

Conception Formelle

TD2: Un premier exemple avec des boucles

Vincent Penelle

2021-2022

Copie de VOTRE NOM

Note : Comment rédiger ?

Regardez le fichier source fourni, et notamment l'exercice 1 du TD1 qui est rédigé. Vous y trouverez toutes les commandes latex dont vous devriez avoir besoin (c'est-à-dire essentiellement WP et `code` pour la syntaxe C, $\{\varphi\}P\{\psi\}$ pour les triplets, ainsi que l'environnement `align*`), ainsi qu'un exemple de comment rédiger (qui est déjà dans le cours). Rédigez vos réponses dans les cadres prévus à cet effet (ceux où il y a écrit "METTEZ VOTRE RÉPONSE ICI"). Et n'oubliez pas de renseigner "VOTRE NOM" dans le bloc ci-dessus.

Si vous ne pouvez pas compiler du latex, rendez-moi simplement le fichier .tex, et je ne râlerais pas si j'ai à faire quelques modifs pour le compiler et que la présentation est bizarre. Sinon, rendez-moi le pdf, et essayez de rendre ça "pas horriblement moche".

Pour l'environnement `align*` : l'utiliser est assez simple.

- Il est par défaut en mathmode (donc pas besoin de \$, mais si vous voulez du texte, il faut utiliser la commande `\text`).
- `&` permet de couper l'endroit où aligner (je le met toujours avant le = dans mes exemples).
- `\\` termine une ligne. Ne l'oubliez pas, sinon vous aurez des résultats surprenants. On se contentera d'un alignement (un `&`) par ligne affichée.

Exercice 1 : Racine carrée entière

On considère la fonction suivante (déjà annotée) :

```
1  /*@ ensures Psi1: \result * \result <= a;
2     ensures Psi2: a < (\result +1) * (\result +1);
3  */
4  int sqrtint(int a){
5     sum = 1;
6     count = 0;
7     /*@ loop invariant I1: 0 <= count <= sum;
8         loop invariant I2: (count+1)*(count+1) == sum;
9         loop invariant I3: count * count <= a;
10        loop variant V: a - count;
11     */
12    while(sum <= a){
13        count = count + 1;
14        sum = sum + 2 * count + 1;
15    }
```

```
16     return count;
17 }
```

On va commencer par déterminer la précondition de cette fonction annotée.

- (a) Calculer $\text{WLP}(\text{sqrtint}, \psi_1 \wedge \psi_2)$, en supposant que tous vos WLP intermédiaires sont bien définis.

Réponse:
METTEZ VOTRE RÉPONSE ICI.

On va maintenant démontrer, pas à pas, que la précondition définie ci-dessus est bien définie.

- (b) Démontrez que $\text{sum} \leq a \wedge I_1 \wedge I_2 \wedge I_3 \Rightarrow \text{WLP}(13 - 14, I_1)$.

Réponse:
METTEZ VOTRE RÉPONSE ICI.

- (c) Démontrez que $\text{sum} \leq a \wedge I_1 \wedge I_2 \wedge I_3 \Rightarrow \text{WLP}(13 - 14, I_2)$.

Réponse:
METTEZ VOTRE RÉPONSE ICI.

- (d) Démontrez que $\text{sum} \leq a \wedge I_1 \wedge I_2 \wedge I_3 \Rightarrow \text{WLP}(13 - 14, I_3)$.

Réponse:
METTEZ VOTRE RÉPONSE ICI.

- (e) Démontrez que $\neg(\text{sum} \leq a) \wedge I_1 \wedge I_2 \wedge I_3 \Rightarrow \text{WLP}(15, \psi_1 \wedge \psi_2)$.

Réponse:
METTEZ VOTRE RÉPONSE ICI.

Grâce à tout cela, on sait maintenant que le contrat déterminé plus haut est bien correct. On va maintenant démontrer que cette fonction termine.

- (f) Démontrez que $\text{sum} \leq a \wedge I_1 \wedge I_2 \wedge I_3 \Rightarrow V \geq 0$.

Réponse:
METTEZ VOTRE RÉPONSE ICI.

- (g) Démontrez que $\text{sum} \leq a \wedge I_1 \wedge I_2 \wedge I_3 \Rightarrow \text{WLP}(13 - 14, V < \text{at}(V, 13))$.

Réponse:
METTEZ VOTRE RÉPONSE ICI.