УКРАЇНСЬКА ДЕРЖАВНА АКАДЕМІЯ
ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

Штомпель Микола Анатолійович

УДК 621.391

МЕТОДИ ЗГОРТКОВОГО КОДУВАННЯ ТА ДЕКОДУВАННЯ ДАНИХ НА ОСНОВІ АЛГОРИТМУ ШВИДКОГО ПЕРЕТВОРЕННЯ ФУР'Є

05.12.02 – Телекомунікаційні системи та мережі

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2010

Дисертацією є рукопис.

Робота виконана в Українській державній академії залізничного транспорту Міністерства транспорту та зв'язку України

Науковий керівник: кандидат технічних наук, доцент
Приходько Сергій Іванович, Українська державна академія залізничного транспорту, завідувач кафедри «Транспортний зв'язок».

Офіційні опоненти: доктор технічних наук, професор
Лосєв Юрій Іванович, Харківський національний університет імені В.Н. Каразіна, професор кафедри теоретичної та прикладної системотехніки;

кандидат технічних наук
Дуравкін Євген Володимирович, Харківський національний університет радіоелектроніки, доцент кафедри телекомунікаційних систем.

Захист відбудеться «15» вересня 2010 року о 14^{30} годині на засіданні спеціалізованої вченої ради Д 64.820.01 в Українській державній академії залізничного транспорту, 61050, м. Харків, пл. Фейєрбаха 7.

З дисертацією можна ознайомитись в бібліотеці Української державної академії залізничного транспорту, 61050, м. Харків, пл. Фейєрбаха 7.

Автореферат розісланий «16» серпня 2010 р.

Вчений секретар
спеціалізованої вченої ради _____ Г.В. Альошин

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми дослідження. У теперешній час теорії завадостійкого кодування відомо декілька методів кодування й декодування даних, що забезпечують роботу поблизу пропускної здатності каналу зв’язку. Серед цих методів можна виділити турбо- та турбоподібні коди, які на даному етапі активно розвиваються. Однак, вказані методи характеризуються значною обчислювальною складністю, а це обмежує їх практичне застосування у сучасних високошвидкісних телекомунікаційних системах. У зв'язку з цим виникає проблема пошуку більш простих і менш витратних при практичній реалізації методів кодування й декодування даних. Враховуючи тенденцію постійного зростання швидкостей обміну даними, це питання набуває більшу актуальність. Згорткові коди, хоча й забезпечують менш високий енергетичний виграш кодування у порівнянні з турбокодами, проте знаходять широке застосування в різноманітних системах передачі даних: в системах бездротового зв'язку, в цифрових наземних і супутникових системах зв'язку й віщання, в системах зв'язку з далеким космосом та ін. У той же час впровадження згорткових кодів з великою довжиною кодового обмеження дозволяє підвищити вірогідність переданих даних та це пов’язано з наступними труднощями: складність побудови «хороших» кодів та висока обчислювальна складність методів кодування, а особливо, декодування даних.

Такі проблеми як обмеженість пропускної здатності каналів зв'язку, збільшення потоків переданих даних, необхідність достовірної передачі даних, зростання часу обробки даних в кодері та декодері (кодеку) вимагають розробки нових ефективних методів згорткового кодування й декодування в телекомунікаційних системах.

Значний внесок у дослідження питань теорії завадостійкого кодування, зокрема згорткового кодування й декодування даних, внесли російські й українські вчені: Зигангіров К.Ш., Золотарьов В.В., Овечкин Г.В., Кудряшов Б.Д., Приходько С.І., Банкет В.Л. Серед закордонних учених, які вирішували завдання в області згорткового кодування, необхідно відзначити: Елайеса П., Форні Г.Д., Возенкрафта Д., Фано Р., Мессі Дж., Блейхута Р.

Таким чином, дослідження щодо розробки й удосконалення методів згорткового кодування й декодування даних зі зменшеною обчислювальною складністю стосуються актуальної проблеми подальшого розвитку теорії завадостійкого кодування.

Зв'язок з науковими програмами, планами, темами.

Дослідження дисертаційної роботи виконувалися у відповідності з наступними нормативними актами:

1) Концепція Національної програми інформатизації, схвалена Законом України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 р. № 75/98-ВР;

2) Концепція розвитку зв'язку України до 2010 року, затверджена постановою Кабінету Міністрів України «Про Концепцію розвитку зв'язку України до 2010 року» від 9 грудня 1999 р. № 2238;

3) Концепція створення Державної інтегрованої інформаційної системи забезпечення управління рухомими об'єктами (зв'язок, навігація, спостереження), схвалена розпорядженням Кабінету Міністрів України від 17 липня 2003 р. №410-р.;

4) Концепція розвитку телекомунікацій в Україні, схвалена розпорядженням Кабінету Міністрів України від 7 червня 2006 р. № 316-р.

Мета й завдання дослідження. Метою дисертаційної роботи є розробка методів, що спрямовані на зниження обчислювальної складності згорткового кодування й декодування даних та підвищення швидкості їх обробки в кодері й декодері.

Для досягнення вказаної мети в дисертаційній роботі необхідно вирішити наступні завдання.

1. Проаналізувати методи згорткового кодування й декодування даних, алгоритми швидкого обчислення згортки й швидкого перетворення Фур'є (ШПФ) в кінцевих полях і оцінити їх обчислювальну складність.
2. Розробити метод алгебраїчного представлення згорткових кодів у частотній області, що заснований на описі інформаційної, узагальненої породжуючої й кодової послідовностей у вигляді їх Фур'є-образів.
3. На основі алгоритмів швидкого обчислення згортки Агарвала-Кулі й ШПФ Винограду розробити методи згорткового кодування даних, що спрямовані на зниження обчислювальної складності кодеру.
4. На основі представлення процесу декодування в частотній області та застосування алгоритму ШПФ Винограду розробити метод алгебраїчного декодування згорткових кодів, що забезпечує зменшення обчислювальної складності декодеру.
5. На основі запропонованих методів згорткового кодування та декодування даних розробити алгоритми, оцінити їх обчислювальну складність та здійсніти порівняння з існуючими алгоритмами.
6. Розробити програмну й програмно-апаратну реалізації розроблених алгоритмів згорткового кодування й декодування даних та обґрунтувати практичні рекомендації щодо їх технічної реалізації.

Об'єктом дослідження є процеси згорткового кодування й декодування даних.

Предметом дослідження є методи згорткового кодування й декодування даних зі зменшеною обчислювальною складністю.

Методи дослідження. Розробка методів згорткового кодування та декодування даних проведені з застосуванням методів теорії завадостійкого кодування, теорії кінцевих полей Галуа, теорії чисел та теорії цифрової обробки сигналів. Оцінка обчислювальної складності розроблених алгоритмів проведена з використанням методів теорії складності. Розробка практичних рекомендацій з реалізації запропонованих алгоритмів згорткового кодування та декодування даних проведена з використанням методів теорії цифрових автоматів.

Наукова новизна отриманих результатів в дисертаційній роботі полягає у наступному.

1. Одержав подальший розвиток метод алгебраїчного представлення згорткових кодів у вигляді недвійкових блокових циклічних кодів, що відрізняється від відомого описом інформаційної, узагальненої породжуючої й кодової послідовностей згорткового коду у вигляді їх Фур'є-образів та дозволяє розробити нові методи згорткового кодування й декодування даних з меншою обчислювальною складністю.

2. Вперше на основі алгоритмів обчислення згортки Агарвала-Кулі та ШПФ Винограду розроблено методи згорткового кодування даних, що дозволяють знизити обчислювальну складність кодеру.

3. Удосконалено існуючий метод алгебраїчного декодування згорткових кодів, що відрізняється від відомого представленням процесу декодування в частотній області й застосуванням алгоритму ШПФ Винограду; запропонований метод декодування зменшує обчислювальну складність декодеру за рахунок скорочення необхідної кількості арифметичних операцій.

Практичне значення отриманих результатів досліджень дисертаційної роботи полягає в наступному.

1. На основі запропонованого методу згорткового кодування даних розроблено алгоритм, що має в 1,2 - 3,8 рази меншу обчислювальну складність у порівнянні з існуючим алгоритмом згорткового кодування даних у часовій області, при фіксованих параметрах згорткового коду. На основі запропонованого методу алгебраїчного декодування згорткових кодів розроблено алгоритм, обчислювальна складність якого у 1,3 - 2,6 рази менша, ніж у існуючого алгоритму декодування згорткових кодів у часовій області, при фіксованих параметрах згорткового коду.

2. Розроблено програмну й програмно-апаратну реалізації запропонованих алгоритмів згорткового кодування й декодування даних, що дозволяють забезпечити роботу кодеку при швидкості передачі даних у каналі зв'язку відповідно до 12 Мбіт/с і 500 Мбіт/с.

3. Розроблено практичні рекомендації щодо технічної реалізації алгоритмів частотного згорткового кодування й декодування даних. Для зменшення обчислювальної складності кодеру згорткових кодів з вхідною довжиною кодового обмеження $r \geq 32$ пропонується використовувати розроблений алгоритм згорткового кодування даних, а для зниження обчислювальної складності декодеру згорткових кодів з вхідною довжиною кодового обмеження $r \geq 8$ – запропонований алгоритм декодування даних. Алгоритм ШПФ Винограду необхідно реалізувати у вигляді оптимізованого програмного коду для цифрового сигнального процесору (ЦСП). Для забезпечення роботи згорткового декодеру при швидкості передачі даних по каналу зв'язку понад 500 Мбіт/с пропонується апаратно реалізувати алгоритм Берлекемпа-Мессі й рекурентне продовження синдрому, а також застосувати паралельну версію алгоритму ШПФ Винограду.

4. Отримані результати використані на виробництві при розробці спеціального математичного та програмно-апаратного забезпечення виробу, виконаного в межах дослідно-конструкторської роботи «Жанр-РС-ШШС», у ЦККБ «Протон» (акт реалізації від 16.07.2010 р.) і в навчальному процесі

Української державної академії залізничного транспорту (акт реалізації від 10.02.2010 р.).

Особистий внесок автора. Всі результати, що викладені в дисертаційній роботі, автором отримано особисто. У наукових працях, які виконані у співавторстві й опубліковані у виданнях, що входять до переліку ВАК України, авторові належать: в [1] - запропонований метод алгебраїчного представлення згорткових кодів у частотній області; в [3] - удосконалений метод алгебраїчного декодування згорткових кодів; в [4] - розроблений метод згорткового кодування даних на основі швидкого алгоритму згортки Агарвала-Кулі.

Апробація роботи. Матеріали дисертаційної роботи доповідалися та були схвалені на:

- п’ятій та шостій наукових конференціях Харківського університету Повітряних сил імені Івана Кожедуба (м. Харків, 2009, 2010 рр.);
- дев’ятій міжнародній науково-технічній конференції «Проблеми інформатики та моделювання» НТУ “ХПІ” (м. Харків, 2009 р.).

Публікації. Результати дисертаційної роботи викладені в 8 публікаціях, з них 5 статей у наукових виданнях, що входять до переліку ВАК України, і 3 тези доповідей на науково-технічних конференціях.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновку та додатків. Повний обсяг дисертації становить 136 сторінки, у тому числі 2 додатки на 5 сторінках, 31 рисунок, 5 таблиць, перелік використаних літературних джерел містить 130 найменувань на 12 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовується актуальність теми дисертаційної роботи, формулюється її мета, визначаються завдання наукових досліджень, наводиться наукова новизна отриманих результатів та вказуються їх практичне значення й впровадження.

У першому розділі розглянуті основні параметри й характеристики згорткових кодів. Проаналізовано обчислювальну складність класичних методів згорткового кодування й декодування даних. Наведено методи представлення згорткових кодів у вигляді блокових кодів. Розглянуто особливості перетворення Фур'є в кінцевих полях та здійснено аналіз обчислювальної складності алгоритмів швидкого перетворення Фур'є.

Завадостійкі коди поділяються на два класи: блокові коди й безперервні (згорткові) коди. Відомо, що згорткові коди мають ряд переваг у порівнянні із блоковими кодами, а саме, збереження коригувальної здатності при будь-якій довжині; зручність застосування в системах послідовного й паралельного каскадного кодування; більш низькі вимоги до синхронізації й фазування. З іншого боку, обчислювальна складність методів побудови згорткових кодів з великою довжиною кодового обмеження та процесів їх кодування й декодування залишається досить високою. При цьому під обчислювальною складністю (трудомісткістю) методу розуміється число арифметичних операцій

(множень і додавань), що необхідні для згорткового кодування й декодування деякого блоку даних. Проведений аналіз показав, що обчислювальна складність згорткового кодування лінійно зростає зі збільшенням довжини кодового обмеження, а застосування згорткових кодів з великою довжиною кодового обмеження призводить до відносно значної затримки даних у кодері. З аналізу класичних методів декодування згорткових кодів випливає, що тільки метод послідовного декодування можна застосовувати для згорткових кодів з великою довжиною кодового обмеження, але він має високу обчислювальну складність при зростанні рівня завад в каналі зв'язку. Крім того, зменшення трудомісткості класичних методів декодування згорткових кодів практично неможливо здійснити без урахування їх алгебраїчної структури.

Таким чином, питання щодо розвитку методів, які спрямовані на зниження обчислювальної складності згорткового кодування й декодування даних та підвищення швидкості їх обробки в кодері й декодері стосуються актуальної проблеми.

Установлений зв'язок між згортковими й блоковими кодами дозволяє застосовувати відомі результати з теорії блокових кодів для їх дослідження. Однак класичні методи представлення згорткових кодів у вигляді блокових кодів не враховують їх алгебраїчну структуру, а це обмежує практичне застосування даних методів. Існує метод алгебраїчного представлення згорткових кодів у часовій області, що усуває вказаний недолік. Однак, з теорії блокових кодів відомо, що перехід у частотну область за допомогою перетворення Фур'є дозволяє зменшити обчислювальну складність кодеру й декодеру за рахунок застосування швидких алгоритмів обчислення згортки й перетворення Фур'є. Аналіз алгоритмів ШПФ у кінцевих полях показав, що найменшу обчислювальну складність за кількістю операцій множення має алгоритм Винограду, тому його доцільно використовувати для зниження трудомісткості згорткового кодування та декодування даних.

На основі проведеного аналізу та відповідно до мети дисертаційної роботи сформульовані завдання наукового дослідження.

В другому розділі проведено аналіз методу алгебраїчного представлення згорткових кодів у вигляді недвійкових блокових циклічних кодів і обчислювальної складності згорткового кодування в часовій області. Розроблено метод алгебраїчного представлення згорткових кодів у частотній області за рахунок застосування перетворення Фур'є до інформаційного, узагальненого породжуючого й кодового багаточленів згорткового коду. Визначено обчислювальну складність згорткового кодування даних в частотній області при використанні прямого методу обчислення перетворення Фур'є. Запропоновано методи згорткового кодування даних на основі алгоритмів обчислення згортки Агарвала-Кулі та ШПФ Винограду, а також надана оцінка їх обчислювальної складності.

Встановлено, що згорткове кодування даних у часовій області відповідає задачі обчислення кінцевої лінійної згортки:

$$c_i = \sum_{l=0}^{r-1} i_{i-l} g_l , \qquad i = 0, 1, \dots , n - 1, \qquad (1)$$

де i – елементи інформаційної послідовності згорткового коду, що належать полю $GF(p)$;

g, c – відповідно елементи узагальненої породжуючої й кодової послідовностей згорткового коду, що належать полю $GF(p^m)$;

n – повна довжина кодового обмеження згорткового коду;

r – вхідна довжина кодового обмеження.

Обчислювальна складність згорткового кодування в часовій області визначається за формулою:

$$O_T(n) = (k + 1)\cdot(r + 1) \approx n^2, \qquad (2)$$

де k – довжина інформаційної послідовності згорткового коду кінцевої довжини.

З формули (2) випливає, що обчислювальна складність кодування описується поліноміальним законом, що не є оптимальним з точки зору мінімізації кількості арифметичних операцій.

У зв'язку з цим розроблено метод алгебраїчного представлення згорткових кодів у частотній області. Основні етапи його реалізації наведені нижче.

1. Обчислення перетворення Фур'є інформаційної послідовності згорткового коду:

$$I_j = \sum_{i=0}^{n-1} \alpha^{ij} i_i , \qquad j = 0, 1, \dots , n - 1,$$

де $б$ – примітивний елемент порядку n у полі $GF(p^m)$;

I_j - частотний вектор (Фур'є-образ) інформаційної послідовності над полем $GF(p^m)$.

2. Обчислення перетворення Фур'є узагальненої породжуючої послідовності згорткового коду:

$$G_j = \sum_{i=0}^{n-1} \alpha^{ij} g_i , \qquad j = 0, 1, \dots , n - 1,$$

де G_j - частотний вектор (Фур'є-образ) узагальненої породжуючої послідовності над полем $GF(p^m)$.

3. Знаходження кодової послідовності згорткового коду в частотній області шляхом поточечного множення Фур'є-образів інформаційної й узагальненої породжуючої послідовностей:

$$C_j = I_j G_j, \qquad j = 0, 1, \dots , n - 1, \qquad (3)$$

де C_j – частотний вектор (Фур'є-образ) кодової послідовності згорткового коду над полем $GF(p^m)$.

Розроблений метод можна безпосередньо застосувати для згорткового кодування даних у частотній області, використовуючи прямий метод

обчислення перетворення Фур'є й додатковий етап – знаходження зворотнього перетворення Фур'є. Однак, у цьому випадку обчислювальна складність частотного кодування більше складності кодування в часовій області (2) і визначається за формулою:

$$O_{\mathrm{F}}(n) = O_I(n) + O_C(n) + O_c(n) = n^2 + n + n^2 = 2\cdot n^2 + n, \quad (4)$$

де $O_I(n)$, $O_C(n)$ – відповідно обчислювальна складність знаходження Фур'є-образів інформаційної й кодової послідовностей;

$O_c(n)$ - обчислювальна складність знаходження зворотнього перетворення Фур'є.

Для зменшення обчислювальної складності згорткового кодування даних у випадку, коли повна довжина кодового обмеження згорткового коду являє собою добуток декількох співмножників, пропонується застосовувати алгоритми швидкого обчислення згортки й ШПФ.

Розроблений метод згорткового кодування даних на основі алгоритму Агарвала-Кулі обчислення згортки при використанні згорткового коду з повною довжиною кодового обмеження, що задовольняє умовам $n \mid p^m - 1$ і $n = n'\cdot n''$, складається з наступних етапів.

1. Заміна індексів i і l у формулі (1) парами індексів (i', i'') і (l', l''):

$$i = n''i' + n'i'', \qquad i' = 0,\ldots, n' - 1,\ i'' = 0,\ldots, n'' - 1,$$

$$l = n''l' + n'l'', \qquad l' = 0,\ldots, n' - 1,\ l'' = 0,\ldots, n'' - 1.$$

2. Визначення нових індексів відповідно до китайської теореми про залишки:

$$i' = N''i(\mathrm{mod}\, n'), \qquad l' = N''l(\mathrm{mod}\, n'),$$

$$i'' = N'i(\mathrm{mod}\, n''), \qquad l'' = N'l(\mathrm{mod}\, n''),$$

де N' і N'' - цілі числа, що задовольняють умові $N'n' + N''n'' = 1$.

3. Представлення процесу згорткового кодування даних, що відповідає формулі (1), наступним чином:

$$c_{n''i'+n'i''} = \sum_{l'=0}^{n'-1}\sum_{l''=0}^{n''-1} i_{n''l'+n'l''} g_{n''(i'-l')+n'(i''-l'')}. \quad (5)$$

4. Визначення двовимірних змінних i, g і c:

$$i_{l',l''} = i_{n''l'+n'l''}, \qquad g_{l',l''} = g_{n''l'+n'l''}, \qquad c_{l',l''} = c_{n''l'+n'l''},$$

5. Запис формули (5) у вигляді двовимірного кодового слова згорткового коду:

$$c_{i',i''} = \sum_{l'=0}^{n'-1}\sum_{l''=0}^{n''-1} i_{l',l''} g_{(i'-l'),(i''-l'')}, \quad (6)$$

де перші й другі індекси беруться відповідно за модулями n' і n''.

6. Визначення одновимірних наборів багаточленів (по n'' багаточленів у кожному наборі) шляхом застосування уздовж кожного виміру алгоритму Винограду обчислення згортки:

$$i_{l'}(x) = \sum_{l'=0}^{n'-1} i_{l',l''} x^{l'}, \qquad g_{l'}(x) = \sum_{l'=0}^{n'-1} g_{l',l''} x^{l'}, \qquad c_{l'}(x) = \sum_{l'=0}^{n'-1} c_{l',l''} x^{l'}.$$

7. Запис двовимірної згортки (6) у вигляді одновимірної згортки багаточленів:

$$c_{i''}(x) = \sum_{l'=0}^{n''-1} g_{((l'-l''))}(x) i_{l''}(x) (\mathrm{mod} x^{n'} - 1).$$

Для кожного i'' у цій сумі виконується додавання n'' добутків багаточленів, тоді всього утворюється $(n'')^2$ добутків багаточленів. Кожний з добутків багаточленів є згорткою і обчислюється за допомогою алгоритму Винограду. Для остаточного обчислення кодового слова згорткового коду з використанням алгоритму Агарвала-Кулі необхідно застосувати алгоритм Винограду обчислення згортки також по другому виміру.

Для розглянутого випадку мультиплікативна й арифметична складність розробленого методу відповідно дорівнює:

$$M(n) = M(n')\, M(n''); \qquad A(n) = A(n')\, n'' + M(n')\, A(n''), \tag{7}$$

де $M(n')$ і $M(n'')$ – відповідно число множень у полі $GF(p^m)$, що необхідні для обчислення згорток довжини n' і n'';
$A(n')$ і $A(n'')$ – відповідно число додавань у полі $GF(p^m)$, що необхідні для обчислення згорток довжини n' і n''.

Метод частотного кодування даних на основі алгоритму ШПФ Винограду при використанні згорткового коду з повною довжиною кодового обмеження, що задовольняє умовам $n \mid p^m - 1$ і $n = n_1 n_2$, складається з наступних етапів.

1. Застосування алгоритму ШПФ Винограду до інформаційної послідовності згорткового коду кінцевої довжини:

$$\bar{I} = (CBA)\bar{i}, \tag{8}$$

де A – матриця попередніх додавань над полем $GF(p)$;
B – діагональна матриця коефіцієнтів перетворення Фур'є над полем $GF(p^m)$;
C – матриця наступних додавань над полем $GF(p)$.

2. Знаходження Фур'є-образа кодової послідовності згорткового коду за формулою (3).

3. Обчислення зворотнього ШПФ Винограду кодової послідовності згорткового коду за формулою (8) з попередньо переставленими елементами матриць A та C і її відображення у двійковий вид.

Обчислювальна складність згорткового кодування даних на основі алгоритму ШПФ Винограду дорівнює:

$$O_{\mathrm{FF}}(n) = O_I(n) + O_C(n) + O_c(n) = n \log_2 n + n + n \log_2 n = 2 \cdot n \log_2 n + n. \tag{9}$$

З аналізу формул (2), (4), (7) і (9) випливає, що розроблені методи згорткового кодування даних мають меншу обчислювальну складність, ніж метод згорткового кодування в часовій області.

У третьому розділі розглянуті методи зменшення обчислювальної складності й збільшення коригувальної здатності класичних методів декодування згорткових кодів. Проведено аналіз методу алгебраїчного декодування згорткових кодів у часовій області, що дозволяє декодувати згорткові коди з великою довжиною кодового обмеження, а також здійснена оцінка його обчислювальної складності. Розроблено метод алгебраїчного декодування згорткових кодів у частотній області й проведено аналіз його обчислювальної складності при використанні прямого методу обчислення перетворення Фур'є. Обґрунтовано використання алгоритму ШПФ Винограду для зменшення обчислювальної складності відповідних етапів частотного декодування згорткових кодів.

Проведений аналіз показав, що метод алгебраїчного декодування згорткових кодів у часовій області є перспективним, так як він передбачає фіксовану кількість операцій при заданій коригувальній здатності t й може використовуватися для декодування згорткових кодів з великою довжиною кодового обмеження.

Основні етапи методу алгебраїчного декодування згорткових кодів у часовій області та їх обчислювальна складність наведені в табл. 1.

Таблиця 1

Обчислювальна складність методу алгебраїчного декодування згорткових кодів у часовій області

Номер етапу	Назва етапу декодування	Обчислювальна складність	
		Множення	Додавання
1	Перетворення нескінченої двійкової прийнятої послідовності згорткового коду в символи й розділення її на окремі частини	-	-
2	Обчислення синдрому частини прийнятої послідовності згорткового коду	$2nt$	$2nt$
3	Знаходження багаточлена локаторів помилок (алгоритм Берлекемпа-Мессі)	$4t^2$	$4t^2$
4	Процедура Ченя	nt	nt
5	Обчислення багаточлена значень помилок (алгоритм Форні)	$2t^2 + t$	$2t^2 + t$
6	Виправлення частини прийнятої послідовності згорткового коду	-	n
7	Вилучення частини інформаційної послідовності та її відображення у двійкову послідовність	-	-

Усього	$3nt + 6t^2 + t$	$3nt + 6t^2 + t + n$

З аналізу даних табл. 1 випливає, що найбільш трудомісткими етапами декодування є обчислення синдрому й процедура Ченя. Слід зазначити, що обчислювальна складність декодування суттєво зростає при великих значеннях довжини кодового обмеження, що обмежує область застосування даного методу.

Удосконалення існуючого методу алгебраїчного декодування згорткових кодів можливо за рахунок представлення етапів обчислення синдрому й процедури Ченя з частотної точки зору.

Основні етапи методу алгебраїчного декодування згорткових кодів у частотній області представлені нижче.

1. Перетворення елементів поля $GF(p)$ нескінченої прийнятої послідовності згорткового коду в символи поля $GF(p^m)$ та їх розбиття на частини довжиною n:

$$v = v_0^m, v_1^m, ..., v_{n-1}^m, v_n^m, v_{n+1}^m, ..., v_{2n-1}^m, ... \quad (10)$$

де v_i^m - i - елемент нескінченої прийнятої послідовності.

Величина v_i^m знаходиться за формулою:

$$v_i^m = c_i^m + e_i^m,$$

де c_i^m – кодова послідовність над полем $GF(p^m)$;

e_i^m – послідовність помилок над полем $GF(p^m)$.

2. Застосування n-точечного перетворення Фур'є до прийнятого блоку згорткового коду (10) для обчислення перевірочних частот (синдрому):

$$V_j^m = \sum_{i=0}^{n-1} \alpha^{ij} v_i^m = v_i^m(\alpha^j), \qquad j = 1, \ldots, 2t,$$

де t – максимальна кількість помилок, що виправляються, у прийнятому блоці.

Якщо перевірочні частоти прийнятого блоку $V_0^m = ... = V_{n-k-1}^m = 0$, то в ньому помилок немає. В іншому випадку даний блок викривлений завадами і необхідно обчислити вектор помилок e_i^m.

3. Знаходження багаточлена локаторів помилок за допомогою методу Берлекемпа-Мессі:

$$\Lambda(x) = \prod_{k=1}^{u} (1 - x\alpha^{i_k}) = \Lambda_u x^u + \Lambda_{u-1} x^{u-1} + ... + \Lambda_0,$$

де $u \le t$ – кількість помилок, що мають місце та не перевищують коригувальну здатність коду.

4. Рекурентне продовження синдрому й обчислення вектора помилок у частотній області:

$$E_k^m = -\sum_{j=1}^{t} \Lambda_j E_{((k-j))}^m, \qquad k = 0, \ldots, n-1.$$

5. Виправлення прийнятого блоку згорткового коду в частотній області:

$$C_j^m = V_j^m + E_j^m,$$

$j = 0, \ldots, n - 1.$ (11)

6. Застосування зворотнього перетворення Фур'є до блоку кодової послідовності згорткового коду, що визначається за формулою (11):

$$v_i^m = \frac{1}{n}\sum_{i=0}^{n-1} \alpha^{ij} V_j^m, \quad j = 0, \ldots, n-1. \quad (12)$$

7. Вилучення частини інформаційної послідовності згорткового коду та її перетворення в елементи поля $GF(p)$.

Для зменшення обчислювальної складності частотного декодування згорткових кодів у випадку, коли виконуються умови $n \mid p^m - 1$ і $n = n_1 \cdot n_2$, доцільно застосовувати алгоритм ШПФ Винограду, як найбільш ефективний у порівнянні з прямим методом обчислення перетворення Фур'є.

Основні етапи розробленого методу алгебраїчного декодування згорткових кодів у частотній області з використанням ШПФ Винограду та їх обчислювальна складність наведені в табл. 2.

Таблиця 2

Обчислювальна складність методу алгебраїчного декодування згорткових кодів у частотній області з використанням ШПФ Винограду

Номер етапу	Назва етапу декодування	Обчислювальна складність	
		Множення	Додавання
1	Перетворення нескінченої двійкової кодової послідовності згорткового коду в символи й розділення її на окремі частини	-	-
2	Обчислення прямого перетворення Фур'є за допомогою ШПФ Винограду частини прийнятої послідовності згорткового коду	$n \log_2 n$	$n \log_2 n$
3	Знаходження багаточлена локаторів помилок (алгоритм Берлекемпа-Мессі)	$4t^2$	$4t^2$
4	Рекурентне продовження синдрому	$t(n - 2t)$	$t(n - 2t)$
5	Виправлення частини прийнятої послідовності	-	n

	згорткового коду в частотній області		
6	Обчислення зворотного перетворення Фур'є за допомогою ШПФ Винограду	$n \log_2 n$	$n \log_2 n$
7	Вилучення частини інформаційної послідовності та її відображення у двійкову послідовність	-	-
Усього		$2n \log_2 n + nt + 2t^2$	$2n \log_2 n + nt + 2t^2 + n$

Аналіз даних табл. 1, 2 свідчить, що метод алгебраїчного декодування в частотній області з використанням алгоритму ШПФ Винограду має меншу обчислювальну складність, ніж реалізація даного методу декодування в часовій області.

У четвертому розділі наводяться результати з оцінки обчислювальної складності алгоритмів, що реалізують розроблені методи частотного згорткового кодування й декодування даних, в залежності від вхідної та повної довжин кодового обмеження. Проведено аналіз способів технічної реалізації запропонованих алгоритмів. Розраховано швидкодію згорткового кодеру й декодеру при програмній та програмно-апаратній реалізаціях даних алгоритмів, а також розроблені практичні рекомендації щодо їх технічної реалізації.

Оцінка обчислювальної складності алгоритму, що реалізує розроблений метод згорткового кодування даних на основі ШПФ Винограду, відповідно до формул (2) і (9) показала, що при вхідній довжині кодового обмеження $r \geq 32$ в 1,2 - 3,8 рази зменшується кількість операцій множення у порівнянні з алгоритмом згорткового кодування даних в часовій області. Слід зазначити, розрахунки виконувалися за умови, що вхідна довжина кодового обмеження становить $r \approx n/2$. При фіксованій повній довжині кодового обмеження n можливо одержати виграш за числом операцій множення для меншої вхідної довжини кодового обмеження, а саме:

- при $n = 378$ - $17 \leq r \leq 45$;
- при $n = 889$ - $16 \leq r \leq 111$;
- при $n = 2040$ - $18 \leq r \leq 237$.

Таким чином, із проведених розрахунків випливає, що розроблений алгоритм частотного згорткового кодування необхідно використовувати для згорткових кодів із вхідною довжиною кодового обмеження $r \geq 16$ при $n \geq 378$ або в загальному випадку при $r \geq 32$.

Результати розрахунків за формулами, які наведені в табл. 1, 2, свідчать, що алгоритм, що реалізує метод частотного декодування згорткових кодів, забезпечує в 1,3 - 2,6 рази меншу обчислювальну складність у порівнянні з алгоритмом алгебраїчного декодування в часовій області при вхідній довжині кодового обмеження $r \geq 8$ (у випадку виконання умови $r \approx n/2$). При

фіксованій повній довжині кодового обмеження та змінних значеннях вхідної довжини кодового обмеження алгоритм алгебраїчного декодування в частотній області вимагає меншої кількості операцій множення у наступних випадках:

- при $n = 60$ - $r \geq 6$;
- при $n = 155$ - $r \geq 8$;
- при $n = 378$ - $r \geq 11$;
- при $n = 889$ - $r \geq 13$;
- при $n = 2040$ - $r \geq 16$.

Таким чином, із проведених розрахунків випливає, що розроблений алгоритм частотного декодування на основі ШПФ Винограду доцільно застосовувати для згорткових кодів із вхідною довжиною кодового обмеження $r \geq 6$, при цьому суттєве зменшення обчислювальної складності спостерігається при $r \geq 11$.

Аналіз способів технічної реалізації запропонованих алгоритмів згорткового кодування й декодування даних показав, що їх програмна реалізація на базі ЦСП має ряд переваг, серед яких основною є забезпечення роботи в реальному часі при швидкості передачі даних по каналу зв'язку до 12 Мбіт/с.

Для забезпечення роботи кодеку при швидкості передачі даних по каналу зв'язку до 500 Мбіт/с розроблені алгоритми необхідно реалізувати програмно-апаратним способом на базі ЦСП й зовнішньої програмованої користувачем вентильної матриці, що призначена для множення й додавання елементів поля $GF(p^m)$.

Розроблено практичні рекомендації щодо технічної реалізації запропонованих алгоритмів згорткового кодування й декодування даних.

У **додатках** наведена структурна схема та технічні характеристики ЦСП TMS320C6416T, що використовувався для розрахунку швидкодії згорткового кодеку, та акти реалізацій результатів дисертаційної роботи.

ВИСНОВКИ

У дисертаційній роботі проведене теоретичне узагальнення й отримане нове рішення наукового завдання, що полягає у розробці методів згорткового кодування й декодування даних зі зменшеною обчислювальною складністю на основі алгоритму швидкого перетворення Фур'є для підвищення швидкості обробки даних в кодері й декодері. Основні висновки по роботі полягають у наступному.

1. Проведений аналіз показав, що в теперешній час відомо декілька методів кодування й декодування даних, що забезпечують роботу поблизу пропускної здатності каналу зв'язку, зокрема, турбо- та турбоподібні коди. Однак, дані методи мають значну обчислювальну складність, що ускладнює їх практичне застосування у високошвидкісних телекомунікаційних системах. Згорткові коди забезпечують менш високий енергетичний виграш кодування у порівнянні з турбокодами, але вони також широко застосовуються в різноманітних

системах передачі даних. Впровадження згорткових кодів з великою довжиною кодового обмеження дозволяє підвищити вірогідність переданих даних та це пов’язано з наступними труднощями: складність побудови «хороших» кодів та висока обчислювальна складність методів кодування, а особливо, декодування даних. Такі проблеми як обмеженість пропускної здатності каналів зв'язку, збільшення потоків переданих даних, необхідність достовірної передачі даних, зростання часу обробки даних в кодеку вимагають розробки методів згорткового кодування й декодування даних зі зменшеною обчислювальною складністю.

2. В ході виконання дисертаційної роботи отримані наступні наукові результати:

- одержав подальший розвиток метод алгебраїчного представлення згорткових кодів у вигляді недвійкових блокових циклічних кодів, що відрізняється від відомого описом інформаційної, узагальненої породжуючої й кодової послідовностей згорткового коду у вигляді їх Фур'є-образів та дозволяє розробити нові методи згорткового кодування й декодування даних з меншою обчислювальною складністю;

- вперше на основі алгоритмів обчислення згортки Агарвала-Кулі та ШПФ Винограду розроблено методи згорткового кодування даних, що дозволяють знизити обчислювальну складність кодеру;

- удосконалено існуючий метод алгебраїчного декодування згорткових кодів, що відрізняється від відомого представленням процесу декодування в частотній області й застосуванням алгоритму ШПФ Винограду; запропонований метод декодування зменшує обчислювальну складність декодеру за рахунок скорочення необхідної кількості арифметичних операцій.

3. В процесі проведення дисертаційних досліджень отримані наступні практичні результати:

- на основі запропонованого методу згорткового кодування даних розроблено алгоритм, що має в 1,2 - 3,8 рази меншу обчислювальну складність у порівнянні з існуючим алгоритмом згорткового кодування даних у часовій області, при фіксованих параметрах згорткового коду. На основі запропонованого методу алгебраїчного декодування згорткових кодів розроблено алгоритм, обчислювальна складність якого у 1,3 - 2,6 рази менша, ніж у існуючого алгоритму декодування згорткових кодів у часовій області, при фіксованих параметрах згорткового коду;

- розроблено програмну й програмно-апаратну реалізації запропонованих алгоритмів згорткового кодування й декодування даних, що дозволяють забезпечити роботу кодеку при швидкості передачі даних у каналі зв'язку відповідно до 12 Мбіт/с і 500 Мбіт/с;

- розроблено практичні рекомендації щодо технічної реалізації алгоритмів частотного згорткового кодування й декодування даних. Для зменшення обчислювальної складності кодеру згорткових кодів з вхідною довжиною кодового обмеження $r \geq 32$ пропонується використовувати розроблений алгоритм згорткового кодування даних, а для зниження обчислювальної складності декодеру згорткових кодів з вхідною довжиною кодового

обмеження $r \geq 8$ – запропонований алгоритм декодування даних. Алгоритм ШПФ Винограду необхідно реалізувати у вигляді оптимізованого програмного коду для цифрового сигнального процесору (ЦСП). Для забезпечення роботи згорткового декодеру при швидкості передачі даних по каналу зв'язку понад 500 Мбіт/с пропонується апаратно реалізувати алгоритм Берлекемпа-Мессі й рекурентне продовження синдрому, а також застосувати паралельну версію алгоритму ШПФ Винограду;

- отримані результати використані на виробництві при розробці спеціального математичного та програмно-апаратного забезпечення виробу, виконаного в межах дослідно-конструкторської роботи «Жанр-РС-ШШС», у ЦККБ «Протон» (акт реалізації від 16.07.2010 р.) і в навчальному процесі Української державної академії залізничного транспорту (акт реалізації від 10.02.2010 р.).

4. Обґрунтованість отриманих результатів заснована на коректному застосуванні основних положень теорії завадостійкого кодування, теорії кінцевих полей Галуа, теорії чисел, теорії цифрової обробки сигналів, теорії складності та теорії цифрових автоматів.

5. Достовірність отриманих результатів підтверджується збіжністю теоретичних результатів з експериментальними даними, що отримані шляхом математичного моделювання запропонованих методів згорткового кодування та декодування даних.

6. Результати дисертаційної роботи доцільно використовувати: при проведенні науково-дослідних робіт з розробки методів і засобів підвищення вірогідності переданих даних; при проведенні конструкторських робіт зі створення нових технічних програмних і програмно-апаратних засобів, що спрямовані на підвищення вірогідності переданих даних; при вивченні навчальних дисциплін з завадостійкого кодування й передачі даних в телекомунікаційних системах.

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Приходько С.И. Фурье-преобразование сверточных кодов / С.И. Приходько, Н.А. Штомпель // Інформаційно-керуючі системи на залізничному транспорті – 2008. - №4. – С. 66 - 68.

2. Штомпель М.А. Метод алгебраїчного декодування згорткових кодів у частотній області / М.А. Штомпель // Зб. наук. праць. – Харків: УкрДАЗТ, 2008. – Вип. 98. – С. 104 - 111.

3. Приходько С.И. Метод блокового частотного декодирования сверточных кодов / С.И. Приходько, Н.А. Штомпель, А.В. Бушримас // Системи обробки інформації. – 2008. – Вип. 7 (74). – С. 109 – 111.

4. Приходько С.И. Метод сверточного кодирования на основе быстрых алгоритмов / С.И. Приходько, Н.А. Штомпель // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2009. – Вып. 159. – С. 283 - 287.

5. Штомпель М.А. Згорткове кодування з використанням ШПФ Винограда / М.А. Штомпель // Зб. наук. праць УкрДАЗТ. – Харків: УкрДАЗТ, 2010. – Вип. 114. – С. 46-49.

6. Приходько С.И. Метод частотного декодирования сверточных кодов / С.И. Приходько, Н.А. Штомпель, В.В. Босько // П'ята наукова конференція Харківського університету Повітряних Сил імені Івана Кожедуба "Новітні технології – для захисту повітряного простору", 15-16 квітня 2009 року: тези доповідей. – Х.: ХУПС ім. І. Кожедуба, 2009. – С. 113.

7. Приходько С.И. Метод алгебраического декодирования сверточных кодов в частотной области / С.И. Приходько, Н.А. Штомпель // Проблеми інформатики та моделювання. Матеріали дев'ятої міжнародної науково-технічної конференції. – Х.: НТУ "ХПІ", 2009. – С. 48.

8. Штомпель М.А Кодування згорткових кодів з використанням ШПФ Винограда / М.А. Штомпель // Шоста наукова конференція Харківського університету Повітряних Сил імені Івана Кожедуба "Новітні технології – для захисту повітряного простору", 14-15 квітня 2010 року: тези доповідей. – Х.: ХУПС ім. І. Кожедуба, 2010. – С. 222-223.

АНОТАЦІЯ

Штомпель М.А. Методи згорткового кодування та декодування даних на основі алгоритму швидкого перетворення Фур'є. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – Телекомунікаційні системи та мережі. – Українська державна академія залізничного транспорту, Харків, 2010.

Дисертаційна робота присвячена розробці методів згорткового кодування й декодування даних зі зменшеною обчислювальною складністю на основі алгоритму швидкого перетворення Фур'є для підвищення швидкості обробки даних в кодері й декодері. Дані методи засновані на запропонованому методі алгебраїчного представлення згорткових кодів у вигляді недвійкових блокових циклічних кодів у частотній області, що описує інформаційну, узагальнену породжуючу та кодову послідовності згорткового коду за допомогою їх Фур'є-образів. Розроблені методи частотного згорткового кодування та декодування даних дозволяють знизити відповідно обчислювальну складність кодеру та декодеру при використанні згорткових кодів з великою довжиною кодового обмеження. Розроблені програмна та програмно-апаратна реалізації запропонованих методів згорткового кодування та декодування даних.

Ключові слова: згортковий код, блоковий код, декодування, згортка, перетворення Фур'є, швидкі алгоритми, обчислювальна складність.

АННОТАЦИЯ

Штомпель Н.А. Методы сверточного кодирования и декодирования данных на основе алгоритма быстрого преобразования Фурье. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.12.02 – Телекоммуникационные системы и сети. – Украинская государственная академия железнодорожного транспорта, Харьков, 2010.

Диссертационная работа посвящена разработке методов сверточного кодирования и декодирования данных с уменьшенной вычислительной сложностью на основе алгоритма быстрого преобразования Фурье для повышения скорости обработки данных в кодере и декодере.

Проведенный анализ показал, что в настоящее время известно несколько методов кодирования и декодирования данных, обеспечивающих работу вблизи пропускной способности канала связи, в частности, турбо- та турбоподобные коды. Данные методы имеют значительную вычислительную сложность, что ограничивает их практическое применение в высокоскоростных телекоммуникационных системах. Сверточные коды обеспечивают менее высокий энергетический выигрыш кодирования по сравнению с турбокодами, но они также широко применяются в различных системах передачи данных. Внедрение сверточных кодов с большой длиной кодового ограничения позволяет повысить достоверность переданных данных, но это связано со следующими трудностями: сложность построения «хороших» кодов и высокая вычислительная сложность методов кодирования, а особенно, декодирование данных. Такие проблемы как ограниченность пропускной способности каналов связи, возрастание потоков передаваемых данных, необходимость достоверной передачи данных, увеличение времени обработки данных в кодере и декодере (кодеке) требуют разработки методов сверточного кодирования и декодирования данных с уменьшенной вычислительной сложностью.

Из анализа характеристик сверточных кодов следует, что они имеют ряд преимуществ по сравнению с блоковыми кодами. С другой стороны, вычислительная сложность методов построения сверточных кодов с большой длиной кодового ограничения и процессов их кодирования и декодирования остаются достаточно высокими. Установленная связь между сверточными и блоковыми кодами позволяет применять известные результаты из теории блоковых кодов для их исследования. Однако классические методы представления сверточных кодов в виде блоковых кодов не учитывают их алгебраическую структуру, а это ограничивает практическое применение данных методов. Существует метод алгебраического представления сверточных кодов во временной области, устраняющий указанный недостаток. Однако, из теории блоковых кодов известно, что переход в частотную область с помощью преобразования Фурье позволяет уменьшить вычислительную сложность кодера и декодера за счет применения быстрых алгоритмов вычисления свертки и преобразования Фурье. В связи с этим разработан метод алгебраического представления сверточных кодов в виде недвоичных блоковых циклических кодов, отличающийся от известного описанием информационной, обобщенной порождающей и кодовой последовательностей сверточного кода в виде их Фурье-образов, что позволяет разработать новые методы сверточного кодирования и декодирования данных с меньшей вычислительной сложностью.

Анализ алгоритмов быстрого преобразования Фурье (БПФ) в конечных полях показал, что наименьшую вычислительную сложность с точки зрения количества операций умножения имеет алгоритм Винограда, поэтому его целесообразно использовать для уменьшения трудоемкости процессов сверточного кодирования и декодирования данных. Установлено, что сверточное кодирование данных во временной области соответствует задаче вычисления конечной линейной свертки. Вычислительная сложность кодирования описывается полиномиальным законом, который не является оптимальным с точки зрения минимизации количества арифметических операций. Для уменьшения вычислительной сложности кодирования в случае, когда длина полного кодового ограничения сверточного кода представляет собой произведение нескольких сомножителей, разработаны методы сверточного кодирования данных на основе алгоритма Агарвала-Кули вычисления свертки и алгоритма БПФ Винограда.

Проведенный анализ показал, что метод алгебраического декодирования сверточных кодов во временной области является перспективным, так как он требует фиксированного количества операций при заданной корректирующей способности и может использоваться для декодирования сверточных кодов с большой длиной кодового ограничения. При этом вычислительная сложность декодирования существенно возрастает при больших значениях длины кодового ограничения, что ограничивает область применения данного метода. В связи с этим усовершенствован существующий метод алгебраического декодирования сверточных кодов, отличающийся от известного представлением процесса декодирования в частотной области и применением алгоритма БПФ Винограда; предложенный метод декодирования уменьшает вычислительную сложность декодера за счет сокращения необходимого количества арифметических операций.

На основе предложенных методов сверточного кодирования и декодирования данных разработаны их программная и программно-аппаратная реализации.

Ключевые слова: сверточный код, блоковый код, декодирование, свертка, преобразование Фурье, быстрые алгоритмы, вычислительная сложность.

ABSTRACT

Shtompel N.A. Methods of convolutional coding and decoding data based on fast Fourier transform algorithm. – the Manuscript.

Thesis for the degree of candidate of technical sciences, specialty 05.12.02 - Telecommunication systems and networks. - Ukrainian State Academy of Railway Transport, Kharkov, 2010.

The thesis is devoted to developing methods for convolutional coding and decoding data with reduced computational complexity based on fast Fourier transform algorithm to improve the speed of data processing in the encoder and decoder. These methods are based on the method of algebraic representation convolutional codes in the form of non-binary block cyclic codes in the frequency

domain, describes the information, the synthesis and generating the code sequence of a convolutional code with their Fourier transforms. The methods of the frequency convolutional coding and decoding of data can reduce, respectively, the computational complexity of encoder and decoder using convolutional codes with long code restrictions. Developed software and hardware and software implementation of the proposed methods of convolutional coding and decoding data.

Keywords: convolutional code, block code, decoding, convolution, Fourier transform, fast algorithms, computational complexity.

Підписано до друку 09.08.2010 р.
Формат 60х84 1/16 Друк. різограф.
Папір офсетний. Обсяг 0,9 друк. арк. Наклад 100 прим.
Зам. № 353. Безкоштовно.

Видавництво УкрДАЗТ.
Свідоцтво про державну реєстрацію ДК № 2874 від 12.06.2007 р.
61050, м. Харків, пл. Фейєрбаха, 7
Друкарня УкрДАЗТу, 61050, м. Харків, пл. Фейєрбаха, 7