выделены следующие множества: множество источников $I=\{ii: i=1...i0\}$ и исполнителей $P=\{pj: j=1...j0\}$, множество элементов информационного потока $R=\{rkij: k=1,...,k0, i=1,...,i0, j=1...j_0\}$, множество принадлежности заданий $W=\{Wl: l=1...l0\}$ и множества источников $Ii^*=\{Ii:I \in \{1,i0\}\}$ и исполнителей $Pj^*=\{Pj: j \in \{1,j0\}\}$, создающие "узкие места".

3. Описание алгоритма

На первом этапе алгоритма формируются множества источников $I=\{i_i: i=1...i_0\}$ и исполнителей $P=\{p_j: j=1...j_0\}$, определяются их характеристики (свойства, технические характеристики, параметры и т. д.), задаются виды параметров состояний w для заданий R.

На втором этапе формируются подмножества $r_{kij,}$ соответствующие каждому i_i. При этом для каждого r_{kij} задается время $t_{ij,}$ необходимое для его обработки исполнителем $p_{j.}$ Далее все элементы r_{kij} объединяются в один информационный поток, который направлен от источников I к исполнителям P.

На следующем этапе элементы информационного потока объединяются в подмножества r'_{kij}, соответствующие конкретным исполнителям информации p_j. Каждый r_{kij} характеризуется параметром состояния w(R), определяющим степень обработки элемента r_{kij}. Состояние определяется набором значений, которые могут принимать задания множества R в любой момент времени. На основании значений параметра w(R), а также текущего времени и множества R формируется множество $W=\{W_l: l=1...l_0\}$, которое образует группы элементов R'_{kij}, принадлежащих конкретному исполнителю p_j.

Каждое множество W_l позволяет отслеживать в любой момент времени состояние элементов r'_{kij} информационного потока, а также определять их принадлежность к источникам i_i и исполнителям p_j.

На заключительном этапе осуществляется анализ элементов множества W' и формируются множества источников I^* и исполнителей P^*, элементы которых образуют “узкие места” в работе системы.

Рассматриваемая процедура, названная “групповым контролем”, ориентирована на описание функционирования информационной системы для систем большой размерности. Процедуры группового контроля позволяют накапливать статистические данные по обработке информационного потока, подмножества исполнителей, регулярно не справляющихся с обработкой, и группу источников, генерирующих особо сложные для выполнения задания.

Задачи группового контроля дискретной системы имеют широкий спектр применения, например диспетчерские задачи (контроль материального потока), контроль состояния оборудования (работоспособность элементов оборудования), потока документов.

Выводы

Разработанная математическая модель связи элементов системы позволяет сформировать корректную постановку задачи на разработку дисциплины обслуживания заявок. Предлагаемые процедуры контроля позволяют не только решить локальные задачи мониторинга системы, но и выявить причины понижения эффективности функционирования всей системы.

Литература: 1. Groupware enablers and business solutions / *Morton Marjorie S., Holman Richard A., Bess David A.* // IEEE Int. Conf. Syst., Man. and Cybern. Emergent Innov. Inf. Transfer Process and Decis. Mak., Chicago, I11., Oct. 18 − 21, 1992. Vol. 2. Piscataway (N.J.), 1992. P. 943-948. 2. Автоматизация подготовки учебных планов и поручений в информационно- справочной системе “Деканат − студент” / *Рындин А.А., Туренко И.И., Шишкин В.М.* // Компьютериз. в мед. /Воронежский политехнический институт. Воронеж, 1993. С.143− 146. 3. Автоматизированная система обработки информации и управления: Межвуз.сб.научн.тр. / Новочеркаский политехнический институт / Ред. *Черноморов Г.А.* Новочеркасск, 1993. 107 с. 4. Информационные системы для обеспечения деятельности кафедр высших учебных заведений / *Гайдаров К.А.* Изв.вузов. Геод. и аэрофотосъемка. 1992. N2. С.166-176.

Поступила в редколлегию 25.05.98

Рецензент: д-р техн. наук, проф. Хажмурадов М.А.

Саенко Владимир Иванович, канд. техн. наук, доцент кафедры информационных управляющих систем ХТУРЭ. Научные интересы: администрирование, мониторинг и управление процессами в компьютерных сетях. Увлечения: филателия. Адрес: 310726, Украина, Харьков, пр. Ленина, 14. тел. 40-94-51.

Клименко Александр Васильевич, старший преподаватель кафедры ИУС ХТУРЭ. Научные интересы: управление распределенными информационными системами. Увлечения и хобби: путешествия. Служебный адрес: 310726, Украина, Харьков, пр. Ленина 14, тел.40-94-51.

УДК 519.15:725

ПРИНЦИПЫ ПОСТРОЕНИЯ ОТДЕЛЬНЫХ КОМПОНЕНТОВ k−ЗНАЧНЫХ СТРУКТУР ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ЧЕТВЕРИКОВ Г.Г., СТОРОЖЕНКО А.В., РЕВЕНЧУК И.А., БАВЫКИН В.Н.

Предложен подход и общие принципы построения сверхбыстродействующих структур систем искусственного интеллекта, цифровых систем, систем коммуникаций. Предельное быстродействие пространственных структур достигается за счет введения функции коммутации в промежуточные одноступенчатые линейные дешифраторы синтезируемых структур.

Практическая реализация k-значного кодирования начинается построением двузначно-k-значных преобразователей (устройств внешнего обмена (УВО)), которые широко примененяются во всех системах связи с импульсно-кодовой модуляцией. Преимущество разных видов УВО с k-значным кодированием позволяет прогнозировать их применение в современных сверхбыстродействующих системах управления связью, обработки данных и для создания ИИ [1]. Особенно эффективно применение УВО с подбором соответствующих информационных признаков в разнообразных системах и сетях телекоммуникаций, для которых характерны высокие требования к производительности. Необходимость обработки данных в реальном масштабе времени обуславливает жесткие требования к быстродействию блоков и узлов систем телекоммуникаций. Кроме этого, часто приходится передавать

параллельным образом многоразрядные двузначные слова, что требует большого числа функциональных связей и приводит к увеличению количества линий связи как на элементном, так и на структурном и системном уровнях. В целях повышения пропускной способности УВО в системах телекоммуникаций предлагается использовать многоуровневое (k–значное) кодирование.

Применение k-значного кодирования позволяет в $\log_2 k$ раз понизить число функциональных связей без потери пропускной способности интерфейса системы, а также уменьшить массу, габаритные размеры и стоимость соединительных разъемов и кабелей. В данный момент для повышения пропускной способности двузначных каналов внешнего обмена применяется: 1) повышение тактовой частоты коммутации сообщений; 2) передача однобитных сообщений через отдельные параллельные линии связи.

Оба эти пути имеют ряд недостатков. Первый путь характеризуется физическими ограничениями для тактовой частоты, связанными с возможностью УВО в микроэлектронном исполнении работать с частотами не выше определенного граничного значения, а также энергетическими ограничениями, которые определяют скорость переключения микросхем и имеют максимальное значение для определенных типов корпусов микросхем. Второй путь характеризуется тем, что чем больший объем данных необходимо передавать, тем большее число соединений нужно осуществлять. Увеличение количества кабельных связей ведет к возрастанию массы, габаритных размеров и стоимости аппаратуры, понижает надежность.

Возможным выходом из создавшегося положения является использование многозначного кодирования сообщений, которые передаются через канал внешнего обмена с помощью устройств внешнего обмена, построенных с использованием различных видов схемотехники.

В зависимости от отрасли применения УВО подразделяются на две группы: 1) для обмена между корпусами БИС и печатными платами; 2) для межблочного и межсистемного обмена.

Обмен между корпусами БИС и ТЭЗами в настоящее время осуществляется с применением КМОП–схемотехники, межблочный и межсистемный обмен – с применением КМОП и гибридной схемотехники. В свою очередь, по принципу действия УВО делятся на однонаправленные и дуплексные. Дуплексный обмен осуществляется с использованием $I^2Л$ и гибридной схемотехники. Применение многозначной логической системы прогнозируется в комплексе с двухзначной в виде операционных средств обмена данными между отдельными корпусами БИС, блоками и системами: комбинационных схем и функциональных блоков вычислительной техники; микропрограммных автоматов; процессоров обработки сигналов; адаптивных и самоорганизационных систем [2].

Разнородность перечисленных признаков классификации радиоэлектронных средств многозначных систем объясняется разнообразием требований, противоречий и проблем, которые решаются многозначной логической системой во время ее разработки, создания и использования.

Так как некоторый канал связи характеризуется отношением сигнал/шум, существенной при организации многозначного канала связи является задача обеспечения высокой помехоустойчивости сообщений, которые передаются. Преобразование двоичных кодовых сообщений в многозначный код проще всего реализуется при преобразовании потенциальных двузначных кодовых сообщений в потоковые многоуровневые сообщения. Поэтому во время передачи сигналов в канал внешнего обмена необходимо отдавать потоковые сообщения, которые бы существенно превышали уровни наведенных токов помех и обеспечивали помехоустойчивость сообщений.

Рассмотрим детальнее вопросы организации канала обмена с многозначным кодированием. В таблице приведены соответствия многозначных и двузначных кодов, а также токов, которые соответствуют данным значениям кодов. (ДК – значение двоичного кода; МК – значения многозначных кодов; УТ – значения уровней тока, которые посылают в канал связи, мкА; звездочкой отмечены уровни токов, которые соответствуют унитарным значениям двоичного кода и могут служить основой для формирования всех остальных значений уровней k-значных сигналов; тире — отсутствие какой-либо значности для заданной совокупности значений двоичного кода и одноразрядного k). Значения основ многозначных кодов могут быть выбраны, исходя из тех соображений, что связь между двузначным и многозначным кодом является простейшей тогда, когда основа кода – целое число и степень двойки. Кроме этого, в современных ЭВМ для задач ввода данных используются именно такие высшие основы кодов.

Значения уровней тока, которые передаются в канал связи, выбраны исходя из опыта, а также с учетом требования помехоустойчивости линий каналов связи. Принимая шаг квантования порядка 5 мкА для $I^2Л$-схем, из таблицы получаем диапазон изменения токов, которые направляются в линию связи от 5 до 75 мкА, когда k пробегает значения, которые реализуются УВО, от 4 до 16.

Рассмотрим теперь логический синтез промежуточных пространственных дешифраторов. УВО структурно имеет с передающей стороны входной дешифратор позиционного (двузначного) кода в пространственный и преобразователь пространственного кода в k-значный, а с приемной – преобразователь k-значного кода в пространственный и выходной дешифратор пространственного кода в двузначный позиционный, аналогичный входному. Входной дешифратор осуществляет преобразование двузначного вектора в унитарный пространственный код, который преобразованием трансформируется в соответствующий многоуровневый сигнал и передается через канал связи.

С приемной стороны преобразователь аналого–цифрового типа осуществляет обратное преобразование многоуровневого сигнала в единичный пространственный код, а выходной дешифратор формирует из последнего двузначный позиционный код, аналогичный входному.

Структура и особенности принципов действия дешифраторов зависят от ориентации на параллельную работу для получения предельно высокого

Д К	МК			УТ		
	к=4	к=8	к=16	к=4	к=8	к=16
0000	0	0	0	0	0	0
0001	1	1	1	5*	5*	5*
0010	2	2	2	10*	10*	10*
0011	3	3	3	15	15	15
0100	–	4	4	–	20*	20*
0101	–	5	5	–	25	25
0110	–	6	6	–	30	30
0111	–	7	7	–	35	35
1000	–	–	8	–	–	40*
1001	–	–	9	–	–	45
1010	–	–	10	–	–	50
1011	–	–	11	–	–	55
1100	–	–	12	–	–	60
1101	–	–	13	–	–	65
1110	–	–	14	–	–	70
1111	–	–	15	–	–	75

быстродействия и от значности, которая используется в УВО. В целях сравнения и анализа этих отличий возможно совмещение таблиц истинности и математических моделей комбинационных схем для k=4, 8, 16. Выбор значений k связан, во-первых, с тем, что УВО преобразуют позиционные двузначные коды в k-значные, и наоборот – k-значные в двузначные. Такое преобразование, как уже отмечалось ранее, удобнее всего осуществлять, если $k=2^n$, где n – число разрядов двузначного кода, тогда коэффициент сжатия $e=\log_2 k$ и для k=4 - e=2, для k=8 - e=3, для k=16 - e=4. Во–вторых, выбор верхнего значения k связан с исследованиями [3] взаимосвязи значности и жесткости допуска на шаг квантования в k-значных микроэлектроник-структурах, которые ограничили верхнее значение на указанном уровне. Дальнейшее повышение значности означает перемещение из области k-значных структур в область аналого-цифровых устройств, где методы построения и принципы действия несколько иные.

Входные дешифраторы предельного быстродействия синтезированы по структуре одноступенчатых линейных дешифраторов, а выходные – по структуре усеченного параллельно-последовательного сумматора, поскольку его входные сигналы никогда не пробегают всего множества значений. Последовательность в алгоритме и структуре возникает в силу необходимости анализировать во время суммирования многоразрядных чисел межразрядные связи и переносы.

Регулярность значений таблиц истинности и структур дешифраторов при k=4,8,16 позволяет построить два максимальных варианта входного и выходного дешифраторов для k=16, которые состоят из однотипных субблоков дешифрации. Дополнительно обратим внимание на то, что полученная однородность структур есть проявление и следствие применения принципа симбиоза: синтезированные структуры как входного, так и выходного дешифраторов в максимальном варианте k=16 включают в состав все субблоки дешифрации предыдущих значимостей.

Литература: 1. *Бондаренко М.Ф., Коноплянко З.Д., Четвериков Г.Г.* Основи теорії синтезу надшвидкодіючих структур мовних систем штучного інтелекту. К.: ІЗМН, 1997.264 с. 2. *Коноплянко З.Д.* Принципы построения многозначных систем искусственного интелекта // Проблемы бионики. Х.: Основа, 1990. Вып. 45. С. 27–35. 3. *Четвериков Г.Г.* Многозначные структуры (анализ, сравнение, синтез, обобщение). Ч.1: Учеб. пособие. К.: ИСМО, 1997.192 с. 4. *А.с. 1241483 СССР, МКИ НОЗМ 7/00.* Модуль для преобразования кодов, заданных логическими уравнениями / Г.Г. Четвериков, М.Ф. Бондаренко, Ю.П. Шабанов-Кушнаренко (СССР) // Открытия. Изобретения. 1984. №3844735/24–24.

Рецензент: д-р физ.-мат. наук, проф. Яковлев С.В.

Четвериков Григорий Григорьевич, канд. техн. наук, доцент кафедры ПО ЭВМ ХТУРЭ. Научные интересы: разработка теории и практика использования методов синтеза многозначных структур языковых систем искусственного интеллекта. Адрес: 310726, Украина, Харьков, пр. Ленина, 14, тел. 40-94-46, 27-97-48.

Стороженко Александра Владимировна, асистент кафедры экономики и менеджмента ХТУРЭ. Научные интересы: мнгозначные структуры в системах искусственного интеллекта. Адрес: 310726, Украина, Харьков, пр. Ленина, 14, тел. 40-94-46, 43-49-02.

Ревенчук Илона Анатольевна, аспирант кафедры ПО ЭВМ ХТУРЭ. Научные интересы: архитектура и принципы построения цифровых многозначных элементов и структур. Адрес: 310726, Украина, Харьков, пр. Ленина, 14, тел. 40-94-46.

Бавыкин Виктор Николаевич: асприрант кафедры ПО ЭВМ ХТУРЭ. Научные интересы: многозначные структуры в системах искусственного интеллекта. Адрес: 310726, Украина, Харьков, пр. Ленина, 14, тел. 40-94-46.

УДК 681.3.06: 519.248.681

ПОСТРОЕНИЕ СИЛЬНЫХ ПРОСТЫХ ЧИСЕЛ ДЛЯ НЕСИММЕТРИЧНЫХ КРИПТОСИСТЕМ

ГОРБЕНКО И.Д., ЖИЛИН О.В.

Работа посвящена проблеме построения аналитически простых чисел специального вида. Требуемый вид результирующего числа N обеспечивается заранее известным разложением N±1. Проведены необходимые теоретические исследования, и на их основании разработан и реализован алгоритм построения простых чисел нужного вида. Выполнены экспериментальные исследования и анализ вычислительной сложности разработанных алгоритмов.

Введение

В несимметричных криптографических системах в качестве общесистемного параметра используются большие простые числа. В наиболее широко распространенном алгоритме RSA [1] в качестве общего модуля используется число N – произведение двух “сильных” простых чисел P и Q. Для реализации алгоритмов шифрования и цифровой подписи класса Эль-Гамаля [2], а также протокола распространения ключей Диффи-Хелмана [3] необходимы простые числа специального вида.

Методы получения простых чисел можно разделить на три группы. К первой относятся методы, основанные на вероятностных тестах. Наиболее широко применяются тесты Соловея-Штрассена [4], Рабина-Миллера [5], Бейли-Вагстаффа [6]. После применения каждого теста можно либо с определенной вероятностью утверждать, что число про-