プログラミング第一

10 月 2 日

今週の目標

- Scala のビルドツール sbt と ScalaTest を用いた単体テストができるようになる。

今日の課題 (提出締切は今週金曜日 23 時 59 分 59 秒)

1. フィボナッチ数を計算する複数のプログラムの作成とそれらを利用したテストをする。

今日のワークフロー

1. GitHub 上の `prg1-2018/assignment1` を fork する。
2. GitHub 上の **自分のアカウント名**`/assignment1` を clone してフィボナッチ数についての課題を終わらせる。
3. GitHub 上の **自分のアカウント名**`/assignment1` に push する。
4. GitHub 上の `prg1-2018/assignment1` に Pull request を送る (次回から課題の提出方法に関するワークフローは書きません)。

1 フィボナッチ数を計算するアルゴリズムとテスト

1.1 概要

プログラムを書くときにまず「効率は悪いけれども確実に正しく動作する実装」をまず書いてから「正しく動作するか少し不安だけど効率がよい実装」を書くことがあるかと思います。今回はフィボナッチ数を例に前者の実装を用いて後者の実装を sbt と ScalaTest を使ってテストしてみましょう。ここでは非負の n について、n 番目のフィボナッチ数 $\mathsf{fib}(n)$ を

$$\begin{aligned}\mathsf{fib}(0) &= 0\\ \mathsf{fib}(1) &= 1\\ \mathsf{fib}(n) &= \mathsf{fib}(n-1) + \mathsf{fib}(n-2), \qquad \text{for } n \geq 2\end{aligned}$$

と定義します。

1.2 効率は悪いが確実に正しく動作するアルゴリズム

フィボナッチ数の定義をそのままプログラムにしてしまえば確実に正しく動きます。

```
def fib_rec(n: Int): BigInt = n match {
  case 0 | 1 => n
  case _ => fib_rec(n-1) + fib_rec(n-2)
}
```

ここで `BigInt` は任意精度整数の型です (n 番目のフィボナッチ数は n に比べて指数関数的に大きいので単に `Int` としてしまうと $n = 48$ で桁溢れします)。

1.3 効率はまあまあよいが正しく動作するかちょっと不安なアルゴリズム

反復を使った $O(n)$ 回の整数の加算演算で n 番目のフィボナッチ数を計算するプログラムです。

Algorithm 1 n 番目のフィボナッチ数を計算するアルゴリズム

```
m ← n
a ← 1
b ← 0
while m ≥ 1 do
    (a, b) ← (a + b, a)
    m ← m − 1
end while
return b
```

1.4 効率はかなりよいが正しく動作するか結構不安なアルゴリズム

一般に

$$\begin{bmatrix} \mathsf{fib}(n+1) \\ \mathsf{fib}(n) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \mathsf{fib}(n) \\ \mathsf{fib}(n-1) \end{bmatrix}$$

という関係が $n \geq 1$ について成り立ちます。よって

$$\begin{bmatrix} \mathsf{fib}(n+1) \\ \mathsf{fib}(n) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

が成り立ちます。行列 $A := \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ とおきます。A^n を効率よく計算するためにはどのようにすればよいでしょうか。もしも n が 2 の冪であれば $A^2 = A \times A$, $A^4 = A^2 \times A^2$, $A^8 = A^4 \times A^4$, ... と計算していけば $\log_2 n$ 回の行列積の計算で A^n が計算できます。一般の n については

$$A^n = \begin{cases} A(A^2)^{(n-1)/2}, & \text{if } n \text{ is odd} \\ (A^2)^{n/2}, & \text{if } n \text{ is even} \end{cases}$$

という関係を用いればアルゴリズム 2が得られます。

Algorithm 2 $\mathsf{pow}(A, n)$: A^n を計算するアルゴリズム $(n \geq 0)$

```
if n = 0 then
    return I
else if n is odd then
    return A × pow(A^2, (n − 1)/2)
else
    return pow(A^2, n/2)
end if
```

このアルゴリズムは反復回数が $\lfloor \log_2 n \rfloor + 1$ なので高々 $2(\lfloor \log_2 n \rfloor + 1)$ 回の行列積の計算で A^n が計算できます。このアルゴリズムを用いれば $O(\log n)$ 回の整数演算で n 番目のフィボナッチ数が計算できます。

2 課題

まずフィボナッチ数の計算について定義通りの実装を除く残り 2 つの実装を Scala で書いてください。また、$O(\log n)$ 回の整数演算のプログラムを書くときには汎用的な pow は書く必要はなく、フィボナッチ数が計算できればよいです。そして定義通りの実装を使って $O(n)$ 回の整数演算をする実装をテストしてください。定義通りの実装はとても遅いのであまり大きい n では計算が終わりません。

次に $O(n)$ 回の整数演算をする実装を使って $O(\log n)$ 回の整数演算をする実装をテストしてください。この場合は $n = 100$ でもすぐに計算が終わります。この二段階のテストが上手くいったら自信を持って $O(\log n)$ 回の整数演算をする実装を利用することができます。

余談: ユークリッドの互除法とフィボナッチ数

ユークリッドの互除法は次のプログラムで表わされるアルゴリズムです (簡単のため引数が非負であることは仮定しています)。

```
def gcd(x: Int, y: Int): Int = {
  if(x == 0) y
  else gcd(y % x, x)
}
```

ユークリッドの互除法は「ユークリッド原論」に記されており、最古の非自明なアルゴリズムと考えられています。このアルゴリズムの反復回数 (gcd が呼ばれる回数) を見積ってみましょう。

定理 1. 非負整数のペア (x, y) が $y > x$ 満たすとき、ユークリッドの互除法で gcd(x, y) を計算したときに反復回数が n であるならば $y \geq \mathsf{fib}(n+1)$, $x \geq \mathsf{fib}(n)$ である。

証明. 帰納法により示す。$n = 0$ のとき、明らかに成り立つ。$n \leq k$ について、定理が成立していると仮定する。$n = k + 1$ のとき、gcd(y%x, x) は k 回の反復で計算ができるので、帰納法の仮定により $x \geq \mathsf{fib}(k+1)$, $y\%x \geq \mathsf{fib}(k)$ が成り立つ。また、$y \geq x + y\%x \geq \mathsf{fib}(k+1) + \mathsf{fib}(k) = \mathsf{fib}(k+2)$ が成り立つ。 □

余談: べき乗に必要な最小の演算回数について

アルゴリズム 2は行列のべき乗に限らず任意のモノイドにおけるべき乗の計算に適用できます (モノイドとは結合法則を満たす 2 項演算 $\times$ と単位元を持つ集合のことです)。このアルゴリズムは $\lfloor \log_2 n \rfloor + \mathsf{popcount}(n) - 1$ 回のモノイドの演算 $\times$ で $A^n := \underbrace{A \times A \times \cdots \times A}_{n個}$ を計算します。ここで $\mathsf{popcount}(n)$ は n の二進数表現に含まれる 1 の数です。しかしこれは必ずしも最小の演算回数ではありません。例えば A^{15} の計算を考えてみましょう。アルゴリズム 2では 6 回の演算をします (A^2, A^4, A^8 を計算するのに 3 回、$A \times A^2 \times A^4 \times A^8$ を計算するのに 3 回)。しかし一方で $C = A^3$ を 2 回の演算で計算してから C^5 を 3 回の演算で計算すれば 5 回ですみます。関数 $l(n)$ を「A^n を計算するのに必要な最小の演算回数」と定義します。この関数 $l(n)$ は入力サイズ $\lfloor \log_2 n \rfloor + 1$ に関して多項式時間で計算できるのでしょうか？そのようなアルゴリズムは未だ知られていません。また直感に反する事実として $l(2n) = l(n)$ となるような n の存在が知られています。A^{2n} は A^n を二乗すればよいので $l(2n) = l(n) + 1$ となるような気がするのですがそれは一般には正しくないのです。しかもそれどころか $l(2n) = l(n) - 1$ となる n が存在します。例えば $n = 375494703$ のときです。これを実際にプログラムで確認できたらすごいです。$l(n)$ を計算するプログラムを書いてみるのはいい腕試しになります ($l(2n) = l(n)$ となるような n は見つけられます)。

他にも類似の問題として割り算も使える (例えば $A^7 = A^8/A$ と計算できる) としたときの最小演算回数 ($\times$ も / も 1 回と数える) を考えるのも面白いです。実用的には群 (全ての元が逆元を持つモノイド。a の逆元 a^{-1} は $a \times a^{-1} = a^{-1} \times a = e$ を満す元。ここで e は単位元) において逆元の計算が群演算 $\times$ に比べてずっと効率的な場合、そのような群の上でべき乗を効率的に計算するのに役に立ちます。上記のような性質を持つ群の具体例としては、暗号でよく利用されている楕円曲線上の群があります。