

Komputery, obliczenia, algorytmy



The Sunway TaihuLight (神威 · 太湖之光)

■ Michał Rad

18.10.2018

Co i po co będziemy robić

- Cele zajęć informatycznych:
 - Alfabetyzacja komputerowa
 - Biegłość komputerowa
 - Myślenie komputacyjne

• Co to jest myślenie komputacyjne?

- Takie sformułowanie problemu, że można posłużyć się w jego rozwiązaniu komputerem
- Problem polega na logicznej organizacji danych
- Problem daje się rozwiązać za pomocą algorytmu
- Projektowanie, analiza i implementacja prowadzi do rozwiązania efektywnego, wykorzystującego możliwości komputera
- Nabyte doświadczenie daje się wykorzystać do rozwiązywanie innych podobnych problemów

Szersze podejście do informatyki - *computing*

- **Computer Engineering** – budowa i konstrukcja sprzętu komputerowego;
- **Information Systems** – tworzenie systemów informacyjnych;
- **Information Technology** – technologia informacyjna, zastosowania informatyki w różnych dziedzinach;
- **Software Engineering** – produkcja oprogramowania;
- **Computer Science** – studia podstawowe, uniwersyteckie studia informatyczne.

Inna definicja informatyki

Informatyka jest dziedziną wiedzy i działalnością zajmującą się algorytmami

Algorytmy? A komputery?

*Informatyka jest w takim sensie nauką
o komputerach,
jak biologia jest nauką o mikroskopach,
a astronomia – nauką o teleskopach.*

Edsger Dijkstra



*(1930 -2002)
algorytm znajdowania najkrótszej drogi
problem ucztujących filozofów*

A więc komputer - narzędziem

Mówi się często, że człowiek dotąd nie zrozumie czegoś, zanim nie nauczy tego – kogoś innego.

W rzeczywistości, człowiek nie zrozumie czegoś naprawdę, zanim nie zdoła nauczyć tego – komputera.

Donald Knuth

*The Art of Computer Programming
TEX
literate programming.*



Czy komputer może wszystko?

Najlepszym sposobem przyspieszania komputerów jest obarczanie ich mniejszą liczbą działań.

Ralph Gomory

IBM

Algorytm jest najważniejszy

- Prosty przykład: podnoszenie do potęgi:
- x^n to $x * x * \dots$ (n mnożeń)

Algorytm – czas potrzebny do realizacji

- Podniesienie x do potęgi zawierającej 35 cyfr zajęło by metodą „zwykłą” $4 \cdot 10^8$ lat na superkomputerze o prędkości 1PFlops (czyli 10^{15} operacji na sekundę)

Lepsze podejście

- A można tak: $x^n = (x^{n/2})^2$
- Wykonywanych jest ok $2 \log_2 n$ mnożeń

$$x^n = \begin{cases} 1 & \text{jeśli } n=0 \\ (x^{(n/2)})^2 & \text{jeśli } n \text{ jest parzyste} \\ (x^{n-1})x & \text{jeśli } n \text{ jest nieparzyste} \end{cases}$$

- Tą metodą podniesienie x do potęgi zawierającej 35 cyfr wymaga 206 mnożeń
- A po co podnosić liczby do takich potęg?
 - algorytm szyfrowania RSA

Co to jest RSA?

- RSA – jeden z pierwszych i obecnie najpopularniejszych asymetrycznych algorytmów kryptograficznych z kluczem publicznym, zaprojektowany w 1977 przez Rona Rivesta, Adi Shamira oraz Leonarda Adlemana.
- Bezpieczeństwo szyfrowania opiera się na trudności faktoryzacji dużych liczb złożonych
- Z algorytmu RSA korzysta narzędzie do szyfrowania poczty i podpisów cyfrowych PGP

Wyjaśnienie

- Algorytm asymetryczny szyfrowania – algorytm z dwoma lub więcej kluczami szyfrowania: publicznym i prywatnym (publiczny koduje, prywatny dekoduje)
- Faktoryzacja – rozkład na czynniki które po wymnożeniu dadzą rozkładana liczbę
- Pretty Good Privacy (PGP) – narzędzie do szyfrowania poczty elektronicznej.

Dygresja

- 1 Flops – to jest jedna operacja zmiennoprzecinkowa na sekundę (**F**loating **o**perations **p**er **s**econd) i jest to miara prędkości komputera
- Przedrostki Giga – 10^9 Tera – 10^{12} , Peta – 10^{15}
- Obecnie najszybsze komputery to:
 - 1) Sunway TaihuLight - Sunway MPP, Sunway SW26010 260C 1.45GHz, 93014.6 Tflops
(National Supercomputing Center in Wuxi) Moc 15371 Kw
 - 2) Tianhe-2 (MilkyWay-2) (chiński uniwersytet obrony)
33862.7 Tflops
 - 3) Piz Daint - Cray XC50 (USA) 19590 Tflops
(<http://www.top500.org/lists>)
- Komputery „domowe” mają wydajność pojedynczych GFlops

A u nas?

- PROMETHEUS 1670.1 Tflops
wg ostatniego rankingu 103 na liście top500
(poprzednio 71)
- ZEUS 266.9 Tflops
wg ostatniego rankingu poza listą



- *Komputery należą do ACK Cyfronet*

Wracając do algorytmu...

```
1 #include <stdio.h>
2
3 long int potega(long int x, long int n)
4     {
5         if (n==1) return x;
6         else return x*potega(x,n-1);
7     }
8
9 main(int argc, char *argv[])
10 {
11     long int x;
12     long int n;
13     x=atoi(argv[1]);
14     n=atoi(argv[2]);
15
16     printf("\n %ld do %ld to %ld \n", x , n, potega(x ,n ));
17
18 }
```

Algorytm „lepszy”

```
1 #include <stdio.h>
2
3 long int potega(long int x, long int n)
4 {
5     if (n==1) return x;
6     if ((n % 2) == 0)
7     {
8         long int p=potega(x, n/2);
9         return p*p;
10    }
11    else
12    {
13        return potega(x, n-1)*x;
14    }
15 }
16
17 main(int argc, char *argv[])
18 {
19     long int x;
20     long int n;
21     x=atoi(argv[1]);
22     n=atoi(argv[2]);
23     printf("\n %ld do %ld to %ld \n", x , n, potega(x ,n ));
24 }
```

$$x^n = \begin{cases} 1 & \text{jeśli } n=0 \\ (x^{(n/2)})^2 & \text{jeśli } n \text{ jest parzyste} \\ (x^{n-1})x & \text{jeśli } n \text{ jest nieparzyste} \end{cases}$$

Czym różnią się te algorytmy?

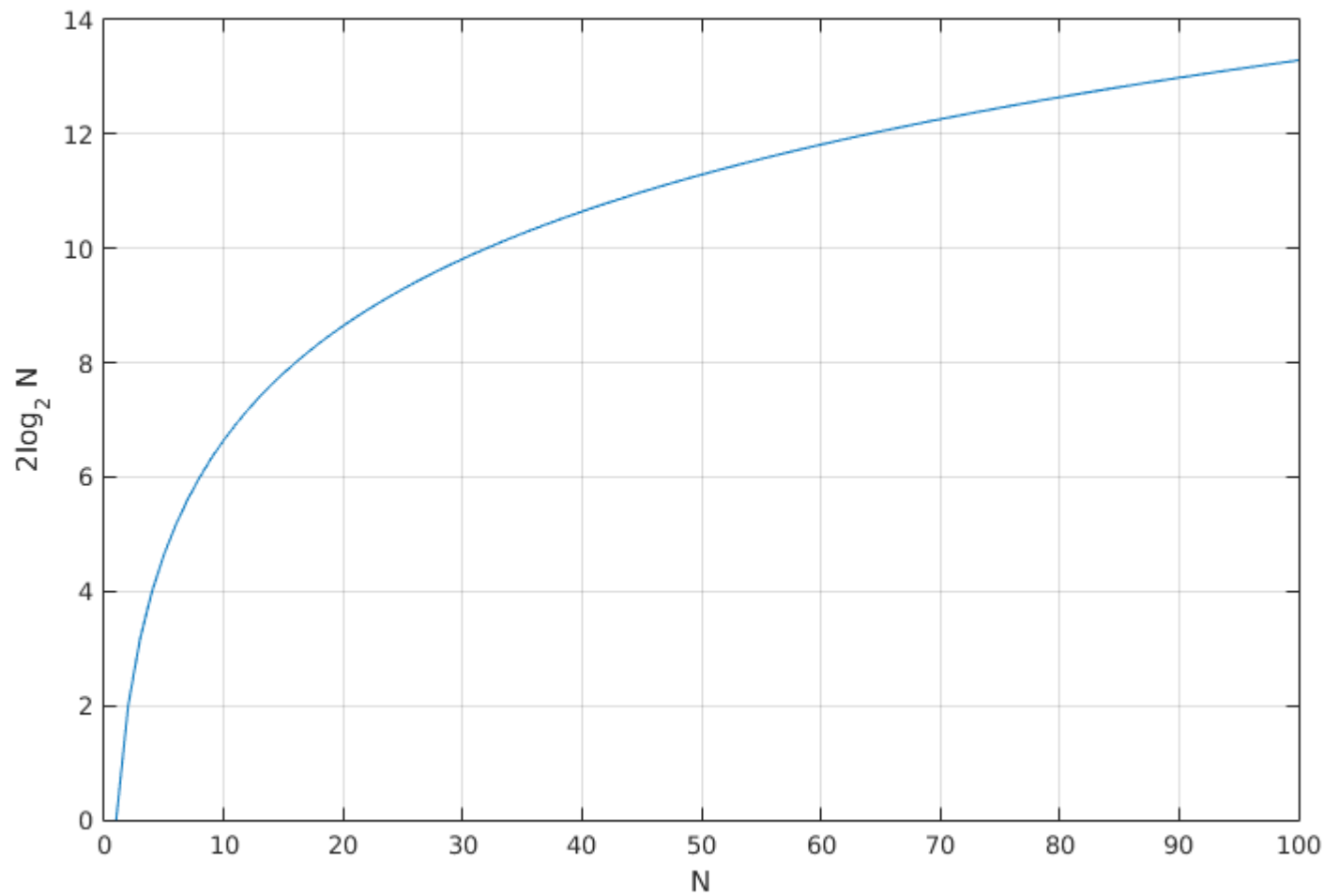
- Różnią się złożonością obliczeniową n oraz $2\log_2 n$

- Co to jest w takim razie złożoność obliczeniowa?

Jest to funkcja określająca ilość zasobów potrzebnych do wykonania danego algorytmu w zależności od rozmiaru danych wejściowych

- zasobami mogą być: czas, pamięć, ilość procesorów

Złożoność obliczeniowa



Ułożmy pierwszy algorytm

- Algorytm obliczania miejsc zerowych wielomianu
- Dane wejściowe a, b, c
- Przepis
- Dane wyjściowe

Algorytm najkrótszej drogi

- Dany jest zbiór węzłów (np. miast) oraz tabela odległości między nimi – należy znaleźć najkrótszą drogę
- Algorytm 'tępy' – sprawdzić wszystkie możliwości. Jeżeli jest n miast to $n!$
- Algorytm Dijkstry – złożoność n^2 (w zależności od implementacji)

Algorytm Dijkstry

■ Opis algorytmu Dijkstry:

Algorytm Dijkstry znajduje najkrótszą drogę z wierzchołka s (zwanego źródłem) do wierzchołka t (zwanego ujściem) w grafie, w którym wszystkim krawędziom nadano nieujemne wagi. Polega na przypisaniu wierzchołkom pewnych wartości liczbowych. Taką liczbę nazwijmy cechą wierzchołka. Cechę wierzchołka v nazwiemy stałą gdy jest równa długości najkrótszej drogi z s do v albo, w przeciwnym przypadku, tymczasową. Na początku wszystkie wierzchołki, oprócz s , otrzymują tymczasowe cechy ∞ (czyli ddl). Źródło s otrzymuje cechę stałą równą 0. Następnie wszystkie wierzchołki połączone krawędzią z wierzchołkiem s otrzymują cechy tymczasowe równe odległości od s . Potem wybierany jest spośród nich wierzchołek o najmniejszej cesze tymczasowej. Oznaczmy go v . Cechę tego wierzchołka zamieniamy na stałą oraz przeglądamy wszystkie wierzchołki połączone z v . Jeśli droga z s do któregoś z nich, przechodząca przez v ma mniejszą długość od tymczasowej cechy tego wierzchołka, to zmniejszamy tą cechę. Ponownie znajdujemy wierzchołek o najmniejszej cesze tymczasowej i zamieniamy cechę tego wierzchołka na stałą. Kontynuujemy to postępowanie aż do momentu zamiany cechy wierzchołka t na stałą (czyli obliczenia długości najkrótszej drogi z s do t).

Algorytm Dijkstry

- Jest to algorytm zachłanny – algorytm, który w celu wyznaczenia rozwiązania w każdym kroku dokonuje zachłannego, tj. najlepiej rokującego w danym momencie wyboru rozwiązania częściowego
- Nie zawsze algorytm zachłanny prowadzi do optymalnego rozwiązania

Problem komiwojażera

- Typowy problem należący do problemów o złożoności obliczeniowej $n!$
- Jest to problem np-trudny (nie ma algorytmu dokładnego o wielomianowej złożoności obliczeniowej)
- Istnieją natomiast algorytmy przybliżone, heurystyczne

***heurystyka** - zbiór reguł oraz wskazówek, które mogą, lecz nie muszą, prowadzić do właściwego rozwiązania.*

Kompresja

- Prawo Parkinsona w odniesieniu do komputerów:

Dane zajmują zwykle całą pamięć możliwą do zapełnienia

- Co w takim razie można zrobić?

Odpowiedzią jest kompresja danych

Na czym polega kompresja?

- Kompresja danych - minimalizowanie ich objętości przez reprezentację w zwartej postaci.
- Na czym może polegać?

Na wykorzystaniu pewnych własności danych – np. zastąpieniu często powtarzających się fragmentów umownym krótszym znakiem

Przykład

- Alfabet Morse'a został tak opracowany aby litery występujące najczęściej w języku Angielskim kodowane były najmniejszą liczbą znaków

Kropka to 1, kreska to 0

i	n	f	o	r	m	a	t	y	k	a
11	01	1101	000	100	00	10	0	0100	010	10

Razem 28 bitów zamiast $11 \cdot 8$ w kodzie ASCII

Kompresja stratna i bezstratna

- Powyższe przykłady to przykłady kompresji bezstratnej – tzn. takiej z której można odtworzyć dokładnie kompresowane dane
- Istnieje także kompresja stratna – wtedy ścisłe odzyskanie danych nie jest możliwe
przykłady JPG, MP3

...

Pojęcia z wykładu

- Flops, Tflops, Pflops,
- Złożoność obliczeniowa, problem np-trudny, algorytm zachłanny, heurystyka
- Kompresja danych stratna, bezstratna

Wykład został opracowany w oparciu między innymi o teksty ze strony <http://www.informatykaplus.edu.pl/>