Распределенные алгоритмы и системы

mk.cs.msu.ru → Лекционные курсы → Распределенные алгоритмы и системы

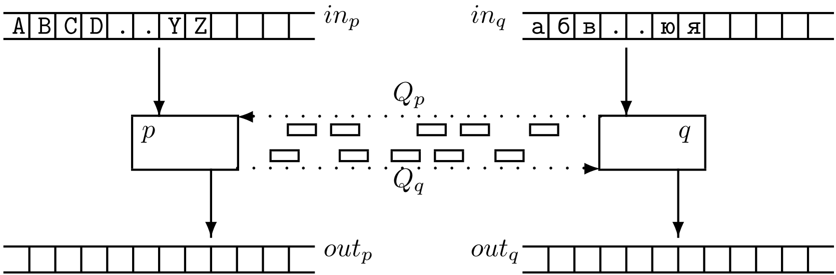
Блок 11

Корректность
симметричного протокола раздвижного окна

Лектор:
Подымов Владислав Васильевич
E-mail:
valdus@yandex.ru

ВМК МГУ, 2022/2023, весенний семестр

Напоминание



Безопасность BSWP: в каждой достижимой конфигурации для каждого номера i верно $out_p[i] \in \{in_q[i], \perp\}$ и значение $out_q[i] \in \{in_p[i], \perp\}$

$$\forall x \in \mathfrak{R}(S) : \forall i \in \mathbb{N}_0 : out_p[i] \in \{in_q[i], \perp\} \,\&\, out_q[i] \in \{in_p[i], \perp\}$$

Живость BSWP для номера k, $k \in \mathbb{N}_0$:
в любом вычислении содержится конфигурация, в которой все значения $out_p[0], \ldots, out_p[k], out_q[0], \ldots, out_q[k]$ отличны от $\perp$

$$\forall \pi \in \Pi(S) : \forall k \in \mathbb{N}_0 : \exists \sigma \in \pi : \forall i \in \{0, 1, \ldots, k\} : out_p[i] \neq \perp \,\&\, out_q \neq \perp$$

Напоминание

var $s_p : \mathbb{N}_0 = 0;$

var $a_p : \mathbb{N}_0 = 0;$

var in_p : **array of word** = все данные для отправки;

var out_p : **array of word** $= (\bot, \bot, \dots);$

Процедура $\mathbf{S}_p$ (предусловие: $a_p < s_p + \ell_p$)

1. Выбрать $i \in \mathbb{N}_0$: $a_p \leq i < s_p + \ell_p$
2. $send(\mathbf{pack}, \langle in_p[i], i\rangle)$

Процедура $\mathbf{R}_p$ (предусловие: очередь Q_p непуста)

1. $receive(\mathbf{pack}, \langle w, i\rangle)$
2. Если $out_p[i] = \bot$:
   - 2.1 $out_p[i] := w;$
   - 2.2 $a_p := \max(a_p, i - \ell_q + 1);$
   - 2.3 $s_p := \min(j \mid out_p[j] = \bot);$

Процедура $\mathbf{L}_p$ (предусловие: очередь Q_p непуста)

1. $receive(\mathbf{pack}, \langle w, i\rangle)$

Будем считать, что переход в с.п. отвечает однократному полному выполнению одной из процедур

Безопасность BSWP

Рассмотрим такую совокупность утверждений:

p^0: $\forall i \in \{0, 1, \ldots, s_p - 1\} : out_p[i] \neq \bot$

p^1: $\forall i \in \mathbb{N}_0 : (\mathbf{pack}, \langle w, i\rangle) \in Q_p \Rightarrow w = in_q[i] \,\&(i < s_q + \ell_q)$

p^2: $\forall i \in \mathbb{N}_0 : out_p[i] \neq \bot \Rightarrow out_p[i] = in_q[i] \,\&(a_p > i - \ell_q)$

p^3: $a_p \leq s_q$

q^0: $\forall i \in \{0, 1, \ldots, s_q - 1\} : out_q[i] \neq \bot$

q^1: $\forall i \in \mathbb{N}_0 : (\mathbf{pack}, \langle w, i\rangle) \in Q_q \Rightarrow w = in_p[i] \,\&(i < s_p + \ell_p)$

q^2: $\forall i \in \mathbb{N}_0 : out_q[i] \neq \bot \Rightarrow out_q[i] = in_p[i] \,\&(a_q > i - \ell_p)$

q^3: $a_q \leq s_p$

$$P_{BSWP} = p^0 \,\&\, p^1 \,\&\, p^2 \,\&\, p^3 \,\&\, q^0 \,\&\, q^1 \,\&\, q^2 \,\&\, q^3$$

Lemma

st= об инварианте BSWP P_{BSWP} *— инвариант BSWP*

Безопасность BSWP

Доказательство.

По определению инварианта, следует доказать два утверждения:

1. Для любой начальной конфигурации γ верно $P_{BSWP}(\gamma)$
2. Если $P_{BSWP}(\gamma)$ и $\gamma \to \delta$, то $P_{BSWP}(\delta)$

1.

p^0: $\forall i \in \{0, 1, \ldots, s_p - 1\} : out_p[i] \neq \bot$

В начальной конфигурации верно $p^0 = 0$

p^1: $\forall i \in \mathbb{N}_0 : (\textbf{pack}, \langle w, i \rangle) \in Q_p \Rightarrow w = in_q[i] \,\&(i < s_q + \ell_q)$

В начальной конфигурации очередь Q_p пуста

p^2: $\forall i \in \mathbb{N}_0 : out_p[i] \neq \bot \Rightarrow out_p[i] = in_q[i] \,\&(a_p > i - \ell_q)$

В начальной конфигурации все значения $out_p[i]$ равны $\bot$

p^3: $a_p \leq s_q$

В начальной конфигурации верно $a_p = 0 \leq 0 = s_q$

q^0, q^1, q^2, q^3 — аналогично

Безопасность BSWP

Доказательство. *2.* $P_{BSWP}(\gamma)\,\&(\gamma \to \delta) \Rightarrow P_{BSWP}(\delta)$

Подробно рассмотрим переход $\gamma \to \delta$, отвечающий выполнению процедуры $\mathbf{R}_p$

Процедура $\mathbf{R}_p$ (предусловие: очередь Q_p непуста)

1. $receive(\mathbf{pack}, \langle w, i\rangle)$
2. Если $out_p[i] = \bot$:
   - 2.1 $out_p[i] := w$;
   - 2.2 $a_p := \max(a_p, i - \ell_q + 1)$;
   - 2.3 $s_p := \min(j \mid out_p[j] = \bot)$;

p^0: $\forall i \in \{0, 1, \dots, s_p - 1\} : out_p[i] \neq \bot$

Если out_p не изменяется, то и s_p не изменяется

Иначе по (2.3) после выполнения $\mathbf{R}_p$ верно $s_p = \min(j \mid out_p[j] = \bot)$

p^1: $\forall i \in \mathbb{N}_0 : (\mathbf{pack}, \langle w, i\rangle) \in Q_p \Rightarrow w = in_q[i]\,\&(i < s_q + \ell_q)$

После выполнения $\mathbf{R}_p$ в Q_p не появляются новые пакеты, in_q не изменяется и s_q не уменьшается

Безопасность BSWP

Доказательство. *2.* $P_{BSWP}(\gamma)\,\&(\gamma \to \delta) \Rightarrow P_{BSWP}(\delta)$

Процедура $\mathbf{R}_p$ (предусловие: очередь Q_p непуста)

1. $receive(\mathbf{pack}, \langle w, i \rangle)$
2. Если $out_p[i] = \perp$:
   - 2.1 $out_p[i] := w$;
   - 2.2 $a_p := \max(a_p, i - \ell_q + 1)$;
   - 2.3 $s_p := \min(j \mid out_p[j] = \perp)$;

p^2: $\forall j \in \mathbb{N}_0 : out_p[j] \neq \perp \Rightarrow out_p[j] = in_q[j]\,\&(a_p > j - \ell_q)$

После выполнения $\mathbf{R}_p$:

- in_q и $out_p[j]$ для всех j, кроме i, не изменяются
- Если перед (2) $out_p[i] \neq \perp$, то out_p и a_p не изменяются
- Если перед (2) $out_p[i] = \perp$, то:
  - Согласно p^1, после (1) верно $w = in_q[i]$
  - Значит, после (2.1) верно $out_p[i] = w = in_q[i]$
  - После (2.2) a_p может только увеличиться, и согласно правой части присваивания, верно $a_p \geq i - \ell_q + 1$, то есть $a_p > i - \ell_q$

Безопасность BSWP

Доказательство. *2.* $P_{BSWP}(\gamma)\,\&(\gamma \to \delta) \Rightarrow P_{BSWP}(\delta)$

Процедура $\mathbf{R}_p$ (предусловие: очередь Q_p непуста)

1. $\mathit{receive}(\mathbf{pack}, \langle w, i\rangle)$
2. Если $\mathit{out}_p[i] = \bot$:
   - 2.1 $\mathit{out}_p[i] := w$;
   - 2.2 $a_p := \max(a_p, i - \ell_q + 1)$;
   - 2.3 $s_p := \min(j \mid \mathit{out}_p[j] = \bot)$;

p^3: $a_p \leq s_q$

После выполнения $\mathbf{R}_p$:

- Значение s_q не изменяется
- Если перед (2) $\mathit{out}_p \neq \bot$, то и значение a_p не изменяется
- Если перед (2) $\mathit{out}_p = \bot$, то после (2.2):
  - Из p^1 следует $i < s_q + \ell_q$
  - Значит, $i - \ell_q + 1 < s_q + 1$, то есть $i - \ell_q + 1 \leq s_q$
  - Если a_p изменяется, то $a_p = i - \ell_q + 1 \leq s_q$

Безопасность BSWP

Доказательство. *2.* $P_{BSWP}(\gamma)\,\&(\gamma \to \delta) \Rightarrow P_{BSWP}(\delta)$

Процедура $\mathbf{R}_p$ (предусловие: очередь Q_p непуста)

1. $receive(\mathbf{pack}, \langle w, i \rangle)$
2. Если $out_p[i] = \perp$:
   - 2.1 $out_p[i] := w$;
   - 2.2 $a_p := \max(a_p, i - \ell_q + 1)$;
   - 2.3 $s_p := \min(j \mid out_p[j] = \perp)$;

q^0: $\forall i \in \{0, 1, \dots, s_q - 1\} : out_q[i] \neq \perp$

Значения s_q и out_q не изменяются

q^1: $\forall i \in \mathbb{N}_0 : (\mathbf{pack}, \langle w, i \rangle) \in Q_q \Rightarrow w = in_p[i]\,\&(i < s_p + \ell_p)$

Значение s_p не уменьшается, значения Q_q и in_p не изменяются

q^2: $\forall i \in \mathbb{N}_0 : out_q[i] \neq \perp \Rightarrow out_q[i] = in_p[i]\,\&(a_q > i - \ell_p)$

Значения out_q, in_p и a_q не изменяются

q^3: $a_q \leq s_p$

Значение a_q не изменяется, s_p — не уменьшается

Безопасность BSWP

Доказательство. *2.* $P_{BSWP}(\gamma)\,\&(\gamma \to \delta) \Rightarrow P_{BSWP}(\delta)$

Процедура $\mathbf{S}_p$ (предусловие: $a_p < s_p + \ell_p$)

1. Выбрать $i \in \mathbb{N}_0$: $a_p \leq i < s_p + \ell_p$
2. $send(\mathbf{pack}, \langle in_p[i], i\rangle)$

Процедура $\mathbf{L}_p$ (предусловие: очередь Q_p непуста)

1. $receive(\mathbf{pack}, \langle w, i\rangle)$

Задача 1. Завершить доказательство для этих двух процедур

▼

Безопасность BSWP

Теорема (безопасность BSWP). **С.п. S BSWP обладает свойством безопасности BSWP**

$$\forall x \in \mathfrak{R}(S) : \forall i \in \mathbb{N}_0 : out_p[i] \in \{in_q[i], \bot\} \,\&\, out_q[i] \in \{in_p[i], \bot\}$$

Доказательство.

По последней лемме, P_{BSWP} — инвариант BSWP

При этом из P_{BSWP} следуют

- p^2 $(\forall i \in \mathbb{N}_0 : out_p[i] \neq \bot \Rightarrow out_p[i] = in_q[i] \,\&(a_p > i - \ell_q))$, из чего следует $\forall i \in \mathbb{N}_0 : out_p[i] \in \{in_q[i], \bot\}$
- q^2 $(\forall i \in \mathbb{N}_0 : out_q[i] \neq \bot \Rightarrow out_q[i] = in_p[i] \,\&(a_q > i - \ell_p))$, из чего следует $\forall i \in \mathbb{N}_0 : out_q[i] \in \{in_p[i], \bot\}$

Значит, из P_{BSWP} следует
$\forall i \in \mathbb{N}_0 : out_p[i] \in \{in_q[i], \bot\} \,\&\, out_q[i] \in \{in_p[i], \bot\}$

Осталось только применить теорему о проверке безопасности с.п. ▼

Живость BSWP

К сожалению, если не наложить на устройство и выполнения BSWP дополнительных ограничений, то он не будет обладать свойством живости (Почему?)

Ограничения на устройство протокола:

- Все элементы in_p и in_q отличны от $\perp$
- $\ell_p, \ell_q \in \mathbb{N}_0$, $\ell_p + \ell_q > 0$

Ограничения справедливости:

F1 Если бесконечно часто возникает возможность отправки пакета, то этот пакет будет отправляться бесконечно часто

F2 Если пакет отправляется бесконечно часто, то он и принимается бесконечно часто

BSWP с этими ограничениями будем обозначать BSWP*

Оказывается, что этих ограничений достаточно для обеспечения живости протокола

Живость BSWP

Лемма (об узости окна). В любой достижимой конфигурации BSWP* верно:

$$s_p - \ell_q \le a_p \le s_q \le a_q + \ell_p \le s_p + \ell_p$$

Доказательство.

По теореме о безопасности инварианта, любая достижимая конфигурация BSWP* обладает свойством P_{BSWP}

Неравенство $s_p - \ell_q \le a_p$ следует из

- p^0 $(\forall i \in \{0, 1, \dots, s_p - 1\} : out_p[i] \ne \perp)$ и
- p^2 $(\forall i \in \mathbb{N}_0 : out_p[i] \ne \perp \Rightarrow out_p[i] = in_q[i] \,\&(a_p > i - \ell_q))$

Неравенство $a_p \le s_q$ — это условие p^3

Неравенство $s_q \le a_q + \ell_p$ (то есть $s_q - \ell_p \le a_q$) следует из q^0 и q^2

Неравенство $a_q + \ell_p \le s_p + \ell_p$ (то есть $a_q \le s_p$) — это условие q^3 ▼

Таким образом, створки s_q и $a_q + \ell_p$ окна узла q отстоят друг от друга не более чем на $\ell_p + \ell_q$ (аналогично — створки окна узла p)

Живость BSWP

Лемма (об открытости окна). В любой достижимой конфигурации BSWP* выполнено хотя бы одно из предусловий процедур отправки пакета $\mathbf{S}_p$ ($a_p < s_p + \ell_p$), $\mathbf{S}_q$ ($a_q < s_q + \ell_q$)

Доказательство.

По лемме об узости окна, верны неравенства

$$s_p - \ell_q \leq a_p \leq s_q \leq a_q + \ell_p \leq s_p + \ell_p$$

В частности, это означает, что $a_p \leq s_q$ и $a_q + \ell_p \leq s_p + \ell_p$

То есть $a_p \leq s_q$ и $a_q \leq s_p$

Кроме того, согласно ограничению $\ell_p + \ell_q > 0$, верно $s_p - \ell_q < s_p + \ell_p$

Следовательно, хотя бы одно из неравенств леммы об узости окна является строгим

Последнее означает, в частности, что $s_p - \ell_q < s_q \vee s_q < s_p + \ell_p$

То есть $s_p < s_q + \ell_q \vee s_q < s_p + \ell_p$

Следовательно, верно $a_p \leq s_q < s_p + \ell_p \vee a_q \leq s_p < s_q + \ell_q$ ▼

Живость BSWP

Теорема (живость BSWP). С.п. S BSWP* в условиях справедливости (F1) и (F2) обладает свойством живости BSWP

$$\forall \pi \in \Pi(S) : \forall k \in \mathbb{N}_0 : \exists \sigma \in \pi : \forall i \in \{0, 1, \dots, k\} : out_p[i] \neq \bot \,\&\, out_q \neq \bot$$

Доказательство.

Согласно p^0 ($\forall i \in \{0, 1, \dots, s_p - 1\} : out_p[i] \neq \bot$), q^0 ($\forall i \in \{0, 1, \dots, s_q - 1\} : out_q[i] \neq \bot$) и безопасности BSWP, достаточно показать, что каждое из значений s_p, s_q увеличивается бесконечно часто

Предположим от противного, что это не так

По лемме об узости окна, верны неравенства $s_p - \ell_q \leq s_q \leq s_p + \ell_p$ и $s_q - \ell_p \leq s_p \leq s_q + \ell_q$, а значит, значения обеих переменных s_p, s_q увеличиваются лишь конечное число раз

Пусть k_p, k_q — наибольшие значения s_p и s_q соответственно

Живость BSWP

Теорема (живость BSWP). С.п. S BSWP* в условиях справедливости (F1) и (F2) обладает свойством живости BSWP

$\forall \pi \in \Pi(S) : \forall k \in \mathbb{N}_0 : \exists \sigma \in \pi : \forall i \in \{0, 1, \ldots, k\} : out_p[i] \neq \perp \,\&\, out_q \neq \perp$

Доказательство.

По лемме об открытости окна, бесконечно часто допустимо действие отправления хотя бы одного из пакетов $(\mathbf{pack}, \langle in_p[k_q], k_q\rangle)$, $(\mathbf{pack}, \langle in_q[k_p], k_p\rangle)$

Пусть, для ясности, это пакет $(\mathbf{pack}, \langle in_q[k_p], k_p\rangle)$

Согласно (F1), этот пакет отправляется бесконечно часто

Согласно (F2), этот пакет принимается бесконечно часто

По устройству протокола и ограничению $in_q[k_p] \neq \perp$, приём этого сообщения приводит к увеличению значения s_p (*противоречие*) ▼

Живость BSWP

Задача 2. Покажите, что последняя теорема перестаёт быть верной, если убрать хотя бы одно из ограничений (F1), (F2), и для этого приведите соответствующий «неживой» сценарий выполнения протокола

Задача 3. Докажите, что если в BSWP* выполняется равенство $\ell_p + \ell_q = 1$ и начальные значения a_p и a_q заменить соответственно на $-\ell_q$ и $-\ell_p$, то во всех достижимых конфигурациях выполняются равенства $a_p + \ell_q = s_p$ и $a_q + \ell_p = s_q$