## *Лабораторна робота №6*
## ФОРМУВАННЯ КОНТРОЛЬНОЇ СУМИ ПАКЕТІВ ІНФОРМАЦІЇ

**Мета роботи:** навчитися складати програми для формування контрольної суми пакетів інформації з використанням циклічних кодів.

### Теоретичні відомості

Застосування контролю процесу передавання пакетів інформації

В перших системах та мережах зв'язку передавання інформації відбувалося з використання комутації каналів. Прикладом використання комутації каналів є телефонна мережа загального користування. Комутація каналів зв'язку користувачів здійснюється для передавання інформації в мережі, наприклад голосової. Ефективність функціонування систем та мереж зв'язку, які використовують цей метод передавання інформації є низькою, оскільки основною задачею, яка тут вирішується є лише встановлення з'єднання між кінцевими абонентами та передавання інформації при відношенні сигнал/шум не нижче деякого порогового значення. Для подолання цих недоліків було запропоновано метод пакетного передавання інформації. Цей метод передбачає розбиття одного інформаційного повідомлення на декілька окремих та їхнього передавання мережею зв'язку як самостійних повідомлень у формі пакетів інформації з контролем за їхньою доставкою.

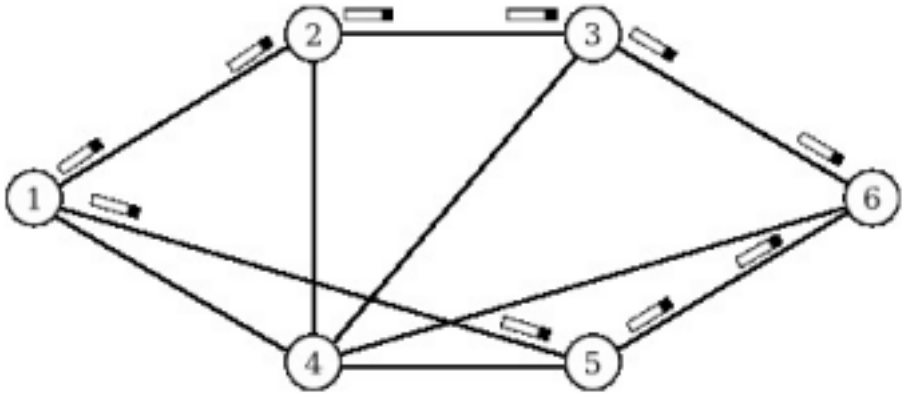


Рис. 6.1. Схема проходження пакетів інформації альтернативними маршрутами між вузлами мережі зв'язку

За рахунок такого розбиття повідомлення на пакети, можливості їхнього проходження будь-якою ділянкою мережі, що забезпечується маршрутизацією

та контролю за доставкою (встановлення сеансу, використання контролю цілісності пакетів), підвищується ефективність процесу передавання інформації каналами зв'язку. Це в свою чергу підвищує ефективність використання та функціонування самої мережі зв'язку.

Для забезпечення можливості передавання пакетів інформації мережею, їхня структура повинна бути такою:

• заголовок пакету — містить службову інформацію, яка використовується для забезпечення проходження пакету мережею (використовується для аналізу самого пакету — для чого він призначений та як його обробляти);

• блок даних — складова пакету з інформацією, яку необхідно передати;

• перевірочна частина пакету — складова пакету, що містить сформовані спеціальним чином перевірочні розряди для виявлення факту порушення цілісності пакету (наявності в ньому бітових помилок).

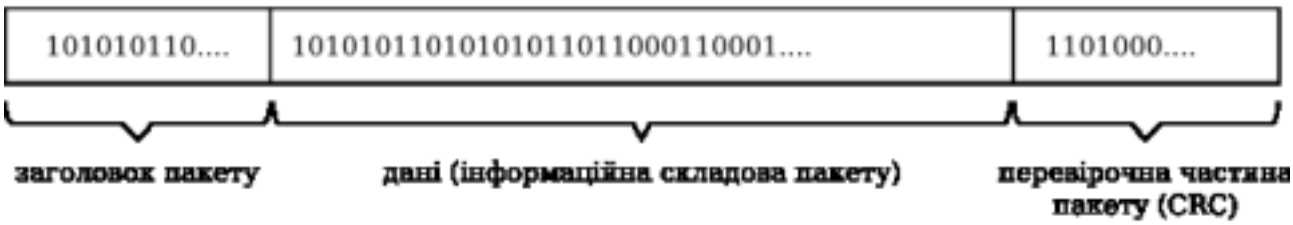


Рис. 6.2. Структура пакету інформації

Оскільки для перевірки цілісності пакетів в сучасних інформаційних системах використовуються циклічні коди її назвали циклічною перевіркою надлишковості — CRC (Cyclic redundancy check).

В процесі передавання інформації можуть виникати бітові помилки внаслідок дії завад та шумів і необхідно здійснювати контроль їхньої наявності. Надійне передавання пакетів інформації (без бітових помилок) можна реалізувати на основі кодів, що виявляють, або виправляють помилки. При цьому виникає необхідність узгодження методики забезпечення цього процесу між кінцевими пристроями мережі. Виправлення помилок в кодах є доволі складною задачею, що вимагає виконання декодером коду багатьох операцій. Тому, процес виправлення бітових помилок в прийнятих пакетах інформації залежить від складності та довжини використовуваного коду. В сучасних мережах зв'язку безпосереднє виправлення бітових помилок в пакетах інформації зазвичай виконується для кодових комбінацій малої довжини, наприклад 10÷20 біт. При великих довжинах виправлення помилок

здійснюється шляхом повторного передавання пакету.

Метод автоматичного запиту повторного передавання описує процес контролю та виправлення помилок в пакетах інформації, які виникають під час проходження пакетів мережею. Згідно цього методу для підтвердження правильності прийому пакетів інформації (без бітових помилок) використовується підтвердження, яке є спеціальним повідомленням про стан прийому інформації. В цьому повідомленні вказується про стан прийому пакету інформації — без помилок, або з помилками. Якщо передавач отримує позитивне підтвердження, передавання пакетів інформації продовжується, а в протилежному випадку здійснюється повторне передавання. Методи автоматичного запиту повторного передавання пакетів інформації поділяються на такі категорії:

• передавання з очікуванням — передавання наступного пакету інформації відбувається після позитивного підтвердження прийому одного пакету, в протилежному випадку відбувається повторне передавання пакету;

• передавання з поверненням — передавання наступної групи пакетів інформації відбувається після позитивного підтвердження прийому попередньої групи переданих пакетів, в протилежному випадку відбувається повторне передавання цієї групи пакетів;

• вибіркове передавання — повторне передавання відбувається лише для тих пакетів, для яких не було отримано позитивне підтвердження.

## Циклічні коди

Циклічні коди складають окремий клас завадостійких кодів, основною властивістю яких є те, що на основі однієї дозволеної кодової комбінації шляхом циклічного зсуву, можна отримати решту кодових комбінацій. Наприклад, якщо кодова комбінація $\mathbf{a_0, a_1, a_{n-1}}$ є дозволеною кодовою комбінацією, тоді кодова комбінація отримана шляхом циклічного зсуву $\mathbf{a_1, a_{n-1}, a_0}$ є також дозволеною. Циклічні коди забезпечують можливість виявлення та виправлення бітових помилок, а їхнє широке застосування пояснюється простою апаратною реалізацією кодерів та декодерів коду на основі регістрів циклічного зсуву. Для формування та дослідження властивостей циклічних кодів використовують поліномну форму представлення цих кодів. В такому вигляді можна виконувати всі необхідні операції для формування дозволених кодових комбінацій.

Формування циклічних кодів зводиться до виконання операції знаходженні

остачі від ділення двійкової інформаційної послідовності на породжуючий поліном. Ідея виявлення помилок циклічним кодом полягає в тому, що при повторному діленні прийнятої кодової комбінації на породжуючий поліном остача від ділення буде рівна нулеві, якщо бітові помилки відсутні. В протилежному випадку буде виявлено факт появи помилок.

Структура кодової комбінації циклічного коду у поліномній формі описується таким рівнянням:

$$F(x)=P(x)\cdot x^n+R(x) \qquad (6.1)$$

де P(x) - інформаційний поліном;
R(x) - остача від ділення від ділення $P(x)\cdot x^n$ на породжуючий поліном g(x).

Для формування циклічних кодів необхідно:

• записати інформаційну послідовність у вигляді інформаційного поліному, наприклад:

1 0 1 0 1 1

$$P(x)=1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x^1+1\cdot x^0=x^5+x^3+x^1+1$$

• помножити інформаційний поліном на $x^n$ (n - максимальна степінь породжуючого поліному), наприклад, якщо $g(x) = x^2 + x + 1$:

$$P(x)\cdot x^2=(x^5+x^3+x^1+1)\cdot x^2=x^7+x^5+x^3+x^2$$

операція множення поліному еквівалентна побітовому зсуву на n позицій;

• знайти остачу R(x) від ділення $P(x)\cdot x^n$ на породжуючий поліном g(x):

$$R(x)=mod(P(x),g(x))=x+1$$

на відміну від правил ділення чисел у десятковій формі, під час знаходження остачі від ділення R(x) необхідно використовувати двійкову арифметику;

• дописати остачу від ділення R(x) до поліному $P(x)\cdot x^n$ , що дасть шукану кодову комбінацію:

$$P(x)\cdot x^2+R(x)=x^7+x^5+x^3+x^2+x+1$$

1 0 1 0 1 1 1 1

Визначення поля CRC відбувається на основі інформаційної складової пакету за правилами формування циклічних кодів.

## Порядок роботи

1. Запустити середовище розробки програм на мові C/C++ (BorlandC, GCC, MinGW, Dev-C++, Visual Studio, тощо).
2. Вибрати із залікової книжки дві останні цифри **m** (передостання) та **n** (остання).
3. Сформувати згідно варіанту (табл. 6.1) двійкову послідовність (кодову комбінацію циклічного коду), яка містить розраховану за допомогою програми перевірочну частину - CRC.

*Таблиця 6.1*

**Варіанти завдань**

| Варіант mod(mn, 20) | Інформаційна послідовність P(x) у шістнадцятковій формі (12 біт) | Породжуючий поліном g(x) |
|---|---|---|
| 0 | BDF | $1+x+x^4$ |
| 1 | 8C4 | $1+x^3+x^4$ |
| 2 | 81B | $1+x+x^4$ |
| 3 | 95D | $1+x^3+x^4$ |
| 4 | A0B | $1+x+x^4$ |
| 5 | 88B | $1+x^3+x^4$ |
| 6 | FCC | $1+x+x^4$ |
| 7 | EFE | $1+x^3+x^4$ |
| 8 | 950 | $1+x+x^4$ |
| 9 | D41 | $1+x^3+x^4$ |
| 10 | CAC | $1+x+x^4$ |
| 11 | A79 | $1+x^3+x^4$ |
| 12 | C70 | $1+x+x^4$ |
| 13 | E58 | $1+x^3+x^4$ |
| 14 | AA5 | $1+x+x^4$ |
| 15 | B25 | $1+x^3+x^4$ |
| 16 | A97 | $1+x+x^4$ |
| 17 | 99F | $1+x^3+x^4$ |
| 18 | E19 | $1+x+x^4$ |
| 19 | EE0 | $1+x^3+x^4$ |

## Контрольні запитання

1. Якою  є структура пакету інформації?
2. Для чого призначений заголовок пакету?
3. Для чого використовується перевірочна частина пакету?
4. Яким чином формується перевірочна частина пакету?
5. Що таке циклічний код?
6. Які властивості має циклічний код?
7. Яким чином формується кодова комбінація циклічного коду?
8. Що таке породжуючий поліном?
9. Які властивості породжуючого поліному?
10. Як відбувається ділення поліномів?

## Зміст звіту

1. Титульний лист
2. Тема та мета роботи
3. Короткі теоретичні відомості
4. **Результати виконаної роботи**
5. **Висновок**

## ЛІТЕРАТУРА


1. Березин Б.И., Березин С.Б. Программирование на C и C++ - М.: ДИАЛОГ-МИФИ, 2001. - 288 с.
2. Блейхут Р. Теория и практика кодов, контролирующих ошибки. Пер. с англ. М.: Мир, 1986, 576 с.
3. Бояринов И.М. Помехоустойчивое кодирование числовой информации – М. Наука, 1983, 196 с.
4. Витерби А.Д., Омура Д.К. Принципы цифровой связи и кодирования – М. Ридио и связь, 1982, 536 с.
5. Керниган Б., Ритчи Д.. Язык программирования C, 2-е издание - М.: Вильямс — 2009. - 292 с.
6. Лафоре Л. Объектно-ориентирование программирование в C++, 4-е издание — М.: Питер, 2004. - 923 с.
7. Папас К., Мюррей У. Программирование на C и C++ - К.: Издательская група BHV, 2000. - 320 с.
8. Скляр Б. Цифровая связь. Теоретические основы и практическое применение.2-е изд. : Пер. с англ. - М. Издательский дом “Вильямс”, 2004. - 1104 с.
9. Шилдт Г. Справочник программиста C/C++, 3-е изд.: Пер. с англ. - М. Издательский дом “Вильямс”, 2003. - 432 с.
10. Цымбал В.П. Теория информации и кодирование: 4-е изд., перераб. и доп. - К. : Вища шк., 1992, 263 с.: ил.