УДК 681.3

В.И. Барсов

Украинская инженерно-педагогическая академия, Харьков

ПРИМЕНЕНИЕ ПОЛИНОМИАЛЬНОЙ МОДУЛЯРНОЙ СИСТЕМЫ СЧИСЛЕНИЯ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СЕТИ ПАКЕТНОЙ ПРЕРЫВИСТОЙ СВЯЗИ

Рассматривается возможность применения методов обработки информации в полиномиальной модулярной системе счисления при создании сети пакетной связи использующей метеорные радиоканалы для повышения тактико-технических характеристик сети.

Ключевые слова: *метеорный радиоканал, полиномиальная модулярная система счисления, обработка информации.*

Введение

Постановка задачи. Устойчивое управление структурными элементами сложного пространственно разнесённого технического комплекса предполагает наличие эффективной системы обработки и передачи разнородной информации между субъектами процесса управления. Одно из решений данной задачи может быть получено путём применения, для организации каналов передачи команд управления и получения донесений, в качестве резерва, сети пакетной связи использующей метеорные радиоканалы (СПСМРК). Такая сеть может иметь комбинированную иерархическую структуру, совпадающую с соответствующей структурой информационно управляющей системы (ИУС). Для повышения надёжности и оперативности обмена данными в сети целесообразно также рассмотреть возможность применения и дейтаграмного метода (использование набора параллельных виртуальных каналов). Специфика прерывистого метеорного радиоканала (МРК) способствует устранению основного недостатка присущего дейтаграмному способу передачи пакетов – неустойчивости, вызванной колебаниями при выборе оптимального маршрута. Приемлемым, в рассматриваемом случае, может оказаться асинхронно сбалансированный режим работы сети, позволяющий организовать дуплексные каналы связи и возможность работы каждой станции, при необходимости, в режиме первичной либо вторичной.

С позиции теории массового обслуживания рассматриваемую модель СПСМРК можно представить как совокупность графов типа M/G/1, объединённых по принципу одноуровневой централизации. Практически получаем систему массового обслуживания смешанного типа с ограничением по времени нахождения пакета в очереди, что определяется старением оперативной информации. Перерывы в работе обслуживающего устройства имеют случайную длительность, определяемую прерывистым характером и рабочим циклом МРК. В рассматриваемом случае природа распределения вероятностей длительности обслуживания μ зависит от специфических особенностей МРК связанных с сезонными и суточными колебаниями числа метеорных вспышек, а также длительностью существования метеорных следов. Граф возможных состояний и переходов, для одного направления, исследуемой СПСМРК, с учётом возможности использования одного транзитного узла представлен на рис. 1, где параметр λ характеризует интенсивность поступления информационных пакетов подлежащих передаче, а параметр ν – очередь пакетов подлежащих передаче. S_i – состояния канала, определяемые заявками на обслуживание связанными с системой.

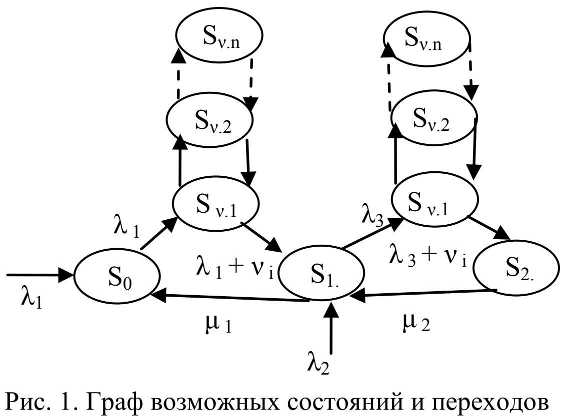

Рис. 1. Граф возможных состояний и переходов

Как известно на эффективность функционирования СПСМРК существенно влияют следующие две характеристики: пропускная способность и средняя задержка пакета, что вызвано специфическими особенностями МРК, такими как прерывистый характер, ограниченная длительностью сеанса связи, низкая скорость передачи данных, низкая помехо и отказоустойчивость.

Точный баланс между пропускной способностью и средней задержкой пакета устанавливается, реализуемым информационно управляющей системой, алгоритмом управления потоками, что определяет повышенные требования к ней по производительности и устойчивости к отказам, вызванным как неисправностями или сбоями в работе оборудования, так и ошибками, возникающими при обработке информации. Поиск и исследование путей повышения производительности ИУС, в данном случае функционирующей в составе СПСМРК, без снижения отказоустойчивости, показал, что с одной стороны в пределах позиционной системы счисления (ПСС) этого добиться практически невозможно, без существенного ухудшения основных характеристик ИУС. ПСС обладает существенным недостатком - наличием межразрядных связей, что не позволяет кардинально улучшить такие характеристики ИУС как производительность, достоверность и отказоустойчивость. Также наличие межразрядных связей является причиной невозможности распараллелить решаемые алгоритмы на уровне элементарных операций и значительно увеличивает длительность выполнения операций[1, 2].

Проведенные в рассматриваемом направлении исследования, как отечественными, так и зарубежными учеными показали перспективность применения при создании специализированных систем управления и связи непозиционной модулярной системы счисления (МСС) [1, 2].

Необходимо отметить, что многие алгоритмы приложений МСС базируются на вычислительных процедурах ортогональных преобразований и свертках, когда исходные последовательности дискретных отчетов $x_i(nT)$ представляются в полиномиальной форме. Такие процедуры в полиномиальной модулярной системе счисления (ПМСС) выполняются с высокой скоростью и точностью при относительно небольшом динамическом диапазоне вычислений и использовании только арифметических операций умножения и сложения. Поэтому ПМСС нашла широкое применение в области цифровой обработки сигналов, где успешно реализуются алгоритмы, основанные на процедуре умножения с накоплением, это: цифровая фильтрация, спектральный анализ с использованием ортогональных преобразований, дискретное и быстрое преобразование Фурье, умножение векторов, вектора на матрицу, перемножение матриц и др. Рассматривая вопрос создания высокоскоростных и отказоустойчивых ИУС необходимо также отметить потенциальные возможности ПМСС в решении задач контроля и коррекции ошибок в процессе функционирования вычислительного комплекса, без остановки процесса обработки информации, что обусловлено основными свойствами МСС [1, 2].

Цель работы – показать, что предлагаемый подход позволяет найти новые, интересные решения рассматриваемой научно-технической задачи, а использование ПМСС, при создании специализированной информационно-управляющей системы СПСМРК, может улучшить её тактико-технические характеристики. при существенно меньших, чем для ИУС в ПСС, дополнительных аппаратных и массово-габаритных затратах.

Основная часть

Повышение эффективности применения СПСМРК тесно связано с решением задачи увеличения рабочего цикла и как следствие пропускной способности МРК, которые в значительной степени зависят от уровня насыщенности метеорного следа. При решении данной задачи, в зависимости от изменения, в течение сеанса связи, насыщенности метеорного следа, может быть полезной способность устройств обработки информации (УОИ), функционирующих в МСС выполнять обменные операции между достоверностью и производительностью (скоростью решения конкретных задач) в динамике процесса обработки информации. Варьируя количеством информационных и контрольных оснований, можно добиться требуемых значений основных показателей качества функционирования процессора ИУС. Количество и величины контрольных оснований $\left\{p_i^r(z)\right\}$ ПМСС определяются в зависимости от принятой математической модели отказоустойчивости вычислительного устройства.

Решение многих прикладных задач осуществляется в реальном масштабе времени, что не позволяет возвращаться назад и исправлять появляющиеся ошибки. Поэтому способность устройств обработки информации в МСС выполнять контроль, диагностику и исправление ошибок, без остановки процесса обработки информации, обеспечивая тем самым возможность своевременного обнаружения отказов, сбоев и других причин появления ошибочных результатов также является полезным свойством ПМСС.

Равноправность остатков является основным свойством ПМСС позволяющим строить коды, способные обнаруживать и корректировать ошибки в процессе реализации арифметических операций. Это обусловлено, прежде всего, тем, что каждый остаток модулярного кода несёт информацию обо всём исходном операнде. Отправной точкой в построении корректирующих модулярных кодов является независимость обработки данных по основаниям. Отсутствие взаимосвязи между вычислительными трактами УОИ ПСКВ не позволяет ошибкам перемещаться по другим основаниям. При этом изменение кратности ошибки не приводит к размножению ошибки как между разрядами внутри основания, так и от одного основания к другому. Важно также отметить, что существование особых структурных закономерностей в строении кодов ПМСС, обеспечивает возможность реальной реализации таких кодов.

Адекватные математические модели обработки данных в МСС, ориентированных на реализацию отказоустойчивых ИУС предполагает применение соответствующего математического аппарата и определяет структуру ИУС (рис. 2).

Малоразрядность обрабатываемых данных в МСС в значительной мере повышает производительность системы. Однако необходимость осуществления непозиционных операций несколько снижает значение данного показателя.

В частности наличие операции деления при выполнении процедуры определения остатков является основным сдерживающим фактором широкого применения нетрадиционной арифметики.

Операция деления является одной из основных немодульных процедур при реализации прямого преобразования позиционных кодов в код ПМСС расширенного поля Галуа. Однако операция деления не входит в состав алгебраических операций определяемых в кольце полиномов $Z_{P_{\text{олн}}}$, образованного декартовым произведением колец $Z_{p_1}, Z_{p_2}, ..., Z_{p_n}$ порожденных простыми минимальными многочленами.

Как известно, представление операнда в позиционном счислении определяется следующим образом

$$A(z) = a_r z^r + a_{r-1} z^{r-1} + ... + a_1 z + a^0,$$

где a_j – элементы поля GF(2), $j = 0,…,r$.

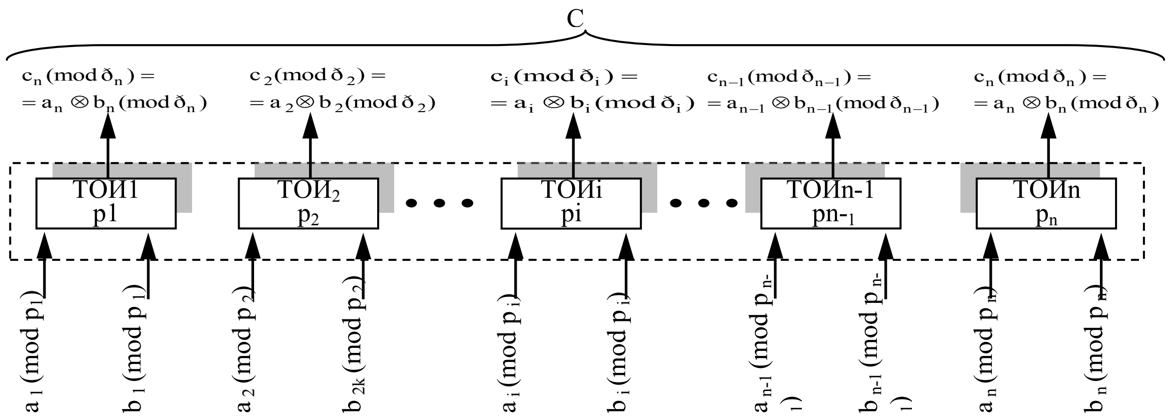

Рис. 2. Структурная схема УОИ в МСС

Для перевода из позиционной системы счисления в непозиционную, заданную взаимно простыми основаниями $p_1(z), p_2(z), ..., p_n(z)$, необходимо выполнить операции деления на модули $p_i(z)$, $i = 1, 2, ..., n$. Остаток $\alpha_i(z)$ в этом случае получается следующим образом

$$\alpha_i(z) = A(z) - [A(z)/p_i(z)] p_i(z),$$

где $[A(z)/p_i(z)]$ – наименьшее целое от деления $A(z)$ на основание $p_i(z)$.

Также можно осуществлять преобразование исходного $A(z)$, заданного в расширенном поле $GF(p^v)$, в ПМСС с помощью набора констант, являющихся эквивалентами степеней оснований 2^i и коэффициентов при соответствующих степенях оснований a_i, представленных в ПМСС. В этом случае перевод из позиционного двоичного кода в полиномиальную МСС осуществляется следующим образом:

$$\alpha_i(z) \equiv A(z) \bmod p_i(z) = \sum_{l=0}^{k} a_1(z) z^l \bmod p_i(z).$$

Для получения $A(z)$ в ПМСС с основаниями $p_1(z), p_2(z), ..., p_n(z)$ необходимо получить в этой системе значения $a_1(z) z^l \bmod p_i(z)$. В этом случае остаток по модулю $p_i(z)$ определяется как

$$\alpha_i(z) = \left| \sum_{l=0}^{k} (a_1^i z^l) \bmod p_i(z) \right|_2^+, \qquad (1)$$

где $a_1^i = a_1 \bmod p_i(z)$; $i = 1, 2, 3, .., n$.

В соответствии с выражением (1), перевод A(z) из позиционной системы счисления в непозиционную можно свести к суммированию по модулю два величин $(a_1^i z^l) \bmod p_i(z)$ в соответствии с заданным полиномом A(z).

Таким образом, применение китайской теоремы об остатках (КТО) обеспечивает однозначное отображение одномерных величин в многомерные. Рассмотренные преобразования из позиционной системы счисления в ПМСС позволяют реализовать переход от одномерного описания полинома, заданного в расширенном поле $GF(p^v)$, к n-мерному изображению по основаниям $p_i(z)$, $i = 1, 2, ..., n$ ПМСС.

Данная процедура характеризуется минимальными аппаратурными затратами по сравнению с известными методами понижения разрядности и итеративного последовательного преобразования. Кроме того, применение алгоритма (1) позволяет осуществлять процедуру преобразования из двоичного кода в ПМСС за одну итерацию. Таким образом, очевидно, что модификация и реализация метода непосредственного суммирования для полиномиальной МСС позволяет разрабатывать высоконадежные преобразователи кодов для вычислительных структур реального времени. Восстановления заданного полинома $A(z) \in GF(p^v)$ по совокупности его остатков $(\alpha_1(z), \alpha_2(z), ..., \alpha_n(z))$ также является важной задачей, от решения которой во многом зависит эффективность функционирования непозиционной ИУС. Метод перевода непозиционного кода МСС в позиционную систему счисления может бать реализован с помощью процедур построенных либо на основе ортогональных базисов с использованием КТО, либо на основе применения обобщенной полиадической системы (ОПС).

В общем виде для первой процедуры задача перевода n-мерного представления полинома $A(z) \in GF(p^v)$ к позиционному виду представляется следующим образом: для заданного набора модулей $p_i(Z)$, $i = 1, 2, ..., n$ необходимо осуществить преобразование n-мерного образа $A(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_n(z))$ в систему с основанием $P(z) = \prod_{i=1}^{n} p_i(z)$ так, чтобы выполнилось условие

$$A(z) = \alpha_1(z)B_1(z) + \alpha_2(z)B_2(z) + ... + \alpha_n(z)B_n(z)\,, \quad (2)$$

где $B_i(z)$ – базисы системы; $i = 1, 2, ..., n$.

Любой базис можно представить в непозиционном виде как $B_i(z) = (\beta_1^i(z), \beta_2^i(z), ..., \beta_n^i(z))$, где $\beta_j^i(z) \equiv B_i(z) \bmod p_j(z)$; $i, j = 1, 2, ..., n$.

С другой стороны известно, что любой элемент $A(z) \in P(z)$ можно представить как сумму ортогональных полиномов $A_1(z), A_2(z), ...A_n(z)$, то есть

$$\begin{gathered} A(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_n(z)) = A_1(z) + A_2(z) + \\ + ... + A_n(z) = (\alpha_1(z), 0, ..., 0) + +(0, \alpha_2(z), 0, ..., 0) + \\ + ... + (0, 0, ..., \alpha_n(z)). \end{gathered} \quad (3)$$

Под ортогональным полиномом понимается элемент расширенного поля $GF\left(p^v\right)$ заданного основаниями $p_1(z)$, …, $p_n(z)$ такими, что $P(z) = \prod_{i=1}^{n} p_i(z)$, у которого все остатки равны нулю, за исключением цифры по модулю $p_i(z)$ $A_i(z) = (0, 0, ..., 0, \alpha_i(z), 0, ...0)$, где $i = 1, 2, ..., n$.

Приравнивая выражения (2) и (3) и учитывая независимость выполнения арифметических операций по модулям ПМСС, получаем, что $\alpha_i(z)B_i(z) = (0, 0, ..., 0, \alpha_i(z), 0, ...0)$. Исходя из условия представления базисов системы, имеем

$$\begin{gathered} (\alpha_i(z)\beta_1^i(z), ..., \alpha_i(z)\beta_i^i(z), ..., \alpha_i(z)\beta_n^i(z)) = \\ = (0, 0, ..., \alpha_i(z), ..., 0). \end{gathered}$$

Следовательно, ортогональные базисы $B_i(z)$, $i = 1, 2, ..., n$ системы ПМСС расширенного поля Галуа $GF\left(p^v\right)$ можно представить в следующем виде

$$\begin{gathered} B_1(z) = (1, 0, ..., 0, ..., 0); ..., B_i(z) = \\ = (0, 0, ..., 1, ..., 0); ..., B_n(z) = (0, 0, ..., 0, ..., 1). \end{gathered} \quad (4)$$

Итак, выражение (2) можно записать как

$$A(z) = \sum_{i=1}^{n} \alpha_i(z)B_i(z) \bmod P(z)\,. \quad (5)$$

Для получения значений ортогональных базисов ПМСС воспользуемся КТО и равенствами (5), согласно которым

$$B_i(z) = \begin{cases} 0 \bmod p_u(z),\ u \neq i, \\ 1 \bmod p_u(z),\ u = i. \end{cases} \quad (6)$$

где $B_i(z) = m_i(z) \prod_{\substack{u=1 \\ u \neq i}}^{n} p_u(z)$; $m_i(z) \cdot \prod_{\substack{u=1 \\ u \neq i}}^{n} p_u(z) \equiv 1 \bmod p_i(z)$.

Преобразуя выражение (6), получаем формулу для вычисления ортогонального базиса по i-му основанию $B_i(z) = m_i(z) \cdot P(z) / p_i(z)$,

где $m_i(z)$ – вес ортогонального базиса.

Вес ортогонального базиса выбирается из условия $B_i(z) \bmod p_i(z) \equiv 1$. Обобщая выше сказанное, можно представить алгоритм определения значений ортогональных базисов $B_i(z)$ $i = 1, 2, ..., n$ для системы ПМСС поля Галуа $GF\left(p^v\right)$, согласно которому на первом этапе осуществляется вычисления значения $P_i^*(z) = \dfrac{P(z)}{p_i(z)} = \prod_{u=1, u \neq i}^{n} p_u(z)$.

Далее, поскольку величина $P_i^*(z)$ составлена из множителей, взаимно простых с $p_i(z)$, то значение остатка определяется в соответствии с выражением $\delta_i(z) = \mathrm{rest}(P_i^* / p_i(z)$.

В соответствии с условием (6) выбирается значение $m_i(z)$, такое, что выполняется условие $m_i(z)\delta_i(z) \bmod p_i(z) \equiv 1$.

После этого вычисляется значение ортогонального базиса $B_i(z) = m_i(z)P_i^*(z)$.

Из выше представленной процедуры наглядно видно, что она аналогична процедуре вычисления ортогональных базисов в МСС.

Основа второй процедуры обратного преобразования из ПМСС в ПСС базируется на применении промежуточной обобщенной полиадической системы счисления (ОПС). Введение промежуточной смешанной системы счисления, позволяет изображать число A в виде

$$A = a_1 + a_2p_1 + a_3p_1p_2 + ... + a_np_1 \cdots p_{n-1} = \sum_{k=1}^{n} a_kq_{k-1}\,,$$

где a_k – цифры в ОПС; $q_k = q_{k-1}p_k$ – вес цифры в ОПС (смешанный базис). Если обеспечить соответствие между основаниями ОПС и основаниями МСС, то справедливо равенство

$$\begin{gathered} A(z) = \left[\alpha_1(z),\quad \alpha_2(z),\quad ...,\quad \alpha_n(z)\right] = \\ = [a_1(z),\quad a_2(z),\quad ...,\quad a_n(z)]. \end{gathered} \quad (7)$$

Тогда на основании (7) можно сделать вывод о возможности перевода кода ПМСС в кодовую последовательность ОПС. Причем вся процедура перевода должна осуществляться в модулярной арифметике.

Можно выделить три основных подхода к построению УОИ, предназначенных для выполнения этой немодульной операции.

Основу первого подхода составляют процедуры, базирующиеся на рекуррентном алгоритме вычисления коэффициентов. В работах [3] описан алгоритм перевода в позиционную систему счисления с использованием коэффициентов ОПС, который можно представить следующим образом

$$a_k = \text{rest } A_k (\text{mod } p_k), \tag{8}$$

где A_k определяется по рекуррентной формуле

$$A_k = (A_{k-1} - \alpha_{k-1}) w_{k-1}, \tag{9}$$

$A_1 = A$; $w_k = p_k^j$ – формальная обратная величина k-ого основания по j-му основанию ($j \neq k$); $\alpha^*_{к-1}$ – набор остатков по всем модулям, номера которых выше номера $k-1$; $k = 1,...,n$. При этом все операции по вычислению коэффициентов a_k производятся в МСС. Одна из процедур, позволяющая повысить скорость преобразования ПМСС – ОПС, базируется на подобранных специальным образом основаниях МСС, в соответствии с данным алгоритмом

$$p_j = \prod_{i=1}^{j-1} p_i + 1, \; j = 2,3,...,n.$$

При указанном способе выбора оснований число операций, необходимых для вычислений коэффициентов ОПС уменьшается в два раза, но при этом наблюдается резкий рост аппаратурных затрат при увеличении разрядности обрабатываемых данных. Кроме этого, такая процедура невыполнима в расширенных полях Галуа. Основу более рационального подхода к вычислению коэффициентов ОПС в расширенных полях Галуа составляет процедура, при осуществлении которой наиболее трудоемкий этап перевода в ОПС (остаток – коэффициенты) выполняется путем параллельно-конвейерного вычисления коэффициентов. Реализовав ортогональные базисы модулей ПМСС, в виде коэффициентов ОПС, получаем выражение

$$A(z) = \alpha_1 \left[\gamma_1^1, \gamma_2^1, ..., \gamma_{k+r}^1\right] + ... + \alpha_{k+r}\left[0, \quad 0, ..., \quad \gamma_{\;k+r}^{\;k+r}\right],$$

где γ_i^j – коэффициенты ОПС j-го ортогонального базиса. Тогда, проведя умножение вычетов α_i на коэффициенты ОПС помодульно и поразрядно, учитывая превышение модуля p_i как перенос единицы при суммировании результата, коэффициенты ОПС могут быть найдены непосредственно из выражения

$$a_i = \left| \left| \sum_{j=1}^{i} \left| \alpha_j \gamma^j \right|_{p_i}^{+} \right|_{p_i}^{+} + \delta_{i-1} \right|_{p_i}^{+},$$

где δ_{i-1} – переполнение, полученное при суммировании по модулю p_{i-1}.

Одним из важнейших свойств кодов ПМСС, определенных в расширенных полях Галуа $GF(p^v)$, является отсутствие межразрядных переносов при вычислении результата по модулю $p_i(z)$. Это позволяет свести операцию итеративного получения коэффициентов ОПС к однотактной процедуре, определяемой выражением

$$a_i(z) = \left| \left| \sum_{j=1}^{i} \alpha_j(z) \gamma^j(z) \right|_{p_i(z)}^{+} \right|_{p_i(z)}^{+}, \tag{10}$$

где $i = 1, 2, ..., n$ – количество оснований кода ПМСС.

Выводы

1. Использование ПМСС, при создании специализированной ИУС СПСМРК позволяет предложить новые, интересные решения научно-технической задачи обеспечения её более высокой производительности, пропускной способности и отказоустойчивости системы, при существенно меньших, чем в ПСС, дополнительных аппаратных и массово-габаритных затратах.

2. Применение рассмотренных процедур перевода кодов из ПСС в ПМСС и обратно позволяет повысить эффективность функционирования ИУС, за счет использования одноитерационной процедуры, в отличие от распространённых подходов, предполагающих n-итераций на каждую процедуру.

Список литературы

1. Барсов В.И. Методы многоверсионной обработки информации в модулярной арифметике / [В.И. Барсов, В.А. Краснобаев и др.]. – Х.: МОН, УИПА, 2008. – 460 с.

2. Методы контроля и коррекции ошибок в высокоскоростных системах обработки информации АСУ ТП энергоблоков функционирующих в полиномиальной системе классов вычетов / Энергетика та електрифікація: наук.-виробн. ж. – К., 2009. – № 8. – С. 41-46.

3. Модулярные параллельные вычислительные структуры нейропроцессорных систем / Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2003. – 288 с.

Поступила в редколлегию 10.10.2012

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Полтавский национальный технический университет им. Юрия Кондратюка, Полтава.

ЗАСТОСУВАННЯ ПОЛІНОМІАЛЬНОЇ МОДУЛЯРНОЇ СИСТЕМИ ЧИСЛЕННЯ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ МЕРЕЖІ ПАКЕТНОГО ПЕРЕРИВЧАСТОГО ЗВ'ЯЗКУ

В.І. Барсов

Розглядається можливість застосування методів обробки інформації в поліноміальній модулярній системі числення при створенні мережі пакетного зв'язку, що використовує метеорні радіоканали для підвищення ТТХ мережі.

***Ключові слова:** метеорний радіоканал, поліноміальна модулярна система числення, обробка інформації.*

APPLICATION OF POLYNOMIAL MODULYARNOY OF SCALE OF NOTATION IS FOR INCREASE OF EFFICIENCY OF FUNCTIONING OF PACKAGE IRREGULAR COMMUNICATION NETWORK

V.I. Barsov

Possibility of application of methods of treatment of information is examined in the modular system of polynomial of calculation at networking package connection which utillizes meteor radio channels for the increase of performance descriptions of network.

***Keywords:** meteor radio channel, modular system of polynomial of calculation, treatment of information.*