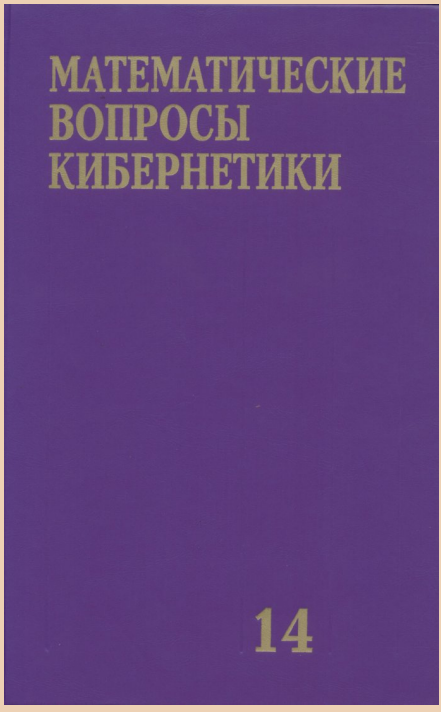
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 14



А. В. Черемушкин

Линейная и аффинная классификация дискретных функций (обзор публикаций)

Рекомендуемая форма библиографической ссылки: Черемушкин А. В. Линейная и аффинная классификация дискретных функций (обзор публикаций) // Математические вопросы кибернетики. Вып. 14. — М.: Физматлит, 2005. — С. 261–280. URL: http://library.keldysh.ru/mvk.asp?id=2005-261

ЛИНЕЙНАЯ И АФФИННАЯ КЛАССИФИКАЦИЯ ДИСКРЕТНЫХ ФУНКЦИЙ *)

(обзор публикаций)

А. В. ЧЕРЕМУШКИН

(МОСКВА)

Под классификацией функций будем понимать описание орбит (классов эквивалентности) групп преобразований, действующих на множестве функций. Следует различать задачу классификации и задачу перечисления. *Задача перечисления* состоит в нахождении числа классов эквивалентности функций в данной классификации. *Задача классификации* состоит в получении полного списка представителей и описании классов эквивалентности **).

Обе задачи имеют уже более, чем полувековую историю. После интенсивного развития на раннем этапе, когда удалось получить первые общие результаты и провести вычисления для всех функций от четырех переменных, наступил относительно долгий период постепенного освоения больших размерностей. Обзоры результатов по обеим задачам можно найти соответственно в [2] и [9]. Вместе с тем, за последние годы интерес к данным вопросам вновь обострился. Это произошло во многом благодаря развитию техники работы с факторпространствами, получаемыми из подпространств функций ограниченной степени нелинейности (кодов Рида — Маллера), основанной на использовании преобразования Фурье, производных по направлению и ограничений на многообразия (подробнее см., например, в [38, 41, 49]), а также распространению на случай факторпространств перечислительных результатов (см. [66, 67]), позволивших существенно облегчить работу по получению классификаций.

§ 1. Задача классификации функций

Основные обозначения. Пусть $n \geqslant 1$, $V_n(2) = GF(2)^n$, $\mathscr{F}_n = \{f\colon V_n(2) \to GF(2)\}$ — множество двоичных функций, $GL(n, 2)$ — полная линейная группа преобразований, $AGL(n, 2) = GL(n, 2)H_n$ — полная аффинная группа, H_n — группа сдвигов пространства $V_n(2)$ (группы инвертирований переменных), S_n — группа перестановок переменных, $Q_n = S_n \cdot H_n$ — группа Джевонса.

Действие элементов группы $AGL(n, 2)$ на V_n будем записывать в виде $x^\alpha = x^\beta \oplus b$, где $x \in V_n(2)$, $\alpha \in AGL(n, 2)$, $\beta \in GL(n, 2)$, $b \in V_n(2)$, либо

*) Работа выполнена при поддержке гранта Президента РФ НШ № 2358.2003.9.

**) Иногда используют термин *полное перечисление* (complete enumeration), который означает построение полного списка представителей с указанием мощностей классов.

© А. В. Черемушкин, 2005

использовать матричную запись $x^\alpha = xA \oplus b$, где A — обратимая матрица. Группа $G \leqslant AGL(n, 2)$ действует на множестве $\mathcal{F}_n$ по правилу:

$$f^\alpha(x) = f(x^{\alpha^{-1}}), \quad f \in \mathcal{F}_n, \alpha \in G, x \in V_n(2).$$

Определим для каждого целого $s \geqslant 0$ подпространства

$$\mathcal{U}_s = \{f\colon \deg f \leqslant s\} = RM(s, n) \leqslant \mathcal{F}_n. \tag{1}$$

Так как $\mathcal{U}_0 = \{0, 1\} \neq \{0\}$, то имеет смысл при $s < 0$ положить $\mathcal{U}_s = \{0\}$. Пусть также

$$\mathcal{U}_s^{(0)} = \{f \in \mathcal{U}_s\colon f(0) = 0\} = RM_0(s, n).$$

Действие группы G, $G \leqslant AGL(n, 2)$, на факторпространствах $\mathcal{U}_k/\mathcal{U}_s = \{f \oplus \oplus \mathcal{U}_s\}$, $-1 \leqslant s < k \leqslant n$, определяется обычным образом: $(f \oplus \mathcal{U}_s)^\alpha = f^\alpha \oplus \mathcal{U}_s$, $f \in \mathcal{U}_k$, $\alpha \in G$.

Несложно показать, что подпространства $\mathcal{U}_s$ ($\mathcal{U}_s$ и $\mathcal{U}_s^{(0)}$) при $-1 \leqslant s \leqslant n-1$ образуют множество всех собственных инвариантных подпространств в $\mathcal{F}_n$ относительно группы $AGL(n, 2)$ ($GL(n, 2)$), а факторпространства $\mathcal{U}_{s+1}/\mathcal{U}_s$ являются неприводимыми представлениями группы $GL(n, 2)$.

Определим также группы

$$G\mathcal{U}_s = \{(\alpha, h)\colon \alpha \in G, \ h \in \mathcal{U}_s\}. \tag{2}$$

Операция в этой группе имеет вид $(\alpha, h) \cdot (\beta, f) = (\alpha\beta, h^\beta \oplus f)$, где (α, h), $(\beta, f) \in G\mathcal{U}_s$, а действие на множестве функций $\mathcal{F}_n$ определяется как $f^{(\alpha, h)} = f^\alpha \oplus h$, где $f \in \mathcal{F}_n$ и $(\alpha, h) \in G\mathcal{U}_s$. (Если $G \leqslant GL(n, 2)$, то удобнее рассматривать группы $G\mathcal{U}_s^{(0)}$.)

Группа инерции функции f в группе $G\mathcal{U}_s$ определяется равенством

$$(G\mathcal{U}_s)_f = \{(\alpha, h) \in G\mathcal{U}_s\colon f^{(\alpha, h)} = f\}.$$

Если для всех целых s положить $G_f^{(s)} = \{\alpha \in G\colon \exists h, (\alpha, h) \in (G\mathcal{U}_s)_f\}$, то, как легко видеть,

$$G_f^{(s)} \cong G_{\{f \oplus \mathcal{U}_s\}} \cong (G\mathcal{U}_s)_f, \tag{3}$$

$$G_f = G_f^{(-1)} \leqslant G_f^{(0)} \leqslant G_f^{(1)} \leqslant \ldots \leqslant G_f^{(\deg f)} = G.$$

Поэтому группы $G_f^{(s)}$ можно рассматривать как «верхние оценки» или «последовательные приближения» группы G_f.

Известные классификации. Основной проблемой, с которой приходится сталкиваться при построении списка представителей конкретной классификации является быстрый рост числа функций с ростом числа переменных. В табл. 1 приведены значения числа классов эквивалентности двоичных функций относительно введенных выше групп [58, 61, 82].

Таблица 1

n	1	2	3	4	5	6	7
H_n	3	7	46	4 336	134 281 216	288 230 380 379 570 176	$> 10^{36}$
S_n	4	12	80	3 984	37 333 248	25 626 412 338 274 304	$> 10^{34}$
Q_n	3	6	22	402	1 228 158	400 507 806 843 728	$> 10^{32}$
$GL(n, 2)$	4	8	20	92	2 744	950 998 216	$> 10^{24}$
$AGL(n, 2)$	3	5	10	32	382	15 768 919	$> 10^{21}$

Если допустить совпадение функций с точностью до инвертирования, то можно уменьшить число классов эквивалентности [60] см. табл. 2.

Таблица 2

n	1	2	3	4	5	6	7
$H_n\mathcal{U}_0$	2	5	30	2 228	67 172 352	144 115 192 303 714 304	$>10^{36}$
$S_n\mathcal{U}_0$	2	6	40	1 992	18 666 624	12 813 206 169 137 152	$>10^{34}$
$Q_n\mathcal{U}_0$	2	4	14	222	616 126	200 253 952 527 184	$>10^{32}$
$GL(n,2)\mathcal{U}_0$	2	4	10	46	1 372	475 499 108	$>10^{23}$
$AGL(n,2)\mathcal{U}_0$	2	3	6	18	206	7 888 299	$>10^{21}$

Из таблиц видно, что первые три группы удобны для классификации только при $n \leqslant 4$, линейная и аффинная группы — только при $n \leqslant 5$, а при $n \geqslant 6$ надо либо увеличить группу преобразований, действующую на множестве функций, либо — ограничить рассматриваемый класс функций. Увеличение групп не всегда удобно, так как если группа слишком велика, то классификация становится бедной и содержит малое число классов очень больших размеров. В связи с этим при выборе класса функций и группы преобразований приходится искать компромисс, при котором классификация не тривиальна, не очень велика, и при этом достаточно информативна.

В [28] предложена группа самодвойственных преобразований, имеющая достаточно большой порядок, но она не нашла широкого применения.

Заметим, что группа $AGL(n,2)$ ($GL(n,2)$) — максимальна в симметрической (знакопеременной группе) подстановок пространства $V_n(2)$ ($V_n(2)\setminus\{0\}$) [17, 69, 72]. Поэтому для получения эффективных классификаций функций от большого числа переменных необходимо уменьшить множество классифицируемых функций. Наиболее удобным для случая линейной и аффинной групп является введение ограничений на степень нелинейности. При этом ее можно ограничивать как сверху, рассматривая только функции ограниченной степени нелинейности из $\mathcal{U}_k$, так и снизу, заменяя равенство функций сравнением по модулю подпространства $\mathcal{U}_s$, что фактически означает переход к факторпространству $\mathcal{U}_k/\mathcal{U}_s$, $-1 \leqslant s < k \leqslant n$.

В силу равенства (2) задача классификации элементов факторпространства $\mathcal{U}_k/\mathcal{U}_s$ относительно группы G равносильна задаче классификации функций из $\mathcal{U}_k$ относительно группы $G\mathcal{U}_s$, причем во многих случаях последний подход оказывается более удобным, так как вместо действия группы G на факторпространстве $\mathcal{U}_k/\mathcal{U}_s$ с элементами $f \oplus \mathcal{U}_s$ проще изучать действие группы $G\mathcal{U}_s$ на пространстве $\mathcal{U}_k$, элементами которого являются обычные функции.

Впервые идея такого подхода применена в [70, 71, 77], где вводится так называемая обобщенная аффинная группа $RAG(n)$ (в наших обозначениях это $AGL(n,2)\mathcal{U}_1$), допускающая помимо аффинного преобразования на множестве аргументов добавление аффинной функции. Как обобщение этого подхода в [51] предлагается рассматривать равенство функций с точностью до одночленов произвольной степени нелинейности и приведена асимптотика числа классов для этого случая. В табл. 3 приведены значения для числа классов эквивалентности при $n \leqslant 7$ [41, 70, 73].

Таблица 3

n	1	2	3	4	5	6	7
$GL(n,2)\mathcal{U}_1$	1	2	3	14	176	7 880 620	$>8\cdot10^{21}$
$AGL(n,2)\mathcal{U}_1$	1	2	3	8	48	150 357	$>6\cdot10^{19}$

Данный поход оказывается удобным еще и по следующим соображениям. Так как подпространства $\mathcal{U}_k$ при $-1 \leqslant k \leqslant n$ вложены друг в друга, то задачу классификации функций из подпространства $\mathcal{U}_k$ можно решать последовательно путем составления сначала классификации элементов факторпространства $\mathcal{U}_k/\mathcal{U}_{k-1}$, затем — из $\mathcal{U}_k/\mathcal{U}_{k-2}$, и т. д. Переход от классификации факторпространства $\mathcal{U}_k/\mathcal{U}_{k-t}$ к классификации факторпространства $\mathcal{U}_k/\mathcal{U}_{k-t-1}$, $1 \leqslant t \leqslant k$, требует для каждого представителя уже полученной классификации перебора не более $|\mathcal{U}_{k-t}|/|\mathcal{U}_{k-t-1}| = 2^{\binom{n}{k-t}}$ вариантов в качестве кандидатов в представители новой классификации.

Для $n = 4$ классификация относительно группы Q_n (точнее $Q_n\mathcal{U}_0$) с указанием минимальной электроламповой реализации была получена в известном Гарвардском каталоге [64]. Затем в [76, 77] она была уточнена и дополнена линейной и аффинной классификацией. В работе [32] собран сводный каталог для разных групп. В последующие годы данная классификация дополнялась путем исследования различных свойств этих функций, так в [14] найдены минимальные реализации в классе пороговых схем, а в [3] — классификация функций по классам Т. Шеффера, характеризующая сложность решения систем уравнений с такими функциями.

Для $n = 5$ первая классификация была получена для группы $AGL(5, 2)\mathcal{U}_1$ в работе [45]. Затем в [33] была построена классификация для группы $AGL(5, 2)$.

Для $n = 6$ в [24] построена аффинная и линейная классификация функций третьей степени с точностью до линейной части, позднее аффинная классификация аннонсирована в [47]. В [73] описан алгоритм получения классификации и найдено число классов эквивалентности для группы $AGL(6, 2)\mathcal{U}_1$. В [36] найдена аффинная и линейная классификация всех функций от шести переменных с точностью до кубической части. Там же найдена аффинная и линейная классификация функций четвертой степени с точностью до квадратичной части, позднее аффинная классификация была аннонсирована в [75].

Для $n = 7$ аффинная классификация функций третьей степени с точностью до квадратичной части получена в [35], а с точностью до линейной части — аннонсирована в [75].

В табл. 4 приведены найденные в [66] числа классов эквивалентности однородных форм от n переменных из $\mathcal{U}_k/\mathcal{U}_{k-1}$ степени k относительно группы $GL(n, 2)$ для $6 \leqslant n \leqslant 11$. Жирным шрифтом отмечены случаи, когда классификация уже известна.

Таблица 4

(k,n)	
(3,6)	**6**
(3,7)	**12**
(3,8)	**32**
(3,9)	**349**
(3,10)	3 691 561
(3,11)	60 889 759 853 600
(4,8)	999
(4,9)	121 597 673 132 830
(4,10)	4 490 513 974 418 226 922 710 218 421 015 600
(4,11)	2 847 591 793 161 852 775 156 648 952 439 351 349 039 810 229 699 431 354 841 358 028
(5,10)	19 749 489 318 110 485 970 697 971 583 208 968 127 316 501 515
(5,11)	15 503 764 406 428 075 099 751 345 714 321 442 971 845 134 712 815 092 309 403 084 719 632 923 886 700 698 844 470 235 742 196 625 592 840

Классификация квадратичных форм получена еще в [52]. Классификация однородных кубических форм для $n=6$ приведена в [80], при $n=7$ получена в [35], а затем в [67]. В приложении к работе [67] приведен список представителей для $n=8$. В [37, 38] получено полное описание строения групп инерции для $n=8$. В [81] найдены порядки групп инерции и весовое распределение кода $RM(3, 8)$. В статье [49] объявлено о завершении классификации для $n=9$ и найдено весовое распределение кода $RM(3, 9)$.

Основные задачи, которые приходится решать при построении классификации — это: поиск представителей классов эквивалентности, доказательство неэквивалентности двух функций, доказательство эквивалентности двух функций и нахождение групп инерции.

Рассмотрим их более подробно. Первые две задачи в основном решаются с использованием инвариантов действия группы на множестве функций, а для решения третьей и четвертой задачи, как правило, применяют инварианты действия группы инерции на связанных с функцией пространствах $V_n(2)$ и двойственном к нему пространстве $V_n^*(2)$.

Поиск представителей классов эквивалентности. Если известно точное число классов эквивалентности, то для нахождения представителей классов достаточно осуществить поиск нужного числа попарно неэквивалентных представителей. Неэквиваелнтность функций проще всего доказывать сравнением значений инвариантов рассматриваемой группы на данных функциях. Порядки классов можно вычислять путем вычисления групп инерции, либо из мощностных соображений после проведения полного перебора.

Если сразу определить точное число классов эквивалентности не удается, то одновременно с проверкой попарной неэквивалентности представителей приходится одновременно вычислять порядки их групп инерции и мощности классов эквивалентности, причем поиск осуществляется до тех пор, пока суммарное число функций в найденных классах эквивалентности не совпадет с мощностью множества классифицируемых функций

$$\sum_{i=1}^{K} \frac{|G|}{|G_{f_i}|} = |\mathcal{F}|,$$

где f_i — представители классов эквивалентности.

Случайный поиск, как наглядно продемонстрировано в [71], обычно не позволяет получить весь список представителей, поскольку мощности классов эквивалентности различаются очень существенно. Поэтому при его применении в подавляющем большинстве случаев получаются функции из классов, мощность которых относительно велика, и практически не находятся функции из классов с относительно малой мощностью.

Для сокращения перебора можно применять различные приемы. Например, каждую функцию от n переменных можно линейным преобразованием привести к виду

$$f(x) = f_1(x_1, \ldots, x_{n-1})x_n \oplus f_0(x_1, \ldots, x_{n-1}),$$

где функция $f_1(x_1, \ldots, x_{n-1})$ имеет степень нелинейности меньшую, чем у исходной функции. Функция $f_0(x_1, \ldots, x_{n-1})$ — может иметь такую же степень, но у нее меньше переменных. Учитывая наличие полученных ранее классификаций функций от $n-1$ переменных, можно выбрать линейное преобразование так, чтобы функция f_1 совпала с одним из описанных ранее представителей. Поэтому достаточно для каждого из известных представителей f_1 перебрать все возможные функции f_0. Этот прием оказывается особенно эффективным в случае классификации однородных форм [38, 49, 66].

При этом, как показано в работе [49], используя известные соотношения эквивалентности, можно дополнительно сократить набор в 2^n раз.

Взаимосвязь аффинной и линейной классификаций. Существует простой способ получения аффинной классификации из линейной и наоборот. Если уже построена аффинная классификация, то для получения из нее линейной надо для каждого представителя $f(x)$ аффинной классификации рассмотреть множество функций $f_a(x)=f(x\oplus a)$, $a\in V_n(2)$, и проверить их попарную (не)эквивалентность между собой относительно линейной группы. Для этого полезным оказывается следующее утверждение.

Утверждение 1. *Пусть* $-1\leqslant s\leqslant n-2$ *и* $f\in\mathscr{F}_n$ — *некоторая функция. Число* $t(f)$ *векторов* $a\in V_n(2)$, *при которых* $f(x)$ *и* $f(x\oplus a)$ *эквивалентны относительно группы* $GL(n,2)\mathscr{U}_s$, *равно индексу* $(AGL(n,2)_f^{(s)}\colon GL(n,2)_f^{(s)})$.

Наоборот, если известна линейная классификация, то для получения из нее аффинной надо объединить классы с аффинно-эквивалентными представителями. Удобнее всего это сделать сравнивая значения инвариантов и применяя утверждение 1.

Еще одним свойством, позволяющим получать из одной классификации другую, является двойственность факторпространств однородных форм

$$\mathscr{U}_k/\mathscr{U}_{k-1}\cong\mathscr{U}_{n-k}/\mathscr{U}_{n-k-1},$$

где $1\leqslant k<n$. Впервые этот факт упоминается [45], потом независимо получен в [67], а затем в другой форме опубликован в [10]. Установим соответствие между однородными формами степеней k и $n-k$ следующим образом. Одночлену $X=x_{i_1}\dots x_{i_k}$, поставим в соответствие одночлен $X^o=x_{j_1}\dots x_{j_{n-k}}$, если

$$\{j_1,\dots,j_{n-k}\}=\{1,\dots,n\}\backslash\{i_1,\dots,i_k\}.$$

Однородной форме $f=\sum\limits_s X_s$ теперь поставим в соответствие однородную форму вида $f^o=\sum\limits_s X_s^o$. Для любого линейного преобразования $\beta\in GL(n,2)$ обозначим через β^* линейное преобразование, матрица которого транспонирована по отношению к обратной матрице линейного преобразования β. Для произвольной подгруппы G группы $GL(n,2)$ обозначим через G^* группу, состоящую из преобразований, матрицы которых получаются транспонированием и обращением матриц преобразований группы G.

Теорема 1. *Пусть* $1\leqslant k<n$. *Для любой однородной формы* f *степени* k *и любого линейного преобразования* $\beta\in GL(n,2)$ *выполнено равенство* $(f^\beta)^o=(f^o)^{\beta^*}$, *где* $\beta^*=(\beta^{-1})^t$. *В частности,*

$$GL(n,2)_{f^o}^{(n-k-1)}=(GL(n,2)_f^{(k-1)})^*.$$

Эта теорема позволяет, в частности, по уже построенной или имеющейся линейной классификации однородных форм степени k построить линейную классификацию однородных форм степени $n-k$.

Заметим, что хотя для неоднородных форм двойственность для представителей и их групп инерции уже не имеет место, тем не менее, как показано [66] для числа $m(n,s,t)$ классов эквивалентности пространства $\mathscr{U}_t/\mathscr{U}_s$ относительно группы $AGL(n,2)$ (и, аналогично, для группы $GL(n,2)$) имеет место следующее соотношение симметрии.

Теорема 2. *Для любого аффинного преобразования* $\alpha\in AGL(n,2)$ *и всех* $-1\leqslant s<t\leqslant n$ *для числа* $N_{(n,t,s)}(\alpha)$ *неподвижных элементов пространства* $\mathscr{U}_t/\mathscr{U}_s$ *относительно* α *выполняется равенство*

$$N_{(n,t,s)}(\alpha)=N_{(n,n-s-1,n-t-1)}(\alpha),$$

в частности, $m(n, s, t) = m(n, n-t-1, n-s-1)$.

Значения $m(n, s, t)$ для $n = 6, 7$ приведены ниже в табл. 10, 11.

Инварианты на множестве функций. Перечислим основные виды инвариантов. При $s \leqslant 1$ наиболее удобны инварианты на основе преобразования Уолша W, $W_f(x) = (\chi_f)^*(x)$, которое представляет собой композицию отображения $\chi_f(x) = (-1)^{f(x)}$, задающего вложение множества двоичных функций в множество целозначных функций на $V_n(2)$, и дискретного преобразования Фурье F: $h \mapsto h^*$, где

$$h^*(a^*) = \sum_{x \in V_n(2)} h(x)(-1)^{(x, a^*)}, \quad a^* \in V_n^*(2),$$

которое задает взаимно однозначное соответствие между множествами комплекснозначных функций на $V_n(2)$ и $V_n^*(2)$. Если определить действие группы $AGL(n, 2)\mathcal{U}_1$ на множестве функций h: $GF(2)^n \to C$, где C — поле комплексных чисел, следующим образом:

$$h^{(A, b, c^*, d)}(x) = h^{(A, b)}(x) \cdot (-1)^{(x, c^*) \oplus d}, \quad x \in V_n(2),$$

где $A \in GL(n, 2)$, $b \in V_n(2)$, $c^* \in V_n^*$, $d \in \{0, 1\}$, и аналогичное действие на множестве функций на $V_n^*(2)$, то можно записать

$$(h^{(A, b, c^*, d)})^* = (h^*)^{(A^*, c^*, b, (b, c^*) \oplus d)}. \tag{4}$$

откуда

$$W_f^{(A, b, c^*, d)} = (W_f)^{(A^*, c^*, b, (b, c^*) \oplus d)}. \tag{5}$$

Таким образом, получаем коммутативную диаграмму

$$\begin{array}{ccccc} f & \longmapsto & \chi_f & \longmapsto & W_f \\ \downarrow (A, b, c^*, d) & & \downarrow (A, b, c^*, d) & & \downarrow (A^*, c^*, b, (b, c^*) \oplus d) \\ f^{(A, b, c^*, d)} & \longmapsto & \chi_{f^{(A, b, c^*, d)}} & \longmapsto & W_{f^{(A, b, c^*, d)}} \end{array}$$

В частности, группа инерции функции f в группе $AGL(n, 2)\mathcal{U}_1$ будет изоморфна группе инерции функции W_f в аналогичной группе преобразований множества функций $V_n^*(2) \to C$. Так как простейшим инвариантом группы, действующей на множестве аргументов, является набор частот значений функции, то, используя этот изоморфизм и свойства преобразования Фурье, можно строить различные серии инвариантов действия линейной и аффинной групп на множестве функций. Например,

— набор частот (модулей) значений W_f является инвариантом группы $AGL(n, 2)_f$ ($(AGL(n, 2)\mathcal{U}_1)_f$);

— набор частот (модулей) значений обратного преобразования Фурье для $(W_f)^2$ будет инвариантом группы $AGL(n, 2)_f$ ($(AGL(n, 2)\mathcal{U}_1)_f$). Заметим, что эти числа задают *функцию автокорреляции*, определяемую равенством

$$r_f(a) = \sum_{x \in V_n(2)} (-1)^{f(x) \oplus f(x \oplus a)} = \frac{1}{2^n} \sum_{b^* \in V_n^*(2)} (W_f(b^*))^2 (-1)^{(a, b^*)},$$

и удовлетворяет свойству

$$r_{f^{(A, b, c^*, d)}} = (r_f)^{(A, c^*)}; \tag{6}$$

— аналогичным способом можно построить серии инвариантов при $k, m = 1, 2, \ldots$ на основе наборов чисел вида:

$$S_f^{(k)}(u) = \sum_{a \in V_n^*} W_f(a^*)^k \cdot (-1)^{(u, a^*)}, \quad u \in V_n(2),$$

$$S_f^{(k, m)}(w^*) = \sum_{a^* \in V_n^*} W_f(a^*)^k \cdot W_f(a^* \oplus w^*)^m, \quad w^* \in V_n^*(2).$$

При $s \geqslant 2$ очень эффективным оказывается подход, основанный на переходе к *производным по направлению* $\Delta_a(x) = f(x \oplus a) \oplus f(x)$, $a \in V_n(2)$. Если $f^{(A, b, h)} = f^{(A, b)} \oplus h$, $(A, b) \in AGL(n, 2)$, $h \in \mathcal{U}_s$, то

$$\Delta_{aA}(f^{(A, b, h)}) = (\Delta_a f)^{(A, b)} \oplus \Delta_{aA} h. \tag{7}$$

Поэтому набор частот значений инварианта группы $G\mathcal{U}_{s-1}$ для всех производных является инвариантом для действия группы $G\mathcal{U}_s$. Таким образом, выбирая различные инварианты группы $G\mathcal{U}_{s-1}$ и рассматривая векторы частот значений инвариантов всех производных данной функции, мы получаем возможность строить инварианты для параметра s, исходя из уже построенных инвариантов для параметра $s-1$. Если обозначить трудоемкость вычисления такого инварианта через $T_1(n, k, s)$, то справедливо соотношение

$$T_1(n, k, s) = (2^n - 1) T_1(n-1, k-1, s-1).$$

Еще один важный класс составляют инварианты на основе множества *ограничений функции на гиперплоскости*. Для ограничения $f|_{a^{*\perp}}$ функции f на гиперплоскость $a^{*\perp} = \{x\colon (x, a^*) = 0\}$, $a^* \in V_n(2)^*$, справедливо равенство

$$f^{(A, h)}|_{(a^* A^*)^\perp} = (f|_{a^{*\perp}})^A \oplus h|_{(a^* A^*)^\perp}, \tag{8}$$

где $f^{(A, h)} = f^A \oplus h$, $A \in GL(n, 2)$, $h \in \mathcal{U}_s$, набор частот встречаемости значений инвариантов всех ограничений исходной функции на всевозможные гиперплоскости будет инвариантом группы $G\mathcal{U}_s$ на множестве функций степени нелинейности не выше k от n переменных. Если функция от n переменных имеет степень нелинейности k, то ее ограничение на произвольную гиперплоскость будет двоичной функцией степени нелинейности не выше k от $n-1$ переменного. Поэтому для трудоемкости вычисления этого инварианта справедливо соотношение

$$T_2(n, k, s) = (2^n - 1) T_2(n-1, k, s).$$

Заметим, что эти два типа инвариантов в определенном смысле двойственны друг другу, так как для единичного базиса $e^1, \ldots, e^n$ пространства $V_n(2)$, соответствующего стандартному представлению функции f, функции f_1 и f_0, участвующие в разложении по первому переменному

$$f(x_1, \ldots, x_n) = x_1 f_1(x_2, \ldots, x_n) \oplus f_0(x_2, \ldots, x_n),$$

представляют собой соответственно производную $\Delta_{e^1} f(x)$ и ограничение функции f на гиперплоскость $e^{1*\perp} = < e^2, \ldots, e^n >$.

Как правило, наиболее эффективным оказывается подход, в котором используются системы различных инвариантов. Например, в [49] для классификации однородных кубических форм от девяти переменных применена полная система из двух инвариантов (Φ_1, Φ_2) следующего вида. Пусть $J^{(k, n)}$ — инвариант классификации форм из $\mathcal{U}_k^{(0)}/\mathcal{U}_{k-1}^{(0)}$. Обозначим $\delta\colon\ a \mapsto \Delta_a f$, $\rho\colon\ a^* \mapsto f|_{a^{*\perp}}$, $a \in V_n(2)$, $a^* \in V_n^*(2)$, $\circ$ — суперпозиция отображений $J \circ h(x) = J(h(x))$. Тогда инварианты Φ_1 и Φ_2 определяются соответственно как наборы частот значений функций $J_1\colon V_n^*(2) \to C^2$ и $J_2\colon V_n(2) \to C^2$ вида

$$J_1(a^*) = ((J^{(3, 8)} \circ \rho)(a^*), (J^{(2, 9)} \circ \delta)^*(a^*)),\ a^* \in V_n^*(2),$$

$$J_2(a) = ((J^{(3, 8)} \circ \rho)^*(a), (J^{(2, 9)} \circ \delta)(a)),\ a \in V_n(2).$$

Еще один из путей построения инвариантов группы инерции для действия на пространстве $V_n(2)$ заключается в вычислении инвариантов функций из 1-окрестности. 1-*окрестность функции* f определяется как множество, состоящее из 2^n функций вида $f_{(a)} = f \oplus i_a$, $a \in V_n(2)$, где

$$i_a(x) = \begin{cases} 1, & x = a; \\ 0, & x \neq a. \end{cases}$$

Для $\alpha = (A, b, g) \in AGL(n, 2)\mathcal{U}_s$ выполнено равенство

$$(f_{(a)})^\alpha = f^\alpha \oplus i_a^{(A, b)} = f^\alpha \oplus i_{a^{(A, b)}} = f^\alpha_{(a^{(A, b)})}. \tag{9}$$

Поэтому набор частот встречаемости значений инвариантов функций из 1-окрестности относительно группы $AGL(n, 2)\mathcal{U}_s$ также является инвариантом группы $AGL(n, 2)\mathcal{U}_s$. При $s = 1$ данный инвариант введен в работе [55].

Интересный инвариант для однородных форм был предложен в работе [67]. Пусть $f = \sum\limits_K a_K X_K$ — однородная форма степени k, где $X_K = \prod\limits_{i \in K} x_i$, $|K| = k$, $2 \leqslant k \leqslant n$. Для положительных s и t, $s + t = k$, определим матрицу $D_{st}(f)$ размера $\binom{n}{s} \times \binom{n}{t}$, строки и столбцы которой индексируются подмножествами мощности s и t соответственно, причем $d_{S, T} = a_{S \cup T}$. Легко проверить, для $\alpha \in GL(n, 2)$ справедливо равенство

$$D_{st}(f^\alpha) = A_s(\alpha)^T D_{st}(f) A_t(\alpha),$$

где $A_s(\alpha)$ — матрица, соответствующая линейному преобразованию на факторпространстве $\mathcal{U}_s / \mathcal{U}_{s-1}$, порожденном множеством одночленов X_S, $|S| = s$. Поэтому отображение

$$I^{(s, t)}: f \mapsto \operatorname{rank}(D_{st}(f)) \tag{10}$$

является инвариантом группы $GL(n, 2)$ при ее действии на множестве форм степени k. Строке с номером $S = \{i_1, \ldots i_s\}$ матрицы $D_{st}(f)$ соответствуют кратная производная $\Delta_{e^{*i_1}} \ldots \Delta_{e^{*i_s}} f$. Поэтому значение $I_{st}(f)$ равно размерности пространства

$$\{\Delta_{e^{*i_1}} \ldots \Delta_{e^{*i_s}} f: \ 1 \leqslant i_1 < \ldots < i_s \leqslant n\} = \{\Delta_{a^{*1}} \ldots \Delta_{a^{*s}} f: \ a^{*1}, \ldots, a^{*s} \in V^*\}.$$

В частности, $I_{1,1}$ при $k = 2$ совпадает с рангом квадратичной формы, а $I_{1, k-1}$ — с размерностью пространства существенных переменных функции f по модулю $\mathcal{U}_{k-1}$. В [67] при поиске представителей в случае $k = 3$, $n = 8$ полным инвариантом оказался инвариант, представляющий собой распределение значений $I^{(2,2)}(\Delta_a f^o)$, $a \in V_n(2)$, где $f^o \in R^*(5, 8)$ — двойственная к f форма.

Общая схема построения инвариантов групп инерции. Пусть $G \leqslant AGL(n, 2)\mathcal{U}_s$, $V = V_n(2)$ или $V_n^*(2)$, $R^V = \{V \to R\}$, R — некоторое множество. Рассмотрим оператор $D: \mathcal{F}_n \to R^V$, где $f \mapsto D_f$. Пусть оператор D удовлетворяет свойству: существуют гомоморфизмы

$$(\varphi, \psi): \ G \longrightarrow AGL(V) \times S(R)$$

(если $G \subseteq GL(n, 2)\mathcal{U}_s$, то надо взять группу $GL(V)$), при которых коммутативна диаграмма

$$\begin{array}{ccc} f & \mapsto & D_f \\ \downarrow \alpha & & \downarrow (\varphi(\alpha), \psi(\alpha)) \\ f^\alpha & \mapsto & D_{f^\alpha} \end{array}$$

то есть

$$D_{f^\alpha} = (D_{f^\alpha}(a),\ a \in V) = (D_f(a^{\varphi(\alpha)^{-1}})^{\psi(\alpha)},\ a \in V) = D_f^{(\varphi(\alpha),\,\psi(\alpha))}.$$

Теорема 3. *Пусть* $f \in \mathcal{F}_n$, $G \subseteq AGL(n,2)\mathcal{U}_s$ ($G \subseteq GL(n,2)\mathcal{U}_s$), D *— введенный выше оператор.*

1) *Если* J *— инвариант группы* $(R, \psi(G))$, *то функция* $I(a) = J(D_f(a))$, $a \in V$, *будет инвариантом группы* $(V, \varphi(G_f))$.

2) *Пусть* $X_1, X_2, \ldots, X_m$ *— разбиение пространства* V *на подмножества, состоящие из векторов* a, *для которых инвариант* I *принимает одинаковые значения. Тогда выполняется включение*

$$\varphi(G_f) \subseteq \bigcap_{i=1}^{m} AGL(V)_{\{X_i\}} \quad (\varphi(G_f) \subseteq \bigcap_{i=1}^{m} GL(V)_{\{X_i\}}).$$

3) *Пусть* $\mathcal{P}$ *— некоторое свойство элементов из* R, *инвариантное относительно действия группы* $\psi(G) \subseteq S(R)$, *и* $M_{\mathcal{P}}$ *— множество векторов* $a \in V$, *для которых* $D_f(a)$ *обладает свойством* $\mathcal{P}$. *Тогда справедливо включение*

$$\varphi(G_f) \subseteq AGL(V)_{\{M_{\mathcal{P}}\}} \quad (\varphi(G_f) \subseteq GL(V)_{\{M_{\mathcal{P}}\}}).$$

Примерами таких операторов являются коэффициенты преобразования Уолша, функция автокорреляции, операторы нахождения производных по направлению, ограничений на гиперплоскости, окрестностей исходной функции и др. Например, для группы $AGL(n,2)\mathcal{U}_1$ в силу равенств (5), и (6) операторы имеют вид, приведенный в табл. 5.

Таблица 5

$D_f(a)$	V	R	α	$\varphi(\alpha)$	$\psi(\alpha)$
$W_f(a^*)$	$V_n^*(2)$	$\boldsymbol{Z}$	(A, b, c^*, d)	(A^*, c^*)	$(b, (b, c^*) \oplus d)$
$\sigma_f(a)$	$V_n(2)$	$\boldsymbol{Z}$	(A, b, c^*, d)	A	c^*

А для действия группы $AGL(n,2)$ на факторпространстве $\mathcal{F}_n/\mathcal{U}_s$ для произвольного целого $s \geqslant -1$ в силу равенств (7), (8) и (9) соответственно получаем операторы, приведенные в табл. 6.

Таблица 6

$D_f(a)$	V	R	α	$\varphi(\alpha)$	$\psi(\alpha)$
$\Delta_a f$	$V_n(2)$	$\mathcal{F}_n/\mathcal{U}_{s-1}$	(A, b)	A	(A, b)
$f\|_{a^{*\perp}}$	$V_n^*(2)$	$\mathcal{F}_{n-1}/\mathcal{U}_s$	A	A^*	A
$f_{(a)}$	$V_n(2)$	$\mathcal{F}_n/\mathcal{U}_s$	(A, b)	(A, b)	(A, b)

Описание групп инерции функций, представимых в виде суммы и произведения функций от меньшего числа переменных можно найти в [39, 40].

Заметим, что при наличии полной системы инвариантов можно избежать необходимости нахождения групп инерции. Так, если известна классификация K функций от $n-1$ переменного из $\mathcal{U}_k^{(0)}$ относительно группы $GL(n-1,2)\mathcal{U}_s^{(0)}$, и J — полный инвариант классификации функций от n переменных из $\mathcal{U}_k^{(0)}$ относительно группы $GL(n,2)\mathcal{U}_s^{(0)}$, то мощность класса эквивалентности с представителем f можно вычислить по формуле

$$\frac{|\,GL(n,2)\,|}{|\,GL(n,2)_f^{(s)}\,|} = \sum_{h \in K} \frac{|\,GL(n-1,2)\,|}{|\,GL(n-1,2)_h^{(s)}\,|} \times |\,\{g \in \mathcal{U}_{k-1}^{(0)} :\ h + g \cdot x_n \sim f\}\,|,$$

где вторые сомножители в сумме вычисляются путем сравнения значений инварианта J (см. [49]).

Доказательство эквивалентности двух функций осуществляется во многом аналогично нахождению групп инерции. Обычно для этого производится вычисление значений инвариантов групп инерции для обеих функций в их действии на пространствах $V_n(2)$ или $V_n(2)^*$, а затем после сопоставления их значений производится перебор возможных вариантов преобразований, переводящих элементы с одинаковыми значениями инвариантов для первой функции в элементы с такими же значениями инвариантов у другой функции, и выяснение, какие из этих преобразований на самом деле преобразуют одну функцию в другую. Полезным оказывается также следующий прием (см., например, [38, 55]), позволяющий вычислять матрицу линейной части преобразования. Для линейного преобразования образы векторов из единичного базиса образуют строки матрицы искомого преобразования. Поэтому нам достаточно найти все возможные образы векторов единичного базиса, а потом составить из них возможные варианты матриц для непосредственной отбраковки.

§ 2. Задача перечисления функций

История вопроса. Впервые задачу подсчета числа классов эквивалентности двоичных функций относительно групп поставил в общем случае Д. Пойа в [79], он же вычислил значения при малых n для групп S_n, Q_n. В [82] указана связь рассматриваемой задачи с теорией представлений групп и найдены явные формулы для вычисления числа классов для этих групп в общем случае. Затем этот подход уточнялся и обобщался в работах [23, 26] и др. В [12] найдено число классов эквивалентности для группы $GL(n, 2)$ при $n \leqslant 5$.

Свой современный вид, как применение теории перечисления Пойа [78], подход приобрел в работах Де Брёйна [4, 50], который привел несколько различных обобщений основной теоремы Пойа, в том числе рассмотрел случай, когда группа действует не только на множестве аргументов, но и значений функции.

Для применения этой теории необходимо подсчитать цикловые индексы групп, в их действии на векторном пространстве. В [44] найден цикловой индекс группы H_n, в [57] получены явные формулы для цикловых индексов групп S_n и Q_n, в [61] — для линейной и аффинной групп [61]. В дальнейшем с помощью результатов Де Брёйна эти результаты были распространены на случай совпадения функций с точностью до инвертирования значений функции [60], систем функций, задающих отображения, и в том числе обратимые преобразования, векторных пространств, [21, 57, 59], а также обобщены на случай k-значных функций [15, 18, 20, 21, 26, 62] и др. В [28, 32] найден цикловой индекс самодвойственной группы. Отметим также работу [19], где теорема Пойа обобщается на случай частично определенных булевых функций.

Способ нахождения циклового индекса группы $AGL(n, 2)\mathcal{U}_1$ путем вложения ее в линейную группу размерности $n+2$ указан в [70, 71], где вычислено число классов для $n \leqslant 5$. В [73] без применения теории Пойа чисто алгоритмически вычислено число классов эквивалентности относительно группы $AGL(6, 2)\mathcal{U}_1$.

Вопрос о применении теории перечисления для групп $GL(n, 2)\mathcal{U}_s$ и $AGL(n, 2)\mathcal{U}_s$ при $s \geqslant 2$ долгое время оставался открытым, пока Хоу в [66, 67] не привел общий способ вычисления числа орбит

групп $AGL(n, 2)$ и $GL(n, 2)$ на $\mathcal{U}_k/\mathcal{U}_s$, основанный непосредственном применении леммы Бернсайда к полиномиальному заданию функций.

Приведем точные формулировки этих результатов.

Асимптотические оценки для числа классов эквивалентности. Свойство тривиальности групп инерции почти всех функций от n переменных при $n \to \infty$, получившее название эффекта Шеннона [42], обеспечивает асимптотическую оценку числа N классов эквивалентности функций относительно группы G вида

$$\frac{2^{2^n}}{|G|} < N \leqslant \frac{2^{2^n}}{|G|}(1 + o(1)).$$

В [8] это свойство было доказано в общем виде для групп, действующих на множестве аргументов функций, в [1] уточнены первые члены асимптотического разложения, а в [5] оно обобщено на группы $AGL(n, 2)\mathcal{U}_s$ (случай $s = 0$ был ранее рассмотрен в [60], а $s = 1$ в [70]). Отметим также работу [6], в которой введена пороговая функция в эффекте Шеннона, равная минимальному числу значений функции в табличном задании, которое надо исправить для нарушения эффекта Шеннона.

Приведем здесь обобщение результата работы [5] на случай факторпространств $\mathcal{U}_k/\mathcal{U}_s$.

Теорема 4 [41]. *Пусть* $s = s(n) \leqslant \frac{n}{2}(1 - \delta)$, $k = k(n) \geqslant \frac{n}{2}(1 + \varepsilon)$, $0 < \delta \leqslant 1$ *и* $0 < \varepsilon \leqslant 1$. *Тогда при* $n \to \infty$ *почти все функции* $f \in \mathcal{U}_k$ *имеют тривиальную группу инерции в группе* $AGL(n, 2)\mathcal{U}_s$.

Теория Пойа — Де Брёйна. Пусть G — группа подстановок множества Ω ($|G| = n$, $|\Omega| = m$). В основе теории перечисления лежит следующая лемма, впервые опубликованная Бернсайдом, но, по-видимому, хорошо известная еще Коши и Фробениусу.

Лемма 1. *Число орбит группы* (G, Ω) *равно*

$$\frac{1}{|G|}\sum_{g \in G} i(g) = \frac{1}{|G|}\sum_{C \subset G} |C| \cdot i(g),$$

где $i(g)$ *— число неподвижных элементов из* Ω *относительно подстановки* $g \in G$, C *— класс сопряженных элементов.*

Цикловой индекс группы (G, Ω) определяется равенством

$$P_G(x_1, \ldots, x_m) = \frac{1}{|G|}\sum_{C} |C| \cdot x_1^{b_1} x_2^{b_2} \ldots x_m^{b_m},$$

где подстановке $g \in G$, имеющей цикловую структуру $[1^{b_1} 2^{b_2} \ldots m^{b_m}]$, $b_1 + 2b_2 + \ldots + mb_m = m$, поставлено в соответствие произведение $x_1^{b_1} x_2^{b_2} \ldots x_m^{b_m}$. Так как число функций $f\colon \Omega \to R$, неподвижных относительно преобразования g на множестве аргументов Ω, равно $|R|^t$, где t — число циклов подстановки g, то в получаем следующий простейший случай теоремы Пойа для перечисления функций.

Теорема 5. *Число классов эквивалентности относительно действия группы* (G, Ω) *на множестве функций* $R^\Omega = \{f\colon \Omega \to R\}$, *задаваемого равенством* $f^g(x) = f(x^{g^{-1}})$, $x \in \Omega$, $g \in G$, *равно* $P_G(|R|, |R|, \ldots, |R|)$, *где* $P_G(x_1, \ldots, x_m)$ *— цикловой индекс группы* (G, Ω).

Сформулируем теперь так называемую основную теорему Пойа. Пусть Q — поле рациональных чисел и $W\colon R^\Omega \to Q$ — некоторое отображение, инвариантное относительно действия группы (G, Ω) на множестве R^Ω. Отображение W задается следующим образом: задаем веса $w(r)$,

$r \in R$, полагаем $W(f) = \prod_{a \in \Omega} w(f(a))$. Если K класс эквивалентности, то $W(K) = W(f)$, $f \in K$.

Теорема 6. *Сумма весов классов эквивалентности относительно действия группы (G, Ω) на множестве функций $R^{\Omega} = \{f: \Omega \to R\}$, задаваемого равенством $f^g(x) = f(x^{g^{-1}})$, $x \in \Omega$, $g \in G$, равна*

$$\sum_K W(K) = P_G\Big(\sum_{r \in R} w(r), \sum_{r \in R} w(r)^2, \ldots, \sum_{r \in R} w(r)^m\Big),$$

где $P_G(x_1, x_2, \ldots, x_m)$ — цикловой индекс группы (G, Ω).

Теорема 5 соответствует случаю, когда веса выбраны равными единице.

Для перечисления k-значных функций представляют интерес два обобщения основной теоремы Пойа, полученные Дж. Де Брейном [4].

Теорема 7. *Сумма весов классов эквивалентности относительно группы $(G, \Omega) \times (H, R)$ на множестве однозначных отображений $R^{\Omega} = \{f: \Omega \to R\}$, равна значению выражения*

$$\sum_K W(K) = P_G\left(\frac{\partial}{\partial z_1}, \frac{\partial}{\partial z_2}, \frac{\partial}{\partial z_3}, \ldots\right) P_H(1 + z_1, 1 + 2z_2, 1 + 3z_3, \ldots), \qquad (11)$$

вычисленному при $z_1 = z_2 = z_3 = \ldots = 0$. В частности, если $|R| = |\Omega|$, то число классов эквивалентности однозначных отображений равно значению выражения

$$P_G\left(\frac{\partial}{\partial z_1}, \frac{\partial}{\partial z_2}, \frac{\partial}{\partial z_3}, \ldots\right) P_H(z_1, 2z_2, 3z_3, \ldots), \qquad (12)$$

вычисленному при $z_1 = z_2 = z_3 = \ldots = 0$.

В табл. 7 приведено число классов эквивалентности однозначных отображений множества двоичных векторов для групп H_n, S_n и Q_n [57],

Таблица 7

Группа $G \times H \setminus n$	1	2	3	4
$H_n \times H_n$	1	6	924	81 738 720 000
$S_n \times S_n$	2	7	1 172	36 325 278 240
$Q_n \times Q_n$	1	2	52	142 090 700

а в табл. 8 — для линейной и аффинной групп [46, 61].

Таблица 8

Группа $G \times H \setminus n$	1	2	3	4	5
$GL(n, 2) \times GL(n, 2)$	2	2	10	52 246	2 631 645 209 645 100 680 644
$AGL(n, 2) \times AGL(n, 2)$	1	1	4	302	2 569 966 041 123 963 092

Для произвольных, не обязательно однозначных, отображений справедлива

Теорема 8. *Сумма весов классов эквивалентности относительно действия группы $(G, \Omega) \times (H, R)$ на множестве функций R^{Ω}, равна значению выражения*

$$\sum_K W(K) = P_G\left(\frac{\partial}{\partial z_1}, \frac{\partial}{\partial z_2}, \frac{\partial}{\partial z_3}, \ldots\right) P_H\left(e^{z_1 + z_2 + z_3 + \ldots}, e^{2(z_2 + z_4 + z_6 + \ldots)}, e^{3(z_3 + z_6 + z_9 + \ldots)}, \ldots\right), \qquad (13)$$

вычисленному при $z_1 = z_2 = z_3 = \ldots = 0$.

Примеры вычислений приведены в табл. 9 [59].

Таблица 9

Группа $G \times H \setminus n$	1	2	3	4
$H_n \times H_n$	2	22	265 728	72 057 598 064 459 776
$S_n \times S_n$	4	88	497 760	32 031 538 353 966 080
$Q_n \times Q_n$	2	13	8 906	125 147 156 711 032
$GL(n, 2) \times GL(n, 2)$	4	20	1 204	45 568 388 658
$AGL(n, 2) \times AGL(n, 2)$	2	5	70	179 125 249

Перечисление классов эквивалентности для полной линейной и аффинной групп. Пусть $G = GL(n, q)$, $q = p^r \geqslant 2$. Каждый класс сопряженных элементов группы $GL(n, q)$ однозначно определяется по второй нормальной форме матрицы. Пусть t_n — число неприводимых многочленов степени не выше n над полем $GF(q)$ (за исключением многочлена $p(x) = x$). Обозначим d_i и e_i степень и показатель многочлена $p_i(x)$. Теперь классы сопряженных элементов группы $GL(n, q)$ можно перенумеровать t_n-наборами $\widehat{a} = (\widehat{a}_1, \widehat{a}_2, \ldots, \widehat{a_{t_n}})$, $\widehat{a}_i = (\alpha_{i1}, \ldots, \alpha_{i m_i})$, описывающими разбиения вида

$$\sum_{i=1}^{t_n} a_i d_i = n, \quad a_i = \sum_{j=1}^{m_i} j\alpha_{ij}, \tag{14}$$

$m_i = \lfloor n/d_i \rfloor$, $i = \overline{1, t_n}$. В итоге описание цикловой структуры матрицы A сводится к двум задачам: нахождению цикловой структуры клеток нормальной формы матрицы A, нахождению цикловой структуры для декартова произведения. Ответ на первую задачу дает следующая теорема.

Теорема 9 [52]. *Если многочлену $f_i(x)$ соответствует разбиение $\widehat{a}_i$ вида $a_i = kd_i$, то соответствующий граф имеет 1 цикл длины 1, и*

$$h_{ij} = \frac{q^{jd_i} - q^{(j-1)d_i}}{q_{ij}}$$

циклов длины $g_{ij} = e_i p^{b_j}$, $b_j = -\lfloor -log_p j \rfloor$ ($\lfloor x \rfloor$ — целая часть числа x), или иначе $p^{b_j - 1} < j \leqslant p^{b_j}$, для каждого $j = \overline{1, k}$.

Таким образом, цикловая структура такого преобразования описывается произведением

$$x_1 \prod_{j=1}^{k} x_{g_{ij}}^{h_{ij}}.$$

Вторая задача решается с помощью введения формальной операции X *декартова произведения многочленов* [82], которая определяется равенством

$$\left(\prod_{s=1} x_s^{i_s}\right) \mathsf{X} \left(\prod_{t=1} x_t^{j_t}\right) = \prod_{s,\,t} \left(x_s^{i_s} \mathsf{X} x_t^{j_t}\right),$$

где $x_s^{i_s} \mathsf{X} x_t^{j_t} = x_{[s,\,t]}^{i_s j_t (s,\,t)}$. Здесь (s, t) и $[s, t]$ обозначают наибольший общий делитель и наименьшее общее кратное чисел s и t. Для записи *декартовой степени* необходимо ввести знак операции $\times$ в показатель: $x^{\times k} = \overbrace{x \times \ldots \times x}^{k}$. Это объясняется тем, что в противном случае символ x^k может обозначать как $\overbrace{x \cdot \ldots \cdot x}^{k}$, так и $\overbrace{x \times \ldots \times x}^{k}$.

Лемма 2 [52]. *Цикловая структура класса сопряженных элементов группы* $GL(n, q)$, *в ее действии на пространстве* $V_n(q)$, *соответствующего* t_n*-набору* $\widehat{a}=(\widehat{a_1}, \widehat{a_2}, \ldots, \widehat{a_{t_n}})$, *где* $\widehat{a_i}$ — *разбиения вида* (14), $i=\overline{1, t_n}$, *описывается выражением*

$$\mathop{\mathsf{X}}_{i=1}^{t_n}\mathop{\mathsf{X}}_{j=1}^{m_i}\left(x_1\prod_{k=1}^{j}x_{q_{ik}}^{h_{ik}}\right)^{\times\alpha_{ij}}.$$

Порядки централизаторов вычисляются следующим образом.

Теорема 10 [52]. *Мощность класса сопряженных элементов группы* $GL(n, q)$, *соответствующего* t_n*-набору* $\widehat{a}=(\widehat{a_1}, \widehat{a_2}, \ldots, \widehat{a_{t_n}})$, *где* $\widehat{a_i}$ — *разбиения вида* (14), $i=\overline{1, t_n}$, *равна*

$$C(\widehat{a})=\frac{|GL(n, q)|}{\prod\limits_{j=1}^{t_n}\left(\prod\limits_{k=1}^{m_j}q^{\alpha_{jk}^2(k-1)}\prod\limits_{k=1}^{m_j-1}\prod\limits_{l=k+1}^{m_j}q^{2k\alpha_{jk}\alpha_{jl}}\right)^{d_j}\prod\limits_{p=1}^{m_j}|GL(\alpha_{jp}, q^{d_j})|}.$$

В итоге получаем выражения для циклового индекса.

Теорема 11 [61]. *Цикловой индекс группы* $GL(n, 2)$, *рассматриваемой как группа подстановок на множестве векторов пространства* $V_n(q)$, *имеет вид*

$$P_{GL(n, q)}(x_1, x_2, \ldots)=\frac{1}{|GL(n, q)|}\cdot\sum_{\widehat{a}}C(\widehat{a})\mathop{\mathsf{X}}_{i=1}^{t_n}\mathop{\mathsf{X}}_{j=1}^{m_i}\left(x_1\prod_{k=1}^{j}x_{g_{ik}}^{h_{ik}}\right)^{\times\alpha_{ij}}.$$

Теорема 12 [61]. *Цикловой индекс группы* $AGL(n, q)$, *рассматриваемой как группа подстановок на множестве векторов пространства* $V_n(q)$, *имеет вид*

$$P_{AGL(n, q)}(x_1, x_2, \ldots)=\frac{1}{|AGL(n, q)|}\cdot\sum_{\widehat{a}}C(\widehat{a})\mathop{\mathsf{X}}_{i=1}^{t_n}\mathop{\mathsf{X}}_{j=1}^{m_i}\left(u_{ij}\right)^{\times\alpha_{ij}},$$

где

$$u_{ij}=\begin{cases}q^{j-1}x_1\prod\limits_{k=1}^{j}x_{g_{1k}}^{h_{1k}}+(q^j-q^{j-1})x_{g_{1, j+1}}^{q^j/g_{1, j+1}}, & i=1;\\ q^{jd_i}x_1\prod\limits_{k=1}^{j}x_{q_{ik}}^{h_{ik}}, & i>1.\end{cases}$$

Перечисление классов эквивалентности для обобщенных линейной и аффинной групп. При $s=1$ можно воспользоваться следующими теоремами [41], в основе доказательства которых лежит идея вложения этих групп в линейную группу большей размерности из работ [70, 71].

Теорема 13. *Число классов эквивалентности двоичных функций относительно группы* $GL(n, 2)\mathcal{U}_1^{(0)}$ *равно*

$$\frac{1}{2^n|GL(n, 2)|}\sum_{\widehat{a}}2^{r(\widehat{a})}C(\widehat{a})\cdot 2^{\nu(\widehat{a})}, \tag{15}$$

где суммирование ведется по всем классам сопряженных элементов группы $GL(n, 2)$, $\nu(\widehat{a})=\sum\limits_{i=1}^{m}b_i$, $[1^{b_1}2^{b_2}, 3^{b_3}\ldots]$ — *цикловая структура линейного преобразования* α: $x\mapsto xA$ *из группы* $GL(n, 2)$, *описываемая* t_n*-набором* $\widehat{a}=(\widehat{a_1}, \widehat{a_2}, \ldots, \widehat{a_{t_n}})$,

$$r(\widehat{a})=\sum_{j=1}^{m_i}(j-1)\alpha_{1j}+\sum_{i=2}^{t_i}\sum_{j=1}^{m_i}j\alpha_{ij}d_i=n-\sum_{j=1}^{m_i}\alpha_{1j}.$$

Теорема 14. *Число классов эквивалентности двоичных функций относительно группы* $AGL(n, 2)\mathcal{U}_1$ *равно значению* $P(2, 2, \ldots)$ *многочлена*

$$P(x_1, x_2, \ldots) = \frac{1}{2^{2n+1} \mid GL(n, 2) \mid} \sum_{\widehat{a}} \prod_{i=1}^{t_n} \prod_{j=1}^{m_i} (w_{ij})^{\times \alpha_{ij}}, \qquad (16)$$

где суммирование ведется по всем классам сопряженных элементов группы $GL(n, 2)$ *и*

$$w_{ij} = \begin{cases} 2^{2(j-1)} x_1 \prod\limits_{k=1}^{j} x_{g_{1k}}^{h_{1k}} + 2^{2j-1} x_{g_{1,j+1}}^{2^j / g_{1,j+1}}, & i = 1; \\ 2^{2(j-1)d_i - 1} x_1 \prod\limits_{k=1}^{j} x_{q_{ik}}^{h_{ik}} & i > 1. \end{cases}$$

Перечисление классов эквивалентности для факторпространств $\mathcal{U}_k/\mathcal{U}_s$ в общем случае при $-1 \leqslant s < k \leqslant n$ получено в [66, 67]. Обозначим пространство многочленов двоичных функций $\mathcal{P}_n$, и пусть $A(\alpha)$ — матрица линейного преобразования на $\mathcal{P}_n$, соответствующая аффинному преобразованию α пространства $V_n(2)$. Она имеет блочный треугольный вид, на ее диагонали стоят подматрицы, соответствующие действию на однородные компоненты многочлена. Пусть $A^{(k,s)}(\alpha)$ — подматрица матрицы $A(\alpha)$, соответствующая одночленам $X_S = \prod\limits_{i \in S} x_i$, $S \subset \{1, \ldots, n\}$, $s < \mid S \mid \leqslant k$. Она же является матрицей линейного преобразования, соответствующего действию преобразования α на пространстве $\mathcal{U}_k/\mathcal{U}_s$ в базисе $\{X_S\}$.

Теорема 15. *Пусть* $-1 \leqslant s < k \leqslant n$. *Число орбит группы* $G \leqslant AGL(n, 2)$ *на* $\mathcal{U}_k/\mathcal{U}_s$ *равно*

$$\frac{1}{\mid G \mid} \sum_{C} \mid C \mid \cdot 2^{n(k,s) - \operatorname{rank}(A^{(k,s)}(\alpha) - E)},$$

где сумма берется по всем классам C *сопряженных элементов группы* G, $\alpha \in C$, E *— единичная матрица.*

Матрицу $A(\alpha)$ можно, например, вычислить с использованием формулы $A(\alpha) = B^{[n]} P(\alpha) B^{[n]}$, где $P(\alpha)$ — подстановочная матрица, соответствующая действию преобразования α на пространстве $V_n(2)$ при лексикографическом упорядочении векторов, а $B^{[n]}$ — n-я кронекерова степень матрицы $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

В заключение приведем (табл. 10 и табл. 11) число классов аффинной эквивалентности форм из $\mathcal{U}_k/\mathcal{U}_s$ при $n = 6, 7$ ([66]). Жирным шрифтом, как и выше, отмечены случаи, когда классификация уже известна.

Таблица 10

$s \setminus k$	0	1	2	3	4	5	6
-1	**2**	**3**	**11**	205	150 357	7 888 299	15 468 919
0		**2**	**7**	120	75 761	3 947 989	7 888 299
1			**4**	**34**	**2 499**	75 761	**150 357**
2				**6**	**34**	120	205
3					**4**	**7**	**11**
4						**2**	**3**
5							**2**

Таблица 11

$s \setminus k$	0	1	2	3	4	5	6	7
-1	**2**	**3**	**12**	3 486	30 230 045 341 814	63 379 147 320 777 408 548	8 112 499 583 888 855 378 066	16 244 999 167 506 438 730 294
0		**2**	**8**	1 890	15 115 039 412 866	31 689 573 670 826 699 852	4 056 249 792 080 063 701 952	8 112 499 583 888 855 378 066
1			**4**	**179**	118 140 881 980	247 576 791 326 613 080	31 689 573 670 826 699 852	63 379 147 320 777 408 548
2				**12**	68 433	118 140 881 980	15 115 039 412 866	30 230 045 341 814
3					**12**	179	1 890	3 486
4						**4**	**8**	**12**
5							**2**	**3**
6								**2**

В табл. 12 и 13 приведено число классов линейной эквивалентности форм из $\mathcal{U}_k/\mathcal{U}_s$ при $n = 6, 7$. Программа для вычисления этих значений с использованием метода [66] написана Лакаевым К. С.

Таблица 12

$s \setminus t$	0	1	2	3	4	5	6
-1	**2**	**4**	**20**	1 534	7 880 620	475 499 108	950 998 216
0		**2**	**10**	767	3 940 310	237 749 554	475 499 108
1			**4**	**85**	74 596	3 940 310	7 880 620
2				**6**	**85**	767	1 534
3					**6**	**10**	**20**
4						**2**	**4**
6							**2**

Таблица 13

$s \setminus t$	0	1	2	3	4	5	6	7
-1	**2**	**4**	**22**	161 652	3 868 829 382 074 516	8 112 499 583 617 583 352 228	1 038 397 981 840 994 509 577 948	2 076 795 963 681 989 019 155 896
0		**2**	**11**	80 826	1 934 414 691 037 258	4 056 249 791 808 791 676 114	519 198 990 920 497 254 788 974	1 038 397 981 840 994 509 577 948
1			**4**	1 596	15 115 005 928 948	31 689 573 649 950 738 696	4 056 249 791 808 791 676 114	8 112 499 583 617 583 352 228
2				**12**	7 384 214	15 115 005 928 948	1 934 414 691 037 258	3 868 829 382 074 516
3					**12**	1 596	80 826	161 652
4						**4**	11	22
5							**2**	**4**
6								**2**

СПИСОК ЛИТЕРАТУРЫ

1. Амбросимов А. С., Шаров Н. Н. Некоторые асимптотические разложения для числа функций с нетривиально группой инерции // Проблемы кибернетики. Вып. 36. — М.: Наука, 1979. — С. 65–86.

2. Гаврилов Г. П., Лисковец В. А., Пермяков П. П., Селиванов Б. И. О некоторых тенденциях теории перечисления // В сб. Перечислительные задачи комбинаторного анализа. Под. ред. Г. П. Гаврилова. — М.:Мир, 1979. — С. 36–138.
3. Гизунов С. А., Носов В. А. О классификациии всех булевых фунций от четырех пременных по классам Шеффера // Обозрение прикладной и промышленной математики. — 1995. — 2. — № 3. — С. 440–467.
4. Де Брейн Н. Дж. Теория перечисления Пойа // В сб. Прикладная комбинаторная математика. Под. ред. Э. Беккенбаха. — М.:Мир, 1968. — С. 61–106.
5. Денев И., Тончев В. О числе классов эквивалентности булевых фунций относительно некоторых групп преобразований // Матем. и матем. образование. Научн. съобщ. на 9-та практ. конф. на съюза на мат. в България, 1980, София. — 1980. — С. 41–43.
6. Денисов О. В. Пороговая функция в эффекте Шеннона для булевых функций относительно симметрической группы // Дискретная математика. — 1993. — Т. 5, вып. 3. — С. 64–75.
7. Дьедонне Ж., Кэрол Дж., Мамфород Д. Геометрическая теория инвариантов. — М.: Мир, 1974.
8. Клосс Б. М., Нечипорук Э. Н. О классификации функций многозначной логики // Проблемы кибернетики. Вып. 9. — М.: Физматгиз, 1963. — С. 27–36.
9. Кузнецов Ю. В., Шкарин С. А. Коды Рида — Маллера (обзор публикаций) // Математические вопросы кибернетики. Вып. 6. — М.: Наука. Физматлит, 1996. — С. 5–50.
10. Логачев О. А., Ященко В. В., Сальников А. А. Об одном свойстве ассоциированных представлений группы $GL(n, k)$ // Дискретная математика. — 2000. — Т. 12, вып. 2. — С. 154–159.
11. Майоров С. А., Паленко В. В., Скорубский В. И. Алгоритмические методы классификации булевых функций // Вопросы теории электронных цифровых математичкеских машин. Труды семинара. — Киев., 1968(69). — Вып. 3. — С. 63–80.
12. Нечипорук Э. И. О синтезе схем с помощью линейных преобразований переменных // ДАН СССР. — 1958. — 123. — 4.
13. Нечипорук Э. И. Булевы функции с инверсиями аргументов // Проблемы кибернетики. Вып. 7. — М.: Физматгиз, 1962. — С. 115–126.
14. Никонов В. Г. Классификация минимальных базисных представлений всех булевых функций от четырех переменных // Обозрение промышленной и прикладной математики. — Т. 1. — Вып. 3. — 1994. — С. 458–545.
15. Окольнишникова Е. А. О распределении типов фукнций q-значной логики по мощности // Методы дискретного анализа в теории графов и логических функций. Вып. 28. — Новосибирск, ИМ СО АН СССР, 1976. — С. 65–77.
16. Поваров Г. Н. О групповой инвариантности булевых функций // An. Stiint. Univ. Iasi. — 1958. — Sec. 1. — № 4. — 39–44. // Сб. Применение Логики в науке и технике. — М., АН СССР, 1960. — С. 263–340.
17. Погорелов Б. А. О максимальных подгруппах симметрческих групп, заданных на проективных пространствах над конечным полем // Матем. заметки. — 1974. — Т. 16. — № 1. С. 91–100.
18. Попов В. А., Скибенко И. Т., Мокляк Н. Г. О числе типов систем k-значных логических функций // Кибернетика. — 1973. — № 3. — С. 18–27.
19. Попов В. А., Лысенко Э. В., Мокляк Н. Г., Скибенко И. Т. Перечисление типов недоопределенных булевых функций // В сб. «Автоматизир. сист. упр. и приборы автоматики. Респ. межведомств. тематич. сб.». — 1974. — № 31. — С. 59–65.
20. Применко Э. А. О числе типов обратимых преобразований в многозначных логиках // Кибернетика. — 1977. — № 5. — С. 27–29.
21. Применко Э. А. О числе типов обратимых булевых функций // Автоматика и вычислительная техника. — 1977. — № 6. — С. 12–14.
22. Сагалович Ю. Л. О групповой инвариантности булевых функций // Успехи математических наук. — 1959. — Т. 14. — № 6. — С. 191–195.
23. Сагалович Ю. Л. О числе типов симметрии контактых $(1, k)$-полюсников // Проблемы передачи информации. — 1960. — Вып. 8. — С. 82–96.
24. Семенов А. С., Черемушкин А. В. Классификация функций степени нелинейности не выше трех от шести переменных // Вопросы радиоэлектроники. Серия ЭВТ. — 1988. — Вып. 11. — С. 132–140.
25. Симонян Л. Об однотипности булевых функций // Уч. зап. Латв. ун-т. — 1963. — Т. 47. — С. 267–279.
26. Страздинь И. Э. О числе типов l-ичных функций // Уч. зап. Рижск. политехн. ун-т. — 1963. — Т. 10. — С. 167–186.
27. Страздинь И. Э. Типы троичных переключательных функций двух переменных // Уч. зап. Латв. ун-т. — 1964. — Т. 58.
28. Страздинь И. Э. Группа самодвойственных преобразований булевых фунций // В сб. Теория дискретных автоматов. — Рига: Зинатне. — 1967. — С. 191–199.
29. Страздинь И. Э. Группы инерции булевых фукнций четырех переменных // Автоматика и вычислительная техника. — 1968. — № 5. — С. 18–22.
30. Страздинь И. Э. Таблицы типов булевых функций четырех переменных // Деп. в редкол. журн. Автоматика и вычислительная техника., № 1495-Деп. — 1974. — 68 с.

31. Страздинь И. Э., Страздиня Д. П. О возможности укрупнения гарвардской классификации булевых функций // В сб.: Теория конечных автоматов и ее приложения. — Рига: Зинатне. — 1973. — Вып. 2. — С .24–40.
32. Страздинь И. Э. Линейная самодвойственная группа над $GF(2)$ и ее действие на алгебру булевых функций // Кибернетика. — 1974. — 5. — С. 146–147.
33. Страздинь И. Э. Аффинная классификация булевых функций пяти переменных // Автоматика и вычислительная техника. — 1975. — № 1. — С. 1–9.
34. Страздинь И. Э. Групповая инвариантность в конечнозначной логике. — Дисс. ...доктора физ.-мат. наук. — Рига, 1988.
35. Черемушкин А. В. Кубические формы от семи переменных // 4 межгосуд. семинар по дискретной математике и ее прилож. 2–4 февраля 1993 г.: Сб. трудов / Под ред. О. Б. Лупанова. — М.: Изд-во механико-матем.ф-та МГУ, 1998. — С. 145.
36. Черемушкин А. В. Классификация двоичных функций от шести переменных // 4 межгосуд. семинар по дискретной математике и ее приложениям, 2–4 февраля 1993 г.: Сб. трудов / Под ред. О. Б. Лупанова. — М.: Изд-во механико-матем. ф-та МГУ, 1998. — С. 143–144.
37. Черемушкин А. В. Кубические формы от восьми переменных // Проблемы теоретической кибернетики. Тез. докл. XII Международной конференции (Нижний Новгород, 17–22 мая 1999 г.). Часть II. — М.: МГУ. — 1999. — С. 245.
38. Черемушкин А. В. Методы аффинной и линейной классификации двоичных функций // Труды по дискретной математике. Т. 4. — М.: Физико-математическая литература. — 2001. — С. 273–314.
39. Черемушкин А. В. Однозначность разложения двоичной функции в бесповторное произведение нелинейных неприводимых сомножителей // Вестник Московского государственного университета леса — Лесной вестник. — 2004. — № 4(35). — С. 86–190.
40. Черемушкин А. В. Проблемы декомпозиции и линейной классификации дискретных функций // Дискретные модели в теории управляющих систем: VI Международная конференция: Москва, 7–11 декабря 2004 г./ Ред. кол. В. Б. Алексеев, В. А. Захаров, Д. С. Романов. — М.: Изд. отдел факультета ВМиК МГУ им. М. В. Ломоносова (лицензия ИД № 05899 от 24.09.2001 г.), 2004. — С. 88–92. С. 273–314.
41. Черемушкин А. В. Декомпозиция и классификация дискретных функций. — М.: ТВП — ОППМ, 2005.
42. Шеннон К. Синтез двухполюсных переключательных схем // Работы по теории информации и кибернетике. — М.: ИЛ, 1963. — С. 59–105.
43. Яблонский С. В. Функциональные построения в k-значной логике. — Тр. матем. ин-та им. Стеклова. — Т. 51. — 1958.
44. Ashenhurst R. L. The application of counting techniques // Proc. ACM, Pitsburg Meeting. — 1952. — P. 293–305.
45. Berlekamp E. R., Welch L. R. Weight distributions of the cosets of the (32; 6) Reed-Muller Code // IEEE Trans. Inform. Theory. — January 1972. — IT-18. — № 1. — P. 203–207.
46. Biryukov A., De Canni‘ere C., Braeken A., Preneel B. A toolbox for cryptanalysis: linear and affine equivalence algorithms // EUROCRYPT'03. — LNCS 2656. — P. 33–50.
47. Braeken A., Borissov Y., Nikova S., Preneel B. Classification of Boolean functions of 6 variables or less with respect to cryptographic properties // url: http://www.iacr.org.
48. Brian M. Permutation groups containing affine groups of the same degree // J. London Math. Soc. — 1977. — Vol. 15. — № 3. — P. 445–455.
49. Brier R., Langevin P. Classification of Boolean cubic forms of nine variables // 2003 Information Theory Workshop (ITW 2003). — IEEE Press, 2003. — P. 179–182.
50. deBruijn N. G. Generalization of Pólia's fundamental theorem in enumerative combinatorial analysis // Nederl. Acad. Wetensch. Proc., Ser A. — V. 62. — Indag. Math. — 1959. — 21. — P. 59–69.
51. Denev J. D., Tonchev V. D. On the number of equivalence classes of Boolean functions under a transfoimation group // IEEE Trans. Inform. Theory. — 1980. — IT-26. — № 5. — P. 625–626.
52. Dixon L. E. Linear groups with exposition Galois field theory. — Leipzig, 1901. /2nd ed. — Dover Publications, New York, 1958.
53. Dobbertin H., Leander G. Cryptographer's toolkit for construction of 8-bit bent functions // url: http://eprint.iacr.org/2005/089.
54. Fendel D. The number of classes of linerly equivalent functions // J. Cominatorial. Theory. — 1967. — 3. — P. 48–53.
55. Fuller J., Millan W. On Linear Redundancy in the AES S-Box // FSE 2003. — LNCS 2887. — Springer-Verlag. — P. 249–266.
56. Golomb S. W. On the classification of Boolean functions // IRE Trans. Circuit Theory. — 1959. — CT-6. — Spec. Suppl. — P. 176–186.
57. Harrison M. A. On the number of classes of invertible Boolean functions // J. Soc. for Indust. and Appl. Math. — 1963. — V. 10. — № 1. — P. 25–28.

58. Harrison M. A. On the number of transitivity sets of Boolean functions // J. Soc. for Indust. and Appl. Math. — 1963. — V. 11. — № 3. — P. 806–828.
59. Harrison M. A. On the number of classes of (n, k)-switching networks // J. Frankl. Inst. — 1963. — № 4. — P. 313–327.
60. Harrison M. A. The number of equivalence classes of Boolean functions under groups containing negation // IEEE Trans. Electr. Comput. — 1963. — EC-12. — № 5. — P. 559–561.
61. Harrison M. A. On the classification of Boolean function by the general linear and affine groups // J. Soc. for Indust. and Appl. Math. — 1964. — V. 12. — № 2. — P. 285–299.
62. Harrison M. A. Sur la classification des fonctioms logiques á plusieurs valeurs. — Bull. Math. Soc. Sci. Math. de la R.S. de Roumantic. — 1969. — B (61). — № 1. — P. 41–54.
63. Harrison M. A. Counting theorems and their applications to classifications of switching functions // in A. Mukhopadhyay ed. Recent developments in switching theory. — Academic Press: New York, Lodon, 1971. — P. 85–120.
64. Harvard Computation Laboratory Staff, Synthesis of electronic computing and control circuits. — Cambridge, Mass.: Harvard Univ. Press, 1951. (Русский перевод: Синтез электронных вычислителных и управляющих схем. — М.: ИЛ, 1954.)
65. Hou X. Classification of cosets of the Reed-Muller code R(m-3,m) // Discrete Math. — V. 128. — 1994. — P. 203–224.
66. Hou X. AGL(m,2) Acting on $R(r, m)/R(s, m)$ // J. of Algebra. — 1995. — V. 171. — № 3. — P. 921–938.
67. Hou X. $GL(m, 2)$ Acting on $R(r, m)/R(r-1, m)$ // Discrete Math. — V. 149. — 1996. — P. 99–122.
68. Hou X. $GL(m, 2)$ Cubic bent functions // Discrete Math. — V. 189. — 1998. — P. 149–161.
69. Kantor W. M, McDough T. P. On the maximality of $PSL(d+1, q)$, $d \geqslant 2$ // J. London Math. Soc. — V. 8. — № 3. — P. 426.
70. Lechner R. J. Affine equivalence of switching functions. — Ph.D.Dissertation, Harvard Univ., Cambridge. Mass., January 1963. / Submited to Bell Telephone Labs. as "Theory of switching" Harvard Computation Labs., Cambridge. Mass., Rept BL-33.
71. Lechner R. J. A transform approach to login design // IEEE Trans. Computers. — 1970. — C-19. — № 7. — P. 627–640.
72. List R. On permutation groups containing containing $PSL_n(q)$ as a subgroup // Geom. Dedic. — 1975. — V. 4. — № 2–4. — P. 373–375.
73. Maiorana J. A. A Classification of the Cosets of the Reed-Muller code $R(1, 6)$ // Mathematics of Computation. — July 1991. — V. 57. — № 195. — P. 403–414.
74. Masaki S., Yoshiyuki I., Noburu T., Tadao K. Weight distribution of (128, 64)–Reed–Muller Code // IEEE Trans. Inform. Theory. — IT-17. — Sept., 1971. — P. 627–628.
75. Meng Qing-shu, Yang min, Zhang huan-guo and Liu yu-zhen. Analysis of affinely equivalent Boolean functions // url: http://eprint.iacr.org/2005/025.
76. Ninomia I. A study of the structures of boolean functions and its application to the synthesis of switching circuits // Mem. Fac. Eng., Nagoya Univ. — 1961. — V. 13. — № 2. — P. 149–363.
77. Ninomia I. A study of the structures of boolean functions and its application to the synthesis of switching circuits. — Ph. D. diss. Nagoya Univ., Nagoya, Japan. — 1958. // Publ. in Mem. Fac. Eng., Nagoya Univ. — 1961. — V. 13. — № . 2. // IEEE Trans. Electronic Computers. — 1963. — EC-12. — P. 152.
78. Pólia G. Kombinatorische Anzahlbestimmungen fur Gruppen, Graphen, und chemische Verbindungen // Acta Math. — 1937. — 68. — P. 145–253. / русск. перев. Пойа Д. Комбинаторные вычисления для групп, графов и химических соединений // в сб. «Перечислительные задачи комбинаторного анализа». Под. ред. Г. П. Гаврилова. — М.: Мир, 1979. — С. 36–138.
79. Pólia G. Sur les types des propositions composees // J. Symb. Logic. — 1937. — 5. — P. 98–103.
80. Rothaus O. S. On «bent» functions // J. Combin. Theory. — 1976. — 20A. — P. 300–306.
81. Sugita T., Kasami T., Fujiwara T. Weight distributions of the third and fifth order Reed-Muller codes of length 512. — Nara Inst. Sci. Tech. Report, Feb. 1996.
82. Slepian D. On the number of symmetry types of Boolean functions of n variables // Canad. J. Math. — 1953. — V. 5. — № 2. — P. 185–193.
83. Stone H. J., Jackson C. L. Structures of the affine families of switching functions // IEEE Trans. on Comput. — 1969. — C-18. — № 3. — P. 251–257.

Поступило в редакцию 17 VII 2005