语义等价与精化

定义与例子

```
Record eequiv (e1 e2: expr): Prop := {
  nrm_eequiv:
    ⟦ e1 ⟧.(nrm) == ⟦ e2 ⟧.(nrm);
  err_eequiv:
    ⟦ e1 ⟧.(err) == ⟦ e2 ⟧.(err);
}.
```

```
Record erefine (e1 e2: expr): Prop := {
  nrm_erefine:
    ⟦ e1 ⟧.(nrm) ⊆ ⟦ e2 ⟧.(nrm) ∪ (⟦ e2 ⟧.(err) × int64);
  err_erefine:
    ⟦ e1 ⟧.(err) ⊆ ⟦ e2 ⟧.(err);
}.
```

```
Record cequiv (c1 c2: com): Prop := {
  nrm_cequiv: ⟦ c1 ⟧.(nrm) == ⟦ c2 ⟧.(nrm);
  err_cequiv: ⟦ c1 ⟧.(err) == ⟦ c2 ⟧.(err);
  inf_cequiv: ⟦ c1 ⟧.(inf) == ⟦ c2 ⟧.(inf);
}.
```

```
Record crefine (c1 c2: com): Prop := {
  nrm_crefine:
    ⟦ c1 ⟧.(nrm) ⊆ ⟦ c2 ⟧.(nrm) ∪ (⟦ c2 ⟧.(err) × state);
  err_crefine:
    ⟦ c1 ⟧.(err) ⊆ ⟦ c2 ⟧.(err);
  inf_crefine:
    ⟦ c1 ⟧.(inf) ⊆ ⟦ c2 ⟧.(inf) ∪ ⟦ c2 ⟧.(err);
}.
```

精化的例子

```
Lemma const_plus_const_refine: forall n m: Z,
  EConst (n + m) <<= [[n + m]].
```

证明见 Coq 代码。

语义等价的例子

- **定理**： $c_1; (c_2; c_3) \equiv (c_1; c_2); c_3$。

语义等价的例子

- **定理**：$c_1;(c_2;c_3) \equiv (c_1;c_2);c_3$。
- **证明**：程序正常终止的情况

$$
\begin{aligned}
& [\![c_1;(c_2;c_3)]\!].\mathrm{nrm} \\
= \quad & [\![c_1]\!].\mathrm{nrm} \circ ([\![c_2]\!].\mathrm{nrm} \circ [\![c_3]\!].\mathrm{nrm}) \\
= \quad & ([\![c_1]\!].\mathrm{nrm} \circ [\![c_2]\!].\mathrm{nrm}) \circ [\![c_3]\!].\mathrm{nrm} \\
= \quad & [\![(c_1;c_2);c_3]\!].\mathrm{nrm}
\end{aligned}
$$

- **上面证明用到集合运算性质**：$A \circ (B \circ C) = (A \circ B) \circ C$。

语义等价的例子

- **定理**：$\text{if } (e) \text{ then}\{c_1\} \text{ else } \{c_2\}; c_3 \equiv \text{if } (e) \text{ then}\{c_1; c_3\} \text{ else } \{c_2; c_3\}$。

语义等价的例子

- **定理**：$\mathsf{if}\ (e)\ \mathsf{then}\{c_1\}\ \mathsf{else}\ \{c_2\}; c_3 \equiv \mathsf{if}\ (e)\ \mathsf{then}\{c_1; c_3\}\ \mathsf{else}\ \{c_2; c_3\}$。
- **证明**：程序正常终止的情况

$$
\begin{aligned}
& [\![\mathsf{if}\ (e)\ \mathsf{then}\{c_1\}\ \mathsf{else}\ \{c_2\}; c_3]\!].\mathrm{nrm} \\
= \quad & (\mathsf{test\_true}([\![e]\!]) \circ [\![c_1]\!].\mathrm{nrm} \cup \mathsf{test\_false}([\![e]\!]) \circ [\![c_2]\!].\mathrm{nrm}) \circ \\
& [\![c_3]\!].\mathrm{nrm} \\
= \quad & \mathsf{test\_true}([\![e]\!]) \circ [\![c_1]\!].\mathrm{nrm} \circ [\![c_3]\!].\mathrm{nrm} \cup \\
& \mathsf{test\_false}([\![e]\!]) \circ [\![c_2]\!].\mathrm{nrm} \circ [\![c_3]\!].\mathrm{nrm} \\
= \quad & [\![\mathsf{if}\ (e)\ \mathsf{then}\{c_1; c_3\}\ \mathsf{else}\ \{c_2; c_3\}]\!].\mathrm{nrm}
\end{aligned}
$$

- **上面证明用到集合运算性质**：$(A \cup B) \circ C = (A \circ C) \cup (B \circ C)$。

语义等价于精化的性质

语义等价关系是一种等价关系

- 对于任意表达式 E, $E \equiv E$。

语义等价关系是一种等价关系

- 对于任意表达式 E, $E \equiv E$。
- 证明：
  - 求值成功的情况：$[\![E]\!].\mathrm{nrm} = [\![E]\!].\mathrm{nrm}$ （集合相等的自反性）；
  - 求值失败的情况：$[\![E]\!].\mathrm{err} = [\![E]\!].\mathrm{err}$ （集合相等的自反性）；

语义等价关系是一种等价关系

- 对于任意表达式 E, $E \equiv E$。
- 证明：
  - 求值成功的情况：$[\![E]\!].\mathrm{nrm} = [\![E]\!].\mathrm{nrm}$ （集合相等的自反性）；
  - 求值失败的情况：$[\![E]\!].\mathrm{err} = [\![E]\!].\mathrm{err}$ （集合相等的自反性）；
- 对于任意表达式 E_1 与 E_2，如果 $E_1 \equiv E_2$，那么 $E_2 \equiv E_1$。

语义等价关系是一种等价关系

- 对于任意表达式 E, $E \equiv E$。
- 证明：
  - 求值成功的情况：$[\![E]\!].\mathrm{nrm} = [\![E]\!].\mathrm{nrm}$ （集合相等的自反性）；
  - 求值失败的情况：$[\![E]\!].\mathrm{err} = [\![E]\!].\mathrm{err}$ （集合相等的自反性）；
- 对于任意表达式 E_1 与 E_2，如果 $E_1 \equiv E_2$，那么 $E_2 \equiv E_1$。
- 证明：
  - 求值成功的情况：由 $E_1 \equiv E_2$ 这一假设可知 $[\![E_1]\!].\mathrm{nrm} = [\![E_2]\!].\mathrm{nrm}$，故 $[\![E_2]\!].\mathrm{nrm} = [\![E_1]\!].\mathrm{nrm}$ （集合相等的对称性）。
  - 求值失败的情况：由 $E_1 \equiv E_2$ 这一假设可知 $[\![E_1]\!].\mathrm{err} = [\![E_2]\!].\mathrm{err}$，故 $[\![E_2]\!].\mathrm{err} = [\![E_1]\!].\mathrm{err}$ （集合相等的对称性）。

语义等价关系是一种等价关系

- 对于任意表达式 E_1，E_2 与 E_3，如果 $E_1 \equiv E_2$ 且 $E_2 \equiv E_3$，那么 $E_1 \equiv E_3$。

语义等价关系是一种等价关系

- 对于任意表达式 E_1，E_2 与 E_3，如果 $E_1 \equiv E_2$ 且 $E_2 \equiv E_3$，那么 $E_1 \equiv E_3$。
- 证明：
  - 求值成功的情况：由 $E_1 \equiv E_2$ 与 $E_2 \equiv E_3$ 这两条假设可知 $[\![E_1]\!].\mathrm{nrm} = [\![E_2]\!].\mathrm{nrm}$ 并且 $[\![E_2]\!].\mathrm{nrm} = [\![E_3]\!].\mathrm{nrm}$，故 $[\![E_1]\!].\mathrm{nrm} = [\![E_3]\!].\mathrm{nrm}$（集合相等的传递性）。
  - 求值失败的情况：由 $E_1 \equiv E_2$ 与 $E_2 \equiv E_3$ 这两条假设可知 $[\![E_1]\!].\mathrm{err} = [\![E_2]\!].\mathrm{err}$ 并且 $[\![E_2]\!].\mathrm{err} = [\![E_3]\!].\mathrm{err}$，故 $[\![E_1]\!].\mathrm{err} = [\![E_3]\!].\mathrm{err}$（集合相等的传递性）。

语义等价关系是一种等价关系

- 对于任意表达式 E_1，E_2 与 E_3，如果 $E_1 \equiv E_2$ 且 $E_2 \equiv E_3$，那么 $E_1 \equiv E_3$。
- 证明：
  - 求值成功的情况：由 $E_1 \equiv E_2$ 与 $E_2 \equiv E_3$ 这两条假设可知 $[\![E_1]\!].\mathrm{nrm} = [\![E_2]\!].\mathrm{nrm}$ 并且 $[\![E_2]\!].\mathrm{nrm} = [\![E_3]\!].\mathrm{nrm}$，故 $[\![E_1]\!].\mathrm{nrm} = [\![E_3]\!].\mathrm{nrm}$（集合相等的传递性）。
  - 求值失败的情况：由 $E_1 \equiv E_2$ 与 $E_2 \equiv E_3$ 这两条假设可知 $[\![E_1]\!].\mathrm{err} = [\![E_2]\!].\mathrm{err}$ 并且 $[\![E_2]\!].\mathrm{err} = [\![E_3]\!].\mathrm{err}$，故 $[\![E_1]\!].\mathrm{err} = [\![E_3]\!].\mathrm{err}$（集合相等的传递性）。

请看 Coq 证明演示