1.1 Теорема об однозначном представлении булевой функции многочленом Жегалкина.

Теорема (Жегалкина): Каждая булева функция единственным образом представляется в виде полинома Жегалкина.

▲ Заметим, что различных булевых функций от n переменных 2^{2^n} штук. При этом конъюнкций вида $x_{i_1} \dots x_{i_k}$ существует ровно 2^n, так как из n возможных сомножителей каждый или входит в конъюнкцию, или нет. В полиноме у каждой такой конъюнкции стоит 0 или 1, то есть существует 2^{2^n} различных полиномов Жегалкина от n переменных.
Теперь достаточно лишь доказать, что различные полиномы реализуют различные функции. Предположим противное.
Тогда приравняв два различных полинома и перенеся один из них в другую часть равенства, получим полином, тождественно равный нулю и имеющий ненулевые коэффициенты. Тогда рассмотрим слагаемое с единичным коэффициентом наименьшей длины, то есть с наименьшим числом переменных, входящих в него (любой один, если таких несколько). Подставив единицы на места этих переменных и нули на места остальных, получим, что на этом наборе только одно это слагаемое принимает единичное значение, то есть нулевая функция на одном из наборов принимает значение 1. Противоречие. Значит, каждая булева функция реализуется полиномом Жегалкина единственным образом. ■

1.2 Теорема о дедукции для исчисления высказываний.

Теорема о дедукции: Пусть Γ, A – это $\Gamma \cup \{A\}$, тогда верно:

$$\frac{\Gamma \vdash A \to B}{\Gamma, A \vdash B} \Updownarrow$$

▲ ($\Downarrow$) Пусть $\Gamma \vdash A \to B$, тогда $\Gamma, A \vdash A,\ A \to B$. К выводу применим MP: $A,\ A \to B \vdash B$. Тогда по транзитивности $\Gamma, A \vdash B$.
($\Uparrow$) Доказывается индукцией по длине вывода B из Γ, A

(1) Если этот вывод – длины 1, то B – аксиома или гипотеза (т.е. формула из Γ).
Если B – аксиома, то имеем вывод $A \to B$ (из $\varnothing$):

1. B	(аксиома)
2. $B \to (A \to B)$	(аксиома A1)
3. $A \to B$	(1,2, MP)

(2) Если $B \in \Gamma$, то имеем такой же вывод $A \to B$ из Γ:

1. B	(гипотеза)
2. $B \to (A \to B)$	(аксиома A1)
3. $A \to B$	(1,2, MP)

(3) Если $B = A$, то $A \to B = A \to A$. Но $\vdash A \to A$ (пример из определений в пункте 6).

(4) Предположим теперь, что Γ, $A \vdash B$ и утверждение ($\Uparrow$) верно для всех более коротких выводов, т.е.
для всех C, если $\Gamma, A \vdash C$ и вывод C из Γ, A короче, чем вывод B, то $\Gamma \vdash A \to C$.
Докажем, что $\Gamma \vdash A \to B$:
Рассмотрим вывод из Γ, A, который заканчивается формулой B. При этом B может оказаться аксиомой или гипотезой (тогда все предыдущие формулы для доказательства B не нужны). Но в этом случае $\vdash A \to B$ по (1)–(3).

Остается случай, когда B получается по MP из формул $C, C \to B$, причем $\Gamma,\ A \vdash C$ и $\Gamma,\ A \vdash C \to B$ с более короткими доказательствами. По предположению индукции имеем:

(*) $\Gamma \vdash A \to C,\ A \to (C \to B)$.

С другой стороны,

(**) $A \to C,\ A \to (C \to B) \vdash A \to B$:

1. $A \to C$	(гипотеза)
2. $A \to (C \to B)$	(гипотеза)
3. $(A \to (C \to B)) \to ((A \to C) \to (A \to B))$	(аксиома A2)
4. $(A \to C) \to (A \to B)$	(2,3, MP)
5. $A \to B$	(1,4, MP)

Из (*), (**) по транзитивности получаем $\Gamma \vdash A \to B$. ■

1.3 Теорема о полноте исчисления высказываний.

Теорема 10. *Справедливы следующие правила вывода (каждый раз сверху от горизонтальной черты записаны условия теоремы, а снизу — утверждение):*

1) *Правило вывода конъюнкции:* $\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$;

2) *Правило сечения:* $\dfrac{\Gamma \vdash A \quad \Gamma, A \vdash B}{\Gamma \vdash B}$. *В общем виде:*

$$\frac{\Gamma \vdash A_1 \quad \ldots \quad \Gamma \vdash A_k \quad \Gamma, A_1, \ldots, A_k \vdash B}{\Gamma \vdash B};$$

3) *Правило разбиения конъюнкции:* $\dfrac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}$;

4) *Правило разбора случаев:* $\dfrac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$;

5) *Правило исчерпывающего разбора случаев:* $\dfrac{\Gamma, A \vdash C \quad \Gamma, \neg A \vdash C}{\Gamma \vdash C}$;

6) *Правило рассуждения от противного:* $\dfrac{\Gamma, A \vdash B \quad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$;

Доказательство. 1) Напишем подряд выводы A и B, затем пятую аксиому $A \to (B \to (A \wedge B))$. Теперь двумя применениями modus ponens выводится $A \wedge B$.

2) Достаточно написать все выводы подряд. Тогда в последнем выводе формулы A_i будут использоваться не как посылки, а как уже выведенные формулы.

3) Достаточно в начало вывода дописать цепочку формул $A \wedge B;\ (A \wedge B) \to A;\ (A \wedge B) \to B;\ A;\ B$.

4) По теореме о дедукции из $\Gamma, A \vdash C$ следует $\Gamma \vdash A \to C$, а из $\Gamma, B \vdash C$ следует $\Gamma \vdash B \to C$. Далее добавляем восьмую аксиому: $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$ — и после двух применений modus ponens получаем $\Gamma \vdash (A \vee B) \to C$. Применив лемму о дедукции в обратную сторону, получаем $\Gamma, A \vee B \vdash C$, что и требовалось.

5) Аналогично предыдущему, получаем $\Gamma, A \vee \neg A \vdash C$. Но $A \vee \neg A$ является аксиомой, поэтому её можно исключить из посылок. Действительно, та же самая цепочка формул будет выводом не только из $\Gamma \cup \{A \vee \neg A\}$, но и из Γ. Отметим, что тут можно сослаться и на правило сечения, ведь $\Gamma \vdash A \vee \neg A$.

6) Аналогично правилу разбора случаев имеем $\Gamma \vdash A \to B$ и $\Gamma \vdash A \to \neg B$. После добавления десятой аксиомы: $(A \to B) \to ((A \to \neg B) \to \neg A)$ — и двойного применения modus ponens получаем $\Gamma \vdash \neg A$, что и требовалось.

□

Утверждение 14. *Выводим закон добавления двойного отрицания:* $\vdash A \to \neg\neg A$.

Доказательство. По теореме о дедукции достаточно доказать $A \vdash \neg\neg A$, а для этого по правилу рассуждения от противного достаточно доказать, что из A и $\neg A$ выводятся две противоречивые формулы. Но это очевидно: сами A и $\neg A$ и будут такими формулами.

□

Для доказательства теоремы о полноте понадобятся две вспомогательные леммы.

Базовая лемма: Представление таблицы истинности для данных четырех связок.

Для дизъюнкции:	Для конъюнкции:	Для импликации:	Для отрицания:
$A, B \vdash A \vee B$	$A, B \vdash A \wedge B$	$A, B \vdash A \to B$	$A \vdash \neg(\neg A)$
$\neg A, B \vdash A \vee B$	$\neg A, B \vdash \neg(A \wedge B)$	$\neg A, B \vdash A \to B$	$\neg A \vdash \neg A$
$A, \neg B \vdash A \vee B$	$A, \neg B \vdash \neg(A \wedge B)$	$A, \neg B \vdash \neg(A \to B)$	
$\neg A, \neg B \vdash \neg(A \vee B)$	$\neg A, \neg B \vdash \neg(A \wedge B)$	$\neg A, \neg B \vdash A \to B$	

1. Первые три выводимости про дизъюнкцию следуют из A_6 и A_7 по лемме о дедукции (D). Последняя:

$$\dfrac{\dfrac{\dfrac{A_9}{\vdash \neg A \to (A \to B)}}{\neg A, \neg B, A \vdash B}\,(DD) \qquad \neg A, \neg B, \textcircled{B} \vdash \textcircled{B}}{\neg A, \neg B, A \vee B \vdash B}\,\text{(разбор случаев)} \qquad \neg A, \textcircled{\neg B}, A \vee B \vdash \textcircled{\neg B}$$

$$\neg A, \neg B \vdash \neg(A \vee B)\,\text{(от противного)}$$

2. Первая выводимость про конъюнкцию следует из A_5 по D, остальные получаются контрапозицией из A_3 и A_4:

$$\dfrac{\dfrac{A \to B, \neg B, A \vdash B \qquad A \to B, \neg B, A \vdash \neg B}{A \to B, \neg B \vdash \neg A}\,\text{(от противного)}}{\vdash (A \to B) \to (\neg B \to \neg A)}\,(DD)$$

В частности, подставим A_3 и получим

$$((A \wedge B) \to A) \to (\neg A \to \neg(A \wedge B))$$

тк аксиома, то верно $\vdash \neg A \to \neg(A \wedge B)$ т.е. $\neg A \vdash \neg(A \wedge B)$

3. Первая, третья и четвертая выводимость про импликацию следуют из A_1 и A_9 по D. Вторая выводится так:

$$\frac{A, \neg B, A \to B \vdash B \qquad A, \neg B, A \to B \vdash \neg B}{A, \neg B \vdash \neg(A \to B)} \text{ (от противного)}$$

4. Первая выводимость про отрицание доказана в утверждении 14, вторая тривиальна.

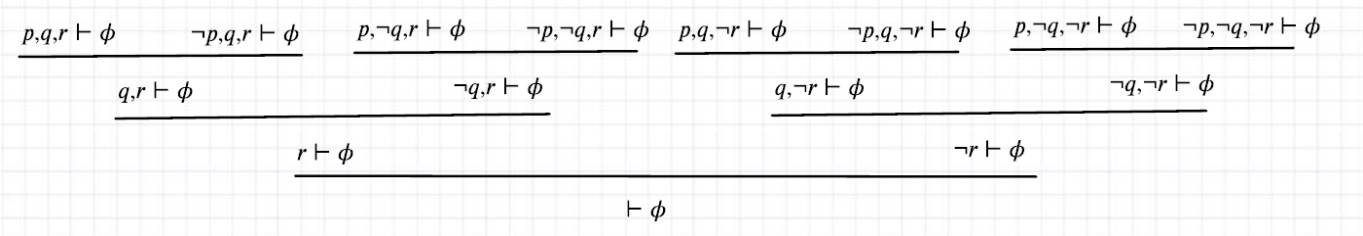
Основная лемма: Пусть $\phi(a_1, \ldots, a_n) = a$. Тогда верно следующее:

$$p_1^{a_1}, p_2^{a_2}, \ldots, p_n^{a_n} \vdash \phi^a, \qquad \text{где } p^a = \begin{cases} p, a = 1 \\ \neg p, a = 0 \end{cases}$$

▲ Доказательство будет вестись индукцией по построению формулы с использованием базовой леммы в качестве базы и в переходе.
База индекции: ϕ содержит одну связку. Тогда это утверждение сводится к базовой лемме.
Переход: пусть $\phi = \psi \wedge \gamma$. Тогда можно записать: $\phi(a_1, \ldots, a_n) = \psi(a_1, \ldots, a_n) \wedge \gamma(a_1, \ldots, a_n)$
Пусть $\psi(a_1, \ldots, a_n) = \alpha$, $\gamma(a_1, \ldots, a_n) = \beta$
Применим предположение индукции: $p_1^{a_1}, \ldots, p_n^{a_n} \vdash \psi^\alpha$, $p_1^{a_1}, \ldots, p_n^{a_n} \vdash \gamma^\beta$
Воспользуемся базовой леммой: $\psi^\alpha, \gamma^\beta \vdash (\psi \wedge \gamma)^{(\alpha \wedge \beta)} = \phi^a$
Записав все выводы подряд, получаем: $p_1^{a_1}, p_2^{a_2}, \ldots, p_n^{a_n} \vdash \phi^a$
Аналогичные действия проделаем и для других связок. Имеются база и переход, значит, по индукции докажем лемму для всех формул. ■

Пример: $\phi = \neg p \wedge (q \vee r)$; $\phi(0,1,0) = 1$; $\phi(1,0,0) = 1$
Лемма утверждает следующее: $\neg p, q, \neg r \vdash \phi$; $p, \neg q, \neg r \vdash \neg\phi$

Теорема о полноте ИВ: Если формула ϕ является тавтологией, то тогда ϕ – выводима.
▲ Пусть ϕ – тавтология. Тогда $\forall a_1 \ldots a_n \quad \phi(a_1, \ldots, a_n) = 1$. Значит, по основной лемме $p_1^{a_1}, p_2^{a_2}, \ldots, p_n^{a_n} \vdash \phi$ при $\forall a_1 \ldots a_n$. Далее воспользуемся правилом исчерпывающего разбора случаев, а также закон исключенного третьего:



Такое рассуждение можно провести не только для трех литералов, но и для любого количества. Значит, теорема о полноте доказана. ■