Сравнительная вычислительная мощность квантовых и классических компьютеров широко изучается, начиная с изобретения квантовых вычислений. С этим связан вопрос, является ли квантовый оракул более мощным, чем классический.

Квантовый оракул — квантовый аналог устройства типа «черного ящика».

Квантовый оракул для квантовой гамильтоновой системы может быть определен как унитарный оператор

$$U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle,$$

где символом $\oplus$ обозначено побитовое сложение.

Унитарный оператор U_f для двухкубитной системы представляется четырьмя квантовыми вентилями, описываемыми матрицами 4 на 4, которые соответствуют четырем возможным функциям $f(x)$:

$$\hat{\mathrm{I}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$\hat{\mathrm{I}} \otimes \mathrm{NOT} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$\mathrm{CNOT} \cdot (\hat{\mathrm{I}} \otimes \mathrm{NOT}) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Квантовый оракул является обобщением классического оракула — устройства, вычисляющего функцию $f : G \rightarrow B^n$, где G — конечная группа, а $B = \{0,1\}$ — булево множество.

Квантовые оракулы используется в квантовых алгоритмах: алгоритме Дойча — Йожи и алгоритме Гровера.

В моделях квантовых роботов квантовые оракулы рассматриваются как частные случаи окружающей среды, не зависящей от времени.

- Валиев К. А., Кокин А. А. Квантовые компьютеры: надежды и реальность. Москва, Ижевск: Регулярная и хаотическая динамика, 2004. (стр.71-73)
- Китаев А., Шень А., Вялый М., Классические и квантовые вычисления. М.: МЦНМО, 1999. — 192 с. (стр.88-90)
- Бенёв П. «Квантовые роботы и окружающая среда» в книге Квантовые вычисления: за и против. РХД, 1999. — 213с. (стр.168-182)
- Квантовый оракур в arXiv.org

Источник — «http://ru.wikipedia.org/w/index.php?title=Квантовый_оракул&oldid=62259864

В статье http://math.mit.edu/news/summer/SPURprojects/2013Hwang.pdf рассмотрели две темы, которые дают частичные ответы на этот вопрос. Авторы показали, что возможно имитировать полиномиальное число столбцов квантового оракула классическим оракулом. В последнее время с появлением квантовых вычислений, исследователи http://theoryofcomputing.org/articles/v003a007/v003a007.pdf рассмотрели квантовые (QMA) протоколы Артура Мерлина http://en.wikipedia.org/wiki/Arthur%E2%80%93Merlin_protocol, позволяющие доказательству утверждения быть квантовым состоянием, а верификатору - квантовым компьютером. Кроме того, они определили систему QCMA доказательств, в которой доказательство классическое, но верификация является квантовой. Тогда возникает естественный вопрос: является QMA мощным, чем QCMA? Многие считают, что это правда, но это не было доказано. Лучшим известным результатом является разделение квантовых оракулов QMA и QCMA по Aaronson и Kuperberg http://theoryofcomputing.org/articles/v003a007/v003a007.pdf. В http://math.mit.edu/news/summer/SPURprojects/2013Hwang.pdf обобщили квантовое разделение оракулов QMA (Quantum Merlin Arthur) и QCMA (Quantum Classical Merlin Arthur), чтобы получить квантовый оракул, порожденный классическим оракулом и разделить эти классы.