Кушнир Д. В.
Пестов И. Е.
Шемякин С. Н.

Булевы функции в криптографии. Основы теории

Министерство цифрового развития, связи и массовых коммуникаций
Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования «Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М. А. Бонч-Бруевича»
(СПбГУТ)

Д. В. Кушнир, И. Е. Пестов, С. Н. Шемякин

БУЛЕВЫ ФУНКЦИИ В КРИПТОГРАФИИ

ОСНОВЫ ТЕОРИИ

Учебное пособие

Электронное издание
локального распространения

Санкт-Петербург
Наукоемкие технологии
2025

© Кушнир Д. В., Пестов И. Е.,
Шемякин С. Н., 2025
© Санкт-Петербургский государственный
университет телекоммуникаций им. проф.
М. А. Бонч-Бруевича, 2025
ISBN 978-5-00271-138-3

УДК 519.7(075.8)
ББК 22.18я73
К96

Рецензенты:
А. А. Миняев, кандидат технических наук, руководитель Центра информационной безопасности ООО «Диджиталь»;
Д. В. Окунева, кандидат технических наук, декан факультета ИКСС, доцент кафедры ПИиВТ, преподаватель базовой кафедры КБП

К96 **Кушнир, Д. В.**
Булевы функции в криптографии. Основы теории [Электронный ресурс]: учебное пособие / Д. В. Кушнир, И. Е. Пестов, С. Н. Шемякин, СПбГУТ. – Электрон, текстовые дан. (2,7 Мб). – СПб.: Наукоемкие технологии, 2025. – 94 с. – 1 электрон., опт. диск (CD-ROM).

ISBN 978-5-00271-138-3

Рассматриваются основы теории булевых функций. Вводятся основные понятия и инструменты для изучения свойств двоичных преобразований. Исследуются способы построения и задания функций, вопросы, связанные с такими понятиями, как статистическая независимость и корреляционная иммунность, нелинейность булевых функций и лавинные характеристики. Обсуждается связь свойств булевых функций со стойкостью большого спектра криптографических преобразований.

Предназначено для студентов, обучающихся по направлениям подготовки 10.04.01 «Информационная безопасность», 10.05.02 «Информационная безопасность телекоммуникационных систем».

Утверждено редакционно-издательским советом СПбГУТ в качестве учебного пособия (Протокол № 5 от 06.03.2025)

Текстовое электронное издание
Минимальные системные требования:
– процессор: Intel x86, x64, AMD x86, x64 не менее 1 ГГц;
– оперативная память RAM ОЗУ: не менее 512 МБайт;
– свободное место на жестком диске (HDD): не менее 120 МБайт;
– операционная система: Windows XP и выше;
– Adobe Acrobat Reader;
– дисковод CD-ROM;
– мышь.

УДК 519.7(075.8)
ББК 22.18я73

© Кушнир Д. В., Пестов И. Е., Шемякин С. Н., 2025
© Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2025

ISBN 978-5-00271-138-3

Учебное издание

Кушнир Дмитрий Викторович
Пестов Игорь Евгеньевич
Шемякин Сергей Николаевич

Булевы функции в криптографии
Основы теории

Учебное пособие

Электронное издание
локального распространения

Редактор *Л. К. Паршина*
Корректор *Е. А. Матюшкина*
Компьютерная верстка *С. Н. Скляровой*
Главный редактор *В. М. Коровин*

Издательство «Наукоемкие технологии»
ООО «Корпорация «Интел Групп»
https://publishing.intelgr.com
E-mail: publishing@intelgr.com
Тел.: +7 (812) 945-50-63
Интернет-магазин издательства
https://shop.intelgr.com/

Подписано к использованию 06.03.2025 г.
Объем издания – 2,7 Мб.
Комплектация издания – 1 CD.
Тираж 20 CD.

ISBN 978-5-00271-138-3



СОДЕРЖАНИЕ

ОСНОВНЫЕ ОБОЗНАЧЕНИЯ 5

ПРЕДИСЛОВИЕ 7

1. АЛГЕБРА ЛОГИКИ 8
   1.1. Элементарные функции алгебры логики 9
   1.2. Совершенная дизъюнктивная нормальная форма 10
   1.3. Свойства булевых операций 12

2. АЛГЕБРА ДИСКРЕТНЫХ ФУНКЦИЙ 15
   2.1. Вес функции 16
   2.2. Алгебраическая нормальная форма дискретной функции 18
   2.3. Линейные функции и переменные 24

3. КОРРЕЛЯЦИОННАЯ ИММУННОСТЬ 29
   3.1. Основные определения 29
   3.2. Свойства корреляционной иммунности 30
   3.3. Неравенство Зигенталера 33

4. ПРЕДСТАВЛЕНИЕ БУЛЕВЫХ ФУНКЦИЙ В БАЗИСАХ ФУНКЦИОНАЛЬНЫХ ПРОСТРАНСТВ 35
   4.1. Преобразование Фурье 38
   4.2. Преобразование Уолша – Адамара 40
   4.3. Свойства преобразования Уолша – Адамара 42
   4.4. Статистическая структура 46
   4.5. Матрицы в представлениях булевых функций 49

5. КРИТЕРИИ СТАТИСТИЧЕСКОЙ НЕЗАВИСИМОСТИ И КОРРЕЛЯЦИОННОЙ ИММУННОСТИ 54
   5.1. Статистическая независимость 54
   5.2. Статистическая независимость суперпозиции функций 56
   5.3. Необходимые условия корреляционной иммунности 59

6. НЕЛИНЕЙНОСТЬ БУЛЕВЫХ ФУНКЦИЙ 60
   6.1. Основные свойства нелинейности 62
   6.2. Максимально нелинейные (бент-) функции и их свойства 63
   6.3. Совершенная нелинейность 68
   6.4. Нелинейность и корреляционная иммунность 73

7. ЛАВИННЫЕ ХАРАКТЕРИСТИКИ БУЛЕВЫХ ФУНКЦИЙ 79
   7.1. Автокорреляция и взаимная корреляция 79
   7.2. Строгий лавинный критерий 81
   7.3. Критерий распространения 84
   7.4. Глобальные лавинные характеристики 86
   7.5. Частичные бент-функции 88

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 92

ОСНОВНЫЕ ОБОЗНАЧЕНИЯ

$\mathbb{N}$ – множество натуральных чисел
$\mathbb{Z}$ – кольцо целых чисел
$\mathbb{C}$ – поле комплексных чисел
$\mathbb{Q}$ – поле рациональных чисел
$\mathbb{Z}_2 = \{0,1\}$ – множество из двух чисел
$\mathbb{Z}_k$ – кольцо классов вычетов по модулю k
$\mathbb{Z}_2^n$ – множество двоичных векторов длины n
$\mathbb{Z}_k^n$ – множество векторов длины n с компонентами из $\mathbb{Z}_k$
АНФ$_f$ – коэффициенты алгебраической нормальной формы (полинома Жегалкина) булевой функции $f(\boldsymbol{x})$
$K_{m,\,m}$ – множество матриц размера $m \times m$ над некоторым полем K
$(\mathbb{C},\ \cdot)$ – мультипликативная группа поля комплексных чисел
$\boldsymbol{\Omega}$ = {да, нет} – множество-носитель булевой алгебры логических функций
Ω_2^n – множество векторов длины n из логических переменных
$\mathrm{cor}(\boldsymbol{f})$ – максимальный порядок корреляционной иммунности функции f
$\deg(\boldsymbol{f})$ – степень АНФ функции f; алгебраическая нелинейность
$\mathrm{dist}(\boldsymbol{x}, \boldsymbol{y})$ – Хеммингово расстояние между векторами, число несовпадающих компонент у двоичных векторов
sut (f) – максимальный порядок устойчивости функции f
wt ($\boldsymbol{a}$) – вес двоичного вектора $\boldsymbol{a}$, число единиц у вектора $\boldsymbol{a}$
$x \in \mathbb{Z}_2, \Omega$ – переменная скалярная
$\boldsymbol{x} \in \mathbb{Z}_2^n$ – переменная вектор
$\mathbf{0}$ – вектор из нулей
$\mathbf{1}$ – вектор из единиц
$\boldsymbol{f}$ – вектор значений функции $f(\boldsymbol{x})$, строка истинности функции
$f(\boldsymbol{x})$ – булева функция f: $\mathbb{Z}_2^n \to \mathbb{Z}_2$
f^b – подфункция исходной функции f
$F(\boldsymbol{x})$ – функция $f(\boldsymbol{x})$ в характеристическом представлении
$\boldsymbol{F_f}$ – вектор значений характеристического представления булевой функции
$\boldsymbol{F_a}$ – вектор значений характеристического представления линейной функции с задающим вектором $\boldsymbol{a}$
X – дискретная случайная величина
U – пространство значений случайной величины X
Z – дискретная случайная величина
V – пространство значений случайной величины Z
$\mathcal{A}(n)$ – множество всех аффинных функций в $P_2(n)$
$\mathcal{B}(n)$ – множество всех бент-функций, множество максимально нелинейных функций в $P_2(n)$
$\mathcal{L}(n)$ – множество всех линейных функций в $P_2(n)$
$\mathcal{LS}(n)$ – множество функций с линейной структурой от n переменных

$GF\,(2)$ – простое поле Галуа, результат сложения и умножения приводится по модулю 2

$GF\,(2^n)$ – расширение поля Галуа; линейное пространство над двоичным полем, размерности n

$P_2(n)$ – множество всех булевых функций от n двоичных переменных

$P\{A\}$ – вероятность события A

SAC – строгий лавинный критерий

$l_a(\boldsymbol{x})$ – линейная функция на задающем векторе $\boldsymbol{a}$, $l_a(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x})$

$\boldsymbol{l_a}$ – вектор истинности (вектор значений) линейной функции

$(\boldsymbol{a}, \boldsymbol{x})$ – скалярное произведение двоичных векторов в двоичном поле

$\langle \boldsymbol{a}, \boldsymbol{x} \rangle$ – скалярное произведение в арифметике целых чисел, результат – целое число

$H(X)$ – энтропия случайной величины X

$H(X|Z)$ – условная энтропия случайной величины X относительно случайной величины Z

$I(X, Z)$ – взаимная информация X и Z

C_f – спектр преобразования Фурье

CN_f – совершенная нелинейность булевой функции

S_f – спектр статистической структуры

W_f – спектр преобразования Уолша; функция Уолша, определенная на f; одно из представлений булевой функции $f(\boldsymbol{x})$

$W_f(\boldsymbol{a})$ – значение коэффициента преобразования Уолша на задающем векторе $\boldsymbol{a}$ линейной функции $l_{\boldsymbol{a}}(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x})$; значение целочисленное

Nl_f, $Nl(f)$ – нелинейность функции $f(\boldsymbol{x})$; значение целочисленное

$(P_2, \cup, \&, \neg)$ – булева алгебра логических функций

$(P_2, \cdot, \oplus)$ – булева алгебра дискретных функций

$\| \boldsymbol{a} \|$ – норма вектора $\boldsymbol{a}$ или вес двоичного вектора $\boldsymbol{a}$

$\rho\,(\boldsymbol{x}, \boldsymbol{y})$ – метрика линейного пространства; Хеммингово расстояние между булевыми векторами, количество несовпадающих компонент у векторов $\boldsymbol{x}$, $\boldsymbol{y}$

$\delta(x, y)$ – дельта-функция; равна 1 при $x = y$, нулю при неравных x, y

δ_p – перекос вероятностей

σ_f – глобальная лавинная характеристика булевой функции, сумма квадратов

Δ_f – глобальная лавинная характеристика булевой функции, абсолютный показатель

μ_f, $\mu(f)$ – преобразование Мёбиуса

$\mu_f(\boldsymbol{a})$ – значение преобразования Мёбиуса функции $f(\boldsymbol{x})$ на векторе $\boldsymbol{a}$

$\Phi_{n,m}(\boldsymbol{x})$ – булево отображение $\Phi_{n,m}$: $Z_2^n \to Z_2^m$;

$\forall\, x$ – квантор всеобщности для высказывания; для всех x выполняется …

$\oplus$ – сложение по модулю два

$\otimes$ – тензорное произведение матриц

■ – завершение доказательства

Если читаешь учебник и ничего не понятно –
это дискретная математика

Фольклор студентов
МГТУ им. Н. Э. Баумана

ПРЕДИСЛОВИЕ

Существенно важная роль булевых функций в криптографии определяется использованием их в шифрах гаммирования и в блочных шифрах. Генераторы псевдослучайных последовательностей в шифрах гаммирования используют булевы функции – как фильтрующие, так и комбинационные. Основная цель – повышение линейной сложности последовательности на выходе генератора. В блочных шифрах булевы функции используются для реализации отображений в блоках замены.

Оказалось, что для обеспечения достаточной стойкости шифров к различным видам криптографического анализа применяемые булевы функции должны обладать определенным множеством свойств. В настоящее время список этих свойств не завершен. Требования, предъявляемые к функциям, зачастую оказываются противоречивыми, поэтому при поиске подходящей функции возникает задача многокритериальной оптимизации на дискретных множествах. Данная задача общего решения не имеет, приходится часть параметров ограничивать.

В числе некоторых свойств функций укажем следующие:

– уравновешенность;
– отсутствие фиктивных переменных;
– высокая алгебраическая нелинейность;
– высокая нелинейность в метрике Хемминга;
– отсутствие корреляции значений функции со значениями аргументов;
– отсутствие запретов;
– выполнение критериев распространения;
– ограничения на лавинные характеристики.

Булеву функцию с указанными свойствами можно назвать криптографической.

Данное пособие заведомо не является полным, кроме того, предполагается знакомство с основами криптографии, например, [1, 5, 8] и с основами функционального анализа.

Изложение материала соответствуют [3, 7, 10, 11, 12, 8], источники указаны в порядке значимости. Следует указать, что понятия, термины и обозначения в общедоступной литературе не устоялись, поэтому используемые в пособии определения не всегда совпадают с таковыми в указанных источниках. Обозначения использованы в основном согласно [10, 14], но вместе с тем сделана попытка вернуться хотя бы частично к стандартным математическим терминам и обозначениям вместо специфических, которые были определены в работах по данной области дискретной математики.

1. АЛГЕБРА ЛОГИКИ

Здесь приведены некоторые сведения из указанного раздела дискретной математики. Более подробное изложение можно найти в [4, 15, 6].

Зададим множество Ω из двух элементов. Существующие имена одного из элементов: 0, нет, ложно, Л, False; другого: 1, да, истина, И, True. Общее имя переменных и выражений в алгебре логики – высказывание, которое принимает значение на множестве Ω. Высказывание может быть только истинным или только ложным, оба значения одновременно оно принимать не может. Определим Ω как множество из элементов $\{0, 1\}$. Множество Ω и возможные действия на данном множестве называется *алгеброй логики, алгеброй высказываний*. Действия в алгебре логики задаются *функциями алгебры логики* или *логическими функциями*. Формально функция есть отображение $f(x_1, x_2, \ldots, x_n)$, $x_i \in \Omega$:

$$\boldsymbol{f}: \Omega^n \rightarrow \Omega\,.$$

Обозначим множество всех логических функций как P_2, а множество всех логических функций от n переменных как $P_2(n)$. Таким образом, алгебра логики есть множество Ω с заданными на нем логическими функциями.

Любая логическая функция от n переменных стандартно имеет *табличное представление*. Рассмотрим табл. 1.1, которая задает функцию от трех переменных.

Таблица 1.1

x_1	x_2	x_3	f
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Наборы переменных в аргументе функции перечислены в лексикографическом порядке; он совпадает с порядком возрастания наборов, представленных в двоичном виде. Тогда логическая функция полностью определяется вектор-столбцом длины 2^n значений функции. Поэтому число $|P_2(n)|$ различных функций от n переменных равно 2^{2^n}.

Вектор значений или *строка значений* или *вектор истинности* или *строка истинности* функции обычно записывается в виде вектор-строки. Вектор значений функции $f(\boldsymbol{x})$ из табл. 1.1 в двоичной и шестнадцатеричной записи имеет вид:

$$\boldsymbol{f} = (0\,1\,0\,0\,1\,1\,0\,0)_2 = (4\,\mathrm{C})_{16}.$$

Символ $\boldsymbol{f}$ здесь обозначает вектор, имена векторов записываются полужирным шрифтом. Логическая функция имеет как минимум два представления (способа записи): табличную и строкой истинности.

Переменная x_i функции $f(x_1, \ldots x_{i-1}, x_i, x_{i+1}, \ldots, x_n)$ называется *несущественной*, *фиктивной*, если

$$f(x_1, \ldots x_{i-1}, 0, x_{i+1}, \ldots, x_n) = f(x_1, \ldots x_{i-1}, 1, x_{i+1}, \ldots, x_n)$$

для любых значений переменных $x_1, \ldots x_{i-1}, x_{i+1}, \ldots, x_n$.

Функции, различающиеся только несущественными переменными и совпадающие на значениях существенных переменных, будем считать равными.

Для криптографических булевых функций условие существенности всех переменных является необходимым.

1.1. Элементарные функции алгебры логики

Логических функций от одной переменной существует всего четыре (табл. 1.2).

Таблица 1.2

x	φ_0	φ_1	φ_2	φ_3
0	0	0	1	1
1	0	1	0	1

1) $\varphi_0(x) = 0$ – константа 0;

2) $\varphi_3(x) = 1$ – константа 1;

3) $\varphi_1(x) = x$ – *тождественная функция x*; *повторение x*;

4) $\varphi_2(x) = \neg x = \overline{x}$ = **НЕ** *x* – *отрицание x*;

Всего существует 16 логических функций от двух переменных, которые приведены в табл. 1.3.

Таблица 1.3

x_1	x_2	ψ_0	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5	ψ_6	ψ_7	ψ_8	ψ_9	ψ_{10}	ψ_{11}	ψ_{12}	ψ_{13}	ψ_{14}	ψ_{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

1) $\psi_1(x_1, x_2) = x_1 \cdot x_2 = x_1x_2 = x_1 \,\&\, x_2 = x_1 \wedge x_2 = x_1 \cap x_2$ – *конъюнкция* x_1 и x_2; *логическое умножение*; функция **И**;

2) $\psi_7(x_1, x_2) = x_1 \vee x_2 = x_1 \cup x_2$ – *дизъюнкция* x_1 и x_2; *логическое сложение*; функция **ИЛИ**;

3) $\psi_6(x_1, x_2) = x_1 \oplus x_2 = x_1 + x_2 \bmod 2$ – *сложение по модулю* 2, *неравнозначность*;

4) $\psi_8(x_1, x_2) = x_1 \downarrow x_2$ – стрелка Пирса;

5) $\psi_9(x_1, x_2) = (x_1 \sim x_2) = (x_1 \equiv x_2)$ – *эквивалентность, равнозначность*;

6) $\psi_{13}(x_1, x_2) = x_1 \rightarrow x_2$ – *импликация* x_1 и x_2; из x_1 следует x_2; если x_1, то x_2, *логическое следование*;

7) $\psi_{14}(x_1, x_2) = x_1 \,/\, x_2 = x_1 \mid x_2$ – штрих Шеффера.

Остальные функции названий не имеют. Из шестнадцати функций от двух переменных шесть функций имеют несущественные переменные.

1.2. Совершенная дизъюнктивная нормальная форма

Любая логическая функция $f(\boldsymbol{x})$ может быть представлена суперпозицией дизъюнкций, конъюнкций и отрицаний. Другими словами, данные элементарные функции образуют *полную систему функций*. В свое время такой выбор определился особенностями существующей в тот момент элементной базы для устройств управления и автоматического регулирования.

Обозначим $x^\sigma = \overline{x}$ при $\sigma = 0$ – отрицание; $x^\sigma = x$ при $\sigma = 1$ – повторение. При различных значениях переменных в выражении, т. е. $x \neq \sigma$, получим, что $x^\sigma = 0$; при равных значениях получаем $x^\sigma = 1$.

Ясно, что для произвольной булевой функции верно разложение Шеннона:

$$f(x_1, x_2, \dots, x_n) = \overline{x}_1 f(0, x_2, \dots, x_n) \cup x_1 f(1, x_2, \dots, x_n).$$

Рассмотрим следующую теорему о разложении произвольной булевой функции по переменным.

Теорема 1.1. Любая логическая функция $f(x_1, \dots, x_n)$ может быть представлена в виде:

$$f(x_1, \dots, x_m, x_{m+1}, \dots, x_n) = \cup x_1^{\sigma_1} \ \dots \ x_m^{\sigma_m} f(\sigma_1, \dots, \sigma_m, x_{m+1}, \dots, x_n), \quad (1.1)$$

где дизъюнкция берется по всем 2^m наборам значений переменных $x_1, \dots, x_m$.

Представление булевой функции в виде выражения (1.1) называется *разложением по переменным* $x_1, \dots, x_m$.

Пример 1.1

Пусть $n = 4$, $m = 2$; тогда

$$f(x_1, x_2, x_3, x_4) = \overline{x_1 x_2} f(0, 0, x_3, x_4) \cup \overline{x_1} x_2 f(0, 1, x_3, x_4) \cup \\ \cup x_1 \overline{x_2} f(1, 0, x_3, x_4) \cup x_1 x_2 f(1, 1, x_3, x_4).$$

Важным случаем является разложение по всем n переменным. Все переменные в правой части выражения (1.1) принимают фиксированные значения, функции в конъюнкциях становятся равными 0 или 1. Это приводит к следующему выражению:

$$f(x_1, \dots, x_n) = \cup x_1^{\sigma_1} \ \dots \ x_n^{\sigma_n}.$$

Дизъюнкция берется по всем наборам $(\sigma_1, \dots, \sigma_n)$, где $f(\sigma_1, \dots, \sigma_n) = 1$. Данное представление называется *совершенной дизъюнктивной нормальной формой* (СДНФ) функции $f(\boldsymbol{x})$.

СДНФ функции $f(\boldsymbol{x})$ содержит столько конъюнкций, сколько единичных значений в таблице истинности функции. Каждому значению функции, равному единице, соответствует набор $(\sigma_1, \dots, \sigma_n)$. В конъюнкции переменных x_i переменную выписываем с отрицанием, если $\sigma_i = 0$, и без отрицания, если $\sigma_i = 1$.

Пример 1.2

СДНФ функции, определенной в табл. 1.1, имеет вид:

$$f(x_1, x_2, x_3) = \overline{x_1 x_2} x_3 \cup x_1 \overline{x_2 x_3} \cup x_1 \overline{x_2} x_3.$$

Единственной функцией, которая не может быть представлена в форме СДНФ, является константа 0. Она может быть записана в виде $0 = x\overline{x}$.

Алгебра (P_2, $\cup$, &, $\neg$), где основным множеством является все множество булевых функция, а операциями – дизъюнкция, конъюнкция и отрицание, называется *булевой алгеброй логических функций*.

Следует помнить, что любую функцию можно записать бесконечным множеством формул. Фактически мы рассматриваем не сами функции, а их

представление в виде тех или иных формул. Возникает понятие классов формул, реализующих в одном классе одну функцию. Алгебра классов формул оказывается изоморфной булевой алгебре, путаница между понятиями функции и формулы, изоморфными булевыми алгебрами в таком случае оказывается вполне естественной.

1.3. Свойства булевых операций

Ассоциативность:

$x_1 (x_2 x_3) = (x_1 x_2) x_3$;
$(x_1 \vee x_2) \vee x_3 = x_1 \vee (x_2 \vee x_3)$.

Коммутативность:

$x_1 x_2 = x_2 x_1$;
$x_1 \vee x_2 = x_2 \vee x_1$.

Дистрибутивность конъюнкции относительно дизъюнкции:

$x_1(x_2 \vee x_3) = x_1 x_2 \vee x_1 x_3$.

Дистрибутивность дизъюнкции относительно конъюнкции:

$x_1 \vee (x_2 x_3) = (x_1 \vee x_2)(x_1 \vee x_3)$.

Идемпотентность:

$xx = x$;
$x \vee x = x$.

Двойное отрицание:

$\bar{\bar{x}} = x$.

Свойства констант:

$x \,\&\, 1 = x$; $\quad x \,\&\, 0 = 0$;
$x \vee 1 = 1$; $\quad x \vee 0 = x$;
$\overline{0} = 1$; $\quad \overline{1} = 0$.

Правила де Моргана:

$\overline{x_1 \,\&\, x_2} = \overline{x}_1 \vee \overline{x}_2$;
$\overline{x_1 \vee x_2} = \overline{x}_1 \,\&\, \overline{x}_2$.

Закон противоречия:

$x\overline{x} = 0$.

Закон исключенного третьего:

$x \vee \overline{x} = 1$.

Следующую группу формул называют эквивалентными преобразованиями. Основное их назначение – получение формул с меньшим числом символов, т. е. в итоге уменьшение числа элементов в схеме и упрощение связей в устройстве управления.

Элементарное поглощение:

$x \vee xy = x$;
$x(x \vee y) = x$.

Элементарное склеивание:

$xy \vee \overline{y} = x$.

Обобщенное склеивание:

$xz \vee y\overline{z} \vee xy = xz \vee y\overline{z}$.

Прочие равносильности:

$x \vee \overline{x}y = x \vee y$;
$x \oplus y = \overline{x}y \vee x\overline{y}$;
$x \to y = \overline{x} \vee y$;
$x \sim y = \overline{xy} \vee xy$;
$x \downarrow y = \overline{x} \cdot \overline{y}$;
$x / y = \overline{x} \vee \overline{y}$.

Контрольные вопросы и задания

1. Доказать, что булева функция f линейна, если и только если $f(x \oplus y) = f(x) \oplus f(y)$ для всех x, y.

2. Построить таблицу истинности, найти СДНФ следующих функций:

а) $x_1 \vee x_2 \vee x_3$;

б) $x_1 \sim x_2$;

в) $x_1x_2x_3$;

г) $(x_1 \sim x_2) \sim x_3$;

д) $(x_1 \vee x_2)\, x_3 \to x_2$.

Вариант: № по списку в группе $(\mathrm{mod}\ 5) + 1$.

3. Найти длину, вес и десятичное представление набора (1101) $\oplus$ № по списку в группе.

4. Найти расстояние Хемминга между вершинами α = (1010) и β = № по списку в группе в кубе B^4. Определить, являются ли эти наборы противоположными или соседними.

5. Перечислить все фиктивные и существенные переменные функции, заданной вектором истинности из 8 бит, старшие биты нули, 4 последних бита – № по списку в группе.

6. Найти двойственную функцию для $f = x \oplus y$.

2. АЛГЕБРА ДИСКРЕТНЫХ ФУНКЦИЙ

Алгебра (P_2, ∪, &, ¬) – булева алгебра логических функций – алгебра полная, т. е. позволяет представить любую булеву функцию. В работах по криптографии, однако, принято использование другой алгебры: (P_2, · , ⊕). Ее можно назвать *булевой алгеброй дискретных функций*. Множество-носитель, на котором определяются операции вместо, Ω обозначается как $\mathbb{Z}_2$. Здесь $\mathbb{Z}_2$ – множество из двух целых чисел: нуль и единица, $\mathbb{Z}_2 = \{0, 1\}$. Знак (·) – знак умножения, ⊕ – знак суммирования в поле классов вычетов по модулю 2. В современном курсе алгебры (например, [2]) $\mathbb{Z}_2$ называют полем Галуа и обозначают *GF* (2) или $\mathbb{F}_2$.

Множество $\mathbb{Z}_2^n$ является *линейным векторным пространством*, состоящем из *n*-мерных двоичных векторов $\boldsymbol{x}$.

Каждому вектору $\boldsymbol{x} \in \mathbb{Z}_2^n$ можно поставить в соответствие целое неотрицательное число; его называют *нормой* этого элемента и обозначают $\|\boldsymbol{x}\|$. В терминах булевой алгебры это вес вектора. Аксиомы нормы при этом заведомо выполняются [9]. Множество $\mathbb{Z}_2^n$ можно назвать в таком случае *нормированным пространством.*

В этом пространстве можно ввести метрику

$$\rho(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} \oplus \boldsymbol{y}\|.$$

Легко проверить, что определенное таким образом Хеммингово расстояние между элементами пространства $\mathbb{Z}_2^n$ удовлетворяет всем аксиомам метрики. Множество $\mathbb{Z}_2^n$ можно назвать в таком случае *метрическим пространством.* Значение метрики является целым неотрицательным числом, оно показывает, сколько компонент у векторов $\boldsymbol{x}, \boldsymbol{y}$ не совпадают.

Для пары векторов $\boldsymbol{x}, \boldsymbol{y}$ введем еще одну операцию – скалярное произведение:

$$(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{n} x_i y_i \mod 2;$$

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_{i=1}^{n} x_i y_i.$$

Второе скалярное произведение дает результат в целых числах. Теперь множество $\mathbb{Z}_2^n$ можно назвать евклидовым пространством.

В евклидовом пространстве $\mathbb{Z}_2^n$ выражение для нормы вектора можно представить в следующем виде:

$$\|\boldsymbol{x}\| = \langle \boldsymbol{x}, \boldsymbol{x} \rangle.$$

Определение 2.1. Пусть n натуральное число, тогда произвольная функция $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *булевой функцией*.

Определение 2.2. Пусть числа n, m являются натуральными и $n \geq m$. Произвольное отображение $\Phi_{n,m}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ называется *булевым отображением*.

Отображение $\mathbb{Z}_2^n \to \mathbb{Z}_2^m$ однозначно определяется координатными функциями

$$\Phi_{n,m}(\boldsymbol{x}) = (f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), \dots, f_m(\boldsymbol{x})),$$

где $\boldsymbol{x} = (x_1, x_2, \dots, x_n)$ – вектор из n значений входных переменных, а $(f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), \dots, f_m(\boldsymbol{x}))$ – вектор из m значений на выходе отображения $\Phi_{n,m}(\boldsymbol{x})$.

Отличие введенной алгебры дискретных функций от алгебры логических функций заключается в следующем: булевы функции в алгебре дискретных функций определены на числовых переменных, а булевы функции в алгебре логики – на логических переменных (т. е. принимающих значения Ложь или Истина). Кроме того, у них разный состав операций.

Преимуществом введенной алгебры оказалась возможность обнаружения и исследования свойств различных булевых функций, которые влияют на стойкость шифров.

Среди особенностей булевой алгебры дискретных функций над полем $GF(2)$ следует указать:

$0 \oplus 1 = 1$;
$x \cdot 0 = 0$;
$x \cdot x = x$;
$x \oplus x = 0$.

Алгебра дискретных функций полна. Для этого достаточно показать, что функции булевой алгебры логических функций можно представить полиномами:

конъюнкция: $(x\&y) \sim x \cdot y$;
дизъюнкция: $(x \cup y) \sim x \cdot y \oplus x \oplus y$;
отрицание: $(\overline{x}) \sim x \oplus 1$.

2.1. Вес функции

Весом булева вектора $\boldsymbol{a} = (a_1, a_2, \dots, a_n)$, *нормой вектора* $\boldsymbol{a}$ называется количество единичных компонент в нем; известные обозначения – $w(\boldsymbol{a})$, $wt(\boldsymbol{a})$, $\| \boldsymbol{a} \|$. Для вектора $\boldsymbol{a} = (00101)$ вес будет $\| \boldsymbol{a} \| = 2$.

Весом булевой функции $f(\boldsymbol{x})$ называется вес вектора значений функции. Функция в табл. 1.1 имеет вектор значений $\boldsymbol{f} = (4\ \mathrm{C})_{16} = (0\ 1\ 0\ 0\ 1\ 1\ 0\ 0)_2$. Тогда $\|\boldsymbol{f}\| = 3$.

Если $\|\boldsymbol{f}\| = 2^{n-1}$, то функция $f(\boldsymbol{x})$ называется *уравновешенной, равновероятной, устойчивой, сбалансированной.* В двоичной записи вектора $\boldsymbol{f}$ значений функции $f(\boldsymbol{x})$ количество единиц равно количеству нулей. Это значит, что при равновероятном выборе значений аргумента $\boldsymbol{x}$ булевой функции $f(\boldsymbol{x})$ значения функции с равной вероятностью принимают значение нуль и единица. Или другими словами: функция сохраняет равновероятность аргументов. В криптографических приложениях большей частью рассматриваются уравновешенные функции. Поэтому данное свойство булевой функции можно назвать криптографическим.

Утверждение 2.1.

1. $0 \le \|\boldsymbol{f}\| \le 2^n$.
2. $\|\boldsymbol{f} \oplus \boldsymbol{1}\| = 2^n - \|\boldsymbol{f}\|$.
3. $\|\boldsymbol{f} \oplus \boldsymbol{g}\| = \|\boldsymbol{f}\| + \|\boldsymbol{g}\| - 2\langle \boldsymbol{f}, \boldsymbol{g} \rangle$.
4. Пусть y – фиктивная переменная функции $\boldsymbol{g}$, т. е. $g(\boldsymbol{x}, y) = f(\boldsymbol{x})$. Тогда $\|\boldsymbol{g}\| = 2\|\boldsymbol{f}\|$.
5. Пусть $f(\boldsymbol{x}) \in P_2(n)$ и $g(\boldsymbol{y}) \in P_2(m)$ зависят от непересекающихся множеств переменных, $\boldsymbol{x} \cap \boldsymbol{y} = \emptyset$. Тогда:

а) функция $f(\boldsymbol{x}) \cdot g(\boldsymbol{y})$ не уравновешена, если $f(\boldsymbol{x})$ и $g(\boldsymbol{y})$ не константы 1;

б) функция $f(\boldsymbol{x}) \oplus g(\boldsymbol{y})$ уравновешена, тогда и только тогда, когда $f(\boldsymbol{x})$ или $g(\boldsymbol{y})$ уравновешены.

Доказательство.

а) Пусть $\|\boldsymbol{f}\| = r < 2^n$, $\|\boldsymbol{g}\| = s < 2^m$. Так как $f(\boldsymbol{x}) \cdot g(\boldsymbol{y}) = 1$ тогда и только тогда, когда ($f(\boldsymbol{x})$= 1) & ($g(\boldsymbol{y})$ = 1), то $\|\boldsymbol{f} \cdot \boldsymbol{g}\| = rs$.

Предположим, что функция $f \cdot g$ уравновешена, или $2^{n+m-1} = \|\boldsymbol{f} \cdot \boldsymbol{g}\| = rs$. Тогда $r = 2^k$, $s = 2^l$ для некоторых $k \le n - 1$, $l \le m - 1$. Получается, что

$$\|\boldsymbol{f} \cdot \boldsymbol{g}\| \le 2^{n+m-2}.$$

Условие уравновешенности не выполняется. ■

б) Предварительно: $f(\boldsymbol{x}) \oplus g(\boldsymbol{y}) = 1$ тогда и только тогда, когда $f(\boldsymbol{x}) \ne g(\boldsymbol{y})$. Следовательно, $\|\boldsymbol{f} \oplus \boldsymbol{g}\| = \|\boldsymbol{f}\| \cdot \|\bar{\boldsymbol{g}}\| + \|\bar{\boldsymbol{f}}\| \cdot \|\boldsymbol{g}\|$.

Достаточность. Пусть f функция уравновешена, $\|\boldsymbol{f}\| = \|\overline{\boldsymbol{f}}\| = 2^{n-1}$. Тогда получаем, что

$$\|\boldsymbol{f} \oplus \boldsymbol{g}\| = 2^{n-1}2^m = 2^{n+m-1}.$$

Необходимость. Пусть $\|\boldsymbol{f}\| = r$, $r \neq 2^{n-1}$; $\|\boldsymbol{g}\| = s$. Отсюда следует, что

$$\|\boldsymbol{f} \oplus \boldsymbol{g}\| = r(2^m - s) + s(2^n - r) = 2^{n+m-1}.$$

Так как функция $f(\boldsymbol{x}) \oplus g(\boldsymbol{y})$ уравновешена. Тогда выражение для s будет

$$S = \frac{2^{n+m-1} - r\,2^m}{2^n - 2r} = 2^{m-1}.$$

Следовательно, функция $g(\boldsymbol{x})$ уравновешена. ■

2.2. Алгебраическая нормальная форма дискретной функции

С учетом введенных операций можно записать разложение Шеннона в следующем виде:

$$f(\boldsymbol{x}) = (x_1 \oplus 1)f(0, x_2, \dots, x_n) \oplus x_1 f(1, x_2, \dots, x_n).$$

Утверждение 2.2.

Пусть $f(\boldsymbol{x}) \in P_2(n)$, $m \leq n$. Тогда для $\forall\, \boldsymbol{\alpha} \in Z_2^m$ выполняется разложение функции f:

$$f(\boldsymbol{x}) = \bigoplus (x_1 \oplus \alpha_1 \oplus 1) \cdot \dots \cdot$$
$$\cdot \dots \cdot (x_m \oplus \alpha_m \oplus 1) f(\alpha_1, \dots, \alpha_m, x_{m+1}, \dots, x_n). \qquad (2.1)$$

Формула $f(\alpha_1, \dots, \alpha_m, x_{m+1}, \dots, x_n)$ из (2.1) называется *коэффициентом разложения функции* $f(\boldsymbol{x})$ *по переменным* $x_1, \dots, x_m$.

Утверждение 2.3.

Пусть $f_1, \dots, f_{2^m}$ – коэффициенты разложения f по m переменным. Тогда

$$\|\boldsymbol{f}\| = \sum_{i=1}^{2^m} \|f_i\|.$$

Доказательство следует из того факта, что области определения функций f_i разбивают область определения f на непересекающиеся области, а каждая из них в своей области определения совпадает с f. ■

Выпишем разложение функции $f(\boldsymbol{x}) \in P_2(n)$ по всем переменным:

$$f(\boldsymbol{x}) = \bigoplus (x_1 \oplus\ \alpha_1 \oplus 1) \cdot \dots \cdot (x_n \oplus \alpha_n \oplus 1)\,, \qquad (2.2)$$

где $\boldsymbol{\alpha} \in \mathbb{Z}_2^n$ / $f(\boldsymbol{\alpha}) = 1$.

Представление булевой функции (2.2) называется *совершенной алгебраической нормальной формой* (САНФ) функции *f*. Выполнив раскрытие скобок и приведение подобных слагаемых ($x \oplus x = 0$) получим *алгебраическую нормальную форму* (АНФ) функции $f(\boldsymbol{x})$ или *полином Жегалкина*.

АНФ представляет собой сумму слагаемых, *мономов* вида

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n},$$

где $x^0 = 1$, $x^1 = x$.

Представление булевой функции в виде АНФ единственно, при этом любая булева функция может быть представлена в виде АНФ. В этой форме функция представляется в следующем виде:

$$f(x) = \bigoplus \mathrm{g}(\boldsymbol{\alpha})\, x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}, \qquad \boldsymbol{\alpha} \in Z_2^n. \tag{2.3}$$

При этом $g(\boldsymbol{\alpha}) = 1$ только в том случае, когда соответствующим моном входит в состав АНФ функции $f(\boldsymbol{x})$. Значения функции g называются *коэффициентами АНФ* функции *f*. Отображение μ: $\boldsymbol{f} \to \mu_f$, $\mu_f \in Z_2^{2^n}$, $g = \mu_f$ – называется *преобразованием Мебиуса*. Другими словами, это отображение булевой функции *f* в вектор значений функции $\boldsymbol{g}$.

Построение АНФ

Способы построения АНФ рассмотрим на примерах.

Способ 1. Метод неопределенных коэффициентов

Для построение алгебраической нормальной формы часто используют метод неопределенных коэффициентов. Например, булева функция задана таблицей (табл. 2.1)

Таблица 2.1

x_1	x_2	$f(x_1, x_2)$
0	0	0
0	1	1
1	0	1
1	1	1

Тогда:

$$\begin{gathered} f(x_1, x_2) = a_0 + a_1 \cdot x_1 + a_2 \cdot x_2 + a_3 \cdot x_1 \cdot x_2, \\ f(0,0) = 0 = a_0 + a_1 \cdot 0 + a_2 \cdot 0 + a_3 \cdot 0, \\ f(0,1) = 1 = a_0 + a_1 \cdot 0 + a_2 \cdot 1 + a_3 \cdot 0, \\ f(1,0) = 1 = a_0 + a_1 \cdot 1 + a_2 \cdot 0 + a_3 \cdot 0, \\ f(1,1) = 1 = a_0 + a_1 \cdot 1 + a_2 \cdot 1 + a_3 \cdot 1. \end{gathered}$$

Получаем: $a_0 = 0$, $a_1 = 1$, $a_2 = 1$ $a_3 = 1$. Выражение для функции:

$$f(x) = x_1 \oplus x_2 \oplus x_1 \cdot x_2.$$

Способ 1. Приведение САНФ к АНФ

Пример 2.1.

Зададим функцию $f(\boldsymbol{x})$ следующей таблицей (табл. 2.2).

Таблица 2.2

x_1	x_2	x_3	f
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Поскольку алгебры логических и дискретных функций изоморфны, то свершенной дизъюнктивной нормальной форме (СДНФ) булевой функции в алгебре дискретных функций соответствует совершенная алгебраическая нормальная форма (САНФ), которая строится аналогично. Пользуясь (2.2), запишем совершенную алгебраическую нормальную форму функции *f*, затем, раскрыв скобки и выполнив сокращения, получим алгебраическую нормальную форму:

$$f(\boldsymbol{x}) = (x_1 \oplus 1)(x_2 \oplus 1)x_3 \oplus (x_1 \oplus 1)x_2x_3 \oplus x_1x_2(x_3 \oplus 1) \oplus x_1x_2x_3 = \\ = x_1x_3 \oplus x_3 \oplus x_1x_2.$$

Преобразования Мёбиуса функции *f* приведены в табл. 2.3.

Таблица 2.3

a_1	a_2	a_3	μ_f
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Получили булеву функцию μ ($\boldsymbol{a}$), где $\boldsymbol{a} \in Z_2^n$. Вектор $\boldsymbol{a}$ показывает, какой моном рассматривается, например, $\boldsymbol{a}_0$ = (0, 0, 0), это моном константы 1. Значение μ ($\boldsymbol{a}_0$) = 0, следовательно, константа 1 в АНФ функции $f(\boldsymbol{x})$ отсутствует. Далее, $\boldsymbol{a}_5$ = (1, 0, 1), значение функции μ ($\boldsymbol{a}_5$) = 1, следовательно в рассматриваемом представлении $f(\boldsymbol{x})$ присутствует моном $x_1 x_3$.

Расчет значений функции Мёбиуса, исходя из САНФ, достаточно трудоемок и мало пригоден для программной реализации. Приведем другие способы определения АНФ [12].

Способ 2. Модификация приведения САНФ к АНФ

Данный способ отыскания АНФ позволяет достаточно простую программную реализацию. Перепишем табл. 2.1 в другой форме (табл. 2.4) и только для таких $\boldsymbol{x}$, для которых значения функции $f(\boldsymbol{x})$ = 1.

Таблица 2.4

x_1	0	0	1	1
x_2	0	1	1	1
x_3	1	1	0	1
f	1	1	1	1

Пользуясь табл. 2.4, заполняем табл. 2.5 следующим образом: первый столбец из табл. 2.4 вставляем без изменений. Очередные столбцы – это первый столбец, где вместо нулей записаны все возможные комбинации из нулей и единиц. Далее записываем второй столбец из табл. 2.4 и аналогично заполняем очередные столбцы и т. д.

Таблица 2.5

x_1	0	1	0	1	0	1	1	1	1
x_2	0	0	1	1	1	1	1	1	1
x_3	1	1	1	1	1	1	0	1	1
			#	#	#	#		#	#

Просматриваем столбцы и помечаем (или удаляем) пары одинаковых, например, знаком #. Заполняем очередную таблицу (табл. 2.6), куда вписываем только непомеченные столбцы, она дает функцию Мёбиуса.

Таблица 2.6

x_1	0	1	1
x_2	0	0	1
x_3	1	1	0
μ_f	1	1	1

$f(\boldsymbol{x}) = x_1 x_3 \oplus x_3 \oplus x_1 x_2$.

Способ 3. Списки значений аргументов.

На множестве векторов из $\mathbb{Z}_2^n$ введем отношение порядка $\preccurlyeq$.

Определение 2.3. Пусть векторы $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_2^n$. Будем говорить, что $\boldsymbol{x} \preccurlyeq \boldsymbol{y}$ (вектор $\boldsymbol{y}$ больше вектора $\boldsymbol{x}$, вектор $\boldsymbol{y}$ следует за вектором $\boldsymbol{x}$) если для $\forall\ i = 1, \ldots, n$ выполняются неравенства $x_i \le y_i$.

Данное отношение порядка является частичным, поскольку не для каждой пары векторов можно записать неравенство.

Пользуясь табл. 2.3 запишем списки векторов, меньших или равных выбранному:

$\boldsymbol{a}_0 = (0,0,0)$.	Список: $\boldsymbol{a}_0$.
$\boldsymbol{a}_1 = (0,0,1)$.	Список: $\boldsymbol{a}_0, \boldsymbol{a}_1$.
$\boldsymbol{a}_2 = (0,1,0)$.	Список: $\boldsymbol{a}_0, \boldsymbol{a}_2$.
$\boldsymbol{a}_3 = (0,1,1)$.	Список: $\boldsymbol{a}_0, \boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3$.
$\boldsymbol{a}_4 = (1,0,0)$.	Список: $\boldsymbol{a}_0, \boldsymbol{a}_4$.
$\boldsymbol{a}_5 = (1,0,1)$.	Список: $\boldsymbol{a}_0, \boldsymbol{a}_1, \boldsymbol{a}_4, \boldsymbol{a}_5$.
$\boldsymbol{a}_6 = (1,1,0)$.	Список: $\boldsymbol{a}_0, \boldsymbol{a}_2, \boldsymbol{a}_4, \boldsymbol{a}_6$.
$\boldsymbol{a}_7 = (1,1,1)$.	Список: $\boldsymbol{a}_0, \boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{a}_4, \boldsymbol{a}_5\ \boldsymbol{a}_6, \boldsymbol{a}_7$.

Для функции $f(\boldsymbol{x})$ алгебраическая нормальная форма (2.3) принимает следующий вид:

$$f(\boldsymbol{x}) = \bigoplus \mu(\boldsymbol{a}), \qquad \boldsymbol{a} \preccurlyeq \boldsymbol{x}. \tag{2.4}$$

Например, $f(1,0,0) = \mu(0,0,0) \oplus \mu(1,0,0) = 0 \oplus 0 = 0$.

Оказывается, что верно и обращение формулы (2.4).

Утверждение 2.4. (без доказательства).

Пусть $f(\boldsymbol{x}) \in P_2(n)$, $g(\boldsymbol{a}) = \mu_f(\boldsymbol{a})$. Тогда для любого $\boldsymbol{a} \in \mathbb{Z}_2^n$ имеет место

$$g(\boldsymbol{a}) = \bigoplus f(\boldsymbol{x}), \qquad \boldsymbol{x} \preccurlyeq \boldsymbol{a}. \tag{2.5}$$

Итак, расчет функции Мёбиуса ведется следующим образом. Для заданной размерности n готовится список упорядоченных векторов. Он пригоден для произвольной функции $f(\boldsymbol{x}) \in P_2(n)$. Преобразование Мёбиуса ведется по формуле (2.5) с использованием списка.

Пример 2.2 для функции $f(\boldsymbol{x})$ из табл. 2.2:

- $\mu(\boldsymbol{a}_0) = f(\boldsymbol{a}_0) = 0$;
- $\mu(\boldsymbol{a}_1) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_1) = 0 \oplus 1 = 1$;
- $\mu(\boldsymbol{a}_2) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_2) = 0 \oplus 0 = 0$;
- $\mu(\boldsymbol{a}_3) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_1) \oplus f(\boldsymbol{a}_2) \oplus f(\boldsymbol{a}_3) = 0 \oplus 1 \oplus 0 \oplus 1 = 0$;
- $\mu(\boldsymbol{a}_4) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_4) = 0 \oplus 0 = 0$;
- $\mu(\boldsymbol{a}_5) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_1) \oplus f(\boldsymbol{a}_4) \oplus f(\boldsymbol{a}_5) = 0 \oplus 1 \oplus 0 \oplus 0 = 1$;

- $\mu(\boldsymbol{a}_6) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_2) \oplus f(\boldsymbol{a}_4) \oplus f(\boldsymbol{a}_6) = 0 \oplus 0 \oplus 0 \oplus 1 = 1;$
- $\mu(\boldsymbol{a}_7) = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_1) \oplus f(\boldsymbol{a}_2) \oplus f(\boldsymbol{a}_3) \oplus f(\boldsymbol{a}_4) \oplus f(\boldsymbol{a}_5) \oplus$
$\oplus f(\boldsymbol{a}_6) \oplus f(\boldsymbol{a}_7) = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 = 0.$

Способ 4. Треугольник Паскаля

Выписываем строку значений функции $f(\boldsymbol{x})$, под ней заполняем следующую строку по правилу: очередной элемент равен сумме двух верхних элементов по модулю 2 (рис. 2.1).

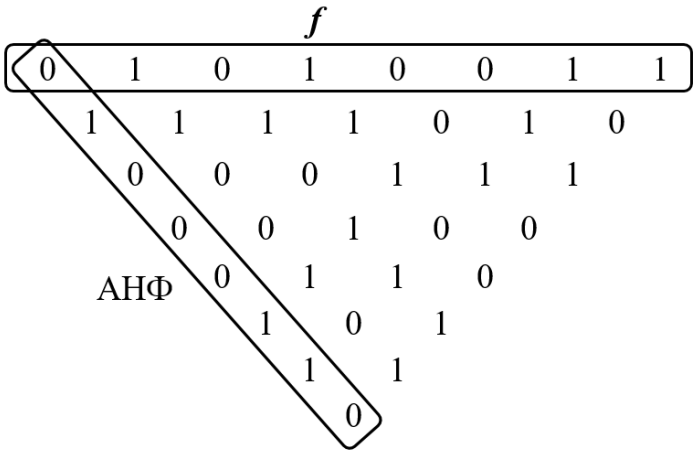


Рис. 2.1. Треугольник Паскаля. АНФ

Левая сторона треугольника дает коэффициенты АНФ в булевой алгебре дискретных функций:

АНФ: (0, 1, 0, 0, 0, 1, 1, 0);

$$f(\boldsymbol{x}) = x_1 x_3 \bigoplus x_3 \bigoplus x_1\, x_2.$$

Следствие 1. $\mu\big(\mu(f)\big) = f$.

По коэффициентам АНФ восстанавливаем вектор значений функции $f(\boldsymbol{x})$ (рис. 2.2).

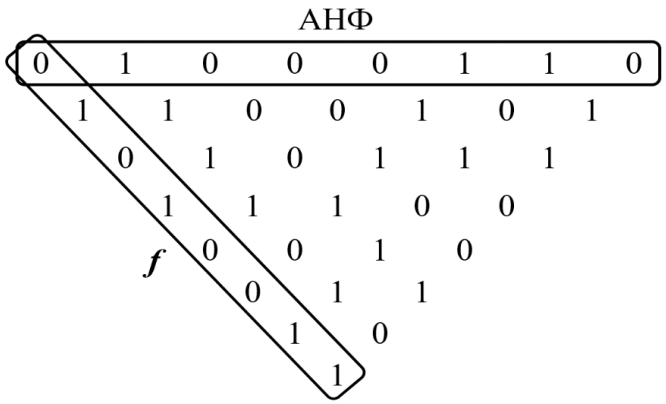


Рис. 2.2. Треугольник Паскаля. Значения функции

Построение списка значений аргументов с помощью треугольника Паскаля

Расчет коэффициентов преобразования Мёбиуса с помощью списков значений аргументов требует минимальных вычислительных затрат. Для построения списка можно воспользоваться треугольником Паскаля. Обозначим (рис. 2.1)

$$f_{ij} = f_i \oplus f_j.$$

Здесь i – номер строки в треугольнике; j – номер символа в строке i (нумерация строк и символов начинается с нуля).

Тогда коэффициенты преобразования Мёбиуса можно выразить через значения булевой функции. Для примера найдем выражение для μ_1 и μ_4. По построению треугольника имеем:

$$\mu(\boldsymbol{a}_1) = \mu_1 \equiv f_{10} = f_{00} \oplus f_{01} = f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_1) = 1;$$

$$\mu(\boldsymbol{a}_4) = \mu_4 \equiv f_{40} = f_{30} \oplus f_{31} = f_{20} \oplus f_{21} \oplus f_{21} \oplus f_{22} =$$
$$= f_{10} \oplus f_{11} \oplus f_{12} \oplus f_{13} =$$
$$= f_{00} \oplus f_{01} \oplus f_{01} \oplus f_{02} \oplus f_{02} \oplus f_{03} \oplus f_{03} \oplus f_{04} =$$
$$= f(\boldsymbol{a}_0) \oplus f(\boldsymbol{a}_4) = 0.$$

Определение 2.4. *Степенью монома* называется количество сомножителей в нем. Наибольшая степень монома в АНФ функции $f(\boldsymbol{x})$ называется *степенью* (*алгебраической степенью*) функции $f(\boldsymbol{x})$; обозначается deg *f*.

Следствие 2. Пусть $f(x) \in P_2(n)$. Тогда степень функции deg $f = n$, если и только если вес функции нечетный. (Доказательство очевидно).

Таким образом, половина дискретных функций имеет максимальную степень.

Утверждение 2.5. (О связи веса и степени функции. Без доказательства.)
Если $f(x) \in P_2(n)$ и $\deg f = d \geq 1$, то $2^{n-d} \leq \|f\| \leq 2^n - 2^{n-d}$.
При $d = 1$ функция уравновешена.
Для криптографических булевых функций имеем требование: $\deg f \geq 2$ или алгебраическая нелинейность не менее двух; дискретные криптографические функции должны быть нелинейными.

2.3. Линейные функции и переменные

Зададим ненулевой вектор $\boldsymbol{a} \in \mathbb{Z}_2^n$. Для этого вектора можно записать выражение соответствующей *линейной функции:*

$$l_a(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x}) = a_1 x_1 \oplus \ldots \oplus a_n x_n.$$

Вектор $\boldsymbol{a}$ будем называть *задающим вектором линейной функции*. Множество всех линейных функций от n переменных обозначается $\mathcal{L}(n)$:

$$\mathcal{L}(n) = \{(\boldsymbol{a}, \boldsymbol{x}) \mid \boldsymbol{a}, \boldsymbol{x} \in \mathbb{Z}_2^n\}.$$

Вектор значений линейной функции обозначим $\boldsymbol{l_a}$.

Множество линейных функций входит во множество так называемых *аффинных функций*. Последние определяются тем, что их алгебраическая степень равна 0 или 1. Само множество аффинных функций обозначается $\mathcal{A}(n)$:

$$\mathcal{A}(n) = \{(\boldsymbol{a}, \boldsymbol{x}) \oplus c_0 \mid c_0 \in \mathbb{Z}_2, \boldsymbol{a}, \boldsymbol{x} \in \mathbb{Z}_2^n\}.$$

Тогда $\mathcal{L}(n) \subseteq \mathcal{A}(n)$.

Наличие линейных свойств у дискретных функций и отображений считается криптографической слабостью. Поэтому необходимой характеристикой функции является значение расстояния от вектора значений функции $f(x)$ до векторов значений функций из класса аффинных. Поскольку хороших криптографических функций в $P_2(3)$ нет, приведем таблицу векторов истинности для линейных функций из $P_2(4)$ (табл. 2.7).

Таблица 2.7

x_1	x_2	x_3	x_4	$\boldsymbol{a}_0$	$\boldsymbol{a}_1$	$\boldsymbol{a}_2$	$\boldsymbol{a}_3$	$\boldsymbol{a}_4$	$\boldsymbol{a}_5$	$\boldsymbol{a}_6$	$\boldsymbol{a}_7$	$\boldsymbol{a}_8$	$\boldsymbol{a}_9$	$\boldsymbol{a}_{10}$	$\boldsymbol{a}_{11}$	$\boldsymbol{a}_{12}$	$\boldsymbol{a}_{13}$	$\boldsymbol{a}_{14}$	$\boldsymbol{a}_{15}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	0	1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	0	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
0	1	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	1	0	1	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0
0	1	1	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0
0	1	1	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1
1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	0	0	1	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0
1	0	1	0	0	0	1	1	0	0	1	1	1	1	0	0	1	1	0	0
1	0	1	1	0	1	1	0	0	1	1	0	1	0	0	1	1	0	0	1
1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
1	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0	0	1	0	1
1	1	1	0	0	0	1	1	1	1	0	0	1	1	0	0	0	0	1	1
1	1	1	1	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0

Здесь $\boldsymbol{a}_0 = (0, 0, 0, 0)$ – задающий вектор линейной функции $l_0(\boldsymbol{x}) = 0$; соответственно, $\boldsymbol{a}_1 = (0, 0, 0, 1)$ – задающий вектор линейной функции

$l_1(\boldsymbol{x}) = x_4, \ldots$, $\boldsymbol{a}_{15}$ = (1, 1, 1, 1) – задающий вектор для функции $l_{15}(\boldsymbol{x}) = x_1 \oplus x_2 \oplus x_3 \oplus x_4$.

Определение 2.5. *Функция $f(\boldsymbol{x})$ линейно зависит от переменной x_i*, если функцию можно представить в виде:

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \oplus x_i,$$

где $g \in P_2(n-1)$.

Из утверждения 2.1, свойство 5б следует: если функция линейно зависит от некоторой своей переменной, то она уравновешена.

Определение линейной зависимости от переменной может быть записано в следующем виде: функция $f(\boldsymbol{x})$ зависит от переменной x_i линейно, если для любого $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in \mathbb{Z}_2^{n-1}$ выполняется неравенство

$$f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \neq f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n).$$

Определение 2.6. *Функция $f(\boldsymbol{x})$ зависит от двух переменных x_i и x_j квазилинейно*, если для любого $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) \in \mathbb{Z}_2^{n-2}$ выполняются неравенства

$$f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n) \neq$$
$$\neq f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_{j-1}, 1, x_{j+1}, \ldots, x_n);$$

$$f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_{j-1}, 1, x_{j+1}, \ldots, x_n) \neq$$
$$\neq f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n).$$

Утверждение 2.6. Функция $f(\boldsymbol{x}, y, z)$ зависит от y, z квазилинейно тогда и только тогда, когда f может быть представлена в виде:

$$f(\boldsymbol{x}, y, z) = g(\boldsymbol{x}, y \oplus z) \oplus y.$$

Доказательство. Пусть $\boldsymbol{x} \in Z_2^n$.

Достаточность.

$f(\boldsymbol{x}, 0,0) = g(\boldsymbol{x}, 0)$;
$f(\boldsymbol{x}, 1,1) = g(\boldsymbol{x}, 0) \oplus 1$.

Следовательно, $f(\boldsymbol{x}, 0,0) \neq f(\boldsymbol{x}, 1,1)$.
$f(\boldsymbol{x}, 0,1) = g(\boldsymbol{x}, 1)$;
$f(\boldsymbol{x}, 1,0) = g(\boldsymbol{x}, 1) \oplus 1$.

Следовательно, $f(\boldsymbol{x}, 0,1) \neq f(\boldsymbol{x}, 1,0)$. Определение квазилинейности выполнено. ■

Необходимость. После разложения $f(\boldsymbol{x}, y, z)$ по переменным y, z и упрощения полученного выражения можно получить требуемое представление. ■

Утверждение 2.7. Функция, зависящая от двух своих переменных квазилинейно, уравновешена.

Доказательство. Пусть $\boldsymbol{x} \in \mathbb{Z}_2^n$, $f(\boldsymbol{x}, y, z) \in P_2(n+2)$, функция f зависит от y, z квазилинейно. По определению квазилинейности:

$$f(\boldsymbol{x}, y, z) = g(\boldsymbol{x}, y \oplus z) \oplus y.$$

После разложения по переменным y, z получим:

$$f(\boldsymbol{x}, y, z) = y \cdot z \cdot (g(x, 0) \oplus 1) \oplus y \cdot (z \oplus 1) \cdot (g(x, 1) \oplus 1) \oplus$$
$$\oplus (y \oplus 1) \cdot z \cdot g(x, 1) \oplus (y \oplus 1) \cdot (z \oplus 1) \cdot g(x, 0).$$

Области определения слагаемых не пересекаются и покрывают всю область определения функции f. Тогда

$$\|\boldsymbol{f}\| = \left\|\overline{g\ (\boldsymbol{x}, 0)}\right\| + \|g\ (\boldsymbol{x}, 0)\| + \left\|\overline{g\ (\boldsymbol{x}, 1)}\right\| + \|g\ (\boldsymbol{x}, 1)\| = 2^{n+1}.$$

Условие уравновешенности выполнено. ■

Пример 2.3. Зададим функцию таблично (табл. 2.8).

Таблица 2.8

x_1	x_2	x_3	f	$\mu(f)$
0	0	0	0	0
0	0	1	1	1
0	1	0	0	0
0	1	1	1	0
1	0	0	0	0
1	0	1	0	1
1	1	0	1	1
1	1	1	1	0

Проверяем выполнение квазилинейности от переменных x_2, x_3:

$$f(0,0,0) \neq f(0,1,1);$$

$$f(0,0,1) \neq f(0,1,0);$$

$$f(1,0,0) \neq f(1,1,1);$$

$$f(1,0,1) \neq f(1,1,0).$$

Условия выполнены, функция квазилинейна от переменных x_2, x_3. Запишем АНФ функции:

$$f(x_1, x_2, x_3) = x_3 \oplus x_1x_3 \oplus x_1x_2 = x_1(x_2 \oplus x_3) \oplus x_3.$$

Критерий квазилинейности выполняется.

Контрольные вопросы и задания

1. Сколько существует уравновешенных функций в P_2 (n)?

2. Какова мощность класса $\mathcal{A}(n)$?

3. Какова мощность класса $\mathcal{L}(n)$?

4. Построить таблицу истинности для функции, заданной вектором истинности из 8 бит, четные биты нули, 4 нечетных бита – № по списку в группе.

Записать ее в совершенной алгебраической нормальной форме.

В записи САНФ функции раскрыть скобки, сократить подобные для приведения ее к алгебраической нормальной форме.

Проверить соответствие АНФ с таблицей истинности.

5. Привести САНФ к АНФ модифицированным методом.

6. Привести САНФ к АНФ методом «списки значений аргументов».

7. Провести преобразование Мёбиуса методом «треугольник Паскаля».

8. Указать вес функции, уравновешенность и ее алгебраическую нелинейность.

3. КОРРЕЛЯЦИОННАЯ ИММУННОСТЬ

Пусть X – случайная величина со значениями в U, и Z – случайная величина со значениями в V.

Величины X, Z называются *статистически независимыми*, если выполняется

$$\forall\, u \in U, \forall\, v \in V$$

$$P\{X = u, Z = v\} = P\{X = u\} \cdot P\{Z = v\}.$$

Пусть $f(\boldsymbol{x}) \in P_2(n)$; $X^1, X^2, \ldots, X^n$ – независимые равномерно распределенные случайные величины со значениями в $\mathbb{Z}_2$ или для всех $i = 1, \ldots, n$ вероятности $P\{X^i = 0\} = 0{,}5$ и $P\{X^i = 1\} = 0{,}5$ равны. Значением функции на случайных аргументах будет случайная величина $Z = f(X^1, X^2, \ldots, X^n)$. Закон распределения вероятностей для случайной величины Z:

$$P\{Z = 1\} = \frac{||f||}{2^n}; \qquad P\{Z = 0\} = 1 - \frac{||f||}{2^n}.$$

3.1. Основные определения

Определение 3.1. Функция $f(x) \in P_2(n)$ *не зависит статистически от подмножества своих переменных* $\{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\}$, $0 < m \leq n$, если случайные, взаимно независимые величины $X^{(i_1,\ i_2,\ \ldots,\ i_m)} = (X^{i_1}, \ldots, X^{i_m})$ и $Z = f(X^1, X^2, \ldots, X^n)$ статистически независимы.

Определение 3.2 (статистическое). Функция $f(x) \in P_2(n)$ называется *корреляционно-иммунной порядка* m, $0 < m \leq n$, если она статистически не зависит от любого m-элементного подмножества из своих аргументов, другими словами, если для любого набора индексов $(i_1, i_2, \ldots, i_m)$, $1 \leq i_1 < i_2 < , \ldots, < i_m \leq n$, то случайные величины $X^{(i_1,\ i_2,\ \ldots,\ i_m)}$ и $Z = f(X^1, X^2, \ldots, X^n)$ статистически независимы.

Теоретико-информационная интерпретация статистической независимости

Взаимной информацией $I(X, Z)$ случайных переменных X и Z называется величина

$$I(X, Z) = H(X) - H(X|Z),$$

где $H(X)$ – энтропия случайной величины X;

$H(X|Z)$ – условная энтропия случайной величины X относительно случайной величины Z.

Взаимная информация X и Z равна нулю, если условная и безусловная энтропии равны. Эквивалентное утверждение: известность значения случайной величины Z не добавляет информации о случайной величине X.

Определение 3.3. Пусть $0 < m \leq n$, $f(x) \in P_2(n)$, $g(x) \in P_2(n-m)$. Зафиксируем m переменных функции $f(x)$, подставив вместо них нули и единицы. Результат назовем функцией g ($\boldsymbol{x}$); эту функцию называют *подфункцией* функции f, *сужением* функции f.

Определение 3.4 (теоретико-информационное). Функция $f(x) \in P_2(n)$ называется *корреляционно-иммунной порядка* m, $0 < m \leq n$, если для любого набора индексов $(i_1, i_2, \dots, i_m)$, $1 \leq i_1 < i_2 <, \dots, < i_m \leq n$, справедливо:

$$I\left(\left(X^{i_1}, \dots, X^{i_m}\right), f(X^1, X^2, \dots, X^n)\right) = 0.$$

Определение 3.4 (комбинаторное). Функция $f(\boldsymbol{x}) \in P_2(n)$ называется *корреляционно-иммунной порядка* m, $0 < m \leq n$, если для любого ее сужения g от $n - m$ переменных выполняется равенство

$$P\{g = 1\} = P\{g = 0\} = 0{,}5.$$

Эквивалентная запись:

$$\| g \| = \frac{\| f \|}{2^m} = 2^{n-m-1}.$$

Получаем критерий корреляционной иммунности уравновешенной функции f ($\boldsymbol{x}$) порядка m: все возможные сужения функции f от $n - m$ переменных уравновешены.

Определение 3.4 (вероятностное). Функция $f(\boldsymbol{x}) \in P_2(n)$ называется *корреляционно-иммунной порядка* m, $0 < m \leq n$, если для любого набора индексов $(i_1, i_2, \dots, i_m)$, $1 \leq i_1 < i_2 <, \dots, < i_m \leq n$, справедливо:

$$P\{X^{i_1}, \dots, X^{i_m}\} = P\{X^{i_1}, \dots, X^{i_m} / f(X^1, X^2, \dots, X^n)\}.$$

Определение 3.5. Уравновешенная корреляционно-иммунная функция порядка m называется *m-устойчивой.*

3.2. Свойства корреляционной иммунности

Требование корреляционной иммунности возникло из-за необходимости противостояния корреляционной атаке на алгоритмы шифрования, которая применяется при криптографическом анализе комбинирующего

генератора шифрующей гаммы (например, [1, 5, 8]). В дальнейших рассуждениях предполагаем, что функция $f(\boldsymbol{x})$ – уравновешена.

Утверждение 3.1. Если уравновешенная функция $f(\boldsymbol{x})$ не корреляционно-иммунная порядка 1, то существует такая переменная x_i, для которой $P\{f = x_i\} \neq 0{,}5$.

Доказательство. Так как функция $f(\boldsymbol{x})$ не корреляционно-иммунная порядка 1, следовательно, существует переменная x_i, которую можно зафиксировать так, что полученное сужение $g(\boldsymbol{x})$ от $n - 1$ переменной не является уравновешенным.

Функцию $f(\boldsymbol{x})$ можно разложить по переменной x_i:

$$f(\boldsymbol{x}) = x_i f_1 \oplus (\mathrm{x_i} \oplus 1) f_2. \tag{3.1}$$

Одна из функций f_1 или f_2 совпадает с сужением g. Так как

$$\|\boldsymbol{f}\| = \|\boldsymbol{f}_1\| + \|\boldsymbol{f}_2\|,$$

то получаем, что $\|\boldsymbol{f}_1\| \neq \|\boldsymbol{f}_2\|$ (так как одна из функций f_1 или f_2 – обязательно неуравновешенная). Вероятность несовпадения значений функции $f(\boldsymbol{x})$ и переменной x_i можно записать следующим образом:

$$P\{f(\boldsymbol{x}) \neq x_i\} = \frac{\left|\|f(\boldsymbol{x}) \oplus x_i\|\right|}{2^n}. \tag{3.2}$$

Используя выражение (3.1), получим:

$$f(\boldsymbol{x}) \oplus x_i = x_i (f_1 \oplus 1) \oplus (x_i \oplus 1) f_2.$$

Распишем числитель в выражении (3.2):

$$\|f \oplus x_i\| = \|f_1 \oplus 1\| + \|f_2\| = 2^{n-1} - \|f_1\| + \|f_2\| \neq 2^{n-1}.$$

Следовательно, $P\{f = x_i\} \neq 0{,}5$. ■

Утверждение 3.2. Корреляционно-иммунная функция порядка m является корреляционно-иммунной функцией любого меньшего порядка.

Доказательство. Для доказательства достаточно показать, что корреляционно-иммунная функция порядка m является корреляционно-иммунной функцией на один порядок меньше, т. е. для значения порядка $m - 1$.

Пусть g – произвольное сужение функции f и $g(\boldsymbol{x}) \in P_2(n - m + 1)$. Выполним разложение g по любой переменной:

$$g = x_i g_1 \oplus (x_i \oplus 1) g_2.$$

Функции g_1 и g_2 – сужения функции f, причем $g_1(\boldsymbol{x})$, $g_2(\boldsymbol{x}) \in P_2(n-m)$. Так как f корреляционно-иммунная функция порядка m, то

$$\| \boldsymbol{g_1} \| = \| \boldsymbol{g_2} \| = \frac{\|\boldsymbol{f}\|}{2^m}.$$

Тогда

$$\| \boldsymbol{g} \| = \| \boldsymbol{g_1} \| + \| \boldsymbol{g_2} \| = \frac{\| \boldsymbol{f} \|}{2^{m-1}}.$$

Полученное соотношение означает, что $f(\boldsymbol{x})$ является корреляционно-иммунной функцией порядка $m-1$. ■

Теперь введем обозначения для максимального порядка корреляционной иммунности:

cor (f) = 0, если функция $f(\boldsymbol{x})$ – не корреляционно-иммунная порядка 1;
cor (f) = max $\{m \in \mathbb{N} \mid f$ – корреляционно-иммунная порядка $m\}$.

Пусть для данной функции cor (f) = 4. Тогда порядок корреляционной иммунности m может принимать значения 1, 2, 3 и 4.

Для уравновешенных функций достаточно заметить, что m-устойчивая функция остается k-устойчивой для любого значения $k < m$. Аналогично введем характеристику для максимального порядка устойчивости sut (f):

sut (f) = -1, если функция не уравновешена;
sut (f) = cor (f), если функция f уравновешена.

Далее без доказательства перечислим некоторые свойства иммунности и устойчивости:

1) cor (f) = cor ($f \oplus 1$);
2) если $\| \boldsymbol{f} \| = 2^t r$, где r нечетное, то cor (f) $\leq t$;
3) если функция линейно зависит от s переменных, то sut (f) $\geq s-1$;
4) все корреляционно-иммунные порядка n функции в $P_2(n)$ – это константа 0 и константа 1;
5) порядок корреляционной иммунности уравновешенной функции из $P_2(n)$ не превышает $n-1$.

Утверждение 3.3. (Без доказательства.) Если $f(\boldsymbol{x}) = x_1 f_1 \oplus (x_1 \oplus 1) f_2$, а функции f_1, f_2 – m-устойчивы, то функция $f(\boldsymbol{x})$ также m-устойчива.

Утверждение 3.4. Пусть все 2^l компонент разложения функции f по l переменным m-устойчивы. Тогда f также m-устойчива. Доказательство следует из утверждения 3.3.

3.3. Неравенство Зигенталера

Теорема 3.1. Пусть $f(\boldsymbol{x}) \in P_2(n)$, тогда:
1) если cor $(f) = m$, то deg $(f) \le n - m$;
2) если f уравновешена и sut $(f) = m$, то deg $(f) \le n - m - 1$.

Доказательство. Пусть deg $(f) = d$. Выберем в АНФ функции $f(\boldsymbol{x})$ любое слагаемое степени d и зафиксируем $n - d$ переменных, не входящих в это слагаемое. Получим подфункцию g степени d от d переменных. По следствию 2 утверждения 2.4 вес подфункции g оказывается нечетным.

1. Зафиксируем в g еще одну переменную, сначала значением ноль, затем значением единица. Таким образом получим очередные подфункции g_1 и g_2 от $d - 1$ переменных. Так как $\| g_1 \| + \| g_2 \| = \| g \|$ нечетное число, то получаем, что $\| g_1 \| \neq \| g_2 \|$. Поскольку cor $(f) = m$, все сужения функции f от k переменных при $k \ge n - m$ имеют одинаковый вес. Следовательно, $d - 1 < n - m$. Тогда получаем $d \le n - m$.

2. Из условия sut $(f) = m$ следует, что $d < n - m$, или $d \le n - m - 1$. Иначе, при $d = n - m$ подфункция на максимальном мономе степени d от d переменных, которые входят в этот моном, имела бы нечетный вес, а значит sut $(f) < m$, что противоречит условию. ■

Обычно неравенства Зигенталера записываются в следующем виде:

$$\text{cor}(f) + \deg(f) \le n;$$

$$\text{sut}(f) + \deg(f) \le n - 1.$$

Неравенство Зигенталера представляет собой пример противоречивости криптографических характеристик булевых функций: высокий порядок корреляционной иммунности функции влечет за собой ее невысокую алгебраическую нелинейность и наоборот, что затрудняет выбор и анализ криптографических преобразований.

Далее определим булевы функции в $P_2(n)$, для которых cor $(f) = n - 1$.

Утверждение 3.5. Все функции в $P_2(n)$, для которых cor $(f) = n - 1$ являются функциями вида

$$f(\boldsymbol{x}) = x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus c, \quad c \in \mathbb{Z}_2.$$

Доказательство. Пусть $f(\boldsymbol{x}) \in P_2(n)$, cor $(f) = n - 1$. По неравенству Зигенталера deg $(f) \le 1$. Однако, если deg $(f) = 0$, то cor $(f) = n$, следовательно, deg $(f) = 1$ и функция f уравновешена.

Если функция f зависит от некоторой переменной фиктивно, то при фиксации остальных $n - 1$ переменных получим константу, а это неуравновешенная подфункция. Противоречие с условием cor $(f) = n - 1$. Следовательно, f существенно зависит от всех своих переменных и таких функций степени один всего две: линейная и аффинная. ■

Сами m-устойчивые функции $f(\boldsymbol{x}) \in P_2(n)$ максимально возможной степени для $m \leq n - 2$ имеют специальное название.

Определение 3.6. Уравновешенная функция $f(\boldsymbol{x}) \in P_2(n)$, sut $(f) = m \leq n - 2$ и с алгебраической степенью deg $(f) = n - m - 1$, называется *m-оптимальной функцией*.

Контрольные вопросы и задания

Привести статистическое определение корреляционной иммунности дискретной функции.

1. Привести теоретико-информационное определение корреляционной иммунности дискретной функции.
2. Привести комбинаторное определение корреляционной иммунности дискретной функции.
3. Дать определение m-устойчивости дискретной функции.
4. Перечислить свойства иммунности.
5. Привести формулировку и доказательство Теоремы Зигенталера.
6. Дать определение m-оптимальности.

4. ПРЕДСТАВЛЕНИЕ БУЛЕВЫХ ФУНКЦИЙ В БАЗИСАХ ФУНКЦИОНАЛЬНЫХ ПРОСТРАНСТВ

В данном разделе используются поля только с характеристикой $p = 2$ т. е., $\forall\, x \in \mathbb{Z}_2$ выполняется $x \oplus x = 0$.

На множестве $P_2(n)$ булевых функций зададим операции сложения и умножения на скаляр:

$$(f_1 \oplus f_2)(\boldsymbol{x}) = f_1(\boldsymbol{x}) \oplus f_2(\boldsymbol{x}),$$

$$(r \cdot f)(\boldsymbol{x}) = r \cdot f(\boldsymbol{x}).$$

Сами функции можно представлять векторами их значений. Тогда выполняется следующее утверждение.

Утверждение 4.1. Множество $P_2(n)$ является векторным пространством относительно заданных операций над полем Галуа $GF(2)$ размерности 2^n.

Проверка выполнения аксиом векторного пространства может быть проведена непосредственно. Один из базисов линейного векторного пространства $P_2(n)$ достаточно часто используется при рассмотрении свойств дискретных функций.

Рассмотрим аддитивную группу поля $GF(2^n)$. Она может быть представлена как группа векторов из $GF(2)^n$ по операции сложения, или в наших обозначениях – из $\mathbb{Z}_2^n$. Множество гомоморфизмов φ этой группы в мультипликативную группу поля комплексных чисел определяется следующей теоремой.

Теорема 4.1. Множество всех гомоморфизмов φ, $\varphi : (\mathbb{Z}_2^n, \oplus) \to (\mathbb{C}, \cdot)$, состоит из 2^n различных гомоморфизмов χ_α, $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}_2^n$, каждый из которых однозначно определяется своим действием на вектор $\boldsymbol{e}_j$, $j \in 1, \ldots, n$ ортонормированного базиса линейного пространства следующим образом:

$$\chi_\alpha(\boldsymbol{e_j}) = exp\left\{\frac{2\pi i}{p}\alpha_j\right\}. \qquad (4.1)$$

Так как функции мы рассматриваем только над двоичным полем, а характеристика этого поля составляет $p = 2$, то выражение (4.1) приобретает следующий вид:

$$\chi_\alpha(\boldsymbol{e_j}) = 1 \qquad \text{при } \alpha_j = 0;$$

$$\chi_\alpha(\boldsymbol{e_j}) = -1 \qquad \text{при } \alpha_j = 1.$$

Доказательство. Так как φ – гомоморфизм, то для любого вектора $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}_2^n$ получаем

$$\varphi(\boldsymbol{\gamma}) = \varphi\left(\oplus_{j=1}^{n} \gamma_j \boldsymbol{e}_j\right) = \prod_{j=1}^{n} \varphi(\boldsymbol{e}_j)^{\gamma_j}.$$

Следовательно, любой гомоморфизм определяется действием на базисные векторы $\boldsymbol{e}_j$. Кроме того, для любого j выполняется соотношение:

$$1 = \varphi(\mathbf{0}) = \varphi(\boldsymbol{e}_j \oplus \boldsymbol{e}_j) = \varphi(\boldsymbol{e}_j)^2.$$

Таким образом, $\varphi(\boldsymbol{e}_j)$ является корнем второй степени из единицы. Для $\varphi(\boldsymbol{e}_j)$ получаем:

$$\varphi(\boldsymbol{e}_j) = (-1)^k, \quad k \in \{0, 1\}.$$

Следовательно, φ является одним из гомоморфизмов вида χ_α, определенных в условии теоремы. ■

В итоге получаем для произвольного вектора $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ из $\mathbb{Z}_2^n$

$$\chi_{\boldsymbol{\alpha}}(\boldsymbol{\beta}) = (-1)^{(\boldsymbol{\alpha},\boldsymbol{\beta})}. \tag{4.2}$$

Гомоморфизмы $\chi_{\boldsymbol{\alpha}}$ называются *аддитивными характерами* поля $GF(2^n)$.

Одно из основных свойств характеров докажем в следующем утверждении.

Утверждение 4.2 (Соотношение ортогональности). Для любых $\boldsymbol{\alpha}$, $\boldsymbol{\beta} \in \mathbb{Z}_2^n$ выполняется равенство

$$\sum_{\boldsymbol{\gamma} \in \mathbb{Z}_2^n} \chi_{\boldsymbol{\alpha}}(\boldsymbol{\gamma})\,\overline{\chi_{\boldsymbol{\beta}}}(\boldsymbol{\gamma}) = 2^n \delta(\boldsymbol{\alpha}, \boldsymbol{\beta}),$$

здесь $\delta(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 1$ при $\boldsymbol{\alpha} = \boldsymbol{\beta}$;

$\delta(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 0$ при $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$;

$\overline{\chi_{\boldsymbol{\beta}}}(\boldsymbol{\gamma})$ – комплексное сопряжение характера $\chi_{\boldsymbol{\alpha}}(\boldsymbol{\gamma})$.

Доказательство. Поскольку характеристика поля $p = 2$, знак комплексного сопряжения значения не имеет, тогда левая часть равенства записывается в следующем виде:

$$\sum_{\boldsymbol{\gamma} \in \mathbb{Z}_2^n} (-1)^{(\boldsymbol{\alpha},\boldsymbol{\gamma})}(-1)^{(\boldsymbol{\beta},\boldsymbol{\gamma})} = 2^n \delta(\boldsymbol{\alpha}, \boldsymbol{\beta}).$$

При $\boldsymbol{\alpha} = \boldsymbol{\beta}$ под знаком суммы получаем $(-1)^2 = (-1)^0 = 1$, слагаемых всего 2^n, соотношение выполняется.

При $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$ получаем $\boldsymbol{d} = \boldsymbol{\alpha} \oplus \boldsymbol{\beta} \neq \mathbf{0}$. Тогда в поле *GF* (2) уравнение

$$d_1 x_1 \oplus \ldots \oplus d_n x_n = c$$

при любом значении c имеет ровно 2^{n-1} решений. Тогда, если вектор $\boldsymbol{\gamma}$ принимает все значения из $\mathbb{Z}_2^n$, то $(\boldsymbol{d}, \boldsymbol{x})$ будет принимать значения нуль и единица ровно по 2^{n-1} раз.

Получаем, что значение последнего выражения равно нулю. ■

Оказывается, что система аддитивных характеров образует базис в пространстве дискретных функций $P_2(n)$. Функции здесь представлены векторами значений.

Теорема 4.2. Множество $\{ \chi_\alpha | \boldsymbol{\alpha} \in \mathbb{Z}_2^n \}$ образует базис пространства $P_2(n)$.

Доказательство. Количество характеров в точности равно размерности векторов значений $\boldsymbol{f}$ функций из $P_2(n)$. Остается показать линейную независимость системы характеров. Допустим обратное. Тогда существует нетривиальный набор $\{ c_\alpha | \boldsymbol{\alpha} \in \mathbb{Z}_2^n \}$, такой, что

$$\sum_{\alpha \in \mathbb{Z}_2^n} (c_{\boldsymbol{\alpha}} \chi_{\boldsymbol{\alpha}}(x)) = 0.$$

Для произвольного $\boldsymbol{\beta} \in \mathbb{Z}_2^n$ умножим обе части последнего равенства на $\overline{\chi_{\boldsymbol{\beta}}}$ и просуммируем по всем $\boldsymbol{x}$ из $\mathbb{Z}_2^n$:

$$\sum\nolimits_{\boldsymbol{x} \in Z_2^n} \sum_{\boldsymbol{\alpha} \in Z_2^n} (c_{\boldsymbol{\alpha}} \chi_{\boldsymbol{\alpha}}(\boldsymbol{x}) \overline{\chi_{\boldsymbol{\beta}}(\boldsymbol{x})} = 0.$$

После изменения порядка суммирования получим

$$2^n \cdot \sum_{\boldsymbol{\alpha} \in Z_2^n} c_{\boldsymbol{\alpha}} \cdot \delta(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 2^n c_{\boldsymbol{\beta}} = 0.$$

Тогда $c_{\boldsymbol{\beta}} = 0$. Таким образом, все коэффициенты $c_{\boldsymbol{\alpha}}$ равны нулю, т. е. набор оказался тривиальным. Это противоречит исходному предположению и, следовательно, множество характеров линейно независимо. ■

4.1. Преобразование Фурье

Определение 4.1. Разложение произвольной функции $f(\boldsymbol{x}) \in P_2(n)$ по базису характеров $\{ \chi_{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in \mathbb{Z}_2^n \}$

$$f\ (\boldsymbol{x}) = \frac{1}{2^n} \sum_{\boldsymbol{\alpha}}\ C_f(\boldsymbol{\alpha})\, \chi_{\boldsymbol{\alpha}}(\boldsymbol{x})$$

называется *разложением функции* $f(\boldsymbol{x})$ в *ряд Фурье*, число $C_f(\boldsymbol{\alpha})$ – *коэффициентом Фурье*, соответствующем вектору $\boldsymbol{\alpha}$. Отображение строк истинности функций из $P_2(n)$ в векторы значений коэффициентов Фурье называется *преобразованием Фурье*. Множество коэффициентов Фурье булевой функции называется *спектром Фурье*.

С учетом (4.2) получим следующее выражение для разложения в ряд Фурье:

$$f(\boldsymbol{x}) = \frac{1}{2^n} \sum_{\boldsymbol{\alpha}}\ C_f(\boldsymbol{\alpha})\, (-1)^{(\boldsymbol{\alpha},\boldsymbol{x})}, \qquad \boldsymbol{\alpha} \in\ \mathbb{Z}_2^n. \tag{4.5}$$

В некоторых источниках данное преобразование называют преобразованием Уолша – Адамара первого рода (соответственно, $C_f(\boldsymbol{\alpha})$ называют *коэффициентами Уолша – Адамара первого рода*, а их совокупность – *спектром Уолша – Адамара первого рода*).

Для вычисления коэффициентов Фурье используется следующее утверждение.

Утверждение 4.3. Пусть $\boldsymbol{\gamma} \in \mathbb{Z}_2^n$. Тогда

$$C_f(\boldsymbol{\gamma}) = \sum_{\boldsymbol{\alpha}} f(\boldsymbol{\alpha}) \cdot \overline{\chi_{\boldsymbol{\gamma}}(\boldsymbol{\alpha})} = \sum_{\boldsymbol{\alpha}} f(\boldsymbol{\alpha}) \cdot (-1)^{(\boldsymbol{\alpha},\boldsymbol{\gamma})}\,. \tag{4.6}$$

Здесь суммирование ведется по всем векторам $\boldsymbol{\alpha} \in\ \mathbb{Z}_2^n$. Результат – целое число.

Доказательство. Следует непосредственно после подстановки (4.5) в (4.6) и применения соотношения ортогональности. ■

Для булевых функций более удобны следующие выражения, используемые при вычислении коэффициентов Фурье.

Утверждение 4.4. Пусть $f(\boldsymbol{x}) \in P_2(n)$. Тогда на нулевом наборе $\mathbf{0}$:

$$C_f(\mathbf{0}) = \|\boldsymbol{f}\|.$$

На остальных наборах $\boldsymbol{a} \neq \mathbf{0}$:

$$C_f(\boldsymbol{a}) = \rho(\boldsymbol{f}, \boldsymbol{l_a}) - 2^{n-1} = \| \boldsymbol{f} \oplus \boldsymbol{l_a} \| - 2^{n-1},$$

где ρ () – метрика, хеммингово расстояние между двоичными векторами;

$\boldsymbol{l_a}$ – вектор значений линейной функции $l_a(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x})$.

Доказательство. Запишем выражение для коэффициента Фурье:

$$C_f(\boldsymbol{a}) = \sum_{\boldsymbol{x}} f(\boldsymbol{x}) \cdot (-1)^{(\boldsymbol{a},\boldsymbol{x})}. \qquad (4.7)$$

Определим два множества:

$$\Omega_1 = \{\boldsymbol{x} \mid f(\boldsymbol{x}) = 1 \ \& \ (\boldsymbol{a}, \ \boldsymbol{x}) = 0\},$$

$$\Omega_2 = \{\boldsymbol{x} \mid f(\boldsymbol{x}) = 1 \ \& \ (\boldsymbol{a}, \ \boldsymbol{x}) = 1\}.$$

Тогда в выражении (4.7) под знаком суммы получаем:

$$C_f(\boldsymbol{a}) = \sum_{\boldsymbol{x} \in \Omega_1} 1 - \sum_{\boldsymbol{x} \in \Omega_2} 1. \qquad (4.8)$$

Количество положительных и отрицательных слагаемых в (4.8):

$$\sum_{\boldsymbol{x} \in \Omega_1} 1 = |\Omega_1| = \langle \boldsymbol{f}, \boldsymbol{l_a} \oplus \mathbf{1} \rangle = \|\boldsymbol{f}\| - \langle \boldsymbol{f}, \boldsymbol{l_a} \rangle;$$

$$\sum_{\boldsymbol{x} \in \Omega_2} 1 = |\Omega_2| = \langle \boldsymbol{f}, \boldsymbol{l_a} \rangle.$$

Получаем после подстановки:

$$C_f(\boldsymbol{a}) = \|\boldsymbol{f}\| - 2\langle \boldsymbol{f}, \boldsymbol{l_a} \rangle = \|\boldsymbol{f}\| + \|\boldsymbol{l_a}\| - 2\langle \boldsymbol{f}, \boldsymbol{l_a} \rangle - \|\boldsymbol{l_a}\|.$$

При $\boldsymbol{a} = \mathbf{0}$ имеем $\|\boldsymbol{l_a}\| = 0$ и $\langle \boldsymbol{f}, \boldsymbol{l_a} \rangle = 0$, тогда

$$C_f(\mathbf{0}) = \|\boldsymbol{f}\|.$$

При $\boldsymbol{a} \neq \mathbf{0}$

$$C_f(\boldsymbol{a}) = \|\boldsymbol{f} \oplus \boldsymbol{l_a}\| - 2^{n-1}.$$

Слагаемое 2^{n-1} возникает, поскольку любая линейная ненулевая функция уравновешена. ■

4.2. Преобразование Уолша – Адамара

В значительной части источников вместо преобразования Фурье рассматривается и применяется *преобразование Уолша – Адамара второго рода*, или просто Уолша. Данное преобразование возникает при разложении в ряд Фурье *характеристического* представления булевой функции:

$$F(\boldsymbol{x}) = (-1)^{f(\boldsymbol{x})}.$$

Пример характеристического представления булевой функции представлен в таблице (табл. 4.1).

Таблица 4.1

x_1	x_2	x_2	f	F
0	0	0	0	1
0	0	1	1	–1
0	1	0	0	1
0	1	1	1	–1
1	0	0	0	1
1	0	1	0	1
1	1	0	1	–1
1	1	1	1	–1

Коэффициенты Фурье характеристического представления называют *коэффициентами Уолша,* обозначение $W_{\boldsymbol{f}}(\boldsymbol{a}) = C_F(\boldsymbol{a})$. Множество коэффициентов Уолша называют *спектром Уолша*.

Разложение в ряд Фурье для этого представления имеет вид:

$$F(\boldsymbol{x}) = \frac{1}{2^n} \sum_{\boldsymbol{a}} W_f(\boldsymbol{a}) (-1)^{(\boldsymbol{a},\boldsymbol{x})};$$

$$f(\boldsymbol{x}) = 0{,}5 - 2^{-n-1} \sum_{\boldsymbol{a}} W_f(\boldsymbol{a}) (-1)^{(\boldsymbol{a},\boldsymbol{x})}. \qquad (4.9)$$

Определение 4.2. *Преобразованием Уолша – Адамара функции* $f(\boldsymbol{x}) \in P_2(n)$, *функцией Уолша*, *представлением булевой функции в форме Уолша* называется функция $W_{\boldsymbol{f}}: \mathbb{Z}_2^n \to \mathbb{Z}$, ее аргументами являются вектора $\boldsymbol{a} \in \mathbb{Z}_2^n$, а значениями целые числа из $\mathbb{Z}$:

$$W_f(\boldsymbol{a}) = \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} (-1)^{f(\boldsymbol{x}) \oplus (\boldsymbol{a},\boldsymbol{x})} = \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} F(\boldsymbol{x})^{(\boldsymbol{a},\boldsymbol{x})}.$$

Пусть при некотором значении переменной $\boldsymbol{x}$ функция $f(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x})$, тогда

$$(-1)^{f(\boldsymbol{x}) \oplus (\boldsymbol{a},\boldsymbol{x})} = 1.$$

Если $f(\boldsymbol{x}) \neq (\boldsymbol{a}, \boldsymbol{x})$, то

$$(-1)^{f(\boldsymbol{x}) \oplus (\boldsymbol{a},\boldsymbol{x})} = -1.$$

Получаем, что $W_f(\boldsymbol{a}) = \sigma - \delta$, где σ – количество совпадений функции $f(\boldsymbol{x})$ и значений линейной функции $l_a(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x})$, $\sigma = \| \boldsymbol{f} \oplus \boldsymbol{l_a} \oplus \boldsymbol{1} \|$; δ – Хеммингово расстояние между их векторами истинности (количество несовпадений), $\delta = \rho(\boldsymbol{f}, \boldsymbol{l_a}) = \| \boldsymbol{f} \oplus \boldsymbol{l_a} \|$. Так как $\sigma = 2^n - \delta$, получаем:

$$W_f(\boldsymbol{a}) = 2^n - 2 \cdot \| \boldsymbol{f} \oplus \boldsymbol{l_a} \| = 2^n - 2\delta.$$

В табл. 4.2 дан пример значений функции и ее коэффициентов Уолша.

Таблица 4.2

x_1	x_2	f	W
0	0	0	–2
0	1	1	2
1	0	1	2
1	1	1	2

В табл. 4.3 приведен пример расчета коэффициентов Уолша; $\boldsymbol{a}_i$ – задающие вектора линейных функций, $l_{\boldsymbol{a}}(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x})$; $\boldsymbol{a}_0 = (0, 0)$, $\boldsymbol{a}_1 = (0, 1)$, …

Таблица 4.3

x_1	x_2	f	$\boldsymbol{a}_0$	$\boldsymbol{a}_1$	$\boldsymbol{a}_2$	$\boldsymbol{a}_3$
0	0	0	0	0	0	0
0	1	1	0	1	0	1
1	0	1	0	0	1	1
1	1	1	0	1	1	0
		δ	3	1	1	1
		W	–2	2	2	2

Итак, имеем:

$$W_f(\boldsymbol{a}) = \sigma - \delta = \| \boldsymbol{f} \oplus \boldsymbol{l_a} \oplus \boldsymbol{1} \| - \| \boldsymbol{f} \oplus \boldsymbol{l_a} \|.$$

Другими словами, коэффициент Уолша есть разница между числом совпадений функции $\boldsymbol{f}$ с линейной функцией $\boldsymbol{l_a}$ и, соответственно, числом совпадений функции $\boldsymbol{f}$ с аффинной функцией $\boldsymbol{l_a} \oplus \boldsymbol{1}$. Если $W_f(\boldsymbol{a}) > 0$,

то функция $\boldsymbol{f}$ ближе к линейной функции, при $W_f(\boldsymbol{a}) < 0$, функция $\boldsymbol{f}$ ближе к аффинной функции. В случае $W_f(\boldsymbol{a}) = 0$ функция $\boldsymbol{f}$ максимально удалена от пары функций $\boldsymbol{l_a}$ и $\boldsymbol{l_a} \oplus \mathbf{1}$. Поскольку задающих векторов $\boldsymbol{a}$ линейных функций $\boldsymbol{l_a}$ ровно 2^n, то и число коэффициентов Уолша ровно такое же число. Тогда $W_f(\boldsymbol{x})$ можно считать функцией с областью определения в виде задающих векторов $\boldsymbol{a}$ и областью значений в кольце целых чисел $\mathbb{Z}$.

Обозначим $F_{\boldsymbol{a}}(\boldsymbol{x})$ характеристическое представление некоторой линейной функции $l_{\boldsymbol{a}}(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x})$, а $\boldsymbol{F_a}$ – ее вектор значений. Тогда имеем:

$$W_f(\boldsymbol{a}) = < \boldsymbol{F}_f, \boldsymbol{F_a} >.$$

Здесь $\boldsymbol{F}_f$ – вектор значений характеристического представления $f(\boldsymbol{x})$.

4.3. Свойства преобразования Уолша – Адамара

1. $W_f(\mathbf{0}) = 2^n - 2\cdot\|f\|$, $W_f(\mathbf{0}) = 0$, если и только если функция $f(\boldsymbol{x})$ уравновешена.

2. Если $g(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus 1$, то $W_g(\boldsymbol{a}) = -W_f(\boldsymbol{a})$ для $\forall\, \boldsymbol{a} \in \mathbb{Z}_2^n$.

3. Если $g(\boldsymbol{x}) = f(\boldsymbol{x} \oplus \boldsymbol{b})$, т. е. функция g получена из функции f отрицанием значений некоторых переменных, то

$$W_g(\boldsymbol{a}) = \sum_{\boldsymbol{x}\in\mathbb{Z}_2^n}(-1)^{f(\boldsymbol{x}\oplus\boldsymbol{b})\,\oplus\,(\boldsymbol{a},\boldsymbol{x})} = \sum_{\boldsymbol{x}\in\mathbb{Z}_2^n}(-1)^{f(\boldsymbol{x})\,\oplus\,(\boldsymbol{a},\boldsymbol{x}\oplus\boldsymbol{b})} =$$
$$= (-1)^{(\boldsymbol{a}.\,\boldsymbol{b})}\, W_f(\boldsymbol{a}).$$

4. Пусть $f(\boldsymbol{x}) \in P_2(n)$, $\boldsymbol{b} \in \mathbb{Z}_2^n$, $g(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus (\boldsymbol{b}, \boldsymbol{x})$. Тогда

$$W_g(\boldsymbol{a}) = \sum_{\boldsymbol{x}}(-1)^{f(\boldsymbol{x})\,\oplus(\boldsymbol{b},\boldsymbol{x})\oplus(\boldsymbol{a},\boldsymbol{x})} = \sum_{\boldsymbol{x}}(-1)^{f(\boldsymbol{x})\oplus(\boldsymbol{a}\,\oplus\boldsymbol{b},\boldsymbol{x})} = W_f(\boldsymbol{a}\oplus\boldsymbol{b}).$$

5. Пусть $f(\boldsymbol{x}) = c$ – константа. Функция $g(\boldsymbol{x}) = c \oplus (\boldsymbol{a}, \boldsymbol{x})$ уравновешена для всех $\boldsymbol{a} \neq \mathbf{0}$, следовательно, $W_f(\boldsymbol{a}) = 0$ для всех ненулевых $\boldsymbol{a}$. Кроме того:

$$W_f(\mathbf{0}) = 2^n - 2\cdot\|\boldsymbol{f}\| = 2^{-n} \text{ при } c = 1;$$
$$W_f(\mathbf{0}) = 2^n - 2\cdot\|\boldsymbol{f}\| = 2^n \text{ при } c = 0.$$

6. Пусть $f(\boldsymbol{x}) = (\boldsymbol{b}, \boldsymbol{x}) \oplus c$ – аффинная функция. Тогда

$$W_f(\boldsymbol{a}) = 0 \text{ при } \boldsymbol{a} \neq \boldsymbol{b},$$
$$W_f(\boldsymbol{a}) = (-1)^c \cdot 2^n \text{ при } \boldsymbol{a} = \boldsymbol{b}.$$

7. Пусть $f(\boldsymbol{x},\boldsymbol{y}) = g(\boldsymbol{x}) \oplus h(\boldsymbol{y})$, где $g \in P_2(n)$; $h \in P_2(m)$; множества переменных в векторах $\boldsymbol{x}$, $\boldsymbol{y}$ не пересекаются. Тогда для $\forall$ $\boldsymbol{a}$, $\boldsymbol{b}$ | $\boldsymbol{a} \in \mathbb{Z}_2^n$, $\boldsymbol{b} \in \mathbb{Z}_2^m$, выполняется соотношение

$$W_f(\boldsymbol{ab}) = \sum_{\boldsymbol{x},\boldsymbol{y}} (-1)^{g(\boldsymbol{x}) \oplus h(\boldsymbol{y}) \oplus (\boldsymbol{a},\boldsymbol{x}) \oplus (\boldsymbol{b},\boldsymbol{y})} =$$
$$= \sum_{\boldsymbol{x}}(-1)^{g(\boldsymbol{x}) \oplus (\boldsymbol{a},\boldsymbol{x})} \cdot \sum_{\boldsymbol{x}}(-1)^{h(\boldsymbol{x}) \oplus (\boldsymbol{b},\boldsymbol{x})} = W_f(\boldsymbol{a})\, W_f(\boldsymbol{b}).$$

8. Пусть функция $f(\boldsymbol{x}) \in P_2(n)$ зависит от переменной x_i фиктивно. Тогда $W_f(\boldsymbol{a}) = 0$ для всех таких задающих векторов $\boldsymbol{a}$, у которых координата $a_i = 1$.

Доказательство. Обозначим

$\boldsymbol{x}' = (x_1, \ldots\ x_{i-1}, x_{i+1}, \ldots\ x_n)$,
$\boldsymbol{a}' = (a_1, \ldots\ a_{i-1}, a_{i+1}, \ldots\ a_n)$.

Воспользуемся соотношением $(\boldsymbol{a},\boldsymbol{x}) = (\boldsymbol{a}',\boldsymbol{x}') \oplus a_i \cdot x_i$. Если $a_i = 1$, то

$$W_f(\boldsymbol{a}) = \sum_{\boldsymbol{x}\in\mathbb{Z}_2^n} (-1)^{f(\boldsymbol{x}) \oplus (\boldsymbol{a},\boldsymbol{x})} = \sum_{\boldsymbol{x},\, x_i=0} (-1)^{f(\boldsymbol{x}) \oplus (\boldsymbol{a}',\boldsymbol{x}')} +$$
$$+ \sum_{\boldsymbol{x},\, x_i=1}(-1)^{f(\boldsymbol{x}) \oplus (\boldsymbol{a}',\boldsymbol{x}') \oplus 1} = 0.\blacksquare$$

Из свойств 2, 4 можно сделать вывод о том, что аффинная добавка не изменяет спектр функции.

Определение 4.3. Функция $g(\boldsymbol{x}) \in P_2(n)$ получается из функции $f(\boldsymbol{x}) \in P_2(n)$ с помощью *аффинного преобразования переменных*, если существуют невырожденная булева матрица $A_{n,n}$ и вектор $\boldsymbol{b} \in \mathbb{Z}_2^n$, такие, что $\forall$ $\boldsymbol{x} \in \mathbb{Z}_2^n$ выполняется соотношение

$$g(\boldsymbol{x}) = f(A\boldsymbol{x} \oplus \boldsymbol{b}).$$

Пример 4.1. Пусть $f(x,y) = x \oplus y \oplus x \cdot y$, $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\boldsymbol{b} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Тогда

$$g(\boldsymbol{x},\boldsymbol{y}) = f(A\boldsymbol{x} \oplus \boldsymbol{b}) = f(x \oplus y, y \oplus 1) =$$
$$= x \oplus y \oplus y \oplus 1 \oplus x \cdot y \oplus x = x \cdot y \oplus 1.$$

Утверждение 4.5. Пусть функция $g(\boldsymbol{x})$ получена из функции $f(\boldsymbol{x})$ аффинным преобразованием переменных. Тогда спектры $g(\boldsymbol{x})$ и $f(\boldsymbol{x})$ совпадают.

Доказательство. Обозначим $\boldsymbol{y} = A\boldsymbol{x} \oplus \boldsymbol{b}$, матрица A невырожденная, следовательно, она обратимая: $\boldsymbol{x} = A^{-1}(\boldsymbol{y} \oplus \boldsymbol{b})$. Получаем:

$$W_g(\boldsymbol{a}) = \sum_{\boldsymbol{x}}(-1)^{f(A\boldsymbol{x} \oplus \boldsymbol{b}) \oplus (\boldsymbol{a},\boldsymbol{x})} =$$

$$= \sum_{\boldsymbol{y}} (-1)^{f\,(\boldsymbol{y}) \,\oplus\, (\boldsymbol{a}, A^{-1}\boldsymbol{y})}\ (-1)^{(\boldsymbol{a}, A^{-1}\boldsymbol{b})} = \pm \sum_{\boldsymbol{y}} (-1)^{f\,(\boldsymbol{y}) \,\oplus\, (\boldsymbol{a}, A^{-1}\boldsymbol{y})} =$$

$$= \pm \sum_{\boldsymbol{y}} (-1)^{f\,(\boldsymbol{y}) \,\oplus\, (\boldsymbol{a}A^{-1}, \boldsymbol{y})} = \pm\, W_f(\boldsymbol{a}A^{-1}).\ \blacksquare$$

Пусть $f(\boldsymbol{x}) \in P_2(n)$, $\boldsymbol{b} \in \mathbb{Z}_2^n$. Обозначим f^b подфункцию (сужение) исходной функции *f,* она получается фиксацией $x_i = 0$ для всех индексов i, таких, что $b_i = 1$.

Пример 4.2. Построение функции f^b (табл. 4.4)

Таблица 4.4

x_1	x_2	f		x_2	f^b
0	0	1		0	1
0	1	0	b = (1,0) =>	1	0
1	0	0		–	–
1	1	1		–	–

Теорема 4.3 (Тождество Саркара. Без доказательства).

$$\sum_{\boldsymbol{a} \prec \boldsymbol{b}} W_f(\boldsymbol{a}) = 2^n - \ 2^{||\,\boldsymbol{b}\,||+1} \cdot ||\ f^b\ ||\ .$$

Следствие.

$$\sum_{\boldsymbol{a}} W_f = (-1)^{f(\boldsymbol{0})} \cdot 2^n.$$

Для линейных функций выполняется соотношение:

$$\sum_{\boldsymbol{x}} (-1)^{(\boldsymbol{a}, \boldsymbol{x})} = 2^n \cdot \delta\,(\boldsymbol{a}, \boldsymbol{0}).$$

Теорема 4.4 (*Соотношение ортогональности* для функции Уолша). Пусть $f(\boldsymbol{x}) \in P_2(n)$. Тогда

$$\sum_{\boldsymbol{a}} W_f(\boldsymbol{a}) W_f(\boldsymbol{x} \,\oplus\, \boldsymbol{a}) = 2^{2n}\ \delta\,(\boldsymbol{x}, \boldsymbol{0}).$$

Доказательство.

$$\sum\nolimits_{\boldsymbol{a}} W_f(\boldsymbol{a}) W_f(\boldsymbol{x} \oplus \boldsymbol{a}) =$$

$$= \sum\nolimits_{\boldsymbol{a}} \Big(\sum\nolimits_{\boldsymbol{y}} (-1)^{f(\boldsymbol{y}) \,\oplus\, (\boldsymbol{a}, \boldsymbol{y})}\Big) \Big(\sum\nolimits_{\boldsymbol{z}} (-1)^{f(\boldsymbol{z}) \,\oplus\, (\boldsymbol{x} \oplus \boldsymbol{a}, \boldsymbol{z})}\Big) =$$

$$= \sum\nolimits_{\boldsymbol{a}, \boldsymbol{x}, \boldsymbol{z}} (-1)^{f\,(\boldsymbol{y}) \,\oplus\, f\,(\boldsymbol{z}) \oplus\, (\boldsymbol{a}, \boldsymbol{y}) \,\oplus\, (\boldsymbol{x} \,\oplus\, \boldsymbol{a}, \boldsymbol{z})} =$$

$$= \sum_{\boldsymbol{y},\boldsymbol{z}} (-1)^{f\,(\boldsymbol{y}) \oplus f(\boldsymbol{z}) \oplus (\boldsymbol{x},\,\boldsymbol{z})} \sum_{\boldsymbol{a}} (-1)^{(\boldsymbol{a},\,\boldsymbol{y} \oplus \boldsymbol{z})} =$$

$$= \sum_{\boldsymbol{y},\boldsymbol{z}} (-1)^{f\,(\boldsymbol{y}) \oplus f\,(\boldsymbol{z}) \,\oplus\, (\boldsymbol{x},\,\boldsymbol{z})}\; 2^n \delta\,(y, z) =$$

$$= 2^n \delta\,(y, z)\; \textstyle\sum_{\boldsymbol{z}} (-1)^{(\boldsymbol{x},\boldsymbol{z})} \sum_{\boldsymbol{y}} (-1)^{f\,(\boldsymbol{y}) \oplus f\,(\boldsymbol{z})} =$$

$$= 2^n \textstyle\sum_{\boldsymbol{z}} (-1)^{(\boldsymbol{x},\boldsymbol{z})} = 2^{2n}\; \delta\,(\boldsymbol{x}, \boldsymbol{0}).\blacksquare$$

Следствие (равенство Парсеваля). Пусть $f(\boldsymbol{x}) \in P_2(n)$. Тогда

$$\sum_{\boldsymbol{a}} W_f^2(\boldsymbol{a}) = \; 2^{2n}.$$

Целочисленная функция Уолша однозначно определяет исходную булеву функцию $f(\boldsymbol{x})$. Однако не всякий целочисленный вектор размерности 2^n является вектором значений преобразования Уолша-Адамара для некоторой булевой функции.

Утверждение 4.6. Пусть $g : \mathbb{Z}_2^n \;\rightarrow\; \mathbb{Z}$ – некоторая целочисленная функция. Булева функция *f,* такая, что $W_{\boldsymbol{f}}(\boldsymbol{a}) = g\;(\boldsymbol{a})$ для $\forall\; \boldsymbol{a} \in \mathbb{Z}_2^n$, существует если и только если выполнено соотношение ортогональности

$$\sum_{\boldsymbol{a}} g\;(\boldsymbol{a})\; g\;(\boldsymbol{x} \;\oplus \boldsymbol{a}) = 2^{2n}\; \delta\;(\boldsymbol{x}, \boldsymbol{0}).$$

Доказательство. Необходимость следует из теоремы 4.4. Достаточность следует из того, что восстановление булевой функции по формуле (4.9) возможно при выполнении соотношения

$$\sum_{\boldsymbol{y}} g\;(\boldsymbol{y})(-1)^{(\boldsymbol{x},\boldsymbol{y})} = \;\pm\; 2^n.$$

Воспользуемся тем, что если $\boldsymbol{z}$ пробегает множество $\mathbb{Z}_2^n$, то $\boldsymbol{y} \oplus \boldsymbol{z}$ пробегает то же множество при любом фиксированном значении $\boldsymbol{y} \in \mathbb{Z}_2^n$:

$$\left(\textstyle\sum_y g\;(\boldsymbol{y})\;\; (-1)^{(\boldsymbol{x},\boldsymbol{y})}\right)^2 = \textstyle\sum_y g\;(\boldsymbol{y})\;\; (-1)^{(\boldsymbol{x},\boldsymbol{y})} \sum_{\boldsymbol{z}} g\;(\boldsymbol{z})\;\; (-1)^{(\boldsymbol{x},\boldsymbol{z})} =$$

$$= \textstyle\sum_y g\;(\boldsymbol{y})\;\; (-1)^{(\boldsymbol{x},\boldsymbol{y})} \sum_{\boldsymbol{z}} g\;(\boldsymbol{y} \oplus \boldsymbol{z})\;\; (-1)^{(\boldsymbol{x},\boldsymbol{y} \,\oplus\, \boldsymbol{z})} =$$

$$= \textstyle\sum_{\boldsymbol{z}} (-1)^{(\boldsymbol{x},\boldsymbol{z})} \sum_{\boldsymbol{y}} g\;(\boldsymbol{y}) g\;(\boldsymbol{y} \;\oplus \boldsymbol{z}) = \sum_{\boldsymbol{z}} (-1)^{(\boldsymbol{x},\boldsymbol{z})} \cdot 2^{2n} \cdot \delta\;(\boldsymbol{z}, \boldsymbol{0}) = 2^{2n}.$$

Получается, что

$$\textstyle\sum_{\boldsymbol{y}} g\;(\boldsymbol{y})(-1)^{(\boldsymbol{x},\boldsymbol{y})} = \pm\, 2^n. \blacksquare$$

Теорема 4.5 (Теорема о свертке). Пусть $h(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus g(\boldsymbol{x})$. Тогда для $\forall\ \boldsymbol{a} \in \mathbb{Z}_2^n$ выполняется

$$W_h(\boldsymbol{a}) = \frac{1}{2^n} \sum_{\boldsymbol{b}} W_g(\boldsymbol{b})\, W_f(\boldsymbol{a} \oplus \boldsymbol{b}).$$

Доказательство. Воспользуемся формулой обращения:

$$W_h(\boldsymbol{a}) = \sum_{\boldsymbol{x}} (-1)^{f(\boldsymbol{x}) \oplus g(\boldsymbol{x}) \oplus (\boldsymbol{a},\boldsymbol{x})} =$$

$$= \frac{1}{2^n} \sum_{\boldsymbol{x}} (-1)^{f(\boldsymbol{x}) \oplus (\boldsymbol{a},\boldsymbol{x})} \sum_{\boldsymbol{v}} W_g(\boldsymbol{v})\, (-1)^{(\boldsymbol{v},\boldsymbol{x})} =$$

$$= \frac{1}{2^n} \sum_{\boldsymbol{v}} W_g(\boldsymbol{v}) \sum_{\boldsymbol{x}} (-1)^{f(\boldsymbol{x}) \oplus (\boldsymbol{a} \oplus \boldsymbol{v},\boldsymbol{x})} = \frac{1}{2^n} \sum_{\boldsymbol{v}} W_g(\boldsymbol{v})\, W_f(\boldsymbol{a} \oplus \boldsymbol{v}). \blacksquare$$

4.4. Статистическая структура

В некоторых источниках применяется еще одно преобразование булевой функции. Его коэффициенты рассчитываются по формуле

$$S_f(\boldsymbol{a}) = 2^{n-1} - \|f \oplus l_a\|. \tag{4.10}$$

Определение 4.4. *Статистической структурой* функции $f(\boldsymbol{x}) \in P_2(n)$, называется множество (спектр)

$$S_f = \{S_f(\boldsymbol{a}),\ \boldsymbol{a} \in \mathbb{Z}_2^n\}.$$

Статистическая структура – это целочисленная функция $S_{\boldsymbol{f}}: \mathbb{Z}_2^n \to \mathbb{Z}$, ее аргументами являются вектора $\boldsymbol{a} \in \mathbb{Z}_2^n$, а значениями целые числа из $\mathbb{Z}$. Значения коэффициентов статистической структуры могут быть представлены в следующем виде:

$$S_f(\boldsymbol{a}) = 0{,}5\, W_f(\boldsymbol{a}) = 0{,}5\langle F_f, F_{\boldsymbol{a}}\rangle. \tag{4.11}$$

Аналогично спектрам Фурье и Уолша – Адамара, спектр статистической структуры однозначно определяет булеву функцию

$$f(\boldsymbol{x}) = 0{,}5 - 2^{-n} \sum_{\boldsymbol{a}} S_f(\boldsymbol{a})(-1)^{(\boldsymbol{a},\boldsymbol{x})}.$$

Для спектра статистической структуры выполняется аналог равенства Парсеваля:

$$\sum_{\boldsymbol{a}} {S_f}^2(\boldsymbol{a}) = 2^{2n-2}.$$

Определение 4.5. Функция $g(\boldsymbol{x})$ называется *статистическим аналогом* функции $f(\boldsymbol{x})$, если при равновероятном выборе значений аргумента $\boldsymbol{x} \in \mathbb{Z}_2^n$ вероятность совпадения их значений больше 0,5, или

$$P\{f(\boldsymbol{x}) = g(\boldsymbol{x})\} > 0{,}5.$$

На замене исходной функции $f(\boldsymbol{x})$ ее статистическим аналогом основаны многие методы криптографического анализа систем шифрования. При этом, как правило, используются линейный или аффинный аналог функции.

Утверждение 4.7. Для любой функции $f(\boldsymbol{x}) \in P_2(n)$ и $\boldsymbol{a} \in \mathbb{Z}_2^n$ справедливо равенство

$$P\{f(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x})\} = 0{,}5 + \frac{S_f(\boldsymbol{a})}{2^n}.$$

Доказательство.

$$P\{f(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x})\} = P\{f(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x}) = 0\} =$$

$$= 2^{-n}(2^n - \|f(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x})\|) = (2^{n-1} + S_f(\boldsymbol{a}))\, 2^{-n} = 0{,}5 + \frac{S_f(\boldsymbol{a})}{2^n}. \blacksquare$$

Таким образом, статистическая структура дает полную информацию о линейных статистических аналогах булевой функции.

Определение 4.6. *Перекосом вероятностей* δ_p называется величина

$$\delta_p = P\{f(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x})\} - 0{,}5 = \frac{S_f(\boldsymbol{a})}{2^n}.$$

Значение $\delta_p \in (-0{,}5, +0{,}5)$. Чем больше модуль перекоса, тем лучше статистическая структура отражает свойства булевой функции.

Существует связь между коэффициентами статистической структуры функции

$$f(x_1, x_2, \ldots, x_n)$$

и ее подфункциями f_0 и f_1

$$f_0(x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n),$$

$$f_1(x_2, \ldots, x_n) = f(1, x_2, \ldots, x_n).$$

Утверждение 4.8. Для любой функции $f(\boldsymbol{x}) \in P_2(n)$ и $\boldsymbol{a} = (a_2, a_3, \ldots, a_n) \in \mathbb{Z}_2^{n-1}$ справедливо равенство

$$S_f(0, a_2, a_3, \ldots, a_n) = S_{f_0}(\boldsymbol{a}) + S_{f_1}(\boldsymbol{a}),$$
$$S_f(1, a_2, a_3, \ldots, a_n) = S_{f_0}(\boldsymbol{a}) - S_{f_1}(\boldsymbol{a}).$$

Доказательство. Расписываем первое равенство:

$$S_f(0, a_2, a_3, \ldots, a_n) = 2^{n-1} - \| f(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x}) \| =$$
$$= 2^{n-1} - \| f_0(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x}) \| - \| f_1(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x}) \| =$$
$$= (2^{n-2} - \| f_0(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x}) \|) + (2^{n-2} - \| f_1(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x}) \|) = S_{f_0}(\boldsymbol{a}) + S_{f_1}(\boldsymbol{a}).$$

Второе равенство доказывается аналогично. ■

Пример 4.3. Вычисление статистической структуры функции

$$f(\boldsymbol{x}) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3.$$

Имеем:

$$f_0 = f(0, x_2, x_3) = x_2x_3.$$

Для подфункции f_0 коэффициенты статистической структуры можно рассчитать по формуле (4.10) или (4.11). Тогда получим

$$S_{f_0} = (S_{f_0}(0,0), S_{f_0}(0,1), S_{f_0}(1,0), S_{f_0}(1,1)) = (1, 1, 1, -1).$$

Аналогично расписываем подфункцию f_1:

$$f_1 = f(1, x_2, x_3) = x_2 \oplus x_2x_3 \oplus x_3.$$

Коэффициенты статистической структуры для f_1:

$$S_{f_1} = (S_{f_1}(0,0), S_{f_1}(0,1), S_{f_1}(1,0), S_{f_1}(1,1)) = (-1, 1, 1, 1).$$

Из утверждения 4.8 следует, что коэффициенты статистической структуры функции $f(\boldsymbol{x})$ имеют вид

$S_f(0, 0, 0) = 0;$
$S_f(0, 0, 1) = 2;$
$S_f(0, 1, 0) = 2;$
$S_f(0, 1, 1) = 0;$ — $S_{f_0}(\boldsymbol{a}) + S_{f_1}(\boldsymbol{a})$
$S_f(1, 0, 0) = 2;$
$S_f(1, 0, 1) = 0;$
$S_f(1, 1, 0) = 0;$ — $S_{f_0}(\boldsymbol{a}) - S_{f_1}(\boldsymbol{a})$
$S_f(1, 1, 1) = -2.$

Утверждение 4.9. Пусть $f(\boldsymbol{x}) \in P_2(n)$ и $g(\boldsymbol{y}) \in P_2(m)$ и векторы $\boldsymbol{x}, \boldsymbol{y}$ общих переменных не имеют; пусть $h(\boldsymbol{x}, \boldsymbol{y}) = f(\boldsymbol{x}) \oplus g(\boldsymbol{y})$. Тогда

$$S_h(\boldsymbol{a}, \boldsymbol{b}) = 2\, S_f(\boldsymbol{a})\, S_g(\boldsymbol{b}).$$

Доказательство. Истинность утверждения 4.9 следует из правильности следующей цепочки равенств.

$$0{,}5 + S_h(\boldsymbol{a}, \boldsymbol{b})\, 2^{-n-m} = P\,\{h\,(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{a}, \boldsymbol{x}) \oplus (\boldsymbol{b}, \boldsymbol{y})\} =$$

$$= P\,\{f(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x}) = g\,(\boldsymbol{y}) \oplus (\boldsymbol{b}, \boldsymbol{y})\} =$$

$$= P\,\{f(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x}) = 0\} \cdot P\,\{g\,(\boldsymbol{y}) \oplus (\boldsymbol{b}, \boldsymbol{y}) = 0\} +$$

$$+ P\,\{f(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x}) = 1\} \cdot P\,\{g\,(\boldsymbol{y}) \oplus (\boldsymbol{b}, \boldsymbol{y}) = 1\} =$$

$$= (0{,}5 + S_f(\boldsymbol{a})\, 2^{-n})\,(0{,}5 + S_g(\boldsymbol{b})\, 2^{-m}) + (0{,}5 - S_f(\boldsymbol{a})\, 2^{-n})\,(0{,}5 - S_g(\boldsymbol{b})\, 2^{-m}) =$$

$$= 0{,}5 + 2\, S_f(\boldsymbol{a})\, S_g(\boldsymbol{b})\, 2^{-n-m}. \blacksquare$$

Пример 4.3. Вычисление статистической структуры функции

$$f(\boldsymbol{x}) = x_1x_2 \oplus x_3x_4 \oplus x_2 \oplus x_3.$$

Представим $f\,(\boldsymbol{x})$ в виде суммы двух функций: $f\,(\boldsymbol{x}) = \varphi_1 \oplus \varphi_2$, где $\varphi_1 = x_1x_2 \oplus x_2$ и $\varphi_2 = x_3x_4 \oplus x_3$.

Тогда

$S_{\varphi_1}(0,0) = 1;$ $\quad S_{\varphi_2}(0,0) = 1;$
$S_{\varphi_1}(0,1) = 1;$ $\quad S_{\varphi_2}(0,1) = -1;$
$S_{\varphi_1}(1,0) = -1;$ $\quad S_{\varphi_2}(1,0) = 1;$
$S_{\varphi_1}(1,1) = 1.$ $\quad S_{\varphi_2}(1,1) = 1.$

Получаем: S_f = (2, –2, 2, 2, 2, –2, 2, 2, –2, 2, –2, –2, 2, –2, 2, 2).

4.5. Матрицы в представлениях булевых функций

Выберем некоторую невырожденную $2^n \times 2^n$ матрицу A над двоичным полем. Пусть $\boldsymbol{f}$ – вектор-столбец значений булевой функции $f(\boldsymbol{x}) \in P_2(n)$. Обозначим

$$\boldsymbol{g} = A^{-1}\boldsymbol{f}, \qquad (\text{т. е.}, \boldsymbol{f} = A\boldsymbol{g}). \tag{4.12}$$

Для произвольного $\boldsymbol{a} \in \mathbb{Z}_2^n$ обозначим $\boldsymbol{g}\,(\boldsymbol{a})$ координату вектора $\boldsymbol{g}$, соответствующую этому набору. Равенством (4.12) задается биективное отображение множества $\mathbb{Z}_2^n$ во множество векторов 2^{2^n}. Вектор $\boldsymbol{g}$ называют *представлением* функции $f(\boldsymbol{x})$.

Столбцы матрицы A можно пронумеровать, эти номера назовем $\boldsymbol{a}$. Вектор $\boldsymbol{a}$ есть по сути двоичное представление десятичного номера, например,

$\boldsymbol{a}_0$ – это вектор из нулей. Обозначим $\boldsymbol{h_a}$ столбцы матрицы A, тогда выполняется равенство

$$\boldsymbol{f} = \sum_{\boldsymbol{a} \in Z_2^n} \boldsymbol{h_a}\, \boldsymbol{g}.$$

Каждый вектор-столбец $\boldsymbol{h_a}$ можно считать вектором значений некоторой функции h_a $(\boldsymbol{x})$, а так как матрица A невырожденная, то набор $\{\boldsymbol{h_a}, \boldsymbol{a} \in Z_2^n\}$ образует базис функционального пространства P_2 (n). Тогда вектор $\boldsymbol{g}$ – есть вектор координат функции $\boldsymbol{f}$ в разложении ее по этому базису, и задает эту функцию однозначно. Таким образом, с каждой невырожденной матрицей может быть связано некоторое представление булевой функции. Представления булевых функций, описание которых дано ранее, можно получить с помощью матриц специального вида.

Тензорное (Кронекерово) произведение матриц

Определение 4.7. Пусть $A = (a_{ij})$ и $B = (b_{ij})$ – матрицы размеров $m \times m$ и $n \times n$ над двоичным полем соответственно. *Тензорным* (*Кронекеровым*) *произведением матриц* A и B называется матрица C размера $mn \times mn$ следующего вида:

$$C = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & & a_{2n}B \\ \vdots & & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{pmatrix}.$$

Обозначение тензорного произведения: $C = A \otimes B$. Тензорная степень k матрицы A обозначается $A^{[k]}$. Матрицы размера $m \times m$ обозначим $K_{m,m}$. Единичная квадратная матрица будет обозначаться E.

Теорема 4.6 (Свойства тензорного произведения). Пусть A, B, C – квадратные матрицы подходящих размеров над двоичным полем. Тогда справедливы следующие соотношения:

1) $A \otimes (B \otimes C) = (A \otimes B) \otimes C$;

2) $(A \oplus B) \otimes C = A \otimes C \oplus B \otimes C$,

$A \otimes (B \oplus C) = A \otimes B \oplus A \otimes C$;

3) если $A, C \in K_{m,m}$, а $B, D \in K_{n,n}$, то $(A \otimes B)(C \otimes D) = AC \otimes BD$;

4) матрица $A \otimes B$ обратима тогда и только тогда, когда обратимы матрицы A и B. При этом $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$;

5) $(AB)^{[n]} = A^{[n]} \otimes B^{[n]}$.

Без доказательства.

Следствие.

$$A^{[n]} = (A \otimes E \otimes \dots E)(E \otimes A \otimes \dots E) \dots (E \otimes E \otimes \dots \otimes A).$$

Пример 4.4. Преобразование Мёбиуса (определение коэффициентов АНФ функции).

Пусть задана некоторая булева функция $f(\boldsymbol{x}) \in P_2(n)$, а $\boldsymbol{f}$ – ее вектор истинности. Вектор коэффициентов АНФ для функции $f(\boldsymbol{x})$ обозначим $\boldsymbol{АНФ}_f$. В двоичном поле зададим матрицу

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Кронекерова степень *n* матрицы *B* имеет вид

$$B^{[n]} = \begin{pmatrix} B^{[n-1]} & \mathbf{0} \\ B^{[n-1]} & B^{[n-1]} \end{pmatrix}.$$

Преобразование Мёбиуса записывается следующим образом:

$$\boldsymbol{АНФ}_f = \mu(\boldsymbol{f}) = B^{[n]}\boldsymbol{f};$$
$$\boldsymbol{f} = \mu(\boldsymbol{АНФ}_f) = B^{[n]}(B^{[n]}\boldsymbol{f}).$$

Вычисления ведем в двоичном поле. Данные формулы являются матричной записью определения коэффициентов АНФ способом «треугольник Паскаля».

Пример 4.5. Преобразование Уолша – Адамара.

Данное преобразование проводим в поле $\mathbb{Q}$ рациональных чисел. Предварительно определим некоторые понятия.

Определение 4.8. *Матрицей Адамара порядка k* называется квадратная $k \times k$ матрица *H* с элементами ± 1, такая, что $H \cdot H^{\mathrm{T}} = kE$, где *E* – единичная матрица.

Приведем более общее определение матрицы Адамара.

Определение 4.9. *Циркулянтной матрицей* или *матрицей Адамара* называется квадратная матрица размера $k \times k$, задаваемая своей первой строкой (индекс строки равен нулю)

$$H = (h_{ij}) = cir(a_0, a_1, \dots, a_{k-1}),$$

$$h_{ij} = a_{i+j,}$$

где *i, j* = 0, 1, …, *k* – 1 и сложение в индексах производится по модулю *k*.

Пример матрицы Адамара для $k = 4$:

$$\begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}$$

Определение 4.10. *Матрицей Сильвестра – Адамара* $H^{[n]}$ называется квадратная матрица размера 2^n, определяемая рекуррентным соотношением:

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H^{[n]} = \begin{pmatrix} H^{[n-1]} & H^{[n-1]} \\ H^{[n-1]} & -H^{[n-1]} \end{pmatrix}.$$

Матрицу Сильвестра – Адамара можно определить еще иначе. Обозначим h_{ij} элемент, который находится в строке i и в столбце j матрицы $H^{[n]}$ Сильвестра – Адамара. Номера строк и столбцов этой матрицы лежат во множестве $\{0, 1, \ldots, 2^n - 1\}$. Двоичное представление этих номеров можно рассматривать как векторы в Евклидовом пространстве Z_2^n. Пусть, например, $n = 3$, $i = 0$. Соответствующий вектор будет $\boldsymbol{i} = (0, 0, 0)$. Для $i = 1$ соответствующий вектор будет $\boldsymbol{i} = (0, 0, 1)$. Можно убедиться, что тогда

$$h_{ij} = (-1)^{(\boldsymbol{i},\boldsymbol{j})}.$$

Третий способ формирования матрицы Сильвестра – Адамара основан на ранее приведенной формуле:

$$W_f(\boldsymbol{a}) = < \boldsymbol{F}_f, \boldsymbol{F}_{\boldsymbol{a}} >.$$

где $W_f(\boldsymbol{a})$ – значение функции Уолша на задающем векторе $\boldsymbol{a}$ линейной функции:

$$l_{\boldsymbol{a}}(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x});$$

$\boldsymbol{F}_f, \boldsymbol{F}_{\boldsymbol{a}}$ *– характеристические представления булевой функции* $f(\boldsymbol{x})$ и линейной функции $l_{\boldsymbol{a}}(\boldsymbol{x})$ соответственно. Задающий вектор линейной функции имеет размерность n, его можно рассматривать как двоичную запись некоторого числа из множества целых чисел $\{0, 1, \ldots, 2^n - 1\}$. Столбцы матрицы $H^{[n]}$ и характеристические последовательности линейных функций будем нумеровать числами из этого множества. Тогда справедливо:

$$H^{[n]} = [\boldsymbol{F}_0 \ldots \boldsymbol{F}_{2^n-1}].$$

В матричном виде преобразование Уолша – Адамара записывается в следующем виде:

$$\boldsymbol{W}_f = \boldsymbol{F}_f \cdot H^{[n]}.$$

Свойства матрицы Адамара позволяют записать обращение данной формулы:

$$\boldsymbol{F}_f = \frac{1}{2^n}\,\boldsymbol{W}_f \cdot H^{[n]}.$$

Контрольные вопросы и задания

1. Аддитивный характер поля Галуа. Общее определение.
2. Показать ортогональность аддитивных характеров.
3. Выполнить разложение функции по базису аддитивных характеров (преобразование Фурье) на примере функции f = (№ в списке группы, 4 бита).
4. Привести выражение для вычисления спектра Уолша – Адамара первого рода.
5. Привести порядок расчета коэффициентов Фурье.
6. Характеристическое представление дискретной функции. Дать определение. Привести пример.
7. Привести выражение для вычисления спектра Уолша – Адамара второго рода.
8. Привести порядок расчета коэффициентов преобразования Уолша.
9. Перечислить свойства преобразования Уолша.
10. Статистическая структура дискретной функции. Дать определение. Привести пример.
11. Привести равенство Парсеваля для статистической структуры дискретной функции.
12. Статистический аналог дискретной функции. Дать определение. Привести пример.
13. Привести рекурсивный метод расчета спектра статистической структуры.
14. Привести порядок применения тензорного произведения в расчетах преобразований Мёбиуса, Уолша.

5. КРИТЕРИИ СТАТИСТИЧЕСКОЙ НЕЗАВИСИМОСТИ И КОРРЕЛЯЦИОННОЙ ИММУННОСТИ

5.1. Статистическая независимость

Утверждение 5.1. Функция $f(\boldsymbol{x}, \boldsymbol{y})$, где $\boldsymbol{x}, \boldsymbol{y}$ переменные, которые определены в линейных пространствах $\mathbb{Z}_2^n$ и $\mathbb{Z}_2^m$ соответственно, статистически не зависит от переменных в векторе $\boldsymbol{x}$, тогда и только тогда, когда функция $f(\boldsymbol{x}, \boldsymbol{y}) \oplus (\boldsymbol{u}, \boldsymbol{x})$ уравновешена для любого ненулевого вектора $\boldsymbol{u} \in \mathbb{Z}_2^n$.

Доказательство. Условие статистической независимости функции f от переменных в векторе $\boldsymbol{x}$ равносильно выполнению равенства

$$\| f(\boldsymbol{a}, \boldsymbol{y}) \| = \frac{\| \boldsymbol{f} \|}{2^n}$$

для любого вектора $\boldsymbol{a} \in \mathbb{Z}_2^n$.

Необходимость. Разложим функцию $f(\boldsymbol{x}, \boldsymbol{y}) \oplus (\boldsymbol{u}, \boldsymbol{x})$ по всем переменным вектора $\boldsymbol{x}$; коэффициенты этого разложения имеют вид

$$f_a(\boldsymbol{y}) = f(\boldsymbol{a}, \boldsymbol{y}) \oplus (\boldsymbol{u}, \boldsymbol{a})$$

для всевозможных $\boldsymbol{a} \in \mathbb{Z}_2^n$. Если $(\boldsymbol{u}, \boldsymbol{a}) = 0$, то

$$\| f_{\boldsymbol{a}}(\boldsymbol{y}) \| = \| f(\boldsymbol{a}, \boldsymbol{y}) \| = \frac{\| \boldsymbol{f} \|}{2^n}.$$

Если $(\boldsymbol{u}, \boldsymbol{a}) = 1$, то

$$\| f_{\boldsymbol{a}}(\boldsymbol{y}) \| = 2^m - \| f(\boldsymbol{a}, \boldsymbol{y}) \| = 2^m - \frac{\| \boldsymbol{f} \|}{2^n}.$$

Вес функции $f(\boldsymbol{x}, \boldsymbol{y}) \oplus (\boldsymbol{u}, \boldsymbol{x})$ будет

$$\| f(\boldsymbol{x}, \boldsymbol{y}) \oplus (\boldsymbol{u}, \boldsymbol{x}) \| = \frac{2^{n-1}}{2^n} \| \boldsymbol{f} \| + 2^{n-1} \left(2^m - \frac{\| \boldsymbol{f} \|}{2^n} \right) = 2^{n+m-1},$$

что доказывает уравновешенность функции $f(\boldsymbol{x}, \boldsymbol{y}) \oplus (\boldsymbol{u}, \boldsymbol{x})$.

Достаточность. Покажем, что для $\boldsymbol{a} = \boldsymbol{0}$ выполняется соотношение для веса функции: $\| f(\boldsymbol{x}, \boldsymbol{y}) \| = \frac{\| \boldsymbol{f} \|}{2^n}$. Запишем вес функции $f(\boldsymbol{x}, \boldsymbol{y}) \oplus (\boldsymbol{u}, \boldsymbol{x})$ как сумму весов коэффициентов разложения и учтем уравновешенность этой функции:

$$\| f(\boldsymbol{x}, \boldsymbol{y}) \oplus (\boldsymbol{u}, \boldsymbol{x}) \| = 2^{n+m-1} =$$

$$= \sum_{\boldsymbol{a} \in \mathbb{Z}_2^n} \| f(\boldsymbol{a}, \boldsymbol{y}) \oplus (\boldsymbol{u}, \boldsymbol{a}) \| =$$

$$= \sum_{\boldsymbol{a}, (\boldsymbol{u}, \boldsymbol{a}) = 0} \left| \| f(\boldsymbol{a}, \boldsymbol{y}) \| \right| + \sum_{\boldsymbol{a}, (\boldsymbol{u}, \boldsymbol{a}) = 1} (2^m - \| f(\boldsymbol{a}, \boldsymbol{y}) \|).$$

Отсюда следует, что

$$\sum_{\boldsymbol{a},(\boldsymbol{u},\boldsymbol{a})=0} \big||f\ (\boldsymbol{a},\boldsymbol{y})|\big| = \sum_{\boldsymbol{a},(\boldsymbol{u},\boldsymbol{a})=1} \big||f\ (\boldsymbol{a},\boldsymbol{y})|\big|.$$

Просуммируем обе части последнего равенства по всем $\boldsymbol{u} \neq \boldsymbol{0}$:

$$\sum_{\boldsymbol{u}\neq\boldsymbol{0}} \sum_{\boldsymbol{a},(\boldsymbol{u},\boldsymbol{a})=0} \big||f\ (\boldsymbol{a},\boldsymbol{y})|\big| = \sum_{\boldsymbol{u}\neq\boldsymbol{0}} \sum_{\boldsymbol{a},(\boldsymbol{u},\boldsymbol{a})=1} \big||f\ (\boldsymbol{a},\boldsymbol{y})|\big|.$$

При любых фиксированных $\boldsymbol{a} \neq \boldsymbol{0}$ и всех $\boldsymbol{u} \neq \boldsymbol{0}$ равенство $(\boldsymbol{u},\boldsymbol{a}) = 1$ выполняется 2^{n-1} раз, а равенство $(\boldsymbol{u},\boldsymbol{a}) = 0$ верно в остальных $2^{n-1}-1$ случаях. При $\boldsymbol{a} = \boldsymbol{0}$ равенство $(\boldsymbol{u},\boldsymbol{a}) = 0$ выполняется всегда. Получаем соотношение

$$(2^n-1)\big||f\ (\boldsymbol{0},\boldsymbol{y})|\big| + (2^{n-1}-1)\sum_{\boldsymbol{a}\neq\boldsymbol{0}} \big||f\ (\boldsymbol{a},\boldsymbol{y})|\big| = 2^{n-1}\sum_{\boldsymbol{a}\neq\boldsymbol{0}} \big||f\ (\boldsymbol{a},\boldsymbol{y})|\big|.$$

Тогда

$$\sum_{\boldsymbol{a}} \big||f\ (\boldsymbol{a},\boldsymbol{y})|\big| = 2^n\big||f\ (\boldsymbol{0},\boldsymbol{y})|\big|$$

$$\big||f\ (\boldsymbol{0},\boldsymbol{y})|\big| = \frac{||\boldsymbol{f}||}{2^n}.$$

Пусть $\boldsymbol{a} \neq \boldsymbol{0}$. Рассмотрим функцию $g(\boldsymbol{x},\boldsymbol{y}) = f(\boldsymbol{x} \oplus \boldsymbol{a},\boldsymbol{y})$. Очевидно, что $\|\boldsymbol{f}\| = \|\boldsymbol{g}\|$ и $f(\boldsymbol{a},\boldsymbol{y}) = g(\boldsymbol{0},\boldsymbol{y})$; кроме того, функция $g(\boldsymbol{x},\boldsymbol{y}) \oplus (\boldsymbol{u},\boldsymbol{x})$ уравновешена в случае уравновешенности функции $f(\boldsymbol{x},\boldsymbol{y}) \oplus (\boldsymbol{u},\boldsymbol{x})$, так как

$$\|g\ (\boldsymbol{x},\boldsymbol{y})\ \oplus\ (\boldsymbol{u},\boldsymbol{x})\ \| = \sum_{\boldsymbol{x},\boldsymbol{y}} \big(f\ (\boldsymbol{x}\ \oplus\ \boldsymbol{a},\boldsymbol{y})\ \oplus\ (\boldsymbol{u},\boldsymbol{x})\big) =$$

$$= \sum_{\boldsymbol{x},\boldsymbol{y}} \big(f\ (\boldsymbol{x},\boldsymbol{y})\ \oplus\ (\boldsymbol{u},\boldsymbol{x}\ \oplus \boldsymbol{a})\big) = \sum_{\boldsymbol{x},\boldsymbol{y}} \big(f\ (\boldsymbol{x},\boldsymbol{y})\ \oplus\ (\boldsymbol{u},\boldsymbol{x}) \oplus (\boldsymbol{u},\boldsymbol{a})\big).$$

Последняя сумма есть вес функции $f(\boldsymbol{x},\boldsymbol{y}) \oplus (\boldsymbol{u},\boldsymbol{x})$. Так как $\|g\ (\boldsymbol{0},\boldsymbol{y})\| = \|\boldsymbol{g}\| \cdot 2^{-n}$, то $\|f\ (\boldsymbol{a},\boldsymbol{y})\| = \|\boldsymbol{f}\| \cdot 2^{-n}$.■

Ясно, что функция $f(\boldsymbol{x},\boldsymbol{y}) \oplus (\boldsymbol{u},\boldsymbol{x})$, уравновешена, тогда и только тогда, когда $W_f(\boldsymbol{u},\boldsymbol{0}) = 0$. С учетом этого критерий статистической независимости может быть переформулирован в следующее утверждение.

Утверждение 5.2. Функция $f(\boldsymbol{x},\boldsymbol{y}) \oplus (\boldsymbol{u},\boldsymbol{x})$, где $\boldsymbol{x}$, $\boldsymbol{y}$ – переменные со значениями в пространствах $\mathbb{Z}_2^n$ и $\mathbb{Z}_2^m$ соответственно статистически

не зависят от переменных в $\boldsymbol{x}$, тогда и только тогда, когда для любого ненулевого вектора $\boldsymbol{u} \in \mathbb{Z}_2^n$ имеет место равенство $W_f(\boldsymbol{u}, \boldsymbol{0}) = 0$.

Пример 5.1. Зададим функцию f и определим W_f (табл. 5.1)

Таблица 5.1

x_1	x_2	x_3	f	W_f
0	0	0	1	0
0	0	1	1	0
0	1	0	0	–4
0	1	1	0	4
1	0	0	0	0
1	0	1	1	0
1	1	0	1	–4
1	1	1	0	–4

Из табл. 5.1 видно, что функция статистически не зависит от переменной x_1, x_3.

Основное следствие

Теорема 5.1. (без доказательства) Функция $f(\boldsymbol{x}) \in P_2(n)$ является корреляционно-иммунной порядка m тогда и только тогда, когда $W_f(\boldsymbol{a}) = 0$ для $\forall\ \boldsymbol{a} \in \mathbb{Z}_2^n$, таких, что $1 \le \| \boldsymbol{a} \| \le m$.

Другими словами, функция $f(\boldsymbol{x}) \in P_2(n)$ является m-устойчивой тогда и только тогда, когда $W_f(\boldsymbol{a}) = 0$ для $\forall\ \boldsymbol{a} \in \mathbb{Z}_2^n$, таких, что $0 \le \| \boldsymbol{a} \| \le m$.

5.2. Статистическая независимость суперпозиции функций

Утверждение 5.3. Пусть $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ – переменные из пространств $\mathbb{Z}_2^n$, $\mathbb{Z}_2^m$ и $\mathbb{Z}_2^l$ соответственно; функция $f(\boldsymbol{x}, \boldsymbol{y})$ статистически не зависит от переменных в $\boldsymbol{x}$. Тогда и функция $h(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = g(f(\boldsymbol{x}, \boldsymbol{y}), \boldsymbol{z})$, где g – любая функция от $l + 1$ переменных, статистически не зависит от переменных в $\boldsymbol{x}$.

Доказательство. Пусть $\boldsymbol{u}$ – любой ненулевой вектор из $\mathbb{Z}_2^n$; тогда $W_f(\boldsymbol{u}, \boldsymbol{0}) = 0$. Вычислим коэффициент Уолша – Адамара для функции h:

$$W_h(\boldsymbol{u}, \boldsymbol{0}, \boldsymbol{0}) = \sum_{\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}} (-1)^{g\,(f\,(\boldsymbol{x},\boldsymbol{y}),\boldsymbol{z}) \oplus (\boldsymbol{u},\boldsymbol{x})} =$$

$$= \sum_{\boldsymbol{z}} \left(\sum_{\boldsymbol{x},\boldsymbol{y}, f(\boldsymbol{x},\boldsymbol{y})=0} (-1)^{g\,(0,\boldsymbol{z}) \oplus (\boldsymbol{u},\boldsymbol{x})} + \sum_{\boldsymbol{x},\boldsymbol{y}, f(\boldsymbol{x},\boldsymbol{y})=1} (-1)^{g\,(1,\boldsymbol{z}) \oplus (\boldsymbol{u},\boldsymbol{x})} \right).$$

Для каждого $\boldsymbol{z} \in \mathbb{Z}_2^l$ имеет место один из двух следующих случаев:
1) $g\,(0, z) = g\,(1, z) = c \in \mathbb{Z}_2$, тогда

$$A = (-1)^c \sum_{\boldsymbol{x},\boldsymbol{y}} (-1)^{(\boldsymbol{u},\boldsymbol{x})} = 0;$$

2) $g\,(0, z) = g\,(1, z) \oplus 1 = c \in \mathbb{Z}_2$, тогда

$$A = (-1)^c \left(\sum_{\boldsymbol{x},\boldsymbol{y},f(\boldsymbol{x},\boldsymbol{y})=0} (-1)^{(\boldsymbol{u},\boldsymbol{x})} - \sum_{\boldsymbol{x},\boldsymbol{y},f(\boldsymbol{x},\boldsymbol{y})=1} (-1)^{(\boldsymbol{u},\boldsymbol{x})} \right) =$$

$$= (-\mathbf{1})^{\boldsymbol{c}} \sum_{\boldsymbol{x},\boldsymbol{y}} (-\mathbf{1})^{\boldsymbol{f}\,(\boldsymbol{x},\boldsymbol{y}) \oplus (\boldsymbol{u},\boldsymbol{x})} = (-\mathbf{1})^{\boldsymbol{c}}\, \boldsymbol{W_f}\,(\boldsymbol{u}, \mathbf{0}) = \mathbf{0}.$$

Таким образом, $W_h\,(\boldsymbol{u}, \mathbf{0}, \mathbf{0}) = 0$, утверждение доказано. ■

Обобщение доказанного утверждения на случай суперпозиции от нескольких функций в общем не выполняется.

Утверждение 5.4. Пусть $\boldsymbol{x}, \boldsymbol{y}, z$ – переменные из пространств $\mathbb{Z}_2^n$, $\mathbb{Z}_2^m$ и $\mathbb{Z}_2^l$ соответственно; функции $f_1(\boldsymbol{x}, \boldsymbol{y})$, $f_2(\boldsymbol{x}, \boldsymbol{y})$, $u(\boldsymbol{x}, \boldsymbol{y}) = f_1(\boldsymbol{x}, \boldsymbol{y}) \oplus f_2(\boldsymbol{x}, \boldsymbol{y})$ статистически не зависят от переменных в $\boldsymbol{x}$. Тогда и функция $h(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = g(f_1(\boldsymbol{x}, \boldsymbol{y}), f_2(\boldsymbol{x}, \boldsymbol{y}), \boldsymbol{z})$, где g – любая функция от $l + 1$ переменных, статистически не зависит от переменных в $\boldsymbol{x}$.

Доказательство. $\forall\, \boldsymbol{a} \in \mathbb{Z}_2^n, i, j \in \mathbb{Z}_2$ обозначим

$$c_{i,j}^{\boldsymbol{a}} = |\{\boldsymbol{y} \in \mathbb{Z}_2^m : f_1(\boldsymbol{a}, \boldsymbol{y}) = i, f_2(\boldsymbol{a}, \boldsymbol{y}) = j\}|.$$

В силу статистической независимости функций f_1, f_2, u от переменных в $\boldsymbol{x}$ для любого $\boldsymbol{a} \in \mathbb{Z}_2^n$ выполняется

$$c_{10}^{\boldsymbol{a}} + c_{11}^{\boldsymbol{a}} = \frac{\|f_1\|}{2^n},$$

$$c_{01}^{\boldsymbol{a}} + c_{11}^{\boldsymbol{a}} = \frac{\|f_2\|}{2^n},$$

$$c_{01}^{\boldsymbol{a}} + c_{10}^{\boldsymbol{a}} = \frac{\|u\|}{2^n}.$$

Отсюда получаем, что

$$c_{01}^{\boldsymbol{a}} = \frac{\|u\| - \|f_1\| + \|f_2\|}{2^{n+1}},$$

$$c_{10}^{\boldsymbol{a}} = \frac{\|u\| + \|f_1\| - \|f_2\|}{2^{n+1}},$$

$$c_{11}^{\boldsymbol{a}} = \frac{\|f_1\| + \|f_2\| - \|u\|}{2^{n+1}},$$

$$c_{00}^{\boldsymbol{a}} = 2^m - \frac{\|f_1\| + \|f_2\| + \|u\|}{2^{n+1}}.$$

Другими словами, $c_{i,j}^{\boldsymbol{a}}$ не зависит от $\boldsymbol{a}$ для всех $i, j \in \mathbb{Z}_2$. Тогда и вес подфункции h, полученной фиксацией переменных в $\boldsymbol{x}$ набором значений в $\boldsymbol{a}$, не зависит от $\boldsymbol{a}$, так как

$$\|h\,(\boldsymbol{a}, \boldsymbol{y}, \boldsymbol{z})\| = \sum_{i,j \in \mathbb{Z}_2} c_{i,j}^{\boldsymbol{a}} \cdot \|g\,(i, j, \boldsymbol{z})\|.$$

Следовательно, функция h статистически не зависит от переменных в $\boldsymbol{x}$. ■

Следующее утверждение дает условия статистической независимости от переменных в $\boldsymbol{x}$ для суммы двух функций в одном частном случае – когда одна из функций зависит только от $\boldsymbol{x}$.

Утверждение 5.5. Пусть $\boldsymbol{x}$, $\boldsymbol{y}$ – переменные из пространств $\mathbb{Z}_2^n$ и $\mathbb{Z}_2^m$ соответственно и функция $f(\boldsymbol{x}, \boldsymbol{y})$ статистически не зависит от переменных в $\boldsymbol{x}$. Тогда сумма функций $f(\boldsymbol{x}, \boldsymbol{y}) + g(\boldsymbol{x})$, где $g(\boldsymbol{x})$ – любая функция от n переменных, статистически не зависит от переменных в $\boldsymbol{x}$, тогда и только тогда, когда f уравновешена или g является константой.

Доказательство. По условию теоремы для всякого $\boldsymbol{a} \in \mathbb{Z}_2^n$ выполняется

$$\|f\,(\boldsymbol{a}, \boldsymbol{y})\,\| = \frac{\|f\|}{2^n},$$

следовательно, $\|f(\boldsymbol{a}, \boldsymbol{y}) \oplus g(\boldsymbol{a})\|$ не зависит от $\boldsymbol{a}$ тогда и только тогда, когда g является константой или

$$\frac{\|f\|}{2^n} = 2^m - \frac{\|f\|}{2^n}.$$

Последнее равенство равносильно уравновешенности. ■

5.3. Необходимые условия корреляционной иммунности

Теорема 5.2.

1. Если функция $f(\boldsymbol{x}) \in P_2(n)$ является корреляционно-иммунной порядка $m \le n - 1$, то значение $\boldsymbol{W_f(a)}$ делится на 2^{m+1} для всех $\boldsymbol{a} \in \mathbb{Z}_2^n$.

2. Если $f(\boldsymbol{x}) \in P_2(n)$ уравновешена и корреляционно-иммунная порядка $m \le n - 2$, то значение $\boldsymbol{W_f(a)}$ делится на 2^{m+2} для всех $\boldsymbol{a} \in \mathbb{Z}_2^n$.

Доказательство проводится индукцией по весу задающего вектора $\boldsymbol{a}$.

База индукции

Имеем:

- $\boldsymbol{W_f(0)} = 2^n - 2\,\|\boldsymbol{f}\|$;
- 2^n делится на 2^{m+1}, так как $m + 1 \le n$;
- $\|\boldsymbol{f}\|$ делится на 2^m в силу корреляционной иммунности функции $f(\boldsymbol{x})$.

Тогда $\boldsymbol{W_f(0)}$ делится на 2^{m+1}.

Кроме того, ясно, что коэффициенты спектра Уолша $\boldsymbol{W_f(a)}$ делятся на 2^{m+1} для всех векторов $\boldsymbol{a}$, вес которых не превосходит m, так как для этих векторов выполняется равенство $\boldsymbol{W_f(a)} = 0$.

Предположение индукции

Пусть $\boldsymbol{W_f(b)}$ делится на 2^{m+1} для всех таких векторов $\boldsymbol{b}$, $\|\boldsymbol{b}\| \le k$, $k \ge m$.

Шаг индукции

Пусть $\|\boldsymbol{a}\| = k + 1$. Воспользуемся тождеством Саркара:

$$\sum_{\boldsymbol{b} \le \boldsymbol{a}} W_f(\boldsymbol{b}) = 2^n - 2^{k+2} \cdot \|f^{\boldsymbol{a}}\|.$$

В правой части тождества 2^n делится на 2^{m+1} и 2^{k+2} делится на 2^{m+1}; в левой части тождества по предположению индукции все слагаемые кроме $\boldsymbol{W_f(a)}$ делятся на 2^{m+1}. Следовательно, $\boldsymbol{W_f(a)}$ делится на 2^{m+1}.

Для уравновешенной функции $\boldsymbol{W_f(0)} = 0$, поэтому $\boldsymbol{W_f(0)}$ делится на 2^{m+2}. Доказательство по индукции проводится аналогично. ■

Контрольные вопросы и задания

1. Привести критерий статистической независимости функции от переменных в ее аргументе.
2. Сформулировать критерий m-устойчивости дискретной функции.
3. Сформулировать необходимые условия корреляционной иммунности.

6. НЕЛИНЕЙНОСТЬ БУЛЕВЫХ ФУНКЦИЙ

Для дискретных функций, определенных над полем *GF* (2), понятие нелинейности и ее численное значение являются базовыми характеристиками. В отличие от алгебраической нелинейности данная характеристика определяет удаленность булевой функции от классов линейных и аффинных функций.

Считается, что существование у криптографической функции свойств, близких к линейным, безусловно считается слабостью.

Определение 6.1. *Нелинейностью N_f булевой функции* $f(\boldsymbol{x})$ называется расстояние в метрике Хемминга от вектора значений данной функции до ближайшего вектора значений аффинных функций.

Нелинейность может быть определена через коэффициенты спектра Уолша – Адамара:

$$N_f = \rho(\boldsymbol{f}, \mathcal{A}(n)) = 2^{n-1} - 0{,}5 \max_{\boldsymbol{a} \in Z_2^n} \left|W_f(\boldsymbol{a})\right|.$$

Воспользуемся равенством Парсеваля:

$$\sum_{\boldsymbol{a} \in Z_2^n} W_f^2(\boldsymbol{a}) = 2^{2n}.$$

Поскольку количество коэффициентов в спектре Уолша – Адамара равно 2^n, для максимального по модулю значения коэффициента Уолша – Адамара справедливо неравенство

$$\max_{\boldsymbol{a} \in Z_2^n} \left|W_f(\boldsymbol{a})\right| \geq 2^{n/2}.$$

Отсюда следует, что для нелинейности N_f произвольной булевой функции $f(\boldsymbol{x})$ выполняется верхняя оценка

$$N_f \leq 2^{n-1} - 2^{n/2-1}.$$

Для булева отображения $\varphi_{n,m}$: $Z_2^n \to Z_2^m$, $\varphi(\boldsymbol{x}) = (f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), \ldots, f_m(\boldsymbol{x}))$ нелинейность характеризуется параметром

$$N_\varphi = \min_{\boldsymbol{c} \neq \boldsymbol{0},\ \boldsymbol{c} \in \mathbb{Z}_2^{\boldsymbol{m}}} \{N_{(\boldsymbol{c}, \boldsymbol{\varphi})}\},$$

где $N_{(\boldsymbol{c}, \boldsymbol{\varphi})}$ – нелинейность булевой функции $(\boldsymbol{c}, \boldsymbol{\varphi}) = c_1 f_1 \oplus c_2 f_2 \oplus \ldots \oplus c_m f_m$.

Определение 6.2. *Наилучшим аффинным приближением функции* $f(\boldsymbol{x})$ (*статистическим аналогом*) называется ближайшая к $\boldsymbol{f}$ аффинная функция.

Процедура определения статистического аналога булевой функции выполняется следующим образом. Пусть нашелся вектор $\boldsymbol{b}$, на котором достигается экстремум функции Уолша:

$$\max_{\boldsymbol{a} \in Z_2^n} \left|W_f(\boldsymbol{a})\right| = \left|W_f(\boldsymbol{b})\right|.$$

Если $W_f(\boldsymbol{b}) > 0$, то статистическим аналогом будет линейная функция

$$l_b(\boldsymbol{x}) = (\boldsymbol{b}, \boldsymbol{x}).$$

Если же $W_f(\boldsymbol{b}) < 0$, то наилучшим приближением будет аффинная функция $(\boldsymbol{b}, \boldsymbol{x}) \oplus 1$.

Пример 6.1. Пусть $\boldsymbol{f}$ = (0111 1010). Коэффициенты преобразования Уолша – Адамара будут W_f = (–2, –2, 2, 2, 2, 6, 2, 2). Max | W_f | = 6 = W_f (5). $5_{10} = 101_2$. Статистический аналог функции составит

$$l_5(\boldsymbol{x}) = (\boldsymbol{a}_5, \boldsymbol{x}) = x_1 \oplus x_3.$$

Расстояние от любой булевой функции до класса аффинных: $\rho(\boldsymbol{f}, \mathcal{A}(n)) = 2^2 - 0{,}5 \cdot 6 = 1$.

Вероятность совпадения значений булевой функции и ее статистического аналога:

$$P\{f(\boldsymbol{x}) = (\boldsymbol{a}_5, \boldsymbol{x})\} = 0{,}5 + \frac{S_f(\boldsymbol{a}_5)}{2^n} = 0{,}5 + \frac{W_f(\boldsymbol{a}_5)}{2^{n+1}} = \frac{7}{8} = 0{,}875.$$

Перекос вероятности:

$$\delta_p = 0{,}375.$$

В табл. 6.1 даны номера задающих векторов $\boldsymbol{a_i}$, векторные представления этих векторов (или аргументы булевой функции), вектора значений булевой функции, ее характеристического представления, вектор коэффициентов спектра Уолша – Адамара и значения ближайшей линейной функции.

Таблица 6.1

№	$\boldsymbol{a}, \boldsymbol{x}$			$f(\boldsymbol{x})$	$F_f(\boldsymbol{x})$	$W_f(\boldsymbol{a})$	$x_1 \oplus x_3$
0	0	0	0	0	1	–2	0
1	0	0	1	1	–1	–2	1
2	0	1	0	1	–1	2	0
3	0	1	1	1	–1	2	1
4	1	0	0	1	–-1	2	1
5	1	0	1	0	1	6	0
6	1	1	0	1	–1	2	1
7	1	1	1	0	1	2	0

6.1. Основные свойства нелинейности

1. Пусть $f(\boldsymbol{x}) \in P_2(n)$, $h(\boldsymbol{x}) \in \mathcal{A}(n)$. Тогда $N_f = N_{f \oplus h}$.

Это следует из того, что аффинная добавка не меняет спектра функции. ■

2. Пусть $f(\boldsymbol{x}, y) = g(\boldsymbol{x}) \oplus c \cdot y$, $c \in \mathbb{Z}_2$, т. е. функция f зависит от переменной y фиктивно или линейно. Тогда $N_f = 2N_g$.

Доказательство. Пусть $\boldsymbol{x}, \boldsymbol{a} \in \mathbb{Z}_2^n$, $b, y \in \mathbb{Z}_2$. Тогда

$$N_f = \min_{\boldsymbol{a}, \boldsymbol{x}, e} \rho\,(f, (\boldsymbol{a}b\,,\ \boldsymbol{x}y) \oplus e) = \min_{\boldsymbol{a}, \boldsymbol{x}, e} \|h\,(\boldsymbol{x}, y)\|.$$

Здесь

$$h\,(\boldsymbol{x}, y) = \ g(\boldsymbol{x})\ \oplus cy\ \oplus (\boldsymbol{a}, \boldsymbol{x})\ \oplus by\ \oplus e.$$

Если $c \oplus b = 1$, то h зависит от y линейно, следовательно она уравновешена: $\|\boldsymbol{h}\| = \ 2^n$.

Если $c \oplus b = 1$, то h зависит от y фиктивно. Тогда

$$\|\boldsymbol{h}\| = \ 2\,\|g\,(\boldsymbol{x})\ \oplus(\boldsymbol{a}, \boldsymbol{x})\ \oplus e\| = 2\rho\,(\boldsymbol{g},\ (\boldsymbol{a}, \boldsymbol{x})\ \oplus e)\ \geq 2N_f\,.$$

Первое равенство верно по утверждению 1, последнее неравенство – по определению нелинейности, для некоторых $\boldsymbol{a}$, e в нем достигается равенство. Таким образом,

$$N_f = \min\left(2^n, 2N_g\right).$$

Ввиду $N_g < 2^{n-1}$ получаем $N_f = 2N_g$. ■

3. Пусть $f(\boldsymbol{x}, y, z) = g(\boldsymbol{x}, y \oplus z) \oplus y$, т. е. f зависит от переменных y, z квазилинейно. Тогда $N_f = 2N_g$.

Доказательство. Пусть $\boldsymbol{x}, \boldsymbol{a} \in \mathbb{Z}_2^n$, $b, c, d \in \mathbb{Z}_2$. Тогда

$$N_f = \min_{\boldsymbol{a}, \boldsymbol{x}, c, d} \|h\,(\boldsymbol{x}, y, z)\|.$$

Здесь

$$h\,(\boldsymbol{x}, y, z) = f\,(\boldsymbol{x}, y, z) \oplus (\boldsymbol{a}, \boldsymbol{x}) \oplus by\ \oplus cz\ \oplus d =$$

$$= g\,(\boldsymbol{x}, y\ \oplus z) \oplus (\boldsymbol{a}, \boldsymbol{x})\ \oplus (b\ \oplus 1) \oplus cz\ \oplus d.$$

Вариант 1. $b = c$.

В таком варианте получаем:

$$h\,(\boldsymbol{x}, y, z) = \ g\,(\boldsymbol{x}, y\ \oplus z) \oplus (\boldsymbol{a}, \boldsymbol{x}) \oplus b(y\ \oplus z) \oplus y \oplus d =$$

$$= h'\,(\boldsymbol{x}, y\ \oplus z) \oplus y.$$

То есть, функция h по определению имеет квазилинейные переменные. Кроме того

$$\|h\| = 2^{n+1}.$$

Вариант 2. $b \oplus 1 = c$.

В этом варианте получаем:

$$h\,(\boldsymbol{x}, y, z) = g\,(\boldsymbol{x}, y \oplus z) \oplus (\boldsymbol{a}, \boldsymbol{x}) \oplus c(y \oplus z) \oplus d = h'\,(\boldsymbol{x}, y \oplus z).$$

Для веса функции h имеем выражение

$$\|h\| = 2\,\|h'\| \geq 2\,N_g.$$

Для некоторых $\boldsymbol{a}$, c, d равенство достигается. Таким образом,

$$N_f = \min\left(2^{n+1}, 2N_g\right) = 2N_g. \blacksquare$$

6.2. Максимально нелинейные (бент-) функции и их свойства

Определение 6.3. Функция $f(\boldsymbol{x}) \in P_2(n)$ называется *максимально нелинейной функцией*, если ее нелинейность N_f достигает максимального для функций из $P_2\,(n)$ значения.

Определение описывает класс функций $\mathcal{B}\,(n)$, максимально удаленных от класса $\mathcal{A}\,(n)$ аффинных булевых функций.

Определение 6.4. Функция $f(\boldsymbol{x}) \in P_2(n)$ называется *бент-функцией*, если все коэффициенты Уолша – Адамара данной функции равны $\pm 2^{n/2}$.

Поскольку коэффициенты Уолша – Адамара являются целыми числами, то для нечетного n бент-функции не определены. Из равенства Парсеваля следует представленное далее утверждение.

Утверждение 6.1. При четном n множество максимально нелинейных функций совпадает с множеством бент-функций.

Простейшие свойства бент-функций

1. Бент-функции не уравновешены.
2. Если $f(\boldsymbol{x}) \in \mathcal{B}(n)$, то $\|\boldsymbol{f}\| = 2^{n-1} \pm 2^{\,n/2-1}$.
3. Бент-функции статистически зависят от всех своих аргументов.
4. Пусть $f(\boldsymbol{x}) \in \mathcal{B}(n)$, $h(\boldsymbol{x}) \in \mathcal{A}\,(n)$. Тогда $f \oplus h \in \mathcal{B}(n)$.

5. $f(x_1, x_2) = x_1 x_2$ – бент-функция.

6. Пусть $f(\boldsymbol{x}) \in P_2(n)$, $g(\boldsymbol{x}) \in P_2(m)$ – функции от непересекающихся множеств переменных. Тогда $f \oplus g \in \mathcal{B}(n)$ тогда и только тогда, когда $(f \in \mathcal{B}(n))$ & $(g \in \mathcal{B}(n))$.

Доказательство

Достаточность. Пусть $W_f(\boldsymbol{a}) = \pm 2^{n/2}, W_g(\boldsymbol{b}) = \pm 2^{m/2}$.

Тогда

$$W_{f\oplus g}(\boldsymbol{ab}) = W_f(\boldsymbol{a}) W_g(\boldsymbol{b}) = \pm 2^{(n+m)/2}.$$

Следовательно, $f \oplus g$ – бент-функция.

Необходимость. Пусть

$$W_{f\oplus g}(\boldsymbol{ab}) = \pm 2^{(n+m)/2}$$

для всех $\boldsymbol{a}$, $\boldsymbol{b}$. Предположим, что $W_f(\boldsymbol{a}) = k$ для некоторого $\boldsymbol{a}$. Тогда

$$W_g(\boldsymbol{b}) = \frac{\pm 2^{(n+m)/2}}{k}$$

для всех $\boldsymbol{b} \in \mathbb{Z}_2^m$. Воспользуемся равенством Парсеваля и запишем

$$2^{2m} = \sum_{\boldsymbol{b}} W_g(\boldsymbol{b})^2 = 2^m \frac{2^{n+m}}{k^2}.$$

Отсюда получаем, что $k^2 = 2^n$, $k = \pm 2^{n/2}$, $W_g(\boldsymbol{b}) = \pm 2^{m/2}$. Следовательно, f, g – бент-функции. ■

7. Класс бент-функций замкнут относительно аффинного преобразования переменных.

Теорема 6.1. (О степени бент-функции).

Пусть $f(\boldsymbol{x}) \in \mathcal{B}(n)$, $n \geq 4$. Тогда

$$\deg(f) \leq n/2.$$

Доказательство. Воспользуемся тождеством Саркара:

$$\sum_{\boldsymbol{a} \preccurlyeq \boldsymbol{b}} W_f(\boldsymbol{a}) = 2^n - 2^{\|\boldsymbol{b}\|+1} \cdot \left\| f^{\boldsymbol{b}} \right\|.$$

В подфункции $f^{\boldsymbol{b}}$ вектор $\boldsymbol{b}$ определяет фиксацию переменных в $\boldsymbol{x}$. Если компонента b_i равна единице, то на месте компоненты x_i аргумента $\boldsymbol{x}$ функции $f(\boldsymbol{x})$ записывается нуль. Нулевое значение компоненты b_i

на компоненту x_i не влияет. Другими словами, подфункция $f^{\boldsymbol{b}}$ определена на векторах $\boldsymbol{x}$, для которых выполняется неравенство $\boldsymbol{x} \preccurlyeq \overline{\boldsymbol{b}}$. В таком случае воспользуемся преобразованием Мебиуса и получим

$$\left\| f^{\boldsymbol{b}} \right\| = \sum_{\boldsymbol{x} \preccurlyeq \overline{\boldsymbol{b}}.} f\ (\boldsymbol{x}) = g\left(\overline{\boldsymbol{b}}\right) \bmod 2.$$

Здесь $g = \mu\ (f)$. Из двух последних равенств получаем следующее:

$$g\left(\overline{\boldsymbol{b}}\right) = \ 2^{n - \|\boldsymbol{b}\| - 1} - \frac{1}{2^{\|\boldsymbol{b}\| + 1}} \sum_{\boldsymbol{a} \preccurlyeq \boldsymbol{b}} W_f(\boldsymbol{a}) =$$

$$= \ 2^{\|\overline{\boldsymbol{b}}\| - 1} - \frac{1}{2^{\|\boldsymbol{b}\| + 1}} \sum_{\boldsymbol{a} \preccurlyeq \boldsymbol{b}} W_f(\boldsymbol{a}) \bmod 2.$$

Рассмотрим произвольный вектор $\boldsymbol{b}$, такой, что $\left\|\overline{\boldsymbol{b}}\right\| > 0{,}5\, n$, или $\|\boldsymbol{b}\| < 0{,}5\ n$. Так как $0{,}5n \geq 2$, получаем

$$2^{\|\overline{\boldsymbol{b}}\| - 1} = 0 \bmod 2.$$

Рассмотрим сумму $S = \sum_{\boldsymbol{a} \preccurlyeq \boldsymbol{b}} W_f(\boldsymbol{a})$. Если $\|\boldsymbol{b}\| = 0$, то $S = W_f(\boldsymbol{0}) = \ = \ \pm 2^{n/2}$, тогда $0{,}5 \cdot S = 0 \bmod 2$.

Если $\|\boldsymbol{b}\| \neq 0$, то S – сумма четного числа слагаемых вида $\pm\ 2^{n/2}$, или $S = (k_1 - k_2)2^{n/2}$, коэффициенты k_1 и k_2 – количества положительных и отрицательных слагаемых соответственно. Так как $k_1 - k_2 = 0 \bmod 2$ получаем, что $S = 0 \bmod 2^{n/2\ -1}$. Отсюда $\frac{S}{2^{\|\boldsymbol{b}\| + 1}} = 0 \bmod 2$ ввиду того, что $\|\boldsymbol{b}\| > n/2$. Следовательно, deg $(f) \leq\ n/2$. ■

Из данной теоремы получается верхняя оценка количества бент-функций:

$$|\mathcal{B}\ (n)| \leq\ 2^{2^{n-1}\ + 0{,}5 C_n^{n/2}}.$$

Отметим, что все квадратичные бент-функции от n переменных аффинно-эквивалентны функции

$$f(\boldsymbol{x}) = \ x_1 x_2 \oplus x_3 x_4 \oplus \ldots \oplus x_{n-1} x_n.$$

Следующая теорема характеризует бент-функции с помощью матриц Адамара.

Теорема 6.2. Функция $f(\boldsymbol{x}) \in P_2(n)$, где n – четное, является бент-функцией тогда и только тогда, когда матрица

$$H = 2^{-n/2}\left(W_f\,(\boldsymbol{a} \oplus \boldsymbol{b}\right)$$

есть матрица Адамара.

Здесь $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_2^n$. Представление координат векторов $\boldsymbol{a}, \boldsymbol{b}$ двоичными числами дает номер строки матрицы H (вектор $\boldsymbol{a}$) и номер столбца матрицы H (вектор $\boldsymbol{b}$). Нумерация их начинается с нуля.

Доказательство

Достаточность. Элементы матрицы Адамара принимают значения ± 1, поэтому $W_f(\boldsymbol{a} \oplus \boldsymbol{b}) = \pm 2^{n/2}$ для всех $\boldsymbol{a}, \boldsymbol{b}$, т. е. f – бент-функция.

Необходимость.

Ясно, что элементы матрицы H принимают значения ± 1.

Рассмотрим произвольный элемент h_{ij} произведения матриц HH^{T}:

$$h_{ij} = 2^{-n} \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} W_f\,(\boldsymbol{a} \oplus \boldsymbol{x}) W_f\,(\boldsymbol{x} \oplus \boldsymbol{b}) =$$

$$= 2^{-n} \sum_{\boldsymbol{x}} W_f(\boldsymbol{x}) W_f(x \oplus \boldsymbol{a} \oplus \boldsymbol{b}) = 2^{-n} 2^{2n}\, \delta(\boldsymbol{a} \oplus \boldsymbol{b}, \boldsymbol{0}) = 2^n \delta(\boldsymbol{a}, \boldsymbol{b}).$$

Определение матрицы Адамара выполняется. ■

Определение 6.5. Пусть $f(\boldsymbol{x}) \in \mathcal{B}\,(n)$. *Дуальной к f функции* называется функция $\tilde{f}$, определяемая из соотношения

$$(-1)^{\tilde{f}(\boldsymbol{x})} = \frac{1}{2^{n/2}} W_f(\boldsymbol{x}).$$

Очевидно, что $\tilde{f}(\boldsymbol{x}) \in P_2(n)$.

Пример 6.2.

В табл. 6.2 приведены представления функции, ее представления Уолша и ее функции, дуальной к ней.

Таблица 6.2

$\boldsymbol{x}$		$f(\boldsymbol{x})$	$W_f(\boldsymbol{x})$	$\tilde{f}(\boldsymbol{x})$
0	0	1	2	0
0	1	0	–2	1
1	0	0	–2	1
1	1	0	–2	1

Свойства дуальных функций

1. $\tilde{f}(\boldsymbol{x})$ – бент-функция. *Доказательство:*

$$W_{\check{f}}(\boldsymbol{a}) = \sum_{\boldsymbol{x}} (-1)^{\tilde{f}(x) \oplus (\boldsymbol{a},\boldsymbol{x})} =$$

$$= 2^{-\frac{n}{2}} \sum_{\boldsymbol{x}} W_f(\boldsymbol{x})(-1)^{(\boldsymbol{a},\boldsymbol{x})} = 2^{\frac{n}{2}}(-1)^{f(\boldsymbol{a})} = \pm 2^{\frac{n}{2}}.$$

2. $\tilde{\tilde{f}} = f$, так как

$$(-1)^{\tilde{\tilde{f}}} = 2^{-n/2} W_{\tilde{f}}(\boldsymbol{x}) = (-1)^{f(\boldsymbol{x})}.$$

Утверждение 6.2. Если $f(\boldsymbol{x}) \in \mathcal{B}(n)$, то

$$\left((-1)^{f(\boldsymbol{a} \oplus \boldsymbol{b})}\right)$$

является матрицей Адамара.

Доказательство.

$$\left((-1)^{f(\boldsymbol{a} \oplus \boldsymbol{b})}\right) = 2^{-n/2}\left(W_{\tilde{f}(\boldsymbol{a} \oplus \boldsymbol{b})}\right),$$

т. е., $\tilde{f}$ – бент-функция. ■

Теорема 6.3. (Конструкция Майорана – Мак-Фарланда).

Пусть $\boldsymbol{x}$, $\boldsymbol{y} \in \mathbb{Z}_2^n$, π – взаимно однозначное отображение на $\mathbb{Z}_2^n$, $g(\boldsymbol{x}) \in P_2(n)$ – произвольная функция. Тогда функция $f(\boldsymbol{x}, \boldsymbol{y}) = (\pi(\boldsymbol{x}), \boldsymbol{y}) \oplus g(\boldsymbol{x})$ – бент-функция от $2n$ переменных.

Доказательство. Найдем коэффициенты Уолша – Адамара для функции $f(\boldsymbol{x}, \boldsymbol{y})$:

$$W_f(\boldsymbol{ab}) = \sum_{\boldsymbol{x},\boldsymbol{y} \in \mathbb{Z}_2^n} (-1)^{(\pi(\boldsymbol{x}),\boldsymbol{y}) \oplus g(\boldsymbol{x}) \oplus (\boldsymbol{a},\boldsymbol{x}) \oplus (\boldsymbol{b},\boldsymbol{y})} =$$

$$= \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} (-1)^{g(\boldsymbol{x}) \oplus (\boldsymbol{a},\boldsymbol{x})} \sum_{\boldsymbol{y} \in \mathbb{Z}_2^n} (-1)^{(\pi(\boldsymbol{x}) \oplus \boldsymbol{b},\boldsymbol{y})} =$$

$$= 2^n \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} (-1)^{g(\boldsymbol{x}) \oplus (\boldsymbol{a},\boldsymbol{x})} \delta(\pi(\boldsymbol{x}), \boldsymbol{b}) =$$

$$= 2^n (-1)^{g(\pi^{-1}(\boldsymbol{b})) \oplus (\boldsymbol{a}, \pi^{-1}(\boldsymbol{b}))} = \pm 2^n. \blacksquare$$

Функции вида $f(\boldsymbol{x}, \boldsymbol{y}) = (\pi(\boldsymbol{x}), \boldsymbol{y}) \oplus g(\boldsymbol{x})$ образуют класс Майорана – МакФарланда, обозначение его $\mathcal{M}(2n)$. При фиксированном значении $\boldsymbol{x} = \boldsymbol{a}$ подфункция f (***a, y***) является аффинной. Тогда вектор значений функции $f(\boldsymbol{x}, \boldsymbol{y})$ представляет собой конкатенацию векторов значений аффинных функций.

При четном $n > 2$ существует бент-функция степени d для любого $d = 2, 3, \ldots, n/2$. Для ее формирования в конструкции Майорана – МакФарланда достаточно выбрать функцию $g(x)$ степени d.

Утверждение 6.3. $|\mathcal{M}(2n)| = 2^n! \cdot 2^{2^n}$.

Доказательство. Количество подстановок π на $\mathbb{Z}_2^n$ равно $2^n!$, количество функций $g(x)$ степени d равно 2^{2^n}. Теперь достаточно показать, что различным парам (π, g) соответствуют разные функции из $\mathcal{M}(2n)$.

Допустим обратное:

$$(\pi_1(\boldsymbol{x}), \boldsymbol{y}) \oplus g_1(\boldsymbol{x}) = (\pi_2(\boldsymbol{x}), \boldsymbol{y}) \oplus g_2(\boldsymbol{x}).$$

Тогда

$$(\pi_1(\boldsymbol{x}) \oplus \pi_2(\boldsymbol{x}), \boldsymbol{y}) = g_1(\boldsymbol{x}) \oplus g_2(\boldsymbol{x}).$$

Получаем, что левая часть последнего равенства не зависит от ***y.*** В результате имеем, что

$$\pi_1(\boldsymbol{x}) \oplus \pi_2(\boldsymbol{x}) \equiv 0,$$
$$(\pi_1(\boldsymbol{x}) = \pi_2(\boldsymbol{x})) \,\&\, (g_1(\boldsymbol{x}) = g_2(\boldsymbol{x})) = 1. \blacksquare$$

Оценка нижней границы количества бент-функций

$$|\mathcal{B}(n)| \geq 2^n! \cdot 2^{2^n}.$$

6.3. Совершенная нелинейность

Определение 6.6. *Производной функции $f(\boldsymbol{x})$ по направлению вектора* ***a*** называется функция

$$f'_{\boldsymbol{a}}(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{a}).$$

Пример 6.3. Построение производных для функции (табл. 6.3)

Таблица 6.3

$\boldsymbol{x}$		$f(\boldsymbol{x})$	$f'_{00}(\boldsymbol{x})$	$f'_{01}(\boldsymbol{x})$	$f'_{10}(\boldsymbol{x})$	$f'_{11}(\boldsymbol{x})$
0	0	0	0	0	0	1
0	1	0	0	0	1	0
1	0	0	0	1	0	0
1	1	1	0	1	1	0

Свойства производных

1. Производная любой функции по направлению $\boldsymbol{a} = \mathbf{0}$ есть функция-константа 0.

2. $f'_{\boldsymbol{a}}(\boldsymbol{x}) = f'_{\boldsymbol{a}}(\boldsymbol{x} \oplus \boldsymbol{a})$.

3. $(f \oplus g)'_{\boldsymbol{a}} = f'_{\boldsymbol{a}} \oplus g'_{\boldsymbol{a}}$.

4. $\forall \boldsymbol{a}\ f'_{\boldsymbol{a}}(\boldsymbol{x}) \equiv 0 \Leftrightarrow f$ константа.

5. (*Без доказательства*). Производные функции $f(\boldsymbol{x})$ по всем направлениям являются константами тогда и только тогда, когда $f \in \mathcal{A}(n)$.

6. $f'_{\boldsymbol{a}\oplus\boldsymbol{b}}(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{a} \oplus \boldsymbol{b}) =$
$= f(\boldsymbol{x}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{a}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{a}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{a} \oplus \boldsymbol{b}) =$
$= f'_{\boldsymbol{a}}(\boldsymbol{x}) \oplus f'_{\boldsymbol{b}}(\boldsymbol{x} \oplus \boldsymbol{a})$.

7. Если $f \neq$ const, то $\deg f' \leq \deg f - 1$.

Определение 6.7. Говорят, что *функция* $f(\boldsymbol{x}) \in P_2(n)$, *имеет линейную структуру,* если существует ненулевое направление $\boldsymbol{a} \in \mathbb{Z}_2^n$, такое, что $f'_{\boldsymbol{a}}(\boldsymbol{x}) =$ const.

Множество векторов $\boldsymbol{a} \in \mathbb{Z}_2^n$, по направлениям которых производная функции $f(\boldsymbol{x})$ равна константе, образует линейное пространство.

Класс функций с линейной структурой от n переменных обозначается $\mathcal{LS}(n)$.

Свойства класса $\mathcal{LS}(n)$

1. $\mathcal{A}\ (n) \subseteq \mathcal{LS}(n)$.

2. Если f имеет линейную или фиктивную переменную, то $f \in \mathcal{LS}(n)$.
Пусть $f(x_1, x_2, \ldots, x_{n-1}, y) = g(x_1, x_2, \ldots, x_{n-1}) \oplus cy$, $c \in \{0, 1\}$.
Тогда $f'_{0\ldots01} = c$.

3. Если функция f зависит квазилинейно от некоторых своих переменных, то $f \in \mathcal{LS}(n)$.

4. Если $f \in \mathcal{LS}(n)$, $g \in \mathcal{A}\ (n)$, то $f \oplus g \in \mathcal{LS}(n)$.

Утверждение 6.4. Пусть $f \in \mathcal{LS}(n)$. Тогда существует невырожденная булева матрица A размерами $n \times n$, такая, что функция $g\ (\boldsymbol{x}) = f\ (A\boldsymbol{x})$ имеет линейную или фиктивную переменную.

Доказательство.

Пусть $f'_{\boldsymbol{a}}(\boldsymbol{x}) =$ const $= c \in \mathbb{Z}_2$. Тогда $f\ (\boldsymbol{x} \oplus u\boldsymbol{a}) = f\ (\boldsymbol{x}) \oplus uc$ для всех аргументов функции $\boldsymbol{x} \in \mathbb{Z}_2^n$ и $u \in \mathbb{Z}_2^n$. Определим $\{\boldsymbol{e}_i\}$ – множество векторов длины n с единственной единицей в компоненте i, $i = 1, 2, \ldots, n$. Построим невырожденную матрицу A, первый столбец которой равен вектору $\boldsymbol{a}$, а остальные произвольные. Ясно, что $A\boldsymbol{e}_1 = \boldsymbol{a}$. Для вектора $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ можно записать:

$$f(A\boldsymbol{x}) = f(A(x_1\boldsymbol{e}_1 \oplus x_2\boldsymbol{e}_2 \ldots \oplus x_n\boldsymbol{e}_n) =$$
$$= f(x_1(A\boldsymbol{e}_1) \oplus A(x_2\boldsymbol{e}_2 \ldots \oplus x_n\boldsymbol{e}_n)) =$$
$$= f\big(x_1\boldsymbol{a} \oplus A(x_2\boldsymbol{e}_2 \ldots \oplus x_n\boldsymbol{e}_n)\big) = f\big(A(x_2\boldsymbol{e}_2 \ldots \oplus x_n\boldsymbol{e}_n)\big) \oplus cx_1.$$

Получили, что x_1 является фиктивной или линейной переменной в зависимости от значения константы *c*. ■

Таким образом, одно из требований к булевым функциям, используемых при построении криптографических систем, а именно – отсутствие линейных и фиктивных переменных – сводится к более общему, то есть к требованию удаленности выбранной булевой функции от класса $\mathcal{LS}(n)$ функций с линейной структурой.

Пример 6.4. Пусть $f(x_1, x_2, x_3) = 1 \oplus x_1 \oplus x_2x_3 \oplus x_1x_3$. Линейных и фиктивных переменных у этой функции нет. Найдем производную по направлению $\boldsymbol{a} = (110)$:

$$f'_{110} = 1 \oplus x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus 1 \oplus (x_1 \oplus 1) \oplus (x_2 \oplus 1)x_3 \oplus$$
$$\oplus (x_1 \oplus 1)x_3 = 1.$$

Оказалось, что функция *f* имеет линейную структуру.

Строим невырожденную матрицу *A*:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

После аффинного преобразования переменных функции *f* получаем

$$g(\boldsymbol{x}) = f(A\boldsymbol{x}) = 1 \oplus x_1 \oplus (x_1 \oplus x_2)x_3 \oplus x_1x_3 = 1 \oplus x_1 \oplus x_2x_3.$$

Полученная функция *g* линейна по переменной x_1.

Определение 6.8. *Совершенной нелинейностью функции f* называется минимальное Хеммингово расстояние от вектора значений функции *f* до векторов значений из класса функций с линейной структурой.

Совершенная нелинейность функции *f* обозначается CN_f (*Complete Nonlinearity*):

$$CN_f = \rho(f, \mathcal{LS}(n)) = \min_{g \in \mathcal{LS}(n)} \|f, g\|.$$

Множество аффинных функций $\mathcal{A}(n)$ входит также и во множество функций с линейной структурой $\mathcal{LS}(n)$, тогда значение совершенной нелинейности CN_f булевой функции не превосходит значения ее нелинейности Nl_f: $Nl_f \geq CN_f$.

Утверждение 6.5. Для произвольной булевой функции $f(\boldsymbol{x}) \in P_2(n)$:

1) $CN_f \leq 2^{n-2}$;

2) $CN_f = 2^{n-2}$ тогда и только тогда, когда производные функции $f(\boldsymbol{x})$ уравновешены по всем ненулевым направлениям.

Доказательство. Множество векторов в $\mathbb{Z}_2^n$, их ровно 2^n, разобьем на пары. Произвольно выбираем ненулевой вектор $\boldsymbol{a} \in \mathbb{Z}_2^n$ и выборкой без возвращения сформируем множество пар векторов $\{\boldsymbol{x}, \boldsymbol{x} \oplus \boldsymbol{a}\}$. Таких пар будет 2^{n-1}, пересечений по векторам у этих пар нет. Множество этих пар разобьем на два подмножества:

$$Q(\boldsymbol{a}, f) = \{\{\boldsymbol{x}, \boldsymbol{x} \oplus \boldsymbol{a}\}/f(\boldsymbol{x}) = f(\boldsymbol{x} \oplus \boldsymbol{a})\} = \{\{\boldsymbol{x}, \boldsymbol{x} \oplus \boldsymbol{a}\}/f'_{\boldsymbol{a}}(\boldsymbol{x}) = 0\};$$

$$R(\boldsymbol{a}, f) = \{\{\boldsymbol{x}, \boldsymbol{x} \oplus \boldsymbol{a}\}/f(\boldsymbol{x}) \neq f(\boldsymbol{x} \oplus \boldsymbol{a})\} = \{\{\boldsymbol{x}, \boldsymbol{x} \oplus \boldsymbol{a}\}/f'_{\boldsymbol{a}}(\boldsymbol{x}) = 1\}.$$

Суммарная мощность этих подмножеств будет

$$|Q\ (\boldsymbol{a}, f)| + |R\ (\boldsymbol{a}, f)| = 2^{n-1}.$$

В таком случае получим неравенство:

$$\min\{|Q\ (\boldsymbol{a}, f)|, |R\ (\boldsymbol{a}, f)|\} \leq 2^{n-2}.$$

В последнем соотношении имеет место равенство, если и только если производная $f'_{\boldsymbol{a}}(\boldsymbol{x})$ уравновешена.

Построим функцию $g_1(\boldsymbol{x}) \in \mathcal{LS}(n)$, которая будет ближайшей к функции $f(\boldsymbol{x})$.

1. Множество $Q\ (\boldsymbol{a}, f)$.

В каждой паре из $Q\ (\boldsymbol{a}, f)$ выбираем один из векторов $\boldsymbol{x}$ или $\boldsymbol{x} \oplus \boldsymbol{a}$, назовем его $\boldsymbol{y}$. Полагаем:

$$g_1(\boldsymbol{y}) = f(\boldsymbol{y}).$$

Равенство должно выполняться только для одного из векторов пары. Тогда для второго вектора $\boldsymbol{y} \oplus \boldsymbol{a}$ из пары получится

$$g_1(\boldsymbol{y} \oplus \boldsymbol{a}) = g_1(\boldsymbol{y}) \oplus 1.$$

На множестве переменных из $R\ (\boldsymbol{a}, f)$ значения функции $g_1(\boldsymbol{x})$ положим равными значениям функции $f(\boldsymbol{x})$. В результате получили функцию с линейной структурой $g_1(\boldsymbol{x}) \in \mathcal{LS}(n)$, она является ближайшей к функции $f(\boldsymbol{x})$ из всех функций, для которых производная по направлению $\boldsymbol{a}$ равна константе 1.

2. Множество $R\ (\boldsymbol{a}, f)$.

Аналогичным образом строим функцию $g_2(\boldsymbol{x}) \in \mathcal{LS}(n)$: в каждой паре из $R\ (\boldsymbol{a}, f)$ выбираем один их векторов $\boldsymbol{x}$ или $\boldsymbol{x} \oplus \boldsymbol{a}$, назовем его $\boldsymbol{y}$. Полагаем:

$$g_2(\boldsymbol{y}) = f(\boldsymbol{y}).$$

Равенство должно выполняться только для одного из векторов пары. Тогда для второго вектора $\boldsymbol{y} \oplus \boldsymbol{a}$ из пары получится

$$g_2(\boldsymbol{y} \oplus \boldsymbol{a}) = g_2(\boldsymbol{y}).$$

На множестве переменных из $Q(\boldsymbol{a}, f)$ значения функции $g_2(\boldsymbol{x})$ положим равными значениям функции $f(\boldsymbol{x})$. В результате получим функцию с линейной структурой $g_2(\boldsymbol{x}) \in \mathcal{LS}(n)$. Она является ближайшей к функции $f(\boldsymbol{x})$ из всех функций, для которых производная по направлению $\boldsymbol{a}$ равна константе 0.

Учтем, что

$$\rho(f, g_1) = |Q(\boldsymbol{a}, f)|,$$

$$\rho(f, g_2) = |R(\boldsymbol{a}, f)|.$$

Тогда получаем:

$$CN_f = \rho\left(f, LS(n)\right) = \min_{\boldsymbol{a} \neq \boldsymbol{0}} \min\{|Q(\boldsymbol{a}, f)|, |R(\boldsymbol{a}, f)|\} \leq 2^{n-2}.$$

Равенство достигается тогда и только тогда, когда

$$|Q(\boldsymbol{a}, f)| = |R(\boldsymbol{a}, f)| = 2^{n-2}$$

для всех $\boldsymbol{a} \neq \boldsymbol{0}$, т. е. в случае уравновешенности производных по всем ненулевым направлениям. ■

Определение 6.9. Функция $f(\boldsymbol{x}) \in P_2(n)$ называется *совершенно нелинейной*, если $CN_f = 2^{n-2}$.

Совершенно нелинейные функции максимально удалены от класса функций с линейной структурой и их производные уравновешены по всем ненулевым направлениям.

Утверждение 6.6. Функция $f(\boldsymbol{x}) \in P_2(n)$ является совершенно нелинейной тогда и только тогда, когда $f(\boldsymbol{x})$ – бент-функция.

Доказательство.

Необходимость:

$$W_f^2(\boldsymbol{a}) = \sum_{\boldsymbol{x} \in Z_2^n} (-1)^{f(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x})} \sum_{\boldsymbol{y} \in Z_2^n} (-1)^{f(\boldsymbol{y}) \oplus (\boldsymbol{a}, \boldsymbol{y})} =$$

$$= \sum_{\boldsymbol{x}, \boldsymbol{y}} (-1)^{f(\boldsymbol{x}) \oplus f(\boldsymbol{y}) \oplus (\boldsymbol{a}, \boldsymbol{x} \oplus \boldsymbol{y})} =$$

$$= \sum_{\boldsymbol{x} = \boldsymbol{y}} (-1)^{f(\boldsymbol{x}) \oplus f(\boldsymbol{y}) \oplus (\boldsymbol{a}, \boldsymbol{x} \oplus \boldsymbol{y})} + \sum_{\boldsymbol{x} \neq \boldsymbol{y}} (-1)^{f(\boldsymbol{x}) \oplus f(\boldsymbol{y}) \oplus (\boldsymbol{a}, \boldsymbol{x} \oplus \boldsymbol{y})}.$$

Первая сумма равна 2^n, во второй сумме делаем замену $\boldsymbol{b} = \boldsymbol{x} \oplus \boldsymbol{y}$. Получаем:

$$W_f^2(\boldsymbol{a}) = 2^n + \sum_{\boldsymbol{b}\neq\boldsymbol{0}} (-1)^{(\boldsymbol{a},\boldsymbol{b})} \sum_{\boldsymbol{x}} (-1)^{f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus\boldsymbol{a})} = 2^n.$$

Последнее равенство имеет место в силу уравновешенности функции $f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus\boldsymbol{a})$ при любом ненулевом векторе $\boldsymbol{b}$. Получается, что

$$W_f(\boldsymbol{a}) = \pm 2^{n/2},$$

т. е. $f(\boldsymbol{x})$ – бент-функция.

Достаточность. Если $f(\boldsymbol{x}) \in \mathcal{B}(n)$, то матрица

$$H = \left((-1)^{f(\boldsymbol{a}\oplus\boldsymbol{b})}\right)$$

является матрицей Адамара. Рассмотрим элемент матрицы $HH^{\mathrm{T}} = 2^n E = (h_{\boldsymbol{ab}})$:

$$h_{\boldsymbol{ab}} = \sum_{\boldsymbol{x}} (-1)^{f(\boldsymbol{a}\oplus\boldsymbol{x})\oplus f(\boldsymbol{b}\oplus\boldsymbol{x})} = 2^n \delta(\boldsymbol{a}, \boldsymbol{b}).$$

Для $\boldsymbol{b} = \boldsymbol{0}$ и любого $\boldsymbol{a} \neq \boldsymbol{0}$ получаем, что

$$\sum_{\boldsymbol{x}} (-1)^{f(\boldsymbol{a}\oplus\boldsymbol{x})\oplus f(\boldsymbol{x})} = \sum_{\boldsymbol{x}} (-1)^{f'_a(\boldsymbol{x})} = 0.$$

Отсюда следует, что $f'_{\boldsymbol{a}}(\boldsymbol{x})$ уравновешена, тогда $f(\boldsymbol{x})$ совершенно нелинейна. ■

Теорема 6.4. Критерий Ротхауза.

Функция является совершенно нелинейной (является бент-функцией) тогда и только тогда, когда ее производные по всем ненулевым направлениям уравновешены.

Доказательство. Следует из предыдущих утверждений.

Таким образом, при четном значении *n* классы бент-функций и совершенно нелинейных функций совпадают.

6.4. Нелинейность и корреляционная иммунность

Ранее было показано, что такие параметры булевой функции как порядок корреляционной иммунности *m* и ее алгебраическая нелинейность deg (*f*) взаимно ограничены неравенствами Зигенталера:

$$\mathrm{cor}\,(f) + \deg(f) \leq n;$$

$$\text{sut}(f) + \deg(f) \le n - 1.$$

Аналогичная связь существует между параметрами корреляционной иммунности m и метрической нелинейностью Nl_f.

Теорема 6.5. Пусть функция $f(\boldsymbol{x}) \in P_2(n)$, cor ($f$) = $m \le n - 1$, f не уравновешенная. Тогда

$$Nl_f \le 2^{n-1} - 2^m.$$

Доказательство. Напомним, что cor (f) = cor ($\overline{f}$), $Nl_f = Nl_{\overline{f}}$. Выберем из f и $\overline{f}$ ту функцию, вес которой меньше 2^{n-1}и назовем ее f. Для ее подфункции g от $n - m$ переменных выполняется условие

$$\|g\| = \frac{\|f\|}{2^m} \le 2^{n-m-1} - 1.$$

Отсюда

$$\|f\| = 2^m\|g\| \le 2^{n-1} - 2^m.$$

Воспользуемся тем, что $Nl_f \le \|f\|$ и получим нужное неравенство. ■

Теорема 6.6. Пусть функция $f(\boldsymbol{x}) \in P_2(n)$, cor($f$) = $m \le n - 2$. Тогда, если

$$Nl_f \ne 2^{n-1} - 2^m,$$

то

$$Nl_f \le 2^{n-1} - 2^{m+1}.$$

Доказательство. Напомним необходимое условие корреляционной иммунности порядка m: для любого задающего вектора $\boldsymbol{a}$ линейной функции $l_{\boldsymbol{a}}(\boldsymbol{x})$ коэффициенты преобразования Уолша $W_f(\boldsymbol{a})$ делится на 2^{m+1}. Так как

$$Nl_f = 2^{n-1} - 0{,}5 \cdot \max_{\boldsymbol{a} \in \mathbb{Z}_2^n} \left|W_f(\boldsymbol{a})\right| \ne 2^{n-1} - 2^m,$$

то $\max\limits_{\boldsymbol{a} \in \mathbb{Z}_2^n} \left|W_f(\boldsymbol{a})\right| \ne 2^{m+1}$.

Следовательно, существует вектор $\boldsymbol{a}$, для которого $\left|W_f(\boldsymbol{a})\right| \ge 2^{m+2}$. Отсюда получается утверждение теоремы. ■

Теорема 6.7. Пусть функция $f(\boldsymbol{x}) \in P_2(n)$ является уравновешенной и m-устойчивой, $m \le n - 2$. Тогда

$$Nl_f \le 2^{n-1} - 2^{m+1}.$$

Доказательство. Для m-устойчивых булевых функций для всех векторов $\boldsymbol{a}$ коэффициенты преобразования Уолша $W_f(\boldsymbol{a})$ делится на 2^{m+2}. Значит, существует вектор $\boldsymbol{a}$, на котором $\left|W_f(\boldsymbol{a})\right| \geq 2^{m+2}$. Следовательно, $\max\limits_{\boldsymbol{a}\in\mathbb{Z}_2^n} \left|W_f(\boldsymbol{a})\right| \geq 2^{m+2}$ и теорема доказана. ■

В классе m-устойчивых булевых функций (уравновешенные и имеющие порядок корреляционной иммунности, равный m) выделяют подкласс m-оптимальных булевых функций (уравновешенные и имеющие предельные значения параметров алгебраической нелинейности и корреляционной иммунности: sut(f) + deg(f) = n – 1). Определим еще один подкласс m-устойчивых булевых функций – с предельными значениями параметров корреляционной иммунности m и нелинейности Nl_f.

Определение 6.10. Уравновешенная функция $f(\boldsymbol{x}) \in P_2(n)$ называется *m-насыщенной*, если для нее выполняются неравенства:

$$\text{sut}\,(f) = m \leq n - 2;$$

$$Nl_f = 2^{n-1} - 2^{m+1}.$$

Теорема 6.8. (О нелинейности неоптимальных булевых функций).

Если функция $f(\boldsymbol{x}) \in P_2(n)$ уравновешена, sut(f) = $m \leq n - 3$ и deg(f) $\leq n - m - 2$, то

$$Nl_f \leq 2^{n-1} - 2^{m+2}.$$

Доказательство. По определению иммунности для функции f существует подфункция f_1 от $n - m - 1$ переменных, такая, что

$$\|f_1\| \neq 2^{n-m-2}.$$

Вес подфункции f_1 является четным, так как

$$\{f_1 \in P_2(n-m-1)\}\ \&\ \{\deg f_1 \leq \deg f < n - m - 1\}.$$

В таком случае

$$\|f_1\| \leq 2^{n-m-2} - 2$$

или

$$\|f_1\| \geq 2^{n-m-2} + 2.$$

Это равносильно тому, что

$$\|\overline{f_1}\| \leq 2^{n-m-2} - 2.$$

Из свойств преобразования Уолша – Адамара следует, что отрицание функции и ее переменных влияет только на знаки коэффициентов Уолша – Адамара. Значение нелинейности и устойчивости сохраняются. Поэтому рассмотрим только случай, когда $\|f_1\| \leq 2^{n-m-2} - 2$, будем считать при этом, что подфункция f_1 получена фиксацией $m + 1$ переменных нулями.

Пусть $\boldsymbol{b} \in \mathbb{Z}_2^n$, $\|\boldsymbol{b}\| = m + 1$, $b_i = 1$, если и только если переменная x_i фиксирована. Тогда $f_1 = f^{\boldsymbol{b}}$ из тождества Саркара. С учетом условия sut(f) = m можно записать

$$W_f(\boldsymbol{b}) = \sum_{\boldsymbol{a} \preccurlyeq \boldsymbol{b}} W_f(\boldsymbol{a}) = 2^n - 2^{m+2} \cdot \|f_1\| \geq 2^{m+3}.$$

Отсюда $Nl_f \leq 2^{n-1} - 2^{m+2}$. ■

Утверждение 6.7. Если функция m-насыщенная, то она m-оптимальна.

Доказательство. Для $m \leq n - 3$ утверждение следует из теоремы 6.8. В случае, когда sut (f) = $m = n - 2$, по неравенству Зигенталера и в силу уравновешенности функции имеем: deg (f) = 1 = $n - m - 1$. ■

Определение 6.11. Если для функции $f(\boldsymbol{x}) \in P_2(n)$ квадрат каждого коэффициента преобразования Уолша – Адамара равен либо нулю, либо 2^{2n-2r}, то функция $f(\boldsymbol{x})$ называется *платовидной функцией порядка* $2r$.

Бент-функции платовидны порядка n; аффинные функции платовидны порядка нуль.

Для платовидной порядка $2r$ функции значения коэффициентов преобразования Уолша – Адамара могут иметь только три значения:

$$W_f(\boldsymbol{a}) \in \{0, -2^{n-r}, 2^{n-r}\}.$$

Величина 2^{n-r} называется *амплитудой платовидной функции*.

Теорема 6.9. Если функция $f(\boldsymbol{x}) \in P_2(n)$ является m-насыщенной, то она является платовидной порядка $2(n - m - 2)$.

Доказательство. Для m-насыщенной функции имеем по определению

$$Nl_f = 2^{n-1} - 2^{m+1}.$$

По определению нелинейности Nl_f имеем:

$$\max_{\boldsymbol{a}} \left|W_f(\boldsymbol{a})\right| = 2^{m+2}.$$

Корреляционная иммунность порядка m подразумевает, что все коэффициенты Уолша – Адамара данной функции делятся на 2^{m+2}. Следовательно,

$$W_f(\boldsymbol{a}) \in \{0, -2^{m+2}, 2^{m+2}\}. \blacksquare$$

Перечислим известные ограничения для нелинейности булевой функции.

Неуравновешенная корреляционно-иммунная порядка m функция:

$$Nl_f \leq 2^{n-1} - 2^m.$$

Уравновешенная корреляционно-иммунная порядка m функция:

$$Nl_f \leq 2^{n-1} - 2^{m+1}.$$

Произвольная булева функция:

$$Nl_f \leq 2^{n-1} - 2^{n/2-1}.$$

Для функций с малым порядком корреляционной иммунности границы нелинейности определяет следующая теорема.

Теорема 6.10. Пусть функция $f(\boldsymbol{x}) \in P_2(n)$, n – четное.

1. Если $0 < \text{cor}(f) = m \leq n/2 - 1$, то
2. $Nl_f \leq 2^{n-1} - 2^{n/2-1} - 2^m$.
3. Если функция уравновешенная, $\text{sut}(f) = m \leq n/2 - 2$, то

$$Nl_f \leq 2^{n-1} - 2^{n/2-1} - 2^{m+1}.$$

Доказательство. Пункт 2. Функция уравновешенная, поэтому она не является бент-функцией. Тогда

$$\max_{\boldsymbol{a}} \left|W_f(\boldsymbol{a})\right| > 2^{n/2}.$$

Необходимые условия корреляционной иммунности порядка m требуют делимости всех коэффициентов Уолша на 2^{m+2}. Кроме того, $2^{n/2}$ делится на 2^{m+2}, так как по условию теоремы $m \leq n/2 - 2$. Следовательно,

$$\max_{\boldsymbol{a}} \left|W_f(\boldsymbol{a})\right| \geq 2^{n/2} + 2^{m+2}.$$

Вспоминая определение нелинейности, получаем утверждение пункта 2 теоремы. Пункт 1 доказывается аналогично.

Контрольные вопросы и задания

1. Привести определение нелинейности дискретной функции, расчет с помощью коэффициентов Уолша.

2. Дана функция от трех переменных f = (0101 № по журналу группы).

Найти коэффициенты преобразования Уолша.

Определить расстояние от функции до класса аффинных функций.

Определить статистический аналог функции.

Найти перекос вероятности.

3. Перечислить основные свойства нелинейности (геометрической нелинейности).

4. Дать определение бент-функции, перечислить ее свойства.

5. Конструкция Майорана – МакФарланда построения бент-функций.

6. Дать определение производной дискретной функции, привести пример вычисления производной по направлению для функции от двух переменных.

7. Функции с линейной структурой, привести определение таких функций.

8. Дать определение совершенной нелинейности дискретной функции.

9. Привести критерий совершенной нелинейности.

10. Дать определение m-насыщенной функции.

7. ЛАВИННЫЕ ХАРАКТЕРИСТИКИ БУЛЕВЫХ ФУНКЦИЙ

7.1. Автокорреляция и взаимная корреляция

Определение 7.1. Пусть функции $f(\boldsymbol{x}), g(\boldsymbol{x}) \in P_2(n)$. *Функцией взаимной корреляции* f и g называется функция $\Delta_{f,g}\colon \mathbb{Z}_2^n \to \mathbb{Z}$, где для любого $\boldsymbol{u} \in \mathbb{Z}_2^n$

$$\Delta_{f,g}(\boldsymbol{u}) = \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} (-1)^{f(\boldsymbol{x}) \oplus g(\boldsymbol{x} \oplus \boldsymbol{u})}.$$

Значение $\Delta_{f,g}(\boldsymbol{u})$ равно разности между числом совпадений и числом несовпадений значений функций $f(\boldsymbol{x})$ и $g(\boldsymbol{x} \oplus \boldsymbol{u})$. При равновероятном выборе пары булевых функций из $P_2(n)$ вероятность совпадения их значений равна 0,5.

Определение 7.2. Пусть функции $f(\boldsymbol{x}), g(\boldsymbol{x}) \in P_2(n)$. Функции f, g называются *совершенно некоррелированными*, если $\forall\ \boldsymbol{u} \in \mathbb{Z}_2^n$ выполняется $\Delta_{f,g}(\boldsymbol{u}) = 0$.

Определение 7.3. *Функция автокорреляции* для $f(x) \in P_2(n)$:

$$\Delta_f(\boldsymbol{u}) = \Delta_{f,f}(\boldsymbol{u}) = \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} (-1)^{f(\boldsymbol{x}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{u})} = \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} (-1)^{f'_u(\boldsymbol{x})}.$$

Свойства функции автокорреляции

1. $\Delta_f(\mathbf{0}) = 2^n$.

2. $\Delta_f(\boldsymbol{u}) = 0$ тогда и только тогда, когда производная $f'_u(\boldsymbol{u})$ уравновешенная.

3. $\Delta_f(\boldsymbol{u}) = \Delta_{\overline{f}}(\boldsymbol{u})$ для любого вектора $\boldsymbol{u}$.

4. $\Delta_f(\boldsymbol{u}) = W_{f'_u}(\mathbf{0})$.

5. Пусть функции $f(\boldsymbol{x}) \in P_2(n)$, $g(\boldsymbol{x}) \in \mathcal{A}\ (n)$. Тогда $\forall\ \boldsymbol{u} \in \mathbb{Z}_2^n$ выполняется

$$\Delta_{f \oplus g}(\boldsymbol{u}) = \pm \Delta_f(\boldsymbol{u}).$$

6. Пусть $h\ (\boldsymbol{x}, \boldsymbol{y}) = f\ (\boldsymbol{x}) \oplus g\ (\boldsymbol{y})$, множества компонент векторов $\boldsymbol{x}$, $\boldsymbol{y}$ не пересекаются. Тогда

$$\Delta_h(\boldsymbol{ab}) = \Delta_f(\boldsymbol{a}) \cdot \Delta_g(\boldsymbol{b}).$$

7. С помощью функции автокорреляции можно вычислить совершенную нелинейность CN_f функции $f(\boldsymbol{x})$:

$$CN_f = 2^{n-2} - 0{,}25 \max_{\boldsymbol{a}\neq\boldsymbol{0}} \left|\Delta_f(\boldsymbol{a})\right|.$$

Без доказательства.

Теорема 7.1. (О взаимной корреляции).
Пусть функции $f(\boldsymbol{x}), g(\boldsymbol{x}) \in P_2(n)$. Тогда

$$\left(\Delta_{f,g}(\boldsymbol{0}), \dots, \Delta_{f,g}(\boldsymbol{1})\right) \cdot H_{2^n} = \left(W_f(\boldsymbol{0})W_g(\boldsymbol{0}), \dots, W_f(\boldsymbol{1})W_g(\boldsymbol{1})\right).$$

Здесь H_{2^n} – матрица Сильвестра – Адамара.

Доказательство. В выражении слева вычислим компоненту на векторе $\boldsymbol{v}$.

$$\sum_{\boldsymbol{u}} \Delta_{f,g}(\boldsymbol{u})(-1)^{(\boldsymbol{u},\boldsymbol{v})} = \sum_{\boldsymbol{u}}\sum_{\boldsymbol{x}} (-1)^{f(\boldsymbol{x})\oplus g(\boldsymbol{x}\oplus\boldsymbol{u})\oplus(\boldsymbol{u},\boldsymbol{v})} =$$

$$= \sum_{\boldsymbol{x}} (-1)^{f(\boldsymbol{x})} \sum_{\boldsymbol{u}} (-1)^{g(\boldsymbol{x}\oplus\boldsymbol{u})\oplus(\boldsymbol{u},\boldsymbol{v})} = \sum_{\boldsymbol{x}} (-1)^{f(\boldsymbol{x})} \sum_{\boldsymbol{z}} (-1)^{g(\boldsymbol{z})\oplus(\boldsymbol{z}\oplus\boldsymbol{x},\boldsymbol{v})} =$$

$$= \sum_{\boldsymbol{x}} (-1)^{f(\boldsymbol{x})\oplus(\boldsymbol{x},\boldsymbol{v})} \sum_{\boldsymbol{z}} (-1)^{g(\boldsymbol{z})\oplus(\boldsymbol{z},\boldsymbol{v})} = W_f(\boldsymbol{v})W_g(\boldsymbol{v}).$$

Теорема доказана. ■

Следствие 1. При $f = g$ получаем

$$\left(\Delta_f(\boldsymbol{0}), \dots, \Delta_f(\boldsymbol{1})\right) \cdot H_{2^n} = \left(W_f^2(\boldsymbol{0}), \dots, W_f^2(\boldsymbol{1})\right).$$

Следствие 2.

$$\left(\Delta_{f,g}(\boldsymbol{0}), \dots, \Delta_{f,g}(\boldsymbol{1})\right) = \left(W_f(\boldsymbol{0})W_g(\boldsymbol{0}), \dots, W_f(\boldsymbol{1})W_g(\boldsymbol{1})\right) H_{2^n}.$$

Следствие 3.

$$\left(\Delta_f(\boldsymbol{0}), \dots, \Delta_f(\boldsymbol{1})\right) = 2^{-n}\left(W_f^2(\boldsymbol{0}), \dots, W_f^2(\boldsymbol{1})\right) H_{2^n}.$$

Следствие 4. Функции $f(\boldsymbol{x}), g(\boldsymbol{x}) \in P_2(n)$ совершенно некоррелированы тогда и только тогда, когда $\forall\ \boldsymbol{u} \in \mathbb{Z}_2^n$ выполняется $W_f(\boldsymbol{u})W_g(\boldsymbol{u}) = 0$.

7.2. Строгий лавинный критерий

Определение 7.4. Для функции $f(\boldsymbol{x}) \in P_2(n)$ выполняется *строгий лавинный критерий* (SAC – *Strict Avalanche Criterion*), если

$$\forall\ \boldsymbol{u} \in \mathbb{Z}_2^n\ /\ \|\boldsymbol{u}\| = 1 \text{ выполняется } \Delta_f(\boldsymbol{u}) = 0.$$

Эквивалентно: функция $f(\boldsymbol{x})$ удовлетворяет строгому лавинному критерию, если ее производные с весом единица по всем направлениям уравновешены.

Эквивалентно: функция $f(\boldsymbol{x})$ удовлетворяет строгому лавинному критерию, если для любого i = 1, 2, …, n при равновероятном выборе $\boldsymbol{x} \in \mathbb{Z}_2^n$ и замене x_i на $x_i \oplus 1$ значение функции $f(\boldsymbol{x})$ изменится с вероятностью p = 0,5.

Пример 7.1. Зададим функцию $f(x)$ и определим $\Delta_f(u)$ (табл. 7.1).

Таблица 7.1

x_1	x_2	$f(\boldsymbol{x})$	$\Delta_f(\boldsymbol{u})$
0	0	0	4
0	1	1	0
1	0	1	0
1	1	1	0

Проверим выполнение строгого лавинного критерия для функции, заданной в табл. 7.1.

Заменим значение бита x_1 на противоположное. При $\boldsymbol{x}$ = (0 0), $\boldsymbol{x}$ = (1 0) значение функции меняется. При $\boldsymbol{x}$ = (0 1) или $\boldsymbol{x}$ = (1 1) значение функции не меняется.

Заменим значение бита x_2 на противоположное. При $\boldsymbol{x}$ = (0 0), $\boldsymbol{x}$ = (0 1) значение функции меняется. При $\boldsymbol{x}$ = (1 0) или $\boldsymbol{x}$ = (1 1) значение функции не меняется.

Значение функции меняется с вероятностью 0,5, следовательно, функция $f(\boldsymbol{x})$ удовлетворяет строгому лавинному критерию.

Приведем вероятностное определение корреляционной иммунности порядка m.

Определение 7.5. (вероятностное). Функция $f(\boldsymbol{x}) \in P_2(n)$ называется *корреляционно-иммунной порядка* m, $0 < m \le n$, если для произвольного набора индексов $(i_1, i_2, \ldots, i_m)$, $1 \le i_1 < i_2 <, \ldots, < i_m \le n$, справедливо:

$$P\{X^{i_1}, \ldots, X^{i_m}\} = P\{X^{i_1}, \ldots, X^{i_m}\ /f(X^1, X^2, \ldots, X^n)\}.$$

Эквивалентно. Априорные вероятности значений m-подмножеств компонент аргумента $\boldsymbol{x}$ функции $f(\boldsymbol{x})$ равны их апостериорным вероятностям.

Проверим корреляционную иммунность порядка $m = 1$ для функции, заданной в табл. 7.1.

Компонента x_1:

$$P\{x_1 = 0\} = 0{,}5; \quad P\{x_1 = 0/f(\boldsymbol{x}) = 0\} = 1.$$
$$P\{x_1 = 0\} = 0{,}5; \quad P\{x_1 = 0/f(\boldsymbol{x}) = 1\} = 1/3.$$
$$P\{x_1 = 1\} = 0{,}5; \quad P\{x_1 = 1/f(\boldsymbol{x}) = 0\} = 0.$$
$$P\{x_1 = 1\} = 0{,}5; \quad P\{x_1 = 1/f(\boldsymbol{x}) = 1\} = 2/3.$$

Априорные и апостериорные вероятности не совпадают, статистическая независимость результата функции и значения x_1 отсутствуют, корреляционная иммунность отсутствует.

Для компоненты x_2 результат аналогичен.

Утверждение 7.1. Пусть функция $f(\boldsymbol{x}) \in P_2(n)$ и для нее выполняется строгий лавинный критерий. Тогда:

1) функция $f(\boldsymbol{x})$ не имеет линейных и фиктивных переменных;

2) если $n \geq 3$, то $\|f\| = 0 \bmod 2$, следовательно, deg (f) < n.

Доказательство.

1. Предположим противное, т. е. имеется линейная переменная:

$$f\ (\boldsymbol{x})\ =\ g(x_1, \ldots, x_{n-1}) \oplus cx_n.$$

Выберем направление $\boldsymbol{u}$ = (0, 0, …, 0, 1). Производная $f'_u(\boldsymbol{u})$ = c, она уравновешенной не является, тогда $\Delta_f(\boldsymbol{u}) \neq 0$ и определение строгой лавинности не выполняется.

2. Выберем произвольный орт $\boldsymbol{u}$ из $\mathbb{Z}_2^n$, т. е. вектор с весом единица, $\|\boldsymbol{u}\| = 1$. Производная $f'_u(\boldsymbol{u})$ уравновешена, Поэтому

$$|Q\ (\boldsymbol{a}, f)| = |R\ (\boldsymbol{a}, f)| = 2^{n-2}.$$

Здесь $R\ (\boldsymbol{a}, f) = \{\boldsymbol{x}/f(\boldsymbol{x}) \neq f(\boldsymbol{x} \oplus \boldsymbol{a})\}$; $Q(\boldsymbol{a}, f) = \{\boldsymbol{x}/f(\boldsymbol{x}) = f(\boldsymbol{x} \oplus \boldsymbol{a})\}$.

Функция f принимает значение единица точно на одном векторе в каждой паре из $R\ (\boldsymbol{a}, f)$ и обоих векторов для некоторых пар из $Q\ (\boldsymbol{a}, f)$.

Тогда $\|f\| = 0 \bmod 2$. ■

Определение 7.6. Для функции $f(\boldsymbol{x}) \in P_2(n)$ выполняется *строгий лавинный критерий порядка m* (SAC (m)), если для любой ее подфункции от $n - m$ переменных выполняется строгий лавинный критерий SAC.

Из утверждения 7.1 следует что в $P_2\ (n)$ не существует функций, для которых выполняется SAC (n – 1).

Утверждение 7.2. Если для некоторой функции выполняется критерий SAC(m), тогда для нее выполняется критерий SAC (m – 1).

Доказательство. Пусть функция $f(\boldsymbol{x}) \in P_2(n)$, при этом $m < n - 1$, или $n - m + 1 > 2$. Выберем произвольную подфункцию $g(\boldsymbol{y}) \in P_2(n - m + 1)$ функции $f(\boldsymbol{x})$ и произвольный вектор $\boldsymbol{a}$ длины $n - m + 1$ с весом единица. Разложим подфункцию по переменной y_i, соответствующей $a_i = 0$:

$$g\ (\boldsymbol{y}) = y_i\ h\ (\boldsymbol{z}) \oplus (y_i \oplus 1)\ q(\boldsymbol{z}).$$

Здесь $\boldsymbol{z} = (y_1, y_2, \dots,\ y_{i-1},\ y_{i+1}, \dots, y_{n-m+1})$.

Пусть $\boldsymbol{b} = (a_1, a_2, \dots,\ a_{i-1}, a_{i+1}, \dots, a_{n-m+1})$, очевидно, что $\|\boldsymbol{b}\| = 1$.

Вычислим производную функции g (y) по направлению вектора $\boldsymbol{a}$:

$$g'_{\boldsymbol{a}}(y) = y_i h(\boldsymbol{z}) \oplus (y_i \oplus 1)\ q(\boldsymbol{z}) \oplus y_i h(\boldsymbol{z} \oplus \boldsymbol{b}) \oplus (y_i \oplus 1)\ q(\boldsymbol{z} \oplus \boldsymbol{b}) =$$

$$= y_i h'_{\boldsymbol{b}}(\boldsymbol{z}) \oplus (y_i \oplus 1)\ q'_{\boldsymbol{b}}(\boldsymbol{z}).$$

Подфункции h, g от $n - m$ переменных, их производные по направлению вектора с весом единица уравновешены, так как функция f удовлетворяет критерию SAC(m). Производная $g'_a(y)$ является уравновешенной, так как x

$$\|g'_{\boldsymbol{a}}\| = \|h'_{\boldsymbol{b}}\| + \|q'_{\boldsymbol{b}}\|.$$

Произвольность выбора подфункции $g(y)$ и вектора $\boldsymbol{a}$ доказывает утверждение. ■

Теорема 7.2. Во множестве $P_2(n)$ критерий SAC (n – 2) выполняется для функций вида

$$f(\boldsymbol{x}) = \sum_{1 \le i < j \le n} x_i x_j \oplus (\boldsymbol{a}, \boldsymbol{x}) \oplus b$$

и только таких.

Доказательство.

1. Достаточность. Докажем, что для функции данного вида выполняется критерий SAC (n – 2). Зафиксируем произвольно любые (n – 2) переменные, получим подфункцию

$$h(x_i, x_j) = x_i x_j \oplus c_i x_i \oplus c_j x_j \oplus c.$$

Можно убедиться, что производные подфункции h по направлениям (0 1) и (1 0) с весом единица оказываются уравновешенными.

2. Необходимость. Выберем произвольно пару переменных $x_i, x_j, i \neq j$, зафиксируем остальные нулями. В АНФ подфункции останутся слагаемые

из АНФ исходной функции, степень которых не более двух. Для полученной подфункции выполняется критерий SAC, поэтому она не имеет линейных и фиктивных переменных. Это значит, что в ее АНФ входит моном $x_i x_j$. Следовательно, АНФ функции $f(\boldsymbol{x})$ содержит слагаемые вида $x_i x_j$ для всех пар $i \neq j, i < j$.

Докажем, что deg (*f*) = 2. Допустим противное: deg (*f*) > 2. Выберем моном наибольшей степени и две переменные из него x_i, x_j. Пусть $\boldsymbol{y} = \{x_1, x_2, \ldots, x_n\} \setminus \{x_i, x_j\}$ и разложим функцию по переменным x_i, x_j:

$$f(\boldsymbol{x}) = x_i x_j f_1(\boldsymbol{y}) \oplus x_1 f_2(\boldsymbol{y}) \oplus x_2 f_3(\boldsymbol{y}) \oplus f_4,$$

где по предположению $f_1 \neq \text{const}$. Тогда существует значение $\boldsymbol{y}$, при котором $f_1(\boldsymbol{y}) = 0$, и при соответствующей фиксации переменных получим аффинную подфункцию. Для нее критерий SAC не выполняется, это противоречит требованию SAC (*n* – 2). ■

Теорема 7.3. (О степени функции, для которой выполняется критерий SAC).

Пусть $f(\boldsymbol{x}) \in P_2(n)$, $n \geq 3$, выполняется критерий SAC (m) для $m < n - 2$. Тогда

$$\deg(f) \leq n - m - 1.$$

Доказательство. Предположим обратное: deg (*f*) = *d* > *n* – *m* – 1. Выберем в алгебраической нормальной форме функции *f* моном длины *d* и зафиксируем все переменные, которые не входят в него. Получим подфункцию степени *d* от *d* переменных. По условию теоремы и предположению получим $d \geq 3$. Для таких функций критерий SAC не выполняется. Следовательно, для функции *f* не выполняется критерий SAC (*n* – *d*). Получаем, что $n - d \leq m$, а по условию теоремы критерий с таким значением должен выполняться. ■

7.3. Критерий распространения

Определение 7.7. Для функции $f(\boldsymbol{x}) \in P_2(n)$ выполняется *критерий распространения* (PC, *Propagation Criterion*), по направлению $\boldsymbol{a}$, если $\Delta_f(\boldsymbol{a}) = 0$, (или $f'_{\boldsymbol{a}}$ уравновешена).

Для функции $f(\boldsymbol{x}) \in P_2(n)$ выполняется *критерий распространения степени k* (обозначается PC (*k*)), если $\Delta_f(\boldsymbol{a}) = 0$ для всех векторов $\boldsymbol{a}$ таких, что $1 \leq \|\boldsymbol{a}\| \leq k$.

Смысл критерия распространения следующий. При выполнении критерия РС (k) для любого набора индексов

$$1 \le i_1 < i_2 < \cdots < i_l \le n, l \le k,$$

Изменение компонент аргумента $\boldsymbol{x}$ функции $f(\boldsymbol{x})$ с номерами $i_1, \ldots i_l$ с вероятностью $p = 0{,}5$ приводит к изменению значения функции.

Определение 7.8. Для функции $f(\boldsymbol{x}) \in P_2(n)$ выполняется *критерий распространения степени k порядка m* (РС (k, m)), если для любой ее подфункции от $n - m$ переменных выполняется критерий РС (k).

Из определений получаем, что РС (1) = SAC, РС (1, m) = SAC (m).

Свойства критерия распространения

1. Если $f(\boldsymbol{x}) \in P_2(n)$ и для нее выполняется критерий РС (k), $g \in \mathcal{A}$ (n), то для $f \oplus g$ также выполняется критерий РС (k).

2. Если для функций $f(\boldsymbol{x})$ и $g(\boldsymbol{y})$ выполняется критерий РС (k) и множество переменных в аргументах функций $\boldsymbol{x}, \boldsymbol{y}$ не пересекаются, то и для функции $h(\boldsymbol{x}, \boldsymbol{y}) = f(\boldsymbol{x}) \oplus g(\boldsymbol{y})$ выполняется критерий РС (k).

3. Критерий РС (n) в P_2 (n) выполняется только для бент-функций.

4. Если для $f(\boldsymbol{x}) \in P_2(n)$ выполняется критерий РС ($n - 1$), то cor(f) ≤ 1.

Теорема 7.4. (О функции, для которой выполняется критерий SAC ($n - 2$)).

Пусть $f(\boldsymbol{x}) \in P_2(n)$ и для нее выполняется критерий SAC ($n - 2$). Тогда для f выполняется критерий РС (k, m), если $k + m \le n - 1$ либо $(k + m = n)$ & (k – четное).

Доказательство. Согласно теореме 7.2 достаточно рассмотреть только функции вида

$$f(\boldsymbol{x}) = \sum_{1 \le i < j \le n} x_i x_j \oplus (\boldsymbol{a}, \boldsymbol{x}) \oplus b.$$

Производная такой функции по направлению $\boldsymbol{c}$ имеет вид

$$f'_c(\boldsymbol{x}) = \sum_{1 \le i < j \le n} x_i x_j \oplus \sum_{1 \le i < j \le n} (x_i \oplus c_i)(x_j \oplus c_j) \oplus d =$$

$$= \sum_{i \ne j} c_i x_j \oplus e = \sum_{c_j = 1} \sum_{i \ne j} x_i \oplus e.$$

Пусть $\|\boldsymbol{c}\| = k > 0$. Тогда для любого j переменная x_j входит в сумму k или $k-1$ раз, если $c_j = 0$ или $c_j = 1$. Зафиксируем любые m переменных. Если $k < n - m$, то среди компонент вектора $\boldsymbol{c}$, которые соответствуют незафиксированным переменным, есть и нулевые и единичные. В таком случае хотя бы одна переменная входит в сумму нечетное число раз, а тогда производная подфункции оказывается уравновешенной. Следовательно, для функции $f(\boldsymbol{x})$ выполняется критерий РС (k, m).

Если $k < n - m$, то при фиксации m переменных, которые соответствуют нулевым компонентам вектора $\boldsymbol{c}$, для оставшихся переменных выполняется условие $c_j = 1$, т. е. они входят в сумму $k-1$ раз. В таком случае производная будет уравновешена только при нечетности числа $k-1$ или четности числа k. ■

7.4. Глобальные лавинные характеристики

Критерий распространения РС (k) характеризует только локальные свойства функции: на множестве векторов $\boldsymbol{a}$, $1 \le \|\boldsymbol{a}\| \le n$, должно выполняться $\Delta_f(\boldsymbol{a}) = 0$. Можно определить глобальные лавинные характеристики, они характеризуют функцию автокорреляции в целом.

Сумма квадратов:

$$\sigma_f = \langle \Delta_f, \Delta_f \rangle = \sum_{\boldsymbol{u}} \Delta_f^2(\boldsymbol{u}).$$

Абсолютный показатель:

$$\Delta_f = \max_{\boldsymbol{u} \neq \boldsymbol{0}} |\Delta_f(\boldsymbol{u})|.$$

Чем меньше значения σ_f и Δ_f, тем лучше лавинные характеристики функции $f(\boldsymbol{x})$.

Утверждение 7.3. (свойства σ_f). Пусть $f(\boldsymbol{x}) \in P_2(n)$. Тогда:

1) $2^{2n} \le \sigma_f \le 2^{3n}$;

2) $\sigma_f = 2^{2n}$ для бент-функций и только для них;

3) $\sigma_f = 2^{3n}$ для аффинных функций и только для них.

Доказательство. Поскольку $\Delta_f(\boldsymbol{0}) = 2^n$ и $\sigma_f \ge \Delta_f^2(\boldsymbol{0})$, неравенство $2^{2n} \le \sigma_f$ выполняется. Равенство будет иметь место тогда и только тогда, когда $\Delta_f(\boldsymbol{0}) = 0$ для всех векторов $\boldsymbol{u} \neq \boldsymbol{0}$, а это выполняется для бент-функций и только для них.

Обозначим:

$$\boldsymbol{a} = \left(\Delta_f(\mathbf{0}), \dots, \Delta_f(\mathbf{1})\right),$$

$$\boldsymbol{b} = \left(W_f^2(\mathbf{0}), \dots, W_f^2(\mathbf{1})\right).$$

Тогда $\sigma_f = \langle \boldsymbol{a}, \boldsymbol{a} \rangle$ для вектора $\boldsymbol{a}$ выполняется соотношение

$$\boldsymbol{a} = 2^{-n} \boldsymbol{b} H_{2^n}.$$

Рассмотрим скалярное произведение

$$\langle \boldsymbol{b}H_{2^n}, \boldsymbol{b}H_{2^n} \rangle = \sum_i \left(\sum_j b_j (-1)^{(i,j)} \sum_k b_k (-1)^{(i,k)} \right) =$$

$$= \sum_j b_j \sum_k b_k \sum_i (-1)^{(i,k \oplus j)} = 2^n \sum_j b_j \sum_k b_k \, \delta\,(k,j) = 2^n \sum_j b_j^2.$$

Теперь можно выписать выражение для характеристики суммы квадратов:

$$\sigma_f = (\boldsymbol{a}, \boldsymbol{a}) = 2^{2n} (\boldsymbol{b}H_{2^n}, \boldsymbol{b}H_{2^n}) = 2^{-n} \sum_j W_f^4(j) \leq$$

$$\leq 2^{-n} \left(\sum_j W_f^2(j) \right)^2 = 2^{-n} (2^{2n})^2 = 2^{3n}.$$

Последнее равенство выполняется в силу равенства Парсеваля. В данной цепочке соотношений неравенство становится равенством тогда и только тогда, когда

$$W_f^2(\boldsymbol{u}) W_f^2(\boldsymbol{v}) = 0$$

для всех $\boldsymbol{u} \neq \boldsymbol{v}$. Это значит, что $W_f(\boldsymbol{u}) \neq 0$ для единственного вектора $\boldsymbol{u} \in \mathbb{Z}_2^n$. Из равенства Парсеваля получаем

$$W_f(\boldsymbol{u}) = \pm 2^n.$$

Следовательно, функция $f(\boldsymbol{x})$ совпадает с линейной функцией $(\boldsymbol{u}, \boldsymbol{x})$ или ее отрицанием. ■

Утверждение 7.4 (свойства Δ_f). Пусть $f(\boldsymbol{x}) \in P_2(n)$. Тогда:
1) $0 \leq \Delta_f \leq 2^n$;

2) $\Delta_f = 0$ для бент-функций и только для них;

3) $\Delta_f = 2^n$ для функций, имеющих линейную структуру и только для них.

Доказательство. Свойство 1 следует из определения абсолютного показателя; свойство 2 выполняется только для функций, для которых производные по всем ненулевым направлениям уравновешены, т. е. для бент-функций. Свойство 3 выполняется, если производная функции по некоторому направлению равна константе, т. е. функция обладает линейной структурой. ■

7.5. Частичные бент-функции

Пусть $f(\boldsymbol{x}) \in P_2(n)$. Обозначим

$$M_{\Delta_f} = \left|\left\{\boldsymbol{x} \in \mathbb{Z}_2^n \mid \Delta_f(\boldsymbol{x}) \neq 0\right\}\right|;$$
$$M_{W_f} = \left|\left\{\boldsymbol{x} \in \mathbb{Z}_2^n \mid \mathrm{W}_f(\boldsymbol{x}) \neq 0\right\}\right|.$$

Утверждение 7.5 (соотношение неопределенности). Для любой функции $f(\boldsymbol{x})$ из множества $P_2(n)$

$$M_{\Delta_f} \cdot M_{W_f} \geq 2^n.$$

Доказательство. Пусть

$$\max_{\boldsymbol{x}} \left|W_f(\boldsymbol{x})\right| = \left|W_f(\boldsymbol{a})\right|.$$

Рассмотрим функцию $g(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x})$; для пары f, g имеем:

$$M_{\Delta_f} = M_{\Delta_g};$$
$$M_{W_f} = M_{W_g}.$$

(см. свойства автокорреляции и свойства преобразования Уолша – Адамара).

Кроме того,

$$\left|W_g(\mathbf{0})\right| = \left|W_f(\boldsymbol{a})\right| = \max_{\boldsymbol{x}} \left|W_g(\boldsymbol{x})\right|,$$

так как спектры функций f и g совпадают.

Выведем соотношение неопределенности для функции $g(\boldsymbol{x})$:

$$\sum_{\boldsymbol{x}} \Delta_g(\boldsymbol{x}) \leq M_{\Delta_g} \cdot \max_{\boldsymbol{x}} \Delta_g(\boldsymbol{x}) = M_{\Delta_g} \cdot 2^n;$$

$$\sum_{\boldsymbol{x}} W_g^2(\boldsymbol{x}) = 2^{2n} \leq M_{W_g} \cdot W_g^2(\mathbf{0}) = M_{W_g} \cdot \sum_{\boldsymbol{x}} \Delta_g(\boldsymbol{x}) \leq M_{W_g} \cdot M_{\Delta_g} \cdot 2^n.$$

Соотношение неопределенности выполняется для функции $g(\boldsymbol{x})$, следовательно, и для функции $f(\boldsymbol{x})$.

Определение 7.9. Функция $f(\boldsymbol{x}) \in P_2(n)$ называется *частично бент-функцией*, если

$$M_{\Delta_f} \cdot M_{W_f} = 2^n.$$

Количество и распределение нулевых значений функции Уолша – Адамара определяют корреляционную иммунность функции. Нулевые значения автокорреляционной функции определяют выполнение критерия распространения. Можно сказать, что частичные бент-функции оптимальны по этим двум характеристикам. Примерами частичных бент-функций являются все бент-функции – для них $M_{W_f} = 2^n$, $M_{\Delta_f} = 1$; а также все аффинные функции – для них $M_{W_f} = 1$, $M_{\Delta_f} = 2^n$.

Утверждение 7.6. Частично бент-функции платовидны.

Доказательство. Пусть $f(\boldsymbol{x}) \in P_2(n)$ – частично бент-функция, для нее имеем

$$\max_{\boldsymbol{x}} \left|W_f(\boldsymbol{x})\right| = \left|W_f(\boldsymbol{a})\right|.$$

Определим функцию $g(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x})$. Функция $g(\boldsymbol{x})$ также является частично бент-функцией, для нее имеем:

$$\sum_{\boldsymbol{x}} W_g^2(\boldsymbol{x}) = M_{W_g} \cdot W_g^2(\boldsymbol{0}).$$

Следовательно,

$$\sum_{\boldsymbol{x}} W_f^2(\boldsymbol{x}) = M_{W_f} \cdot \max_{\boldsymbol{x}} W_f^2(\boldsymbol{x}).$$

Это возможно, если все ненулевые значения $W_f^2(\boldsymbol{x})$ одинаковы и равны $\max_{\boldsymbol{x}} W_f^2(\boldsymbol{x})$. ■

Утверждение 7.7. Пусть $f(\boldsymbol{x}) \in P_2(n)$ – частично бент-функция. Тогда существует вектор $\boldsymbol{a} \in \mathbb{Z}_2^n$, такой, что для всякого $\boldsymbol{x} \in \mathbb{Z}_2^n$ выполняется одно из равенств:

$$\Delta_f(\boldsymbol{x}) = 0,$$

$$\Delta_f(\boldsymbol{x}) = (-1)^{(\boldsymbol{a},\boldsymbol{x})} \cdot 2^n.$$

Доказательство. В случае, если все ненулевые значения $\Delta_g(\boldsymbol{x}) = 2^n$, выполняется равенство

$$\sum_{\boldsymbol{x}} \Delta_g(\boldsymbol{x}) = M_{\Delta_g} \cdot 2^n.$$

Для функции $f(\boldsymbol{x}) = g(\boldsymbol{x}) \oplus (\boldsymbol{a}, \boldsymbol{x})$ получим

$$\Delta_f(\boldsymbol{x}) = \sum_{\boldsymbol{u}} (-1)^{g(\boldsymbol{u}) \oplus (a,u) \oplus g(\boldsymbol{x} \oplus \boldsymbol{u}) \oplus (a, \boldsymbol{u} \oplus x)} = (-1)^{(\boldsymbol{a},\boldsymbol{x})} \Delta_g(\boldsymbol{x}). \blacksquare$$

Итог: производные частичной бент-функции или уравновешены, или константы. Вектором направления производной можно выбрать тот, на котором значение функции Уолша-Адамара не равно нулю.

Утверждение 7.8. Пусть $f(\boldsymbol{x}) \in P_2(n)$ – частично бент-функция, множество E_f – пространство ее линейных структур:

$$E_f = \{\boldsymbol{a} \in \mathbb{Z}_2^n, \mid f'_{\boldsymbol{a}} = \text{const}\}.$$

Тогда для $f(\boldsymbol{x})$ выполняется критерий РС (k) тогда и только тогда, когда вес любого ненулевого вектора в E_f больше k.

Без доказательства.

Утверждение 7.9. Частично бент-функция уравновешена тогда и только тогда, когда ее производная по некоторому направлению равна константе 1.

Доказательство. Необходимость. Пусть $f(\boldsymbol{x}) \in P_2(n)$ – уравновешенная частично бент-функция. Тогда $W_f(\boldsymbol{0}) = 0$. По следствию 1 теоремы 7.1 имеем

$$W_f^2(\boldsymbol{0}) = \sum_{\boldsymbol{a}} \Delta_f(\boldsymbol{a}).$$

Кроме того, $\Delta_f(\boldsymbol{a}) \in \{0, 2^n\}$. Тогда, в силу уравновешенности функции $f(\boldsymbol{x})$,

$$W_f^2(\boldsymbol{0}) = \sum_{\boldsymbol{a}} \Delta_f(\boldsymbol{a}) = 2^n(c_1 - c_2) = 0.$$

Здесь c_1 – количество положительных значений $\Delta_f(\boldsymbol{a})$ (случай $f'_{\boldsymbol{a}} = \text{const} = 0$); c_2 – количество отрицательных значений $\Delta_f(\boldsymbol{a})$ (случай $f'_{\boldsymbol{a}} = \text{const} = 1$). Число $c_1 > 0$ в силу условия $\Delta_f(\boldsymbol{0}) = 2^n$, тогда и $c_2 > 0$.

Достаточность. Если $f'_{\boldsymbol{a}} = \boldsymbol{1}$, то $f(\boldsymbol{x}) = f(\boldsymbol{x} \oplus \boldsymbol{a}) \oplus 1$ для всех $\boldsymbol{x} \in \mathbb{Z}_2^n$. Это означает уравновешенность функции. ■

Контрольные вопросы и задания

1. Функция автокорреляции дискретной функции. Привести определение, перечислить основные свойства.

2. Указать связь функции автокорреляции и значения совершенной нелинейности для дискретной функции.

3. Указать связь вектора значений функции автокорреляции и вектора значений коэффициентов преобразования Уолша.

4. Дать определение и эквивалентные формулировки выполнения для дискретной функции строгого лавинного критерия.

5. Дискретные функции, для которых выполняется строгий лавинный критерий максимального порядка.

6. Привести выражение для связи алгебраической нелинейности порядка строгого лавинного критерия.

7. Глобальные лавинные характеристики, привести формулы для определения их значений.

8. Перечислить свойства суммы квадратов.

9. Перечислить свойства абсолютного показателя.

10. Соотношение неопределенности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Основы криптографии : учебное пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – 3-е изд., испр. и доп. – Москва : Гелиос АРВ, 2005. – 480 с.

2. *Глухов, М. М.* Алгебра : учебник в 2-х т. Том 1 / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. – Москва : Гелиос АРВ, 2003. – 336 с.

3. *Глухов, М. М.* Математическая логика. Дискретные функции. Теория алгоритмов : учебное пособие / М. М. Глухов, А. Б. Шишков. – Санкт-Петербург : Изд-во «Лань», 2012. – 416 с.

4. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов : учебное пособие для вузов / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков. – 3-е изд., стер. – Санкт-Петербург : Изд-во «Лань», 2022. – 112 с.

5. *Коржик, В. И.* Основы криптографии / В. И. Коржик, В. А. Яковлев. – Санкт-Петербург : Интермедия, 2016. – 312 с.

6. *Кузнецов, О. П.* Дискретная математика для инженера / О. П. Кузнецов. – 6-е изд., стер. – Санкт-Петербург : Изд-во «Лань», 2014. – 400 с.

7. *Логачёв, О. А.* Булевы функции в теории кодирования и криптологии / О. А. Логачёв, А. А. Сальников, В. В. Ященко. – Москва : МЦНМО, 2004.

8. *Лось, А. Б.* Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. – 2-е изд., испр. – Москва : Изд-во Юрайт, 2016, 473 с. – Серия: Бакалавр, Академический курс.

9. *Люстерник, Л. А.* Элементы функционального анализа / Л. А. Люстерник, В. И. Соболев – Москва : Гос. изд. технико-теоретической литературы, 1951. – 390 с.

10. *Панкратова, И. А.* Булевы функции в криптографии : учебное пособие / И. А. Панкратова. – Санкт-Петербург : Изд-во «Лань», 2019. – 92 с.

11. *Сачков, В. Н.* Введение в комбинаторные методы дискретной математики / В. Н. Сачков. – 2-е изд., испр. и доп. – Москва : МЦНМО, 2004. – 424 с.

12. *Супрун, В. П.* Основы теории булевых функций / В. П. Супрун. – Москва : ЛЕНАНД, 2017. – 208 с.

13. *Токарева, Н. Н.* Нелинейные булевы функции: бент-функции и их обобщения / Н. Н. Токарева. – Saarbrucken : LAP LAMBERT Academic Publishing, 2011.

14. *Фомичёв, В. М.* Криптографические методы защиты информации. В 2-х ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников; под ред. В. М. Фомичёва. – Москва : Изд-во Юрайт. 2017. – 209 с. – Серия; Бакалавр. Академический курс.

15. *Яблонский, С. В.* Введение в дискретную математику : учебное пособие для вузов / С. В. Яблонский ; под ред. В. А. Садовничего. – 4-е изд., стер. – Москва : Высшая шк.; 2003. – 384 с.

УКАЗАТЕЛЬ

m-оптимальная функция, 34
m-устойчивость, 30
аддитивный характер поля, 36
алгебра высказываний, 8
алгебраическая нормальная форма (АНФ), 19
алгебра логики, 8
амплитуда платовидной функции, 76
аффинное преобразование переменных, 43
аффинные функции, 25
бент-функция, 63
булева алгебра дискретных функций, 15
булево отображение, 16
булева алгебра логических функций, 11
вектор значений, 9
вектор истинности, 9
вес булева вектора, 16
вес булевой функции, 17
взаимная информация, 29
дуальная функция, 66
задающий вектор линейной функции, 25
квазилинейная зависимость, 26
класс функций с линейной структурой, 69
корреляционная иммунность порядка *m*, 29, 81
коэффициент разложения функции, 18
коэффициенты АНФ, 19
коэффициенты Уолша, 40
коэффициенты Уолша – Адамара первого рода, 38
критерий корреляционной иммунности уравновешенной функции, 30
критерий распространения, 84
критерий распространения степени *k*, 84
критерий распространения степени *k* порядка *m*, 85
линейная зависимость от переменной, 26
линейная структура функции, 69
линейная функция, 24
линейное векторное пространство, 15
логические функции, 8
максимально нелинейная функция, 63
матрица Адамара порядка *k*, 51
матрица Сильвестра – Адамара, 52
метрическое пространство, 15
моном, 19
наилучшее аффинное приближение функции, 60
нелинейность булевой функции, 60
несущественная или фиктивная переменная, 9
норма, 15
норма вектора, 16

нормированное пространство, 15
перекос вероятностей, 47
платовидная функция, 76
подфункция, 30
полином Жегалкина, 19
полная система функций, 10
представление булевой функции в форме Уолша, 40
представление функции, 49
преобразование Мёбиуса, 19
преобразование Уолша – Адамар второго рода, 40
преобразование Уолша – Адамара, 40
производная функции $f(x)$ по направлению вектора, 68
разложение по переменным, 11
разложение функции в ряд Фурье, 38
сбалансированная функция, 17
совершенная дизъюнктивная нормальная форма (СДНФ), 11
совершенная нелинейность функции, 70
совершенно некоррелированные функции, 79
совершенно нелинейная функция, 72
спектр Уолша, 40
спектр Уолша – Адамара первого рода, 38
спектр Фурье, 38
статистическая независимость, 29
статистическая независимость от подмножества своих переменных, 29
статистическая структура, 46
статистический аналог, 47
степень (алгебраическая степень) функции, 24
степень монома, 24
строгий лавинный критерий, 81
строгий лавинный критерий порядка m, 82
строка значений, 9
строка истинности, 9
табличное представление логической функции, 8
тензорное (кронекерово) произведение матриц, 50
уравновешенная функция, 17
функции алгебры логики, 8
функция автокорреляции, 79
функция взаимной корреляции, 79
функция Уолша, 40
характеристическое представление булевой функции, 40, 52
циркулянтная матрица, 51
частично бент-функция, 89