МИНОБРНАУКИ РОССИИ Федеральное государственное бюджетное образовательное учреждение
высшего образования «Хакасский государственный университет им. Н.Ф. Катанова»
Колледж педагогического образования, информатики и права

ПЦК естественнонаучных дисциплин, математики и информатики

РЕФЕРАТ

на тему:
Применение теории кодирования для повышения помехозащищенности комбинационных схем

Автор реферата: _____ Сургутский Д. В.
(подпись) (инициалы, фамилия)

Специальность: 230115 - Программирование в компьютерных системах

Курс: II Группа: И -21
Зачет/незачет:_____
Руководитель: _____ _Когумбаева О.П.
(подпись, дата) (инициалы, фамилия)

г. Абакан, 2017г.

Введение

Среди известных подходов к проектированию помехоустойчивых интегральных схем (ИС) широко распространено дублирование с выбором результата по мажоритарному принципу. Традиционным методом повышения отказоустойчивости при информационных сбоях в каналах связи является помехоустойчивое кодирование. Для парирования информационных сбоев, возникших в результате сбоев аппаратных, возможно использование следующих подходов - Аппаратное и информационное резервирование.

Актуальность: В последнее время всё больший интерес вызывают попытки применения для решения данной задачи методов помехоустойчивого кодирования, которые аналогичны по своей сути подходам к защите от помех потоков информации при ее передаче по линиям связи.

Цель: Изучить использование блоковых кодов специального вида.

Задачи: Рассмотреть существующие подходы применения кодирования информации для решения задачи повышения помехозащищенности комбинационных схем. Выяснить, где применяется кодирование.

1. Анализ существующих методов блокового кодирования

1.1. Общие понятия

Кодирование заключается в сопоставлении каждому состоянию автомата набора (кода) состояний элементов памяти. При этом наборы для всех состояний должны иметь одинаковую длину, а разным состояниям автомата должны соответствовать разные наборы. Если элементы памяти двоичные, то их число $R \geq \lceil \log_2 M \rceil$.

Опишем кратко основные положения теории кодов, исправляющих ошибки. Помехоустойчивость кодирования достигается введением избыточности в код. Наиболее простая модель возникновение ошибок - двоичный симметричный канал со случайным некоррелированным информационным потоком, в котором некоторые биты случайно, равновероятно и независимо друг от друга могут оказаться инвертированными, а добавления или стирания бит отсутствуют. При этом могут ставиться задачи автоматического обнаружения и/или исправления ошибок.

Одним из один из возможных подходов к решению проблемы является разбиение потока информации на сообщения – непересекающиеся блоки фиксированной длины k. Каждый блок можно кодировать независимо от других – блоковое кодирование или в зависимости от предыдущих – свёрточное кодирование. В результате вместо сообщений передают кодовые слова длины $n > k$ каждое. Естественно требовать построения кода минимальной длины, позволяющего восстановить сообщение, содержащее не более данного количества r ошибок.

Далее будем рассматривать исключительно блоковое кодирование.

Если кодовое слово длины $n = k + m$ содержит в себе k бит исходного сообщения (информационные биты) и дополнительно ещё m проверочных бит, то говорят о разделимом блоковом кодировании. В неразделимых кодах выделить информационные и проверочные биты невозможно. Величину m/n называют избыточностью кода. Увеличение m ведёт, вообще говоря, к увеличению кодового расстояния d и, следовательно, к увеличению количества ошибок, которые может исправить код. Минимальное расстояние d между словами кода называется кодовым расстоянием. Очевидно у кода, исправляющего r ошибок $d \geqslant 2r + 1$.

Разделимый блоковый код описывают тройкой параметров (n, k, d) или парой (n, k).

Определение кодового расстояния d произвольного кода – сложная задача. Поэтому при создании помехоустойчивых кодов на первый план выходит проблема построения кодов с заданным кодовым расстоянием. Она решается при использовании БЧХ-кодов. На сегодняшний день БЧХ-коды с практически значимыми параметрами уже построены.

Блоковое кодирование есть взаимно-однозначное отображение множества сообщений (всех векторов $u \in 2^k$) во множество кодовых слов (некоторых векторов $v \in 2^n$). Оно всегда может быть осуществлено с использованием таблицы размера $2^k \times n$. Однако такое табличное кодирование весьма неэффективно: значения n и k на практике могут достигать десятков и сотен тысяч. Известны две конструкции т.н. совершенных кодов, плотно заполняющих шарами радиуса r с центрами в кодовых словах весь куб 2^n: это коды Хемминга $(2^q - 1, 2^q - q - 1, 3)$ и код Голея $(23, 12, 7)$.

При передаче по каналу с шумом кодовое слово v превращается в принятое слово $w = v + e$, где e – вектор ошибок. Код Хэмминга может быть построён так, что проверочные биты будут содержать номер (единственной) искажённой позиции принятого слова.

Декодирование состоит в определении сообщения по кодовому слову. Декодирование кодов обычно значительно сложнее кодирования. (исключением являются т. н. экспандерные коды с линейным декодированием, для которых неизвестны субквадратичные алгоритмы кодирования). Декодирование (n, k, d)кода

2^n k

основано на разбиении единичного куба на областей, содержащих шары радиуса $\lfloor (d-1)/2 \rfloor$ с центрами в кодовых словах. Тогда восстановление сообщения переданного сообщения u состоит в (1) определении слова v, ближайшего к полученному w и (2) удалению из v проверочных бит. В общем случае эти операции потребуют использования таблиц экспоненциального по k размера. Таким образом декодирование блокового (n,k)-кода общего вида – весьма ресурсоёмкий процесс и поэтому его использование таких кодов возможно лишь при небольших значениях n и k. Однако, приняв ряд дополнительных ограничений на множество кодовых слов, можно перейти от экспоненциальных требований по памяти и по сложности алгоритмов кодирования/декодирования к линейным по и . Эти ограничения приводят к использованию блоковых кодов специального вида: групповых, а из групповых – циклических.

1.2. Групповые (линейные) коды

Большая часть теории блокового кодирования построена на линейных кодах, образующих векторное подпространство координатного пространства 2^n. В линейных кодах сумма по $mod\ 2$ любых кодовых слов – также кодовое слово. Линейные коды позволяют реализовывать эффективные алгоритмы кодирования/декодирования и в двоичном случае их называют групповыми, т. к. они образуют группу относительно операции «сумма по $mod\ 2$». Линейные (n,k) коды могут быть заданы матрицами - порождающей $G_{n\times k}$ или проверочной $H_{m\times n}$. Для них выполняются соотношения $v = Gu$, $Hv = 0$ для любого кодового слова v, а невыполнение последнего равенства свидетельствует о наличии ошибки.

На практике удобно использовать систематическое кодирование [8], при котором биты сообщения копируются в фиксированные позиции кодового слова, а затем вычисляются остальные проверочные биты. Такая возможность основана на том, что порождающая и проверочная матрицы определены с точностью до эквивалентных преобразований столбцов и строк соответственно, что эквивалентно переходу к другому базису пространствах кодовых слов и ортогонального ему. Фиксирование позиций информационных бит задаёт

порождающую и проверочную матрицы однозначно. При этом второй этап декодирования (удаление проверочных бит) становится тривиальным.

Декодирование групповых кодов проводят с использованием синдромов – векторов $s = Hw \in 2^m$. Вычисление вектора ошибок e сводится к решению СЛАУ $He = s$, которое ищут в виде суммы частного решения данной и общего решения соответствующей однородной системы. После нахождения решения все возможные кодовые слова $u_1, \ldots, u_{2k}$ входного вектора дадут 2^k вариантов вектора ошибок, среди которых выбирают с наименьшим хэмминговым весом.

Таким образом, кодирование групповыми кодами осуществляется умножением вектора сообщения на порождающую матрицу. Декодирование также значительно упрощается по сравнению с общим случаем: используются легко вычисляемые синдромы при элементарном этапе удаления проверочных бит в случае систематического кодирования. Однако алгоритм декодирования линейного кода в общем случае остаётся экспоненциально трудоёмким и по памяти, и по числу операций.

Для линейных кодов, рассчитанных на исправление многократных ошибок, часто более простыми оказываются декодирующие устройства, построенные по мажоритарному принципу. Это метод декодирования называют также принципом голосования или способом декодирования по большинству проверок и тоже базируется на системе проверочных равенств.

1.3. Циклические коды

Циклические коды – подкласс линейных. Код называется циклическим (сдвиговым) (Cyclic Redundancy Code, CRC), если он инвариантен относительно циклических сдвигов.

В теории конечных полей (полей Галуа) показывается, что идеал неприводимого делителя бинома $x^n - 1$ образует циклическое подпространство в факторкольце многочленов $\mathbb{F}_2[x]/(x^n - 1)$ (а циклический сдвиг в нём осуществляется умножением на x). Поэтому для построения циклического кода $g(x)$ $x^n - 1$

выбирают некоторый неприводимый делитель бинома и в качестве кодовых слов рассматривают порождённый им идеал $(g(x))$ – все многочлены, делящиеся на $g(x)$ без остатка. При удачном выборе $g(x)$ коэффициенты многочленов из данного идеала будут давать код с малой избыточностью при большом кодовом расстоянии. Однако известны только несколько конструкций циклических кодов с хорошими параметрами, а в общем случае определение кодового расстояния циклического кода чрезвычайно сложно.

При использовании циклических кодов удобно пользоваться представлением векторов сообщения u и кодового слова v в виде полиномов $u(x), v(x) \in \mathbb{F}_2[x]$: например, $u = [u_0, u_1, \ldots, u_{k-1}]^T \leftrightarrow u(x) = u_0 + u_1 x + \ldots + u_{k-1}x^{k-1}$.

Различают систематическое и несистематическое кодирование циклическими кодами, которое приводит к разделимому и неразделимому кодированию. Несистематическое осуществляется путём умножения кодируемого вектора на $g(x)$: $v(x) = u(x)g(x)$, а систематическое - дописыванием к кодируемому слову остатка $r(x)$ от деления $x^{n-k}u(x)$ на $g(x)$: $v(x) = x^m u(x) + r(x)$ - в этом случае полином $v(x)$ содержит коэффициенты полинома $u(x)$ в крайних правых позициях (т. е. при старших степенях x).

Синдромом $s(x)$ принятого полинома $w(x)$, закодированного циклическим (n, k)-кодом с порождающим полиномом $g(x)$, называют остаток от деления $w(x)$ на $g(x)$ (очевидно, это перефразировка в терминах полиномов синдрома для групповых кодов). Равенство $s(x) = 0$ означает, что, то $w(x)$ – кодовое слово.

Декодирование циклического кода проходит по общей схеме декодирования линейного кода: вычисляется синдром $s(x)$ принятого слова $w(x)$, ищутся решения системы $e(x) = s(x) + g(x)u(x)$ для всех 2^k возможных полиномов $u(x)$ степени $k-1$, определяется полином ошибок как решение с минимальным числом ненулевых слагаемых и, наконец, восстанавливается переданное сообщение $u(x) = w(x) + e(x)$.

Циклические коды общего вида могут иметь произвольную длину n, но, в отличие от линейных, его параметры m и k уже не произвольны. При использовании

циклических кодов вместо матричных умножений и решения СЛАУ используются более простые операции умножения и деления с остатком полиномов, легко реализуемые на регистрах сдвига с обратными связями. Однако общий алгоритм декодирования по-прежнему имеет экспоненциальную сложность по k. Существуют и альтернативные методы декодирования циклических кодов общего вида, но и они не имеют удовлетворительных характеристик.

Таким образом, обнаружение ошибок при помощи циклического кода обеспечивается тем, что в качестве разрешённых комбинаций выбираются такие, которые делятся без остатка на некоторый заранее выбранный порождающий полином. Если принятая комбинация содержит искажённые символы, то такое деление осуществляется с остатком и при этом формируется сигнал, свидетельствующий об ошибке. Большим преимуществом циклических кодов является простота построения кодирующих и декодирующих устройств, которые по своей структуре представляют регистры сдвига с обратными связями.

Важной особенностью комбинационных схем является то, что искажение информации, возникающее при их сбоях, вряд ли адекватно описывается в рамках традиционной описанной выше модели двоичного симметрического канала. Кажется, обоснованным предположение о том, что сбои ИС от описанных выше причин приводят к ошибкам константного (stick-at faults) типа, в результате чего типичной является ситуация либо полного отсутствия, либо наличия сразу достаточно большого количества ошибок.

1.4. Избыточное кодирование выходных данных цифровых комбинационных схем

При использовании избыточного кодирования выходных данных комбинационных схем обычно штатную схему дополняют ещё одной, вычисляющей проверочные биты. Ясно, что в рассматриваемой задаче требования к качеству используемых кодов (избыточность при данном числе обнаруживаемых/исправляемых ошибок) не являются слишком жёсткими: для

реальных схем с длинами входных и выходных векторов в несколько десятков бит разница между «хорошими» и «наилучшими» кодами несущественна и здесь на первый план выходят вопросы простоты практической реализации алгоритмов кодирования и декодирования. При этом имеющиеся технологические и схемные решения позволяют обеспечить существенно более высокий уровень помехозащищённости кодирующей схемы по сравнению с основной, что позволяет считать работу данной схемы безошибочной. Данные решения обосновываются тем, что длина вектора проверочных бит значительно короче вектора бит информационных. Это позволяет предполагать и существенно меньшую сложность кодирующей схемы по сравнению с основной и поэтому затраты на её защиту указанными средствами предполагаются оправданными.

При построении избыточных кодов используют лишь часть возможных комбинаций бит в кодовых словах, которые называют разрешёнными (остальные комбинации запрещённые). Опишем кратко избыточные коды, применяемые и перспективные к применению для повышения помехозащищённости комбинационных схем.

Примером нелинейного избыточного кода является код Бергера, у которого проверочные символы представляют двоичную запись числа единиц (или нулей) в последовательности информационных символов. Например, таким является разделимый систематический $(5,3)$-код

$00000;\ 00101;\ 01001;\ 01111;\ 10001;\ 10110;\ 11010;\ 11111$. Коды Бергера обнаруживают все одиночные ошибки и некоторую часть многократных.

Существует два основных методов декодирования рассматриваемых кодов: на основе кодов-спутников и проверочных соотношений. Первый требует хранения больших объёмов данных, второй основан на вычислении синдромов. При этом легко вычисляются синдромы, позволяющие определить место одиночной ошибки, но для исправления ошибок большей кратности связано со значительными вычислительными трудностями.

Код с простым повторением информационных символов — тривиальный избыточный код. Очевидно, применение его и его разновидностей (корреляционный, инверсный и т.д. коды) не даёт решения нашей задачи.

Код Рида-Маллера - линейный блочный $(2^q, k, 2^{q-\delta})$-код с параметрами $q \geqslant 3,\ \delta < m$ - порядок кода, количество информационных разрядов $k = \sum_{i=0}^{\delta} C_q^i$. Имеется простой способ построения порождающей матрицы, при котором код Рида-Маллера является систематическим и циклическим. Важным свойством рассматриваемых кодов является простота их декодирования, при котором исключается этап определения места ошибок и имеется возможность использования мажоритарного принципа декодирования.

Если число единиц во всех комбинациях кода будет постоянным, то такой код будет кодом с постоянным весом. Это блочные неразделимые коды.

Наибольшее применение получили коды «3 из 7», «3 из 8»; здесь первая цифра указывает на вес кода, вторая — на общее число символов в комбинации.

Например, кодовыми словами кода «3 из 7» являются содержащие три единицы независимо от их места в комбинации, и таких слов 128. Обнаружение ошибки сводится к определению веса принятого слова и сравнению его с заданным. Код обнаруживает ошибки нечётной кратности и часть ошибок чётной кратности. Не обнаруживаются ошибки смещения, при которых несколько единиц превращается в нули и столько же нулей - в единицы.

Коды CRC (Cyclic Redundancy Check, циклическая избыточная проверка) являются систематическими кодами, предназначенными не для исправления ошибок, а для их обнаружения. Они используют способ систематического кодирования и декодирования с порождающим полиномом, изложенный выше.

Линейные коды низкой плотности (LDPC, Low Density Parity-check Codes) или коды с малой плотностью проверок на чётность были предложены ещё в 1963 г., но потом были почти что забыты. В 1990-х годах обнаружилась их связь со

специальным классом графов - экспандерами, теория которых сейчас активно развивается. Данные коды описываются разреженными проверочными матрицами, что уменьшает число количество символов, входящих в проверочные соотношения. Существенной положительной стороной таких кодов является то, что не только кодирование, но и декодирование их выполняется достаточно быстро.

2. Применение помехоустойчивого кодирования для повышения помехозащищённости комбинационных интегральных схем

Для повышения помехозащищённости комбинационных схем был выбран метод с применением циклических кодов. Применение таких кодов позволяет не только обнаружить наличие ошибок в переданном сообщении, но и исправить определённое число ошибок. Количество ошибок, которое можно исправить определяется свойствами образующего многочлена . Данный метод не приводит к неоправданной избыточности, а также обеспечивает возможность оптимального сочетания требований к минимизации аппаратных затрат и достижение требуемого уровня отказоустойчивости. Схема предлагаемого подхода представлена на рисунке 1.

Для кодирования сообщений применяется операция умножения на образующий многочлен, при этом вектор исходного сообщения $a_{k-1}, \dots, a_0$ представляется в виде многочлена $a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_0$, где k – длина сообщения. Для декодирования сообщения используется операция деления переданного сообщения на образующий многочлен. Остаток от деления принятого слова на образующий многочлен называется синдромом. Если ошибок в переданном сообщении нет, то синдром равен нулю. Вектор ошибок находится по вычисленному синдрому.

Для кодирования выходного вектора комбинационной схемы $u = [a_0, a_1, \dots, a_{k-1},]^T$ он представляется в виде многочлена $u(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_0$, который умножается на образующий многочлен $g(x)$. Для декодирования возможно искажённого выходного вектора, представленного многочленом $w(x)$, последний делится на образующий многочлен с вычислением остатка от деления - синдрома $s(x) \equiv_{g(x)} w(x)$. В случае $s(x) \neq 0$ по вычисленному синдрому находится вектор ошибок.

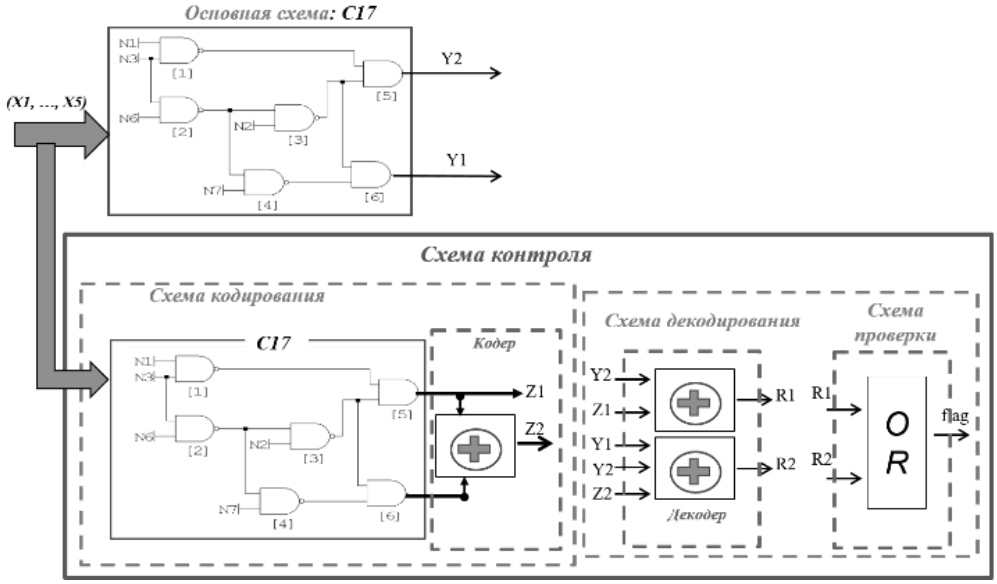

Рисунок 1. Предлагаемый подход

В задаче передачи сообщений для реализации операций умножения и деления многочленов используются сдвиговые регистры, так как сигнал передаётся в виде последовательности нулей и единиц. В случае комбинационных схем сигналы на выходы приходят параллельно, поэтому в данном случае необходимо использовать в качестве схем кодирования и декодирования логические схемы.

Принципиальное отличие задачи кодирования данных для передачи через канал связи от задачи повышения помехоустойчивости комбинационных схем состоит в следующем. Так как в задаче повышения помехоустойчивости сама комбинационная схема подвержена ошибкам, схема кодирования реализуется за счёт дублирования исходной схемы с последующей оптимизацией совместно со схемой кодирования. Для синтеза схемы кодирования используется операция умножения многочлена выходного сообщения комбинационной схемы $a_{k-1}x^{k-1} + \cdots + a_0$ на образующий многочлен $g^m(x)$, где m – степень образующего многочлена.

Ключевая проблема задачи передачи сообщений - минимизация площади или размера схем кодирования и декодирования. Одним из путей оптимизации схемы является построение логических функций на основе применения аппарата бинарных диаграмм решений (BDD, Binary Decision Diagram), представляющих

булеву функцию в виде направленного ациклического графа. Предлагаемое при этом использование синтеза булевых функций в полях Галуа на основе редуцированных диаграмм двоичных решений (ROBDD, Reduced Ordered Binary Decision Diagram), позволяет снять существующее в настоящее время ограничение на размерность проектируемых комбинационных схем (число входов и выходов). Использование предлагаемой методики обеспечивает управляемость и предсказуемость процесса проектирования схем при достижении оптимального сочетания заданных требований по отказоустойчивости и минимизации структурных затрат. Критерием оценки площади при применении BDD может служить количество узлов дерева. Оценку задержек можно рассчитать исходя из длины цепи от входа до выхода при предположении мультиплексорной реализации.

Проведённые исследования показали, что на качество результата в терминах занимаемой площади существенное влияние оказывает не только переупорядочивание входов, как в случае стандартной BDD, но и порядок коммутации выходов в схеме кодирования.

Для выбора оптимального варианта коммутации предлагается использовать оценочную функцию, вычисленную на основе расчёта взаимных корреляций между выходами. Примеры синтеза схемы контроля на основе предложенного подхода приводились ранее в статьях. Наибольший эффект от оптимизации схемы кодирования достигается при условии вхождения в одну формулу схемы кодирования выходов схемы, имеющих взаимные корреляции. Для всех выходов дублирующей схемы применяют предложенные методы анализа логических корреляций в цифровой схеме для получения весовых функций. На основе полученных весовых функций выбирается порядок коммутации выходов дублирующей схемы на основе анализа вероятностей распространения парных корреляций.

Заключение

В данной работе проведён обзор существующих подходов применения кодирования информации для решения задачи повышения помехозащищенности

комбинационных схем. Предложен подход к оптимизации схем кодирования за счёт выбора варианта коммутирования выходов дубликата основной схемы на основе результатов анализа вероятностей логических корреляций.

Библиографический список

1. Черкесов Г. Н. Надёжность аппаратно-программных комплексов // Учебное пособие. – СПб.: Питер, 2004. – 479 с.

2. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение // пер. с англ. В.Б. Афанасьева. – М.: Техносфера, 2006. – 320 с.

3. Poolakkaparambil M., Mathew J. BCH Code Based Multiple Bit Error Correction in Finite Field Multiplier Circuits // ISQED, 2011, pp. 1-6.

4. Гаврилов С. В., Иванова Г. А., Рыжова Д. И., Стемпковский А. Л. Методы повышения надёжности комбинационных микроэлектронных схем на основе мультиинтервального анализа быстродействия // Системы высокой доступности. №4. 2015. - С. 69-76.

5. Соловьёв А. Н., Стемпковский А. Л. Методы повышения отказоустойчивости работы устройства управления микросистемы за счёт введения структурной избыточности // Информационные технологии. 2014, №10, С. 17-22.

6. Вернер М. Основы кодирования // Учебник для ВУЗов. – М.: Техносфера, 2004. – 288 с.

7. Керниган Б., Ритчи Д. Язык программирования Си: Пер. с англ. — М.: Финансы и статистика, 1992.

8. Культин Н.Б. Программирование в Turbo Pascal и Delphi.— СПб.: BHV — Санкт-Петербург, 1998.

9. Ляхович В.Ф. Руководство к решению задач по основам информатики и вычислительной техники. — М.: Высшая школа, 1994.

10. Марченко А.И., Марченко Л.А. Программирование в среде Turbo Pascal 7.0 / Под ред. В. П.Тарасенко. — Киев: ВЕК+; М.: Бином Универсал, 1998.

11. Миков А. И. Информатика. Введение в компьютерные науки. — Пермь: Изд-во ПГУ, 1998.