А.Н. Непейвода, дополнительные материалы

- Решение уравнений в словах посредством анализа последовательностей конфигураций уравнений в свободном моноиде, удовлетворяющих хорошему предпорядку.
- Поиск атак в пинг-понг протоколах посредством анализа нётеровых последовательностей конфигураций в полугруппах с частичной инволюцией.

$\preceq$ — хороший предпорядок, если во всякой бесконечной последовательности $\{P_i\}$ существуют i, j, такие, что $i < j$ и $P_i \preceq P_j$.

$\preceq$ — нётерово отношение (относительно эквивалентности $\equiv$), если во всякой бесконечной последовательности $\{P_i\}$ такой, что $P_i \preceq P_j$, существует k такое, что $\forall n(n > k \Rightarrow P_n \equiv P_{n+1})$.

Решение уравнений в словах

Основная идея: факторизация путей вычисления уравнения в свободном моноиде по отношению эквивалентности.
Путь вычисления — параметр.

Варианты решателей уравнений

- Базовый (только преобразование Нильсена) $\mathrm{WIBase}_{\mathscr{L}}$;
- С использованием анализа гомоморфных образов уравнений в арифметике:
  - простейший случай — $\mathrm{WICount}_{\mathscr{L}}$;
  - с использованием рекомпрессии (Jez, 2016).
- С использованием уравнений как порождающих полусистему Туэ (как систем переписывания термов) (WiP).

Классы уравнений, для которых последовательности конфигураций вдоль путей вычислений, порождённых решателем, удовлетворяют свойству хорошего предпорядка относительно отношения сводимости уравнений друг к другу, варьируют в зависимости от выбора решателя.

Результаты анализа (за 2021 год)

В качестве инструмента построения остаточной программы использован суперкомпилятор SCP4.

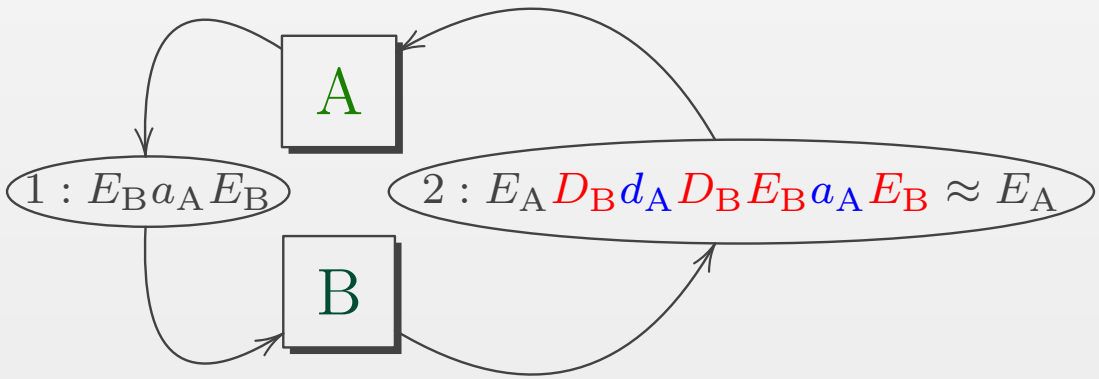
Бенчмарк	Тесты	Неудачи		
		!!! CVC4	!!! Z3str3	!!! $\text{WICount}_{\mathscr{L}}$
Track 1 (Woorpje)!!!	200	8	13	21
Track 5 (Woorpje)!!!	200	4	14	19
Our Track !!!	50	21	28	10

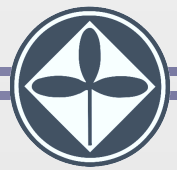
Пинг-понг протокол для двух участников

Легальные пользователи — A, B. Злоумышленник — Z (одного всегда достаточно).
Изначальное сообщение — M (обычно засекреченное).
Σ_x — словарь операторов x. E_x — зашифровка открытым ключом x, D_x — расшифровка E_x, a_x — приписывание к сообщению имени x, d_x — удаление префикса сообщения, совпадающего с именем x.

Протокол — набор α_i (слов протокола) и указаний, кто посылает α_i.

Пример





Модель угрозы по Долеву–Яо

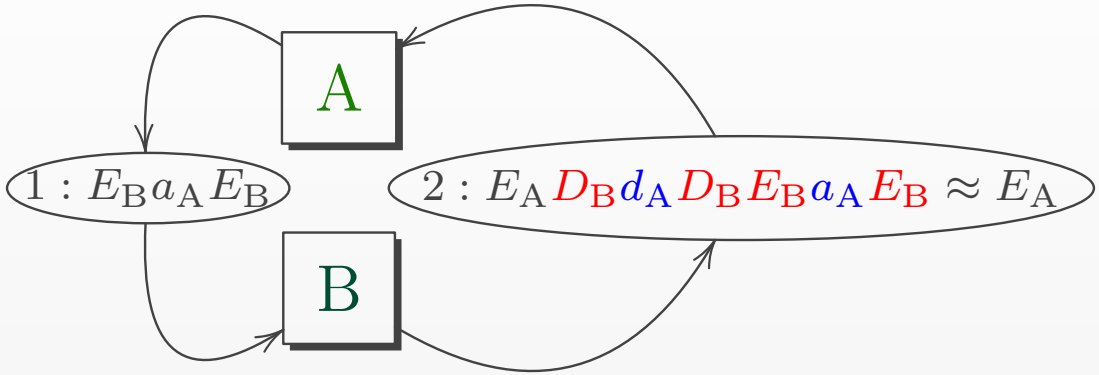
Двухсторонний протокол включает шесть возможных случаев взаимодействия: $\mathbf{P}[\mathrm{A},\mathrm{B}]$, $\mathbf{P}[\mathrm{A},\mathrm{Z}]$, $\mathbf{P}[\mathrm{B},\mathrm{A}]$, $\mathbf{P}[\mathrm{B},\mathrm{Z}]$, $\mathbf{P}[\mathrm{Z},\mathrm{A}]$, $\mathbf{P}[\mathrm{Z},\mathrm{B}]$.

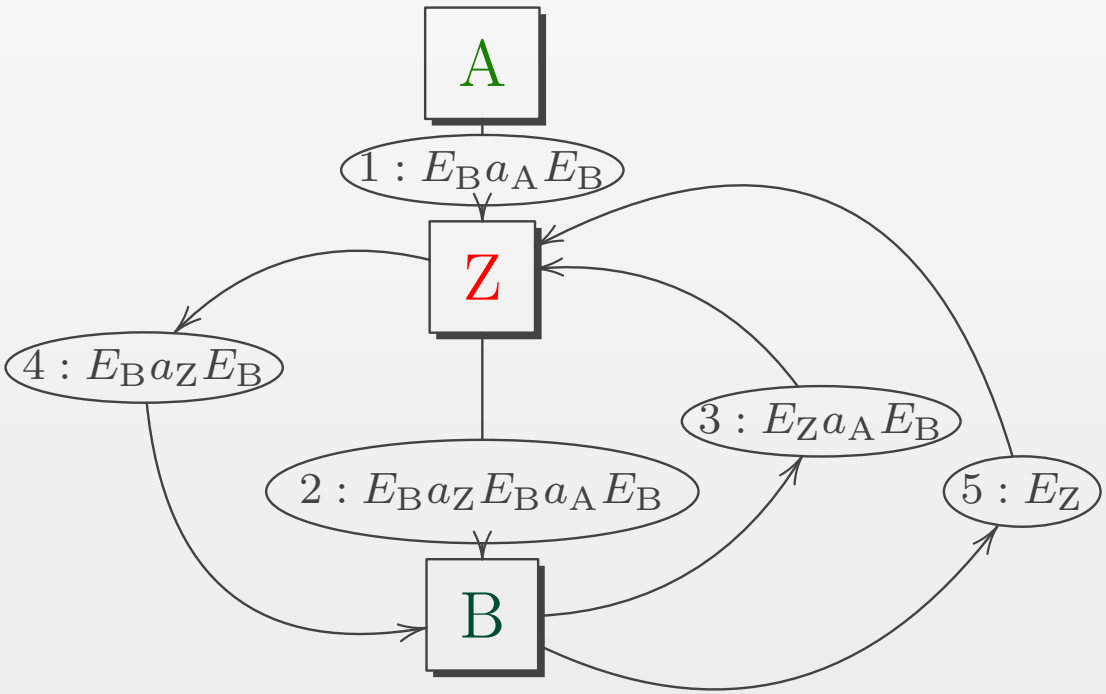
Определение

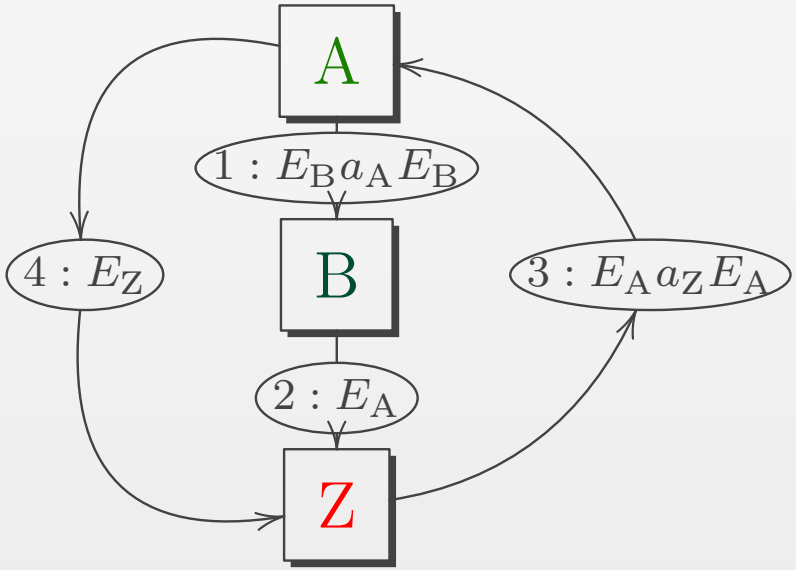
Протокол $\mathbf{P}[\mathrm{A},\mathrm{B}]$ ненадёжен, если существует такая композиция действий протокола (подстановок в слова $\mathbf{P}[\mathrm{U}_1,\mathrm{U}_2]$), применённая к начальному слову $\alpha_1[\mathrm{A},\mathrm{B}](M)$, что злоумышленник может получить доступ к слову из множества INSEC.

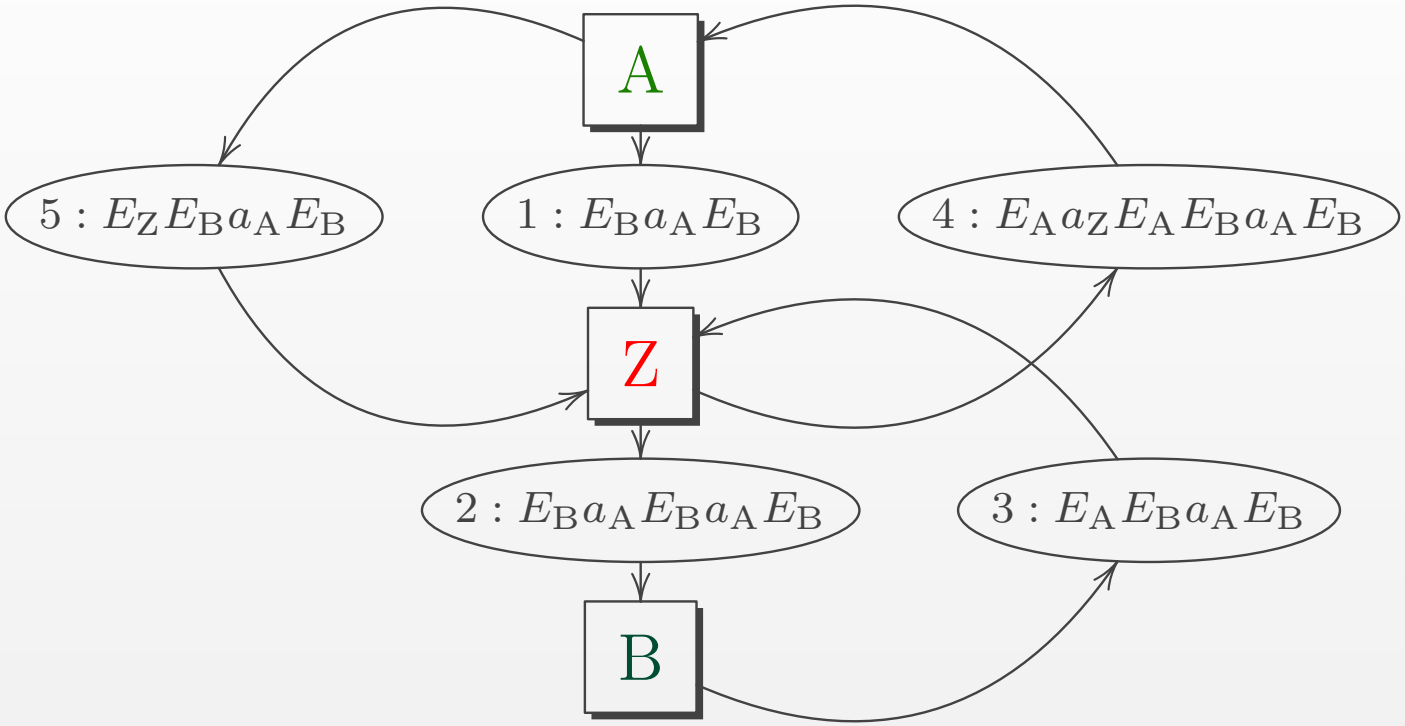
Обычно $\mathrm{INSEC} = \{M\}$ (исходное сообщение).

На один и тот же протокол может быть несколько атак:









После шага 5 Z может применить свой ключ D_Z к $E_Z E_B a_A E_B$, и ситуация повторится. Такие атаки уже не представляют практического интереса.

Алгебра действий в протоколе

- Элементарные действия $\bigcup \Sigma_x$ — конечный алфавит; соотношения $D_x \circ E_x = E_x \circ D_x = \varepsilon$ — частичная инволюция; случаи взаимодействия по протоколу $\mathbf{P}$ — образующие.
- Проверка надёжности: $\mathrm{INSEC} \cap \langle \mathbf{P}[X, Y] \rangle \neq \varnothing$.
- Пути взаимодействия по протоколу $\mathbf{P}$ — слова в префиксной грамматике с базисом $\alpha_1[\mathrm{A}, \mathrm{B}]$ и правилами, определёнными алгеброй действий.
- Нётеровость множества уникальных «атак» в $\mathbf{P}[X, Y]^1, \ldots, \mathbf{P}[X, Y]^n, \ldots \Rightarrow$ критерий остановки символьной интерпретации протокола (развёртки префиксной грамматики).