О генерической сложности некоторых алгоритмических проблем

Александр Рыбалов

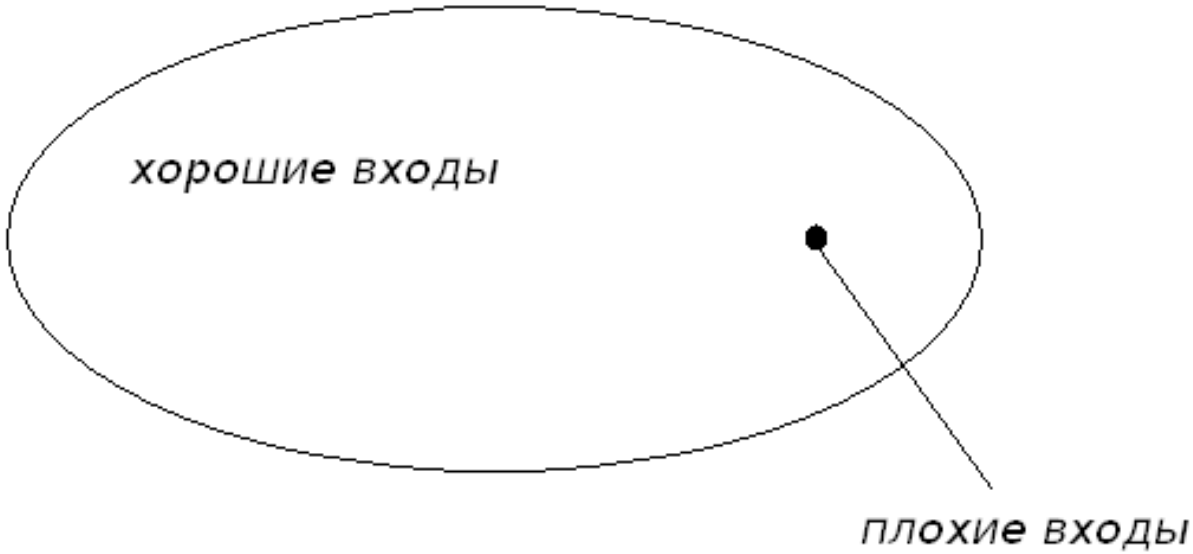
Институт математики им.С.Л.Соболева СО РАН, Омск

30 сентября, 2023

Классический подход

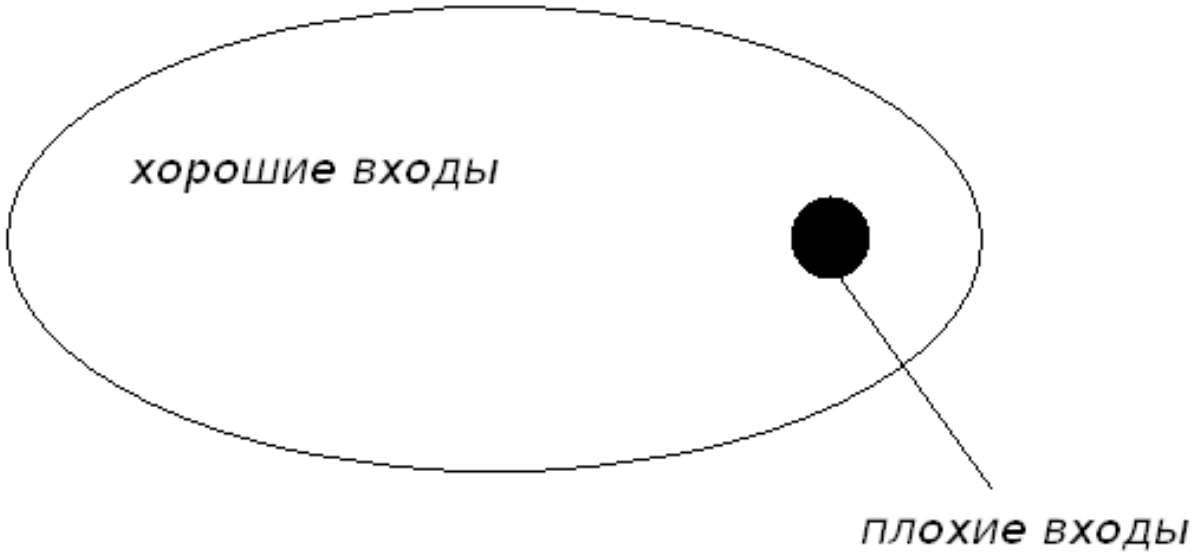
Алгоритм (быстро) работает на всех входах.

Сложность в среднем



Алгоритм быстро работает на почти всех входах, медленно на плохих, но $M(T_n) \leq p(n)$.

Генерический подход



Алгоритм быстро работает на почти всех входах и игнорирует плохие.

Сравнение подходов

Разрешимость (за полиномиальное время):

- Классически разрешима $\Rightarrow$ В среднем разрешима $\Rightarrow$ Генерически разрешима.
- Классически разрешима $\not\Leftarrow$ В среднем разрешима $\not\Leftarrow$ Генерически разрешима.

История

- 2003: И.Капович, А.Мясников, П.Шупп, В.Шпильрайн: Генерический подход к алгоритмическим проблемам в теории групп.

История

- 2003: И.Капович, А.Мясников, П.Шупп, В.Шпильрайн: Генерический подход к алгоритмическим проблемам в теории групп.
- 2008: А.Мясников, А.Рыбалов: Генерически неразрешимые проблемы в алгебре, логике, теории чисел.

История

- 2003: И.Капович, А.Мясников, П.Шупп, В.Шпильрайн: Генерический подход к алгоритмическим проблемам в теории групп.
- 2008: А.Мясников, А.Рыбалов: Генерически неразрешимые проблемы в алгебре, логике, теории чисел.
- 2012: К.Джокуш, П.Шупп: Генерическая вычислимость в рамках классической теории вычислимости, грубая вычислимость, генерические сводимости.

Предпосылки

- Проект MAGNUS – 1990-2000-е.
- Криптография
- Сложность в среднем (Левин, Гуревич, 1980-е)
- Симплекс-метод (А.Вершик, В.Спорышев, С.Смейл, 1984), Изоморфизм графов (П.Эрдеш, Л.Бабаи, С.Селков, 1980)

Позитивные результаты

1. Классические проблемы в различных конечно порожденных группах: И.Капович, А.Мясников, П.Шупп, В.Шпильрайн, В.Н.Ремесленников, А.Боровик, В.А.Романьков, Р.Гилман, В.Диккерт, А.Ушаков, А.Вайс, и др.

Позитивные результаты

1. Классические проблемы в различных конечно порожденных группах: И.Капович, А.Мясников, П.Шупп, В.Шпильрайн, В.Н.Ремесленников, А.Боровик, В.А.Романьков, Р.Гилман, В.Диккерт, А.Ушаков, А.Вайс, и др.
2. Проблема равенства в некоторых полугруппах (Цейтина, Маканина, с одним соотношением): Д.Вон (2008), А.Рыбалов (2022).

Позитивные результаты

1. Классические проблемы в различных конечно порожденных группах: И.Капович, А.Мясников, П.Шупп, В.Шпильрайн, В.Н.Ремесленников, А.Боровик, В.А.Романьков, Р.Гилман, В.Диккерт, А.Ушаков, А.Вайс, и др.
2. Проблема равенства в некоторых полугруппах (Цейтина, Маканина, с одним соотношением): Д.Вон (2008), А.Рыбалов (2022).
3. Проблема остановки для машин Тьюринга с лентой, бесконечной в одном направлении: А.Мясников, Д.Хэмкинс (2004).

Позитивные результаты

1. Классические проблемы в различных конечно порожденных группах: И.Капович, А.Мясников, П.Шупп, В.Шпильрайн, В.Н.Ремесленников, А.Боровик, В.А.Романьков, Р.Гилман, В.Диккерт, А.Ушаков, А.Вайс, и др.
2. Проблема равенства в некоторых полугруппах (Цейтина, Маканина, с одним соотношением): Д.Вон (2008), А.Рыбалов (2022).
3. Проблема остановки для машин Тьюринга с лентой, бесконечной в одном направлении: А.Мясников, Д.Хэмкинс (2004).
4. Проблема изоморфизма конечных полугрупп: А.Рыбалов (2021).

Отрицательные результаты

1. Проблема остановки для нормализованных машин Тьюринга (А.Рыбалов, 2016).

Отрицательные результаты

1. Проблема остановки для нормализованных машин Тьюринга (А.Рыбалов, 2016).
2. Проблема равенства в некоторых полугруппах (А.Рыбалов, А.Мясников, 2008).

Отрицательные результаты

1. Проблема остановки для нормализованных машин Тьюринга (А.Рыбалов, 2016).
2. Проблема равенства в некоторых полугруппах (А.Рыбалов, А.Мясников, 2008).
3. Некоторые элементарные теории (А.Рыбалов, А.Мясников, 2008).

Отрицательные результаты

1. Проблема остановки для нормализованных машин Тьюринга (А.Рыбалов, 2016).
2. Проблема равенства в некоторых полугруппах (А.Рыбалов, А.Мясников, 2008).
3. Некоторые элементарные теории (А.Рыбалов, А.Мясников, 2008).
4. Десятая проблема Гильберта (А.Рыбалов, 2013).

Отрицательные результаты

1. Проблема остановки для нормализованных машин Тьюринга (А.Рыбалов, 2016).
2. Проблема равенства в некоторых полугруппах (А.Рыбалов, А.Мясников, 2008).
3. Некоторые элементарные теории (А.Рыбалов, А.Мясников, 2008).
4. Десятая проблема Гильберта (А.Рыбалов, 2013).
5. Арифметика Пресбургера (А.Рыбалов, 2010).

Отрицательные результаты

1. Проблема остановки для нормализованных машин Тьюринга (А.Рыбалов, 2016).
2. Проблема равенства в некоторых полугруппах (А.Рыбалов, А.Мясников, 2008).
3. Некоторые элементарные теории (А.Рыбалов, А.Мясников, 2008).
4. Десятая проблема Гильберта (А.Рыбалов, 2013).
5. Арифметика Пресбургера (А.Рыбалов, 2010).
6. Конечно порожденная группа с генерически неразрешимой проблемой равенства (А.Мясников, Д.Осин, 2009).

Открытые проблемы

Проблема 1 (А.Мясников, Д.Хэмкинс, 2004)

Будет ли генерически разрешимой проблема остановки для машин Тьюринга с лентой, бесконечной в обоих направлениях?

Открытые проблемы

Проблема 1 (А.Мясников, Д.Хэмкинс, 2004)

Будет ли генерически разрешимой проблема остановки для машин Тьюринга с лентой, бесконечной в обоих направлениях?

Проблема 2 (А.Мясников, Д.Осин, 2009)

Существует ли конечно определенная группа с генерически неразрешимой проблемой равенства?

Открытые проблемы

Проблема 1 (А.Мясников, Д.Хэмкинс, 2004)

Будет ли генерически разрешимой проблема остановки для машин Тьюринга с лентой, бесконечной в обоих направлениях?

Проблема 2 (А.Мясников, Д.Осин, 2009)

Существует ли конечно определенная группа с генерически неразрешимой проблемой равенства?

Проблема 3 (А.Мясников, 2016)

Существует ли конечно порожденная группа с разрешимой проблемой равенства, генерически неразрешимой за полиномиальное время?

Генерические множества

Определение

Пусть I – все входы, I_n – все входы размера n.

Асимптотическая плотность множества $S \subseteq I$

$$\rho(S) = \lim_{n\to\infty} \rho_n = \lim_{n\to\infty} \frac{|S \cap I_n|}{|I_n|}.$$

Генерические множества

Определение

Пусть I – все входы, I_n – все входы размера n.

Асимптотическая плотность множества $S \subseteq I$

$$\rho(S) = \lim_{n\to\infty} \rho_n = \lim_{n\to\infty} \frac{|S \cap I_n|}{|I_n|}.$$

Определение

Множество входов $S \subseteq I$ называется

- **генерическим** если $\rho(S) = 1$,

Генерические множества

Определение

Пусть I – все входы, I_n – все входы размера n.

Асимптотическая плотность множества $S \subseteq I$

$$\rho(S) = \lim_{n\to\infty} \rho_n = \lim_{n\to\infty} \frac{|S \cap I_n|}{|I_n|}.$$

Определение

Множество входов $S \subseteq I$ называется

- **генерическим** если $\rho(S) = 1$,
- **пренебрежимым** если $\rho(S) = 0$,

Генерические множества

Определение

Пусть I – все входы, I_n – все входы размера n.

Асимптотическая плотность множества $S \subseteq I$

$$\rho(S) = \lim_{n\to\infty} \rho_n = \lim_{n\to\infty} \frac{|S \cap I_n|}{|I_n|}.$$

Определение

Множество входов $S \subseteq I$ называется

- **генерическим** если $\rho(S) = 1$,
- **пренебрежимым** если $\rho(S) = 0$,
- **сильно генерическим** если последовательность ρ_n экспоненциально быстро стремится к 1,

Генерические множества

Определение

Пусть I – все входы, I_n – все входы размера n.

Асимптотическая плотность множества $S \subseteq I$

$$\rho(S) = \lim_{n\to\infty} \rho_n = \lim_{n\to\infty} \frac{|S \cap I_n|}{|I_n|}.$$

Определение

Множество входов $S \subseteq I$ называется

- **генерическим** если $\rho(S) = 1$,
- **пренебрежимым** если $\rho(S) = 0$,
- **сильно генерическим** если последовательность ρ_n экспоненциально быстро стремится к 1,
- **сильно пренебрежимым**, если ρ_n экспоненциально быстро стремится к 0.

Генерические алгоритмы

Определение

Алгоритм $\mathcal{A}$ с множеством входов I и множеством выходов $J \cup \{?\}$ $(? \notin J)$ называется **(сильно) генерическим**, если

1. $\mathcal{A}$ останавливается на всех входах из I,
2. множество $BH(\mathcal{A}) = \{x \in I : \mathcal{A}(x) = ?\}$ (сильно) пренебрежимо.

Генерические алгоритмы

Определение

Алгоритм $\mathcal{A}$ с множеством входов I и множеством выходов $J \cup \{?\}$ $(? \notin J)$ называется **(сильно) генерическим**, если

1. $\mathcal{A}$ останавливается на всех входах из I,
2. множество $BH(\mathcal{A}) = \{x \in I : \mathcal{A}(x) = ?\}$ (сильно) пренебрежимо.

Определение

Генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если для всех $x \in I$ $\mathcal{A}(x) = y \in J \Rightarrow f(x) = y$.

Генерические алгоритмы

Определение

Алгоритм $\mathcal{A}$ с множеством входов I и множеством выходов $J \cup \{?\}$ $(? \notin J)$ называется **(сильно) генерическим**, если

1. $\mathcal{A}$ останавливается на всех входах из I,
2. множество $BH(\mathcal{A}) = \{x \in I : \mathcal{A}(x) = ?\}$ (сильно) пренебрежимо.

Определение

Генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если для всех $x \in I$ $\mathcal{A}(x) = y \in J \Rightarrow f(x) = y$.

Определение

Множество $A \subseteq I$ **генерически (сильно) разрешимо**, если существует (сильно) генерический алгоритм, вычисляющий характеристическую функцию множества A.

Свежие результаты

1. Проблема о рюкзаке для матричных полугрупп
2. Проблема извлечения корня по простому модулю
3. Проблема кластеризации графа с ограничениями на размеры кластеров
4. Проблема факторизации целых чисел

Проблема о рюкзаке в полугруппах

Мясников, Николаев и Ушаков в 2015 году сформулировали аналог классической проблемы о рюкзаке для произвольных (полу) групп. Пусть S – полугруппа.

Проблема о рюкзаке в полугруппах

Мясников, Николаев и Ушаков в 2015 году сформулировали аналог классической проблемы о рюкзаке для произвольных (полу) групп. Пусть S – полугруппа.

Проблема о рюкзаке в S

Пусть даны элементы $(a_1, a_2, \ldots, a_n, a)$ из S. Определить, существуют ли степени $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \mathbb{N} \cup \{0\}$ такие, что имеет место

$$a_1^{\varepsilon_1} a_2^{\varepsilon_2} \ldots a_n^{\varepsilon_n} = a.$$

Проблема о рюкзаке в полугруппах

Мясников, Николаев и Ушаков в 2015 году сформулировали аналог классической проблемы о рюкзаке для произвольных (полу) групп. Пусть S – полугруппа.

Проблема о рюкзаке в S

Пусть даны элементы $(a_1, a_2, \ldots, a_n, a)$ из S. Определить, существуют ли степени $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \mathbb{N} \cup \{0\}$ такие, что имеет место

$$a_1^{\varepsilon_1} a_2^{\varepsilon_2} \ldots a_n^{\varepsilon_n} = a.$$

Лемма

Проблема о рюкзаке в полугруппах целочисленных матриц порядка больше 1 является NP-полной.

Моноид $SL(2, \omega)$

- ω – натуральные числа с 0.

Моноид $SL(2, \omega)$

- ω – натуральные числа с 0.
- Моноид $SL(2, \omega)$ – множество матриц порядка 2 с элементами из ω и определителем 1.

Моноид $SL(2, \omega)$

- ω – натуральные числа с 0.
- Моноид $SL(2, \omega)$ – множество матриц порядка 2 с элементами из ω и определителем 1.
- Размер матрицы $M \in SL(2, \omega)$ есть максимум длин двоичной записи элементов.

Моноид $SL(2, \omega)$

- ω – натуральные числа с 0.
- Моноид $SL(2, \omega)$ – множество матриц порядка 2 с элементами из ω и определителем 1.
- Размер матрицы $M \in SL(2, \omega)$ есть максимум длин двоичной записи элементов.
- Во входе $(M_1, \ldots, M_n, M)$ размера n все M_i имеют размер $\leq n$, а M имеет размер $\leq n^2$.

Структура $SL(2,\omega)$

Теорема (Нильсен, 1924)

$SL(2,\omega)$ – свободный моноид с порождающими:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Структура $SL(2,\omega)$

Теорема (Нильсен, 1924)

$SL(2,\omega)$ – свободный моноид с порождающими:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Найти словарное представление матрицы $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ можно с помощью вычитательного алгоритма Евклида:

$$A^{-1}M = \begin{pmatrix} a-c & b-d \\ c & d \end{pmatrix},\ B^{-1}M = \begin{pmatrix} a & b \\ c-a & d-b \end{pmatrix}.$$

$$M \to M_1 \to M_2 \to \ldots \to M_t = E.$$

Словарное представление для почти всех матриц

Лемма

Множество матриц $M \in SL(2, \omega)$ таких, что их словарное представление $\leq size(M)^2$, является генерическим.

Словарное представление для почти всех матриц

Лемма

Множество матриц $M \in SL(2, \omega)$ таких, что их словарное представление $\leq size(M)^2$, является генерическим.

Теорема (Кнут, Яо, 1975)

Пусть $t(m, n)$ есть число шагов вычитательного алгоритма Евклида на входе (m, n). Тогда

$$\sum_{m \leq n} t(m, n) = \frac{6}{\pi} n (\log n)^2 + O(n \log n (\log \log n)^2).$$

Проблема о рюкзаке над $SL(2, \omega)$

Теорема

Проблема о рюкзаке над $SL(2, \omega)$ генерически полиномиально разрешима.

Проблема о рюкзаке над $SL(2, \omega)$

Теорема

Проблема о рюкзаке над $SL(2, \omega)$ генерически полиномиально разрешима.

Идея: динамическое программирование!

Проблема извлечения квадратного корня по простому модулю

Проблема

Заданы простое число p и натуральное число $a < p$ в двоичном виде. Найти такое натуральное $x < p$, что $x^2 = a \mod p$, если оно существует.

Проблема извлечения квадратного корня по простому модулю

Проблема

Заданы простое число p и натуральное число $a < p$ в двоичном виде. Найти такое натуральное $x < p$, что $x^2 = a \mod p$, если оно существует.

Открытый вопрос (Адлеман, МакКарли, 1994)

Существует ли полиномиальный алгоритм для решения этой проблемы?

Проблема извлечения квадратного корня по простому модулю

Определение

Натуральное число $a < p$ называется **квадратичным вычетом** по модулю p, если существует натуральное $x < p$ такое, что $x^2 = a \mod p$. Иначе это **квадратичный невычет**.

Проблема извлечения квадратного корня по простому модулю

Определение

Натуральное число $a < p$ называется **квадратичным вычетом** по модулю p, если существует натуральное $x < p$ такое, что $x^2 = a \mod p$. Иначе это **квадратичный невычет**.

Известный факт

Среди чисел $\{1, 2, \ldots, p-1\}$ половина – квадратичные вычеты, половина – невычеты.

Проблема извлечения квадратного корня по простому модулю

Определение

Натуральное число $a < p$ называется **квадратичным вычетом** по модулю p, если существует натуральное $x < p$ такое, что $x^2 = a \mod p$. Иначе это **квадратичный невычет**.

Известный факт

Среди чисел $\{1, 2, \ldots, p-1\}$ половина – квадратичные вычеты, половина – невычеты.

Теорема (Эйлер)

Пусть p – нечетное простое число. Натуральное число a является квадратичным вычетом по модулю p тогда и только тогда, когда

$$a^{(p-1)/2} = 1 \ (\mod p).$$

Проблема извлечения квадратного корня по простому модулю

Алгоритм (Чиполла, 1904)

1. Вход: (p, a) и квадратичный невычет b.
2. Квадратный корень получается путем вычисления по формуле $x = \left(a + \sqrt{b}\right)^{(p+1)/2}$ в поле $\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{b})$ – квадратичном расширении поля $\mathbf{F}_p$.

Проблема извлечения квадратного корня по простому модулю

Алгоритм (Чиполла, 1904)

1. Вход: (p, a) и квадратичный невычет b.
2. Квадратный корень получается путем вычисления по формуле $x = \left(a + \sqrt{b}\right)^{(p+1)/2}$ в поле $\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{b})$ – квадратичном расширении поля $\mathbf{F}_p$.

Проблема

Как быстро найти квадратичный невычет?

Проблема извлечения квадратного корня по простому модулю

Алгоритм (Чиполла, 1904)

1. Вход: (p, a) и квадратичный невычет b.
2. Квадратный корень получается путем вычисления по формуле $x = \left(a + \sqrt{b}\right)^{(p+1)/2}$ в поле $\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{b})$ – квадратичном расширении поля $\mathbf{F}_p$.

Проблема

Как быстро найти квадратичный невычет?

Пусть $\eta(p)$ – наименьший квадратичный невычет по модулю p.

Проблема извлечения квадратного корня по простому модулю

Алгоритм (Чиполла, 1904)

1. Вход: (p, a) и квадратичный невычет b.
2. Квадратный корень получается путем вычисления по формуле $x = \left(a + \sqrt{b}\right)^{(p+1)/2}$ в поле $\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{b})$ – квадратичном расширении поля $\mathbf{F}_p$.

Проблема

Как быстро найти квадратичный невычет?

Пусть $\eta(p)$ – наименьший квадратичный невычет по модулю p.

Теорема (Анкени, 1952)

В предположении истинности расширенной гипотезы Римана, существует константа C такая, что для любого простого p имеет место $\eta(p) < C(\log p)^2$.

Проблема извлечения квадратного корня по простому модулю

Теорема

Проблема извлечения квадратного корня по простому модулю генерически разрешима за полиномиальное время.

Проблема извлечения квадратного корня по простому модулю

Теорема

Проблема извлечения квадратного корня по простому модулю генерически разрешима за полиномиальное время.

Теорема (П.Эрдеш, 1961)

Существует константа $3 < C < 4$ такая, что

$$\lim_{k\to\infty} \frac{\sum_{p\le k} \eta(p)}{\pi(k)} = C.$$

Здесь суммирование берется по простым p.

Проблема кластеризации графа

Определение

Граф называется **кластерным**, если каждая его связная компонента является полным графом. Обозначим через $\mathcal{M}^{\leq p}(V)$ множество всех кластерных графов на множестве вершин V, у которых каждая компонента связности имеет не более p вершин.

Проблема кластеризации графа

Определение

Граф называется **кластерным**, если каждая его связная компонента является полным графом. Обозначим через $\mathcal{M}^{\leq p}(V)$ множество всех кластерных графов на множестве вершин V, у которых каждая компонента связности имеет не более p вершин.

Определение

Если $G_1 = (V, E_1)$ и $G_2 = (V, E_2)$ – графы на одном и том же множестве вершин V, то **расстояние** $\rho(G_1, G_2)$ между ними есть число несовпадающих рёбер в графах G_1 и G_2.

Проблема кластеризации графа

Определение

Граф называется **кластерным**, если каждая его связная компонента является полным графом. Обозначим через $\mathcal{M}^{\leq p}(V)$ множество всех кластерных графов на множестве вершин V, у которых каждая компонента связности имеет не более p вершин.

Определение

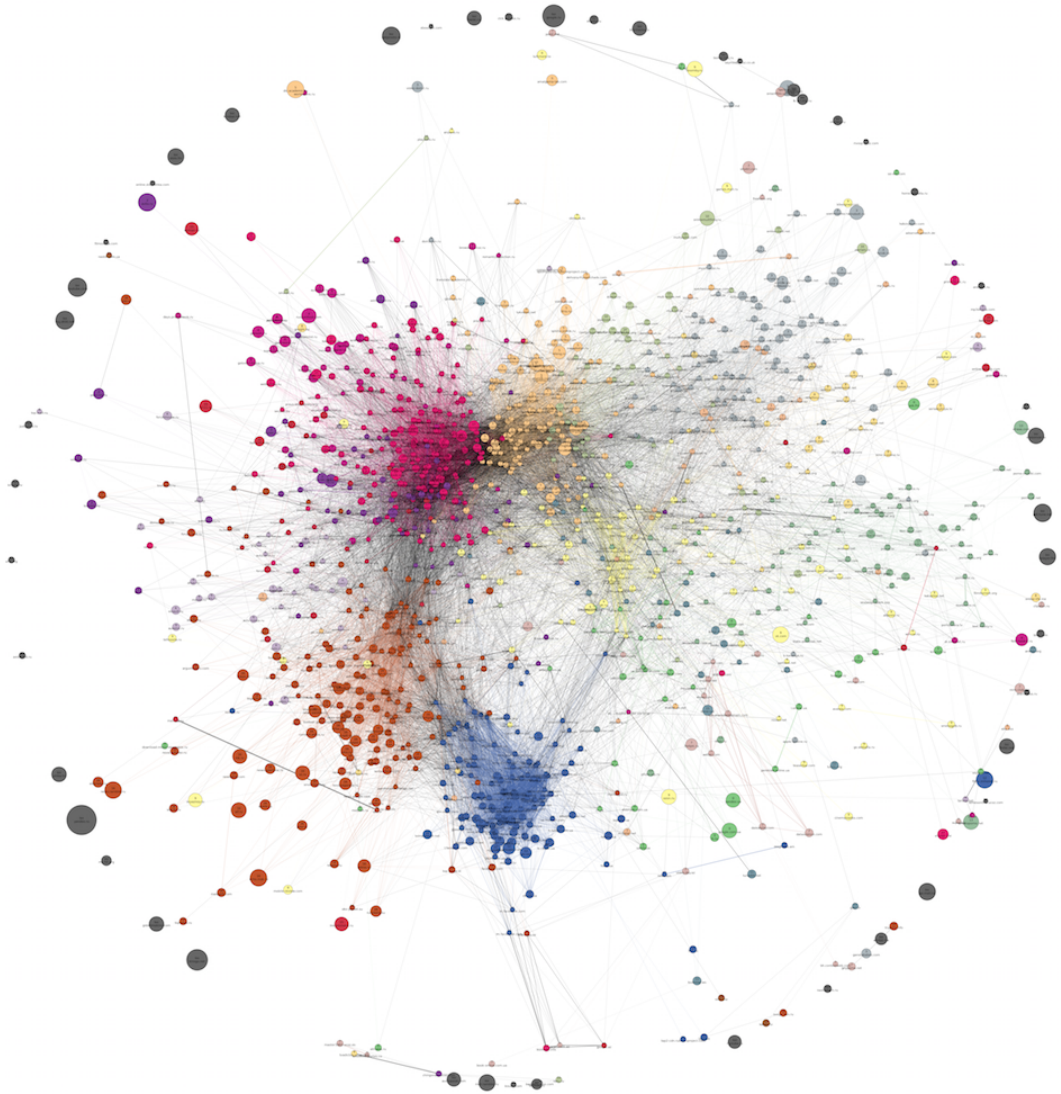
Если $G_1 = (V, E_1)$ и $G_2 = (V, E_2)$ – графы на одном и том же множестве вершин V, то **расстояние** $\rho(G_1, G_2)$ между ними есть число несовпадающих рёбер в графах G_1 и G_2.

Проблема p-кластеризации графа

Задан граф $G = (V, E)$. Найти такой граф $M^* \in \mathcal{M}^{\leq p}(V)$, что

$$\rho(G, M^*) = \min_{M \in \mathcal{M}^{\leq p}(V)} \rho(G, M).$$

Проблема кластеризации графа



Проблема кластеризации графа

Теорема (В.П.Ильев, А.А.Навроцкая, 2011)

Проблема p-кластеризации графа является NP-трудной при $p \geq 3$.

Проблема кластеризации графа

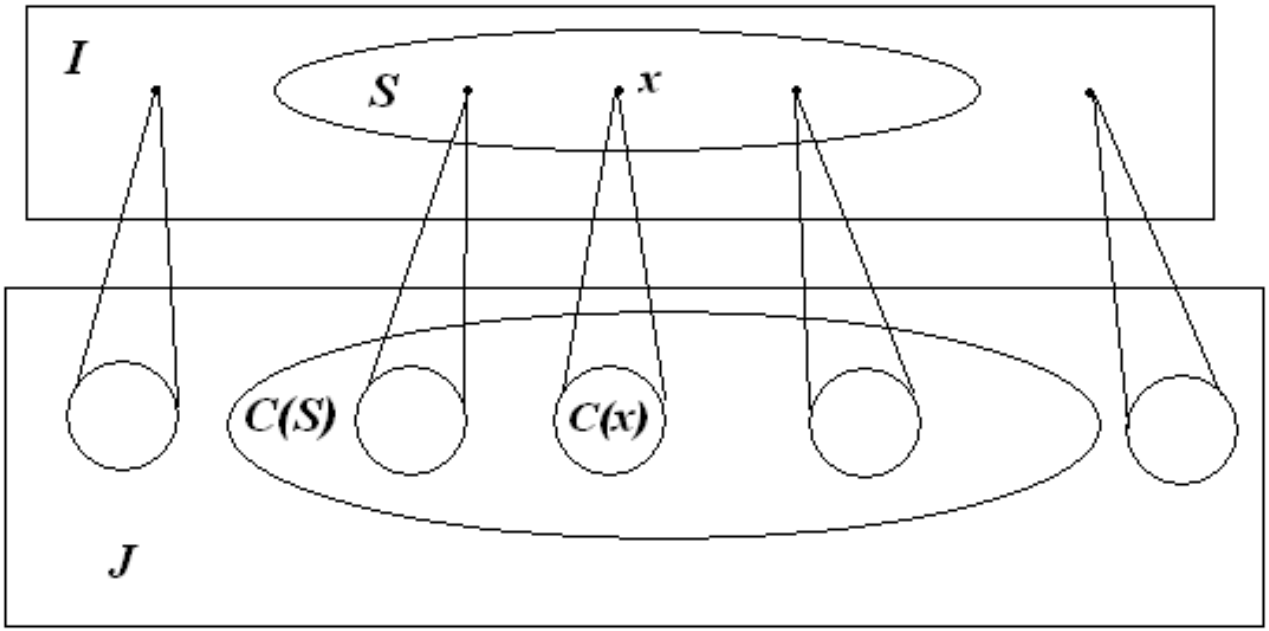
Теорема (В.П.Ильев, А.А.Навроцкая, 2011)

Проблема p-кластеризации графа является NP-трудной при $p \geq 3$.

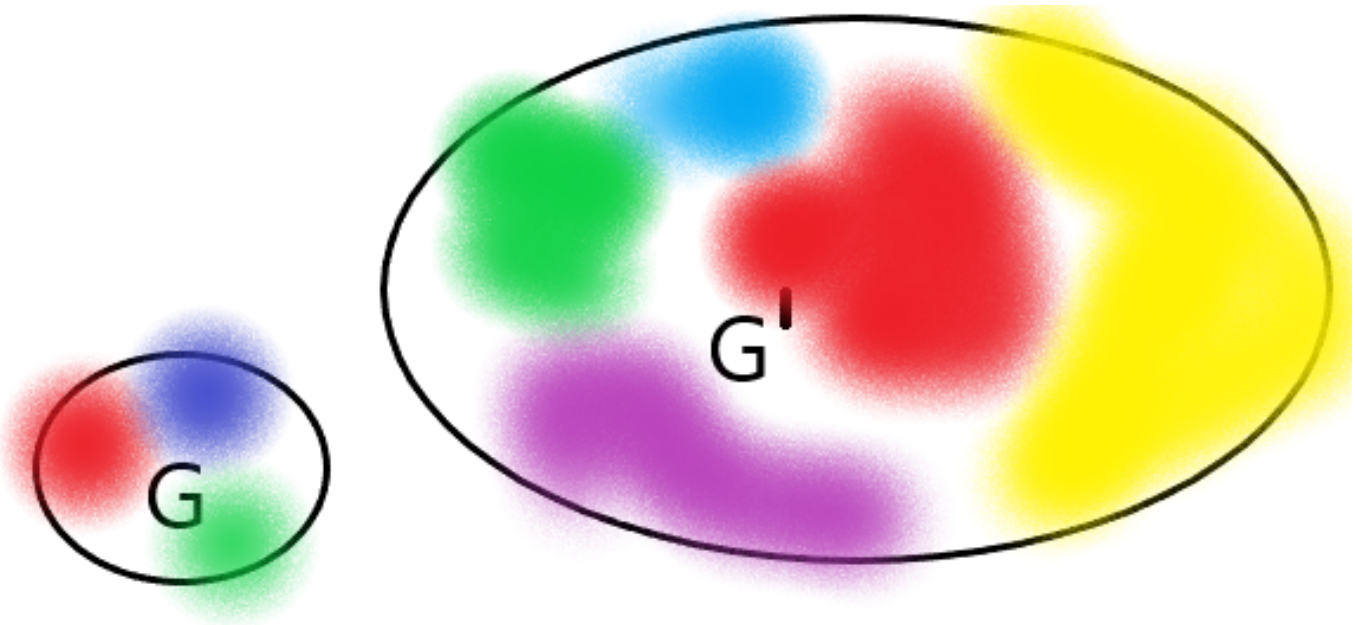
Теорема

Не существует сильно генерического полиномиального алгоритма для решения проблемы p-кластеризации графов при $p \geq 3$, если $P \neq NP$ и $P = BPP$.

Генерическая амплификация



Генерическая амплификация проблемы кластеризации графа



Проблема факторизации целых чисел

Проблема факторизации

Дано натуральное число N, записанное в двоичной системе. Необходимо найти его разложение в произведение степеней простых чисел: $N = p_1^{k_1} \dots p_m^{k_m}$.

Проблема факторизации целых чисел

Проблема факторизации

Дано натуральное число N, записанное в двоичной системе. Необходимо найти его разложение в произведение степеней простых чисел: $N = p_1^{k_1} \dots p_m^{k_m}$.

Открытый вопрос

Существует ли полиномиальный алгоритм для решения проблемы факторизации?

Проблема факторизации целых чисел

Проблема факторизации

Дано натуральное число N, записанное в двоичной системе. Необходимо найти его разложение в произведение степеней простых чисел: $N = p_1^{k_1} \dots p_m^{k_m}$.

Открытый вопрос

Существует ли полиномиальный алгоритм для решения проблемы факторизации?

Открытый вопрос (Адлеман, МакКарли, 1994)

Существует ли генерический полиномиальный алгоритм для решения проблемы факторизации? Или хотя бы полиномиальный алгоритм, решающий ее на непренебрежимом множестве?

Проблема факторизации целых чисел

Теорема

Если для проблемы факторизации не существует полиномиального алгоритма и $\mathrm{P} = \mathrm{BPP}$, то для нее не существует сильно генерического полиномиального алгоритма.

Проблема факторизации целых чисел

Теорема

Если для проблемы факторизации не существует полиномиального алгоритма и P = BPP, то для нее не существует сильно генерического полиномиального алгоритма.

Лемма (Идея амплификации)

Существует полиномиальный алгоритм, который для любых натуральных чисел N, M по разложению на простые множители их произведения $NM = p_1^{k_1} \dots p_m^{k_m}$ находит разложение на простые множители отдельно для чисел N и M.

Спасибо за внимание!

Спасибо за внимание!