Theoretical foundations

Introduction to Algorithmic Number Theory

Jean-Sébastien Coron

Université du Luxembourg

September 26, 2009

Summary

- C language
  - Arrays
  - `argc` and `argv`
- Number theory.
  - GCD
  - Euclid's algorithm

Arrays in C

- Arrays can store a group of variables of the same type.
  - For example:

```
int notes[5]; // array of 5 integers
notes[0]=15; // first entry
notes[1]=8;
notes[2]=16;
notes[3]=17;
notes[4]=9;// 5th entry
```

Arrays type

- Arrays type:
  - `float tabf[5]`: array of 5 `float`.
  - `double tabd[10]`: array of 10 `double`.
  - `int tabi[7]`: array of 7 `int`.
- Index:
  - An array of n elements is indexed from 0 to $n-1$:
  - `int tabi[7]`.
    - From `tab[0]` to `tab[6]`.

Constant size

- An array must be of constant size.
  - This size must be written in the program, for example `int tab[10]`
  - `#define`:

```
#include <stdio.h>
#define N 10    // one defines N=10
int main()
{
  int tab[N];
  int autretab[5];
}
```

Characters

- Stored in a byte (8 bits).
  - ASCII encoding:
  - `'A'` $\longrightarrow$ 65, `'B'` $\longrightarrow$ 66,...
  - `'0'` $\longrightarrow$ 48,...
- Printing a character:

```
char x;
x='A';
printf("%c",x);
```

Strings

- A string is an array of characters.
  - `char ch[10]="hello";` creates an array of characters such that :
  - `ch[0]='h'`, `ch[1]='e'`, `ch[2]='l'`, `ch[3]='l'`, `ch[4]='o'`
  - `ch[5]='\0'` is the last character.
  - The others elements are not initialized.
- Printing a string :
  - `printf("%s",ch);`

Initialization of an array

- Using `for`:

```
#define N 10
int main()
{
  int tab[N];
  int i;
  for(i=0;i<N;i++)
  {
    tab[i]=0;
  }
}
```

Example

- Factorial using array :
  - $n! = n \cdot (n-1) \cdots 2 \cdot 1$

```
#define N 10
int main()
{
  int fac[N];
  int i;
  fac[0]=1;
  for(i=1;i<N;i++)
  {
    fac[i]=fac[i-1]*i;
  }
}
```

2-dimensional arrays

- One can declare arrays with two dimensions or more :
  - `int tab[4][3];` declares an array of size 4*3.
- Initialization :

```
#define M 10
#define N 5
int main()
{
  int tab[M][N];
  int i,j;
  for(i=0;i<M;i++)
    for(j=0;j<N;j++)
      tab[i][j]=0;
}
```

Command-line arguments

- Obtaining command-line arguments :
  - One would like to be able to write :
    `$ fact 5`
    `120`
- Advantage :
  - No need to write `int n=5` in the code (then code needs to be recompiled each time n is changed).
  - Avoid a `scanf`.

argc and argv

- Command-line arguments are stored in array `argv`.
- `argc` contains the number of arguments (size of `argv`).

```
#include <stdio.h>
int main(int argc,char *argv[])
{
  int i;
  for(i=0;i<argc;i++)
  {
    printf("%s\n",argv[i]);
      // print each argv[i] word
  }
}
```

Using `argc` and `argv`

- If the previous program is named `affiche`, then :
  - ```
    $ affiche hello world 2
    affiche
    hello
    world
    2
    ```
- Here `argc=4`.
    ```

Converting a string to an integer

- `int atoi()` enables to convert a string to an integer.
  - Example : print the square of an integer.

```
#include <stdio.h>
#include <stdlib.h>
int main(int argc,char *argv[])
{
  int a=atoi(argv[1]); // conversion
  printf("%d\n",a*a);
}
```

- ```
  $ carre 3
  9
  ```
  ```

GCD

- Common divisor :
  - Let a, b be two integers. A common divisor of a and b is an integer m such that $m|a$ and $m|b$.
- GCD.
  - GCD of two integers a and b is the greatest common divisor of a and b.
  - If $d = \mathrm{GCD}(a, b)$, then for all m such that $m|a$ and $m|b$, we have $m|d$.
- Example
  - $\mathrm{GCD}(9, 6) = 3$
  - $\mathrm{GCD}(7, 5) = 1$.

Euclid's algorithm

- Euclid's algorithm :
  - Input: a, b.
  - Let $r_0 = a$ and $r_1 = b$.
  - For $i \geq 0$, one defines the sequence (r_i) and (q_i) such that :

    $$r_i = q_i \cdot r_{i+1} + r_{i+2}$$

    where q_i and r_{i+2} are the quotient and remainder of the division of r_i by r_{i+1}
  - The exists $k > 0$ such that $r_k = 0$.
  - Then $\mathrm{GCD}(a, b) = r_{k-1}$.

Proof

- Let $a > 0$ and $b \geq 0$.
  - If $b = 0$, then $\text{GCD}(a, b) = \text{GCD}(a, 0) = a$
  - Otherwise, let $a = b \cdot q + r$ with $0 \leq r < b$.
  - Then $\text{GCD}(a, b) = \text{GCD}(b, r)$.
  - (b, r) is less than (a, b).
- $\text{GCD}(a, b) = \text{GCD}(b, r)$
  - If $d|a$ and $d|b$, then $d|r$, and then $d|\text{GCD}(b, r)$. Then $\text{GCD}(a, b)|\text{GCD}(b, r)$.
  - If $d'|b$ and $d'|r$, then $d'|a$, and then $d'|\text{GCD}(a, b)$. Then $\text{GCD}(b, r)|\text{GCD}(a, b)$.
  - Then $\text{GCD}(a, b) = \text{GCD}(b, r)$.