Зведення мов та задач

Андрій Фесенко

Поняття зведення

Зведенням і називають певну процедуру (або алгоритм) перетворення однієї (обчислювальної) задачі в іншу.
Задача Π_1 зводиться до задачі Π_2:

1. використати наявний розв'язок задачі Π_2
2. довести складність розв'язку задачі Π_1

Поняття зведення

Зведенням і називають певну процедуру (або алгоритм) перетворення однієї (обчислювальної) задачі в іншу.
Задача Π_1 зводиться до задачі Π_2:

1. використати наявний розв'язок задачі Π_2
2. довести складність розв'язку задачі Π_1

Приклад

- задача Π_1 — задача знайти розв'язок квадратного рівняння $ax^2 + bx + c = 0$ для довільних дійсних чисел a, b і c

Поняття зведення

Зведенням і називають певну процедуру (або алгоритм) перетворення однієї (обчислювальної) задачі в іншу.
Задача Π_1 зводиться до задачі Π_2:

1. використати наявний розв'язок задачі Π_2
2. довести складність розв'язку задачі Π_1

Приклад

- задача Π_1 — задача знайти розв'язок квадратного рівняння $ax^2 + bx + c = 0$ для довільних дійсних чисел a, b і c
- задача Π_2 — задача знайти розв'язок квадратного рівняння $x^2 + bx + 1 = 0$ для довільного дійсного числа b

Поняття зведення

Зведенням і називають певну процедуру (або алгоритм) перетворення однієї (обчислювальної) задачі в іншу.
Задача Π_1 зводиться до задачі Π_2:

1. використати наявний розв'язок задачі Π_2
2. довести складність розв'язку задачі Π_1

Приклад

- задача Π_1 — задача знайти розв'язок квадратного рівняння $ax^2 + bx + c = 0$ для довільних дійсних чисел a, b і c
- задача Π_2 — задача знайти розв'язок квадратного рівняння $x^2 + bx + 1 = 0$ для довільного дійсного числа b
- задача Π_3 — задача знайти розв'язок квадратного рівняння $x^2 - 2x + 1 = 0$

Поняття зведення

Зведенням і називають певну процедуру (або алгоритм) перетворення однієї (обчислювальної) задачі в іншу.
Задача Π_1 зводиться до задачі Π_2:

1. використати наявний розв'язок задачі Π_2
2. довести складність розв'язку задачі Π_1

Приклад

- задача Π_1 — задача знайти розв'язок квадратного рівняння $ax^2 + bx + c = 0$ для довільних дійсних чисел a, b і c
- задача Π_2 — задача знайти розв'язок квадратного рівняння $x^2 + bx + 1 = 0$ для довільного дійсного числа b
- задача Π_3 — задача знайти розв'язок квадратного рівняння $x^2 - 2x + 1 = 0$
- $\Rightarrow$ задача Π_3 зводиться до задачі Π_2

Поняття зведення

Зведенням і називають певну процедуру (або алгоритм) перетворення однієї (обчислювальної) задачі в іншу.
Задача Π_1 зводиться до задачі Π_2:

1. використати наявний розв'язок задачі Π_2
2. довести складність розв'язку задачі Π_1

Приклад

- задача Π_1 — задача знайти розв'язок квадратного рівняння $ax^2 + bx + c = 0$ для довільних дійсних чисел a, b і c
- задача Π_2 — задача знайти розв'язок квадратного рівняння $x^2 + bx + 1 = 0$ для довільного дійсного числа b
- задача Π_3 — задача знайти розв'язок квадратного рівняння $x^2 - 2x + 1 = 0$
- $\Rightarrow$ задача Π_3 зводиться до задачі Π_2
- $\Rightarrow$ задача Π_2 зводиться до задачі Π_1

Приклади зведень

Приклад

Доведення нерозв'язності задачі $HALT_\varepsilon$:
з існування розв'язку задачі $HALT_\varepsilon$ будувався розв'язок задачі $HALT$
$\Rightarrow$ зведення задачі $HALT$ до задачі $HALT_\varepsilon$

Приклади зведень

Приклад

- *PRIME* — для заданого натурального числа визначити, чи є воно простим;

Приклади зведень

Приклад

- *PRIME* — для заданого натурального числа визначити, чи є воно простим;
- *COMPOSITE* — для заданого натурального числа визначити, чи має воно нетривіальні дільники (відмінні від числа 1 та самого заданого числа);

Приклади зведень

Приклад

- *PRIME* — для заданого натурального числа визначити, чи є воно простим;
- *COMPOSITE* — для заданого натурального числа визначити, чи має воно нетривіальні дільники (відмінні від числа 1 та самого заданого числа);
- *FACTOR* — для заданих натуральних чисел m і k визначити, чи має число m нетривіальний дільник, який є не більшим за число k.

Приклади зведень

Приклад

- *PRIME* — для заданого натурального числа визначити, чи є воно простим;
- *COMPOSITE* — для заданого натурального числа визначити, чи має воно нетривіальні дільники (відмінні від числа 1 та самого заданого числа);
- *FACTOR* — для заданих натуральних чисел m і k визначити, чи має число m нетривіальний дільник, який є не більшим за число k.
- задача *COMPOSITE* зводиться до задачі *PRIME*

Приклади зведень

Приклад

- *PRIME* — для заданого натурального числа визначити, чи є воно простим;
- *COMPOSITE* — для заданого натурального числа визначити, чи має воно нетривіальні дільники (відмінні від числа 1 та самого заданого числа);
- *FACTOR* — для заданих натуральних чисел m і k визначити, чи має число m нетривіальний дільник, який є не більшим за число k.
- задача *COMPOSITE* зводиться до задачі *PRIME*
- задача *PRIME* зводиться до задачі *COMPOSITE*

Приклади зведень

Приклад

- *PRIME* — для заданого натурального числа визначити, чи є воно простим;
- *COMPOSITE* — для заданого натурального числа визначити, чи має воно нетривіальні дільники (відмінні від числа 1 та самого заданого числа);
- *FACTOR* — для заданих натуральних чисел m і k визначити, чи має число m нетривіальний дільник, який є не більшим за число k.
- задача *COMPOSITE* зводиться до задачі *PRIME*
- задача *PRIME* зводиться до задачі *COMPOSITE*
- задачі *PRIME* та *COMPOSITE* зводяться до задачі *FACTOR*

Приклади зведень

Приклад

- *PRIME* — для заданого натурального числа визначити, чи є воно простим;
- *COMPOSITE* — для заданого натурального числа визначити, чи має воно нетривіальні дільники (відмінні від числа 1 та самого заданого числа);
- *FACTOR* — для заданих натуральних чисел m і k визначити, чи має число m нетривіальний дільник, який є не більшим за число k.
- задача *COMPOSITE* зводиться до задачі *PRIME*
- задача *PRIME* зводиться до задачі *COMPOSITE*
- задачі *PRIME* та *COMPOSITE* зводяться до задачі *FACTOR*
- задача *FACTOR* не зводиться ні до задачі *PRIME*, ні до задачі *COMPOSITE*

Означення зведення

Означення

Зведенням мов називають довільне бінарне відношення на множині всіх мов над алфавітом $\{0, 1\}$, яке є рефлексивне та транзитивним. Мова $L_1 \subseteq \{0, 1\}$ **зводиться** до мови $L_2 \subseteq \{0, 1\}$, якщо впорядкована пара (L_1, L_2) належить бінарному відношенню, яке задає зведення. Для позначення зведення мов використовують символ $\leq$ з можливим використанням нижніх та верхніх індексів для уточнення конкретного зведення.

Означення зведення

Означення

Зведенням мов називають довільне бінарне відношення на множині всіх мов над алфавітом $\{0, 1\}$, яке є рефлексивне та транзитивним. Мова $L_1 \subseteq \{0, 1\}$ **зводиться** до мови $L_2 \subseteq \{0, 1\}$, якщо впорядкована пара (L_1, L_2) належить бінарному відношенню, яке задає зведення. Для позначення зведення мов використовують символ $\leq$ з можливим використанням нижніх та верхніх індексів для уточнення конкретного зведення.

Наслідок

Обчислювальна задача Π_1 **зводиться** до обчислювальної задачі Π_2, якщо існують такі схеми кодування e_1 та e_2 задач Π_1 та Π_2 відповідно, що мова $L[\Pi_1, e_2]$ зводиться до мови $L[\Pi_2, e_2]$.

Означення зведення

Означення

Зведенням мов називають довільне бінарне відношення на множині всіх мов над алфавітом $\{0, 1\}$, яке є рефлексивне та транзитивним. Мова $L_1 \subseteq \{0, 1\}$ **зводиться** до мови $L_2 \subseteq \{0, 1\}$, якщо впорядкована пара (L_1, L_2) належить бінарному відношенню, яке задає зведення. Для позначення зведення мов використовують символ $\leq$ з можливим використанням нижніх та верхніх індексів для уточнення конкретного зведення.

Наслідок

Обчислювальна задача Π_1 **зводиться** до обчислювальної задачі Π_2, якщо існують такі схеми кодування e_1 та e_2 задач Π_1 та Π_2 відповідно, що мова $L[\Pi_1, e_2]$ зводиться до мови $L[\Pi_2, e_2]$.

Зауваження

Є застосовним для довільних множин.

Означення зведення

Означення

- нехай r — довільне зведення мов над алфавітом $\{0, 1\}$, а L_1 та L_2 — довільні мови над алфавітом $\{0, 1\}$.

Означення зведення

Означення

- нехай r — довільне зведення мов над алфавітом $\{0, 1\}$, а L_1 та L_2 — довільні мови над алфавітом $\{0, 1\}$.
- $L_1 \leq_r L_2$ — мова L_1 **зводиться за допомогою зведення** r до мови L_2

Означення зведення

Означення

- нехай r — довільне зведення мов над алфавітом $\{0, 1\}$, а L_1 та L_2 — довільні мови над алфавітом $\{0, 1\}$.
- $L_1 \leq_r L_2$ — мова L_1 **зводиться за допомогою зведення** r до мови L_2
- $L_1 \not\leq_r L_2$ — мова L_1 не зводиться за допомогою зведення r до мови L_2

Означення зведення

Означення

- нехай r — довільне зведення мов над алфавітом $\{0, 1\}$, а L_1 та L_2 — довільні мови над алфавітом $\{0, 1\}$.
- $L_1 \leq_r L_2$ — мова L_1 **зводиться за допомогою зведення** r до мови L_2
- $L_1 \not\leq_r L_2$ — мова L_1 не зводиться за допомогою зведення r до мови L_2
- $L_1 <_r L_2$ — $L_1 \leq_r L_2$ та $L_2 \not\leq_r L_1$.

Означення зведення

Означення

- нехай r — довільне зведення мов над алфавітом $\{0,1\}$, а L_1 та L_2 — довільні мови над алфавітом $\{0,1\}$.
- $L_1 \leq_r L_2$ — мова L_1 **зводиться за допомогою зведення** r до мови L_2
- $L_1 \not\leq_r L_2$ — мова L_1 не зводиться за допомогою зведення r до мови L_2
- $L_1 <_r L_2$ — $L_1 \leq_r L_2$ та $L_2 \not\leq_r L_1$.
- $L_1 |_r L_2$ — $L_1 \not\leq_r L_2$ та $L_2 \not\leq_r L_1$.

Означення зведення

Означення

- нехай r — довільне зведення мов над алфавітом $\{0,1\}$, а L_1 та L_2 — довільні мови над алфавітом $\{0,1\}$.
- $L_1 \leq_r L_2$ — мова L_1 **зводиться за допомогою зведення** r до мови L_2
- $L_1 \not\leq_r L_2$ — мова L_1 не зводиться за допомогою зведення r до мови L_2
- $L_1 <_r L_2$ — $L_1 \leq_r L_2$ та $L_2 \not\leq_r L_1$.
- $L_1 |_r L_2$ — $L_1 \not\leq_r L_2$ та $L_2 \not\leq_r L_1$.
- $L_1 =_r L_2$ — мови L_1 і L_2 називають **еквівалентними відносно зведення** r (або r-**еквівалентними**), якщо $L_1 \leq_r L_2$ і $L_2 \leq_r L_1$

Означення зведення

Означення

- нехай r — довільне зведення мов над алфавітом $\{0,1\}$, а L_1 та L_2 — довільні мови над алфавітом $\{0,1\}$.
- $L_1 \leq_r L_2$ — мова L_1 **зводиться за допомогою зведення** r до мови L_2
- $L_1 \not\leq_r L_2$ — мова L_1 не зводиться за допомогою зведення r до мови L_2
- $L_1 <_r L_2$ — $L_1 \leq_r L_2$ та $L_2 \not\leq_r L_1$.
- $L_1 |_r L_2$ — $L_1 \not\leq_r L_2$ та $L_2 \not\leq_r L_1$.
- $L_1 =_r L_2$ — мови L_1 і L_2 називають **еквівалентними відносно зведення** r (або r-**еквівалентними**), якщо $L_1 \leq_r L_2$ і $L_2 \leq_r L_1$
- бінарне відношення $=_r$ є еквівалентністю і окремий клас еквівалентності за відношенням $=_r$ називають r-**степенем**

Означення зведення

Означення

- нехай r — довільне зведення мов над алфавітом $\{0,1\}$, а L_1 та L_2 — довільні мови над алфавітом $\{0,1\}$.
- $L_1 \leq_r L_2$ — мова L_1 **зводиться за допомогою зведення** r до мови L_2
- $L_1 \not\leq_r L_2$ — мова L_1 не зводиться за допомогою зведення r до мови L_2
- $L_1 <_r L_2$ — $L_1 \leq_r L_2$ та $L_2 \not\leq_r L_1$.
- $L_1 |_r L_2$ — $L_1 \not\leq_r L_2$ та $L_2 \not\leq_r L_1$.
- $L_1 =_r L_2$ — мови L_1 і L_2 називають **еквівалентними відносно зведення** r (або r-**еквівалентними**), якщо $L_1 \leq_r L_2$ і $L_2 \leq_r L_1$
- бінарне відношення $=_r$ є еквівалентністю і окремий клас еквівалентності за відношенням $=_r$ називають r-**степенем**
- r-степені будь-якого зведення r є частково впорядкованими зведенням r

Порівняння зведень

Означення

- нехай r_1 та r_2 є довільними зведеннями мов над алфавітом $\{0, 1\}$

Порівняння зведень

Означення

- нехай r_1 та r_2 є довільними зведеннями мов над алфавітом $\{0, 1\}$
- зведення r_1 є **сильнішим ніж зведення** r_2 (відповідно зведення r_2 є **слабкішим ніж зведення** r_1), якщо для довільних мов $L_1, L_2 \subseteq \{0, 1\}^*$ з умови $L_1 \leq_{r_1} L_2$ випливає, що $L_1 \leq_{r_2} L_2$.

Порівняння зведень

Означення

- нехай r_1 та r_2 є довільними зведеннями мов над алфавітом $\{0, 1\}$
- зведення r_1 є **сильнішим ніж зведення** r_2 (відповідно зведення r_2 є **слабкішим ніж зведення** r_1), якщо для довільних мов $L_1, L_2 \subseteq \{0, 1\}^*$ з умови $L_1 \leq_{r_1} L_2$ випливає, що $L_1 \leq_{r_2} L_2$.
- зведення r_1 є **строго сильнішим ніж зведення** r_2 (відповідно зведення r_2 є **строго слабкішим ніж зведення** r_1), якщо зведення r_1 є сильнішим ніж зведення r_2 та існують такі мови $L_1, L_2 \subseteq \{0, 1\}^*$, що $L_1 \leq_{r_2} L_2$, але $L_1 \not\leq_{r_1} L_2$

Порівняння зведень

Означення

- нехай r_1 та r_2 є довільними зведеннями мов над алфавітом $\{0,1\}$
- зведення r_1 є **сильнішим ніж зведення** r_2 (відповідно зведення r_2 є **слабкішим ніж зведення** r_1), якщо для довільних мов $L_1, L_2 \subseteq \{0,1\}^*$ з умови $L_1 \leq_{r_1} L_2$ випливає, що $L_1 \leq_{r_2} L_2$.
- зведення r_1 є **строго сильнішим ніж зведення** r_2 (відповідно зведення r_2 є **строго слабкішим ніж зведення** r_1), якщо зведення r_1 є сильнішим ніж зведення r_2 та існують такі мови $L_1, L_2 \subseteq \{0,1\}^*$, що $L_1 \leq_{r_2} L_2$, але $L_1 \not\leq_{r_1} L_2$
- зведення r_1 є **еквівалентним зведенню** r_2, якщо для довільних мов $L_1, L_2 \subseteq \{0,1\}^*$ твердження $L_1 \leq_{r_1} L_2$ є правильним тоді й тільки тоді, коли $L_1 \leq_{r_2} L_2$

Порівняння зведень

Означення

- нехай r_1 та r_2 є довільними зведеннями мов над алфавітом $\{0,1\}$
- зведення r_1 є **сильнішим ніж зведення** r_2 (відповідно зведення r_2 є **слабкішим ніж зведення** r_1), якщо для довільних мов $L_1, L_2 \subseteq \{0,1\}^*$ з умови $L_1 \leq_{r_1} L_2$ випливає, що $L_1 \leq_{r_2} L_2$.
- зведення r_1 є **строго сильнішим ніж зведення** r_2 (відповідно зведення r_2 є **строго слабкішим ніж зведення** r_1), якщо зведення r_1 є сильнішим ніж зведення r_2 та існують такі мови $L_1, L_2 \subseteq \{0,1\}^*$, що $L_1 \leq_{r_2} L_2$, але $L_1 \not\leq_{r_1} L_2$
- зведення r_1 є **еквівалентним зведенню** r_2, якщо для довільних мов $L_1, L_2 \subseteq \{0,1\}^*$ твердження $L_1 \leq_{r_1} L_2$ є правильним тоді й тільки тоді, коли $L_1 \leq_{r_2} L_2$

Якщо зведення r_1 є сильнішим ніж зведення r_2, то кожен r_2-степінь складається з одного або декількох r_1-степенів.

Порівняння зведень

Означення

- нехай C — деякий клас складності (деяка множина) мов над алфавітом $\{0, 1\}$, r — деяке зведення мов над алфавітом $\{0, 1\}$

Порівняння зведень

Означення

- нехай C — деякий клас складності (деяка множина) мов над алфавітом $\{0,1\}$, r — деяке зведення мов над алфавітом $\{0,1\}$
- клас складності C є **замкненим відносно зведення** r, якщо для довільної мови $L_c \subseteq \{0,1\}^*$ з класу складності C і довільної мови $L_1 \subseteq \{0,1\}^*$ з умови $L_1 \leq_r L_c$ випливає, що $L_1 \in C$

Порівняння зведень

Означення

- нехай C — деякий клас складності (деяка множина) мов над алфавітом $\{0,1\}$, r — деяке зведення мов над алфавітом $\{0,1\}$
- клас складності C є **замкненим відносно зведення** r, якщо для довільної мови $L_c \subseteq \{0,1\}^*$ з класу складності C і довільної мови $L_1 \subseteq \{0,1\}^*$ з умови $L_1 \leq_r L_c$ випливає, що $L_1 \in C$
- мова L_1 — **складна для класу складності** C (C-**складна**) **відносно зведення** r, якщо для кожної мови L_c з класу складності C виконується твердження $L_c \leq_r L_1$

Порівняння зведень

Означення

- нехай C — деякий клас складності (деяка множина) мов над алфавітом $\{0,1\}$, r — деяке зведення мов над алфавітом $\{0,1\}$
- клас складності C є **замкненим відносно зведення** r, якщо для довільної мови $L_c \subseteq \{0,1\}^*$ з класу складності C і довільної мови $L_1 \subseteq \{0,1\}^*$ з умови $L_1 \leq_r L_c$ випливає, що $L_1 \in C$
- мова L_1 — **складна для класу складності** C (C-**складна**) **відносно зведення** r, якщо для кожної мови L_c з класу складності C виконується твердження $L_c \leq_r L_1$
- мова L_1— **повна для класу складності** C (C-**повна**) **відносно зведення** r, якщо вона є складною для класу складності C відносно зведення r і належить класу складності C

Порівняння зведень

Означення

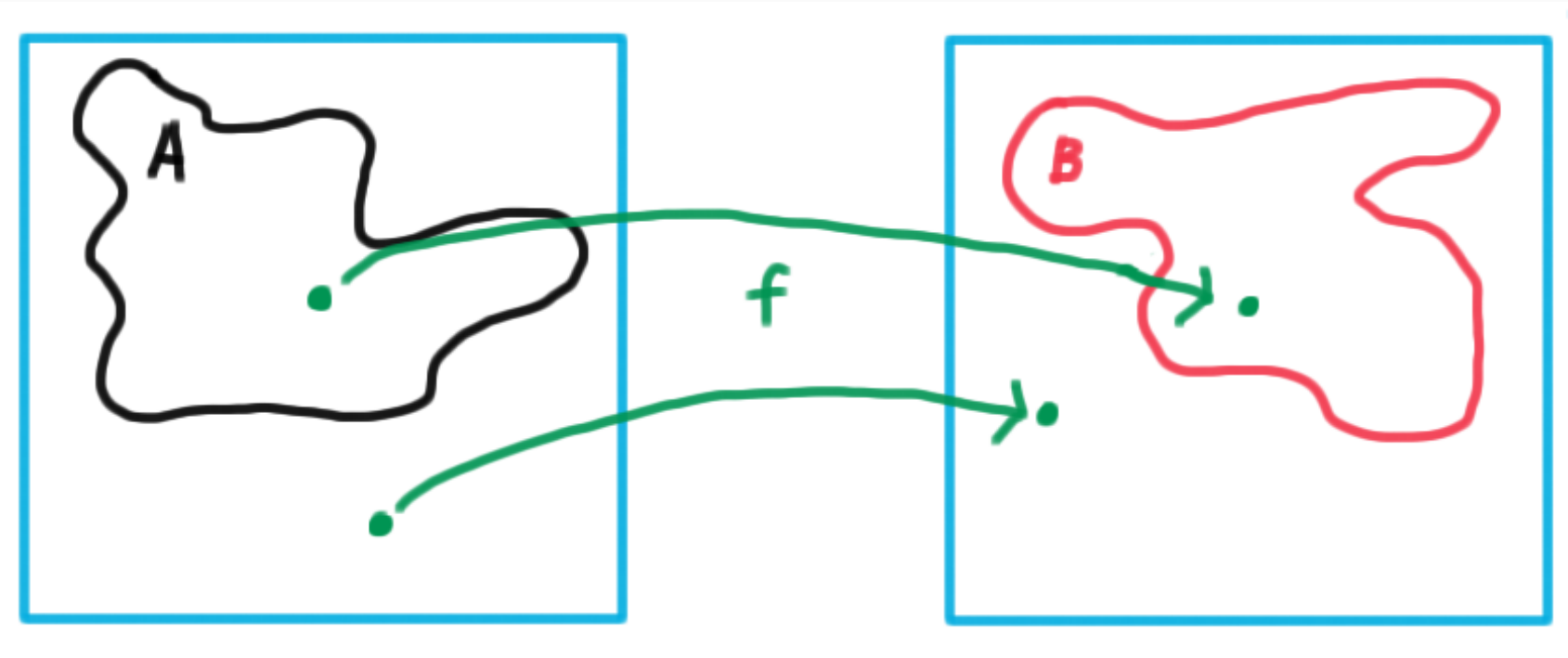
- нехай C — деякий клас складності (деяка множина) мов над алфавітом $\{0,1\}$, r — деяке зведення мов над алфавітом $\{0,1\}$
- клас складності C є **замкненим відносно зведення** r, якщо для довільної мови $L_c \subseteq \{0,1\}^*$ з класу складності C і довільної мови $L_1 \subseteq \{0,1\}^*$ з умови $L_1 \leq_r L_c$ випливає, що $L_1 \in C$
- мова L_1 — **складна для класу складності** C (C-**складна**) **відносно зведення** r, якщо для кожної мови L_c з класу складності C виконується твердження $L_c \leq_r L_1$
- мова L_1— **повна для класу складності** C (C-**повна**) **відносно зведення** r, якщо вона є складною для класу складності C відносно зведення r і належить класу складності C
- $\leq_r (C)$ — множина всіх мов, які зводяться до мов класу складності C за допомогою зведення r

Порівняння зведень

Означення

- нехай C — деякий клас складності (деяка множина) мов над алфавітом $\{0,1\}$, r — деяке зведення мов над алфавітом $\{0,1\}$
- клас складності C є **замкненим відносно зведення** r, якщо для довільної мови $L_c \subseteq \{0,1\}^*$ з класу складності C і довільної мови $L_1 \subseteq \{0,1\}^*$ з умови $L_1 \leq_r L_c$ випливає, що $L_1 \in C$
- мова L_1 — **складна для класу складності** C (C-**складна**) **відносно зведення** r, якщо для кожної мови L_c з класу складності C виконується твердження $L_c \leq_r L_1$
- мова L_1— **повна для класу складності** C (C-**повна**) **відносно зведення** r, якщо вона є складною для класу складності C відносно зведення r і належить класу складності C
- $\leq_r (C)$ — множина всіх мов, які зводяться до мов класу складності C за допомогою зведення r
- $\leq_r (L_1)$ — множина всіх мов, які зводяться до мови L_1 за допомогою зведення r

Види зведень



Функціональне зведення

Означення

- L_1 і L_2 — деякі мови над алфавітом $\{0, 1\}$ і F — множина всюди визначених функцій виду $\{0, 1\}^* \to \{0, 1\}^*$, яка є замкненою відносно операції композиції функцій та містить тотожну функцію

Функціональне зведення

Означення

- L_1 і L_2 — деякі мови над алфавітом $\{0,1\}$ і F — множина всюди визначених функцій виду $\{0,1\}^* \to \{0,1\}^*$, яка є замкненою відносно операції композиції функцій та містить тотожну функцію
- мова L_1 **зводиться за допомогою зведення функціонального типу з множиною функцій** F до мови L_2, якщо існує функція f в множині F (яку називають **функцією зведення**) така, що для довільного слова $x \in \{0,1\}^*$ $x \in L_1$ тоді й тільки тоді, коли $f(x) \in L_2$

Функціональне зведення

Означення

- L_1 і L_2 — деякі мови над алфавітом $\{0,1\}$ і F — множина всюди визначених функцій виду $\{0,1\}^* \to \{0,1\}^*$, яка є замкненою відносно операції композиції функцій та містить тотожну функцію
- мова L_1 **зводиться за допомогою зведення функціонального типу з множиною функцій** F до мови L_2, якщо існує функція f в множині F (яку називають **функцією зведення**) така, що для довільного слова $x \in \{0,1\}^*$ $x \in L_1$ тоді й тільки тоді, коли $f(x) \in L_2$
- мова L_1 — **мова, яка зводиться**

Функціональне зведення

Означення

- L_1 і L_2 — деякі мови над алфавітом $\{0,1\}$ і F — множина всюди визначених функцій виду $\{0,1\}^* \to \{0,1\}^*$, яка є замкненою відносно операції композиції функцій та містить тотожну функцію
- мова L_1 **зводиться за допомогою зведення функціонального типу з множиною функцій** F до мови L_2, якщо існує функція f в множині F (яку називають **функцією зведення**) така, що для довільного слова $x \in \{0,1\}^*$ $x \in L_1$ тоді й тільки тоді, коли $f(x) \in L_2$
- мова L_1 — **мова, яка зводиться**
- мова L_2 — **мова, до якої зводять**

Функціональне зведення

Означення

- L_1 і L_2 — деякі мови над алфавітом $\{0,1\}$ і F — множина всюди визначених функцій виду $\{0,1\}^* \to \{0,1\}^*$, яка є замкненою відносно операції композиції функцій та містить тотожну функцію
- мова L_1 **зводиться за допомогою зведення функціонального типу з множиною функцій** F до мови L_2, якщо існує функція f в множині F (яку називають **функцією зведення**) така, що для довільного слова $x \in \{0,1\}^*$ $x \in L_1$ тоді й тільки тоді, коли $f(x) \in L_2$
- мова L_1 — **мова, яка зводиться**
- мова L_2 — **мова, до якої зводять**
- позначають $L_1 \leq_F L_2$

Функціональне зведення

Означення

- L_1 і L_2 — деякі мови над алфавітом $\{0,1\}$ і F — множина всюди визначених функцій виду $\{0,1\}^* \to \{0,1\}^*$, яка є замкненою відносно операції композиції функцій та містить тотожну функцію
- мова L_1 **зводиться за допомогою зведення функціонального типу з множиною функцій** F до мови L_2, якщо існує функція f в множині F (яку називають **функцією зведення**) така, що для довільного слова $x \in \{0,1\}^*$ $x \in L_1$ тоді й тільки тоді, коли $f(x) \in L_2$
- мова L_1 — **мова, яка зводиться**
- мова L_2 — **мова, до якої зводять**
- позначають $L_1 \leq_F L_2$

$f(L_1) \subseteq L_2$ і $f(\overline{L_1}) \subseteq \overline{L_2}$, f — необов'язково ін'єктивна

Функціональне зведення

Наслідок

Нехай F є множиною функцій деякого зведення функціонального типу. Для довільних мов $L_1, L_2, L_3 \subseteq \{0,1\}$ виконується твердження, що, якщо функція $f \in F$ є функцією зведення мови L_1 до мови L_2, а функція $g \in F$ є функцією зведення мови L_2 до мови L_3, то функція $f \circ g$ є функцією зведення мови L_1 до мови L_3.

Функціональне зведення

Наслідок

Нехай F є множиною функцій деякого зведення функціонального типу. Для довільних мов $L_1, L_2, L_3 \subseteq \{0,1\}$ виконується твердження, що, якщо функція $f \in F$ є функцією зведення мови L_1 до мови L_2, а функція $g \in F$ є функцією зведення мови L_2 до мови L_3, то функція $f \circ g$ є функцією зведення мови L_1 до мови L_3.

Наслідок

Всі зведення функціонального типу є рефлексивними і транзитивними відношеннями на множині мов над алфавітом $\{0,1\}$.

Функціональне зведення

Наслідок

Нехай F є множиною функцій деякого зведення функціонального типу. Для довільних мов $L_1, L_2, L_3 \subseteq \{0,1\}$ виконується твердження, що, якщо функція $f \in F$ є функцією зведення мови L_1 до мови L_2, а функція $g \in F$ є функцією зведення мови L_2 до мови L_3, то функція $f \circ g$ є функцією зведення мови L_1 до мови L_3.

Наслідок

Всі зведення функціонального типу є рефлексивними і транзитивними відношеннями на множині мов над алфавітом $\{0,1\}$.

Теорема

Для довільних мов $L_1, L_2 \subseteq \{0,1\}^*$ і довільної множини F всюди визначених функцій виду $\{0,1\}^* \to \{0,1\}^*$, яка є замкненою відносно операції композиції функцій та містить тотожну функцію, з умови $L_1 \leq_F L_2$ випливає, що $\overline{L_1} \leq_F \overline{L_2}$.

Приклади замкнених множин

Приклад

- множина всіх всюди визначених функцій виду $\{0,1\}^* \to \{0,1\}^*$
- множина всіх обчислювальних всюди визначених функцій виду $\{0,1\}^* \to \{0,1\}^*$
- множина всіх всюди визначених функцій виду $\{0,1\}^* \to \{0,1\}^*$, які обчислюються машинами Тюрінга за поліноміальний час
- множина всіх всюди визначених функцій виду $\{0,1\}^* \to \{0,1\}^*$, які обчислюються машинами Тюрінга за лінійний час

m-зведення

Означення

m-**зведенням** називають зведення функціонального типу відносно множини всіх всюди визначених обчислювальних функцій.
Позначають як $L_1 \leq_m L_2$.

m-зведення

Означення

m-**зведенням** називають зведення функціонального типу відносно множини всіх всюди визначених обчислювальних функцій.
Позначають як $L_1 \leq_m L_2$.

Властивості m-зведення

Для довільних мов $L_1, L_2 \subseteq \{0,1\}^*$, якщо $L_1 \leq_m L_2$ і

- L_2 є вирішуваною мовою, то мова L_1 також є вирішуваною

m-зведення

Означення

m-**зведенням** називають зведення функціонального типу відносно множини всіх всюди визначених обчислювальних функцій.
Позначають як $L_1 \leq_m L_2$.

Властивості m-зведення

Для довільних мов $L_1, L_2 \subseteq \{0,1\}^*$, якщо $L_1 \leq_m L_2$ і

- L_2 є вирішуваною мовою, то мова L_1 також є вирішуваною
- L_1 є невирішуваною мовою, то мова L_2 також є невирішуваною

m-зведення

Означення

m-**зведенням** називають зведення функціонального типу відносно множини всіх всюди визначених обчислювальних функцій. Позначають як $L_1 \leq_m L_2$.

Властивості m-зведення

Для довільних мов $L_1, L_2 \subseteq \{0,1\}^*$, якщо $L_1 \leq_m L_2$ і

- L_2 є вирішуваною мовою, то мова L_1 також є вирішуваною
- L_1 є невирішуваною мовою, то мова L_2 також є невирішуваною
- L_2 є рекурсивно зліченною мовою, то мова L_1 також є рекурсивно зліченною

m-зведення

Означення

m-зведенням називають зведення функціонального типу відносно множини всіх всюди визначених обчислювальних функцій. Позначають як $L_1 \leq_m L_2$.

Властивості m-зведення

Для довільних мов $L_1, L_2 \subseteq \{0,1\}^*$, якщо $L_1 \leq_m L_2$ і

- L_2 є вирішуваною мовою, то мова L_1 також є вирішуваною
- L_1 є невирішуваною мовою, то мова L_2 також є невирішуваною
- L_2 є рекурсивно зліченною мовою, то мова L_1 також є рекурсивно зліченною
- L_2 є корекурсивно зліченною мовою, то мова L_1 також є корекурсивно зліченною

m-зведення

Означення

m-**зведенням** називають зведення функціонального типу відносно множини всіх всюди визначених обчислювальних функцій.
Позначають як $L_1 \leq_m L_2$.

Властивості m-зведення

Для довільних мов $L_1, L_2 \subseteq \{0,1\}^*$, якщо $L_1 \leq_m L_2$ і

- L_2 є вирішуваною мовою, то мова L_1 також є вирішуваною
- L_1 є невирішуваною мовою, то мова L_2 також є невирішуваною
- L_2 є рекурсивно зліченною мовою, то мова L_1 також є рекурсивно зліченною
- L_2 є корекурсивно зліченною мовою, то мова L_1 також є корекурсивно зліченною

Наслідок

Класи складності R, RE та $coRE$ є замкненими відносно m-зведення.

1-зведення

Означення

1-**зведенням** мови $L_1 \subseteq \{0,1\}^*$ до мови $L_2 \subseteq \{0,1\}^*$ називають зведення функціонального типу відносно множини всіх всюди визначених обчислювальних функцій, якщо існує ін'єктивна всюди визначена обчислювальна функція $f\colon \{0,1\}^* \to \{0,1\}^*$ така, що для довільного слова $x \in \{0,1\}^*$ $x \in L_1$ тоді й тільки тоді, коли $f(x) \in L_2$. 1-зведення мови $L_1 \subseteq \{0,1\}^*$ до мови $L_2 \subseteq \{0,1\}^*$ позначають як $L_1 \leq_1 L_2$.

1-зведення

Означення

1-**зведенням** мови $L_1 \subseteq \{0,1\}^*$ до мови $L_2 \subseteq \{0,1\}^*$ називають зведення функціонального типу відносно множини всіх всюди визначених обчислювальних функцій, якщо існує ін'єктивна всюди визначена обчислювальна функція $f\colon \{0,1\}^* \to \{0,1\}^*$ така, що для довільного слова $x \in \{0,1\}^*$ $x \in L_1$ тоді й тільки тоді, коли $f(x) \in L_2$. 1-зведення мови $L_1 \subseteq \{0,1\}^*$ до мови $L_2 \subseteq \{0,1\}^*$ позначають як $L_1 \leq_1 L_2$.

Наслідок

m-зведення є слабкішим за 1-зведення.

Машиною Тюрінга з оракулом

Машиною Тюрінга з оракулом називають абстрактний обчислювальний пристрій, який визначається кортежем $(k, \Gamma, \Sigma, \#, Q, Q_F, q_0, q^O_{query}, q^O_{yes}, q^O_{no}, \delta)$, де

$k \in \mathbb{N}$, $k \geq 3$ — кількість стрічок машини Тюрінга;

Γ — алфавіт машини Тюрінга або алфавіт стрічки;

$\# \in \Gamma$ — порожній символ;

$\Sigma \subseteq \Gamma \setminus \{\#\}$ — вхідний алфавіт;

Q — множина внутрішніх станів;

$Q_F \subseteq Q$ — множина кінцевих внутрішніх станів;

$q_0 \in Q$ — початковий стан;

$q^O_{query} \in Q$ — виділений внутрішній стан запиту до оракулу;

$q^O_{yes} \in Q$, $q^O_{yes} \neq q^O_{query}$, — виділений внутрішній стан відповіді оракула ‘так’;

$q^O_{no} \in Q$, $q^O_{no} \neq q^O_{query}$, $q^O_{no} \neq q^O_{yes}$, — виділений внутрішній стан відповіді оракула ‘ні’;

$\delta\colon Q \setminus (Q_F \cup \{q^O_{query}\}) \times \Gamma^k \nrightarrow Q \times \Gamma^{k-1} \times \{L, S, R\}^k$ — функція переходів.

Зведення за Тюрінгом

Означення

Мова $L_1 \subseteq \{0,1\}^*$ **зводиться за Тюрінгом** до мови $L_2 \subseteq \{0,1\}^*$ (**за час** $T(n)$), якщо існує машина Тюрінга з оракулом, яка вирішує мову L_1 (за час $T(n)$) з використанням мови L_2 як мови оракула, і позначають це як $L_1 \leq_T L_2$.

Зведення за Тюрінгом

Означення

Мова $L_1 \subseteq \{0,1\}^*$ **зводиться за Тюрінгом** до мови $L_2 \subseteq \{0,1\}^*$ (**за час** $T(n)$), якщо існує машина Тюрінга з оракулом, яка вирішує мову L_1 (за час $T(n)$) з використанням мови L_2 як мови оракула, і позначають це як $L_1 \leq_T L_2$.

Твердження

Зведення за Тюрінгом є слабкішим за m-зведення.

tt-зведення

Мова $L_1 \subseteq \{0,1\}^*$ зводиться до мови $L_2 \subseteq \{0,1\}^*$ за допомогою **табличного зведення**, якщо існують обчислювані всюди визначені функції $f_1 \colon \{0,1\}^* \to \mathbb{N}$, $f_2 \colon \{0,1\}^* \to \bigcup\limits_{k \in \mathbb{N}} \left(\{0,1\}^*\right)^k$ та $f_3 \colon \{0,1\}^* \to U$, де U — множина всіх булевих функцій, тобто всіх відображень $\{0,1\}^k \to \{0,1\}$ для всіх чисел $k \in \mathbb{N}$, такі, що для довільного слова $x \in \{0,1\}^*$ $f_3(x) = \varphi(b_1, \ldots, b_{f_1(x)})$, де φ є булевою функцією від $f_1(x)$ булевих змінних виду $\{0,1\}^{f_1(x)} \to \{0,1\}$, а $f_2(x) = (z_1, \ldots, z_{f_1(x)})$, де $z_1, \ldots, z_{f_1(x)} \in \{0,1\}^*$, і $x \in L_1$ тоді й тільки тоді, коли $\varphi(L_2(z_1), \ldots, L_2(z_{f_1(x)})) = 1$. Позначають це через запис $L_1 \leq_{tt} L_2$.

tt-зведення

Мова $L_1 \subseteq \{0,1\}^*$ зводиться до мови $L_2 \subseteq \{0,1\}^*$ за допомогою **табличного зведення**, якщо існують обчислювані всюди визначені функції $f_1\colon \{0,1\}^* \to \mathbb{N}$, $f_2\colon \{0,1\}^* \to \bigcup\limits_{k\in\mathbb{N}} \left(\{0,1\}^*\right)^k$ та $f_3\colon \{0,1\}^* \to U$, де U — множина всіх булевих функцій, тобто всіх відображень $\{0,1\}^k \to \{0,1\}$ для всіх чисел $k \in \mathbb{N}$, такі, що для довільного слова $x \in \{0,1\}^*$ $\quad f_3(x) = \varphi(b_1, \ldots, b_{f_1(x)})$, де φ є булевою функцією від $f_1(x)$ булевих змінних виду $\{0,1\}^{f_1(x)} \to \{0,1\}$, а $f_2(x) = (z_1, \ldots, z_{f_1(x)})$, де $z_1, \ldots, z_{f_1(x)} \in \{0,1\}^*$, і $x \in L_1$ тоді й тільки тоді, коли $\varphi(L_2(z_1), \ldots, L_2(z_{f_1(x)})) = 1$. Позначають це через запис $L_1 \leq_{tt} L_2$.

- функція f_1 — кількість запитів для кожного слова
- функція f_2 — побудова конкретних запитів (слів, щодо яких оракул має відповісти, чи належать вони мові L_2)
- функція f_3 — обробка результатів цих запитів та обчислення результату

Означення

Мова $L_1 \subseteq \{0,1\}^*$ зводиться до мови $L_2 \subseteq \{0,1\}^*$ за допомогою **слабкого табличного зведення**, якщо існують машина Тюрінга M з оракулом L_2 та обчислювані всюди визначені функції $f_1\colon \{0,1\}^* \to \mathbb{N}$ та $f_2\colon \{0,1\}^* \to \bigcup\limits_{k\in\mathbb{N}} \left(\{0,1\}^*\right)^k$ такі, що для довільного вхідного слова $x \in \{0,1\}^*$ машина Тюрінга M з оракулом L_2 зробить точно $f_1(x)$ запитів $(z_1, \ldots, z_{f_1(x)})$ до оракулу, які визначаються значенням $f_2(x) = (z_1, \ldots, z_{f_1(x)})$, де $z_1, \ldots, z_{f_1(x)} \in \{0,1\}^*$, і при цьому машина Тюрінга M з оракулом L_2 вирішує мову L_1. Позначають це через запис $L_1 \leq_{wtt} L_2$.

wtt-зведення

Означення

Мова $L_1 \subseteq \{0,1\}^*$ зводиться до мови $L_2 \subseteq \{0,1\}^*$ за допомогою **слабкого табличного зведення**, якщо існують машина Тюрінга M з оракулом L_2 та обчислювані всюди визначені функції $f_1\colon \{0,1\}^* \to \mathbb{N}$ та $f_2\colon \{0,1\}^* \to \bigcup\limits_{k\in\mathbb{N}} \left(\{0,1\}^*\right)^k$ такі, що для довільного вхідного слова $x \in \{0,1\}^*$ машина Тюрінга M з оракулом L_2 зробить точно $f_1(x)$ запитів $(z_1, \ldots, z_{f_1(x)})$ до оракулу, які визначаються значенням $f_2(x) = (z_1, \ldots, z_{f_1(x)})$, де $z_1, \ldots, z_{f_1(x)} \in \{0,1\}^*$, і при цьому машина Тюрінга M з оракулом L_2 вирішує мову L_1. Позначають це через запис $L_1 \leq_{wtt} L_2$.

- функція f_1 — кількість запитів для кожного слова
- функція f_2 — побудова конкретних запитів (слів, щодо яких оракул має відповісти, чи належать вони мові L_2)
- обробка результатів цих запитів та обчислення результату в машині Тюрінга

wtt-зведення

Твердження

Зведення за Тюрінгом є слабкішим за *wtt*-зведення.

wtt-зведення є слабкішим за *tt*-зведення.

tt-зведення є слабкішим за *m*-зведення.

wtt-зведення

Твердження

Зведення за Тюрінгом є слабкішим за *wtt*-зведення.

wtt-зведення є слабкішим за *tt*-зведення.

tt-зведення є слабкішим за *m*-зведення.

Означення

Мова $L_1 \subseteq \{0,1\}^*$ **обмежено зводиться за Тюрінгом** до мови $L_2 \subseteq \{0,1\}^*$ (**за час** $T(n)$) (або **зводиться за допомогою обмеженого зведення за Тюрінгом**), якщо існують всюди визначена обчислювальна функція $f : \mathbb{N} \to \mathbb{N}$ і машина Тюрінга з оракулом, яка вирішує мову L_1 (за час $T(n)$) з використанням мови L_2 як мови оракула, причому довжина кожного запиту до оракула не перевищує значення $f(|x|)$ для будь-якого вхідного слова $x \in \{0,1\}^*$, і позначають це як $L_1 \leq_{bT} L_2$.

wtt-зведення

Твердження

Зведення за Тюрінгом є слабкішим за *wtt*-зведення.

wtt-зведення є слабкішим за *tt*-зведення.

tt-зведення є слабкішим за *m*-зведення.

Означення

Мова $L_1 \subseteq \{0,1\}^*$ **обмежено зводиться за Тюрінгом** до мови $L_2 \subseteq \{0,1\}^*$ (**за час** $T(n)$) (або **зводиться за допомогою обмеженого зведення за Тюрінгом**), якщо існують всюди визначена обчислювальна функція $f : \mathbb{N} \to \mathbb{N}$ і машина Тюрінга з оракулом, яка вирішує мову L_1 (за час $T(n)$) з використанням мови L_2 як мови оракула, причому довжина кожного запиту до оракула не перевищує значення $f(|x|)$ для будь-якого вхідного слова $x \in \{0,1\}^*$, і позначають це як $L_1 \leq_{bT} L_2$.

Твердження

Обмежене зведення за Тюрінгом є еквівалентним *wtt*-зведенню.

Степені Тюрінга

$L_1, L_2 \subseteq \{0,1\}^*$: $L_1 \leq_1 L_2 \Rightarrow L_1 \leq_m L_2 \Rightarrow L_1 \leq_{tt} L_2 \Rightarrow L_1 \leq_{wtt} L_2 \Rightarrow L_1 \leq_T L_2$

Степені Тюрінга

$L_1, L_2 \subseteq \{0,1\}^*$: $L_1 \leq_1 L_2 \Rightarrow L_1 \leq_m L_2 \Rightarrow L_1 \leq_{tt} L_2 \Rightarrow L_1 \leq_{wtt} L_2 \Rightarrow L_1 \leq_T L_2$

Означення

Класи еквівалентності за зведенням за Тюрінгом називають **степенем Тюрінга** або **степенем нерозв'язності**. Для довільної мови $L_1 \subseteq \{0,1\}^*$ через $[L_1]$ позначають степінь Тюрінга, якому належить мова L_1. Множину всіх степенів Тюрінга позначають як $\mathcal{D}$.

0 — найменший степінь Тюрінга, містить всі вирішувані мови