Assignment 3

CS 487/687 – CM 730
due MONDAY, March 12, 5pm
February 24, 2018

Submission by email to cs487@student.cs.uwaterloo.ca

1. (6 marks) Give the steps of the XGCD algorithm with inputs $A_0 = 3 + x - x^2 + x^3$ and $A_1 = 1 - x + x^2$.

2. (6 marks) Consider the sequence $(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots)$. Using the XGCD algorithm, find a linear recurrence of order 2, with constant coefficients, that is satisfied by this sequence.

3. (12 marks) Define $\psi = 1 + \sqrt{7}$.
   - Find a polynomial $P$ of degree 2 with rational coefficients such that $P(\psi) = 0$
   - Use Euclidean division and XGCD computation to express $\psi/(2\psi + 1)$ as $a_0 + a_1 \psi$,
     with $a_0, a_1$ rational numbers.
   - More generally, how could you rewrite an expression such as
     $$e_0 + e_1 \psi + \cdots + e_{d-1} \psi^{d-1}$$
     $$f_0 + f_1 \psi + \cdots + f_{d-1} \psi^{d-1},$$
     where all $e_i$ and $f_i$ are rationals? Using the results given for the complexity of Euclidean division and XGCD computation, give the complexity of finding the simplified form (in terms of $d$), assuming that the denominator does not vanish.

4. (18 marks) Remember that the Fibonacci numbers are defined by
   $$f_0 = 0, \quad f_1 = 1, \quad f_{n+2} - f_{n+1} - f_n = 0.$$
   We will admit that $f_n \simeq 0.447 \cdot 1.61^n$ for $n \to \infty$.
   (a) Compute $f_0, f_1, f_2, f_3, f_4, f_5, f_6$. 

1
(b) Consider the algorithm
\[ \text{fib}(n) \]
- if \( n = 0 \) then return 0
- if \( n = 1 \) then return 1
- return \( \text{fib}(n - 2) + \text{fib}(n - 1) \)

Let \( F_n \) be the number of operations in \( \mathbb{Q} \) done in this algorithm (there are only additions, actually). “If” and “return” are free. Show that
\[
F_0 = 0, \ F_1 = 0, \ F_2 = 1, \ F_3 = 2, \ F_4 = 4, \ F_5 = 7
\]
and that the sequence \( (F_n) \) satisfies the recurrence
\[
F_n - F_{n-1} - F_{n-2} = 1 \quad (1)
\]
for \( n = 2, 3, 4, \ldots \).

(c) By comparing these values to the Fibonacci numbers, guess and prove a relation between the sequences \( (F_n) \) and \( (f_n) \). Deduce that the running time of \text{fib} is exponential in \( n \).

\textit{The goal of this problem is to show how to derive this result without guessing anything.}

(d) Prove that
\[
x^2 + x^3 + x^4 + x^5 + \cdots = \frac{x^2}{1 - x}.
\]

(e) Let \( S \) be the generating series
\[
S = F_0 + F_1 x + F_2 x^2 + \cdots = \sum_{n \geq 0} F_n x^n.
\]

Using the same kind of summation as we did in class, show that
\[
S = \frac{x^2}{(1 - x)(1 - x - x^2)}.
\]

(f) Rewrite \( S \) as
\[
S = \frac{a}{1 - x} + \frac{b}{1 - x - x^2},
\]
for some constants \( a, b \) in \( \mathbb{Q} \). Explain how you found \( a \) and \( b \) (using an XGCD calculation would be a good idea).

(g) Use the latter expression to recover the relation between the sequences \( (F_n) \) and \( (f_n) \).
5. (10 marks) Given points $a_1, \ldots, a_n$ and values $v_1, \ldots, v_n$, with $a_i \neq a_j$ for $i \neq j$, we want to find a rational function $P = \frac{N}{D}$, with $\deg(N) < n/2$ and $\deg(D) = n/2$ such that $P(a_i) = v_i$ for all $i$.

Suppose that we know a polynomial $Q(x)$ of degree less than $n$ such that $Q(a_i) = v_i$ for all $i$. Let also $M = (x - a_1) \cdots (x - a_n)$. Using the same idea as for the rational function reconstruction seen in class, explain how you could solve your problem by applying the XGCD algorithm to $Q$ and $M$.

I’m not asking for a detailed proof, but for the idea of the algorithm, and an informal justification of why it should work.

6. (2 marks) How much time did you spend on the assignment?