Laboratorio di Programmazione a.a. 2020-21

Problema 9

14 / 17 Dicembre 2020

Descrizione – Parte I

Per *"Cifrario di Cesare"* oggi si intende una semplice regola crittografica di sostituzione che "ruota" ciascuna lettera del testo in chiaro di un numero prefissato di posizioni nell'ordine alfabetico. L'entità della rotazione, detta anche *"chiave"* di decodifica, è concordata fra il mittente e il destinatario del messaggio. Stando ai resoconti di Svetonio, Giulio Cesare avrebbe utilizzato questo rudimentale sistema di crittazione con chiave 3. Per esempio, tenuto conto che le lettere dell'alfabeto Latino dell'epoca erano: A B C D E F G H I L M N O P Q R S T V X , La frase

ALEA IACTA EST IVLIVS CAESAR DIXIT

sarebbe stata trasformata nel messaggio cifrato

DOHD NDFAD HXA NBONBX FDHXDV GNCNA

A differenza del testo riportato sopra in una forma che ne facilita la lettura, il messaggio crittato non contiene spazi bianchi per separare le parole, ma è costituito da una sequenza ininterrotta di lettere. Basandoti sul modello sviluppato a lezione, definisci una procedura *con valori procedurali* che, data una chiave compresa nell'intervallo [0, 19], restituisce la corrispondente funzione di crittazione, da lettera maiuscola a lettera maiuscola, per l'alfabeto Latino dell'epoca Repubblicana. (Suggerimento: l'alfabeto Latino può essere codificato tramite una stringa oppure una lista di caratteri.)

Descrizione – Parte II

Le operazioni di addizione (*add*), moltiplicazione (*mul*), elevamento a potenza (*pow*) nel dominio dei numeri naturali possono essere definite una dall'altra in modo induttivo, a partire dalla funzione successore (*succ*):

$$add(\, m,\, 0\,) = m$$
$$add(\, m,\, n\,) = succ(\, add(m,n-1)\,) \qquad per\ \ n > 0$$

$$mul(\, m,\, 0\,) = 0$$
$$mul(\, m,\, n\,) = add(\, m,\, mul(m,n-1)\,) \qquad per\ \ n > 0$$

$$pow(\, m,\, 0\,) = 1$$
$$pow(\, m,\, n\,) = mul(\, m,\, pow(m,n-1)\,) \qquad per\ \ n > 0$$

Se si sostituisce la funzione di un argomento $succ(v) = v+1$ con la funzione di due argomenti $s2(u,v) = v+1$, allora tutte queste definizioni hanno una struttura comune:

$$h(\, m,\, 0\,) = f(m)$$
$$h(\, m,\, n\,) = g(\, m,\, h(m,n-1)\,) \qquad per\ \ n > 0$$

Tale struttura è caratterizzata dall'operatore funzionale H, tale che $h = H(f, g)$. In particolare si ha:

$$add = H(\, i,\, s2\,)$$

$$mul = H(\, z,\, add\,)$$

$$pow = H(\, u,\, mul\,)$$

dove i, z, u sono rispettivamente la funzione *identità* (che assume il valore dell'argomento), la funzione costante *zero* (che assume valore 0 per ogni argomento), la funzione costante *uno* (che assume valore 1 per ogni argomento).

H può essere modellata da una procedura `H` con argomenti e valore procedurali.

Definisci `H` in Scheme, quindi definisci le procedure corrispondenti alle operazioni *add*, *mul* e *pow* applicando `H`, per esempio:

```
(define mul (H (lambda (x) 0) add))
```

Verifica infine i risultati su campioni significativi di dati.