

## **ОЦЕНКА ПОМЕХОУСТОЙЧИВОСТИ ДВОИЧНЫХ ДЕШИФРАТОРОВ**

*проф. Борисенко А.А., студ. Гутенко Д.В.*

При работе двоичных дешифраторов могут возникать различные сбои, которые становятся причиной возникновения ошибочной информации на выходе. Для того, что бы уменьшить вероятность ошибки на выходе устройства используют различные способы защиты от ошибок.

Применение того или иного способа защиты обусловлено не только обеспечением высокой достоверности в работе дешифратора, но и от других факторов таких как: цена, дополнительные габариты и т. д. Таким образом различные способы защиты находят своё применения в тех или иных отраслях техники.

Тем не менее, создание универсального способа защиты, который удовлетворял бы большинству требований и обеспечивал высокую достоверность информации на выходе, является важной задачей при построении таких систем.

Для анализа контроля ошибок различными способами защиты проводилось исследование количества обнаруживаемых и необнаруживаемых ошибок на выходе дешифратора. На основании полученных данных проводилось сравнение для определения способа защиты, который бы обеспечивал лучшие показатели.

Так же большое значение имеет вероятность перехода правильной комбинации в ту или иную ошибочную. Для определения соответствующих характеристик была выбрана модель перехода из 0 в 1 и из 1 в 0 на выходах логических элементов. На основании формул, выведенных для рассматриваемых способов защиты, были получены значения для различных характеристик дешифраторов. В результате анализа полученных данных был выбран способ защиты от ошибок, который бы обеспечивал оптимальные значения по выбранным параметрам.

## СИСТЕМА КОДОВОЙ ЗАЩИТЫ

доц. Новгородцев А.И., доц., Лопатченко Б.К., студ. Шевченко А.С..

Характерной особенностью последнего времени стало чрезвычайное разнообразие случаев хищения.

Секретные ключи представляют собой основу криптографических преобразований, для которых, следуя правилу Кирхгофа, стойкость хорошей шифровальной системы определяется лишь секретностью ключа.

Однако в практике создание, распределение и хранение ключей редко были сложными технически, хотя и дорогими задачами.

Основная проблема классической криптографии долгое время заключалась в трудности генерирования непредсказуемых двоичных последовательностей большой длины с применением короткого случайного ключа.

Интересным примером сочетания цифровых и аналоговых методов является формирование псевдослучайных двоичных последовательностей (ПСДП).

Оказывается, удивительно легко сформировать последовательность битов или слов, обладающую хорошими статистическими свойствами, т. е. последовательность, которая имеет такие же вероятностные и корреляционные характеристики, как и идеальный процесс бросания монеты.

Поскольку эти последовательности вырабатываются стандартными детерминированными логическими элементами (регистрами сдвига), они фактически являются известными наперед и периодически повторяющимися, однако любой отрезок такой последовательности выглядит как случайное чередование нулей и единиц.

Пропуская ПСДП через простой НЧ – фильтр, можно получить белый гауссов шум с ограниченной полосой, т. е. напряжение, имеющее плоский энергетический спектр в пределах некоторой частоты среза.

С другой стороны, путем взвешенного суммирования содержимого нескольких регистров сдвига можно произвести цифровую фильтрацию, дающую тот же результат. Этот способ позволяет обеспечить плоский спектр шума в пределах нескольких мегагерц.

Эти последовательности также широко используются в кодах с обнаружением и исправлением ошибок, поскольку они позволяют формировать такие блоки данных, в которых правильные сообщения оказываются разделенными большим расстоянием Хемминга (оно измеряется числом ошибочных битов).

Благодаря хорошим автокорреляционным свойствам эти последовательности идеально подходят для помехозащищенных радарных систем, в которых ответный сигнал сравнивается с переданной строкой битов (точнее, взаимно коррелируется). Их также можно использовать в качестве компактных делителей по модулю  $n$ .

Наиболее простым и распространенным генератором ПСДП является регистр сдвига с обратной связью (рис. 1.1). Регистр сдвига, имеющий длину  $m$  бит, тактируется с фиксированной частотой  $f_0$ . С помощью вентиля Исключающее ИЛИ на вход регистра подается последовательный сигнал, представляющий собой сумму по модулю 2  $n$ -го и последнего ( $m$ -го) разрядов регистра. Такая схема является циклической с периодом  $K$ .

Число возможных состояний  $m$  – разрядного регистра составляет  $K = 2^m$ , т. е. равно числу двоичных комбинаций из  $m$  бит. Однако состояние, когда в регистре содержатся все 0, является для данной схемы «тупиковым», поскольку Исключающее ИЛИ будет формировать на входе 0. Вследствие этого максимальная длина последовательности, которую можно сформировать с помощью данной схемы, равна  $2^m - 1$ . Оказывается, что получать такие последовательности максимальной длины можно лишь в том случае, если  $m$  и  $n$  выбраны правильно и результирующая последовательность битов является псевдослучайной.

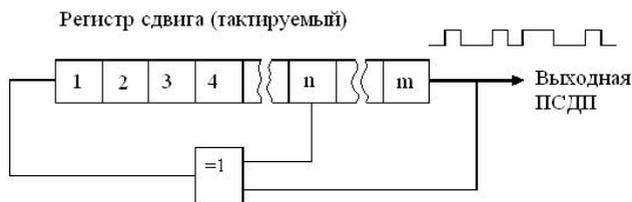


Рисунок 1.1 – Генератор псевдослучайной двоичной последовательности.

## УСТРОЙСТВО ПРЕОБРАЗОВАНИЯ ДВОИЧНЫХ ЧИСЕЛ В БИНОМИАЛЬНЫЙ МОДИФИЦИРОВАННЫЙ КОД

*Ассист. Гриненко В.В., студ. Дуюн А.А.*

Одной из проблем, которая препятствует широкому применению биномиальных модифицированных кодов, является отсутствие быстродействующих устройств кодирования-декодирования. Предлагается устройство преобразования двоичных чисел в биномиальный модифицированный код.

Комбинации биномиального модифицированного кода с параметрами  $n$  и  $k$  с числом единиц  $q$  представляют собой комбинацию равновесного кода длиной  $n-l+q-k$  с количеством единиц  $q$  с дополнительными  $k-q$  нулевыми разрядами до длины  $n-l$ .

Процедура кодирования состоит в реализации двух задач: определения подмножества кодов с постоянным числом единиц  $q_i$ , к которому принадлежит исходная комбинация, и представления двоичной комбинации в равновесном коде с данным числом единиц  $q_i$  и дополнение нулевыми разрядами.

Для определения подмножества, к которому принадлежит выходная комбинация, устройство сравнивает количественный эквивалент исходной комбинации  $N_{ex}$  с количеством комбинаций  $S$  с числом единиц  $q_i$ , где  $q_i$  - элемент множества  $W$  разрешенных значений  $q$  идущих в порядке возрастания. Если  $S \geq N_{ex}$ , то из количественного эквивалента вычитается количество комбинаций  $N_{ex} = N_{ex} - S$ , и переходим к следующему значению  $q_i$ . Если  $S < N_{ex}$ , то производится определение по количественному эквиваленту  $N_{ex}$  соответствующей комбинации в равновесном коде с длиной  $n-l+q_i-k$  и числом единиц  $q_i$ .

Одним из быстродействующих алгоритмов преобразования в равновесный код, является алгоритм, использующий принцип поразрядного взвешивания. Используя данный принцип можно добиться того, что число тактов преобразования будет равно длине ядра комбинации, представляющего собой комбинацию равновесного кода.

## СИСТЕМА РАСПОЗНАВАНИЯ СИГНАЛА ПРИ ВОЗДЕЙСТВИИ АДДИТИВНОГО ШУМА

студ. Федоров А. Г., доц. Онанченко Е. Л.

При передаче сигналов по каналу связи возникновение шумов практически неизбежно. Условием нормального приема сигнала в этом случае является превышение значения уровня сигнала над уровнем шума, как правило, с достаточным запасом. При этом иногда достаточно остро стоит проблема уменьшения влияния шума на сигнал. При наличии помехи, сравнимой по амплитуде с сигналом, нормальный прием невозможен.

Для решения этой проблемы сигнал, подвергшийся воздействию помехи, в отдельных случаях можно классифицировать. При этом с известной вероятностью определяется, какому значению исходного сигнала соответствует принятый сигнал.

В данной работе предложен нейроподобный классификатор, позволяющий распознать двухуровневый сигнал при воздействии произвольного аддитивного шума.

Суть работы классификатора заключается в проверке гипотез, каждая из которых заключается в том, что был получен заданный уровень сигнала. Таким образом, считается, что был передан сигнал уровня, соответствующего более вероятной гипотезе.

Разработанный классификатор имеет свойства инвариантности, что означает, что при известных значениях входного сигнала вероятность ошибочного подтверждения гипотезы определяется только шумом, воздействующим на сигнал в канале связи.

В основу синтеза такого нейроподобного классификатора положены ранговые предикаты, обладающие свойствами инвариантности, вида

$$p(u_i - u_j) = \begin{cases} 0 & u_i < u_j \\ 1 & u_i \geq u_j \end{cases}$$

где  $u_i, u_j$  –  $i$  и  $j$  элементы выборки исследуемого сигнала

С их помощью было реализовано решающее правило проверки гипотез

$$u^{(n)} \underset{H_0}{\overset{H_1}{>}} 2U_c - u^{(1)},$$

где  $u^{(n)} = \max\{u_1, \dots, u_n\}$ ;

$u^{(1)} = \min\{u_1, \dots, u_n\}$  – непрерывная (нечеткая, бесконечнозначная) конъюнкция;

$U_c = (U_0 + U_1)/2$  – среднее значение уровней исходного сигнала;

$H_1, H_0$  – гипотезы, заключающиеся в том, что был передан сигнал высокого или низкого уровня соответственно.

Таким образом, для аддитивного гаусовского шума при коэффициенте сдвига относительно  $U_c$ , не превышающего амплитуду сигнала  $U_m$ , были получены следующие выражения, определяющие ошибочную проверку гипотезы для сигнала высокого и низкого уровня соответственно, для заданного числа элементов выборки  $n$ :

$$P_{01} = [F_\sigma(-U_m)]^n,$$

$$P_{00} = [1 - F_\sigma(U_m)]^n.$$

где  $F_\sigma$  – интегральная функция распределения шума.

## ПОСТРОЕНИЕ МНОГОУРОВНЕВЫХ КОДОВ ПРИ АДАПТИВНОЙ ПЕРЕДАЧЕ СИГНАЛОВ

студ. Ткаченко Р.А., доц. Онанченко Е. Л.

Проблема адаптивной передачи начинается со случая однопользовательской многочастотной системы. Как известно, принятый сигнал в многочастотных системах может быть представлен как:

$$r_i = \mu_i s_i + \eta_i, \quad i = 1 \dots N,$$

где  $s_i$  — сигнал, переданный по  $i$ -му подканалу,  $\eta_i$  — отсчет аддитивного Гауссовского шума с дисперсией  $\sigma^2$ ,  $\mu_i$  — передаточный коэффициент  $i$ -го подканала. Каждый подканал может быть охарактеризован своим отношением канал/шум

$$\xi = |\mu_i|^2 / \sigma^2$$

Для повышения точности адаптации в подобной системе необходимо наличие большого семейства схем кодирования и модуляции с малым шагом скоростей. Строятся семейства многоуровневых кодов с указанными свойствами на основе заданного набора компонентных кодов.

Данная процедура построения многоуровневого кода, использующего  $M$ -ичную амплитудную модуляцию и способного функционировать с заданной вероятностью ошибки  $P$  на заданном отношении сигнал/шум  $\gamma$ , состоит из следующих шагов:

- для каждого из компонентных кодов  $C_j$  построить теоретически или путем имитационного моделирования кривую  $p_j(\gamma)$  вероятности ошибки в зависимости от отношения сигнал/шум при передаче по аддитивному Гауссовскому каналу;

- для каждого из имеющихся компонентных кодов  $C_j$  найти отношение сигнал/шум, обеспечивающее заданную вероятность ошибки, т.е. решить уравнение  $p_j(\gamma)=P$ . Это дает отображение  $r_j \leftrightarrow \gamma_j$  или  $r_j \leftrightarrow C(\gamma_j)$ , которое также может быть аппроксимировано некоторой функцией  $r(C)$ . Здесь  $C(\gamma)$  — пропускная способность аддитивного Гауссовского канала при отношении сигнал/шум  $\gamma$ ;

- вычислить пропускные способности  $C_i$ ,  $i=0..l-1$  эквивалентных подканалов  $M$ -ичной амплитудной модуляции с помощью стандартных выражений для пропускной способности эквивалентных подканалов в многоуровневом коде;

- для каждого из подканалов  $i$  найти скорость кода  $r(C_i)$ , пригодного для использования в качестве компонентного на данном подканале. Для кодирования данных на  $i$ -м уровне многоуровневого кода должен использоваться компонентный код из семейства  $\{C_j\}$  с наибольшей скоростью, не превосходящей  $r(C_i)$ .

Описанная процедура позволяет выбрать для каждого  $\gamma$  набор компонентных кодов, максимизирующих скорость передачи при заданной вероятности ошибки. Ясно, что если имеется возможность использования сигнальных множеств с различным числом уровней  $M$ , то для каждого  $\gamma$  может быть выбрано сигнальное множество, обеспечивающее максимальную скорость передачи.

Данный метод построения многоуровневых кодов может рассматриваться как модификация известного правила равных вероятностей ошибки. Действительно, для каждого компонентного кода вероятность ошибки при передаче по аддитивному Гауссовскому каналу однозначно определяется отношением сигнал/шум. С другой стороны, отношение сигнал/шум однозначно характеризует пропускную способность канала, т.е. пропускная способность канала однозначно определяет вероятность ошибки декодирования.

Предлагаемый метод основывается на предположении о том, что при переходе от аддитивного Гауссовского канала к эквивалентным подканалам в многоуровневом коде эта зависимость не претерпевает существенных изменений. Основным достоинством предлагаемого метода является простота процедуры построения многоуровневого кода, которая не требует достаточно сложного анализа вероятности ошибки декодирования. Для многих кодов такой анализ практически неосуществим.

Для построения семейства многоуровневых кодов описанная процедура должна быть выполнена для набора значений  $\gamma$  с некоторым достаточно малым шагом  $\Delta$ . Это позволяет построить большое число многоуровневых кодов на основе сравнительно небольшого семейства компонентных кодов.

## ЭЛЕКТРОННАЯ СИСТЕМА ДИСПЕТЧЕРСКОГО КОНТРОЛЯ РАБОТЫ КОТЕЛЬНОЙ

*студ. Странадко А.В., доц. Новгородцев А.И. с. н. с. Покотило В.Н.*

Происходящая научно-техническая революция в области построения и исследования автоматических и автоматизированных систем управления ставит новые задачи и проблемы по развитию теоретических основ и технического совершенствования адаптивных систем оптимального управления, обеспечивающих управление тем или иным классом объектов с наилучшим, в смысле выбранного критерия, качеством и в оптимальных режимах.

Особая актуальность данной работы обусловлена необходимостью создания высококачественных и экономически эффективных систем управления и контроля нестационарными динамическими объектами, где по сей день остаётся ряд нерешенных проблем.

Разрабатываемая система предназначена для местного и (или) удалённого контроля нестационарных динамических параметров при работе автономной газовой котельной.

В данной работе сформулирована и математически поставлена задача исследований, основу которой составляет метод пространства состояний. Согласно этому методу НДП представляется математической моделью, адекватно изображающей физические процессы, происходящие в реальном объекте управления.

При разработке подобных систем управления объектами с переменными параметрами возникает необходимость автоматического учёта текущей информации о состоянии объекта, т. е. учёта его динамических характеристик в процессе функционирования.

Учёт динамических характеристик нестационарного объекта управления в процессе его нормальной эксплуатации возможен с применением систем идентификации. Наиболее эффективным методом решения задач идентификации является компенсационный, т. е. метод самонастраивающейся модели объекта управления с параллельным включением.

В ходе работы рассматриваются некоторые аспекты решения задач синтеза информационных систем, а также особенности работы систем анализа и принятия решений.

## МЕТОД СЖАТИЯ ДВОИЧНЫХ СООБЩЕНИЙ НА ОСНОВЕ МНОГОЗНАЧНЫХ БИНОМИАЛЬНЫХ ЧИСЕЛ

*студ. Свистунов А.А., ст. преп. Протасова Т.А*

Сжатие информации представляет собой операцию, в результате которой данному коду или сообщению ставится в соответствие более короткий код или сообщение

Актуальность проблемы сжатия различных сигналов в настоящее время очевидна. Сжатие информации имеет целью — ускорение и удешевление процессов механизированной обработки, хранения и поиска информации, экономию памяти ЭВМ.

К рассмотрению предлагается аппаратная реализация алгоритма сжатия нумерацией двоичных последовательностей на основе многозначной биномиальной системы счисления.

Известные методы нумерации осуществляют процедуру сжатия в течение одной процедуры. Однако эти методы сложны и трудно реализуемы аппаратно и при этом недостаточно универсальны.

Устранить эти недостатки можно путем использования структурных систем счисления, в частности, многозначной биномиальной системы счисления. При использовании структурных систем счисления нумерация осуществляется в два этапа: сначала организовывается переход к числу в биномиальной системе счисления, а затем происходит переход от этого числа к его номеру.

При решении задачи нумерации сигналов двоичные последовательности рассматриваются как равновесные кодовые комбинации. Это объясняется тем, что подвергать процедуре сжатия путем нумерации можно только кодовые комбинации, характеризующиеся одинаковой вероятностью их генерирования.

Исходное двоичное слово характеризуется следующими параметрами: длиной слова -  $m$  и количеством единиц -  $k$ . Эти параметры являются исходными для определения параметра многозначной биномиальной системы счисления, который определяется согласно соотношению  $q=m-k$ .

На следующем этапе формируют комбинаторную конфигурацию типа сочетания, затем осуществляется переход к биномиальному числу, далее производится подсчет количественного эквивалента биномиального числа.

## МЕТОДЫ И СПОСОБЫ ДИАГНОСТИКИ ИМС

студ. Онанченко С.А., доц. Онанченко Е.Л.

Представим микросхему в виде устройства с несколькими входами, на которые поступают двоичные входные сигналы, и несколькими выходами, с которых снимаются двоичные выходные сигналы.

Для проверки работоспособности такого устройства на его входы необходимо подать тестовую последовательность комбинаций входных сигналов и сравнить получаемые значения выходных сигналов со значениями, указанными в документации. В общем случае при проверке существенной проблемой является сжатие информации о правильных и наблюдаемых при контроле реакциях устройства на тестовые последовательности.

Для сжатия длинных двоичных последовательностей и получения кодов сигнатур используется сигнатурный анализатор, основу которого составляет сдвиговой регистр с внутренними обратными связями, замыкаемыми через сумматор по модулю 2, на вход которого также поступает последовательность бит, снимаемая с контролируемой точки.

Сигнатурный анализ основывается на следующем принципе сжатия данных: двоичная последовательность  $x$  в виде информационного полинома  $G(x)$  поступает с выхода проверяемой схемы на сдвиговой регистр и делится в виде полинома  $x^k G(x)$  (где  $k$  - количество разрядов сдвигового регистра) на порождающий полином  $P(x)$  степени  $k$ . Деление не порождающий полином  $P(x)$  реализуется с помощью сдвигового регистра с обратными связями. Результатом деления является остаток  $R(x)$ , получающийся в сдвиговом регистре после приема входной последовательности.

Математически процесс описывается формулой

$$x^k G(x) = Q(x)P(x) \oplus R(x),$$

где  $Q(x)$  - частное;  $R(x)$  - остаток;  $P(x)$  - порождающий полином степени  $k$ , а  $G(x)$  - информационный полином, соответствующий входной двоичной последовательности  $x$ .

При прохождении последовательности  $x$  через сдвиговой регистр  $R(x)$  изменяется до тех пор, пока не закончится вся последовательность  $x$ . Конечное выражение  $R(x)$  является сигнатурой.

## ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМОВ БИНОМИАЛЬНОГО ДВОИЧНОГО СЧЕТА

*проф.* Борисенко А. А., *студ.* Кремезный В. В.

Рассматриваемые алгоритмы работают в биномиальной двоичной системе счисления. Данная система счисления относится к системам счисления с функциональным основанием, где в качестве основания используется выражение для биномиальных коэффициентов.

Применение такого алгоритма целесообразно в системах телеавтоматики со сквозным контролем ошибок, в специализированных помехоустойчивых преобразователях информации, в генераторах и нумераторах сочетаний.

Полезными свойствами биномиального счета являются его помехоустойчивость при передаче, хранении, и обработке информации, возможность организации на его основании генерации и перебора комбинаций биномиальных кодов, возможность построения помехоустойчивых цифровых устройств, кодирования информации.

Алгоритмы биномиального счета являются основой биномиальных счетчиков, конкретная структура которых может быть задана в виде программы для ЭВМ, микропроцессорного устройства, или устройства с жесткой логикой, собранного из отдельных элементов или изготовленного в виде интегральной схемы.

Использование программы биномиального счета в ЭВМ имеет практическое значение в случае помехоустойчивого кодирования данных или если стоит задача перебора, генерирования или нумерации сочетаний.

На основе алгоритма биномиального двоичного счета была разработана и испытана программа. В качестве языка программирования был использован С. Результатом работы программы является формирование массива неравномерных или равномерных биномиальных чисел, соответствующих заданным параметрам  $n$  и  $k$ . Основные функции данной программы при соответствующей доработке предполагается использовать в различных программных реализациях алгоритмов, использующих биномиальную двоичную систему счисления.

## **ОСОБЕННОСТИ ПОСТРОЕНИЯ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМ С ПОВЫШЕННОЙ ТОЧНОСТЬЮ ИЗМЕРЕНИЯ КОЛИЧЕСТВА ЭЛЕКТРОЭНЕРГИИ**

*доцент Бережная О.В., ст. преп. Арбузов В.В., студ. Бережной А.И.*

Развитие Оптового рынка электроэнергии (ОРЭ) в Украине в немалой степени зависит от эффективности внедрения субъектами ОРЭ автоматизированных систем коммерческого учета электроэнергии (АСКУЭ) как основного инструмента контроля и учета вырабатываемой и перераспределяемой между субъектами ОРЭ электроэнергии.

Для практического применения АСКУЭ в такой роли необходима аттестация в установленном порядке методики выполнения измерений небалансов, а одной из обязательных функций АСКУЭ должна быть функция наблюдения за погрешностью результатов измерений количества электроэнергии, перераспределяемой на ОРЭ, при формировании отчетных показателей генерации, потребления по совокупности точек учета, входящих в периметр (сечение) субъектов ОРЭ, при формировании небалансов между приемом и полезным отпуском электрической энергии, осуществляемых, как правило, с помощью косвенных и совокупных измерений. Наиболее целесообразно осуществлять решение комплекса этих задач в рамках развития концепции «метрологического наблюдателя» применительно к измерениям электрической энергии и мощности с помощью АСКУЭ [1].

Так как изменение погрешности связано, в основном, с изменением условий измерений и параметров объекта измерений, в первую очередь, изменение диапазонов измерения трансформаторов тока (ТТ), и с появлением в этом случае в нижней части шкалы повышенных значений амплитудных и угловых погрешностей целесообразно, в первую очередь, с помощью «метрологического наблюдателя» как встроенного программного модуля в составе вычислительной компоненты АСКУЭ решить следующие основные задачи:

– контроль условий измерений и параметров объекта измерения с помощью метода вспомогательных измерений в реальном режиме времени за интегрированными значениями с периодом интеграции  $\tau$ ,

– оценка погрешности результатов косвенных и совокупных измерений количества электроэнергии и мощности с помощью метода вспомогательных измерений существенных параметров объекта и условий измерений;

– контроль отклонений наблюдаемой погрешности измерений за учетные периоды от нормируемых значений;

– осуществление коррекции результатов измерений количества электрической энергии и мощности путем введения поправок за счет исключения систематических погрешностей ТТ и трансформаторов напряжений (ТН), входящих в состав измерительного канала (ИК).

Наблюдение за погрешностью измерений в реальном режиме времени позволяет выделять коммерческую составляющую в небалансах, упрощая анализ причин возникновения технологических потерь и превышения нормативных небалансов, и создает возможность «справедливого» распределения физического небаланса на оптовом и розничном энергорынках между его субъектами.

## **СПИСОК ЛИТЕРАТУРЫ**

Арбузов В.В., Бережная О.В. Особенности применения метрологического наблюдателя при построении АСКУЭ субъектов ОРЭ / Информационные технологии в энергетике: Материалы 3 научно-практической конференции (Партенит, 28 сентября – 02 октября 2004). – К., 2004 – с. 24-33.

## УДОСКОНАЛЕННЯ МЕТЕОРОЛОГІЧНОЇ ПІДГОТОВКИ ПРИ СТРІЛЬБІ НА ВЕЛИКІ ДАЛЬНОСТІ ЗА ДОПОМОГОЮ СИСТЕМИ GPS – ТРЕКЕР

к.т.н., доц. Макеєв В.І., студ. Єськов І.Є.

*Актуальність і важливість розробки.* Помилки метеорологічної підготовки помітно зростають зі збільшенням часу старіння бюлетеня „метеосередній” і з віддаленням метеостанції від району застосування бюлетеню. Проведені розрахунки показали, що при стрільбі на великі дальності та при нерегулярному надходженні в артилерійські підрозділи бюлетенів „метеосередній” серединні помилки повної підготовки будуть складати за дальністю  $E_{xy}=1,5-2,5\%D$ , за напрямом  $E_{zy}=6-14$  под. кутоміра. Тоді, при стрільбі на граничні дальності, для різних систем відхилення центра розсіювання снарядів від цілі по дальності буде складати 150 – 1250 м, за направленням 60 – 700 м, що може привести до невиконання вогневої задачі.

*Методика розв’язання задачі.* У зв’язку з вищеподаним у даній роботі пропонується новий спосіб визначення установок для стрільби на ураження неспостерегаємих цілей з використанням системи «Снаряд з GPS трекером – Базова станція GPS», який дозволяє врахувати реальний вплив метеорологічних умов стрільби на політ снаряду в межах усієї траєкторії на всі дальності стрільби, визначити помилки на відхилення цих умов від табличних та врахувати їх при стрільбі іншими зразками озброєння, батареями того ж калібру та зразку.

Система GPS трекер – базова GPS станція призначена для отримання метеорологічних та балістичних поправок для стрільби артилерії без викриття вогневої позиції та намірів на викриття вогню по цілі. Може використовуватись всіма типами артилерійських та реактивних систем, які будуть мати на озброєнні снаряди з GPS трекером.

Основою GPS-трекеру є GPS-приймач — радіоприймальний пристрій для визначення географічних координат поточного місцеположення антени приймача, на основі даних про часові затримки приходу радіосигналів, які випромінюються супутниками групи NAVSTAR. GPS-приймач встановлюється на снаряді без змін його балістичних характеристик. Максимальна точність вимірювання складає 3-5 метрів.

Суттєвий вплив на сумарну помилку підготовки і, як результат ефективність ураження цілей при стрільбі на великі дальності при визначенні установок за даними ПОР чинять помилки через змінності метеорологічних умов за часом, вага помилок складає  $g_{x_M} = 35 - 70\%$ .

В умовах бойової обстановки не завжди є можливим переносити вогонь на ціль одразу ж після пристрілки снарядом з «відповідачем». Перенос вогню на ціль, як правило, проводиться через деякий проміжок часу після створення репера. Допустима величина цього проміжку залежить від змінності умов та їх впливу на політ снаряда. Найбільш стійким за часом є атмосферний тиск. Крім того, поправки на відхилення атмосферного тиску за своєю величиною є незначними. Другим за стійкістю фактором є температура повітря. За стійкої погоди серединна зміна балістичного відхилення температури повітря за 3 години для висот траєкторії від 500-1500 м. характеризується величиною, що дорівнює  $1^{\circ}\text{C}$ , а для великих висот траєкторії балістичне відхилення температури повітря протягом 3 годин можна вважати практично незмінним.

*Приклад реалізації.* Для реалізації даного методу в дивізіоні виділяється контрольна гармата, яка буде створювати фіктивний репер на значному віддаленні від району цілей, при цьому розриву снаряду при зустрічі з перешкодою відбуватись не буде. Виконання даної задачі буде відбуватися з тимчасових вогневих позицій, що дозволяє не демаскувати реальний бойовий порядок артилерійських підрозділів.

Система GPS трекер спостерігає за польотом снаряду з «відповідачем» на всій траєкторії польоту та в момент падіння снаряду видає його координати  $X, Y, Z$  з точністю 15 м.

Проведені розрахунки з оцінки ефективності стрільби по різним цілям при застосуванні снарядів із «відповідачем» в системі GPS трекер у порівнянні з повною підготовкою і застосування даних пристрілкових гармат показують, що відносний приріст показника ефективності  $\Delta P(\Delta M)$  буде складати 15-45%. Прийmemo в якості вихідного, що спосіб буде доцільним в тому випадку, якщо відносне підвищення показника ефективності  $\Delta M$  ( $\Delta P$ )  $\geq 0,1$  (10%), тоді отримані результати дозволяють зробити висновок, що використання запропонованого способу обліку метеорологічних умов стрільби у межах всієї траєкторії польоту снаряда з «відповідачем» в системі GPS трекер є доцільним, що дає нам основу для розробки й застосування таких снарядів.

## СТВОРЕННЯ 3D МОДЕЛІ ТА ВІЗУАЛІЗАЦІЯ САМОХІДНОЇ АРТИЛЕРІЙСЬКОЇ ГАРМАТИ 2С3 М

к.т.н., доц. Ляпа М.М., студ. Скалозубов В.О., студ. Тітов П.Г.

*Актуальність і важливість розробки.* В умовах стрімкого розвитку та всебічного застосування обчислювальної техніки для вирішення задач по вдосконаленню військової техніки стало можливим більш широке застосування систем автоматизованого проектування (САПР). Створення 3D моделей зразків озброєння та військової техніки є перспективним напрямком військової науки та надає змогу проводити оцінку ефективності функціонування окремих блоків та системи в цілому.

*Методика розв'язання задачі.* В останні роки особливо бурхливо розвивалися універсальні САПР. На даний час вони об'єднують у собі системи комп'ютерного проектування CAD (Computer Aided Design) та інженерного аналізу CAE (Computer Aided Engineering). Це дозволяє моделювати, аналізувати і синтезувати елементи нових або модернізованих бойових броньованих машин, які характеризуються підвищеними вимогами до міцності, захищеності в умовах обмеженого часу.

*Приклад реалізації.* Для раціонального створення 3D моделі використовується САПР на основі програмного забезпечення Solid-Works 2005. Це дає змогу моделювання вузлів агрегатів, їх складання, візуалізації створених моделей, проведення ряду випробувань складних фізико-механічних процесів на прикладі самохідної артилерійської гармати (САГ) 2С3 М.

*Висновки.* Отримана модель дозволить:

1. Поліпшити навчальний процес, а саме підвищити якість проведення як теоретичних так і практичних занять та в умовах відсутності зразків озброєння вивчати склад, будову та принцип дії військової техніки.
2. Проводити наукові дослідження у сфері модернізації та створення нових зразків озброєння та проводити віртуально випробування діючого або спроектованого зразку озброєння по напрямку бронезахищеності, живучості як екіпажу так і військової техніки, а також розрахунок необхідних матеріалів для конструювання як вузлів та агрегатів так і системи озброєння в цілому.

## СИСТЕМА КОНТРОЛЯ ПАРАМЕТРОВ ЭЛЕКТРОТУРБИНЫ

*студ. Ткач А.Н., доц. Новгородцев А.И.*

Совершенствование технических систем неразрывно связано с повышением информативности и качеством управления процессами (объектами), число которых постоянно растет.

Появляются новые задачи и проблемы технического совершенствования информационно-управляющих систем, обеспечивающих управление тем или иным классом объектов с наилучшим, в смысле выбранного критерия, качеством в оптимальных режимах.

Возникает необходимость в построении адаптивной системы оптимального управления скоростью вращения электротурбины в качестве нестационарного динамического объекта.

Учет динамических характеристик нестационарных объектов управления в процессе их нормальной эксплуатации возможен с применением систем параметрической идентификации.

Наиболее эффективным методом решения задач идентификации, т.е. задач оценок динамических характеристик нестационарных объектов управления, заданных параметрическими передаточными функциями, является компенсационный, т.е. метод самонастраивающейся модели объекта управления с параллельным включением.

При построении сложных адаптивных систем оптимального управления основополагающим является системный подход.

Повышение качества управления и автоматизацию процесса осуществляем с помощью использования системы параметрической идентификации и системы анализа состояния, которые позволяют производить учет динамических характеристик системы в процессе ее функционирования.

Разработанная система управления скоростью электротурбины с элементами самонастройки может применяться на гидроэлектростанциях для улучшения качества управления турбиной.

Достоинством системы является то, что учет динамических характеристик системы происходит в процессе ее функционирования, т.е. параметры системы подстраиваются в зависимости от изменения нагрузки на валу электротурбины.

## ФОРМИРОВАТЕЛЬ КОМПОЗИЦИЙ НА ОСНОВЕ БИНОМИАЛЬНЫХ СИСТЕМ СЧИСЛЕНИЯ С МНОГОЗНАЧНЫМ АЛФАВИТОМ

студ. Протасова Е.А., ст. преп. Протасова Т.А.

В автоматизированных системах обработки и хранения данных при решении специальных задач достаточно часто используются различные комбинаторные конфигурации: перестановки, сочетания, сочетания с повторениями, композиции.

Существующие алгоритмы формирования комбинаторных конфигураций, а также устройства на их основе достаточно сложны и не являются универсальными, что снижает эффективность их использования.

Более эффективно задачу генерирования комбинаторных конфигураций можно решить с помощью многозначной биномиальной системы счисления.

При построении формирователей комбинаторных конфигураций на основе биномиальных систем счисления решение задачи генерирования разбивается на два этапа: сначала осуществляется преобразование исходного числа позиционной системы счисления в биномиальную систему счисления, а затем выполняется переход из биномиальной системы счисления в требуемый код. Такое устройство будет состоять из двух блоков – в первом блоке будет формироваться многозначное биномиальное число, а во втором (параллельно) – все возможные комбинаторные конфигурации.

Рассмотрим решение задачи генерирования комбинаторных конфигураций на примере построения композиций.

Алгоритмы прямого и обратного преобразования основаны на следующих утверждениях.

Утверждение 1. Если  $\alpha_1\alpha_2\dots\alpha_i\dots\alpha_k$  есть многозначное число, то если к каждой, кроме последней  $\alpha_i$  - й цифре этого числа прибавить единицу -  $\beta_i = \alpha_i + 1$ , вычислить последнюю цифру  $\beta_{k+1}$ , равную разности параметра  $P$  и суммы  $\sum_{i=1}^k \beta_i$  всех, ранее вычисленных элементов,  $\beta_{k+1} = P - \sum_{i=1}^k \beta_i$  то полученные цифры являются элементами по-

следовательности, которая образует композицию  $P$  из  $m = k + 1$  частей  $\beta_1\beta_2\dots\beta_{k+1}$ .

Соответствующий алгоритм перехода от многозначного биномиального числа к композиции, будет иметь следующий вид:

1. Прибавить к каждой цифре многозначного биномиального числа единицу. Этим формируются все разряды композиции, кроме последнего.

2. Вычислить сумму  $S$  всех полученных в пункте 1 разрядов композиции.

3. Вычислить параметр  $P = q + m = q + k + 1$ .

4. Вычислить  $Z = P - S$ , где  $Z$  равно значению искомой цифры последнего  $k + 1$ -го разряда композиции.

Обратный переход от композиции к биномиальному числу может быть построен на основе следующего утверждения.

Утверждение 2. Если  $\beta_1\beta_2\dots\beta_i\dots\beta_{k+1}$  есть композиция и если от каждой  $\beta_i$  цифры отнять единицу, то первые  $k$  цифр  $\alpha_i = \beta_i - 1$  являются элементами последовательности, которая образует многозначное биномиальное число  $\alpha_1\alpha_2\dots\alpha_i\dots\alpha_k$ .

Алгоритм преобразования композиции в многозначное биномиальное число имеет следующий вид:

1. Вычислить цифру многозначного биномиального числа по формуле  $\alpha_i = \beta_i - 1$ .

2. Пункт 1 повторять до тех пор, пока не будет получена  $k$ -ая младшая цифра многозначного биномиального числа.

Таким образом, структурные системы счисления и, в частности, биномиальные позволяют формировать разнообразные комбинаторные объекты, структура которых совпадает со структурой чисел соответствующих систем счисления и организовывать их перебор и порождение в случайном порядке. Это свойство может быть положено в основу соответствующих комбинаторных устройств, отличающихся универсальностью, простотой и повышенной надежностью в работе.

## ПРОБЛЕМИ РОЗРОБКИ ТА ПОБУДОВИ ІМПУЛЬСНИХ ПІДСИЛЮВАЧІВ ЗВУКОВОЇ ЧАСТОТИ

студ. Крючко Є.В. асист. Гриненко В.В. инж. Любивый А.А.

При виконанні даної роботи переді мною стояло питання дослідження різних схем вихідних підсилювачів звукової частоти (Далі ППЗЧ). Для дослідження бралися як класичні лінійні схеми ППЗЧ (Класи АВ, В, С) так і схеми з імпульсним режимом роботи ключового каскаду (D, T).

Дослідження велося з використанням програмного продукту Multisym 11.0 для лінійних схем підсилювачів та Proteus 8.0 для схем з широтно-імпульсною модуляцією.

Були виготовлені діючі макети підсилювачів класів АВ (класична схема з глибоким ЗНЗЗ та схемою Дарлінгтона у вихідному каскаді) та D та було проведено порівняння параметрів ППЗЧ лінійного та імпульсного режимів. У якості вимірювального приладу використовувався вимірювальний USB АЦП DF-430 (Що виконував роль осцилографа та аналізатора спектру.) Розрахунок коефіцієнту нелінійних спотворень виконувався за допомогою програми MAPLE 8 по алгоритму описаному в літературі при обробці вихідного сигналу ППЗЧ (сигнал знімався з виводів динамічної головки)

Крім того метою роботи було вивчення доцільності використання в імпульсних підсилювачах широтно-імпульсної модуляції з цифровою чи аналоговою генерацією несучої.

Аналоговий спосіб генерації полягає в тому що на один вхід компаратора подається вхідний сигнал, а на інший з генератора пилоподібної напруги, сигнал несучої. Суттєвою перевагою описаного способу є простота схемної реалізації і відсутність дорогих комплектуючих.

Недоліком є невисокий ККД і занадто значний коефіцієнт нелінійних спотворень. Крім того досить складно побудувати генератор пилоподібної напруги з високою вірністю вихідного сигналу. (Використання замість лінійного експоненціального сигналу збільшує коефіцієнт спотворень майже на порядок).

Цифровий спосіб генерації (рис. 1) передбачає попередню оцифровку вхідного сигналу, обробку даних сигнальним процесором і

генерацію широтно промодульованих імпульсів. Даний спосіб має дуже високий ККД (до 95%) і коефіцієнт спотворень, що близький до значень підсилувачів побудованих по схемі АВ. Але цифровий метод передбачає використання досить складних мікропроцесорних компонентів і складний в схемній реалізації.

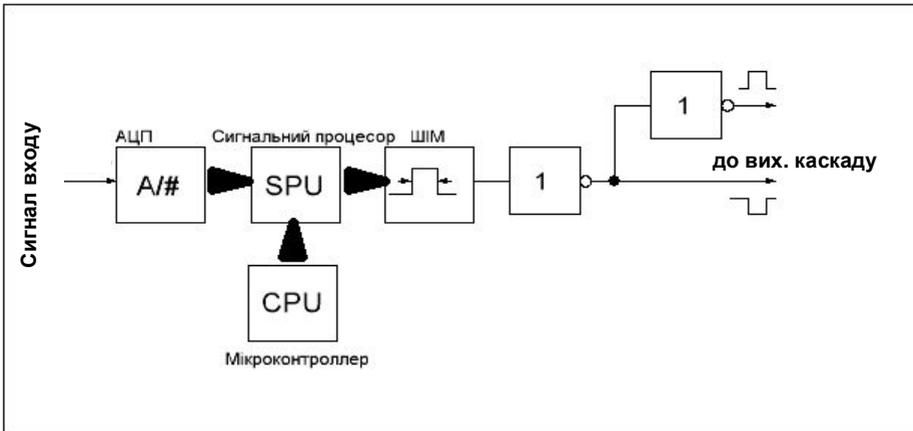


Рисунок 1 Блок-схема цифрового ШІМ класу D

Проведена робота показала можливість створення діючих ППЗЧ класу D без використання спеціалізованих мікросхем на основі широкодоступної елементної бази.

В результаті проведеної роботи було визначено:

- використання аналогового методу модуляції доцільне лише в тих випадках, коли по тим чи іншим причинам допустимі високі нелінійні спотворення;

- ППЗЧ класу D доцільно використовувати лише при необхідності отримати велику вихідну потужність, де нівелюються висока складність схеми ППЗЧ (особливо цифрового ШІМ) та високий (~ 1%) коефіцієнт нелінійних спотворень;

- при проектуванні ППЗЧ класу D необхідно використовувати методи цифрової обробки сигналу, спрямовані на зменшення нелінійних спотворень (в найпростішому випадку зменшувати кратні гармоніки несучої).

## **БИНОМИАЛЬНЫЕ СЧЕТНЫЕ УСТРОЙСТВА**

*проф. Борисенко А.А., студ. Петров В.В.*

Имеются две основные тенденции в развитии средств обработки данных - применение микропроцессоров и создание достаточно полного набора микроэлектронных устройств. Первая предусматривает программный, вторая - схемотехнический способ реализации вычислительных функций. Схемная реализация по сравнению с программной имеет во много раз большую скорость выполнения операций и поэтому незаменима в устройствах работающих в реальном масштабе времени.

Особое место среди схем, применяемых для обработки данных, занимают счетчики. К ним можно отнести любое устройство, которое в процессе работы проходит сквозь несколько своих состояний.

Широкое применение счетчиков требует повышения их надежности, в частности, помехоустойчивости. Последнее свойство достигается введением в счетчики запрещенных состояний. Однако их обнаружение выливается подчас в довольно сложную задачу и требует разработки дополнительно к счетчику контролирующего устройства, за правильностью работы которого необходимо следить дополнительно. Счетчик при этом приобретает неоднородную структуру, которую непросто проектировать и отлаживать, а его надежность в некоторых случаях может даже снижаться.

Преодолеть указанные противоречия можно путем применения помехоустойчивых систем счисления. Разработанные на их основе счетчики однородны и помехоустойчивы и при этом не содержат специального контролирующего устройства.

Достоинством таких счетчиков является возможность перебирать комбинаторные конфигурации: сочетания, сочетания с повторениями, перестановки и т. д. Таким образом, счетчики помехоустойчивых систем счисления обладают немаловажными достоинствами - помехоустойчивостью и многофункциональностью. К этому классу устройств принадлежат счетчики, работающие в биномиальной системе счисления - биномиальные счетчики. Важной их особенностью является значительное уменьшение аппаратуры, необходимой для дешифрации их состояний. Кроме того, эти счетчики позволяют изменением коэффициента пересчета, адаптироваться к интенсивности и характеру помех.

Наиболее перспективно применение биномиальных счетчиков в специализированных помехоустойчивых устройствах автоматики и телемеханики в качестве надежных распределителей импульсов, пересчетных схем, переключаемых помехоустойчивых счетчиков, кодирующих и декодирующих устройств, автоматике и вычислительной технике.

## **МОДУЛЬ ВВОДА АНАЛОГОВЫХ ДАННЫХ В ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР**

*студ. Тимохин В.А., инж. Гапич В.Н., доц. Новгородцев А.И.*

Применяя микропроцессоры и персональный компьютер для управления и контроля сложными производственными процессами, можно обрабатывать в реальном масштабе времени сигналы, поступающие одновременно от многих источников и датчиков, и восстанавливать аналоговую информацию на выходе МП или персонального компьютера, а также распределять ее между различными потребителями (исполнительными устройствами). При этом перед пользователем возникает задача аналого-цифрового и цифроаналогового преобразования многоканальной информации, имеющей некоторые особенности, связанные с различием характеристик сигналов отдельных каналов: динамического диапазона изменения, уровня помех, частотного спектра и т. д. Отсюда вытекает необходимость нормализации сигналов различных датчиков.

Устройства, осуществляющие нормализацию и аналого-цифровое преобразование сигналов с последующим вводом информации в микропроцессор или персональный компьютер, называют системами сбора данных (ССД), а устройства, обеспечивающие восстановление аналоговой информации на выходе микропроцессора или персонального компьютера, системами распределения данных (СРД).

Обычно источники сигналов и каналы связи располагают вблизи от агрегатов энергетических установок, электрических кабелей и другого электротехнического оборудования, которое является источником помех. Помехи вносят погрешности в аналоговые сигналы и искажают цифровые данные. Поэтому одной из основных задач ССД является улучшение качества сигналов, поступающих от различных датчиков. Качество сигнала в наиболее компактной форме выражается в виде отношения сигнал/шум в тракте от аналогового входа до цифрового выхода АЦП. Это отношение является универсальным показателем, позволяющим оценить характеристику ССД, основной задачей которой является получение такого соотношения сигнал/шум в каждом канале ССД, которое обеспечило бы требуемую точность преобразования и длину слова на входе микропроцессора или персонального компьютера. Действительно, нетрудно показать, что использование

многоразрядного АЦП будет оправданным только тогда, когда обеспечивается достаточное отношение сигнал/шум на входе преобразователя, иначе младшие разряды АЦП бесполезны, так как воспроизводят лишь помехи. Широко распространены структуры ССД с мультиплексированием аналоговых и цифровых сигналов, позволяющие обеспечить высокую производительность и качество преобразования.

В текущее время широкой популярности приобретают компьютерные средства обработки информации. Ввод нескольких контролируемых параметров (преобразованы к уровню напряжения) с помощью микропроцессорной подсистемы ввода данных может быть экономически неоправданно. В данной ситуации целесообразно применить устройство преобразования аналоговой величины и непосредственного ввода в компьютер. Структурная схема такого устройства приведена на рисунке 1.

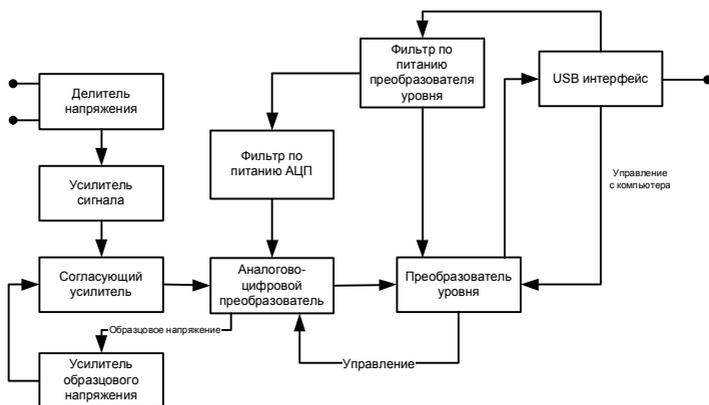


Рисунок 1 – Схема электрическая структурная

Данное устройство может применяться в малых системах ввода аналоговых данных с контролируемых объектов, на технологических линиях, на этапе отладки программного обеспечения микроконтроллера как средство отладки и как средство контроля правильности работы микропроцессорной системы в целом и конкретно программной части.

## МЕТОД ВЫЧИСЛЕНИЯ БИНОМИАЛЬНЫХ КОЭФФИЦИЕНТОВ НА ОСНОВЕ КАНОНИЧЕСКОЙ ФОРМЫ ЗАПИСИ ЧИСЕЛ

Скордина Е.М., студ. гр. ЕС-42  
Науч. руковод. доц. Кулик И.А.

Целый ряд устройств и методов нумерационного кодирования требуют подсчёта чисел сочетаний  $C_n^k$  для различных длин  $n$  двоичных последовательностей и числа  $k$ , содержащихся в них единиц. Достаточно большое распространение получили методы нумерационного кодирования на основе биномиальных систем счисления, в качестве весовых коэффициентов которых применяются числа сочетаний  $C_n^k$ . Эффективность методов биномиального кодирования, например методов биномиального сжатия, прямо пропорционально зависит от значений  $n$  и  $k$ . Следовательно, актуальной является задача вычисления биномиальных коэффициентов  $C_n^k$  при больших длинах  $n$  двоичных комбинаций и  $k$ , содержащихся в них единиц.

Традиционные методы подсчета биномиальных коэффициентов  $C_n^k$  при больших значениях  $n$  и  $k$  достаточно трудно реализовать на практике по следующим причинам:

- 1) громоздкость вычислений, связанных с подсчётом факториалов  $n!$  и  $k!$ ;
- 2) сложность представления конечного результата, достигающего огромных значений (например, при  $n=500$  и  $k=250$  –  $C_{500}^{250} \approx 1,17 \times 10^{149}$ ).

Особую остроту эти трудности приобретают при построении специализированных устройств подсчёта  $C_n^k$  и устройств нумерационного кодирования на основе биномиальных систем счисления.

Для устранения указанных недостатков предлагается при вычислении биномиальных коэффициентов  $C_n^k$  с большими значениями  $n$  и  $k$  использовать каноническую форму записи чисел. Тогда произведение и деление над численными значениями в формуле для подсчёта

$C_n^k$  могут быть заменены операциями сложения и вычитания над степенями простых чисел их составляющих, как показано в выражении (1):

$$C_n^k = f(n, k) = \frac{n!}{k!(n-k)!} = \frac{q_1^{a_1} \cdot q_2^{a_2} \cdot \dots \cdot q_m^{a_m}}{(q_1^{b_1} \cdot q_2^{b_2} \cdot \dots \cdot q_m^{b_m}) \cdot (q_1^{c_1} \cdot q_2^{c_2} \cdot \dots \cdot q_m^{c_m})} = \quad (1)$$

$$= q_1^{a_1-b_1-c_1} \cdot q_2^{a_2-b_2-c_2} \cdot \dots \cdot q_m^{a_m-b_m-c_m}.$$

Чтобы дополнительно упростить процесс вычисления биномиальных коэффициентов и сократить при этом время проведения вычислительных операций в данной работе была так же исследована структура числа сочетаний  $C_n^k$ . В результате анализа разложения биномиальных коэффициентов получены следующие утверждения:

1) для представления числа сочетаний в канонической форме  $C_n^k = q_1^{a_1} \times q_2^{a_2} \times \dots \times q_j^{a_j} \times \dots \times q_m^{a_m}$  достаточен набор простых чисел  $q_j$ , значения которых не больше  $n$ , т.е.  $q_j \leq n$  при  $j = 1, 2, \dots, m$ ;

2) число сочетаний  $C_n^k$  в канонической форме записи содержит весь ряд простых чисел, для которого выполняется условие:  $q_j \geq n - k + 1, k \leq \frac{n}{2}$  и  $q_j \geq k + 1, k > \frac{n}{2}$ , для каждого из которых показатель степени будет равен единице  $a_j = 1, j = 1, 2, \dots, m$ .

В заключение можно сказать, что предложенный подход к вычислению числа сочетаний  $C_n^k$  на основе канонической формы его записи позволяет:

1) существенно уменьшить время вычисления биномиальных коэффициентов;

2) сократить объём памяти для хранения промежуточных и конечных значений при вычислении  $C_n^k$ ;

3) позволяет упростить построение специализированных устройств вычисления чисел сочетаний  $C_n^k$  и нумерационного кодирования на основе биномиальных систем счисления.

## ДВОИЧНО-КАНОНИЧЕСКАЯ ФОРМА ЗАПИСИ ЧИСЕЛ СОЧЕТАНИЙ

Скордина Е.М., студ. гр. ЕС-42  
Научн. руковод. доц. Кулик И.А.

Часто в практике нумерационного кодирования возникает необходимость оперировать большими числами, например числами сочетаний  $C_n^k$  при больших значениях  $n$  и  $k$ , где  $n$  – длина кодируемых двоичных последовательностей, а  $k$  – количество содержащихся в них единиц. Но хранение и оперирование огромными числами  $C_n^k$  связано с необходимостью использования большого количества двоичных разрядов. Следовательно, необходимо разработать метод представления больших чисел  $C_n^k$  при больших параметрах  $n$  и  $k$ . В связи с этим предлагается к рассмотрению разработанная двоично-каноническая форма записи числа, основанная на разложении его на простые числа:

$$z = q_1^{a_1} q_2^{a_2} \dots q_j^{a_j} \dots q_m^{a_m},$$

где  $q_j$  –  $j$ -й элемент ряда простых чисел,  $j = 1, 2, \dots, m$ ;

$a_j$  – показатель степени простого числа  $q_j$ ;

$m$  – количество простых чисел  $q_j$ , необходимых для представления числа  $z$ .

С целью разработки экономичного метода представления больших чисел  $C_n^k$  были проведены исследования свойств канонического разложения биномиальных коэффициентов:

1) для представления числа сочетаний в канонической форме  $C_n^k = q_1^{a_1} \times q_2^{a_2} \times \dots \times q_j^{a_j} \times \dots \times q_m^{a_m}$  достаточен набор простых чисел  $q_j$ , значения которых не больше  $n$ , то есть  $q_j \leq n$  при  $j = 1, 2, \dots, m$ ;

2) число сочетаний  $C_n^k$  в канонической форме записи содержит весь ряд простых чисел  $q_j$ , для которого выполняются условия:

$q_j \geq n - k + 1, k \leq \frac{n}{2}$  и  $q_j \geq k + 1, k > \frac{n}{2}$ , для каждого из которых показатель степени будет равен единице  $a_j = 1, j = 1, 2, \dots, m$ .

С учетом найденных свойств разложения чисел сочетаний  $C_n^k$  предлагаемый метод представления при больших значениях  $n$  и  $k$  позволяет существенно сократить количество двоичных разрядов, необходимых для хранения биномиальных коэффициентов  $C_n^k$ .

Например, процесс нахождения простых множителей и их степеней с учётом приведенных свойств выглядит следующим образом:

$$C_{50}^{17} = 2^{16} \cdot 3^7 \cdot 5^5 \cdot 7^4 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 37 \cdot 41 \cdot 43 \cdot 47.$$

При этом, кодируя показатели степени двоичным кодом, получаем:

$$1111.111.101.100.1.1.1.1.1.0.0.1.1.1.1,$$

то есть для записи числа  $C_{50}^{17}$  необходимо 24 разряда в отличие от обычного двоичного кодирования, требующего 46 разрядов. Таким образом, экономия двоичных разрядов, необходимых для представления и хранения числа сочетания  $C_{50}^{17}$  в двоично-каноническом виде, составляет  $46/24 \approx 1,9$  раза.

Для однозначности представления в двоично-канонической форме степени простых множителей предлагается записывать в префиксном коде, например биномиальном, тем самым легко определяется начало и конец степени простого числа. Кроме того, использование двоично-канонической формы записи чисел позволяет свести операции произведения и деления к сложению и вычитанию степеней соответствующих простых чисел.

Таким образом, двоично-каноническая форма представления чисел сочетаний  $C_n^k$  позволяет:

1) в значительной мере сократить количество используемых двоичных разрядов для хранения биномиальных коэффициентов;

упростить вычисления над числами  $C_n^k$ , а также подсчет самих чисел  $C_n^k$ , путем замены операций умножения и деления более простыми операциями сложения и вычитания.

## АНАЛИЗ ИЗВЕСТНЫХ МЕТОДОВ ДЕКОДИРОВАНИЯ НЕДВОИЧНЫХ БЛОКОВЫХ КОДОВ

**студ. Лысенко АВ, доц. Онанченко Е.Л.**

Развитие информационно телекоммуникационных сетей (ИТС) тесно связано с повышением скорости и достоверности обработки и передачи информации. Решение этой проблемы за счет повышения энергетических ресурсов системы практически себя исчерпало. Одно из направлений, которое получило мировое развитие связывают с разработкой теории и практики построения избыточных кодов с заданными характеристиками.

В этой отрасли науки получены фундаментальные теоретические результаты, разработаны и внедрены практические методы кодирования и декодирования помехоустойчивых кодов.

В основе большинства известных методов декодирования недвоичных блоковых кодов лежат различные модификации отдельных этапов декодера Питерсона-Горенштейна-Цирлера. Схема декодирования Питерсона-Горенштейна-Цирлера ориентирована на декодирование кодов БЧХ (кодов Рида-Соломона в том числе).

Схема декодирования Питерсона-Горенштейна-Цирлера использует разные алгоритмы например Берлекемпа. Суть алгоритма Берлекемпа состоит в синтезе регистра сдвига наименьшей длины с линейной обратной связью, генерирующего последовательность синдромов (синдромный вектор). Реализация второго этапа декодирования при использовании алгоритма Берлекемпа требует порядка  $t^2$  операций.

Сейчас разработаны модифицированные алгоритмы Берлекемпа, позволяющие снизить сложность декодирования, ускорить быстродействие (алгоритм Берлекемпа–Месси и его модификации).

Алгоритм Евклида состоит в нахождении наибольшего общего делителя двух многочленов при решении ключевого уравнения. Алгоритм Евклида по числу операций сравним с алгоритмом Берлекемпа. Подробное решение задачи декодирования кодов БЧХ с помощью введенного в рассмотрение многочлена локаторов ошибок.

На следующем этапе алгебраического декодирования вычисляются локаторы, однозначно указывающие на положение ошибок.

## АЛГОРИТМ ГЕНЕРАЦИИ ПЕРЕСТАНОВОК НА ОСНОВЕ ФАКТОРИАЛЬНЫХ ЧИСЕЛ

*проф. Борисенко А.А., асп. Горячев А.Е.*

Перестановки широко и эффективно используются на практике для решения ряда комбинаторных задач, помехоустойчивой передачи данных и их защите от несанкционированного доступа. Таким образом, необходима разработка универсальных методов, позволяющих быстро генерировать перестановки в произвольном или заданном порядке. Одним из таких методов является использование факториальных чисел.

Нумерационная функция факториальной системы счисления имеет вид:

$$F_{\langle \phi \rangle} = X_n \cdot n! + X_{n-1} \cdot (n-1)! + \dots + X_i \cdot i! + \dots + X_1 \cdot 1! + X_0 \cdot 0!,$$

где  $i = 0, 1, \dots, 0 \leq X_i \leq i$ .

Переход от факториального числа к перестановке осуществляется в соответствии со следующим алгоритмом: цифра каждого разряда числа сравнивается последовательно с цифрами старших его разрядов, начиная с минимального значения. Если значение рассматриваемого разряда больше значения старшего разряда, то необходимо увеличить его на 1, в противном случае оно остаётся без изменений. Таким образом значение первого элемента перестановки  $V_n$  всегда соответствует значению максимального разряда факториального числа  $X_n$ , для получения элемента  $V_{n-1}$  значение разряда  $X_{n-1}$  сравнивается с  $X_n$  и так далее.

Для осуществления обратного перехода необходимо каждый элемент перестановки уменьшить на число единиц, равное количеству предыдущих элементов перестановки, меньших данного.

Предложенный алгоритм генерации перестановок на основе факториальных чисел позволяет снизить затраты времени на получение перестановок, кроме того упростить техническую реализацию систем, генерирующих перестановки. Также важными достоинствами метода являются простота преобразования десятичных чисел в факториальные и обратно, способность факториальных систем счисления к выявлению и исправлению ошибок.