Semerenko Vasyl Petrovych, Vinnytsia National Technical University, UKRAINE
Ph.D, lecturer, Department of Computer Technique,
E-mail: vpsemerenko@mail.ru

Parallel Algorithms of the Error-Correcting Coding

Семеренко Василий Петрович, Винницкий национальный технический университет,
к.т.н., доцент, кафедра вычислительной техники
E-mail: vpsemerenko@mail.ru

Параллельные алгоритмы помехоустойчивого кодирования

1. Вступление

В настоящее время разработаны параллельные алгоритмы для широкого круга задач: численных, обработки изображений, цифровой обработки сигналов и других. Гораздо меньше внимания уделяется параллельной обработке в системах передачи дискретных данных. Дальнейшее развитие мобильной и спутниковой связи требует увеличения объема вычислений, что делает актуальной разработку параллельной модели помехоустойчивого кодирования.

В статье рассматриваются особенности параллельной обработки в задачах обнаружения и исправления ошибок с помощью циклических кодов. Использование теории линейных последовательностных схем (ЛПС) [1] позволяет не только дать строгое математическое обоснование традиционных задач параллельного декодирования, но и предложить новые методы распараллеливания, в частности, на основе симметрии времени.

2. Основные определения

Будем рассматривать циклический (n,k)-код Ω над полем Галуа $GF(q)$ с минимальным кодовым расстоянием $d_{\min}$. Кодовое слово $Z=(z_1, z_2, \ldots, z_n)$ кода Ω имеет длину n, размерность k и позволяет исправлять все независимые ошибки кратности 1, 2, … , $\tau_{\min}$ ($\tau_{\min} = \frac{d_{\min}-1}{2}$).

Для представления циклического кода Ω будем использовать математический аппарат ЛПС. Согласно [1], ЛПС Λ с l входами, m выходами и r элементами памяти в дискретные моменты времени t задается функцией состояний (переходов)

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(q)$$

и функцией выходов

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(q),$$

где $A = \|a_{ij}\|_{r \times r}$, $B = \|b_{ij}\|_{r \times l}$, $C = \|c_{ij}\|_{m \times r}$, $D = \|d_{ij}\|_{m \times l}$ – характеристические матрицы ЛПС,

$S = \|s_i\|_r$, $U = \|u_i\|_l$, $Y = \|y_i\|_m$ – векторы состояний, входной и выходной.

Размерности матриц ЛПС Λ и параметры циклического кода Ω связаны через коэффициент r, который для кода равен числу контрольных разрядов кодового слова Z при систематическом кодировании ($r = n - k$).

На основе теории ЛПС разработаны новые методы декодирования циклических кодов на основе их автоматной и графовой моделей в двоичных и недвоичных полях Галуа [4,5].

Целью настоящей работы является исследование параллельного декодирования циклических кодов на основе этих моделей для поиска различных типов ошибок.

Для циклического (n,k)-кода с минимальным кодовым расстоянием $d_{\min}$ будем рассматривать следующие виды ошибок в кодовом слове Z:

1) случайных регулярных ошибок в циклическом интервале длины $(n-k)$,

2) случайных нерегулярных ошибок в интервале всего кодового слова,

3) разреженных пакетов ошибок в циклическом интервале длины $(n-k)$,

4) плотных пакетов ошибок в интервале всего кодового слова,

5) случайных стираний в интервале всего кодового слова,

6) пакетов стираний в циклическом интервале длины $(n-k)$.

Случайной регулярной ошибкой кратности τ в кодовом слове Z_{err} называется случайная ошибка, которой соответствует синдромное слово, содержащее в циклическом интервале длины $(n-k)$ τ единиц, одна из которых расположена в младшем, (левом) разряде ($\tau \le \tau_{\min}$).

Первые четыре вида ошибок относятся к классу инверсных ошибок, которые заключаются в изменении правильных разрядов кодового слова Z на противоположные в поле $GF(2)$, либо на другие символы поля $GF(q)$ $(q>2)$. Для ошибок из класса стираний известны их позиции, но неизвестны значения.

Декодирование каждого вида ошибок из приведенного списка является отдельной самостоятельной задачей, для каждой задачи разработан оригинальный алгоритм (соответственно Алгоритм 1, … , Алгоритм 6) [4,5].

3. Геометрическая декомпозиция в помехоустойчивом кодировании

Рассмотрим интерпретацию декомпозиции по данным с помощью многовходовой (многоканальной по терминологии [1]) ЛПС.

Если одновходовая n-мерная ЛПС имеет характеристические матрицы A, B, C, D, тогда ее h-входовый $(h \le (n-k))$ аналог имеет следующие характеристические матрицы A_h и B_h:

$$A_h = \left| A^h \right|; \qquad B_h = \left| A^{h-1}B, \dots, AB, B \right|;$$

Преимуществом h-входовой ЛПС является то, что она работает в h раз быстрее одновходовой ЛПС. С помощью такой ЛПС можно реализовать декомпозицию по данным, которые поступают для кодирования и декодирования, двумя способами.

1) Одновременное кодирование i-х разрядов всех h информационных слов на стороне источника и одновременное декодирование i-х разрядов всех h кодовых слов на стороне приемника ($i = 1 \div n$). По сути это будет еще одной реализацией многоканальной связи, но только с помощью одного параллельного h-входового кодера и одного параллельного h-входового декодера.

2) Одновременное кодирование h последовательных разрядов одного информационного слова на стороне источника и одновременное декодирование h последовательных разрядов одного кодового слова на стороне приемника. Этот способ означает ускорение работы для одноканальной связи в $\frac{k}{h}$ раз при кодировании и в $\frac{n}{h}$ раз при декодировании. Для реализации такого способа параллелизма необходимо, чтобы тактовая скорость передачи данных была в h раз больше тактовой скорости работы кодера и декодера.

4. Предположительная декомпозиция в помехоустойчивом кодировании

Предположительная (speculative) декомпозиция основана на выборе из Ψ различных вычислительных задач только ρ ($\rho < \psi$) задач в зависимости от выполнения определенного условия λ. При последовательном подходе необходимо вначале оценить условие λ, а затем выбрать соответствующие задачи. Если для проведения оценки условия λ требуется период времени T_λ, тогда на такой же период времени будет задержано начало запуска задач. Можно избежать потерь времени, если запустить на выполнение все задачи одновременно с проведением оценки условия λ, а затем использовать результаты только некоторых из задач. Предположительная декомпозиция эффективна на этапе декодирования, где можно организовать поиск различного вида ошибок.

Как правило, перед началом декодирования уже известен характер происшедших ошибок и, поэтому, можно выбрать одну из следующих стратегий: либо декодирование только инверсных ошибок, либо декодирование стираний и инверсных ошибок.

В рамках первой стратегии ведется одновременный поиск случайных ошибок и пакетов ошибок с помощью первых четырех алгоритмов. В зависимости от кратности ошибки, интервала распространения, степени группирования и позиций ошибочных разрядов либо все алгоритмы выдадут различные результаты декодирования, либо результаты некоторых алгоритмов будут совпадать. Например, в рамках первой стратегии возможны следующие ситуации для ошибок кратности τ ($\tau \le \tau_{\min}$):

– ошибочные разряды кратности τ расположены в интервале $1 \div n$, (результаты всех алгоритмов будут различны и только Алгоритм 2 даст правильный результат);

– ошибочные разряды кратности τ расположены в произвольном порядке и в циклическом интервале $1 \div (n-k)$, (результаты всех алгоритмов будут различны и только Алгоритм 1 даст правильный результат);

– ошибочные разряды кратности τ расположены в произвольном порядке и в циклическом интервале $1 \div (\frac{n-k}{2})$, (правильные результаты дадут Алгоритм 1 и Алгоритм 3);

– ошибочные разряды кратности τ расположены подряд в циклическом интервале $1 \div (\frac{n-k}{2})$, (правильные результаты дадут Алгоритм 1, Алгоритм 3 и Алгоритм 4).

Совпадение результатов работы двух и более алгоритмов декодирования с большой долей вероятности свидетельствует о правильном определении параметров ошибок. Если же каждый алгоритм декодирования выдает свой результат, тогда возникает проблема выбора правильного результата.

Кстати, такая же проблема возникает и при традиционном декодировании одним алгоритмом, поскольку одинаковые синдромы могут давать ошибки различной природы.

В общем случае, правильная интерпретация результатов декодирования является фундаментальной проблемой теории помехоустойчивого кодирования.

На практике эта проблема решается выбором модели канала связи и связанным с ним характером ошибок. Если выбирается модель канала связи с памятью, с замираниями, тогда предпочтение отдается пакетам ошибок; при выборе модели биномиального канала – случайным ошибкам.

Однако, в реальных условиях каналы связи имеют нестационарный характер, их характеристики изменяются с течение времени и по случайному закону. Имеются специальные алгоритмы адаптации, позволяющие на основе заданных критериев определять смену состояний канала и, соответственно, изменять параметры системы кодирования-декодирования. При этом процесс смены параметров системы связи всегда запаздывает от

момента смены характеристик канала, что приводит в итоге к неправильной интерпретации работы всей системы в целом и снижению ее производительности [6].

Иная ситуация при параллельной работе различных алгоритмов декодирования циклических кодов. Указанные алгоритмы одинаково функционируют при любой модели канала, изменяется лишь критерий выбора результатов работы алгоритмов в соответствии с предпочтительным характером ошибок при передаче текущего кодового слова. Такая смена критериев требует гораздо меньше времени, чем традиционная адаптация параметров системы связи.

5. Декомпозиция на основе симметрии времени

Традиционные методы помехоустойчивого кодирования используют концепцию времени, при которой вычислительные процессы происходят только в одном линейном направлении: от прошлого к будущему. Однако, законы науки не делают различия между направлениями “вперед” и “назад” во времени [2]. Фундаментальные законы и классической, и квантовой динамики подразумевают эквивалентность причин и следствий, что влечет за собой эквивалентность прошлого и будущего.

Безусловно, термодинамическая и космологическая стрелы времени необратимы и направлены в будущее, в данном случае рассматриваются темпоральные (временные) модели только с позиций математики.

Как показал в своих работах И. Пригожин [3], обратимость во времени справедлива только для интегрируемых динамических систем (ДС), к которым принадлежат, в частности, автономные ДС.

В интегрируемых ДС последовательность смен состояний во времени образует фазовую траекторию в пространстве состояний системы. Для автономных ДС фазовая траектория – окружность (цикл). Обычно движение по фазовой траектории направлено вдоль точек (состояний), которые соответствуют моментам времени в порядке их возрастания, т.е. от “настоящего” в “будущее”. С математической точки зрения не существует запрета движения в обратном направлении по фазовой траектории, имеющей вид окружности. Если интерпретировать движение по циклической фазовой траектории от состояния s_{beg} в разные стороны как одновременное движение в противоположных временных направлениях, тогда можно рассмотреть задачу выигрыша во времени за счет выбора более короткой длины пути от s_{beg} к s_{end} (рис. 1). В итоге мы приходим к идее распараллеливания вычислений на основе темпоральных (временных) моделей.

В качестве интегрируемых ДС можно использовать автономные линейные автоматы, т.е. автономные ЛПС. Функционирование автономной ЛПС не зависит от входных воздействий и описывается функциями переходов и выходов:

$$S(t+1) = A \times S(t), \quad Y(t) = S(t), \qquad GF(q).$$

Функционирование обратной автономной ЛПС описывается следующими функциями переходов и выходов:

$$S(t-1) = A_{inv} \times S(t), \quad Y(t) = S(t), \qquad GF(q).$$

Матрицу A_{inv} обратной автономной ЛПС легко определить в результате решения матричного уравнения $A_{inv} \times A = E$ относительно единичной матрицы E и известной матрицы A.

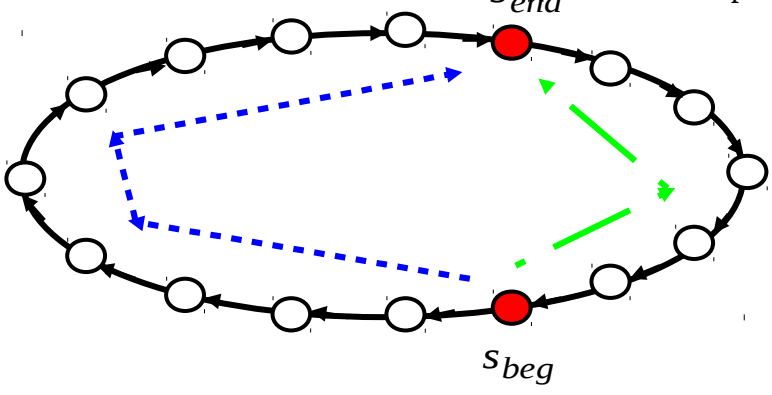

Рис. 1. – Направления движения по фазовой траектории для автономной ДС.

Приведенные типы автономных ЛПС можно использовать для параллельного декодирования циклических кодов. Особенностью графа переходов этих кодов, исправляющих кратные ошибки, является наличие многочисленных нулевых циклов (НЦ), образованных нулевыми дугами. Методы поиска ошибок по графу переходов состоят в построении кодового пути ошибки, который проходит через указанные НЦ и особые вершины v_{ks}, с помощью которых различные НЦ связаны между собой единичными дугами [4,5]. В терминах темпоральной модели особые вершины v_{ks} в каждом НЦ играют роль заключительных состояний в фазовой траектории.

6. Декодирование циклических кодов на основе параллельных алгоритмов

На основе трех изложенных видов декомпозиции разработана обобщенная процедура параллельного декодирования циклических кодов. В этой процедуре имеется три вложенных друг в друга способа параллельной обработки. Самый внутренний параллелизм реализован на основе двух темпоральных моделей: в рамках каждой темпоральной модели на основе вычислений состояний $S(i+1)$ и $S(i-1)$ строится свой кодовый путь по графу переходов ЛПС. Далее четыре параллельных алгоритма с помощью восьми параллельных потоков одновременно ищут четыре вида инверсных ошибок. Наконец, самый внешний параллелизм реализован с помощью геометрической декомпозиции, коэффициент распараллеливания определяется степенью h характеристических матриц ЛПС.

7. Выводы

Декодирование циклических кодов на основе теории ЛПС позволяет организовать эффективную параллельную обработку на основе различных типов декомпозиции. С помощью геометрической декомпозиции можно получить ощутимый выигрыш не только при многоканальной передаче, но и при одноканальной. При использовании предположительной декомпозиции достигается не только эффект распараллеливания, но и повышается достоверность результата декодирования.

Одним из основных резервов повышения производительности параллельных вычислительных систем является эффективное использование фактора времени. Предложенная темпоральная модель на основе автономных ЛПС вводит новый тип параллелизма – параллелизм на основе симметрии времени.

Рассмотренные алгоритмы декодирования и исправления ошибок реализованы программно на языке C++ с использованием технологии параллельных вычислений OpenMP.

Литература

1. Gill A. “Linear Sequential Circuits. Analysis, Synthesis and Application”, McGraw-Hill Book Company, New York, London, 1967.
2. Hawking S. “A Brief History of Time: From the Big Bang to Black Holes”, New York, Bantam Books, 1998.
3. Prigogine I., Stengers I. “Time, Chaos, Quant”, Publishers group “Progress”, Moscow, 1994. —272 p. (Russian edition).
4. Semerenko V.P. Burst-Error Correction for Cyclic Codes. Proceeding of International IEEE Conference EUROCON2009, S.Petersburg, Russia, pp.1646-1651.
5. Semerenko, V.P. “Parallel decoding of shortened cyclic codes”, Optic-electronic and information-energy technologies, 2012, No.1, pp.30-41. (Russian edition).
6. Мелентьев О.Г. Теоретические аспекты передачи данных по каналам с группирующимися ошибками. — М.: Горячая линия – Телеком, 2007. — 232 с.