Introduction à la Programmation des Algorithmes

3.3. Langage C – Pointeurs et mémoire

François Fleuret
https://fleuret.org/11x001/

Comme nous l'avons vu, les informations qu'un ordinateur manipule sont stockées dans une **mémoire vive**, qui est une suite d'octets, chacun avec une adresse, et pouvant stocker une valeur entre 0 et 255 inclus.

En particulier, une variable est une suite consécutive d'octets qui représentent une valeur à laquelle est associé un type.

Contrairement à la plupart des autres langages de programmation, le langage C permet de manipuler directement la mémoire.

Le concept central pour cela est celui de **pointeur**, qui est une variable contenant **une adresse en mémoire**.

Deux nouveaux opérateurs nous permettent de manipuler des pointeurs:

- l'opérateur `*` permet (1) de déclarer une variable de type pointeur, et (2) de manipuler la variable qui est pointée,
- l'opérateur `&` permet d'obtenir l'adresse en mémoire d'une variable.

La déclaration d'un pointeur se fait avec

```
type *identifiant;
```

l'accès à une variable pointée avec

```
*identifiant
```

et l'accès à l'adresse d'une variable avec

```
&identifiant
```

L'adresse d'une variable est en réalité celle du premier octet qui la compose.

Donc, par exemple

```
int *a;
```

veut dire “je déclare une variable a qui peut stocker l’adresse d’une variable de type `int`”,

```
a = &k;
```

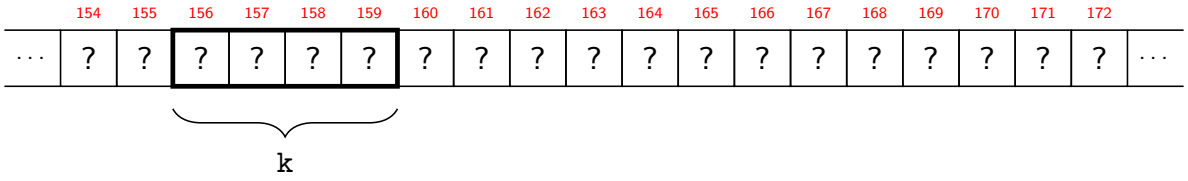
veut dire “copie dans a l’adresse de `k`”, et

```
*a = 65535;
```

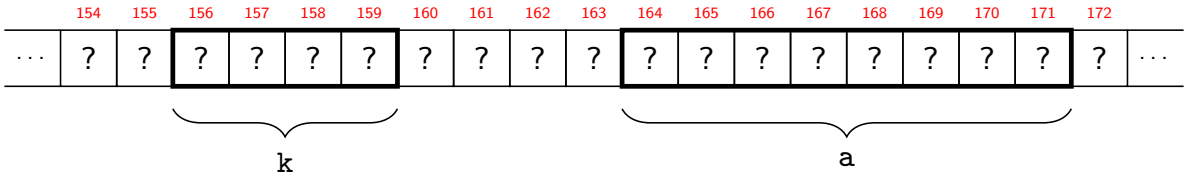
veut dire “copie 65535 dans la variable de type `int` dont l’adresse est dans a”.

	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	
...	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	...

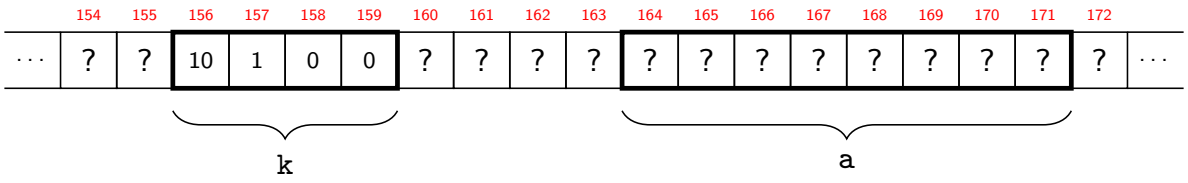
```
1   int k;
```



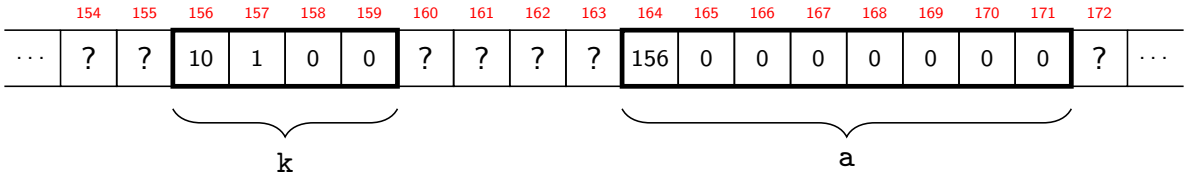

```
1   int k;
2   int *a;
```



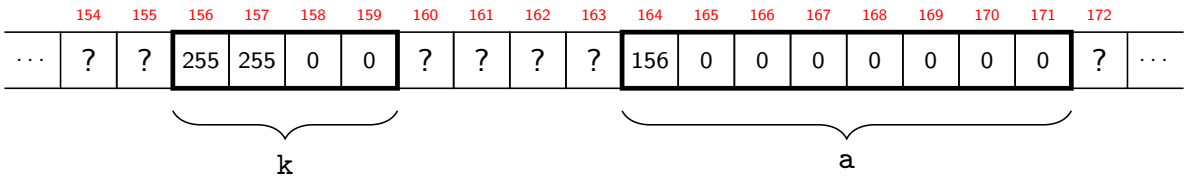
```
1   int k;
2   int *a;
3   k = 266;
```




```
1   int k;
2   int *a;
3   k = 266;
4   a = &k;
```



```c
int k;
int *a;
k = 266;
a = &k;
*a = 65535;
```




```c
int a = 1;
printf("a=%d\n", a);

int *q;
q = &a;

printf("*q=%d\n", *q);

*q = 2;
printf("a=%d\n", a);
```

La ligne 4 déclare une variable q de type pointeur vers `int` (ou plus simplement de type `int *`). La ligne 5 copie dans la variable q l'adresse de la variable a.

La ligne 7 accède à la valeur de la variable pointée par q, donc a, et la ligne 9 modifie la variable pointée par q.

⚠ Lors de la déclarations de plusieurs variables à la suite, l'opérateur `*` ne concerne que la variable à laquelle il est explicitement appliqué.

Par exemple

```
1  int *a, b, *c
```

déclare `a` et `c` de type pointeur sur `int`, et `b` de type `int`.

⚠ Faire en même temps la déclaration et l'affectation d'un pointeur résulte en un point de syntaxe particulièrement confus du langage C.

```
1  int *truc = &x;
```

veut dire

```
1  int *truc;
2  truc = &x;
```

et pas

```
1  int *truc;
2  *truc = &x;
```

qui de toute façon n'aurait aucun sens en ce qui concerne le typage, puisque `*truc` est de type `int` et `&x` de type `int *`.

Un pointeur est concrètement un entier de taille suffisante pour représenter une adresse arbitraire. Un entier sur 4 octets permet de représenter au maximum $2^{32} = 4'294'967'296$ adresses, donc un maximum de 4Gb.

Les ordinateurs actuels représentent les adresses sur 8 octets ce qui lève toute contrainte sur l'espace mémoire adressable.

```
1  int *q;
2  printf("%d\n", sizeof(q));
```

affiche

```
8
```


La spécification de format %p de `printf` permet d'afficher des pointeurs (en base 16).

```
1  int a, b;
2  printf("%p %p\n", &a, &b);
```

affiche

```
0x7fffbf56d658 0x7fffbf56d65c
```

Une variable de type tableau est directement convertible en pointeur, sans l'opérateur `&`.

```
1  int u[10];
2  int *p;
3  p = u;
4  printf("%p\n", u);
5  printf("%p\n", p);
6  printf("%p\n", &u[0]);
```

affiche

```
0x7ffee59e7a20
0x7ffee59e7a20
0x7ffee59e7a20
```


Il est possible de faire des opérations arithmétiques qui combinent pointeurs et entiers, ce qui permet par exemple de manipuler le contenu d'un tableau.

Ajouter ou soustraire un entier `n` à un pointeur `un_type *p` ajoute ou soustrait `n` fois la taille de `un_type` pour que cela corresponde à un déplacement de `n` éléments et non pas de `n` octets.

L'opérateur `[]` que nous avons appliqué à des tableaux peut être appliqué à des pointeurs. Dans ce cas, l'expression

```
p[n]
```

est exactement équivalente à

```
*(p + n)
```

```c
int u[10];
for(int k = 0; k < 10; k++) u[k] = k;
*(u + 3) = 13;
int n = 3;
*(u + n * 2 + 1) = 17;
for(int k = 0; k < 10; k++) printf("%d %d\n", k, u[k]);
```

affiche

```
0 0
1 1
2 2
3 13
4 4
5 5
6 6
7 17
8 8
9 9
```


La différence de deux pointeurs de même type retourne de manière similaire un entier égal au nombre d'éléments qui les séparent.

```c
float tab[1024];
float *p, *q;
p = tab;
q = &(tab[277]);
printf("%d\n", q-p);
```

affiche

277

La manipulation de pointeurs doit être faite de manière très rigoureuse, car comme pour les accès hors tableau, l'accès à une zone mémoire incorrecte peut entraîner des erreurs très imprédictibles et graves. Cela peut être la corruption de valeurs ou le crash au niveau du système.

Passage d'arguments par référence

Comme nous l'avons vu, lors de l'appel à une fonction, les valeurs passées en arguments sont **copiées** dans des variables locales créées au moment de l'appel.

Dans le cas d'un type composé comme un tableau ou une structure, cette copie peut prendre du temps.

Si la valeur à passer en argument est dans une variable, il est plus efficace de passer à la fonction un pointeur vers cette variable, qui est un type de petite taille fixe, plutôt que de faire une copie.

On parle alors de passer les arguments par **référence** plutôt que par **valeur**.

Les structures sont très souvent manipulées de cette façon, et le C offre l'opérateur `->` pour accéder aux champs d'une structure à partir de son adresse.

Si `p` est un pointeur vers une structure contenant un champ `truc`, l'expression

```
p->truc
```

est équivalente à

```
(*p).truc
```

```c
#include <stdio.h>
#include <math.h>

typedef struct {
  float x, y, z;
} vecteur3d;

float longueur(vecteur3d v) {
  return sqrt(v.x * v.x + v.y * v.y + v.z * v.z);
}

int main(void) {
  vecteur3d u = { -1, -1, 0 };
  float l = longueur(u);
  u.x /= l;
  u.y /= l;
  u.z /= l;
  printf("%f\n", longueur(u));
  return 0;
}
```

affiche

```
1.000000
```



```c
#include <stdio.h>
#include <math.h>

typedef struct {
  float x, y, z;
} vecteur3d;

float longueur(vecteur3d *p) {
  return sqrt(p->x * p->x + p->y * p->y + p->z * p->z);
}

int main(void) {
  vecteur3d u = { -1, -1, 0 };
  float l = longueur(&u);
  u.x /= l;
  u.y /= l;
  u.z /= l;
  printf("%f\n", longueur(&u));
  return 0;
}
```

affiche

```
1.000000
```

Passer un pointeur sur une variable permet également de la modifier si besoin est.

```
1  void trie(float *a, float *b) {
2    if(*a > *b) {
3      float k = *a;
4      *a = *b;
5      *b = k;
6    }
7  }
8
9  int main(void) {
10   float x = 1.2, y = 1.1;
11   printf("%f %f\n", x, y);
12   trie(&x, &y);
13   printf("%f %f\n", x, y);
14   return 0;
15 }
```

affiche

```
1.200000 1.100000
1.100000 1.200000
```



```
1  float longueur(vecteur3d *p) {
2    return sqrt(p->x * p->x + p->y * p->y + p->z * p->z);
3  }
4
5  void normalise(vecteur3d *p) {
6    float l = longueur(p);
7    p->x /= l;
8    p->y /= l;
9    p->z /= l;
10 }
```

Allocation dynamique de la mémoire

Il arrive très fréquemment que l'on veuille créer un tableau dont le nombre d'éléments n'est pas connu à l'avance et dépend du contexte dans lequel le programme est exécuté.

Un texte, une image, un échantillon sonore peuvent être de tailles variables et il est nécessaire pour les manipuler de créer des tableaux dynamiquement.

Dans certaines situations, on peut déclarer une variable locale de type tableau dont la taille dépend de l'exécution mais:

- la taille mémoire disponible sur la pile est limitée, et
- on peut avoir besoin que ce tableau continue à exister en dehors de la portée où il a été créé (par exemple si l'on veut qu'une fonction le crée).

La solution est de créer explicitement une variable dynamiquement en réservant un espace mémoire pour cela.

L'essentiel de la mémoire disponible constitue le **tas** (*heap*), et c'est dans cette zone que les programmes placent la quasi-totalité des variables créées dynamiquement.

On a donc les **variables locales** qui sont sur la pile et les **variables dynamiques** sur le tas.

Les mécanismes de réservations de sous-parties du tas en C sont très primitifs et reposent sur deux fonctions de la librairies `stdlib.h`:

- `void *malloc(size_t size);` pour allouer de la mémoire (*"memory allocate"*), et
- `void free(void *ptr);` pour libérer de la mémoire.

Le type `void *` peut être copié dans n'importe quel type pointeur sans erreur du compilateur.

La fonction `malloc` renvoie `0` si l'espace demandé n'est pas disponible, et `free` ne fait rien si l'adresse qui lui est passée en argument est nulle.

```c
#include <stdio.h>
#include <stdlib.h>

int main(void) {
  int *t;
  t = malloc(sizeof(int));
  *t = 5;
  printf("%d\n", *t);
  free(t);
  return 0;
}
```

affiche

5

On peut de même allouer dynamiquement un tableau

```c
int n = 25;
int *tab;
tab = malloc(sizeof(int) * n);
for(int k = 0; k < n; k++) tab[k] = 0;
free(tab);
```

Les fonctions `malloc` et `free` se limitent à réserver ou libérer de la mémoire.

En particulier:

- `malloc` ne met pas à zéro la zone mémoire réservée,
- `free` ne met pas à zéro la zone mémoire libérée,
- `free` ne change évidemment pas le pointeur qui lui est passé en argument.

Les erreurs de programmation dues aux pointeurs sont graves, imprédictibles, et difficiles à trouver.

Bien qu'un tableau puisse être converti en pointeur (c'est alors l'adresse du premier élément) et que l'opérateur [] puisse être appliqué à un tableau ou à un pointeur, ces deux types sont différents. En particulier **un pointeur ne fournit aucune information sur la taille de la zone allouée.**

```
1  int blah[100];
2  int *blih;
3  blih = malloc(sizeof(int) * 100);
4  printf("%d %d\n", sizeof(blah), sizeof(blih));
5  free(blih);
```

affiche

```
400 8
```

```
1  int nb_nb_premiers(int max) {
2    int *est_premier;
3    est_premier = malloc(sizeof(int) * max);
4    int nb = 0;
5
6    for(int n = 0; n < max; n++)
7      est_premier[n] = (n >= 2);
8
9    for(int n = 0; n < max; n++)
10     if(est_premier[n]) {
11       nb++;
12       for(int k = 2 * n; k < max; k += n)
13         est_premier[k] = 0;
14     }
15
16   free(est_premier);
17
18   return nb;
19 }
```

Si on avait utilisé une variable locale pour `est_premier` au lieu d'une allocation dynamique ligne 2, le programme crasherait pour `max > 2M`.

Une fonction peut renvoyer une valeur de type pointeurs

```
1  int *tableau_d_entiers_a_zero(int taille) {
2    int *t;
3    t = malloc(sizeof(int) * taille);
4    for(int k = 0; k < taille; k++) t[k] = 0;
5    return t;
6  }
```

Utiliser un pointeur sur une variable locale en dehors de la portée de cette dernière n'a aucun sens puisqu'elle n'existe plus.

```
1  int *ne_faites_jamais_ca(int n) {
2    int k[n];
3    for(int i = 0; i < n; i++) k[i] = i;
4    return k;
5  }
```


On appelle **fuite de mémoire** une erreur de programmation qui fait que le programme utilise de plus en plus de mémoire.

C'est généralement parce qu'un `free` manque et qu'un tableau qui n'est plus utile n'est pas libéré.