Épreuve d'informatique de l'X - 2008 - MP/PC

(PSI*)

Codage de César

Question 1 : le codage de « `maitrecorbeau` » avec un décalage de 5 donne le message codé : « `hvdomzxjmwzvp` ».

Question 2 : ligne 5, on remplit le tableau représentant le texte codé avec les « lettres » du texte initial (représenté par un tableau d'entiers) décalés de d vers la gauche, ce qui se fait modulo le nombre de lettres dans l'alphabet soit 26.

```
1  codageCesar := proc (t, n, d)
2  local tt, i;
3  tt := array(0..n-1);
4  for i from 0 to n-1 do
5    tt[i] := (t[i]-d) mod 26
6  od;
7  return tt;
8  end;
```

Question 3 : même principe que dans la fonction précédente sauf que l'on effectue le décalage dans l'autre sens.

```
1  decodageCesar := proc (t, n, d)
2  local tt, i;
3  tt := array(0..n-1);
4  for i from 0 to n-1 do
5    tt[i] := (t[i]+d) mod 26
6  od;
7  return tt
8  end;
```

On aurait aussi pu utiliser la fonction précédente en effectuant un décalage dans l'autre sens de la manière suivante :

```
1  decodageCesar := proc (t, n, d)
2    return codageCesar(t,n,26-d)
3  end;
```

Question 4 : On commence par créer et initialiser le tableau des fréquences (lignes 3-6) puis on parcourt le tableau représentant le texte. À la lecture de la i-ème lettre du texte, on incrémente la case correspondante dans le tableau des fréquences (lignes 7-10).

```
1  frequences := proc (tt, n)
2  local i, freq, lettre;
3  freq := array(0..25);
4  for i from 0 to 25 do
5     freq[i] := 0
6  od;
7  for i from 0 to n-1 do
8     lettre := tt[i];
9     freq[lettre] := freq[lettre]+1
10 od;
11 return freq
12 end;
```

Question 5 : dans `decodageAuto`, on commence par récupérer le tableau des fréquences des apparitions des lettres dans le texte codé (ligne 3). On parcourt le tableau des fréquences pour repérer la fréquence d'apparition maximale ainsi que l'indice du tableau correspondant (ligne 5-11). On calcule la clé (ligne 12) en prenant en compte le fait que 'e' est la cinquième lettre de l'alphabet et enfin on décode le texte (ligne 13).

```
1  decodageAuto := proc (tt, n)
2  local i, freq, cle, maxi, imaxi;
3  freq := frequences(tt, n);
4  cle := 0; maxi := 0; imaxi := 0;
5  for i from 0 to 25 do
6      if maxi <= freq[i]
7           then
8                maxi := freq[i];
9                imaxi:= i;
10     if;
11 od;
12 cle := (4-imaxi) mod 26;
13 decodageCesar(tt, n, cle);
14 end;
```

Question 6 : Le codage du texte "`becunfromage`" en utilisant la clé de codage "`jean`" est "`kichwjrbvegr`".

Question 7 : Même principe que pour le codage de César sauf que le décalage dépend de la position de la lettre du texte à coder modulo k et s'obtient à partir des lettres de la clé. Le décalage pour la i-ème lettre du texte à coder est égal à $c[i \bmod k]$ (le décalage se fait cette fois-ci vers la droite).

```
1  codageVigenere := proc (t, n, c, k)
2  local i, tt;
3  tt := array(0 .. n-1);
4  for i from 0 to n-1 do
5     tt[i] := (t[i]+c[i mod k]) mod 26
6  od;
7  return tt;
8  end;
```

Question 8 : On programme un classique calcul de pgcd en utilisant les propriétés suivantes (les nombres sont supposés positifs) :

$$pgcd(0,b) = b, \quad pgcd(a,0) = a, \text{ et } pgcd(a,b) = \begin{cases} pgcd(a,b-a) \text{ si } a \leqslant b \\ pgcd(a-b,b) \text{ si } a > b \end{cases}.$$

```
1  pgcd := proc (x, y)
2  local a, b;
3  a := x; b := y;
4  while a <> 0 and b <> 0 do
5     if a <= b then b := b-a else a := a-b fi;
6  od;
7  if a = 0 then return b else return a fi;
8  end;
```

Question 9 : On mémorise la répétition des trois lettres $\langle tt[i], tt[i+1], tt[i+2]\rangle$ du texte codé dans les variables $t0$, $t1$, $t2$ (ligne 4-6), puis on fait une boucle pour regarder si la séquence $\langle tt[j], tt[j+1], tt[j+2]\rangle$ coïncide avec la séquence de départ pour j variant de $i+3$ à $n-4$. Si c'est le cas, on modifie la variable `PGCD` qui contiendra le résultat final. On y met `pgcd`($PGCD$, $j-i$) (ligne 10).

On utilise la propriété $pgcd(a_1,\ldots,a_p) = pgcd(pgcd(a_1,\ldots,a_{p-1}),a_p)$ et la propriété $pgcd(0,a) = a$.

```
1  pgcdDesDistancesEntreRepetitions := proc (tt, n, i)
2  local j, t0, t1, t2, PGCD, ecart;
3  PGCD := 0;
4  t0 := tt[i];
5  t1 := tt[i+1];
6  t2 := tt[i+2];
7  for j from i+3 to n-4 do
8     ecart := j-i;
9     if tt[j] = t0 and tt[j+1] = t1 and tt[j+2] = t2
10       then PGCD := pgcd(PGCD, ecart)
11    fi;
12 od;
13 return PGCD:
14 end;
```

Question 10 : Dans cette fonction, on essaye de trouver la longueur de la clé. Pour cela, on calcule les distances de répétition de $\langle tt[i], tt[i+1], tt[i+2]\rangle$ pour i variant de 0 à $n-7$. Comme on a supposé que toute répétition d'une séquence de 3 lettres dans le texte codé t' provient exclusivement d'une séquence de 3 lettres répétée du texte original t, ces distances seront toutes des multiples de la longueur de la clé. On retourne donc le $pgcd$ de toutes les distances non nulles pour obtenir le plus petit multiple possible de k (on espère trouver ainsi la longueur exacte de la clé avec ce procédé).

```
1  longueurDeLaCle := proc (tt, n)
2  local longueur, i;
3  longueur := 0;
4  for i from 0 to n-7 do
5     longueur := pgcd(longueur,pgcdDesDistancesEntreRepetitions(tt,n,i))
6  od;
7  return longueur;
8  end;
```

Question 11 : Dans la fonction `longueurDeLaCle`, on a au plus $n-6$ appels à la fonction `pgcd`. Mais il ne faut pas oublier que la fonction `pgcdDesDistancesEntreRepetitions` fait aussi appel à la fonction `pgcd` et que le nombre de ces appels est majoré par $n-i$.
On peut donc majorer le nombre total d'appels à la fonction `pgcd` par $n+\sum_{i=1}^{n} n-i = n+\frac{n(n+1)}{2}$ ce qui nous donne une complexité quadratique (en $O(n^2)$).

Question 12 : Une fois que l'on a k la longueur de la clé, on peut retrouver chacune des lettres de la clé en appliquant la méthode d'analyse des fréquences aux mots construits à partir du mot codé en prenant une lettre sur k. Pour le mot codé $\langle t'_0, \ldots, t'_{n-1}\rangle$ et $0 \leqslant j < k$, on fait une analyse en fréquence sur le mot $\langle t'_j, t'_{j+k}, \ldots, t'_{j+m.k}\rangle$, où $m = \lfloor \frac{((n-1)-j)}{k} \rfloor$. Cela nous permet de trouver la j-ème lettre de la clé de la même façon que dans la fonction `decodageAuto` de la question 5, à ceci près que les décalages se font vers la droite pour le codage de Vigenère et vers la gauche pour le codage de César.

Question 13 : En fait, on va créer la clé de décodage plutôt que la clé de codage pour pouvoir réutiliser la fonction `codageVigenere`. On commence par récupérer la longueur k de la clé que l'on obtient grâce à la fonction `longueurDeLaCle` (ligne 4). Pour trouver la j-ème lettre de la clé, on fait une analyse en fréquence du sous mot obtenu à partir du texte codé en partant de la j-ème lettre et en ne gardant qu'une lettre sur k (lignes 7-12). Une fois que l'on a le tableau des fréquences du sous mot, on le parcourt pour trouver la fréquence maximale qui correspondra normalement au codage de la lettre 'e' (lignes 13-18). On peut ainsi reconstituer la j-ème lettre de la clé de décodage (ligne 19). Une fois que l'on dispose de la clé de décodage, il ne reste plus qu'à décoder le texte (ligne 21).

```
1  decodageVigenereAuto := proc (tt, n)
2  local t, j, i, k, m, sousMot, l, freq, cle, maxi, imaxi;
3  t := array(0 .. n-1);
4  k := longueurDeLaCle(tt, n);
5  cle := array(0 .. k-1);
6  for j from 0 to k-1 do
7     m := floor((n-j-1)/k);
8     sousMot := array(0 .. m);
9     for l from 0 to m do
10       sousMot[l] := tt[j+l*k]
11    od;
12    freq := frequences(sousMot, m+1);
13    maxi := 0; imaxi := 0;
14    for i from 0 to 25 do
15       if maxi <= freq[i]
16          then maxi := freq[i]; imaxi := i
17       fi;
18    od;
19    cle[j] := (30-imaxi) mod 26
20 od;
21 return(codageVigenere(tt, n, cle, k))
22 end;
```