КАФЕДРА
ТЕЛЕМАТИКА

Санкт-Петербургский Государственный Политехнический Университет

Институт прикладной математики и механики

Методы исследовательской работы

анализ проблемы сложности вычислений
(занятие 5)

10 марта
2022 г.

Что было на прошлой лекции. Если все таки будет доказано, что P = NP, то

Это будет научная «революция» 5.0

- Доказательство любых математических теорем может быть найдено за полиномиальное время
- Любые последовательности (кодовые образцы) в множестве экспериментальных данных могут быть найдены за полиномиальное время от длины рассматриваемой последовательности данных
- Проблем Искусственного Интеллекта будут иметь полиномиально- эффективные алгоритмы.

Что надо было прочитать и постараться понять

АКАДЕМИЯ НАУК СССР

Научный совет по комплексной проблеме «Кибернетика»

Ю. А. ГАСТЕВ

ГОМОМОРФИЗМЫ И МОДЕЛИ

Логико-алгебраические аспекты моделирования

ИЗДАТЕЛЬСТВО «НАУКА»

Москва 1975

числа - «тени» Реальности

чтобы по «тени» «восстановить» еальность надо использовать интуицию

Под интуицией я подразумеваю **понимание**, настолько отчетливое, что не остается никакого сомнения относительно того, что мы разумеем.

Р. Декарт (1596 – 1650)

By **understanding**, I mean forming a physical picture that **intuitively** feels perfectly clear.

Р. Фейнман (1918-1988

Новая тема для доклада: утверждения о сложности вычислений как мере физической реализуемости

(A. Yao) Computational complexity of physical theories (e.g., general relativity)?

(Denek and Douglas): Computational complexity as a possible way to choose between various solutions ("landscapes") in physical theory.

Обсудим, суть фундаментальных проблем компьютерных наук

«…тем хуже для фактов, если они не укладываются в теорию»

М. Планк

- С точки зрения компьютерных наук любая сущность может быть материализована с помощью каскада вычислительных операций, если… эта сущность принципиально вычислима, т.е. мыслима (thinkable), - имеет конечное описание. Однако, с проведением самих вычислений связаны такие сложности как
  - оценка количества операций, которые требуются для получения решения
  - принцип относительности применительно к характеристики «точность/время вычислений;
  - отсутствие, в силу неравенства Гейзенберга, у некоторых объектов реальности «точной позиции»
  - модальность логических законов (эпистимическая, темпоральная логики)

Эти сложности могут ставить под вопрос «объективность» вычисленных результатов, с точки зрения их точности, своевременности, избыточности затрат и пр.

Суть проблем выражается в сентенции

«Computo ergo sum

\- **существует то, что можно вычислить**.

Любые вычисления обладают свойством интенсиональности, т.е. направленности на «что-то». Это свойство – есть инвариант механизма процессов «вычислений», т.е. механизм вычислений не зависит от того, существует ли или нет в данный момент то, **что вычисляется**.

В свою очередь, в основе «направленности» лежит феномен **понимания**, который не зависит от того «понимаем ли мы»

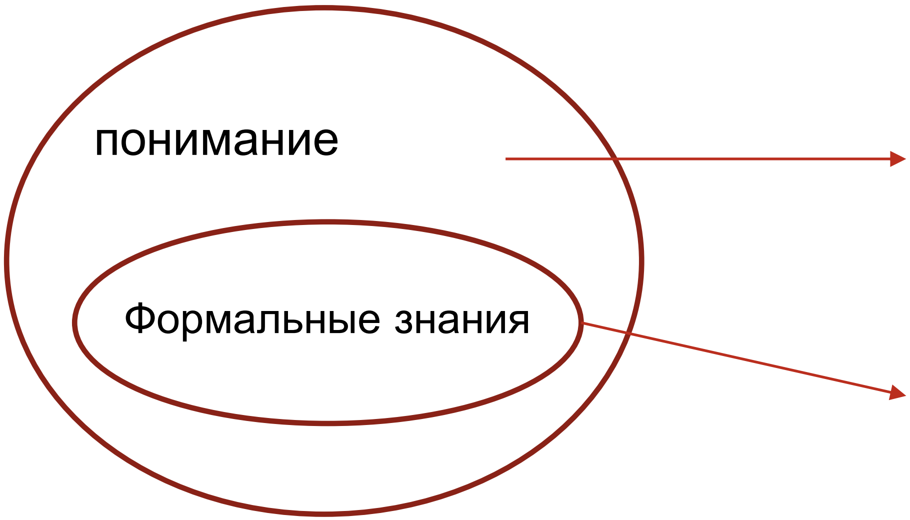
1) реальный, 2) лишь мыслимый или 3) вымышленный объект, т.е. природа «объекта» не важна или не имеет значение вычисляется

- атрибут конкретного объекта,
- параметры модели изучаемого объекта
- нечто воображаемое, т.е. существующее . виртуальное

Вопрос: Какими свойствами должен обладать «объект», чтобы его можно было вычислить ?

1) Объект должен «пониматься» как элемент некоторой **«числовой» структуры**
2) Над объектом можно проводить некоторые **«арифметические» операции**

Теория групп и задачи компьютерных наук



Использование <u>интуитивных</u> представлений о мыслимом объекте

Использование <u>формального</u> описания мыслимого объекта с помощью абстрактных понятий

В компьютерных науках :

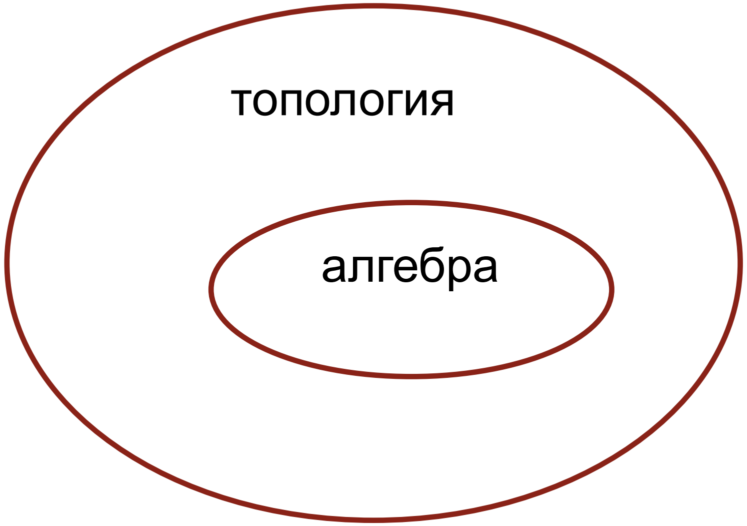
- **представление** - непрерывная схематизация взаимодействия субъекта с объектами природы на основе ассоциаций и использования классов эквивалентности.
- **описание** в форме кода исполняемой программы, включающей строгие теоретико-множественные, алгебраические или топологические структуры и операции

Абстракции и их интерпретации

Абстракция непрерывности – основа топологии и восприятия объектов реальности

топологическая алгебра;

алгебраическая топология



Основа вычислений: «универсальность» арифметических абстракций, что является необходимым условием существования «компьютерных» моделей реальности

Абстракция операций – основа логики, алгебры и арифметики и…. проблемы вычислительной сложности описания объектов и процессов Природы.

категории мышления с позиций сложности вычислений

Ключевой вопрос: Как сформулировать задачу, чтобы она имела решение, которое можно не только эффективно вычислить, но и ….. объяснить.
Для ответа на вопрос определяющее значение имеют **категории научного мышления**, которые основаны на том, что

- у любой проблемы есть решение
- решения состоят из последовательных этапов
- ошибки повышают уровень понимания задачи

В свою очередь категории математического мышления включают в себя подходы к решению задач на основе, развиваемой **в теории групп**:

- к исследуемому объекту (алгебраическое уравнение, дифференциальное уравнение, функция) применяют группу преобразований и анализируют полученную «реакцию».
- Инвариантность объекта по отношению к той или иной группе преобразований дает информацию об устройстве этого объекта и сложности вычисления его характеристик…..

Итого. Вся сложность вычислений в постановке задачи, а именно, что в задаче известно и какое свойство требуется найти, к какому воздействию задача инвариантна (т.е. не меняется решение задачи)...

Контраст причин появления задачи и следствий ее решения

причины незаметны, так как банальны, следствия загадочны и хорошо «замаскированы». В итоге, важные следствия порождаются весьма «пустяковыми» причинами.

- Так, все законы сохранения физики – следствия различных свойств симметрии, которые можно обнаружить в физическом пространстве.
- В основе любой симметрии лежит **инвариантность по отношению** к той или иной **группе преобразований**: *сдвиг во времени, перемещение и вращение 3D объекта как твердого тела* …

Формально, чтобы совокупность Ф преобразований f: X->X была **группой**, требуется:

1. если f(x), g(x) принадлежат Ф, то и f(g(x)) принадлежит Ф
2. в Ф входит тождественное отображение e(x)=x
3. любое отображение f из Ф имеет f^{-1} ,которое также принадлежит Ф. (не все физические процессы допускают «обращение», например в рамках парадигмы термодинамики имеется «стрела времени», нарушающая симметрию во времени

Примеры «групп»

- группа преобразований Лоренца – основа теория относительности
- группа Галуа преобразований алгебраических уравнений – основа решения уравнений в радикалах, полиномиальная арифметика
- группа Ли инвариантных преобразований гладких вещественных или комплексных многообразий

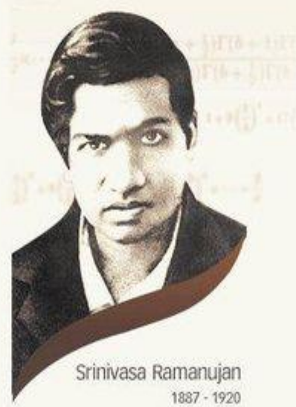
Группу комплексных чисел **a+ib** по умножению эквивалентно заменяет **группа** матриц:

$$\begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a * \underbrace{\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}}_{\text{“1”}} + b* \underbrace{\begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix}}_{\text{“i”}}$$

где $a^2 + b^2 = 1$, а умножение матриц – композиция операторов

Симметрично все, что закономерно, что закономерно - вычислимо

$$\sqrt{\frac{\pi e}{2}} = \cfrac{1}{1+\cfrac{1}{1+\cfrac{2}{1+\cfrac{3}{1+\cfrac{4}{1+\cfrac{5}{1+\cfrac{6}{1+\cfrac{7}{1+\cfrac{8}{1+\ddots}}}}}}}}} + \left\{1+\frac{1}{1\cdot 3}+\frac{1}{1\cdot 3\cdot 5}+\frac{1}{1\cdot 3\cdot 5\cdot 7}+\frac{1}{1\cdot 3\cdot 5\cdot 7\cdot 9}+\cdots\right\}$$



$$\sqrt{1+2\sqrt{1+3\sqrt{1+4\sqrt{1+\ldots}}}} = 3,$$

$$\sqrt{6+2\sqrt{7+3\sqrt{8+4\sqrt{9+\ldots}}}} = 4,$$

$$\sqrt{8-\sqrt{8+\sqrt{8-\sqrt{8-\ldots}}}} = 1+2\sqrt{3}\sin\frac{\pi}{9},$$

$$\sqrt{11-2\sqrt{11+2\sqrt{11-2\sqrt{11-\ldots}}}} = 1+4\sin\frac{\pi}{18},$$

$$\sqrt{23-2\sqrt{23+2\sqrt{23-2\sqrt{23-\ldots}}}} = 1+4\sqrt{3}\sin\frac{\pi}{9}.$$

Формулы Рамануджана:

Мир симметричен, любой закон природы и формулы математики свидетельствуют о той или иной инвариантности к изменению внешних условий. В чем причина инвариантных свойств – это групповые свойства преобразований

- движения, сохраняющих расстояние,
- переноса во времени
- зеркального отражения

Но уравнения физики не симметричны относительно свойств «причина/следствие»;

Справа или слева «причина» ?

$mx^{(2)} = F$

$\mathrm{rot}\, E = -a*dH/dt$

Знак «=« маскирует ответ.

О пользе абстрагирования

Вопрос: что важнее для вычислений – объект или операции над ним ? Давно замечено, что **аналоги** обычных арифметических операций имеются далеко **за пределами числовых систем**, т].е. умножать и складывать можно

как многочлены, матрицы, …

так и выпуклые тела и пр. объекты реального мира.

Абстрагирование от числовой специфики облегчает «алгебраизацию» наблюдаемых природных явлений, носителями которых может быть:

поле действительных или комплексных чисел, которые являются «единственными конечномерными действительными ассоциативно-коммутативными алгебрами без делителей нуля»;

тело кватернионов, которые являются единственной конечномерной ассоциативной, но не коммутативной алгеброй без делителей нуля….

что позволяет не допускать нелепых обобщений и выбирать «правильные инструменты» для решения прикладных задач.

Абстрагирование – путь к вычислениям

Понятие «абстрактное натуральное число» – для всех стало банальностью….неким очевидным «кирпичиком» описания физической реальности,….но есть и другие абстракции, например, «мнимая единица», многим не ясно, что это

– фикция, не имеющая физического аналога,
- особая точка д|р функции
- «тень» от обратных арифметических операций ?

Суть дела в том, что на определенной стадии манипулирования числами процесс выходит на новый уровень абстракции, фиксируя внимание не на самих числах-объектах, а на операциях с ними. Действия оказываются важнее тех объектов, над которыми они выполняются.

От арифметики над числами к абстрактной алгебре над кольцами телами полями

Можно ли вводить понятие «число», начиная не с натурального ряда и примеров, которые могут наглядно пояснить, в чем суть операций «сложения и умножения» ?
Для этого кроме самого «числа» надо определить свойства операций над ними. Эти операции должны удовлетворять свойствам, известным из арифметики над числами, например:

$a(b+c)=ab+ac$

Именно так поступают в рамках методов «абстрактной алгебры»

Примеры: чем можно заменить «число»

Кольцо – множество X с двумя бинарными операциями сложения и умножения, при условии:

- X – коммутативная группа по сложению
- умножение ассоциативно и выполняется дистрибутивный закон относительно введенных операций p*(q+r)=p*q+p*r

Если умножение еще и коммутативно, то кольцо называется «коммутативным», а если в X есть «единица», то по умножению, то говорят о кольце с единицей….например, кольцом являются различные числовые системы:

действительная прямая R
комплексная плоскость C
множество рациональных чисел Q
множество целых числе Z

а также:

множество квадратных матриц
множество многочленов с операциями сложения/умножения

Определение не исключает ситуацию a*b=0, при ненулевых a,b - это кольцо с делителями нуля. Кольца без делителей нуля – **целостные**.

Операции над алгебраическими кольцами

С помощью двух **колец** X, Y можно построить их прямую сумму X+Y, состоящую из всевозможных пар (x,y)….

Ненулевые элементы кольца могут составить группу по умножению (мультипикативную группу). Такое кольцо называется **телом, а** тело с коммутативным умножением называется **полем.**
Итак, поле

- это ненулевое коммутативное кольцо, в котором разрешимо любое уравнение ax=b, при a#0.
- вместе с любыми a,b содержит a*b, a+b, a-b, a/b.

Структура **поля** гарантирует разрешимость линейных уравнений, поэтому их изучение имеет важное значение.

Числовые объекты, операции, свойства

- Множество объектов, над которыми производятся операции, должно быть таким, чтобы с их помощью всегда можно представить решение уравнений:
    1. x+a=b, ax=b, решение находится в поле рациональных чисел Q, размерность числе n=1.
    2. $P_n(x)=0$, решение находится в поле комплексных чисел C a+bi, где i- мнимая единица sqrt(-1) =(+/-) i, размерность n=2.
- С точки зрения «физической реальности» число «i» не больше «фикция», чем отрицательные и дробные числа.
- Для операций сложения и умножения (обратные операции – вычитание и деление) комплексные числа «последняя граница» расширения натурального ряда. (но есть еще и т/н алгебраические и трансцендентные числа).
- За областью комплексных чисел новой «числовой земли» нет, так как при увеличении размерности чисел теряются не или иные их «арифметические» свойства:
    - при переходе от действительных (n=1) к комплексным (n=2) числам пропадает упорядоченность,
    - переход к квантернионам (n=4) теряется коммутативность умножения, при переходе к числам Кэли (n=8) теряется ассоциативность операций умножения…

Роль вычислительной сложности

Некоторые физические теории невозможны, так как конфликтуют с фундаментальными ограничениями, которые есть следствия принципиальной вычислительной сложности физической реальности…

Следствия теории сложности:

- существует мера вычислительной сложности
- существуют разрешимые и неразрешимые проблемы сложности
- существуют классы сложности P /NP/NP- полные классы
- сложность комбинаторных задач
- Имеют место «фазовые переходы» вычислительной сложности

Теория сложности в аспекте связей между физикой, математикой и компьютерными науками

- Обмена идеями и методами между физикой и компьютерными науками почти не происходит, исключая результаты, связанные с прямым численным моделированием процессов с использованием суперкомпьютеров
- Не смотря на это, те немногие научные результаты, которые были получены в последние несколько десятков лет, приводили к удивительным открытиям в обеих областях.
- Особый интерес имеет обмен идеями и методами между статистической механикой и теорией сложности вычислений.
- Так, рассмотрение физических проблем с позиций необходимых для их решения вычислительных ресурсов (процессорное время, память), уже привело к понятиям полиномиально (легко) и экспоненциально (сложно) решаемых физических проблем.

Формально трудные проблемы, как правило, можно переформулировать и ….легко численно решить.

- Теория сложности основана на оценках, относящихся к наихудшему случаю, который очень часто значительно отличается от типичного случая, усредненного по разумной совокупности экземпляров задач.
- Практика вычислений состоит в том, что трудные проблемы в общем случае, как правило, легко решить, но чтобы получить действительно трудные NP-полные для решения задачи их параметры должны быть тщательно подобраны из множества критических значений.
- При этом, вариация задачи в критической области ее параметров приводит к резким изменения вычислитепльтной сложности решаемой проблемы, что напоминает изменения, связанные с фазовыми переходами в физических системах – **лед-вода-пар**….

Фазовые переходы в физических и вычислительных системах

- Фазовые переходы в физике изучаются в рамках статистической механики, а аналогичные процессы изменения сложности в компьютерных науках – методами вероятностного анализа вычислительных задач, что позволяет
  - формальные оптимизационные задачи сформулировать в терминах достижения экстремальных значений переменных, имеющих ясный физический смысл (например, оптимизация методом «отжига»).
  - искать решения в классе суперпозиции возможных состояний (квантовые вычисления), а выбор конкретных значений производить методом статистических решений.

Мера сложности алгоритмов

- Понятие вычислительная сложность на практике это мера на множестве вычислительных ресурсов, которые отражают затраты времени, необходимых для решения прикладной проблемы. Однако, величина время существенно зависит от реализации алгоритма, а также от компьютера, на котором работает программа.
- В рамках теория сложности надо, прежде всего ответить на вопрос:
  - Что значит, что рассматриваемая физическая проблема вычислительно не разрешима ?
- Формально, проблема является разрешимой, если она может быть решена с помощью компьютерной программы, написанной на некотором языке программирования.

Временная сложность

- Рассмотрим наихудшую временную сложность $T(n) = \max t(x)$, где $t(x)$ – время работы алгоритма для входных данных x , а максимум берется по всем экземплярам задачи размера n.
- Время наихудшего случая является верхней границей для времени работы и основана на единице времени, которая не зависит от тактовой частоты конкретного процессора.
- Такой единицей является время, необходимое для выполнения элементарной операции, такой как сложение двух целых чисел.
- Измерение времени в этом случае означает подсчет количества элементарных операций, выполняемых алгоритмом.
- Далее не будем рассматривать точное число T(n) элементарных операций, а только их асимптотическое поведение T(n) для больших значений n, обозначаемых символами O (g(n))

$$T(n) \leq c*g(n), \text{ для } n \geq n_0$$

классы сложности

- временная сложность алгоритма является лишь верхней границей для его алгоритмической сложности, которая зависит от n – «размера задачи» .
- Пример. Умножение двух матриц n × n требует n^3 умножений, означает ли это, что задача умножения двух матриц n × n имеет сложность $O(n^3)$?
  - Нет, быстрый алгоритм умножения требует $O(n^a)$, $a<3$. Так «рекордное значение» $a=2.38$.
- Квадратная матрица nxn имеет n^2 элементов и не может иметь меньше элементов. Итак, проблема сложности вычислений зависит от двусмысленного понятия «размера».
- Все проблемы, которые могут быть решены полиномиальным алгоритмом, т.е. алгоритмом с временной сложностью (n^k) для некоторого k, объединяются вместе в класс «разрешимых».
- Проблемы, которые могут быть решены только алгоритмами с временем работы $O(2^n)$ или $O(n!)$, объединяются в один класс и называются «неразрешимых».

Полиномиальный и экспоненциальный аспект сложности

- . С практической точки зрения
  - экспоненциальный алгоритм $O(2^n)$ означает жесткий предел величины n доступного размера проблемы, решение которой возможно на имеющемся оборудовании.
  - полиномиальный алгоритм $O(n)$ или $O(n^2)$ гораздо менее драматично влияет на размер проблемы и может быть легко компенсировано модернизацией существующего оборудования
- Хотя алгоритм (n^{100}) превосходит алгоритм (2^n) только для задач, которые могут никогда не возникнуть в конкретном приложении.
- Полиномиальный алгоритм для задачи обычно сопровождается пониманием сути решаемой задачи, что позволяет найти полиномиальный алгоритм с малой степенью (n^k), $k = 1, 2,3$. Полиномиальные алгоритмы с $k > 10$ встречаются редко и возникают в довольно эзотерических случаях.

Пример. Взвешенный граф и его spanning tree – разрешимая задача

Рассмотрим граф G = (V,E), где вершины V, а E ребра взвешенного графа.

Задача состоит в том, чтобы найти подграф, соединяющий все вершины в графе, т.е. охватывающий подграф, ребра которого имеют минимальный суммарный вес.

Заметим, что граф не должен содержать циклов, а граф без циклов - это дерево, поэтому мы ищем минимальное остовное дерево во взвешенном графе.

Итак, найдите «остовное» дерево $T \subseteq G$ с минимальным общим весом.

Пример. Задача коммивояжера - Неразрешимые проблемы

Задача. Спланировать маршрут для коммивояжера, который должен посетить n городов. Дана карта со всеми городами и расстояниями между ними. Вопрос. В каком порядке коммивояжер должен посетить города, чтобы минимизировать общее расстояние, которое ему придется преодолеть.

На карте задается матрица расстояний (dij), где dij обозначает расстояние между городом номер i и городом номер j.

Маршрут задается циклической перестановкой : [1 . . . n] 7→ [1 . . . n], где (i) обозначает преемника города i, и ваша задача может быть определена как:

Дана матрица расстояний n × n с элементами dij ≥ 0. Найдите циклическую перестановку
p: [1 . . . n] → [1 . . . n], которая минимизирует

$$c_n(p) = \sum_{i=1}^{n} d_{ip(i)}$$

Заключение.
Можно найти хорошее решение для данной задачи ?

- В задаче коммивояжера существует (n - 1)! циклических перестановок, вычисление длины одного маршрута может быть выполнено за время O(n), следовательно, исчерпывающий поиск имеет сложность O(n!).
- Итого, оптимальный маршрут можно вычислить для «маленьких» значений n . (50! > число атомов во Вселенной)
- Существует ли идея, которая дает возможность быстро найти оптимальное решение ? **Этого пока никто не знает! Полиномиальный алгоритм для этой задачи до сих пор не найден**.
- Однако, есть несколько эффективных (т.е. полиномиальных) алгоритмов, которые позволяют **найти «хорошие» решения**, но не гарантируют получение оптимума. Согласно определению, эта задача формально является неразрешимой.
- **Вопрос: нужны ли в принципе «оптимальные» решения ? .**