Петрозаводский государственный университет
Кафедра информатики и математического обеспечения

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

Научные руководители:

к.т.н., доцент Юрий Анатольевич Богоявленский
к.ф.-м.н., доцент Дмитрий Жоржевич Корзун

Структура диссертации

Гл. 1. Однородные системы неотрицательных линейных диофантовых уравнений, ассоциированные с контекстно-свободными грамматиками

Гл. 2. Алгоритмы решения и генерации систем одАНЛДУ

Гл. 3. Экспериментальное исследование алгоритмов

Гл. 4. Диофантова модель сети MPLS

Системы одНЛДУ и одАНЛДУ

Однородная система линейных диофантовых уравнений,
система 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:

$$I^{n,m} = \{I_0, I_1, \ldots, I_n\}; \quad E_{k,i}(I^{n,m}) = \begin{cases} 1, & i \in I_k, \\ 0, & \text{иначе}, \end{cases}$$

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

1одАНЛДУ: $\sum_{i \in I_1} x_i = \sum_{j \in I_0} a_j x_j$; $\quad$ содАНЛДУ: $\sum_{i \in I_k} x_i = \sum_{i \in J_k} x_i$

Пример системы одАНЛДУ

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

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

Базис Гильберта

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

Постановка задачи

1. Развитие теории систем одАНЛДУ. Разработка, обоснование, реализация и тестирование алгоритмов решения и генерации этих систем.
2. Разработка ПО для тестирования, экспериментального и сравнительного анализа алгоритмов решения систем одАНЛДУ.
3. Исследование практической значимости полученных результатов на примере задачи восстановления соединений в сети MPLS.

Список результатов выносимых на защиту

1. Преобразование системы одАНЛДУ к трапециевидной форме и обратная подстановка
2. Псевдополиномиальный алгоритм решения произвольной системы одАНЛДУ
3. Алгоритмы генерации систем одАНЛДУ
4. Система Web-SynDic и экспериментальная площадка
5. Результаты экспериментального исследования
6. Диофантова модель сети MPLS для задачи восстановления

Преобразование к трапециевидной форме

$$S^{(1)} \to S^{(1)} \to \dots \to S^{(r)}$$

L_k — неизвестные, не встречающиеся в оставшихся уравнениях

1. Строим $L_k \neq \varnothing$ для уравнения системы $S^{(k)}$.

2. Систему $S^{(k)}$ представим в виде:

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

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

Трапециевидная форма системы одАНЛДУ:

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

Обратная подстановка

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

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

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

2. Находим базис $\widetilde{\mathcal{H}}$ решая (1) относительно $(x_i)_{i \in L_k}$ и $(\alpha_h)_{h \in \mathcal{H}^{(k+1)}}$
3. Вычисляем $\mathcal{H}^{(k)} = \min\left\{ \sum_{i \in L_k} x_i e_i + \sum_{h \in \mathcal{H}^{(k+1)}} \alpha_h h \mid \binom{x}{\alpha} \in \widetilde{\mathcal{H}} \right\}$.
4. $S^{(k)} \to S^{(k-1)}$

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

где $d_{kh} = \sum_{i \notin I_k} a_{ki} h_i - \sum_{i \in I_k \setminus L_k} h_i$.

Теорема (1.1)

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

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

Теорема (1.2)

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

Теорема (1.3)

Пусть $T_k = \bigcup_{j=0}^{k-1} I_j$. Тогда для любых $k = 1, 2, \ldots, r$ и $h \in \mathcal{H}^{(k)}$ выполняется: (а) $\sum_{i \in T_k} h_i \leqslant 1$; (б) если $k \neq 1$, то $d_{k-1,h} \geqslant -1$.

Алгоритм решения

I. Выполнить преобразование 1 исходной системы к трапециевидной форме. $S^{(0)}, S^{(1)}, \ldots, S^{(r)}$.

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. $\mathcal{H}^{(r)}, \mathcal{H}^{(r-1)}, \ldots, \mathcal{H}^{(0)}$.

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

Теорема (частный случай)

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

Алгоритм JordanGen

- Базис Гильберта

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

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

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

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

Алгоритм GaussGen

- Базис Гильберта

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

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

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

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

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

Алгоритм ExtGaussGen

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

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

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

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

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

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

Алгоритм SymGen

- Базис Гильберта

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

- 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 $G(n,p)$
  - построение матриц $E(I^{n,m})$ и $E(I^{n,m})$

Алгоритм ExtSymGen

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

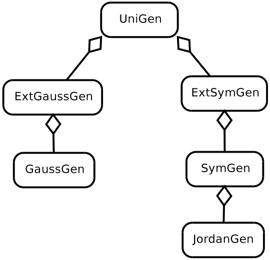
$$\mathcal{H} = \{h^{(s)}\}_{s=1}^{q}, \quad h^{(s)} = \begin{cases} h_i^{(s)} = G_{si} \geqslant 0, & \text{если} \quad i \leqslant p, \\ h_i^{(s)} = g_i \in \{0,1\}, & \text{если} \quad i > p; \end{cases}$$

- Система одАНЛДУ:

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

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

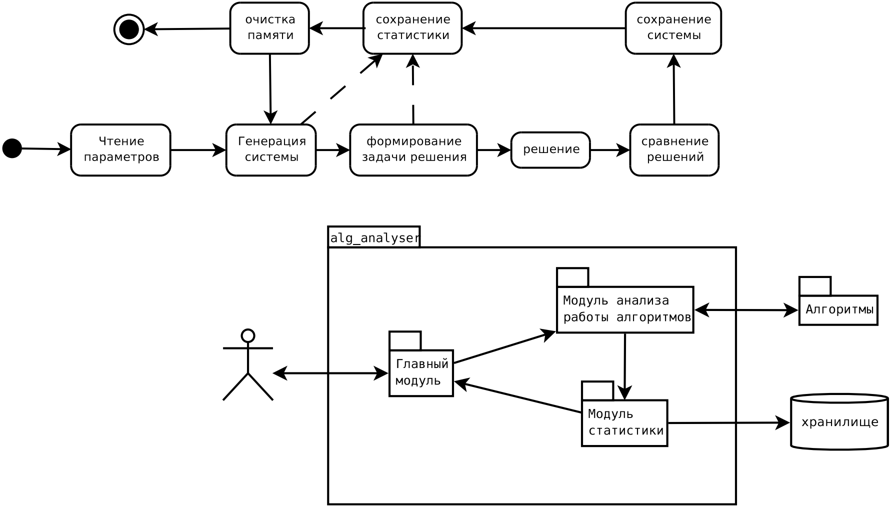
Сводка алгоритмов



Алгоритм	Временна́я сложность	Емкостная сложность
TransSol	$O(mnQ^2)$	$O(mQ)$
TransSol (т.4)	$O(mnq)$	$O(mq)$
Syntactic	$O(m^2n^2Q^3)$	$O(mn^2Q)$
JordanGen	$O(m^2)$	$O(mn)$
GaussGen	$O(mn(m-n))$	$O(m^2)$
ExtGaussGen	$O(mnq)$	$O(m(n+q))$
SymGen	$O(m(m+n)q)$	$O(m(n+q))$
ExtSymGen	$O(m(m+n)q)$	$O(m(n+q))$
UniGen	$O(m(m+n)q)$	$O(m(n+q))$

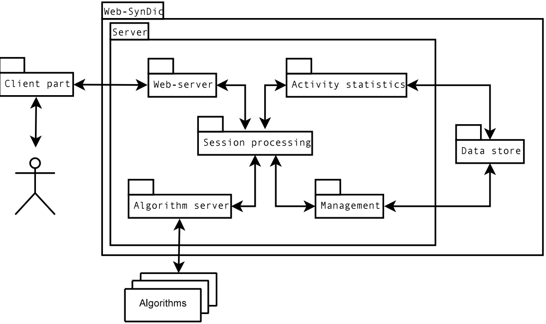
Программная система alg_analyser

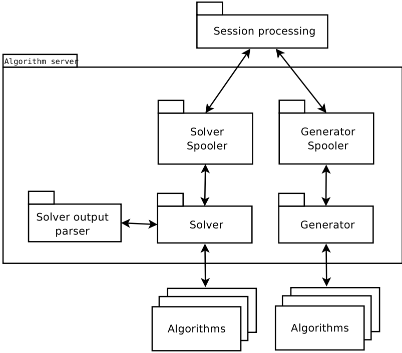
Тестирование, экспериментальный анализ и сравнение алгоритмов



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

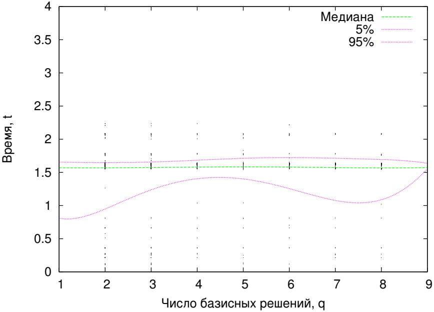
Метрика	"Algorithm server"	система Web-SynDic
LOC	3805	11907
BLOC	491	1356
CLOC	1275	2757
NCSL	2207	5356
%(NCSL)	58	45

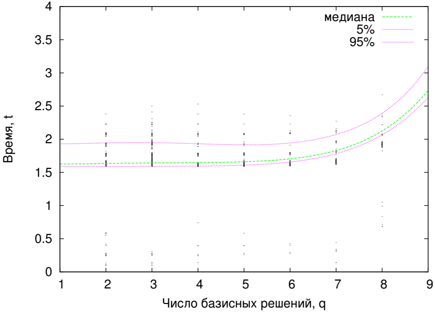
Тестирование алгоритмов

Задача	Ограничения	Число тестов
1. Тестирование	$n, m \leqslant 10^3$, $\|\|A\|\| \leqslant 10^5$	$> 1.5 * 10^6$
2. Сравнение алгоритмов	$n, m \leqslant 20$, $\|\|A\|\| \leqslant 100$	10000

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	—	—

Тестирование алгоритмов



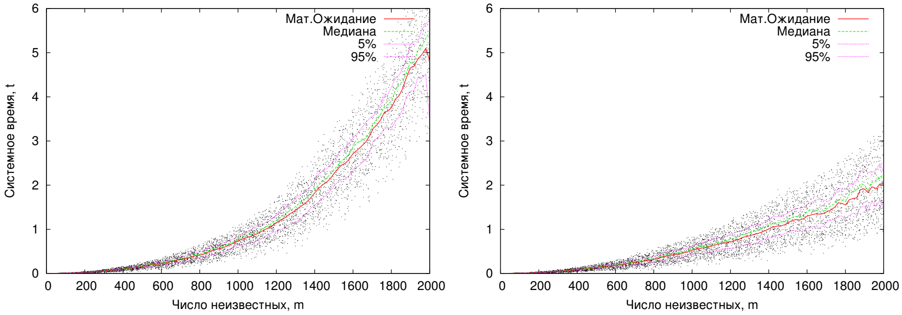


- Рост времени решения для SlopesSys при увеличении размерности в отличие от Syntactic
- Более низкая верхняя граница у Syntactic
- Сравнимость Syntactic и Slopes

Экспериментальное сравнение

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

Экспериментальное сравнение



- TransSol эффективнее Syntactic ($\sim$ mn)
- Дискретность потребления ресурсов
- Рост потребления ресурсов для Syntactic при $10 < m < 100$
- Компактная верхняя граница у TransSol

Задача восстановления

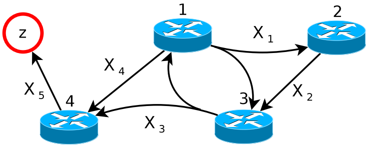
- Сеть MPLS (мультипротокольная коммутация по меткам):
  - Разделение трафика на классы эквивалентности FEC
  - Сопоставление метки пакету
  - Множество меток — таблица маршрутизации
- Потеря соединения:
  - нарушение линии связи или выход из строя узла
  - Задача построения обходного маршрута (поиск 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)
- Local protection (Fast reroute)
  - Расширение IP reroute
  - Локальное восстановление
- Short Leap Shared Protection
  - Разбиение маршрута на пересекающиеся домены
  - Построение набора циклов
  - Комбинация локального и глобального восстановлений
- Path protection
  - Построение резервного маршрута
  - Глобальное восстановление

Диофантова модель сети MPLS

- система одАНЛДУ
  $$\sum_{i \in I_k} x_i = \sum_{i=1}^{m} a_{ki}$$
- $k \in S$ — узлы сети
- x_i — линии связи
- I_k — исходящие линии
- a_{ki} — мера линии связи
- $h^{(s)} \in \mathcal{H}$ — маршрут в сети



$$\begin{cases} x_1 + x_4 = 2x_3 \\ x_2 = 3x_1 \\ x_3 = 2x_1 + x_2 \\ x_5 = x_4 + x_3 \end{cases}$$

Заключение

- Единый подход к задачам решения и генерации
- Алгоритм решения произвольной системы одАНЛДУ
- Пять алгоритмов генерации систем одАНЛДУ
- Программные системы alg_analyser и Web-SynDic
- Результаты экспериментального исследования
- 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 homogenious 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.

Спасибо за внимание!