Cookbook

Chao Xu

Last update: December 2, 2011

Contents

Chapter 1

Algebraic Algorithms

1.1 Exponentiation by squaring

Problem 1.1.1. yy

Input
Given the operator $\cdot$, element a and positive integer n. Where a is an element of a semigroup under $\cdot$.

Output
Find a^n, where $a^n = a \cdot a^{n-1}$.

The general method to solve the problem is exponentiation by squaring. It is originally used for integer exponentiation, but any associate operator can be used in it's place. Here is a theorem stated in algebraic flavor.

Theorem 1.1.1. *For any semigroup $(S, \cdot)$, $x \in S$ and $n \in \mathbb{N}$, x^n can be computed with $O(\log n)$ applications of $\cdot$.*

Proof. Express n as binary $c_k c_{k-1} \dots c_0$, where $c_i \in \{0, 1\}$. We make sure $0 \cdot a$ is the treated as the identity, and $1 \cdot a = a$ for all a. The following observations are crucial.

$$\begin{aligned} a^n &= c_0 a^{2^0} \cdot c_1 a^{2^1} \cdot \ldots \cdot c_k a^{2^k} \\ a^{2^{i+1}} &= a^{2^i} \cdot a^{2^i} \end{aligned}$$

The code that compute a^n from the above two equalities.

```
import Data.Digits
exponentiationBySquaring :: Integral a ⇒ (b → b → b) → b → a → b
exponentiationBySquaring op a n = foldr1 op $ [y | (x, y) ← (zip binary twoPow), x ≢ 0]
  where twoPow = a : zipWith op twoPow twoPow
    binary = digitsRev 2 n
```

One can analyze the number of times the operator is used. The *twoPow* is the infinite list $[a, a^2, \dots, a^{2^i}, \dots]$. It takes k operations to generate the first $k + 1$ elements. At most k additional operations are required to combine the result with the operator. Therefore the operator is used $O(\log n)$ times. □

This result can of course be extended to monoid and groups, so it work for all non-negative and integer exponents, respectively.

1.2 Linear homogeneous recurrence relations with constant coefficients

Definition 1.2.1 (Linear homogeneous recurrence relations with constant coefficients)**.** A linear homogeneous recurrence relations in ring R with constant coefficients of order k is a sequence with the following recursive relation

$$a_n = \sum_{i=1}^{k} c_i a_{n-i}$$

, where c_i are constants.

We use linear recurrence relation to abbreviate.

The most common example is the Fibonacci sequence. $F_0 = 0, F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ in the ring $\mathbb{Z}$. The Fibonacci sequence have a simple implementation. $fibs = 0 : 1 : zipWith\ (+)\ fibs\ (tail\ fibs)$. We want to generalize it.

1.2.1 Lazy sequence

Problem 1.2.1.

Input

1. A list of coefficients $[c_1, c_2, \ldots, c_n]$ of a linear recurrence relation.
2. A list of base cases $[a_0, a_1, \ldots, a_{n-1}]$ of a linear recurrence relation.

Output
The sequence of values of the linear recurrence relation as a infinite list $[a_0, a_1, \ldots$.

Here is a specific implementation where we are working in the ring $\mathbb{Z}$.

```
import Data.List
linearRecurrence :: Integral a ⇒ [a] → [a] → [a]
linearRecurrence coef base = a
  where a = base ++ map (sum ∘ (zipWith (∗) coef)) (map (take n) (tails a))
    n = (length coef)
```

One can generalize it easily to any ring.

Having a infinite list allows simple manipulations. However, finding the nth element in the sequence cost $O(nk)$ time. It becomes unreasonable if a person only need to know the nth element.

1.2.2 Determine nth element in the index

If n is very large, a more common technique would be solve for a_n using matrix multiplication.

1.2.3 Linear Recurrence in Finite Ring

Linear recurrence is perodic in finite rings. Therefore one might want to produce only the periodic part of the ring. [INSERT MORE ON THIS SUBJECT]

1.3 A particular kind of recurrence

A common recurrence has the form

$$a_n = \sum_{i=0}^{\infty} b_i a_{n-m_i}$$

, where m_i and b_i are both *infinite* sequences. $m_i \in \mathbb{N}$. $a_{-i} = 0$ for all positive i. This is well defined as long as b_i, a_i are in the same ring.

Problem 1.3.1.

Input
Infinite sequence b_i and m_i, $m_i \in \mathbb{N}$. Finite sequence $c_0, \ldots, c_k$

Output
The infinite sequence defined as

$$a_n = \begin{cases} \sum_{i=0}^{\infty} b_i a_{n-m_i} & \text{if } n > k \\ c_n & \text{if } n \leqslant k \end{cases}$$

One can use a balanced binary tree to store the entire infinite list, and the time to generate the nth element is $O(d(n) \log n)$, where d is the density function of $\{m_i\}$.

Using an array would make it $O(d(n))$, but it is too imperative for our taste, how about we only use list and achieve $O(d(n))$ time, elegantly?

```
import Data.List
rec :: Num a ⇒ [a] → [a] → [Int] → [a]
rec c b m = a
  where a = c ++ rest
    rest = next [] 0 m
    next xs k (m : ms)
      | k ≡ m = next (a : xs) k ms
      | otherwise = val ++ next (map tail xs) (k + 1) (m : ms)
      where val = if (k < length c) then [] else [sum $ zipWith (∗) (reverse (map head xs)) b]
```

It's important to note the base case doesn't have to be a consective set of integers. It is better to feed a set of base cases as pairs instead.

Chapter 2

Combinatorial Algorithms

2.1 Integer Partitions

Definition 2.1.1 (Integer Partition)**.** A integer partition of n is a multiset $\{a_1, \ldots, a_k\}$, such that $\sum_{i=1}^{k} a_i = n$.

Definition 2.1.2 (Partition Numbers)**.** The sequence of partition numbers $\{p(n)\}$ is the number of integer partitions for n.

Problem 2.1.1.

Input
Integer n.

Output
List of partitions of n.

To find all possible partition of a integer, we proceed with a simple recursive formula.

Let $p(n, k)$ be the list of ways to partition integer n using integers less or equal to k. $p(n, n)$ is the solution to our problem. It is implemented as *part* in the code.

```
integerPartitions :: Integral a ⇒ a → [a]
integerPartitions n = part n n
  where part 0 _ = [[]]
    part n k = [(i : is) | i ← [1 .. min k n], is ← part (n − i) i]
```

Problem 2.1.2.

Input
None

Output
The infinite list of partition numbers.

Naively, `0 : map (length ∘ integerPartitions) [1 ..]` works well, except the time complexity is $O(np(n))$, and $p(n)$ is exponential. A more well known approach, that only cost $\sqrt{n}$ additional to generate the nth number, will be given instead.

First, extend the definition of the partition number, such that $p(0) = 1$ and $p(-n) = 0$ for all positive integer n. The partition number $p(n)$ has the relation

$$p(n) = \sum_{k=0}^{\infty} (-1)^k (p(n - p_{2k+1}) + p(n - p_{2k+2}))$$

where p_n is the sequence of generalized pentagonal number.

We have already developed the tools to work with this kind of recurrence in section .

```
integers :: [Integer]
integers = (0:) $ concat $ zipWith (λx y.[x, y]) [1..] (map negate [1..])
generalizedPentagonalNumbers :: [Integer]
generalizedPentagonalNumbers = [(3 * n ↑ 2 − n) `div` 2 | n ← integers]
partitionNumbers :: [Integer]
partitionNumbers = rec [1] (cycle [1, 1, −1, −1]) (tail generalizedPentagonalNumbers)
```

2.2 Find the primitive word in a free monoid

Problem 2.2.1.

Input
A word w in a free monid.

Output
A primitive word p, such that $p^n = w$ for some integer n.

A word p is primitive if $p = w^k$ implies $k = 1$. This will use the algorithm in [1]. [Nah, just KMP...]

2.3 Period of a eventually periodic sequence

Problem 2.3.1.

Input
1. A integer of the upper bound u of the period. 2. A infinite list that represent a eventually periodic sequence, such that if two finite sequence of length u are equal and the starting index is less than u apart, then they must be inside the periodic part of the sequence.

Output
A pair of the initial sequence and the periodic part.

The naive algorithm, for each finite sequence of length u, see if the second condition in the input holds, does pretty well if u is small. In fact $O(nu^2)$ where n is the length of the aperiodic part.

```
import Data.List
import Data.Maybe
eventuallyPeriodic :: Eq a ⇒ [a] → Int → ([a], [a])
eventuallyPeriodic sequence bound = (ini, take period rep)
  where table = map (take (bound + 1)) (tails (map (take bound) (tails sequence)))
    exist      = map (λx. elemIndex (head x) (tail x)) table
    period     = 1 + (fromJust $ head just)
    (no, just) = span isNothing exist
    (ini, rep) = splitAt (length no) sequence
```

Of course it can be improved to $O(nu)$ easily by using a smarter string search algorithm. Or even better, $O(n)$.[Implement them later]

A variation of the problem could be the upper bound for length of the non-periodic part of the sequence is known.

Bibliography

[1] Artur Czumaj and Leszek Gasieniec. On the complexity of determining the period of a string, 2000.