

SPIS TREŚCI

Przedmowa	7
Spis oznaczeń	8
1. WPROWADZENIE	11
1.1. Algorytm, analiza i projektowanie algorytmów	11
1.2. Złożoność obliczeniowa algorytmu – podstawowe pojęcia	13
1.3. Sposoby opisu algorytmów	19
1.4. Zapisy asymptotyczne	26
1.5. Elementarne struktury danych	33
1.6. Rekurencja i metody projektowania algorytmów	38
1.7. Równania rekurencyjne	46
1.8. Algorytmy probabilistyczne	49
2. ZŁOŻONOŚĆ OBLICZENIOWA I NP-ZUPEŁNOŚĆ	53
2.1. Teoria złożoności obliczeniowej	53
2.2. Problemy obliczeniowe	54
2.3. Problemy decyzyjne	56
2.4. Klasy złożoności	57
2.5. Klasy złożoności algorytmów probabilistycznych	62
3. ALGORYTMY SORTOWANIA	65
3.1. Problem sortowania	65
3.2. Sortowanie bąbelkowe (<i>bubblesort</i>)	72
3.3. Zmodyfikowane sortowanie bąbelkowe (<i>modified bubblesort</i>)	73
3.4. Sortowanie przez wstawianie (<i>insertionsort</i>)	75
3.5. Sortowanie przez selekcję (<i>selectionsort</i>)	81
3.6. Sortowanie przez scalanie (<i>mergesort</i>)	82
3.7. Sortowanie przez kopcowanie (<i>heapsort</i>)	85
3.8. Sortowanie szybkie (<i>quicksort</i>)	96
3.9. Szybkie algorytmy wyznaczania elementu k -tego co do wartości w ciągu	101
3.10. Algorytmy sortowania w czasie liniowym (<i>countsort, radixsort, bucketsort</i>)	105
3.11. Sortowanie zewnętrzne	115
3.12. Sieci sortujące	117

4.	ALGORYTMY WYSZUKIWANIA WZORCA	126
4.1.	Problem wyszukiwania wzorca	126
4.2.	Algorytm „naiwny” wyszukiwania wzorca	131
4.3.	Algorytm Rabina-Karpa	135
4.4.	Algorytm wyszukiwania wzorca wykorzystujący automat skończony	138
4.5.	Algorytm Knutha-Morrisa-Pratta	146
5.	ALGORYTMY GRAFOWE	155
5.1.	Wstęp	155
5.2.	Przeszukiwanie grafu wszerz	160
5.3.	Przeszukiwanie grafu w głąb	167
5.4.	Badanie cykliczności i spójności grafu	174
5.5.	Grafy ważone skierowane. Problem najkrótszej ścieżki	179
5.6.	Problem minimalnych drzew rozpinających w grafach ważonych nieskierowanych ...	191
6.	SŁOWNIKI I OPERACJE NA SIŁOWNIKACH	197
6.1.	Wstęp	197
6.2.	Algorytmy słownikowe o złożoności liniowej	199
6.3.	Algorytmy wykorzystujące słownik liniowo uporządkowany zaimplementowany w tablicach	204
6.4.	Słownik zaimplementowany w drzewie poszukiwań binarnych	210
6.5.	Słownik liniowo uporządkowany zaimplementowany w tablicach indeksowanych kluczami	219
6.6.	Słownik liniowo uporządkowany zaimplementowany w tablicach mieszających	220
7.	ALGORYTMY TEORIOLICZBOWE	231
7.1.	Obliczanie NWD i algorytm Euklidesa	231
7.2.	Rozszerzony algorytm Euklidesa	244
7.3.	Szybkie algorytmy podnoszenia do potęgi modulo m	256
7.4.	Algorytm obliczania odwrotności w pierścieniu liczb całkowitych modulo n	259
7.5.	Zastosowania szybkiego algorytmu podnoszenia do potęgi modulo m – algorytm RSA	262
7.6.	Szybki algorytm obliczania iloczynów potęg	265
7.7.	Algorytm wyszukiwania generatorów grupy multiplikatywnej Z_p^*	267
7.8.	Algorytmy testowania pierwszościami	279
7.9.	Algorytm mnożenia Montgomery’ego	295
7.10.	Algorytm Barretta redukcji modulo	312
7.11.	Chińskie twierdzenie o resztach i algorytmy konwersji z zapisu RNS na naturalny zapis wagowy	316
7.12.	Algorytmy obliczania pierwiastków kwadratowych modulo n	330
	Bibliografia	347