Фізико-технічний інститут **Осінь 2021**
кафедра математичних методів захисту інформації

Теорія складності

Конструктивні функції

4.3 Конструктивні функції

Деякі функції виду $\mathbb{N} \to \mathbb{N}$ важко використовувати як функції, які обмежують часову чи просторову складність деякої машини Тюрінга, при деяких застосуваннях. Наприклад, коли треба визначити за час $\mathcal{O}(t(n))$ чи виконала деяка машина Тюрінга $t(n)$ тактів з певним вхідним словом з довжиною n, $n \in \mathbb{N}$. Це є необхідним для моделювання однією машиною Тюрінга роботи іншої машини Тюрінга з деяким вхідним словом. З цього випливає, що значення функції t обчислюється за час $\mathcal{O}(t(n))$, а це не завжди виконується для довільної функції виду $\mathbb{N} \to \mathbb{N}$.

Більше того, розглянемо клас функцій виду $\{0,1\}^* \to \{0,1\}^*$, які можна обчислити за допомогою машин Тюрінга з часовою складністю $t(n)$, $t : \mathbb{N} \to \mathbb{N}$, та клас функцій виду $\{0,1\}^* \to \{0,1\}^*$, які можна обчислити за допомогою машин Тюрінга з часовою складністю $2^{2^{t(n)}}$. Інтуїтивно можна очікувати, що другий клас функцій має бути значно більшим, оскільки відповідні машини Тюрінга мають значно більше ресурсів щодо часу виконання, а, отже, можуть обчислити більше функцій. Для деяких функцій t такі класи функцій будуть однаковими.

Якщо функції $s_1 : \mathbb{N} \to \mathbb{N}$ і $s_2 : \mathbb{N} \to \mathbb{N}$ є просторовими обмеженнями двох множин машин Тюрінга, і функція s_1 зростає швидше на асимптотиці ніж функція s_2, то знову інтуїтивно можна очікувати, що перша множина машин Тюрінга обчислює більший клас функцій виду $\{0,1\}^* \to \{0,1\}^*$. Але, якщо різниця між функціями s_1 та s_2 є невеликою та важкою для обчислення (в то му сенсі, що просторова складність такого обчислення є більшою за цю різницю), то машини Тюрінга з першого класу не зможуть обчислити додаткову кількість комірок, які їх можна використовувати для обчислень.

Щоб уникнути описаних випадків, висувають певні вимоги до функцій, які обмежують часову чи просторову складність машин Тюрінга. Основною вимогою є існування хоча б однієї машини Тюрінга, функція часової (або просторової) складності якої збігається з функцією, що буде використовуватися для обмеження. З метою більш формального означення використовують поняття конструктивної за часом та конструктивної за пам'яттю функцій.

Означення 4.1. Функцію $f : \mathbb{N} \to \mathbb{N}$, називають *конструктивною за часом* (англ. time-constructible), якщо існує така багатострічкова детермінована машина Тюрінга M з часом роботи $\mathcal{O}(f(n))$ з довільним вхідним словом з довжиною n, і результатом роботи машини Тюрінга M з вхідним словом 1^n є слово $1^{f(n)}$.

Приклад 4.1. Стала функція, $f_1(n) = n$, $f_2(n) = n \log n$, $f_3(n) = n^3$ і $f_4(n) = 2^n$, $n \in \mathbb{N}$, є прикладами конструктивних за часом функцій.

Означення 4.1 будемо використовувати далі, але воно не є єдиним означенням конструктивних за часом функцій. Основною метою конструктивних за часом функцій є побудова формальної ідеалізованої моделі "годинника", яка допоможе одній машині Тюрінга змоделювати роботу іншої машини Тюрінга з деяким вхідним словом без перевищення певної часової складності. Одним з варіантів моделі такого "годинника" є використання додаткових стрічок, на яких спочатку обчислюється значення відповідної кількості тактів моделювання (в залежності від довжини вхідного слова), наприклад у вигляді слова $1^{f(n)}$, де $n \in \mathbb{N}$ — довжина вхідного слова, для якого моделюється робота деякої машини Тюрінга, а далі, при моделюванні роботи цієї машини Тюрінга, на кожному такті йде затирання одного символу слова $1^{f(n)}$, поки вони не закінчаться. Більш строгим варіантом моделі такого "годинника" є використання машини Тюрінга, яка працює точно $f(n)$ з будь-яким словом з довжиною n (або хоча б з одним словом, наприклад, зі словом 1^n). Така модель "годинника" також працює з окремими стрічками при моделюванні, але працює "паралельно" з модельованою машиною Тюрінга і моделювання закінчується, коли "годинник" дійде до кінцевого стану.

З урахуванням також різних можливих варіантів машин Тюрінга, які використовуються як основна модель обчислень маємо, що в різних джерелах зустрічаються й інші означення, більшість з яких є еквівалентними означенню 4.1, але деякі можуть відрізнятися, визначаючи дещо різні класи конструктивних за часом функцій.

Означення 4.2. Функцію $f : \mathbb{N} \to \mathbb{N}$ називають *конструктивною за часом*, якщо існують багатострічкова детермінована машина Тюрінга M і натуральне число $n_0 \in \mathbb{N}$ такі, що для довільного значення $n \in \mathbb{N}$, $n \geq n_0$, час роботи машини Тюрінга M з довільним вхідним словом з довжиною n дорівнює $O(f(n))$ і машина Тюрінга M зупиняється з вхідним словом 1^n, виконавши точно $f(n)$ тактів.

Означення 4.3. Функцію $f : \mathbb{N} \to \mathbb{N}$ називають *конструктивною за часом*, якщо існує така багатострічкова детермінована машина Тюрінга M, що для довільного значення $n \in \mathbb{N}$ час роботи машини Тюрінга M з довільним вхідним словом з довжиною n дорівнює $O(f(n))$ та існує вхідне слово з довжиною n, з яким машина Тюрінга M зупиняється, виконавши точно $f(n)$ тактів.

Означення 4.4. Функцію $f : \mathbb{N} \to \mathbb{N}$ називають *конструктивною за часом*, якщо існує така багатострічкова детермінована машина Тюрінга M, що для довільного значення $n \in \mathbb{N}$ час роботи машини Тюрінга M з довільним вхідним словом з довжиною n дорівнює $\mathcal{O}(f(n))$ і машина Тюрінга M є застосовною до вхідного слова 1^n, а результатом роботи машини Тюрінга M з вхідним словом 1^n є слово $\lfloor f(n) \rfloor$.

Твердження 4.1. Якщо функція $f : \mathbb{N} \to \mathbb{N}$ є конструктивною за часом функцією, то або $f \in \Omega(n)$, $n \in \mathbb{N}$, або функція f є сталою на асимптотиці.

Твердження 4.2. Нехай функції $f_1, f_2 : \mathbb{N} \to \mathbb{N}$ є конструктивними за часом функціями. Тоді функції

- $f_1 + f_2$;
- $f_1 \cdot f_2$;
- $f_1^{f_2}$;
- c^{f_1}, для довільного натурального числа $c \in \mathbb{N}$, $c > 1$,

також є конструктивними за часом функціями.

Іноді, також виділяють схожий клас функцій.

Означення 4.5. Функцію $f : \mathbb{N} \to \mathbb{N}$ називають *повністю конструктивною за часом* (англ. fully time-constructible), якщо існують багатострічкова детермінована машина Тюрінга M і натуральне число $n_0 \in \mathbb{N}$ такі, що для довільного значення $n \in \mathbb{N}$, $n \geq n_0$, машина Тюрінга M зупиняється, виконавши точно $f(n)$ тактів, з довільним вхідним словом з довжиною n.

Наслідок. Будь-яка повністю конструктивна за часом функція є конструктивною за часом функцією.

Іноді, в означеннях 4.1 і 4.4 замість умови, що для довільного значення $n \in \mathbb{N}$ час роботи машини Тюрінга M з довільним вхідним словом з довжиною n дорівнює $O(f(n))$, використовується вимога, що машина Тюрінга M з довільним вхідним словом з довжиною n повинна зробити щонайбільше $f(n)$ тактів. Але все ж таки має використовуватися асимптотична нотація.

Розглянемо, наприклад, конструктивну за часом функцію $f(n) = \max\{1, n-2\}$, $n \in \mathbb{N}$. Згідно з визначенням функції f вона приймає такі значення: $f(0) = 1$, $f(1) = 1$, $f(2) = 1$, $f(3) = 1$ і $f(4) = 2$. За умови, що машина Тюрінга з довільним вхідним словом з довжиною n повинна зробити щонайбільше (або точно) $f(n)$ тактів, виходить, що будь-яка машина Тюрінга повинна вже на першому такті здогадатися чи довжина вхідного слова є більшою ніж 3 (інакше, вона має зупинитися після першого такту), а це не є можливим. З цією ж метою в означення конструктивної функції вводиться додаткове натуральне число, щоб умова означення виконувалася, починаючи з певного значення. Існує велика кількість конструктивних за часом функцій, які зростають дуже повільно, наприклад, як функція $f(n) = \lceil n \log(\log(\log(\sqrt[8]{n})))\rceil$, і для яких обчислення значення для невеликих значень аргументу виглядає набагато складнішим ніж розмір вхідних даних (в таких випадках, як правило, при побудові машин Тюрінга використовують передобчислені значення для певної скінченної кількості аргументів). Тому знову ж таки найважливішим є поведінка функцій на асимптотиці і формальні означення мають містити відповідні умови.

Більш того, означення конструктивної за часом функції, які використовують точну кількість тактів, мають певні додаткові обмеження. Наприклад, розглянемо функцію $f : \mathbb{N} \to \mathbb{N}$, $f(n) = \begin{cases} n, & n \neq 2^k \text{ для деякого } k \in \mathbb{N} \\ n+1, & n = 2^k \text{ для деякого } k \in \mathbb{N} \end{cases}$. Згідно з означенням 4.1 така функція f є конструктивною за часом, але не за означенням 4.2.

Вказана в означеннях конструктивної за часом функції, модель обчислень у вигляді багатострічкової детермінованої машини Тюрінга є важливою складовою означень. Наприклад, якщо обмежити детерміновану машину Тюрінга використанням лише однієї стрічки, то клас конструктивних за часом функцій зміниться. Стала функція є конструктивною за часом згідно з означенням 4.1, але не буде такою, якщо замінити в означенні 4.1 багатострічкову детерміновану машину Тюрінга на однострічкову.

Зауваження. Досить часто, не без підстав, висувають в означенні конструктивних за часом функцій додаткову вимогу: для будь-якої конструктивної за часом функції $f : \mathbb{N} \to \mathbb{N}$ та будь-якого натурального числа $n \in \mathbb{N}$ має виконуватися нерівність $f(n) \geq n$ (або, в залежності від використаного варіанту машини Тюрінга як обчислювальної моделі: $f(n) \geq n+1$, або $f(n) \geq n \log n$ для всіх значень $n \in \mathbb{N}$). Мінімальна вимога $f(n) \geq n$ висувається з метою, щоб машина Тюрінга повністю прочитала вхідне слово, і зробити означення більш стійким до змін обчислювальної моделі. Але з урахування обраної моделі обчислень далі будемо вважати, що такі вимоги є додатковими і не входять до означення конструктивної за часом функції.

Також, іноді додатковою вимогою є те, що всі конструктивні за часом функції мають бути неспадними функціями. Цю вимогу також будемо вважати корисною при деяких застосуваннях, але необов'язковою.

Так само вводиться клас конструктивних за пам'яттю функцій.

Означення 4.6. Функцію $f : \mathbb{N} \to \mathbb{N}$ називають *конструктивною за пам'яттю* (англ. space-constructible), якщо існує така багатострічкова детермінована машина Тюрінга M, що для довільного значення $n \in \mathbb{N}$ машина Тюрінга

M є застосовною до довільного вхідного слова з довжиною n і при цьому використовується $\mathcal{O}(f(n))$ пам'яті, а результатом роботи машини Тюрінга M з вхідним словом 1^n є слово $1^{f(n)}$.

Прикладами конструктивних за пам'яттю функцій є також стала функція, $f_1(n) = n$, $f_2(n) = n \log n$, $f_3(n) = n^3$ і $f_4(n) = 2^n$, $n \in \mathbb{N}$, але важливою відмінністю є функція $f(n) = \log n$, $n \in \mathbb{N}$, яка є конструктивною за пам'яттю, але не є конструктивною за часом. А, наприклад, функція $f(n) = \log \log n$, $n \in \mathbb{N}$, не є конструктивною за пам'яттю функцією.

Досить часто, не без підстав, додають в означення конструктивних за пам'яттю функцій додаткову вимогу: для будь-якої конструктивної за часом функції $f : \mathbb{N} \to \mathbb{N}$ та будь-якого значення $n \in \mathbb{N}$ має виконуватися нерівність $f(n) \geq \log n$, але також цю вимогу не будемо вважати частиною означення.

Наслідок. Будь-яка конструктивна за часом функція є конструктивною за пам'яттю функцією.

Твердження 4.3. Нехай функції $f_1, f_2 : \mathbb{N} \to \mathbb{N}$ є конструктивними за пам'яттю функціями. Тоді функції

- $f_1 + f_2$;
- $f_1 \cdot f_2$;
- $f_1^{f_2}$;
- c^{f_1}, для довільного натурального числа $c \in \mathbb{N}$, $c > 1$,

також є конструктивними за пам'яттю функціями.