

TD n°1: Langage Caml

BATOG Guillaume

07 septembre 2006

Exercice 1 On considère la suite d'entiers définie par récurrence

$$\begin{cases} u_0 = 2 \\ u_{n+1} = 16\,033 u_n \bmod 65\,519 \quad \text{pour tout } n \geq 0 \end{cases}$$

1. Que valent u_{787} et $u_{997\,362}$?
2. Combien d'indices $1\,000 \leq i \leq 9\,999$ vérifient

$$(u_i \bmod 11) \geq \frac{(u_{i-1} \bmod 11)}{1 + (u_{i+1} \bmod 11)} ?$$

Même question pour $1\,000 \leq i \leq 999\,999$.

Exercice 2 Que retourne les programmes suivants ?

```
# let a = ref 3 and b = ref (1+2) in
  ( a = b , a == b );;

# let v = make_vect 3 0 in
  let matrice = make_vect 3 v in
  (matrice.(2)).(0) <- 1;
  (matrice.(0)).(0);;

# let v2 = copy_vect v and m2 = copy_vect matrice in
  v.(1) <- 352; v2;;
# m2;;

# let mm = concat_vect m m in
  m.(0) <- make_vect 3 0; mm;;

# v.(2) <- 18; mm;;
```

Exercice 3 [Fonctionnelles polymorphes]

1. Écrire la fonction `itere` qui à une fonction f et à un entier n retourne la fonction f^n , f composée n fois avec la convention $f^0 = id$.
2. Écrire avec le minimum de caractères une fonction qui retourne la liste des nombres pairs d'une liste d'entiers.

Exercice 4 [Cryptanalyse statistique du chiffrement de Vigenère]

Le chiffrement de Vigenère (1523-1596) repose sur un décalage des lettres en fonction de leur position. C'est un chiffrement symétrique par bloc : on découpe un texte t en blocs

code	0	1	2	3	4	5	6	7	8	9
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT
10	LF	VT	NP	CR	SO	SI	DLE	DC1	DC2	DC3
20	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS
30	RS	US	SP	!	"	#	\$	%	&	'
40	()	*	+	,	-	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[\]	^	_	`	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{		}	~	DEL		

FIG. 1 – Le code ASCII

de longueur n la taille de la clé K secrète, et pour chacun de ces blocs, on applique la fonction de chiffrement C_K ou de déchiffrement D_K définies par :

$$C_K(x_1, \dots, x_n) = (x_1 + k_1, \dots, x_n + k_n)$$

$$D_K(y_1, \dots, y_n) = (y_1 - k_1, \dots, y_n - k_n).$$

où $K = (k_1, \dots, k_n)$. La i^e lettre de l'alphabet latin correspond au nombre $i - 1$ et les additions sont effectuées modulo 26. Pour $n = 1$, on retrouve exactement le chiffrement de César (chiffrement par décalage) facile à casser à l'aide d'une simple analyse des fréquences des lettres. La cryptanalyse du système de Vigenère est fondée sur cette analyse statistique.

- Question 1.* Écrire une fonction **frequence** qui prend en argument le nom d'un fichier et qui retourne le tableau des fréquences des lettres apparaissant dans ce fichier.
- Question 2.* On définit l'indice de coïncidence IC par la probabilité que deux lettres choisies aléatoirement dans un texte soient identiques. Écrire une fonction **ic** qui prend en argument un tableau de fréquences et qui retourne l'indice de coïncidence IC correspondant. Que vaut IC pour un texte français ? pour un texte anglais ? pour un texte aléatoire ? Montrer que IC est stable par permutation des lettres.
- Question 3.* Écrire une fonction **afficheFreq** qui enregistre le tableau des fréquences de façon lisible dans un fichier.
- Question 4.* Écrire une fonction **chiffreVigenere** qui prend en argument une clé K et le nom d'un fichier texte t et qui écrit dans un nouveau fichier le chiffré de t pour le chiffrement de Vigenère de clé K . Écrire la fonction inverse **dechiffreVigenere**.
- Question 5.* Soit n une longueur de clé fixée. Pour un texte t , on considère les n sous-textes $t^{(j)} = t_j t_{j+n} t_{j+2n} \dots$ pour $1 \leq j \leq n$. Écrire une fonction **icSousTexte** qui à un texte t et un entier n , imprime la liste des indices de coïncidence des sous-textes $t^{(j)}$ et leur moyenne.
- Question 6.* Tenter de déchiffrer le texte enregistré sous le fichier **concoursblanc.tex**.

Exercice 5 [Graphisme récursif]

Dans un espace affine euclidien d'origine O , on définit une suite $(P_n)_{n \geq 0}$ de k -gones réguliers de centre O où P_0 possède un sommet sur la demi-droite $[Ox)$ et les sommets de P_{n+1} sont exactement les milieux des côtés de P_n . Écrire une fonction qui dessine les premiers k -gones de cette suite.