Université de Bordeaux — **N1MA9W05 – Master CSI**
Mathématiques — 2015–2016

FEUILLE D'EXERCICES n° 1

Exercice 1 – Pour un entier $N \geqslant 1$, on désire construire le vecteur $[1, \ldots, N]$.

1) Quelle complexité attendez-vous ?

2) Utiliser `gettime()` pour mesurer le temps écoulé. Quelle est la complexité pratique des constructeurs suivants :

a) `vector(N, i, i);`
b) `v = vector(N); for (i=1, N, v[i] = i);`
c) `v = []; for (i=1, N, v = concat(v,i));`
d) `v = List(); for (i=1, N, listput(v, i));`

Note.

- Pour chronométrer une instruction trop rapide : chronométrer une boucle qui l'exécute un grand nombre de fois (et soustraire le temps pris par la même boucle vide, s'il a une influence).
- Pour estimer α, β dans une fonction $f(N)$ qu'on devine de la forme βN^{α}, il est plus judicieux d'étudier $\ln f(N)/\ln(N) \simeq \alpha$ d'abord, puis $f(N)/N^{\alpha}$. On pourrait aussi faire une régression linéaire sur $\ln f(N) = \alpha \ln N + \ln \beta$ vue comme fonction de $\ln N$ et trouver simultanément α et $\ln \beta$.

3) Donner des explications possibles.

Exercice 2 – Soit $n > 0$ un entier ; a, b désignent deux entiers dans $[2^{n-1}, 2^{n}[$.

★ **1)** Écrire une fonction `TIME` générique permettant d'estimer la complexité pratique d'une opération binaire, comme $a, b \to a + b$, sans intervention manuelle.

Note.

- On pourra utiliser `random()`.
- Pour estimer le nombre d'itération nécessaire pour obtenir un temps significatif (en utilisant la technique de boucle du premier exercice), commencer par une itération, puis doubler le nombre d'itération tant que le temps de calcul est inférieur à $1s$ par exemple. Quel est au pire le temps total passé à chronométrer un calcul qui prendra finalement un temps T (en comptant le calibrage) ?
- La construction suivante peut être utile (passage d'une fonction anonyme en paramètre) :

```
TIME(N,a,b, f) = for(i=1, N, f(a, b))
TIME(10^6, 10,15, (a,b)->a+b)
```

2) Estimer la complexité pratique des opérations suivantes :

a) $a + b$, $\quad a - b$;
b) $a \times b$, $\quad a^2$;
c) $a \mod b$ (opérateur `%`), $\quad \lfloor a/b \rfloor$ (opérateur `\`) ;
d) division euclidienne de a par b (`divrem`) ;
e) a^{-1} dans $\mathbb{Z}/b\mathbb{Z}$;
f) obtention de l'identité de Bezout $au + bv = \mathrm{pgcd}(a, b)$ associée à (a, b).