УДК 681.3+681.5:007

ПРИМЕРЫ ПОСТРОЕНИЯ ПОМЕХОУСТОЙЧИВЫХ К НЕСИММЕТРИЧНЫМ РЕГУЛЯРНЫМ ПОМЕХАМ АЛГОРИТМОВ ПОИСКА ТОЧКИ С ХАРАКТЕРНЫМ ПРИЗНАКОМ

АЛИПОВ Н.В., АЛИПОВ И.Н., ОХАПКИН А.А., РЕБЕЗЮК Л.Н.

Строятся алгоритмы помехоустойчивого поиска точки экстремума унимодальной функции в условиях несимметричного регулярного воздействия, определяющие функционирование дискретных автоматов систем защиты информации.

Рассмотрим построение таких алгоритмов для случая $h = l = \Delta t$. Его необходимо начинать с $i = 1$, затем для $i = 2,3$ и т.д.

Пусть $k = 1$, $a = 4h$ (h - дискретность преобразования). Тогда, как это следует из соотношения (7) в работе [1], имеют место соотношения

$$\Psi^{4,1,1}(0,1) = 1; \quad \Psi^{4,1,1}(1,1) = 1.$$

Для $i = 2$ (см. соотношение (8) в работе [1]) соответственно имеем

$$\Psi^{4,1,1}(2,1) = 2.$$

Алгоритм заключается в следующем:

1-й шаг: положить $x_1^1 = h$;

2-й шаг: положить $x_1^2 = x_1^1 = h$.

Если при этом на этих шагах имеют место соотношения

$$x(t_1) \in \left[0, x_1^1\right); \quad x(t_1 + \Delta t) \in \left[x_1^1, 1\right),$$

либо соотношения

$$x(t_1) \in \left[x_1^1, 1\right); \quad x(t_1 + \Delta t) \in \left[0, x_1^1\right),$$

то

$$x \in \left[0, x_1^1\right);$$

если

$$x(t_1) \in \left[x_1^1, 1\right]; \quad x(t_1 + \Delta t) \in \left[x_1^1, 1\right),$$

то

$$x \in \left[x_1^1, 1\right).$$

Пусть $i = 3$. Тогда в результате совершения первого шага алгоритма могут возникнуть исходы:

а) $x(t_1) \in \left[0, x_1^1\right)$; b) $x(t_1) \in \left[x_1^1, 1\right)$.

Для первого исхода, как известно, на отрезке $\left[0, x_1^1\right]$ действует оптимальный $(i-1)$-шаговый алгоритм, который нами уже построен. Этот алгоритм разобьет отрезок $\left[0, x_1^1\right)$ на две равные части. Поэтому для исхода а) длина отрезка $\left[0, x_1^1\right)$ равна двум h, т.е.

$$L\left(\left[0, x_1^1\right]\right) = 2h. \qquad (1)$$

Для исхода b) на втором шаге эксперимент повторяем: $x_1^2 = x_1^1$. При этом могут возникнуть исходы:

$$b_1) \ x(t_1 + \Delta t) \in \left[0, x_1^2\right); \quad b_2) \ x(t_1 + \Delta t) \in \left[x_1^2, 1\right).$$

Для исхода b_1) характерно то, что проявление помехи обнаружено – она действовала на первом шаге алгоритма. Поскольку, по условию, она же будет проявляться и на третьем шаге алгоритма, то на отрезке $\left[0, x_1^1\right]$ действует помехоустойчивый $(i-2)$-шаговый алгоритм, который разобьет его на $\Psi_{1,8}^{4,1,1}(1,1)$ равных частей. При таком сочетании исходов

$$x_1^1 = x_1^2 = h\Psi_{1,8}^{4,1,1}(1,1) = h. \qquad (2)$$

Исходя из минимаксного критерия для x_1^1, из двух его значений (см. (1) и (2)) необходимо выбрать минимальное:

$$x_1^1 = h \min\left\{\Psi^{4,1,1}(2,1), \Psi^{4,1,1}(1,1)\right\} = h. \qquad (3)$$

Если возникает исход b_2), то на отрезке $\left[x_1^2, 1\right]$ действует одношаговый помехоустойчивый алгоритм. По этой причине

$$L\left(\left[x_1^2, 1\right]\right) = h. \qquad (4)$$

Из соотношений (3) и (4) получаем

$$\Psi_{1,8}^{4,1,1}(3,1) = 2\Psi_{1,8}^{4,1,1}(1,1) = 2. \qquad (5)$$

Пусть $i = 4$. Тогда после совершения первого шага возникают такие же исходы, как и для $i = 3$: а) и b).

Для исхода а) имеет место соотношение (1):

$$x_1^1 = h\Psi_{1,8}^{4,1,1}(3,1) = 2h. \qquad (6)$$

Для исхода b) выполняется второй шаг, для которого $x_1^2 = x_1^1$. При этом также может возникнуть один из исходов – b_1) или b_2).

Для исхода b_1), как это было доказано (см. (3) в работе [1]), имеет место соотношение

$$L\left(\left[0, x_1^1\right]\right) = h\varphi_2(\alpha_1, k) = 2h. \qquad (7)$$

Для исхода b_2) на отрезке $\left[x_1^2, 1\right]$ действует (см. (1) в работе [1]) помехоустойчивый $(i-2)$-шаговый алгоритм, который разбивает этот отрезок на $\Psi_{1,8}^{4,1,1}(2,1)$ равные части. На этом основа-нии устанавливаем

$$\Psi_{1,8}^{4,1,1}(4,1) = \min\left\{\Psi_{1,8}^{4,1,1}(3,1), \varphi_2(\alpha_1, 1)\right\} + \Psi_{1,8}^{4,1,1}(2,1) = 4. \qquad (8)$$

Пусть $i = 5$. Тогда по аналогии, если после первого шага возникает исход а), то на отрезке $\left[0, x_1^1\right]$ приме-

няется помехоустойчивый $(i-1)$-шаговый алгоритм. На этом основании получаем

$$x_1^1 = h\Psi_{1,8}^{4,1,1}(i-1,1) = h\Psi_{1,8}^{4,1,1}(4,1) = 4h\,. \qquad (9)$$

Для исхода b) выполняется второй шаг известным способом – $x_1^2 = x_1^1$.

При этом, если возникает исход b_1), то по аналогии с ранее рассмотренными алгоритмами устанавливаем

$$x_1^2 = h\varphi_2(\alpha_1,1) = 2h\,. \qquad (10)$$

Если же после второго шага возникает исход b_2), то отрезок $\left[x_1^2,1\right]$ будет разбит $(i-2)$-шаговым алгоритмом на $\Psi_{1,8}^{4,1,1}(3,1)$ равные части:

$$L\left(\left[x_1^2,1\right]\right) = h\Psi_{1,8}^{4,1,1}(3,1) = 2h\,. \qquad (11)$$

На основании соотношений (9)-(11) устанавливаем:

$$\Psi_{1,8}^{4,1,1}(5,1) = \min\left\{\Psi_{1,8}^{4,1,1}(4,1),\varphi_2(\alpha_1,1)\right\} + \Psi_{1,8}^{4,1,1}(3,1) = 4\,.$$

Пусть $i=6$. Тогда соответственно (см. приведенную схему анализа исходов) будем иметь:

$$\Psi_{1,8}^{4,1,1}(6,1) = \min\left\{\Psi_{1,8}^{4,1,1}(5,1),\varphi_2(\alpha_1,1)\right\} + \\ + \Psi_{1,8}^{4,1,1}(4,1) = \min\{4,4\} + 4 = 8\,.$$

Для $i=7$ будут справедливы такие соотношения:

$$\Psi_{1,8}^{4,1,1}(6,1) = 8;\ x_1^{1,1} > 0;\ L\left(\left[x_1^{1,1},x_1^1\right]\right) = 4h;$$

$$\varphi_2(\alpha,1) = 4;\ \Psi_{1,8}^{4,1,1}(5,1) = 4\,.$$

Поскольку амплитуда помехи равна $4h$ и непомехоустойчивый алгоритм разбивает отрезок $\left[x_1^{1,1},x_1^1\right]$ на четыре равные части (независимо от исхода реализуется одна и та же точность разбиения на всем отрезке $\left[0,x_1^1\right]$), будем иметь

$$\Psi_{1,8}^{4,1,1}(7,1) = \Psi_{1,8}^{4,1,1}(6,1) + \Psi_{1,8}^{4,1,1}(5,1) = 12\,.$$

Можно показать, что для $i>7$ при $a=4h$ выполняется соотношение

$$\Psi_{1,8}^{4,1,1}(i,1) = \Psi_{1,8}^{4,1,1}(i-1,1) + \Psi_{1,8}^{4,1,1}(i-2,1)\,. \qquad (12)$$

На основании приведенных примеров построения помехоустойчивых алгоритмов получим следующий ряд значений функции $\Psi_{1,8}^{4,1,1}(i,1)$ (табл. 1).

Таблица 1

i	0	1	2	3	4	5	6	7	8	9	10	11	12
	1	1	2	2	4	4	8	12	20	32	52	84	136

Пусть $a=8$. Тогда для первых семи значений, начиная с $i=0$ и кончая $i=6$, значения $\Psi_{1,8}^{8,1,1}(i,1)$ равны соответствующим значениям $\Psi_{1,8}^{4,1,1}(i,1)$ (табл. 2).

Таблица 2

i	0	1	2	3	4	5	6
	1	1	2	2	4	4	8

Найдем значение этой функции для $i=7$. Пусть совершен первый шаг семишагового алгоритма и возник один из известных исходов – a) или b).

Тогда для исхода a) соответственно будем иметь

$$x_1^1 = h\Psi_{1,8}^{8,1,1}(6,1) = 8h\,. \qquad (13)$$

Для исхода b) второй шаг, как известно, заключается в том, что $x_1^2 = x_1^1$. При этом могут возникнуть известные нам исходы b_1) и b_2).

Для исхода b_1) на отрезке $\left[x_1^{1,1},x_1^1\right)$ действует непомехоустойчивый α_1-шаговый алгоритм, который разбивает его на $\varphi_1(\alpha_1,1)$ равные части. Поскольку $x_1^1 = 0$, то справедливо также и соотношение

$$x_1^2 = h\varphi_1(\alpha_1,1)\,,$$

где

$$\alpha_1 = \begin{cases} \dfrac{i-3}{2}, & \text{если } (i-3)\bmod 2 = 0; \\ \left]\dfrac{i-3}{2}\right[, & \text{если } (i-3)\bmod 2 \neq 0; \end{cases}$$

$$\varphi_1(\alpha_1,1) = 2^{\alpha_1}\,.$$

Для нашего примера имеем $\alpha_1 = \dfrac{7-3}{2} = 2$. Поэтому функция $\varphi_1(2,1)$ принимает значение $\varphi_1(2,1) = 4$.

Для исхода b_2) на отрезке $\left[x_1^2,1\right]$ действует помехоустойчивый $(i-2)$-шаговый алгоритм. Как известно, пятишаговый помехоустойчивый алгоритм разобьет отрезок $\left[x_1^2,1\right]$ на $\Psi_{1,8}^{8,1,1}(5,1)$ равных частей. С учетом этого анализа получаем

$$\Psi_{1,8}^{8,1,1}(7,1) = \min\left\{\Psi_{1,8}^{8,1,1}(6,1),\varphi_1(2,1)\right\} + \\ + \Psi_{1,8}^{8,1,1}(5,1) = 8\,.$$

Для других значений i при $a=8$ справедливо соотношение

$$\Psi_{1,8}^{8,1,1}(i,1) = \Psi_{1,8}^{8,1,1}(i-1,1) + \Psi_{1,8}^{8,1,1}(i-2,1)\,.$$

Значения этой функции приведены в табл. 3.

Таблица 3

i	0	1	2	3	4	5	6	7	8	9	10	11	12
	1	1	2	2	4	4	8	8	16	24	40	64	104

Анализ значений целевой функции в приведенных таблицах показывает, что если $ah = 2^j h$, то, начиная с $i=2$ до $i=\left(2(j+1)-1\right)$, справедливо соотношение

$$\Psi_{1,8}^{a,1,1}(i,1) = 2\Psi_{1,8}^{a,1,1}(i-2,1)\,,$$

затем – соотношение

$$\Psi_{1,8}^{a,1,1}(i,1) = \Psi_{1,8}^{a,1,1}(i-1,1) + \Psi_{1,8}^{a,1,1}(i-2,1). \quad (14)$$

Для предельного значения параметра a , равного диапазону изменения координаты точки с характерным признаком, показано, что

$$\Psi_{1,8}^{a,1,1}(i-1,1) \geq \varphi_1(\alpha_1,1). \quad (15)$$

По этой причине для таких условий значения функции $\Psi_{1,8}^{a,1,1}(i,1)$ образуют l-последовательность, для которой l=1, а для $\Psi_{1,8}^{a,1,1}(i,1)$ справедливо соотношение

$$\Psi_{1,8}^{a,1,1}(i,1) = 2\Psi_{1,8}^{a,1,1}(i-2,1). \quad (16)$$

В табл. 4 приведены значения функции $\Psi_{1,8}^{a,1,1}(i,1)$ при различных параметрах a и i .

Таблица 4

a \ i	0	1	2	3	4	5	6	7	8	9	10	11	12	13
4	1	1	2	2	4	4	8	12	20	32	52	84	136	-
8	1	1	2	2	4	4	8	8	16	24	40	64	104	-
16	1	1	2	2	4	4	8	8	16	16	32	48	80	-
32	1	1	2	2	4	4	8	8	16	16	32	32	64	96
	1	1	2	2	4	4	8	8	16	16	32	32	64	64

Рассмотрим принцип построения алгоритмов для другого характерного случая, когда $h > 1$.

Пусть $l = 1,\ h = 2,\ a = 4h$. Тогда, как было показано,

$$\Psi_{1,8}^{4,1,2}(0,1) = \Psi_{1,8}^{4,1,2}(1,2) = 1;\ \Psi_{1,8}^{4,1,2}(2,1) = 2.$$

Для $i = 3$ после первого шага:

если возникает исход a), будем иметь

$$x_1^1 = h\Psi_{1,8}^{4,1,2}(2,1) = 2h;$$

если возникает исход b), то на втором шаге при возникновении исхода c_1) для x_1^2 справедливо соотношение

$$x_1^2 = h\varphi_3(\alpha,\alpha_1,1) = 2h.$$

В случае возникновения исхода c_2) справедливо выражение

$$L\left(\left[x_1^2,1\right)\right) = h\Psi_{1,8}^{4,1,2}(i-2,1) = 2h.$$

С учетом полученных соотношений для x_1^2, x_1^1 и соотношения для длины отрезка $\left[x_1^2,\ 1\right]$ будет справедливо равенство

$$\Psi_{1,8}^{4,1,2}(3,1) = \min\left\{\varphi_3(\alpha,\alpha_1,1), \Psi_{1,8}^{4,1,2}(2,1)\right\} + \Psi_{1,8}^{4,1,2}(i-2,1) = 3.$$

Пусть $i = 4$. Тогда аналогичным образом можно показать, что

$$\Psi_{1,8}^{4,1,2}(3,1) = 3;\ \varphi_3(\alpha,\alpha_1,1) = 2;\ \Psi_{1,8}^{4,1,2}(2,1) = 2.$$

На этом основании устанавливаем

$$\Psi_{1,8}^{4,1,2}(4,1) = \min\left\{\Psi_{1,8}^{4,1,2}(3,1), \varphi_3(\alpha,\alpha_1,1)\right\} + \Psi_{1,8}^{4,1,2}(2,1) = 4.$$

Для последующих i справедливо выражение

$$\Psi_{1,8}^{4,1,2}(i,1) = \Psi_{1,8}^{4,1,2}(i-1,1) + \Psi_{1,8}^{4,1,2}(i-2,1).$$

Для $a = 8h$ будем соответственно иметь:

$$\Psi_{1,8}^{8,1,2}(0,1) = \Psi_{1,8}^{8,1,2}(1,1) = 1;$$

$$\Psi_{1,8}^{8,1,2}(2,1) = 2;\ \Psi_{1,8}^{8,1,2}(3,1) = 3;$$

$$\Psi_{1,8}^{8,1,2}(4,1) = 4.$$

Для всех $i > 4$ справедливо соотношение Фибоначчи:

$$\Psi_{1,8}^{8,1,2}(i,1) = \Psi_{1,8}^{8,1,2}(i-1,1) + \Psi_{1,8}^{8,1,2}(i-2,1).$$

Для $a = 16h$ будем иметь первоначальный ряд

1, 1, 2, 3, 4, 7, 11, 15,

затем для $i > 7$ будет справедливо соотношение Фибоначчи.

Показано, что если $a = 2^j h$, то начиная с $i = 2$ до $i = 2j-1$, для целевой функции справедливо соотношение

$$\Psi_{1,8}^{a,1,2}(i,1) = \min\left\{\Psi_{1,8}^{a,1,2}(i-1,1), \varphi_3(\alpha,\alpha_1,1)\right\} + \Psi_{1,8}^{a,1,2}(i-2,1),$$

а для всех других значений справедливо соотношение Фибоначчи.

В табл.5 приведены значения функции $\Psi_{1,8}^{a,1,2}(i,1)$ при различных параметрах a и i .

Таблица 5

a \ i	0	1	2	3	4	5	6	7	8	9	10	11
4	1	1	2	3	4	7	11	18	29	47	76	-
8	1	1	2	3	4	7	11	15	26	41	67	108
16	1	1	2	3	4	7	11	15	26	41	67	108

Анализ табл. 5 показывает, что, начиная с $a = 8h$, значения целевой функции не зависят от параметра a .

Рассмотрим еще один пример построения алгорит-ма поиска точки с характерным признаком, для которого $h > l$ и $l = 2,\ h = 3$.

Для $a = 4h$ с учетом соотношения (8) в работе [1] будем иметь

$$\Psi_{1,8}^{4,2,3}(0,1) = \Psi_{1,8}^{4,2,3}(1,1) = \Psi_{1,8}^{4,2,3}(2,1) = 1;\ \Psi_{1,8}^{4,2,3}(3,1) = 2.$$

Пусть $i = 4$. Тогда после первого шага алгоритма, как нам уже известно, на отрезке $\left[0, x_1^1\right]$ действует $(i-1)$-шаговый алгоритм поиска, который разобьет указанный отрезок на $\Psi_{1,8}^{4,2,3}(3,1)$ равные части. Наихудшим будет случай, когда в результате выполнения второго шага алгоритма возник исход c_2), затем на третьем шаге – исход c_1). При такой ситуации (см. соотношение (13)) отрезок $\left[0, x_1^1\right]$ будет разбит на $\varphi_5\left(\overline{\alpha}, \overline{\alpha_1}, 1\right)$ равных частей. Если же возникнет исход c_2), то отрезок $\left[x_1^2,1\right]$ разбиваем [1] на $\Psi_{1,8}^{4,2,3}(2,1)$ равных частей. На этом основании устанавливаем истинность соотношения

$$\Psi_{1,8}^{4,2,3}(4,1) = \min\left\{\Psi_{1,8}^{4,2,3}(3,1), \varphi_5\left(\overline{\alpha}, \overline{\alpha_1}, 1\right)\right\} +$$
$$+ \Psi_{1,8}^{4,2,3}(2,1) = 3 .$$

Нетрудно убедиться, что начиная с i = 3 для последующих i выполняется соотношение Фибоначчи.

Производя аналогичные преобразования, можно получить ряды целых положительных чисел, являющихся значением целевой функции для конкретных значений аргумента i .

В табл. 6 приведены значения функции $\Psi_{1,8}^{a,2,3}(i,1)$ при различных параметрах a и i .

Таблица 6

a \ i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
4	1	1	1	2	3	5	8	13	21	34	55	89	144	-	-	-	-
8	1	1	1	2	3	5	7	9	15	24	39	63	102	-	-	-	-
16	1	1	1	2	3	5	7	9	15	24	39	63	102	-	-	-	-
64	1	1	1	2	3	5	7	9	15	24	39	56	71	120	-	-	-
	1	1	1	2	3	5	7	9	15	24	39	56	71	120	191	311	447

Таким образом, на основании каждого полученного в этой работе ряда целых положительных чисел может быть построено избыточное представление десятичных чисел. Поскольку такие представления оригинальны, их можно использовать для защиты не стратегической информации.

Литература: 1. *Алипов Н.В., Алипов И.Н., Охапкин А.А., Ребезюк Л.Н.* Алгоритмы поиска точки с характерным признаком в условиях несимметричного регулярного воздействия // Радиоэлектроника и информатика. 1999. №2 С. 101-107.

Поступила в редколлегию 25.04.99

Рецензент: д-р техн. наук, проф. Руденко О.Г.

Алипов Николай Васильевич, д-р техн. наук, профессор кафедры конструирования электронно-вычислительных машин ХТУРЭ. Научные интересы: защита информации, алгоритмизация задач автоматизированного проектирования электронных вычислительных средств. Адрес: Украина, 310189, Харьков, ул. Иртышская, 8, тел. 40-94-25.

Алипов Илья Николаевич, канд. техн. наук. Научные интересы: защита информации. Адрес: Украина, 310189, Харьков, ул. Иртышская, 8, тел. 40-94-25.

Охапкин Александр Александрович, аспирант кафедры конструирования электронно-вычислительных машин ХТУРЭ. Научные интересы: защита информации. Адрес: Украина, 310007, Харьков, ул. Бекетова, 19/17, кв. 21, тел. 40-94-25.

Ребезюк Леонид Николаевич, канд. техн. наук, доцент кафедры конструирования электронно-вычислительных машин ХТУРЭ. Научные интересы: защита информации, автоматизация проектирования электронных вычислительных средств. Адрес: Украина, 310136, Харьков, ул. Ком. Уборевича, 40-б, кв. 17, тел. 69-79-38.