Н. А. Крицына, Ю. П. Кулябичев, А. А. Малюк, А. А. Суханов

К ПРОБЛЕМЕ ФОРМИРОВАНИЯ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ. ОРГАНИЗАЦИЯ СОБСТВЕННОЙ СИСТЕМЫ СЧИСЛЕНИЯ ПРИ ПОЛНОМ ПЕРЕБОРЕ АРГУМЕНТОВ ПОИСКА ГЛОБАЛЬНОГО ЭКСТРЕМУМА

Необходимость учета множества факторов, влияющих на защиту информации и находящихся в сложном динамическом взаимодействии, приводит к представлению системы защиты как многокритериального развивающегося объекта [2].

Такой объект определяется как множество реализаций сложной системы, описываемой заданным набором критериев и развивающейся под действием внешних объективных и внутренних субъективных факторов. При этом критерии качества оптимизации процесса защиты, как правило, оказываются неявно выраженными и многоэкстремальными функциями многих переменных — аргументов оптимизации. Наличие ограничений, накладываемых на аргументы оптимизации, еще больше усложняет процесс оптимизации. Для исключения потери информации оптимизацию в этом случае целесообразно проводить по ряду ограничивающих интервалов изменения аргумента путем введения собственной системы счисления.

В общем виде задача условной оптимизации многомерного критерия выглядит следующим образом:

найти минимум (максимум) критерия $J(x_1, x_2, \cdots, x_m) = \psi(x_1, x_2, \cdots, x_m)$ (1)

при ограничениях $f_j(x_1, x_2, \cdots, x_m) \geq (\leq)\ 0,\ \ j = \overline{1,n}$.

Причем, как уже отмечалось, и критерий, и функции ограничений часто носят неявный характер относительно аргументов оптимизации $x_1, x_2, \cdots, x_m$.

В такой ситуации наиболее надежным способом определения глобального экстремума критерия является полный перебор допустимых значений аргументов.

Как правило, алгоритмы организации процесса полного перебора в задачах условной оптимизации являются достаточно трудоемкими и используют сложную систему логических предикатов.

Однако в том случае, если накладываемые на аргументы оптимизации $x_1, x_2, \cdots, x_m$ ограничения имеют простой вид типа:

$$x_i^{\min} \leq x_i \leq x_i^{\max},\ \ i = \overline{1,m}\ , \tag{2}$$

целесообразно использовать процедуру полного перебора, основанную на формировании некоторого числа в произвольной системе счисления без использования сложных логических построений.

Представим интервал определения аргумента x_i в виде суммы квантов разбиения этого интервала:

$$x_i^{\max} - x_i^{\min} = \sum_{k=0}^{p_i} \Delta x_{ik},\ \ \Delta x_{i0} = 0,\quad i = \overline{1,m}\ , \tag{3}$$

где Δx_{ik} , $k = \overline{0, p_i}$ — заданные кванты дискретизации аргумента x_i , p_i — целое положительное число интервалов разбиения области допустимых значений i-го аргумента.

Таким образом, значение аргумента x_i с точностью до ошибок дискретизации можно представить в виде:

$$x_i \cong x_i^{\min} + \sum_{k=0}^{a_i} \Delta x_{ik},\ \ i = \overline{1,m}\ , \tag{4}$$

причем верхние параметры суммирования a_i не только являются целыми неотрицательными числами, но и удовлетворяют условию:

$$0 \leq a_i \leq p_i\ ,\ \ i = \overline{1,m}. \tag{5}$$

Учитывая изложенное выше, критерий оптимизации (1) можно представить в виде многомерной функции целых неотрицательных чисел a_i :

$$J(a_1, a_2, \cdots, a_m) = \varphi(a_1, a_2, \cdots, a_m), \tag{6}$$

при условии, что a_i удовлетворяют неравенствам:

$$0 \le a_i \le p_i, \ i = \overline{1,m}. \tag{7}$$

Таким образом, принимая во внимание условия, накладываемые на параметры a_i , $i = \overline{1,m}$, их можно трактовать как коэффициенты разложения целого неотрицательного числа B в числовой ряд по m разрядам с переменным основанием разрядов $p_i + 1$, $i = \overline{1,m}$.

Итак, сформируем собственную систему счисления, имеющую m разрядов, причем основания разрядов будут иметь значения $p_i + 1$, $i = \overline{1,m}$, т. е. будут превышать на единицу число отрезков дискретизации интервала определения i-го аргумента.

Представим целое положительное число B в виде разложения в числовой ряд по m разрядам в системе счисления с переменным основанием каждого разряда [2]:

$$B = a_m \prod_{i=1}^{m-1}(p_i + 1) + a_{m-1} \prod_{i=1}^{m-2}(p_i + 1) + \cdots + a_3(p_2 + 1)(p_1 + 1) + a_2(p_1 + 1) + a_1, \tag{8}$$

где коэффициенты разложения $a_m, a_{m-1}, \cdots, a_3, a_2, a_1$ — целые неотрицательные числа, удовлетворяющие условию:

$$0 \le a_i \le p_i, \ i = \overline{1,m}. \tag{9}$$

Как видим, условия (7) и (9) полностью совпадают.

Очевидно, максимальное число $B^{\max}$, которое может быть получено с помощью такого представления, будет:

$$B^{\max} = p_m \prod_{i=1}^{m-1}(p_i + 1) + p_{m-1} \prod_{i=1}^{m-2}(p_i + 1) + \cdots + p_3(p_2 + 1)(p_1 + 1) + p_2(p_1 + 1) + (p_1). \tag{10}$$

Именно такое количество расчетов необходимо произвести для выявления экстремума критерия (6) при использовании метода полного перебора.

Решим обратную задачу, а именно:

будем искать целочисленные неотрицательные коэффициенты $0 \le a_i \le (p_i); \ i = \overline{1,m}$, *соответствующие любому неотрицательному целому числу* B, *удовлетворяющему условию* $0 \le B \le B^{\max}$.

Прежде всего, определим значение коэффициента старшего разряда m как целую часть деления числа B на произведение оснований предыдущих разрядов:

$$a_m = \left[\frac{B}{\prod_{i=1}^{m-1}(p_i + 1)} \right]. \tag{11}$$

Для определения коэффициента следующего разряда a_{m-1} выделим остаток от предыдущего деления:

$$B := B - a_m \prod_{i=1}^{m-1}(p_i + 1). \tag{12}$$

Разделим на произведение оснований оставшихся разрядов полученный остаток от деления и выделим целую часть:

$$a_{m-1} = \left[\frac{B}{\prod_{i=1}^{m-2} (p_i + 1)} \right]. \tag{13}$$

Повторяя процедуры (12), (13), получим рекуррентную последовательность нахождения коэффициентов, состоящую для каждого j, удовлетворяющего условию $m \geq j \geq 3$, из двух элементарных вычислений:

$$B := B - a_j \prod_{i=1}^{j-1} (p_i + 1), \tag{14}$$

$$a_{j-1} = \left[\frac{B}{\prod_{i=1}^{j-2} (p_i + 1)} \right]. \tag{15}$$

Причем значение старшего разряда a_m вычисляется по формуле (11).

В результате реализации рекуррентной последовательности (14), (15) будут найдены значения коэффициентов: $a_{m-1}, a_{m-2}, \cdots, a_2$.

После определения коэффициентов высших разрядов a_{j-1}, $m \geq j \geq 3$, нетрудно рассчитать коэффициент младшего разряда, который находится по формуле:

$$a_1 = B - a_2(p_1 + 1), \tag{16}$$

Таким образом, решение задачи (6) при ограничениях (7) методом полного перебора сводится к последовательному перебору целых чисел от 0 до $B^{\max}$; расчету коэффициентов a_j ($j = \overline{1,m}$), соответствующих текущему значению B, по формулам (11), (14), (15), (16); расчету критерия (6) и проверке полученного значения на экстремальность.

На основе изложенного подхода ниже приведен алгоритм решения задачи (1) при ограничениях (2):

1. Задание начальных данных и организация предварительных расчетов.

1. 1. Исходные данные:

$x_i^{\min}, x_i^{\max}$, $i = \overline{1,m}$ — максимальное и минимальное значения области определения i-го аргумента;

Δx_{ik}, $k = \overline{0, p_i}$, $i = \overline{1,m}$ — кванты дискретизации аргумента x_i, p_i — целое положительное число интервалов разбиения области допустимых значений i-го аргумента.

1. 2. Предварительные расчеты:

Вычисляем максимальное число расчетов критерия (6):

$$B^{\max} = p_m \prod_{i=1}^{m-1} (p_i + 1) + p_{m-1} \prod_{i=1}^{m-2} (p_i + 1) + \cdots + p_3(p_2 + 1)(p_1 + 1) + p_2(p_1 + 1) + p_1,$$

$B = 0$ — начальное число для организации последующего цикла расчетов;

$J^{opt} = \varphi(a_1 = 0, a_2 = 0, \cdots, a_m = 0)$ — начальное значение критерия оптимизации, соответствующее нижним границам области определения аргументов.

2. Основной цикл расчетов:

2. 1. Для текущего B вычисляем значения коэффициентов a_j, $j = \overline{1,m}$, по формулам (11), (14), (15), (16).

2. 2. Рассчитываем значение критерия $J(a_1, a_2, \cdots, a_m) = \varphi(a_1, a_2, \cdots, a_m)$.

2. 2. 1. Сравниваем $J(a_1, a_2, \cdots, a_m) < J^{onm}$.

2. 2. 1. 1. Если $J(a_1, a_2, \cdots, a_m) < J^{onm}$ выполняется, то присваиваем $J^{onm} = J$, $a_j^{onm} = a_j \quad (j = \overline{1, m})$; проверяем условие полного перебора $B = B^{\max}$. Если условие полного перебора выполняется, то переходим к пункту 3, если не выполняется, то увеличиваем B на единицу ($B = B + 1$) и переходим к пункту 2.1.

2. 2. 1. 2. Если $J(a_1, a_2, \cdots, a_m) < J^{onm}$ не выполняется, то проверяем условие полного перебора $B = B^{\max}$. Если условие полного перебора выполняется, то переходим к пункту 3, если не выполняется, то увеличиваем B на единицу ($B = B + 1$) и переходим к пункту 2.1.

3. В результате проведенных действий найдено оптимальное решение — a_j^{onm} $(j = \overline{1, m})$ и оптимальное значение критерия $J(a_1^{onm}, a_2^{onm}, \cdots, a_m^{onm}) = J^{onm}$.

4. Рассчитываем значения исходных аргументов, соответствующих оптимальному значению критерия:

$$x_i^{onm} \cong x_i^{\min} + \sum_{k=0}^{a_i^{onm}} \Delta x_{ik}, \quad i = \overline{1, m}, \qquad J(x_1^{onm}, x_2^{onm}, \cdots, x_m^{onm}).$$

Как видим, предлагаемая процедура полного перебора аргументов оптимизации является достаточно компактной и не требует сложных логических построений. Кроме того, она обеспечивает надежную идентификацию точки глобального экстремума в случае многоэкстремальных критериев.

СПИСОК ЛИТЕРАТУРЫ:

1. *Загребаев А. М., Крицына Н. А., Кулябичев Ю. П., Шумилов Ю. Ю.* Методы математического программирования в задачах оптимизации сложных технических систем. М: МИФИ, 2007. – 332 с.

2. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия — Телеком, 2004. – 280 с.