

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Московский физико-технический институт
(национальный исследовательский университет)»



СБОРНИК программ и заданий

**Высшая школа программной инженерии
(ВШПИ)**

**для студентов 3 курса
на осенний семестр
2024–2025 учебного года**

МОСКВА
МФТИ
2024

Сборник программ и заданий для студентов 3 курса
на осенний семестр 2024–2025 учебного года. **Высшая школа
программной инженерии (ВШПИ).** – Москва : МФТИ, 2024. – 16 с.

© Федеральное государственное
автономное образовательное
учреждение высшего образования
«Московский физико-
технический институт (национальный
исследовательский университет)», 2024

УТВЕРЖДЕНО
Проректор по учебной работе
А. А. Воронов
17 июня 2024 г.

ПРОГРАММА

по дисциплине: **Формальные языки и сложность вычислений**
по направлению: **09.03.01 «Информатика и вычислительная техника»**
подготовки:
физтех-школа: **ВШПИ**
кафедра: **высшей математики**
курс: **3**
семестр: **5**

лекции — 30 часов
практические (семинарские)
занятия — 30 часов
лабораторные занятия — нет

Экзамен — 5 семестр

ВСЕГО АУДИТОРНЫХ ЧАСОВ — 60

Самостоятельная работа:
теор. курс — 45 часов

Программу составил

к. ф.-м. н., ст. преп. А. В. Зухба

Программа принята на заседании кафедры
высшей математики 11 апреля 2024 г.

Заведующий кафедрой
д. ф.-м. н., профессор

Г. Е. Иванов

Тема 7: Формальные языки (5 недель)

1. Формальный язык. Операции с формальными языками. Регулярные языки и регулярные выражения. Детерминированный конечный автомат (ДКА), распознавание языка на ДКА. Недетерминированный конечный автомат (НКА), распознавание языка на НКА.
2. Эквивалентность описаний регулярных языков различными формализмами. Замкнутость регулярных языков относительно теоретико-множественных операций.
3. Лемма о накачке, разделяющие суффиксы, теорема Майхилла–Нероуда.
4. Другие используемые виды формальных языков. Иерархия Хомского. Контекстно-свободные грамматики.
5. Канонические формы КС-грамматик (нормальная форма Хомского). Свойства замкнутости КС-языков (КСЯ), незамкнутость КСЯ относительно пересечения. Дерево вывода КСГ. Однозначность КС-грамматик. Лемма о накачке для КСЯ. Проверка принадлежности слова КСГ (алгоритм Кока–Янгера–Касами)*. Автоматы с магазинной памятью*.

Тема 8: Вычислительная сложность (7 недель)

1. Детерминированные и недетерминированные машины Тьюринга
2. Временная и пространственная сложность вычислений. Теорема об ускорении. Теоремы об иерархии. Классы DTIME, NTIME, их связь. Классы P и NP, два определения класса NP, их эквивалентность. NP-трудные и NP-полные языки, связанные с этим задачи.
3. Сводимость по Тьюрингу, по Куку и по Карпу. Использование сводимости по Карпу для доказательства NP-полноты. Теорема Кука–Левина.
4. Со-классы, класс coNP, его связь с P и NP, примеры задач из класса coNP. Полиномиальная иерархия.
5. Самосводимость и задачи поиска. Аппроксимационные алгоритмы для решения NP-полных задач. Вычисления с оракулом.
6. Вероятностная машина Тьюринга, понятие о вероятностном вычислении. Классы RP и coRP, их связь с NP и coNP. Классы BPP и PP, их связь и связь с невероятностными классами.
7. Амплификация и независимость вероятностных классов от значений вероятностей. Дерандомизация вероятностных алгоритмов.
8. Классы DSPACE, NSPACE, их связь с временными классами. Класс PSPACE. Теорема Савича. Класс L, класс NL, логарифмическая сводимость. NL-полнота. Теорема Иммермана–Селепченя.

Литература

1. Хопкрофт Д., Мотвани Р., Ульман Д. Введение в теорию автоматов, языков и вычислений – пер. с англ. Васылык О.И. [и др.]. — 2-е изд. — Москва : Вильямс, 2002, 2008.
2. Ахо А., Сети Р., Ульман Дж. Компиляторы. Принципы, технологии, инструменты. — Москва, Санкт-Петербург : Вильямс, 2001.
3. Журавлев Ю.И., Флеров Ю.А., Вялый М.Н. Дискретный анализ. Формальные системы и алгоритмы: Учеб. пособие для вузов — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023.
4. Верецагин Н.К., Шень А. Вычислимые функции. Лекции по математической логике и теории алгоритмов. Ч. 3., изд. 4-е. — Москва : МЦНМО, 2012.
5. Гэри М. и Джонсон Д. Вычислительные машины и труднорешаемые задачи. — Москва : Мир, 1982.
6. Абрамов С. А. Лекции о сложности алгоритмов. — Москва : МЦНМО, 2012.

ПЕРВОЕ ЗАДАНИЕ

(срок сдачи 14–19 октября)

I. Формальные языки

1. Определим язык $L \subseteq \{a, b\}^*$ индуктивными правилами:
 - $\epsilon, b, bb \in L$;
 - вместе с любым словом $x \in L$ в L также входят слова $ax, bax, bba x$;
 - никаких других слов в L нет.Язык $T \subseteq \{a, b\}^*$ состоит из всех слов, в которых нет трёх букв b подряд.
 - (a) Докажите или опровергните, что $L = T$. Если равенство неверно, то нужно явно указать слово, принадлежащее одному языку и не принадлежащее другому. Если равенство верно, то нужно провести доказательство по индукции в обе стороны: $L \subseteq T$ и $T \subseteq L$.
 - (b) Запишите язык T в виде регулярного выражения.
 - (c) Постройте конечный автомат, принимающий T . Докажите (по индукции), что построенный автомат принимает язык T .
2. К языку L_1 добавили конечный язык R и получили язык L ($L = L_1 \cup R$). Язык L оказался регулярным. Верно ли, что язык L_1 мог быть нерегулярным?
3. Пусть $X_1, X_2, \dots, X_n, \dots$ – бесконечное семейство регулярных языков.
 - (a) Верно ли, что язык $X = \bigcup_{n=1}^{\infty} X_i$ является регулярным языком?
 - (b) Верно ли, что язык $X = \bigcap_{n=1}^{\infty} X_i$ является регулярным языком?
4. Опишите язык $\{a^{3n} \mid n > 0\} \cap \{a^{5n+1} \mid n \geq 0\}^*$ регулярным выражением.

5. Выполните следующие задания.

- (а) Построить ДКА, принимающий язык L , состоящий из всех слов в алфавите $\{0, 1\}$, которые содержат чётное число нулей и нечётное число единиц.
- (б) Построить эквивалентную праволинейную грамматику. Будет ли она однозначной?

6. Постройте НКА, принимающий язык L_3 , состоящий из слов в алфавите $\{a, b\}$, у которых третий от конца символ равен « a ». Затем, используя алгоритм, постройте эквивалентный полный ДКА.

7. Докажите, что язык $L_{\geq} = \{a^n b^m \mid n \geq m\}$ нерегулярен.

8. Будут ли регулярными следующие языки?

- (а) $L_1 = \{a^{2019n+5} \mid n = 0, 1, \dots\} \cap \{a^{503k+29} \mid k = 401, 402, \dots\} \subseteq \{a^*\}$.
- (б) $L_2 = \{a^{200n^2+1} \mid n = 1000, 1001, \dots\} \subseteq \{a^*\}$.
- (с) Язык L_3 всех слов в алфавите $\{0, 1\}$, которые представляют числа в двоичной записи, дающие остаток два при делении на три (слово читается со старших разрядов). Например, $001010 \notin L_3$ ($1010_2 = 10_{10} = 3 \times 3 + 1$), а $10001 \in L_3$ ($10001_2 = 17_{10} = 5 \times 3 + 2$).

9. Покажите, что следующий язык удовлетворяет лемме о разрастании для регулярных языков, но сам регулярным не является:

$$L = \{ab^{2^i} \mid i \geq 0\} \cup \{b^j \mid j \geq 0\} \cup \{a^m b^n \mid m > 1, n \geq 0\}.$$

10. Докажите или опровергните, что лемма о разрастании является критерием для регулярных языков в однобуквенном алфавите.

11. Найдите все классы эквивалентности Майхилла–Нероуда для языка $(a+b)^* ab(a+b)^*$ и постройте по ним ДКА.

12. Опишите классы эквивалентности Майхилла–Нероуда для языка L . В случае конечности множества классов, постройте минимальный полный ДКА, распознающий L .

(а) $L = \{w \mid |w|_a = |w|_b\}$.

(б)* $L = \{w \mid |w|_{ab} = |w|_{ba}\}$.

13. Известно, что L_1 — КС язык, не являющийся регулярным, а L_2 — не КС-язык. Может ли язык $L_2 L_1$ быть регулярным языком? При положительном ответе привести пример.

14. Язык $L^=$ является языком всех слов с равным числом символов a и b .

(а) Покажите индукцией по длине слова, что КС-грамматика с правилами $S \rightarrow SS \mid aSb \mid bSa \mid \varepsilon$ порождает язык $L^=$.

(б)* Грамматика называется линейной, если в правые части правил вывода входит не более одного нетерминала. Покажите, что язык $L^=$ не порождается никакой линейной КСГ.

15. КС-грамматика называется *левооднозначной*, если каждое слово порожаемого ею языка имеет единственный левый вывод. Аналогично определяется *правооднозначная грамматика*. Можно ли построить пример левооднозначной, но не правооднозначной КС-грамматики?
16. Является ли язык L КС ?
- $L = \{a^n b^n c^n \mid n \in \mathbb{N}_0\}$.
 - $L = \{w c w \mid w \in \{a, b\}^*\}$.
17. Палиндромами называют слова, которые одинаково читаются слева направо и справа налево, например, «ротор». Пусть задан произвольный конечный алфавит, состоящий более чем из одного символа.
- Покажите, что язык палиндромов не является регулярным.
 - Покажите, что язык палиндромов является КС-языком.
 - * Покажите, что дополнение к языку палиндромов (язык всех непалиндромов) также является КС-языком.
 - Постройте КС-грамматику языка палиндромов в алфавите $\Sigma = \{a, b\}$ (с доказательством корректности).
 - Приведите грамматику к нормальной форме Хомского.
 - * Для данной грамматики продемонстрируйте работу алгоритма Кока–Янгера–Касами на слове *abaaba*.
18. Для языка правильных скобочных выражений:
- Покажите, что язык не является регулярным.
 - Постройте КС-грамматику данного языка (с доказательством корректности).
 - Приведите грамматику к нормальной форме Хомского.
 - * Для данной грамматики продемонстрируйте работу алгоритма Кока–Янгера–Касами на слове $(())()$.
- 19.* Для языка $L = \{w \mid w = xcy, x, y \in \{a, b\}^*; |x| = |y|\}$
- постройте КС-грамматику G , порождающую язык L ;
 - постройте недетерминированный МА, эквивалентный этой грамматике;
 - продемонстрируйте работу построенного МА на слове *acab* (проанализируйте все варианты поведения).

ВТОРОЕ ЗАДАНИЕ

(срок сдачи 9–14 декабря)

I. Вычислительная сложность

1. Ответьте на следующие вопросы. Ответ необходимо обосновать.

- (a) Верно ли, что дополнение любого конечного языка лежит в классе P ?
- (b) Верно ли, что каждый регулярный язык принадлежит классу P ?
- 2. Исследовать следующие языки на принадлежность классу P :
 - (a) $L_A = \{\langle M, w \rangle : \text{машина } M \text{ принимает слово } w\}$;
 - (b) $L_B = \{\langle M, w \rangle : \text{машина } M \text{ принимает слово } w \text{ за } 2^{100} \text{ шагов}\}$;
 - (c) $L_C = \{\langle M, w, 1^t \rangle : \text{машина } M \text{ принимает слово } w \text{ за } t \text{ шагов}\}$.
- 3. Докажите, что следующие языки принадлежат классу P :
 - (a) 2-COL: язык описаний графов, допускающих раскраску в два цвета;
 - (b) 2-CNF: язык описаний выполнимых 2-КНФ;
 - (c) $L_1 = \{\langle G, k \rangle : \text{граф } G \text{ имеет ровно } k \text{ компонент связности}\}$;
 - (d) $L_2 = \{\langle a, b, c, p \rangle : a^b = c \pmod{p}\}$.
- 4. Приведите пример языка, который не принадлежит классу P , но его итерация этому классу принадлежит.
- 5. Рассмотрим сертификатное определение класса NP .

Язык $L \subseteq \{0, 1\}^$ лежит в классе NP если существуют полиномы $p, q : \mathbb{N} \rightarrow \mathbb{N}$ и ДМТ M (называемая верификатором L), такая что для всех $x \in \{0, 1\}^*$*

$$x \in L \Leftrightarrow \exists u \in \{0, 1\}^{p(|x|)}, \text{ такое что } M(x, u) = 1.$$

И при этом машина M останавливается на входе (x, u) не более, чем за $q(|(x, u)|)$ шагов. Такое u мы будем называть сертификатом слова x . Всюду под «можно ли» подразумевается следующее: останется ли при такой замене класс языков NP неизменным.

- (a) В определении стоит $y \in \Sigma^{p(|x|)}$. Можно ли смягчить требование, положив $y \in \Sigma^*, |y| \leq p(|x|)$?
- (b) В определении МТ останавливается за $q(|x| + |y|)$ шагов. Можно ли убрать из требования y , оставив $p(|x|)$ шагов?
- (c) Можно ли после предыдущих упрощений вообще убрать полиномиальное ограничение на y , получив такое определение $L \in NP$, если: существует ДМТ M , существует полином $p(n)$, такие, что для любых $x \in \Sigma^*, y \in \Sigma^*$ машина M останавливается на входе (x, y) не более, чем за $p(|x|)$ шагов и

$$(x \in L) \Leftrightarrow \exists y (y \in \Sigma^* \wedge M(x, y) = 1).$$

- (d) Можно ли в 3 пункте заменить $p(|x|)$ на $p(|y|)$?
- 6. Докажите, что $NP \subseteq coNP$ влечёт $NP = coNP$.
- 7. Ответьте на следующие вопросы. Ответ необходимо обосновать.
 - (a) Верно ли, что если $L \in NP$ и $L \in coNPC$, то $NP = coNP$?

(b) Верно ли, что язык $L \in NPC$ тогда и только тогда, когда $\bar{L} \in coNPC$?

(c) Верно ли, что если $L_1 \leq_p L_2$, то $\bar{L}_1 \leq_p \bar{L}_2$?

8. Докажите, что язык *FACTOR* принадлежит классу $NP \cap coNP$.

$FACTOR = \{(n, k) \mid n \in \mathbb{N} \text{ содержит делитель, больший } 1, \text{ но не превосходящий } k\}$.

9. Докажите, что язык всех (простых неориентированных) графов G , в которых существует остовное дерево, содержащее не более 42 листьев, является NP -полным.

10. Докажите, что

(a) для любого i выполняется $co\Sigma_i^P = \Pi_i^P$;

(b) для любого i выполняется $\Sigma_i^P \subset \Sigma_{i+1}^P, \Sigma_i^P \subset \Pi_{i+1}^P, \Pi_i^P \subset \Sigma_{i+1}^P, \Pi_i^P \subset \Pi_{i+1}^P$.

11. Докажите, что язык *EXACTLY2* принадлежит $\Sigma_2^P \cap \Pi_2^P$.

$EXACTLY2 = \{\varphi : \text{булева формула } \varphi \text{ имеет ровно два выполняющих набора}\}$.

12. Докажите, что если проверять наличие в графе клики данного размера можно за 1 шаг, то можно и найти максимальную клику за полиномиальное время.

13. Докажите, что для задачи минимизации вершинного покрытия порог аппроксимации не больше 0,5. В качестве стоимости решения рассматривается количество вершин в вершинном покрытии.

14. Докажите, что если язык является $PSPACE$ -трудным, то он является NP -трудным.

15. Докажите принадлежность следующих языков классу L :

(a) $PAL = \{a : a = a^R\}$;

(b) $SUBSEQ = \{(s, t) : s \text{ является подпоследовательностью } t\}$;

(c) $UCONNECTED = \{G : \text{неориентированный граф } G \text{ связан}\}$.

16. Докажите NL -полноту языков:

(a) $CYCLE = \{G : \text{в ориентированном графе } G \text{ есть цикл}\}$;

(b) $TWOCOMPS = \{G : \text{в ориентированном графе } G \text{ есть хотя бы две компоненты сильной связности}\}$.

17. Покажите, что NL замкнуто относительно звезды Клини.

18. Докажите, что сложность в среднем для быстрой сортировки равна $O(n \log n)$.

19. Рассмотрим сертификатное определение класса NL :

Язык A лежит в NL тогда и только тогда, когда существует машина V с двумя входами, к первому из которых доступ не ограничен,

а второй имеет полиномиальную длину от первого, и его можно читать только один раз слева направо, используя логарифмическую память (от длины первого входа) на рабочей ленте, такая что $x \in A$ тогда и только тогда, когда для некоторого s выполнено $V(x, s) = 1$.

- (a) Какой класс получится, если убрать требование полиномиальности сертификата?
 - (b) Какой класс получится, если заменить полиномиальную длину сертификата на логарифмическую и убрать ограничение на чтение сертификата единожды?
 - (c) Какой класс получится, если заменить полиномиальную длину сертификата на логарифмическую, но оставить ограничение на чтение сертификата единожды?
 - (d) Какой класс получится, если оставить полиномиальную длину сертификата и убрать ограничение на чтение сертификата единожды?
20. Докажите, что если $NP \subset BPP$, то $NP = RP$. *Указание. $RP = BPP_{0,1/n^c}$, где c — произвольная положительная константа.*
- 21.* Докажите, что $PERFECTMATCHING = \{G \mid \text{в графе } G \text{ есть совершенное паросочетание}\}$ лежит в RP .

Составитель задания

к. ф.-м. н., ст. преп. А. В. Зухба

УТВЕРЖДЕНО
Проректор по учебной работе
А. А. Воронов
17 июня 2024 г.

ПРОГРАММА

по дисциплине: **Сетевые технологии**

по направлению подготовки: **09.03.01 «Информатика и вычислительная техника»**

физтех-школа: **ВШПИ**

кафедра: **информатики и вычислительной математики**

курс: **3**

семестр: **5**

лекции – 30 часов

Экзамен – нет

практические (семинарские)

Диф. зачёт – 5 семестр

занятия – 30 часов

лабораторные занятия –

Самостоятельная работа – 75 часов

ВСЕГО АУДИТОРНЫХ ЧАСОВ – 60

Программу составил старший преподаватель Д. А. Подлесных

Программа принята на заседании
кафедры информатики и вычислительной математики
30 января 2024 г.

Заведующий кафедрой,
доцент, д.ф.-м.н.

Н. И. Хохлов

1. Основные понятия компьютерных сетей: типы, топологии, методы доступа к среде передачи.
2. Аппаратные компоненты компьютерных сетей. Принципы пакетной передачи данных.
3. Понятие сетевой модели. Сетевая модель OSI и другие сетевые модели. Модель TCP/IP. Инкапсуляция.
4. L1: витая пара, оптическое волокно, USB, беспроводные сети, медиа-конвертеры, виды топологии сети.
5. L2: коммутация, Ethernet (802.11), VLAN, широковещательный домен, шторм, STP, LAG.
6. L3: маршрутизация, протокол IP (адреса, маски, бесклассовая организация сетевого пространства, wildcard), статическая и динамическая маршрутизация (RIP, EIGRP, OSPF и BGP). Протоколы ARP и DHCP.
7. L4: Транспортный уровень. UDP, TCP (структура пакета, принцип работы, особенности), SCTP, алгоритмы контроля перегрузки сети.
8. L5: Сесансовый уровень, SOCKS, NetBIOS, RPC.
9. L6: Уровень представления данных, шифрование и кодирование, сжатие с потерями и без потерь, алгоритм Хаффмана, кодеки, JPEG, Код Хэмминга.
10. L7: DNS, HTTP/HTTPS, почтовые протоколы: SMTP, POP3, IMAP. FTP. XMPP.
11. Беспроводные сети и их безопасность.
12. Написание клиент-серверного приложения.
13. DevOps. Разворачивание собственного сайта.
14. Common Gateway Interface.
15. Вызов удалённых процедур. Вызов методов удалённых объектов.
16. REST API.
17. Protocol Buffers.
18. FLASK.
19. Тестирование web-приложения на безопасность. OWASP Top-10.
20. SQL -инъекции. Утилита sqlmap.

Литература

Основная

1. *Таненбаум Э., Уэзеролл Д.* Компьютерные сети : учебник для вузов / пер. с англ. А. Гребенькова. Санкт-Петербург : Питер, 2015.
2. *Олифер В.Г., Олифер Н.А.* Компьютерные сети: принципы, технологии, протоколы : учеб. пособие для вузов. 3-е изд. Санкт-Петербург : Питер, 2007 . 958 с.

Электронные ресурсы

1. <http://lms.mipt.ru>
2. <http://judge.mipt.ru>

ЗАДАНИЕ

(срок сдачи 16–21 декабря)

1. Напишите e-mail преподавателю.
2. Скачайте и установите xmpp-клиент (jabber). Добавьте преподавателя в контакты. Подключитесь к конференции.
3. Зарегистрируйтесь в констесте на ejudge.
4. Выясните, какие Wi-Fi сети видны у Вас дома или в общежитии. На каких частотах, каналах, с каким шифрованием?
5. Как обжаты кабели в аудитории, по варианту А или по В.
6. Где в кампусе находятся оптоволоконные кабели?
7. Какие хосты встречаются по пути от Вашего компьютера до сервера, на котором хостится сайт kernel.org?
8. Выясните MAC-адрес компьютера в аудитории. Подключите свой ноутбук, выставив этот же MAC-адрес.
9. Какой MAC-адрес маршрутизатора, к которому подключены компьютеры в аудитории?
10. Какие порты открыты на judge.mipt.ru?
11. Какая версия SSH стоит на lms.mipt.ru?
12. Найдите флаг в исходном тексте страницы.
13. Найдите флаг по robots exclusion standart.
14. По данным, выведенным свитчем, сделайте вывод о наличии колец в сети.
15. Декодируйте данные из base64.
16. Выясните IP-адрес почтового сервера fsb.ru, который принимает почту, если основной недоступен.
17. Через bgp looking glass выясните, с какими автономными системами связана автономная система МФТИ?
18. С каких IP-адресов могут приходить легальные почтовые сообщения с отправителем в домене @mipt.ru (через DNS и SPF)?
19. Зайдите по ssh на выданный контейнер. Добавьте пользователя, настройте вход по ключу.
20. Поднимите в контейнере HTTP-сервер.
21. Получите сертификат от Let's Encrypt.
22. Удостоверьтесь в работоспособности https до Вашего контейнера.
23. Сделайте перенаправление с http на https.

Учебное издание

**СБОРНИК
программ и заданий**

**Высшая школа программной инженерии
(ВШПИ)**

**для студентов 3 курса
на осенний семестр
2024–2025 учебного года**

Редакторы и корректоры: *И.А. Волкова, Н.Е. Кобзева*
Компьютерная верстка *В.А. Дружининой*

Подписано в печать 18.07.2024. Формат 60 × 84 1/16. Усл. печ. л. 1,75. Тираж 42 экз.
Заказ № 157.

Федеральное государственное автономное образовательное учреждение
высшего образования «Московский физико-технический институт (национальный
исследовательский университет)»
141700, Московская обл., г. Долгопрудный, Институтский пер., 9 Тел. (495) 408-58-22,
e-mail: rio@mipt.ru

Отдел оперативной полиграфии «Физтех-полиграф»

141700, Московская обл., г. Долгопрудный, Институтский пер., 9 Тел. (495) 408-84-30, e-mail:
polygraph@mipt.ru

Для заметок