1 Эквивалентность формул

Определение 1. *Булевы формулы Φ и Ψ называются* эквивалентными*, если соответствующие им функции f_Φ и f_Ψ равны.*

Обозначение: $\Phi \equiv \Psi$.

1.1 Основные эквивалентности (тождества)

Пусть $\circ$ - это одна из функций $\wedge, \vee, +$. Для этих трех функций выполнены следующие две эквивалентности (законы ассоциативности и коммутативности).
(1) Ассоциативность:

$$((X_1 \circ X_2) \circ X_3) \equiv (X_1 \circ (X_2 \circ X_3))$$

(2) Коммутативность:

$$(X_1 \circ X_2) \equiv (X_2 \circ X_1))$$

(3) Дистрибутивные законы:

$$((X_1 \vee X_2) \wedge X_3) \equiv ((X_1 \wedge X_3) \vee (X_2 \wedge X_3))$$

$$((X_1 \wedge X_2) \vee X_3) \equiv ((X_1 \vee X_3) \wedge (X_2 \vee X_3))$$

$$((X_1 + X_2) \wedge X_3) \equiv ((X_1 \wedge X_3) + (X_2 \wedge X_3))$$

(4) Двойное отрицание:

$$\neg(\neg X) \equiv X$$

(5)Законы де Моргана (внесение отрицания внутрь скобок):

$$\neg(X_1 \vee X_2) \equiv (\neg X_1 \wedge \neg X_2)$$

$$\neg(X_1 \wedge X_2) \equiv (\neg X_1 \vee \neg X_2)$$

(6) Повторения переменной, константы:

$$(X \wedge X) \equiv X \qquad (X \vee X) \equiv X$$

$$(X \wedge \neg X) \equiv 0 \qquad (X \vee \neg X) \equiv 1$$

$$(X \wedge 0) \equiv 0 \qquad (X \vee 0) \equiv X$$

$$(X \wedge 1) \equiv X \qquad (X \vee 1) \equiv 1$$

Следующие две эквивалентности позволяют выразить импликацию и сложение по модулю 2 через дизъюнкцию, конъюкцию и отрицание.
(7) $(X_1 \to X_2) \equiv (\neg X_1 \vee X_2)$
(8) $(X_1 + X_2) \equiv ((X_1 \wedge \neg X_2) \vee (\neg X_1 \wedge X_2))$

Задача 1. *Проверьте все вышеприведенные эквивалентности, непосредственно вычисляя функции для левых и правых частей.*

1.2 Эквивалентные преобразования формул

Соглашения об упрощенной записи формул.
1. Законы ассоциативности показывают, что значения формул, составленных из переменных и операций конъюнкции, не зависят от расстановки скобок. Поэтому вместо формул $(X_1 \wedge X_2) \wedge X_3)$ и $(X_1 \wedge (X_2 \wedge X_3))$ мы будем для упрощения писать выражение $(X_1 \wedge X_2 \wedge X_3)$, которое не является формулой, но может быть превращено в нее с помощью расстановки скобок. Аналогично, будем использовать выражения $(X_1 \vee X_2 \vee X_3)$ и $(X_1 + X_2 + X_3)$ для сокращения формул, состоящих из дизъюнкций и сложений по модулю 2, соответственно.
2. Как и в обычной арифметике, будем считать, что знак логического умножения $\wedge$ (конъюнкция) связывает свои аргументы сильнее, чем знак логического сложения $\vee$ (дизъюнкция). Поэтому для упрощения записи формул вида $((X \wedge Y) \vee Z)$, будем использовать выражения $X \wedge Y \vee Z$.
3. Если внешней функцией в формуле является одна из функций $\wedge, \vee, +, \to$, то внешние скобки в записи формулы можно опустить.

Таким образом, с использованием этих соглашений формула
$(((X \vee Y) \vee (Z \wedge \neg X)) \to ((Y + Z) + \neg X))$
может быть записана как $(X \vee Y \vee Z \wedge \neg X) \to (Y + Z + \neg X)$.

Из определения эквивалентности формул непосредственно следует
Принцип замены эквивалентных подформул:
пусть формула α является подформулой формулы Φ, формула α' эквивалентна α и формула Φ' получена из Φ посредством замены некоторого вхождения α на α'. Тогда Φ' эквивалентна Φ, т.е. $\Phi\prime \equiv \Phi$.

Применяя этот принцип и используя основные тождества, можно находить для заданной формулы другие эквивалентные ей формулы. Часто это может приводить к существенному упрощению исходной формулы. Например, если в формуле $((X \wedge 0) \vee Y)$ заменим на основании тождеств (6) подформулу $(X \wedge 0)$ на 0, то получим эквивалентную формулу $(0 \vee Y)$. По закону коммутативности (2) эта формула эквивалентна формуле $(Y \vee 0)$, которая, в свою очередь, по одному из тождеств группы (6) эквивалентна формуле Y. Эту цепочку эквивалентных преобразований можно записать также следующим образом:
$((X \wedge 0) \vee Y) \underset{(6)}{\equiv} (0 \vee Y) \underset{(2)}{\equiv} (Y \vee 0) \underset{(6)}{\equiv} Y.$
В этой цепочке вспомогательные номера под знаками эквивалентности указывают, с помощью какой группы основных тождеств эта эквивалентность получается.

Назовем *логическим произведением* формулу вида $\Phi_1 \wedge \Phi_2 \wedge \ldots \wedge \Phi_n$ (в этом выражении использованы соглашения о сокращении записи!). Ее подформулы $\Phi_i, 1 \leq i \leq n$, , будем называть *сомножителями.* Аналогично, *логической суммой* назовем формулу вида $\Phi_1 \vee \Phi_2 \vee \ldots \vee \Phi_n$. Ее подформулы $\Phi_i, 1 \leq i \leq n$, , будем называть *слагаемыми.*

Задача 2. *Покажите, что из основных тождеств можно вывести следующие правила преобразования логических произведений и сумм.*
C1) Если в логическом произведении один из сомножителей равен 0, то и все произведение равно 0.
C2) Если в логической сумме одно из слагаемых равно 1, то и вся сумма равна 1.
C3) Если в логическом произведении $n \geq 2$ и есть сомножитель, равный 1, то его можно вычеркнуть.
C4) Если в логической сумме $n \geq 2$ и есть слагаемое, равное 0, то его можно вычеркнуть.

Выведем еще несколько важных логических тождеств, позволяющих проводить упрощения сложных формул. Их называют *законы поглощения.*

П1) $X \vee (X \wedge \Phi) \underset{(6)}{\equiv} (X \wedge 1) \vee (X \wedge \Phi) \underset{(3)}{\equiv} X \wedge (1 \vee \Phi) \underset{(2,6)}{\equiv} X \wedge 1 \underset{(6)}{\equiv} X$

П2) $(X \wedge \Phi) \vee (\neg X \wedge \Phi) \underset{(3)}{\equiv} (X \vee \neg X) \wedge \Phi \underset{(6)}{\equiv} 1 \wedge \Phi \underset{(6)}{\equiv} \Phi$

П3) $(X_1 \wedge X_2) \vee (\neg X_1 \wedge X_3) \vee (X_2 \wedge X_3) \underset{(2,6)}{\equiv} (X_1 \wedge X_2) \vee (\neg X_1 \wedge X_3) \vee (X_1 \vee \neg X_1) \wedge (X_2 \wedge X_3)$
$\underset{(3,2)}{\equiv} ((X_1 \wedge X_2) \vee (X_1 \wedge X_2 \wedge X_3)) \vee ((\neg X_1 \wedge X_2) \vee (\neg X_1 \wedge X_2 \wedge X_3)) \underset{(3)}{\equiv} ((X_1 \wedge X_2) \wedge (1 \vee X_3)) \vee$
$((\neg X_1 \wedge X_2) \wedge (1 \vee X_3)) \underset{(6)}{\equiv} ((X_1 \wedge X_2) \wedge 1) \vee ((\neg X_1 \wedge X_2) \wedge 1) \underset{(6)}{\equiv} (X_1 \wedge X_2) \vee (\neg X_1 \wedge X_3)$

Задача 3. *Используя основные тождества, доказать эквивалентность следующих пар формул.*
(a) $\neg(X \vee \neg Y) \wedge (X \to \neg Y)$ *и* $(\neg X \wedge Y)$;
(b) $\neg[(X \wedge \neg Y) \to (\neg X \vee Z)]$ *и* $(X \wedge \neg Y \wedge \neg Z)$;
(c) $(X + Y) \to (X \wedge \neg Y)$ *и* $(\neg X \wedge \neg Y) \vee X$.

2 Дизъюнктивные и конъюнктивные нормальные формы

В этом разделе мы интересуемся представлением произвольной булевой функции посредством формул специального вида, использующих только операции $\wedge, \vee$ и $\neg$.

Пусть $\mathbf{X} = \{X_1, \ldots, X_n\}$ - это множество пропозициональных переменных. Введем для каждого $i = 1, ..., n$ обозначения: $X_i^0 = \neg X_i$ и $X_i^1 = X_i$. Формула $X_{i_1}^{\sigma_1} \wedge X_{i_2}^{\sigma_2} \wedge \ldots \wedge X_{i_k}^{\sigma_k}$ $(X_{i_1}^{\sigma_1} \vee X_{i_2}^{\sigma_2} \vee \ldots \vee X_{i_k}^{\sigma_k})$, в которой $\sigma_{i_j} \in \{0, 1\}$ и все переменные разные, т.е. $X_{i_j} \neq X_{i_r}$ при $j \neq r$, называется *элементарной конъюнкцией (элементарной дизъюнкцией).*

Определение 2. *Формула $\mathcal{D}$ называется* дизъюнктивной нормальной формой (ДНФ), *если она является дизъюнкцией элементарных конъюнкций, т.е. имеет вид $\mathcal{D} = K_1 \vee K_2 \vee \ldots \vee K_r$,* *где каждая формула K_j $(j = 1, ..., r)$ - это элементарная конъюнкция. $\mathcal{D}$ называется совершенной ДНФ, если в каждую из ее конъюнкций K_j входят все n переменных из* $\mathbf{X}$. *Аналогично, формула $\mathcal{C}$ называется* конъюнктивной нормальной формой (КНФ), *если она является конъюнкцией элементарных дизъюнкций, т.е. $\mathcal{C} = D_1 \vee D_2 \vee \ldots \vee D_r$, где каждая формула D_j $(j = 1, ..., r)$ - это элементарная дизъюнкция. Она является совершенной КНФ,если в каждую D_j входят все n переменных из* $\mathbf{X}$.

2.1 Совершенные ДНФ и КНФ

Рассмотрим произвольную булеву функцию $f(X_1, \ldots, X_n)$, зависящую от переменных из $\mathbf{X}$. Обозначим через N_f^+ множество наборов значений переменных, на которых f принимает значение 1, а через N_f^- множество наборов, на которых f принимает значение 0, т.е. $N_f^+ = \{(\sigma_1, \ldots, \sigma_n) \mid f(\sigma_1, \ldots, \sigma_n) = 1\}$ и $N_f^- = \{(\sigma_1, \ldots, \sigma_n) \mid f(\sigma_1, \ldots, \sigma_n) = 0\}$. Определим по этим множествам две формулы:

$$\mathcal{D}_f = \bigvee_{(\sigma_1,\ldots,\sigma_n)\in N_f^+} X_1^{\sigma_1} \wedge X_2^{\sigma_2} \wedge \ldots \wedge X_n^{\sigma_n}$$

и

$$\mathcal{C}_f = \bigwedge_{(\sigma_1,\ldots,\sigma_n)\in N_f^-} (X_1^{\neg\sigma_1} \vee X_2^{\neg\sigma_2} \vee \ldots \vee X_n^{\neg\sigma_n})$$

Теорема 1. *(1) Если функция f не равна тождественно 0, то формула $\mathcal{D}_f$ - это совершенная ДНФ, задающая функцию f.*
(2) Если функция f не равна тождественно 1, то формула $\mathcal{C}_f$ - это совершенная КНФ, задающая функцию f.

Следствие 1.1. *Каждая булева функция может быть задана формулой, содержащей переменные и функции конъюнкции, дизъюнкции и отрицания.*

Приведенные выше формулы для $\mathcal{D}_f$ и $\mathcal{C}_f$ позволяют эффективно строить совершенные ДНФ и КНФ по табличному представлению функции f (Каким образом?). Можно ли получить такие специальные представления по произвольной формуле, задающей f, не выписывая ее полной таблицы? Приводимая ниже процедура позволяет это сделать, используя основные эквивалентности формул.

Процедура *Приведение к совершенной ДНФ*
Вход: формула Φ, включающая функции $\neg, \wedge, \vee, \rightarrow$ и $+$.
(1) Используя эквивалентности (7) и (8), заменить все функции $\rightarrow$ и $+$ на $\neg, \wedge$ и $\vee$.
(2) Используя законы де Моргана (5) и снятие двойного отрицания (4), внести все знаки отрицания внутрь скобок так, чтобы все оставшиеся отрицания находились непосредственно перед переменными.
(3) Получившаяся после шага (2) формула Φ' имеет одну из двух форм: (а) $\Phi' = \Phi_1 \wedge \Phi_2$ или (б) $\Phi' = \Phi_1 \vee \Phi_2$.

Поскольку каждая из формул Φ_1, Φ_2 проще (короче) формулы Φ', то предположим по индукции, что для них уже построены эквивалентные ДНФ $D_1 = K_1^1 \vee K_1^2 \vee \ldots \vee K_1^r$ и $D_2 = K_2^1 \vee K_2^2 \vee \ldots \vee K_2^s$, соответственно.

Тогда в случае (а) имеем:
$\Phi' \equiv (K_1^1 \vee K_1^2 \vee \ldots \vee K_1^r) \wedge (K_2^1 \vee K_2^2 \vee \ldots \vee K_2^s) \underset{(3)}{\equiv} (K_1^1 \wedge K_2^1) \vee \ldots \vee (K_1^i \wedge K_2^j) \vee \ldots (K_1^r \wedge K_2^s)$. Каждый член $(K_1^i \wedge K_2^j)$ этой дизъюнкции представляет собой конъюнкцию переменных и их отрицаний. Применяя эквивалентности групп (1), (2) и (6), можно удалить из него повторения переменных, после чего он превратится в некоторую элементарную конъюнкцию или константу. Проделав такие преобразования со всеми парами $(i, j), i = 1, ..., r; j = 1, ..., s$, и удалив, если потребуется, константы 0, мы получим ДНФ, эквивалентную исходной формуле Φ.
В случае (б) формула $\Phi' \equiv (K_1^1 \vee K_1^2 \vee \ldots \vee K_1^r) \vee (K_2^1 \vee K_2^2 \vee \ldots \vee K_2^s)$ сама уже является ДНФ.
(4) Используя эквивалентности групп (1), (2) и (6) удалить из получившейся после шага (3) формулы повторные вхождения одинаковых конъюнкций.
(5) Пусть после шага (4) получилась ДНФ $\Phi'' = K_1 \vee K_2 \vee \ldots \vee K_m$. Чтобы получить эквивалентную совершенную ДНФ, построим для каждой K_i, $(i = 1, \ldots, m)$ эквивалентную совершенную ДНФ, заменим ею K_i, а затем устраним повторения одинаковых конъюнкций.

Задача 4.
(1) Предложите алгоритм, который по произвольной элементарной конъюнкции строит эквивалентную ей совершенную ДНФ.
(2) Предложите алгоритм, который по произвольной элементарной дизъюнкции строит эквивалентную ей совершенную КНФ.

Отметим, что порядок выполнения преобразований на этапах (1) и (2) процедуры не определен однозначно. Например, на этапе (1) можно сначала устранять $\to$, а затем $+$, или наоборот, или даже чередовать эквивалентности (7) и (8) в произвольном порядке. В любом случае наша процедура должна привести к требуемому результату.

Предложение 1. *На этапе (1) процедуры при любом порядке выполнения преобразований (7), (8) до тех пор, пока ни одно из них не применимо, полученная в результате формула не будет содержать функций $\to$ и $+$.*

Задача 5. *Докажите Предложение 1, используя индукцию по общему количеству функций $\to$ и $+$ в формуле.*

Предложение 2. *На этапе (2) процедуры при любом порядке выполнения преобразований групп (4) и (5) до тех пор, пока ни одно из них не применимо, в полученной в результате формуле все знаки отрицания будут стоять непосредственно перед переменными.*

Перед доказательством этого утверждения введем некоторые обозначения. Определим для каждой формулы Φ, построенной из функций множества F, ее *глубину* $dep(\Phi)$ индукцией по построению формулы.
(а) Если Φ - это символ переменной или константа, то $dep(\Phi) = 0$.
(б) Если $\Phi = f(\Phi_1, \dots, \Phi_n)$, где f - это n-местная функция из F, то

$$dep(\Phi) = \max_{1 \le i \le n} dep(\Phi_i) + 1$$

.

Например, формула $\Phi = ((X+Y) \to ((X \vee \neg Z) \wedge Y)))$, построенная над $F = \{\vee, \wedge, \neg, \to, +\}$, имеет глубину $dep(\Phi) = 4$.

Пусть Φ - это формула над $F = \{\vee, \wedge, \neg\}$. Определим для каждой ее "отрицательной"подформулы вида $\neg(\Psi)$ *высоту* $h(\neg(\Psi))$ как $3^{dep(\Psi)} - 1$. И пусть *высота всей формулы* $H(\Phi)$ равна сумме высот всех ее отрицательных подформул.

Доказательство Предложения 2 проведем индукцией по высоте формул.

Базис индукции. Если $H(\Phi) = 0$, то либо в Φ нет отрицаний, либо все отрицания находятся непосредственно перед переменными. Следовательно, Φ удовлетворяет требованию Предложения 2.

Шаг индукции. Предположим, что при $n \le k$ для всех формул высоты n Предложение 2 выполнено. Пусть Φ - произвольная формула высоты $H(\Phi) = k+1$. Докажем наше утверждение для нее. Поскольку $H(\Phi) \ge 1$, то Φ содержит хотя бы одну отрицательную подформулу $\neg(\Psi)$, у которой $h(\neg(\Psi)) \ge 1$ и, следовательно, $dep(\Psi) \ge 1$. К такой формуле обязательно можно применить либо снятие двойного отрицания (4), либо один из законов де Моргана (5). (*Объясните почему ?*) Пусть $\neg(\Psi)$ - это та подформула Φ, которая на (2)-ом этапе процедуры первой заменяется на эквивалентную формулу Ψ' в соответствии с одной из указанных эквивалентностей. Пусть Φ' - это формула, получившаяся в результате этой замены из Φ. Нетрудно проверить (*проделайте эту проверку!*), что при любом из преобразований (4), (5) $H(\Psi') < H(\neg(\Psi))$ и, следовательно, $H(\Phi') < H(\Phi)$. Тогда, $H(\Phi') \le k$ и по предположению индукции применение эквивалентностей (4), (5) в произвольном порядке приведет в конце концов к формуле, у которой все отрицания будут стоять непосредственно перед переменными. Это означает, что Предложение 2 выполнено при $n = k+1$, что завершает индукционный шаг и все доказательство.

Задача 6. *Как изменить (3)-ий, (4)-ый и (5)-ый этапы процедуры, чтобы в результате получить совершенную КНФ, эквивалентную исходной формуле.*

Рассмотрим применение процедуры приведения к совершенной ДНФ на примере.

Пример 1. *Пусть формула* $\Phi = ((\neg X \vee Z) \to (Y \to (X+Z)))$.

На (1)-ом этапе процедуры получаем следующую цепочку эквивалентностей:
$\Phi \underset{(7)}{\equiv} \neg(\neg X \vee Z) \vee (Y \rightarrow (X + Z)) \underset{(7)}{\equiv} \neg(\neg X \vee Z) \vee (\neg Y \vee (X + Z)) \underset{(8)}{\equiv} \neg(\neg X \vee Z) \vee (\neg Y \vee ((X \wedge \neg Z) \vee (\neg X \wedge Z)))$.
На (2)-ом этапе вносим отрицание внутрь первой скобки и получаем формулу
$\Phi' = (\neg\neg X \wedge \neg Z) \vee (\neg Y \vee ((X \wedge \neg Z) \vee (\neg X \wedge Z)))$. Устранив двойное отрицание, получим
$\Phi'' = (X \wedge \neg Z) \vee (\neg Y \vee ((X \wedge \neg Z) \vee (\neg X \wedge Z)))$.
Нетрудно видеть, что это уже ДНФ. Удалим на (4)-ом этапе повторное вхождение первой конънкции и получим ДНФ
$\Phi_1 = (X \wedge \neg Z) \vee \neg Y \vee (\neg X \wedge Z)$.
Эта ДНФ не является совершенной, так как в каждую из ее трех конъюнкций входят не все переменные. Построим на этапе (5) для них эквивалентные совершенные ДНФ (используя решение задачи 4!).
$(X \wedge \neg Z) \equiv (X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y \wedge \neg Z)$,
$\neg Y \equiv (X \wedge \neg Y \wedge Z) \vee (X \wedge \neg Y \wedge \neg Z) \vee (\neg X \wedge \neg Y \wedge Z) \vee (\neg X \wedge \neg Y \wedge \neg Z)$,
$(\neg X \wedge Z) \equiv (\neg X \wedge Y \wedge Z) \vee (\neg X \wedge \neg Y \wedge Z)$.
Подставив эти формулы в Φ_1 и устранив повторения конъюнкций, получим совершенную ДНФ, эквивалентную исходной формуле Φ:
$\Phi_2 = (X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y \wedge \neg Z) \vee (X \wedge \neg Y \wedge Z) \vee (\neg X \wedge \neg Y \wedge Z) \vee (\neg X \wedge \neg Y \wedge \neg Z) \vee (\neg X \wedge Y \wedge Z)$.

Мы видим, что ДНФ Φ_1, полученная после 4-го этапа, выглядит существенно проще, т.е. является более короткой, чем совершенная ДНФ Φ_2. Однако совершенные ДНФ и КНФ обладают важным свойством единственности, которое следует из их конструкции в теореме 1.

Следствие 1.2. *Для каждой булевой функции от n переменных, не равной тождественно 0, существует единственная с точностью до перестановки конъюнкций и переменных внутри конъюнкций совершенная ДНФ, задающая эту функцию.*

Это следствие позволяет предложить следующую процедуру для проверки эквивалентности формул Φ и Ψ.
(1) Построить для Φ и Ψ эквивалентные совершенные ДНФ Φ' и Ψ', используя процедуру приведения к совершенной ДНФ.
(2) Упорядочить в соответствии с некоторой нумерацией переменных $\mathbf{X}$ вхождения переменных в каждую конъюнкцию, а затем лексикографически упорядочить между собой конъюнкции, входящие в Φ' и Ψ'. Пусть в результате получатся совершенные ДНФ Φ'' и Ψ''.
(3) Если $\Phi'' = \Psi''$, то выдать ответ "Да", иначе – ответ "Нет".

Замечание. Аналогичную процедуру можно построить с использованием совершенных КНФ.

2.2 Сокращенные ДНФ

Сокращенные ДНФ являются еще одним способом однозначного представления булевых функций, которое во многих случаях может оказаться более простым, чем представление с помощью совершенных ДНФ.

Напомним, что мы рассматриваем булевы функции над переменными $\mathbf{X} = \{X_1, \ldots, X_n\}$. С каждой элементарной конъюнкцией $K = X_{i_1}^{\sigma_1} \wedge X_{i_2}^{\sigma_2} \wedge \ldots \wedge X_{i_k}^{\sigma_k}$ связано множество N_K^+ наборов переменных, на которых K принимает значение 1. Нетрудно понять, что это множество содержит $2^{(n-k)}$ наборов, в которых каждая из входящих в K переменных X_{i_r} $(1 \leq r \leq k)$ имеет фиксированное значение σ_r, а значения остальных $(n-k)$ переменных произвольны.

Определение 3. *Пусть f - произвольная булева функция над $\mathbf{X}$. Элементарная конъюнкция K называется* допустимой для f, *если $N_K^+ \subseteq N_f^+$.*
Элементарная конъюнкция K называется максимальной для f, *если для любой элементарной конъюнкции L из условия $N_K^+ \subseteq N_L^+ \subseteq N_f^+$ следует, что $N_K^+ = N_L^+$.*
Сокращенной ДНФ *для функции f называется дизъюнкция всех максимальных для этой функции элементарных конъюнкций.*

Из этого определения непосредственно следует, что сокращенная ДНФ для функции f единственна (с точностью до порядка элементарных конъюнкций и порядка переменных в них) и в точности задает функцию f.

Примером сокращенной ДНФ является формула $\Phi_1 = (X \wedge \neg Z) \vee \neg Y \vee (\neg X \wedge Z)$ из примера 1.

Сокращенную ДНФ можно получить из произвольной ДНФ D, используя процедуру, называемую **методом Блэйка**.

(1) Применять, сколько возможно, закон поглощения
(П3): $(X \wedge K_1) \vee (\neg X \wedge K_2) \equiv (X \wedge K_1) \vee (\neg X \wedge K_2) \vee (K_1 \wedge K_2)$
слева направо при условии, что конънкция $(K_1 \wedge K_2)$ непротиворечива, т.е. не содержит одновременно некоторую переменную и ее отрицание. (Заметим, что на этом этапе число элементарных конъюнкций в ДНФ, вообще говоря, увеличивается).
(2) Применять, сколько возможно, правило поглощения (П1): $X \vee (X \wedge K) \equiv X$. Затем удалить повторные вхождения конъюнкций.

Теорема 2. *В результате применения метода Блейка к произвольной ДНФ через конечное число шагов будет получена эквивалентная ей сокращенная ДНФ.*

Доказательство.

Пусть после (1)-го этапа процедуры ДНФ D функции f преобразовалась в эквивалентную ДНФ D_1. Покажем, что *для всякой допустимой для f элементарной конъюнкция K в D_1 найдется такая конъюнкция K', что $N_K^+ \subseteq N_{K'}^+$.* Доказательство проведем возвратной индукцией по числу переменных в K.

Базис индукции. Пусть K содержит все n переменных из $\mathbf{X}$. Тогда N_K^+ состоит из единственного набора и, поскольку $N_K^+ \subseteq N_{D_1}^+$, то в D_1 сущетсвует конъюнкция K', для которой $N_K^+ \subseteq N_{K'}^+$.
Шаг индукции. Пусть для некоторого $k < n$ утверждение верно для всех допустимых для f конъюнкций, содержащих не менее $(k+1)$-ой переменной. Докажем, что оно верно и для допустимых конъюнкций с k переменными.

Пусть допустимая для f элементарная конъюнкция K содержит k переменных и пусть $X \in \mathbf{X}$ - переменная, не входящая в K. Тогда обе элементарные конъюнкции $K_1 = (X \wedge K)$ и $K_2 = (\neg X \wedge K)$ являются допустимыми для f и по предположению индукции для них в Φ_1 найдутся такие K_1' и K_2', что $N_{K_1}^+ \subseteq N_{K_1'}^+$ и $N_{K_2}^+ \subseteq N_{K_2'}^+$. Если хотя бы одна из них не содержит X, то ее можно выбрать в качестве K'. В противном случае, их можно представить в виде $K_1' = (X \wedge K_1'')$ и $K_2' = (\neg X \wedge K_2'')$. При этом $N_K^+ \subseteq N_{K_1''}^+$ и $N_K^+ \subseteq N_{K_2''}^+$. Поскольку все преобразования вида (П3) выполнены, то D_1 тогда содержит и конъюнкцию $K' = (K_1'' \wedge K_2'')$, для которой $N_K^+ \subseteq N_{K'}^+$.

Заметим, что если K максимальна для f, то $N_K^+ = N_{K'}^+$. Таким образом, все максимальные конъюнкции входят в D_1.

Теперь, чтобы завершить доказательство теоремы, нужно показать, что на этапе (2) из D_1 будут удалены все немаксимальные элементарные конъюнкции. (*Докажите это индукцией по числу немаксимальных конъюнкций в D_1.*)

Пример 2. *Применим метод Блейка к совершенной ДНФ функции $f(X_1, X_2, X_3)$, принимающей значение 1 на наборах множества $N_f^+ = \{(001), (010), (011), (101)\}$.*

Ее совершенная ДНФ
$$D = (\neg X_1 \wedge \neg X_2 \wedge X_3) \vee (\neg X_1 \wedge X_2 \wedge \neg X_3) \vee (\neg X_1 \wedge X_2 \wedge X_3) \vee (X_1 \wedge \neg X_2 \wedge X_3).$$
После применения преобразовнаий (П3) на (1)-ом этапе получим
$D_1 = (\neg X_1 \wedge \neg X_2 \wedge X_3) \vee (\neg X_1 \wedge X_2 \wedge \neg X_3) \vee (\neg X_1 \wedge X_2 \wedge X_3) \vee (X_1 \wedge \neg X_2 \wedge X_3) \vee (\neg X_2 \wedge X_3) \vee (\neg X_1 \wedge X_2) \vee (\neg X_1 \wedge X_3)$
После поглощений (П1) на втором этапе останется сокращенная ДНФ
$$D_2 = (\neg X_2 \wedge X_3) \vee (\neg X_1 \wedge X_2) \vee (\neg X_1 \wedge X_3).$$
Заметим, что она не является самой короткой ДНФ для f, т.к. $D_2 \equiv (\neg X_2 \wedge X_3) \vee (\neg X_1 \wedge X_2)$.

3 Многочлены Жегалкина

Напомним, что **многочленами Жегалкина** назваются формулы над множеством функций $F_J = \{0, 1, *, +\}$ (здесь $*$ - это другое обозначение конъюнкции). Таким образом, каждый многочлен Жегалкина (возможно, после раскрытия скобок и "приведения"подобных членов) представляет сумму (по модулю 2) *положительных (монотонных)* элементарных конъюнкций (т.е. элементарных конъюнкций без отрицаний). Поскольку для $+$ и * справедливы законы ассоциативности, мы будем при записи многочлена Жегалкина опускать скобки, считая, что $*$ связывает аргументы сильнее, чем $+$.

Нетрудно проверить, что справедливы следующие эквивалентности:

$$
\begin{array}{lrcl}
(J1) & \neg X & \equiv & (X+1), \\
(J2) & (X_1 \wedge X_2) & \equiv & (X_1 * X_2), \\
(J3) & (X_1 \vee X_2) & \equiv & (X_1 * X_2 + X_1 + X_2) \equiv (X_1+1)*(X_2+1)+1, \\
(J4) & (X_1+X_2)*(X_3+X_4) & \equiv & (X_1 * X_2 + X_1 * X_3 + X_2 * X_3 + X_2 * X_4).
\end{array}
$$

Из этих эквивалентностей и теоремы 1 легко получить первую часть следующего утверждения.

Теорема 3. *Для любой булевой функции существует задающий ее многочлен Жегалкина. Он единственен с точностью до перестановок слагаемых и порядка переменных в конъюнкциях.*

Доказательство. Существование такого многочлена следует из того, что для любой ДНФ или КНФ можно с помощью указанных эквивалентностей найти эквивалентный многочлен Жегалкина: (J1)-(J3) позволяют заменять все вхождения $\neg$, $\wedge$ и $\vee$ на $+$ и *, а (J4) - перемножать получившиеся после такой замены многочлены.

Для доказательства единственности представления подсчитаем число различных многочленов Жегалкина от n переменных. Каждая положительная элементарная конъюнкция имеет вид $X_{i_1} * \ldots * X_{i_k}$, где $1 \leq i_1 < \ldots < i_k \leq n$. Таких конъюнкций столько же, сколько подмножеств множества $\mathbf{X} = \{X_1, \ldots, X_n\}$, т.е. 2^n. (Конъюнкция, соответствующая пустому подмножеству переменных равна 1). Упорядочим их произвольным образом (например, лексикографически): $K_1, K_2, \ldots, K_{2^n}$. Тогда каждый многочлен Жегалкина единственным образом можно представить как сумму

$$\alpha_1 * K_1 + \alpha_2 * K_2 + \ldots + \alpha_{2^n} * K_{2^n},$$

где все коэффициенты α_i равны 0 или 1. Следовательно, число многочленов Жегалкина равно 2^{2^n}, т.е. числу всех булевых функций от n переменных. Поэтому каждая функция задается в точности одним многочленом Жегалкина.

Пример 3. *Пусть функция $f(X_1, X_2, X_3)$ задается ДНФ $\Phi = (X_1 \wedge \neg X_2) \vee (\neg X_1 \wedge X_2 \wedge \neg X_3)$. Найдем полином Жегалкина, который также задает эту функцию.*

Сначала заменяем $\wedge$ на *, а затем,применяя эквивалентность (J1), устраняем отрицания и получаем:
$\Phi \equiv X_1 * (X_2 + 1) \vee (X_1 + 1) * X_2 * (X_3 + 1)$.
Перемножив по правилам (J4), получим:
$\Phi \equiv (X_1 * X_2 + X_1) \vee (X_1 * X_2 * X_3 + X_1 * X_2 + X_2 * X_3 + X_2)$
Эквивалентность (J3) позволяет устранить $\vee$:
$\Phi \equiv (X_1 * X_2 + X_1) * (X_1 * X_2 * X_3 + X_1 * X_2 + X_2 * X_3 + X_2) + (X_1 * X_2 + X_1) + (X_1 * X_2 * X_3 + X_1 * X_2 + X_2 * X_3 + X_2)$.
Снова, используя (J4), перемножим первые две скобки и устраним повторения переменных в конъюнкциях:
$\Phi \equiv (X_1 * X_2 * X_3 + X_1 * X_2 + X_1 * X_2 * X_3 + X_1 * X_2 * X_3 + X_1 * X_2 + X_1 * X_2 * X_3 + X_1 * X_2 + X_1 * X_2) + (X_1 * X_2 + X_1) + (X_1 * X_2 * X_3 + X_1 * X_2 + X_2 * X_3 + X_2)$.
Упростим эту сумму, используя эквивалентности: $X + X \equiv 0$ и $X + 0 \equiv X$. В результате получим многочлен Жегалкина
$P(X_1, X_2, X_3) = X_1 + X_2 + X_2 * X_3 + X_1 * X_2 * X_3$,
эквивалентный исходной ДНФ Φ.

Если функция $f(X_1, \ldots, X_n)$ задана таблично, то для построения реализующего ее многочлена Жегалкина можно применить метод *неопределенных коэфициентов*.

Сопоставим i-ому набору значений переменных $\sigma_i = (\sigma_i^1, \ldots, \sigma_i^n)$ в таблице положительную конъюнкцию $K_i = \bigwedge_{\sigma_i^j = 1} X_j$ переменных, равных 1 в этом наборе. В частности, K_1 - пустая конъюнкция, $K_2 = X_n,\ K_3 = X_{n-1},\ K_4 = (X_n * X_{n-1})$. и т.д. Тогда для получения нужного многочлена Жегалкина достаточно определить все коэффициенты $\alpha_i,\ i = 1, \ldots, 2^n$, в выражении

$$f(X_1,\dots,X_n)=\alpha_1*K_1+\alpha_2*K_2+\ldots+\alpha_{2^n}*K_{2^n},$$

Подставляя в это равенство значения переменных из набора σ_i, $i=1,\dots,2^n$, мы получим 2^n линейных уравнений относительно 2^n неизвестных коэффициентов α_i. Решив эту систему, получим требуемый многочлен Жегалкина. Эта система треугольная и легко решается "сверху-вниз": каждое α_i определяется по значениям $\alpha_1,\dots,\alpha_{i-1}$ из уравнения, соответствующего набору σ_i.

Рассмотрим в качестве примера функцию $f(X_1,X_2,X_3)$, заданную следующей таблицей.

X_1	X_2	X_3	$f(X_1,X_2,X_3)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1.	1	1

Многочлен Жегалкина для нее (как и для любой функции от 3-х переменных) представляется в виде

$$p(X_1,X_2,X_3)=\alpha_0+\alpha_1*X_1+\alpha_2*X_2+\alpha_3*X_3+\alpha_{12}*X_1*X_2+\alpha_{13}*X_1*X_3+$$
$$\alpha_{23}*X_2*X_3+\alpha_{123}*X_1*X_2*X_3$$

В этом представлении в индексах у коэффициентов α перечислены переменные, входящие в соответствующие конъюнкции.

Последовательно подставляя значения переменных и f из таблицы, получаем:

$p(0,0,0)=\alpha_0=1;$

$p(0,0,1)=\alpha_0+\alpha_3=0\ \Rightarrow\alpha_3=1;$

$p(0,1,0)=\alpha_0+\alpha_2=0\ \Rightarrow\alpha_2=1;$

$p(0,1,1)=\alpha_0+\alpha_2+\alpha_3+\alpha_{23}=0\ \Rightarrow\alpha_{23}=1;$

$p(1,0,0)=\alpha_0+\alpha_1=1\ \Rightarrow\alpha_1=0;$

$p(1,0,1)=\alpha_0+\alpha_1+\alpha_3+\alpha_{13}=0\ \Rightarrow\alpha_{13}=0;$

$p(1,1,0)=\alpha_0+\alpha_1+\alpha_2+\alpha_{12}=0\ \Rightarrow\alpha_{12}=0;$

$p(1,1,1)=\alpha_0+\alpha_1+\alpha_2+\alpha_3+\alpha_{12}+\alpha_{13}+\alpha_{23}+\alpha_{123}=1\ \Rightarrow\alpha_{123}=1.$

Следовательно, функция $f(X_1,X_2,X_3)$ представляется многочленом Жегалкина

$$p_f(X_1,X_2,X_3)=1+X_3+X_2+X_2*X_3+X_1*X_2*X_3.$$