Содержание

1 Линейная алгебра.

1.1 Введение.

Пример. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$
$A \times B = \{(a, b) | a \in A, b \in B\}$
F — поле, 2 операции, обе обратимы.
Векторное пространство V над F: $(V, +, *)$

1. $\forall v, u, w \in V$: $(v + u) + w = v + (u + w)$
2. $\forall v, u \in V$: $v + u = u + v$
3. $\exists v \in V$: $\forall v \in V$: $0 + v = v$
4. $\forall v \in V$: $\exists$ "$-v$": v + "$-v$"$= 0$
5. $\forall v \in V; \alpha, \beta \in F$: $\alpha * (\beta * v) = (\alpha\beta) * v$
6. $\forall v \in V; \alpha, \beta \in F$: $(\alpha + \beta) * v = \alpha * v + \beta * v$
7. $\forall v, w \in V; \alpha \in F$: $\alpha * (v + w) = \alpha * v + \alpha * w$
8. $\forall v \in V$: $1 * v = v$

Утверждение 1.1. *Если v, w — векторное пространство над F, то и $v \times w$ — тоже векторное пространство над F.*

V — векторное пространство над F.

Определение 1.1. *$W \subseteq V$ — подпространство.*

1. *$\forall w_1, w_2 \in W$: $w_1 + w_2 \in W$*
2. *$\forall w \in W; \alpha \in F$: $\alpha w \in W$*

$V = R \times R$, $W = \{v \in V | x + y = 0\}$

Определение 1.2. *Линейное отображение:*

1. *$f(x) + f(y) = f(x + y)$*
2. *$f(\alpha x) = \alpha f(x)$*

1.2 Фактор-пространства.

Определение 1.3. *Поле F, $W \subseteq V$ — векторное пространство; V/W — факторизация. Отношение $\sim$ на V: $v \sim u \Leftrightarrow u - v \in W$.*

1. *$u - u = 0 \in W$*
2. *$u - v \in W \Leftrightarrow v - u \in W$*
3. *$(u - v) \in W \wedge (v - w) \in W \Rightarrow (u - v) + (v - w) \in W \Rightarrow u - w \in W$*

$[v]$ — класс эквивалентности вектора v.

1. $[v] + [u] = [v + u]$

2. $\alpha[v] = [\alpha v]$

$v_1 \sim v_2 \Rightarrow u + v_1 \sim u + v_2$
$v_1 \sim v_2 \Rightarrow \alpha v_1\ \alpha v_2$

Отображение векторного пространства.

V, W — векторные пространства над F.
$f : V \to W$ — линейная, если

1. $\forall v_1, v_2 \in V : f(v_1) + f(v_2) = f(v_1 + v_2)$
2. $\forall v \in V, \alpha \in F : \alpha f(v) = f(\alpha v)$

Если f — биекция, то f — изоморфизм, V и W — изоморфны.

1. Рефлективна $f = id\ V \to V : v \to v$
2. Симметрична $V \xrightarrow{f} W$ f^{-1} — обратное отображение: $f^{-1}(x) + f^{-1}(y) = f^{-1}(x + y)$
3. $V \xrightarrow{f} W$, $W \xrightarrow{g} U$. f, g — линейная биекция, $f \circ g$ — линейная биекция.

$\mathbb{R}^n = (x_1, x_2, \dots, x_n)$, $\mathbb{R}^m = (y_1, y_2, \dots, y_m)$
Табличка $n \times m$: $\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$
Отображение $\mathbb{R}^n \to \mathbb{R}^m$ (линейное):
$(x_1, \dots, x_n) \to \begin{pmatrix} a_{11}x_1 + \dots + a_{1n}x_n \\ a_{21}x_1 + \dots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n \end{pmatrix}$

Определение 1.4. *V — векторное пространство над F. Набор $v_1, \dots, v_k$. $\sum \alpha_i v_i, \alpha_i \in F \to$ конечное число $\alpha_i \neq 0$. Все линейные комбинации образуют векторное подпространство $span(v_1, \dots, v_k, \dots)$.*

Определение 1.5. *$v_1, \dots, v_k, \dots$ — линейно независимая $\Leftrightarrow \nexists$ нетривиальных линейных комбинаций (не все коэффициенты равны 0), те все коэффициенты равны 0, и других решений нет. Линейно зависимая иначе.*

Определение 1.6. *$v_1, \dots, v_k, \dots$ — порождающая система, если $span(v_1, \dots, v_k, \dots) = V$ ($span()$ — множество всех возможных линейных комбинаций).*

Определение 1.7. *Базис = линейно независимая + порождающая система. Базис — максимальная линейно независимая система векторов в пространстве V.*

Определение 1.8. *V — конечномерное $\Leftrightarrow \exists$ конечная порождающая система.*

Возьмем минимальную (по включению) порождающую систему. $v_1, \dots, v_e$. Пусть оказалась линейно зависимой. $\sum \alpha_i v_i = 0$. НУО $\alpha_1 \neq 0$. $v_1 = \sum \frac{-d_j}{d_1} v_j$. Тогда можем выкинуть.
(!) Любой базис одинакового размера. $e_1, \dots, e_k$; $f_1, \dots, f_m$. $m > k$. Хотим e_i: $(e_i, f_2, \dots, f_m)$ — линейно независимая система. Пусть нет. Тогда $\forall i \exists \alpha_1, \dots, \alpha_m : \alpha_1 e_i + \alpha_2 f_2 + \dots + \alpha_m f_m = 0 \Rightarrow e_i = \sum \beta_{ij} f_j \Rightarrow$ f_2 – f_m — порождают все ?! Значит $(e_1, f_2, \dots, f_m)$ — линейно независимая система. $e_1 = \sum \alpha_j f_j \Rightarrow$ $\alpha \neq 0 \Rightarrow f_1 = \frac{1}{\alpha_1} e_1 - \sum\limits_{j \neq 1} \frac{\alpha_j}{\alpha_1} f_j \Rightarrow (e_1, f_2, \dots, f_m)$ — базис.

Определение 1.9. $\dim V =$ *количество элементов базиса.*

$A \xrightarrow{f} B$: $f(A)$ — векторное подпространство в B.

Утверждение 1.2. *Линейное независимые системы не бывают больше, чем базис.*

Доказательство. $e_1,\dots,e_k$; $f_1,\dots,f_{k+1}$. Рассмотрим наборы $(e_1,f_2,\dots,f_{k+1})$; $(e_1,\dots,e_k,f_{k+1})$ — линейно независимая система. $\square$

Теорема 1.1. *V — векторное пространство над полем $F \Rightarrow V \cong F^{\dim V}$.*

Доказательство. fix базис $e_1,\dots,e_n$, где $n=\dim V$.

Лемма 1.1. *$\forall v \in V\ \exists!(\alpha_1,\dots,\alpha_k)$: $V=\sum \alpha_k e_k$.*

Доказательство. Пусть есть два набора $(\alpha_1,\dots,\alpha_k)$ и $(\beta_1,\dots,\beta_k)$. $0=V-V=\sum(\alpha_k-\beta_k)e_k \Rightarrow \alpha_k = \beta_k \forall k$. $\square$

$f : F^n \to V$
$(x_1,\dots,x_n) \to \sum x_i e_i$
$(y_1,\dots,y_n) \to \sum y_i e_i$
$(x_1+y_1,\dots,x_n+y_n) \to \sum(x_i+y_i)e_i$
$f(\lambda(x_1,\dots,x_n)) = \sum(\lambda x_i)e_i = \lambda(\sum x_i e_i)$
<u>Инекция.</u> $f(x_1,\dots,x_n)=f(y_1,\dots,y_n) \Rightarrow (x_1,\dots,x_n)=(y_1,\dots,y_n)$
<u>Сюръекция.</u> $V=\sum \alpha_i e_i \Rightarrow v = f(\alpha_1,\dots,\alpha_n)$ $\square$

1.3 Матрицы.

$\underline{\mathbb{R}^n \xrightarrow{f} \mathbb{R}^m}$

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

$$(x_1,\dots,x_n) \to \begin{pmatrix} a_{11}x_1+\dots+a_{1n}x_n \\ a_{21}x_1+\dots+a_{2n}x_n \\ \vdots \\ a_{m1}x_1+\dots+a_{mn}x_n \end{pmatrix}$$

$e_1=(1,0,\dots,0) \to (b_{11},b_{21},\dots,b_{m1})$
$e_2=(0,1,\dots,0) \to (b_{12},b_{22},\dots,b_{m2})$
$\vdots$
$e_n=(0,0,\dots,1) \to (b_{1n},b_{2n},\dots,b_{mn})$
$f((x_1,x_2,\dots,x_n)) = x_1 f(e_1)+x_2 f(e_2)+\dots+x_n f(e_n) = x_1(b_{11},b_{21},\dots,b_{m1})+x_2(b_{12},\dots,b_{m2})+\dots=$
$(x_1b_{11}+x_2b_{12}+\dots+x_nb_{1n},$
$x_1b_{21}+x_2b_{22}+\dots+x_nb_{2n},$
$\dots,$
$x_1b_{m1}+\dots+x_nb_{mn})$

Сложение матриц.

$A=\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$, $B=\begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix}$; X — матрица, f_X — линейное отображение.

$f_A : (x_1,\dots,x_n) \to \begin{pmatrix} a_{11}x_1+\dots+a_{1n}x_n \\ \vdots \\ a_{m1}x_1+\dots+a_{mn}x_n \end{pmatrix}$, $f_B : (x_1,\dots,x_n) \to \begin{pmatrix} b_{11}x_1+\dots+b_{1n}x_n \\ \vdots \\ b_{m1}x_1+\dots+b_{mn}x_n \end{pmatrix}$

$f_A+f_B : (x_1,\dots,x_n) \to \begin{pmatrix} (a_{11}+b_{11})x_1+\dots+(a_{1n}+b_{1n})x_n \\ \vdots \\ (a_{m1}+b_{m1})x_1+\dots+(a_{mn}+b_{mn})x_n \end{pmatrix}$

$A+B := (a_{ij}+b_{ij})$
$\lambda A := (\lambda a_{ij})$

Произведение матриц (композиция).

$\mathbb{R}^n \xrightarrow{f_A} \mathbb{R}^m \xrightarrow{f_B} \mathbb{R}^k$

f_A и f_B построены по матрицам $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$ и $B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix}$

$f_C(V) = f_B(f_A(V))$

$C := B \cdot A$

$e_1 = (1, 0, \dots, 0)$; $f_A(e_1) = (a_{11}, \dots, a_{m1})$

1 столбец: $f_B(a_{11}, \dots, a_{m1}) =$

$(b_{11}a_{11} + b_{12}a_{21} + \dots + b_{1m}a_{m1},$

$b_{21}a_{11} + b_{22}a_{21} + \dots + b_{2m}a_{m1},$

$\vdots,$

$b_{k1}a_{11} + b_{k2}a_{21} + \dots + b_{km}a_{m1})$

$f_A(e_i) = (a_{1i}, \dots, a_{mi})$

i столбец: $f_B(f_A(e_i)) =$

$(b_{11}a_{1i} + b_{12}a_{2i} + \dots + b_{1m}a_{mi},$

$b_{21}a_{1i} + b_{22}a_{2i} + \dots + b_{2m}a_{mi},$

$\vdots,$

$b_{k1}a_{1i} + b_{k2}a_{2i} + \dots + b_{km}a_{mi})$

$C = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & & \vdots \\ c_{k1} & \dots & c_{kn} \end{pmatrix}$

$c_{ij} = b_{i1}a_{1j} + b_{i2}a_{2j} + \dots + b_{im}a_{mj} = \sum\limits_{\alpha=1}^{m} b_{i\alpha}a_{\alpha j}$

Определение 1.10. $F^n \xrightarrow{f_a} F^m$, $f_a(v) = Av$. $Imf = \{u \in F^m | \exists v \in F^n : u = f(v)\}$. $Kerf = \{u \in F^n | f(u) = 0\}$.

Утверждение 1.3. *Imf и $Kerf$ — линейные подпространства.*

Теорема 1.2 (Теорема о гомоморфизме)**.** *Для любого линейного отображения $f : V \to W$ между векторными пространствами факторпространство пространства V по ядру f изоморфно образу f: $V/Kerf \cong Imf$.*

Доказательство. Построение отображения: определим отображение $\phi : V/Kerf \to Imf$, $\phi(v + Kerf) = f(V)$; $v + Kerf$ — это класс эквивалентности в фактропространстве $V/Kerf$. Корректность определения: пусть $v_1 + Kerf = v_2 + Kerf \Rightarrow v_1 - v_2 \in Kerf \Rightarrow f(v_1 - v_2) = 0 \Rightarrow f(v_1) - f(v_2) = 0 \Rightarrow f(v_1) = f(v_2)$. Линейность отображения ϕ: очевидно, остается для доказательство читателю. Сюръективность ϕ: докажем, что для любого элемента $w \in Imf$ найдется прообраз в $V/Kerf$; по определению образа, если $w \in Imf$, то существует такой вектор $v \in V$, что $f(v) = w \Rightarrow$ для класса $v + Kerf$ верно: $\phi(v + Kerf) = f(v) = w \Rightarrow \phi$ — сюръективно. Инъективность ϕ: докажем, что если $\phi(v + Kerf) = 0$, то весь класс $v + Kerf$ является нулевым элементом в $V/Kerf$ (то есть $v + Kerf = 0 + Kerf$); пусть $\phi(v + Kerf) = 0 \Rightarrow$ по определению ϕ: $f(v) = 0$; это означает, что $v \in Kerf \Rightarrow v + Kerf = 0 + Kerf$ (так как в классе эквивалентности $v + Kerf$ лежит сам вектор v, а если $v \in Kerf$, то этот класс совпадает с ядром, которое является нулевым элементом в факторпространстве). ☐

Утверждение 1.4. $V/Kerf \xrightarrow{g} Imf$, $[v] \xrightarrow{g} f(v)$. *Тогда:*

- $[v] \xrightarrow{g} f(v)$ *— корректно заданное отображение.*
- $v_1 - v_2 \in Kerf \Rightarrow f(v_1) = f(v_2) \Leftrightarrow f(v_1 - v_2) = 0$, *тк* $g([v]) = 0 \Rightarrow v \in Kerf \Rightarrow [v]$.
- $u \in Imf \Rightarrow \exists u = f(v) \Rightarrow u = g([v])$.

Определение 1.11. *$rankA := \dim(ImA)$, где A — матрица. Также это размерность линейного замыкания пространства столбцов матрицы. $ImA =$ линейное замыкания пространства столбцов, тк $u \in ImA = f(\sum \alpha_i e_i) = \sum \alpha_i f(e_i)$. $f(e_i)$ — i-ый столбец матрицы.*

Определение 1.12. *Множество всех матриц $n \times m$ над полем F обозначается $M_{n\times m}(F)$. Это множество кольцо с 1 (ассоциативность сложение, нейтральный элемент сложения, обратимость сложения, коммутативность сложения, ассоциативность умножения, дистрибутивность, нейтральный элемент умножения).*

Определение 1.13. *Верхне-треугольная матрица — матрица, в которой под диагональю все нули. Аналогично нижне-треугольная. Они образуют линейное подпространство. Матрица, которая и верхне-треугольная, и нижне-треугольная — диагональная.*

Определение 1.14. *Симметричная матрица — $a_{ij} = a_{ji}$.*

Утверждение 1.5. $\dim(Lin(U \cup W)) + \dim(u \cap w) = \dim(u) + \dim(v)$.

Утверждение 1.6. $rank(AB) = \min(rankA, rankB)$.

Утверждение 1.7. $T^{-1}ATT^{-1}BT = T^{-1}(AB)T$.

Определение 1.15. *Матрица перехода A из базиса e в базис f такова, что $\forall v \in V : v = \sum \alpha_i e_i \Rightarrow v = \sum \beta_i f_i$, где верно, что $A\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$*

1.4 Системы линейных уравнений.

Определение 1.16. *Система линейных уравнений — $\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n = b_m \end{cases} \Leftrightarrow Av = b$, $v = \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix}$. Как устроенно множество решений:*

- $\emptyset$
- *v_0 — единственное решение.*
- *Решений много $\Rightarrow$ это $v_0 + L := \{v_0 + l | l \in L\}$, где v_0 — какое-то решение, L — линейное подпространство ($L = KerA$).*
  $Av_0 = b$; $Av_1 = b \Leftrightarrow A(v_1 - v_0) = 0 \Leftrightarrow (v_1 - v_0) \in KerA$

Определение 1.17. *Присоединение матриц. $(A|b) = \begin{pmatrix} a_{11} & \dots & a_{1n} & |b_1 \\ a_{21} & \dots & a_{2n} & |b_2 \\ \vdots & & \vdots & \\ a_{m1} & \dots & a_{mn} & |b_n \end{pmatrix}$*

Теорема 1.3 (Теорема Кронекера-Капелли)**.** *Система имеет решение $\Leftrightarrow rank(A) = rank(A|b)$.*

Доказательство. $\Leftarrow$: $ImA = \{Av | v \in F^n\}$; $Im(A|b) = \{Av + \alpha b | v \in F^n, \alpha \in F\}$; В ImA есть базис $u_1, \dots, u_k$; $u_1, \dots, u_k \in Im(A|b) \Rightarrow u_1, \dots, u_k$ — базис в $Im(A|b)$; $A(\sum \beta_i u_i) = \sum \beta_i (Av_i) = \sum \beta_i u_i = b$.
$\Rightarrow$: $b = Av_0 \Rightarrow \{Av + \alpha b | v \in F^n, \alpha \in F\} = \{Av | v \in F^n\}$, тк $Av + \alpha b = Av + \alpha(Av_0) = A(v + \alpha v_0) \in ImA$. □

Метод 1.1 (Гаусса)**.** *Приводит матрицу к виду, в котором понятно, решается она или нет. Можно:*

1. *Умножать строку на ненулевое число.*

2. *Переставить две строчки.*

3. *Заменить строку на сумму ее и какой-то другой.*

4. *Прибавить ко второй строке $\alpha \cdot$ первую.*

1.5 Определитель.

Определение 1.18. *Матрица — n строк размера m ($v_i = (a_1, \ldots, a_m)$). Тогда функция det — это такая функция $(v_1, \ldots, v_n) \xrightarrow{\det} F$ ($charF \neq 2$), что она:*

- *Полилинейная:* $\det(v_1 + u_1, v_2, \ldots, v_n) = \det(v_1, v_2, \ldots, v_n) + \det(u_1, v_2, \ldots, v_n)$, $\det(\alpha v_1, v_2, \ldots, v_n) = \alpha \det(v_1, v_2, \ldots, v_n)$.

- *Кососимметричная:* $\det(v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_{j-1}, v_i, v_{j+1}, \ldots, v_n) = -\det(v_1, \ldots, v_n)$.

Свойства:

- Если есть нулевая строка, то $\det A = 0$.

- Если есть две равные (или пропорциональные) строки, то $\det A = 0$ (если $charF \neq 2$).

- 4-ая операция метода Гаусса не меняет определитель.

Утверждение 1.8. *Определитель не более чем один.*

Доказательство. Все операции метода Гаусса контролируемо меняют определитель. Тогда есть два варианта, когда мы дошли до конца алгоритма:

1. Нижняя строка 0. Тогда определитель 0. Тогда он и был 0, тк мы только умножаем его. Отсюда следует, что если определитель 0, то матрица не обратима.

2. Все строки не 0. Тогда делаем из матрицы единичную. У нее определитель 1. Идя в обратную сторону мы однозначно восстанавливаем определитель.

□

Утверждение 1.9. $\det(AB) = \det(A) \cdot \det(B)$.

1.6 Метод Крамера.

Метод 1.2 (Крамера)**.** *Дана матрица A размера $n \times n$ с $\det(A) \neq 0$, X — столбец неизвестных $(x_1, \ldots, x_n)$ и B — столбец свободных членов $(b_1, \ldots, b_n)$. Тогда решение по методу Крамера выглядит вот так:*

> *Каждый неизвестный x_i вычисляется по формуле $x_i = \frac{\det(A_i)}{\det(A)}$, где $\det(A)$ — определитель основной матрицы, $\det(A_i)$ — определитель матрицы, полученной заменой i-го столбца матрицы A на столбец B.*

1.7 Ранговый метод в комбинаторике.

Вершины — $\{0, 1, 2\}^n$. Ребра — соединяем вершину со всеми, которые получаются прибавлением единицы.

1.8 Определенные и полу-определенные матрицы.

Определение 1.19 (Определенная матрица)**.** *Квадратная матрица A размера $n \times n$ называется положительно определенной, если для любого ненулевого вектора $x \in R^n$ выполняется условие: $x^T Ax > 0$.*

Определение 1.20 (Полу-определенная матрица)**.** *Квадратная матрица A размера $n \times n$ называется положительно полу-определенной, если для любого вектора $x \in R^n$ выполняется условие: $x^T Ax \geqslant 0$.*

Утверждение 1.10. $(AB)^T = B^T A^T$.

Утверждение 1.11. *Пусть A — матрица смежности G; $\det A \equiv^2 \#$ совершенных паросочетаний G.*
Пусть в G все степени $\vdots\, 2$; тогда в G четное число совершенных паросочетаний.

Утверждение 1.12. *Пусть S — конечное множество натуральных чисел. $A \subseteq S$ — хорошее, если $\Pi_{x \in A} x = m^2$. Тогда $\#$ хороших множеств $= 2^k$.*

Утверждение 1.13. *Пусть G — связный граф на 100 вершинах. E — его ребра. $A \subseteq F$ — хорошее, если $\forall v\ \# \{uv \in A\} \vdots\, 2$. $\#$ хороших множеств $= 2^{|E|-100+1}$.*

2 Теория типов.

2.1 Основы математической логики. Классическое исчисление высказываний.

Приоритет операций: $\neg \wedge \vee \rightarrow$.

$f : P \rightarrow \{\text{True, False}\}$. $[\![\alpha]\!]^f = \begin{cases} f(X) & \alpha = X \\ \text{True} & \alpha = \beta \wedge \gamma, [\![\beta]\!] = [\![\gamma]\!] = \text{True} \\ \text{True} & \alpha = \beta \vee \gamma, [\![\beta]\!] = \text{True}/[\![\gamma]\!] = \text{True} \end{cases}$

Определение 2.1. *α — общезначимое, если при любой $f : [\![\alpha]\!]^f = True$. $\vDash \alpha$.*

Аксиомы:

1. $\alpha \rightarrow \beta \rightarrow \alpha$
2. $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow \alpha \rightarrow \gamma$
3. $\alpha \rightarrow \beta \rightarrow \alpha \wedge \beta$
4. $\alpha \wedge \beta \rightarrow \alpha$
5. $\alpha \wedge \beta \rightarrow \beta$
6. $\alpha \rightarrow \alpha \vee \beta$
7. $\beta \rightarrow \alpha \vee \beta$
8. $(\alpha \rightarrow \gamma) \rightarrow (\beta \rightarrow \gamma) \rightarrow \alpha \vee \beta \rightarrow \gamma$
9. $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \neg\beta) \rightarrow \neg\alpha$
10. $\neg\neg\alpha \rightarrow \alpha$

Утверждение 2.1. *$A \rightarrow A$.*

Доказательство.

1. $A \rightarrow A \rightarrow A$
2. $(A \rightarrow A \rightarrow A) \rightarrow (A \rightarrow (A \rightarrow A) \rightarrow A) \rightarrow (A \rightarrow A)$
   $\alpha = A$, $\beta = A \rightarrow A$, $\gamma = A$
3. $(A \rightarrow (A \rightarrow A) \rightarrow A) \rightarrow A \rightarrow A$. Modus Ponens из 1 и 2.
4. $A \rightarrow (A \rightarrow A) \rightarrow A$
   $\alpha = A$, $\beta = A \rightarrow A$
5. $A \rightarrow A$

□

Определение 2.2. *$\vdash \alpha$ — есть доказательство α. $\gamma_1, \gamma_2, \dots \vdash \alpha$ — есть доказательство α из $\gamma_1, \gamma_2, \dots$.*

Теорема 2.1 (Теорема о дедукции)**.** *$\Gamma, \alpha \vdash \beta$ ттт $\Gamma \vdash \alpha \rightarrow \beta$.*

Утверждение 2.2. *$\vdash \alpha$ ттт $\vDash \alpha$.*

Утверждение 2.3. *Если из* $\vDash \alpha$ *следует* $\vdash \alpha$*, то оценка полна. Если из* $\vdash \alpha$ *следует* $\vDash \alpha$*, то оценка корректна.*

Доказательство. Доказательство корректности:

Индукция по длине доказательства $\Gamma \vdash \alpha$.
Если α — гипотеза, то очевидно, что следует $\Gamma \vDash \alpha$.
Если α — аксиома, то нужно проверить все аксиомы. На примере 9 аксиомы:

$(\alpha \to \beta) \to (\alpha \to \neg\beta) \to \neg\alpha$
Если $[\![\alpha]\!] = \text{False}$, то True, тк в конце $\neg\alpha$.
Если $[\![\alpha]\!] = \text{True}$, то либо первая либо вторая скобка — False.

Переход:

Аксиома — понятно, тк она аксиома. Гипотеза — тоже понятно, тк доказана по ИП. Modus Ponens — понятно, тк то, из чего он получен — истино.

Доказательство полноты:

Используем: $A \vee \neg A$, $(\alpha \to \beta) \to (\neg\alpha \to \beta) \to \beta$, и если $\Gamma, \alpha \vdash \beta$ и $\Gamma, \neg\alpha \vdash \beta$, то $\Gamma \vdash \beta$
fix f: $x_1 := \text{True}, x_2 := \text{False}, x_3 := \text{False}, \dots$
$x_1, x_2, x_3, \dots \vdash \alpha$

$$\begin{cases} x_1, x_2, \dots, x_n \vdash \alpha \\ x_1, x_2, \dots, \neg x_n \vdash \alpha \\ \vdots \end{cases}$$

$(\!|\, \gamma \,|\!) = \begin{cases} \gamma & [\![\gamma]\!] = \text{True} \\ \neg\gamma & [\![\gamma]\!] = \text{False} \end{cases}$ Это надо, чтобы либо утверждение, либо его отрицание точно были доказуемые.

$\square$

Внимание! Какие-то челики поменяли 10 аксиому на эту: $\alpha \to \neg\alpha \to \beta$.
Новая оценка: $]X \subset \mathbb{R}$. X — открыто, если $\forall x \in X \exists r > 0 : (x - r; x + r) \subset X$. $IntX = \{x \in X | \exists r > 0 (x - r; x + r) \subset X\}$
$[\![\alpha \wedge \beta]\!] = [\![\alpha]\!] \cap [\![\beta]\!]$
$[\![\alpha \vee \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$
$[\![\alpha \to \beta]\!] = Int(\mathbb{R} \setminus [\![\alpha]\!] \cup [\![\beta]\!])$
$[\![\neg\alpha]\!] = Int(\mathbb{R} \setminus [\![\alpha]\!])$

2.2 Интуиционистское исчисление высказываний. Естественный вывод.

Правила вывода:

1. $\dfrac{}{\Gamma, \alpha \vdash \alpha}$

2. $\dfrac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \to \beta}$

3. $\dfrac{\Gamma \vdash \alpha \to \beta \quad \Gamma \vdash \alpha}{\Gamma \vdash \beta}$

4. $\dfrac{\Gamma \vdash \alpha \quad \Gamma \vdash \beta}{\Gamma \vdash \alpha \wedge \beta}$

5. $\dfrac{\Gamma \vdash \alpha \wedge \beta}{\Gamma \vdash \alpha}$

6. $\dfrac{\Gamma \vdash \alpha \wedge \beta}{\Gamma \vdash \beta}$

7. $\dfrac{\Gamma \vdash \alpha \to \gamma \quad \Gamma \vdash \beta \to \gamma \quad \Gamma \vdash \alpha \vee \beta}{\Gamma \vdash \gamma}$

8. $\dfrac{\Gamma \vdash \alpha}{\Gamma \vdash \alpha \vee \beta}$

9. $\dfrac{\Gamma \vdash \beta}{\Gamma \vdash \alpha \vee \beta}$

10. $\dfrac{\Gamma \vdash \perp}{\Gamma \vdash \alpha}$ в ИИВ; $\dfrac{\Gamma, \alpha \to \perp \vdash \perp}{\Gamma \vdash \alpha}$ в КИВ

2.3 Исчисление предикатов.

Логические переменные — пропозициональные. Численные — предметные.
Квантор — $\forall a.$; функция — $f(a)$; предикат — принимает не логическое выражение, возвращает логическое.
Если φ — функциональный символ, нужно $F\varphi : D^n \to D$.
Если p — предикатный символ, нужно $Tp : D^n \to \{\text{True}, \text{False}\}$.
Если x — переменная, то $E(x) \in D$.
$[\![p(\theta_1, \ldots, \theta_n)]\!] = Tp([\![\theta_1]\!], \ldots, [\![\theta_n]\!])$
$[\![\varphi(\theta_1, \ldots, \theta_n)]\!] = F\varphi([\![\theta_1]\!], \ldots, [\![\theta_n]\!])$
$[\![\forall x.\alpha]\!] = \text{True}$, если для всех $d \in D : E(x) = d$, то $[\![\alpha]\!] = \text{True}$.
$\alpha[x := \theta]$ — заменяет все свободные x на θ.

Определение 2.3. *θ называется свободным для подстановки в α вместо x, если $\alpha[x := \theta]$ не сделает свободные вхождения в θ связанными.*

1. $x \notin FV(\Gamma) \mid \dfrac{\Gamma \vdash \alpha}{\Gamma \vdash \forall x.\alpha}$

2. Нужна свобода для подстановки $\mid \dfrac{\Gamma \vdash \forall x.\alpha}{\Gamma \vdash \alpha[x := \theta]}$

3. Нужна свобода для подстановки $\mid \dfrac{\Gamma \vdash \alpha[x := \theta]}{\Gamma \vdash \exists x.\alpha}$

4. $x \notin FV(\Gamma, \beta) \mid \dfrac{\Gamma \vdash \exists x.\alpha \quad \Gamma, \alpha \vdash \beta}{\Gamma \vdash \beta}$

Теорема 2.2. *Если $\Gamma \vdash \alpha$ в классическом исчислении предикатов, то $\Gamma \vDash \alpha$ в двоичной оценки для предикатов.*

Доказательство. Индукция по длине доказательства.
База.

$$\overline{\Gamma, \alpha \vdash \alpha} \text{ очевидно } \Gamma, \alpha \vDash \alpha$$

Переход.

$\dfrac{\Gamma \vdash \alpha \wedge \beta}{\Gamma \vdash \alpha}$. Есть $\Gamma \models \alpha \wedge \beta$, надо $\Gamma \models \alpha$.
$\dfrac{\Gamma, \alpha \to \perp \vdash \perp}{\Gamma \vdash \alpha}$. Есть $\Gamma, \alpha \to \perp \models \perp$, надо $\Gamma \models \alpha$.

□

2.4 λ — исчисления.

Опр. λ — исчисления — способ описать математику в программировании.
Тезис 1. Функции больше одного агрумента не нужны.
Опр. $\lambda x.P$ — принимает x и делает P.
Опр. $FV(\alpha)$ — множество свободных переменных α.
Опр. θ называется свободным для подстановки в α вместо x, если $\alpha[x := \theta]$ не сделает свободные вхождения в θ связанными.
Опр. $P =_\alpha Q$, если одно из следующего:

- P и Q — одна и та же формула
- $P = A_1B_1$, $Q = A_2B_2$; $A_1 =_\alpha A_2$ и $B_1 =_\alpha B_2$
- $P = \lambda x.A_1$, $Q = \lambda y.A_2$; $A_1[x := t] =_\alpha A_2[y := t]$

С этого момента любое $=$ — это $=_\alpha$.
Опр. $(\lambda x.P)Q$ — β — редекс. $A \to_\beta B$, если:

- $A = (\lambda x.P)Q$, $B = P[x := Q]$, есть свобода
- $A = P_1Q_1$, $B = P_2Q_2$; ($P_1 = P_2$ и $Q_1 \to_\beta Q_2$) или ($Q_1 = Q_2$ и $P_1 \to_\beta P_2$)
- $A = \lambda x.P_1$, $B = \lambda x.P_2$; $P_1 \to_\beta P_2$

Опр. $\omega = (\lambda y.yy)(\lambda x.xx)$
Опр. $A \twoheadrightarrow_\beta B$ за несколь (в том числе 0) шагов.
Опр. Нормальный порядок — редуцируем самый левый β — редекс. Аппликативный порядок — из самых вложенных берем левый β — редекс.
Опр. $A \rightrightarrows_\beta B$, если:

- $A = B$
- $A = \lambda x.P_1$, $B = \lambda x.P_2$; $P_1 \rightrightarrows_\beta P_2$
- $A = P_1Q_2$, $B = P_2Q_2$; $P_1 \rightrightarrows_\beta P_2$ и $Q_1 \rightrightarrows_\beta Q_2$
- $A = (\lambda x.P_1)Q_1$, $B = P_2[x := Q_2]$; $P_1 \rightrightarrows_\beta P_2$ и $Q_1 \rightrightarrows_\beta Q_2$

Теорема Черча — Россера. Если $A \twoheadrightarrow_\beta B$, $A \twoheadrightarrow_\beta C$ и $B \neq C$, то существует D, такое что $B \twoheadrightarrow_\beta D$ и $C \twoheadrightarrow_\beta D$.
Доказательство:

Лемма. Если $P_1 \rightrightarrows_\beta P_2$ и $Q_1 \rightrightarrows_\beta Q_2$, то $P_1[x := Q_1] \rightrightarrows_\beta P_2[x := Q_2]$ — свобода есть.

- Случай $P_1 = P_2$ — ясно.
- Индукция по длине P_1.

- $P_1 = A_1B_1$
  $P_2 = A_2B_2$
  $A_1 \rightrightarrows_\beta A_2$
  $B_1 \rightrightarrows_\beta B_2$
  $A_1[x := Q_1] \rightrightarrows_\beta A_2[x := Q_2]$
  $B_1[x := Q_1] \rightrightarrows_\beta B_2[x := Q_2]$
  $P_1[x := Q_1] = (A_1[x := Q_1])(B_1[x := Q_1])$
  $P_2[x := Q_2] = (A_2[x := Q_2])(B_2[x := Q_2])$
  $P_1[x := Q_1] \rightrightarrows_\beta P_2[x := Q_2]$
- $P_1 = \lambda y.A_1$
  $P_2 = \lambda y.A_2$
  $A_1 \rightrightarrows_\beta A_2$
  $A_1[x := Q_1] \rightrightarrows_\beta A_2[x := Q_2]$
  $P_1[x := Q_1] = \lambda y.(A_1[x := Q_1])$
  $P_2[x := Q_2] = \lambda y.(A_2[x := Q_2])$
  $P_1[x := Q_1] \rightrightarrows_\beta P_2[x := Q_2]$
- $P_1 = (\lambda y.A_1)B_1$
  $P_2 = A_2[y := B_2]$
  $A_1 \rightrightarrows_\beta A_2$
  $B_1 \rightrightarrows_\beta B_2$
  $A_1[x := Q_1] \rightrightarrows_\beta A_2[x := Q_2]$
  $B_1[x := Q_1] \rightrightarrows_\beta B_2[x := Q_2]$
  $(\lambda y.A_1[x := Q_1])(B_1[x := Q_1]) \rightrightarrows_\beta ? A_2[y := B_2][x := Q_2]$
  $y \in ? FV(Q_2)$, если да, то $y \in FV(Q_1)$
  $y \in FV(A_1)$ — иначе ясно.
  $y \notin FV(Q_2)$
  $A_2[y := B_2][x := Q_2] = A[x := Q_2][y := B_2[x := Q_2]]$
  $y = x$ аналогично

Лемма. Если $P \rightrightarrows_\beta P_1$, $P \rightrightarrows_\beta P_2$ и $P_1 \neq P_2$, то существует P_3, такое что $P_1 \rightrightarrows_\beta P_3$ и $P_2 \rightrightarrows_\beta P_3$.

Индукция по элементам P.

- $P = P_1$ — $P_3 = P_2$
- $P = \lambda x.A$, $P_1 = \lambda x.A_1 \Rightarrow P_2 = \lambda x.A_2$. $P_3 = \lambda x.A_3$. $A \rightrightarrows_\beta A_1$, $A \rightrightarrows_\beta A_2$, $A_1 \rightrightarrows_\beta A_3$, $A_2 \rightrightarrows_\beta A_3$
- $P = AB$, $P_1 = A_1B_1$
  (I) $P_2 = A_2B_2$
  $A \rightrightarrows_\beta A_1$, $A \rightrightarrows_\beta A_2$; $B \rightrightarrows_\beta B_1$, $B \rightrightarrows_\beta B_2$.
  $\exists A_3, B_3; P_3 = A_3B_3$
  (II) $P = (\lambda x.C)B$, $P_2 = C_2[x := B_2]$, $P_1(\lambda x.C_1)B_1$
  $A \rightrightarrows_\beta A_1$ — тогда $A_1 = \lambda x.C_1$
  $B \rightrightarrows_\beta B_1$, $B \rightrightarrows_\beta B_2$; $C \rightrightarrows_\beta C_1$, $C \rightrightarrows_\beta C_2$
  C_3, B_3: $C_1 \rightrightarrows_\beta C_3$, $C_2 \rightrightarrows_\beta C_3$; $B_1 \rightrightarrows_\beta B_3$, $B_2 \rightrightarrows_\beta B_3$. $P_3 = C_3[x := B_3]$
- $P = (\lambda x.C)B$, $P_1 = C_1[x := B_1]$
  (I) $P_2 = A_2B_2$. (?)$C \rightrightarrows_\beta A_2$, $B \rightrightarrows_\beta B_2$
  $C \rightrightarrows_\beta C_1$, $C \rightrightarrows_\beta C_2$; $B \rightrightarrows_\beta B_1$, $B \rightrightarrows_\beta B_2$
  (II) $P_2 = C_2[x := B_2]$
  $\exists C_3, B_3$: $C_1 \rightrightarrows_\beta C_3$, $C_2 \rightrightarrows_\beta C_3$; $B_1 \rightrightarrows_\beta B_3$, $B_2 \rightrightarrows_\beta B_3$. $P_3 = C_3[x := B_3]$

$P \rightrightarrows_\beta \dots \rightrightarrows_\beta P_1 \rightrightarrows_\beta \dots \rightrightarrows_\beta P_3$, $P \rightrightarrows_\beta \dots \rightrightarrows_\beta P_2 \rightrightarrows_\beta \dots \rightrightarrows_\beta P_3$
Двойной параллельный β — редекс $=\twoheadrightarrow_\beta$

2.5 Просто — типизированное λ — исчисление.

Опр. $\alpha \to \beta$ — тип функции, которая принимает объект типа α и возвращает объект типа β.
Правила вывода:

1. $\overline{\Gamma, x : \alpha \vdash x : \alpha}$, $x \notin \Gamma$
2. $\dfrac{\Gamma \vdash P : \alpha \to \beta \quad \Gamma \vdash Q : \alpha}{\Gamma \vdash PQ : \beta}$
3. $\dfrac{\Gamma, x : \alpha \vdash P : \beta}{\Gamma \vdash \lambda x.P : \alpha \to \beta}$, $x \notin \Gamma$ — по Карри.
$\dfrac{\Gamma, x : \alpha \vdash P : \beta}{\Gamma \vdash \lambda x^\alpha.P : \alpha \to \beta}$ — по Черчу.

Теорема о редукции. Если $A \twoheadrightarrow_\beta B$ и $\vdash A : \sigma$, то $\vdash B : \sigma$.
Теорема об ограниченном свойстве распространения типизации. Если $A \twoheadrightarrow_\beta B$, $\vdash A : \sigma$ и $\vdash B : \tau$, то $\tau = \sigma$. Верно только в Черче.
Утв. Полное свойство распространения типизации. $A \twoheadrightarrow_\beta B$ и $\vdash B : \sigma$, то $A : \sigma$. Неверно нигде.
Теорема о равносильности исчисления по Карри и по Черчу.

- $\Gamma \vdash P : \alpha$ — Черч, стираем аннотацию и получаем доказуемое в Карри.
- $\Gamma \vdash P : \alpha$ — Карри, то есть способ приписать типовые аннотации и получить доказуемое в Черче.

Теорема. Изоморфизм Карри — Ховард.

2.6 Нормализуемость $\lambda_\to$. Система F.

Опр. Выражение называется сильно нормализуемым, если нет способа редуцировать его бесконечно.
Опр. SN — множество всех сильно нормализуемых выражений. $X \subset SN$ насыщенно, если

- Если $m_1, \dots, m_n \in SN$, то $xm_1m_2 \dots m_n \in X$
- Если $m_1, \dots, m_n \in SN$, $M \in SN$, N — любое и $N[x := M]m_1, \dots, m_n \in X$, то $(\lambda x.N)mm_1, \dots, m_n \in X$

Лемма. SN — насыщенно.
A, B — множество выражений. $A \to B = \{X | \forall Y \in A. XY \in B\}$. Если A, B — насыщенные, то $A \to B$ — насыщенное.
σ — тип. $[\sigma] = \begin{cases} SN & \sigma \text{ — переменная} \\ [\tau_1] \to [\tau_2] & \sigma = \tau_1 \to \tau_2 \end{cases}$
$[\alpha \to \alpha \to \alpha] = SN \to SN \to SN$.
Лемма. $[\sigma]$ — насыщенно из предыдущего.
Опр. ρ из переменных в λ-выражениях — оценка.
Опр. $M[x := \rho(x), y := \rho(xy), ...] = [\![M]\!]^\rho$.
Утв. Для любой ρ такой что для всех $x : \tau \in \Gamma$ верно $\rho(x) \in [\tau]$.
Утв. $\Gamma \vDash M : \sigma$, если выполнено $[\![M]\!]^\rho \in [\sigma]$
Теорема. Если $\Gamma \vdash M : \sigma$, то $\Gamma \vDash M : \sigma$.
Доказательство:

Индукция по размеру дерева вывода $\Gamma \vdash M : \sigma$

Опр. Λ — принимает типовую переменную.
Новые правила вывода:

- $\dfrac{\Gamma \vdash P : \alpha}{\Gamma \vdash \Lambda x.P : \forall x.\alpha,\ x \notin FV(\Gamma)}$
- $\dfrac{\Gamma \vdash P : \forall x.\alpha}{\Gamma \vdash P\beta : \alpha[x := \beta]}$ — есть свобода.

2.7 Экзистенциальные типы. Система HM.

Опр. $\exists p.p \wedge (\nu \wedge p \to p) \wedge (p \to \nu \wedge p)$, ν — тип натурального числа. Это стек из программирования (обозначим σ). После квантора существования — набор методов стека.
$\dfrac{\Gamma \vdash : \sigma[p := \alpha]}{\Gamma \vdash ??N?? : \exists p.\sigma}$
$\dfrac{\Gamma \vdash N : \exists p.\sigma \quad \Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash ??N, M?? : \tau}$
$rank \sigma = \begin{cases} 1 & \sigma \text{ без кванторов} \\ \max(rank \tau, 1) & \sigma = \forall x.\tau \\ \max((rank \tau_1) + 1, rank \tau_2) & \sigma = \tau_1 \to \tau_2 \end{cases}$
Опр. Тип в HM — тип в просто-типизированном λ-исчислении. Типовая схема в HM — тип с поверхностными кванторами в просто-типизированном λ-исчислении. Далее в этой теме: σ — схемы, τ — типы.
Правила вывода в системе HM:

- $\dfrac{}{\Gamma, x : \sigma \vdash x : \sigma}$
- $\dfrac{\Gamma, x : \tau_1 \vdash P : \tau_2}{\Gamma \vdash \lambda x.P : \tau_1 \to \tau_2,\ x \notin \Gamma}$
- $\dfrac{\Gamma \vdash P : \tau_1 \quad \Gamma \vdash Q : \tau_1 \to \tau_2}{\Gamma \vdash PQ : \tau_2}$
- $\dfrac{\Gamma \vdash P : \sigma \quad \Gamma, x : \sigma \vdash Q : \tau}{\Gamma \vdash \text{let } x := P \text{ in } Q : \tau}, x \notin \Gamma$
- $\dfrac{\Gamma \vdash P : \sigma_1}{\Gamma \vdash P : \sigma_2,\ \sigma_1 \sqsubseteq \sigma_2}$
- $\dfrac{\Gamma \vdash P : \sigma}{\Gamma \vdash P : \forall \alpha.\sigma,\ \alpha \notin FV(\Gamma)}$

Правила вывода эквирекурсивных типов:

- $\dfrac{\Gamma \vdash P : \mu\alpha.\tau}{\Gamma \vdash P : \tau[\alpha := \mu\alpha.\tau]}$
- $\dfrac{\Gamma \vdash P : \tau[\alpha := \mu\alpha.\tau]}{\Gamma \vdash P : \mu\alpha.\tau}$

Правила вывода изорекурсивных типов:

- $\dfrac{\Gamma \vdash \mu\alpha.\tau}{\Gamma \vdash \text{unroll } P : \tau[\alpha := \mu\alpha.\tau]}$
- $\dfrac{\Gamma \vdash P : \tau[\alpha := \mu\alpha.\tau]}{\Gamma \vdash \text{roll } P : \mu\alpha.\tau}$

2.8 Обобщенная система типов.

Опр. int — тип, $\bigstar$ — род, $\bigstar \to \bigstar$ — род, $\square$ — сорт.
Правила вывода:

- $\dfrac{}{\vdash \bigstar : \square}$
- $\dfrac{\Gamma \vdash \alpha : \sigma}{\Gamma, x : \alpha \vdash x : \alpha}, x \notin \Gamma$
- $\dfrac{\Gamma \vdash F : \Pi x^{\alpha}.\beta \quad \Gamma \vdash \sigma : \alpha}{\Gamma \vdash FG : \beta[x := \sigma]}$
- $\dfrac{\Gamma \vdash A : \alpha \quad \Gamma \vdash \alpha' : \sigma}{\Gamma \vdash A : \alpha'}, \alpha =_{\beta} \alpha'$
- $\dfrac{\Gamma \vdash A : \beta \quad \Gamma \vdash \alpha : \sigma}{\Gamma, x : \alpha \vdash A : \beta}, x \notin \Gamma$
- $\dfrac{\Gamma \vdash \alpha : \sigma_1 \quad \Gamma, x : \alpha \vdash P : \beta \quad \Gamma, x : \alpha \vdash \beta : \sigma_2}{\Gamma \vdash \lambda x^{\alpha}.P : \Pi x^{\alpha}.\beta}, \sigma_1, \sigma_2 \in S \subset \{\langle \bigstar, \square \rangle, \langle \bigstar, \bigstar \rangle, \langle \square, \square \rangle, \langle \square, \bigstar \rangle\}$
- $\dfrac{\Gamma \vdash \alpha : \sigma_1 \quad \Gamma, x : \alpha \vdash \beta : \sigma_2}{\Gamma \vdash \Pi x^{\alpha}.\beta : \sigma_2}, \sigma_1, \sigma_2 \in S \subset \{\langle \bigstar, \square \rangle, \langle \bigstar, \bigstar \rangle, \langle \square, \square \rangle, \langle \square, \bigstar \rangle\}$

2.9 Гомотопическая теория типов.

2.10 Иерархия универсумов. $\backslash Prop$ и $\backslash Set$.