PROG
DS

2019-10-16

Exercice 1 : Questions courtes

Q.1 : Pour chaque déclaration suivante, quel est le type de la variable déclarée ? Dans chaque cas, que pouvez-vous dire sur sa valeur après déclaration ?

1. `int a = 2;`
2. `double a;`
3. `uint16_t a[32];`
4. `uint16_t *a;`
5. `char *a = "all is well";`
6. `struct {int a; int b;} a;`

Q.2 : Pour chacune des suites d'expressions suivantes, décrivez le résultat attendu et si celui-ci mène à une erreur ou un comportement non souhaité.

1. `int t[256]; t[256] = 0;`
2. `int *t; t = 64;`
3. `int *t; *t = 64;`
4. `int *t = (int *)malloc(64); t[63] = 64;`
5. `int t[10][10]; t[0] = 4;`
6. `int t[10000][10000]; t[0][0] = 4;`

Q.3 : Quel problème pose la fonction suivante ? Comment pouvez-vous y remédier ?

```
void *allocaa(size_t n)
{
        uint8_t t[n];
        return (void *)t;
}
```

Q.4 : Quel problème pose la fonction suivante ? Comment pouvez-vous y remédier ?

```
int (int *t, unsigned n)
{
        unsigned nn = n/2;
        int *tt = t+nn;
        int res = 0;
        ...
        free(t);
        free(tt);
        return res;
}
```

Q.5 : Quel problème pose l'extrait de code suivant ? Comment pouvez-vous y remédier ?

```
for (uint64_t i = 17; i >= 0; i--)
{
        ...
}
```

Q.6 : Quel problème pose l'extrait de code suivant ? Comment pouvez-vous y remédier ?

```
if (((x % n) > 3) && (n != 0))
{
        ...
}
```

Exercice 2 : Évaluation de polynômes multivariés sur $\mathbb{F}_2$

Dans cet exercice, on s'intéresse à l'évaluation de polynômes en n variables à coefficients dans $\mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z}$. Puisque $1\times1 = 1$ et $0\times0 = 0$, on identifie les mônômes X_i^k, $k > 1$, avec X_i. Autrement dit, on travaille dans l'anneau $\boldsymbol{R}_n := \mathbb{F}_2[X_1, X_2, \ldots, X_n]/\langle X_1^2 - X_1, X_2^2 - X_2, \ldots, X_n^2 - X_n\rangle$, où le degré de chaque indéterminée est au plus un. Tout monôme est alors de la forme $\prod_{i=1}^n X_i^{e_i}$, $e_i \in \{0, 1\}$, et on défini son degré comme $\sum_{i=1}^n e_i$. Le degré d'un polynôme de $\boldsymbol{R}_n$ est défini de façon analogue au cas univarié, c-à-d qu'il est égal au degré maximum de ses monômes.

Exemples :

- $X_1^2X_2 + X_3 \notin \boldsymbol{R}_3$, car X_1 apparaît avec un degré $2 > 1$.
- $X_1X_1X_2 + X_3 \notin \boldsymbol{R}_3$, car X_1X_1 se simplifie en X_1^2.
- $X_1X_2 + X_3 \in \boldsymbol{R}_3$; son degré est 2.
- $X_1 + X_2 + X_3 + 1 \in \boldsymbol{R}_3$; son degré est 1.

Q.1 :

1. Quels sont les monômes non nuls de degré 0 de $\boldsymbol{R}_n$?
2. Quels sont les monômes de degré 1 de $\boldsymbol{R}_n$?
3. Combien y a-t il de monômes de degré $k \leq n$ dans $\boldsymbol{R}_n$?
4. Quelle est le cardinal de $\boldsymbol{R}_n$?

On suppose pour l'instant qu'on dispose des deux fonctions suivantes :

- `uint64_t map(int *monomial, int n);`
- `int *unmap(uint64_t monomial, int n);`

qui implémentent une bijection entre l'ensemble des monômes de $\boldsymbol{R}_n$ représentés par le tableau des exposants e_i des n indéterminées et $[\![0, 2^n - 1]\!]$.

Q.2 : Définissez une structure de donnée permettant de représenter un polynôme quelconque de $\boldsymbol{R}_n$ (et justifiez là).

Q.3 : Écrivez une fonction `eval_mon` qui évalue un monôme de $\boldsymbol{R}_n$ en un point de $\mathbb{F}_2^n$.

Q.4 : Écrivez une fonction `eval_poly` qui évalue un polynôme quelconque de $\boldsymbol{R}_n$ en un point de $\mathbb{F}_2^n$.

Q.5 : Proposez une implémentation de `map` et `unmap`.

Q.6 : Quelle est la complexité naïve de l'évaluation d'un polynôme de $\boldsymbol{R}_n$ sur *tous* les points de $\mathbb{F}_2^n$? Pensez-vous qu'il est possible de faire mieux ?