Содержание

1 Билет 78 (Язык модальной логики)

Определение 1.1. *Введём две связки:* $\Box$ *— необходимость,* $\Diamond$ *— возможность.*

Определение 1.2. *Фиксируем счётное множество функциональных переменных* $Var = \{P_1, P_2, \ldots\}$. *Язык модальной логики высказываний (множество модальных пропозициональных формул) строится из пропозициональных переменных, связок* ($\neg$, $\vee$, $\wedge$, $\to$, $\Box$) *и скобок по рекурсии:*

1. *Если* $A = P_i$, *то* A *— модальная пропозициональная формула.*
2. *Если* $A = \neg B$, *где* B *— модальная пропозициональная формула, то* A *— модальная пропозиционая формула.*
3. *Если* $A = B \vee C$, *где* B *и* C *— модальные пропозициональные формулы, то* A *— модальная пропозиционая формула.*
4. *Если* $A = B \wedge C$, *где* B *и* C *— модальные пропозициональные формулы, то* A *— модальная пропозиционая формула.*
5. *Если* $A = B \to C$, *где* B *и* C *— модальные пропозициональные формулы, то* A *— модальная пропозиционая формула.*

6. *Если $A = \Box B$, где B — модальная пропозициональная формула, то A — модальная пропозиционая формула.*

Обозначение: Fm.

Определение 1.3. *Шкала Крипке — это пара (W, R), где $W \neq \varnothing$ (множество миров), $W \subseteq R \times R$ (отношение достижимости).*

Определение 1.4. *Модель Крипке на шкале (W, R) — тройка (W, R, θ), где $\theta : Var \to P(W)$ (оценка переменных).*

Определение 1.5. *Истинность формул в модели Крипке $M = (W, R, \theta)$ строится по рекурсии:*

1. $M, x \models P_i := x \in \theta(P_i)$.
2. $M, x \models (A \vee B) := M, x \models A$ *или* $M, x \models B$.
3. $M, x \models (A \wedge B) := M, x \models A$ *и* $M, x \models B$.
4. $M, x \models (A \to B) := M, x \not\models A$ *или* $M, x \models B$.
5. $M, x \models (\neg A) := M, x \not\models A$.
6. $M, x \models (\Box A) := \forall y((xRy) \to (M, y \models A))$.

Определение 1.6. *Формула A общезначима на шкале Крипке (W, R), если она истинна во всех мирах в любой модели Крипке (W, R). Обозначение: $(W, R) \models A$.*

2 Билет 79 (Общезначимость тавтологий)

Лемма 2.1. *Все тавтологии общезначимы на всех шкалах Крипке.*

Доказательство. Зададим классическую оценку f с условием $f(P_i) = 1 \Leftrightarrow M, x \models P_i$. По индукции по числу связок получаем, что $\overline{f}(A) = 1 \Leftrightarrow M, x \models A$. Поэтому, если A — тавтология, то тогда её значение всегда равно 1, а значит, $M, x \models A$, то есть A общезначима. ■

3 Билет 80 (Исчисления K и S5)

Определение 3.1. *Подстановочный пример формулы A получается заменой пропозициональных переменных на произвольные модальные формулы.*

Определение 3.2. *Модальное исчисление K в языке Fm задаётся следующим образом:*

1. *Аксиомы:*

   (a) *Все подстановочные примеры тавтологий.*

   (b) $\Box(A \to B) \to (\Box A \to \Box B)$

2. *Формулы вывода:*

   (a) $\frac{A \quad A \to B}{B}$

   (b) $\frac{A}{\Box A}$

Определение 3.3. *Модальное исчисление $S5$ в языке Fm задаётся из аксиом исчисления K добавлением следующих аксиом:*

1. $\Box A \to A$

2. $\Box A \to \Box\Box A$

3. $\Diamond\Box A \to A$

4 Билет 81 (Корректность исчисления K)

Теорема 4.1. *Если $\vdash_K A$, то A общезначима во всех шкалах.*

Доказательство. Проведём индукцию по длине вывода формулы A.

1. Пусть $A(P_1, \ldots, P_k)$ — формула. Заменим все P_i на B_i. Зададим классическую оценку f с условием $f(P_i) = 1 \Leftrightarrow M, x \models B_i$. Тогда по индукции для любой формулы A

$$\overline{f}(A) = 1 \Leftrightarrow M, x \models A(B_1, \ldots, B_k)$$

   Если A — тавтология, то $M, x \models A(B_1, \ldots, B_k)$.

2. Пусть xRy, тогда из $M, x \models \Box(A \to B)$ имеем $M, y \models (A \to B)$. Из $M, x \models \Box A$ имеем $M, y \models A$. Значит, $M, y \models B$, а значит, $M, x \models \Box B$. Таким образом, формула $\Box(A \to B) \to (\Box A \to \Box B)$ истинна.

3. $M, x \models A$ и $M, x \models (A \to B)$, тогда $M, x \models B$.

4. Пусть A общезначима во всех шкалах. Рассмотрим произвольную модель Крипке и мир x. Тогда $M, x \models \Box A$, так как $M, y \models A$ для любого y в силу общезначимости A.

∎

5 Билет 82 (Корректность исчисления S5)

Определение 5.1. *Универсальное отношение на* W *— это* $W \times W$.

Теорема 5.1. *Если* $\vdash_{S5} A$, *то* A *общезначима на всех шкалах Крипке с универсальным отношением достижимости.*

Доказательство.

1. Пусть $A(P_1, \ldots, P_k)$ — формула. Заменим все P_i на B_i. Зададим классическую оценку f с условием $f(P_i) = 1 \Leftrightarrow M, x \models B_i$. Тогда по индукции для любой формулы A

   $$\overline{f}(A) = 1 \Leftrightarrow M, x \models A(B_1, \ldots, B_k)$$

   Если A — тавтология, то $M, x \models A(B_1, \ldots, B_k)$.

2. Пусть xRy, тогда из $M, x \models \Box(A \to B)$ имеем $M, y \models (A \to B)$. Из $M, x \models \Box A$ имеем $M, y \models A$. Значит, $M, y \models B$, а значит, $M, x \models \Box B$. Таким образом, формула $\Box(A \to B) \to (\Box A \to \Box B)$ истинна.

3. $M, x \models A$ и $M, x \models (A \to B)$, тогда $M, x \models B$.

4. Пусть A общезначима во всех шкалах. Рассмотрим произвольную модель Крипке и мир x. Тогда $M, x \models \Box A$, так как $M, y \models A$ для любого y в силу общезначимости A.

5. Пусть $\Box A$ общезначима, тогда $\forall y(xRy \to (M, y \models A))$, значит, $M, x \models A$.

6. Пусть $\Box A$ общезначима, тогда $\forall y(xRy \to (M, y \models A))$.

7. Пусть $\Diamond\Box A$ общезначима, тогда $M, y \models \Box A$ для некоторого y. Тогда $M, x \models A$, так как x достижимо из y.

■

6 Билет 83 (Стандартный перевод модальных формул в формулы логики предикатов, связь модальной истинности и классической истинности)

Определение 6.1. *Перевод формулы модальной логики в формулу логики предикатов определяется по рекурсии:*

1. $P_i^*(a) = P_i^1(a)$.

2. $(A \circ B)^*(a) = (A^*(a) \circ B^*(a))$ *для* $\neg$, $\vee$, $\wedge$.

3. $(\neg A)^*(a) = (\neg(A^*))(a)$.

4. $(\Box A)^*(a) = \forall x(R(a,x) \to A^*(x))$.

Такой перевод называется стандартным переводом.

Определение 6.2. *По каждой модели крипке $M = (W, \underline{R}, \theta)$ построим модель M^* сигнаъуры Ω с носителем W:*

1. $M^* \models P_i^1(u) \Leftrightarrow M, u \models P_i$

2. $M^* \models R(u,v) \Leftrightarrow u\underline{R}v$

Утверждение 6.1. *Для любой модальной формулы A и мира u $M^* \models A^*(u) \Leftrightarrow M, u \models A$.*

Доказательство. Проведём индукцию по длине A.
База индукции: Следует из определения M^*.
Шаг индукции: Для случаев $1-4$ это очевидно из предположения индукции и определения стандартного перевода. Рассмотрим случай $A = \Box B$. $M^* \models A^*(u) \Leftrightarrow \forall x(R(u,x) \to B^*(x)) \Leftrightarrow \forall v(uRv \to M^* \models B^*(v))$. По предположению индукции и определению истинности в модели Крипке полученная формула равносильна $\forall v(uRv \to M, v \models B) \Leftrightarrow M, u \models A$. ■

Теорема 6.1. *Для любой модальной формулы $A \models \forall x A^*(x) \;\Leftrightarrow \models A$.*

Доказательство. $\Longleftarrow$ Пусть $\models A$, тогда для всех M и u имеем $M, u \models A$. По утверждению выше для любых M^* и u имеем $M^* \models A^*(u)$, а значит, $M^* \models \forall x A^*(x)$. Но всякая модель формулы в сигнатуре Ω имеет вид M^*. Из определения M^* легко видеть как строится M.
$\Longrightarrow$ Пусть $\models \forall x A^*(x)$, тогда для любой модели M имеем $M^* \models \forall x A^*(x)$ и проводим рассуждения выше, только в обратном порядке. ■

7 Билет 84 (Перевод Вайсберга, связь модальной истинности с универсальной достижимостью)

Определение 7.1. *Каждую модальную формулу A можно преобразовать в формулу логики предикатов $A^*(a)$ с одной свободной переменной a. Такой перевод называется переводом Вайсберга и определяется по рекурсии:*

1. $P_i^*(a) = P_i^1(a)$.

2. $(A \circ B)^*(a) = (A^*(a) \circ B^*(a))$ *для* $\neg$, $\vee$, $\wedge$.

3. $(\neg A)^*(a) = (\neg(A^*))(a)$.

4. $(\Box A)^*(a) = \forall x\ A^*(x)$.

Определение 7.2. *По каждой модели Крипке M можно построить модель M^* сигнатуры Ω с носителем W: $M^* \models P_i^*(u) \Leftrightarrow M, u \models P_i$.*

Лемма 7.1. *Для любой модальной формулы A и мира u $M^* \models A^*(u) \Leftrightarrow M, u \models A$.*

Доказательство. Проведём индукцию по длине формулы A.
База индукции: следует из определения M^*.
Шаг индукции: для $A = \Box B$: $M^* \models (\Box B)^*(u) \Leftrightarrow M^* \models \forall x B^*(x) \Leftrightarrow \forall u\ M^* \models B^*(u) \Leftrightarrow \forall u\ M, u \models B(u) \Leftrightarrow M, u \models A$. Первый переход по пореределению перевода, второй переход по определению истинности в классической логике, третий переход по предположению индукции. ■

Теорема 7.1. *Для любой модальной формулы A формула $\forall x A^*(x)$ общезначима $\Longleftrightarrow$ A общезначима на всех шкалах Крипке с универсальной достижимостью.*

Доказательство. $\Longleftarrow$ Пусть $\models M$, тогда для всех M и u имеем $M, u \models A$. По лемме выше для любых M^* и u имеем $M^* \models A^*(u)$, а значит, $M^* \models \forall x A^*(x)$. Но всякая модель формулы в сигнатуре Ω имеет вид M^*. Из определения M^* легко видеть как строится M

$\Longrightarrow$ Пусть $\models \forall x A^*(x)$, тогда для любой модели M имеем $M^* \models \forall x A^*(x)$ и проводим рассуждения выше, только в обратном порядке. ■

8 Билет 85 (Эквивалентность классической формулы с одноместными предикатами и дизъюнкции конъюнкций переводов модальных формул)

Теорема 8.1. *Всякая формула в сигнатуре с одноместными предикатными символами со свободными переменными $a_1, \ldots, a_n$ эквивалентна дизъюнкции формул вида $A_1^*(a_1) \wedge \ldots \wedge A_n^*(a_n)$.*

Доказательство. Рассуждаем по индукции.
База индукции: $A = P^1(a_i)$ очевидно.
Шаг индукции:

1. Если $A = B \vee C$, то из предположения индукции имеем утверждение теоремы.

2. Если $A = \neg B$, где $B \sim \bigvee\limits_j (\bigwedge\limits_i A_{ij}^*(a_i))$, то $A \sim \bigwedge\limits_j (\bigvee\limits_i \neg A_{ij}^*(a_i)) \sim \bigwedge\limits_j (\bigvee\limits_i (\neg A_{ij})^*(a_i)) \sim$

3. Пусть $A = \exists x[x/a_1]B$, где $B = \bigvee\limits_j(\bigwedge\limits_i A^*_{ij}(a_i))$. Тогда из основных равносильностей из билета 45 имеем $A \sim \bigvee\limits_j(\exists[x/a_1]\bigwedge\limits_i A^*_{ij}(a_i))$, $\exists x[x/a_1](\bigwedge\limits_i A^*_{ij}(a_i)) \sim \exists x A^*_{1j}(x) \wedge \bigwedge\limits_{i\neq 1} A^*_{ij}(a_i) \sim (\Diamond A_{1j})^*(a_1) \wedge \bigwedge\limits_{i\neq 1} A^*_{ij}(a_i)$

■

Следствие 8.1.1. *Всякая формула в сигнатуре с одноместными предикатными символами со свободной переменной a эквивалентна формуле вида $A^*(a)$.*

9 Билет 86 (Теорема полноты для K, модальные таблицы, противоречивые таблицы)

Теорема 9.1 (Теорема полноты для K)**.** *Для любой модальной формулы A следующия условия равносильны:*

1. $\vdash_K A$.
2. *A общезначима на всех шкалах Крипке.*
3. *A общезначима на всех конечных шкалах Крипке.*

Определение 9.1. *Таблица — пара конечных множеств модальных формул (Γ, Δ).*

Определение 9.2. *Таблица (Γ, Δ) противоречива, если $\vdash_K (\bigwedge \Gamma \to \bigvee \Delta)$.*

Определение 9.3. $(\Gamma, \Delta) \subseteq (\Gamma', \Delta')$, *если* $\Gamma \subseteq \Gamma'$ *и* $\Delta \subseteq \Delta'$.

Определение 9.4. *Формула A называется разобранной, если выполнено одно из условий:*

1. $\neg A \in \Gamma$ *разобрана, если* $A \in \Delta$.
2. $\neg A \in \Delta$ *разобрана, если* $A \in \Gamma$.
3. $(A \vee B) \in \Gamma$ *разобрана, если* $A \in \Gamma$ *или* $B \in \Gamma$.
4. $(A \vee B) \in \Delta$ *разобрана, если* $A \in \Delta$ *или* $B \in \Delta$.
5. *Все пропозициональные формулы и формулы вида $\Diamond A$ разобраны.*

Лемма 9.1. *d6Всякая непротиворечивая таблица расширяется до непротиворечивой таблицы, в которой все формулы разобраны.*

Доказательство. Для каждой таблицы рассмотрим два числа n_1 — максимальная длина неразобранных формул и n_2 — число неразобранных формул максимальной длины. Проведём индукцию по n_1, внутри которой проведём индукцию по n_2.
База индукции: если $n_1 = 0$, то доказывать нечего.
Шаг индукции: пусть дана некоторая таблица, в которой $n_1 = n_1^0$ и $n_2 = n_2^0$, и утверждение доказано для всех $n_1 < n_1^0$ и всех таблиц, где $n_1 = n_1^0$ и $n_2 < n_2^0$. Рассмотрим формулу X максимальной длины.

1. Пусть $X = \neg A \in \Gamma$. Предположим, что таблица противоречива. $\vdash_K (\bigwedge \Gamma \to \bigvee \Delta \vee A)$, тогда $\vdash_K ((\neg A \wedge \bigwedge \Gamma) \to \bigvee \Delta)$. Тогда $\vdash_K (\bigwedge \Gamma \to \bigvee \Delta)$, то есть таблица (Γ, Δ) противоречива — противоречие.
   Если $n_2^0 = 1$, то есть формула $\neg A$ не повторяется, то в новой таблице число $n_1 < n_1^0$. Если $n_2^0 > 1$, то в новой таблице $n_1 = n_1^0$ и $n_2 < n_2^0$, значит, по предположению внутренней индукции $(\Gamma, \Delta \cup \{A\})$ расширяется до непротиворечивой таблицы, в которой все формулы разобраны.

2. Пусть $X = \neg A \in \Delta$. Предположим, что таблица противоречива. $\vdash_K ((\bigwedge \Gamma \wedge A) \to \bigvee \Delta)$, тогда $\vdash_K (\wedge \bigwedge \Gamma \to \bigvee \Delta \vee \neg A)$. Тогда $\vdash_K (\bigwedge \Gamma \to \bigvee \Delta)$, то есть таблица (Γ, Δ) противоречива — противоречие.
   Если $n_2^0 = 1$, то есть формула $\neg A$ не повторяется, то в новой таблице число $n_1 < n_1^0$. Если $n_2^0 > 1$, то в новой таблице $n_1 = n_1^0$ и $n_2 < n_2^0$, значит, по предположению внутренней индукции $(\Gamma \cup \{A\}, \Delta)$ расширяется до непротиворечивой таблицы, в которой все формулы разобраны.

3. Пусть $X = (A \vee B) \in \Delta$. Предположим, что таблица противоречива. $\vdash_K (\bigwedge \Gamma \to (\bigvee \Delta \vee (A \vee B)))$, тогда это эквивалентно $\vdash_K (\bigwedge \Gamma \to \bigvee \Delta)$. Значит, таблица (Γ, Δ) противоречива — противоречие. Значит, построенная таблица не противоречива. Аналогично с предыдущими пунктами применяем предположение индукции.

4. Пусть $X = (A \vee B) \in \Gamma$. Предположим, что каждая из таблиц $(\Gamma \cup \{A\}, \Delta)$ и $(\Gamma \cup \{B\}, \Delta)$. Тогда $\vdash_K (\bigwedge \Gamma \wedge A \to \bigvee \Delta)$ и $\vdash_K (\bigwedge \Gamma \wedge B \to \bigvee \Delta)$, тогда, используя тавтологию $((p \wedge q) \to s) \to (((p \wedge r) \to s) \to ((p \wedge (q \vee r)) \to s))$, а применив первое правило вывода $(\frac{A \quad A \to B}{B})$, получим $\vdash_K (\bigwedge \Gamma \wedge (A \vee B) \to \bigvee \Delta)$. Тогда удалив повторы получаем $\vdash_K (\bigwedge \Gamma \to \bigvee \Delta)$ — противоречие. Значит, одна из таблиц непротиворечива. Значит, применив предположение индукции к непротиворечивой таблице, получим утверждение леммы.

■

10 Билет 87 (Конечные не транзитивные деревья, предшествование таблиц, дерево таблиц)

Определение 10.1. *Нетранзитивное дерево с корнем r — конечное множество X с отношением $<$ со следующими свойствами:*

1. *$r \in X$*
2. *Для каждого $x \in X$ существует единственный путь от r к x, то есть существует конечная последоательность $r = x_1, \ldots, x_n = x$, в которой $x_i < x_{i+1}$ для всех $i = \overline{1, n-1}$.*

Определение 10.2. *R нвзывается отношением предшествования для таблиц (Γ, Δ) (Γ', Δ'), если для любой формулы A $\Diamond A \in \Delta \Longrightarrow A \in \Delta'$.*

Определение 10.3. *Дерево таблиц — это отображение δ дерева с корнем r в множество непротиворечивых таблиц, при котором, если $x < y$, то $\delta(x) R\ \delta(y)$.*

Определение 10.4. *Дефект в таблице (Γ, Δ) — это формула $\Diamond A \in \Gamma$. Этот дефект устраняется в таблице (Γ', Δ'), если $A \in \Gamma'$ и $(\Gamma, \Delta) R\ (\Gamma', \Delta')$*

Определение 10.5. *Дефект в узле дерева таблиц — это дефект в таблице $\delta(x)$. Этот дефект устраняется в таблице $y > x$, если он устраняется в таблице $\delta(y)$.*

Свойства 1.

1. *Если $\vdash_K A \to B$, то $\vdash_K \Box A \to \Box B$*
2. *Если $\vdash_K A \to B$, то $\vdash_K \Diamond A \to \Diamond B$*
3. *$\vdash_K (\Box A \land \Box B) \to \Box(A \land B)$*
4. *$\vdash_K \Diamond(A \lor B) \to (\Diamond A \lor \Diamond B)$*

Доказательство.

1. Применим второе правило вывода $(\frac{A}{\Box A})$, а затем аксиому $\Box(A \to B) \to (\Box A \to \Box B)$.
2. Пусть $\vdash_K A \to B$, тогда применим тавтологию $(p \to q) \to (\neg q \to \neg p)$, значит, по первому правилу первода $(\frac{A\ \ A \to B}{B}) \vdash_K (\neg B \to \neg A)$. Применим пункт 1 и получим $\vdash_K (\Box \neg B \to \Box \neg A) \Longrightarrow \vdash_K (\Diamond A \to \Diamond B)$.
3. Рассмотрим тавтологию $A \to (B \to (A \land B))$, тогда по пункту 1 $\Box A \to \Box(B \to (A \land B))$. Применим аксиому $(\Box(A \to B) \to (\Box A \to \Box B))$, тогда $\Box(B \to (A \land B)) \to (\Box B \to \Box(A \land B))$. Применим тавтологию $(p \to q) \to ((p \to r) \to (q \to r))$ и получим $\vdash_K \Box A \to (\Box B \to \Box(A \land B))$. Применим тавтологию $(p \to (q \to r)) \leftrightarrow ((p \land q) \to r)$ и получим $\vdash_K (\Box A \land \Box B) \to \Box(A \land B)$.

4. Из пункта 3 имеем $\vdash_K (\Box\neg A \wedge \Box\neg B) \to \Box(\neg A \wedge \neg B)$, тогда по закону Де Мортана и пункту 1 имеем $\vdash_K \Box(\neg A \wedge \neg B) \to \Box\neg(A \vee B)$. Тогда по транзитивности $\vdash_K (\Box\neg A \wedge \Box\neg B) \to \Box\neg(A \vee B)$. Тогда по контрпозицию $((p \to q) \to (\neg q \to \neg p))$ имеем $\vdash_K \neg\Box\neg(A \vee B) \to \neg(\Box\neg A \wedge \Box\neg B)$. По законам Де Моргана и транзитивности: $\vdash_K \neg\Box\neg(A \vee B) \to (\neg\Box\neg A \vee \neg\Box\neg B)$, что равносильно утверждению пункта.

■

Лемма 10.1. *Пусть* (Γ, Δ) *— непротиворечивая таблица с дефектом* $\Diamond A$*, тогда существует непротиворечивая таблица, устраняющая данный дефект.*

Доказательство. Рассмотрим таблицу $(\Gamma', \Delta') = (\{A\}, \{B | \Diamond B \in \Delta)$. По определению эта таблица устраняет дефект. Предположим, что она противоречива, тогда $\vdash_K A \to \bigvee\{B | \Diamond B \in \Delta\}$. Применим свойства выше и получим $\vdash_K \Diamond A \to \bigvee\{\Diamond B | \Diamond B \in \Delta\}$. Так как $\Diamond A \in \Gamma$, то по тавтологии имеем $\vdash_K \bigwedge \Gamma \to \Diamond A$. По тавтологии $\vdash_K \bigwedge \Gamma \bigvee\{B | \Diamond B \in \Delta\} \to \bigvee \Delta$ имеем $\vdash_K \bigwedge \Gamma \to \bigvee \Delta$. ■

Теорема 10.1 (Теорема полноты для K)**.** *Для любой модальной формулы A следующия условия равносильны:*

1. $\vdash_K A$*.*
2. *A общезначима на всех шкалах Крипке.*
3. *A общезначима на всех конечных шкалах Крипке.*

Доказательство.

1. $1 \Longrightarrow 2$ По теоерме корректности из билета 81.
2. $2 \Longrightarrow 3$ Очевидно.
3. $3 \Longrightarrow 1$ для формулы $\neg A$. Предположим, что формула A непротиворечива и докажем выполнимость A в конечной модели Крипке.
   Пусть формула A_0 непротиворечива в K, тогда последовательно строим дерево таблиц, начиная с корня.
   (a) Пусть $(\{A_0\}, \varnothing)$ — исходная непротиворечивая таблица, тогда расширяем её до непротиворечивой таблицы (Γ_0, Δ_0), где все формулы разобраны (это можно сделать по лемме из билета 86). Эту таблицу помещаем в корень дерева.
   (b) Устраняем дефекты в таблице (Γ_0, Δ_0) (это можно сделать по лемме выше). Получим новые таблицы, в которых также разбираем все формулы (расширяем эти таблицы по лемме из билета 86). Добавляем в дерево узлы $x_i > r$ и помещаем в них построенные таблицы.

Докажем,что этот процесс закончится.

Определение 10.6. *Уровень таблицы — максимальная длина формулы в данной таблице.*

Заметим, что при разборе таблицы уровень не изменяется, так как во время разбора мы только меняем формулы на более короткие. Исходя из доказательства леммы, при устранении дефекта уровень таблицы уменьшается. Значит, на каждом шаге построения уровень таблицы уменьшается, значит, число преобразований конечно.
Таким образом, мы получили конечное дерево таблиц без дефектов, где все формулы разобраны.
Построим модель Крипке на этом дереве таблиц, положив $M, x \models P_i \Leftrightarrow P_i \in \Gamma$, если $\delta(x) = (\Gamma, \Delta)$.

Лемма 10.2. *Пусть $\delta(x) = (\Gamma, \Delta)$, тогда для всех формул A:*

(a) если $A \in \Gamma$, то $M, x \models A$

(b) если $A \in \Delta$, то $M, x \not\models A$

Доказательство. Проведём индукцию по длине формулы A сразу для всех x.
База индукции:

(a) Пусть $A = P_i \in \Gamma$, тогда по определению $M, x \models A$.

(b) Пусть $A = P_i \in \Delta$, тогда по определению $M, x \not\models A$, а в силу непротиворечивости $A \notin \Gamma$.

Шаг индукции:

(a) Пусть $A = \neg B \in \Gamma$, тогда в силу разобранности имеем $B \in \Delta$. Значит, по предположению индукции $M, x \not\models B$, значит, $M, x \models \neg B$, то есть $M, x \models A$.

(b) Для $A = \neg B \in \Delta$ аналогично.

(c) Пусть $A = B \vee C$, тогда в силу разобранности $B \in \Gamma$ или $A \in \Gamma$, значит, по предположению индукции $M, x \models A$ или $M, x \models B$, то есть $M, x \models (A \vee B)$.

(d) Пусть $A = \Diamond B \in \Gamma$. Так как дефектов нет, то найдётся $y > x$, где B окажется в таблице слева. По предположению индукции $M, y \models B$, значит, $M.x \models A$.

(e) Пусть $A = \Diamond B \in \Delta$, Если $x < y$, то $\delta(x) R \delta(y)$ по определению дерева таблиц. Пусть $\delta(y) = (\Gamma', \Delta')$, тогда по определению отношения R $B \in \Delta'$. Значит, по предположению индукции $M, y \not\models B$, тогда для всех $y > x$ $M, y \not\models B$. Значит, $M, x \not\models A$.

■

Из этой леммы получаем, что $M, r \models A_0$.

■

11 Билет 88 (Модальные формулы глубины 1, приведение их к нормальной форме, синтаксические свойства S5)

Определение 11.1. *Модальные формулы глубины 1 — это подстановочный пример классической формулы вида $A(P_1, \dots, P_n, \Diamond B_1, \dots, \Diamond B_n)$, где A, B_1, ..., B_n — классические формулы.*

Лемма 11.1. *В S5 формула глубины 1 эквивалентна дизъюнкции конъюнкций литералов и формул вида $\Diamond B$ $\neg\Diamond B$, где B — классическая формула.*

Доказательство. Так как любая пропозициональная формула имеет СДНФ (теорема из билета 36), то все P_i можно заменить на СДНФ этого P_i. Тогда полученная формула будет иметь нужный вид. ■

Свойства 2.

1. $\Diamond(A \vee B) \leftrightarrow (\Diamond A \vee \Diamond B)$
2. $\Diamond(A \wedge \Diamond B) \leftrightarrow (\Diamond A \wedge \Diamond B)$
3. $\Diamond(A \wedge \neg\Diamond B) \leftrightarrow (\Diamond A \wedge \neg\Diamond B)$

Доказательство.

1. По аналогичной лемме для K из билета 87.

2. $\Longrightarrow$ Из общезначимости и теоремы о полноте для K имеем $\vdash_{S5} (\Diamond(A \wedge C) \to (\Diamond A \wedge \Diamond C)) \Longrightarrow \vdash_{S5} (\Diamond(A \wedge \Diamond B) \to (\Diamond A \wedge \Diamond\Diamond B)$. $\vdash_{S5} \Diamond A \to \Diamond\Diamond A$, так как $\vdash_{S5} \neg\Box\neg\neg\Box\neg B \to \neg\Box\neg B$ (в силу свойств для K из билета 87, тавтологии $\vdash_{S5} \Box A \to \neg\neg\Box A$ и транзитивности). Тогда получим из транзитивности и $\vdash_{S5} \neg\Box\neg A \leftrightarrow \Diamond A$, что $\vdash_{S5} (\Diamond A \wedge \Diamond\Diamond B) \to (\Diamond A \to \Diamond B)$. Тогда по транзитивности получим $\Diamond(A \wedge \Diamond B) \to (\Diamond A \wedge \Diamond B)$.
$\Longleftarrow$ Из общезначимости и полноты K имеем $\vdash_K (\Diamond X \wedge \Box Y) \to \Diamond(X \wedge Y)$. Значит, $\vdash_{S5} (\Diamond A \wedge \Box\Diamond B) \to \Diamond(A \wedge \Diamond B)$. То есть остаётся показать, что $\vdash_{S5} (\Diamond A \wedge \Diamond B) \to (\Diamond A \wedge \Box\Diamond B)$. Из аксиом $S5$ имеем $\vdash_{S5} \Diamond\Box X \to \Diamond\Box\Box X$ и $\vdash_{S5} \Diamond\Box\Box X \to \Box X$, тогда по транзитивности $\vdash_{S5} \Diamond\Box X \to \Box X$. Так как $\vdash_{S5} \neg\Box\neg X \leftrightarrow \Diamond X$, то $\neg\Box\neg\Box X \to \Box X$.

По контрапозиции имеем $\vdash_{S5} \neg\Box X \to \neg\neg\Box\neg\Box X$, тогда, сняв двойное отрицание (по тавтологии), получим $\vdash_{S5} \neg\Box X \to \Box\neg\Box X$. Заменив $X = \neg B$, получим $\vdash_{S5} \Diamond B \to \Box\Diamond B$, а значит, по транзитивности $\vdash_{S5} (\Diamond A \wedge \Diamond B) \to (\Diamond A \wedge \Box\Diamond B)$.

3. $\Longrightarrow$ Из первой части доказательства пункта 2 имеем $\vdash_{S5} \Diamond(A\wedge\neg\Diamond B) \to (\Diamond A\wedge\Diamond\neg\Diamond B)$. $\vdash_{S5} (\Diamond\neg\Diamond X) \leftrightarrow (\Diamond\neg\neg\Box\neg X)$, $\vdash_{S5} (\Diamond\neg\neg\Box\neg X) \leftrightarrow (\Diamond\Box\neg X)$. А по доказанному в пункте 2 утверждению ($\vdash_{S5} \Diamond\Box X \to \Box X$), значит, $\vdash_{S5} (\Diamond\Box\neg X) \to (\Box\neg X)$. Значит, $(\vdash_{S5} \Diamond\Box\neg X) \to (\neg\Diamond X)$, что и требовалось.
   $\Longleftarrow$ Из второй части доказательства пункта 2 имеем $\vdash_K (\Diamond X \wedge \Box Y) \to \Diamond(X \wedge Y)$. Тогда, заменив, $Y = \neg\Diamond B$ получим $\vdash_{S5} (\Diamond X \wedge \Box\neg\Diamond B) \to \Diamond(X \wedge \neg\Diamond B)$. Остаётся показать, что $\vdash_{S5} (\Diamond A \wedge \neg\Diamond B) \to (\Diamond X \wedge \Box\neg\Diamond B)$. Из аксиом $S5$ имеем $\Box C \to \Box\Box C$ и $\vdash_{S5} \Box\Box C \to \Box\neg\neg\Box C$. Заменив $C = \neg B$, получим $\vdash_{S5} \Box\neg B \to \Box\neg\neg\Box\neg B$. Тогда, навесив двойное отрицание слева, получим $\vdash_{S5} \neg\neg\Box\neg B \to \Box\neg\neg\Box\neg B \Longrightarrow \vdash_{S5} \neg\Diamond B \to \Box\neg\Diamond B$, что и требовалось.

■

Теорема 11.1. *В $S5$ любая формула эквивалентна формуле глубины 1.*

Доказательство. Проведём идукцию по построению формулы.
База индукции $A = P_i$ очевидно.
Шаг индукции: случаи $\neg$ и $\vee$ очевидны из леммы. Рассморим $A = \Diamond B$, тогда по лемме можно рассмотреть соответствующую СДНФ, а по свойствам можем рассматривать только СДНФ такого вида $B = X \wedge \Diamond C_1 \wedge \ldots \wedge \Diamond C_m \wedge \neg\Diamond D_1 \wedge \ldots \wedge \neg\Diamond D_n$, где C_i и D_j — классические формулы. Тогда по свойствам формула $A = \Diamond B$ тоже формула глубины 1 (последовательно вносим $\Diamond$ в конъюнкции) ■

12 Билет 89 (Теорема полноты для $S5$)

Теорема 12.1 (Теорема полноты для S5)**.** *Для любой модальной формулы A следующия условия равносильны:*

1. $\vdash_{S5} A$.
2. *A общезначима на всех шкалах Крипке.*
3. *A общезначима на всех конечных шкалах Крипке.*

Доказательство.

1. 1 $\Longrightarrow$ 2 По теоерме корректности из билета 82.
2. 2 $\Longrightarrow$ 3 Очевидно.

3. $3 \implies 1$ для формулы $\neg A$. Предположим, что формула A непротиворечива и докажем выполнимость A в конечной модели Крипке.
   Пусть формула A_0 непротиворечива в $S5$, тогда последовательно строим дерево таблиц, начиная с корня. По теореме из билета 88 A_0 — формула глубины 1.

   (a) Пусть $(\{A_0\}, \varnothing)$ — исходная непротиворечивая таблица, тогда расширяем её до непротиворечивой таблицы (Γ_0, Δ_0), где все формулы разобраны (это можно сделать по лемме из билета 86).

   (b) Множество Δ_0 может содержать формулы вида $\Diamond B$. Все B такого вида будем добавлять к Δ_0, то есть рассмотрим таблицу $(\Gamma_0, \Delta_0') = (\Gamma_0, \Delta_0 \cup \{B | \Diamond B \in \Delta_0\})$.

      Утверждение 12.1. *Таблица* (Γ_0, Δ_0') *непротиворечива.*

      Доказательство. Предположим, что она противоречива, тогда по определению $\vdash_{S5} \bigwedge \Gamma_0 \to (\bigvee \Delta_0 \vee \bigvee \{B | \Diamond B \in \Delta_0\})$. Заметим, что из аксиомы $\vdash_{S5} A \to \Box A$ следует $\vdash_{S5} \neg A \to \Diamond \neg A$, то есть $\vdash_{S5} B \to \Diamond B$. Тогда по монотонности дизъюнкции имеем $\vdash_{S5} (\bigvee \Delta_0 \vee \bigvee \{B | \Diamond B \in \Delta_0\}) \to (\bigvee \Delta_0 \vee \bigvee \{\Diamond B | \Diamond B \in \Delta_0\})$. Сокращаем повторы в последней дизъюнкции $\vdash_{S5} (\bigvee \Delta_0 \vee \bigvee \{\Diamond B | \Diamond B \in \Delta_0\}) \to \bigvee \Delta_0$. Тогда по транзитивности $\vdash_{S5} \bigwedge \Gamma_0 \to \bigvee \Delta_0$ — противоречие. ■

      Разбираем все формулы B в таблице (Γ_0, Δ_0'), тогда получим новую таблицу (Γ_1, Δ_1), в которой все формулы разобраны и новых $\Diamond$ не появится, так как A_0 — формула глубины 1, а значит, все новые формулы B классические. Эту таблицу помещаем в корень дерева r.

   (c) Устраняем дефекты в таблице (Γ_1, Δ_1). Получаем новые непротиворечивые таблицы, в которых также разбираем все формулы. Добавив новые точки x_i, помещаем в них построенные таблицы. В этих таблицах дефектов нет, так как они состоят из классических формул.

   Докажем,что этот процесс закончится.

Определение 12.1. *Уровень таблицы — максимальная длина формулы в данной таблице.*

Заметим, что при разборе таблицы уровень не изменяется, так как во время разбора мы только меняем формулы на более короткие. Исходя из процесса устранения дефекта, при устранении дефекта уровень таблицы уменьшается. Значит, на каждом шаге построения уровень таблицы уменьшается, значит, число преобразований конечно.

Таким образом, мы получили конечное дерево таблиц без дефектов, где все формулы разобраны.
Построим модель Крипке на этом дереве таблиц, положив $M, x \models P_i \Leftrightarrow P_i \in \Gamma$, если $\delta(x) = (\Gamma, \Delta)$.

Лемма 12.1. *Пусть $\delta(x) = (\Gamma, \Delta)$, тогда для всех формул A:*

(a) если $A \in \Gamma$, то $M, x \models A$

(b) если $A \in \Delta$, то $M, x \not\models A$

Доказательство. Проведём индукцию по длине формулы A сразу для всех x.
База индукции:

(a) Пусть $A = P_i \in \Gamma$, тогда по определению $M, x \models A$.

(b) Пусть $A = P_i \in \Delta$, тогда по определению $M, x \not\models A$, а в силу непротиворечивости $A \notin \Gamma$.

Шаг индукции:

(a) Пусть $A = \neg B \in \Gamma$, тогда в силу разобранности имеем $B \in \Delta$. Значит, по предположению индукции $M, x \not\models B$, значит, $M, x \models \neg B$, то есть $M, x \models A$.

(b) Для $A = \neg B \in \Delta$ аналогично.

(c) Пусть $A = B \vee C$, тогда в силу разобранности $B \in \Gamma$ или $A \in \Gamma$, значит, по предположению индукции $M, x \models A$ или $M, x \models B$, то есть $M, x \models (A \vee B)$.

(d) Пусть $A = \Diamond B \in \Gamma$, тогда $x = r$ и по построению найдётся x_i, где B окажется в таблице слева. По предположению индукции $M, x_i \models B$, а значит, $M, x \models A$.

(e) Пусть $A = \Diamond B \in \Delta$, тогда $x = r$ и по построению $B \in \Delta$. B находится справа во всех таблицах всех точек x_i (из-за процесса устранения дефекта). По предположению индукции $M, y \not\models B$ для всех y, тогда $M, x \not\models A$.

■

Из этой леммы следует, что $M, r \models A_0$.

■

13 Билет 90 (Понятие алгоритма, тезис Чёрча—Тьюринга)

Определение 13.1. *Определим алгоритм следующими свойствами:*

1. *Алгоритм работает со словами.*

2. *Алгоритм основан на программе, где программа — конечный набор команд, записываемых словами.*

3. *Алгоритм содержит процессор, который обращается к программе и изменяет текущее состояние (слово).*

4. *Имеется начальное слово (вход) и конечное слово (выход). Если конечное слово не появляется, то алгоритм работает бесконечно долго (зацикливается).*

5. *Вычисление разбивается на дискретные шаги.*

6. *Вычисление детерменированно, то есть каждый следующий шаг определён однозначно, и не обращается к случайным числам.*

Определение 13.2. *Тезис Чёрча—Тьюринга утверждает все определения алгоритмов (рекурсивные функции, машины Тьюринга и т.д.) эквивалентны интуитивному пониманию вычислимости.*

14 Билет 91 (Машины Тьюринга)

Определение 14.1. *Машина Тьюринга задаётся двумя алфавитами (рабочим алфавитом и алфавитом состояний). Имеются особые состояния q_0 (начальное) и q_1 (заключительное) и особый символ $\sim$ (пробел). Имеется программа, состоящая из команд вида $qa \to q'a'X$, где q и q' — состояния, a, a' — рабочие символы, X — индекатор сдвига.*

Правила работы машины Тьюринга:

1. Машина работает с конечной лентой, на которой написаны рабочие числа и по которой движется каретка. Каретка видит ровно 1 символ.

2. В начале каретка находится в состоянии q_1, а в конце q_0.

3. Если каретка видит символ a в состоянии q и программа содержит команду $qa \to q'a'X$, то она заменяет a на a', сдвигается на 1 ячейку влево, вправо или остаётся на месте в зависимости от X и переходит в состояние q'.

4. Если лента закончилась и сдвиг невозможен, то наращивается дополнительная ячейка с символом пробела на ней.

15 Билет 92 (Вычислимые функции)

Определение 15.1. *Рассмотрим функции f из $\mathbb{N}^k$ в $\mathbb{N} = \omega$. Обозначение: $f : \mathbb{N}^k \to ?\mathbb{N}$. Если функция f всюду определена, то обозначим $f : \mathbb{N}^k \to \mathbb{N}$. Область функции обозначается $domf$, область значений — imf.*

Определение 15.2. *Функция $f : \mathbb{N}^k \to ?\mathbb{N}$ называется вычислимой, если существует алгоритм M со следующими свойствами:*

1. *Если $x \in domf$, то M заканчивает работу и выдаёт $f(x)$.*

2. *Если $x \notin domf$, то M на входе x зацикливается.*

Определение 15.3. *Рассмотрим функцию f на словах. Если Δ — конечный алфавит, то Δ^∞ — множество слов. Тогда рассматриваем функции из Δ^∞ в Δ^∞. Все обозначения аналогичны.*

Определение 15.4. *Функция $f : \Delta^\infty \to ?\Delta^\infty$ называется вычислимой, если существует алгоритм M со следующими свойствами:*

1. *Если $x \in domf$, то M заканчивает работу и выдаёт $f(x)$.*

2. *Если $x \notin domf$, то M на входе x зацикливается.*

16 Билет 93 (Разрешимые множества, разрешимость конечных множеств)

Определение 16.1. *Множество $A \subseteq \Delta^\infty$ называется разрешимым, если его характеристическая функция вычислима. Характеристической функцией называется функция $\chi : \Delta^\infty \to \{0, 1\}$, принимающая 1 на A и 0 на $\Delta^\infty \setminus A$.*

Определение 16.2. *Множество $A \subseteq \mathbb{N}^k$ называется разрешимым, если его характеристическая функция вычислима. Характеристической функцией называется функция $\chi : \mathbb{N}^k \to \{0, 1\}$, принимающая 1 на A и 0 на $\mathbb{N}^k \setminus A$.*

Утверждение 16.1.

1. *Если A разрешимо, то его дополнение разрешимо.*

2. *Если A и B разрешимы, то $A \cup B$ и $A \cap B$ разрешимы.*

Доказательство.

1. $\chi_{-A}(x)$ получается из $\chi_A(x)$ заменой 1 на 0 и на оборот.

2. Вычисляем $\chi_A(x)$ и $\chi_B(x)$ и выбираем наибольшее или наименьшее соответственно.

■

Следствие 16.0.1. *Конечные множества разрешимы.*

Доказательство. $A = \varnothing$, тогда $\chi_\varnothing = 0$, то есть вычислима.
Если $\alpha \in \Delta^\infty$, то $\{a\}$ разрешимо, так как любое слово можно сравнить с α побуквенно. Конечное множество — объединение одноэлементных, тогда по утверждению оно будет разрешимо. ■

17 Билет 94 (Полуразрешимые множества, их объединение и пересечение)

Определение 17.1. *Множество слов $A \subseteq \Delta^\infty$ ($A \subseteq \mathbb{N}^k$) называется полуразрешимо, если его полухарактеристическая функция вычислима. Полухарактеристической функцией называется частичная функция $\chi_A^- \Delta^\infty \to \{1\}$, то есть принимает значение 1 на A и неопределена на дополнении.*

Утверждение 17.1. *Если A и B полуразрешимы, то $A \cup B$ и $A \cap B$ полуразрешимы.*

Доказательство.

1. Параллельно вычисляем $\chi_A^-(x)$ и $\chi_B^-(x)$. Если одно из них закончится, то $\chi_{A\cup B}^-(x) = \{1\}$, иначе неопределена.

2. Параллельно вычисляем $\chi_A^-(x)$ и $\chi_B^-(x)$. Если оба закончатся, то $\chi_{A\cap B}^-(x) = \{1\}$, иначе неопределена.

■

18 Билет 95 (Теорема Поста)

Теорема 18.1. *Множество слов $A \subseteq \Delta^\infty$ разрешимо $\Longleftrightarrow$ A и $-A$ полуразрешимы.*

$\underline{\Longrightarrow}$ Разрешимое множество полуразрешимо, так как из $\chi_A(x)$ можно получить $\chi_A^-(x)$, просто сказав, что программа зацикливается при $\chi_A(x) = 0$. Значит, A полуразрешимо. По утверждению из билета 93 дополнение разрешимо, а значит, и полу разрешимо.
$\underline{\Longleftarrow}$ Вычисляем параллельно $\chi_A^-(x)$ и $\chi_{-A}^-(x)$, тогда одно из этих вычислений даёт 1. Таким образом находим $\chi_A(x)$.

19 Билет 96 (Композиция вычислимых функций, перечислимые множества)

Теорема 19.1. *Существуют вычислимые биекции* $\mathbb{N} \to \Delta^{\infty}$ *и* $\mathbb{N} \to \mathbb{N}^k$. *Обратные к ним функции также вычислимы.*

Утверждение 19.1. *Композиция вычислимых функций вычислима.*

Определение 19.1. *Последовательность — всюду определённая функция на* $\mathbb{N}$.

Определение 19.2. *Множество слов* $A \subseteq \Delta^{\infty}$ *перечислимо, если оно либо пусто, либо является множеством значений вычислимой последовательности* $f : \mathbb{N} \to \Delta^{\infty}$.

Теорема 19.2. *Множество слов* $A \subseteq \Delta^{\infty}$ *перечислимо* $\iff$ *оно полуразрешимо.*

Доказательство. По предыдущей теореме достаточно рассмотреть случай $A \subseteq \mathbb{N}$.
$\underline{\Longrightarrow}$ $\varnothing$ разрешимо.
$A = imf$ для вычислимой $f : \mathbb{N} \to \mathbb{N}$, тогда функция χ_A^- вычислима следующим алгоритмом:

Алгоритм 19.1.

1. *Пусть на входе дано* n.
2. *Полагаем* $i = 0$.
3. *В цикле по* i *проверяем равенство* $f(i) = n$. *Если оно верно, то выдаём 1 и заканчиваем работу. Иначе* $i = i + 1$ *и продолжаем цикл.*

$\underline{\Longleftarrow}$ $\varnothing$ перечислиимо. Пусть $A \neq \varnothing$, тогда выберем $a_0 \in A$. Пусть $\gamma : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ — вычислимая биекция (существует по предыдущей теореме) и пусть $\gamma(n) = (\alpha(n), \beta(n))$, тогда строим вычислимую последовательность $f : \mathbb{N} \to \mathbb{N}$ с образом A.
Для нахождения $f(n)$ делаем $\beta(n)$ шагов в вычисление $\chi_A^-(\alpha(n))$ или меньше, если процесс завершится раньше. Если за это время вычисления закончились, то полагаем $f(n) = \alpha(n)$, иначе $f(n) = a_0$.
Докажем, что $imf = A$.
Пусть $a \in A$, тогда $\chi_A^-(a)$ вычислится за какое-то k шагов. Так как γ — биекция, то имеем $\gamma(n) = (a, k)$ для некоторого n, то есть $\alpha(n) = a$, $\beta(n) = k$. Тогда по построению $f(n) = a \Longrightarrow a \in imf$. Значит, $A \subseteq imf$.
Если $f(n) = a_0$, то $f(n) \in A$. Если $f(n) = \alpha(n)$, то по определению полувычислимости имеем $\alpha(n) \in A$. Значит, $imf \subseteq A$. Тогда $imf = A$. ∎

20 Билет 97 (Перечислимость образа и прообраза перечислимой функции, перечислимость множества значений вычилимой функции)

Теорема 20.1. *Пусть $h : \Delta^\infty \to \Delta^\infty$ — вычислимая тотальная (всюду определённая) функция, тогда*

1. *Если $A \subseteq \Delta^\infty$ разрешимо, то $h^{-1}(A)$ разрешимо.*
2. *Если $A \subseteq \Delta^\infty$ перечислимо, то $h(A)$ и $h^{-1}(A)$ перечислимо.*

Доказательство.

1. $\chi_{h^{-1}(A)} = \chi_A \circ h$, тогда по утверждению из билета 96 (композиция вычислимых функций вычислима) $\chi_{h^{-1}(A)}$ вычислима, а значит, по определению $h^{-1}(A)$ разрешимо.
2. (a) Для $h^{-1}(A)$ $\chi^-_{h^{-1}(A)} = \chi^-_A \circ h$. По теореме из билета 96 χ^-_A вычислима, тогда по утверждению из билета 96 (композиция вычислимых функций вычислима) имеем, что $\chi^-_{h^{-1}(A)}$ вычислима, а значит, по определению $h^{-1}(A)$ полуразрешимо, а по теореме из билета 96 оно перечислимо.

   (b) Для $h(A)$, если $A = \varnothing$, то очевидно. Если $A \neq \varnothing$, то $A = imf$ для вычислимой последовательности f. Тогда $h(A) = im(h \circ f)$, а по утверждению из билета 96 (композиция вычислимых функций вычислима) имеем $h \circ f$ вычислима, а значит, по опредению $h(A)$ перечислимо.

■

Теорема 20.2. *Множество значений вычислимой функции перечислимо.*

Доказательство. Функция вычислима, тогда по теореме Поста из билета 95 она полувычислима. Тогда по определению её образ полуразрешим. По теореме из билета 96 он перечислим. ■

21 Билет 98 (Аксиоматичекие исчисления, порождаемые множества слов)

Определение 21.1. *Формальный язык в алфавите Σ — это подмножество Σ^∞.*

Определение 21.2. *k-посылочное правило вывода над Φ — это подмножество Φ^{k+1}.*

Определение 21.3. *Пусть Q-k-посылочное правило вывода. Слово β получается по правилу Q из слов α_1, …, α_k, если $(\alpha_1, \dots, \alpha_k, \beta) \in Q$.*

Определение 21.4. *Аксиоматическое исчисление (Гильбертовская система) — это тройка* $X = (\Phi, A, R)$*, где*

1. Φ *— формальный язык.*

2. $A \subseteq \Phi$.

3. R *— множество правил вывода над* Φ.

Определение 21.5. *Вывод или доказательство слова* β *в исчислении* $X = (\Phi, A, R)$ *из множества* Γ *— это последовательность слов* $\alpha_1, \ldots, \alpha_n = \beta$*, где* α_i *либо аксиома из* A*, либо принадлежит* Γ*, либо выводится по одному из правил вывода из предыдущих.*

Определение 21.6. $\Gamma \vdash_X \beta$*, существует вывод* β *из* Γ *в* X.

Определение 21.7. *Аксиоматическое исчисление называется эффективно или конструктивно заданным, если*

1. *алфавит* Σ *конечен, а язык* Φ *разрешим,*

2. *множество* A *аксиом разрешимо,*

3. *объединение всех правил вывода* $\bigcup R$ *разрешимо.*

Определение 21.8. *Теорема исчисления* X *— это слово выводимое из пустого множества.*

Определение 21.9. *Множество всех теорем эффективно заданного исчисления называется порождаемым.*

Лемма 21.1. *Пусть* Док(X) *— множество доказательств* X*, тогда* Док(X) *перечислимо.*

Доказательство. Используя тезис Чёрча, проведём такой алгоритм:

Алгоритм 21.1.

1. *Пусть дано на вход слово* β *разобъём его на части* $\alpha_1, \ldots, \alpha_n$ *и будем последовательно анализировать* α_i.

2. *Проверим, верно ли, что* $\alpha_i \in A$*. Если да, то переходим к* α_{i+1}*. Если дошли до* α_n*, то завершаем алгоритм с положительным результатом. Если нет, то переходим к шагу 3.*

3. *Рассмотрим подпоследовательностей* $\gamma_1, \ldots, \gamma_m$ *и* $\alpha_1, \ldots, \alpha_{i-1}$*. Если нашлась подпоследовательность* $\gamma_1, \ldots, \gamma_m$ *такая, что* $(\gamma_1, \ldots, \gamma_m, \alpha_i) \in \bigcup R$*, то переходим к* α_{i+1}*. Если такая подпоследовательность не нашлась, то завершаем алгоритм с отрицательным результатом.*

■

Теорема 21.1. *Порождаемое множество перечислимо.*

Доказательство. Пусть $X = (\Phi, A, R)$ — эффективно заданное исчисление, $[X]$ — множество его теорем. Запишем доказательство $\alpha_1, \ldots, \alpha_n$ как слово $\alpha_1\#\ldots\#\alpha_n$, где $\#$ — разделитель (буква, не входящая в алфавит X). Заметим, что $[X] = h(\text{Док}(X))$ для некоторой вычислимой функции h. По лемме Док(X) перечислимо, тогда по теореме из билета 97 $h(\text{Док}(X)) = [X]$ перечислимо. ■

22 Билет 99 (Порождаемость перечислимых множеств, примеры порождаемых множеств)

Теорема 22.1. *Перечислимое множество порождаемо.*

Пример 1. *Рассмотрим определение модальной формулы:*

1. *Если $A \in Var$, то $A \in Fm$.*
2. *Если A, $B \in Fm$, то $A \wedge B \in Fm$.*
3. *Если A, $B \in Fm$, то $A \vee B \in Fm$.*
4. *Если A, $B \in Fm$, то $A \to B \in Fm$.*
5. *Если $A \in Fm$, то $\neg A \in Fm$.*
6. *Если $A \in Fm$, то $\Box A \in Fm$.*

Var порождается одной аксиомой и одним правилом вывода:
Аксиома: $P(|)$.
Правило вывода: $\frac{P(x)}{P(x|)}$. Добавим следующие правила вывода:

1. $\frac{A,\ B}{A \vee B}$
2. $\frac{A,\ B}{A \wedge B}$
3. $\frac{A,\ B}{A \to B}$
4. $\frac{A}{\neg A}$
5. $\frac{A}{\Box A}$

Определение 22.1. *Грамматика — исчисление специального вида, при помощи которого можно порождать перечислимые множества.*

Определение 22.2. *Контекстно-свободная грамматика — грамматика с алфавитом из 2 видов символов: вспомогательные и терминальные. Аксиома КС грамматика — однобуквенное слово S (специальное символ вспомогательного алфавита). Все правила вывода записываются в виде $P \to \alpha$, где P — вспомогательный символ, α — слово в алфавите грамматики.*

Определение 22.3. *Язык выводимый грамматикой — это множество выводимых в ней слов, состоящих из терминальных символов.*

Пример 2. *Множество Fm порождается КС грамматикой, где терминальные символы p, $(,)$, $|$, логические связки, а вспомогательные — N, S.*

Утверждение 22.1. *Язык, порождаемый КС грамматикой, разрешимы.*

Доказательство. Если в языке нет пустого слова, то все правые части правил вывода можно считать не пустыми. Тогда в процессе вывода слова не удлиняются.
Для проверки выводимости конкретного слова α переберём все слова той же или меньше длины и оставим из них только те, из которых α выводится за 1 шаг. И повторим процесс для них. Этот алгоритм закончится так как длина слов уменьшается. ■

23 Билет 100 (Разрешимые исчисления и теории)

Определение 23.1. *Исчисление называется разрешимым, если разрешимо его множество теорем.*

Определение 23.2. *Теория T конечной сигнатуры разрешима, если разрешимо её логическое замыкание, то есть разрешимо $[T] = \{A | T \models A\}$.*

Теорема 23.1. *Если T — множество замкнутых формул конечной сигнатуры, то множество $[T]$ перечислимо.*

Доказательство. Пусть Ω — данная сигнатура. По теореме Гёделя о полноте из билета 74 $[T] = \{A \in CFm | T \vdash A\}$. Рассмотрим исчисление предикатов PC с аксиомами

1. $\forall x([x/a]A) \to [t/a]A$
2. $[t/a]A \to \exists x[x/a]A$
3. $\forall x[x/a](A \to B) \longrightarrow (A \to \forall x[x/a]B)$, если $a \notin A$.
4. $\forall x[x/a](B \to A) \longrightarrow (\exists x[x/a]B \to A)$, если $a \notin A$.

Везде $(x \notin A) \wedge (x \notin B)$.
А так же добавим к ним аксиомы из T. Тогда X эффективно задано, так как PC задаётся эффективно и множество T разрешимо. По теореме из билета 98 (перечислимость порождаемого множества) $[X]$ перечислимо.
Запишем $[T] = [X] \cap CFm_\Omega$. Так как CFm_Ω порождается КС грамматикой, то оно перечислимо и разрешимо. Так как $[X]$ перечислимо, то по теореме из билета 96 оно полуразрешимо. Тогда по утверждению из билета 94 имеем, что $[T]$ полуразрешимо, тогда по теореме из билета 96 оно перечислимо. ■

24 Билет 101 (Теорема Яничака)

Теорема 24.1. *Если теория T конечной сигнатуры полна и задаётся разрешимым множеством аксиом, то она разрешима.*

Доказательство. Будем считать, что теория выполнима, иначе она порождает все формулы и доказывать нечего. По теореме из билета 100 $[T]$ перечислимо, а из теореме Поста из билета 95 следует, что достаточно доказать перечислимость дополнения.
Рассмотрим $\Sigma^\infty \setminus [T] = (\Sigma^\infty \setminus CFm_\Omega) \cup (CFm_\Omega \setminus [T])$. Первое множество разрешимо как дополнение разрешимого CFm_Ω.
Рассмотрим второе. Если $A \notin [T]$, то $\neg A \in [T]$ из полноты и выполнимости T. Таким образом, $CFm_\Omega \setminus [T] = h^{-1}([T])$, где h — функция добавляющая отрицание к формулам. Так как h вычислима, то по теореме из билета 97 $CFm_\Omega \setminus [T]$ перечислимо. Значит, $\Sigma^\infty \setminus [T]$ перечислимо, как объединение перечислимых. ■

Пример 3. *Категоричные теории разрешимы.*

25 Билет 102 (Теорема Харропа)

Определение 25.1. *Модальное исчисление L полно относительно шкал Крипке, если найдётся множество конечных шкал S такое, что для любой модальной формулы A $\vdash_L A \Leftrightarrow \forall F \in S \; F \models A$.*

Теорема 25.1. *Если модальное исчисление получается из K добавлением конечного числа аксиом и полно, относительно конечных шкал, то оно разрешимо.*

Доказательство. По теореме из билета 98 (порождаемое множество перечислимо) L порождает перечислимое множество теорем $\{A | \vdash_L A\}$, значит, оно полуразрешимо по теореме из билета 96, то есть достаточно доказать полуразрешимость дополнения.
Будем последовательно строить все возможные шкалы мощности 1, 2, ..., на каждой из

них будем проверять $F \in S$, то есть общезначимость аксиом L. По условию они получаются как подстановычные примеры конечного числа форул $B_1, \ldots, B_n$. Для каждой B_i проверим, верно ли, что $F \models B_i$. Если $F \not\models B_i$, то переходим к следующей шкале.
Если все аксиомы общезначимы на F, то проверяем общезначимость A. Если $F \not\models A$, то алгоритм возвращает 1. Иначе переходит к следующей шкале.
Так как $\nvdash_L A \Leftrightarrow \exists F \in S\ F \not\models A$, то алгоритм удовлетворяет нужному нам условию: он возвращает 1, если $\nvdash_L A$ и зацикливается в противном случае. Значит, множество $\{A \in F | \vdash_L A\}$ полуразрешимо, тогда по теореме Поста из билета 95 множество L разрешимо. ■

Следствие 25.1.1. *Исчисления K и $S5$ разрешимы.*

Доказательство. По теореме о полноте для K из билета 87 имеем, что K полно, тогда по теореме выше K разрешимо.
По определению $S5$ получается из K добавлением конечного числа аксиом, а по теореме о полноте для $S5$ из билета 89 $S5$ полна, тогда по теореме выше она разрешима. ■

Следствие 25.1.2. *Исчисление предикатов без равенства в сигнатуре с одноместными предикатами разрешимо.*

Доказательство. По переводу Вайсберга из билета 84 каждую модальную формулу можно преобразовать в формулу логики предикатов с одной свободной переменной. ■

26 Билет 103 (Машины Тьюринга)

Определение 26.1. *Код машины Тьюринга — это натуральное число, кодирующее её алфавиты и программу. Обозначение: $Code(M)$. По коду можно восстановить программу*

Определение 26.2. *Универсальная машина Тьюринга, получив на вход число n и слово α, выдаёт $M_n(\alpha)$ — результат работы M_n (машина с кодом n) на слове α, или зацикливается, если $M_n(\alpha)$ не определён. Обозначение: UM.*

Теорема 26.1. *Существует универсальная машина Тьюринга.*

Доказательство. Дана пара (n, α), тогда по коду M_n найдём программу M_n. Найдём слово $M_n(\alpha)$ и расположим его на ленте, окружив пробелами #. ■

27 Билет 104 (Теорема об универсальной вычислимой функции)

Теорема 27.1. *Существует универсальная вычислимая функция $F : \mathbb{N}^2 \to ?\mathbb{N}$ со следующим свойством: для любой вычислимой $f : \mathbb{N} \to ?\mathbb{N}$ найдётся m такое, что для всех n $F(m, n) =? f(n)$.*

Доказательство. Положим $F(m,n) =?|UM(m\Box n)|$, где $UM(m\Box n) =?M_n(n)$, $\Box$ — разделитель, $|\dots|$ — длина слова.
Пусть $f : \mathbb{N} \to ?\mathbb{N}$ и M_m — машина Тьюринга, вычисляющая f. Тогда всех n $f(n) = ?M_m(n) = UM(m\Box n) = F(m,n)$. ■

28 Билет 105 (Построение перечисломого неразрешимого модмножества в $\mathbb{N}$)

Теорема 28.1. *Существует перечислое неразрешимое модмножество в* $\mathbb{N}$.

Доказательство. Обозначим через φ_m — вычислимую функцию с номером m, то есть $\varphi_m(n) =?F(m,n)$. Пусть $d(x) =?F(x,x) =?\varphi_x(x)$.
Рассмотрим $K = dom\ d$, тогда K полуразрешимо, а значит, перечислимо, и докажем, что $-K$ не перечислимо.
Предположим противное, пусть $-K$ перечислимо, тогда $-K = dom\ \varphi_n$, где $\varphi_n = \chi^-_{-K}$. Тогда $x \notin K \Leftrightarrow x \in dom\ \varphi_n$, а значит, $n \notin K \Leftrightarrow n \in dom\ \varphi_n$. Но по определению K $n \in K \Leftrightarrow n \in dom\ \varphi_n$. То есть мы получили, что $n \in K \Leftrightarrow n \notin K$ — противоречие.
Значит, $-K$ не полуразрешимо, а значит, по теореме Поста из билета 95 K не разрешимо. ■

29 Билет 106 (Неразрешимость проблемы остановки машины Тьюринга)

Утверждение 29.1. *Область определения универсальной вычислимой функции не разрешима.*

Доказательство. Имеем $n \in K \Leftrightarrow n \in dom\ F$, тогда $K = g^{-1}(F)$, где $g : \mathbb{N} \to \mathbb{N}^2$ — вычислимая функция. Если $dom\ F$ разрешим, то по теореме из билета 97 K разрешимо, что противоречит теореме из билета 105. ■

Утверждение 29.2. *Множество* $\{(n,\alpha) | M_n$ заканчивает свою работу на входе $\alpha\}$ *неразрешимо.*

Доказательство. Обозначим это множество за X. Заметим, что $X \subseteq \mathbb{N} \times \Delta^\infty$, где $\Delta = \{0,1\}$.
По построению UM $(n,\alpha) \in X \Leftrightarrow UM$ заканчивает работу на входе $n\Box\alpha$.
По построению F $(n,\alpha) \in dom\ F \Leftrightarrow UM$ заканчивает работу на входе $n\Box\alpha$.
Тогда $(n,\alpha) \in dom\ F \Leftrightarrow (n,\alpha) \in X$. То есть $dom\ F = X \cap \mathbb{N}^2$, а X не разрешимо, так как $dom\ F$ не разрешимо по предыдущему утверждению. ■

30 Билет 107 (Арифметические множества, первая теорема Гёделя)

Определение 30.1. *Определимые подмножества стандартной модели* $(\mathbb{N}, 0, 1, +, \cdot, =)$ *называются арифметическими.*

Теорема 30.1 (Теорема Гёделя об определимости)**.** *Любое перечислимое подмножество* $\mathbb{N}$ *является арифметическим.*

Теорема 30.2 (Первая теорема Гёделя о полноте)**.** *Пусть T — теория в сигнатуре арифметики Пеано (AP) с разрешимым множеством аксиом, причём* $\mathbb{N} \models T$*. Тогда теория T не полна. В частности, AP неполна.*

Доказательство. Предположим, что T полна, тогда по теореме Яничака из билета 101 $[T]$ разрешимо. Так как $\mathbb{N} \models T$, то $[T] = Th(\mathbb{N})$, значит, $Th(\mathbb{N})$. Рассмотрим множество $K = dom\ d$, где $d = ?F(x, x) = ?\varphi_x(x)$. По теореме Гёделя об определимости существует формула A такая, что для всех n $n \in K \Leftrightarrow \mathbb{N} \models A(n)$.
Введём обозначение $\underline{n} := 1 + \ldots + 1$, $\underline{0} := 0$.
Такие символы называются нумералами. Очевидно, что $\mathbb{N} \models (\underline{n} = n)$, значит, $\mathbb{N} \models (A(\underline{n}) \leftrightarrow A(n))$. Тогда $n \in K \Leftrightarrow A(\underline{n}) \in Th(\mathbb{N})$, то есть $K = h^{-1}(Th(\mathbb{N}))$, где h — вычислимая функция, переводящая n в $A(\underline{n})$. Тогда по теореме из билета 97 (прообраз вычислимой функции от разрешимого множества разрешим) K разрешимо — противоречие, значит, T неполна. ∎

31 Билет 108 (Арифметическая теория Q, теорема Гёделя о представимости разрешимых множеств)

Определение 31.1. *Теория Q получается из теории Пеано удалением схемы индукции, то есть она содержит следующие 7 аксиом:*

1. $\forall x(x + 1 \neq 0)$
2. $\forall x \forall y((x + 1 = y + 1) \to (x = y))$
3. $\forall x((x \neq 0) \to \exists y(x = y + 1))$
4. $\forall x(x + 0 = x)$
5. $\forall x \forall y(x + (y + 1) = (x + y) + 1)$
6. $\forall x(x \cdot 0 = 0)$
7. $\forall x \forall y(x \cdot (y + 1) = x \cdot y + x)$

Теорема 31.1 (Теорема Гёделя о представимости)**.** *Пусть* $R \subseteq \mathbb{N}^k$ *— разрешимое отношение. Тогда существует арифметическая формула* $A(a_1, \dots, a_k)$ *такая, что для всех* $n_1, \dots, n_k \in \mathbb{N}$*:*

1. *Если* $(n_1, \dots, n_k) \in R$*, то* $Q \vdash A(\underline{n_1}, \dots, \underline{n_k})$*.*

2. *Если* $(n_1, \dots, n_k) \notin R$*, то* $Q \vdash (\underline{n_1}, \dots, \underline{n_k})$*.*

Теорема 31.2 (Теорема о слабой представимости)**.** *Пусть* T *— теория в сигнатуре арифметики,* $Q \subseteq T \subseteq Th(\mathbb{N})$*,* $S \subseteq \mathbb{N}$ *— перечислимое множество. Тогда существует арифметическая формула* $B(a)$ *такая, что для всех* $n \in \mathbb{N}$ $n \in S \Leftrightarrow T \vdash B(\underline{n})$*.*

Доказательство. По теореме из билета 99 (перечислимое множество порождаемо) имеем S порождаемо, то есть $S = [X]$ для некоторого эффективно заданного исчисления X. Из доказательства теоремы из билета 98 знаем $[X] = h[\text{Док}(X)]$ для некоторой вычислимой функции h, причём $\text{Док}(X)$ разрешимо. Доказательства в X можно закодировать натуральными числами, тогда получим разрешимое множество $\text{КДок}(X)$ и биекцию $\varphi : \text{КДок}(X) \to \text{Док}(X)$ (декодирование). Таким образом, имеем $n \in S \Leftrightarrow \exists m(n \in \text{КДок}(X) \wedge n = h(\varphi(m)))$.
Заметим, что $R := \{(m, n) | n \in \text{КДок}(X) \wedge n = h(\varphi(m))\}$ разрешимо как пересечение разрешимых. Тогда по теореме Гёделя о представимости существует арифметическая формула $A(a, b)$ такая, что:

1. Если $(m, n) \in R$, то $Q \vdash A(\underline{m}, \underline{n})$.

2. Если $(m, n) \notin R$, то $Q \vdash \neg A(\underline{m}, \underline{n})$.

Рассмотрим $B(a) := \exists x A(x, a)$.

1. Пусть $n \in S$, тогда $(m, n) \in R$ для некоторого m. Значит, $Q \vdash A(\underline{m}, \underline{n})$, а из исчисления предикатов $Q \vdash \exists x A(\underline{n}, x)$, тогда $T \vdash \exists x A(\underline{n}, x)$.

2. Пусть $T \vdash B(n)$, тогда $\mathbb{N} \models \exists x A(x, \underline{n}) \Longrightarrow \mathbb{N} \models A(m, \underline{n})$ для некоторого m. Тогда $\mathbb{N} \models A(\underline{m}, \underline{n})$. Если $(m, n) \notin R$, то $Q \vdash \neg A(\underline{m}, \underline{n})$, а значит, $\mathbb{N} \models \neg A(\underline{m}, \underline{n})$ — противоречие. Значит, $(m, n) \in R$

Таким образом, мы получили, что $B(n)$ — искомая формула. ■

32 Билет 109 (Теорема о неразрешимости теорий, содержащих Q)

Теорема 32.1. *Пусть* T *— теория в сигнатуре арифметики и* $Q \subseteq T \subseteq Th(\mathbb{N})$*, тогда* T *неразрешима.*

Доказательство. Рассмотрим множество $K = dom\ d$, где $d =?F(x,x) =?\varphi_x(x)$. По теореме о слабой представимости из билета 108 существует функция $B(n)$ такая, что $n \in K \Leftrightarrow T \vdash B(n)$, то есть $K = h^{-1}[T]$, где h — вычислимая функция, переводящая n в $B(\underline{n})$. Если T разрешима, то по теореме из билета 97 и разрешимости $[T]$ следует разрешимость K — противоречие. Значит, T неразрешима. ■

Теорема 32.2 (Теорема Чёрча)**.** *Исчисление предикатов в сигнатуре арифметики неразрешимо.*

Доказательство. Из следствия теоремы дедукции из билета 70 имеем для случая $T = Q$ $Q \vdash_{PC^=_\Omega} A \Leftrightarrow \vdash_{PC^=_\Omega} (\bigwedge Q \to A)$. Рассмотрим вычислимую функцию $f : A \to (\bigwedge Q \to A)$, тогда $[Q] = f^{-1}(\{B | \vdash_{PC^=_\Omega} B\})$. Предположим, что $PC^=_\Omega$ разрешимо, тогда по теореме из билета 97 $[Q]$ разрешимо, что противоречит предыдущей теореме. Значит, $PC^=_\Omega$ неразрешимо. ■

33 Билет 110 (Теорема о главной универсальной вычислимой функции)

Определение 33.1. *Универсальная вычислимая функция $F : \mathbb{N}^2 \to ?\mathbb{N}$ называется главной, если для любой вычислимой функции $g : \mathbb{N}^2 \to ?\mathbb{N}$ существует тотальная (всюду определённая) функция $s : \mathbb{N} \to \mathbb{N}$ такая, что $\forall e \forall x g(e,x) =?F(s(e),x)$.*

Теорема 33.1. *Рассмотрим $F(m,n) =?|UM(m\Box n)|$. Функция F — главная универсальна вычислимая функция.*

Доказательство. Пусть $F(m,n) =?|UM(m\Box n)| =?M_m(n)$. Если дана вычислимая $g : \mathbb{N}^2 \to \mathbb{N}$, то для каждого e имеем вычислимую функцию $f_e : \mathbb{N} \to \mathbb{N}$.
Имея x, строим $e\Box x$ и подаём это на вход программе для g. Таким образом, получаем функцию s, переводящую число e в код программы для вычисления f_e.
То есть $F(s(e),x) =?|M_{s(e)}(x)| =?f_e(x) =?g(e,x)$. ■

34 Билет 111 (Индексные множества, теорема Успенского—Райса)

Определение 34.1. *Пусть C — какое-то множество вычислимых функций $f_i : \mathbb{N} \to ?\mathbb{N}$. Индексным множеством для C называется множество всех их номеров, то есть $I_C = \{n | f_n \in C\}$.*

Теорема 34.1 (Теорема Успенского—Райса)**.** *Пусть C — нетривиальное множество вычислимых функций $f_i\mathbb{N} \to ?\mathbb{N}$, то есть C не пусто и не состоит из всех таких функций, тогда I_C неразрешимо.*

Доказательство. Будем считать, что $\varnothing \notin C$, в противном случае будем рассматривать дополнение C. Зафиксируем функцию $f_0 \in C$.
Рассмотрим множество $K = dom\ d$, где $d = ?F(x,x) = ?\varphi_x(x)$. Построим вычислимую функцию $g : \mathbb{N}^2 \to \mathbb{N}$ следующим образом:
$$g(e,x) = \begin{cases} f_0(x), \text{ если } e \in K \text{ и } x \in dom\ f_0 \\ ?, \text{ иначе} \end{cases}$$
По второй теореме из билета 110 существует $s : \mathbb{N} \to \mathbb{N}$ такое, что для всех x $g(e,x) = ?F(s(e),x)$. Тогда, если $e \in K$, то $\forall x F(s(e),x) = ?g(e,x) = ?f_0(x)$. То есть, если $e \in K$, то $\varphi_{s(e)} = f_0$ по определнию K.
Аналогично, если $e \notin K$, то $\varphi_{s(e)} = \varnothing$.
Значит, $e \in K \Leftrightarrow \varphi_{s(e)} \in C$ или, что тоже самое $e \in K \Leftrightarrow\ s(e) \in I_C$. Значит, $K = s^{-1}(I_c)$.
Предположим, что I_C разрешимо, тогда по теореме из билета 97 получаем, что K разрешимо, что противоречит теореме из билета 105. Значит, I_C неразрешимо. ■

35 Билет 112 (Недетерминированные вычисления, классы NP и P)

Определение 35.1. *Недетерминированное вычисление — это преобразование входного слова в соответствии с командами.*

Определение 35.2. *Машина преобразует слово α в слово β, если существует хотя бы одно вычисление, выполняющее такое преобразование.*

Теорема 35.1. *Всякая функция, вычислимая недетерминированной машиной Тьюринга, вычислима и детерминированной машиной.*

Определение 35.3. *Разрешимое множество слов S принадлежит классу NP, если принадлежность к S распознаётся на какой-нибудь недетерминированной машине M за полиномиальное время. То есть, если существует полином $p(x)$ такой, что для любого входного слова $\alpha \in S$ машина M может получить результат 1 за время, не превосходящее $p(|\alpha|)$.*

Определение 35.4. *Разрешимое множество слов S принадлежит классу NP, если его характеристическая функция χ_S вычислима на какой-нибудь детерминированной машине за полиномиальное время.*

Определение 35.5. *Обозначим SAT — множество всех выполнимых классических пропозициональных формул (то есть $A \notin SAT$, если $\neg A$ — тавтология).*

Теорема 35.2. *$SAT \in P$.*

Доказательство. Пусть дана пропозициональная формула $A(P_1, \ldots, P_n)$. Ясно, $n \leqslant |A|$. Если задана оценка переменных P_1, …, P_n, то можно подставить их значения в A и найти значение A за полиомиальное время от n.
Если вычисление детерминированно, то надо будет перебрать все оценки переменных и в каждом случае найти значение A. Количество оценок 2^n, а значит, этот алгоритм не укладывается в полиномиальное время.
Если вычисление недетерминированно, то можно оставить для каждой переменной оба значения 0 и 1 в качестве вариантов перехода. Значит, если формула выполнима (это верно так как SAT — множество выполнимых формул), то найдётся процесс вычисления, дающий в результате 1. Он будет работать за полиномиальное время, так как он будет сразу выбирать подходящую комбинацию значений и будет совершать проверку, то есть будет работать за $O(n)$. ■

Теорема 35.3 (Проблема перебора)**.** *Верно ли, что* $P \neq NP$*?*