Квантовые вычисления

Практическое занятие № 3. Вычисление булевых и арифметических функций

Любая булева функция $f(x_1,\ldots,x_n)$ может быть вычислена с помощью квантового преобразования *F*, которое действует по схеме

$$F\left|x_n\cdots x_1 y\right\rangle = \left|x_n\cdots x_1 y\oplus f(x_1,\ldots,x_n)\right\rangle.$$

Матрица *F* может быть получена из таблицы истинности булевой функции. Рассмотрим, как это делается, на примере булевой функции от двух переменных. Пусть функция *f* задана таблицей истинности

x_2	x_1	f
0	0	1
0	1	1
1	0	0
1	1	1

Опишем отображение, которое должно выполнять преобразование *F*, для всех наборов входных переменных:

x_2	x_1	y		x_2	x_1	$y\oplus f$
0	0	0		0	0	1
0	0	1		0	0	0
0	1	0		0	1	1
0	1	1	→	0	1	0
1	0	0		1	0	0
1	0	1		1	0	1
1	1	0		1	1	1
1	1	1		1	1	0

Интерпретируя каждую строку преобразования как число, записанное в двоичной системе счисления, получаем следующие переходы: $0\to 1$, $1\to 0$, $2\to 3$, $3\to 2$, $4\to 4$, $5\to 5$, $6\to 7$, $7\to 6$. Матрицу *F* размером 8×8 заполняем нулями, затем для каждого перехода $i\to j$ пишем единицу на пересечении *i*-й строки и *j*-го столбца (нумерация строк и столбцов с нуля). Для нашего примера получается

$$F = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Как видим, получаемые таким путем матрицы – разряженные (единица появляется один раз в каждой строке), поэтому для их хранения в памяти целесообразно предусмотреть компактную структуру данных.

Теперь поговорим о вычислении арифметических функций. Они фактически отличаются от булевых тем, что результатом является число, а не просто единица или ноль. Но любое число может быть записано в двоичной системе счисления. Каждый бит этого числа может рассматриваться как булева функция. Таким образом, вычисление любой арифметической функции сводится к вычислению нескольких булевых функций. Именно так производят вычисления обычные компьютеры. Но если в обычном компьютере одну булеву переменную мы можем одновременно подать на входы нескольких логических вентилей, то в квантовом компьютере кубит не может разветвляться на несколько преобразователей, т.к. он связан с одним квантовым объектом, который не может делиться или размножаться.

Рассмотрим для примера функцию $f(x) = 3x \bmod 4$, где аргумент принимает значения 0, 1, 2, 3. Ясно, что для записи значений аргумента и функции достаточно двух бит. Нарисуем таблицу значений функции в двоичной системе, обозначив отдельные биты аргумента и функции индексами:

x_2	x_1	f_2	f_1
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1

Таким образом, задача вычисления функции f сводится к задаче вычисления двух булевых функций f_1 и f_2 для общего аргумента x. Запишем преобразование и построим матрицу в соответствии с методикой, изложенной выше (см. след. стр.):

x_2	x_1	y_2	y_1		x_2	x_1	$y_2 \oplus f_2$	$y_1 \oplus f_1$
0	0	0	0		0	0	0	0
0	0	0	1		0	0	0	1
0	0	1	0		0	0	1	0
0	0	1	1		0	0	1	1
0	1	0	0		0	1	1	1
0	1	0	1		0	1	1	0
0	1	1	0		0	1	0	1
0	1	1	1	$\rightarrow$	0	1	0	0
1	0	0	0		1	0	1	0
1	0	0	1		1	0	1	1
1	0	1	0		1	0	0	0
1	0	1	1		1	0	0	1
1	1	0	0		1	1	0	1
1	1	0	1		1	1	0	0
1	1	1	0		1	1	1	1
1	1	1	1		1	1	1	0

$$F = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}$$

В принципе, данную матрицу F можно было получить из матриц F_1 и F_2, построенных независимо для булевых функций f_1 и f_2. Эта возможность отдается на самостоятельное рассмотрение студентам.

Задание.

1. Построить матрицу, реализующую произвольную булеву функцию от двух переменных. Булеву функцию задавать таблицей истинности. Проверить полученную матрицу на унитарность.

2. Смоделировать квантовое вычисление функции $f(x) = a^x \bmod m$. Разрешается использовать конкретные значения a и m, например, $a = 2$, 3, …, $m = 15$, 21, 33, …, но лучше написать универсальную программу.