нарощуваних параметризованих процесорних ядер спеціалізованих надвеликих інтегральних схем // Вісн. ДУ "Львівська політехніка". №350. С.44 – 47. 6. R.L. Rivest, A. Shamir, and L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2): 120-126, February 1978. 7. T. El Gamal. A Public Key Cryptosystem and a Signature System Based in Discrete Logarithms. IEEE Trans. on Information Theory. V.IT-31, no.4, pp.469-472, July 1985. 8. Информационная технология. Криптографическая защита информации. Процедуры проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма ГОСТ34.310-95, М., 1995. 9. Информационная технология. Криптографическая защита информации. Функция хеширования ГОСТ34.311-95, М., 1995. 10. J.Daemen. Cipher and Hash Function Design. Strategies Based on Linear and Differention Cryptanalysis. Doctoral Dissertation, Katholieke Universiteit Leuven, 1995. 11. Hi-Fi, Inc. The 7711 Encryption Processor Data sheet. DS-0001-001, 1998. 12. VLSI Technology, Inc. The VMS115 Data Sheet, 1999. 13. Системы обработки информа ции. Защита криптографическая. Алгоритм криптографического преобразования. ГОСТ 28147–89, М., 1989.

УДК 621.382

Мельник Р.А., Масько Д.В.
ДУ “Львівська політехніка”, кафедра ПЗ

ДЕКОМПОЗИЦІЙНИЙ АЛГОРИТМ ПОБУДОВИ МІНІМАЛЬНИХ ЗВ’ЯЗУВАЛЬНИХ ДЕРЕВ

Розглянуто декомпозиційний алгоритм побудови мінімального зв’язуючого дерева, що базується на методі побудови дерева оптимального згортання. Використано поняття нечіткого з’єднання між блоками (кластерами) та окремими точками на площині.

Вступ. Відсутність достатньо ефективних алгоритмів побудови МЗД [1] є причиною використання декомпозиційного підходу, який базується на факті, що для двох-трьох контактів ланцюга (назвемо їх елементами) точний розв’язок завжди може бути знайдений. Розглянемо метод, який дозволяє отримати близьке до оптимального МЗД і який базується на оптимальному згортанні цих елементів у нечіткі кластери (блоки) [2].

Стратегії та критерії згортання. За блок певного рівня приймаємо сукупність елементів, об’єднаних у вершинах дерева згортання в процесі його побудови. На площині (ДТРП) цьому блоку відповідає прямокутна область, яка охоплює елементи, що попадають у кластер в процесі об’єднання. Найнижчий рівень дерева відповідає елементам множини I, тобто контактам. В процесі побудови дерева згортання об’єднання вершин дерева відповідає трьом типам реального об’єднання на площині, а саме: “елемент-елемент”, “блок-елемент” і “блок-блок”. Критерієм для вибору найкращих пар вершин дерева $T_з$ для згортання є мінімальна віддаль між ними у ортогональній метриці, тобто

$$F_{ij} = \min_{i,j \in I} L\,(i,j),$$

де віддаль *L (i,j)* для кожного окремого випадку визначається за формулами:

- “елемент-елемент”

$$L(i,j) = |x_i - x_j| + |y_i - y_j|,$$

- “блок-елемент”

$$L(i,j) = \min\{|x_i^1 - x_j|, |x_i^2 - x_j|\} + \min\{|y_i^1 - y_j|, |y_i^2 - y_j|\},$$

- “блок-блок”

$$L(i,j) = \min\{|x_i^1 - x_j^1|, |x_i^1 - x_j^2|, |x_i^2 - x_j^1|, |x_i^2 - x_j^2|\} + \min\{|y_i^1 - y_j^1|, |y_i^1 - y_j^2|, |y_i^2 - y_j^1|, |y_i^2 - y_j^2|\}.$$

При об’єднанні окремих вершин утворюються прямокутні блоки, які в подальшому об’єднуються як з вершинами, так і з самими блоками (рис. 1).

Координатами нових блоків є координати охоплюючих прямокутників:

$$x_i^1 = \min\{x_i^1, x_j^1\},$$
$$x_j^2 = \max\{x_i^2, x_j^2\},$$
$$y_i^1 = \min\{y_i^1, y_j^1\},$$
$$y_j^2 = \max\{y_i^2, y_j^2\}.$$

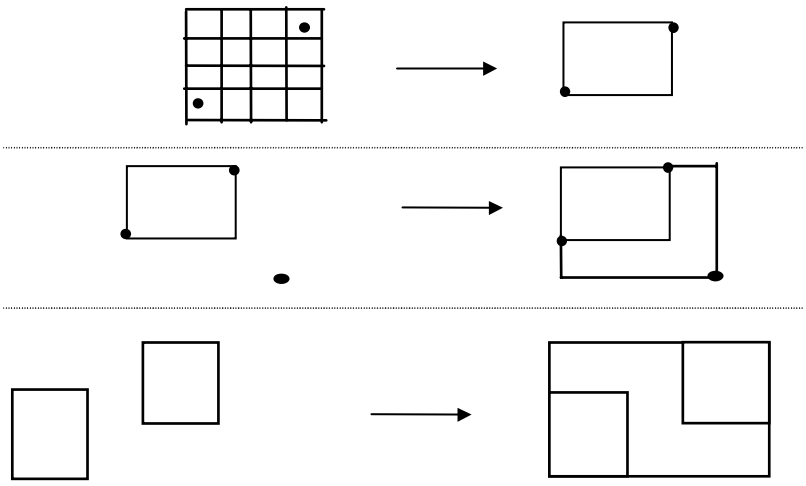

Рис.1. Об’єднання вершин і блоків

Обмеженнями на формування блоків виступають умови неперевищення розмірів блоків, тобто коли одночасно всі або окремо виконуються умови

$$\max\{|x_i^1 - x_j^1|, |x_i^1 - x_j^2|, |x_i^2 - x_j^1|, |x_i^2 - x_j^2|\} > L_x^h$$
$$\max\{|y_i^1 - y_j^1|, |y_i^1 - y_j^2|, |y_i^2 - y_j^1|, |y_i^2 - y_j^2|\} > L_y^l,$$

де L_x^h L_y^l – максимально допустимі розміри блоків.

Ілюстрацією сказаного є рис.2, де зображені фрагмент дерева згортання (а) і відповідні новим вершинам блоки (б).

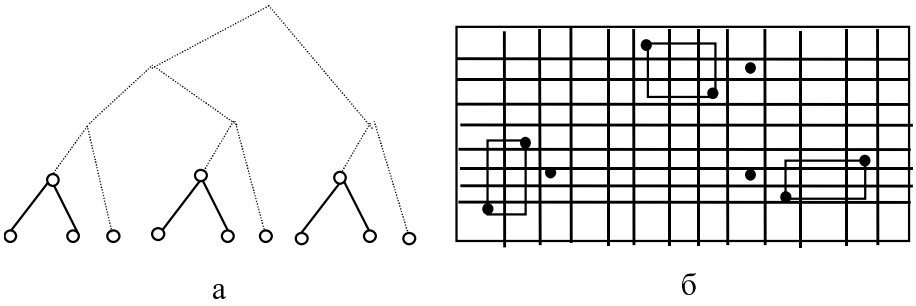

Рис.2. Фрагмент дерева згортання елементів і блоків

Обмеження дають можливість формувати блоки бажаної структури, надаючи їм пріоритети розширення у вертикальному чи горизонтальному напрямах (рис.3).

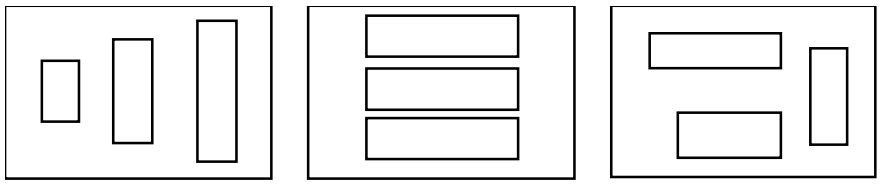

Рис.3. Побудова блоків з різними пріоритетами і стратегіями

Практично для згортання вершин використовується принцип побудови вільного дерева згортання, в якому в першу чергу об'єднуються найближчі елементи. У ієрархічному підході можливими є різні стратегії побудови фрагментів МЗД: проведення бінарних з'єднань, коли на кожному рівні блок розглядається як сукупність двох блоків нижчого рівня, пошук 3-арних з'єднань для розбиття на три блоки (рис.3.) тощо. Збільшення арності задачі ускладнює її, але приводить до кращих значень цільової функції.

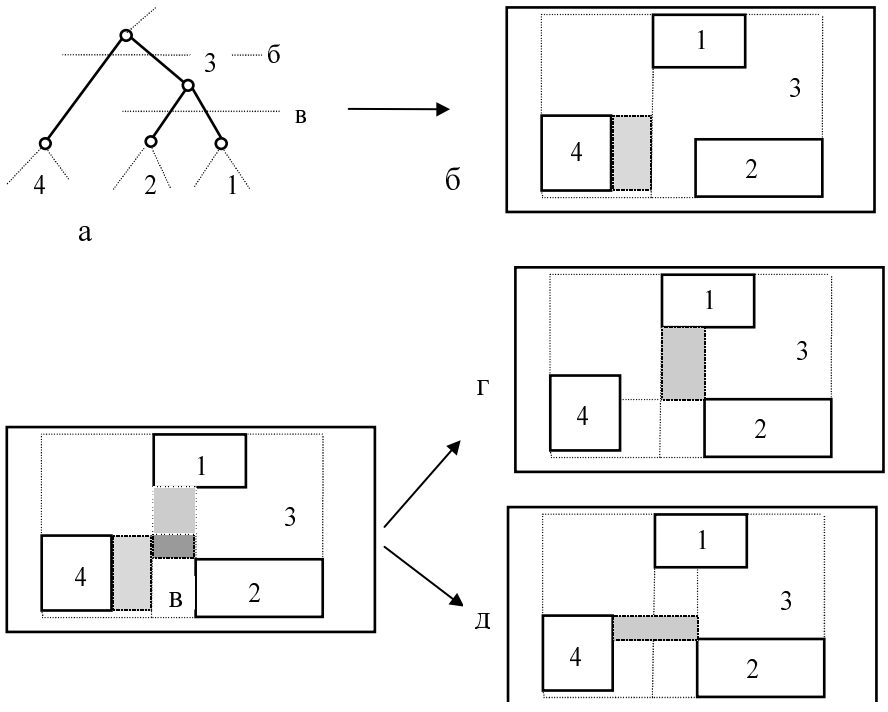

Рис.4. Побудова МЗД між блоками

Проведення міжз'єднань.Після побудови дерева згортання задача побудови МЗД ланцюга на площині розбивається на декілька задач знаходження МЗД окремих блоків. При цьому можливими є чотири типові для декомпозиційних методів стратегії, ов'язані з алгоритмами обходу дерева згори-донизу чи знизу-догори. Найкращою є стратегія згори-донизу, оскільки вона дозволяє підтримувати невизначеніть призначення з'єднань при проходженні від верхніх до найнижчих елементів. Розглянемо цю стратегію на *i*-му кроці опрацювання дерева (рис.4.).

Побудова з'єднань між блоками не має однозначного розв'язання, а існує множина МЗД (заштриховані області відповідають деревам мінімальної ваги). Фрагменти МЗД для з'єднань блоків можуть бути у вигляді ліній, смуг ліній та їх комбінацій, тобто конкретні лінії чи смуги не зафіксовані (не визначені). Їх часткове уточнення можливе при розгляді топології у блоках нижчого рівня. У відповідних блоках нижчого рівня дерева згортання фрагменти МЗД необхідно будувати з врахуванням підведених фрагментів МЗД, побудованих на попередньому вищому рівні На рис.4.б з'єднання між *3*-м та *4*-м блоками зображене смугою невизначеності. На рис.4.в зображено з'єднання блоків *1* та *2* межах *3* з врахуванням з'єднання на попередньому рівні. Подальше закріплення смуг невизначенності можливе з врахуванням розташування об'єктів у блоках *1* і *2* (варіанти на рис.4.г,д).. Тобто розв'язок на *i*-му кроці обходу дерева пов'язаний з розв'язуванням окремих задач на (*i-1*)-му рівні дерева згортання. На рис.5 наведено приклад наведення внутрішніх смуг невизначеності при розгляді (*i-1*)-го рівня і зміни зовнішних для і-го рівня дерева згортання.

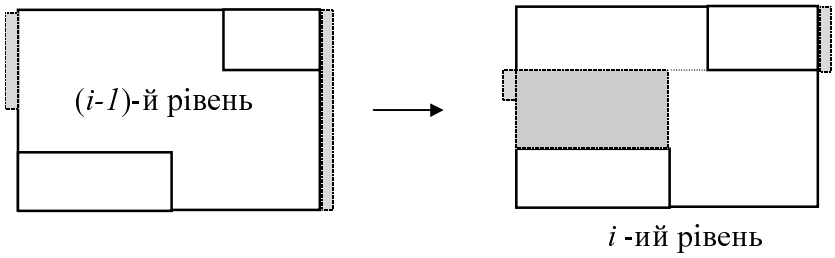

Рис.5. Смуги невизначеності МЗД

Подібна задача є на найнижчому рівні вершин дерева (рис.6). В результаті розв'язування задачі знаходження фрагменту МЗД у блоці позиції виходу назовні блоку можуть мати різний тип:

- повна смуга невизначеності зберігається,
- смуга невизначеності зменшується,
- смуга невизначеності перетворюється в лінію, оскільки зміни координат лінії в смузі приводить до збільшення довжини МЗД в блоці.

Такі рекурсивні процедури реалізуються для всіх вершин дерева згортання, що відповідають блокам бажаного рівня. На найнижчому рівні, коли блок містить три вершини, здійснюється побудова МЗД як фрагмента повного МЗД. Наприклад, (рис.7) можна побудувати декілька дерев, що задовольняють умові мінімальної ваги. Якщо вибрати дерево *а*, невизначеність на лівій і правій границях зникне. Дерево *б* підтримує невизначеність в межах довжин фрагмента *d* дерева.

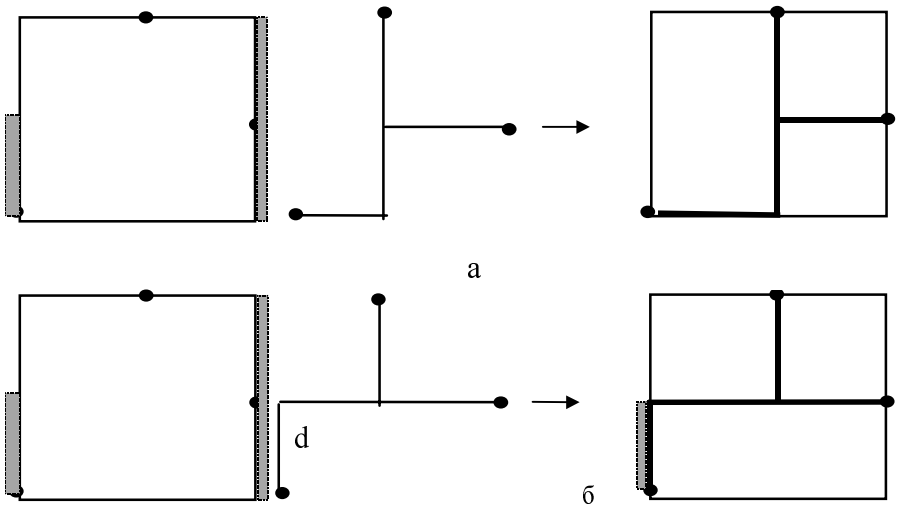

Рис.6. Побудова МЗД у найнижчому блоці

Зменшення невизначеності однієї границі приводить до зменшення невизначеності границі іншого блоку, що зменшує кількість варіантів МЗД у ньому. Приклад наведено на рис.7, в якому після побудови МЗД у правому блоці невизначеність зведеться до мінімуму (однієї лінії) і в сусідньому блоці вже будь-яке зв'язуюче з виходом назовні не є оптимальним. У випадку дерева, зображеного на рис.7, зона невизначеності зберігається протягом вертикального фрагмента дерева. Тоді у сусідньому блоці МЗД може бути побудоване оптимальним чином.

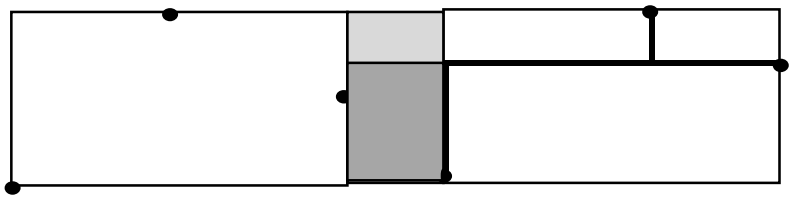

Рис.7. Побудова дерева з виходом назовні

Окремий випадок розглядається, якщо об'єднання блоків перетинається з іншим блоком (рис.8). При цьому розмірність задачі для знаходження фрагментів або смуг МЗД збільшується на одиницю.

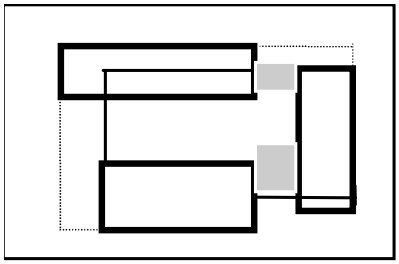

Рис.8. Перетин об'єднання блоків

Отже, при виборі стратегії побудови МЗД необхідно зберегти максимум можливих смуг невизначеності на всіх рівнях дерева згортання. При виборі стратегії знизу-догори подібний ефект не може бути досягнений через необхідність закріплення фрагментів

нижніх рівнів без врахування наступних міжблочних з'єднань. Підсумовуючи зазначені міркування, сформулюємо алгоритм побудови МЗД для всіх елементів на ДТРП.

Алгоритм Ш1 (декомпозиційний).

П1. Побудова дерева згортання елементів (контактів) ланцюга згідно з критеріями і обмеженнями на згортання.

П2. Побудова смуг невизначеності МЗД між блоками різних рівнів.

П3. Уточнення координат МЗД від блоків нижчих до блоків вищих рівнів.

Складність алгоритму визначається складністю алгоритму побудови дерева згортання $O(n^2)$ і складністю алгоритму побудови смуг невизначеності між блоками $O(n)$, який реалізований за допомогою двох способів: алгебраїчних перетворень і хвильового алгоритму. Приклади часової залежності алгоритму для різної кількості контактів наведено в наступній таблиці.

кількість	100	150	200	250	300
довжина	136	136	133	137	169
час	0.83 с.	2.74 с.	6.7 с.	11.53 с.	21.25 с.

1. A.B.Kahng and G. G.Robins. A new class of iterative steiner tree heuristics with goood perfomance. IEEE Transactions on Computer-Aided Design, vol.11, No.7, pp.893-902, July 1992.

2. Мельник Р.А. Розбиття схем на основі методу оптимального згортання з нечіткими характеристиками вершин дерева // Вісн. ДУ "Львівська політехніка". 1998, № 351, с.82-86.

УДК 621.378 : 681.3

Муравський Л.І., Кулинич Я.П., Вороняк Т.І.

Фізико-механічний інститут ім. Г.В. Карпенка НАН України, Львів

ОПТИКО-ЦИФРОВА СИСТЕМА ІДЕНТИФІКАЦІЇ ФАЗОВИХ МАСОК

На базі архітектури корелятора спільного перетворення Фур'є створено макет гібридної оптико-цифрової системи ідентифікації фазових та трансформованих фазових масок. Проведена оцінка мінімальних розмірів оптичної ланки системи. Наведена процедура ідентифікації трансформованих масок, що вводяться на вхід системи. Отримано і проаналізовано залежності співвідношення пік/шум для кореляційних піків, що формуються на виході системи, від ефективної фокусної віддалі оптичної ланки системи та від розмірів апертури реєстрації спільного енергетичного спектру.

Вступ. В останні роки досить суттєвими є досягнення у розвитку нових високоефективних методів оптичного захисту [1]. Серед нових методів слід виділити так званий метод охоронної перевірки, який забезпечує значно вищий рівень захисту кредитних карток, документів і виробів від підробки порівняно з відомими методами [2]. Цей метод