

# Алгоритмы генерации и решения систем однородных неотрицательных линейных диофантовых уравнений и их приложения

Кирилл Александрович Кулаков

05.13.18 — Математическое моделирование,  
численные методы и комплексы программ

Диссертация на соискание ученой степени  
кандидата физико-математических наук

Научный руководитель: к.т.н., доцент Ю. А. Богоявленский

## Объект исследования

- Однородная система неотрицательных линейных диофантовых уравнений (НЛДУ):  $Ax = \mathbb{O}$ ,  $A \in \mathbb{Z}^{n \times m}$ ,  $x \in \mathbb{Z}_+^m$
- Множество неразложимых решений — базис Гильберта
- Задача решения
  - Проверка совместности
  - Нахождение частного решения (полиномиальная сложность)
  - Проверка решения на принадлежность базису (coNP-полная)
  - Нахождение базиса Гильберта (NP-сложная)
- Приложение систем НЛДУ и алгоритмов решения
  - Определение минимального набора унификаторов
  - Построение универсального тестового множества
  - Управление памятью и распараллеливание программ
  - Моделирование сети передачи данных
- M. Filgueiras, A.-P. Tomas — ассоциированные с КС-грамматиками системы НЛДУ (АНЛДУ)

- Концепция базиса Гильберта  
D. Hilbert, P. Gordan, J. G. van der Corput, E. B. Elliot, P. A. MacMahon
- Термин “базис Гильберта”  
F. Giles, W. Pulleyblank
- Текущее состояние: A. Shreiver
- Теория чисел: Решение уравнений по модулю (сравнения)  
З. И. Бореvич, И. Р. Шафаревич, М. А. Фрумкин
- Теория целочисленных полиэдров и качественные вопросы целочисленного программирования  
В. А. Емеличев, М. М. Ковалев, В. Н. Шевченко, М. Henk, R. Weismantel
- Приведение базиса в целочисленных решетках  
K. Aardal, A. K. Lenstra
- Метод нахождения базиса Гильберта с помощью производящей функции  
E. B. Elliot (1 уравнение), P. A. MacMahon (система)
- Алгоритмы на основе верхних границ компонент базисных решений  
G. Huet, L. Pottier, I. Borosh, L. B. Treybig
- Покомпонентное построение решений начиная с нулевого  
M. Clausen, A. Fortenbacher, E. Contejean

- Алгоритмы на основе метода Elliot–MacMahon  
E. Domenjoud, D. V. Pasechnik
- Нахождение решения с минимальным носителем  
E. Domenjoud, M. Filgueiras, A. Tomás, С. Л. Крывый
- Нахождение базиса Гребнера в идеале кольца полиномов  
L. Pottier, P. Pisón-Casares, A. Vigneron-Tenorio
- Анализ сложности  
Ch. H. Papadimitriou, A. Durand, L. Juban
- Вопросы совместности и применение в математической логике  
Н. К. Косовский
- Кибернетика и системный анализ, Дискретная математика, Дискретный анализ и исследование операций, Успехи математических наук, Linear Algebra and its Applications, J. Association for Computing Machinery, SIAM J. Computing, Information Processing Letters, Information Computing, Mathematics of Operations Research, Proc. American Mathematical Society, Elsevier Discrete Mathematics, Kluwer J. Automated Reasoning, Elsevier Theoretical Computer Science, J. Symbolic Computation, Annals of Combinatorics, Contributions to Algebra and Geometry, Springer-Verlag Mathematical Foundations of Computer Science, Lecture Notes in Computer Science

# Актуальность

- Алгоритмы нахождения базиса Гильберта систем НЛДУ востребованы в приложениях
- Задача решения произвольной системы НЛДУ является вычислительно сложной (NP, coNP)
- Исследование частного класса систем одНЛДУ — системы одАНЛДУ
- Использование алгоритмов на практике требует проведения массового тестирования и экспериментального исследования
- Предоставление доступа к разработанным алгоритмам и программам
- Дискретное моделирование сети MPLS для задачи восстановления

## Цель диссертационной работы

- 1** Развитие теории систем одАНЛДУ. Разработка, обоснование, реализация и тестирование алгоритмов решения и генерации этих систем.
- 2** Разработка комплекса программ для автоматизации массового тестирования, экспериментального и сравнительного анализа алгоритмов решения систем одАНЛДУ, а также для предоставления заинтересованным членам научного сообщества доступа через Интернет к этим алгоритмам.
- 3** Исследование возможности практического применения полученных результатов на примере задачи восстановления соединения в сети MPLS.

## Список результатов выносимых на защиту

- 1 Преобразование системы одАНЛДУ к трапецевидной форме и обратная подстановка базиса Гильберта
- 2 Псевдополиномиальный алгоритм нахождения базиса Гильберта произвольной системы одАНЛДУ
- 3 Алгоритмы генерации систем одАНЛДУ
- 4 Комплекс программ, включающий систему `alg_analyser` и систему `Web-SynDic`
- 5 Тестирование и экспериментальное исследование алгоритмов решения
- 6 Диофантова модель сети MPLS для задачи восстановления соединения

# Структура и объем работы

Гл. 1. Системы одАНЛДУ

Гл. 2. Алгоритмы решения и генерации систем одАНЛДУ

Гл. 3. Экспериментальное исследование алгоритмов

Гл. 4. Диофантова модель сети MPLS

- 3 приложения (6 страниц)
- Библиографический список использованной литературы (98 наименований)
- Общий объем 170 машинописных страниц
- Содержит 31 рисунок и 13 таблиц



## Системы одНЛДУ и одАНЛДУ

Однородная система линейных диофантовых уравнений (одНЛДУ):

$$Ax = 0, \quad A \in \mathbb{Z}^{n \times m}, \quad x \in \mathbb{Z}_+^m$$

## Базис Гильберта

- Конечное множество неразложимых (минимальных) решений
- Единственность базиса
- Общее решение  $x = \sum_{s=1}^q \alpha_s h^{(s)}$ ,  $\alpha_s \in \mathbb{Z}_+$

Ассоциированные с КС-грамматиками системы одНЛДУ:

Индексное разбиение:  $I^{n,m} = \{I_0, I_1, \dots, I_n\}$

$$\bigcup_{k=0}^n I_k = \mathbb{N}_m; \quad I_k \cap I_j = \emptyset \quad k \neq j; \quad I_k \neq \emptyset \quad \forall k \neq 0.$$

Матрица разбиения:  $E_{k,i}(I^{n,m}) = \begin{cases} 1, & i \in I_k, \\ 0, & \text{иначе,} \end{cases}$

одАНЛДУ:  $\sum_{i \in I_k} x_i = \sum_{i=1}^m a_{ki} x_i, \quad k = 1, 2, \dots, n, \quad a_{ki} \in \mathbb{Z}_+$

## Пример системы одАНЛДУ

$$\begin{cases} x_1 + x_3 = 2x_4 + x_5 \\ x_2 = 5x_1 + 7x_3 + 2x_4 + 3x_5 \\ x_4 = 2x_5 \\ x_6 = 0 \end{cases} \quad E(I^{4,6}) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$I_0 = \{5\}, I_1 = \{1, 3\}, I_2 = \{2\}, I_3 = \{4\}, I_4 = \{6\}$$

Базис Гильберта

$$\mathcal{H} = \left\{ \begin{pmatrix} 5 \\ 32 \\ 0 \\ 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 4 \\ 34 \\ 1 \\ 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 36 \\ 2 \\ 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 38 \\ 3 \\ 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 40 \\ 4 \\ 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 42 \\ 5 \\ 2 \\ 1 \\ 0 \end{pmatrix} \right\}$$

## 1одАНЛДУ и содАНЛДУ

Система с одним уравнением (1одАНЛДУ):  $\sum_{i \in I_1} x_i = \sum_{j \in I_0} a_j x_j$

## Свойство (1.2)

Базис Гильберта 1одАНЛДУ состоит из всех векторов  $\begin{pmatrix} b \\ \mathbf{e}_j \end{pmatrix}$ , где  $b \in \mathbb{Z}_+^{|I_1|}$ ,  $\sum_{i \in I_1} b_i = a_j$ , а  $\mathbf{e}_j$  — единичный вектор из  $\mathbb{Z}^{|I_0|}$  для  $j \in I_0$ .

## Симметричная система (содАНЛДУ)

Система имеет вид  $Mx = 0$ ,  
где  $M$  — матрица инцидентности  
орфафа  $G(\mathbb{N}_n, \mathbb{N}_m)$ .

$$\begin{cases} \sum_{i \in I_k \setminus J_k} x_i = \sum_{i \in J_k \setminus I_k} x_i, & k = 1, \dots, n \\ \sum_{i \in Z} x_i = 0, & Z \subseteq \mathbb{N}_m \\ \sum_{i \in F} x_i = \sum_{i \in F} x_i. & F \subseteq \mathbb{N}_m. \end{cases}$$

## Свойство (1.3)

Любое базисное решение  $h \in \mathcal{H}$  системы содАНЛДУ соответствует некоторому простому контуру в  $G$  и наоборот, причем  $h \in \{0, 1\}^m$ .

## Преобразование к трапециевидной форме

$$S^{(1)} \rightarrow S^{(2)} \rightarrow \dots \rightarrow S^{(r)}$$

$L_k$  — индексы неизвестных уравнения  $k$ , не встречающиеся в оставшихся уравнениях с положительными коэффициентами:

$$\sum_{i \in L_k} x_i + \sum_{i \in I_k \setminus L_k} x_i = \sum_{i \notin I_k} a_{ki} x_i.$$

1. Строим  $L_k \neq \emptyset$  для уравнения системы  $S^{(k)}$ .
2. Систему  $S^{(k)}$  представим в виде:

$$S^{(k)} = \begin{cases} \sum_{i \in L_k} x_i + \sum_{i \in I_k \setminus L_k} x_i = \sum_{i \notin I_k} a_{ki} x_i, \\ S^{(k+1)}. \end{cases}$$

3.  $S^{(k)} \rightarrow S^{(k+1)}$

Трапецевидная форма системы одАНЛДУ:

$$\begin{cases} \sum_{i \in L_k} x_i + \sum_{i \in I_k \setminus L_k} x_i = \sum_{i \notin I_k} a_{ki} x_i, & k = 1, 2, \dots, r-1, \\ S^{(r)}. \end{cases}$$

### Теорема (1.2)

Система  $S^{(r)}$  равносильна либо 1одАНЛДУ (при  $r = n$ ), либо системе содАНЛДУ (при  $r < n$ ).

$$1\text{одАНЛДУ: } \sum_{i \in I_1} x_i = \sum_{j \in I_0} a_j x_j;$$

$$\text{содАНЛДУ: } \begin{cases} \sum_{i \in I_k \setminus J_k} x_i = \sum_{i \in J_k \setminus I_k} x_i, & k = 1, \dots, n \\ \sum_{i \in Z} x_i = 0, & Z \subseteq \mathbb{N}_m \\ \sum_{i \in F} x_i = \sum_{i \in F} x_i. & F \subseteq \mathbb{N}_m. \end{cases}$$

## Доказательство

Случай  $r = n$  очевиден. Пусть  $r < n$ .

Сложим уравнения в  $S^{(r)}$ :

$$\sum_{i \in U_r} c_i x_i = 0, \text{ где } c_i = \sum_{k=r}^n (a_{ki} - E_{ki}), U_r = \mathbb{N}_m \setminus \bigcup_{k=1}^{r-1} L_k.$$

1. Если  $c_i < 0$ , то  $L_{k_0} \neq \emptyset$ .
2. Если  $c_i > 0$ , то  $x_i = 0$ . Пусть  $Z = \{i \mid c_i > 0\}$ , добавляем  $\sum_{i \in Z} x_i = 0$ .
3. Остальные  $c_i = 0$ .

- 3.a.  $\sum_{k=r}^n E_{ki} = \sum_{k=r}^n a_{ki} = 0$ . Пусть  $F = \{i \mid \sum_{k=r}^n (E_{ki} + a_{ki}) = 0\}$ .

- 3.b. Найдутся  $k_0$  и  $j$  такие, что  $k_0 \neq j$ ,  $a_{ji} \geq 1$  и  $E_{k_0 i} = 1$ .

Поскольку  $c_i = \sum_{k=r}^n a_{ki} - E_{k_0 i} = 0$ , то  $a_{ji} = 1$ ,  $a_{ki} = 0$  для  $k \neq j$ .

$$\left( \begin{array}{c|c} 0 & 0 \\ \vdots & \vdots \\ E_{k_0 i} = 1 & 0 \\ \vdots & \vdots \\ 0 & a_{ji} = 1 \\ \vdots & \vdots \\ 0 & 0 \end{array} \right)$$

Следовательно, матрица  $A$  системы  $S^{(r)}$  определяется некоторым индексным разбиением  $J$ .

Таким образом, для  $r < n$  система  $S^{(r)}$  эквивалентна содАНЛДУ.

## Подстановка базиса Гильберта

- Система одНЛДУ  $S = (Ax = \mathbb{O}) = \begin{cases} S' = (A'x = \mathbb{O}) \\ S'' = (A''x = \mathbb{O}) \end{cases}$   
 $\mathcal{H}' = \{f^{(1)}, f^{(2)}, \dots, f^{(q1)}\}$  — базис Гильберта системы  $S'$
- Подстановка общего решения  $x = \sum_{p=1}^{q1} \alpha_p f^{(p)}$  системы  $S'$  в систему  $S''$ , получая систему  $\tilde{S}$  из уравнений  $k = 1, \dots, n''$  и неизвестных  $\alpha_1, \dots, \alpha_{q1}$

### Теорема (1.1)

Пусть  $\tilde{\mathcal{H}} = \{g^{(1)}, g^{(2)}, \dots, g^{(q2)}\}$  есть базис Гильберта системы  $\tilde{S}$ . Тогда базис Гильберта исходной системы  $S$  есть

$$\mathcal{H} = \min \left\{ h^{(s)} = \sum_{p=1}^{q1} g_p^{(s)} f^{(p)} \mid s = 1, 2, \dots, q2 \right\}.$$



## Доказательство

Система  $\tilde{S}$  имеет вид:  $\sum_{p=1}^{q1} \left( \sum_{i=1}^m a''_{ki} f_i^{(p)} \right) \alpha_p = 0, \quad k = 1, \dots, n''.$

Подставим ее общее решение  $\alpha_p = \sum_{s=1}^{q2} \beta_s g_p^{(s)}:$

$$\begin{aligned} 0 &= \sum_{p=1}^{q1} \left( \sum_{i=1}^m a''_{ki} f_i^{(p)} \right) \left( \sum_{s=1}^{q2} \beta_s g_p^{(s)} \right) = \\ &= \sum_{i=1}^m a''_{ki} \left( \sum_{s=1}^{q2} \beta_s \left( \sum_{p=1}^{q1} g_p^{(s)} f_i^{(p)} \right) \right) = \sum_{i=1}^m a''_{ki} \left( \sum_{s=1}^{q2} \beta_s h^{(s)} \right). \end{aligned}$$

$x = \sum_{s=1}^{q2} \beta_s h^{(s)}$  есть решение системы  $S''$  при любых  $\beta_s$ .

Решение  $x$  является и решением  $S'$  (можно разложить по  $\mathcal{H}'$ ):

$$x = \sum_{s=1}^{q2} \beta_s h^{(s)} = \sum_{s=1}^{q2} \beta_s \left( \sum_{p=1}^{q1} g_p^{(s)} f^{(p)} \right) = \sum_{p=1}^{q1} \left( \sum_{s=1}^{q2} \beta_s g_p^{(s)} \right) f^{(p)} = \sum_{p=1}^{q1} \gamma_p f^{(p)}.$$

Пусть  $y$  решение  $S$ , тогда  $y = \sum_{p=1}^{q1} \gamma_p f^{(p)}$ . Вектор  $\gamma$  дает решение  $\tilde{S}$ , т.к.

$$\sum_{p=1}^{q1} \left( \sum_{i=1}^m a''_{ki} f_i^{(p)} \right) \gamma_p = \sum_{i=1}^m a''_{ki} \left( \sum_{p=1}^{q1} \gamma_p f_i^{(p)} \right) = \sum_{i=1}^m a''_{ki} y_i = 0, \quad k = 1, \dots, n''.$$

Последнее равенство верно, т.к.  $y$  есть решение  $S''$ . Следовательно,

имеет место представление  $\gamma = \sum_{s=1}^{q2} \beta_s g^{(s)}$ , откуда  $y = \sum_{s=1}^{q2} \beta_s h^{(s)}$ .

## Обратная подстановка

$$\mathcal{H}^{(r)} \rightarrow \mathcal{H}^{(r-1)} \rightarrow \dots \rightarrow \mathcal{H}^{(1)}$$

Пусть  $\mathcal{H}^{(r)}$  — базис Гильберта системы  $S^{(r)}$

1. Подставляем  $\mathcal{H}^{(k+1)}$  в первое уравнение  $S^{(k)}$  получая  $\tilde{S}$

$$\sum_{i \in L_k} x_i + \sum_{i \in I_k \setminus L_k} \sum_{h \in \mathcal{H}^{(k+1)}} h_i \alpha_h = \sum_{i \notin I_k} a_{ki} \sum_{h \in \mathcal{H}^{(k+1)}} h_i \alpha_h.$$

2. Находим базис  $\tilde{\mathcal{H}}$  решая  $\tilde{S}$  относительно  $(x_i)_{i \in L_k}$  и  $(\alpha_h)_{h \in \mathcal{H}^{(k+1)}}$

3. Вычисляем  $\mathcal{H}^{(k)} = \min \left\{ \sum_{i \in L_k} x_i \mathbf{e}_i + \sum_{h \in \mathcal{H}^{(k+1)}} \alpha_h h \mid \begin{pmatrix} x \\ \alpha \end{pmatrix} \in \tilde{\mathcal{H}} \right\}$  (теор. 1.1).

4.  $S^{(k)} \rightarrow S^{(k-1)}$

Пусть  $d_{kh} = \sum_{i \notin I_k} a_{ki} h_i - \sum_{i \in I_k \setminus L_k} h_i$  и  $\mathcal{H}^{(k+1)} = \mathcal{H}_+^{(k+1)} \cup \mathcal{H}_-^{(k+1)}$ , где

$$\mathcal{H}_+^{(k+1)} = \{h \in \mathcal{H}^{(k+1)} \mid d_{kh} \geq 0\} \text{ и } \mathcal{H}_-^{(k+1)} = \{h \in \mathcal{H}^{(k+1)} \mid d_{kh} = -1\}.$$

Тогда  $\tilde{S}$  есть **1одАНЛДУ**:

$$\sum_{i \in L_k} x_i + \sum_{h \in \mathcal{H}_-^{(k+1)}} \alpha_h = \sum_{h \in \mathcal{H}_+^{(k+1)}} d_{kh} \alpha_h,$$

### Теорема (1.3)

Пусть  $T_k = \bigcup_{j=0}^{k-1} I_j$ . Тогда для любых  $k = 1, 2, \dots, r$  и  $h \in \mathcal{H}^{(k)}$

выполняется: (а)  $\sum_{i \in T_k} h_i \leq 1$ ; (б) если  $k \neq 1$ , то  $d_{k-1, h} \geq -1$ .

## Доказательство

Из (а) следует (б) для любого  $k > 1$ , поскольку

$$d_{k-1,h} = \sum_{i \notin I_{k-1}} a_{k-1,i} h_i - \sum_{i \in I_{k-1} \setminus L_{k-1}} h_i,$$

$$0 \leq \sum_{i \notin I_{k-1}} a_{k-1,i} h_i \quad \text{и} \quad 0 \leq \sum_{i \in I_{k-1} \setminus L_{k-1}} h_i \leq \sum_{i \in T_k} h_i \leq 1.$$

Докажем (а) для  $h \in \mathcal{H}^{(k)}$  индукцией по  $k = r, r-1, \dots, 1$ .

База индукции:  $k = r$ . Достаточно рассмотреть два случая для  $S^{(r)}$ .

1.  $S^{(r)}$  — 1одАНЛДУ  $\sum_{i \in I_r} x_i = \sum_{i \notin I_r} a_{ri} x_i$ . Тогда  $T_r = \{i | i \notin I_r\}$ , а  $\sum_{i \in T_r} h_i = 1$ .
2.  $S^{(r)}$  — система содАНЛДУ. Тогда  $h \in \{0, 1\}$ . Пусть  $h_{i_0} = 1$  для некоторого  $i_0$ . Тогда либо  $i_0 \in F$ , либо  $i_0 \in I_{j_0}$  для некоторого  $j_0 \in \{r, \dots, n\}$ .

а)  $i_0 \in F$ . Тогда  $h = \mathbf{e}_{i_0}$  и  $\sum_{i \in T_r} h_i \leq \sum_i h_i = h_{i_0} = 1$ .

б)  $i_0 \in I_{j_0}$ . Тогда  $h_i = 0$  для любого  $i \in F$  и  $\sum_{i \in T_r} h_i = \sum_{i \in F} h_i = 0$ .

Шаг индукции. Пусть (а) верно для  $j = k + 1$ . Докажем для  $j = k$ .

Подставляем  $\mathcal{H}^{(k+1)}$  в первое уравнение  $S^{(k)}$ :

$$\sum_{i \in L_k} x_i + \sum_{g \in \mathcal{H}^{(k+1)}} \left( \sum_{i \in I_k \setminus L_k} g_i \right) \alpha_g = \sum_{g \in \mathcal{H}^{(k+1)}} \left( \sum_{i \notin I_k} a_{ki} g_i \right) \alpha_g. \quad (1)$$

В силу индукционного предположения  $1 \geq \sum_{i \in T_{k+1}} g_i \geq \sum_{i \in I_k \setminus L_k} g_i$ . Значит,

$\alpha_g$  входят в левую часть с  $(0, 1)$ -коэффициентами, и (1) имеет вид:

$$\sum_{i \in L_k} x_i + \sum_{g \in \mathcal{H}_-^{(k+1)}} \alpha_g = \sum_{g \in \mathcal{H}_+^{(k+1)}} d_{kg} \alpha_g.$$

Решение  $h \in \mathcal{H}^{(k)}$ :

$$h = \sum_{i \in L_k} x_i \mathbf{e}_i + \sum_{g \in \mathcal{H}_+^{(k+1)}} \alpha_g g + \sum_{g \in \mathcal{H}_-^{(k+1)}} \alpha_g g = \sum_{i \in L_k} x_i \mathbf{e}_i + \tilde{g} + \sum_{g \in \mathcal{H}_-^{(k+1)}} \alpha_g g.$$

Поскольку  $T_k \cap L_k = \emptyset$ , то  $\sum_{i \in T_k} h_i = \sum_{i \in T_k} \tilde{g}_i + \sum_{g \in \mathcal{H}_-^{(k+1)}} \alpha_g \sum_{i \in T_k} g_i$

Докажем  $\sum_{i \in T_k} g_i = 0$  для любого  $g \in \mathcal{H}_-^{(k+1)} = \{f \in \mathcal{H}^{(k+1)} \mid d_{kf} = -1\}$ .

$$\sum_{i \in T_{k+1}} g_i = \sum_{i \in T_k} g_i + \sum_{i \in I_k} g_i \leq 1 \text{ и } d_{kg} = \sum_{i \notin I_k} a_{ki} g_i - \sum_{i \in I_k \setminus L_k} g_i = -1.$$

Если  $\sum_{i \in T_k} g_i = 1$ , то  $0 = \sum_{i \in I_k} g_i \geq \sum_{i \in I_k \setminus L_k} g_i \geq 0$ , но  $g \notin \mathcal{H}_-^{(k+1)}!!!$

Таким образом, получаем  $\sum_{i \in T_k} h_i = \sum_{i \in T_k} \tilde{g}_i \leq \sum_{i \in T_{k+1}} \tilde{g}_i \leq 1$ .

## Алгоритм решения

- I. Выполнить преобразование 1 исходной системы к трапецевидной форме.  $S^{(1)}, S^{(2)}, \dots, S^{(r)}$ .
- II. Найти базис Гильберта  $\mathcal{H}^{(r)}$  системы  $S^{(r)}$ . Для случая 1одАНЛДУ используется алгоритм решения 1одАНЛДУ, для случая системы содАНЛДУ — алгоритм решения системы содАНЛДУ.
- III. Выполнить преобразование 2, вычисляя в обратном порядке базисы Гильберта.  $\mathcal{H}^{(r)}, \mathcal{H}^{(r-1)}, \dots, \mathcal{H}^{(1)}$ .

Сложность алгоритма  $T = O(mnQ^2)$  и  $V = O(mQ)$ .

### Теорема (2.3, частный случай)

Пусть  $\mathcal{H}_-^{(k+1)} = \emptyset$  для  $k = r - 1, r - 2, \dots, 1$ . Тогда сложность алгоритма подстановки базиса Гильберта в наихудшем случае составляет  $T = O(mnq)$  и  $V = O(mq)$ .



## Задача генерации

- Построение системы одАНЛДУ и ее базиса Гильберта
- Учет ограничений ( $n$ ,  $m$ ,  $q = |\mathcal{H}|$ ,  $\|A\|$ ,  $\|\mathcal{H}\|$ )
- Непосредственная генерация  $E$  и  $A$  дает, как правило, несовместные системы
- Генерация тестовых (проверка правильности) и эталонных (проверка эффективности) систем
- Алгоритмы генерации
  - JordanGen — преобразование Гаусса-Жордано
  - GaussGen — преобразование Гаусса
  - ExtGaussGen — расширение GaussGen
  - SymGen — системы содАНЛДУ
  - ExtSymGen — расширение SymGen
  - UniGen – Объединение алгоритмов ExtGaussGen и ExtSymGen

# Алгоритм JordanGen

- Базис Гильберта

$$\mathcal{H} = \{e_1, e_2, \dots, e_p\}.$$

- Система одАНЛДУ:  $(E(I^{n,p})|B)x = (E(I^{n,p})|B + \Delta)x$

$$B \in \{0, 1\}^{n \times (m-p)}; \quad \sum_{i=1}^n B_{ik} = 1, \quad k = 1, \dots, m-p$$

$$\Delta \in \mathbb{Z}_+^{n \times (m-p)}; \quad \sum_{i=1}^n \Delta_{ij} > 0, \quad i = 1, \dots, m-p.$$

# Алгоритм GaussGen

## ■ Базис Гильберта

$$\mathcal{H} = \{h^{(s)}\}_{s=1}^{m-n}; \quad h^{(s)} = \begin{cases} h_i^{(s)} = 1, & \text{если } i > n, i = s; \\ h_i^{(s)} = 0, & \text{если } i > n, i \neq s; \\ h_i^{(s)} = G_{si} \geq 0, & \text{если } i \leq n. \end{cases}$$

## ■ Система одАНЛДУ: $(\mathbb{I}|B)x = (D|B + \Delta)x$

$$B \in \{0, 1\}^{n \times (m-n)}; \quad \sum_{i=1}^n B_{ik} = 1, \quad k = 1, \dots, m-n.$$

$$\Delta \in \mathbb{Z}_+^{n \times (m-n)}; \quad \Delta_{nj} > 0, \quad j = 1, \dots, m-n.$$

$$D \in \mathbb{Z}_+^{n \times n}; \quad D = \begin{cases} D_{ij} = 0, & \text{если } i \geq j; \\ D_{ij} \in \mathbb{Z}_+, & \text{если } i + 1 < j; \\ D_{ij} \in \mathbb{N}, & \text{если } i + 1 = j. \end{cases}$$

# Алгоритм ExtGaussGen

- Разбиение  $0 = l_0 < l_1 < l_2 < \dots < l_n = l_{n+1} = p$  для  $n \leq p < m$
- Базис Гильберта

$$\mathcal{H} = \{h^{(s)}\}_{s=1}^q, \quad h^{(s)} = \begin{cases} h_i^{(s)} \in \{0, 1\}, & \text{если } i > l_n \text{ и } \sum_{j=l_n+1}^m h_j^{(s)} = 1, \\ h_i^{(s)} = G_{si} \geq 0, & \text{если } i \leq l_n \end{cases}$$

- Система одАНЛДУ:  $(E(I^{n,p})|B)x = (D|B + \Delta)x$

$$B \in \{0, 1\}^{n \times (m-p)}; \quad \sum_{i=1}^n B_{ik} = 1, \quad k = 1, \dots, m-p.$$

$$\Delta \in \mathbb{Z}_+^{n \times (m-p)}; \quad \Delta_{nj} > 0, \quad j = 1, \dots, m-p.$$

$$D \in \mathbb{Z}_+^{n \times p}; \quad D = \begin{cases} D_{ij} = 0, & \text{если } j \leq l_i; \\ D_{ij} \in \mathbb{N}, & \text{если } l_i < j \leq l_{i+1}; \\ D_{ij} \in \mathbb{Z}_+, & \text{если } j > l_{i+1}. \end{cases}$$

# Алгоритм SymGen

- Базис Гильберта

$$\mathcal{H} = \{h^{(s)} \mid h^{(s)} \in \{0, 1\}^m\}_{s=1}^q$$

- Система одАНЛДУ:  $E(I^{n,m})x = E(J^{n,m})x$

- Алгоритм генерации системы содАНЛДУ  $E(I^{n,m})x = E(J^{n,m})x$

- построение простого контура — орграф  $G(n, p)$
- последовательное добавление  $m - p$  дуг — орграф  $G(n, m)$ .  
Для построения базисных решений используются алгоритмы нахождения простых контуров.
- построение матриц  $E(I^{n,m})$  и  $E(J^{n,m})$  по орграфу

# Алгоритм ExtSymGen

- Алгоритм SymGen для генерации  $E(I^{n-b,m-p})x = E(J^{n-b,m-p})x$
- $0 = l_0 < l_1 < l_2 < \dots < l_b = l_{b+1} = p$ ,  $b \leq p < m$ ,  $0 \leq b < n$
- Базис Гильберта

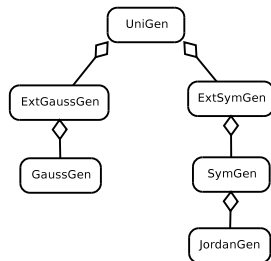
$$\mathcal{H} = \{h^{(s)}\}_{s=1}^q, \quad h^{(s)} = \begin{cases} h_i^{(s)} = G_{si} \geq 0, & \text{если } i \leq p, \\ h_i^{(s)} = g_i \in \{0, 1\}, & \text{если } i > p; \end{cases}$$

- Система одАНЛДУ:

$$\left( \begin{array}{c|c} E(I^{b,p}) & \mathbb{O} \\ \hline \mathbb{O} & E(I^{n-b,m-p}) \end{array} \right) x = \left( \begin{array}{c|c} D & \Delta \\ \hline \mathbb{O} & E(J^{n,m}) \end{array} \right) x$$

$$\Delta \in \mathbb{Z}_+^{n \times (m-p)}, \quad D \in \mathbb{Z}_+^{b \times p}; \quad D = \begin{cases} D_{ij} = 0, & \text{если } j \leq l_i; \\ D_{ij} \in \mathbb{N}, & \text{если } l_i < j \leq l_{i+1}; \\ D_{ij} \in \mathbb{Z}_+, & \text{если } j > l_{i+1}. \end{cases}$$

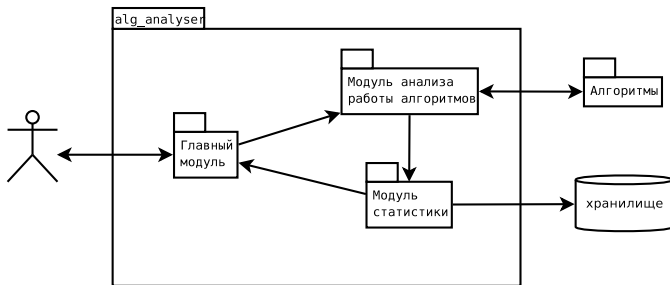
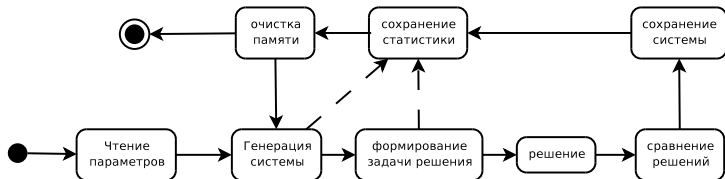
## Сводка алгоритмов



Алгоритм	Временная сложность	Емкостная сложность
TransSol	$O(mnQ^2)$	$O(mQ)$
TransSol (т.2.3)	$O(mnq)$	$O(mq)$
Syntactic	$O(m^2n^2Q_s^3)$	$O(mn^2Q_s)$
JordanGen	$O(m^2)$	$O(mn)$
GaussGen	$O(mn(m-n))$	$O(m^2)$
ExtGaussGen	$O(mnq)$	$O(m(n+q))$
SymGen	$O(m(m+n)q)$	$O(mq)$
ExtSymGen	$O(m(m+n)q)$	$O(m(n+q))$
UniGen	$O(m(m+n)q)$	$O(m(n+q))$

# Программная система alg\_analyser

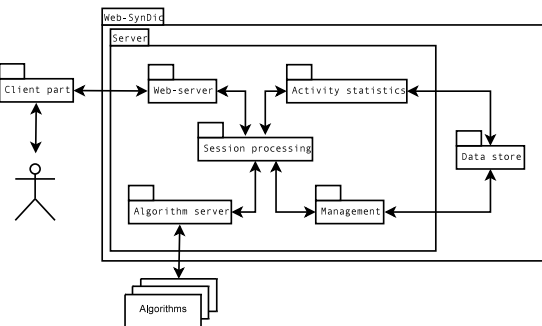
Тестирование, экспериментальный анализ и сравнение алгоритмов



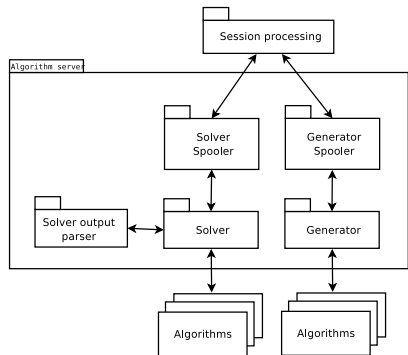


# Программная система Web-SynDic

Удаленная работа с алгоритмами решения и генерации



<http://websyndic.cs.karelia.ru>



## Реализация

- ОС Linux, языки программирования Java и ANSI C
- Реализация алгоритмов и ПС alg\_analyser

Алгоритм	LOC	COM	MVG	Всего строк
JordanGen	588	633	107	1331
GaussGen	631	637	131	1268
ExtGaussGen	992	872	222	2085
SymGen	631	637	131	1268
TransSol	1144	822	226	2176
alg_analyser	2660	1825	538	5029

- Реализация системы Web-SynDic

Метрика	"Algorithm server"	система Web-SynDic
LOC	3805	11907
BLOC	491	1356
CLOC	1275	2757
NCSL	2207	5356
%(NCSL)	58	45

# Экспериментальное исследование

## Алгоритмы решения

- SlopesSys (А. Р. Томás и М. Filgueiras). Поиск решений с минимальным носителем.
- Syntactic (Д. Ж. Корзун). Синтаксический метод.
- TransSol. Преобразование к трапециевидной форме.

## План экспериментального исследования

- Часть I (2002 г.). Тестирование алгоритма Syntactic
- Часть II (2002 г.). Сравнение алгоритмов SlopesSys и Syntactic
- Часть III (2008 г.). Сравнение алгоритмов Syntactic и TransSol

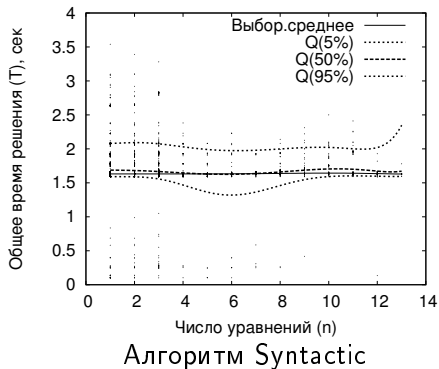
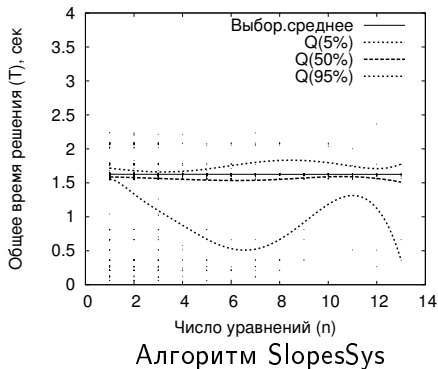
## Часть I. Тестирование алгоритма Syntactic

- Алгоритмы генерации JordanGen и GaussGen
- Ограничения:  $n, m \leq 10^3$ ,  $\|A\|_{l_\infty} \leq 10^5$
- 1 серия, 7 наборов
- Число систем:  $> 1.5 \cdot 10^6$

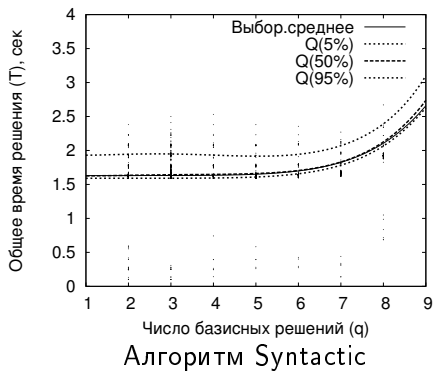
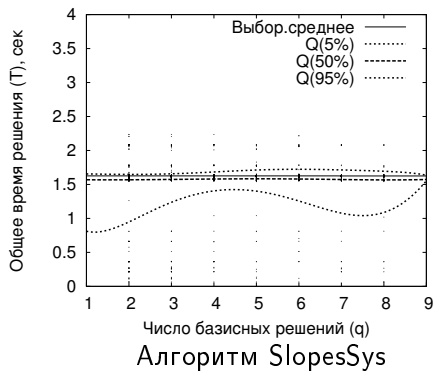
Алгоритм	Дата проведения	Кол-во тестов	Пропущено	Размер матрицы	Размер переменных
GaussGen	26–28.02	410786	0	100	$10^5$
GaussGen	28.02	3	0	500	$10^5$
JordanGen	28.02–07.03	204308	0	1000	$10^5$
GaussGen	28.02–01.03	10	0	300	500
GaussGen	01–07.03	2837	0	1000	$10^4$
GaussGen	18.03–08.07	88640	0	1000	$10^4$
JordanGen	18.03–08.07	937234	0	1000	$10^4$
Итого	26.02–08.07	1643818	0	—	—

## Часть II. Сравнение алгоритмов SlopesSys и Syntactic

- Алгоритмы генерации JordanGen и GaussGen
- Ограничения:  $n, m \leq 20$ ,  $q \leq 9$ ,  $\|A\|_{l_\infty} \leq 100$
- 1 серия, 2 набора
- Число систем: 10000



## Часть II. Сравнение алгоритмов SlopesSys и Syntactic



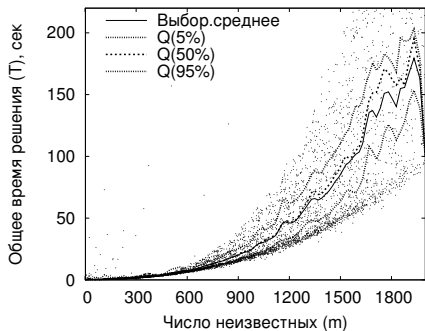
- Более половины систем не решено алгоритмом SlopesSys
- алгоритм Syntactic обеспечивает лучшее гарантированное время решения, а часть систем решает быстрее, чем в типичном случае
- Для алгоритма SlopesSys наиболее вероятная верхняя граница может существенно превышать типичное значение

## Часть III. Сравнение алгоритмов Syntactic и TransSol

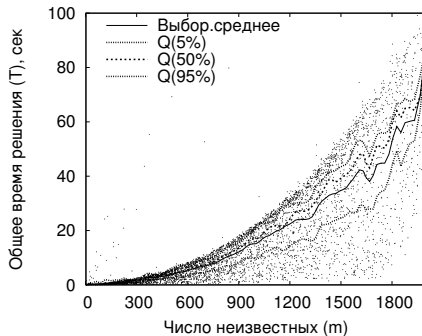
- Алгоритмы генерации JordanGen, GaussGen и ExtGaussGen
- 5 серий по 3 набора

Класс систем	Ограничения	План	Решено
1. Малые размерности систем с малым базисом Гильберта	$n, m \leq 100,$ $q \leq 500, \ A\  \leq 100$	15000	13439
2. Большие размерности систем с малым базисом Гильберта	$n, m \leq 2000,$ $q \leq 500, \ A\  \leq 100$	15000	14597
3. Малые размерности систем с большим базисом Гильберта	$n, m \leq 100,$ $q \leq 10^4, \ A\  \leq 100$	15000	11452
4. Системы с большими коэффициентами	$n, m \leq 100,$ $q \leq 500, \ A\  \leq 10^4$	15000	13773
5. Большие размерностей систем с большими коэффициентами и большим базисом Гильберта	$n, m \leq 2000,$ $q \leq 10^4, \ A\  \leq 10^4$	15000	14884

## Часть III. Сравнение алгоритмов Syntactic и TransSol



Алгоритм SlopesSys



Алгоритм Syntactic

- Алгоритм TransSol эффективнее Syntactic ( $\sim mn$ )
- Часть систем (до 25%) не решена алгоритмом Syntactic
- Для алгоритма TransSol выборочные характеристики подвержены меньшим скачкам, чем для алгоритма Syntactic
- Разница в 10–15 раз между системным и общим временем для алгоритма TransSol.

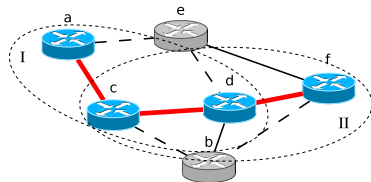


# Задача восстановления

- Сеть MPLS (мультипротокольная коммутация по меткам):
  - Разделение трафика на классы эквивалентности FEC
  - Сопоставление метки пакету
  - Множество меток — таблица маршрутизации
- Потеря соединения:
  - нарушение линии связи или выход из строя узла
  - Задача построения обходного маршрута (поиск маршрута)
  - Задача переключения на новый маршрут (активация маршрута)
- Приложения:
  - Чувствительные к задержкам
  - Чувствительные к потере связности
- Требования:
  - Гарантированное время восстановления
  - Учет дополнительных критериев (число переходов, загруженность линий связи и узлов и др.)

# Методы восстановления

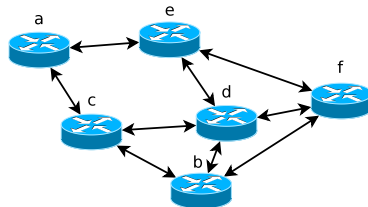
- Базовые методы (RFC 3469)
  - Перенаправление (после потери соединения)
  - Защитное переключение (до потери соединения)
- MPLS local protection (Fast reroute)
  - Расширение IP reroute
  - Локальное восстановление
- Global path protection
  - Построение резервного маршрута
  - Глобальное восстановление
- Short Leap Shared Protection (SLSP)
  - Комбинация локального и глобального восстановлений
  - Построение множества циклов  $CY$
  - Разбиение маршрута  $r$  на пересекающиеся домены  $s$
  - Выбор из  $CY$  множества циклов покрывающие домен  $CY_{r,s}$



# Диофантова модель сети MPLS

- Альтернативная модель для алгоритма SLSP
- Цель моделирования — эффективные на практике способы построения  $CY$  и  $CY_{r,s}$
- Диофантова модель в виде системы одНЛДУ  $E(I^{n,m})x = Ax$
- Построение резервных маршрутов — нахождение базиса Гильберта
- Коэффициенты  $A$  — характеристика пересылки пакета по заданной линии связи
- Наличие двух или более ненулевых коэффициентов в столбце матрицы  $A$  — множественная пересылка

# Модель топологии сети



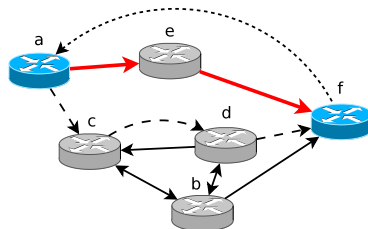
- Основа — матрица инцидентности орграфа
- Каждая линия связи делится на 2 дуги
- Базисное решение — контур орграфа
- содержательно эквивалентна SLSP-модели

$$\begin{cases} a: x_{ac} + x_{ae} = x_{ca} + x_{ea} \\ b: x_{bc} + x_{bd} + x_{bf} = x_{cb} + x_{db} + x_{fb} \\ c: x_{ca} + x_{cb} + x_{cd} = x_{ac} + x_{bc} + x_{dc} \\ d: x_{db} + x_{dc} + x_{de} + x_{df} = x_{bd} + x_{cd} + x_{ed} + x_{fd} \\ e: x_{ea} + x_{ed} + x_{ef} = x_{ae} + x_{de} + x_{fe} \\ f: x_{fb} + x_{fd} + x_{fe} = x_{bf} + x_{df} + x_{ef} \end{cases}$$

Базис Гильберта состоит из 35 решений, определяя все возможные циклы для множества  $CY$  из алгоритма SLSP.

## Модель с фиксированным соединением

- Основа — модель топологии
- Построение маршрута для домена  $s = (a, f)$
- Удаление дуг входящих в  $a$  и исходящих из  $f$
- Удаление внутренних дуг и вершин маршрута
- Добавление фиктивной дуги  $(f, a)$
- Поиск контуров содержащих  $(f, a)$



$$\left\{ \begin{array}{l} a : x_{ac} = x_{fa} \\ b : x_{bc} + x_{bd} + x_{bf} = x_{cb} + x_{db} \\ c : x_{cb} + x_{cd} = x_{ac} + x_{bc} + x_{dc} \\ d : x_{db} + x_{dc} + x_{df} = x_{bd} + x_{cd} \\ f : x_{fa} = x_{bf} + x_{df} \end{array} \right.$$

Базис Гильберта состоит из 9 решений, 4 из которых содержат  $(f, a)$  ( $x_{fa} = 1$ ).

## Модель с характеристиками линии связи

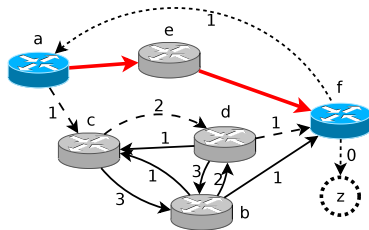
- Условия модели с фиксированным соединением
- Примеры характеристик линии связи
  - Загруженность (напр., слабая:1, средняя:2, высокая:3).
  - Приоритет (напр., высокий:1, нормальный:2, низкий:3).
  - Число промежуточных устройств (переключателей).
- Добавление фиктивной вершины  $z$  и дуги  $(f, z)$
- Вес дуг орграфа  $A = (a_{ki})_{k \in N, i \in L}$ , а дуг  $(v, u)$  и  $(v, z)$  равен 1 и 0

■ Система одАНЛДУ 
$$\begin{cases} x_{fa} + x_{fz} = \sum_{i \notin I_f} a_{fi} x_i, \\ \sum_{i \in I_k} x_i = \sum_{i \notin I_k} a_{ki} x_i, \quad k \in N \setminus \{f\}. \end{cases}$$

- Решение как маршрут из  $a$  в  $f$
- $\sum_{i \notin I_k} a_{ki} x_i$  — характеристика маршрута при достижении  $k$ .
- $\sum_{i \in I_k} x_i$  — кумулятивная характеристика маршрута из  $a$  до  $k$

# Модель с характеристиками линии связи

- Кумулятивная характеристика всего маршрута есть  $x_{fz} + 1$
- Поиск контуров, проходящих через (f, a) с минимальной кумулятивной характеристикой

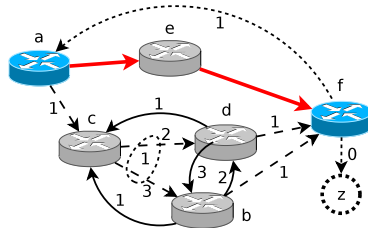


$$\begin{cases} a: x_{ac} = x_{fa} \\ b: x_{bc} + x_{bd} + x_{bf} = 3x_{cb} + 3x_{db} \\ c: x_{cb} + x_{cd} = x_{ac} + x_{bc} + x_{dc} \\ d: x_{db} + x_{dc} + x_{df} = 2x_{bd} + 2x_{cd} \\ f: x_{fa} + x_{fz} = x_{bf} + x_{df} \end{cases}$$

Базис Гильберта состоит из 32 решений, 7 из которых содержат (f, a) ( $x_{fa} = 1$ ), включая маршрут с минимальной кумулятивной характеристикой 2.

# Модель с множественной пересылкой

- Условия модели с характеристиками связи
- Учет множественной пересылки (дополнительные столбцы матрицы  $A$ )
- Базисное решение определяет маршрут с минимальной кумулятивной характеристикой



$$\begin{cases} a: x_{ac} = x_{fa} \\ b: x_{bc} + x_{bd} + x_{bf} = 3x_{cb} + 3x_{db} + x_{(c;b,d)} \\ c: x_{cb} + x_{cd} + x_{(c;b,d)} = x_{ac} + x_{bc} + x_{dc} \\ d: x_{db} + x_{dc} + x_{df} = 2x_{bd} + 2x_{cd} + x_{(c;b,d)} \\ f: x_{fa} + x_{fz} = x_{bf} + x_{df} \end{cases}$$

Базис Гильберта состоит из 48 решений, 10 из которых содержат  $(f, a)$  ( $x_{fa} = 1$ ), два решения определяют маршрут с минимальной кумулятивной характеристикой 2.



## Заклучение

- Преобразование произвольной системы одАНЛДУ и обратная подстановка базиса Гильберта
- Псевдополиномиальный алгоритм решения произвольной системы одАНЛДУ
- Пять алгоритмов генерации систем одАНЛДУ
- Программные системы `alg_analyser` и `Web-SynDic`
- Экспериментальное исследование алгоритмов решения
- Диофантова модель сети MPLS

## Основные публикации

- [1] Кулаков, К. А. Итеративный алгоритм нахождения базиса Гильберта однородных линейных диофантовых систем, ассоциированных с контекстно-свободными грамматиками / К. А. Кулаков, Д. Ж. Корзун, Ю. А. Богоявленский // Вестник Санкт-Петербургского университета. Сер. 10. Вып. 2. — СПб.: Изд-во СПбГУ, 2008. — С. 73–84.
- [2] Кулаков, К. А. Генерация систем неотрицательных линейных диофантовых уравнений / К. А. Кулаков // Материалы международной конференции “Развитие вычислительной техники в России и странах бывшего СССР: история и перспективы”. — Т. 2. — Петрозаводск: Изд-во ПетрГУ, 2006. — С. 58–65.
- [3] Кулаков, К. А. Generating homogenous systems of equations for testing and experimental analysis of linear diophantine solvers / К. А. Кулаков, Д. Ж. Корзун // Труды международного семинара Finnish Data Processing Week at the University of Petrozavodsk (FDPW'2003): Advances in Methods of Modern Information Technology. — Vol. 5. — Петрозаводск: Изд-во ПетрГУ, 2005. — Pp. 259–278.

- [4] Проект Web-SynDic: Система удаленного решения линейных диофантовых уравнений в неотрицательных целых числах / Ю. А. Богоявленский, Д. Ж. Корзун, К. А. Кулаков, М. А. Крышень // Материалы международной конференции “Развитие вычислительной техники в России и странах бывшего СССР: история и перспективы”. — Т. 1. — Петрозаводск: Изд-во ПетрГУ, 2006. — С. 136–145.
- [5] Кулаков, К. А. Диофантова модель сети MPLS для восстановления соединений за полиномиальное время / К. А. Кулаков // Сборник трудов Второй международной научно-практической конференции “Исследование, разработка и применение высоких технологий в промышленности”. — Т. 5. — СПб.: Изд-во Политехн. ун-та, 2006. — С. 137–143.
- [6] Кулаков, К. А. Восстановление соединений сети MPLS с использованием линейных диофантовых моделей / К. А. Кулаков // Труды международного семинара “Распределенные компьютерные и телекоммуникационные сети: теория и приложения (DCCN-2007)”. — Т. 2. — Москва: ИППИ РАН, 2007. — С. 23–27.

## Тезисы докладов

- [1] Кулаков, К. А. Технология автоматизации тестирования алгоритмов решения неотрицательных линейных диофантовых уравнений / К. А. Кулаков, Д. Ж. Корзун // Конкурс-конференция студентов и молодых ученых Северо-Запада “Технологии Microsoft в теории и практике программирования”. — СПб: Изд-во СПбГПУ, 2004. — С. 142–143.
- [2] Кулаков, К. А. Восстановление маршрутов в опорных инфраструктурах высокопроизводительных телекоммуникационных системах на базе MPLS / К. А. Кулаков, Д. Ж. Корзун, Ю. А. Богоявленский // Труды XIV Всероссийской научно-методической конференции Телематика'2007. — Т. 2. — СПб: Изд-во СПбГУ ИТМО, 2007. — С. 398–399.
- [3] Система Web-SynDic для демонстрации и исследования синтаксических алгоритмов решения линейных диофантовых уравнений в неотрицательных целых числах / Д. Ж. Корзун, Ю. А. Богоявленский, К. А. Кулаков и др. // Труды Всероссийской научной конференции “Научный сервис в сети Интернет”. — М.: Изд-во МГУ, 2004. — С. 8–10.
- [4] Web-SynDic — система демонстрации и тестирования синтаксических алгоритмов решения неотрицательных линейных диофантовых уравнений / К. А. Кулаков, А. Ю. Сало, А. В. Ананьин и др. // Конкурс-конференция студентов и молодых ученых Северо-Запада “Технологии Microsoft в теории и практике программирования”. — СПб: Изд-во СПбГПУ, 2004. — С. 43–44.

Спасибо за внимание!