Programmation 1

TD n°1

Aliaume Lopez

18/01/2019

Exercise 1 : Language discovery

For each of the following program or fragment of program, please indicate : (a) What the fragment does (b) Is it written using the imperative or functionnal paradigm (c) In which language the fragment is written.

1. ```
   PROGRAM HELLO
   WRITE(6,*) 'HELLO WORLD'
   STOP
   END
   ```
2. ```
       PROGRAM FACT
       J=1
       DO 1 I=1,10
       J=J*I
   1   CONTINUE
       WRITE(6,2) J
   2   FORMAT(I8)
       STOP
       END
   ```
3. ```
   001  IDENTIFICATION DIVISION.
   002  PROGRAM-ID.  'HELLO'.
   003  ENVIRONMENT DIVISION.
   004  CONFIGURATION SECTION.
   005  SOURCE-COMPUTER.  IBM-360.
   006  OBJECT-COMPUTER.  IBM-360.
   0065 SPECIAL-NAMES.
   0066     CONSOLE IS CNSL.
   007  DATA DIVISION.
   008  WORKING-STORAGE SECTION.
   009  77  HELLO-CONST  PIC X(12) VALUE 'HELLO,WORLD'.
   075  PROCEDURE DIVISION.
   090  000-DISPLAY.
   100      DISPLAY HELLO-CONST UPON CNSL.
   110      STOP RUN.
   ```
4. ```
   10 J=1
   20 FOR I=1 TO 10
   30 J=J*I
   40 NEXT I
   50 PRINT J
   60 END
   ```
5. ```
   (defun fact (n)
      (do* ((i 1 (+ i 1)) (j 1 (* j i)))
           ((>= i n) j)))
   ```
   ```

6.
```
(define (fact n)
  (cond
    ((<= n 1) 1)
    (t (* n (fact (- n 1))))))
```

7. $\square \leftarrow */\iota 10$

8.
```
def factorial(n):
    result = 1
    for i in range(1, n+1):
        result *= i
    return result
```

9.
```
function fact (n:integer):integer
begin
  var i,j : integer;
  j:=1;
  for i:=1 to n do
    j := j*i;
  fact := j
end
```

10.
```
int fact (int n)
{
  int i, j;

  j = 1;
  for (i=1; i<=n; i++)
     j *= i;
  return j;
}
```

11.
```
fact :: Int -> Int
fact 1 = 1
fact n = n * fact (n-1)
```

12.
```
let rec fact n =
     if n==1
        then 1
     else n * fact (n-1);;
```

13.
```
fun fact n =
      if n=1
         then 1
      else n * fact (n-1);
```

14.
```
fact(1, 1).
fact(N, M) :- N > 1, fact (N-1, M1), M=M1*N.
```

15.
```
counter=$1
factorial=1
while [ $counter -gt 0 ]
do
   factorial=$(( $factorial * $counter ))
   counter=$(( $counter - 1 ))
done
echo $factorial
```

16.
```
: fact
  dup 1 = if
  else dup 1 - fact *
  endif ;
```

17.
```
/factorial {
  dup 1 eq {}{
  dup 1 sub factorial mul
  } ifelse
} def
```

18.
```
function Factorial (N : Positive) return Positive is
   Result : Positive := N;
   Counter : Natural := N - 1;
begin
   for I in reverse 1..Counter loop
      Result := Result * I;
   end loop;
   return Result;
end Factorial;
```

19.
```
function fac(n){
    return(n<2)?1:fac(n-1)*n;
}
```

Exercise 2 : Representation of numbers

1. How many values can a 1 bit integer take ? What about 3 bits ? What about n bits ?
2. You're building a fence 100 feet long, with posts every 10 feet. How many posts do you need ?

Unsigned numbers

The sequence $\vec{a} \triangleq a_{n-1} \cdots a_0$ of digits is interpreted as

$$[\![\vec{a}]\!]_u \triangleq \sum_{k=0}^{n-1} a_k 2^k$$

Two's complement. AKA signed numbers

The sequence $\vec{a} \triangleq a_{n-1} \cdots a_0$ of digits is interpreted as

$$[\![\vec{a}]\!]_{tc} \triangleq -a_{n-1} 2^{n-1} + \sum_{k=0}^{n-2} a_k 2^k$$

3. What values can a natural number represented using n bits take ? What about a signed number ?
4. Compute the following additions on 4 bit unsigned numbers :
   (a) $0010 + 0110$
   (b) $0101 + 1010$
   (c) $1011 + 1101$
   (d) $1010 + 0110$
   (e) $1111 + 1111$
5. Interpret the operations when using (a) unsigned numbers (b) signed numbers.

One's complement

The sequence $\vec{a} \triangleq a_{n-1} \cdots a_0$ of digits is interpreted as

$$[\![\vec{a}]\!]_{tc} \triangleq \begin{cases} \sum_{k=0}^{n-2} a_k 2^k & \text{if } a_{n-1} = 0 \\ \sum_{k=0}^{n-2} (a_k - 1) 2^k & \text{otherwise} \end{cases}$$

6. How does one write 1 using One's complement ? What about -1 ? How can you negate a number ?
7. What is a huge drawback of this representation ?
8. Using previous examples, build an algorithm to add two numbers in One's complement. (Hint : the question is, how to handle the carry).
9. Why does your algorithm terminate ?
10. What is printed by the Java program below ?

```
byte i = 101, j = 87, k = -101, l = -99;
byte m, n, o;
m = i+j; n = j+k; o = k+l;
System.out.println(m);
System.out.println(n);
System.out.println(o);
```

Exercise 3 : Representation of text

1. Decode the following ASCII chain (written using hexadecimal codes)

   `64 6f 6e 27 74 20 70 61 6e 69 63`

2. The ASCII code is defined only from `00` up to `7f`. Some extensions exists for `80` up to `ff` ; however they depend on the *page*. One page is Latin-1 (ISO 8859-1). Decode the following text using Latin-1 :

   ```
   55 6e 20 70 ea 63 68 65 75 72
   20 e0 20 6c 61 20 6c 69 67 6e 65
   ```

3. I receive an email containing the following text. What happened ?

   `Je vais Ã_ SÃ¨te cet Ã©tÃ©.`

A few Unicode characters

U+000A	LINE FEED (LF)
U+0020	SPACE
U+0021	EXCLAMATION MARK
U+002C	COMMA
U+0030	DIGIT ZERO
U+0041	LATIN CAPITAL LETTER A
U+0061	LATIN SMALL LETTER A

4. Unicode solves some of the precedent problems. However, there are several formats to write Unicode. Decode the following UTF-32 (UCS-4) chain :

   ```
   00 00 00 6d 00 00 00 61 00 00 00 6d 00 00 00 6d
   00 00 00 61 00 00 00 20 00 00 00 6d 00 00 00 69
   00 00 00 61 00 00 00 21
   ```

5. What could be the shortcomings of UTF-32 ?

UTF-8 encoding

- U+0000 à U+007F : 0xxxxxxx
- U+0080 à U+07FF : 110xxxxx 10xxxxxx
- U+0800 à U+FFFF : 1110xxxx 10xxxxxx 10xxxxxx
- U-10000 à U-1FFFFF : 11110xxx 10xxxxxx 10xxxxxx 10xxxxxx

6. Decode the following UTF-8 chain

   ```
   6a 61 6b 20 7a 65 20 6d 6e c4 85 0a
   ```

7. Does UTF-8 have the same shortcomings as UTF-32 ? How and why ?
8. On the following website

   `http://www.dptinfo.ens-cachan.fr/Conferences/conferences15.php`

   one can read the following text :

   Pierre-Alain Fouque

   Aspects Algorithmiques de Cryptanalyse

   Dans cette conférence, je présenterai quelques algorithmes importants en cryptanalyse au travers d'exemples issus de cryptographie symétrique et asymétrique comme par exemple : les attaques génériques sur les fonctions de hachage, les algorithmes de factorisation ou du logarithme discret, les schémas de signature construit sur la difficulté à résoudre des systèmes quadratiques en plusieurs variables ou la difficulté à résoudre des systèmes linéaires avec du bruit.

   However, the server `projects.lsv.ens-cachan.fr` has sent to my web browser the following (extract) of code :

   ```
   <h2> <a name="Pierre-Alain_Fouque"
         href= "http://www.di.ens.fr/~fouque/" >
        Pierre-Alain Fouque  </a>
   </h2>
   <p><big><b>
      <a> Aspects Algorithmiques de Cryptanalyse </a>
      </b> </big>
   </p>
   <p>
   Dans cette conf&eacute;rence, je pr&eacute;senterai quelques
   algorithmes importants en cryptanalyse au travers d'exemples
   issus de cryptographie sym&eacute;trique et asym&eacute;trique
   comme par exemple: les attaques g&eacute;n&eacute;riques sur
   les fonctions de hachage, les algorithmes de factorisation ou
   du logarithme discret, les sch&eacute;mas de signature
   construit sur la difficult&eacute; &agrave; r&eacute;soudre
   des syst&egrave;mes quadratiques en plusieurs variables ou la
   difficult&eacute; &agrave; r&eacute;soudre des syst&egrave;mes
   lin&eacute;aires avec du bruit.
   </p>
   ```

   (a) Why does the previous code illustrate another answer to the encoding issues ?

   (b) What is the name of this language ?

9. When fetching the following webpage

   ```
   https://projects.lsv.ens-cachan.fr/topology/wp-admin
         /post.php?post=251&action=edit
   ```

my web browser displays :

> Now remember that $(x_i)_{i \text{ in } I, \leq}$ converges to x if and only if every open subset U that contains x is such that x_i is eventually in U. One obtains an equivalent definition by stating that every neighborhood A of x (i.e., in N_x) is such that x_i is eventually in A. In other words, if and only if N_x is included in the convergence filter of the net.

However, the server `projects.lsv.ens-cachan.fr` sent to my browser the following (extract) of code :

```
Now remember that (<em>x<sub>i</sub></em>) <em><sub>i</sub></em>
<sub> in </sub> <em><sub>I, &sqsubseteq;</sub></em> converges to
<em>x</em> if and only if every open subset <em>U</em> that
contains <em>x</em> is such that <em>x<sub>i</sub></em> is
eventually in <em>U</em>. One obtains an equivalent definition
by stating that every neighborhood <em>A</em> of <em>x</em>
(i.e., in <em>N<sub>x</sub></em>) is such that
<em>x<sub>i</sub></em> is eventually in <em>A</em>.
In other words, if and only if <em>N<sub>x</sub></em>
is included in the convergence filter of the net.
```

How does it compare to Unicode ?

10. Going back to the first example of HTML, the file started with :

```
<?
$EXTRA_HEAD="antispam.html";
$ARG_BODY="onload=\"onLoad()\"";
SETLANG("fr");
STYLEDPTINFO();
HEAD("Conf&eacute;rences de rentr&eacute;e 2015");
ADDTITLE("Conf&eacute;rences de rentr&eacute;e 2015");
MKPAGEDPTINFO();
?>
```

This is not HTML. What language is used ? What does it compute ?