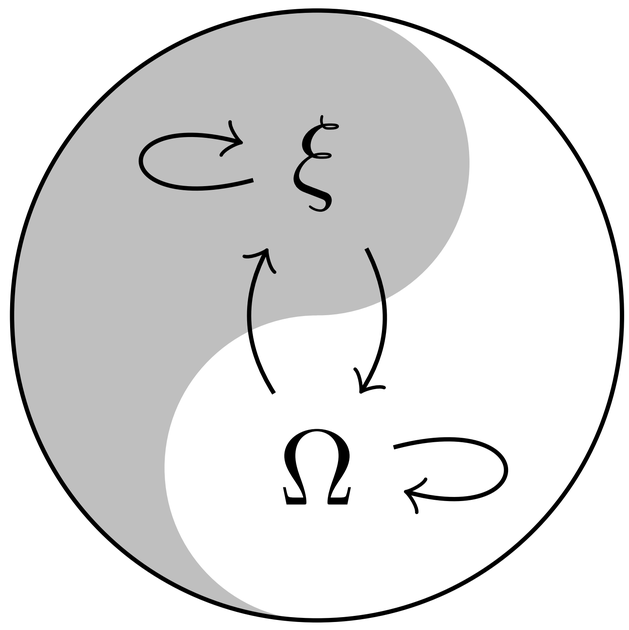
$\mathcal{P} \neq \mathcal{NP}$ и физическая реальность

О применении поля SU(2) к задачам теории графов

Андрей Ширай

School of Sciences,
Miskatonic University

shiray.and@gmail.com



Заседание №$\sqrt{2}$, 12-ого октября 2013, в комнате 401 Института математики (ул. Терещенковская, 3) в 14.00

Аннотация

Доказательство того, что $\mathcal{P} \neq \mathcal{NP}$ является одной из ключевых проблем современной Теоретической Информатики и Математики. Сомнений в том, что $\mathcal{P} \neq \mathcal{NP}$ (почти) нет, и этому есть не только интуитивно-исторические(ну раз так долго не смогли доказать, что равны, то значит неравны) и интуитивно-математические(схлопывание иерархий классов сложности выгледит подозрительно маловероятным), но и объективные физические сведетельства. Мы можем поставить вопрос равности классов $\mathcal{P}$ и $\mathcal{NP}$ в физической формулировке и свести это злополучное неравенство к физическим постулатам(конечность c, второе начало т/д), которые многократно проверены эксперементально и вполне надежны. Вот такая *эксперементальная математика*.

План

1 Физика – это процессы, Информатика – это процессы

1.1 Физика и Информатика с позиции Теории Категорий

Теория категорий	Физика	Теория вычислений
Объект X	Гильбертово пространство X	Тип данных X
Морфизм $f\colon X \to Y$	Оператор $f\colon X \to Y$	Программа $f\colon X \to Y$
Тензорное произведение объектов: $X \otimes Y$	Гильбертово пространство объединённой системы: $X \otimes Y$	Произведение типов данных: $X \otimes Y$

Таблица 1: The Rosetta Stone

1.2 Расширенный тезис Тьюринга-Черча

Утверждение 1.1. *Любая эффективно вычислимая функция может быть эффективно вычислена Машиной Тьюринга*

Утверждение 1.2. *Любая эффективно вычислимая функция может быть эффективно вычислена Вероятносной МТ*

Утверждение 1.3. *Любая эффективно вычислимая функция может быть эффективно вычислена Квантовой МТ*

Какой вариант правильный – мы не знаем. Важным для нас есть тот момент, что *эффективно вычислимая функция* – это чисто физическое понятие, точно так же, как и *вычислимая функция* в Тезиче Тьюринга-Черча. Поэтому их можно *эксперементально* проверить! Есть физическая система и есть алгоритм для расчета ее эволюции? Ок, Тезис Тьюринга-Черча верен. Есть физическая система(квантовая) и мы не можем ее проверить на классическом компьюторе? Значит утверждение 1.1 неверно. И т.д.

1.3 Термодинамика алгоритмических процессов

Исторически теория информации пошла из термодинамики и статфизики. Непосредственный перенос термодинамических соображений на алгоритмы возможен:

$$p = \frac{1}{Z} e^{-\beta E(x) - \gamma V(x) - \delta N(x)}$$

Распределение Гибса со статсуммой: $Z = \sum_{x \in X} e^{-\beta E(x) - \gamma V(x) - \delta N(x)}$ Но! Полученная "термодинамика" будет нефизична, так как статсумма невычислима! [1]

2 Алгоритм Гровера

2.1 Квантовая информатика одной табличной

Стохастика

$$\begin{pmatrix} s_{11} & \dots & s_{1n} \\ \vdots & \ddots & \vdots \\ s_{n1} & \dots & s_{nn} \end{pmatrix} \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} = \begin{pmatrix} q_1 \\ \vdots \\ q_n \end{pmatrix}$$

$$p_i \geq 0, \sum_{i=1}^{n} p_i = 1$$

"Кванты"

$$\begin{pmatrix} u_{11} & \dots & u_{1n} \\ \vdots & \ddots & \vdots \\ u_{n1} & \dots & u_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

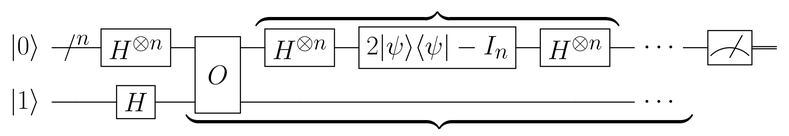
$$\alpha \in \mathbb{C}, \sum_{i=1}^{n} \|\alpha_i\|^2 = 1$$

[1] В часности, при $\beta = 0$, $\gamma = \ln 2$, $\delta = 0$: $Z = \Omega$ –константа Хатина

[2] Очевидно, что $O^2 = I$, так что унитарность сохраняется.

2.2 Алгоритм Гровера

Оператор Гровера G:



Выполняется $O(\sqrt{N})$ раз

Сначала формируют равномерне суперпозицию всех состояний: $\mathrm{H}^{\otimes n} |0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$. Чуть дальше будет обозначать для краткости равномерную суперпозицию как $|\psi\rangle$ Потом последовательно применяется оператор Гровера:

1. К входу применяется оракул O: $|x\rangle \to (-1)^{f(x)}|x\rangle$ Т.е. это единичная матрица, где на месте ответов стоят -1. [2]
2. Опять преобразование Адамара $\mathrm{H}^{\otimes n}$
3. Условный сдвиг фазы: $|x\rangle \to -(-1)^{\delta_{0x}|x\rangle}$, этой операции соответствует унитарный оператор $|0\rangle\langle 0| - I$.
4. Опять преобразование Адамара $\mathrm{H}^{\otimes n}$

$$G = (|\psi\rangle\langle\psi| - I)O$$

Физический смысл оператора G довольно простост – это вращение в двухмерном пространстве, порождаемом вектором $|\psi\rangle$ и ветором-решением. Мы можем переписать $|\psi\rangle$, как:

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$$

,где $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{\neg f(x)} |x\rangle$ и $|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{f(x)} |x\rangle$

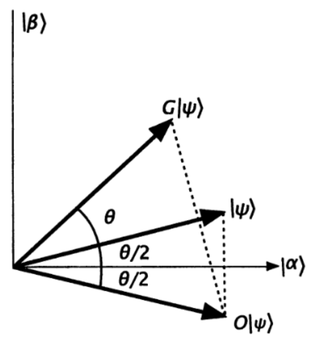


Рис. 1: Геометрическая интерпритация алгоритма Гровера

$$G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$$

$$G^k|\psi\rangle = \cos\frac{(2k+1)\theta}{2}|\alpha\rangle + \sin\frac{(2k+1)\theta}{2}|\beta\rangle$$

И необходимое количество итераций:

$$R = \lfloor \arccos\frac{\sqrt{M/N}}{\theta} \rfloor \overset{M \leq N/2}{=} \lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \rfloor$$

2.3 Оптимальность алгоритма Гровера

Теорема 2.1. *Алгоритм Гровера – оптимальный*

Идея доказательства состоит в оценке D_k – меры отклонения оракулом после k вызовов. Она растет не быстрее, чем $O(k^2)$ и имеет порядок $\Omega(N)$, откуда будет следовать, что необходимо не меньше $\Omega(\sqrt{N})$ обращений к оракулу.

$$O(\sqrt{N}) \wedge \Omega(\sqrt{N}) \Rightarrow \Theta(\sqrt{N})$$

2.4 Нелинейные теории КМ и прочее фричество

1. Линейность квантовой механики $\to$ Предел Гровера $\sqrt{N}$
2. Нелинейная КМ передает сигналы быстрее с и решает $\#\mathcal{P}$-полные проблемы за полиномиальное время! Ура!
3. ... попутно экспоненциально размножая ошибку. #$%&*!
4. Скрытые параметры? Предел Гровера улучшается с $N^{\frac{1}{2}}$ до $N^{\frac{1}{3}}$ – поиск по "историям" траекторий частичек
5. Зеноновские вычисления и всякие прочие супертьюринговые вычисления накрываются по достижении планковской длины.

3 Неподвижные точки и путешествия во времени

3.1 Неподвижные точки

Определение 3.1. ***Неподвижной точкой*** *некоторой функции f называется значение x такое, что $f(x) = x$.*

Определение 3.2. ***Комбинатор неподвижной точки*** *—- функция высшего порядка, которая вычисляет неподвижную точку заданной функции:*

$$f(FIX(f)) = FIX(f)$$

Пример 3.1.

$$Y := \lambda\ f.(\lambda\ x.f\ (x\ x))(\lambda\ x.f\ (x\ x))$$

$$\begin{aligned} Yf = (\lambda\ f.(\lambda\ x.f\ (x\ x))(\lambda\ x.f\ (x\ x)))f = \\ = (\lambda\ x.f\ (x\ x))(\lambda\ x.f\ (x\ x)) = \\ = f((\lambda\ x.f\ (x\ x))(\lambda\ x.f\ (x\ x))) = \\ = f(Yf) \end{aligned}$$

Пример 3.2. ***Факториал, "функциональный" вариант:***

$$F = \lambda\ f\ n.if\ n = 0\ then\ 1\ else\ n * f(n-1)$$

$$fact = YF$$

Функция F соответствует одному шагу рекурсии, комбинатор неподвижной точки реализует (рекурсивное) вычисление

3.2 Time travel for fun and profit

Для начала рассмотрим упрощенную стохастическую, а не квантовую систему

- Убил дедушку: $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$
- Не убил деда: $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- $$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \vec{v} = \vec{v}$$
- Неподвижная точка:

$$\vec{v} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

А теперь переходим от стохастических матриц к матрицам плотности:

$$\rho_{CTC} = S(\rho_{CTC}) \tag{1}$$

S – некий супероператор: $\rho \xrightarrow{S} \sum_i E_i \rho E_i^\dagger, \sum_i E_i^\dagger E_i = I$. Супероператор S не является произвольным. Для того, что бы уравнение 1 имело смысл результатом его применения должна быть матрица плотности.

Основной результат Дойча состоит в том, что:

Теорема 3.1. *Уравнение $\rho_{CTC} = S(\rho_{CTC})$ имеет неподвижную точку(т.е. оно всегда разрешимо)*

Идея времяпутешественных вычислений состоит в использовани временной петли аналогично оракулу.

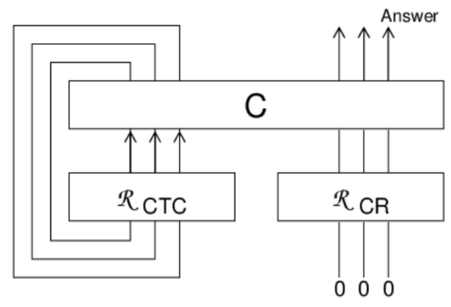


Рис. 2: Time travel for fun and profit

Список литературы

[1] Scott Aaronson. $\mathcal{NP}$-complete problems and physical reality. arXiv:quant-ph/0502072.

[2] Mike Stay John C. Baez. Physics, topology, logic and computation: A rosetta stone. arXiv:0903.0340 [quant-ph].

Благодарности

Я благодарен Николаю Вовчанскому и Василию Кузнецову за живительный пинок и идею организации семинара.