Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики
Кафедра алгоритмических языков

Метод контроля исполнения процессов на основе мониторинга потока управления в объеме исполняемых в операционной системе команд

Конференция «Программирование и вычислительная математика»

Пучкин Данила Андреевич

Москва, 2025

Мониторинг потока управления

- **Исправность процесса** - функционирование процесса в соответствии с предъявляемыми ему требованиями
- Нарушение потока управления процесса – один из признаков нарушения исправности процесса
- **Мониторинг потока управления** - сравнение фактического потока управления процесса с некоторой эталонной моделью потока управления
    - При выявлении несоответствия исполняемого потока управления своему эталону поток управления считается нарушенным

Моделирование потока управления

- **Граф потока управления (Control Flow Graph, CFG)** – орграф, вершины которого называются **базовыми блоками** и соответствуют максимальным линейным участкам команд программы, а ребра определяют порядок следования базовых блоков
- Ключевое при моделировании потока управления с помощью CFG – выбор способа моделирования базовых блоков CFG
- Ключевое при выборе способа моделирования базовых блоков CFG – возможности получения информации о фактическом потоке управления при проведении мониторинга

Методы моделирования базовых блоков

- **Фиксированный набор команд базовых блоков**
  - Примеры:
    - Размерности переменных программы
    - Последовательности команд вызова функций
    - Не зависящие от базовых блоков ключи
  - **Общий недостаток** – мониторинг в ограниченном объеме команд
- **Настраиваемый набор команд базовых блоков**
  - **Общий недостаток существующих методов** – не решается задача получения информации о фактическом потоке управления для осуществления мониторинга

Методы получения информации о фактическом потоке управления

- **Инструментирование программ**
  - **Общий недостаток** – потребность в модификации контролируемых программ
- **Использование аппаратного обеспечения (ЦП, ОЗУ)**
  - **Общий недостаток** – зависимость от аппаратного обеспечения
- **Трассировка исполняемых программ**
  - **Недостаток существующих методов** – использование вероятностных моделей потока управления

Постановка задачи

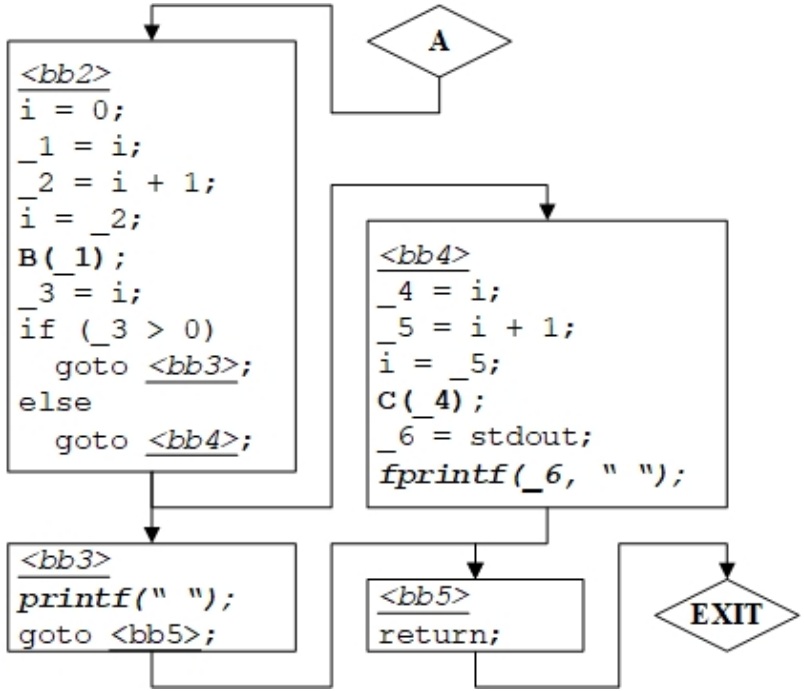
- **Цель работы** – предложить метод мониторинга потока управления программы, который
  - Производится в настраиваемом объеме команд
  - Не требует модификации контролируемой программы
  - Независим от аппаратного обеспечения
- Рассматриваются однопоточные процессы, в которых при прерываниях не исполняются команды модели
  - Рассматриваемый в работе подход может быть расширен для мониторинга процессов более общего вида

Сигнатура потока управления

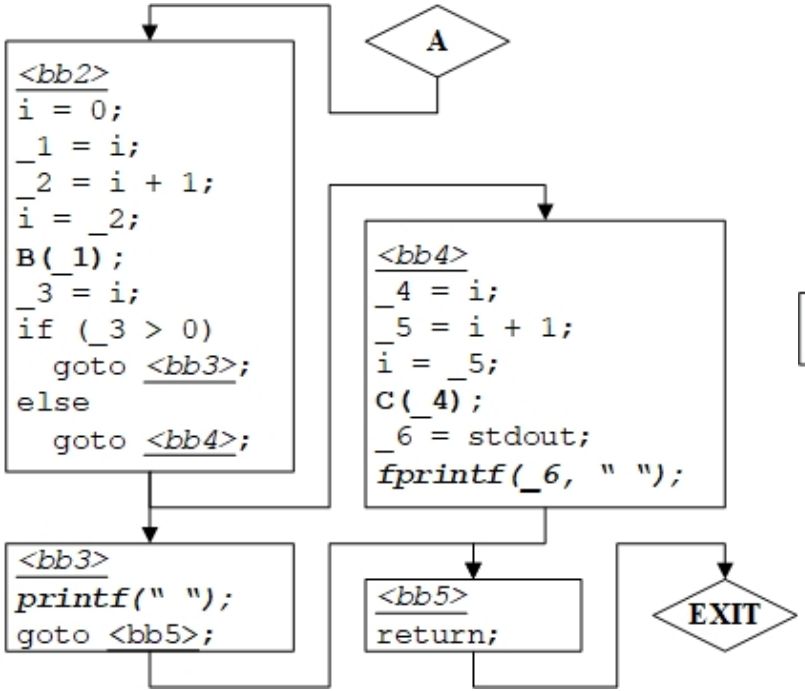
- **Целевые команды** – операторы программы процесса, в объеме которых производится контроль корректности его исполнения
- **Управляющие команды** – операторы программы процесса, определяющие его ПУ
- **Сигнатура потока управления** - модель потока управления программы процесса, отражающая все возможные последовательности целевых команд, которые могут быть исполнены процессом
    - Основой для построения сигнатуры потока управления программы являются графы потока управления функций программы

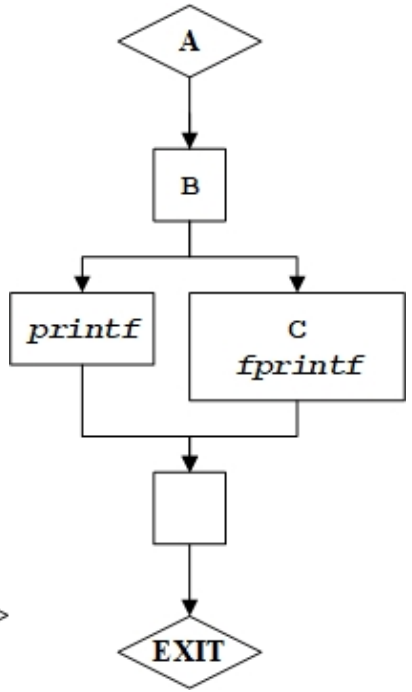
Граф потока управления

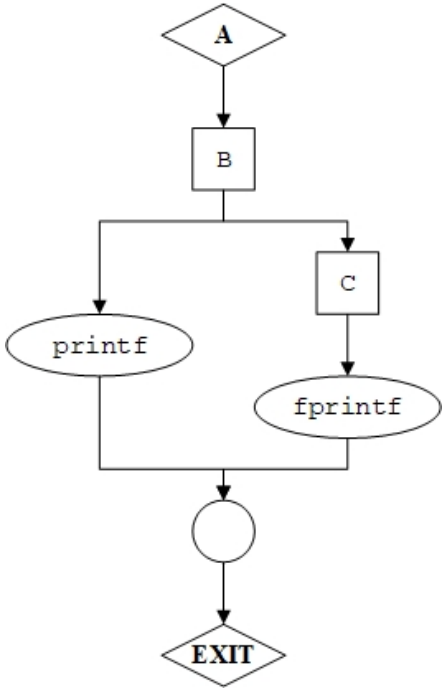
```
 1: void A()
 2: {
 3:   int i = 0;
 4:   B(i++);
 5:   if (i > 0)
 6:   {
 7:     C(i++);
 8:     fprintf(stdout, " ");
 9:   }
10:   else
11:   {
12:     printf(" ");
13:   }
14: }
```



Преобразование CFG

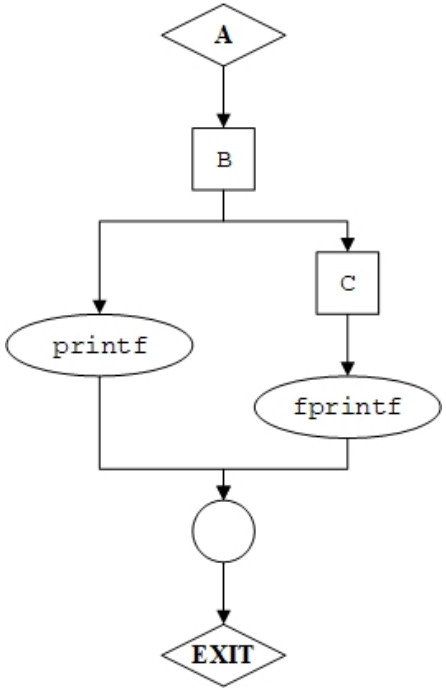






Граф потока вызовов (FFG)

- **Граф потока вызовов (Function calls Flow Graph, FFG)** – CFG, в котором каждой вершине соответствует не более одной целевой или управляющей команды
- **Целевая (управляющая) вершина FFG** – вершина FFG, соответствующая целевой (управляющей) команде
- **Пустая (непустая) вершина FFG** – вершина FFG, не соответствующая ни одной (соответствующая ровно одной) команде
- **Вызывающая вершина (вершина вызова) FFG** – управляющая вершина, соответствующая команде вызова функции



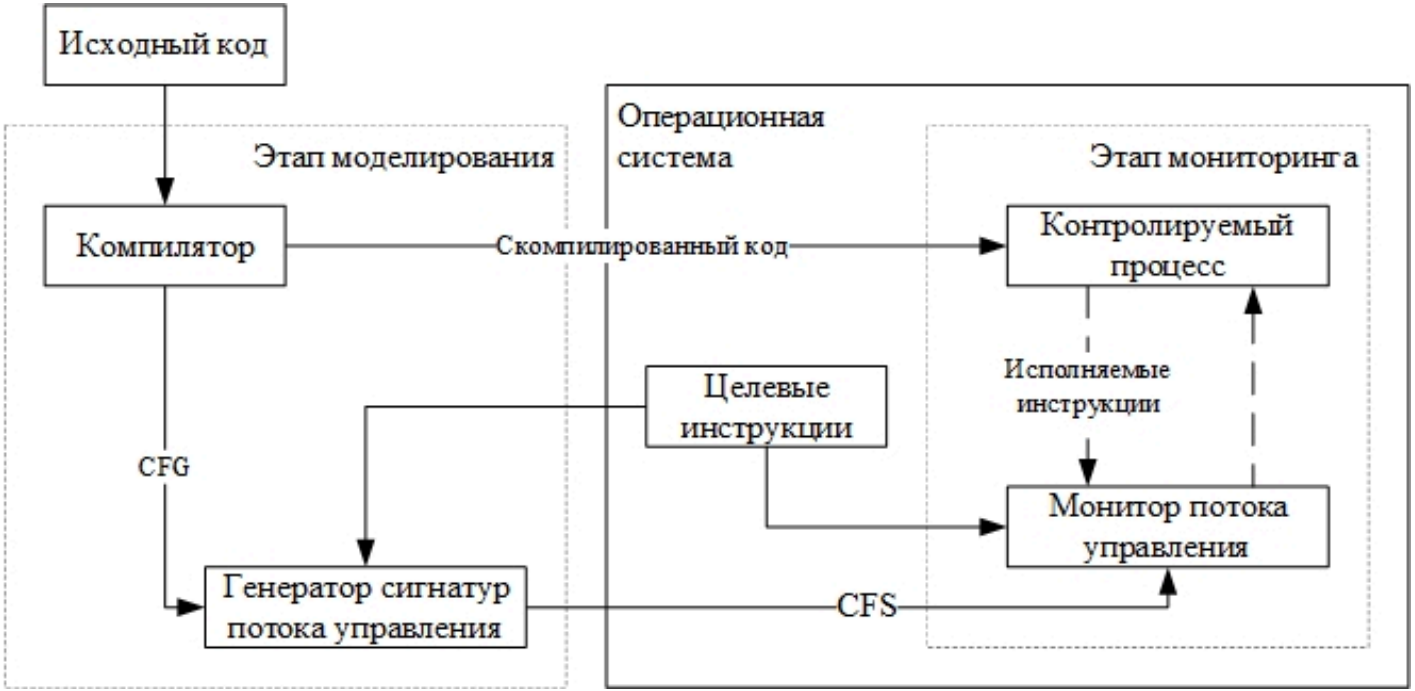
Получение информации о фактическом потоке управления

- Для генерации сигнатуры потока управления требуется набор целевых команд
- Для независимости работы процесса от мониторинга информация об исполнении целевых команд должна поставляться вычислительной системой
- Для независимости мониторинга от аппаратного обеспечения информацию о фактическом потоке управления следует получать от операционной системы
- В результате набор целевых команд определяется возможностями операционной системы по мониторингу исполнения процессов
- Существуют операционные системы, предоставляющие надежные способы получения информации о функционировании процессов

Получение сигнатуры потока управления

- **Генератор сигнатур потока управления** – программа, генерирующая сигнатуру потока управления программы по набору целевых команд и по набору CFG функций программы, среди которых выделен CFG, соответствующий точке входа в программу
- **Связывание FFG** – процедура сопоставления вызывающих вершин FFG и соответствующих им функций
- Этапы построения сигнатуры потока управления:
  - Построение CFG функций программы
  - Преобразование CFG в FFG
  - Связывание FFG
  - Генерация сигнатуры потока управления в соответствии с выбранной формой

Реализация метода



Результаты

- Предложен метод мониторинга потока управления процесса в объеме команд, информация об исполнении которых доступна от операционной системы
- Состав команд для моделирования определяется в зависимости от требований к мониторингу
- Состав команд ограничен только возможностями операционной системы по получению информации об их исполнении

Спасибо за внимание!