

# Conception Formelle

## TD-TP : Un peu de théorie et de pratique.

METTEZ VOS NOMS ICI

2021-2022

Ce travail est à réaliser en binôme. La date de rendu est fixée au 1<sup>er</sup> mai 2022.

Ce sujet (à part le premier exercice) est librement inspiré de l'algorithme Brute Force pour le tsp vu dans le cours de TAP de L3<sup>1</sup>. Rassurez-vous, on va y aller pas à pas et ne démontrer que le plus simple.

Les exercices sont par difficulté croissante. Les deux premiers demandent uniquement d'appliquer le calcul de WP et de trouver des invariants de boucle. Les réaliser parfaitement devrait valoir autour de 9. Le troisième demande de produire un code correct et de le démontrer, et de comprendre un prédicat. Avec les trois premiers exercices parfaits, on devrait arriver vers 15. Le quatrième est plus technique, il demande de formaliser un contrat informel et déterminer les bons invariants de boucle est moins immédiat, mais devrait être suffisamment guidé pour rester faisable. Le cinquième est plus exploratoire, et devrait donc être plus vu comme un bonus (la première question devrait cependant rester accessible).

**Structure du devoir et rendu** Le devoir est constitué du présent document, ainsi que de fichiers de code à compléter en parallèle des questions posées. Le code fourni est découpé ainsi : un fichier `.c` et `.h` pour chaque fonction, et un fichier `formalism.h` pour les prédicats. Ces fichiers sont à remplir au fur et à mesure. `formalism.h` contient uniquement deux prédicat à remplir (à l'exercice 3), le reste vous est donné. Il contient des lemmes qu'on admettra.

Pour répondre aux questions, vous avez deux choix :

- Soit compléter le présent document `.tex` en plaçant vos réponses dans les blocs `solutionorbox` prévues à cet effet. Pour cela, référez-vous aux macros définies dans les sujets de TD.
- Soit produire un document pdf par d'autres moyens (autre logiciel, scan), tant que c'est lisible, ça me conviendra.

Vous devrez rendre (sur la page moodle du cours) :

- Le présent document de réponse (ou votre version).
- Le dossier `code` complété. Dans les fichiers qui le composent, vous pourrez si besoin rajouter des commentaires expliquant comment prouver certaines spécifications si ce n'est pas immédiat, ou expliquer ce qui vous bloque.

**Rappels de logique :** On rappelle que :

- $p \Rightarrow q \equiv \neg p \vee q$
- $(p \wedge q) \Rightarrow r \equiv p \Rightarrow q \Rightarrow r$ .

Vous aurez à manipuler des expressions comprenant des  $\forall$ . Pour ces expressions-là, lorsque vous appliquez un pas de WLP, grossièrement il vous faut découper votre formule

---

1. <https://dept-info.labri.fr/~gavoille/UE-TAP/>

entre partie modifiée et partie non-modifiée, et appliquer le calcul. Plus concrètement ici, ce que vous devriez avoir, c'est quelque chose du genre :

$$\begin{aligned} & \text{WLP}(t[i] = x, \forall j; 0 \leq j \leq i \implies \varphi(t[j])) \\ \equiv & \text{WLP}(t[i] = x, (\forall j; 0 \leq j < i \implies \varphi(t[j])) \wedge \varphi(t[i])) \\ \equiv & (\forall j; 0 \leq j < i \implies \varphi(t[j])) \wedge \varphi(x) \end{aligned}$$

La règle la plus générale d'où vient cela est la suivante : pour  $\varphi$  et  $\psi$  des formules quelconques :

$$\forall j; \varphi(j) \equiv \forall j; \psi(j) \implies \varphi(j) \wedge \forall j; \neg\psi(j) \implies \varphi(j);$$

Un autre point, c'est «soyez paresseux» : si vous arrivez à un moment sur un calcul équivalent à  $\perp \Rightarrow \text{WLP}(i - j, \phi)$ , il est inutile de calculer  $\text{WLP}(i - j, \phi)$  pour déterminer que l'implication est vraie.

Vous devrez aussi prouver des prédicats de la forme **Toto{Pre,Post}(...)**. Pour prouver ce genre de prédicats, rappelez-vous, que Pre correspond au début du programme : il ne sera donc pas modifié par le calcul de WP. Post, au contraire, correspond à la fin du programme et donc au label Here : lors du calcul de WP, les valeurs correspondant à la position courante sont modifiées (donc vous gardez le label Here, où vous mettez la ligne de la position courante). Ça correspond simplement au calcul normal de WP où on laisse la formule abstraite : cette formule contient un label implicite qui est bel et bien Here. Une bonne manière de voir cela, est que, lorsque que vous remplacez le nom du prédicat par sa définition, vous remplacerez les **at(x,Pre)** par  $\text{old}(x)$ , et les **at(x,Post)** par  $x$ , et effectuez le calcul normalement.

On attendra que vos calculs de WP soient suffisamment détaillés, mais vous pouvez sauter quelques étapes si elles sont faciles (comme par exemples, appliquer plusieurs substitutions d'un coup). Évidemment, tant que cela est correct.

Comme dit souvent, pour les justification de vérité de formule, on n'attendra pas de preuves formelles, mais des justifications convaincantes (i.e., qui n'oublie pas de cas, mais on restera tolérant sur la forme). En gros, quand vous aurez une implication, une possibilité sera de dire un truc du genre «l'implication est vraie car telle et telle partie de la partie gauche impliquent bien la partie droite». Un «ben oui» (ou plutôt un remplacement par  $\top$ ) sera admissible pour des propriétés du genre  $\perp \Rightarrow \varphi$ ,  $\varphi \Rightarrow \top$  ou  $a < b \Rightarrow a \leq b$ . Cependant, pour faire cela de manière convaincante, vous auriez intérêt à simplifier vos formules avant.

Dans le présent sujet, on donne une version normalisée du code pour vous faciliter preuves (if then else développés, un seul return, que des while). Évidemment, vous pouvez coder autrement, mais il sera plus aisé de faire ces restrictions sur papier.

Attention : on manipule beaucoup de unsigned int. En pratique, dans vos formules, *quantifiez sur des integer, et non des int.*

**Un mot sur les preuves :** À partir de l'exercice 3, certaines des preuves commencent à être difficiles pour les solveurs, aussi faites bien les trois points suivants :

- Vérifiez que le solveur Z3 est activé (il parvient à démontré des propriétés où alt-ergo échoue).
- Si certaines propriétés ne sont pas prouvées, retentez la preuve : quand les solveurs tentent trop de preuves en même temps, il arrive que certaines timeout pour de mauvaises raisons. Les relancer peut régler le problème.
- Si cela ne marche toujours pas (et que vous avez confiance en la propriété), cliquez sur le nom du but, puis sur la tactique «filter». Cela peut parfois régler le problème.

Si rien de tout cela ne marche, vous avez probablement oublié de spécifier certaines hypothèses (ou votre propriété est fausse), donc reprenez votre stylo.

### Exercice 1 : Swap par xor

On considère une variante du swap sans variable auxiliaire, en utilisant l'opération xor (notée  $\wedge$ ). On va pour l'occasion, augmenter les opérations arithmétiques que l'on s'autorise dans notre langage jouet C1 avec l'opération xor, avec la même sémantique qu'en C. En particulier, on rappelle (et c'est la seule propriété dont on aura besoin) que pour tous entiers  $n, m$ ,  $(n \wedge m) \wedge n = m$ , et que cette opération est commutative (et associative).

À noter que cette version du swap n'est en réalité pas vraiment plus efficace que celle avec mémoire auxiliaire. On va de plus voir qu'elle dispose d'un léger défaut supplémentaire.

```
1 /*@ ensures *a == \old(*b);
2     ensures *b == \old(*a);
3 */
4 void swap(int *a, int *b)
5 {
6     *a = (*a) ^ (*b);
7     *b = (*a) ^ (*b);
8     *a = (*a) ^ (*b);
9     return;
10 }
```

- (a) Si ce n'est pas déjà fait et que vous rendez le présent .tex, mettez vos noms dans la balise author situé en haut de ce document (celle où il y a écrit un message assez explicite). (0 points)
- (b) Calculez  $WP(\text{swap}, \psi)$  pour  $\psi$  la post-condition fournie, et déduisez-en un triplet de HOARE valide.

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (c) Évidemment, on a ici une correction partielle, dans le sens où on n'a pas tenu compte des comportements indéterminés. Quelle information manque-t'il pour assurer qu'il n'y aura pas d'erreur à l'exécution ?

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (d) Quel autre problème voyez-vous à notre preuve ? Quelle hypothèse cachée faut-il rajouter pour qu'elle soit correcte ?

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (e) Compléter le fichier `swap-xor.h` de manière à ce que Frama-C puisse démontrer la post-condition fournie, en ajoutant les assertions RTE. Il est bien évidemment possible (et encouragé) de répondre aux questions précédentes grâce à celle-ci.

## Exercice 2 : Reverse

On veut maintenant une fonction qui va inverser une portion consécutive d'un tableau. Le but de cet exercice est de formaliser le contrat et de le prouver. On considère le code de la fonction, ainsi que la précondition que l'on souhaite démontrer.

```
1 /*@
2 ensures Phi: \forall integer k;
3           i <= k <= j ==> t[k] == \old(t[j-k+i]);
4 */
5 void reverse(int *t, unsigned int i, unsigned int j,
6 unsigned int n)
7 {
8     while (i < j)
9     {
10         int aux = t[i];
11         t[i] = t[j];
12         t[j] = aux;
13         i++;
14         j--;
15     }
16     return;
17 }
```

- (a) Quelle condition doit-être vraie à la sortie de la boucle (question sur 0 points, c'est quand même trivial) ?

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (b) Calculez  $WLP(10 - 14, I)$  pour un invariant  $I$  quelconque.

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (c) Proposez des invariants de boucle pour votre boucle. Vous devriez en avoir qui détermine un ordre sur les variables  $i, j$  et les comparent avec leurs valeurs initiales (un seul peut suffire, mais vous pouvez bien sûr le découper), ainsi qu'un invariant qui donne une relation entre  $i$  et  $j$  (i.e., il ne suffit pas de les encadrer, il faut décrire comment elles évoluent l'une par rapport à l'autre). Vous devriez également avoir des invariants qui parlent de la partie du tableau déjà modifiée, et d'autres qui parlent de la manière non encore modifier. Au total, 4 invariants peuvent suffire, mais ça dépend de comment vous les écrivez (en compressant on peut faire 3, et on peut les découper en plus). Vous leur donnerez des noms (par exemple  $I_1, I_2$ , etc, ou des noms plus explicites). On appellera  $I$  leur conjonction.

Justifiez que  $\neg i < j \wedge I \Rightarrow WLP(16, \varphi)$ .

Pour chaque  $I_i$ , précisez  $WLP(10 - 14, I_i)$  (utilisez le calcul de la question b), et justifiez que  $i < j \wedge I \Rightarrow WLP(10 - 14, I_i)$ .

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (d) Déduisez-en un triplet de HOARE valide pour votre fonction.

**Réponse:**  
METTEZ VOTRE RÉPONSE ICI.

- (e) Démontrez la terminaison de la fonction en donnant un variant de boucle et en démontrant qu'il décroît à chaque tour de boucle et qu'il est toujours positif (vous pouvez utiliser le calcul de la question b).

**Réponse:**  
METTEZ VOTRE RÉPONSE ICI.

- (f) Quelles sont les valeurs mémoires modifiées par cette fonction (et la boucle) ? Vous répondrez en donnant les clauses assigns et loop assigns correspondantes.

**Réponse:**  
METTEZ VOTRE RÉPONSE ICI.

- (g) Que manque-t'il comme précondition pour que la fonction ne puisse pas faire d'erreur à l'exécution ?

**Réponse:**  
METTEZ VOTRE RÉPONSE ICI.

- (h) Complétez les fichiers `reverse.c` et `reverse.h` de manière à ce que le contrat reflète tous les points vus ici et que frama-c accepte de prouver le contrat. Vous pouvez bien évidemment vous servir de cette question pour travailler les précédentes (c'est recommandé, d'ailleurs). On attendra bien sûr que toutes les assertions RTE soient démontrée, ainsi qu'une clause `terminates \true`.
- (i) (Bonus) Proposez une version récursive de la fonction et démontrez (avec Framac-C) qu'elle vérifie le même contrat. En particulier, vous fournirez une clauses `decreases` permettant à la clause `terminates \true` d'être satisfaite (frama-c ne la vérifiera pas, mais moi oui).

### Exercice 3 : Permutations minimales et maximales

On s'intéresse maintenant à des fonctions générant des permutations sur l'ensemble  $\{0, \dots, n-1\}$ , vues comme des tableaux.

**Définition 0.1.** Une permutation sur  $\{0, \dots, n-1\}$  est une fonction  $P$  qui à chaque entier  $i \in \{0, \dots, n-1\}$  associe un entier  $P[i]$  de  $\{0, \dots, n-1\}$  et qui est une bijection.

En C, on va stocker une bijection dans un tableau. On définit donc un bijection avec le prédicat suivant.

```
1 predicate isPermutation(int *t, integer n) =
2 \forall integer i; 0 <= i < n ==> 0 <= v[i] < n &&
3 \forall integer i,j; 0 <= i < j < n ==> v[i] != v[j];
```

- (a) Justifiez (rapidement) que ce prédicat est bien équivalent à la définition d'une permutation.

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

On va également considérer un ordre entre les permutations. On le définit via les trois prédicats suivants :

```
1 predicate unchangedTab{L,M}(int *s, int *t, integer i,
2 integer n) = \forall integer j; i <= j < n ==>
3 \at(s[j],L) == \at(t[j],M);
4
5 predicate isStrictlyBiggerPerm{L,M}(int *t, int *s,
6 integer n) = (\exists integer m; 0 <= m <= n-1 &&
7 (\at(t[m],L) < \at(s[m],M) &&
8 unchangedTab{L,M}(t,s,0,m)));
9
10 predicate isBiggerPerm{L,M}(int* t,int* s, integer n) =
11 isStrictlyBiggerPerm{L,M}(t,s,n) ||
12 (unchangedTab{L,M}(t,s,0,n));
```

- (b) Quelles sont, selon cet ordre, les permutations minimales et maximales? Donnez des prédicats `isMinPerm(int *t, integer n)` et `isMaxPerm(int *t, integer n)` qui ne sont vrais que si le tableau `t` est la permutation minimale (resp. maximale). Complétez ces prédicats dans `formalism.h`. Les deux premiers lemmes de la section exercice 4 devraient être démontrés, mais pas les autres (c'est normal).

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (c) Implémentez maintenant une fonction qui place dans `P` la permutation minimale, avec le prototype et le contrat partiel suivants. Respectez les styles que l'on sait démontrer sur papier, à savoir un seul point de sortie de la fonction et uniquement des boucles `while` (pas de `for`).

```
1 /*@
2 terminates \true;
3 ensures isPermutation(P,n);
4 ensures isMinPerm(P,n);
5 */
6 void initPerm(int *P, unsigned int n);
```

- (d) Déterminez un contrat complet pour cette fonction. Vous aurez évidemment besoin de déterminer des invariants de boucles. On attend à cette question que vous fournissiez les calculs de WLP adéquats.

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (e) Démontrez la terminaison de cette fonction en donnant un variant pour votre boucle, et en démontrant que c'en est un.

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (f) Votre implémentation de `initPerm` doit valider le contrat précédent dans Frama-C, ainsi que valider les assertions RTE, et comprendre la preuve de terminaison.
- (g) Donnez une implémentation de la fonction dont le contrat partiel et le prototype suivent. Attention, alt-ergo n'arrivera a priori pas à tout démontrer, mais Z3 y arrivera. On ne demande pas de démontrer sur papier cette fonction, vous êtes donc libre sur le style. On attend que les assertions RTE soient démontrées, et que vous démontriez que la fonction termine.

```
1 /*@
2  terminates \true;
3  ensures isMaxPerm(P,n) ==> \result == true;
4  ensures !isMaxPerm(P,n) ==> \result == false;
5 */
6 bool isMaxPerm(int *P, unsigned int n);
```

Cela dit, si vous ne parvenez pas à tout démontrer et souhaitez me montrer sur papier ce que vous essayez de faire et faire des preuves partielles, vous pouvez le faire en suivant :

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

#### Exercice 4 : NextPermutation

On va maintenant s'intéresser à la fonction qui permet de considérer la prochaine permutation dans l'ordre défini précédemment.

```
1 bool NextPermutation(int *P, unsigned int n)
2 {
3     unsigned int i = n - 1, j;
4     j = n - 1;
5     while (j > 0 && P[j - 1] >= P[j])
6     {
7         j--;
8     }
9     if (j == 0)
10    {
11        return false;
12    }
13    i = j - 1;
14    while ((j < n) && (P[i] < P[j]))
15        j++;
16    j--;
17    swap(P + i, P + j);
18    reverse(P, i + 1, n - 1, n);
19    return true;
20 }
```

Le but de cet exercice est de déterminer un contrat de fonction pour cette fonction et de le prouver (avec Frama-C). Un mot d'avertissement : sur une telle fonction (et avec le genre de propriété qu'on souhaite montrer), les solveurs vont commencer à suer un peu : certaines propriétés ne seront démontrées qu'avec Z3 (et pas alt-ergo), et il y aura besoin de placer certaines assertions en cours de code pour les aider. En l'occurrence, je vous fournis dans le fichier `NextPermutation.c` les assertions dont j'ai besoin pour démontrer mon contrat (et qui sont sans doute liées au fait qu'on a fait des appels de fonction). Les preuves utilisent les lemmes de la section Exercice 4 de `formalism.h` (qu'on ne demande pas de démontrer).

- (a) Le premier but est donc de formaliser le contrat qui suit :
- Si la fonction reçoit une permutation maximale (i.e., qui satisfait `maxPerm(P,n)`), la fonction renvoie faux et ne modifie rien.
  - Si la fonction reçoit une permutation non-maximale, alors elle renvoie vrai et place dans `P` une permutation strictement plus grande que celle qui y était à l'entrée de la fonction.
  - Dans tous les cas, il y aura une permutation dans `P` à la fin de l'appel de la fonction.

Donnez une formalisation de ces post-conditions :

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

Bon, je ne vais pas vous faire l'insulte de vous demander de calculer les WLP des deux boucles, puisque leur corps n'est pas ultra compliqué.

- (b) Pour la première boucle, déterminez des invariants. Le but est surtout de déterminer ce que fait la boucle. Indication : la boucle s'arrête dès qu'on n'a trouvé un indice  $j$  pour lequel  $P[j-1] > P[j]$ . Que peut-on donc dire sur la fin du tableau si on est en  $j$ ? (ceci est une question rhétorique pour que vous trouviez l'invariant). Déterminez ces invariants et justifiez (rapidement) que c'en sont : il faut deux invariants. Déterminez une clause assigns et un variant.

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (c) Même question pour la seconde boucle. De la même manière, il faut être capable de décrire ce qui est vrai sur la portion du tableau exploré. Intuitivement, cette boucle place  $j$  sur l'élément suivant celui qui est le plus petit élément plus grand que `P[i]` (c'est pour ça qu'on fait  $j-$  après la boucle). Il y a besoin de deux invariants. Donnez la clause assigns et un variant.

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (d) Terminez les annotations dans le fichier pour démontrer le contrat de cette fonction. En particulier, précisez les requires pertinent, la bonne clause assigns pour le contrat, et la clause terminates qui assure que cette fonction termine. Si vous n'utilisez pas de comportements, alors il vous faut un ensures de plus (qui dit que la permutation n'est pas modifiée si la permutation en entrée est maximale). Si vous utilisez des comportements, il est possible d'avoir des clauses assigns différentes et de se passer de cet ensures.

- (e) Le contrat qu'on a donné ici n'est en réalité pas complet (ce qui manque est explicité dans l'exercice 5). Donnez une fonction qui respecte le même contrat (mais plus simple), mais qui ne répond pas à l'idée intuitive de ce que fait `nextPermutation` (on n'attend pas nécessairement que vous la prouviez avec Frama-C, vous pouvez vous contenter d'expliquer pourquoi elle satisfait le contrat). Indication : cette fonction pourrait systématiquement retourner la même permutation.

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

### Exercice 5 : tsp

On va maintenant tenter de démontrer une fonction qui implémente un algo Brute Force pour le travelling salesman problem. Pour cela, on va éluder un détail : on admet l'existence d'une fonction `value` qu'on abstrait (techniquement, il faudrait plus d'arguments, mais ici on s'en fiche). On va également avoir besoin de quelques lemmes qu'on admettra (les solveurs n'arrivent pas à les démontrer). On va également ajouter la partie du contrat qui manque à la fonction précédente, qu'on admettra également (enfin, si vous arrivez à le démontrer, je serai impressionné). Tout cela est défini dans `tsp.h` et dans `formalism.h`.

À partir de ça, on considère le code suivant :

```
1 /*@
2 ensures \forall int* t; \separated(t+(0..n-1),P+(0..n-1))
3 ==> isPermutation(t,n) ==> value(t,n) >= \result;
4 */
5 int tsp(unsigned int n, int *P)
6 {
7     initPerm(P, n);
8     int val = value(P, n);
9     while (!(isMaxPerm(P, n)))
10    {
11        NextPermutation(P, n);
12        if (val > value(P, n))
13            val = value(P, n);
14    }
15    return val;
16 }
```

Une note : dans le contrat que nous avons fourni, vous noterez la présence d'une clause `\separated`. Sans cela, Frama-C est incapable de démontrer le contrat. Cela est dû au fait qu'on formalise nos permutations comme des tableaux, et non réellement comme des objets abstraits, et que comme on modifie la permutation courante via `NextPermutation`, les solveurs ne sont pas capables de montrer qu'une formule quantifiant universellement sur les permutations n'est pas impactée par l'appel de `NextPermutation`. En précisant qu'on ne regarde que les permutations qui ne recourent pas `P`, ils s'en sortent par contre. Ça devrait suffire pour être convaincant, mais ça rend la formalisation un peu plus pénible. Mais je ne vois pas d'autre moyen de quantifier universellement sur des permutations.

Vous aurez bien évidemment besoin de garder cette hypothèse de séparation dans vos

invariants.

Frama-C n'arrivera pas à prouver le contrat sans assertions. Celles qui sont déjà placées dans `tsp.c` devraient être suffisantes.

- (a) Ajoutez les annotations de boucle et les préconditions nécessaires pour démontrer la correction partielle de cette fonction.
- (b) Démontrez sur papier que la fonction termine, en donnant un variant de boucle. Ce variant pourra être dans un autre ordre bien fondé que sur  $\mathbb{N}, <$ .

Je ne demande pas de le faire sur Frama-C (vous pouvez si vous le souhaitez, mais je pense que c'est un peu technique à écrire proprement).

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (c) (Bonus ++) Frama-C n'arrive pas à démontrer certains des lemmes qu'on a admis. Faites-le vous sur papier.

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.

- (d) (Bonus +++) Démontrez que la fonction `nextPermutation` vérifie le contrat supplémentaire qu'on a ajouté à cet exercice. Sur papier, c'est faisable (avec quelques arguments). Sur Frama-C, je n'ai pas réussi (mais pas tenté tant que ça), donc si vous y arrivez, je serai impressionné.

**Réponse:**

METTEZ VOTRE RÉPONSE ICI.