АНАЛИЗ КОРРЕКТИРУЮЩЕЙ СПОСОБНОСТИ ФУНКЦИЙ АЛГЕБРЫ ЛОГИКИ.

М.Г.Карповский, Э.С. Москалев, А.А. Трояновский.

Описываются методы анализа корректирующей способности $b_e^{(\rho)}$ функций алгебры логики (ФАЛ). Показано, что свойство ФАЛ корректировать ошибки заданной кратности может сохраняться даже для минимальных представлений ФАЛ. Для оценки $b_e^{(\rho)}$ на множестве арифметических и неарифметических ошибок используется аппарат дискретных функциональных преобразований.

Рассматриваются некоторые классы булевых функций с точки зрения их корректирующей способности к ошибкам заданной кратности.

Пусть задана система полностью определенных функций алгебры ρ-значной логики (ФАЛ)

$$y^{(j)} = f^{(j)}(x^{(0)}, x^{(1)}, \dots, x^{(k-1)}) \qquad (1)$$

где $(x^{(0)}, x^{(1)}, \dots, x^{(k-1)}) \in X = \{0, 1, \dots, \rho-1\}^k$

$(j = 0, 1, \dots, z-1)$

Под ошибкой для системы ФАЛ будем понимать упорядоченную пару $(x, x') \in X^2$ Система ФАЛ исправляет множество ошибок R, если и только если для любых $(x, x') \in R$ $(R \subseteq X^2)$

$$f^{(j)}(x) = f^{(j)}(x') \quad (j = 0, 1, \dots, z-1) \qquad (2)$$

В дальнейшем ошибку (x, x') будем обозначать $x \ominus x' \pmod{\rho}$ символ $\ominus$ и запись $(\mathrm{mod}\,\rho)$ справа от соответствующего выражения означает операцию покомпонентного вычитания векторов по модулю ρ. Под ошибкой кратности ℓ будем понимать ошибку для которой $\|x \ominus x'\|_\rho = \ell \pmod{\rho}$. Здесь $\|a\|_\rho$ – число ненулевых компонент в ρ-ичном векторе a. Следовательно, множество ошибок R определяется так:

$$R \subseteq \{(x, x') = \gamma \mid \gamma \in \{0, 1, \dots, \rho-1\}^k; \|\gamma\|_\rho = \ell\} \qquad (3)$$

Число исправляемых системой ФАЛ ошибок из множества R обозначим $b_R^{(\rho)}(f)$ и назовем корректирующей способностью системы ФАЛ на множестве ошибок R. Корректирующую способность на множестве всех ошибок кратности ℓ обозначим $b_\ell^{(\rho)}(f)$.

Решетчатую функцию $\tilde{y} = f(\tilde{x})$, представляющую систему (1) построим следующим образом:

$$\tilde{x} = \sum_{j=0}^{k-1} x^{(j)} \rho^{k-j-1} \qquad (4)$$

$$\tilde{y} = \sum_{j=0}^{z-1} y^{(j)} \rho^{z-j-1} \qquad (5)$$

Для решетчатой функции $\tilde{y} = f(\tilde{x})$ построим систему характеристических функций $\{f_i(x)\}$:

$$f_i(x) = \begin{cases} 1 & \text{при } f(\tilde{x}) = i \quad (i = 0, 1, \dots, \rho^z - 1) \\ 0 & \text{в остальных случаях} \end{cases} \qquad (6)$$

Теорема I

$$P_R^{(p)}(f)=\sum_{\gamma\in R}\sum_{i=0}^{p^k-1}B_{p,i}(\gamma) \qquad (7)$$

где

$$B_{p,i}(\gamma)=\sum_{x=0}^{p^k-1}f_i(x)f_i(x\ominus\gamma) \quad (\mathrm{mod}\,p) \qquad (8)$$

функцию $B_{p,i}(\gamma)$ назовем автокорреляционной по модулю p функцией характеристической функции f_i

Таблица I

$\tilde{x},\tilde{f}$	$x^{(0)}$	$x^{(1)}$	$f(\tilde{x})$	$f_0(x)$	$f_1(x)$	$f_2(x)$	$B_{3,1}(\gamma)$	$B_{3,2}(\gamma)$	$\sum_{i=0}^{2}B_{3,i}(\gamma)$
0	0	0	I	0	I	0	5	4	9
I	0	I	2	0	0	I	2	I	3
2	0	2	I	0	I	0	2	I	3
3	I	0	I	0	I	0	4	3	7
4	I	I	2	0	0	I	2	I	3
5	I	2	2	0	0	I	2	I	3
6	2	0	I	0	I	0	4	3	7
7	2	I	2	0	0	I	2	I	3
8	2	2	I	0	I	0	2	I	3

Пример. В таблице I приведена одна функция $f(x)$ троичной логики от двух аргументов ($p=3$, k 2, $r=1$), характеристические функции f_0, f_1, f_2 автокорреляционные функции по модулю 3 $B_{1,3}, B_{2,3}$ ($B_{0,3}\equiv 0$) и их суммы.

Из таблицы I имеем $P_1^{(3)}(f)=20$; $P_2^{(3)}(f)=12$.

Теорема 2

$$B_{p,i}(\gamma)=B_{p,i}(\sigma\ominus\gamma) \quad (\mathrm{mod}\,p) \qquad (9)$$

Соотношение (9) позволяет иное сократить объем вычислений при нахождении $P_e^{(p)}(f)$

Известно, что автокорреляционная функция $B_{p,i}(\gamma)$ связана с самой функцией f_i через двойное спектральное преобразова-

ние Крестенсона $\mathcal{S}^{(p)}$ [I].

$$B_{p,i}(\gamma)=p^{2k}\left(\mathcal{S}^{(p)}\right)^{-1}\left(\mathcal{S}^{(p)}(f_i)\overline{\mathcal{S}^{(p)}(f_i)}\right)(\gamma) \qquad (10)$$

где $\left(\mathcal{S}^{(p)}\right)^{-1}$ и $\overline{\mathcal{S}^{(p)}}$ – преобразования обратные и комплексно сопряженные $\mathcal{S}^{(p)}$, соответственно. Соотношение (10) дает возможность вычисления $P_e^{(p)}$, с помощью повторного применения "быстрого" преобразования Адамара-Крестенсона [1].

Укажем теперь на одно важное свойство $P_e^{(p)}(f)$

Теорема 3 Пусть заданы четыре системы $f_1(x), f_2(x), f_3(x), f_4(x)$ ФАЛ, причем $x\in\{0,1,\dots,p-1\}^k$; $f_1(x), f_2(x), f_3(x), f_4(x)\in\{0,1,\dots,p-1\}^n$, и

$$f_2(x)=f_1(x\oplus\alpha) \quad (\mathrm{mod}\,p) \quad (\alpha\in\{0,1,\dots,p-1\}^n) \qquad (11)$$

$$f_3(x)=f_1(\sigma x) \qquad (12)$$

$$f_4(x)=f_1(x)\oplus\beta \quad (\mathrm{mod}\,p) \quad (\beta\in\{0,1,\dots,p-1\}^n) \qquad (13)$$

где σ –какая-то перестановка $(x^{(0)}, x^{(1)},\dots, x^{(k-1)})$

Тогда для любого $1\le e\le k$

$$P_e^{(p)}(f_1)=P_e^{(p)}(f_2)=P_e^{(p)}(f_3)=P_e^{(p)}(f_4) \qquad (14)$$

Рассмотрим случай, когда класс R состоит из арифметических ошибок кратности e. Арифметической ошибкой кратности будем называть пару (x,x'), такую, что

$$\|x-x'\|_p^{(A)}=e \qquad (15)$$

Где $\|x-x'\|_p^{(A)}$ – минимальное число ненулевых слагаемых при представлении величины $|x-x'|$ в виде арифметической суммы слагаемых вида $a_j p^j$ $(a_j\in\{0,1,\dots,p-1\})$

Корректирующую способность системы ФАЛ для e-кратных арифметических ошибок обозначим $\mathcal{F}_e^{(p)}(f)$. Легко показать, что для случая арифметических ошибок справедливы все ранее приведенные соотношения (3) – (10), только операция $\Theta\,(\mathrm{mod}\,p)$ заменяется операцией $\Theta\,(\mathrm{mod}\,p^k)$. Автокорреляционная функция $B_{p^k,i}(\gamma)$ также связана с функцией $f_i(x)$ двойным дискретным преобразова-

при этом следует лишь бесконечно периодически продолжить $f_i(x)$ по оси x ; эта связь имеет тот же вид, что и (I0).

В отличие от $b_e^{(\rho)}(f)$, $\Sigma_e^{(\rho)}(f)$ не инвариантна к перестановке аргументов. По отношению же к сдвигу справедливо следующее утверждение

Теорема 4 Пусть $f_1(x), f_2(x), f_3(x)$ - три системы функций ρ -значной логики от K аргументов и для любого $x \in \{0,1,\dots,\rho-1\}^K$

$$f_2(x) = f_1(x \oplus \alpha) \pmod{\rho^K} \quad (\alpha \in \{0,1,\dots,\rho-1\}^K) \quad (16)$$

$$f_3(x) = f_1(x) \oplus \beta \pmod{\rho} \quad (\beta \in \{0,1,\dots,\rho-1\}) \quad (17)$$

тогда для любого $1 \le e \le K$

$$\Sigma_e^{(\rho)}(f_1) = \Sigma_e^{(\rho)}(f_2) = \Sigma_e^{(\rho)}(f_3) \quad (18)$$

Учитывая практическую важность, остановимся подробнее на случае, когда система ФАЛ, определяемая (I) является системой булевых функций БФ $(\rho=2)$ и рассмотрим свойства $b_e^{(2)}(f)$ для некоторых классов БФ.

Отметим, что из (I4) следует инвариантность $b_e^{(2)}(f)$ к инверсии и перестановке аргументов БФ, а также к инверсии отдельных функций системы; Соотношение (I0) при $\rho=2$ приводится к виду

$$B_{2,i}(f) = 2^{2K} W(W^2(f_i))(f) \quad (19)$$

где W - спектральное преобразование Уолша [1] .

Теорема 5 Пусть $f(x)$ -линейная БФ, т.е.

$$f(x) = \bigoplus_{i=0}^{K-1} a_i x^{(i)} \pmod 2 \quad (a_i, x^{(i)} \in \{0,1\}) \quad (20)$$

тогда для любого $1 \le e \le k$

$$b_e^{(2)}(f) = \sum_{j=0}^{[e/2]} C_{K-\|a\|}^{e-2j} \cdot C_{\|a\|}^{2j} \cdot 2^K \quad (21)$$

где $C_d^b = 0$ при $b > d$; $\|a\| = \sum_{j=0}^{K-1} a_j$; $[e/2]$ -ближайшее целое, не $e/2$ число.

Следствие, из теоремы 5 следует, что в линейной БФ все ошибки четной кратности.

Теорема 6 $f(x)$ $(x \in \{0,1\}^K)$ - самодвойственная (антисамодвойственная) БФ, тогда и только тогда, если

$$b_K^{(2)}(f) = 0 \; ; \quad (b_K^{(2)}(f) = 2^K) \quad (22)$$

Теорема 7 Пусть $f(x)$ -положительная (отрицательная) БФ от K аргументов. Тогда

$$b_e^{(2)} \ge 2 \sum_{x: f(x)=1} C_{K-\|x\|}^{e} + 2 \sum_{x: f(x)=0} C_{\|x\|}^{e} \quad (23)$$

$$\left(b_e^{(2)} \ge 2 \sum_{x: f(x)=0} C_{K-\|x\|}^{e} + 2 \sum_{x: f(x)=1} C_{\|x\|}^{e} \right) \quad (24)$$

Рассмотрим теперь вопрос о БФ, имеющих заданную мощность, т.е. величину $\sum_{x=0}^{2^K-1} f(x)$ и обладающих максимальной корректирующей способностью. Обозначим $b^{(2)}(f)$ -общее число ошибок всех кратностей выше нуля, исправляемых функцией $f(x)$

$$b^{(2)}(f) = \sum_{e=1}^{K} b_e^{(2)}(f) \quad (25)$$

Теорема 8 Для БФ $f(x)$, имеющей мощность $\|f(x)\|$

$$b^{(2)}(f) = 2^{2K} - 2^K + 2\|f(x)\|^2 - 2^{K+1}\|f(x)\| \quad (26)$$

Из теремы 9 следует, что все БФ от K аргументов, заданной мощности исправляют одно и то же общее число ошибок $b^{(2)}(f)$. Однако, при фиксированной мощности, корректирующая способность одних функций сконцентрирована в области ошибок малой кратности, а других - в области ошибок высокой кратности.

Рассмотрим, например, отрицательные функции $\{R_T(x)\}$

$$R_T(x) = \begin{cases} 1 & \text{при } x \le T \\ 0 & \text{при } x > T \end{cases} \quad (x \in \{0,1\}^K) \quad (27)$$

Теорема 9

$$b_e^{(2)}(R_T) \le \sum_{j=0}^{e} C_t^j C_{K-t}^{e-j} (2^K - 2^j) + C_t^e \cdot 2^e \quad (28)$$

(здесь $t =]\log_2(T+1)[$ где $]a[$ означает округление до ближайшего, не меньшего a целого числа

$$b_e^{(2)}(R_T) = 2 \sum_{x=0}^{T} \sum_{j=0}^{K-1} x^{(j)} C_j^{e-1} + 2 \sum_{x=T+1}^{2^K-1} \overline{x^{(j)}} \cdot C_j^{e-1} \quad (29)$$

где $x^{(j)} \in \{0,1\}$; $\overline{x^{(j)}} = 1 - x^{(j)}$

Граница, определяемая (28) достигается, если мощность $\|f(x)\|$ является степенью двойки.

Из теорем 7 и 9 следует, что функции $R_T(x)$ обладают высокой корректирующей способностью в области ошибок малой кратности.

Выводы:

1. Способность системы ФАЛ корректировать ошибки заданного класса определяется особенностями функций, входящих в систему, и даже при минимальном представлении ФАЛ эта способность может сохраняться.

2. Автокорреляционные по модулю p функции определяют удобный и естественный способ анализа корректирующей способности систем ФАЛ. Связь автокорреляционных функций с исходной функцией через двойной спектральное преобразование определяет простой "машинный" способ их вычисления с помощью повторного использования быстрого преобразования Адамара-Крестенсона (Уолша - при $p=2$)

3. При синтезе комбинационных схем реализующих систему ЕФ, целесообразно использовать представления отдельных функций системы в виде суперпозиции монотонных /положительных или отрицательных/ функций. Такого рода представлениям соответствуют например, реализации систем ЕФ на пороговых элементах и, в частности, на пороговых элементах с весами $\{2^0, 2^1, \ldots, 2^{k-1}\}$

4. При необходимости коррекции ошибок в схеме, реализующей систему булевых функций, ошибок кратности K (где K - число аргументов системы) целесообразно строить схему в соответствии с представлением отдельных функций системы в виде суперпозиции антисамодвойственных функций.

Литература

1. Трахтман А.М. Введение в обобщенную спектральную теорию сигналов. Изд."Сов. Радио", М., 1972.

АНАЛИЗ КОРРЕКТИРУЮЩЕЙ СПОСОБНОСТИ АВТОМАТОВ

М.Г.Карповский, А.А.Трояновский

Описываются методы анализа корректирующей способности $R_K(f)$ абстрактных автоматов и автоматов с произвольными структурными алфавитами. Показано, что способность автоматов корректировать ошибки заданного класса K определяется свойствами реализуемого ими отображения f и может сохраняться даже для минимальных автоматов.

Рассмотрены способы оценки $R_K(f)$ при разных способах задания автоматов и для различных классов ошибок K. В частности, если множество слов алфавита образует коммутативную группу G_m и класс ошибок на G_m описывается в терминах групповой операции /например, ошибки заданной кратности/, то для оценки $R_K(f)$ используются корреляционные функции. Связь корреляционных функций с исходными через двойное дискретное спектральное преобразование позволяет использовать для оценки $R_K(f)$ аппарат спектральных преобразований.