Chapitre 2 : variables, entrée/sortie dans un fichier, nombres aléatoires

Fondamentaux du C++

Master 2 Ingénierie mathématique
Sorbonne Université

Automne 2019

Plan

Organisation de la mémoire

- Mémoire de l'ordinateur : long "ruban" de cases mémoire= suites de 8 bits (=1 *octet*).

Déclaration de variable : réservation d'un certain nombre de cases mémoire (place nécessaire pour stocker la variable).
Exemples :

- `bool` = 1 bit = 1 case mémoire ;
- `char` = 8 bits = 1 case mémoire ;
- `int` = 32 bits = 4 cases mémoire ;
- `double` = 64 bits = 8 cases mémoire.

- adresse mémoire d'une variable `x` accessible par `&x` ;
- `&x` est un objet de type *pointeur* ;
- `std::cout << &x` : affiche l'adresse de la variable.

Visibilité des variables

Visibilité d'une variable : le fait qu'une variable ne puisse pas être utilisée à n'importe quel moment. La visibilité dépend des conditions dans laquelle la variable a été déclarée.

Trois types de variables :

Variables locales

- Une variable définie à l'intérieur d'un bloc n'est visible que dans ce bloc ;
- *Bloc* = groupe d'instructions situé entre deux accolades ;
- Utilisations typiques : variable interne à une fonction, paramètre d'une boucle.

Visibilité des variables

Visibilité d'une variable : le fait qu'une variable ne puisse pas être utilisée à n'importe quel moment. La visibilité dépend des conditions dans laquelle la variable a été déclarée.

Trois types de variables :

Arguments de fonction

- Accessible seulement à l'intérieur de la fonction correspondante ;
- Chaque appel de la fonction définit une nouvelle variable dans laquelle on recopie la valeur passée en argument de la fonction ;
- Notamment, une fonction ne peut pas modifier ses arguments ;
- On verra plus tard qu'une modification des arguments nécessitera de passer par des pointeurs ou des références.

Visibilité des variables

Visibilité d'une variable : le fait qu'une variable ne puisse pas être utilisée à n'importe quel moment. La visibilité dépend des conditions dans laquelle la variable a été déclarée.

Trois types de variables :

Variables globales

- Déclarées hors de toute fonction ;
- Accessibles à tout moment ;
- Attention : ce type de variable peut être modifié sans que l'on s'en aperçoive (par un appel de fonction).
- De préférence, déclarer les variables globales comme étant constantes.
- Usage typique : paramètres d'un problème à ne pas modifier.

Visibilité des variables

- Dans un même programme, plusieurs variables peuvent avoir le même nom.
- La “plus locale” des deux va masquer la “plus globale”.

Trop multiplier les variables différentes ayant le même nom est une mauvaise idée pour avoir un code lisible.

Qualificateur `const`

Une variable peut être déclarée *constante* par la syntaxe

```
type const nom;
```

Cela provoque une erreur à la compilation si la variable est modifiée dans le programme : c'est une aide pour l'écriture du programme.

Utilisation

On conseille de déclarer constante toutes les variables dont on sait qu'elles ne doivent pas être modifiée, afin de détecter toute modification accidentelle.

Qualificateur `static`

Une variable locale peut être déclarée *statique*, par la syntaxe

```
static type nom;
```

Donne une durée de vie permanente à la variable, sans changer sa visiblilité : la variable ne va pas être réinitialisée à chaque passage dans le bloc où elle est déclarée.

Exemples

Compter le nombre d'appel à une fonction ; garder la valeur courante d'un générateur de nombres aléatoires.

Plan

Écriture et lecture dans un fichier

- bibliothèque `fstream`.
- deux *types* `std::ofstream` (sortie (out) vers un fichier) et `std::ifstream` (entrée (in) depuis un fichier).

```
std::ofstream mon_flux; //On déclare un flux de sortie
mon_flux.open("mon_fichier"); // On ouvre un fichier
mon_flux << "Bonjour\n"; // On écrit dans le fichier
mon_flux.close(); // On referme le flux
```

On peut aussi ouvrir le fichier dès la déclaration :

```
std::ofstream mon_flux("mon_fichier");
```

Refermer le fichier n'est pas indispensable, mais c'est un bon réflexe, par exemple si on manipule de nombreux fichiers.

Écriture et lecture dans un fichier

On verra plus tard que `std::ofstream` et `std::ifstream` sont en fait des *classes*, que

```
std::ofstream mon_flux("mon_fichier")
```

est un appel de constructeur, et que

```
mon_flux.open("fichier")
```

et

```
mon_flux.close()
```

sont des appels de méthodes.

Plan

Nombres aléatoires : la théorie

- Ordinateur : aléa impossible.
- *Mais* : il existe des algorithmes *totalement déterministes*, générant des suites vérifiant certaines propriétés statistiques.
- On parle de suites de nombres *pseudo-aléatoires*.

En pratique

- On calcule $x_n \in \{1, \dots, N\}$, avec N grand, "ressemblant" à une suite i.i.d. de loi uniforme sur $\{1, \dots, N\}$.
- Si X est uniforme sur $\{1, \dots, N\}$, alors X/N est approximativement uniforme sur $[0, 1]$.

Un (*mauvais*) exemple : RANDU

On définit $x_n \in \{1, \ldots, 2^{31} - 1\}$ par :

$$\begin{cases} x_0 & \text{donné,} \\ x_{n+1} & = (2^{16} + 3) \times x_n \text{ modulo } 2^{31}. \end{cases}$$

$(x_n)_{n \in \mathbb{N}}$ est $2^{29} \simeq 5 \times 10^8$-périodique. Pour être un "bon" générateur, un générateur doit (entre autres) avoir une longue période. Ici, la période 2^{29} peut être suffisante pour bon nombre de problèmes.

Un (*mauvais*) exemple : RANDU

- Autre condition : corrélations faibles
- Ici : pour tout n $x_{n+2} = 6x_{n+1} - 9x_n \mod 2^{31}$. La suite des $(x_n, x_{n+1}, x_{n+2})/N$ n'est pas du tout uniformément répartie dans $[0,1]^3$.

Remarque

La suite $(x_n)_{n\in\mathbb{N}}$ est indexée par le paramètre x_0, appelé *graine* du générateur.
On obtient plusieurs suites différentes en partant de plusieurs graines différentes.
Deux suites partant de deux graines différentes *ne doivent par contre pas être considérées commme des suites indépendantes*.

Les implémentations : `rand`

La méthode simple

- Fonction `rand` de la bibliothèque `cstdlib`.
- Insuffisant pour certaines applications (méthode de Monte Carlo nécéssitant une longue période).
- Dans certaines implémentations, `rand` a une période de $2^{15} \simeq 32.000$: *beaucoup trop peu*.
- Choix de la graine avec `srand`. Le résultat de `rand` est un entier compris 0 et `RAND_MAX` inclus.

Les implémentations : Mersenne twister

La méthode efficace

- Depuis le standard 2011 (avec g++, option "`-std=c++11`"), le générateur dit "Mersenne twister" est implémenté ;
- Très utilisé pour les calculs de Monte Carlo (période extrêmement grande : $2^{19937} - 1 \simeq 4.32 \times 10^{6001}$) ;
- Pas sûr pour un usage cryptographique.

Les implémentations : Mersenne twister

Remarque : $2^{19937} - 1$ vaut


```
43154247973881626480552355163379198390539350432267115051652505414033306801376580911304513629318584665545269938257648835317902217334584413909528269154609168019007875343741396296801920114486480902661414318443276980300066728104984095451588176077132969843762134621790396391341285205627619600513106646376648615994236675486537480241964350295935168662363900479483476923139783013778207857124190544743328445291831729732423108882650813216264694510777078122822824447750226804880578200287646593991647662652009005614958003440543536903898628940617928720111208336148084474829135473283672778795656483078469091169458662301697024012602401870287466500334457745703154312929960251877807901193759028631710841496424733789862675033089613749057663409052895722900160380005716308751913739795550474681543332534749910462481325045036470806135273543270714478876861861983320777280644806691125713197262581763151313596429547763576367837019349835178462144294960757190918054625114143666384189438525764522893476524546315357404687862289458856546085620580424689873724369214450923153776984071681983765382377486141962070415481063793651231928179990066217664671671134716327154817958770053826943934004030617004576911353491878748889234293493401451705717161811257958888892774954269771499145496239163940148229850253316515114312788020090568084565068188772666098316368838849056218222629339865486456690806721917047404088913498356856624280632311985204368263294152907529727983434294465099922063687813671540917026557727273913294242775293490826005858847665231509574170778319100161684756856586731928608820701797603072698499873548360423717346602576943472355063017441188741412924389581415491006097522168822308876114319964723308423801371109274494835578150375868496445857499177728699267442183696211376751010832785437940817490940910430840967741447084363242794768920562004272279616386691498054898311212446763999319553714840128863607487064795686690485747828552170547401139459296221775025755658110674522014489819919686359653615516812739827407601388996388203187763036687627301575846400427988806918626402686126861808838749395738181250222796899302674462557739595424698316378630001712792271514060341299021815706596505326007758236773981821290873944498591827499990072235924233345678506711865688391867477049600162775406253314406190191299837899147125153652003360579935086016788076875685623778570952555413049029271922201841725023571244499118702106426945650613849193734743245039662677990384023867816868099620158790905865494235046991907435195510437225445157409678290843360259382257807308802738552615519720440756203267806244488034909982321612316877947156134057932495455095280525180101230872587789741158170482455889714385967544080813134383755029887267395233752966416155014060916079832292398272406147832528924797165199369895191878068612211916417477109024806334910917048274412282811866324459071457871383512348422613800746219140048181523866660431333448750679035828382835626880832365754820684796395463838195321745225026823724413632757658756091197836532983120667082171493167735643403792897243939867441398918554166122957393566686126582712346964383771228389980401997390780614436754156710784634046737024037776534781733670848447347020568666361581380036922533822099046646959193016162609792050874217567030650135942860750806159835357541032147095084278461056701367739794932024202998707731017692582046210702212514120429322530431789616262704777611512359793540414708487098546542650277205730090033384790533425060411950303000170400288789294140460334586992636750135509494275055259158163998052319067961078499358026097080451745064488290392073167113076951318922965935090186230948105575195603052407871638092191644337545148633010009159169858562421765636247713289816785482462973762495302513603634127683664561750770319774575349128064331765399959943433081184701471587128161493944212766142282629099500557469810532066100015602957846566161932522694120268311595089496715138451958832171479827488792618514178199790344172855986077272208666776804260903087548238033454465663056192413083744527546681430154877108777280110860043258922622594139682852834970455710627577014217615652627251534074076254051499319894944591064146605343053785767098625200498648809611448692586034737143636591940139627063668513892996928694918051725568185082988249549548157960631695176587414201597987542734280267234524812635691573072131537397810416276537150785985041547972876631229467113481585294188164328250444666927811374744948983850643757875073764963451486253063833915551456900878919553159944629444932352488175999071191357559338212170619147718505493663221115722292033114850248756330311801880568507356984158051811871077865395357129601437294086527040702192438316729032323156791228941948624059403907445232167801938187121909215546076844457357855951361330424220615135645751393727093900970723782710124585383767833816102339758685489423069609154024998790745346131192396385295075475805820562595660081774300719174681265595502174767092246086674774452087560785906233475062709832859348006778945616960249439281376349565759984748577355399095755731320080904083003644649221940993409694873054749430121616568675073574955588234030398987467297545506095773692155919548081551403591570712993005702711728625284319741331230761788679750678426019543676030599034070848146460727895549548774214075357062121719825219297886978691673462561843017545490386411158542950456992090563674153903096804147 1
```

Les implémentations : Mersenne twister

La méthode efficace

- Type `std::mt19937`, défini dans la bibliothèque `random` ;
- `std::mt19937 gen(1234)` déclare une variable `gen` correspondant à un générateur de graine 1234 ;
- Suite pseudo-aléatoire obtenue par des appels successifs de `gen()` ;
- La valeur maximale rendue est `gen.max()` ;
- On verra plus tard que `std::mt19937` est en fait une classe, dont `std::mt19937 x(int)` est un constructeur, et que `x()` correspond à l'appel de l'opérateur `()`.

Les implémentations : Mersenne twister

La méthode efficace

- On peut déclarer des variables correspondant à des lois de probabilité. Par exemple `std::normal_distribution<double> G(0,1);`.
- `G` va alors correspondre à la loi Gaussienne de moyenne 0 et de variance 1 .
- Chaque appel de `G(gen)` renvoie une réalisation de cette variable.

Les implémentations : Mersenne twister

La méthode efficace

- Si on tient absolument à ce que les réalisations des variables aléatoires soient différentes d'une exécution à une autre, on peut initialiser le générateur avec un `std::random_device`. Il s'agit d'un générateur de nombres aléatoires basé sur les capteurs de la machine et non sur un capteur.
- Les appels d'un `std::random_device` sont "plus aléatoires" que les appel d'un `std::mt19937`, mais ausi beaucoup plus lents.