Распределенные алгоритмы и системы

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

Блок 14

Корректность протокола с таймерами

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

ВМК МГУ, 2022/2023, весенний семестр

Напоминание

Рассматриваемая задача: передать массив in_p от генератора через отправителя p получателю q с вручением потребителю по возрастанию номеров

Основные свойства:

1. Отсутствие потерь: для некоторой константы C каждое слово из in_p спустя время C после поступления от генератора будет вручено потребителю или помечено как вероятно потерянное
2. Соблюдение порядка: данные вручаются узлом q согласно возрастанию номеров в in_p

Параметры протокола:

- $\mu \in \mathbb{R}$, $\mu > 0$
- $\mathbf{t} \in \mathbb{R}$, $\mathbf{t} > 0$
- $\mathbf{r} \in \mathbb{R}$, $\mathbf{r} \geq \mathbf{t} + \mu$
- $\mathbf{s} \in \mathbb{R}$, $\mathbf{s} \geq \mathbf{r} + 2\mu$

Напоминание: код отправителя (p)

var in_p : **array of word**

var $Low, High : \mathbb{N}_0 = 0$

var $\vec{\tau}_t$: **array of timer** $= (0, 0, \ldots)$

var τ_s : **timer** $= 0$

var c_p : **bool** $= \mathbb{f}$

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

Поступление блока (G$_p$)

1. Если $c_p = \mathbb{f}$, то устанавливается соединение:
   1.1 $c_p := \mathbb{t}$;
   1.2 $\tau_s := \mathbf{s}$;
2. $\vec{\tau}_t[N + High] := \mathbf{t}$;
3. $High := High + 1$;

Отправка блока (S$_p$)

Предусловие: $c_p \,\&\, Low \leq i < High \,\&\, \vec{\tau}_t[N + i] > 0$

1. $send(\mathbf{data}, (i = Low), i, in_p[N + i], \mu$
2. $\tau_s := \mathbf{s}$;

Напоминание: код отправителя (p)

Приём подтверждения ($\mathbf{R}_p$)

Предусловие: $c_p \,\&\, (\mathbf{ack}, \langle i, \rho \rangle) \in M_p$

1. $\mathit{receive}(\mathbf{ack}, \langle i, \rho \rangle)$
2. $\mathit{Low} := \max(\mathit{Low}, i);$

Пометка блока как потерянного ($\mathbf{L}_p$)

Предусловие: $c_p \,\&\, \vec{\tau}_t[N + \mathit{Low}] \leq -(\mathbf{r} + 2\mu)$

1. $\mathit{lost}[N + \mathit{Low}] := \mathbb{t};$
2. $\mathit{Low} := \mathit{Low} + 1;$

Завершение соединения ($\mathbf{C}_p$)

Предусловие: $c_p \,\&\, \tau_s < 0 \,\&\, \mathit{Low} = \mathit{High}$

1. $N := N + \mathit{High};$
2. $\mathit{Low} := 0;$
3. $\mathit{High} := 0;$
4. Завершить соединение: $c_p := \mathbb{f};$

Напоминание: код получателя (q)

var $Exp : \mathbb{N}_0$ **var** τ_r : **timer** **var** c_q : **bool** $= \mathbb{f}$

Получение пакета ($\mathbf{R}_q$)

Предусловие: $(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q$

1. $receive(\mathbf{data}, \langle b, i, d, \rho \rangle)$
2. Если $c_q = \mathbb{f} \;\&\; b = \mathbb{t}$:
   2.1 Устанавливается соединение: $c_q := \mathbb{t}$;
   2.2 $\tau_r := \mathbf{r}$;
   2.3 $Exp := i + 1$;
   2.4 $done(d)$
3. Если $c_q = \mathbb{t} \;\&\; i = Exp$:
   3.1 $\tau_r := \mathbf{r}$;
   3.2 $Exp := Exp + 1$;
   3.3 $done(d)$

Отправка подтверждения ($\mathbf{S}_q$)

Предусловие: c_q

1. $send(\mathbf{ack}, \langle Exp, \mu \rangle)$

Напоминание: код среды (Ω)

Потеря сообщения (Loss)

Предусловие: $m \in M_x \,\&\, x \in \{p, q\}$

1. $M_x := M_x - \{m\}$;

Дублирование сообщения (Dup)

Предусловие: $m \in M_x \,\&\, x \in \{p, q\}$

1. $M_x := M_x + \{m\}$;

Течение времени (Time)

1. Выбрать произвольное значение $\Delta \in \mathbb{R}$, $\Delta > 0$
2. Для каждого $i \in \mathbb{N}_0$: $\vec{\tau}_t[i] := \vec{\tau}_t[i] - \Delta$;
3. $\tau_s := \tau_s - \Delta$;
4. $\tau_r := \tau_r - \Delta$;
5. Если $\tau_r \leq 0$:
   - 5.1 Завершить соединение в q: $c_q := \mathbb{f}$;
6. Для каждого пакета $m = (\ldots, \langle \ldots, \rho \rangle) \in M_x$, $x \in \{p, q\}$:
   - 6.1 $\rho := \rho - \Delta$;
   - 6.2 Если $\rho \leq 0$:
     - 6.2.1 $M_x := M_x - \{m\}$;

Основной инвариант

Основной инвариант, на котором основывается обоснование корректности протокола, устроим так:

$P_{\Delta t} = p^1 \,\&\, p^2 \,\&\, p^3 \,\&\, p^4 \,\&\, p^5 \,\&\, p^6 \,\&\, p^7 \,\&\, p^8 \,\&\, p^9$, где:

p^1: $c_p \Rightarrow \tau_s \leq \mathbf{s}$

p^2: $c_q \Rightarrow 0 \leq \tau_r \leq \mathbf{r}$

p^3: $\forall i \in \mathbb{N}_0 : \vec{\tau}_t[i] \leq \mathbf{t}$

p^4: $\forall(\ldots, \langle \ldots, \rho \rangle) \in M_p \cup M_q : 0 < \rho \leq \mu$

p^5: $\forall(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : c_p \,\&\, \tau_s \geq \rho + \mu + \mathbf{r}$

p^6: $c_q \Rightarrow c_p \,\&\, \tau_s \geq \tau_r + \mu$

p^7: $\forall(\mathbf{ack}, \langle i, \rho \rangle) \in M_p : c_p \,\&\, \tau_s > \rho$

p^8: $\forall(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : d = in_p[N + i] \,\&\, i < High$

p^9: $\neg c_p \Rightarrow High = 0$

Теорема. $P_{\Delta t}$ **— инвариант протокола с таймерами**

Основной инвариант (доказательство)

Справедливость $P_{\Delta t}$ в начальной конфигурации следует из равенств $N = High = 0$, $c_p = c_q = \mathbb{f}$ и $M_p = M_q = \emptyset$

Основная часть доказательства посвящена соотношению $P_{\Delta t} \to P_{\Delta t}$

Поступление блока ($\mathbf{G}_p$)

1. Если $c_p = \mathbb{f}$, то устанавливается соединение:
   1.1 $c_p := \mathbb{t}$;
   1.2 $\tau_s := \mathbf{s}$;
2. $\vec{\tau}_t[N + High] := \mathbf{t}$;
3. $High := High + 1$;

p^1 $(c_p \Rightarrow \tau_s \leq \mathbf{s})$

Справедливость p^1 после выполнения $\mathbf{G}_p$ следует из того, что значение τ_s либо не изменяется, либо становится равным $\mathbf{s}$

p^2, p^4 $(c_q \Rightarrow 0 \leq \tau_r \leq \mathbf{r};\ \forall(\ldots, \langle \ldots, \rho\rangle) \in M_p \cup M_q : 0 < \rho \leq \mu)$

Следует из того, что переменные, используемые в этих соотношениях, не изменяются

Основной инвариант (доказательство)

Поступление блока ($\mathbf{G}_p$)

1. Если $c_p = \mathbb{f}$, то устанавливается соединение:
   1.1 $c_p := \mathbb{t}$;
   1.2 $\tau_s := \mathbf{s}$;
2. $\vec{\tau}_t[N + High] := \mathbf{t}$;
3. $High := High + 1$;

p^3 $(\forall i \in \mathbb{N}_0 : \vec{\tau}_t[i] \leq \mathbf{t})$

Следует из того, что значение $\vec{\tau}_t[N + High]$ становится равным $\mathbf{t}$, а значения остальных таймеров не изменяются

p^5, p^6, p^7 $(\forall(\mathbf{data}, \langle b, i, d, \rho\rangle) \in M_q : c_p \,\&\, \tau_s \geq \rho + \mu + \mathbf{r}$; $c_q \Rightarrow c_p \,\&\, \tau_s \geq \tau_r + \mu$; $\forall(\mathbf{ack}, \langle i, \rho\rangle) \in M_p : c_p \,\&\, \tau_s > \rho)$

Следует из того, что значение τ_s не уменьшается

p^8 $(\forall(\mathbf{data}, \langle b, i, d, \rho\rangle) \in M_q : d = in_p[N + i] \,\&\, i < High)$

Следует из того, что значение $High$ не уменьшается

p^9 $(\neg c_p \Rightarrow High = 0)$

Следует из того, что значение c_p становится равным $\mathbb{t}$

Основной инвариант (доказательство)

Отправка блока ($\mathbf{S}_p$)

Предусловие: $c_p \,\&\, Low \le i < High \,\&\, \vec{\tau}_t[N+i] > 0$

1. $send(\mathbf{data}, (i = Low), i, in_p[N+i], \mu$
2. $\tau_s := \mathbf{s}$;

p^1 $(c_p \Rightarrow \tau_s \le \mathbf{s})$

Следует из того, что значение τ_s становится равным $\mathbf{s}$

p^2, p^3 $(c_q \Rightarrow 0 \le \tau_r \le \mathbf{r};\ \forall i \in \mathbb{N}_0 : \vec{\tau}_t[i] \le \mathbf{t})$

Следует из того, что переменные, используемые в этих соотношениях, не изменяются

p^4 $(\forall(\dots, \langle \dots, \rho \rangle) \in M_p \cup M_q : 0 < \rho \le \mu)$

Следует из того, что отправляемый пакет имеет время жизни μ, а время жизни остальных пакетов не изменяется

p^5 $(\forall(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : c_p \,\&\, \tau_s \ge \rho + \mu + \mathbf{r})$

Следует из того, что

- c_p входит в предусловие и не изменяется;
- по p^4 и $\mathbf{s} \ge \mathbf{r} + 2\mu$, становится верно $\tau_s = \mathbf{s} \ge \mathbf{r} + 2\mu \ge \rho + \mu + \mathbf{r}$

Основной инвариант (доказательство)

Отправка блока ($\mathbf{S}_p$)

Предусловие: $c_p \mathbin{\&} Low \leq i < High \mathbin{\&} \vec{\tau}_t[N+i] > 0$

1. $send(\mathbf{data}, (i = Low), i, in_p[N+i], \mu$
2. $\tau_s := \mathbf{s}$;

p^6, p^7 $(c_q \Rightarrow c_p \mathbin{\&} \tau_s \geq \tau_r + \mu; \forall(\mathbf{ack}, \langle i, \rho \rangle) \in M_p : c_p \mathbin{\&} \tau_s > \rho)$

Следует из того, что значение τ_s не может уменьшиться

p^8 $(\forall(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : d = in_p[N+i] \mathbin{\&} i < High)$

Следует из того, что для отправляемого пакета соотношения выполняются (согласно предусловию и виду команды отправки), а остальные пакеты не изменяются

p^9 $(\neg c_p \Rightarrow High = 0)$

Следует из предусловия c_p и того, что значение c_p не изменяется

Основной инвариант (доказательство)

Приём подтверждения (R_p)

Предусловие: $c_p \,\&(\mathbf{ack}, \langle i, \rho\rangle) \in M_p$

1. $\mathit{receive}(\mathbf{ack}, \langle i, \rho\rangle)$
2. $\mathit{Low} := \max(\mathit{Low}, i)$;

p^1: $c_p \Rightarrow \tau_s \leq \mathbf{s}$

p^2: $c_q \Rightarrow 0 \leq \tau_r \leq \mathbf{r}$

p^3: $\forall i \in \mathbb{N}_0 : \vec{\tau}_t[i] \leq \mathbf{t}$

p^4: $\forall(\ldots, \langle \ldots, \rho\rangle) \in M_p \cup M_q : 0 < \rho \leq \mu$

p^5: $\forall(\mathbf{data}, \langle b, i, d, \rho\rangle) \in M_q : c_p \,\&\, \tau_s \geq \rho + \mu + \mathbf{r}$

p^6: $c_q \Rightarrow c_p \,\&\, \tau_s \geq \tau_r + \mu$

p^7: $\forall(\mathbf{ack}, \langle i, \rho\rangle) \in M_p : c_p \,\&\, \tau_s > \rho$

p^8: $\forall(\mathbf{data}, \langle b, i, d, \rho\rangle) \in M_q : d = \mathit{in}_p[N + i] \,\&\, i < \mathit{High}$

p^9: $\neg c_p \Rightarrow \mathit{High} = 0$

Следует из того, что все значения, используемые в $P_{\Delta t}$, кроме M_p, не изменяются, а изменение M_p состоит в удалении одного элемента (что сохраняет истинность p^4 и p^7 согласно смыслу $\forall$)

Основной инвариант (доказательство)

Пометка блока как потерянного ($\mathbf{L}_p$)

Предусловие: $c_p \,\&\, \vec{\tau}_t[N + Low] \le -(\mathbf{r} + 2\mu)$

1. $lost[N + Low] := \mathbb{t};$
2. $Low := Low + 1;$

p^1: $c_p \Rightarrow \tau_s \le \mathbf{s}$

p^2: $c_q \Rightarrow 0 \le \tau_r \le \mathbf{r}$

p^3: $\forall i \in \mathbb{N}_0 : \vec{\tau}_t[i] \le \mathbf{t}$

p^4: $\forall(\ldots, \langle \ldots, \rho \rangle) \in M_p \cup M_q : 0 < \rho \le \mu$

p^5: $\forall(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : c_p \,\&\, \tau_s \ge \rho + \mu + \mathbf{r}$

p^6: $c_q \Rightarrow c_p \,\&\, \tau_s \ge \tau_r + \mu$

p^7: $\forall(\mathbf{ack}, \langle i, \rho \rangle) \in M_p : c_p \,\&\, \tau_s > \rho$

p^8: $\forall(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : d = in_p[N + i] \,\&\, i < High$

p^9: $\neg c_p \Rightarrow High = 0$

Следует из того, что все значения, используемые в $P_{\Delta t}$, не изменяются

Основной инвариант (доказательство)

Завершение соединения (C_p)

Предусловие: $c_p \,\&\, \tau_s < 0 \,\&\, Low = High$

1. $N := N + High$;
2. $Low := 0$;
3. $High := 0$;
4. Завершить соединение: $c_p := \mathbb{f}$;

p^1 $(c_p \Rightarrow \tau_s \leq \mathbf{s})$

Следует из того, что c_p становится равным $\mathbb{f}$

p^2, p^3, p^4 $(c_q \Rightarrow 0 \leq \tau_r \leq \mathbf{r};\ \forall i \in \mathbb{N}_0 : \vec{\tau}_t[i] \leq \mathbf{t};$
$\forall (\ldots, \langle \ldots, \rho \rangle) \in M_p \cup M_q : 0 < \rho \leq \mu)$

Следует из того, что значения, используемые в этих утверждениях, не изменяются

p^9 $(\neg c_p \Rightarrow High = 0)$

Следует из присваивания (3)

Основной инвариант (доказательство)

Завершение соединения (C_p)

Предусловие: $c_p \,\&\, \tau_s < 0 \,\&\, Low = High$

1. $N := N + High$;
2. $Low := 0$;
3. $High := 0$;
4. Завершить соединение: $c_p := \mathbb{f}$;

p^5, p^6, p^7, p^8 $(\forall(\mathbf{data}, \langle b, i, d, \rho\rangle) \in M_q : c_p \,\&\, \tau_s \geq \rho + \mu + \mathbf{r}$; $c_q \Rightarrow c_p \,\&\, \tau_s \geq \tau_r + \mu$; $\forall(\mathbf{ack}, \langle i, \rho\rangle) \in M_p : c_p \,\&\, \tau_s > \rho$; $\forall(\mathbf{data}, \langle b, i, d, \rho\rangle) \in M_q : d = in_p[N + i] \,\&\, i < High)$

Если $M_q \neq \emptyset$ или $c_q = \mathbb{t}$ или $M_p \neq \emptyset$, то из соответствующего утверждения p^5, p^6, p^7 и из p^2 можно получить справедливость $\tau_s \geq 0$ перед выполнением, что противоречит предусловию $(\tau_s < 0)$

Значит, перед выполнением верно $M_p = M_q = \emptyset$ и $c_q = \mathbb{f}$, как и после выполнения (эти значения не изменяются), откуда следуют p^5, p^6, p^7, p^8 по смыслу $\forall$ и $\Rightarrow$

Основной инвариант (доказательство)

Получение пакета ($\mathbf{R}_q$)

Предусловие: $(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q$

1. $receive(\mathbf{data}, \langle b, i, d, \rho \rangle)$
2. Если $c_q = \mathbb{f} \,\&\, b = \mathbb{t}$: $c_q := \mathbb{t}$; $\tau_r := \mathbf{r}$; $Exp := i + 1$; $done(d)$
3. Если $c_q = \mathbb{t} \,\&\, i = Exp$: $\tau_r := \mathbf{r}$; $Exp := Exp + 1$; $done(d)$

p^1: $c_p \Rightarrow \tau_s \leq \mathbf{s}$

p^3: $\forall i \in \mathbb{N}_0 : \vec{\tau}_t[i] \leq \mathbf{t}$

p^4: $\forall (\ldots, \langle \ldots, \rho \rangle) \in M_p \cup M_q : 0 < \rho \leq \mu$

p^5: $\forall (\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : c_p \,\&\, \tau_s \geq \rho + \mu + \mathbf{r}$

p^7: $\forall (\mathbf{ack}, \langle i, \rho \rangle) \in M_p : c_p \,\&\, \tau_s > \rho$

p^8: $\forall (\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : d = in_p[N + i] \,\&\, i < High$

p^9: $\neg c_p \Rightarrow High = 0$

Следует из того, что используемые значения не изменяются

Основной инвариант (доказательство)

Получение пакета (R_q)

Предусловие: $(\mathbf{data}, \langle b, i, d, \rho\rangle) \in M_q$

1. $receive(\mathbf{data}, \langle b, i, d, \rho\rangle)$
2. Если $c_q = \mathbb{f} \,\&\, b = \mathbb{t}$: $c_q := \mathbb{t}$; $\tau_r := \mathbf{r}$; $Exp := i + 1$; $done(d)$
3. Если $c_q = \mathbb{t} \,\&\, i = Exp$: $\tau_r := \mathbf{r}$; $Exp := Exp + 1$; $done(d)$

p^2 $(c_q \Rightarrow 0 \leq \tau_r \leq \mathbf{r})$

Следует из того, что в значение τ_r или не изменяется, или становится равным $\mathbf{r}$

p^6 $(c_q \Rightarrow c_p \,\&\, \tau_s \geq \tau_r + \mu)$

Если значение τ_r не изменяется, то и другие значения не изменяются, а иначе следует из p^4 $(\forall(\ldots, \langle \ldots, \rho\rangle) \in M_p \cup M_q : 0 < \rho \leq \mu)$ и p^5 $(\forall(\mathbf{data}, \langle b, i, d, \rho\rangle) \in M_q : c_p \,\&\, \tau_s \geq \rho + \mu + \mathbf{r})$

Основной инвариант (доказательство)

Отправка подтверждения ($\mathbf{S}_q$)

Предусловие: c_q

1. $send(\mathbf{ack}, \langle Exp, \mu \rangle)$

p^1: $c_p \Rightarrow \tau_s \leq \mathbf{s}$

p^2: $c_q \Rightarrow 0 \leq \tau_r \leq \mathbf{r}$

p^3: $\forall i \in \mathbb{N}_0 : \vec{\tau}_t[i] \leq \mathbf{t}$

p^5: $\forall (\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : c_p \,\&\, \tau_s \geq \rho + \mu + \mathbf{r}$

p^6: $c_q \Rightarrow c_p \,\&\, \tau_s \geq \tau_r + \mu$

p^8: $\forall (\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : d = in_p[N + i] \,\&\, i < High$

p^9: $\neg c_p \Rightarrow High = 0$

Следует из того, что используемые значения не изменяются

Основной инвариант (доказательство)

Отправка подтверждения ($\mathbf{S}_q$)

Предусловие: c_q

1. $send(\textbf{ack}, \langle Exp, \mu \rangle)$

p^4 $(\forall(\ldots, \langle \ldots, \rho \rangle) \in M_p \cup M_q : 0 < \rho \leq \mu)$

Следует из того, что время жизни отправляемого пакета равно μ, а остальных — не изменяется

p^7 $(\forall(\textbf{ack}, \langle i, \rho \rangle) \in M_p : c_p \,\&\, \tau_s > \rho)$

Так как c_q содержится в предусловии и не изменяется, то после выполнения верно c_q

По p^6 $(c_q \Rightarrow c_p \,\&\, \tau_s \geq \tau_r + \mu)$, после выполнения также верно c_p и $\tau_s \geq \tau_r + \mu$

По p^2 $(c_q \Rightarrow 0 \leq \tau_r \leq \mathbf{r})$, верно $\tau_r > 0$

По p^4, верно $\rho \leq \mu$

Следовательно, $\tau_s \geq \tau_r + \mu > \mu \geq \rho$

Основной инвариант (доказательство)

Потеря сообщения (Loss)

Предусловие: $m \in M_x \,\&\, x \in \{p, q\}$

1. $M_x := M_x - \{m\}$;

p^1: $c_p \Rightarrow \tau_s \le \mathbf{s}$

p^2: $c_q \Rightarrow 0 \le \tau_r \le \mathbf{r}$

p^3: $\forall i \in \mathbb{N}_0 : \vec{\tau}_t[i] \le \mathbf{t}$

p^6: $c_q \Rightarrow c_p \,\&\, \tau_s \ge \tau_r + \mu$

p^9: $\neg c_p \Rightarrow High = 0$

Следует из того, что используемые значения не изменяются

p^4: $\forall(\ldots, \langle \ldots, \rho \rangle) \in M_p \cup M_q : 0 < \rho \le \mu$

p^5: $\forall(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : c_p \,\&\, \tau_s \ge \rho + \mu + \mathbf{r}$

p^7: $\forall(\mathbf{ack}, \langle i, \rho \rangle) \in M_p : c_p \,\&\, \tau_s > \rho$

p^8: $\forall(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : d = in_p[N + i] \,\&\, i < High$

Следует из того, что мультимножества под кванторами не увеличиваются и остальные значения не изменяются

Основной инвариант (доказательство)

Дублирование сообщения (Dup)

Предусловие: $m \in M_x \mathbin{\&} x \in \{p, q\}$

1. $M_x := M_x + \{m\};$

p^1: $c_p \Rightarrow \tau_s \leq \mathbf{s}$

p^2: $c_q \Rightarrow 0 \leq \tau_r \leq \mathbf{r}$

p^3: $\forall i \in \mathbb{N}_0 : \vec{\tau}_t[i] \leq \mathbf{t}$

p^6: $c_q \Rightarrow c_p \mathbin{\&} \tau_s \geq \tau_r + \mu$

p^9: $\neg c_p \Rightarrow High = 0$

Следует из того, что используемые значения не изменяются

p^4: $\forall(\ldots, \langle \ldots, \rho \rangle) \in M_p \cup M_q : 0 < \rho \leq \mu$

p^5: $\forall(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : c_p \mathbin{\&} \tau_s \geq \rho + \mu + \mathbf{r}$

p^7: $\forall(\mathbf{ack}, \langle i, \rho \rangle) \in M_p : c_p \mathbin{\&} \tau_s > \rho$

p^8: $\forall(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : d = in_p[N + i] \mathbin{\&} i < High$

Следует из того, что множества элементов под кванторами (без учёта кратности), как и другие значения, не изменяются

Основной инвариант (доказательство)

Течение времени (Time)

1. Выбрать произвольное значение $\Delta \in \mathbb{R}$, $\Delta > 0$
2. Для каждого $i \in \mathbb{N}_0$: $\vec{\tau}_t[i] := \vec{\tau}_t[i] - \Delta$;
3. $\tau_s := \tau_s - \Delta$; $\tau_r := \tau_r - \Delta$;
4. Если $\tau_r \leq 0$: завершить соединение в q: $c_q := \mathbb{f}$;
5. Для каждого пакета $m = (\ldots, \langle \ldots, \rho \rangle) \in M_x$, $x \in \{p, q\}$:
   5.1 $\rho := \rho - \Delta$; если $\rho \leq 0$: $M_x := M_x - \{m\}$;

p^8: $\forall(\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : d = in_p[N + i] \,\&\, i < High$

p^9: $\neg c_p \Rightarrow High = 0$

Следует из того, что в этих условиях таймеры не используются (используемые значения не изменяются)

p^1: $c_p \Rightarrow \tau_s \leq \mathbf{s}$

p^2: $c_q \Rightarrow 0 \leq \tau_r \leq \mathbf{r}$

p^3: $\forall i \in \mathbb{N}_0 : \vec{\tau}_t[i] \leq \mathbf{t}$

Следует из того, что значения τ_s, τ_r и $\vec{\tau}_t$ не могут увеличиться, и присваивания $c_q := \mathbb{f}$;, если после уменьшения стало верно $\tau_r \leq 0$

Основной инвариант (доказательство)

Течение времени (Time)

1. Выбрать произвольное значение $\Delta \in \mathbb{R}$, $\Delta > 0$
2. Для каждого $i \in \mathbb{N}_0$: $\vec{\tau}_t[i] := \vec{\tau}_t[i] - \Delta$;
3. $\tau_s := \tau_s - \Delta$; $\tau_r := \tau_r - \Delta$;
4. Если $\tau_r \leq 0$: завершить соединение в q: $c_q := \mathbb{f}$;
5. Для каждого пакета $m = (\ldots, \langle \ldots, \rho \rangle) \in M_x$, $x \in \{p, q\}$:
   5.1 $\rho := \rho - \Delta$; если $\rho \leq 0$: $M_x := M_x - \{m\}$;

p^4 $(\forall (\ldots, \langle \ldots, \rho \rangle) \in M_p \cup M_q : 0 < \rho \leq \mu)$

Следует из того, что значение ρ не может увеличиться, и если становится верным $\rho \leq 0$, то пакет удаляется

p^5: $\forall (\mathbf{data}, \langle b, i, d, \rho \rangle) \in M_q : c_p \,\&\, \tau_s \geq \rho + \mu + \mathbf{r}$

p^6: $c_q \Rightarrow c_p \,\&\, \tau_s \geq \tau_r + \mu$

p^7: $\forall (\mathbf{ack}, \langle i, \rho \rangle) \in M_p : c_p \,\&\, \tau_s > \rho$

Следует из того, что значения τ_s, ρ и τ_r уменьшаются на одну и ту же константу ▼

Отсутствие потерь

Добавим в конфигурацию для каждого блока данных ($in_p[i]$) отметку о том, был ли этот блок вручен потребителю: $delivered(i)$

Пусть $Ok(i)$ — множество всех конфигураций, таких что $lost[i] = \mathbb{t} \vee delivered(i)$

Теорема. Следующее утверждение $Q_{\Delta t}$ является инвариантом протокола с таймерами: $Q_{\Delta t} = P_{\Delta t} \,\&\, p^{10} \,\&\, p^{11} \,\&\, p^{12} \,\&\, p^{13} \,\&\, p^{14} \,\&\, p^{15}$**, где**

p^{10}: $\neg c_p \Rightarrow \forall i \in \mathbb{N}_0, i < N : Ok(i)$

p^{11}: $c_p \Rightarrow \forall i \in \mathbb{N}_0, i < N + Low : Ok(i)$

p^{12}: $\forall(\mathbf{data}, \langle \mathbb{t}, \ell, d, \rho \rangle) \in M_q : \forall i \in \mathbb{N}_0, i < N + \ell : Ok(i)$

p^{13}: $c_q \Rightarrow \forall i \in \mathbb{N}_0, i < N + Exp : Ok(i)$

p^{14}: $\forall(\mathbf{ack}, \langle \ell, \rho \rangle) \in M_p : \forall i \in \mathbb{N}_0, i < N + \ell : Ok(i)$

p^{15}: $\forall(i_1, i_2) \in \mathbb{N}_0^2, i_1 \le i_2 < N + High : \vec{\tau}_t[i_1] \le \vec{\tau}_t[i_2]$

Доказательство. Это **задача 1**

Отсутствие потерь

К сожалению, без дополнительных допущений невозможно доказать свойство отсутствия потерь: протокол им не обладает

Пометка блока как потерянного ($\mathbf{L}_p$)

Предусловие: $c_p \,\&\, \vec{\tau}_t[N + Low] \leq -(\mathbf{r} + 2\mu)$

1. $lost[N + Low] := \mathbb{t}$;
2. $Low := Low + 1$;

В действии пометки блока как потерянного говорится, что отправитель может пометить так блок, если соединение установлено и прошло достаточно много времени с поступления этого блока

Но у отправителя нет обязанности помечать так блок

Добавим допущение **L**, обязывающее отправителя выполнить действие $\mathbf{L}_p$ в разумный срок, если соединение не завершится до выполнения $\mathbf{L}_p$ — например, для определённости, для какого-либо значения не позднее значения $-(\mathbf{r} + 2\mu + \lambda)$ таймера $\vec{\tau}_t[N + Low]$ для некоторого наперёд заданного λ

Отсутствие потерь

Теорема (об отсутствии потерь). **В допущении L для каждого поступившего блока данных $in_p[\ell]$ рано или поздно становится верным хотя бы одно из двух: он вручается потребителю, или спустя не более чем $\mathbf{t} + 2\mu + \mathbf{r} + \lambda$ единиц времени после поступления отмечается как вероятно потерянный**

Доказательство.

Предположим от противного, что некоторый блок $in_p[\ell]$ поступает отправителю, но никогда не вручается потребителю и не отмечается отправителем как вероятно потерянный ($\neg Ok(\ell)$)

Отсутствие потерь

Доказательство.

Случай 1: спустя не более чем $\mathbf{t} + 2\mu + \mathbf{r} + \lambda$ единиц времени после поступления блока $in_p[\ell]$ выполняется $\mathbf{C}_p$ и соединение завершается

Перед этим выполнением $\mathbf{C}_p$ верно $N + High > \ell$, так как

- при поступлении $in_p[\ell]$ выполняется присваивание, делающее это неравенство справедливым, после чего
- по устройству присваиваний протокола выражение $N + High$ не может уменьшаться

После выполнения $\mathbf{C}_p$ становится верным $N > \ell$ и $\neg c_p$

Следовательно, по p^{10} $(\neg c_p \Rightarrow \forall i \in \mathbb{N}_0, i < N : Ok(i))$, верно $Ok(\ell)$ (*противоречие*)

Отсутствие потерь

Доказательство.

Случай 2 (иначе): действие $\mathbf{C}_p$ ни разу не выполняется спустя $\mathbf{t} + 2\mu + \mathbf{r} + \lambda$ единиц времени после поступления $in_p[\ell]$

Подслучай 2.а: в этот момент верно $N + Low \leq \ell$

По p^{15} $(\forall (i_1, i_2) \in \mathbb{N}_0^2, i_1 \leq i_2 < N + High : \vec{\tau}_t[i_1] \leq \vec{\tau}_t[i_2])$, для всех j от $N + Low$ до ℓ верно $\vec{\tau}_t[j] \leq -\mathbf{r} - 2\mu - \lambda$

Тогда, по допущению $\mathbf{L}$, для всех указанных j должно выполниться действие $\mathbf{L}_p$

После этого станет верным $\ell < N + Low$

Подслучай 2.б: в этот момент верно $\ell < N + Low$

По p^{11} $(c_p \Rightarrow \forall i \in \mathbb{N}_0, i < N + Low : Ok(i))$ получаем $Ok(\ell)$ (*противоречие*) ▼

Соблюдение порядка

Для второго требования достаточно показать, что каждый блок, врученный потребителю, имеет порядковый номер в массиве in_p, строго больший, чем у предыдущего врученного блока

Добавим в конфигурацию отметку pr — номер последнего врученного блока в массиве in_p

Для технического удобства будем полагать, что в начальной конфигурации $pr = -1$ и $\vec{\tau}_t[-1] = -\infty$

Теорема. Следующее утверждение $R_{\Delta t}$ является инвариантом протокола с таймером: $R_{\Delta t} = Q_{\Delta t} \,\&\, p^{16} \,\&\, p^{17} \,\&\, p^{18} \,\&\, p^{19}$, где

p^{16}: $\forall(\mathbf{data}, \langle b, i, d, \rho\rangle) \in M_q : \vec{\tau}_t[N+i] > \rho - \mu$

p^{17}: $c_q \Rightarrow \tau_r \geq \vec{\tau}_t[pr] + \mu$

p^{18}: $pr < N + High \,\&(\vec{\tau}_t[pr] > -\mu \Rightarrow c_q)$

p^{19}: $c_q \Rightarrow N + Exp = pr + 1$

Доказательство. Это **задача 2**

Соблюдение порядка

Лемма. В любой достижимой конфигурации верно:

$$(\mathbf{data}, \langle b, \ell, d, \rho\rangle) \in M_q \Rightarrow c_q \vee N + \ell > pr$$

Доказательство. Это **задача 3** (подсказка: p^4, p^{15}, p^{16}, p^{18})

Теорема (о сохранении порядка вручения). Блоки данных, вручаемые получателем потребителю, расположены в строго возрастающем порядке в in_p

Доказательство.

Пусть узел q, выполняя $\mathbf{R}_q$ получает пакет $(\mathbf{data}, \langle b, \ell, d, \rho\rangle)$ и вручает потребителю соответствующий блок d

Достаточно показать, что $N + \ell > pr$

Если перед выполнением $\mathbf{R}_q$ было верно $c_q = \mathbb{f}$, то по последней лемме веро $N + \ell > pr$

Иначе перед выполнением $\mathbf{R}_q$ было верно $c_q = \mathbb{t}$

По устройству $\mathbf{R}_q$, тогда $\ell = Exp$

Из p^{19} $(c_q \Rightarrow N + Exp = pr + 1)$ и последнего равенства следует $N + \ell = pr + 1 > pr$ ▼

Пара слов о свойствах протокола

Протокол, обладающий свойствами отсутствия потерь и сохранения порядка вручения, можно устроить так:

- Не отсылать поступившие блоки данных
  item Помечать все блоки как вероятно потерянные

В хорошем протоколе вероятно потерянными помечается как можно меньше блоков данных

Чтобы уменьшить число вероятно потерянных блоков, следует добавить дополнительные гарантии того, что слово будет пересылаться многократно длительное время с целью увеличить шансы успешной доставки с вручением

Но строгое обсуждение таких гарантий будет долгим и не очень полезным, поэтому остановимся на изложенном «ядре» протокола

Пара слов об инвариантах

Некоторые из утверждений, входящих в рассмотренные инварианты, имеют вид

$$\forall m \in M : P(m)$$

Можно легко убедиться, что истинность таких утверждений сохраняется при дублировании и потере пакетов в M

Аналогичные гарантии для утверждений других видов соблюдаются далеко не всегда

Ещё несколько задач

Задача 4. Опишите выполнение протокола с таймерами в допущении **L**, в котором блок данных помечается как вероятно потерянный, тогда как он был вручен потребителю

Задача 5. Опишите выполнение протокола с таймером, в ходе которого получатель устанавливает соединение после получения пакета данных с номером блока, большим ноля

Задача 6. Предположим, что в процедуре $\mathbf{E}_p$, помечающей блоки данных как вероятно потерянные, неравенство $\vec{\tau}_t[N + Low] < -(\mathbf{r} + 2\mu)$ в предусловии заменено на $\vec{\tau}_t[N + Low] < 0$. Будет ли так изменённый проткол удовлетворять свойствам отсутствия потерь и сохранения порядка вручения? Ответ аргументировать