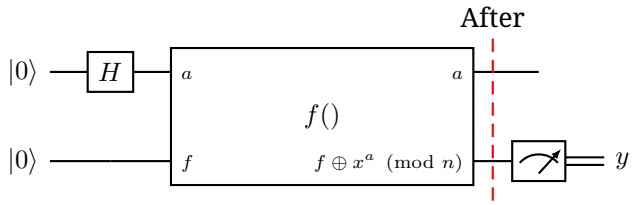

Figure 1: Создание 'периодического' состояния

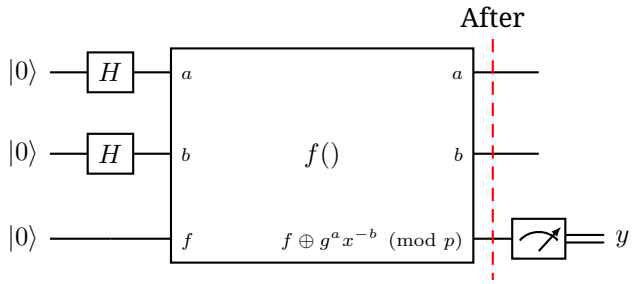

Figure 2: Создание DL состояния

RSA и поиск периода

Shor 96
Пусть n составное, произведение двух простых, x - элемент мультипликативной группы. Построим оракл $f()$ вычисляющий 'степень по модулю'. Измерим некоторый y, получим суперпозицию (линейную комбинацию) базисных состояний с неизвестным периодом.

$$\sum_a |a, x^a \pmod n\rangle \longrightarrow \sum_c e^{\frac{2\pi i}{q} ac} |a, x^a\rangle \tag{1}$$

Qiskit Summer School 2020, lecture 11
Пример 15=3*5 на четырех кубитах, $x = 13$, период (порядок группы) 4.
Если измеряем $y = 7$, получаем состояние $(|3\rangle + |7\rangle + |11\rangle + |15\rangle) \otimes |7\rangle$.

$$13^3 = 13^7 = 13^{11} = 13^{15} = 2197 = 7 \pmod{15} \tag{2}$$

DL и поиск периода

Shor 96
Пусть p простое, g, x - элементы мультипликативной группы, $x = g^r \pmod p$ для неизвестного r. Построим оракл $f()$ вычисляющий групповую операцию, применим QFT к входам, измерим конкретный y. Пусть $y = g^k$ для некоторого k.

$$\sum_{a,b} \left|a, b, g^a x^{-b} \pmod p\right\rangle \longrightarrow \sum_{\substack{c,d \\ a - rb \equiv k}} e^{\frac{2\pi i}{q}(ac+bd)} \left|a, b, g^a x^{-b}\right\rangle \tag{3}$$

Пусть $g^{\alpha_1} x^{\beta_1} = g^{\alpha_2} x^{\beta_2}$, тогда 'логарифм' $= -\frac{\alpha_2 - \alpha_1}{\beta_2 - \beta_1}$.

Новости

Г.Г.Амосов о MIP*=RE, 'Математические методы квантовых технологий'