УДК 638.322

К.т.н, доцент Тесленко О. К., магістрант Гдуля Т. І.

**Національний технічний університет України
«Київський політехнічний інститут»**

МЕТОД ПОБУДОВИ ОБЧИСЛЮВАЛЬНОЇ ЛОГІЧНОЇ МЕРЕЖІ ДЛЯ РЕАЛІЗАЦІЇ ОПЕРАЦІЇ ДОДАВАННЯ ПО МОДУЛЮ

Abstract

Alexandr K. Teslenko, assoc. prof., PhD; Tanya Gdulya, student

Method of construction of logical computing network to implement the operations of adding on the module

This paper concerns the idea for minimization hardware resources for implementation of adder with the variable module which uses separate logical computing network to receive values for transfer without decreasing the speed of calculation. Significant reduction of hardware cost is achieved by maximizing the usage of shared computing units. The proposed method is very productive in terms of its future development.

Вступ

В сучасній комп'ютерній криптографії для обчислення хеш-функцій, реалізації кодерів та декодерів завадостійкого кодування по кодах Ріда-Соломона, а також для реалізації ряду криптографічних протоколів та перетворень (наприклад, алгоритму RSA), для процедур цифрового підпису широко застосовуються алгоритми на основі операцій над залишками чисел по модулю великої розрядності. Серед них базовою є операція додавання $(X+Y)\ modP$, де X,Y та P – цілі невід'ємні n-розрядні двійкові числа, $X,Y<P$.

У випадку створення спеціалізованих обчислювальних пристроїв для таких криптографічних перетворень, наприклад, на основі ПЛІС, має сенс розробка спеціальних апаратних реалізацій суматорів, що враховуватимуть конструкторсько-технологічні особливості проектування обчислювального пристрою та забезпечуватимуть максимальну його швидкодію. Одним з варіантів такої апаратної реалізації є використання одновимірних каскадів конструктивних модулів (ОККМ) [1]. В роботі [2] для суттєвого підвищення швидкості суматора запропоновано використання додаткової логічної мережі пірамідальної структури. Згідно з [2] схеми переносу в будь який i-тий ($i=0,1,\ldots,n-1$) розряд суматора по модулю можуть бути побудовані на основі одного і того ж базового

елемента, який реалізує асоціативну несиметричну операцію. Властивість асоціативності дозволяє на основі таких базових елементів створювати схеми переносу у вигляді двійкових дерев, листками яких є відповідним чином перекодовані значення розрядів чисел *X,Y* та *P*. Максимальна затримка сигналу переносу в такій логічній мережі пропорційна $]log_2(n-1)[$, де *]u[* – найближче більше ціле від *u* (якщо *u* – ціле, то *]u[=u*), що дозволяє підвищити швидкість виконання операції додавання багаторозрядних чисел по модулю на декілька порядків.

Постановка задачі

Безпосередня реалізація схем переносу в вигляді бінарних дерев для кожного з розрядів суматора по модулю призведе до значних апаратних витрат по кількості використаних базових асоціативних елементів. Потенційна можливість для зменшення апаратних витрат без зниження швидкості полягає у використанні спільних гілок різними частинами обчислювальної мережі для реалізації переносу як у молодші, так і у старші розряди. У [3] для перегляду всіх можливих дерев для реалізації переносу у відповідний розряд запропоновано метод, що базується на створенні повного дерева з наступним «обрізанням» зайвих гілок. Його недоліком є громіздкість, відсутність врахування часових відмінностей в реалізації переносу в різні розряди та неможливість знаходження оптимізованих (не гарантовано мінімальних) вирішень за рахунок скорочення часових затрат. Метою даної роботи є створення методу, який би був позбавлений вказаних недоліків.

Термінологія

КМ – конструктивний модуль.

ОККМ – одновимірний каскад конструктивних модулів.

Рівень вузла бінарного дерева – кількість вузлів у піддереві від кореня дерева до поточного вузла включно.

Особливості обчислювальної мережі у вигляді бінарного дерева

В подальшому будемо вважати, що будь який вузол дерева – суть базовий асоціативний елемент. Кількість первинних входів мережі дорівнює *n* (входи нумеруються від *0* до *n-1*). Кожен вузол (елемент) бінарного дерева має по три індекси – старший та молодший розряди чисел *X, Y, P*, що охоплюються даним вузлом, а також індекс, який вказує на рівень вузла в бінарному дереві. Враховуючи несиметричність

асоціативної операції, яку реалізує базовий елемент, до будь-якого вузла нижнього рівня можуть бути приєднані тільки такі два вузла верхніх рівнів, які мають суміжні індекси. Таким чином, вузол бінарного дерева можна подати в наступному вигляді *Node(l,a,b)*, де *l* – рівень вузла, *a* – номер старшого розряду, *b* – номер молодшого розряду чисел *X, Y, P*. Подання вузла у вигляді кортежу з трьох чисел $<l,a,b> = Node(l,a,b)$ однозначно визначає місце вузла в логічній мережі. Кількість $K_r(a,b)$ листків (розрядів) бінарного дерева, які охоплюються даним вузлом, визначається наступним чином: $K_r(a,b) = a-b+1$. Для узагальнення листки бінарного дерева також позначатимемо трійкою чисел $<l,a,a>$.

Опис методу

Для забезпечення мінімальної затримки сигналу переносу, кількість рівнів бінарних дерев логічної мережі не повинна перевищувати максимально допустимого рівня *L* логічної мережі. Спочатку будемо вважати, що $L =]log_2(n-1)[$, а також, що переноси в будь-який КМ ОККМ формуються виключно за допомогою логічної мережі.

На першому рівні логічної мережі мають місце наступні вузли (корені) бінарних дерев. Для переносу в старші розряди – $<1,j,0>$, $(j=n-2,n-3,...,1)$. Для переносу в молодші розряди –$<1,n-1,j>$, $(j=n-2,n-3,...,1)$. При цьому K_r може приймати значення з діапазону від 2 до $n-1$. Перехід на наступний вищий рівень полягає в розбитті діапазону розрядів, заданих числами *a* та *b* на дві суміжні частини. В загальному випадку може існувати не більше $K_r(a,b)$ таких розбиттів, тобто наступними вузлами для вузла $<1,a,b>$ можуть бути вузли $<2,a,a>$ та $<2,a-1,b>$, вузли $<2,a,a-1>$ та $<2,a-2,b>$, і т.д. до вузлів $<2,a,b+2>$ та $<2,b+1,b>$, і, врешті, $<2,a,b+1>$ та $<2,b,b>$. У випадках, коли $]log_2(K_r)[+1>L$ (тобто умова максимально допустимого рівня мережі не виконується), будь-який діапазон розбиття не повинен перевищувати значення $C=2^c$, де $c=[log_2(K_r)]$, $[u]$ – найближче менше ціле за *u* (якщо *u* – ціле, то $[u]= u-1$), тобто наступними вузлами для вузла $<1,a,b>$ можуть бути вузли $<2,a,a-C+1>$ та $<2,a-C,b>$, вузли $<2,a,a-C+2>$ та $<2,a-C+1,b>$, і т.д. до вузлів $<2,a,b+C>$ та $<2,b+C-1,b>$. Суть полягає в тому, щоб кількість рівнів бінарного дерева не перевищувала *L*, тобто $K_r(2,a,a-C+i) \le C$ та $K_r(2,a-C+i-1,b) \le C$ для всіх можливих *i* з ряду 1,2,3… В даному випадку існує $2C-K_r(a,b)+1$ варіантів розбиття діапазону між *a* та *b*. Із викладеного випливає перехід від *l*-го рівня до $l+1$ рівня логічної мережі. Позначимо $B(l,a,b)$ кількість варіантів розбиття діапазону вузла на *l* – тому рівні мережі. Тоді $B(l,a,b) = K_r(a,b) = a-b+1$, якщо $c + l \le L$, та $B(l,a,b)=2C-K_r(a,b)+1$ в іншому випадку. Таким чином, суть методу полягає в перегляді всіх варіантів розбиття діапазонів на всіх

рівнях логічної мережі та виявлення збігів діапазонів на одному і тому ж рівні.

Запропонований метод є досить продуктивним у відношенні його розвитку. Одним із напрямків такого розвитку є подальше зменшення кількості базових асоціативних елементів шляхом реалізації за допомогою логічної мережі переносів не у всі КМ, а в деяку послідовність вибраних КМ. Перенос в невибрані КМ виконується схемами згідно з [1]. Відмітимо, що в результаті деякого вибору таких послідовностей буде уточнено значення *L*, а метод залишається в силі. Окрім того, розглянутий метод дозволяє формувати різноманітні евристичні алгоритми, які значно зменшують об'єм обчислень та дозволяють одержувати результати, близькі до оптимальних.

Висновок

Запропонований метод використовує фактично одну операцію – розбиття діапазону чисел на два піддіапазони, за допомогою якої можна створювати моделі різноманітних логічних мереж у вигляді об'єднань бінарних дерев. Це значно зменшує трудомісткість знаходження логічних мереж, оптимізованих по заданих критеріях.

Метод має значний потенціал у плані його подальшого розвитку, зокрема, визначення оптимізованої послідовності вибраних КМ.

.

Література

1. *Тарасенко В.П.*, *Тесленко О.К.* Реалізація основних арифметичних операцій над залишками на одномірних каскадах конструктивних модулів. Управляющие системы и машины, 2003, № 3(185), С.29-42.
2. *Тарасенко В.П., Тесленко А.К.* Быстродействующие многоразрядные сумматоры по переменному модулю . Материалы международной научно-практической конференции «Инфомационные технологии и информационная безопасность в науке, технике и образвании "ИНФОТЕХ-2007"» СевНТУ, 2007.
3. *Тесленко О.К., Узерчук О.А.* Оптимізація структур швидкодіючих багаторозрядних суматорів за змінним модулем.// І наукова конференція магістрантів та аспірантів «Прикладна математика та комп'ютинг» ПМК-2009, Київ, 15-17 квітня 2009 р. Збірник тез доповідей с.280-284