Алгоритм генерации команд восстановления дерева процессов ОС Linux на основе модели жизненного цикла ресурсов ОС

Горбунов Егор Алексеевич

научный руководитель: маг. прикладной математики и физики Е. А. Баталов

СПб АУ НОЦНТ РАН

13 июня 2017 г.

Задача сохранения и восстановления дерева процессов

Сохранение

Сохранение в виде образов на диск состояния всех ресурсов из которых состоит дерево процессов: *регионы виртуальной памяти, открытые файлы, сокеты, идентификатор процесса, сессии, группы, идентификатор пользователя* и т. д.

Восстановление

Это создание всех ресурсов дерева процессов, существовавших в момент сохранения, а также восстановление их состояния таким, каким оно было в момент сохранения:

- процесс не должен заметить, что что-то произошло

Использование

Живая миграция, ...

Существующие программные решения

- **CRIU**
  - \+ полностью в userspace
  - \+ активно поддерживается на текущий момент
- BLCR[1] (2003)
  - – требует подгрузки модуля к ядру
- DMTCP[2] (2004)
  - – к целевому процессу с момента запуска должна быть подключена библиотека
  - – перехватывает часть `glibc` и системных вызовов
- OpenVZ(2005)
  - – работает внутри собственного ядра Linux

[1] Berkeley Lab Checkpoint/Restart
[2] Distributed MultiThreaded CheckPointing

Проблемы `criu` в подходе к восстановлению

Последовательность действий восстановления чётко зафиксирована в коде (и она очень большая), что приводит к проблемам:

- Код для восстановления каждого типа ресурсов нужно добавить в эту последовательностей так, чтобы он был логически согласован со всем вокруг
- Любые нетривиальные зависимости между ресурсами требуют добавления дополнительного кода
- Отсутствие чёткого понимания того, какие конфигурации ресурсов дерева процессов `criu` гарантированно поддерживает

Подход с генератором и интерпретатором

Для каждого конкретного дерева процессов получаем индивидуальную программу из команд

Цель и задачи

Цель

Отойти от фиксированного порядка восстановления и найти обобщённый подход к восстановлению ресурсов, который будет проще подвергаться анализу

Задачи

- Разработать генератор команд для задачи восстановления дерева процессов в рамках подхода генератор-интерпретатор
- Разработать промежуточные представления

Требования

- Генерируемые команды должны быть исполнимы из пространства пользователя
- Возможность эффективной реализации предлагаемых алгоритмов

Модель дерева процессов

Ресурс — r — сущность в ядре ОС (file struct, group, session, ...)

Handle — h — объект, через который процесс получает доступ к ресурсу (file descriptor, gid, sid, ...)

Процесс

$$P = \{(r_1, h_1), (r_2, h_2), \ldots, (r_n, h_n)\}$$

$pid(P)$ — идентификатор процесса

$parent(P)$ — процесс-родитель, $\neq P$

Дерево процессов

$$T = \{P_1, P_2, \ldots, P_k\}$$

$$root = P_1$$

$$\forall P \in T \wedge P \neq root \; (parent(P) \in T)$$

Свойства ресурсов

isSharable(r) — ресурс, который можно разделить ”при жизни”(file, group, namespace, ...)

isInherited(r) — ресурс, наследуемый ребёнком ”при рождении”(file, private memory area, ...)

possibleCreators(r) — множество процессов, способных создать ресурс

resourceDependencies(r) — множество ресурсов, от которых зависит создание r

canExistTogether($(r_1, h_1), (r_2, h_2)$) — предикат, отвечающий на вопрос: могут ли одновременно два ресурса находиться в контексте одного процесса

Модель жизненного цикла ресурсов и процессов

Действия, которые процессы совершают при жизни:

$$\mathcal{A} = \begin{cases} ForkAction(P_1, P_2) \\ CreateAction(P, r, h) \\ ShareAction(P_{from}, P_{to}, r, h_{from}, h_{to}) \\ RemoveAction(P, r, h) \end{cases}$$

Задача восстановления

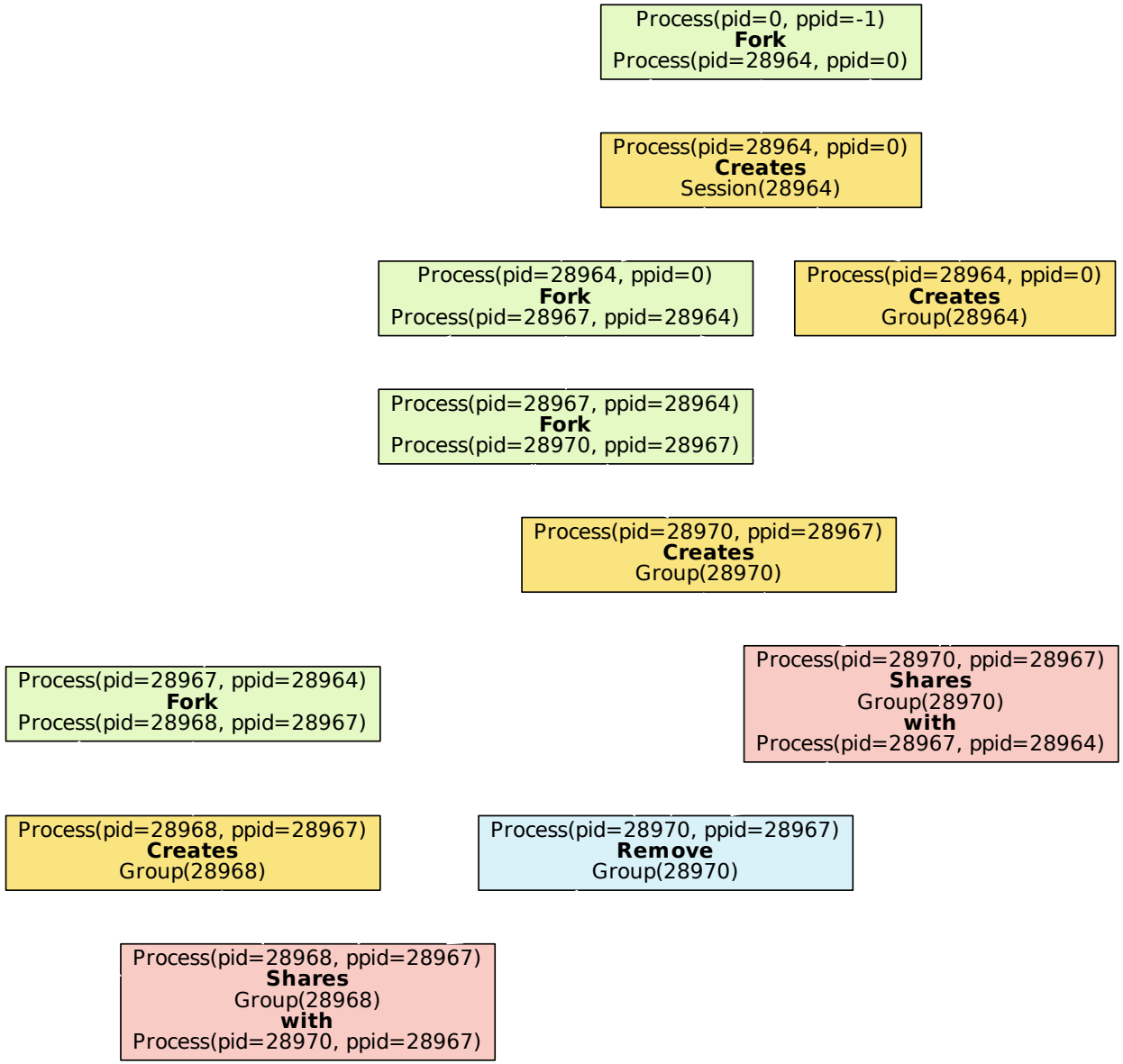
Имея исходное дерево процессов T, найти последовательность действий $[a_i]\,,\ (a_i \in \mathcal{A})$, что:

$$\{P_0\} \xRightarrow{A} \{P_0\} \cup T$$

Построение множества действий

- Для каждого процесса $P \in T$ создаём $ForkAction(parent(P), P)$
- Для каждого ресурса r в дереве выбираем его создателя P, handle h и добавляем действие $CreateAction(P, r, h)$
- Для каждого $isSharable(r)$ ресурса, добавляем $ShareAction(P, ...)$ от создателя P к остальным процессам, держащим ресурс
- Добавляем $RemoveAction(r)$ для всех "временных" ресурсов

Построение множества действий. Пример

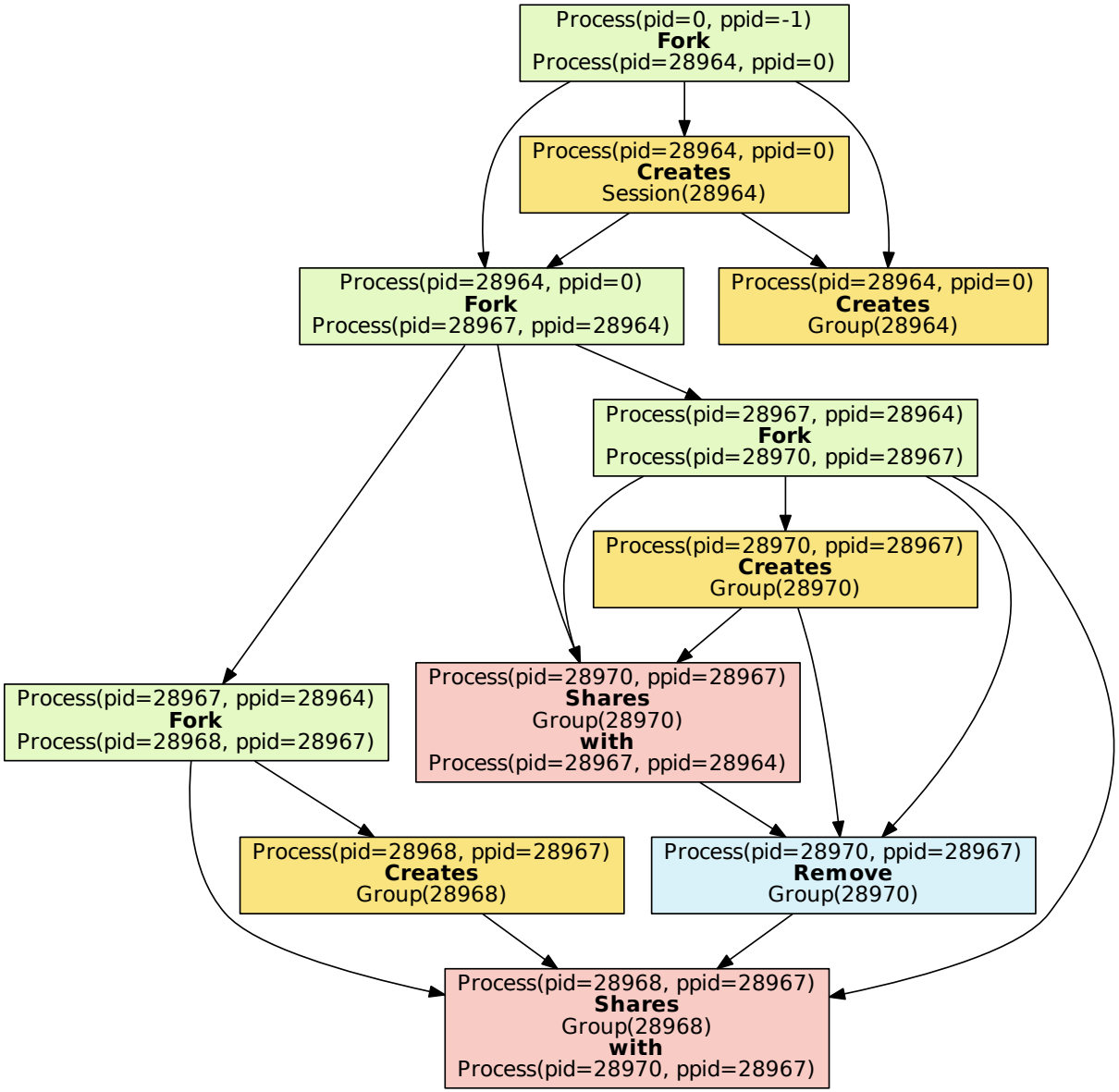


Построение рёбер предшествования

Построение ведётся в несколько этапов, каждый из которых строит часть необходимых рёбер:

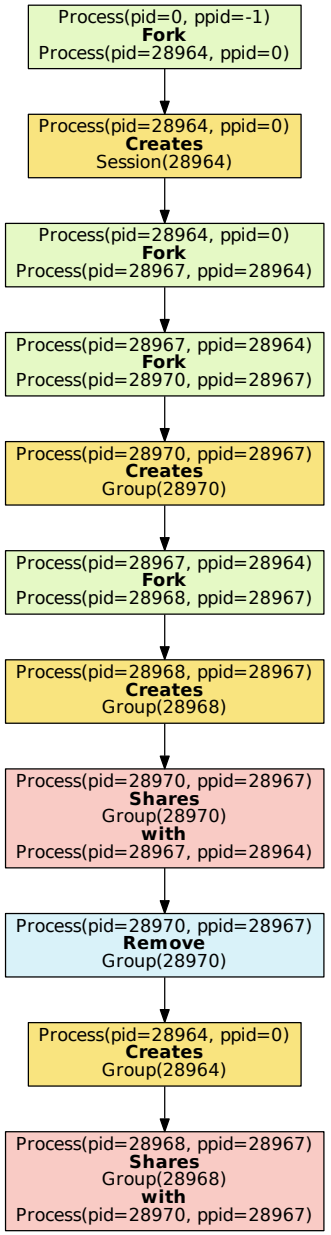
- *ForkAction*$(\_, P)$ *предшествует* любому действию, которое как-то нуждается в процессе P
- *CreateAction*$(\_, r, h)$ *предшествует* любому действию, которое использует (r, h)
- Создание ресурса процессом P должно учитывать наличие зависимостей этого ресурса у процесса P
- Действия должны быть так упорядочены, что в любой момент времени t ни одна пара из текущих ресурсов (r, h) не конфликтует для всех процессов $P \in T_t$
- ...

Построение рёбер предшествования. Пример



Упорядочение графа действий

- Топологическая сортировка графа
- Сложность всего алгоритма: $\mathcal{O}\left(\sum_{P \in T} |P|\right)$
- Если граф не является ациклическим, до в рамках текущей модели восстановление невозможно



Итоги и дальнейшие планы

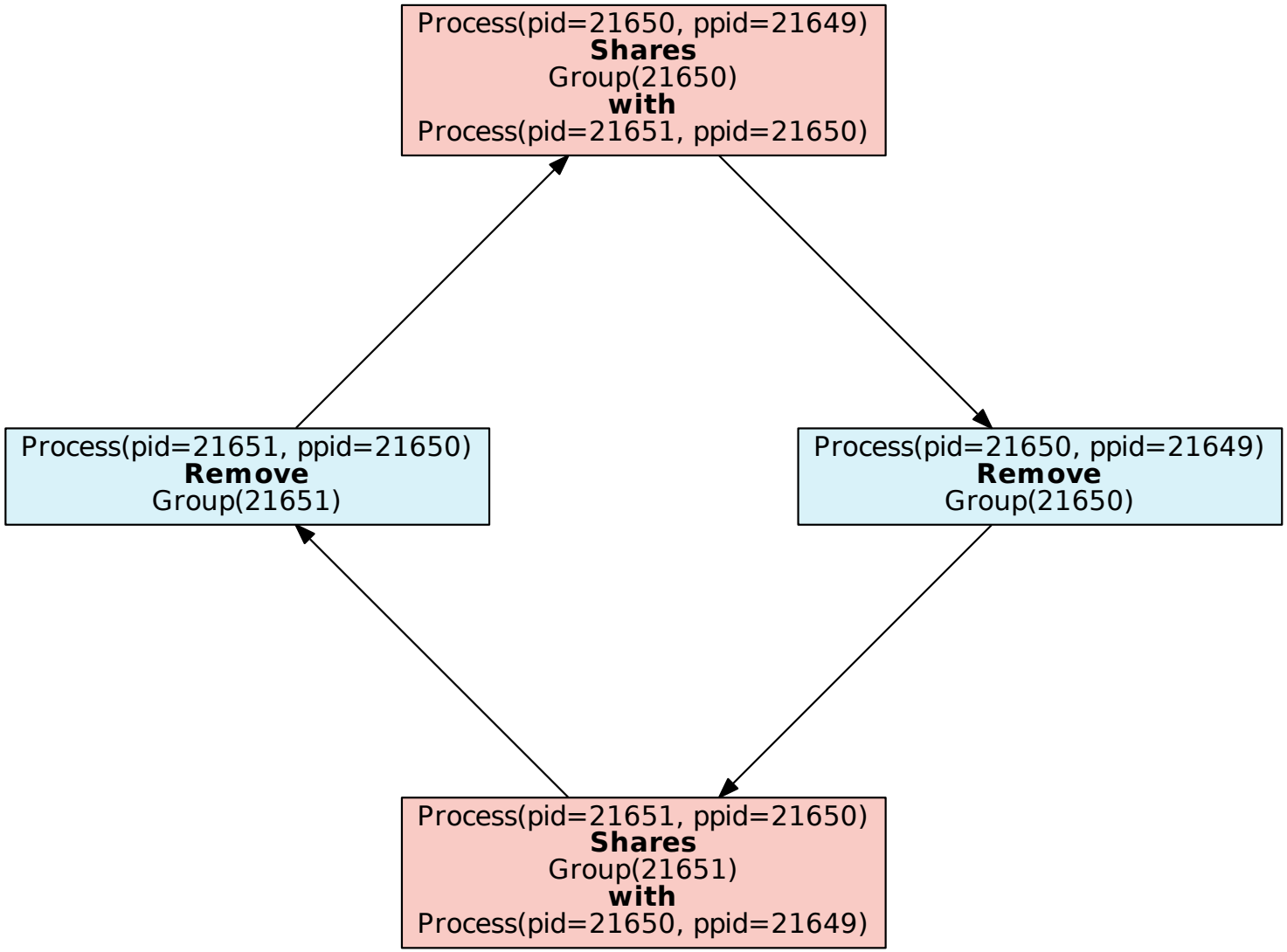
Итоги

- Введена формальная обобщённая модель жизнедеятельности процессов в ОС Linux для решения задачи восстановления
- Предложен и реализован алгоритм генерации промежуточного представления в виде графа действий и последовательности действий для восстановления дерева процессов

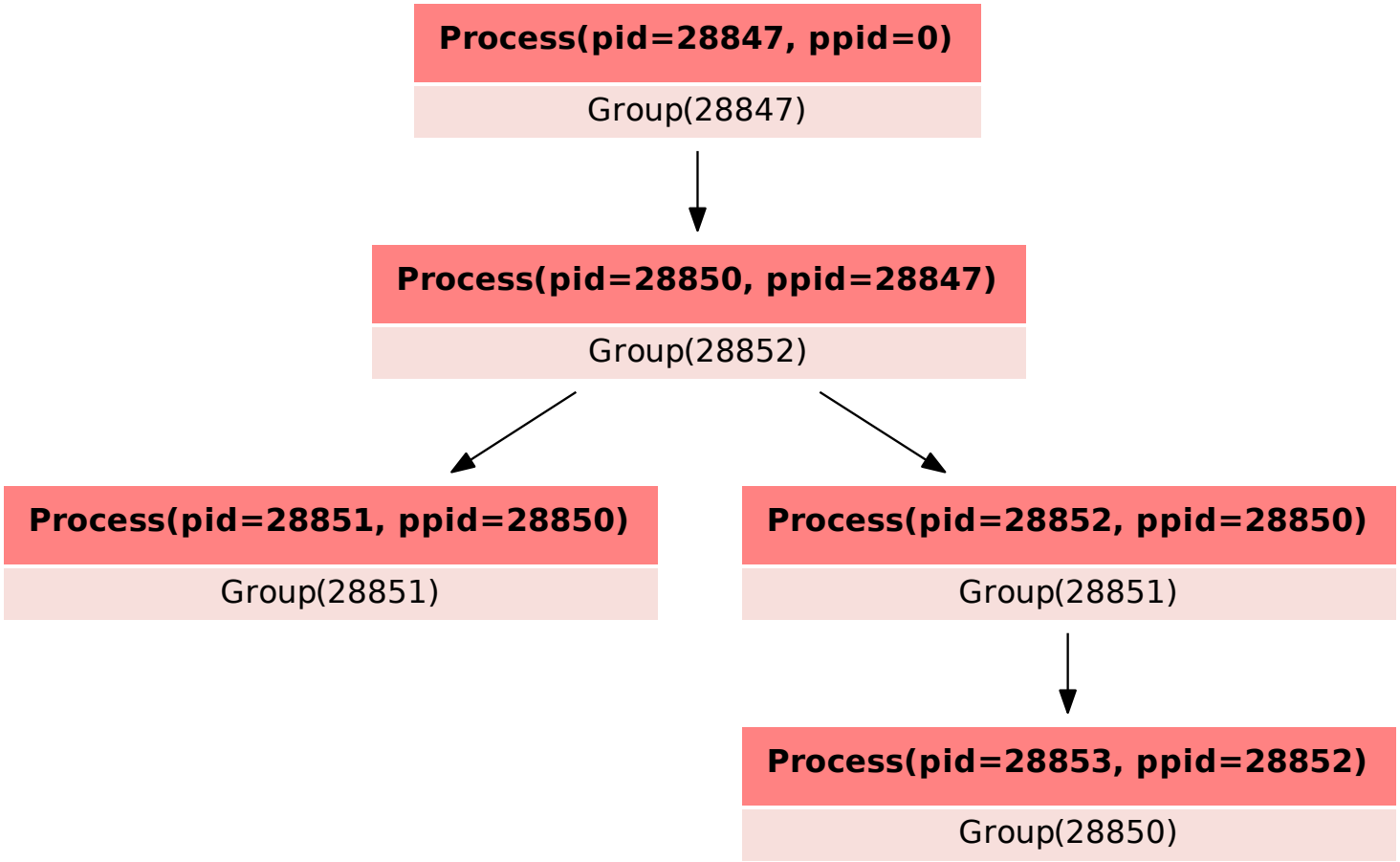
Планы

- Улучшение алгоритма для борьбы с разрешимыми циклами в графе действий
- Реализация интерпретатора команд
- Параллельное исполнение графа действий

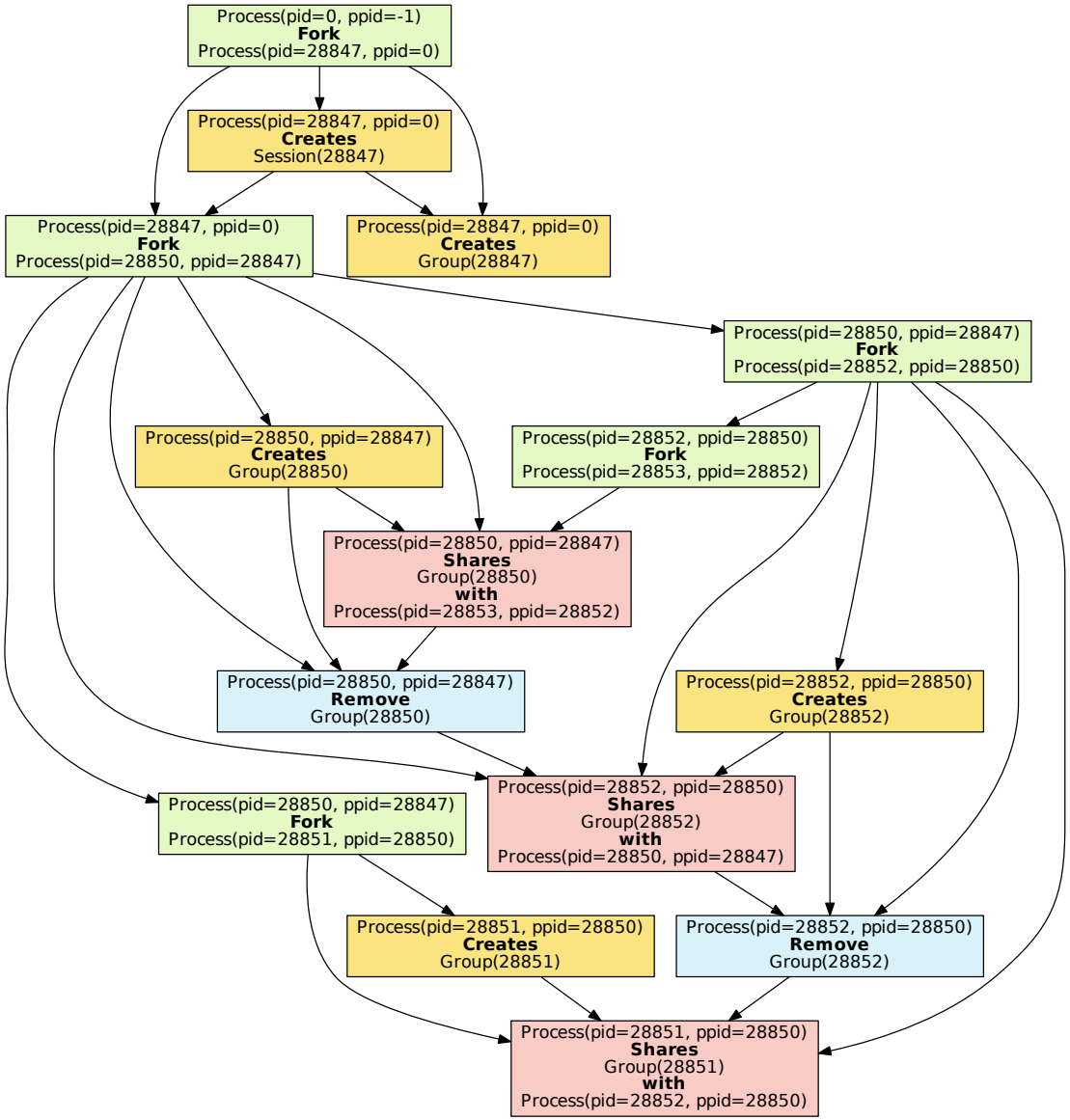
Циклический обмен конфликтующими ресурсами



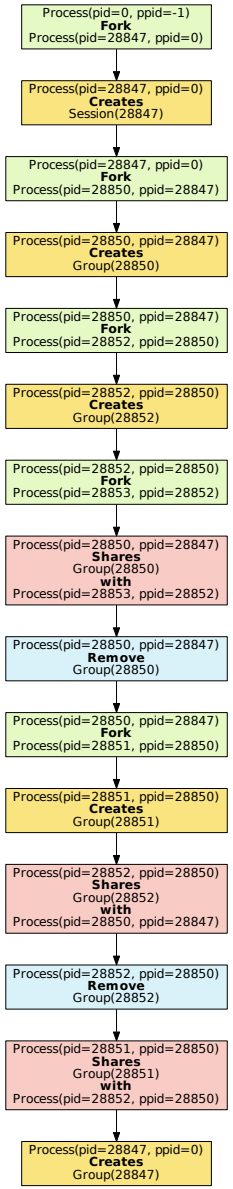
Пример с группами: дерево процессов



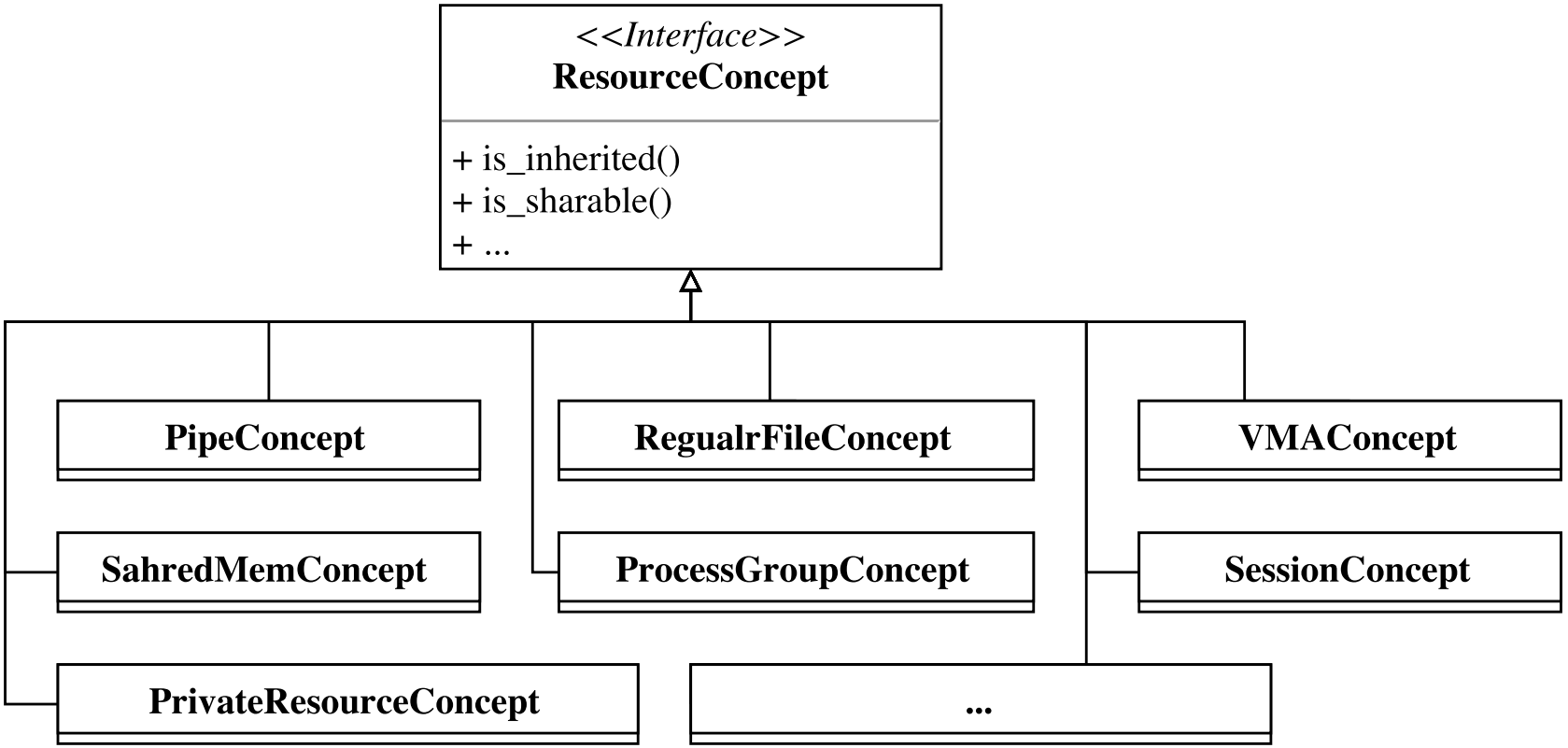
Пример с группами: граф действий



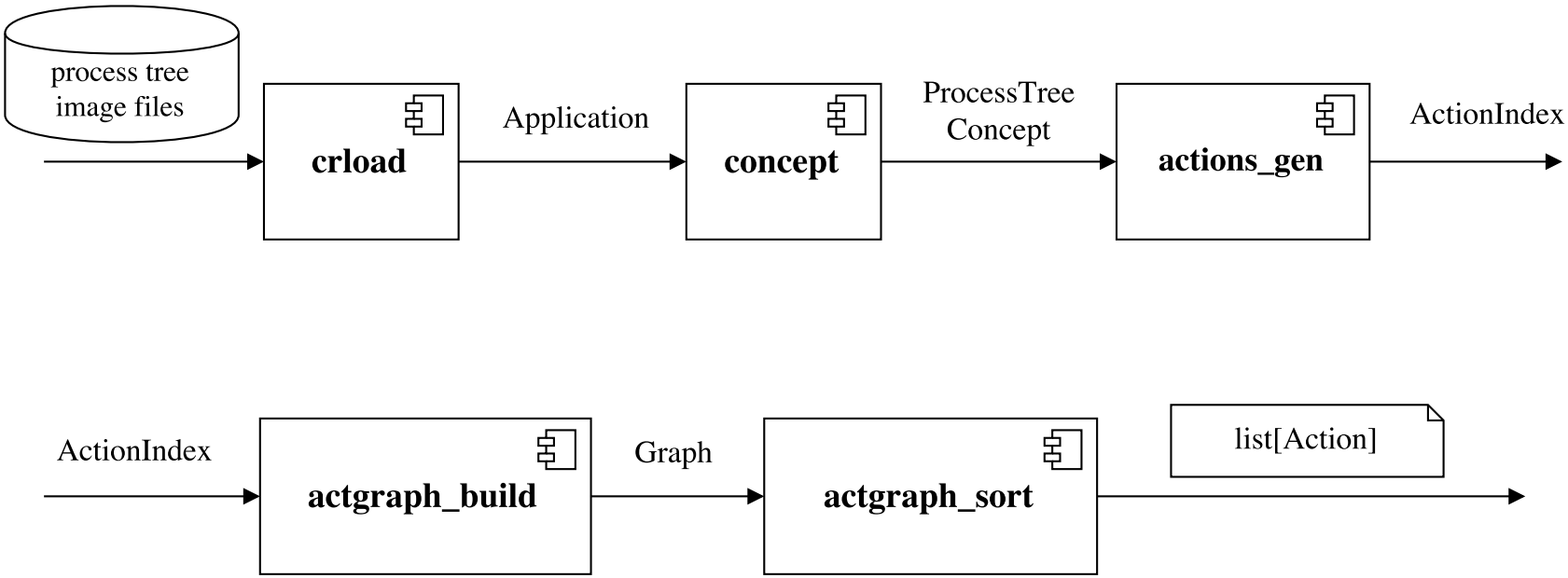
Пример с группами: упорядоченные действия



Иерархия ресурсов



Data flow


process tree
image files
crload
Application
concept
ProcessTree
Concept
actions_gen
ActionIndex
ActionIndex
actgraph_build
Graph
actgraph_sort
list[Action]