МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Санкт-Петербургский
государственный университет аэрокосмического приборостроения

И. Л. Ерош

ДИСКРЕТНАЯ МАТЕМАТИКА

БУЛЕВА АЛГЕБРА, КОМБИНАЦИОННЫЕ СХЕМЫ, ПРЕОБРАЗОВАНИЯ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Учебное пособие

Санкт-Петербург
2001

УДК 519.6(075)
ББК 22.19
Е78

Ерош И. Л.
Е78 Дискретная математика. Булева алгебра, комбинационные схемы, преобразования двоичных последовательностей: Учеб. пособие/СПбГУАП. СПб., 2001. 30 с.

Приводятся методы анализа и синтеза булевых выражений, примеры реализации комбинационных схем, построенных по словесному описанию алгоритма функционирования. Рассмотрены булевы преобразования двоичных последовательностей и показана возможность использования этих преобразований при решении некоторых задач криптографии.

Пособие ориентировано на студентов технических университетов, аспирантов и преподавателей дисциплины “Дискретная математика“ технических вузов.

Рецензенты:
кафедра радиосистем Санкт-Петербургского электротехнического университета;
канд. техн. наук доц. *В. Н. Сасковец*

Утверждено
редакционно-издательским советом университета
в качестве учебного пособия

Предисловие

Цифровые устройства (цифровые автоматы) обычно делятся на два класса: автоматы без памяти (однотактные автоматы, комбинационные схемы) и автоматы с памятью (многотактные автоматы). Комбинационные схемы составляют основу дискретных вычислительных и управляющих устройств. Они могут выполнять как самостоятельные функции: преобразователи кодов, дешифраторы и т. п., – так и входить в состав цифровых автоматов с памятью, реализуя функции переключения элементов памяти в новые состояния, выработку логических и управляющих сигналов. Сами элементы памяти могут быть построены в виде комбинационных схем с обратными связями.

В настоящем учебном пособии в краткой форме изложены основные понятия и методы построения однотактных цифровых устройств контроля и управления, логика работы которых описывается булевыми функциями. Булевы преобразования двоичных последовательностей выделены в самостоятельный раздел, в котором описаны возможные области применения булевых преобразований при решении некоторых задач защиты информации.

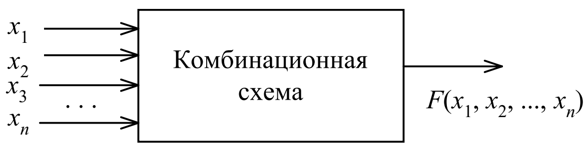
1. БУЛЕВЫ ФУНКЦИИ И КОМБИНАЦИОННЫЕ СХЕМЫ

1.1. Понятие о булевых функциях. Булевы функции одного и двух аргументов

Булевыми функциями (функциями алгебры логики) называют функции, аргументы которых, так же как и сама функция, принимают только два значения – 0 или 1. Алгебра логики является разделом математической логики, в которой изучаются методы доказательства истинности (1) или ложности (0) сложных логических конструкций, составленных из простых высказываний, на основе истинности или ложности последних.

Алгебра Буля оказалась очень удобным и эффективным математическим аппаратом для анализа и синтеза комбинационных схем.

Булевы функции определяют логику работы комбинационных схем следующего вида:



где $x_1 – x_n$, $F \in \{ 0, 1\}$. Рассмотрим частные случаи.

Пусть $n = 1$, тогда входной сигнал x может принимать только два значения – 0 и 1, а выходной сигнал $F(x)$ может обеспечивать четыре различных реакции на выходе. Таблица, в которой каждому набору входных сигналов сопоставляется значение выходного сигнала, называется *таблицей истинности* функции.

Для комбинационных схем с одним входом таблицы истинности всех булевых функций, описывающих логику работы схемы, примут вид (табл. 1).

$F_1 = \text{const } 0$, $F_2 = x$, функция повторения x, $F_4 = \text{const } 1$, F_3 – инверсия аргуменмента x, обозначаемая $\rceil x$ или x и называемая иногда “не x”, “отрицание x”.

Таблица 1

x	F_1	F_2	F_3	F_4
0	0	0	1	1
1	0	1	0	1

При $n = 2$ получаем таблицу истинности 16 различных функций двух аргументов (табл. 2).

Таблица 2

x_1	x_2	F_0	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	F_{13}	F_{14}	F_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Среди функций двух аргументов имеются уже известные функции F_0 и F_{15} , соответственно, “константа 0” и “константа 1” – функции, не зависящие от аргументов, иногда называемые функции нуль аргументов. Функции $F_3 = x_1$ и $F_5 = x_2$ – функции повторения, соответственно, аргументов x_1 и x_2. Функции $F_{12} = \rceil x_1$ и $F_{10} = \rceil x_2$ – функции инверсии, соответственно, аргументов x_1 и x_2. Эти функции считаются функциями одного аргумента.

Рассмотрим новые функции, которые впервые появляются в таблице функций двух аргументов.

F_1 – конъюнкция аргументов x_1 и x_2, обозначается: $F_1 = x_1 \,\&\, x_2 = x_1 \wedge x_2 = x_1 \cdot x_2 = x_1 x_2$. Допустимыми являются все виды приведенных обозначений, но поскольку эта функция называется логическое умножение, функция “И”, то, как и в обычной алгебре, знак умножения часто опускается.

F_7 – дизъюнкция аргументов x_1 и x_2, обозначается: $F_7 = x_1 \vee x_2 = x_1 + x_2$. Обычно используют только первый вид обозначения. Эта функция называется логическое сложение, функция “ИЛИ”, но знак сложения “+” практически не используется.

Для приведенных функций в таблице имеются инверсии. Так, $F_{14} = \overline{F_1}$ (штрих Шеффера), $F_8 = \overline{F_7}$ (стрелка Пирса), но поскольку функции F_{14} и F_8 играют очень важную роль в вычислительной технике, они будут рассмотрены подробнее ниже.

Новыми функциями также являются F_9 и F_6 . Первая называется функцией совпадения (эквиваленция) и обозначается обычно $F_9 = x_1 \equiv x_2$. Вторая функция является ее инверсией и называется функцией сложения по модулю 2, т. е. $F_6 = \overline{F_9} = \overline{x_1 \equiv x_2} = x_1 \oplus x_2$.

Функции F_{13} и F_{11} называются функциями импликации и обозначаются, соответственно, $F_{13} = x_1 \rightarrow x_2$ и $F_{11} = x_2 \rightarrow x_1$ (словесное обозначение: F_{13} – “ x_1 влечет x_2”; F_{11} – “ x_2 влечет x_1”). Функции импликации играют очень важную роль в математической логике, так как описывают логику всех теорем достаточности, которые формулируются в виде: “Если выполняется условие А, то следует В”. При построении комбинационных схем эти функции практически не используются.

Функции F_2 и F_4 из табл. 2 являются инверсиями функций импликации, соответственно F_{13} и F_{11} .

1.2. Булевы функции трех аргументов

Таблица 3

x_1	x_2	x_3	F
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Функции трех аргументов задаются на восьми наборах. Количество функций трех аргументов равно $2^8 = 256$.

Одной из функций трех аргументов является мажоритарная функция. Таблица истинности этой функции имеет следующий вид (табл. 3).

Функция равна 1, если во входном наборе два или три аргумента принимают значение 1, и равна 0 в остальных случаях. Эта функция обладает корректирующей способностью, поэтому на заре развития вычислительной техники были работы, в которых рекомендовалось все комбинационные схемы строить на мажоритарных элементах.

1.3. Булевы функции *n* аргументов. СДНФ и СКНФ

Булева функция n аргументов задается на 2^n наборах. Число таких функций равно 2^{2^n} .

Если булева функция задана таблицей истинности, то она может быть представлена в аналитической форме с использованием операций конъюнкции, дизъюнкции и инверсии с помощью следующих правил:

– каждой единице в таблице истинности ставится в соответствие конъюнкция ранга n, где n – число аргументов функции; рангом конъюнкции называют число аргументов, входящих в конъюнкцию, причем в этой конъюнкции аргумент входит без инверсии, если в соответствующем наборе он принимает значение 1, и с инверсией, если принимает значение 0;

– все полученные конъюнкции объединяются знаками дизъюнкции.

Например, для мажоритарной функции аналитическое выражение будет иметь вид

$$F = \overline{x_1}\, x_2\, x_3 \vee x_1\, \overline{x_2}\, x_3 \vee x_1 x_2\, \overline{x_3} \vee x_1\, x_2\, x_3. \qquad (1)$$

Аналитическое выражение функции вида (1) называют совершенной дизъюнктивной нормальной формой (СДНФ), при этом под совершенной формой понимают аналитическое выражение функции, когда во все конъюнкции входят все аргументы, т. е. все конъюнкции имеют ранг n; под нормальной формой понимают выражение, в котором инверсии применяются только к отдельным аргументам.

Если в таблице истинности число нулей существенно меньше числа единиц, используют аналитическую запись в виде совершенной конъюнктивной нормальной формы (СКНФ). Она строится по следующим правилам:

– каждому нулю в таблице истинности ставится в соответствие дизъюнкция ранга n, где n – число аргументов функции; рангом дизъюнкции называют число аргументов, входящих в дизъюнкцию, причем в этой дизъюнкции аргумент входит без инверсии, если в соответствующем наборе он принимает значение 0, и с инверсией, если принимает значение 1;

– все полученные дизъюнкции объединяются знаками конъюнкции.

Возьмем, например, функцию F, представленную следующей таблицей истинности (табл. 4).

Таблица 4

x_1	x_2	x_3	F	$\overline{F}$
0	0	0	1	0
0	0	1	0	1
0	1	0	1	0
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	0

СДНФ этой функции представляет собой шесть конъюнкций ранга 3, объединенные знаками дизъюнкции, т. е. достаточно громоздкое выражение. В то же время СКНФ этой функции будет выглядеть так:

$$F = (x_1 \vee x_2 \vee \overline{x_3})\,(\overline{x_1} \vee x_2 \vee x_3). \qquad (2)$$

В выражении (2) имеются две дизъюнкции, объединенные знаком конъюнкции.

1.4. Элементарные преобразования булевых выражений

Часто преобразование булевых выражений выполняется с целью упрощения последних или, как говорят, с целью их минимизации. Легко обосновываются следующие правила минимизации:

– поглощения: $x \vee xy = x$; $x(x \vee y) = x$;

– склеивания: $xy \vee x\rceil y = x$;

– обобщенного склеивания: $xz \vee y\rceil z \vee xy = xz \vee y\rceil z$;

– $x \vee \rceil x\, y = x \vee y$.

Покажем, как можно применить правило склеивания для минимизации мажоритарной функции. Аналитическое выражение перепишем в следующем виде:

$$F = \overline{x_1}\, x_2 x_3 \vee x_1 \overline{x_2}\, x_3 \vee x_1 x_2 \overline{x_3} \vee x_1 x_2 x_3 \vee x_1 x_2 x_3 \vee x_1 x_2 x_3. \qquad (3)$$

Повторение конъюнкции $x_1 x_2 x_3$ не меняет значение функции, так как $Y \vee Y = Y$, где Y – любое булево выражение. Тогда, склеивая 1-й и 4-й члены, 2-й и 5-й, 3-й и 6-й, получаем эквивалентное выражение

$$F = x_2 x_3 \vee x_1 x_3 \vee x_1 x_2. \qquad (4)$$

Выражение (4) будет дизъюнктивной, нормальной формой функции, так как в каждую из конъюнкций входят не все аргументы функции.

Преобразование булевых выражений с помощью приведенных правил поглощения, склеивания и обобщенного склеивания применяется достаточно редко, так как имеется более эффективный способ минимизации булевых функций, число аргументов которых не превышает 11. Кроме того, так же просто обосновывается преобразование, называемое правилом де Моргана:

$$а)\ \overline{x_1 x_2} = \overline{x_1} \vee \overline{x_2};$$

$$б)\ \overline{x_1 \vee x_2} = \overline{x_1}\,\overline{x_2}. \qquad (5)$$

Покажем, как применить правило де Моргана для вывода формулы СКНФ. В табл. 4 имеется значение функции, инверсной к F, т. е. $\overline{F}$. Эта функция имеет только две единицы, поэтому СДНФ ее будет представлять собой две конъюнкции, каждая ранга 3, объединенные знаком дизъюнкции:

$$\overline{F} = \overline{x_1}\,\overline{x_2}\,x_3 \vee x_1\,\overline{x_2}\,\overline{x_3} \; . \qquad (6)$$

Проинвертируем левую и правую части выражения (6) и применим к правой части правило де Моргана, тогда получим

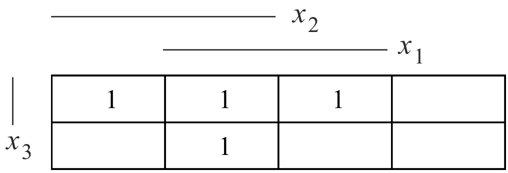
$$F = (x_1 \vee x_2 \vee \overline{x_3})\,(\overline{x_1} \vee x_2 \vee x_3)\; .$$

В результате получена формула СКНФ функции F.

1.5. Минимизация булевых функций с помощью диаграмм Вейча (карт Карно)

Диаграммы Вейча представляет собой ту же таблицу истинности булевой функции, только в более компактной форме. Так, для функции трех аргументов, которая задается на восьми наборах, таблица истинности будет содержать восемь клеток, причем каждая клетка в диаграмме Вейча соответствует некоторому набору в таблице истинности.

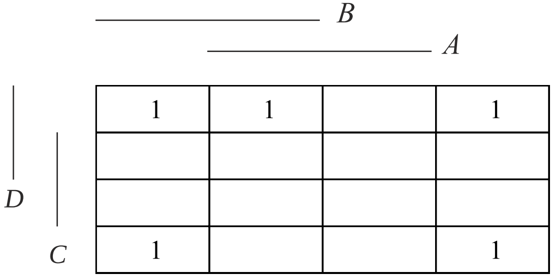
Области в диаграмме Вейча обозначим следующим образом: подчеркнутые столбцы или строки будут соответствовать истинному значению аргумента, а не подчеркнутые – ложному. Тогда диаграмма Вейча мажоритарной функции примет вид



Из полученной диаграммы Вейча легко выписывается минимальное выражение для мажоритарной функции

$$F = x_2 x_3 \vee x_1 x_3 \vee x_1 x_2.$$

Возьмем некоторую функцию F четырех аргументов, диаграмма Вейча которой имеет вид



Эта функция принимает значение 1 на пяти наборах, отмеченных на диаграмме единицами. На остальных наборах функция принимает значение 0. СДНФ этой функции содержала бы пять конъюнкций каждая ранга 4, объединенные знаками дизъюнкций. Однако из диаграммы Вейча легко выписывается минимальное выражение функции в дизъюнктивной нормальной форме

$$F = \overline{A}\overline{C} \vee B\overline{C}D.$$

Области в диаграмме Вейча обозначаются так, чтобы две соседние клетки соответствовали бы "склеивающимся" конъюнкциям (т. е. конъюнкциям, отличающимся значением только одного аргумента). Так, например:

$$A\overline{B}C\overline{D} \vee ABC\overline{D} = AC\overline{D}.$$

Это обеспечивает наглядность минимизации.

В общем случае области в диаграммах Вейча для функций большого числа аргументов обозначаются кодом Грэя. Особенностью этого кода является то, что две соседние комбинации отличаются значением только одного аргумента. Обычный двоичный код этому условию не удовлетворяет.

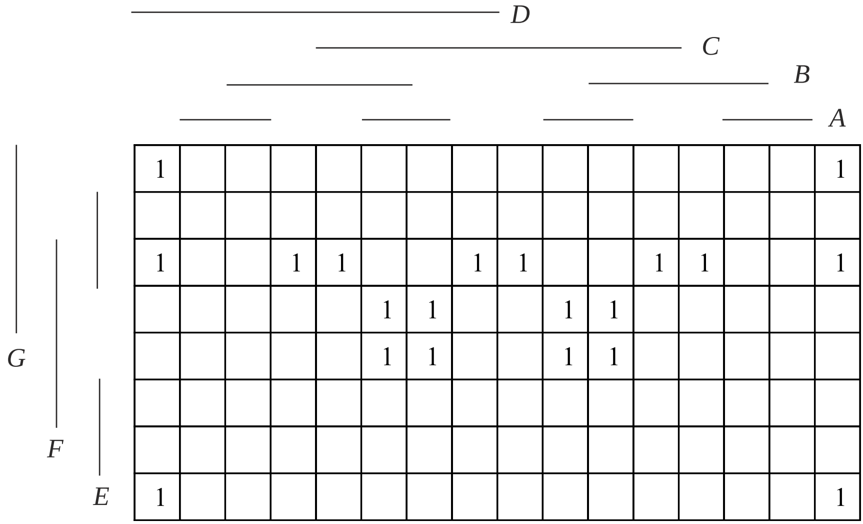
Таблица 5

0000	00**00**
0001	00**01**
0010	00**11**
0011	00**10**
0100	0110
0101	0111
0110	0101
0111	0100
1000	1100
1001	1101
1010	1111
1011	1110
1100	1010
1101	1011
1110	1001
1111	1000

Код Грэя используется в цифровых кодовых датчиках, что позволяет сделать ошибку равномерной при смещениях токосъемников, при этом ошибка равна 2^{-m} где m – число двоичных разрядов кодового датчика. Это свойство кода Грэя используется для обозначения областей в диаграммах Вейча.

В табл. 5 приведен код Грэя для четырех аргументов (разрядов). Если требуется построить код Грэя на меньшее число разрядов, то его легко получить из имеющейся таблицы путем "вырезания" соответствующей части. Так, в приведенной таблице показано, как получить двухразрядный код Грэя. Если требуется построить код Грэя на пять разрядов, то код в таблице следует зеркально отразить вниз и добавить еще один разряд, причем в первой половине в этом разряде будут стоять нули, а во второй – единицы. Аналогично строятся коды Грэя на любое число разрядов.

П р и м е р . Минимизировать функцию семи аргументов, заданную диаграммой Вейча:



Минимальное выражение в дизъюнктивной нормальной форме имеет вид

$$F = AC\overline{E}F \vee \overline{A}EFG \vee \overline{A}\,\overline{B}\,\overline{C}\,\overline{E}\,\overline{F}\,.$$

П р и м е р ы д л я п р а к т и ч е с к и х з а н я т и й .

1. Доказать с помощью диаграмм Вейча равенства, которые использовались для минимизации (поглощения и склеивания, а также правило де Моргана).

2. Построить диаграммы Вейча для следующих функций и выписать минимальные выражения в дизъюнктивной нормальной форме:

а) $\rceil ab \rceil cd \vee \rceil a \rceil b \rceil c \rceil d \vee \rceil ab \rceil c \rceil d \vee \rceil a \rceil b \rceil cd \vee \rceil a \rceil bcd \vee \rceil abcd =$;

б) $abc \vee ab \rceil c \vee \rceil abd \vee \rceil bde =$.

1.6. Минимизация частично определенных булевых функций

Диаграммы Вейча могут использоваться для минимизации не только так называемых полностью определенных логических функций (когда функция в таблице истинности принимает только два значения: 0 или 1), но и для случая частичных (не полностью определенных) функций. При построении реальных цифровых устройств контроля и управления комбинационные схемы описываются, как правило, не полностью определенными булевыми функциями. Очень часто функции не определены на большом числе наборов. В таблице истинности и, следовательно, в диаграммах Вейча такие функции кроме 0 и 1 будут содержать еще и “–”; это означает, что такой набор никогда на вход устройства не поступает. Следовательно, поведение комбинационной схемы при таком наборе не имеет значения, и на месте “–” может быть произвольно поставлена либо 1, либо 0. Этот процесс называется доопределением булевой функции. Доопределение булевой функции желательно выполнять так, чтобы получить возможно более простое выражение. В этом случае, как правило, реализованная комбинационная схема также оказывается более простой.

Пусть задана диаграмма Вейча некоторой не полностью определенной функции:

	B	B, A	A	
	1	–	–	1
			1	–
D		–		–
C	–			1

Приведенная функция имеет прочерки в шести клетках, в каждой из которых может быть поставлена как 1, так и 0. Следовательно, существует $2^6 = 64$ различных способов доопределения булевой функции. Однако из диаграммы легко выбрать наилучший, который дает следующий результат минимизации:

$$F = \overline{A}\,\overline{C} \vee \overline{B}D.$$

П р и м е р ы д л я п р а к т и ч е с к и х з а н я т и й .

Доопределить функцию и выисать минимальное выражение из диаграмм Вейча:

а)

B, A; D, C

1		1	–
–			–
–	1	–	
	1	–	1

б)

c, b, a; e, d

	1	–			–	–	
1	1		–	1			–
	1						
	–	1			1	–	

в)

c, b, a; e, d

	–			–		1	
1	1		–				–
1	–						
	1	–			–	–	–

1.7. Проверка равенств в булевой алгебре

Для того чтобы доказать равенство двух функций в булевой алгебре, например, $F(x_1, x_2, \ldots, x_n) = P(x_1, x_2, \ldots, x_n)$, необходимо и достаточно показать, что на всех наборах аргументов $x_1, x_2, \ldots, x_n$ левая часть равенства совпадает с правой.

Например:

$$(AB \downarrow BC) \to BD = (\overline{\overline{B} \vee A\overline{C}\,\overline{D}}).$$

Для доказательства этого равенства построим диаграммы Вейча для левой и правой части равенства. Левая часть равенства

B, A; D, C

AB

	1		
	1		
	1		
	1		

BC

1	1		
1	1		

$AB{\downarrow}BC$

1		1	1
		1	1
		1	1
1		1	1

BD

1	1		
1	1		

$AB{\downarrow}BC{\to}BD$

1	1		
1	1		
1	1		
	1		

Правая часть равенства

		1	1
		1	1
		1	1
1		1	1

1	1		
1	1		
1	1		
	1		

Поскольку диаграмма Вейча для левой части совпадает с диаграммой для правой, то имеет место приведенное выше равенство.

П р и м е р ы д л я п р а к т и ч е с к и х з а н я т и й .

Упростить булевы выражения:

а) $\overline{X\,Y\,Z \to X\,P} \oplus (YZ / XZP) =$;

б) $(AB \vee \overline{AC\,D}) \equiv (\overline{BC \otimes AC\,D}) =$;

в) $M(AB \to C, ACD, BD \vee AC) =$.

Под $M(X, Y, Z)$ понимается мажоритарная функция от аргументов X, Y, Z, где последние – любые аргументы или булевы выражения.

1.8. Функционально полные наборы и базисные наборы

Функционально полным называется набор булевых функций $\{f_1, f_2, \ldots, f_n\}$ такой, что любая сколь угодно сложная булева функция может быть выражена в виде суперпозиции (сочетания) функций из этого набора.

Базисным называется такой функционально полный набор, из которого нельзя исключить ни одну булеву функцию без ущерба для его функциональной полноты.

Поскольку любая булева функция, заданная таблицей истинности, может быть представлена в виде СДНФ (или СКНФ), то набор

1) $\{\&, \vee, \rceil\}$ – функционально полный набор.

Набор 1) не является базисным набором, так как из него можно исключить либо &, либо $\vee$, а недостающую функцию реализовать с помощью оставшихся функций. Например, если из набора 1) исключена &, то ее можно реализовать так: $AB = \rceil(\rceil A \vee \rceil B)$ (выражение справа понимается так: $\overline{\overline{A} \vee \overline{B}}$). Если же из набора 1) исключена функция $\vee$, то она может быть реализована так: $X \vee Y = \rceil(\rceil X \rceil Y) = \overline{\overline{X}\,\overline{Y}}$.

Таким образом, получаем два функционально полных (базисных) набора:

2) $\{\&, \rceil\}$;

3) $\{\vee, \rceil\}$.

Русский математик Жегалкин показал, что любая булева функция может быть представлена с использованием операций конъюнкции (&) сложения по модулю 2 ($\oplus$) и константы 1. Покажем, как известные функции набора 1) представить в виде декомпозиции функций Жегалкина: $\rceil A = A \oplus 1$; $A \vee B = \rceil(\rceil A \rceil B) = (A \oplus 1)(B \oplus 1) \oplus 1 =$ $= AB \oplus A \oplus B \oplus 1 \oplus 1 = AB \oplus A \oplus B$.

Поэтому следующим функционально полным (базисным) набором будет набор функций Жегалкина:

4) $\{\&, \oplus, 1\}$.

Аналогично можно показать, что набор

5) $\{\vee, \oplus, 1\}$ – базисный набор.

Выше было показано, что мажоритарная функция $M(X, Y, Z) =$ $= XY \vee XZ \vee YZ$. Если на один из входов, например Z, подать константу 1, то получим $M(X, Y, 1) = XY \vee X \vee Y = X \vee Y$, а если на этот же вход Z подать константу 0, то получим $M(X, Y, 0) = XY$. Поэтому получаем еще два базисных набора:

6) $\{M, \rceil, 1\}$;

7) $\{M, \rceil, 0\}$.

Когда говорят о “мажоритарном базисе” , то имеют в виду эти два набора (или их объединение: $\{M, \rceil, 1, 0\}$), предполагая, что 1 и 0 реализуются “без затрат”, а инверсия аргументов всегда присутствует, если комбинационная схема подключается к триггерным устройствам (элементарным автоматам), которые имеют как прямой, так и инверсные выходы.

На практике, как правило, используются базисные наборы, состоящие только из одной функции (“штрих Шеффера” или “стрелка Пирса”):

8) $\{/\}$;

9) $\{\downarrow\}$.

Набор 8) реализует функцию $\rceil(XY) = \overline{XY}$. Инверсия аргумента может быть получена так: $\rceil X = \rceil(XX)$. Конъюнкция $XY = \rceil(\rceil(XY) =$ $= \overline{\overline{X\,Y}} = \overline{\overline{X\,Y}\;\overline{X\,Y}}$. Дизъюнкция может быть реализована так: $X \vee Y =$ $= \rceil(\rceil X \rceil Y) = \overline{\overline{X}\,\overline{Y}} = \overline{\overline{X\,X}\;\overline{Y\,Y}}$.

Набор 9) реализует функцию $\rceil(X \vee Y) = \overline{X \vee Y}$. Инверсия аргумента может быть получена так: $\rceil(X \vee X)$. Дизъюнкция может быть получена так: $X \vee Y = \rceil(\rceil(X \vee Y))$. Конъюнкция может быть получена так: $XY = (\rceil X \vee \rceil Y)$.

П р и м е р . Перевести в базис Шеффера и Пирса функцию, заданную в дизъюнктивной форме:

$$F = \overline{A}B \vee A\overline{CD} \vee \overline{B}D.$$

В базисе Шеффера функция будет иметь вид

$$F = \overline{\overline{\overline{A}B}\,\overline{A\overline{CD}}\,\overline{\overline{B}D}}$$

В базисе Пирса функция будет иметь вид

$$F = \overline{\overline{\overline{A \vee \overline{B}} \vee \overline{\overline{A} \vee \overline{\overline{C}} \vee \overline{\overline{D}}} \vee \overline{B \vee \overline{D}}}}$$

П р и м е р ы д л я с а м о с т о я т е л ь н о й р а б о т ы .

Представить в базисах Шеффера и Пирса следующие функции (при необходимости предварительно упростить):

а) $\overline{\overline{ABC \vee BD} \;\forall\; AC \vee \overline{A}CD}$;

б) $\overline{XZ \vee \overline{ZY \vee ZP}} =$.

1.9. Примеры реализации комбинационных схем

Редко задание на проектирование комбинационных схем формулируется в виде перечисления входных и соответствующих им выходных наборов (таблиц истинности). Часто оно задается в виде описания работы.

П р и м е р 1. Построить однотактное устройство, реализующее следующий алгоритм работы.

На вход устройства подается 5-разрядный двоичный код (x_1, x_2, x_3, x_4, x_5).

На выходе вырабатывается 0, если число единиц в коде равно 0 или 1, и вырабатывается 1, если число единиц равно 4 или 5. Остальные случаи не предусмотрены (на остальных наборах можно проставить “–”).

Построим диаграмму Вейча по данному описанию.

x_3 x_2 x_1

–	–	1	–	–	–	–	0	
–	1	1	1	–	1	–	–	
–	–	1	–	–	–	–	0	x_5
0	–	–	–	0	–	0	0	x_4

Выпишем решение при очевидном способе доопределения и представим его в базисе Шеффера и Пирса:

$$F = x_2x_3 \vee x_4x_5 = \overline{\overline{x_2x_3}\;\overline{x_4x_5}} = \overline{\overline{\overline{\overline{x_2} \vee \overline{x_3}} \vee \overline{\overline{x_4} \vee \overline{x_5}}}}\,.$$

Комбинационные схемы на несколько выходов строятся аналогичным образом. Однако предпринимаются попытки провести совместную минимизацию схем, реализующих отдельные выходные сигналы. Примерами таких схем могут служить различные преобразователи кодов.

П р и м е р 2. Построить однотактное устройство, преобразующее двоичный код в код Грэя.

Выпишем таблицу истинности четырех разрядов кода Грэя.

x_4	x_3	x_2	x_1	y_4	y_3	y_2	y_1
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	0	0	1	1
0	0	1	1	0	0	1	0
0	1	0	0	0	1	1	0
0	1	0	1	0	1	1	1
0	1	1	0	0	1	0	1
0	1	1	1	0	1	0	0
1	0	0	0	1	1	0	0
1	0	0	1	1	1	0	1
1	0	1	0	1	1	1	1
1	0	1	1	1	1	1	0
1	1	0	0	1	0	1	0
1	1	0	1	1	0	1	1
1	1	1	0	1	0	0	1
1	1	1	1	1	0	0	0

Число диаграмм Вейча равно четырем, причем для y_4 она тривиальная ($y_4 = x_4$), а для остальных имеет следующий вид.

Для y_1

x_4 x_3

1	1	1	1
1	1	1	1

x_2 x_1

$$y_1 = x_1\overline{x_2} \vee \overline{x_1}x_2 = x_1 \oplus x_2 .$$

Для y_2

x_4 x_3

1			1
1			1
	1	1	
	1	1	

x_2 x_1

$$y_2 = x_2\overline{x_3}\ \ \overline{x_2} \vee x_3 = x_2 \oplus x_3 .$$

Для y_3

x_4 x_3

1		1	
1		1	
1		1	
1		1	

x_2 x_1

$$y_3 = x_3\ \overline{x_4} \vee \overline{x_3}\,x_4 = x_3 \oplus x_4.$$

1.10. Изображение комбинационных элементов на функциональных схемах

Для изображения комбинационных элементов в различных базисах используются следующие обозначения.

Изображение элемента “И”

Изображение элемента “ИЛИ”

Изображение элемента “И-НЕ” (Шеффера)

Изображение элемента “ИЛИ-НЕ” (Пирса)

Изображение элемента “НЕ”

Изображение элемента “⊕” (сумма по модулю 2)

Упражнение. Нарисуйте функциональные схемы двух устройств в различных базисах, которые были синтезированы в подразд. 1.9.

2. БУЛЕВЫ ПРЕОБРАЗОВАНИЯ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

2.1. Постановка задачи

Пусть имеются две двоичные последовательности $A(a_1, a_2, \ldots, a_n)$ и $B(b_1, b_2, \ldots, b_n)$. При этом a_i, $b_i \in \{0, 1\}$, $i = 1, 2, 3, \ldots, n$. Элементы последовательности B будем получать булевым преобразованием последовательности A, при этом b_i будет результатом булевого преобразования, зависящего от a_i и некоторых элементов из окружения a_i. Максимальное число аргументов булевой преобразующей функции F равно $N = 2n - 1$. Так, для $n = 3$ $N = 5$; для $n = 4$ $N = 7$; для $n = 5$ $N = 9$.

Рассмотрим методы нахождения функций F.

2.2. Теорема о преобразованиях двоичных последовательностей

Сформулируем теорему, на основании которой можно строить булевы функции, преобразующие одну последовательность в другую. Эта теорема является аналогом теоремы, доказанной в литературе[1].

Теорема. Для того чтобы существовала булева функция F, преобразующая произвольную последовательность A в произвольную последовательность B, необходимо и достаточно, чтобы A была ненулевой последовательностью. Число аргументов F не превышает $2n - 1$.

Необходимость следует из того, что при нулевой последовательности A все элементы последовательности B будут либо нулями, либо единицами, и в этом случае B не может быть произвольной последовательностью.

Для доказательства достаточности построим часть таблицы истинности функции F, в которой функция определена:

[1] *Ерош И. Л., Игнатьев М. Б., Москалев Э. С.* Адаптивные системы управления промышленными роботами: Учеб. пособие для втузов / ЛИАП. Л., 1985. 144 с.

$$
\begin{array}{lcl|l}
 & & a_1\ a_2\ \ldots\ a_n & b_1 \\
 & a_1\ a_2\ \ldots\ a_n & & b_2 \\
 & a_1\ a_2\ \ldots\ a_n & & b_3 \\
\ldots\ldots\ldots & \ldots\ldots\ldots & \ldots\ldots\ldots & \ldots \\
a_1\ a_2\ \ldots\ a_{n+1} & & & b_n
\end{array}
$$

Если хотя бы один элемент последовательности A не равен 0, то все наборы, на которых функция определена, будут различными, поэтому не существует ни одной одинаковой пары наборов, на которой функция должна принимать одновременно значение 0 и 1.

П р и м е р . Пусть A (101), B (011). Функция F будет зависеть от аргументов (a_{i-2} , a_{i-1}, a_i , a_{i+1}, a_{i+2}). Таблица истинности этой функции (точнее, только та ее часть, на которой функция определена) будет иметь вид

a_{i-2}	a_{i-1}	a_i	a_{i+1}	a_{i+2}	B
		1	0	1	0
	1	0	1		1
1	0	1			1

Функция пяти аргументов задается на 32 наборах. Однако эта функция задана в примере всего на 3 наборах. На остальных 29 наборах функция не определена и ее можно доопределить 2^{29} способами. Диаграмма Вейча этой функции будет иметь вид

a_{i-2}

a_{i-1}

a_i

–	–	–	–	–	–	0	–
–	–	–	–	–	–	–	–
–	–	–	–	1	–	–	–
–	1	–	–	–	–	–	–

a_{i+2}

a_{i+1}

Доопределить и минимизировать данную функцию достаточно просто: $F = \overline{a_{i+2}}$. Действительно, применив булево преобразование F к A, получим B.

При длинах векторов А и В, равных n, булева функция будет задаваться на n наборах, а на $2^{(2n-1)} - n$ наборах функция будет не определена. Доопределение и минимизация булевой функции не однозначны.

Определение. Два набора A_i и A_j длины n будем называть связанными сдвигом, если при некотором сдвиге одного набора относительно другого у этих наборов совпадают позиции всех единиц. Например, А = 1 0 0 1 0 1 1 0 0 0 и В = 0 0 1 0 0 1 0 1 1 0 – наборы, связанные сдвигом.

Из приведенной выше теоремы сформулируем следствия.

Следствие 1. Если A_i, $i = 1, 2, 3, \ldots, k$ – двоичные векторы, не связанные сдвигом, и В – произвольный вектор, то существует одна булева функция F, преобразующая любой вектор A_i в вектор В, т. е. $B = F(A_i)$, $i = 1, 2, 3, \ldots, k$.

П р и м е р 1. Пусть $A_1 = 1011$; $A_2 = 1001$; $A_3 = 0110$; $B = 0111$. Построим часть таблицы истинности функции F, выписывая только те наборы, на которых функция определена, при этом для удобства введем очевидные переобозначения аргументов.

Пример 1

a	*b*	*c*	*d*	*e*	*g*	*h*	*F*
			1	0	1	1	0
		1	0	1	1		1
	1	0	1	1			1
1	0	1	1				1
			1	0	0	1	0
		1	0	0	1		1
	1	0	0	1			1
1	0	0	1				1
			0	1	1	0	0
		0	1	1	0		1
	0	1	1	0			1
0	1	1	0				1

Упражнение. Постройте диаграмму Вейча функции F и убедитесь в том, что при некотором способе доопределения функция будет иметь вид

$$F = a \vee c \vee e\,\overline{g}\,.$$

Проверьте, что эта функция из любой приведенной последовательности A_i ($i = 1, 2, 3$) строит одну и ту же последовательность В.

Следствие 2. Если A_i и B_i – произвольные векторы, причем A_i не связаны сдвигом, то существует одна булева функция F, преобразующая каждый вектор A_i в соответствующий ему вектор B_i.

П р и м е р 2. Пусть требуется найти одну функцию F, преобразующую векторы:

$A_1 = 1011$ в вектор $B_1 = 0110$,
$A_2 = 0111$ в вектор $B_2 = 1001$,
$A_3 = 0101$ в вектор $B_3 = 1110$.

Построим часть таблицы истинности функции F, выписывая только те наборы, на которых функция определена.

Пример 2

a	b	c	d	e	g	h	F
			1	0	1	1	0
		1	0	1	1		1
	1	0	1	1			1
1	0	1	1				0
			0	1	1	1	1
		0	1	1	1		0
	0	1	1	1			0
0	1	1	1				1
			0	1	0	1	1
		0	1	0	1		1
	0	1	0	1			1
0	1	0	1				0

Упражнение. Постройте диаграмму Вейча функции F и убедитесь в том, что при некотором способе доопределения функция будет иметь вид

$$F = \bar{d} \vee \bar{e} g \bar{h} \vee bc \vee be.$$

В частном случае следствия 2 некоторые значения B_i могут совпадать с соответствующими им A_i.

П р и м е р 3. Пусть требуется найти функцию F, преобразующую векторы:

A_1 = 1011 в вектор B_1 = 1011,

A_2 = 0110 в вектор B_2 = 1101,

A_3 = 1001 в вектор B_3 = 1001.

Здесь векторы $B_1 = A_1$, $B_3 = A_3$, $B_2 \neq A_2$.

Построим часть таблицы истинности функции F.

Пример 3

a	b	c	d	e	g	h	F
			1	0	1	1	1
		1	0	1	1		0
	1	0	1	1			1
1	0	1	1				1
			0	1	1	0	1
		0	1	1	0		1
	0	1	1	0			0
0	1	1	0				1
			1	0	0	1	1
		1	0	0	1		0
	1	0	0	1			0
1	0	0	1				1

Упражнение. Проверьте, что при некотором способе доопределения

$$F = a \vee \rceil b \rceil c \vee bc \vee de.$$

Следствие 3. Если A_i, $i = 1, 2, 3, \ldots, k$ – произвольные двоичные векторы, не связанные сдвигом, то существует одна булева функция F, преобразующая A_1 в любой вектор A_i , т. е. $A_2 = F(A_1)$, $A_3 = F(A_2)$, …, $A_k = F(A_{k-1})$ и $A_1 = F(A_k)$.

П р и м е р 4. Пусть требуется найти булеву функцию F, обеспечивающую следующие преобразования: $A_1 \to A_2 \to A_3 \to A_1$, где A_1 = 1101, A_2 = 0110, A_3 = 1001.

Упражнение. Используя описанную выше методику, выпишите часть таблицы истинности, постройте диаграмму Вейча и найдите один из вариантов решения.

Пример 4

a	b	c	d	e	g	h	F
			1	1	0	1	0
		1	1	0	1		1
	1	1	0	1			1
1	1	0	1				0
			0	1	1	0	1
		0	1	1	0		0
	0	1	1	0			0
0	1	1	0				1
			1	0	0	1	1
		1	0	0	1		1
	1	0	0	1			0
1	0	0	1				1

Таблица истинности этой функции будет иметь следующий вид.

Одно из возможных решений

$$F = a \rceil b \vee g \vee bc \vee \rceil eh.$$

Представляет интерес определение количества наборов длины n, не связанных сдвигом, и их доли в общем числе двоичных наборов длины n.

Расчет произведем для наборов длины n веса q (т. е. содержащих ровно q единиц). Для этого заметим, что если в младшем разряде поставить 1, а остальные $q - 1$ единиц на оставшихся $n - 1$ позициях расставить так, чтобы получить разные двоичные коды, то мы получим все наборы, не связанные сдвигом, содержащие ровно q единиц. Тогда число таких наборов

$$S(n,\ q) = P(n-q,\ q-1) = C_{n-1}^{q-1}.$$

Поскольку общее число наборов длины n веса q равно C_n^q, то доля наборов, не связанных сдвигом, составляет q/n. Так, например, при $n = 20$, $q = 10$ $S(20, 10) = 92378$.

2.3. Минимизация слабо определенных булевых функций

Возьмем теперь произвольный вектор А (1 0 0 1 1 1 0 1 0 0 0 1) и некоторую функцию $F = a_i \,\&\, a_{i-3} \vee a_{i+2} \oplus a_{i+5}$. Применив преобразование F к вектору А, получим вектор В (1 1 0 1 0 1 1 1 0 1 0 0). Для того чтобы найти функцию, которая по вектору В восстанавливала бы вектор А, можно построить таблицу истинности частично определенной функции 23 аргументов (табл. 6.).

Если из данной матрицы выделить минимальный набор столбцов так, чтобы в матрице, построенной только из этих столбцов, строки, на которых элементы вектора А принимают значение 1, отличались бы от строк, на которых элементы вектора А принимают значение 0, то выделенные столбцы будут составлять минимальный набор аргументов функции F.

Обратная к F функция, которая восстанавливает вектор А по вектору В, определена всего на 12 наборах аргументов, а на $N = 2^{23} - 12$

Таблица 6

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	A
											1	1	0	1	0	1	1	1	0	1	0	0	1
										1	1	0	1	0	1	1	1	0	1	0	0		0
									1	1	0	1	0	1	1	1	0	1	0	0			0
								1	1	0	1	0	1	1	1	0	1	0	0				1
							1	1	0	1	0	1	1	1	0	1	0	0					1
						1	1	0	1	0	1	1	1	0	1	0	0						1
					1	1	0	1	0	1	1	1	0	1	0	0							0
				1	1	0	1	0	1	1	1	0	1	0	0								1
			1	1	0	1	0	1	1	1	0	1	0	0									0
		1	1	0	1	0	1	1	1	0	1	0	0										0
	1	1	0	1	0	1	1	1	0	1	0	0											0
1	1	0	1	0	1	1	1	0	1	0	0												1

наборах не определена. Следовательно, ее можно доопределить 2^N способами. Это число настолько велико, что задачу однозначного нахождения обратной к F функции можно считать нереальной.

2.4. Использование булевых преобразований двоичных последовательностей в криптографии

Поскольку преобразование F является односторонней функцией и нахождение обратной функции неоднозначно, можно использовать эти преобразования в криптографии.

1. A и B знают булеву функцию F. A передает B некоторую последовательность A_1, и оба вырабатывают общий ключ $K_1 = F(A_1) = A_2$, который после однократного применения уничтожается. Затем с помощью этой же функции F A и B вырабатывают новый ключ $K_2 = F(A_2) = F(F(A_1))$ и т. д. Последовательность A_1 может формироваться в соответствии с алгоритмом RSA или быть стандартной, например, 101010101010101…, и в этом случае вообще не передаваться по открытому каналу. Периодически исходная последовательность A_1 может меняться. Одноразовые ключи могут использоваться в системе DES или анологичной системе (следствие 3).

2. Булевы преобразования могут использоваться для проверки пароля. Так, если A отправляет B запрос A_1, а B отвечает на него $B_1 = F(A_1)$, то активный перехватчик, даже зная A_1 и B_1, не может однозначно восстановить функцию F, поэтому, маскируясь под “своего”, на другой запрос A_2 ответит результатом преобразования другой функцией $F^{/}(A_2) \neq F(A_2)$ (теорема).

3. Каждый клиент банка снабжен набором паролей. Подписывая свое сообщение любым из них, клиент может быть уверен, что банк определит, от кого пришло сообщение (следствие 2).

4. При заключении контракта по электронной почте отправитель сообщения может ставить под ним различные подписи. Перехватчику при этом трудно отследить автора сообщения. Однако, как получающая сторона, так и арбитр (зная функцию F) сумеют доказать, кто подписывал контракт.

5. Функция F может быть выбрана так, чтобы изменять только некоторые фрагменты текста, например, даты, суммы платежа, шифры, пароли, оставляя текст осмысленным. При обработке всего сообщения функцией F получатель имеет истинный текст, а осмысленность его

вводит перехватчика в заблуждение. При попытке активного перехватчика исказить некоторые фрагменты текста осмысленность сообщения может быть потеряна, и тогда получатель будет знать, что вмешался активный перехватчик (следствие 2, пример 3).

Важно определить класс нетривиальных функций F, при которых уравнение $F(\mathrm{X}) = \mathrm{B}$ разрешимо относительно вектора X ($x_1, x_2, \ldots, x_n$) при любых значениях элементов вектора B ($b_1, b_2, \ldots, b_n$). Снабдив такой функцией F официального получателя сообщений, можно по исходному тексту B_1, B_2, B_3,… вычислять криптотекст X_1, X_2, X_3,…, который и передавать по открытому каналу. Официальный получатель, используя функцию F, восстановит исходное сообщение, так как $\mathrm{B}_1 = F(\mathrm{X}_1)$, $\mathrm{B}_2 = F(\mathrm{X}_2)$, $\mathrm{B}_3 = F(\mathrm{X}_3)$…

В качестве примера такой функции F для 6-разрядных произвольных векторов B ($b_1, b_2, \ldots, b_6$) можно взять функцию $F = \overline{a_{i-2}}\,\overline{a_{i+4}} \oplus \overline{a_{i-4}}\,\overline{a_{i+3}}$. Значения элементов вектора X для этой функции определятся следующим образом:

$$
\begin{aligned}
x_1 &= b_1 \oplus b_2 \oplus b_3 \oplus b_4 \oplus b_6,\\
x_2 &= b_4,\\
x_3 &= b_1 \oplus b_2 \oplus b_3 \oplus b_4 \oplus b_5 \oplus b_6,\\
x_4 &= b_4 \oplus b_6,\\
x_5 &= b_1 \oplus b_4 \oplus b_6,\\
x_6 &= b_1 \oplus b_2 \oplus b_4 \oplus b_6.
\end{aligned}
$$

Для 10-разрядных векторов можно взять функцию $F = a_i \oplus \overline{a_{i\text{-}6}}\;\overline{a_{i+5}}$. В этом случае элементы вектора X будут вычисляться следующим образом:

$$
\begin{aligned}
x_1 &= b_1 \oplus b_6,\\
x_2 &= b_1 \oplus b_2 \oplus b_6 \oplus b_7,\\
x_3 &= b_1 \oplus b_2 \oplus b_3 \oplus b_6 \oplus b_7 \oplus b_8,\\
x_4 &= b_1 \oplus b_2 \oplus b_3 \oplus b_4 \oplus b_6 \oplus b_7 \oplus b_8 \oplus b_9,\\
x_5 &= b_1 \oplus b_2 \oplus b_3 \oplus b_4 \oplus b_5 \oplus b_6 \oplus b_7 \oplus b_8 \oplus b_9 \oplus b_{10},\\
x_6 &= b_6 \oplus 1,\\
x_7 &= b_1 \oplus b_6 \oplus b_7 \oplus 1,\\
x_8 &= b_1 \oplus b_2 \oplus b_6 \oplus b_7 \oplus b_8 \oplus 1,\\
x_9 &= b_1 \oplus b_2 \oplus b_3 \oplus b_6 \oplus b_7 \oplus b_8 \oplus b_9 \oplus b_{10} \oplus 1,\\
x_{10} &= b_1 \oplus b_2 \oplus b_3 \oplus b_4 \oplus b_6 \oplus b_7 \oplus b_8 \oplus b_9 \oplus b_{10} \oplus 1.
\end{aligned}
$$

Если исходный текст состоит из последовательности векторов B_i, например, $\mathrm{B}_1 = 1011100011$; $\mathrm{B}_2 = 1111111111$; $\mathrm{B}_3 = 0111100011$;

B_4 = 0000000000; B_5 = 1011011100; B_6 = 0110001011 ; тогда отправитель сообщений может вычислить соответствующие векторы X_i криптотекста и передать их по открытому каналу: X_1 = 1100010000; X_2 = 0000000000; X_3 = 0100011000; X_4 = 0000011111; X_5 = 0110000101; X_6 = 0010110110.

Получатель сообщения с помощью функции $F = a_i \oplus \overline{a_{i-6}}\ \overline{a_{i+5}}$ преобразует векторы X_i в векторы открытого текста B_i.

Нелегальный перехватчик сообщения, даже зная пары B_i и X_i , не сможет восстановить функцию *F*.

Заключение

В пособии в краткой форме изложены методы анализа и синтеза комбинационных схем на основе свойств булевых функций. Рассмотрен метод минимизации как полностью определенных, так и частично определенных булевых функций с использованием диаграмм Вейча.

Показано, что диаграммы Вейча можно применять и для упрощения произвольных булевых выражений. К сожалению, этот метод имеет существенные ограничения: он может применяться к функциям, число аргументов которых не превышает 10–11.

Рассмотрена задача преобразования произвольных двоичных последовательностей булевыми функциями. Доказана теорема, позволяющая по любым двум произвольным последовательностям находить булево выражение, связывающее эти последовательности.

С помощью приведенной теоремы автором была получена функция, которая для конкретного набора изображений выполняла преобразование, обратное известной функции Конвея. С помощью этой функции из “лапки”, через “улыбку” и все промежуточные двоичные картины восстанавливалось изображение “Чеширского кота”.

Высказаны некоторые соображения по применению булевых преобразований двоичных последовательностей для защиты информации в компьютерных сетях.

Оглавление

Учебное издание

Ерош Игорь Львович

ДИСКРЕТНАЯ МАТЕМАТИКА

БУЛЕВА АЛГЕБРА, КОМБИНАЦИОННЫЕ СХЕМЫ, ПРЕОБРАЗОВАНИЯ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Учебное пособие

Редактор *А. Г. Ларионова*
Компьютерная верстка *Ю. С. Бардуковой*

Лицензия ЛР № 020341 от 07.05.97. Сдано в набор 27.04.01. Подписано к печати 25.05.01 Формат 60×84 1/16. Бумага тип. № 3. Печать офсетная. Усл. печ. л. 1,7. Усл. кр.-отт. 1,8. Уч. -изд. л. 1,9. Тираж 100 экз. Заказ №

Редакционно-издательский отдел
Лаборатория компьютерно-издательских технологий
Отдел оперативной полиграфии
СПбГУАП
190000, Санкт-Петербург, ул. Б. Морская, 67