Extending Probability Generating Function Semantics to Negative Variable Valuations

Bachelor Colloquium

Simon Feiden

12.04.2016

Probabilistic Programs

- Different output on same input
- Probabilistic operations
- Solve hard problems faster
- Mathematical model to prove usefulness

Formal Power Series

- $G = a_0X^0 + a_1X^1 + a_2X^2 + \ldots = \sum_{i=0}^{\infty} a_iX^i$

Formal Power Series

- $G = a_0 X^0 + a_1 X^1 + a_2 X^2 + \ldots = \sum_{i=0}^{\infty} a_i X^i$

Formal Power Series

- $G = a_0 X^0 + a_1 X^1 + a_2 X^2 + \ldots = \sum_{i=0}^{\infty} a_i X^i$

Formal Power Series

- $G = a_0X^0 + a_1X^1 + a_2X^2 + \ldots = \sum_{i=0}^{\infty} a_iX^i$
- $4X^2 + 9X^7$

Formal Power Series

- $G = a_0X^0 + a_1X^1 + a_2X^2 + \ldots = \sum_{i=0}^{\infty} a_iX^i$
- $4X^2 + 9X^7$
- $\sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i X^i$

Formal Power Series

- $G = a_0X^0 + a_1X^1 + a_2X^2 + \ldots = \sum_{i=0}^{\infty} a_iX^i$
- $4X^2 + 9X^7$
- $\sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i X^i = \frac{1}{1-\frac{1}{2}X}$

Formal Power Series

- $G = a_0 X^0 + a_1 X^1 + a_2 X^2 + \ldots = \sum_{i=0}^{\infty} a_i X^i$
- $4X^2 + 9X^7$
- $\sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i X^i = \frac{1}{1 - \frac{1}{2}X}$
- Multivariate FPS: $\sum_{s \in \mathbb{N}^k} \mu_s X_1^{s_1} \cdots X_k^{s_k}$

Operations on FPS

- Let $G = \sum_{i=0}^{\infty} a_i X^i$

Operations on FPS

- Let $G = \sum_{i=0}^{\infty} a_i X^i$ and $F = \sum_{i=0}^{\infty} b_i X^i$.

Operations on FPS

- Let $G = \sum_{i=0}^{\infty} a_i X^i$ and $F = \sum_{i=0}^{\infty} b_i X^i$.
- $G + F = \sum_{i=0}^{\infty} (a_i + b_i) X^i$

Operations on FPS

- Let $G = \sum_{i=0}^{\infty} a_i X^i$ and $F = \sum_{i=0}^{\infty} b_i X^i$.
- $G + F = \sum_{i=0}^{\infty} (a_i + b_i) X^i$
- $\alpha \cdot G = \sum_{i=0}^{\infty} (\alpha \cdot a_i) X^i$

Operations on FPS

- Let $G = \sum_{i=0}^{\infty} a_i X^i$ and $F = \sum_{i=0}^{\infty} b_i X^i$.
- $G + F = \sum_{i=0}^{\infty} (a_i + b_i) X^i$
- $\alpha \cdot G = \sum_{i=0}^{\infty} (\alpha \cdot a_i) X^i$
- $|G| = \sum_{i=0}^{\infty} a_i$

Operations on FPS

- Let $G = \sum_{i=0}^{\infty} a_i X^i$ and $F = \sum_{i=0}^{\infty} b_i X^i$.
- $G + F = \sum_{i=0}^{\infty} (a_i + b_i) X^i$
- $\alpha \cdot G = \sum_{i=0}^{\infty} (\alpha \cdot a_i) X^i$
- $|G| = \sum_{i=0}^{\infty} a_i$
- Analogous for multivariate FPS

PGFs and Programs

- $G = 0.4X^1Y^0 + 0.6X^4Y^4$

PGFs and Programs

- $G = 0.4X^1Y^0 + 0.6X^4Y^4$

PGFs and Programs

- $G = \color{red}{0.4}X^1 Y^0 + 0.6X^4 Y^4$

PGFs and Programs

- $G = 0.4X^1Y^0 + 0.6X^4Y^4$

PGFs and Programs

- $G = 0.4X^1Y^0 + 0.6X^4Y^4$

PGFs and Programs

- $G = 0.4X^1Y^0 + 0.6X^4Y^4$
- *skip*
- *diverge*
- $X := e$

PGFs and Programs

- $G = 0.4X^1Y^0 + 0.6X^4Y^4$
- *skip*
- *diverge*
- $X := e$
- $P_1; P_2$
- $\mathit{if}(B)\{\ P_1\ \}\ \mathit{else}\{\ P_2\ \}$
- $\{P_1\}[p]\{P_2\}$
- $\mathit{while}(B)\{P\}$

Challenges

- Extension to negative variable valuations

Challenges

- Extension to negative variable valuations
- Use formal power series

Challenges

- Extension to negative variable valuations
- Use formal power series
- Usage of closed forms (requires a ring)

Extended PGFs

- $\sum_{s \in \mathbb{N}^k} \mu_s X_1^{s_1} \cdots X_k^{s_k}$

Extended PGFs

- $\sum_{s \in \mathbb{N}^k} \mu_s X_1^{s_1} \cdots X_k^{s_k}$

Extended PGFs

- $\sum_{s \in \mathbb{N}^k} \mu_s X_1^{s_1} \cdots X_k^{s_k}$

- $\sum_{s \in \mathbb{Z}^k} \mu_s X_1^{s_1} \cdots X_k^{s_k}$

Extended PGFs

- $\sum_{s \in \mathbb{N}^k} \mu_s X_1^{s_1} \cdots X_k^{s_k}$
- $\sum_{s \in \mathbb{Z}^k} \mu_s X_1^{s_1} \cdots X_k^{s_k}$
- No ring, no closed forms.

Extended PGFs

- $\sum_{s \in \mathbb{N}^k} \mu_s X_1^{s_1} \cdots X_k^{s_k}$
- $\sum_{s \in \mathbb{Z}^k} \mu_s X_1^{s_1} \cdots X_k^{s_k}$
- No ring, no closed forms.
- Solution: Use PGFs for partitions of the state space.

Partitions

- One variable X

Partitions

- One variable X
- State space is $\mathbb{Z}$.

Partitions

- One variable X
- State space is $\mathbb{Z}$.
- Partitions are
  $\mathbb{N}$
  $-\mathbb{N}_{>0}$

Partitions

- One variable X
- State space is $\mathbb{Z}$.
- Partitions are

  $\mathbb{N}$

  $-\mathbb{N}_{>0}$

- Two variables X, Y

Partitions

- One variable X
- State space is $\mathbb{Z}$.
- Partitions are

  $\mathbb{N}$

  $-\mathbb{N}_{>0}$

- Two variables X, Y
- State space is $\mathbb{Z}^2$.

Partitions

- One variable X
- State space is $\mathbb{Z}$.
- Partitions are
  $$\begin{array}{c} \mathbb{N} \\ -\mathbb{N}_{>0} \end{array}$$

- Two variables X, Y
- State space is $\mathbb{Z}^2$.
- Partitions are
  $$\begin{array}{ccc} \mathbb{N} & \times & \mathbb{N} \\ -\mathbb{N}_{>0} & \times & \mathbb{N} \\ \mathbb{N} & \times & -\mathbb{N}_{>0} \\ -\mathbb{N}_{>0} & \times & -\mathbb{N}_{>0} \end{array}$$

Partitions

- $S_1, S_2, \ldots, S_{2^k}$

Partitions

- $S_1, S_2, \ldots, S_{2^k}$
- $\sum_{s \in S_1} \mu_s X_1^{s_1} \cdots X_k^{s_k},$

Partitions

- $S_1, S_2, \ldots, S_{2^k}$
- $\sum_{s \in S_1} \mu_s X_1^{s_1} \cdots X_k^{s_k}$,

  $\sum_{s \in S_2} \mu_s X_1^{s_1} \cdots X_k^{s_k}$,

Partitions

- $S_1, S_2, \ldots, S_{2^k}$
- $$\sum_{s \in S_1} \mu_s X_1^{s_1} \cdots X_k^{s_k},$$
  $$\sum_{s \in S_2} \mu_s X_1^{s_1} \cdots X_k^{s_k},$$
  $$\vdots$$
  $$\sum_{s \in S_{2k}} \mu_s X_1^{s_1} \cdots X_k^{s_k}$$

Semantic Tuples

Definition (Semantic Tuple)

Let P be a program of k variables. A *semantic tuple* T_G is an object of the form

$$T_G = \left(\sum_{s \in S_1} \mu_s X_1^{s_1} \cdots X_k^{s_k}, \ldots, \sum_{s \in S_{2^k}} \mu_s X_1^{s_1} \cdots X_k^{s_k} \right)$$

Semantic Tuples

Definition (Semantic Tuple)

Let P be a program of k variables. A *semantic tuple* T_G is an object of the form

$$T_G = \left(\sum_{s \in S_1} \mu_s X_1^{s_1} \cdots X_k^{s_k}, \ldots, \sum_{s \in S_{2^k}} \mu_s X_1^{s_1} \cdots X_k^{s_k} \right)$$

- Number of entries grows exponentially.

Semantic Tuples

Definition (Semantic Tuple)

Let P be a program of k variables. A *semantic tuple* T_G is an object of the form

$$T_G = \left(\sum_{s \in S_1} \mu_s X_1^{s_1} \cdots X_k^{s_k}, \ldots, \sum_{s \in S_{2^k}} \mu_s X_1^{s_1} \cdots X_k^{s_k} \right)$$

- Number of entries grows exponentially.
- Use extended PGFs: $\sum_{s \in \mathbb{Z}^k} \mu_s X_1^{s_1} \cdots X_k^{s_k}$

PGF Semantics

- $[\![skip]\!](G) = G$

PGF Semantics

- $[\![skip]\!] (G) = G$
- $[\![diverge]\!] (G) = 0$

PGF Semantics

- $[\![skip]\!]\,(G) = G$
- $[\![diverge]\!]\,(G) = 0$
- $[\![X_j := e]\!]\,(G) = \sum_{s \in \mathbb{Z}^k} \mu_s X_1^{s_1} \cdots X_j^{e(s)} \cdots X_k^{s_k}$

PGF Semantics

- $\llbracket skip \rrbracket (G) = G$
- $\llbracket diverge \rrbracket (G) = 0$
- $\llbracket X_j := e \rrbracket (G) = \sum_{s \in \mathbb{Z}^k} \mu_s X_1^{s_1} \cdots X_j^{e(s)} \cdots X_k^{s_k}$

PGF Semantics

- $[\![skip]\!]\,(G) = G$
- $[\![diverge]\!]\,(G) = 0$
- $[\![X_j := e]\!]\,(G) = \sum_{s\in\mathbb{Z}^k} \mu_s X_1^{s_1} \cdots X_j^{e(s)} \cdots X_k^{s_k}$
- $\langle G \rangle_B = \sum_{s\in\mathbb{Z}^k} \begin{cases} \mu_s X_1^{s_1} \cdots X_k^{s_k} & \text{if } s \models B \\ 0 & \text{otherwise} \end{cases}$

PGF Semantics

- $[\![skip]\!] (G) = G$
- $[\![diverge]\!] (G) = 0$
- $[\![X_j := e]\!] (G) = \sum_{s \in \mathbb{Z}^k} \mu_s X_1^{s_1} \cdots X_j^{e(s)} \cdots X_k^{s_k}$
- $\langle G \rangle_B = \sum_{s \in \mathbb{Z}^k} \begin{cases} \mu_s X_1^{s_1} \cdots X_k^{s_k} & \text{if } s \models B \\ 0 & \text{otherwise} \end{cases}$
- $\left\langle 0.4 X^1 Y^0 + 0.6 X^4 Y^4 \right\rangle_{X=1} = 0.4 X^1 Y^0$

PGF Semantics

- $[\![P_1; P_2]\!]\,(G) = [\![P_2]\!]\,([\![P_1]\!]\,(G))$

PGF Semantics

- $\llbracket P_1; P_2 \rrbracket (G) = \llbracket P_2 \rrbracket (\llbracket P_1 \rrbracket (G))$
- $\llbracket \{P_1\}[p]\{P_2\} \rrbracket (G) = p \cdot \llbracket P_1 \rrbracket (G) + (1 - p) \cdot \llbracket P_2 \rrbracket (G)$

PGF Semantics

- $\llbracket P_1; P_2 \rrbracket (G) = \llbracket P_2 \rrbracket (\llbracket P_1 \rrbracket (G))$
- $\llbracket \{P_1\}[p]\{P_2\} \rrbracket (G) = p \cdot \llbracket P_1 \rrbracket (G) + (1 - p) \cdot \llbracket P_2 \rrbracket (G)$
- $\llbracket if(B)\,\{\,P_1\,\}\,else\,\{\,P_2\,\} \rrbracket (G) = \llbracket P_1 \rrbracket (\langle G \rangle_B) + \llbracket P_2 \rrbracket (\langle G \rangle_{\neg B})$

PGF Semantics

- $\llbracket P_1; P_2 \rrbracket (G) = \llbracket P_2 \rrbracket (\llbracket P_1 \rrbracket (G))$
- $\llbracket \{P_1\}[p]\{P_2\} \rrbracket (G) = p \cdot \llbracket P_1 \rrbracket (G) + (1 - p) \cdot \llbracket P_2 \rrbracket (G)$
- $\llbracket \mathit{if}(B)\,\{\, P_1 \,\}\, \mathit{else}\,\{\, P_2 \,\} \rrbracket (G) = \llbracket P_1 \rrbracket (\langle G \rangle_B) + \llbracket P_2 \rrbracket (\langle G \rangle_{\neg B})$
- $\llbracket \mathit{while}(B)\{P\} \rrbracket (G)$

Loop semantics

- $\mathrm{wh}_{B,P}(G) = \llbracket P \rrbracket \left(\langle G \rangle_B \right)$

Loop semantics

- $\mathrm{wh}_{B,P}(G) = [\![P]\!]\,(\langle G\rangle_B)$
- $\mathrm{wh}^{n}_{B,P}(G)$ is the nth loop iteration.

Loop semantics

- $\mathrm{wh}_{B,P}(G) = [\![P]\!]\left(\langle G\rangle_B\right)$
- $\mathrm{wh}^n_{B,P}(G)$ is the nth loop iteration.
- $\left\langle \mathrm{wh}^n_{B,P}(G)\right\rangle_{\neg B}$ drops out after n iterations.

Loop semantics

- $\mathrm{wh}_{B,P}(G) = [\![P]\!]\left(\langle G\rangle_B\right)$
- $\mathrm{wh}^n_{B,P}(G)$ is the nth loop iteration.
- $\left\langle \mathrm{wh}^n_{B,P}(G)\right\rangle_{\neg B}$ drops out after n iterations.
- $[\![\mathit{while}(B)\{P\}]\!](G) = \sum_{i=0}^{\infty} \left\langle \mathrm{wh}^i_{B,P}(G)\right\rangle_{\neg B}$

Canonical Example

```
while ( F = 0 ) {
  { X := X - 1 }[0.5]{ F := 1 }
}
```

Canonical Example

```
while ( F = 0 ) {
  { X := X - 1 }[0.5]{ F := 1 }
}
```

- $[\![while(B)\{P\}]\!](G) = \sum_{i=0}^{\infty} \left\langle \mathrm{wh}^{i}_{B,P}(G) \right\rangle_{\neg B}$

Canonical Example

```
while ( F = 0 ) {
  { X := X - 1 }[0.5]{ F := 1 }
}
```

- $[\![\mathit{while}(B)\{P\}]\!](G) = \sum_{i=0}^{\infty} \left\langle \mathrm{wh}^{i}_{B,P}(G) \right\rangle_{\neg B}$

Canonical Example

```
while ( F = 0 ) {
  { X := X - 1 }[0.5]{ F := 1 }
}
```

- $[\![\mathit{while}(B)\{P\}]\!](G) = \sum_{i=0}^{\infty} \left\langle \mathrm{wh}^{i}_{B,P}(G) \right\rangle_{\neg B}$
- $B = (F = 0)$

Canonical Example

```
while ( F = 0 ) {
  { X := X - 1 }[0.5]{ F := 1 }
}
```

- $[\![while(B)\{P\}]\!](G) = \sum_{i=0}^{\infty} \left\langle \mathrm{wh}^{i}_{B,P}(G) \right\rangle_{\neg B}$
- $B = (F = 0)$
- $P = \{X := X - 1\}[0.5]\{F := 1\}$

Canonical Example

```
while ( F = 0 ) {
  { X := X - 1 }[0.5]{ F := 1 }
}
```

- $\llbracket while(B)\{P\} \rrbracket (G) = \sum_{i=0}^{\infty} \left\langle \mathrm{wh}^{i}_{B,P}(G) \right\rangle_{\neg B}$
- $B = (F = 0)$
- $P = \{X := X - 1\}[0.5]\{F := 1\}$
- $G = 1X^0F^0 = 1$

Canonical Example

- $\left\langle \mathsf{wh}^{1}_{B,P}(1) \right\rangle_{\neg B} = \frac{1}{2} X^{0} F^{1}$

Canonical Example

- $\left\langle \mathrm{wh}^{1}_{B,P}(1) \right\rangle_{\neg B} = \frac{1}{2} X^{0} F^{1}$
- $\left\langle \mathrm{wh}^{2}_{B,P}(1) \right\rangle_{\neg B} = \frac{1}{4} X^{-1} F^{1}$

Canonical Example

- $\left\langle \mathrm{wh}^1_{B,P}(1) \right\rangle_{\neg B} = \frac{1}{2} X^0 F^1$
- $\left\langle \mathrm{wh}^2_{B,P}(1) \right\rangle_{\neg B} = \frac{1}{4} X^{-1} F^1$
- $\left\langle \mathrm{wh}^n_{B,P}(1) \right\rangle_{\neg B} = \left(\frac{1}{2}\right)^n X^{-(n-1)} F^1$

Canonical Example

- $\left\langle \mathrm{wh}^{1}_{B,P}(1) \right\rangle_{\neg B} = \frac{1}{2} X^{0} F^{1}$
- $\left\langle \mathrm{wh}^{2}_{B,P}(1) \right\rangle_{\neg B} = \frac{1}{4} X^{-1} F^{1}$
- $\left\langle \mathrm{wh}^{n}_{B,P}(1) \right\rangle_{\neg B} = \left(\frac{1}{2}\right)^{n} X^{-(n-1)} F^{1}$
- $\sum_{i=0}^{\infty} \left\langle \mathrm{wh}^{i}_{B,P}(G) \right\rangle_{\neg B} = \frac{1}{2} \cdot \sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^{i} X^{-i} F^{1}$

Canonical Example

- $\left\langle \mathrm{wh}^1_{B,P}(1) \right\rangle_{\neg B} = \frac{1}{2} X^0 F^1$
- $\left\langle \mathrm{wh}^2_{B,P}(1) \right\rangle_{\neg B} = \frac{1}{4} X^{-1} F^1$
- $\left\langle \mathrm{wh}^n_{B,P}(1) \right\rangle_{\neg B} = \left(\frac{1}{2}\right)^n X^{-(n-1)} F^1$
- $\sum_{i=0}^{\infty} \left\langle \mathrm{wh}^i_{B,P}(G) \right\rangle_{\neg B} = \frac{1}{2} \cdot \sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i X^{-i} F^1$
- Closed form: $\frac{F}{2-X^{-1}}$

Canonical Example

- $\left\langle \mathrm{wh}^1_{B,P}(1) \right\rangle_{\neg B} = \frac{1}{2} X^0 F^1$
- $\left\langle \mathrm{wh}^2_{B,P}(1) \right\rangle_{\neg B} = \frac{1}{4} X^{-1} F^1$
- $\left\langle \mathrm{wh}^n_{B,P}(1) \right\rangle_{\neg B} = \left(\frac{1}{2}\right)^n X^{-(n-1)} F^1$
- $\sum_{i=0}^{\infty} \left\langle \mathrm{wh}^i_{B,P}(G) \right\rangle_{\neg B} = \frac{1}{2} \cdot \sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i X^{-i} F^1$
- Closed form: $\frac{F}{2-X^{-1}}$
- Actually: $\left(0, \frac{F}{2-X^{-1}}, 0, 0\right)$

Termination Probability

```
while ( F = 0 ) {
  {
    { X := X + 1 }[0.5]{ diverge }
  }[0.5]{
    F := 1
  }
}
```

Termination Probability

```
while ( F = 0 ) {
  {
    { X := X + 1 }[0.5]{ diverge }
  }[0.5]{
    F := 1
  }
}
```

- $\left\langle \mathrm{wh}^{i}_{B,P}(G) \right\rangle_{\neg B} = \frac{1}{2} \cdot \left(\frac{1}{4}\right)^{i-1} X^{i-1} F^{1}$

Termination Probability

```
while ( F = 0 ) {
  {
    { X := X + 1 }[0.5]{ diverge }
  }[0.5]{
    F := 1
  }
}
```

- $\left\langle \mathrm{wh}^{i}_{B,P}(G) \right\rangle_{\neg B} = \frac{1}{2} \cdot \left(\frac{1}{4}\right)^{i-1} X^{i-1} F^{1}$
- $\sum_{i=0}^{\infty} \left\langle \mathrm{wh}^{i}_{B,P}(G) \right\rangle_{\neg B} = \frac{1}{2} \cdot \sum_{i=0}^{\infty} \left(\frac{1}{4}\right)^{i} X^{i} F^{1}$

Termination Probability

- Closed form: $\frac{F}{2-\frac{1}{2}X}$

Termination Probability

- Closed form: $\frac{F}{2-\frac{1}{2}X}$
- Termination probability using absolute value:

Termination Probability

- Closed form: $\frac{F}{2-\frac{1}{2}X}$
- Termination probability using absolute value:
- $\left|\frac{1}{2} \cdot \sum_{i=0}^{\infty} \left(\frac{1}{4}\right)^{i} X^{i} F^{1}\right|$

Termination Probability

- Closed form: $\frac{F}{2-\frac{1}{2}X}$
- Termination probability using absolute value:
- $\left| \frac{1}{2} \cdot \sum_{i=0}^{\infty} \left(\frac{1}{4}\right)^i X^i F^1 \right| = \frac{1}{2} \cdot \sum_{i=0}^{\infty} \left(\frac{1}{4}\right)^i$

Termination Probability

- Closed form: $\frac{F}{2-\frac{1}{2}X}$
- Termination probability using absolute value:
- $\left|\frac{1}{2}\cdot\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^{i}X^{i}F^{1}\right| = \frac{1}{2}\cdot\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^{i} = \frac{2}{3}$

Termination Probability

- Closed form: $\frac{F}{2-\frac{1}{2}X}$
- Termination probability using absolute value:
- $\left|\frac{1}{2} \cdot \sum_{i=0}^{\infty} \left(\frac{1}{4}\right)^i X^i F^1\right| = \frac{1}{2} \cdot \sum_{i=0}^{\infty} \left(\frac{1}{4}\right)^i = \frac{2}{3}$
- $\left|\frac{F}{2-\frac{1}{2}X}\right| = \frac{1}{2-\frac{1}{2}} = \frac{2}{3}$

Equivalent Programs

```
while ( F = 0 ) {
  { X := X + 1 }[p]{ F := 1 }
};

F := 0;
while ( F = 0 ) {
  { X := X - 1 }[q]{ F := 1 }
}
```

```
{ F := 0 }[0.5]{ F := 1 };
if ( F = 0 ) {
  while ( F = 0 ) {
    { X := X + 1 }[p]{ F := 1 }
  }

} else {
  F := 0;
  while ( F = 0 ) {
    X := X - 1;
    { skip }[q]{ F := 1 }
  }
}
```

Equivalent Programs

```
while ( F = 0 ) {
  { X := X + 1 }[p]{ F := 1 }
};

F := 0;
while ( F = 0 ) {
  { X := X − 1 }[q]{ F := 1 }
}
```

```
{ F := 0 }[0.5]{ F := 1 };
if ( F = 0 ) {
  while ( F = 0 ) {
    { X := X + 1 }[p]{ F := 1 }
  }

} else {
  F := 0;
  while ( F = 0 ) {
    X := X − 1;
    { skip }[q]{ F := 1 }
  }
}
```

- Introduced by Kiefer et al. in 2012.

Equivalent Programs

```
while ( F = 0 ) {
  { X := X + 1 }[p]{ F := 1 }
};

F := 0;
while ( F = 0 ) {
  { X := X − 1 }[q]{ F := 1 }
}
```

```
{ F := 0 }[0.5]{ F := 1 };
if ( F = 0 ) {
  while ( F = 0 ) {
    { X := X + 1 }[p]{ F := 1 }
  }

} else {
  F := 0;
  while ( F = 0 ) {
    X := X − 1;
    { skip }[q]{ F := 1 }
  }
}
```

- Introduced by Kiefer et al. in 2012.
- Proven equivalent in distribution for $p = \frac{1}{2}$ and $q = \frac{2}{3}$.

Equivalent Programs

```
while ( F = 0 ) {
  { X := X + 1 }[p]{ F := 1 }
};

F := 0;
while ( F = 0 ) {
  { X := X − 1 }[q]{ F := 1 }
}
```

```
{ F := 0 }[0.5]{ F := 1 };
if ( F = 0 ) {
  while ( F = 0 ) {
    { X := X + 1 }[p]{ F := 1 }
  }

} else {
  F := 0;
  while ( F = 0 ) {
    X := X − 1;
    { skip }[q]{ F := 1 }
  }
}
```

- Introduced by Kiefer et al. in 2012.
- Proven equivalent in distribution for $p = \frac{1}{2}$ and $q = \frac{2}{3}$.
- Expected value of X is the same if $q = \frac{1}{2-p}$. (Gretz et al.)

Equivalent Programs

```
while ( F = 0 ) {
  { X := X + 1 }[p]{ F := 1 }
};

F := 0;
while ( F = 0 ) {
  { X := X − 1 }[q]{ F := 1 }
}
```

```
{ F := 0 }[0.5]{ F := 1 };
if ( F = 0 ) {
  while ( F = 0 ) {
    { X := X + 1 }[p]{ F := 1 }
  }

} else {
  F := 0;
  while ( F = 0 ) {
    X := X − 1;
    { skip }[q]{ F := 1 }
  }
}
```

- Introduced by Kiefer et al. in 2012.
- Proven equivalent in distribution for $p = \frac{1}{2}$ and $q = \frac{2}{3}$.
- Expected value of X is the same if $q = \frac{1}{2-p}$. (Gretz et al.)
- Today: equivalence in distribution if $q = \frac{1}{2-p}$.

Equivalent Programs

- First program's semantics:

$$\frac{(1-q)\cdot(1-p)}{1-qp} \cdot \left(\frac{F}{1-pX},\ \ q \cdot \frac{X^{-1}F}{1-qX^{-1}}, 0, 0 \right)$$

Equivalent Programs

- First program's semantics:

$$\frac{(1-q)\cdot(1-p)}{1-qp} \cdot \left(\frac{F}{1-pX},\ \ q \cdot \frac{X^{-1}F}{1-qX^{-1}}, 0, 0 \right)$$

- Second program's semantics:

$$\left(\frac{1-p}{2} \cdot \frac{F}{1-pX},\ \ \frac{1-q}{2} \cdot \frac{X^{-1}F}{1-qX^{-1}}, 0, 0 \right)$$

Equivalent Programs

- First program's semantics:

$$\frac{(1-q)\cdot(1-p)}{1-qp} \cdot \left(\frac{F}{1-pX},\ \ q \cdot \frac{X^{-1}F}{1-qX^{-1}}, 0, 0 \right)$$

- Second program's semantics:

$$\left(\frac{1-p}{2} \cdot \frac{F}{1-pX},\ \ \frac{1-q}{2} \cdot \frac{X^{-1}F}{1-qX^{-1}}, 0, 0 \right)$$

Equivalent Programs

- First program's semantics:

$$\frac{(1-q)\cdot(1-p)}{1-qp} \cdot \left(\frac{F}{1-pX},\ \ q \cdot \frac{X^{-1}F}{1-qX^{-1}}, 0, 0 \right)$$

- Second program's semantics:

$$\left(\frac{1-p}{2} \cdot \frac{F}{1-pX},\ \ \frac{1-q}{2} \cdot \frac{X^{-1}F}{1-qX^{-1}}, 0, 0 \right)$$

Equivalent Programs

- First program's semantics:

$$\frac{(1-q)\cdot(1-p)}{1-qp}\cdot\left(\frac{F}{1-pX},\ \ q\cdot\frac{X^{-1}F}{1-qX^{-1}},0,0\right)$$

- Second program's semantics:

$$\left(\frac{1-p}{2}\cdot\frac{F}{1-pX},\ \ \frac{1-q}{2}\cdot\frac{X^{-1}F}{1-qX^{-1}},0,0\right)$$

Equivalent Programs

- First program's semantics:

$$\frac{(1-q)\cdot(1-p)}{1-qp} \cdot \left(\frac{F}{1-pX}, \;\; q \cdot \frac{X^{-1}F}{1-qX^{-1}}, 0, 0 \right)$$

- Second program's semantics:

$$\left(\frac{1-p}{2} \cdot \frac{F}{1-pX}, \;\; \frac{1-q}{2} \cdot \frac{X^{-1}F}{1-qX^{-1}}, 0, 0 \right)$$

- Solve $\frac{(1-q)\cdot(1-p)}{1-qp} = \frac{1-p}{2}$ and $\frac{(1-q)\cdot(1-p)\cdot q}{1-qp} = \frac{1-q}{2}$.

Equivalent Programs

- First program's semantics:

$$\frac{(1-q)\cdot(1-p)}{1-qp} \cdot \left(\frac{F}{1-pX},\ \ q \cdot \frac{X^{-1}F}{1-qX^{-1}}, 0, 0 \right)$$

- Second program's semantics:

$$\left(\frac{1-p}{2} \cdot \frac{F}{1-pX},\ \ \frac{1-q}{2} \cdot \frac{X^{-1}F}{1-qX^{-1}}, 0, 0 \right)$$

- Solve $\frac{(1-q)\cdot(1-p)}{1-qp} = \frac{1-p}{2}$ and $\frac{(1-q)\cdot(1-p)\cdot q}{1-qp} = \frac{1-q}{2}$.

- Equivalent in distribution if $q = \frac{1}{2-p}$.

Comparison of Semantics

- Comparison of PGF and wp semantics (McIver and Morgan)

Comparison of Semantics

- Comparison of PGF and wp semantics (McIver and Morgan)
- Random variables: $E = \{\mathbb{S} \to \mathbb{R}_{\geq 0}\}$

Comparison of Semantics

- Comparison of PGF and wp semantics (McIver and Morgan)
- Random variables: $E = \{\mathbb{S} \to \mathbb{R}_{\geq 0}\}$
- $\mathsf{wp}\colon P \times E \to E$

Comparison of Semantics

- Comparison of PGF and wp semantics (McIver and Morgan)
- Random variables: $E = \{\mathbb{S} \to \mathbb{R}_{\geq 0}\}$
- $\mathsf{wp}\colon P \times E \to E$
- $[\![P]\!]\,(G)$ vs. $\mathsf{wp}\,(P, f)$

Comparison of Semantics

- Comparison of PGF and wp semantics (McIver and Morgan)
- Random variables: $E = \{\mathbb{S} \to \mathbb{R}_{\geq 0}\}$
- $\mathrm{wp}\colon P \times E \to E$
- $[\![P]\!]\,(G)$ vs. $\mathrm{wp}\,(P, f)$
- $\mathbb{E}_\mu(f)$, where μ a measure on program states, f a random variable

Comparison of Semantics

- Comparison of PGF and wp semantics (McIver and Morgan)
- Random variables: $E = \{\mathbb{S} \rightarrow \mathbb{R}_{\geq 0}\}$
- wp: $P \times E \rightarrow E$
- $\llbracket P \rrbracket (G)$ vs. $\mathrm{wp}(P, f)$
- $\mathbb{E}_\mu(f)$, where μ a measure on program states, f a random variable
- Every PGF has a corresponding measure.

Comparison of Semantics

- Comparison of PGF and wp semantics (McIver and Morgan)
- Random variables: $E = \{\mathbb{S} \to \mathbb{R}_{\geq 0}\}$
- $\mathsf{wp}\colon P \times E \to E$
- $[\![P]\!]\,(G)$ vs. $\mathsf{wp}\,(P, f)$
- $\mathbb{E}_{\mu}(f)$, where μ a measure on program states, f a random variable
- Every PGF has a corresponding measure.

Theorem

Given a program P, a measure μ and an expectation f, the following holds:

$$\mathbb{E}_{[\![P]\!](\mu)}(f) = \mathbb{E}_{\mu}(\mathsf{wp}\,(P, f))$$

Bisimulations

- Inspired by coinduction (Arbab et al.)

Bisimulations

- Inspired by coinduction (Arbab et al.)
- Use bisimulations to reason about loops.

Bisimulations

- Inspired by coinduction (Arbab et al.)
- Use bisimulations to reason about loops.
- Weak and strong bisimulations

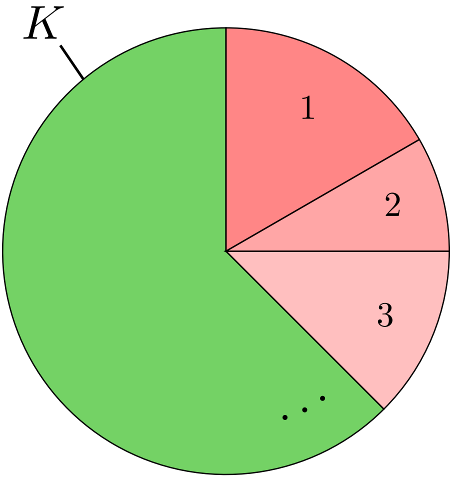
Bisimulations

- Inspired by coinduction (Arbab et al.)
- Use bisimulations to reason about loops.
- Weak and strong bisimulations
- No correlation to transition systems

Bisimulations

- Inspired by coinduction (Arbab et al.)
- Use bisimulations to reason about loops.
- Weak and strong bisimulations
- No correlation to transition systems
- Overapproximation and actual loop semantics

Bisimulations



Bisimulations

Definition (Weak Bisimulation)

Let R be a binary relation. If $(K, G) \in R$, then

Let $G' = \mathrm{wh}_{B,P}(G)$

i) $\langle G' \rangle_{\neg B} \sqsubseteq K$

ii) $(K - \langle G' \rangle_{\neg B}\,, G') \in R$

Bisimulations

Definition (Weak Bisimulation)

Let R be a binary relation. If $(K, G) \in R$, then

Let $G' = \mathrm{wh}_{B,P}(G)$

i) $\langle G' \rangle_{\neg B} \sqsubseteq K$

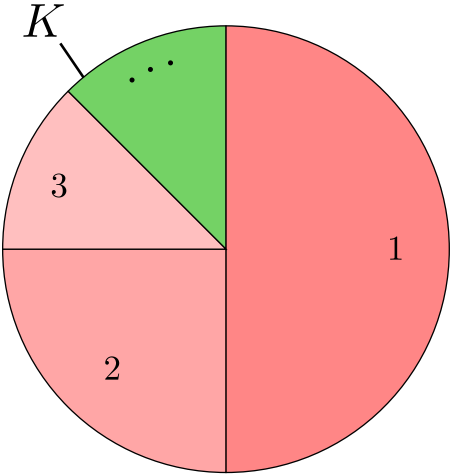
ii) $(K - \langle G' \rangle_{\neg B}, G') \in R$

Theorem

Let R be a weak bisimulation. Then

$$(K, G) \in R \wedge G \models B \implies [\![\mathit{while}(B)\{P\}]\!](G) \sqsubseteq K$$

Bisimulations



Bisimulations

Definition (Strong Bisimulation)

Let R be a binary relation and $\varepsilon \in (0,1)$. If $(K, G) \in R$, then

Let $G' = \mathrm{wh}_{B,P}(G)$

i) $\langle G' \rangle_{\neg B} \sqsubseteq_D K$

ii) $(K - \langle G' \rangle_{\neg B}, G') \in R$

iii) $|\langle G' \rangle_{\neg B}| \geq \varepsilon \cdot |K|$

Bisimulations

Definition (Strong Bisimulation)

Let R be a binary relation and $\varepsilon \in (0,1)$. If $(K, G) \in R$, then

Let $G' = \mathrm{wh}_{B,P}(G)$

i) $\langle G' \rangle_{\neg B} \sqsubseteq_D K$

ii) $(K - \langle G' \rangle_{\neg B}, G') \in R$

iii) $|\langle G' \rangle_{\neg B}| \geq \varepsilon \cdot |K|$

Theorem

Let R be a strong bisimulation. Then

$$(K, G) \in R \wedge G \models B \implies [\![\mathit{while}(B)\{P\}]\!](G) = K$$

Bisimulations

```
while (F = 0) {
  {X := X + 1}[0.5]{F := 1}
}
```

- $G = 1$, $K = \frac{1}{2-X}$

Bisimulations

```
while (F = 0) {
  {X := X + 1}[0.5]{F := 1}
}
```

- $G = 1$, $K = \frac{1}{2-X}$
- Bisimulation: $R = \{(K, G)\} \cup$

Bisimulations

```
while (F = 0) {
  {X := X + 1}[0.5]{F := 1}
}
```

- $G = 1$, $K = \frac{1}{2-X}$
- Bisimulation: $R = \{(K, G)\} \cup \left\{ \left(\left\langle \frac{1}{2-X} \right\rangle_{X \geq n}, \left(\frac{1}{2}\right)^n \cdot \left(X^n F^0 + X^{n-1} F^1\right) \right) \,\middle|\, n \in \mathbb{N}_{>0} \right\}$

Bisimulations

```
while (F = 0) {
  {X := X + 1}[0.5]{F := 1}
}
```

- $G = 1$, $K = \frac{1}{2-X}$
- Bisimulation: $R = \{(K, G)\} \cup$
$$\left\{ \left(\left\langle \frac{1}{2-X} \right\rangle_{X \geq n}, \left(\frac{1}{2}\right)^n \cdot \left(X^n F^0 + X^{n-1} F^1\right) \right) \;\middle|\; n \in \mathbb{N}_{>0} \right\}$$

Bisimulations

```
while (F = 0) {
  {X := X + 1}[0.5]{F := 1}
}
```

- $G = 1$, $K = \frac{1}{2-X}$
- Bisimulation: $R = \{(K, G)\} \cup$
  $$\left\{ \left(\left\langle \frac{1}{2-X} \right\rangle_{X \geq n}, \left(\frac{1}{2}\right)^n \cdot \left(X^n F^0 + X^{n-1} F^1\right) \right) \,\middle|\, n \in \mathbb{N}_{>0} \right\}$$

Bisimulations

```
while (F = 0) {
  {X := X + 1}[0.5]{F := 1}
}
```

- $G = 1$, $K = \frac{1}{2-X}$
- Bisimulation: $R = \{(K, G)\} \cup$
  $\left\{ \left(\left\langle \frac{1}{2-X} \right\rangle_{X \geq n}, \left(\frac{1}{2}\right)^n \cdot \left(X^n F^0 + X^{n-1} F^1\right) \right) \;\middle|\; n \in \mathbb{N}_{>0} \right\}$
- R is in fact a strong bisimulation ($\varepsilon = \frac{1}{2}$)!

Bisimulations

```
while (F = 0) {
  {X := X + 1}[0.5]{F := 1}
}
```

- $G = 1$, $K = \frac{1}{2-X}$
- Bisimulation: $R = \{(K, G)\} \cup$
  $\left\{ \left(\left\langle \frac{1}{2-X} \right\rangle_{X \geq n}, \left(\frac{1}{2}\right)^n \cdot \left(X^n F^0 + X^{n-1} F^1\right) \right) \;\middle|\; n \in \mathbb{N}_{>0} \right\}$
- R is in fact a strong bisimulation ($\varepsilon = \frac{1}{2}$)!
- $[\![while(F = 0)\{\ldots\}]\!]\,(1) \sqsubseteq K$

Bisimulations

```
while (F = 0) {
   {X := X + 1}[0.5]{F := 1}
}
```

- $G = 1$, $K = \frac{1}{2-X}$
- Bisimulation: $R = \{(K, G)\} \cup$
$$\left\{ \left(\left\langle \frac{1}{2-X} \right\rangle_{X \geq n}, \left(\frac{1}{2}\right)^n \cdot \left(X^n F^0 + X^{n-1} F^1\right) \right) \;\middle|\; n \in \mathbb{N}_{>0} \right\}$$
- R is in fact a strong bisimulation ($\varepsilon = \frac{1}{2}$)!
- $\llbracket \mathit{while}(F = 0)\{\ldots\} \rrbracket (1) \sqsubseteq K$
- $\llbracket \mathit{while}(F = 0)\{\ldots\} \rrbracket (1) = K$

Contribution

- Semantics for negative variable valuations with closed forms
- Deeper understanding of two relevant programs
- Comparison to an established semantics
- Novel approach for finding loop semantics

Thank you for your attention!

Wp-semantics

1. Expectations: $E = \{\mathbb{S} \to \mathbb{R}_{\geq 0}\}$
2. $\mathrm{wp}\colon E \to E$
3. $\mathrm{wp}\,(\mathit{skip}, f) = f$.
4. $\mathrm{wp}\,(\mathit{diverge}, f) = 0$.
5. $\mathrm{wp}\,(X := e, f) = f[X/e]$.
6. $\mathrm{wp}\,(P; Q, f) = \mathrm{wp}\,(P, \mathrm{wp}\,(Q, f))$.
7. $\mathrm{wp}\,(\mathit{if}(B)\,\{\,P\,\}\,\mathit{else}\,\{\,Q\,\}, f) = [B]\cdot\mathrm{wp}\,(P, f) + [\neg B]\cdot\mathrm{wp}\,(Q, f)$.
8. $\mathrm{wp}\,(\{P\}[p]\{Q\}, f) = p \cdot \mathrm{wp}\,(P, f) + (1 - p) \cdot \mathrm{wp}\,(Q, f)$.
9. $\mathrm{wp}\,(\mathit{while}\,(B)\{P\}, f) = \mu X.\,([B] \cdot \mathrm{wp}\,(P, X) + [\neg B] \cdot f)$.