Examen du cours Sémantique et application à la vérification
Abstraction de calculs sur les nombres complexes
Épreuve écrite (2 heures)

31 mai 2019

Résumé

Dans ce problème, nous esquissons la conception d'un domaine numérique pour borner le module des nombres complexes qui apparaissent dans les programmes.

1 Pré-requis sur les nombres complexes

Un nombre complexe z est un couple (a, b) de nombres réels. L'ensemble des nombres complexes est noté $\mathbb{C}$. Étant donné des nombres complexes $z \triangleq (a, b)$, $z_1 \triangleq (a_1, b_1)$, et $z_2 \triangleq (a_2, b_2)$ et $\lambda \in \mathbb{R}$ un nombre réel, nous noterons $\overline{z}$, $\lambda . z$, $z_1 + z_2$, et $z_1 \cdot z_2$, les nombres complexes suivants :

— $\overline{z} \triangleq (a, -b)$;
— $\lambda . z \triangleq (\lambda \cdot a, \lambda \cdot b)$;
— $z_1 + z_2 \triangleq (a_1 + a_2, b_1 + b_2)$;
— $z_1 \cdot z_2 \triangleq (a_1 \cdot a_2 - b_1 \cdot b_2, a_1 \cdot b_2 + a_2 \cdot b_1)$.

Le nombre complexe $\overline{z}$ est appelé le conjugué du nombre complexe z ; le nombre complexe $\lambda \cdot z$ est appelé le produit externe entre le nombre réel λ et le nombre complexe z ; les nombres complexes $z_1 + z_2$ et $z_1 \cdot z_2$ sont respectivement appelés la somme et le produit entre les nombres complexes z_1 et z_2.

Enfin, étant donné un nombre complexe $z \triangleq (a, b)$, nous définissons le module $|z|$ comme étant la quantité $\sqrt{a^2 + b^2}$. Nous rappelons que les propriétés suivantes sont valables pour tous nombres complexes $z, z_1, z_2 \in \mathbb{C}$ et tout nombre réel $\lambda \in \mathbb{R}$:

— $|z| = |\overline{z}|$;
— $|\lambda . z| = |\lambda| \cdot |z|$;
— $||z_1| - |z_2|| \leqslant |z_1 + z_2| \leqslant |z_1| + |z_2|$;
— $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$.

2 Domaine abstrait

Nous considérons un ensemble de variables $\mathcal{V}$. Nous voulons abstraire un ensemble de fonctions (ou environnements) de l'ensemble des variables $\mathcal{V}$ vers l'ensemble des nombres réels $\mathbb{R}$, par un ensemble de contraintes portant sur le module des nombres complexes formés à partir des valeurs associées aux variables de l'ensemble $\mathcal{V}$.

Pour commencer, nous introduisons un ensemble d'expressions pour désigner un nombre complexe :

$$v_1, v_2 \in \mathcal{V}$$

$$\lambda \in \mathbb{R}$$
$$E_1, E_2, E \triangleq C(v_1, v_2) \mid \overline{E} \mid (\lambda . E) \mid (E_1 + E_2) \mid (E_1 \cdot E_2)$$

L'expression $C(v_1, v_2)$ représente le nombre complexe dont la première composante est la valeur de la variable v_1 et la seconde la valeur de la variable v_2 ; l'expression $\overline{E}$ représente le nombre complexe qui est le conjugué de celui représenté par l'expression E ; l'expression $(\lambda \cdot E)$ représente le nombre complexe qui est le produit (externe) entre le nombre réel λ et le nombre complexe qui est représenté par l'expression E ; l'expression $(E_1 + E_2)$ représente le nombre complexe qui est la somme des deux nombres complexes représentés par les expressions E_1 et E_2 ; enfin l'expression $(E_1 \cdot E_2)$ représente le nombre complexe qui est le produit entre les deux nombres complexes représentés par les expressions E_1 et E_2.

Question 1 *Définir la sémantique des expressions. Ce sera une fonction associant à un environnment de $\mathcal{V}$ dans $\mathcal{R}$ et à une expression un nombre complexe.*

Nous définissons l'ensemble I des intervalles de nombres réels positifs (c'est à dire l'ensemble des parties convexes de $\mathbb{R}^+$). Nous donnons maintenant la syntaxe de nos contraintes :

$$i \in I$$
$$c \triangleq P(v_1, v_2, i) \mid \mathit{fst}(\mathcal{V}, E) \mid \mathit{snd}(\mathcal{V}, E)$$

Nous distinguons en fait deux types de contraines :
- une contrainte de la forme $P(v_1, v_2, i)$ spécifie que le module du nombre complexe dont la première composante est la valeur de la variable v_1 et la seconde composante la valeur de la variable v_2, doit être compris dans l'intervalle i ;
- une contrainte de la forme $\mathit{fst}(\mathcal{V}, E)$ (resp. $\mathit{snd}(\mathcal{V}, E)$) spécifie que la valeur de la variable $\mathcal{V}$ est la première composante (resp. seconde composante) du nombre complexe qui est représenté par l'expression E.

Notre domaine concret D est l'ensemble des ensembles de fonctions de $\mathcal{V}$ vers $\mathbb{R}$, alors que notre domaine abstrait $D^\sharp$ est l'ensemble des ensembles de contraintes.

Question 2 *Définir une fonction de concrétisation γ qui associe à un ensemble de contraintes $e^\sharp$, l'ensemble des environnements de $\mathcal{V}$ dans $\mathbb{R}$ qui satisfont toutes ces contraintes.*

Nous ordonnons le domaine concret D par l'inclusion (des ensembles de fonctions de $\mathcal{V}$ vers $\mathbb{R}$) et le domaine abstrait par l'inclusion inverse [1] (sur les ensembles de contraintes).

Question 3 *Montrer que la fonction γ est croissante.*

3 Fonctions de transfert

Nous nous intéressons maintenant aux fonctions de transfert qui permettent de mimer dans l'abstrait le calcul des affectations.

La première étape est de proposer une primitive pour oublier une variable.

Question 4 *Proposer une définition inductive de l'ensemble des variables qui apparaissent dans une contrainte.*

Question 5 *Définir une fonction d'oubli, appelée forget, qui associe à un ensemble de contraintes $e^\sharp$ un autre ensemble de contraintes de sortes que :*

$$\{\rho[v \mapsto a] \mid \rho \in \gamma(e^\sharp), a \in \mathbb{R}\} \subseteq \gamma(\mathit{forget}_v(e^\sharp)).$$

1. L'inclusion inverse, $\supseteq$, est définie par l'équivalence $A \supseteq B \iff B \subseteq A$.

Nous pouvons maintenant définir les fonctions de transfert pour l'affectation. Nous considérons pour simplifier la conception du domaine abstrait que toute composante d'un nombre complexe est formée en une seule étape de calcul (ou une seule affectation) et que la sémantique du programme manipule des nombres réels.

Question 6 *Définir des fonctions de transfert :*

$$\begin{cases} scal \ : \ \mathcal{V} \times \mathbb{R} \times \mathcal{V} \times D^\sharp \to D^\sharp, \\ add \ : \ \mathcal{V} \times \mathcal{V} \times \mathcal{V} \times D^\sharp \to D^\sharp, \\ poly_{2+} \ : \ \mathcal{V} \times \mathcal{V} \times \mathcal{V} \times \mathcal{V} \times \mathcal{V} \times D^\sharp \to D^\sharp, \\ poly_{2-} \ : \ \mathcal{V} \times \mathcal{V} \times \mathcal{V} \times \mathcal{V} \times \mathcal{V} \times D^\sharp \to D^\sharp, \end{cases}$$

qui vérifient les contraintes de cohérence suivantes :

- $\{\rho[v \mapsto a{\cdot}\rho(v')] \mid \rho \in \gamma(e^\sharp), a \in \mathbb{R}\} \subseteq \gamma(scal(v, a, v', e^\sharp))$;
- $\{\rho[v \mapsto \rho(v_1) + \rho(v_2)] \mid \rho \in \gamma(e^\sharp)\} \subseteq \gamma(add(v, v_1, v_2, e^\sharp))$;
- $\{\rho[v \mapsto \rho(v_1) \cdot \rho(v_2) + \rho(v_3) \cdot \rho(v_4)] \mid \rho \in \gamma(e^\sharp)\} \subseteq \gamma(poly_{2+}(v, v_1, v_2, v_3, v_4, e^\sharp))$;
- $\{\rho[v \mapsto \rho(v_1) \cdot \rho(v_2) - \rho(v_3) \cdot \rho(v_4)] \mid \rho \in \gamma(e^\sharp)\} \subseteq \gamma(poly_{2-}(v, v_1, v_2, v_3, v_4, e^\sharp))$.

La précision des fonctions de transfert sera prise en compte dans le barème.

4 Réduction

Nous nous intéressons maintenant aux opérateurs de réduction. Nous distinguerons trois sortes de réduction.

Connaissant l'intervalle de variation de deux variables, il est possible de déduire un intervalle de variation pour le module du nombre complexe formé par la valeur de ces deux variables.

Question 7 *Proposer une primitive import-interv* $: \mathcal{V} \times I \times \mathcal{V} \times I \times D^\sharp \to D^\sharp$ *qui exploite les intervalles de variations des variables pour introduire de nouvelles contraintes. Cette primitive vérifiera la propriété suivante :*

$$\{\rho \mid \rho \in \gamma(e^\sharp),\ |\rho(v_1)| \in i_1,\ |\rho(v_2)| \in i_2\} \subseteq \gamma(\textit{import-interv}(v_1, i_1, v_2, i_2, e^\sharp)).$$

Réciproquement, connaissant l'intervalle de variation du module d'un nombre complexe, il est possible de déduire un intervalle de variation pour chacune de ses composantes.

Question 8 *Proposer une primitive export-interv* $: \mathcal{V} \times D^\sharp \to I$*, qui vérifiera la propriété suivante :*

$$\rho \in \gamma(e^\sharp) \Rightarrow |\rho(v)| \in \textit{export-interv}(v, e^\sharp).$$

Lorsque les deux composantes d'un nombre complexe sont connues, il est possible de former une nouvelle contrainte de type $P(v_1, v_2, I)$.

Question 9 *Proposer un opérateur de clôture inférieure combine sur* $(D^\sharp, \supseteq)$ *qui ajoute autant de contraintes de type* $P(v_1, v_2, I)$ *que possible, et qui vérifiera la propriété suivante :*

$$\gamma(e^\sharp) \subseteq \gamma(\textit{combine}(e^\sharp).$$

On veillera à ne pas insérer trop de contraintes inutiles.

5 Pour aller plus loin

Nous supposons désormais que l'évaluation des expressions se fait en arithmétique flottante. Pour simplifier, nous supposerons connue $\varepsilon(E, \rho)$ une borne sur les erreurs d'arrondis pour l'évaluation de toute expression E dans un environnement ρ.

Question 10 *Modifier le domaine abstrait, ses fonctions de transfert, et ses opérations de réduction en conséquence.*