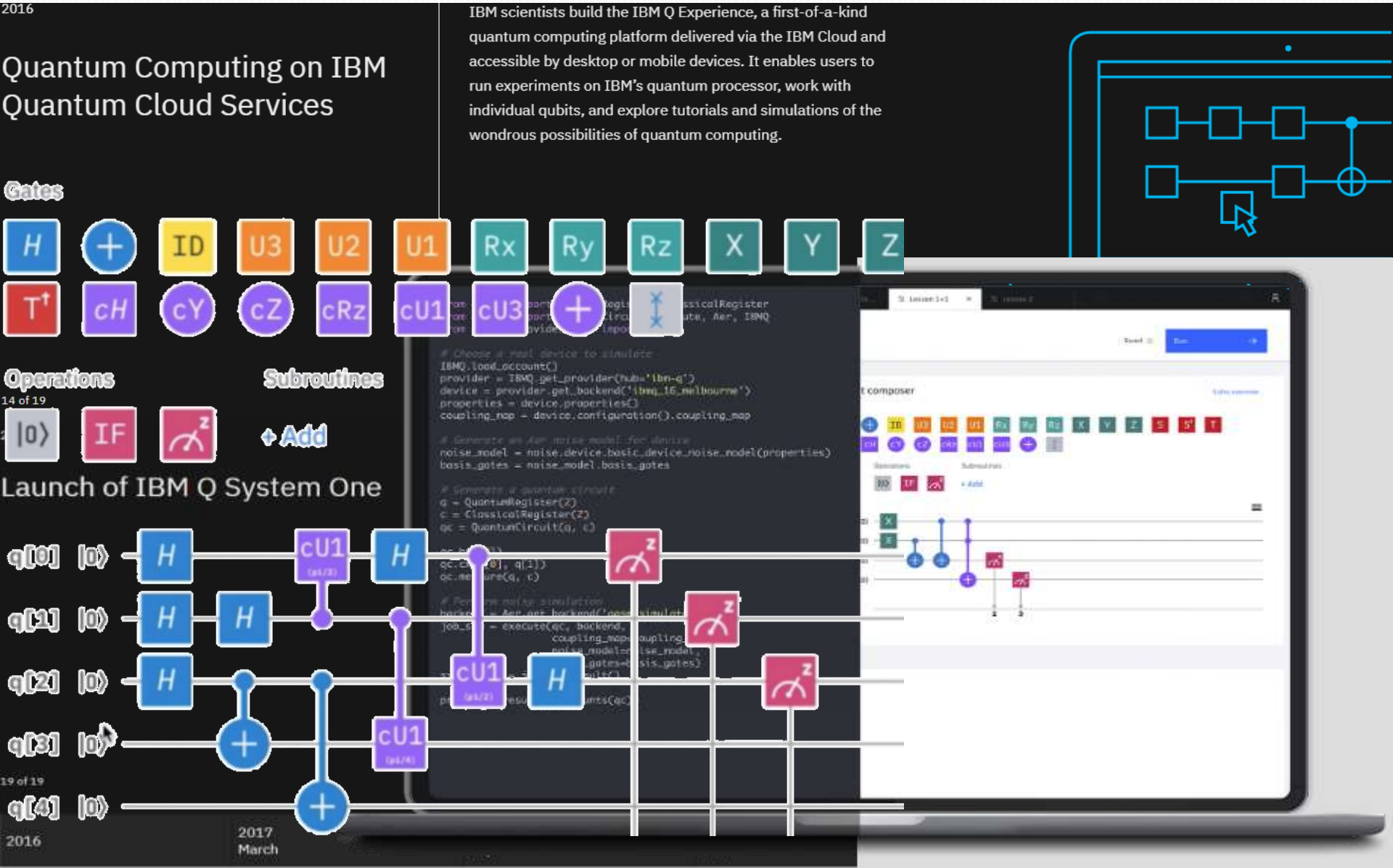
```
open Microsoft.Quantum.Primitive;
    ...
(qubits : Qubit[]) :
    ...
 body {
    CNOT(qubits[2], qubits[1]);
    H(qubits[0]);
    CNOT(qubits[1], qubits[2]);
    CNOT(qubits[0], qubits[1]);
    CNOT(qubits[2], qubits[0]);
    CNOT(qubits[2], qubits[1]);
    CNOT(qubits[0], qubits[1]);
    CNOT(qubits[2], qubits[0]);
    CNOT(qubits[1], qubits[2]);
    H(qubits[0]);
    CNOT(qubits[0], qubits[1]);
    CNOT(qubits[1], qubits[2]);
 }
```

- ProjectQ (Python) (2017)

```
from projectq.cengines import MainEngine
from projectq.ops import All, H, X, Measure
from projectq.meta import Compute, Uncompute,
import revkit
eng = MainEngine()
qubits = eng.allocate_qureg(6)
x = qubits[::2]
y = qubits[1::2]
with Compute(eng):
  All(H) | qubits
  All(X) | [x[0], x[1]]
Uncompute(eng)
All(H) | qubits
Measure | qubits
eng.flush()
```

# Квантовые языки программирования

- IBM (2019): https://www.ibm.com/quantum-computing/



# Квантовые языки программирования

- Open Quantum Assembly Language (OpenQASM), IBM (2017)

Пример (A.W. Cross, L.S. Bishop, J.A. Smolin, J.M. Gambetta):

```
// controlled-NOT
gate cx c,t { CX c,t; }
// Pauli gate: bit-flip
gate x a { u3(pi,0,pi) a; }
// Pauli gate: bit and phase flip
gate y a { u3(pi,pi/2,pi/2) a; }
// Pauli gate: phase flip
gate z a { u1(pi) a; }
// C3 gate: sqrt(S) phase gate
gate t a { u1(pi/4) a; }
// C3 gate: conjugate of sqrt(S)
gate tdg a { u1(-pi/4) a; }
```

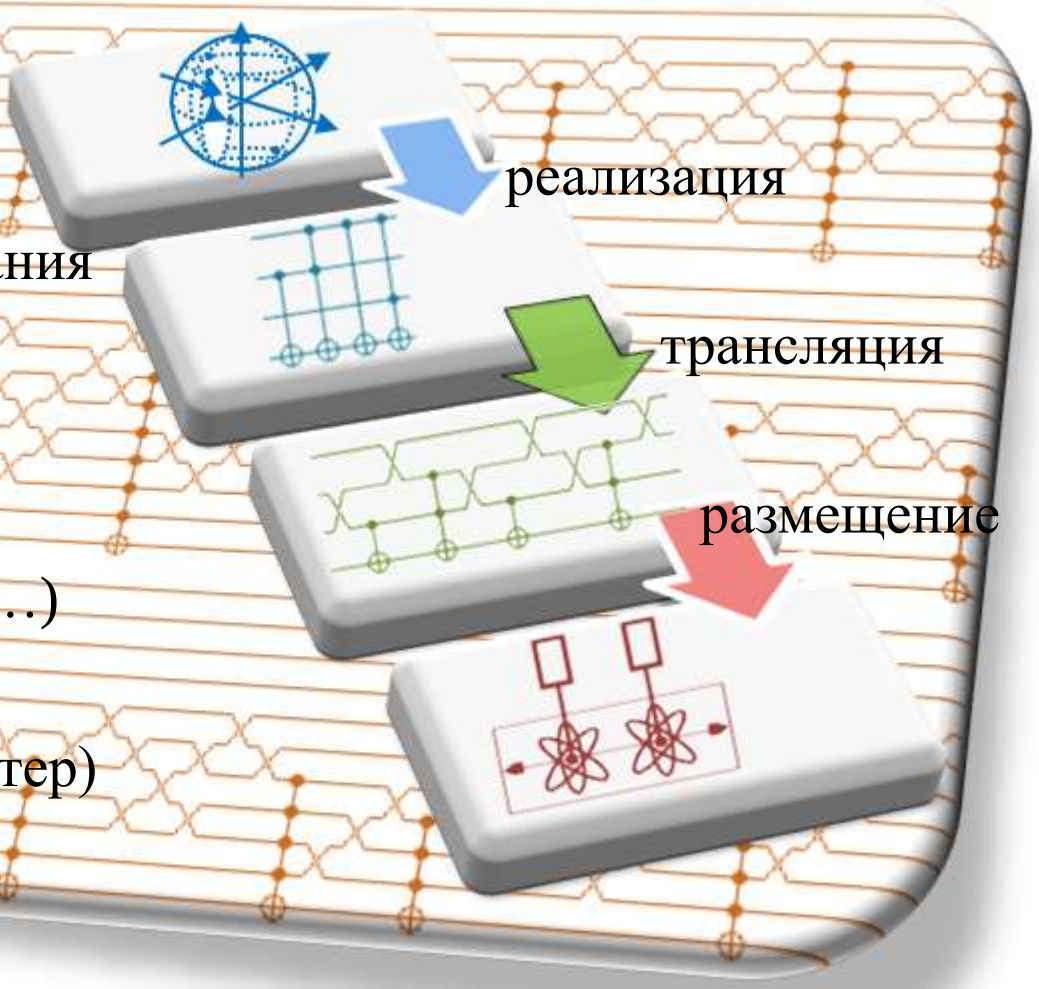
```
// C3 gate: Toffoli
gate ccx a,b,c
{
  h c;
  cx b,c; tdg c;
  cx a,c; t c;
  cx b,c; tdg c;
  cx a,c; t b; t c; h c;
  cx a,b; t a; tdg b;
  cx a,b;
}
```

```
// controlled-H
gate ch a,b {
h b; sdg b;
cx a,b;
h b; t b;
cx a,b;
t b; h b; s b; x b; s a;
}
```

# Квантовые алгоритмы → квантовые компьютеры

Высокоуровневый поток проектирования для отображения квантового алгоритма в среду квантового компьютера:

- квантовый алгоритм
- квантовый язык программирования (Q#, QCL, …)
- квантовая компиляция (библиотеки, оптимизация, набор инструментов, QASM, …)
- целевая платформа (симулятор, квантовый компьютер)



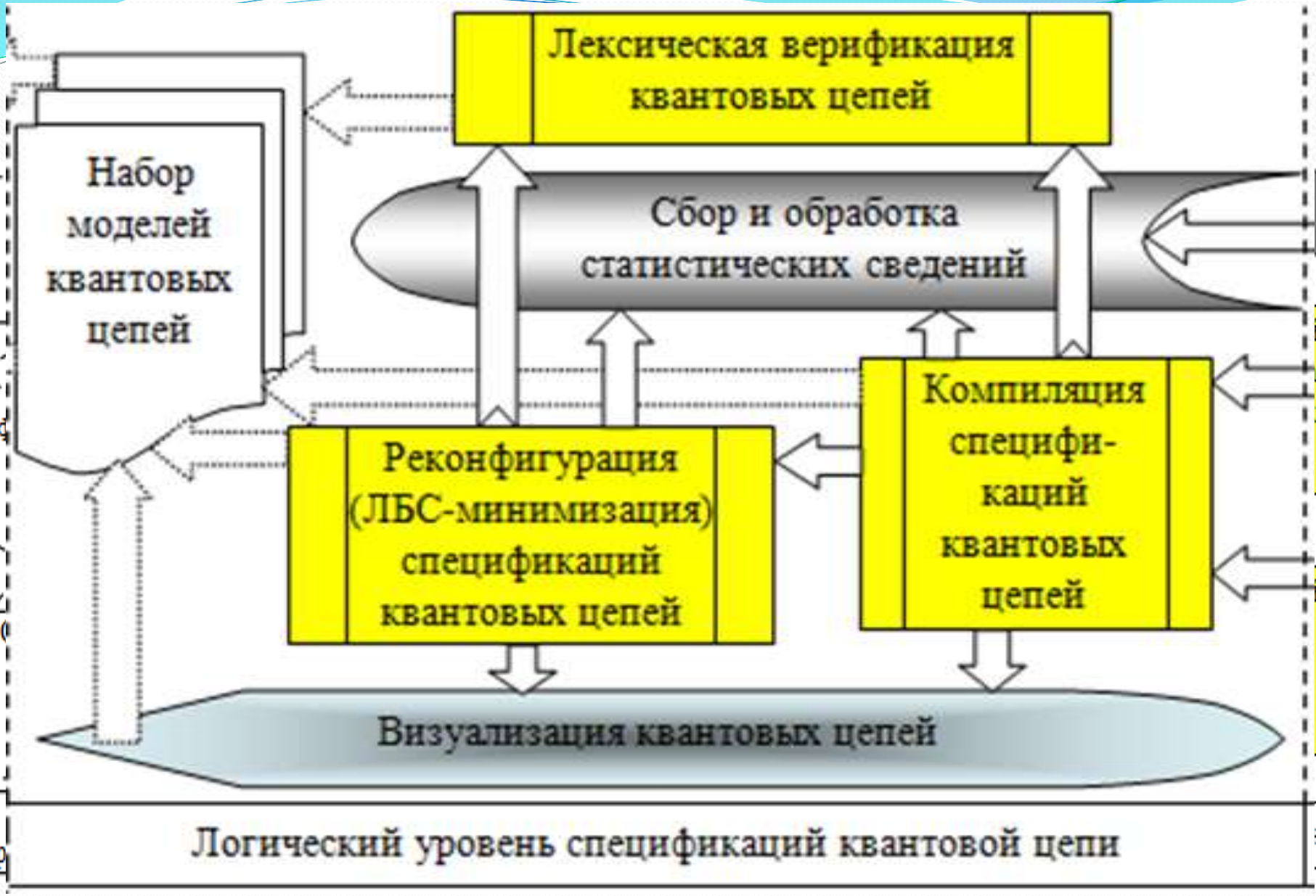
# Основные особенности системы квантовой компиляции

Наш набор приложений для логического уровня: осуществляется переход (компиляция) от математического описания к логическому уровню спецификаций квантовых цепей, после чего становится возможным адаптация к условиям физической реализации на основе реализации квантовых цепей в ЛБС-нотации[1].

- Автоматическая компиляция всех возможных вариантов квантовых цепей по полиномам Рида-Мюллера.
- Автоматические режимы:
  - перехода к линейно ближайшему соседу при минимизации числа преобразователей SWAP на основе масштабируемых шаблонов,
  - сбора статистики (с расчетом оценочных характеристик),
  - визуализации,
  - лексической проверки эквивалентности результатов компиляции квантовых цепей.

[1]ЛБС – линейно ближайшее соседство (LNN – Linear Nearest Neighbor) кубитов преобразователя – учет обеспечения ограничений на взаимодействие кубитов при физической реализации.

# Общая архитектура системы квантовой компиляции



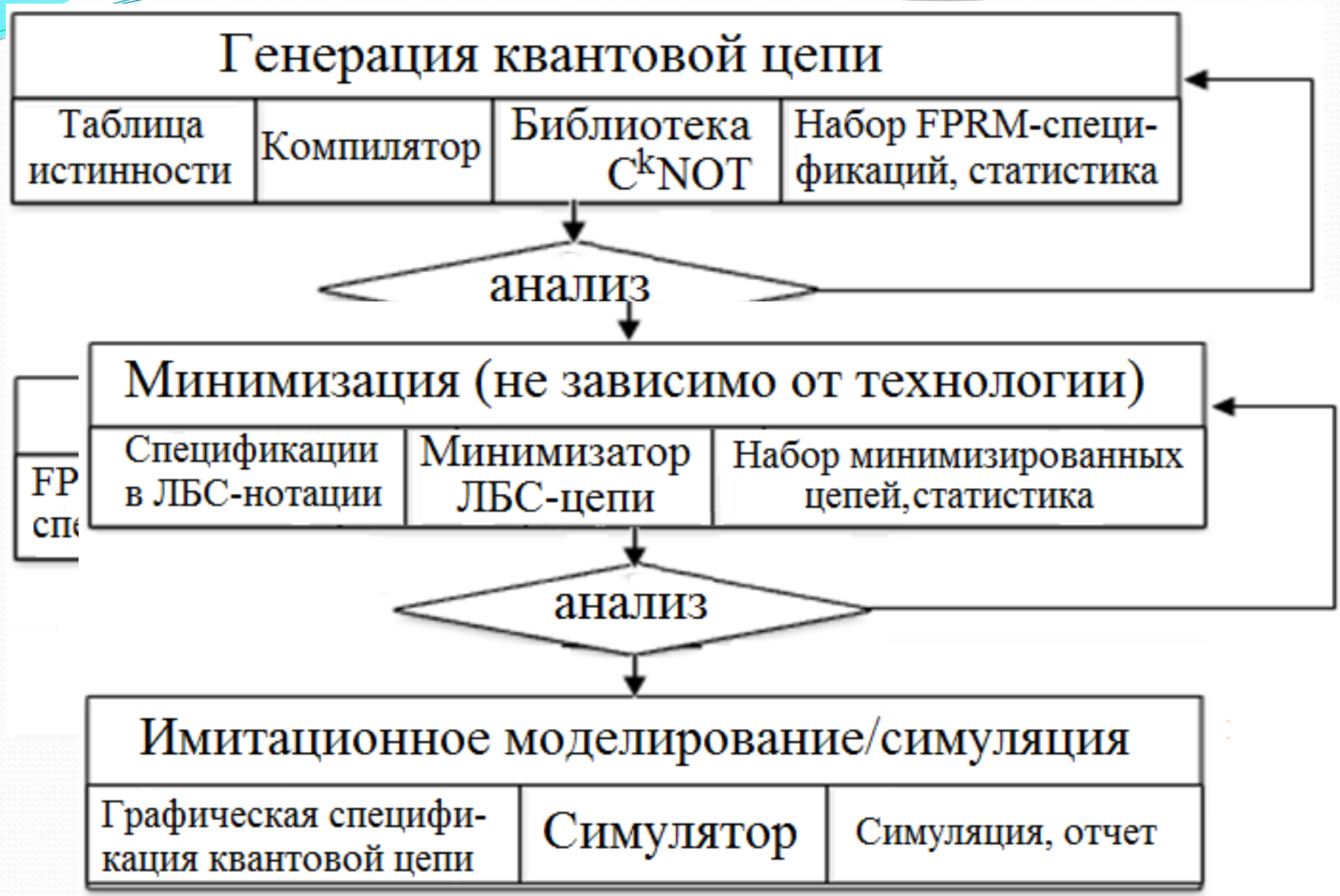
# Математический аппарат полиномов Рида-Маллера

**FPRM-представление** (*поляризованные полиномы Рида-Маллера* с фиксированной полярностью: fixed-polarity Reed-Muller expressions) булевых функций ($n$ входов и 1 выход) – это «сложение по модулю 2» EXOR от AND минитермов, в которых каждая булева переменная представлена либо в прямой, либо в инверсной форме, но не в обеих. Набор всех булевых функций 3-х переменных ($x_k$ и $b_i \in \{0, 1\}$, $0 \le k < n$, $0 \le i \le 2^n - 1$, $n = 3$ и коэффициенты $b_i$ определяют представлен ли минитерм в выражении или нет) может быть представлен как:

$$f(x_0, x_1, x_2) = b_0 \oplus b_1 x_0 \oplus b_2 x_1 \oplus b_3 x_1 x_0 \oplus b_4 x_2 \oplus$$
$$\oplus b_5 x_2 x_0 \oplus b_6 x_2 x_1 \oplus b_7 x_2 x_1 x_0$$

- На этапе синтеза строится поляризованный полином Рида-Маллера (нулевой полярности) и формируется набор поляризованных полиномов FPRM фиксированной полярности (от 1 до $2^n - 1$).
- На основе полученных полиномов генерируются наборы квантовых цепей в нотации квантовых преобразователей.

# Многоуровневая спецификация квантовой цепи



# Результат генерации полиномов Рида-Маллера

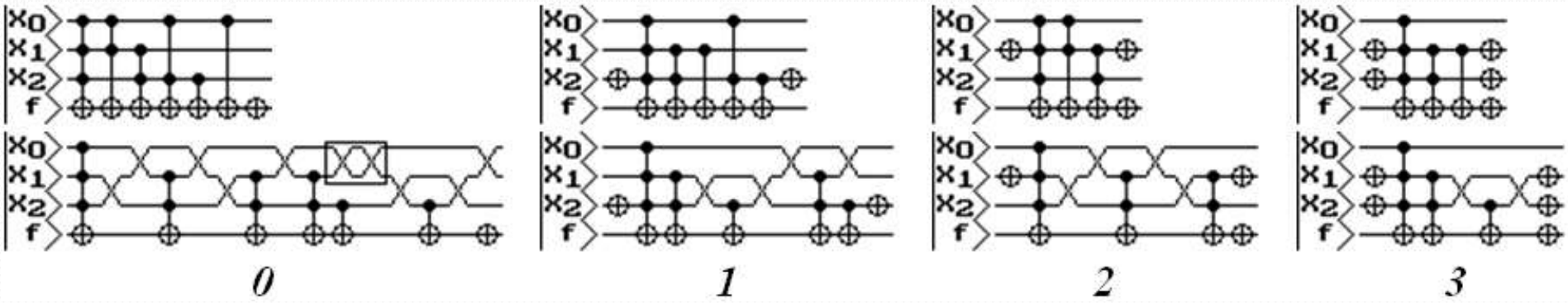
Формирование по заданной таблице истинности для 3 переменных поляризованного полинома Рида–Маллера нулевой полярности и набора поляризованных полиномов FPRM (от 1 до $2^n - 1$).

| № | $x_0$ | $x_1$ | $x_2$ | $f(x_0, x_1, x_2)$ | Полиномы FPRM всех полярностей |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | $f(x_0,x_1,x_2) = x_0x_1x_2 \oplus x_0x_1 \oplus x_1x_2 \oplus x_0x_2 \oplus x_2 \oplus x_0 \oplus 1$ |
| 1 | 0 | 0 | 1 | 0 | $f(x_0,x_1,x_2) = x_0x_1\bar{x}_2 \oplus x_1\bar{x}_2 \oplus x_1 \oplus x_0\bar{x}_2 \oplus \bar{x}_2$ |
| 2 | 0 | 1 | 0 | 1 | $f(x_0,x_1,x_2) = x_0\bar{x}_1x_2 \oplus x_0\bar{x}_1 \oplus \bar{x}_1x_2 \oplus 1$ |
| 3 | 0 | 1 | 1 | 1 | $f(x_0,x_1,x_2) = x_0\bar{x}_1\bar{x}_2 \oplus \bar{x}_1\bar{x}_2 \oplus \bar{x}_1 \oplus 1$ |
| 4 | 1 | 0 | 0 | 0 | $f(x_0,x_1,x_2) = \bar{x}_0x_1x_2 \oplus \bar{x}_0x_1 \oplus x_1 \oplus \bar{x}_0x_2 \oplus \bar{x}_0$ |
| 5 | 1 | 0 | 1 | 0 | $f(x_0,x_1,x_2) = \bar{x}_0x_1\bar{x}_2 \oplus x_1 \oplus \bar{x}_0\bar{x}_2$ |
| 6 | 1 | 1 | 0 | 1 | $f(x_0,x_1,x_2) = \bar{x}_0\bar{x}_1x_2 \oplus \bar{x}_0\bar{x}_1 \oplus \bar{x}_1 \oplus 1$ |
| 7 | 1 | 1 | 1 | 1 | $f(x_0,x_1,x_2) = \bar{x}_0\bar{x}_1\bar{x}_2 \oplus \bar{x}_1 \oplus 1$ |

# Результат генерации спецификаций квантовых цепей

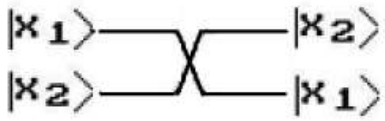
Квантовые цепи согласно 8 полярностям FPRM представлены вместе с соответствующими им ЛБС-нотациями.

| № | Полиномы FPRM всех полярностей |
|---|---|
| 0 | $f(x_0,x_1,x_2)=x_0x_1x_2 \oplus x_0x_1 \oplus x_1x_2 \oplus x_0x_2 \oplus x_2 \oplus x_0 \oplus 1$ |
| 1 | $f(x_0,x_1,x_2)=x_0x_1\bar{x}_2 \oplus x_1\bar{x}_2 \oplus x_1 \oplus x_0\bar{x}_2 \oplus \bar{x}_2$ |
| 2 | $f(x_0,x_1,x_2)=x_0\bar{x}_1x_2 \oplus x_0\bar{x}_1 \oplus \bar{x}_1x_2 \oplus 1$ |
| 3 | $f(x_0,x_1,x_2)=x_0\bar{x}_1\bar{x}_2 \oplus \bar{x}_1\bar{x}_2 \oplus \bar{x}_1 \oplus 1$ |




*0* *1* *2* *3*

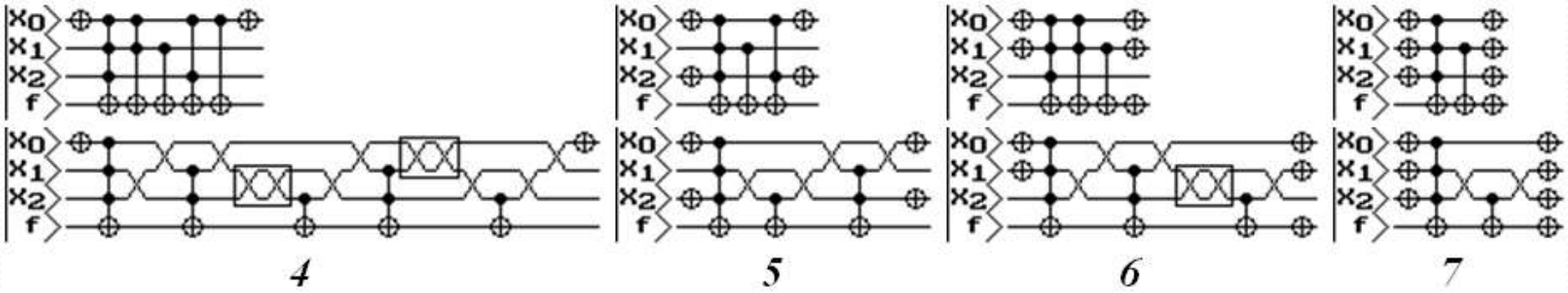
Преобразователь SWAP выполняет обмен состояний кубитов:



# Результат генерации спецификаций квантовых цепей

Квантовые цепи согласно 8 полярностям FPRM представлены вместе с соответствующими им ЛБС-нотациями.

| № | Полиномы FPRM всех полярностей |
|---|---|
| 4 | $f(x_0, x_1, x_2) = \bar{x}_0 x_1 x_2 \oplus \bar{x}_0 x_1 \oplus x_1 \oplus \bar{x}_0 x_2 \oplus \bar{x}_0$ |
| 5 | $f(x_0, x_1, x_2) = \bar{x}_0 x_1 \bar{x}_2 \oplus x_1 \oplus \bar{x}_0 \bar{x}_2$ |
| 6 | $f(x_0, x_1, x_2) = \bar{x}_0 \bar{x}_1 x_2 \oplus \bar{x}_0 \bar{x}_1 \oplus \bar{x}_1 \oplus 1$ |
| 7 | $f(x_0, x_1, x_2) = \bar{x}_0 \bar{x}_1 \bar{x}_2 \oplus \bar{x}_1 \oplus 1$ |



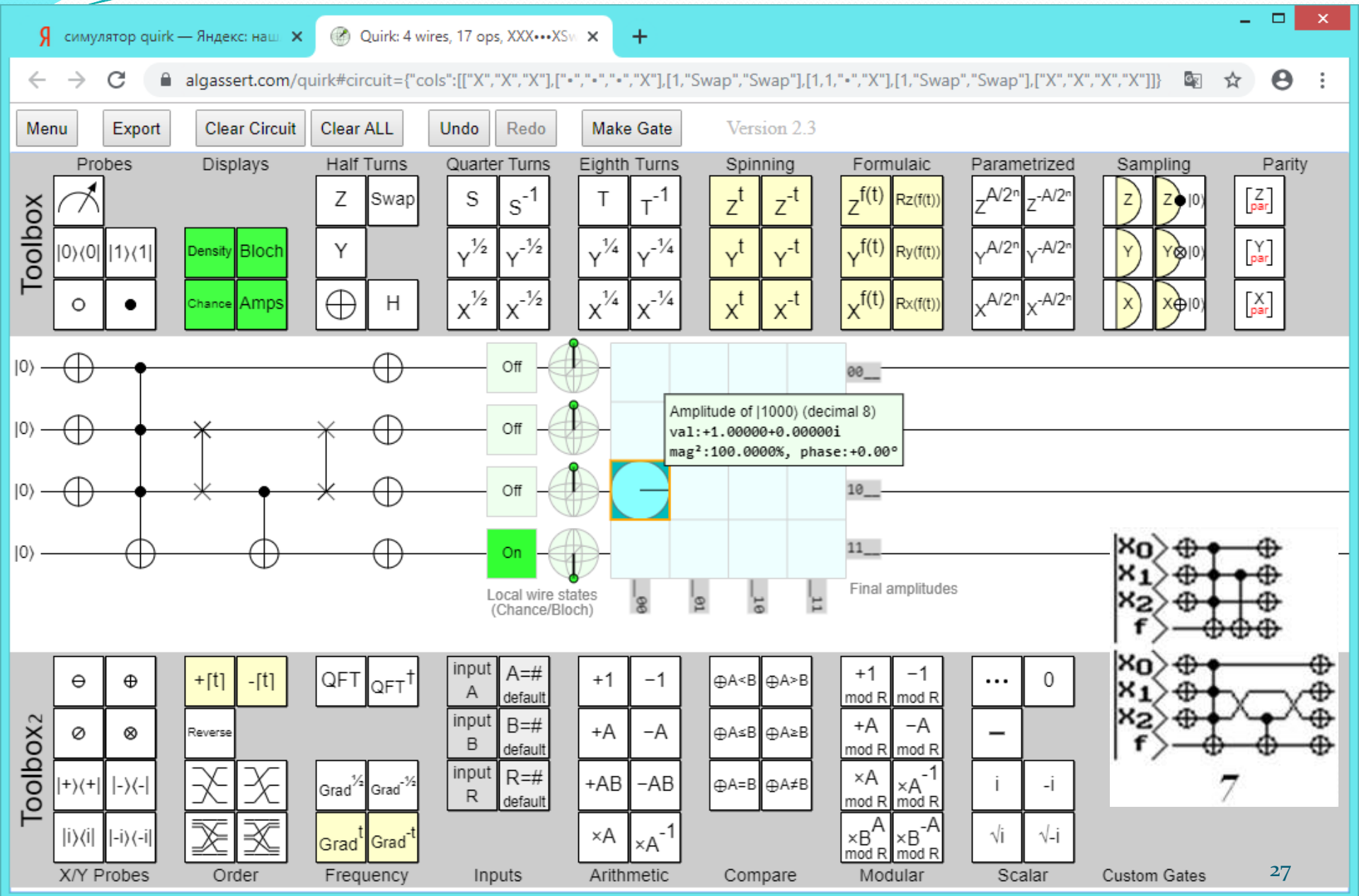
# Статистика для эквивалентных квантовых цепей

Критерии: *количество квантовых преобразователей*, *глубина квантовой цепи* при параллельной расстановке одновременно выполняющихся преобразователей (снижение временных затрат), *квантовая стоимость* для оценки предполагаемой сложности физической реализации преобразователя (принимаем $КС_{NOT}=КС_{CNOT}=1$, $КС_{C^kNOT}=5^{k-1}$, $КС_{SWAP}=3$)

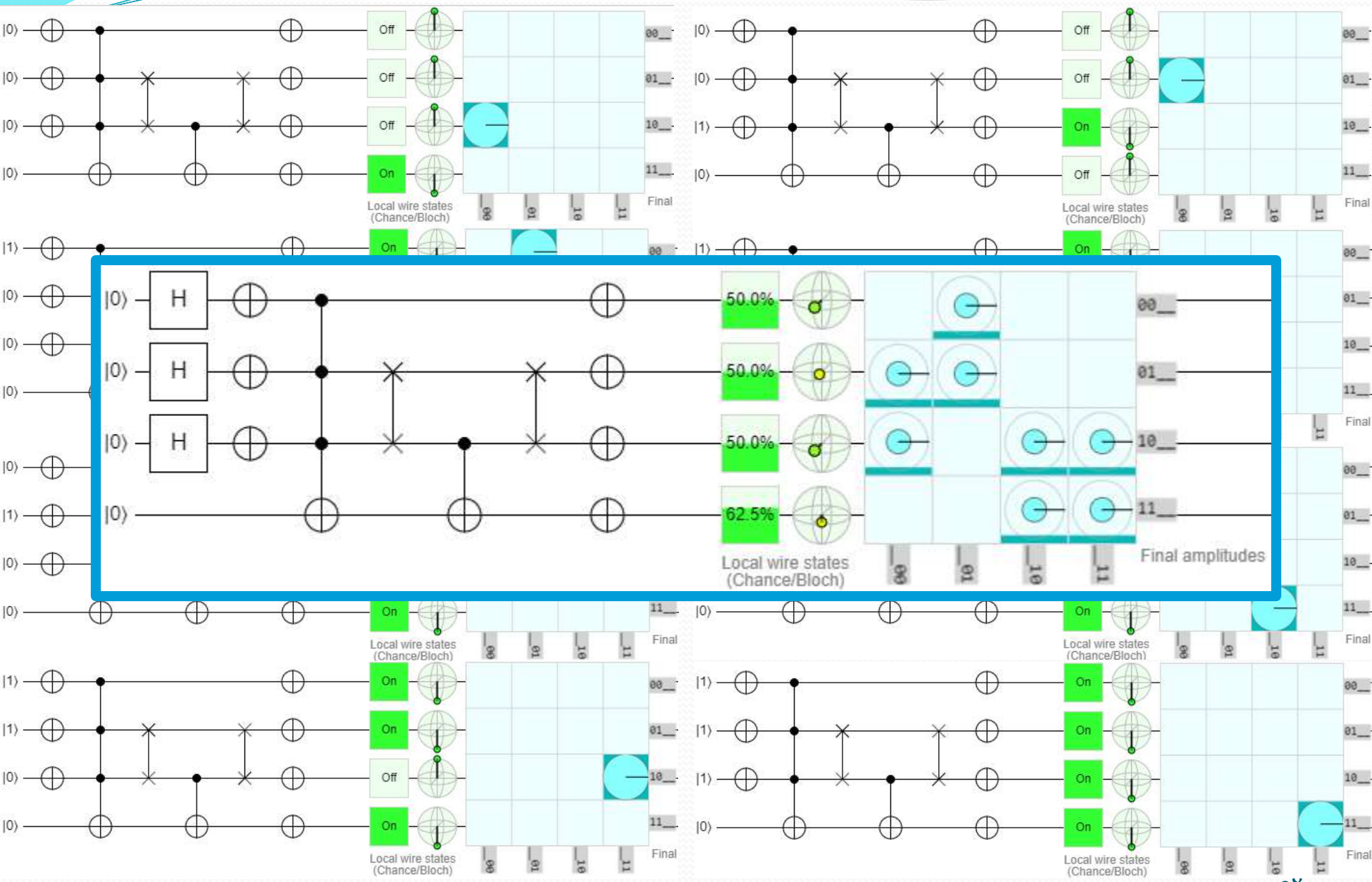
M10 `=F10*$F$12^2+G10*$F$12^1+H10*$F$12^0+(E10+I10)*$G$12+K10*$H$12`

| | A | B | D | E | F | G | H | I | J | K | L | M | O | P | Q | R | S | T | U |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | Control qubits number | | | | | | | | Minimization result | | | | Reduction result | | |
| 2 | x 012 | f | Polarity | NOT-x | 3 | 2 | 1 | NOT-f | C^gates | SWAPs | C^gates +SWAPs | QCost | Depth | SWAPs | C^gates +SWAPs | Qcost | SWAPs | C^gates +SWAPs | Qcost |
| 3 | 000 | 1 | 0 | 0 | 1 | 3 | 2 | 1 | 7 | 10 | 17 | 73 | 14 | 8 | 15 | 67 | 20,00% | 11,76% | 8,22% |
| 4 | 001 | 0 | 1 | 2 | 1 | 2 | 2 | 0 | 7 | 4 | 11 | 51 | 10 | 4 | 11 | 51 | 0,00% | 0,00% | 0,00% |
| 5 | 010 | 1 | 2 | 2 | 1 | 2 | 0 | 1 | 6 | 4 | 10 | 50 | 9 | 4 | 10 | 50 | 0,00% | 0,00% | 0,00% |
| 6 | 011 | 1 | 3 | 4 | 1 | 1 | 1 | 1 | 8 | 2 | 10 | 42 | 7 | 2 | 10 | 42 | 0,00% | 0,00% | 0,00% |
| 7 | 100 | 0 | 4 | 2 | 1 | 2 | 2 | 0 | 7 | 12 | 19 | 75 | 15 | 8 | 15 | 63 | 33,33% | 21,05% | 16,00% |
| 8 | 101 | 0 | 5 | 4 | 1 | 1 | 1 | 0 | 7 | 4 | 11 | 47 | 9 | 4 | 11 | 47 | 0,00% | 0,00% | 0,00% |
| 9 | 110 | 1 | 6 | 4 | 1 | 1 | 1 | 1 | 8 | 6 | 14 | 54 | 9 | 4 | 12 | 48 | 33,33% | 14,29% | 11,11% |
| 10 | 111 | 1 | 7 | 6 | 1 | 0 | 1 | 1 | 9 | 2 | 11 | 39 | 6 | 2 | 11 | 39 | 0,00% | 0,00% | 0,00% |
| 11 | | Gate: | | $C^kNOT$ | | NOT | SWAP | | | | | Minimum: | | | | | | Maximum: | |
| 12 | | Qcost: | | | 5 | 1 | 3 | | 6 | 2 | 10 | 39 | 6 | 2 | 10 | 39 | 33,33% | 21,05% | 16,00% |

# Симулятор квантовых цепей QUIRK (для 7 полярности)

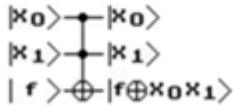
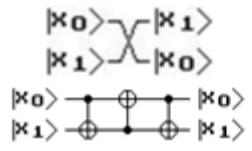


# Симулятор квантовых цепей QUIRK (для 7 полярности)



# Лексическая верификация квантовых цепей

Анализ преобразований над кубитами в скомпилированных квантовых цепях проводится нами на основе пространства лексем для символического вида коэффициентов кубитов в вычислительном базисе. Примеры применения верификации базовых преобразователей для одного кубита и квантового регистра из двух и трех кубитов:

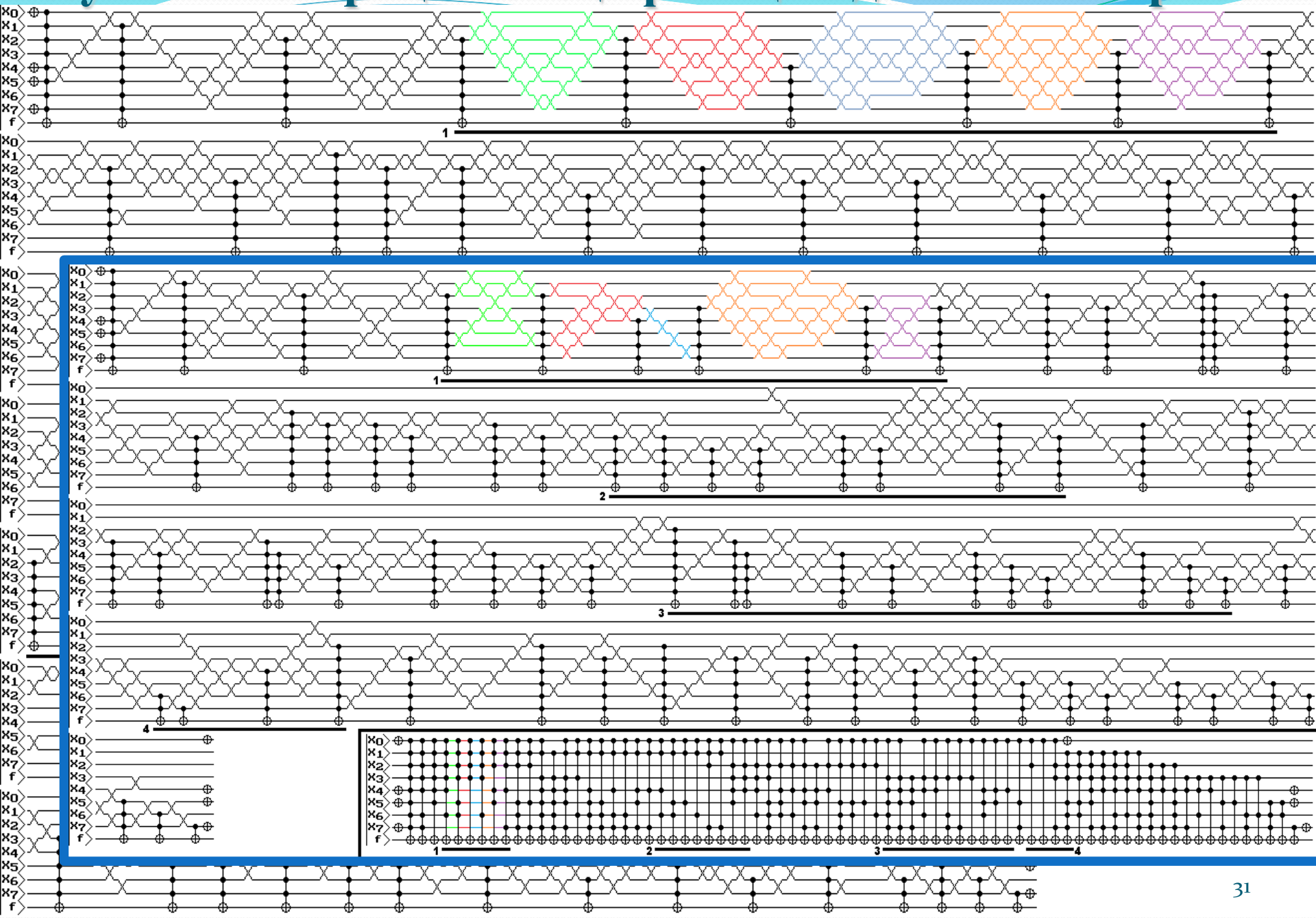
| Преобразователь | Число кубитов и графическая нотация | Лексемы для коэффициентов кубита |
|---|---|---|
| $C^2$NOT (Toffoli) | 3<br>  | $\begin{bmatrix} a \\ c \end{bmatrix} \otimes \begin{bmatrix} b \\ d \end{bmatrix} \otimes \begin{bmatrix} e \\ f \end{bmatrix} = \begin{bmatrix} abe \\ abf \\ ade \\ adf \\ cbe \\ cbf \\ cde \\ cdf \end{bmatrix} \xrightarrow{\text{Tof}} \begin{bmatrix} abe \\ abf \\ ade \\ cdf \\ cbe \\ cbf \\ cde \\ adf \end{bmatrix} = \begin{bmatrix} c \\ a \end{bmatrix} \otimes \begin{bmatrix} 0 \\ d \end{bmatrix} \otimes \begin{bmatrix} 0 \\ f \end{bmatrix} + \begin{bmatrix} a \\ c \end{bmatrix} \otimes \begin{bmatrix} b \\ 0 \end{bmatrix} \otimes \begin{bmatrix} e \\ 0 \end{bmatrix} + \begin{bmatrix} a \\ c \end{bmatrix} \otimes \begin{bmatrix} 0 \\ d \end{bmatrix} \otimes \begin{bmatrix} e \\ 0 \end{bmatrix} + \begin{bmatrix} a \\ c \end{bmatrix} \otimes \begin{bmatrix} b \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ f \end{bmatrix}$ |
| SWAP (через 3 $C^1$NOT) | 2<br>  | $\begin{bmatrix} a \\ c \end{bmatrix} \otimes \begin{bmatrix} b \\ d \end{bmatrix} = \begin{bmatrix} ab \\ ad \\ cb \\ cd \end{bmatrix} \xrightarrow{\text{SWAP}} \begin{bmatrix} ba \\ bc \\ da \\ dc \end{bmatrix} = \begin{bmatrix} b \\ d \end{bmatrix} \otimes \begin{bmatrix} a \\ c \end{bmatrix}$ |

# Фрагмент статистики для FPRM 8 переменных

O15 =C15*$P$1^7+D15*$P$1^6+E15*$P$1^5+F15*$P$1^4+G15*$P$1^3+H15*$P$1^2+I15*$P$1^1+J15*$P$1^0+(B15+K15)*$N$1+M15*$L$1

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | Control qubits number | | | | | | | | SWAP: 3 | | NOT: 1 | | $C^k$NOT: 5 | | Minimization result | | | Reduction result | | |
| 2 | Polarity | NOT-x | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | NOT-f | C^gates | SWAPs | C^gates +SWAPs | QCost | | SWAPs | C^gates +SWAPs | Qcost | SWAPs | C^gates +SWAPs | Qcost |
| 3 | 0 | 0 | 1 | 4 | 14 | 37 | 41 | 32 | 14 | 3 | 1 | 147 | 2076 | 2223 | 219727 | | 1026 | 1173 | 216577 | 50,58% | 47,23% | 1,43% |
| 4 | 1 | 2 | 1 | 3 | 13 | 29 | 36 | 28 | 18 | 4 | 1 | 135 | 1892 | 2027 | 194723 | | 870 | 1005 | 191657 | 54,02% | 50,42% | 1,57% |
| 5 | 40 | 4 | 1 | 2 | 15 | 32 | 39 | 31 | 13 | 3 | 1 | 141 | 1860 | 2001 | 187553 | | 892 | 1033 | 184649 | 52,04% | 48,38% | 1,55% |
| 6 | 41 | 6 | 1 | 1 | 14 | 27 | 37 | 30 | 17 | 5 | 1 | 139 | 1848 | 1987 | 165391 | | 798 | 937 | 162241 | 56,82% | 52,84% | 1,90% |
| 7 | 42 | 6 | 1 | 3 | 13 | 34 | 42 | 38 | 16 | 6 | 0 | 159 | 2134 | 2293 | 199569 | | 976 | 1135 | 196095 | 54,26% | 50,50% | 1,74% |
| 8 | 131 | 6 | 1 | 3 | 15 | 23 | 23 | 16 | 9 | 2 | 1 | 99 | 1322 | 1421 | 193545 | | 632 | 731 | 191475 | 52,19% | 48,56% | 1,07% |
| 9 | 132 | 4 | 1 | 4 | 14 | 31 | 34 | 20 | 7 | 1 | 1 | 117 | 1656 | 1773 | 213509 | | 646 | 763 | 210479 | 60,99% | 56,97% | 1,42% |
| 10 | 133 | 6 | 1 | 3 | 15 | 23 | 24 | 16 | 6 | 2 | 0 | 96 | 1268 | 1364 | 193492 | | 574 | 670 | 191410 | 54,73% | 50,88% | 1,08% |
| 11 | 140 | 6 | 1 | 3 | 13 | 24 | 22 | 21 | 4 | 2 | 1 | 97 | 1424 | 1521 | 188201 | | 574 | 671 | 185651 | 59,69% | 55,88% | 1,35% |
| 12 | 141 | 8 | 1 | 2 | 13 | 18 | 17 | 15 | 7 | 2 | 0 | 83 | 1090 | 1173 | 167065 | | 520 | 603 | 165355 | 52,29% | 48,59% | 1,02% |
| 13 | 142 | 8 | 1 | 4 | 12 | 24 | 20 | 17 | 7 | 2 | 1 | 96 | 1284 | 1380 | 199948 | | 640 | 736 | 198016 | 50,16% | 46,67% | 0,97% |
| 14 | 168 | 6 | 1 | 1 | 14 | 31 | 30 | 22 | 9 | 2 | 1 | 117 | 1464 | 1581 | 165621 | | 678 | 795 | 163263 | 53,69% | 49,72% | 1,42% |
| 15 | 169 | 8 | 1 | 0 | 14 | 28 | 28 | 22 | 12 | 4 | 0 | 117 | 1496 | 1613 | 147985 | | 650 | 767 | 145447 | 56,55% | 52,45% | 1,72% |
| 16 | 170 | 8 | 1 | 2 | 13 | 30 | 34 | 19 | 8 | 1 | 1 | 117 | 1562 | 1679 | 178211 | | 702 | 819 | 175631 | 55,06% | 51,22% | 1,45% |
| 17 | 194 | 6 | 1 | 5 | 14 | 24 | 26 | 17 | 5 | 0 | 1 | 99 | 1296 | 1395 | 222595 | | 580 | 679 | 220447 | 55,25% | 51,33% | 0,96% |
| 18 | 195 | 8 | 1 | 4 | 14 | 17 | 23 | 12 | 4 | 2 | 1 | 86 | 1036 | 1122 | 201314 | | 548 | 634 | 199850 | 47,10% | 43,49% | 0,73% |
| 19 | 196 | 6 | 1 | 5 | 14 | 30 | 33 | 16 | 4 | 1 | 1 | 111 | 1452 | 1563 | 227659 | | 598 | 709 | 225097 | 58,82% | 54,64% | 1,13% |
| 20 | 254 | 14 | 1 | 5 | 20 | 28 | 29 | 19 | 8 | 0 | 1 | 125 | 1524 | 1649 | 244977 | | 764 | 889 | 242697 | 49,87% | 46,09% | 0,93% |
| 21 | 255 | 16 | 1 | 4 | 20 | 29 | 36 | 28 | 12 | 4 | 1 | 151 | 1900 | 2051 | 232231 | | 922 | 1073 | 229297 | 51,47% | 47,68% | 1,26% |
| 23 | Minimum: | | 1 | 0 | 10 | 17 | 17 | 10 | 2 | 0 | 0 | 83 | 1036 | 1122 | 147985 | | 520 | 603 | 145447 | 42,40% | 45,86% | 0,73% |
| 24 | Maximum: | | 1 | 8 | 20 | 39 | 42 | 38 | 23 | 8 | 1 | 171 | 2284 | 2455 | 274406 | | 1034 | 1203 | 271598 | 60,99% | 56,97% | 1,90% |

# Результат генерации спецификаций для 141 полярности



# Полезные сведения

Обзор квантовых алгоритмов:
Душкин Р.В. Квантовые вычисления и функциональное программирование, 2015. Москва: ДМК Пресс. 232 стр.
Квантовые вычисления (Quantum computing) – видеокурс СПбГУ: https://www.coursera.org/learn/kvantovyye-vychisleniya
Программа «Введение в квантовые вычисления», МГУ: https://openedu.ru/course/msu/QUANTUMCOMPUTING/

The Joint Center for Quantum Information and Computer Science (QuICS) – a partnership between the University of Maryland (UMD) and the National Institute of Standards and Technology (NIST): https://quics.umd.edu/

**Росатом запускает масштабный проект по созданию отечественного квантового компьютера** (07 Ноября, 2019 / 10:42) – бюджет более 20 млрд. руб.:
- развитие различных платформ создания кубитов: сверхпроводников, холодных атомов и ионов, фотонов;
- к 2024 г. планируется создать квантовые компьютеры с 50-100 кубитами.
https://www.rosatom.ru/journalist/news/rosatom-zapuskaet-masshtabnyy-proekt-po-sozdaniyu-otechestvennogo-kvantovogo-kompyutera/

# К сведению

ВАК, защиты [2012-2019]:
01.04.03 – Радиофизика: **Моделирование работы квантового компьютера на квадрупольных ядрах (2013)**

ВАК – защиты, 2017:
01.04.02 - Теоретическая физика: Классические и квантовые модели суперсимметричной механики и частиц высших спинов
01.04.05 – Оптика [Акбари Мохсен]: Трёхфотонное спонтанное параметрическое рассеяние света и квантовые логические операции в кольцевых микрорезонаторах
01.04.02 - Теоретическая физика: Роль энтропийной асимметрии в двусоставных квантовых состояний
01.01.03 - Математическая физика: Экстремумы целевых функционалов в задачах управления двухуровневыми квантовыми системами
05.27.01 - Твердотельная электроника, радиоэлектронные компоненты, микро- и наноэлектроника, приборы на квантовых эффектах: Разработка методов и алгоритмов высокоточной томографии квантовых состояний
01.04.05 – Оптика: Квантовая коммуникация на боковых частотах лазерного фазомодулированного излучения по атмосферному каналу связи

# К сведению

ВАК – защиты, 2018:

01.04.02 - Теоретическая физика: Вероятностные, информационные и корреляционные характеристики квантовых систем

01.04.02 - Теоретическая физика: Топологическая фаза Паули и полуцелый орбитальный момент в двумерных квантовомеханических системах: циркулярных квантовых точках и графене с закритической кулоновской примесью

05.13.18 - Математическое моделирование, численные методы и комплексы программ: Модель квантовых графов с рёбрами меняющейся длины

ВАК – защиты, 2019:

05.13.18 - Математическое моделирование, численные методы и комплексы программ: Метод конечных элементов для исследования квантовых систем нескольких частиц

**СПАСИБО !!!**

# Контакты

**Калмычков Виталий Анатольевич**

**СПбГЭТУ «ЛЭТИ», ФКТИ, каф. САПР**

**vakalmychkov@etu.ru**

**Матвеева Ирина Витальевна**

**СПбГЭТУ «ЛЭТИ», ФКТИ, каф. САПР**

**ir_mat@mail.ru**

**https://etu.ru/ru/fakultety/fakultet-kompyuternyh-tehnologiy-i-informatiki/sostav-fakulteta/kafedra-sistem-avtomatizirovannogo-proektirovaniya/rukovodstvo-sostav-kafedry/professorsko-prepodavatelskiy-sostav1/matveeva-irina-vitalevna**