Алгоритмы и модели вычислений.
Задание 10: сортировки

Сергей Володин, 272 гр.

задано 2014.04.17

(каноническое) Задача 41

Модель вычислений: RAM, трудоемкость C — суммарное количество арифметических операций, присваиваний, сравнений.
Мое решение задания 2 $\Rightarrow$

1. $g_n = 2g_{n-1} + g_{n-2}$, $g_0 = 1$, $g_1 = 3$
2. $g_n = \frac{1}{2}\left[(1+\sqrt{2})^{n+1} + (1-\sqrt{2})^{n+1}\right]$

1. (a) Алгоритм:

```
1  number g(number n, number p)
2  {
3    number a = 1;
4    number b = 3;
5
6    if(n == 0) return(a);
7    if(n == 1) return(b);
8
9    number i, bt;
10   for(i = 2; i <= n; i++)
11   {
12     bt = 2 * b + a;
13     a = b;
14     b = bt;
15   }
16
17   return(b);
18 }
```

   (b) Корректность
      i. $g_0 = 1 = g(0)$ (строка 6)
      ii. $g_1 = 3 = g(1)$ (строка 7)
      iii. $n \geqslant 2$:
         A. $P_i = $ [после i-й итерации цикла $a = g_{i-1}$, $b = g_i$]. i-я итерация цикла — при таком значении переменной i.
         B. P_1 (до цикла) верно: (строки 3, 4): $a = g_{1-1} = 1$, $b = g_1 = 3$.
         C. Пусть P_k. Тогда $a \equiv a_{\text{old}} = g_{k-1}$, $b \equiv b_{\text{old}} = g_k$ после k-й итерации. После следующей $(k+1)$ итерации $a = b_{\text{old}} = g_k$, $b = 2b_{\text{old}} + a_{\text{old}} = 2g_k + g_{k-1} \overset{1}{=} g_{k+1}$ $\blacksquare$ $\forall k \geqslant 2 \hookrightarrow P(k)$
         D. В конце (после n-й итерации) $P(n) \Rightarrow b = g_n$ $\blacksquare$ $\forall n \geqslant 2 \hookrightarrow g(n) = g_n$ (строка 17)

   (c) Время работы. При $n \in \{0, 1\}$ $C(0) = 3$, $C(1) = 4$. На каждой итерации цикла трудоемкость константная $c = 8$, поэтому общее количество арифметических операций

$$C(n) = \begin{cases} 3, & n = 0 \\ 4, & n = 1 \\ 5 + 8(n-1), & n \geqslant 2 \end{cases}$$

   (d) Вычисление по модулю: вычислим $g(n)$, вычислим $g(n) \mod p$. Добавляется одна единица трудоемкости.
   (e) Асимптотика $C(n) = O(n)$
   (f) Трудоемкость вычисления $A = g_{10000} \mod 19$: $C(10000) = 5 + 8(9999) = 79997$

2. (a) Фиксируем $p \in \mathbb{N}$. Рассмотрим функцию $f\colon \mathbb{N} \to \overline{0, p-1}^2$: $f(k) = (g_{k-1} \mod p, g_k \mod p)$. Область определения $|D_f| = \infty$, множество значений $|E_f| = p^2$, откуда $|E_f| < |D_f|$, получаем, что f — не инъективна, то есть, $\exists \mathbb{N} \ni i \neq j \in \mathbb{N}\colon f(i) = f(j) \Leftrightarrow (g_{i-1} \mod p, g_i \mod p) = (g_{j-1} \mod p, g_j \mod p)$

(b) Фиксируем эти $i \neq j$: $f(i) = f(j)$. $P(t) \overset{\text{def}}{=} [f(i+t) = f(j+t)]$. $P(0)$ выполнено. Пусть $P(t)$. Тогда $f(i+t) = f(j+t) \Leftrightarrow \begin{cases} g_{i+t-1} = g_{j+t-1} \mod p \\ g_{i+t} = g_{j+t} \mod p \end{cases}$. Тогда $g_{i+t+1} \overset{1}{=} 2g_{i+t} + g_{i+t-1} \overset{P(t)}{=} 2g_{j+t} + g_{j+t-1} \overset{1}{=} g_{j+t+1}$, откуда $f(i+t+1) = f(j+t+1)$ (второе условие из $P(t)$). Значит, $P(t+1)$. По индукции $\forall t \in \mathbb{N} \cup \{0\} \hookrightarrow P(t) \Rightarrow \forall t \in \mathbb{N} \cup \{-1, 0\} \hookrightarrow g_{i+t} = g_{j+t}$

(c) То есть, последовательности $\{g_n\}_{n=i-1}^{\infty} = \{g_n\}_{n=j-1}^{\infty}$, откуда следует, что $\{g_n \mod p\}_{n=0}^{\infty}$ — периодическая с периодом $|i-j|$, начиная с $\min(i-1, j-1)$. Используя рекуррентность «в обратную сторону» получаем, что она периодическая с начала (с $n = 0$).

(d) Оценим период $|i-j|$. $|E_f| = p^2$, откуда $|i-j| \leqslant p^2$. Пусть иначе: $|i-j| \geqslant p^2 + 1$. Без ограничения общности, $i < j$. Тогда $f(i), f(i+1), ..., f(j-1)$ — все различны. Их количество $j - i \geqslant p^2 + 1$, и они из E_f — противоречие, $|E_f| = p^2$.

(e) Для $p = 19$: $|i-j| \leqslant 19^2 = 361$.

(f) Алгоритм: вычисляем период: храним $f(1)$, сравниваем $f(i)$ с $f(1)$. Вычисляем g_i через рекуррентность (см. выше). Ищем место от начала периода для n и выдаем ответ. Сложность $O(p^2)$ (величина периода). Для A: $p^2 = 361$, откуда $C \leqslant 2 \times (\underbrace{5 + 8(361-1)}_{\text{период}}) = 5770$ (2 — т.к. в два прохода, сначала поиск периода, потом вычисление A).

3. $p = 23$. $x = 5$: $x^2 = 25 \equiv 2 \mod p$. Используем 2: $g_n \mod p = \frac{(1+\sqrt{2})^{n+1} + (1-\sqrt{2})^{n+1}}{2} \mod p = 2^{-1}((1+x)^{n+1} + (1-x)^{n+1})$