Вариант 1

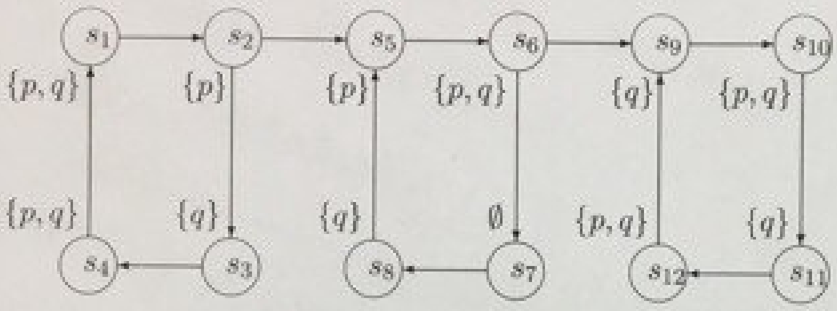
Задача 1. Докажите частичную корректность программы

if `x<y` **then** `x:=x+y; y:=x-y; x:=x-y` **fi**; **while** `x<y` **do** `x:=x+1` **od**

относительно предусловия **x+y=z** и постусловия **x+y=z**.

Задача 2. Запишите формулу PLTL, которая адекватно соответствует следующему утверждению: «Если событие A происходит бесконечно часто, то событие B не будет происходить, до тех пор пока событие A не случится три раза подряд».

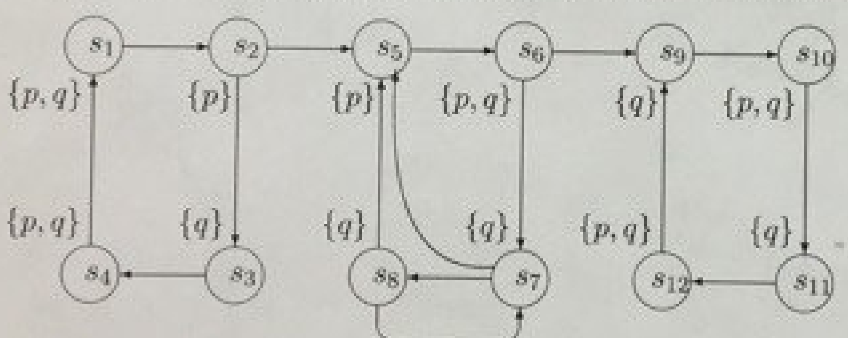
Задача 3. Определите, в каких состояниях модели M выполнима формула $(\mathbf{EG}\ p)\ \mathbf{EU}\ (\mathbf{AF}\ q)$



Задача 4. Упорядочив подходящим образом переменные, построить ROBDD наименьшего размера для булевой функции

$$f(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1 \oplus x_5) \wedge (x_4 \equiv x_6) \wedge (x_2 \equiv x_3)$$

Задача 5. Определите, какие пары состояний модели M являются бисимуляционно эквивалентными.



Задача 6. Какая формула называется слабейшим предусловием для программы π и постусловия ψ?

Задача 7. Какое свойство вычислений программы называется свойством живости? Приведите пример двух свойств вычислений программы, одно из которых является свойством живости, а другое — нет.

Задача 8. Что такое обобщенный автомат Бюхи и каково множество слов, которые распознаются обобщенным автоматом Бюхи?

Задача 9. Что называется конусом влияния заданного множества переменных C в заданной модели синхронной логической схемы? Каким образом конус влияния может быть использован для упрощения модели при ее верификации?

Задача 10. Как формулируется задача ограниченной верификации моделей программ (BMC, bounded model checking)? Какова известная Вам верхняя оценка сложности по времени решения задачи BMC глубины k для модели размера n и формулы размера m?

Шилевой В.Д. 621 | Вариант 1 |

1	2	3	4	5	6	7	8	9	10
3	3+	3	3	2	2	2	1	2	2

ОТЛ

N3 $E(\underbrace{\underbrace{(EGp)}_{f_1}\ U\ \underbrace{(AFq)}_{f_2}}_{f_3})$

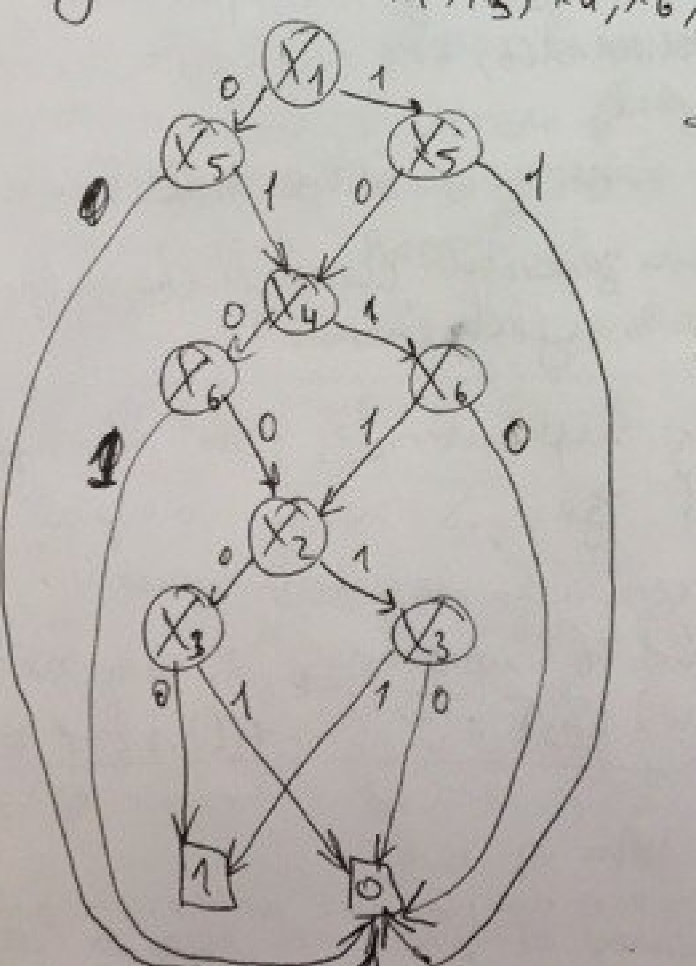
- f_1 выполнено в $\varnothing$, т.к. в M' (в которой удалены все вершины, где $\neg q$) нет компоненты сильной связности с p.
- f_2 выполнено везде, т.к. из любой вершины по любым путям можно достичь q: из $s_1 - s_8$ можно достичь q, добравшись до s_9. Из $s_9, s_{10}, s_{11}, s_{12}$ не нужно ничего достигать, т.к. там уже q.
- f_3: false U true в любой вершине => верно везде

E(true) – везде выполнима.

Ответ: все состояния.

N4 $f = (x_1 \oplus x_5) \wedge (x_4 \equiv x_6) \wedge (x_2 \equiv x_3)$.

На лекциях по ROBDD и оптимальному упорядочению переменных упоминалось, что для компараторов оптимально упорядочить переменные по парам, в которых они сравниваются. Попробуем так: $x_1, x_5, x_4, x_6, x_2, x_3$



Этот ROBDD оптимальна, т.к. для данного порядка нельзя применить ни одно из 3-х правил упрощения.

Эта ROBDD наименьшая, т.к. для каждого из подвыражений можно построить ROBDD минимум из 3-х вершин (x_1 ...), не считая 0 и 1. Здесь три таких выражения и 9 вершин (кроме 0 и 1) => этот порядок оптимален.

№5 Построим мн-во $\pi_1 = \{ (1,4,6,12,10), (2,5), (3,8,7,9,11) \}$.
Каждый член π — это такие s, что $\forall i, j \in$ одному из мн-в π, то
$L(s_i) = L(s_j)$.

Теперь будем строить разбиения: $\pi | D_1$, $\pi | D_2$ ..., пока не перестанет разбиваться.

$\pi_2 = \pi_1 | (2,5) = \{ (1), (4,6,12,10), (2,5), (8), (3,7,9,11) \}$

$\pi_3 = \pi_2 | (1) = \{ (1), (4), (6,12,10), (2,5), (8), (3,7,9,11) \}$

$\pi_4 = \pi_3 | (2,5) = \{ (1), (3), (4), (8), (6,12,10), (2,5), (7,9,11) \}$

$\pi_5 = \pi_4 | (3) = \{ (1), (2), (3), (4), (5), (8), (6,12,10), (7,9,11) \}$

$\pi_6 = \pi_5 | (5) = \{ (1), (2), (3), (4), (5), (7), (8), (6,12,10), (9,11) \}$

$\pi_7 = \pi_6 | (7) = \{ (1), (2), (3), (4), (5), (6), (7), (8), (10,12), (9,11) \}$

~~π_8~~ $\pi_7 = \pi_7 | (1) = \pi_7 | (2) = \ldots = \pi_7 | (9,11)$ — дальше не разбивается.

Ответ: $10 \sim 12$, $9 \sim 11$.

№6 φ_0 — слабейшее предусловие π при постусловии ψ, если
$I \models \{\varphi_0\} \pi \{\psi\}$ и $\forall \varphi: I \models \{\varphi\} \pi \{\psi\} \Rightarrow I \models \varphi \to \varphi_0$

№7 „Что-то хорошее обязательно произойдет."

Формально: ~~...~~ $\forall$ конечной трассы β $\exists$ ее бесконечное продолжение π такое, что $\beta\pi$ удовлетворяет св-ву вычисления. То есть как бы трасса ни начиналась, она всегда еще может принадлежать св-ву вычисления.

Пример живости: „организм в конечном итоге ~~по~~ погибнет.";

Пример безопасности: „красный и зеленый сигналы светофора не могут гореть одновременно".

все как?

№8 Обобщенный автомат Бюхи над алфавитом Σ — это четверка:
$AB = \{ S, l_0, R, \mathcal{F} \}$, где S — мн-во состояний, l_0 — нач. сост. $\in S$,
R — отношение переходов $\subseteq S \times \Sigma \times S$, $\mathcal{F}$ — семейство множеств конечных состояний.
Он распознает бесконечные слова в алфавите Σ, в которых верно:
$\forall w \in L(AB): \forall t \in Tr(AB, w)$ ~~$\forall$~~ $\exists F \in \mathcal{F}: inf(t) \cap F \neq \varnothing$.

№9 Пусть $V = \{v_1, v_2, \ldots v_n\}$ — переменные схемы. C — конус влияния $\subseteq V$
~~...~~ если $v_i \in C$, то все переменные из $f_i \in C$
функции v_i
В конус влияния можно поместить те переменные, которые нас интересуют для проверки чего-то конкретного, где не нужны все переменные. Это уменьшает схему, а схема по конусу симулирует исходную модель.

№0] Для заданной длины пути k, модели M и формулы φ проверить выполнимость

$$M \models_k E\varphi.$$

Оценка: $_2O(k(n+m))$.

№2 ~~$GFa \to [G\neg b \vee (\neg b \wedge \neg(a \wedge Xa \wedge XXa) \, U (\neg b \wedge a \wedge Xa \wedge XXa$~~

$\underbrace{GFa}_{} \to [\underbrace{G\neg b}_{f_1}, \vee (\underbrace{\neg b \wedge X\neg b \wedge XX\neg b \wedge \neg(a \wedge Xa \wedge XXa)}_{f_2}, U \underbrace{(\neg b \wedge X\neg b \wedge XX\neg b \wedge a \wedge Xa \wedge XXa)}_{f_3})]$

если событие a происходит беск. часто, то...

$f_1 = G\neg b$ — событие **b** не происходит никогда — это нужно, чтобы убедиться, что **b** есть в (f_2 U f_3). Иначе Until может не сработать, т.к. если нет **b**, то и **aaa** не обязано быть.

$f_2 = \neg b \wedge X\neg b \wedge XX\neg b \wedge \neg(a \wedge Xa \wedge XXa)$

до f_3 нет ни **aaa**, ни хотя бы одного b. Условие на $Xb \wedge XXb$ нужно, т.к.

№2] $\underbrace{GFa}_{f_1} \to (\underbrace{[\neg b \wedge \neg(a \wedge Xa \wedge XXa)]}_{f_2} \, U \, \underbrace{[\neg b \wedge a \wedge Xa \wedge XXa \wedge X\neg b \wedge XX\neg b]}_{f_3})$

АХАХ

круто!

- f_1 — событие **a** происходит почти всегда.
- f_2 — пока не f_3, нет ни одного b и ни одной тройки aaa.
- f_3 — ~~b~~ f_2 не выполнено в некотором состоянии и достигнуто f_3. Значит либо встречено **b**, либо aaa, либо что, и другое. Но **b** не должно быть раньше трёх **a** ⇒ надо от этого дополнит. защититься, поставив $\neg b \wedge X\neg b \wedge XX\neg b$. Без $X\neg b \wedge XX\neg b$ ~~путь~~ $a \to ab \to ab$ тоже может подойти, хотя это неверно.

Note: я заменил A → a, B → b, т.к. иначе путаю A с квантором пути.

№1] Проведём док-во в два этапа:

покажем, что ~~⊢~~ {true} if x < y then x:=x+y; y:=x-y; x:=x-y; fi {x ≥ y}

$[\, x \le y \;||\; x \ge y \,] = [\,true\,]$.

if $(x \le y)$ then

$[\, x+y \le 2y \,] = [\, x \le y \,]$

$x := x+y$

$[\, x \ge 2x-2y \,] = [\, x \le 2y \,]$

$y := x-y$

$[\, x-y \ge y \,] = [\, x \ge 2y \,]$

$x := x-y$

$[\, x \ge y \,]$

fi

$[\, x \ge y \,]$

Теперь используем это в программе из задания:

доказано

	$\{[\, x+y = z \,]$ ч.т.д.
if $(x<y)$ then	$[\; x+y=z \,] = [\; x+y=z \,]$
$x := x+y$	$[\; \& \; x=z \,] = [\; x=z \,]$
$y := x-y$	$[\; x-y+y=z \,] = [\; y=z \,]$
$x := x-y$	
fi	
$[\, x \ge y \,]$	$[\; \& \; x+y=z \,]$
while $x<y$ do	
$x := x+1$	цикл никогда не выполняется, т.к. дано, что $x \ge y$ — его предусловие.
od	
$[\, x+y = z \,]$ — док-ть.	