промышленного шпионажа.- СП6.:ООО Изд. "Полигон",2000.-896 с.
4. *Хорее АЛ.* Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия России, 1998.-320 с.
5. Специальная техника защиты и контроля информации. Каталог- 98 МАСКОМ, М: 1998.-44с.
6. DigiScan-2000. Новое поисковое программное обеспечение// Бизнес и безопасность. 2000. N4, С. 16-17.
7. *Б.Н. Митяшев.* Определение временного положения импульсов при наличии помех. М.: Сов.радио, 1962.-200 с.
8. *Гриши» Ю.П., Ипатов В.П.,. КазариновЮ.М.* Радиотехнические системы. М.: Высш.шк,1990.-496с.

УДК 681.3

Белошапкин В.К., Пустовит С.Н.,
Пустовит С.С., Терещенко П.И.

ОБ ОДНОМ МЕТОДЕ ДЕКОМПОЗИЦИИ ПРИ ПРОЕКТИРОВАНИИ ТОПОЛОГИЧЕСКОЙ СТРУКТУРЫ КОМПЬЮТЕРНЫХ СИСТЕМ

В настоящей статье предлагается описание и условия применимости метода декомпозиции, позволяющего значительно сокращать расход вычислительных ресурсов при решении задач оптимального проектирования общей топологической структуры компьютерных сетей.

Рассматриваемый способ снижения трудоемкости задачи основан на том, что в процессе решения задачи оптимизации достаточно знать не точное значение целевой функции на каждом шаге, а лишь знак ее изменения. Поэтому, если можно построить такую функцию, которая будет проще в вычислительном отношении и в определенном смысле эквивалентна исходной целевой функции, то за счет построения такой функции и использования ее в качестве целевой можно уменьшить трудоемкость решения задачи.

В рассматриваемой задаче основные сложности при вычислении целевой функции связаны с размерностью задачи. Так, например, в сети из 10 узлов существует 2^{45} вариантов расположения каналов связи. При современном уровне развития вычислительной техники выполнить анализ всех вариантов невозможно. Поэтому цель предлагаемого метода – понижение размерности системы.

Основным приемом в рассматриваемой процедуре является фиксация определенных компонент матрицы соединений в зависимости от выполнения некоторых условий.

Задача общего топологического синтеза формулируется следующим образом.

Пусть заданна матрица информационных потоков между каждой парой узлов:

$$\Lambda = \left\| \Lambda_{ij} \right\|$$

матрица стоимости аренды каналов:

$$C = \left\| c_{ij} \right\|$$

необходимо найти количество и тип каналов связи n_{rh} в каждом соединении (r, h) со скоростью передачи V_{rh} т.е. матрицу соединений

$$N = \left\| n_{rh} \right\|$$

и величины потоков в каждом соединении

$$F = \left\| f_{rh} \right\|$$

так чтобы

$$f_1(n_{rh}) = \sum_r \sum_h C_{rh} n_{rh} \to \min_N \quad (1)$$

$$f_2(n_{rh}) = \sum_r \sum_h V_{rh} n_{rh} \to \max_N \quad (2)$$

при ограничениях

$$\sum_r \sum_h f_{rh} = \sum_i \sum_j \Lambda_{ij} \quad (3)$$

$$f_{rh} \le V_{rh} n_{rh} \quad (4)$$

Предлагается сводить задачу (1)-(4) к последовательности подзадач, в которых экстремум ищется на некоторых подмножествах матрицы соединений $N^k \subset N$ и решается системой меньшей размерности

$$f_1^k(n_{rh}, n_{rh}^k) \to \min_{N^k} f_1(n_{rh}) \quad (5)$$

$$f_2^k(n_{rh}, n_{rh}^k) \to \min_{N^k} f_2(n_{rh}) \quad (6)$$

$$\sum_{r \in j} \sum_{h \in j} (f_{rh}^{(n_{rh})} + \delta f_{rh}) = \sum_{i \in J} \sum_{j \in J} \Lambda_{ij} + \sum_{r \in S} \sum_{h \in S} f_{rk}^k \quad (7)$$

$$f_{rh} \le V_{rh} n_{rh} \ (r \in J, h \in j) \quad (8)$$

где $J \cap S = 0$, $J \cup S = \{1,2.....j\}$ - множество узлов сети

$n_{rk}^k = \arg\min\{f_1^{k-1}(n_{rh}, n_{rh}^{k-1}), n_{rh} \in N^{k-1}\} \cap \arg\max\{f_2^{k-1}(n_{rh}, n_{rh}^{k-1}), n_{rh} \in N_S^{k-1}$

Здесь экстремум понимается в смысле оптимальности по Парето, а δf_{rh} имеет смысл погрешности, возникающей при вычислении f_{rh} в результате формально зафиксированных переменных n_{rh}^k.

Из условия (7) получим матрицу $\left\| f_{rh}(n_{rh}) + \delta f_{rh}(n_{rh}^k) \right\|$.

Погрешность $\delta f_{rh}(n_{rh}^k)$ возникает в результате того, что величины f_{rh}^k заданы в точке n_{rh}^k, а не в точке n_{rh}, для которой решается система. Значения функций f_1^k, f_2^k однозначно определяются элементами множества N^k или разбиениями индексов J, S, а ее значения зависят от точки n_{rh} и точки n_{rh}^k, в которой вычисляется f_{rh}^k.

Таким образом, основная идея метода заключается в том, что для каждого подмножества N^k выделяется матрица соединений $\left\| n_{rh}^k \right\|$, содержащая такие переменные $n_{rk},(r,h)\in S$ которые относительно мало изменяются в процессе решения k-й подзадачи. Компоненты этой матрицы вычисляются лишь в начальной точке данной подзадачи, а в дальнейшем процессе ее решения считаются постоянными. В этой же точке n_{rh}^k для каждой подзадачи могут определяться, в зависимости от конкретных реализаций метода следующие величины: значение функций $f_1(n_{rh}^k), f_2(n_{rh}^k)$ и их приращения в этой точке, множество N^k и множества индексов J, S.

Вычисление $f_1(n_{rh}^k), f_2(n_{rh}^k)$ производится с целью контроля за ходом процесса оптимизации (5)-(8). Это означает, что в случаях, когда условия, обеспечивающие сходимость процесса (5)-(8) к Парето - оптимальному множеству выполняются не для всех подзадач, то на множестве $n_{rh} \in \arg\min\{f_1^{k-1}(n_{rh},n_{rh}^k)\big| n_{rk} \in N^{k-1}\} \cap \arg\max\{f_1^{k-1}(n_{rh},n_{rh}^k)\big| n_{rk} \in N^{k-1}\}$

значение функции f_1 может оказаться не меньше (f_2 - не больше), чем в начальной точке n_{rh}^{k-1} для этой подзадачи. В этом случае для множества N^{k-1} может быть определена более точная функция $f_1^{k-1}(f_2^{k-1})$ и $(k-1)$ подзадача решена еще раз или в качестве начальной точки для k-й подзадачи выбирается n_{rh}^{k-1}. За счет применения данной процедуры основной объем вычислений производится при решении более простых подзадач вида (5)-(8), а вычисление f_1, f_2 в точках n_{rh}^k гарантирует построение оптимизирующей последовательности.

Приращение функций f_1 и f_2 вычисляются в тех случаях, когда множества J и S заранее не заданны, и подзадачи генерируются непосредственно в ходе решения.

Определим связь погрешностей для компонент фиксированной n_{rh}^k и текущей n_{rh} частей переменных.

Рассмотрим формулу (7). Ее можно записать в виде

$$\sum_{r\in J}\sum_{h\in J} f_{rh}(n_{rh}) = \sum_{i\in J}\sum_{j\in J}\Lambda_{ij} + \sum_{r\in S}\sum_{n\in S}(f_{rh}^k + \delta f_{rh}^k), \qquad (9)$$

вычитая (9) из (8) получаем

$$\sum_{r\in J}\sum_{n\in J}\delta f_{rh} = \sum_{r\in S}\sum_{h\in S}\delta f_{rh}^k \qquad (10)$$

Пусть в (4) имеет место предельный случай, т.е.

$$f_{rh} = V_{rh}n_{rh}.$$

Тогда

$$\begin{cases} \delta f_{rh} = V_{rh}\delta n_{rh} \\ \delta f_{rh}^{k} = V_{rh}\delta n_{rh}^{k} \end{cases} \qquad (11)$$

Подставляя (11) в (10) получаем:

$$\sum_{r\in J}\sum_{h\in J} V_{rh}\delta n_{rh} = \sum_{r\in S}\sum_{n\in S} V_{rh}\delta n_{rh}^{k}$$

Отсюда, связь между погрешностями определения фиксированной части каналов и изменяемой определяется структурой множеств J и S, а также скоростями передачи информации по каналам в структуре этих множеств. Дадим теперь интерпретацию метода фиксации переменных на языке теории иерархических многоуровневых систем.

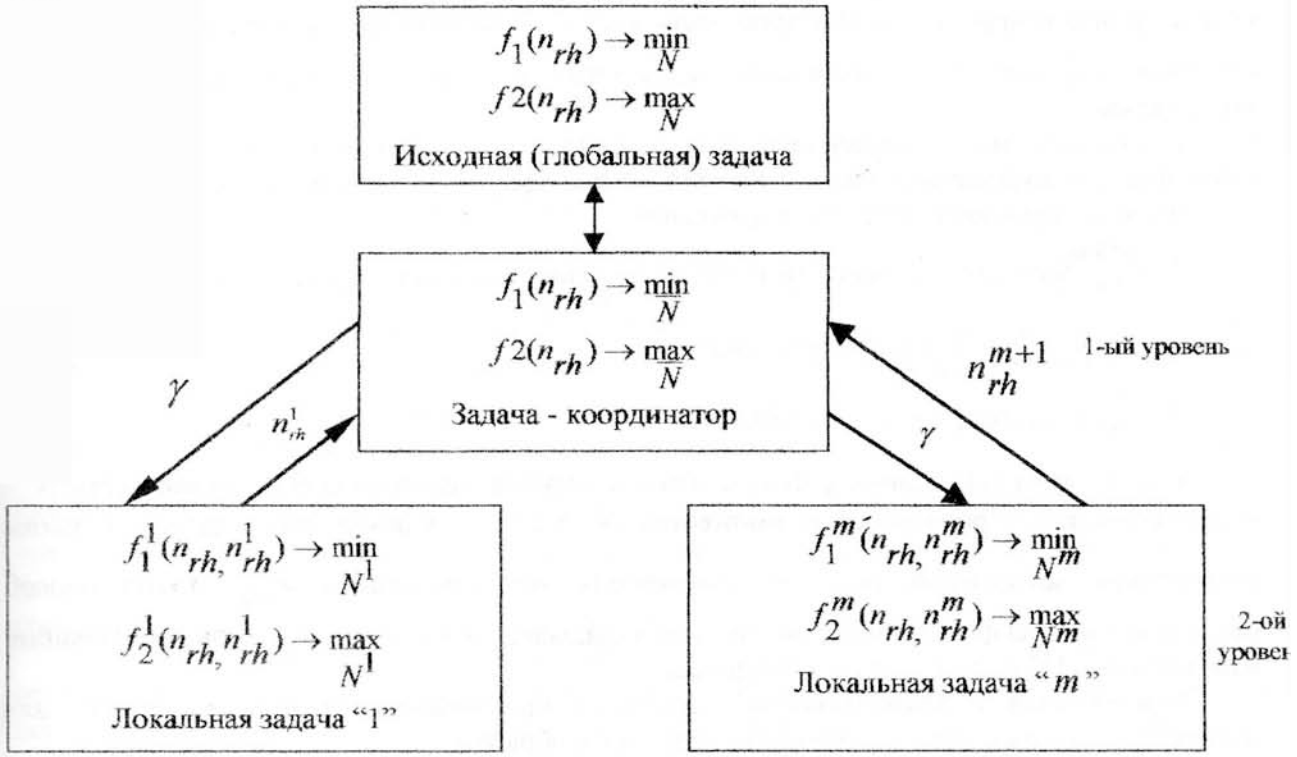
Введем множество точек $\overline{N}$, являющихся решениями задач вида (5)-(8)

$$\overline{N} = \left\{ n_{rh}^{k} \in N : n_{rh}^{k} = \arg\min\left\{ f_1^{k-1}(n_{rh}, n_{rh}^{k-1}) \right\} \cap \arg\max\left\{ f_2^{k-1}(n_{rh}, n_{rh}^{k-1}) \right\} n_{rh} \in N^{k-1}, k = 1,2\ldots \right\}$$

Пусть в процессе (5)-(8) используется 2m различных функций $f_1^k, f_2^k (k = 1,\ldots,m)$.

Тогда рассматриваемую выше декомпозиционную схему решения задачи (1) – (4) можно представить в виде двухуровневой системы с конечным числом подсистем, координация в которых осуществляется с помощью прогнозирования взаимодействий и изменения ограничений [1].

Первый уровень рассматриваемой иерархической системы (рис.1) содержит одну подсистему – задачу – координатор, второй уровень состоит из совокупности m задач или подзадач (подсистем). На вход каждой подсистемы второго уровня подается координирующий сигнал $\gamma \in \Gamma$, вырабатываемый подсистемой первого уровня. В свою очередь на вход подсистемы первого уровня подается результат работы (в данном случае n_{rh}^{k}) каждой из подсистем второго уровня.



Координация способом прогнозирования взаимодействий подразумевает задание с помощью сигнала γ фиксированных значений (прогнозов) для связующих входов локальных подзадач. Связующими входами в данном случае являются значения f_{rh}^{k}, а координирующий сигнал γ содержит номер k, $(k=1,..,m)$ очередной локальной задачи, которая будет решаться, множество N^{k}, начальную точку n_{rh}^{k}.

Координация путем изменения ограничений осуществляется заданием с помощью сигнала γ множества допустимых решений, что и происходит в данном случае в виде задания множеств N^{k} для k-й подзадачи.

В [1] приводятся утверждения о применимости различных принципов координации и, в том числе, принципа прогнозирования взаимодействий. Однако, при этом предполагается, что допустимые множества N^{k} являются сечениями множества N и каждая подсистема находит свою оптимальную компоненту решения n_{rh}^{*k}, такую, что решение глобальной задачи (1)-(4) представимо в виде $n_{rh}^{*}=(n_{rh}^{*1},...,n_{rh}^{*m})$.

Такое предположение будет выполняться для предлагаемого метода, если он реализован с помощью разбиения проектируемой системы на m непересекающихся частей (подсистем). При этом каждая k-я подсистема оптимизируется отдельно с использованием своих функций f_{1}^{k}, f_{2}^{k}. Тогда подсистемы второго уровня соответствуют оптимизируемым частям проектируемого объекта. Каждое множество N^{k} определяется ограничениями на величину проектируемых параметров элементов k-й подсистемы, а величины $f_{rh}^{k}(n_{rh}^{k})$ содержат информацию о значениях переменных в узлах, принадлежащих остальным подсистемам.

В используемых обозначениях утверждение, рассмотренное в [1] о применимости принципа прогнозирования взаимодействий, можно сформулировать в следующем виде:

принцип применим, если из утверждения

1. n_{rh}^{*k} являются решениями соответствующих локальных подзадач и при этом для всех подзадач $f_{rh}^{k}=0$, следует утверждение

2. n_{rh}^{*} является решением глобальной задачи.

В отличие от [1] в данной работе в общем случае размерность любого из множеств N^{k} может совпадать с размерностью множества N, т.е. в k-й локальной подзадаче с таким множеством допустимых решений изменяются все компоненты n_{rh}. Такой способ реализации метода фиксации переменных не укладывается в схему принципов координации, изложенных в [1] и являются их обобщением.

Утверждения о применимости принципа прогнозирования взаимо-действий для нашего случая можно сформулировать следующим образом.

Пусть все локальные подзадачи таковы, что размерность любого множества N^k совпадает с размерностью N. Тогда утверждение о применимости принципа прогнозирования взаимодействий имеет вид:

принцип применим, если из утверждения

1. Существует подзадача с номером k, такая, что решение глобальной задачи n^*_{rh} содержится в N^k,

$$n^*_{rh} = \arg\min\left\{f_1^k(n_{rh}, n^k_{rh})\right\} \cap \arg\max\left\{f_2^k(n_{rh}, n^k_{rh})\right\} n_{rh} \in N^k$$

и при этом для данной задачи правильно прогнозируются взаимодействия, т.е. $f^k_{rh} = 0$, следует утверждение:

2. n^*_{rh} является решением глобальной задачи.

Когда среди m подзадач второго уровня содержатся подзадачи таких, в которых ищется компонента решения $n^*_{rh} = (n^{*1}_{rh}, \ldots, n^l_{rh})$, а в остальных подзадачах меняются все компоненты n_{rh}, утверждение о применимости имеет следующий вид:

принцип применим, если из утверждения

1. или $n^*_{rh} = (n^{*1}_{rh}, \ldots, n^l_{rh})$ являются решениями соответствующих локальных подзадач и при этом для всех подзадач $f^k_{rh} = 0$ или существует подзадача с номером k, $(k = l+1, \ldots, m)$, такая, что решение глобальной задачи содержится в N^k, n^*_{rh} является решением k - ой подзадачи и при этом для данной подзадачи $f^k_{rh} = 0$ следует утверждение

2. n^*_{rh} является решением глобальной задачи.

Двухуровневая система будет состоять из подсистем такого вида в том случае, когда, например, сначала находится некоторое приближение решения с помощью подсистем с номерами $k = 1, \text{K}, l$, а затем полученный результат уточняется с помощью подсистем с номерами $k = l+1, \text{K}, m,$, которые ищут решение на множествах с меньшими линейными размерами, чем исходное и, возможно, с использованием более простых целевых функций, чем f_1 , f_2 . В этом случае искомый результат может быть получен как при решении первых l локальных подзадач, так и при решении одной из подзадач с номером $k = l+1, \text{K}, m$.

Проведем сравнительный анализ предлагаемого метода с известными методами релаксации и закрепления переменных.

Основным следствием применения данного метода является уменьшение числа вариантов состояния системы, подлежащих анализу. В методах релаксации ограничений типа Джоффриона или Розена [2,3] упрощение задачи происходит за счет меньших затрат ресурсов на удовлетворение имеющихся в задаче ограничений, тогда как в данном случае снижается трудоемкость вычисления целевой функции.

Добавим к сказанному, что в методах релаксации часть ограничений просто отбрасывается, тогда как в данном случае уменьшение числа вариантов происходит за счет искусственного фиксирования значений некоторых компонент матрицы N, объединенных в

матрицу N^k, и выражения остальных компонент через фиксированные. Благодаря такому приему исключаются варианты, соответствующие переменным из N^k.

По сравнению с методами закрепления переменных [4,5] одним из отличий является то, что в существующих методах закрепления считаются константами некоторые переменные, которые при этом действительно имеют постоянные значения, а в данном методе только формально считается что часть переменных имеет фиксированные значения, а фактически эти значения в определенных точках просто не вычисляются. Тем самым снимается всякий контроль за изменением этих переменных и делается это благодаря использованию априорной информации о том, что данные переменные достаточно мало меняются в данной подзадаче.

Рассмотрим теперь условия сходимости итерационного процесса (5)-(8) к решению исходной задачи.

Введем следующие обозначения:

$g(n_{rk})$- направление поиска, определяемое используемым методом математического программирования. Предполагается, что $g(n_{rk})$-однозначная функция для всех $n_{rh} \in N$. В дальнейшем, при употреблении этого обозначения аргумент будем опускать.

$\hat{N}$-множество точек оптимизирующей последовательности которая строится используемым методом математического программирования, т.е.

$$\hat{N} = \left\{ n_{rh}^k \in N : \left\{ f_1\left(n_{rh}^{k+1}\right) < f_1\left(n_{rh}^k\right) \right\} \cap \left\{ f_2\left(n_{rh}^{k+1}\right) > f_2\left(n_{rh}^k\right) \right\}, \quad k = 0,1. \right\}$$

где n_{rh}^0- заданная начальная точка.

G-множество направлений g, последовательно выбираемых в точках множества $\hat{N}$, т.е.

$$G = \left\{ g = g(n_{rh}) : n_{rh} \in \hat{N} \right\}.$$

n_{rh}^{mg}- точка на направлении g, являющемся m-м приближением задачи одномерного поиска на g, т.е.

$$n_{rh}^{mg} = n_{rh}^{(m-1)g} + \rho \frac{g}{\|g\|}$$

где ρ-шаг одномерного поиска, причем ρ такой, что $n_{rh}^{mg} \in N$.

N^g- множество точек одномерного поиска на направлении $g \in G$, выбираемом в некоторой точке $n_{rh}^k \in \hat{N}$, т.е.

$$N^g = \left\{ n_{rh}^{mg} \in N : n_{rh}^{mg} = n_{rh}^{(m-1)g} + \rho \frac{g}{\|g\|}, n_{rh}^{og} = n_{rh}^k, n_{rh}^k \in \hat{N} \right\}.$$

Определим приращения в точке n_{rh}^{mg} по направлению g для значений f_{rh} и целевых функций:

$$\Delta_g f_{rh}\left(n_{rh}^{mg}\right) = f_{rh}\left(n_{rh}^{(m+1)g}\right) - f_{rh}\left(n_{rh}^{mg}\right)$$

$$\Delta_g f_i\left(n_{rh}^{mg}\right) = f_i\left(n_{rh}^{(m+1)g}\right) - f_i\left(n_{rh}^{mg}\right), \quad (i = 1,2)$$

$$\Delta_g f_i^k\left(n_{rh}^{mg}, n_{rh}^k\right) = f_i\left(n_{rh}^{(m+1)g}, \delta n_{rh}^{(m+1)gk}\right) - f_i\left(n_{rh}^{mg}, \delta n_{rh}^{mgk}\right), \quad (i = 1,2)$$

Теорема

Примем следующие предположения:

1. $f_1(\cdot), f_2(\cdot)$ удовлетворяют на N требованиям сходимости используемого метода математического программирования к Парето оптимальной области.

2. Функции $f_i^k\left(n_{rh}^{mg}, n_{rh}^k\right)$ $(i=1,2)$ удовлетворяют на множестве требованиям сходимости к соответствующим точкам $n_{rh}^k \in N$.

3. Существует номер *k*, такой, что в соответствующей *k*– ой подзадаче $\arg\min\left\{f_1\left(n_{rh}\right), n_{rh} \in N\right\} \cap \arg\max\left\{f_2\left(n_{rh}\right), n_{rh} \in N\right\} \in N^k$.

4. Для любого $k = 0,1,\text{K}, g \in G$ и любой точки $n_{rh}^{mg} \in N^g$ выполняются равенства

$$\begin{cases} sign\,\Delta_g f_1^k\left(n_{rh}^{mg}, n_{rh}^k\right) = sign\,\Delta_g f_1\left(n_{rh}^{mg}\right) \\ sign\,\Delta_g f_2^k\left(n_{rh}^{mg}, n_{rh}^k\right) = sign\,\Delta_g f_2\left(n_{rh}^{mg}\right) \end{cases}$$

Тогда

$$\lim_{k\to\infty} n_{rh}^k = n_{rh}^* = \arg\min\left\{f_1\left(n_{rh}\right), n \in N\right\} \cap \arg\max\left\{f_2\left(n_{rh}\right), n_{rh} \in N\right\}$$

т.е. n_{rh}^* принадлежит Парето–оптимальному множеству, а итерационный процесс (5)-(8) сходится к решению задачи (1)-(4).

Доказательство. Поскольку последовательность чисел $\left\{f_1\left(n_{rh}^k\right)\right\}, n_{rh}^k \in \hat{N}$ монотонно убывает по построению и ограничена снизу, а последовательность $\left\{f_2\left(n_{rh}^k\right)\right\}, n_{rh}^k \in \hat{N}$ монотонно возрастает и ограничена сверху, то существует $\left\{\lim_{k\to\infty} f_1\left(n_{rh}^k\right)\right\}$ и $\left\{\lim_{k\to\infty} f_2\left(n_{rh}^k\right)\right\}$. Точку из множества Парето–оптимальных решений, являющуюся результатом итерационного процесса (5)-(6) обозначим n_{rh}^*.

Предположим противное: n_{rh}^* не является решением задачи (5)-(8), т.е. согласно предположению 1, существует точка $n_{rh}^0 \neq n_{rh}^*$ такая, что

$$n_{rh}^0 = \arg\min\left\{f_1^k\left(n_{rh}\right), n_{rh} \in N\right\} \cap \arg\max\left\{f_2\left(n_{rh}\right), n_{rh} \in N\right\}$$

Рассмотрим *к*-ю подзадачу, для которой выполняется предположение 3. по предположению 1 существует точка $n_{rh}^j \in \hat{N}$

и $g\left(n_{rh}^j\right) \in G$ такое, что

$$g = n_{rh}^0 - n_{rh}^j$$

и для некоторой точки n_{rh}^{mg} на направлении g при

$$\rho = \left\| n_{rh}^0 - n_{rh}^{mg} \right\|$$

выполняются неравенства

$$\Delta g\, f_1\left(n_{rn}^{mg}\right) < 0$$

$$\Delta g\, f_2\left(n_{rn}^{mg}\right) > 0$$

и в то же время поскольку из предположения 2 и предположения о том, что $n_{rh}^0 \neq n_{rh}^*$ следует, что

$$n_{rh}^0 \neq \arg\min\left\{f_1^k\left(n_{rh}, n_{rh}^k\right), n_{rh} \in N^k\right\} \cap \arg\max\left\{f_2^k\left(n_{rh}, n_{rh}^k\right), n_{rh} \in N^k\right\}$$

то

$$\Delta g\, f_1^k\left(n_{rn}^{mg}, n_{rh}^k\right) \geq 0,$$

$$\Delta g\, f_2^k\left(n_{rn}^{mg}, n_{rh}^k\right) \leq 0$$

и значит для данного *к*, g и n_{rh}^{mg}

$sign\,\Delta g\, f_1^k\left(n_{rn}^{mg}, n_{rh}^k\right) \neq sign\,\Delta g\, f_1\left(n_{rn}^{mg}\right)$,

$sign\,\Delta g\, f_2^k\left(n_{rn}^{mg}, n_{rh}^k\right) \neq sign\,\Delta g\, f_2\left(n_{rn}^{mg}\right)$,

что противоречит условиям теоремы, следовательно,

$n_{rh}^0 = n_{rh}^*$.

Теорема доказана.

Рассмотрим некоторые конкретные свойства задачи (1)-(4), способствующие успешному применению метода.

1. Наличие в оптимизируемой системе относительно слабо связанных подсистем.

Чем меньше степень связности рассматриваемой подсистемы, тем больше может быть погрешность метода, которая мало повлияет на общее значение целевой функции. Это позволяет фиксировать большее число компонент переменных, что повышает эффективность метода.

В частности, если позволяет специфика задачи, матрицу $\left\|f_{rh}\right\|$ желательно преобразовать к блочно-диагональному виду. В этом случае, степень связности подсистем, состоящих из узлов, соответствующих ненулевым блокам матрицы с остальными узлами будет равна нулю. В случае же, когда слабо связанные подсистемы ищутся в матрице общего вида, важным фактором, способствующим применению декомпозиции, является хорошая обусловленность матриц $\left\|N^k\right\|$.

2. Наличие для некоторых множеств $N^g, g \in G$ слабо меняющихся переменных, которые объединяются в фиксированную матрицу $\left\|f_{rn}^S\right\|$.

Отметим, что этот фактор является одним из наиболее важных, поскольку прием искусственного фиксирования матрицы является единственным источником погрешностей данного метода.

3. Монотонность функций $f_1\left(n_{rh}\right)$ и $f_2\left(n_{rh}\right)$.

4. Небольшое число l шагов одномерного поиска. Это условие связано с процессом накопления погрешности, которому соответствует величина

$$\left\|\sum_{j=0}^{l-1} \Delta_g f_{rh}^S\left(n_{rh}^{jg}\right)\right\|.$$

Поскольку основная цель декомпозиции – экономия ресурсов при решении задачи, то желательно за счет использования остальных факторов, способствующих применению декомпозиции обеспечить такое значение l, которое, с одной стороны отвечает требованиям решаемой задачи, а с другой стороны позволяет в l точках данного направления вычислять приближенные функции $f_i^k\left(n_{rh}, n_{rh}^k\right)$, $\left(i = 1,2\right)$.

На основании этих факторов предложим варианты их использования при построении подзадач вида (5) – (8)

1. Пусть свойства сети позволяют выделить подсистемы, которые для любого $n_{rh} \in N^g, g \in G$ будут слабо связаны с сетевыми узлами системы (например, терминальные сети в топологии "звезда " можно считать слабосвязанными). Тогда, для любого множества N^g, определяется матрица $\left\|f_{rh}^j\right\|$ соответствующая одной из слабо связанных подсистем так, чтобы матрица $\left\|f_{rh}^k\right\|$ достаточно мало изменялась на множестве N^g. Матрица $\left\|f_{rh}^j\right\|$ однозначно определяет функции $f_i^k\left(n_{rh}, n_{rh}^k\right)$, $\left(i = 1,2\right)$, которые будут анализироваться.

2. Пусть свойства сети позволяют заранее классифицировать переменные по степени их изменения для любого $n_{rh} \in N^g$ (это может быть обусловлено, например, очевидными отличиями в поведении разных групп узлов проектируемой системы).

Тогда для любого множества N^g из узлов, соответствующих наиболее сильно меняющимся компонентам матрицы $\|f_{rh}\|$ выбирается достаточно слабо связанная подсистема.

Другими словами, матрица $\|f_{rh}^j\|$ формируется из наиболее сильно меняющихся переменных таким образом, чтобы она содержала наименьшее число компонент и при этом выполнялись условия применимости декомпозиции.

Итак, пусть для задачи (1)-(4) построено соответствие между множествами N^k и множеством функций f_i^k, $(i=1,2)$, т.е. задача представлена в виде (5)-(8). При решении этой задачи можно выделить следующую последовательность действий.

Шаг 1. к:=0; выбрать начальную точку n_{rh}^0.

Шаг 2. Выбрать в точке n_{rh}^k направление поиска g, т.е. определить множество N^k.

Шаг 3. Решается подзадача

$$f_1^k\left(n_{rn}^{mg}, n_{rh}^k\right) \to \min_{N^k}$$

$$f_2^k\left(n_{rn}^{mg}, n_{rh}^k\right) \to \max_{N^k}$$

Шаг 4. Если

$$f_1\left(\arg\min\left\{f_1^k\left(n_{rh}, n_{rh}^k\right), n_{rh} \in N^k\right\}\right) < f_1\left(n_{rh}^k\right)$$

$$f_2\left(\arg\max\left\{f_2^k\left(n_{rh}, n_{rh}^k\right), n_{rh} \in N^k\right\}\right) > f_2\left(n_{rh}^k\right)$$

то положить

$$n_{rh}^{k+1} = \arg\min\left\{f_1^k(\cdot)\right\} \cap \arg\max\left\{f_2^k(\cdot)\right\}, k = k+1$$

иначе

множеству N^k поставить в соответствие более точную целевую функцию f_i^k и перейти к шагу 2.

Шаг 5. Если

$$n_{rh}^k = \arg\min\left\{f_1^k\left(n_{rh}, n_{rh}^k\right), n_{rh} \in N\right\} \cap \arg\max\left\{f_2^k\left(n_{rh}, n_{rh}^k\right), n_{rh} \in N\right\}$$

то остановиться

иначе

перейти к шагу 1.

Подобные специфические закономерности в оптимизационных системах, позволяющие применять метод фиксации переменных, зависят от топологии системы и характера информационных потоков. Поэтому трудно дать какие-либо универсальные рекомендации для системы любого вида. Однако, как показывает практика, большинство сложных систем обладает тем или иным свойством, позволяющим упростить задачу, а условия применимости декомпозиции ориентируют на поиск таких свойств.

Список литературы:

1.Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. Мир.М., 1973. 344 с.

2. Лэсдон Л.С. Оптимизация больших систем.М., Наука. 1975, 432 с.

3.Geoffrion A,M. Elements of lorge-seecele mathematical programming. Parts – Management Scsence, 1970, 16, № 11, p 652-691.
4.Левин Г.М. Ганаев В,С, Декомпозиционные методы оптимизации проектных решений. Минск. Наука и техника, 1978, 240 с.
5.Изурков В.И. Декомпозиция в задачах большой размерности. М., Наука, 19981, 352 с.

УДК 519.6

Богданов А.М., Зинченко Я.В.

МОДИФИКАЦИЯ АЛГОРИТМА УМНОЖЕНИЯ СВЕРХБОЛЬШИХ ЧИСЕЛ НА ОСНОВЕ КОЭФФИЦИЕНТОВ УОЛША

В настоящее время при программной реализации асимметричных криптоалгоритмов существует необходимость в быстром выполнении операции умножения многоразрядных чисел, размерность которых реально составляет 512-4096 бит.

Известно, что число шагов (битовых операций), необходимых для умножения двух m-разрядных чисел "в столбик", равняется m^2. Однако, нашли широкое применение методы, позволяющие вычислить требуемое произведение быстрее, чем за m^2 шагов. Это метод Карацубы со сложностью $O\left(m^{1,59}\right)$, модулярный метод, имеющий сложность $O\left(m^{1,63}\right)$, и другие. Алгоритм Шенхаге-Штрассена является асимптотически самым быстрым из известных и позволяет умножить два m-разрядных числа за $m\,log\,m\,log\,log\,m$ шагов [1]. Этот алгоритм основан на идее использования теоремы о дискретной свертке двух функций, т. к. произведение многоразрядных чисел без учета переносов является дискретной циклической сверткой двух сомножителей. Поскольку дискретная циклическая свертка дает основной вклад в оценку сложности алгоритма, то для эффективного ее вычисления используется алгоритм быстрого преобразования Фурье.

В работе [2] описан и проанализирован эффективный алгоритм умножения многоразрядных чисел, в основу которого положен разработанный в [3] алгоритм вычисления циклической свертки, основанный на коэффициентах Уолша и отсутствии перехода в поле комплексных чисел.

В данной статье предлагается методика модификации алгоритма вычисления циклической свертки, предложенного в [3], путем уменьшения общего числа сложений, необходимых для его реализации. Сущность модификации заключается в замене операции вычисления коэффициентов Уолша с использованием быстрого преобразования Уолша (БПУ) на операцию вычисления этих коэффициентов с использованием быстрого преобразования Хаара (БПХ).

Из [3] известно, что общее количество сложений, необходимых для вычисления циклической свертки, равно:

$$Q_{\Sigma}^{+} = Q_1^{+} + Q_2^{+} + Q_3^{+} = n \cdot 2^{n+1} + 4\left(3^{n-1} - 2^{n-1}\right) + 3^{n+1} - 3{,}5 \cdot 2^{n} = \\ = 13 \cdot 3^{n-1} + 2^{n+1}(n - 2{,}75), \qquad (1)$$

где $Q_1^{+} = n \cdot 2^{n+1}$ – количество сложений, необходимых для выполнения шага 1 алгоритма (вычисление коэффициентов Уолша F^{x} и F^{y} исходных последовательностей x и y с использованием БПУ), $Q_2^{+} = 4\left(3^{n-1} - 2^{n-1}\right)$ – число сложений, необходимых для