УДК 621.37:621.391

С.Г. Рассомахин

Харьковский национальный университет им. В.Н. Каразина, Харьков

ЛИНЕЙНОЕ ЦЕЛОЧИСЛЕННОЕ ДЕКОДИРОВАНИЕ ПСЕВДОСЛУЧАЙНЫХ КОДОВ НА ОСНОВЕ МЕТОДА ОТСЕЧЕНИЙ ГОМОРИ

Констатируется перспективность псевдослучайных помехоустойчивых кодов, полученных методом линейной конгруэнтной генерации, для использования в системах передачи информации. Предложено правило декодирования, основанное на методе наименьших проекций. Рассмотрен алгоритм формализации декодирования, позволяющий свести работу декодера к решению задачи целочисленного линейного программирования. Приведена оценка эффективности предложенного метода по сравнению с переборными алгоритмами декодирования.

Ключевые слова: *псевдослучайные коды, амплитудно-фазовая модуляция, линейное целочисленное программирование, симплекс-метод, правило Гомори.*

Введение

Постановка проблемы. Повышение помехоустойчивости и эффективности систем передачи информации (СПИ) может быть достигнуто только при объединении результатов теории кодирования с результатами теории модуляции и потенциальной помехоустойчивости. В настоящее время аксиоматичным стало утверждение о том, что возможности развития методов модуляции и кодирования в значительной мере исчерпаны. Основанием для этого является достаточно высокая степень близости достигаемых скоростей передачи информации к теоретическому пределу Шеннона. Как правило, оценки скоростей производятся для двух случаев: во-первых, при применении наилучших известных комбинаторных кодовых конструкций в области "энергетически" эффективных СПИ, а во-вторых – для "частотно" эффективных сигнально-кодовых конструкций при использовании многопозиционных методов модуляции в сочетании с комбинаторным кодированием. Первые из этих СПИ обладают низкой удельной (на единицу полосы частот) скоростью, а вторые, соответственно, низкой удельной (на один бит) энергетической эффективностью. При этом совершенно очевидно, что проблема создания СПИ, которые являются эффективными одновременно по частотному и энергетическому критериям, остается открытой.

Анализ последних исследований. Теоретической основой для создания эффективных систем кодирования является работа [1], в которой К. Шеннон доказал несколько фундаментальных теорем, в том числе основную теорему кодирования для канала с помехами. Методология доказательства основана на использовании случайно выбираемого кода, а средством достижения произвольно малой вероятности ошибки декодирования при скоростях, не превышающих пропускную способность канала, является увеличение длины блока кода. Доказательство и геометрические построения пространства кода Шеннона основаны на монотонном возрастании среднего взаимного расстояния между кодовыми точками в многомерном *евклидовом* пространстве при возрастании его размерности. При этом если пропускная способность канала не превышена, то скорость возрастания взаимных расстояний (при увеличении длины блока кода) превышает скорость увеличения радиуса сферы неопределенности помех канала. Неконструктивность доказательства, не дающая конкретного способа выбора кода, послужила одной из причин широкого распространения комбинаторных методов кодирования [2], оперирующих с "суррогатным" понятием "кодового расстояния". Принципиальным отличием и неустранимой потерей комбинаторных методов, отошедших от евклидовой метрики кодового пространства, является требование обязательной информационной (символьной) избыточности, вносимой в передаваемые сообщения. Это является причиной низкой частотной эффективности систем комбинаторного помехоустойчивого кодирования. В жертву алгоритмичности и простоте построения и декодирования комбинаторных кодов принесена скорость передачи информации, т.е. частотная эффективность СПИ.

Методология доказательства основной теоремы кодирования Шеннона использована в работах [3] – [5] для построения кодов на основе кодовых слов, выбираемых некоторым случайным образом. При этом (с различной степенью полноты доказательств) показано, что благодаря свойству асимптотической равновероятности, практически любой случайный код является достаточно "хорошим". Объем полезно используемого для размещения кодовых точек евклидова пространства кода, а также средние взаимные расстояния с увеличением блины блока стремятся к наилучшим значениям. Такие коды обеспечивают одновременно частотную и энергетическую эффективность и могут успешно применяться при использовании многопозиционных методов амплитудно-фазовой модуляции, находящих все более широкое распространение в современных стандартах цифровых СПИ.

Существенным препятствием на пути применения случайного кодирования является тот факт, что

декодирование таких кодов, реализующее правило максимального правдоподобия (ПМП), осуществимо только переборными методами. Сложность таких методов возрастает экспоненциально с длиной блока кода, и при желаемых значениях длины блока декодирование становится вычислительно нереализуемым. Поэтому на сегодняшний день задача создания приемлемых по сложности методов декодирования случайных кодов весьма актуальна. Ее решение осуществимо, благодаря тому, что вместо случайных кодов можно использовать псевдослучайные коды, для генерации которых применяются детерминированные методы [6], обладающие аналитическим описанием и допускающие математическую формализацию декодирования в виде задачи поиска экстремума некоторого целевого функционала.

Цель статьи. Целью статьи является разработка конструктивного математического метода декодирования псевдослучайного кода на основе многопозиционной амплитудно-фазовой модуляции в гауссовом канале. Для разработки метода ниже обосновано новое правило декодирования, которое несколько уступает по объективности правилу максимального правдоподобия, но зато позволяет линеаризовать оптимизационную задачу нахождения экстремума целевого функционала декодирования.

Основная часть

1. Построение псевдослучайного кода и общая формулировка задачи декодирования

Наиболее распространенным алгоритмом генерации случайных чисел является использование линейного конгруэнтного генератора [6]. При построении кода получаемые числа, равномерно распределенные в заданном диапазоне, отождествляются с некоторыми значениями одного из информативных параметров сигнала (амплитудой, частотой или фазой). Подходящими переносчиками для построения числовых кодов являются амплитудно-фазовые, частотные, амплитудно-частотные и времяимпульсные методы модуляции, допускающие многоуровневую шкалу градации одного или нескольких информативных параметров. Собственно процесс модуляции в канале не является предметом данной статьи, поэтому в дальнейшем опускается из рассмотрения.

Кодовое слово ПСП кода может быть представлено вектором $\mathbf{X}=\{x_0,x_1,\ldots,x_N\}$ в $(N+1)$-мерном пространстве кода. Скоростью кода является величина $R=M/(N+1)$, $0<R<\infty$, где 2^M – мощность алфавита источника. В отличие от комбинаторных кодов, для которых $R\le 1$, в данном определении скорость теоретически может быть любой неотрицательной величиной. Если источник двоичный, то M – длина блока источника (в символах). Очевидно, что кодово-сигнальные конструкции при $R\ge 1$ обладают одновременно свойствами как энергетической, так и частотной эффективности.

В соответствии со свойствами линейных конгруэнтных последовательностей (ЛКП) [6] элементы $\mathbf{X}$ имеют следующие значения:

- $x_0\in\left[0\ldots\left(2^M-1\right)\right]$ – число, определяющее порядковый номер блока символов источника – порождающее число ПСП;
- $x_k=\mathrm{mod}\left[ax_{k-1}+b,m\right]$, $k\in 1\ldots N$ – числа ПСП, порождаемые x_0 по алгоритму ЛКП;
- a,b,m – целые положительные константы, удовлетворяющие условиям: $m\ge 2^M$, b и m – взаимно простые числа, величина $(a-1)$ кратна любому простому числу, которое меньше m и является его делителем.

Очевидно, что при выполнении данных условий k-е число ПСП связано с порождающим числом ЛКП зависимостью:

$$x_k=\mathrm{mod}\left[a^k x_0+\frac{a^k-1}{a-1}b,m\right],\quad k\in 1\ldots N. \qquad (1)$$

Если известно порождающее число x_0, то остальные числа однозначно определяются из (1) (процесс кодирования). При декодировании кода решается обратная задача – на основании оценки элементов вектора $\mathbf{X}$ требуется как можно наиболее верно оценить порождающее число кодового слова – x_0. Процесс декодирования, по сути, может быть охарактеризован, как *факторизация* ПСП.

Введем линейный алгебраический эквивалент операции вычисления произвольного числа n по модулю в виде

$$\mathrm{mod}[n,m]=n-y\cdot m, \qquad (2)$$

где y – целое неотрицательное число, удовлетворяющее неравенству $\left[(n+1)/m-1\right]\le y\le(n/m)$. Тогда, на основании (1) и (2) может быть составлена система уравнений:

$$a^i y_0+\left[\left(a^i-1\right)/(a-1)\right]b-y_i m=x_i,\ i\in 0,\ldots,N, \qquad (3)$$

или в матричной форме

$$\mathbf{A}\times\mathbf{Y}=\mathbf{X}. \qquad (4)$$

При отсутствии помех (неискаженном векторе наблюдений $\mathbf{X}$) решение (4), приводящее к факторизации ПСП, тривиально: $y_0=x_0$. В условиях искажения чисел на выходе реального гауссова канала, система (4) трансформируется к виду:

$$\mathbf{A}\times\mathbf{Y}\ \square\ \mathbf{Z}, \qquad (5)$$

где $\mathbf{Z}=\mathbf{X}+\mathbf{O}$, $\mathbf{O}=\{\xi_0,\xi_1,\ldots,\xi_N\}$ – вектор случайных, нормально распределенных чисел с нулевым средним и дисперсией $N_0/2$ (N_0 – спектральная плотность мощности аддитивного гауссова шума). Система (5), как правило, не совместна, ее приближенное решение $\mathbf{Y}$ может быть найдено методом наименьших квадратов минимизацией функционала:

$$\min_{\mathbf{Y}}\left|\mathbf{A}\times\mathbf{Y}-\mathbf{Z}\right|^2. \qquad (6)$$

Поскольку решение (6) минимизирует расстояние между правой и левой частями (5), то при декодировании реализуется правило *максимального правдоподобия*, а общую формулировку задачи декодирования можно представить в следующем виде:

найти вектор целых неотрицательных чисел $\mathbf{Y}$, удовлетворяющих системе ограничений

$$0 \le y_0 \le m-1,\ 0 \le a^i y_0 + \frac{a^i-1}{a-1}b - m y_i \le m-1,\quad i \in 1\ldots N, \tag{7}$$

и обращающих в минимум функцию (6).

Несмотря на линейность ограничений (7), общая задача декодирования по правилу максимального правдоподобия (6) является задачей *нелинейного* целочисленного программирования. Для любого ПСП кода целевая функция (6) изобилует локальными экстремумами, количество которых приближается к величине 2^{M-1}. Поэтому никаких эффективных методов направленного перебора вариантов решения предложить невозможно. Это подтверждает тезис о единственной пригодности простого переборного алгоритма для декодирования случайных кодов по методу максимального правдоподобия.

2. Линеаризация задачи факторизации кода ПСП на основе правила наименьших проекций

В соответствии с методом факторизации кода ПСП, реализующим *правило наименьших проекций* (ПНП), для решения предлагается задача в следующей формулировке. При заданной области $\mathbf{И}$ допустимых целочисленных решений необходимо найти

$$\text{при}\quad \begin{array}{c}\mathbf{Y} \Rightarrow \min\langle \mathbf{W}_+ \oplus \mathbf{W}_-\rangle,\\ \mathbf{Y} \in \mathbf{И},\quad \mathbf{A}\times\mathbf{Y} + \mathbf{W}_+ - \mathbf{W}_- = \mathbf{Z},\end{array} \tag{8}$$

где $\mathbf{W}_+$ и $\mathbf{W}_-$ – векторы, координаты которых – неотрицательные действительные числа, оператор $\oplus$ предполагает скалярное суммирование элементов. Задачи (7) и (8) подобны в том смысле, что минимум соответствующих целевых функций достигается, как правило, при одном и том же векторе $\mathbf{Y}$ из области $\mathbf{И}$. С целью замены нелинейного метода наименьших квадратов приближенным линейным методом, уравнения системы (5) включены в ограничения задачи (8) с добавленной (в левой части) парой дополнительных неотрицательных переменных. Одна переменная из этой пары имеет знак "+", а вторая – "-". Назначение вводимых дополнительных переменных – компенсация (уравнивание) искажений правой части исходной системы (4) в результате суммирования с элементами вектора гауссовых случайных величин $\mathbf{O} = \{\xi_0, \xi_1, \ldots, \xi_N\}$. В результате решения задачи (8) половина из общего числа элементов векторов $\mathbf{W}_+$ и $\mathbf{W}_-$ должны оказаться нулевыми. Оставшиеся ненулевые неотрицательные добавочные элементы (входящие в целевую функцию со знаком "плюс" или "минус") являются проекциями кратчайшей (как полагается, но не всегда это верно) прямой, соединяющей в $(N+1)$-мерном пространстве точки $\mathbf{A}\times\mathbf{Y}$, $(\mathbf{Y} \in \mathbf{И})$ и $\mathbf{Z}$. Минимизация скалярной суммы в задаче (8) при всех указанных ограничениях Θ обеспечивает минимально достижимое значение суммы длин проекций этой прямой на оси $(N+1)$-мерного пространства, а, следовательно, нахождение вектора $\mathbf{Y}$, решающего проблему факторизации кода ПСП в условиях помех по правилу наименьших проекций.

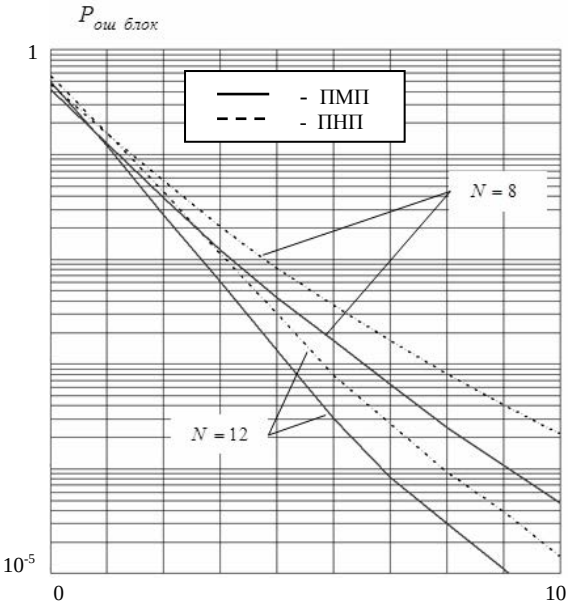

Рис. 1. Вероятность ошибки на блок ПСП кода для декодирования по правилам ПМП и ПНП, как функция отношения сигнал/шум

Рассмотренное правило наименьших проекций, несомненно, проигрывает по объективности оценки принимаемого кодового слова правилу максимального правдоподобия. Сравнительная иллюстрация потерь помехоустойчивости, полученная методом моделирования, при переходе к декодированию по правилу наименьших проекций представлена на рис. 1 для двух значений параметра N. Как следует из приведенных зависимостей, энергетический проигрыш ПНП по сравнению с ПМП при различных длинах блока составляет не более 1 дБ. Это является вполне приемлемой платой за достижение линейности целевой функции задачи декодирования.

3. Декодирование кода ПСП на основе метода отсечений Гомори

Перепишем систему (5) с учетом ограничений-равенств (8):

$$\begin{cases} y_0 + w_1 - w_2 = z_0 \\ a y_0 + b - y_1 m + w_3 - w_4 = z_1; \\ a^2 y_0 + \dfrac{a^2-1}{a-1}b - y_2 m + w_5 - w_6 = z_2; \\ \ldots\ldots\ldots\ldots \\ a^N y_0 + \dfrac{a^N-1}{a-1}b - y_N m + w_{2N+1} - w_{2(N+1)} = z_N. \end{cases} \tag{9}$$

Каждое из двухсторонних ограничений (7) может быть трансформировано в два ограничения-равенства путем соответствующего прибавления или вычитания дополнительных неотрицательных переменных $y_{N+1},\dots y_{3N+1}$, удовлетворяющих условию целочисленности:

$$\begin{cases} y_0 + y_{N+1} = m-1; \\ a y_0 + b - y_1 m - y_{N+2} = 0; \\ a y_0 + b - y_1 m + y_{N+3} = m-1; \\ \\ a^2 y_0 + (a+1)b - y_2 m - y_{N+4} = 0; \\ a^2 y_0 + (a+1)b - y_2 m + y_{N+5} = m-1; \\ \dots\dots\dots\dots\dots \\ a^N y_0 + \dfrac{a^N - 1}{a-1} b - y_N m - y_{3N} = 0; \\ a^N y_0 + \dfrac{a^N - 1}{a-1} b - y_N m + y_{3N+1} = m-1. \end{cases} \qquad (10)$$

На основе (8) – (10) формализованное представление факторизации кода ПСП по правилу наименьших проекций можно представить в каноническом виде задачи линейного программирования следующим образом.

Требуется максимизировать целевую функцию

$$F = -\sum_{i=1}^{2(N+1)} w_i + \sum_{j=0}^{3N+1} 0 \cdot y_j \qquad (11)$$

при условиях

$$y_0 + w_1 - w_2 = z_0;$$

$$\underbrace{a^i y_0 - m y_i + w_{2i+1} - w_{2i+2} = z_i - \frac{a^i - 1}{a-1} b;}_{i \in 1,2,\dots,N}$$

$$y_0 + y_{N+1} = m-1;$$

$$\left.\begin{array}{l} a^j y_0 - m y_j - y_{N+2j} = -\dfrac{a^j - 1}{a-1} b; \\ a^j y_0 - m y_j + y_{N+2j+1} = m - 1 - \dfrac{a^j - 1}{a-1} b; \end{array}\right\} j \in 1, 2, \dots, N;$$

$$\left.\begin{array}{l} y_k \ge 0 \\ y_k - \text{целые} \end{array}\right\}, \quad k \in 0, 1, \dots, 3N+1;$$

$$w_\ell \ge 0, \qquad \ell \in 1, 2, \dots, 2(N+1).$$

Данная задача является частично целочисленной и может быть решена на основе идеи метода отсекающих плоскостей Гомори [7], использующего симплекс-алгоритм нахождения оптимального опорного (допустимого) плана задачи линейного программирования. Суть алгоритма поиска решения сводится к направленному перебору *оптимальных* опорных планов путем последовательных нецелочисленных итераций. Получение исходной симплекс-таблицы для каждой из итераций производится введением дополнительных ограничений в начальную задачу (10), учитывающих требование целочисленности какой-либо из переменных.

Исходная симплекс-таблица задачи (11) (табл. 1) получается при выборе в качестве базиса переменных $w_i, i \in 1,\dots,(2N+2)$ и выражении переменных $y_j, j \in 0,\dots,(3N+2)$ через базисные. Векторная форма ограничений задачи (11) имеет вид:

$$y_0 \mathbf{V}_0 + y_1 \mathbf{V}_1 + \dots + y_{3N+1} \mathbf{V}_{3N+1} + w_1 \mathbf{U}_1 + \dots$$
$$\dots + w_{2N+2} \mathbf{U}_{2N+2} = \mathbf{U}_0;$$

$y_0 \ge 0; \quad y_i, w_i \ge 0; \quad y_0, y_i$ – целые; $\quad i \in 1, \dots, N.$

Здесь

$$\mathbf{V}_0 = \begin{Bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{Bmatrix}; \mathbf{V}_1 = \begin{Bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{Bmatrix}; \dots; \mathbf{V}_{3N+1} = \begin{Bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{Bmatrix} \begin{matrix} \uparrow \\ 3N+2 \text{ – базис;} \\ \downarrow \end{matrix}$$

$\mathbf{U}_0$ – вектор свободных членов задачи (10);

$\mathbf{U}_1,\dots,\mathbf{U}_{2N+2}$ – векторы коэффициентов при базисных переменных.

В столбце $\mathbf{C}_b$ табл. 1 помещены коэффициенты при неизвестных в целевой функции F, соответствующие выбранному базису. Столбец $\mathbf{U}_0$ содержит, фактически, исходный ненулевой план задачи. В столбцах $\mathbf{U}_j$ находится разложение этих векторов по векторам начального базиса. В последней $(3N+3)$- й строке в столбце $\mathbf{U}_0$ находится значение целевой функции F_0 при данном плане.

Значение целевой функции определяется скалярным произведением:

$$F_0 = \mathbf{U}_0 \times \mathbf{U}_b = \sum_{i=0}^{3N+1} (\mathbf{U}_0)_i \, c_i \, .$$

В остальных столбцах последней строки элементы таблицы вычисляются по правилам:

$$\Delta_j = \mathbf{V}_j \times \mathbf{C}_b - c_j, \quad \text{при} \quad j \in 0, \dots, 3N+1;$$

или $\Delta_{3N+1+j} = \mathbf{U}_j \times \mathbf{C}_b - c_{3N+1+j}$, при $j \in 1, \dots, 2N+2,$

где $\mathbf{V}_j \times \mathbf{C}_b = \sum_{i=0}^{3N+1} (\mathbf{V}_j)_i c_i$, $\mathbf{U}_j \times \mathbf{C}_b = \sum_{i=0}^{3N+1} (\mathbf{U}_j)_i c_i$ – соответствующие скалярные произведения; c_i – элементы столбца (вектора) $\mathbf{C}_b$.

При условии равенства нулю всех свободных переменных $w_i = 0$, $i \in 1, \dots, (2N+2)$, исходная таблица содержит оптимальный опорный план решения задачи факторизации кода для декодирования в идеальных условиях при отсутствии помех. Это следует из того что все элементы $\Delta_j \ge 0$ при $j \in 0, \dots, 5N+3$, а элементы вектора $\mathbf{U}_0$ – целые неотрицательные числа. При этом сумма проекций "помехового" вектора на базис $(N+1)$-мерного пространства кода равна нулю, так как достигается минимальное значение целевой функции. В этом случае процесс факторизации тривиален – элемент z_0, расположенный в столбце $\mathbf{U}_0$ строки $\mathbf{V}_1$, равен номеру декодированной последовательности.

Таблица 1

Исходная симплекс-таблица декодирования

№	Базис	$\mathbf{C}_b$	$\mathbf{C}$	0	0	…	0	-1	-1	-1	-1	-1	…	-1	-1	-1
			$\mathbf{U}_0$	$\mathbf{V}_0$	$\mathbf{V}_1$	…	$\mathbf{V}_{3N+1}$	$\mathbf{U}_1$	$\mathbf{U}_2$	$\mathbf{U}_3$	$\mathbf{U}_4$	$\mathbf{U}_5$	…	$\mathbf{U}_{2N}$	$\mathbf{U}_{2N+1}$	$\mathbf{U}_{2N+2}$
0	$\mathbf{V}_0$	0	z_0	1	0	…	0	1	-1	0	0	0	…	0	0	0
1	$\mathbf{V}_1$	0	$\frac{1}{m}(az_0 - z_1 + b)$	0	1	…	0	$\frac{a}{m}$	$-\frac{a}{m}$	$-\frac{1}{m}$	$\frac{1}{m}$	0	…	0	0	0
2	$\mathbf{V}_2$	0	$\frac{1}{m}\left(a^2 z_0 - z_2 + (a+1)b\right)$	0	0	…	0	$\frac{a^2}{m}$	$-\frac{a^2}{m}$	0	0	$-\frac{1}{m}$	…	0	0	0
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
N	$\mathbf{V}_N$	0	$\frac{1}{m}\left(a^N z_0 - z_N + \frac{a^N - 1}{a - 1}b\right)$	0	0	…	0	$\frac{a^N}{m}$	$-\frac{a^N}{m}$	0	0	0	…	0	$-\frac{1}{m}$	$\frac{1}{m}$
N+1	$\mathbf{v}_{N+1}$	0	$m - z_0 - 1$	0	0	…	0	-1	1	0	0	0	…	0	0	0
N+2	$\mathbf{V}_{N+2}$	0	z_1	0	0	…	0	0	0	1	-1	0	…	0	0	0
N+3	$\mathbf{V}_{N+3}$	0	$m - z_1 - 1$	0	0	…	0	0	0	-1	1	0	…	0	0	0
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
3N	$\mathbf{V}_{3N}$	0	z_N	0	0	…	0	0	0	0	0	0	…	0	1	-1
3N+1	$\mathbf{v}_{3N+1}$	0	$m - z_N - 1$	0	0	…	1	0	0	0	0	0	…	0	-1	1
			$F_0 = 0$	0	0	…	0	1	1	1	1	1	…	1	1	1

При наличии помех исходная симплекс таблица может не содержать опорного плана решения. В этом случае осуществляется итерационный поиск оптимального опорного плана в соответствии с методом отсекающих плоскостей Гомори [7]. Собственно алгоритм нахождения решения задачи линейного целочисленного декодирования состоит из двух вложенных циклов итераций (большого и малого) смены опорных планов. Для смены планов используется стандартный алгоритм симплекс-метода пересчета элементов таблицы [7], поэтому здесь он не рассматривается.

В *малом* цикле проверяется допустимость и оптимальность опорного плана задачи. При выполнении этих условий все элементы столбца $\mathbf{U}_0$ и последней строки (кроме ячейки F_0) должны быть неотрицательными. В противном случае производится переход к новому плану путем обмена положением свободного и базисного векторов. Для этого применяется прямой или двойственный метод поиска разрешающего элемента таблицы. При прямом методе (исходный план не оптимален) разрешающим столбцом является столбец $\mathbf{U}_j$ с отрицательным элементом в последней строке, а номер разрешающей строки k определяется из условия

$$\left((\mathbf{U}_0)_k \Big/ (\mathbf{U}_j)_k\right) \Rightarrow \min. \qquad (12)$$

При двойственном методе (исходный план не является допустимым) разрешающей строкой является любая из строк с отрицательным элементом в столбце $\mathbf{U}_0$, в других столбцах которой существуют отрицательные элементы. Разрешающим столбцом является столбец с номером j, для которого, также как и в предыдущем случае, выполняется условие (12).

В *большом* цикле итераций проверяется выполнение условия целочисленности свободных переменных, на которые наложено соответствующее требование в формулировке ограничений задачи (11). Если это условие в полученном оптимальном плане нарушено хотя бы для одной из переменных, то к исходной задаче (11) добавляется дополнительное ограничение. Если таких переменных несколько, то в циклах больших итераций производится последовательный лексикографический перебор целочисленных переменных, для которых поочередно составляются дополнительные ограничения. Поскольку переменные y могут принимать только целые значения, а переменные w – любые, то общее правило составления дополнительного ограничения Гомори для выбранной i-й строки симплекс таблицы с опорным нецелочисленным планом в применении к задаче декодирования кода ПСП может быть представлено в следующем виде:

$$\sum_{j=0}^{3N+1} \alpha_{i,j} y_j + \sum_{j=1}^{2N+2} \beta_{i,j} w_j \geq \mathrm{mod}\left[(\mathbf{U}_0)_i, 1\right], \qquad (13)$$

где в правой части неравенства находится положительная дробная часть соответствующего элемента столбца $\mathbf{U}_0$ последней полученной таблицы, а для вычисления коэффициентов при переменных y и w используются выражения:

- при $\mathrm{mod}\left[(\mathbf{V}_j)_i, 1\right] \leq \mathrm{mod}\left[(\mathbf{U}_0)_i, 1\right]$:

$$\alpha_{i,j} = \mathrm{mod}\left[(\mathbf{V}_j)_i, 1\right];$$

- при $\left|\mathrm{mod}\left[(\mathbf{V}_j)_i, 1\right]\right| > \mathrm{mod}\left[(\mathbf{U}_0)_i, 1\right]$:

$$\alpha_{i,j} = \frac{\mathrm{mod}\left[(\mathbf{U}_0)_i, 1\right]}{1 - \mathrm{mod}\left[(\mathbf{U}_0)_i, 1\right]}\left\{1 - \left|\mathrm{mod}\left[(\mathbf{V}_j)_i, 1\right]\right|\right\};$$

- при $\left(\mathbf{V}_j\right)_i \geq 0$: $\beta_{i,j} = \left(\mathbf{V}_j\right)_i$
- при $\left(\mathbf{V}_j\right)_i < 0$:

$$\beta_{i,j} = \frac{\mathrm{mod}\left[\left(\mathbf{U}_0\right)_i, 1\right]}{1 - \mathrm{mod}\left[\left(\mathbf{U}_0\right)_i, 1\right]} \left|\left(\mathbf{V}_j\right)_i\right| .$$

Формируемое по правилу (13) дополнительное ограничение на каждой итерации большого цикла приводит к добавлению соответствующей строки в исходной симплекс таблице. После этого вновь осуществляются итерации малого цикла с проверкой допустимости, оптимальности и целочисленности решений. Окончание линейного целочисленного декодирования производится в случае, когда все элементы столбца $\mathbf{U}_0$ и последней строки (кроме F_0) неотрицательны, а свободные переменные y_i, $i \in 0,\ldots,3N+1$ исходной задачи (11) принимают целые значения.

Физическая сущность решаемой при декодировании задачи целочисленного линейного программирования всегда предполагает наличие, по крайней мере, одного оптимального решения.

Вычислительная сложность простого переборного алгоритма декодирования для кода с длиной блока N может быть оценена удельным количеством операций на двоичный символ $n_{пер} \sqcap N^{-1} \cdot 2^N$, т.е. возрастает, практически, *экспоненциально* с увеличением длины блока. Для рассмотренного алгоритма линейного целочисленного декодирования доказано (например, в [7]), что для достижения решения максимальное количество итераций не превышает величину $n_{y,w} \cdot n_w$, где $n_{y,w} = 5N + 4$ – общее количество переменных задачи; $n_w = 2N + 2$ – количество базисных переменных. Следовательно, вычислительная сложность растет по показательному закону: $n_{лцд} \sqcap K \cdot N^2$, где $K \leq 10 \div 20$ – константа, зависящая от исходных данных задачи. При больших значениях N рассмотренный метод декодирования обладает неоспоримым преимуществом по достигаемому снижению вычислительной сложности.

Выводы

Основной результат данной статьи заключается в получении универсального метода декодирования кодов ПСП, позволяющего реализовать все преимущества случайного кодирования при обеспечении энергетической и частотной эффективности СПИ.

Список литературы

1. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон. – М.: Изд. ИЛ, 1963. – 830 с.

2. Хэмминг Р.В. Теория кодирования и теория информации: Пер. с англ. / Р.В. Хэмминг. – М.: Радио и связь, 1983. – 176 с.

3. Флейшман Б.С. Конструктивные методы оптимального кодирования для каналов с шумами / Б.С. Флейшман. – М.: Изд. АН СССР, 1963. – 224 с.

4. Коржик В.И. Универсальное стохастическое кодирование в системах с решающей обратной связью / В.И. Коржик, С.А. Осмоловский, Л.М. Финк // Проблемы передачи информации. – М.: ИППИ, 1974. – Вып. 4. – С. 25-29.

5. Осмоловский С.А. Стохастическая информатика: Инновации в информационных системах / С.А. Осмоловский. – М.: Горячая линия-Телеком, 2011. – 320 с.

6. Электронный ресурс. – Режим доступа к ресурсу: http://www.stratum.ac.ru/textbooks/modelir/lection22.

7. Акулич И.Л. Математическое программирование в примерах и задачах / И.Л. Акулич. – М.: Высш. шк., 1986. – 319 с.

Поступила в редколлегию 12.07.2011

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Национальный технический университет сельского хозяйства им. П. Василенко, Харьков.

ЛІНІЙНЕ ЦІЛОЧИСЕЛЬНЕ ДЕКОДУВАННЯ ПСЕВДОВИПАДКОВИХ КОДІВ НА ОСНОВІ МЕТОДУ ВІДСІКАНЬ ГОМОРІ

С.Г. Рассомахін

Констатується перспективність псевдовипадкових завадостійких кодів, отриманих методом лінійної конгруентної генерації, для використання в системах передачі інформації. Запропоновано правило декодування, засноване на методі найменших проекцій. Розглянутий алгоритм формалізації декодування, що дозволяє звести роботу декодера до рішення задачі цілочисельного лінійного програмування. Приведена оцінка ефективності запропонованого методу в порівнянні з переборними алгоритмами декодування.

Ключові слова: *псевдовипадкові коди, амплитудно-фазова модуляція, лінійне цілочисельне програмування, симплекс-метод, правило Гоморі.*

INTEGER LINEAR DECODING OF PSEUDORANDOM CODES BASED ON THE METHOD OF GOMORY'S CUTTING PLANE

S.G. Rassomakhin

The perspective of pseudo-error-correcting codes obtained by the method of linear congruent generation for use in data transmission systems is stated. The rule decoding based on the method of lowest projections is proposed. An algorithm for the formalization of the decoding, which allows to reduce the decoder work to the problem solving of integer linear programming is considered. An estimation of efficiency of the offered method is brought as compared to exhaustive decoding algorithms.

Keywords: *pseudorandom codes, amplitude-phase modulation, linear integer programming, symplex-method, Gomory's rule.*