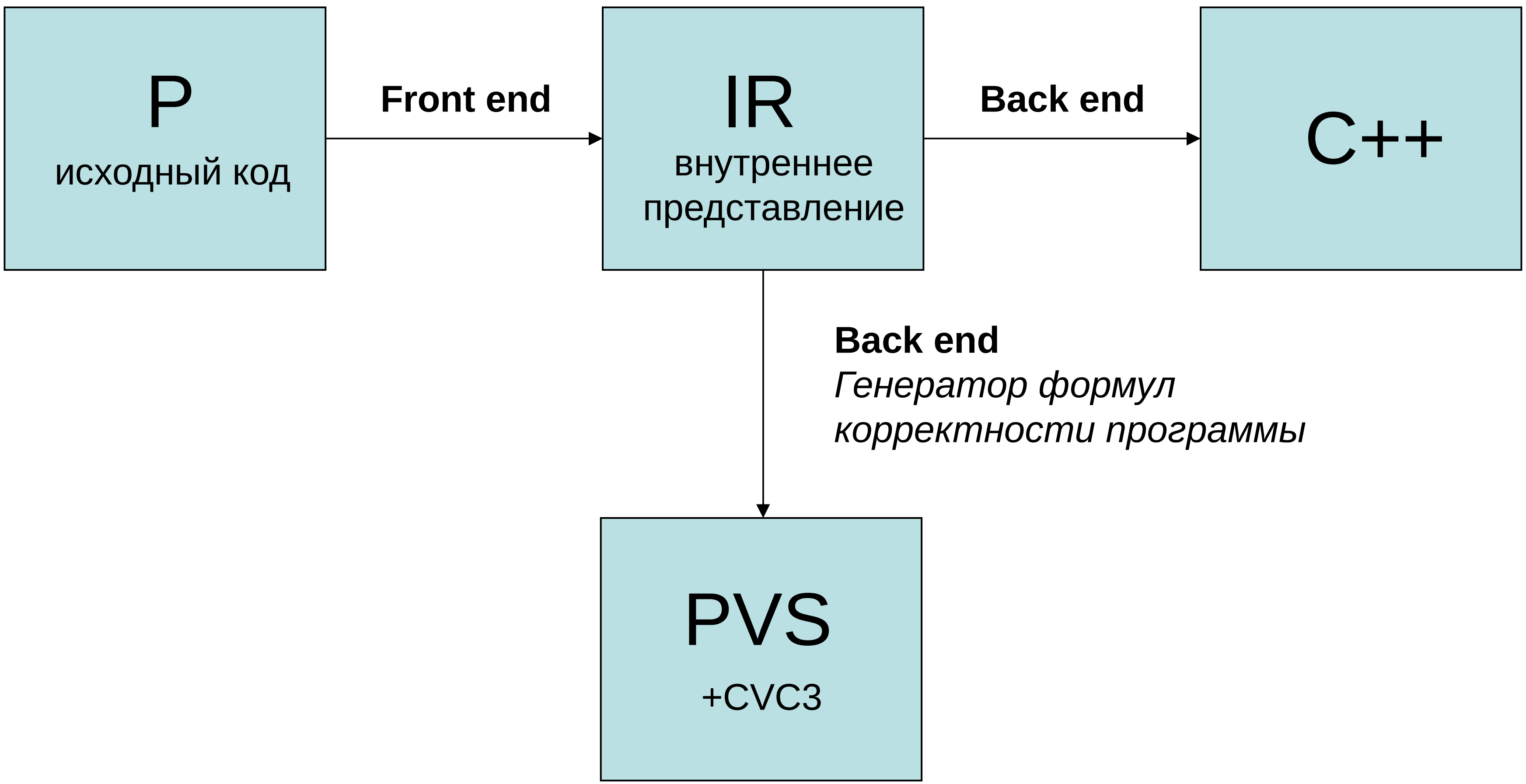
Генерация условий корректности предикатных программ с взаимной рекурсией

Чушкин М.С
ИСИ СО РАН, Новосибирск

Система предикатного программирования



Определение предиката

- A(x: y) **pre** P(x) { S(x: y) } **post** Q(x, y)
- A – имя предиката
- S(x: y) – *оператор*
  - x, y – наборы переменных, аргументы и результаты
- *Спецификация* предиката A(x: y)
  - P(x) – предусловие
  - Q(x, y) – постусловие

Пример определения предиката

```
НОД(nat a, b : nat c)
pre a >= 1 & b >= 1
{
    if (a = b)
          c = a
    else if (a < b)
          НОД(a, b - a : c)
    else
          НОД(a - b, b : c)
}
post gcd(c, a, b)
measure a + b;
```

Классические методы

- Метод Флойда
  - “Assigning meanings to programs”, 1967
- Метод Хоара
  - “An axiomatic basis for computer programming”, 1969

Понятие логики

- *Логика оператора* S(x: y)
  - *сильнейший предикат, истинный при завершении исполнения оператора S(x: y)*

- Примеры:
  - $L(a := E(x)) \cong R(x) \,\&\, a = E(x)$
  - $L(B(x\mathbf{:}\ z);\ C(z\mathbf{:}\ y)) \cong \exists z.\ L(B(x\mathbf{:}\ z)) \,\&\, L(C(z\mathbf{:}\ y))$

Понятие корректности

- *Корректность оператора* S(x: y)
  - $P(x)\ \&\ L(S(x:y)) \Rightarrow Q(x, y)$
    - условие частичной корректности
  - $P(x) \Rightarrow \exists y.\ L(S(x:y))$
    - условие завершения оператора

- Corr(S, P, Q)(x) =

$$P(x) \Rightarrow [\ L(S(x:y)) \Rightarrow Q(x, y)\ ]\ \&\ \exists y.\ L(S(x:y))$$

Корректность рекурсивного предиката

- Схема индукции:

$$\frac{(\forall u \in X\ m(u) < m(t) \Rightarrow W\ (u)) \Rightarrow W\ (t)}{W(x)}$$

  - W – произвольное утверждение
  - m – функция мера
- Корректность рекурсивного предиката

$$\frac{Induct(A, P, Q)(t) \Rightarrow Corr(A, P, Q)(t)}{Corr(A, P, Q)(x)}$$

  - $Induct(A, P, Q)(t) \equiv \forall u\ (m(u) < m(t) \Rightarrow Corr(A, P, Q)(u))$

Корректность рекурсивной программы

- Рекурсивная программа

$A_i(X_i\ x_i\text{: } Y_i\ y_i)$ **pre** $P_i(x_i)$ { $S_i(x_i\text{: } y_i)$ } **post** $Q_i(x_i, y_i)$ **measure** $m_i(x_i)$;

  - $i = 1, ..., N$;
  - в телах $S_i(x_i\text{: } y_i)$ могут встречаться вызовы предикатов $A_1, ..., A_N$

- Корректность рекурсивной программы
  - $\forall t_1, ..., t_N$ $\mathrm{Induct}(A_1, P_1, Q_1)(t_1) \wedge ... \wedge \mathrm{Induct}(A_N, P_N, Q_N)(t_N)$
    $\Rightarrow \mathrm{Corr}(A_1, P_1, Q_1)(t_1) \wedge ... \wedge \mathrm{Corr}(A_N, P_N, Q_N)(t_N)$
  - $\mathrm{Induct}(A_k, P_k, Q_k)(t_k)$

    $\equiv F(t_k\text{: } t'_k) \wedge m(t'_k) < m(t_k) \Rightarrow \mathrm{Corr}(A_k, P_k, Q_k)(t'_k)$

Построение связующих формул

- *Связующая формула $F(x_k: x'_k)$*
  - *Формула, выражающая произвольные фактические параметры x'_k пердиката A_k через его формальные параемтры x_k*
- Метод построения связующих формул
  - $A_k(x_k: x'_k)$
  - $\{ F_r : x_r \rightarrow x'_k \mid r = 1, ..., N \}$
  - F_k - искомая

Примеры правил вывода

Условный оператор:

$$\frac{\mathrm{Corr}(B,\ P \ \&\ E,\ Q)(x); \quad \mathrm{Corr}(C,\ P \ \&\ \neg E,\ Q)(x)}{\mathrm{Corr}(\mathbf{if}\ (E)\ B(x\!:\ y)\ \mathbf{else}\ C(x\!:\ y),\ P,\ Q)(x)}$$

Оператор суперпозиции:

$$\frac{P(x) \Rightarrow \exists z.\ L(B(x\!:\ z)); \quad \mathrm{Corr}(C,\ P \ \&\ L(B(x\!:\ z)),\ Q)(x)}{\mathrm{Corr}(B(x\!:\ z);\ C(z\!:\ y),\ P,\ Q)(x)}$$

Генерация условий корректности

- **Шаг 1.** Преобразование предиката
  - a = E – оператор присваивания
  - A(x: z); B(z: y) – оператор суперпозиции
  - A(x: y) || B(x: y) – параллельный оператор
  - a, b = 1, 2 – групповой оператор присваивания
  - **if** (E) A(x: y) **else** B(x: y) – условный оператор
  - **switch**(…) … – оператор выбора
  - foo(u: v) – оператор вызова

- **Шаг 2.** Вывод условий корректности

  Правило вывода:

$$\frac{\Gamma_1;\ \Gamma_2;\ \dots\ \Gamma_n}{F}$$

  - Γ_i – посылки
  - F – заключение

  Виды посылок:

  - A ⇒ B – формула
  - Corr(S, P, Q)(x)

- **Шаг 2.1.** Вывод формул
  - A → B – формула
    - A, B – конъюнкции
    - Могут содержать логику L(S(x: y))
  - Группы правил
    - Правила для общего случая (**Q**)
    - Правила для корректных подоператоров (**R**)

- **Шаг 2.2.** Декомпозиция $L(S(x: y))$
  - $A \;\&\; L(S(x: y)) \Rightarrow B$
    - Вхождение логики в левой части (**FL**)
  - $A \Rightarrow L(S(x: y))$
    - Вхождение логики в правой части (**F**)
  - $A \Rightarrow \exists y\, L(S(x: y))$
    - Вхождение квантора существования (**E**)

Корректность алгоритма

- Допустимость правил

    Частично доказана

    http://www.iis.nsk.su/persons/vshel/f iles/rules.zip

- Корректность реализации

    Проверялась тестированием

Пример

```
// Formulas
formula P(nat a, b) = a >= 1 & b >= 1;
formula Q(nat a, b, c) = gcd(c, a, b);
formula m(nat a, b : nat) = a + b;

// Lemmas
lemma forall nat a, b. P(a, b) & a = b => exists nat c. c = a;
lemma forall nat a, b, c. P(a, b) & a = b & c = a => Q(a, b, c);
lemma forall nat a, b. P(a, b) & a != b & a < b
                              => m(a, b - a) < m(a, b) & P(a, b - a);
lemma forall nat a, b. P(a, b) & a != b & a >= b
                              => m(a - b, b) < m(a, b) & P(a - b, b);
```

Заключение

- Результаты
  - Разработан метод дедуктивной верификации предикатных программ с произвольной рекурсией;
  - Реализован генератор формул корректности в системе предикатного программирования
- Дальнейшие планы
  - Разработать правила для оставшихся конструкций языка **P**