О некоторых задачах дискретной оптимизации на группах

Андрей Николаев
(Stevens Institute of Technology)

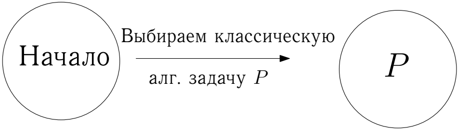
Омск, 30 Апреля 2015

По мотивам совместной работы с
А.Мясниковым, А.Ушаковым и Е.Френкель

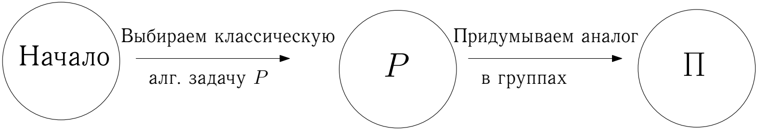
Публикации

- A.Miasnikov, A.N., A.Ushakov.
  - *Knapsack Problems in Groups,*
    Mathematics of Computation, 2015.
  - *The Post correspondence problem in groups,*
    Journal of Group Theory, 2014.
  - *Lattice problems in groups,*
    препринт.
- A.N., A.Ushakov, E.Frenkel.
  - *Knapsack problems in products of groups*
    Journal of Symbolic Computation, принята.

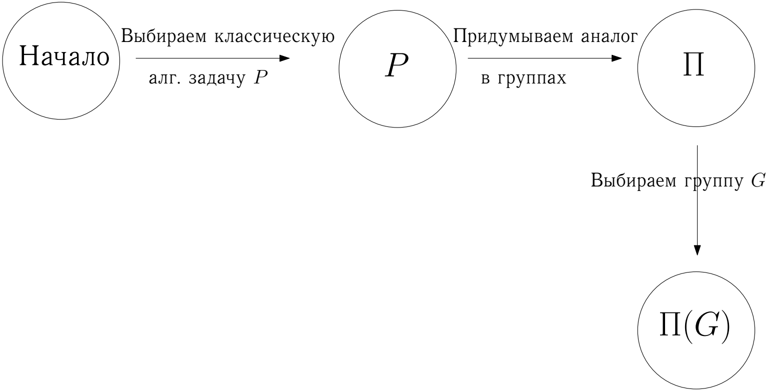
Некоммутативная дискретная оптимизация



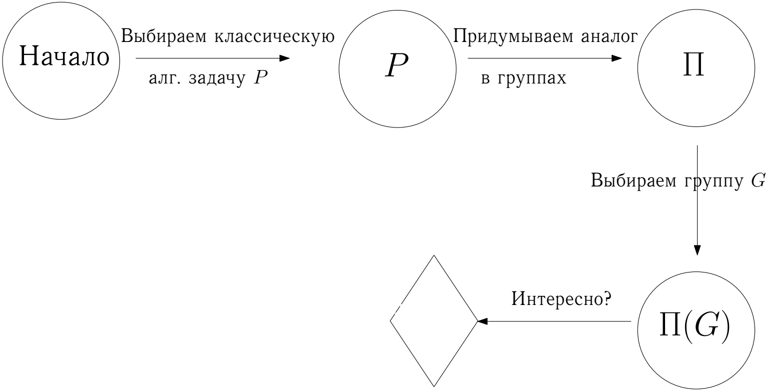
Некоммутативная дискретная оптимизация



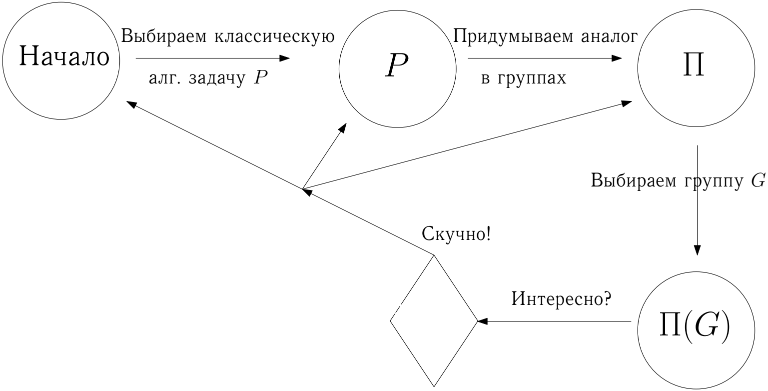
Некоммутативная дискретная оптимизация



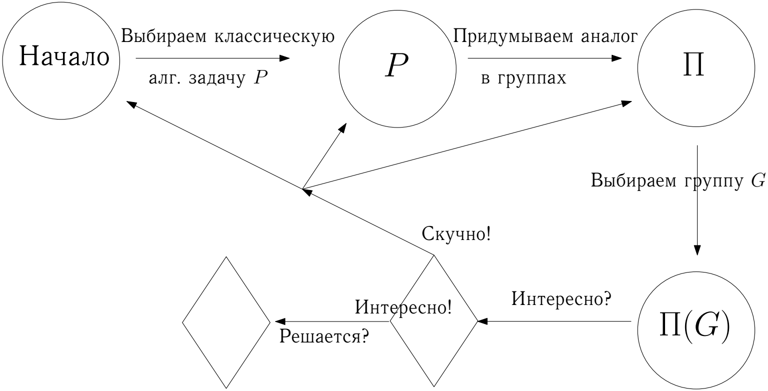
Некоммутативная дискретная оптимизация



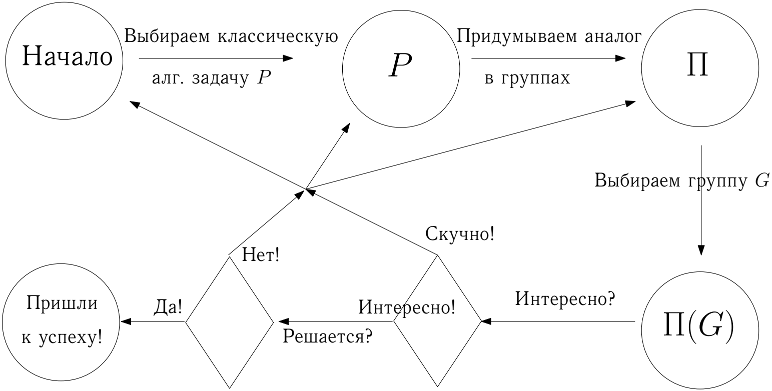
Некоммутативная дискретная оптимизация



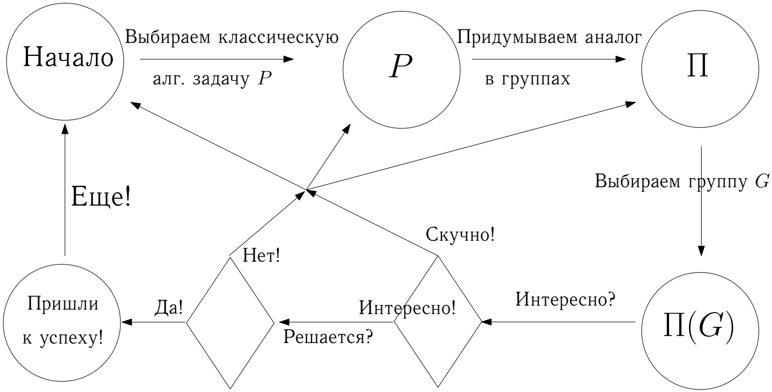
Некоммутативная дискретная оптимизация



Некоммутативная дискретная оптимизация



Некоммутативная дискретная оптимизация



Некоммутативная дискретная оптимизация

Что в этом хорошего:

- Весело.
- Бездонно.
- Расширяет коллекцию алгоритмических задач с известной сложностью в теории групп.
- Позволяет смотреть на классические задачи в новом контексте.
- Оказывается связано с установившимися вопросами и методами в теории групп.

Некоммутативная дискретная оптимизация

Что в этом хорошего:

- Весело.
- Бездонно.
- Расширяет коллекцию алгоритмических задач с известной сложностью в теории групп.
- Позволяет смотреть на классические задачи в новом контексте.
- Оказывается связано с установившимися вопросами и методами в теории групп.

Некоммутативная дискретная оптимизация

Что в этом хорошего:

- Весело.
- Бездонно.
- Расширяет коллекцию алгоритмических задач с известной сложностью в теории групп.
- Позволяет смотреть на классические задачи в новом контексте.
- Оказывается связано с установившимися вопросами и методами в теории групп.

Некоммутативная дискретная оптимизация

Что в этом хорошего:

- Весело.
- Бездонно.
- Расширяет коллекцию алгоритмических задач с известной сложностью в теории групп.
- Позволяет смотреть на классические задачи в новом контексте.
- Оказывается связано с установившимися вопросами и методами в теории групп.

Некоммутативная дискретная оптимизация

Что в этом хорошего:

- Весело.
- Бездонно.
- Расширяет коллекцию алгоритмических задач с известной сложностью в теории групп.
- Позволяет смотреть на классические задачи в новом контексте.
- Оказывается связано с установившимися вопросами и методами в теории групп.

Некоммутативная дискретная оптимизация

Что в этом хорошего:

- Весело.
- Бездонно.
- Расширяет коллекцию алгоритмических задач с известной сложностью в теории групп.
- Позволяет смотреть на классические задачи в новом контексте.
- Оказывается связано с установившимися вопросами и методами в теории групп.

Некоммутативная дискретная оптимизация

Вопросы:

- Разрешимость.
- Принадлежность **NP**.
- Принадлежность **P**.
- **NP**-трудность.

Классы групп:

- Свободные.
- Гиперболические (относительно гиперболические).
- Нильпотентные (почти нильпотентные).
- Метабелевы.
- ...

Некоммутативная дискретная оптимизация

Вопросы:

- Разрешимость.
- Принадлежность **NP**.
- Принадлежность **P**.
- **NP**-трудность.

Классы групп:

- Свободные.
- Гиперболические (относительно гиперболические).
- Нильпотентные (почти нильпотентные).
- Метабелевы.
- ...

Некоммутативная дискретная оптимизация

Вопросы:

- Разрешимость.
- Принадлежность **NP**.
- Принадлежность **P**.
- **NP**-трудность.

Классы групп:

- Свободные.
- Гиперболические (относительно гиперболические).
- Нильпотентные (почти нильпотентные).
- Метабелевы.
- . . .

Вопросы:

- Разрешимость.
- Принадлежность **NP**.
- Принадлежность **P**.
- **NP**-трудность.

Классы групп:

- Свободные.
- Гиперболические (относительно гиперболические).
- Нильпотентные (почти нильпотентные).
- Метабелевы.
- ...

Некоммутативная дискретная оптимизация

Вопросы:

- Разрешимость.
- Принадлежность **NP**.
- Принадлежность **P**.
- **NP**-трудность.

Классы групп:

- Свободные.
- Гиперболические (относительно гиперболические).
- Нильпотентные (почти нильпотентные).
- Метабелевы.
- ...

Некоммутативная дискретная оптимизация

Три класса задач:

- Проблема соответствия Поста.
- Задача о рюкзаке.
- Задачи на решетках (кратчайший вектор и т.п.).

Некоммутативная дискретная оптимизация

Три класса задач:

- Проблема соответствия Поста.
- Задача о рюкзаке.
- Задачи на решетках (кратчайший вектор и т.п.).

Три класса задач:

- Проблема соответствия Поста.
- Задача о рюкзаке.
- Задачи на решетках (кратчайший вектор и т.п.).

Некоммутативная дискретная оптимизация

Три класса задач:

- Проблема соответствия Поста.
- Задача о рюкзаке.
- Задачи на решетках (кратчайший вектор и т.п.).

Проблема соответствия Поста

Проблема соответствия Поста

Пусть A это алфавит, $|A| \geq 2$.

Проблема соответствия Поста (PCP)

Даны пары $(g_1, h_1), \ldots, (g_k, h_k)$ слов из A^*. Требуется установить, существует ли непустое слово $w(x_1, \ldots, x_k) \in X^*$ такое, что $w(g_1, \ldots, g_k) = w(h_1, \ldots, h_k)$ в A^*.

Проблема соответствия Поста

Выложить доминошки так, чтобы верхний ряд $=$ нижнему ряд.

g_{i_1}	g_{i_2}	g_{i_3}	$\dots$	g_{i_n}
h_{i_1}	h_{i_2}	h_{i_3}	$\dots$	h_{i_n}

Разрешима, если число пар $k \leq 2$. Неразрешима, если $k \geq 7$. Неизвестно для $3 \leq k \leq 6$.

Проблема соответствия Поста

Выложить доминошки так, чтобы верхний ряд $=$ нижнему ряд.

g_{i_1}	g_{i_2}	g_{i_3}	$\dots$	g_{i_n}
h_{i_1}	h_{i_2}	h_{i_3}	$\dots$	h_{i_n}

Разрешима, если число пар $k \leq 2$. Неразрешима, если $k \geq 7$. Неизвестно для $3 \leq k \leq 6$.

PCP в группах

Переносим **PCP** в группы:

$A^* \rightsquigarrow$ к.п. группа G,
слова $g_i, h_i \rightsquigarrow$ элементы g_i, h_i, представленные словами в порождающих,
слово $w \rightsquigarrow$ групповое слово,
так?

Получается тривиальная задача:
(a) $w = xx^{-1}$. Запретим нередуцированные слова.
(b) G абелева, $w = [x, y]$. Мало запретили!

PCP в группах

Переносим **PCP** в группы:

$A^* \rightsquigarrow$ к.п. группа G,
слова $g_i, h_i \rightsquigarrow$ элементы g_i, h_i, представленные словами в порождающих,
слово $w \rightsquigarrow$ групповое слово,
так?

Получается тривиальная задача:
(a) $w = xx^{-1}$. Запретим нередуцированные слова.
(b) G абелева, $w = [x, y]$. Мало запретили!

PCP в группах

Переносим **PCP** в группы:

$A^* \rightsquigarrow$ к.п. группа G,
слова $g_i, h_i \rightsquigarrow$ элементы g_i, h_i, представленные словами в порождающих,
слово $w \rightsquigarrow$ групповое слово,
так?

Получается тривиальная задача:
(a) $w = xx^{-1}$. Запретим нередуцированные слова.
(b) G абелева, $w = [x, y]$. Мало запретили!

PCP в группах

Переносим **PCP** в группы:

$A^* \rightsquigarrow$ к.п. группа G,
слова $g_i, h_i \rightsquigarrow$ элементы g_i, h_i, представленные словами в порождающих,
слово $w \rightsquigarrow$ групповое слово,
так?

Получается тривиальная задача:
(a) $w = xx^{-1}$. Запретим нередуцированные слова.
(b) G абелева, $w = [x, y]$. Мало запретили!

PCP в группах

Два (очевидных) способа исправить задачу:

PCP(G) Запретить слова, которые являются тождествами G.

NPCP(G) Рассмотреть неоднородную задачу.

PCP в группах

Два (очевидных) способа исправить задачу:

PCP(G) Запретить слова, которые являются тождествами G.

NPCP(G) Рассмотреть неоднородную задачу.

PCP в группах

Два (очевидных) способа исправить задачу:

PCP(G) Запретить слова, которые являются тождествами G.

NPCP(G) Рассмотреть неоднородную задачу.

Связь NPCP(G) с проблемами в теории групп

Неоднородная проблема соответствия Поста (NPCP)

Даны пары (a, b), (c, d), $(g_1, h_1), \ldots, (g_k, h_k)$ слов из A^*. Требуется установить, существует ли слово $w(x_1, \ldots, x_k) \in X^*$ такое, что $aw(g_1, \ldots, g_k)c = bw(h_1, \ldots, h_k)d$ в A^*.

В случае групп достаточно одной константы:

NPCP(G)

Даны пары $(g_1, h_1), \ldots, (g_k, h_k)$ элементов G и элемент $a \in G$. Требуется установить, существует ли групповое слово $w(x_1, \ldots, x_k) \in F(x_1, \ldots, x_k)$ такое, что $aw(g_1, \ldots, g_k) = w(h_1, \ldots, h_k)$ в G.

Связь $\mathbf{NPCP}(G)$ с проблемами в теории групп

Неоднородная проблема соответствия Поста (NPCP)

Даны пары (a, b), (c, d), $(g_1, h_1), \ldots, (g_k, h_k)$ слов из A^*. Требуется установить, существует ли слово $w(x_1, \ldots, x_k) \in X^*$ такое, что $aw(g_1, \ldots, g_k)c = bw(h_1, \ldots, h_k)d$ в A^*.

В случае групп достаточно одной константы:

$\mathbf{NPCP}(G)$

Даны пары $(g_1, h_1), \ldots, (g_k, h_k)$ элементов G и элемент $a \in G$. Требуется установить, существует ли групповое слово $w(x_1, \ldots, x_k) \in F(x_1, \ldots, x_k)$ такое, что $aw(g_1, \ldots, g_k) = w(h_1, \ldots, h_k)$ в G.

Связь **NPCP**(G) с проблемами в теории групп

Пусть G порождена $x_1, \ldots, x_k$.
Пусть на вход **NPCP**$_k(G)$ даны a, $(g_1, h_1), \ldots, (g_k, h_k)$.

Предположим, отображения
$\varphi : G \to G$, $x_i \to g_i$ и $\psi : G \to G$, $x_i \to h_i$
задают гомоморфизмы.

Тогда $aw(g_1, \ldots, g_k) = w(h_1, \ldots, h_k) \iff aw^\varphi = w^\psi$.

Это

Проблема сопряженности с двойным переподвыподвертом, Endo-TCP

Даны $u, v \in G$ и $\varphi, \psi \in \mathrm{End}(G)$. Требуется установить, существует ли $w \in G$ такой, что

$$uw^\varphi = w^\psi v.$$

Связь **NPCP**(G) с проблемами в теории групп

Пусть G порождена $x_1, \ldots, x_k$.
Пусть на вход $\mathbf{NPCP}_k(G)$ даны a, $(g_1, h_1), \ldots, (g_k, h_k)$.

Предположим, отображения
$\varphi : G \to G$, $x_i \to g_i$ и $\psi : G \to G$, $x_i \to h_i$
задают гомоморфизмы.

Тогда $aw(g_1, \ldots, g_k) = w(h_1, \ldots, h_k) \iff aw^\varphi = w^\psi$.

Это

Проблема сопряженности с двойным переподвыподвертом, Endo-TCP

Даны $u, v \in G$ и $\varphi, \psi \in \mathrm{End}(G)$. Требуется установить, существует ли $w \in G$ такой, что

$$uw^\varphi = w^\psi v.$$

Связь $\mathbf{NPCP}(G)$ с проблемами в теории групп

Пусть G порождена $x_1, \ldots, x_k$.
Пусть на вход $\mathbf{NPCP}_k(G)$ даны a, $(g_1, h_1), \ldots, (g_k, h_k)$.

Предположим, отображения
$\varphi : G \to G$, $x_i \to g_i$ и $\psi : G \to G$, $x_i \to h_i$
задают гомоморфизмы.

Тогда $aw(g_1, \ldots, g_k) = w(h_1, \ldots, h_k) \iff aw^\varphi = w^\psi$.

Это

Проблема сопряженности с двойным переподвыподвертом, Endo-TCP

Даны $u, v \in G$ и $\varphi, \psi \in \mathrm{End}(G)$. Требуется установить, существует ли $w \in G$ такой, что

$$uw^\varphi = w^\psi v.$$

Связь $\mathbf{NPCP}(G)$ с проблемами в теории групп

Пусть G порождена $x_1, \ldots, x_k$.
Пусть на вход $\mathbf{NPCP}_k(G)$ даны a, $(g_1, h_1), \ldots, (g_k, h_k)$.

Предположим, отображения
$\varphi : G \to G$, $x_i \to g_i$ и $\psi : G \to G$, $x_i \to h_i$
задают гомоморфизмы.

Тогда $aw(g_1, \ldots, g_k) = w(h_1, \ldots, h_k) \iff aw^\varphi = w^\psi$.

Это

Проблема сопряженности с двойным переподвыподвертом, Endo-TCP

Даны $u, v \in G$ и $\varphi, \psi \in \mathrm{End}(G)$. Требуется установить, существует ли $w \in G$ такой, что

$$uw^\varphi = w^\psi v.$$

Связь **NPCP**(G) с проблемами в теории групп

Пусть G порождена $x_1, \ldots, x_k$.
Пусть на вход $\mathbf{NPCP}_k(G)$ даны a, $(g_1, h_1), \ldots, (g_k, h_k)$.

Предположим, отображения
$\varphi : G \to G$, $x_i \to g_i$ и $\psi : G \to G$, $x_i \to h_i$
задают гомоморфизмы.

Тогда $aw(g_1, \ldots, g_k) = w(h_1, \ldots, h_k) \iff aw^{\varphi} = w^{\psi}$.

Это

Проблема сопряженности с двойным переподвыподвертом, Endo-TCP

Даны $u, v \in G$ и $\varphi, \psi \in \mathrm{End}(G)$. Требуется установить, существует ли $w \in G$ такой, что

$$uw^{\varphi} = w^{\psi} v.$$

Связь **NPCP**(G) с проблемами в теории групп

Следствие

Пусть G порождена k элементами.

1. Проблема сопряженности с двойным подкручиванием линейно сводится к $\mathbf{NPCP}_k(G)$.
2. Если G является k-порожденной относительно свободной, то эти две проблемы линейно эквивалентны.

Связь **NPCP**(G) с проблемами в теории групп

Следствие

Пусть G порождена k элементами.

1. Проблема сопряженности с двойным подкручиванием линейно сводится к $\mathbf{NPCP}_k(G)$.
2. Если G является k-порожденной относительно свободной, то эти две проблемы линейно эквивалентны.

Наследственная проблема равенства и **NPCP**

Посмотрим на **NPCP** с еще одной стороны.

Пусть G порождена X, w — слово в X.
Пусть R — *конечное* подмножество G.

Вариант конструкции Михайловой: можно построить вход, на котором **NPCP**(G) эквивалентна тривиальности w в фактор-группе $G/\langle R\rangle_G$.

Другими словами, проблема равенства во всех к.пр. фактор-группах группы G сводится к **NPCP**(G).

Посмотрим на **NPCP** с еще одной стороны.

Пусть G порождена X, w — слово в X.
Пусть R — *конечное* подмножество G.

Вариант конструкции Михайловой: можно построить вход, на котором **NPCP**(G) эквивалентна тривиальности w в фактор-группе $G/\langle R \rangle_G$.

Другими словами, проблема равенства во всех к.пр. фактор-группах группы G сводится к **NPCP**(G).

Наследственная проблема равенства(HWP(G)) в группе G

По данному множеству R слов в алфавите $X \cup X^{-1}$ и слову w, установить тривиально ли w в фактор-группе $G/\langle R \rangle_G$.

Теорема

Пусть G — к.пр. группа. Наследственная проблема равенства в G полиномиально сводится к **NPCP**(G).

Наследственная проблема равенства и **NPCP**

Наследственная проблема равенства(HWP(G)) в группе G

По данному множеству R слов в алфавите $X \cup X^{-1}$ и слову w, установить тривиально ли w в фактор-группе $G/\langle R \rangle_G$.

Теорема

Пусть G — к.пр. группа. Наследственная проблема равенства в G полиномиально сводится к **NPCP**(G).

Наследственная проблема равенства и **NPCP**

Теперь сложность проблемы равенства можно перевести в сложность **NPCP**.

Следствие

Пусть F — неабелева свободная группа конечного ранга. **NPCP**(F) неразрешима.

Следствие

Пусть F_k — свободная группа ранга $k \geq 28$. Тогда проблема сопряженности с двойным подкручиванием в F_k (так же как и $NPCP_k(F_k)$) неразрешнима.

Это отвечает на вопрос E.Ventura:
Endo-TCP $\Rightarrow$ Auto-TCP $\Rightarrow$ CP
Endo-TCP $\Leftarrow$? Auto-TCP $\not\Leftarrow$ CP
(последнее решено Богопольским, Martino, Ventura).

Наследственная проблема равенства и **NPCP**

Теперь сложность проблемы равенства можно перевести в сложность **NPCP**.

Следствие

Пусть F — неабелева свободная группа конечного ранга. **NPCP**(F) неразрешима.

Следствие

Пусть F_k — свободная группа ранга $k \geq 28$. Тогда проблема сопряженности с двойным подкручиванием в F_k (так же как и $NPCP_k(F_k)$) неразрешнима.

Это отвечает на вопрос E.Ventura:
Endo-TCP $\Rightarrow$ Auto-TCP $\Rightarrow$ CP
Endo-TCP $\Leftarrow$? Auto-TCP $\not\Leftarrow$ CP
(последнее решено Богопольским, Martino, Ventura).

Теперь сложность проблемы равенства можно перевести в сложность **NPCP**.

Следствие

Пусть F — неабелева свободная группа конечного ранга. **NPCP**(F) неразрешима.

Следствие

Пусть F_k — свободная группа ранга $k \geq 28$. Тогда проблема сопряженности с двойным подкручиванием в F_k (так же как и $NPCP_k(F_k)$) неразрешнима.

Это отвечает на вопрос E.Ventura:
Endo-TCP $\Rightarrow$ Auto-TCP $\Rightarrow$ CP
Endo-TCP $\Leftarrow$? Auto-TCP $\not\Leftarrow$ CP
(последнее решено Богопольским, Martino, Ventura).

Следствие

Если G содержит F_2, то **NPCP**(G) неразрешима.

Наример:

- неэлементарные гиперболические группы,
- неабелевы частично коммутативные группы,
- группы с нетривиальным расщеплением в произведения с объедининием или HNN-расширения,
- группы кос,
- линейные группы (кроме, возможно, почти разрешимых).

Следствие

Если G содержит F_2, то **NPCP**(G) неразрешима.

Наример:

- неэлементарные гиперболические группы,
- неабелевы частично коммутативные группы,
- группы с нетривиальным расщеплением в произведения с объеденинием или HNN-расширения,
- группы кос,
- линейные группы (кроме, возможно, почти разрешимых).

Следствие

Пусть F — свободная группа конечного ранга. Тогда ограниченная версия **NPCP**(F) **NP**-полна.

Наследственная проблема равенства и **NPCP**

Харлампович: существует к.пр. разрешимая группа с неразрешимой проблемой раветсва.

Следствие

Пусть $m \geq 3$. Для достаточно большого k, свободная k-порожденная m-разрешимая группа $S_{m,k}$ имеет неразрешимую Endo-TCP и $NPCP_k$.

Харлампович: существует к.пр. разрешимая группа с неразрешимой проблемой раветсва.

Следствие

Пусть $m \geq 3$. Для достаточно большого k, свободная k-порожденная m-разрешимая группа $S_{m,k}$ имеет неразрешимую Endo-TCP и $NPCP_k$.

PCP(G)

PCP(G)

Даны пары $(g_1, h_1), \ldots, (g_k, h_k)$ элементов группы G. Требуется установить, существует ли слово $w \in F(x_1, \ldots, x_k)$, не являющееся тождеством G, такое что $w(g_1, \ldots, g_k) = w(h_1, \ldots, h_k)$ in G.

В такой формулировке **PCP**(G) сводится к проблеме нахождения (точнее, установления тривиальности) эквалайзера.

Связь **PCP**(G) с проблемами в теории групп

Проблема (тривиальности) эквалайзера

Пусть G, H — фиксированные группы. Даны два гомоморфизма, φ, $\psi : G \to H$. Найти (соотв. установить (не)тривиальность) подгруппу

$$Eq(\varphi, \psi) = \{g \in G \mid \varphi(g) = \psi(g)\}.$$

Связь **PCP**(G) с проблемами в теории групп

Лемма

Пусть G, H — к.п. нильпотентные группы, $\varphi, \psi : G \to H$ — гомоморфизмы. Эквалайзер $Eq(\varphi, \psi)$ можно построить за полиномиальное время.

Следствие

$PCP_k(G)$ полиномиальна в любой к.п. нильпотентной группе G.

Связь **PCP**(G) с проблемами в теории групп

Лемма

Пусть G, H — к.п. нильпотентные группы, $\varphi, \psi : G \to H$ — гомоморфизмы. Эквалайзер $Eq(\varphi, \psi)$ можно построить за полиномиальное время.

Следствие

$PCP_k(G)$ полиномиальна в любой к.п. нильпотентной группе G.

Итого

Что сделано:

	PCP	**NPCP**
свободные		$\checkmark$
нильпотентные	$\checkmark$	

Итого

Что не сделано:

	PCP	**NPCP**
свободные	?	$\checkmark$
нильпотентные	$\checkmark$	?

Итого

Варианты **PCP** оказываются связаны с:

- проблемой сопряженности с двойным подкручиванием (найти $w \in G$ т.ч. $uw^{\varphi} = w^{\psi}v$),
- проблема эквалайзера (найти погруппу элементов g т.ч. $\varphi(g) = \psi(g)$),
- наследственной проблемой равенства (проблема равенства в факторе G по конечно нормально порожденной подгруппе).

Итого

Варианты **PCP** оказываются связаны с:

- проблемой сопряженности с двойным подкручиванием (найти $w \in G$ т.ч. $uw^{\varphi} = w^{\psi}v$),
- проблема эквалайзера (найти погруппу элементов g т.ч. $\varphi(g) = \psi(g)$),
- наследственной проблемой равенства (проблема равенства в факторе G по конечно нормально порожденной подгруппе).

Итого

Варианты **PCP** оказываются связаны с:

- проблемой сопряженности с двойным подкручиванием (найти $w \in G$ т.ч. $uw^{\varphi} = w^{\psi}v$),
- проблема эквалайзера (найти погруппу элементов g т.ч. $\varphi(g) = \psi(g)$),
- наследственной проблемой равенства (проблема равенства в факторе G по конечно нормально порожденной подгруппе).

Задача о рюкзаке

Задача о рюкзаке и ее варианты

Задача о рюкзаке (KP):

Даны $a_1, \ldots, a_k, a \in \mathbb{Z}$. Требуется установить, существуют ли неотрицательные целые $n_1, \ldots, n_k$, т.ч.

$$n_1 a_1 + \ldots + n_k a_k = a$$

Задача о рюкзаке (KP) в группе G:

Даны $g_1, \ldots, g_k, g \in G$ Требуется установить, существуют ли неотрицательные целые $n_1, \ldots, n_k$, т.ч.

$$g_1^{n_1} \ldots g_k^{n_k} = g.$$

Задача о рюкзаке и ее варианты

Задача о рюкзаке (KP):

Даны $a_1, \ldots, a_k, a \in \mathbb{Z}$. Требуется установить, существуют ли неотрицательные целые $n_1, \ldots, n_k$, т.ч.

$$n_1 a_1 + \ldots + n_k a_k = a$$

Задача о рюкзаке (KP) в группе G:

Даны $g_1, \ldots, g_k, g \in G$ Требуется установить, существуют ли неотрицательные целые $n_1, \ldots, n_k$, т.ч.

$$g_1^{n_1} \ldots g_k^{n_k} = g.$$

Задача о рюкзаке и ее варианты

$$g_1^{n_1} \ldots g_k^{n_k} = g.$$

Задача о рюкзаке тесно связана с:

1. методом больших степеней, которых появился задолго до вопросов о сложности (Baumslag, 1962);
2. проблемой вхождения в рациональное подмножество.

Задача о рюкзаке и ее варианты

Задача о рюкзаке:

1. Полиномиальна в абелевых группах (Borosh,Treybig, 1976).
2. Полиномиальна в гиперболических группах. (Потому что геодезические многоугольники тонкие.)
3. Неразрешима в $UT_d(\mathbb{Z})$ для достаточно больших d (Lohrey, 2012?). (Потому что можно интерпретировать полиномиальные диофантовы уравнения.)
4. Неразрешима в нильпотентных группах класса 2 и выше с достаточно широким коммутантом (Мищенко, Трейер, 2014). (Потому что можно интерпретировать полиномиальные диофантовы уравнения лучше, чем у Лори.)

Задача о рюкзаке и ее варианты

Задача о рюкзаке:

1. Полиномиальна в абелевых группах (Borosh,Treybig, 1976).
2. Полиномиальна в гиперболических группах.
   (Потому что геодезические многоугольники тонкие.)
3. Неразрешима в $UT_d(\mathbb{Z})$ для достаточно больших d (Lohrey, 2012?).
   (Потому что можно интерпретировать полиномиальные диофантовы уравнения.)
4. Неразрешима в нильпотентных группах класса 2 и выше с достаточно широким коммутантом (Мищенко, Трейер, 2014).
   (Потому что можно интерпретировать полиномиальные диофантовы уравнения лучше, чем у Лори.)

Задача о рюкзаке и ее варианты

Задача о рюкзаке:

1. Полиномиальна в абелевых группах (Borosh,Treybig, 1976).
2. Полиномиальна в гиперболических группах.
   (Потому что геодезические многоугольники тонкие.)
3. Неразрешима в $UT_d(\mathbb{Z})$ для достаточно больших d (Lohrey, 2012?).
   (Потому что можно интерпретировать полиномиальные диофантовы уравнения.)
4. Неразрешима в нильпотентных группах класса 2 и выше с достаточно широким коммутантом (Мищенко, Трейер, 2014).
   (Потому что можно интерпретировать полиномиальные диофантовы уравнения лучше, чем у Лори.)

Задача о рюкзаке и ее варианты

Задача о рюкзаке:

1. Полиномиальна в абелевых группах (Borosh,Treybig, 1976).
2. Полиномиальна в гиперболических группах.
(Потому что геодезические многоугольники тонкие.)
3. Неразрешима в $UT_d(\mathbb{Z})$ для достаточно больших d (Lohrey, 2012?).
(Потому что можно интерпретировать полиномиальные диофантовы уравнения.)
4. Неразрешима в нильпотентных группах класса 2 и выше с достаточно широким коммутантом (Мищенко, Трейер, 2014).
(Потому что можно интерпретировать полиномиальные диофантовы уравнения лучше, чем у Лори.)

Задача о рюкзаке и ее варианты

Задача о рюкзаке:

1. Полиномиальна в абелевых группах (Borosh,Treybig, 1976).
2. Полиномиальна в гиперболических группах. (Потому что геодезические многоугольники тонкие.)
3. Неразрешима в $UT_d(\mathbb{Z})$ для достаточно больших d (Lohrey, 2012?). (Потому что можно интерпретировать полиномиальные диофантовы уравнения.)
4. Неразрешима в нильпотентных группах класса 2 и выше с достаточно широким коммутантом (Мищенко, Трейер, 2014). (Потому что можно интерпретировать полиномиальные диофантовы уравнения лучше, чем у Лори.)

Задача о рюкзаке:

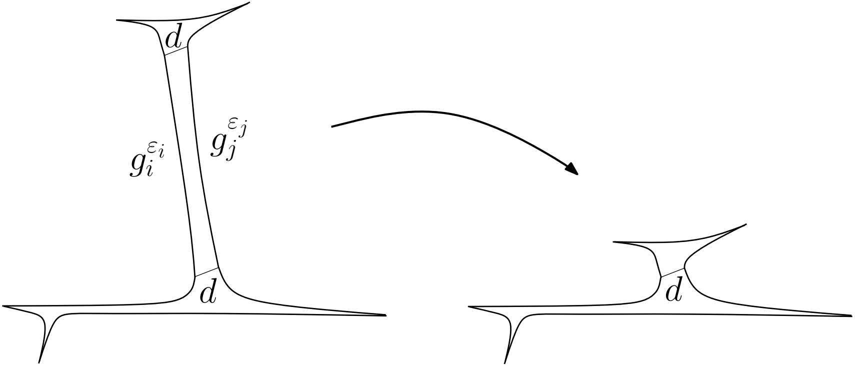
1. Полиномиальна в абелевых группах (Borosh,Treybig, 1976).
2. Полиномиальна в гиперболических группах.
(Потому что геодезические многоугольники тонкие.)
3. Неразрешима в $UT_d(\mathbb{Z})$ для достаточно больших d (Lohrey, 2012?).
(Потому что можно интерпретировать полиномиальные диофантовы уравнения.)
4. Неразрешима в нильпотентных группах класса 2 и выше с достаточно широким коммутантом (Мищенко, Трейер, 2014).
(Потому что можно интерпретировать полиномиальные диофантовы уравнения лучше, чем у Лори.)

Задача о рюкзаке и ее варианты

Задача о рюкзаке:

1. Полиномиальна в абелевых группах (Borosh,Treybig, 1976).
2. Полиномиальна в гиперболических группах.
   (Потому что геодезические многоугольники тонкие.)
3. Неразрешима в $UT_d(\mathbb{Z})$ для достаточно больших d (Lohrey, 2012?).
   (Потому что можно интерпретировать полиномиальные диофантовы уравнения.)
4. Неразрешима в нильпотентных группах класса 2 и выше с достаточно широким коммутантом (Мищенко, Трейер, 2014).
   (Потому что можно интерпретировать полиномиальные диофантовы уравнения лучше, чем у Лори.)

В гиперболических группах:



Ограниченная задача о рюкзаке

Затруднение: даже если проблема равенства в G разрешима, $KP(G)$ может быть неразрешима.

Ограниченная задача о рюкзаке (BKP) в G:

Даны $g_1, \ldots, g_k, g \in G$ и $1^m \in \mathbb{N}$. Установить, существуют ли $\varepsilon_i \in \{0, 1, \ldots, m\}$ т.ч.

$$g = g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}.$$

Эта задача разрешима в любой группе с разрешимой проблемой равенства.

BKP полиномиально эквивалентна случаю $m = 1$ (повторением каждого g_i m раз).

Затруднение: даже если проблема равенства в G разрешима, $KP(G)$ может быть неразрешима.

Ограниченная задача о рюкзаке (BKP) в G:

Даны $g_1, \ldots, g_k, g \in G$ и $1^m \in \mathbb{N}$. Установить, существуют ли $\varepsilon_i \in \{0, 1, \ldots, m\}$ т.ч.

$$g = g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}.$$

Эта задача разрешима в любой группе с разрешимой проблемой равенства.

BKP полиномиально эквивалентна случаю $m = 1$ (повторением каждого g_i m раз).

Ограниченная задача о рюкзаке

Затруднение: даже если проблема равенства в G разрешима, $KP(G)$ может быть неразрешима.

Ограниченная задача о рюкзаке (BKP) в G:

Даны $g_1, \ldots, g_k, g \in G$ и $1^m \in \mathbb{N}$. Установить, существуют ли $\varepsilon_i \in \{0, 1, \ldots, m\}$ т.ч.

$$g = g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}.$$

Эта задача разрешима в любой группе с разрешимой проблемой равенства.

BKP полиномиально эквивалентна случаю $m = 1$ (повторением каждого g_i m раз).

Задаче о сумме подмножества, SSP (= 0–1 KP):

Даны $a_1, \ldots, a_k, a \in \mathbb{Z}$. Установить, можно ли удовлетворить равенство

$$\varepsilon_1 a_1 + \ldots + \varepsilon_k a_k = a,$$

где $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$.

SSP в группе G:

Даны $g_1, \ldots, g_k, g \in G$. Установить, можно ли удовлетворить равенство

$$g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k} = g,$$

где $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$.

Элементы G задаются словами в фиксированном порождающем множестве.

Задаче о сумме подмножества, SSP (= 0–1 KP):

Даны $a_1, \ldots, a_k, a \in \mathbb{Z}$. Установить, можно ли удовлетворить равенство

$$\varepsilon_1 a_1 + \ldots + \varepsilon_k a_k = a,$$

где $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$.

SSP в группе G:

Даны $g_1, \ldots, g_k, g \in G$. Установить, можно ли удовлетворить равенство

$$g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k} = g,$$

где $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$.

Элементы G задаются словами в фиксированном порождающем множестве.

Детали

Классическая SSP псевдополиномиальна

- Если вход унарный, то **SSP** принадлежит **P**,
- Если вход бинарный, то **SSP NP**-полна.

Сложность **SSP**(G) не зависит от конечного порождающего множества группы G, но может зависеть, если допускаются бесконечне порождающие множества.

Например:

SSP$(\mathbb{Z})$

- **SSP**$(\mathbb{Z}) \in$ **P**, если $\mathbb{Z}$ порождена $\{1\}$,
- **SSP**$(\mathbb{Z})$ **NP**-полна, если $\mathbb{Z}$ порождена $\{2^n \mid n \in \mathbb{N}\}$.

Детали

Классическая SSP псевдополиномиальна

- Если вход унарный, то **SSP** принадлежит **P**,
- Если вход бинарный, то **SSP NP**-полна.

Сложность **SSP**(G) не зависит от конечного порождающего множества группы G, но может зависеть, если допускаются бесконечне порождающие множества.

Например:

SSP$(\mathbb{Z})$

- **SSP**$(\mathbb{Z}) \in$ **P**, если $\mathbb{Z}$ порождена $\{1\}$,
- **SSP**$(\mathbb{Z})$ **NP**-полна, если $\mathbb{Z}$ порождена $\{2^n \mid n \in \mathbb{N}\}$.

Детали

Классическая SSP псевдополиномиальна

- Если вход унарный, то **SSP** принадлежит **P**,
- Если вход бинарный, то **SSP NP**-полна.

Сложность **SSP**(G) не зависит от конечного порождающего множества группы G, но может зависеть, если допускаются бесконечне порождающие множества.

Например:

SSP$(\mathbb{Z})$

- **SSP**$(\mathbb{Z}) \in$ **P**, если $\mathbb{Z}$ порождена $\{1\}$,
- **SSP**$(\mathbb{Z})$ **NP**-полна, если $\mathbb{Z}$ порождена $\{2^n \mid n \in \mathbb{N}\}$.

Сложность **SSP**(G):

Группа	Сложность	Почему
Почти нильпотентные	**P**	Полин. рост
$\mathbb{Z} \wr \mathbb{Z}$	**NP**-полна	$\mathbb{Z}^{\omega}$, **ZOE**
Свободная метабелева	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
Группа Томпсона F	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
$BS(1,p)$	**NP**-полна	Бинарная **SSP**$(\mathbb{Z})$
Гиперболические	**P**	Логарифм. глубина
$\mathbb{Z}_2 \wr \mathbb{Z}$, группа фонарщика		Знают Трейер и Мищенко

Отметим, что **NP**-полнота имеет место несмотря на унарный вход.

SSP

Сложность **SSP**(G):

Группа	Сложность	Почему
Почти нильпотентные	**P**	Полин. рост
$\mathbb{Z} \wr \mathbb{Z}$	**NP**-полна	$\mathbb{Z}^\omega$, **ZOE**
Свободная метабелева	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
Группа Томпсона F	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
$BS(1,p)$	**NP**-полна	Бинарная **SSP**($\mathbb{Z}$)
Гиперболические	**P**	Логарифм. глубина
$\mathbb{Z}_2 \wr \mathbb{Z}$, группа фонарщика		Знают Трейер и Мищенко

Отметим, что **NP**-полнота имеет место несмотря на унарный вход.

SSP

Сложность **SSP**(G):

Группа	Сложность	Почему
Почти нильпотентные	**P**	Полин. рост
$\mathbb{Z} \wr \mathbb{Z}$	**NP**-полна	$\mathbb{Z}^{\omega}$, **ZOE**
Свободная метабелева	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
Группа Томпсона F	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
$BS(1,p)$	**NP**-полна	Бинарная **SSP**($\mathbb{Z}$)
Гиперболические	**P**	Логарифм. глубина
$\mathbb{Z}_2 \wr \mathbb{Z}$, группа фонарщика		Знают Трейер и Мищенко

Отметим, что **NP**-полнота имеет место несмотря на унарный вход.

Сложность **SSP**(G):

Группа	Сложность	Почему
Почти нильпотентные	**P**	Полин. рост
$\mathbb{Z} \wr \mathbb{Z}$	**NP**-полна	$\mathbb{Z}^\omega$, **ZOE**
Свободная метабелева	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
Группа Томпсона F	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
$BS(1,p)$	**NP**-полна	Бинарная **SSP**($\mathbb{Z}$)
Гиперболические	**P**	Логарифм. глубина
$\mathbb{Z}_2 \wr \mathbb{Z}$, группа фонарщика		Знают Трейер и Мищенко

Отметим, что **NP**-полнота имеет место несмотря на унарный вход.

Сложность **SSP**(G):

Группа	Сложность	Почему
Почти нильпотентные	**P**	Полин. рост
$\mathbb{Z} \wr \mathbb{Z}$	**NP**-полна	$\mathbb{Z}^\omega$, **ZOE**
Свободная метабелева	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
Группа Томпсона F	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
$BS(1,p)$	**NP**-полна	Бинарная **SSP**($\mathbb{Z}$)
Гиперболические	**P**	Логарифм. глубина
$\mathbb{Z}_2 \wr \mathbb{Z}$, группа фонарщика		Знают Трейер и Мищенко

Отметим, что **NP**-полнота имеет место несмотря на унарный вход.

SSP

Сложность **SSP**(G):

Группа	Сложность	Почему
Почти нильпотентные	**P**	Полин. рост
$\mathbb{Z} \wr \mathbb{Z}$	**NP**-полна	$\mathbb{Z}^\omega$, **ZOE**
Свободная метабелева	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
Группа Томпсона F	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
$BS(1,p)$	**NP**-полна	Бинарная **SSP**($\mathbb{Z}$)
Гиперболические	**P**	Логарифм. глубина
$\mathbb{Z}_2 \wr \mathbb{Z}$, группа фонарщика	[redacted]	Знают Трейер и Мищенко

Отметим, что **NP**-полнота имеет место несмотря на унарный вход.

SSP

Сложность **SSP**(G):

Группа	Сложность	Почему
Почти нильпотентные	**P**	Полин. рост
$\mathbb{Z} \wr \mathbb{Z}$	**NP**-полна	$\mathbb{Z}^\omega$, **ZOE**
Свободная метабелева	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
Группа Томпсона F	**NP**-полна	$\mathbb{Z} \wr \mathbb{Z}$
$BS(1,p)$	**NP**-полна	Бинарная **SSP**$(\mathbb{Z})$
Гиперболические	**P**	Логарифм. глубина
$\mathbb{Z}_2 \wr \mathbb{Z}$, группа фонарщика	[redacted]	Знают Трейер и Мищенко

Отметим, что **NP**-полнота имеет место несмотря на унарный вход.

Итого

SSP и **BKP**:

- **NP**-полны в $\mathbb{Z} \wr \mathbb{Z}$, свободных метабелевых, группе Томспона F, $BS(m,n), m \neq \pm n$.
- **P** в к.п. почти нильпотентных группах, гиперболических группах, $BS(n, \pm n)$.

BSMP:

- **NP**-полна в $F_2 \times F_2$ (тем самым **NP**-сложна в любой группе, содержащей $F_2 \times F_2$, например в $B_{\geq 5}$, $GL(\geq 4, \mathbb{Z})$, частично комм. группах с индуцированным $\boxtimes$.)
- **P** в к.п. почти нильп. группах, гиперболических группах.

KP:

- **P** в к.п. абелевых группах, гиперболических группах.
- неразрешима в многих нильпотентных группах (Lohrey; Мищенко, Трейер).
- Разрешима в обобщенной целочисленной группе Гейзенеберга (Мищенко, Трейер).

Итого

SSP и **BKP**:

- **NP**-полны в $\mathbb{Z} \wr \mathbb{Z}$, свободных метабелевых, группе Томспона F, $BS(m,n), m \neq \pm n$.
- **P** в к.п. почти нильпотентных группах, гиперболических группах, $BS(n, \pm n)$.

BSMP:

- **NP**-полна в $F_2 \times F_2$ (тем самым **NP**-сложна в любой группе, содержащей $F_2 \times F_2$, например в $B_{\geq 5}$, $GL(\geq 4, \mathbb{Z})$, частично комм. группах с индуцированным $\boxtimes$.)
- **P** в к.п. почти нильп. группах, гиперболических группах.

KP:

- **P** в к.п. абелевых группах, гиперболических группах.
- неразрешима в многих нильпотентных группах (Lohrey; Мищенко, Трейер).
- Разрешима в обобщенной целочисленной группе Гейзенеберга (Мищенко, Трейер).

Итого

SSP и **BKP**:

- **NP**-полны в $\mathbb{Z} \wr \mathbb{Z}$, свободных метабелевых, группе Томспона F, $BS(m, n), m \neq \pm n$.
- **P** в к.п. почти нильпотентных группах, гиперболических группах, $BS(n, \pm n)$.

BSMP:

- **NP**-полна в $F_2 \times F_2$ (тем самым **NP**-сложна в любой группе, содержащей $F_2 \times F_2$, например в $B_{\geq 5}$, $GL(\geq 4, \mathbb{Z})$, частично комм. группах с индуцированным $\boxtimes$.)
- **P** в к.п. почти нильп. группах, гиперболических группах.

KP:

- **P** в к.п. абелевых группах, гиперболических группах.
- неразрешима в многих нильпотентных группах (Lohrey; Мищенко, Трейер).
- Разрешима в обобщенной целочисленной группе Гейзенеберга (Мищенко, Трейер).

Что происходит с **SSP**, когда применяются теоретико-групповые конструкции?

B1 Переносится ли **SSP** с G, H на $G * H$?

O1 Это неправильный вопрос.

Это означает, что мы не знаем, но есть похожая проблема, про которую знаем.
AGP(G) — проблема вхождения в конечное рациональное множество, заданное ациклическим графом.

Теорема

AGP$(G) \in$ **P**, **AGP**$(H) \in$ **P** $\Rightarrow$ **AGP**$(G * H) \in$ **P**.

Что происходит с **SSP**, когда применяются теоретико-групповые конструкции?

B1 Переносится ли **SSP** с G, H на $G * H$?

O1 Это неправильный вопрос.

Это означает, что мы не знаем, но есть похожая проблема, про которую знаем.
AGP(G) — проблема вхождения в конечное рациональное множество, заданное ациклическим графом.

Теорема

AGP$(G) \in$ **P**, **AGP**$(H) \in$ **P** $\Rightarrow$ **AGP**$(G * H) \in$ **P**.

Что происходит с **SSP**, когда применяются теоретико-групповые конструкции?

В1 Переносится ли **SSP** с G, H на $G * H$?

О1 Это неправильный вопрос.

Это означает, что мы не знаем, но есть похожая проблема, про которую знаем.

AGP(G) — проблема вхождения в конечное рациональное множество, заданное ациклическим графом.

Теорема

AGP$(G) \in$ **P**, **AGP**$(H) \in$ **P** $\Rightarrow$ **AGP**$(G * H) \in$ **P**.

SSP и теоретико-групповые конструкции

Что происходит с **SSP**, когда применяются теоретико-групповые конструкции?

B1 Переносится ли **SSP** с G, H на $G * H$?

O1 Это неправильный вопрос.

Это означает, что мы не знаем, но есть похожая проблема, про которую знаем.
AGP(G) — проблема вхождения в конечное рациональное множество, заданное ациклическим графом.

Теорема

AGP$(G) \in$ **P**, **AGP**$(H) \in$ **P** $\Rightarrow$ **AGP**$(G * H) \in$ **P**.

B2 Переносится ли **KP** с G, H на $G * H$?

O2 Более-менее да.

Если есть полиномиальная оценка на степени в **KP**(G) и **KP**(H), то есть полиномиальная оценка на степени в **KP**$(G * H)$.

B2 Переносится ли **KP** с G, H на $G * H$?

O2 Более-менее да.

Если есть полиномиальная оценка на степени в $\mathbf{KP}(G)$ и $\mathbf{KP}(H)$, то есть полиномиальная оценка на степени в $\mathbf{KP}(G * H)$.

B2 Переносится ли **KP** с G, H на $G * H$?

O2 Более-менее да.

Если есть полиномиальная оценка на степени в **KP**(G) и **KP**(H), то есть полиномиальная оценка на степени в **KP**$(G * H)$.

В3 Как себя ведет **SSP** в $G \times H$: как проблема равенства или как проблема вхождения?

О3 И так, и так.

Есть пример групп таких, что **SSP**(G), **SSP**$(H) \in$ **P**, но **SSP**$(G \times H)$ **NP**-полна.

ВЗ Как себя ведет **SSP** в $G \times H$: как проблема равенства или как проблема вхождения?

ОЗ И так, и так.

Есть пример групп таких, что $\mathbf{SSP}(G), \mathbf{SSP}(H) \in \mathbf{P}$, но $\mathbf{SSP}(G \times H)$ **NP**-полна.

SSP и теоретико-групповые конструкции

В3 Как себя ведет **SSP** в $G \times H$: как проблема равенства или как проблема вхождения?

О3 И так, и так.

Есть пример групп таких, что $\mathbf{SSP}(G), \mathbf{SSP}(H) \in \mathbf{P}$, но $\mathbf{SSP}(G \times H)$ **NP**-полна.

Задачи на решетках

Задачи на решетках

Идея:
$\mathbb{Z}^n \rightsquigarrow$ группа G,
решетка в $\mathbb{Z}^n \rightsquigarrow$ подгрупа группы G.

Расстояние от элемента до подгруппы

Дана конечно порожденная подгруппа H групы G и элемент $g \in G$. Найти элемент $h \in H$, ближайший к g в словарной метрике на G.

Кратчайший элемент в подгруппе

Дана подгруппа H группы G. Найти элемент H, кратчайший в словарной метрике на G.

Задачи на решетках

Идея:
$\mathbb{Z}^n \rightsquigarrow$ группа G,
решетка в $\mathbb{Z}^n \rightsquigarrow$ подгрупа группы G.

Расстояние от элемента до подгруппы

Дана конечно порожденная подгруппа H групы G и элемент $g \in G$. Найти элемент $h \in H$, ближайший к g в словарной метрике на G.

Кратчайший элемент в подгруппе

Дана подгруппа H группы G. Найти элемент H, кратчайший в словарной метрике на G.

В нильпотентных группах

Теорема

Пусть G — к.п. нильпотентная группа. Проблема вхождения в G разрешима за полиномиальное время.

На самом деле, квазилинейное время и LOGSPACE одновременно (J.Macdonald, A.H., A.Мясников, S.Vassileva).

Теорема

Пусть G — к.п. нильпотентная группа. Проблема вхождения в G разрешима за полиномиальное время.

На самом деле, квазилинейное время и LOGSPACE одновременно (J.Macdonald, A.H., A.Мясников, S.Vassileva).

В нильпотентных группах

Полином. проблема вхожения + полиномиальный рост = ♡

Теорема

Пусть G — к.п. нильпотентная группа. Расстояние от элемента до подгруппы группы G можно найти за полиномиальное время.

Теорема

Пусть G — к.п. нильпотентная группа. Кратчайший элемент подгруппы группы G можно найти за полиномиальное время.

В нильпотентных группах

Полином. проблема вхожения + полиномиальный рост = ♡

Теорема

Пусть G — к.п. нильпотентная группа. Расстояние от элемента до подгруппы группы G можно найти за полиномиальное время.

Теорема

Пусть G — к.п. нильпотентная группа. Кратчайший элемент подгруппы группы G можно найти за полиномиальное время.

В нильпотентных группах

Полином. проблема вхожения + полиномиальный рост = ♡

Теорема

Пусть G — к.п. нильпотентная группа. Расстояние от элемента до подгруппы группы G можно найти за полиномиальное время.

Теорема

Пусть G — к.п. нильпотентная группа. Кратчайший элемент подгруппы группы G можно найти за полиномиальное время.

В свободных и похожих на свободную группах

В свободных группах многие вопросы о подгруппах решаются при помощи графов Столлингса.

Теорема (P.Schupp)

Есть полиномиальный (n^4) алгоритм, который по стандартному представлению группы поверхности или группы Кокстера, удовлетворяющей условию **R**, и набору $(h_1, \ldots, h_m)$ of generators for a subgroup H, строит граф $\Delta(H)$ который, помимо прочего, является графом конечного автомата, который принимает редуцированное по Дену слово u если и только если $u \in H$.

(Условию **R** — это некоторое условие малого сокращения. В случае групп поверхностей просто означает, что род ≥ 2 в ориент. случае и ≥ 4 в неориент. случае.)

В свободных и похожих на свободную группах

В свободных группах многие вопросы о подгруппах решаются при помощи графов Столлингса.

Теорема (P.Schupp)

Есть полиномиальный (n^4) алгоритм, который по стандартному представлению группы поверхности или группы Кокстера, удовлетворяющей условию **R**, и набору $(h_1, \ldots, h_m)$ of generators for a subgroup H, строит граф $\Delta(H)$ который, помимо прочего, является графом конечного автомата, который принимает редуцированное по Дену слово u если и только если $u \in H$.

(Условию **R** — это некоторое условие малого сокращения. В случае групп поверхностей просто означает, что род ≥ 2 в ориент. случае и ≥ 4 в неориент. случае.)

В свободных и похожих на свободную группах

Теорема

Есть полиномиальный алгоритм, который по стандартному представлению

- группы поверхности с условием **R**, или
- группы Кокстера с условием **R**, или
- свободной группы,

и элементам $g, h_1, \ldots, h_m \in G$, находит элемент $h \in H = \langle h_1, \ldots, h_m \rangle$, ближайший к g.

Теорема

То же самое для кратчайшего элемента.

В свободных и похожих на свободную группах

Теорема

Есть полиномиальный алгоритм, который по стандартному представлению

- группы поверхности с условием **R**, или
- группы Кокстера с условием **R**, или
- свободной группы,

и элементам $g, h_1, \ldots, h_m \in G$, находит элемент $h \in H = \langle h_1, \ldots, h_m \rangle$, ближайший к g.

Теорема

То же самое для кратчайшего элемента.

Что дальше?

- Больше задач!
- Больше групп!
- Больше классов сложности!

Что дальше?

- Больше задач!
- Больше групп!
- Больше классов сложности!

Что дальше?

- Больше задач!
- Больше групп!
- Больше классов сложности!

Что дальше?

- Больше задач!
- Больше групп!
- Больше классов сложности!