УДК 004.31:681.5
DOI: 10.15587/1729-4061.2020.194342

Синтез быстродействующих устройств цифровой обработки сигналов на основе теоретико-числовых преобразований

А. В. Ивашко, И. Г. Либерг, Д. А. Лунин

Запропоновано вибір модулів спеціального виду і відповідних їм первісних коренів, які допускають спрощену структуру арифметичних пристроїв, із застосуванням теоретико-числових перетворень. Розроблено метод визначення модулів, що забезпечує мінімальне число арифметичних операцій при виконанні операцій додавання і множення за модулем. Розроблено і промоделювано структури суматорів за модулями спеціального виду, що дозволяють максимально швидко виконувати операцію складання. Синтезовані і протестовані суматори за модулями чисел Ферма, Мерсенна і Голомба, які можна застосувати в арифметичних блоках швидкодіючих кореляторів і фільтрів.

Обчислення кореляцій і згорток в реальному часі стає досить трудомістким завданням у разі довгих вхідних послідовностей. Для вирішення цього завдання доцільно застосувати так звані швидкі алгоритми. Однак це вимагає високої продуктивності обчислювача згорток і кореляцій, які часто перевищують можливості сучасної обчислювальної техніки. Тому запропонована методика визначення модуля і розроблені структурні схеми суматорів за модулями спеціального виду, дозволяють прискорити обчислення кореляцій і згорток з використанням теоретико-числових перетворень.

Так як операція множення за модулем виконується за допомогою операцій додавання і зсуву, то трудомісткість розрахунку теоретико-числових перетворень в значній мірі залежить від кількості одиниць в двійковому поданні ступенів первісного кореня. Операція множення, як правило, зводиться до багаторазового складання чисел, то складність і швидкодія арифметичних пристроїв для теоретико-числових перетворень визначається характеристиками суматорів за модулем.

Запропонований метод проектування обчислювальних модулів для цифрових пристроїв обчислення кореляції і згортки на основі швидких теоретико-числових перетворень забезпечує спрощену апаратну і програмну реалізацію цих структур, що призводить до високошвидкісної обробки сигналів і зображень

Ключові слова: автокореляційна функція, кореляція, згортка, програмовані логічні інтегральні схеми, дискретне перетворення Фур'є

Не є перевиданням

1. Введение

Задачи оценивания корреляционных функций и вычисления сверток возникают в различных областях цифровой обработки сигналов. Расчет автокорреляционных функций (АКФ) и взаимнокорреляцинных (ВКФ) может быть необходим при обработке изображений, в радарных или гидроакустических уста-

новках для дальнометрии и пеленгации, при расчете спектра сигналов и во многих других областях.

Вычисление корреляций и сверток в реальном времени становится достаточно трудоемкой задачей в случае длинных входных последовательностей. Для решения этой задачи целесообразно применить так называемые быстрые алгоритмы. Однако это требует высокой производительности вычислителя сверток и корреляций, которые зачастую превышают возможности современной вычислительной техники.

Эта задача может быть решена путем аппаратной реализации на основе программируемых логических интегральных схем (ПЛИС). Известны примеры аппаратной реализации процессоров корреляции и свертки на ПЛИС [1]. Однако они не в полной мере используют возможности математических методов ускорения вычислений.

Для обеспечения максимального быстродействия процессоров цифровой обработки сигналов необходимо, с одной стороны, оптимизировать алгоритмы вычисления сверток и корреляций, с другой – разработать структуры высокоскоростных арифметических блоков для таких процессоров.

2. Анализ литературных данных и постановка проблемы

Расчет свертки и корреляционных функций требует числа сложений и умножений, пропорционального N^2, где N – длина обрабатываемой последовательности. Такой объем может быть недопустимо велик при обработке сигналов в реальном масштабе времени, поэтому были предложены более быстрые алгоритмы расчета свертки и корреляции. Один из таких методов [2] предполагает вычисление вычисления дискретного преобразования Фурье (ДПФ) последовательностей перемножения коэффициентов полученных ДПФ и вычисления обратного ДПФ полученной последовательности. Однако при вычислении ДПФ последовательностей неизбежно появление комплексных иррациональных значений, что приводит к усложнению вычислений, так как необходимо производить вычисления, как над вещественной, так и над мнимой частью числа.

Другой подход основан на ТЧП [3], которые аналогичны ДПФ и обладают свойством свертки, но коэффициенты которых принимают только целые значения, не превышающие некоторого максимального значения. ТЧП последовательности x_i, i=0…N–1 определяется следующим образом:

$$X_k = \sum_{i=0}^{N-1} x_i \cdot g^{ik} \left(\mathrm{mod}\, p\right), \tag{1}$$

где модуль p и длина последовательности N не имеют общих сомножителей, а g выбирается так, чтобы выполнялось условие:

$$g^N = 1\left(\mathrm{mod}\ p\right). \tag{2}$$

Только для ознакомления

В частности, для любого простого p существует вариант, когда $N=p-1$, а g – так называемый первообразный корень.

Анализ методов нахождения сверток и АКФ с помощью ТЧП показывает, что основными арифметическими операциями, которые необходимо выполнить, являются сложение и умножения по выбранному простому модулю, то есть вычисления остатка от результата выполнения арифметических операций. Для произвольного модуля эти операции достаточно трудоемки, поэтому представляют интерес некоторые модули специального вида, для которых операция сложения по модулю выполняется существенно проще [4].

В качестве простых модулей p применяются, в частности, так называемые числа Мерсенна вида $p=2^n-1$, где n – простое.

Арифметика по модулю чисел Мерсенна описана в работах [5, 6]. Однако в этих работах лишь приводятся теоретические основы модульной арифметики и отсутствуют схемы сумматоров и умножителей, на основе которых могут быть построены специализированные ПЛИС и БИС.

Также удобны с точки зрения снижения аппаратных затрат модули вида $p = 2^{2^t} + 1$, известные как числа Ферма [7]. Аналогично методике для чисел Мерсенна, разряд с весом 2^n представляет величину сравнимую с -1 по модулю p. Поэтому при сложении, разряд переноса с весом 2^n вычитается из младших разрядов [8]. Таким образом, представляет интерес поиск простых модулей p для ТЧП, не являющихся числами Мерсенна и Ферма и обеспечивающих упрощение вычислений этих преобразований.

Отметим также, что мало внимания уделено вопросам аппаратной реализации таких модулей. В работах [9, 10] приведены примеры реализации сумматоров и умножителей для некоторых модулей, однако остался открытым вопрос синтеза структур модулей, применимых ко всем видам ТЧП и достаточно легко реализуемые на ПЛИС.

3. Цель и задачи исследования

Целью работы является разработка методов выбора параметров ТЧП и синтеза арифметических блоков, обеспечивающих ускоренную аппаратную и программную реализацию.

Для достижения поставленной цели необходимо решить следующие задачи:

– исследовать возможности для выбора модулей специального вида и соответствующих им первообразных корней с целью проведения быстрых ТЧП, которые допускают упрощенную структуру арифметических устройств;

– разработать метод определения модулей, обеспечивающих минимальное число арифметических операций при выполнении операций сложения и умножения;

– разработать структуры сумматоров по модулям специального вида, позволяющие максимально быстро выполнять операцию сложения, и оценить эффективность их реализации путем моделирования.

Не для перепечатки

4. Выбор модулей специального вида для ТЧП

При выборе таких параметров ТЧП (1), как размерность преобразования N, простой модуль p и первообразный корень g возникает ряд трудно совместимых требований. Так, для применения так называемых быстрых алгоритмов вычисления ТЧП целесообразно, чтобы размерность преобразования была степенью двойки $N=2^n$. Для упрощения сложения и умножения модуль должен иметь специальный вид, например $2^n\pm1$.

Помимо рассмотренных выше чисел Ферма и Мерсенна, количество которых невелико, могут быть рассмотрены модули

$$p=p_1\cdot p_2+1=(2^a-1)\cdot 2^b+1, \qquad (3)$$

которые также допускают простую аппаратную и программную реализацию ТЧП размерности 2^n.

Частным случаем модулей $p=p_1\cdot p_2+1=(2^a-1)\cdot 2^b+1$ являются модули $p=3\cdot 2^n+1$, известные как числа Голомба [11, 12].

При помощи разработанной программы в среде Matlab были проанализированы все модули вида (3) для a=2..15, b=8..18. Составные модули исключались из рассмотрения, а для каждого из простых производился поиск первообразного корня и проверка, удовлетворяет ли он условию (2).

Выделенные таким образом простые модули вида $p=p_1\cdot p_2+1=(2^a-1)\cdot 2^b+1$, а также соответствующие им длины последовательностей N и первообразные корни g, сведены в табл. 1.

Таблица 1

Простые модули вида $p=(2^a-1)\cdot 2^b+1$

N	a	b	p_1	p_2	p	g
262144	2	18	3	262144	786433	5
65536	1	16	1	65536	65537	3
16384	3	14	7	16384	114689	15
16384	6	14	63	16384	1032193	94
4096	2	12	3	4096	12289	41
4096	4	12	15	4096	61441	19
4096	7	12	127	4096	520193	71
1024	4	10	15	1024	15361	84
1024	6	10	63	1024	64513	21
512	4	9	15	512	7681	62
256	1	8	1	256	257	3
256	2	8	3	256	769	7
256	5	8	31	256	7937	71

Следует отметить, что полученные модули могут использоваться для вычисления ТЧП не только указанной в табл. 1 размерности N, но и меньших сте-

Тільки для читання

пеней двоек. Например, по модулю 61441 может вычисляться ТЧП не только размерности 4096, но и 2048, 1024, 512 и т. д.

Таким образом, значительно расширяется число простых модулей, допускающих упрощенное выполнение сложения и умножения. Так, для случая N=1024 можно выявить целый ряд модулей с числом двоичных разрядов m<20. Кроме известных чисел Ферма 65537, Мерсенна 8191, 131071, 524287 и Голомба 12289, 786433 дополнительно предложено использовать модули 114689, 1032193, 61441, 52019, 15361, 64513.

5. Метод определения модулей, обеспечивающих минимальное число арифметических операций

Так как операция умножения по модулю выполняется с помощью операций сложения и сдвига, то трудоемкость расчета ТЧП в значительной степени зависит от количества единиц в двоичном представлении степеней первообразного корня g. Для ряда значений размерности преобразований N перебирались различные простые модули p и соответствующие им первообразные корни g из табл. 1. Для каждого из возможных модулей была произведена оценка сложности расчета ТЧП по формуле (1) путем подсчета единиц в двоичном представлении степеней первообразного корня g и выбраны те модули и первообразные корни, для которых суммарное число единиц минимально.

Результаты вычислений для часто используемой в обработке сигналов размерности N=1024 приведены в табл. 2.

Таблица 2

Простые модули и соответствующее им число сложений в ТЧП

Модуль p	12289	15361	61441	64513	114689
Число сложений A	29785	28968	32555	33067	33799

Анализ табл. 2 показывает, что минимальный объем вычислений при расчете быстрого ТЧП обеспечивают значения модуля p=15361. Проанализировав табл. 1, определим первообразный корень, как g=84. При этом неверный выбор модуля может потребовать на 17 % вычислений больше. Аналогично, можно найти для любой размерности N и модуля p минимальное число сложений ТЧП.

6. Структуры сумматоров по модулю для ТЧП

Для быстрого вычисления корреляций и сверток при помощи ТЧП необходимо разработать основные «строительные блоки» процессоров ТЧП – сумматоры и умножители по модулю. Поскольку операция умножения, как правило, сводится к многократному сложению чисел, можно утверждать, что сложность и быстродействие арифметических устройств для ТЧП определяется характеристиками сумматоров по модулю.

На рис. 1 представлена предложенная схема сумматора по модулю чисел вида 2^m-1, например, чисел Мерсенна.

Не к печати

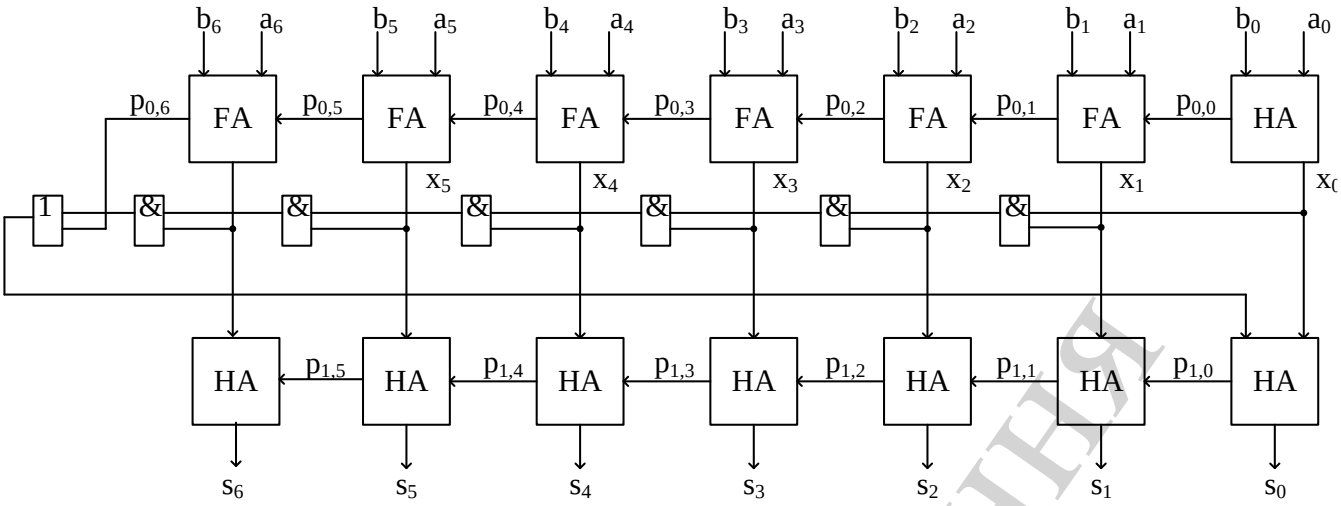

Рис. 1. Структурная схема сумматора по модулю 127

Схема обеспечивает суммирование семиразрядных двоичных чисел по модулю 127.

На схеме блок FA представляет собой полный сумматор с тремя входами: a, b и p_{-1} – входом переноса от предыдущего каскада, а также двумя выходами: s – сумма и p – выходным переносом; блок HA – полусумматор с двумя входами – a и b, и двумя выходами: s – сумма и p – выходным переносом [13].

В схеме обеспечено суммирование разряда переноса с весом 2^n и младшего значащего разряда. Также предусмотрена коррекция результата в случае, если сумма входных значений равна модулю.

Схема сумматора по модулю чисел вида 2^m+1, например чисел Ферма представлена на рис. 2. Изображенный сумматор обеспечивает суммирование девятиразрядных двоичных чисел по модулю 257.

Аналогично, описанной выше методике разряд с весом 2^n представляет величину сравнимую с –1 по модулю p. Поэтому при сложении разряд переноса с весом 2^n вычитается из младших разрядов.

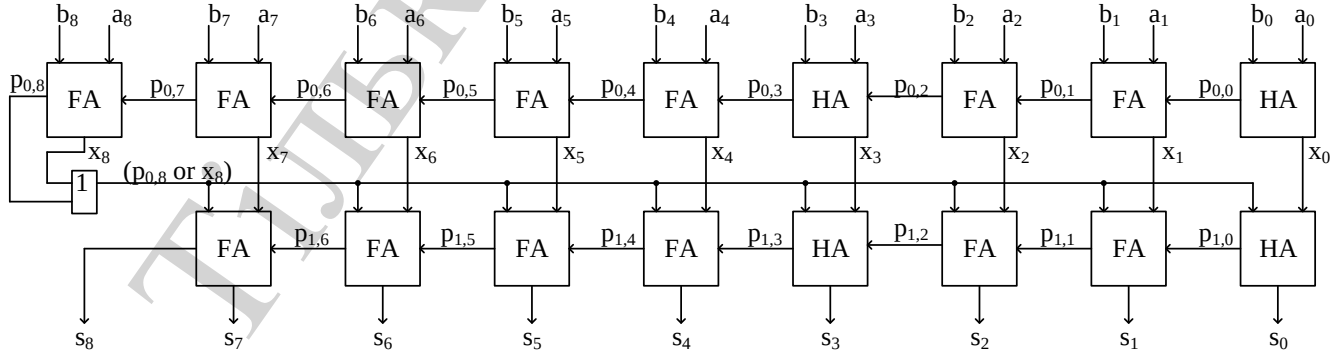

Рис. 2. Структурная схема сумматора по модулю 257

Наибольший интерес представляет разработка сумматоров по модулям $p=p_1 \cdot p_2+1=(2^a-1)\cdot 2^b+1$, обеспечивающих более широкий выбор размерностей ТЧП и диапазонов значений операндов и результатов.

ТОЛЬКО ДЛЯ ЦИТИРОВАНИЯ

Рассмотрим, в частности, сумматор по модулю чисел Голомба, для которых $a=2$, $p=3\cdot 2^n+1$.

Результаты арифметических действий по модулю $p=3\cdot 2^n+1$, могут быть легко приведены к остаткам, если учесть, что $4\cdot 2^n$ сравнимо с (2^n-1) по модулю $3\cdot 2^n+1$. Поэтому при сложении, разряд переноса с весом $4\cdot 2^n$ формирует значение, состоящее из n единичных бит. Далее это сформированное значение необходимо сложить с n – младшими разрядами получившейся суммы. В результате получается сумма по модулю $p=3\cdot 2^n+1$.

В случае, если при сложении, получается разряд переноса равный нулю, необходимо произвести дополнительную обработку результата вычисления. Для этого следует просуммировать $(n-1)$ – младших бит полученной суммы, а потом умножить их на два бита с весом 2^n и 2^{n+1} и логически сложить с битом переполнения, который имеет вес 2^{n+2}. Полученный бит далее суммируется с каждым из n-младших разрядов полученной суммы.

Структурная схема сумматора по модулю чисел Голомба, основанная на приведенных выше рассуждениях, приведена на рис. 3.

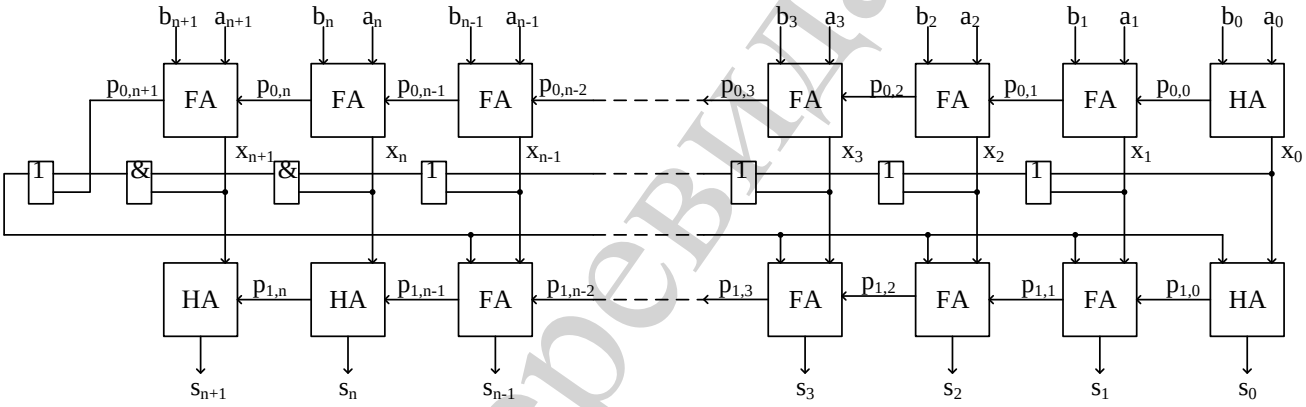

Рис. 3. Структурная схема сумматора по модулю $p=3\cdot 2^n+1$

Все приведенные выше структуры были промоделированы и протестированы в среде Active-HDL ver.9.1, что доказало их работоспособность и возможность построения процессоров ТЧП на основе ПЛИС или специализированных БИС.

На рис. 4 приведена VHDL модель сумматора по модулю числа Мерсенна $8191=2^{13}-1$, на рис. 5 – временные диаграммы работы сумматора.

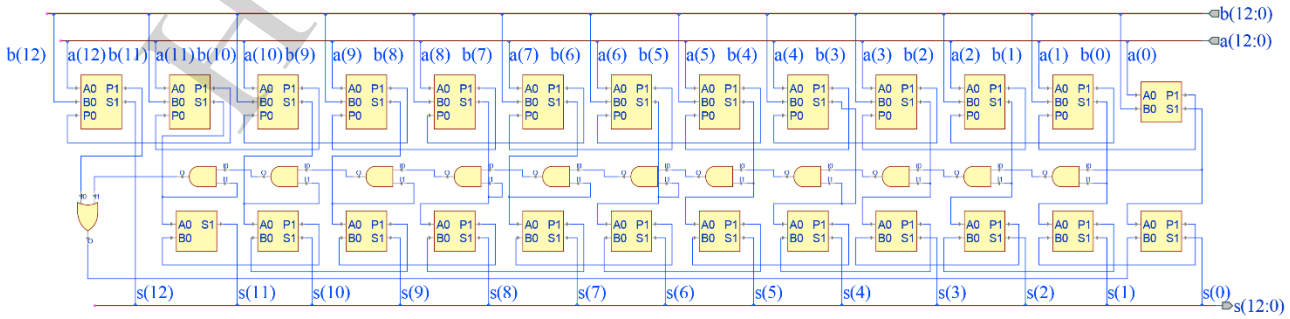

Рис. 4. Модель сумматора по модулю 8191

Не для печати

Рис. 5. Результаты моделирования сумматора по модулю 8191

7. Обсуждение результатов исследования методов ускорения ТЧП

В известных работах рассматриваются лишь модули вида чисел Ферма, Мерсенна и Голомба. Путем применения методов теории чисел в работе удалось в два раза и более увеличить число модулей для теоретико-числовых преобразований (табл. 1). Такое расширение номенклатуры модулей позволяет, с одной стороны, более гибко подстраивать параметры процессора ТЧП под конкретные требования к точности и быстродействию, с другой – ускорять вычисление сложений по модулю.

Кроме того, в известных публикациях мало внимания уделялось виду первообразного корня. Анализ возможных модулей и первообразных корней позволил выбрать те из них, которые обеспечивают упрощение операций возведения в степень и умножения (табл. 2).

Удалось также для широкого спектра модулей, не рассматриваемых в известных публикациях, разработать схемы быстродействующих сумматоров по модулю, легко реализуемых на ПЛИС и специализированных БИС.

Таким образом, проведенные исследования позволили достичь повышения быстродействия устройств вычисления ТЧП благодаря применению, с одной стороны, методов теории чисел, с другой – современных методов синтеза и моделирования цифровых устройств.

Вместе с тем, подбор модулей происходил до некоторой степени эмпирически. Возможно, лучших результатов можно было бы достичь, применив при выборе модулей такой алгебраический аппарат, как поля Галуа и групповые характеры.

Кроме того, в работе не приведены схемы сумматоров по модулю $p=(2^a-1)\cdot 2^b+1$ для случая a>2, то есть по модулю обобщенных чисел Голомба.

В дальнейшем целесообразно синтезировать такие схемы и, по возможности, разработать программные средства для синтеза сумматоров и умножителей по всем возможным модулям специального вида. Эта задача, однако, может потребовать объема вычислений, лежащего на грани возможностей современной вычислительной техники.

Следует также произвести теоретические и экспериментальные оценки быстродействия предложенных структур в зависимости от используемой элементной базы.

8. Выводы

1. Предложена методика выбора оптимальных модулей для вычисления ТЧП, которая в два раза и более увеличить число модулей для ТЧП, а также более гибко подстраивать параметры процессора ТЧП под конкретные требования к точности и быстродействию.

Тільки для читання

2. Предложена методика анализа параметров ТЧП и выбора первообразных корней, позволяющая на 15–20 % ускорить вычисление корреляций и сверток с использованием ТЧП. Предложена методика и разработаны алгоритмы и программы анализа первообразных корней ТЧП, позволяющие ускорить вычисление корреляций и сверток с использованием ТЧП.

3. Синтезированы и протестированы быстродействующие сумматоры по предложенным модулям, которые могут послужить основой для арифметических блоков быстродействующих корреляторов и фильтров.

Литература

1. Ortega Cisneros, S., Rivera D., J., Moreno Villalobos, P., Torres, C., C. A., Hernandez-Hector, H., Raygoza, P., J. J. (2015). An image processor for convolution and correlation of binary images implemented in FPGA. 2015 12th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE). doi: https://doi.org/10.1109/iceee.2015.7357987

2. Ito, I. (2013). A Computing Method for Linear Convolution and Linear Correlation in the DCT Domain. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E96.A (7), 1518–1525. doi: https://doi.org/10.1587/transfun.e96.a.1518

3. Valencia, F., Khalid, A., O'Sullivan, E., Regazzoni, F. (2017). The design space of the number theoretic transform: A survey. 2017 International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS). doi: https://doi.org/10.1109/samos.2017.8344640

4. Zhang, J., Li, S. (2009). Data-recovery algorithm and circuit for cyclic convolution based on FNT. IEICE Electronics Express, 6 (14), 1019–1024. doi: https://doi.org/10.1587/elex.6.1019

5. Boussakta, S., Hamood, M. T., Rutter, N. (2012). Generalized New Mersenne Number Transforms. IEEE Transactions on Signal Processing, 60 (5), 2640–2647. doi: https://doi.org/10.1109/tsp.2012.2186131

6. Campbell, K., Lin, C.-H., Chen, D. (2018). Low-cost hardware architectures for mersenne modulo functional units. 2018 23rd Asia and South Pacific Design Automation Conference (ASP-DAC). doi: https://doi.org/10.1109/aspdac.2018.8297388

7. Toivonen, T., Heikkila, J. (2006). Video filtering with Fermat number theoretic transforms using residue number system. IEEE Transactions on Circuits and Systems for Video Technology, 16 (1), 92–101. doi: https://doi.org/10.1109/tcsvt.2005.858612

8. Zhang, J., Li, S. (2009). High Speed Parallel Architecture for Cyclic Convolution Based on FNT. 2009 IEEE Computer Society Annual Symposium on VLSI. doi: https://doi.org/10.1109/isvlsi.2009.10

9. Kumar, S., Chang, C.-H. (2017). A Scaling-Assisted Signed Integer Comparator for the Balanced Five-Moduli Set RNS {2n - 1, 2n, 2n + 1, 2n+1 - 1, 2n-1 - 1}. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 25 (12), 3521–3533. doi: https://doi.org/10.1109/tvlsi.2017.2748984

10. Efstathiou, C., Vergos, H. T., Nikolos, D. (2003). Modulo 2n ±1 adder design using select-prefix blocks. IEEE Transactions on Computers, 52 (11), 1399–1406. doi: https://doi.org/10.1109/tc.2003.1244938

11. Golomb, S. W., Reed, I. S., Truong, T. K. (1977). Integer Convolution over Finite Field GF(3·2n + 1). SIAM Journal on Applied Mathematics, 32 (2), 356–365. doi: https://doi.org/10.1137/0132029

12. Чернов, В. М., Корепанов, А. О. (2006). Теоретико-числовые преобразования в задачах цифровой обработки сигналов. Самара, 112.

13. Baozhou, Z., Ahmed, N., Peltenburg, J., Bertels, K., Al-Ars, Z. (2019). Diminished-1 Fermat Number Transform for Integer Convolutional Neural Networks. 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA). doi: https://doi.org/10.1109/icbda.2019.8713250

Тільки для читання