Lec\_8

ПОЛІНОМІАЛЬНЕ КОДУВАННЯ ІНФОРМАЦІЇ. ЦИКЛІЧНІ КОДИ

Зручним і наочним способом задання лінійних блокових *(****n****,****k****)-*кодівє подання символів кодових слів***f0, f1.,fn-****1* у вигляді коефіцієнтів многочлена від ***х***, тобто

***F(x) = f0+ f1x + f2x2+ … + fn-1xn-1***. (3.11)

Подання кодових слів у такій формі дозволяє звести дії над комбінаціями символів до дій над поліномами.

Прикладом запису двійкової послідовності 1000101 у вигляді багаточлена є

*F*(*x*)=1⋅ *x*6 +0⋅*x*5 +0⋅ *x*4 +0⋅ *x*3 +1⋅*x*2 +0⋅ *x* +1= *x*6 + *x*2 +1.

Далі, при викладенні матеріалу під багаточленом *A*(х)*x* = *xk*−1 + *xk*−2 +...+1 *x0* слід розуміти двійкову послідовність інформаційних символів, яка підлягає кодуванню ЦК, а *F*(*x*)= *xn*−1 + *xn*−2 +...1 *x0* – є КК в поліномінальній формі ЦК.

12.1 Операції над поліномами в полі двійкових символів GF(2)

*Сумою* двох поліномів ***f*(*x)*** і ***g*(*x*)** в полі двійкових символів ***GF*(2)** називається поліном з ***GF*(2)**, такий, що

, (3.12)

тобто додаванню двох поліномів з ***GF*(2)** відповідає операція додавання за ***mod 2*** коефіцієнтів при однакових степенях ***х***.

Наприклад:

***x3 + x2 + 0∙x + 1***

**+ *x2 + x + 1***

***x3 + 0∙x2 + x + 0 = x3+x***.

*Добутком* двох поліномів ***f*(*x*)** і ***g*(*x*)** в полі двійкових символів ***GF*(2)** називається поліном з ***GF*(2)**, такий, що

, (3.13)

тобто добуток поліномів знаходиться за звичайним правилом множення степеневих функцій, причому коефіцієнти при одному степені ***х*** додаються за ***mod 2***.

Наприклад:

***x3 + x2 + 0∙x + 1***

**× *x2 + x\_\_\_\_\_\_\_ \_***

***x4 + x3 +0⋅x2 + x***

**+ *x5 + x4+ 0⋅x3 + x2***\_\_\_

***x5 +0⋅x4 + x3 + x2 + x = x5 + x3 + x2 + x***.

*Ділення* поліномів здійснюється за правилами ділення степеневих функцій, причому операція віднімання замінюється додаванням за ***mod 2*** (додавання і віднімання за ***mod 2*** збігаються).

***Теорема.*** *Для кожної пари поліномів* ***c(x)*** *і* ***d(x)*** *(****d(x)≠****0) існує єдина пара поліномів, де* ***q(x)*** *– частка,* ***ρ(x)*** *- остача від ділення, таких, що*

***c(x)= q(x)⋅d(x) + ρ(x)***, (3.14)

Наприклад:

***x4 +0⋅x3 + x2 + x + 1 x + 1***

**+ *x4 + x3\_x3 + x2 + 1***

***x3 + x2 + x + 1***

**+ *x3 + x2\_\_\_\_\_\_\_***

***x + 1***

**+*x + 1***

***0*** *– остача* ***ρ(x)***.

12.2 Поліноміальні коди

**Визначення.*****Поліноміальним*** *кодом називається множина всіх многочленів степеня не більше* ***n-1****, що мають спільний множник – деякий фіксований многочлен* ***g(x)*** *степеня* ***r=n-k*** *(де* ***n*** *- довжина кодових слів,* ***k*** *- довжина інформаційного повідомлення;* ***r*** *- кількість перевірних символів). Цей многочлен* ***g(x)*** *називається* ***твірним многочленом******коду****.*

Поліноміальний код з твірним многочленом ***g(x)*** кодує повідомлення ***m(x)*** поліномом вигляду

***F(x)=А(x)⋅g(x)=f0 + f1x + f2x2  + … + fn-1xn-1***, (3.15)

або кодовим словом з коефіцієнтів цього многочлена***f=*(*f0, f1, …, fn-1*)**.

Матриця поліноміального коду з твірним многочленом ***g(x)*** степеня ***r=n-k*** має вигляд

, (3.16)

де ненульові елементи в ***i***-му рядку - це послідовність коефіцієнтів твірного многочлена, розташованих з ***j***-го по **(*j+r*)**-й стовпець.

**Приклад 1** Поліноміальний код заданий твірним многочленом вигляду ***g(x)=*1 + *x*2 + *x*3**. Закодуємо за його допомогою повідомлення **(01011)**.

Повідомленню (**01011**) відповідає многочлен

***A(x)=* 0⋅*x0*+1⋅*x+*0⋅*x2*+1⋅*x3+* 1⋅*x4 = x +* *x3 + x4***

Тоді кодовим словом буде поліном

***F(x)= A(x)⋅g(x) =* (*x + x3 + + x4*)*⋅*(1 *+ x2 + x3*) *= x + x3 + x4 + x3 + +x5+ x6 +x4+x6+x7=x+*(1+1)⋅*x3+*(1+1)⋅*x3+x5+*(1+1)⋅*x6+x7= x + x5+ x7***.

Цьому поліному відповідає кодова послідовність ***F*= (01000101)**.

Інші способи задання поліноміального (5, 8)- коду з твірним поліномом ***g(x)=1+x2+x3*** – це його подання за допомогою твірної матриці



або відображення

**00000 *→* 00000000**,

**00001 *→* 00001011**,

**00010 *→* 00010110**,

**01011***→* **01000101**.

***Теорема.*** *Вектор помилок* ***e=e0, …, en-****1 залишиться не визначеним у тому і лише у тому випадку, якщо його многочлен* ***e(x)=e0+e1x+…+en-1xn-1*** *ділиться на твірний поліном коду* ***g(x)*** *без остачі.*

***Доведення.***Прийнята послідовність***c(x)=A(x)g(x)+e(x)***ділиться на***g(x*)** без остачі тоді і тільки тоді, коли***e(x)***ділиться на***g(x)***без остачі.

Тому будь-яка помилка, многочлен якої не ділиться на***g(x)***,буде знайденою, відповідно будь-яка помилка, многочлен якої ділиться на***g(x)***,знайденою не буде.Отже, виявлення помилки поліноміальним кодом з твірним поліномом ***g(x)*** може бути здійснене за допомогою ділення многочленів: *якщо залишок від ділення многочлена прийнятої послідовності на твірний поліном* ***g(x)*** *ненульовий, то при передачі відбулося спотворення даних.*

***Теорема.*** *Якщо твірний поліном* ***g(x)*** *не є дільником жодного з многочленів вигляду* ***xj+*1***, де* ***j<n****, то мінімальна відстань між кодовими словами відповідного поліноміального коду* ***dmin ≥ 3***.

***Доведення.*** Припустимо ***dmin=*2**. Тоді існує многочлен ***A*(*x*)**, такий, що ***A*(*x*)*⋅g(x)=F*(*x*)** і степінь ***F*(*x*)*≤ n***. Мінімальна вага Хеммінга (мінімальна кодова відстань ***dmin***) ***w*(*F*)=2**, тому ***F(x)=xm+xl***, де ***l<m<n*** Отже, кодовий многочлен можна подати у вигляді ***F(x)=xl*(***xm-l+*1). Тоді двочлен **(*xm-l+*1)** повинен ділитися на ***g*(*x*)**, що унеможливлює умову теореми. Якщо припустити, що ***dmin*=1**, то це приведе до твердження, що ***xm*** повинне ділитися на ***g*(*x*)**, що також суперечить умові.

12.3 Циклічні коди

Серед поліноміальних кодів найпоширеніші ***циклічні коди***.

**Визначення.** *Лінійний блоковий* ***(k****,****n)*** *- код називається* ***циклічним****, якщо в результаті циклічного зсуву кодового слова виходить інше кодове слово даного коду.* Іншими словами*, якщо* ***F=(f0, f1, …, fn-1)*** *–* ***кодове слово****, то і* ***v=(fn-1, f0, f1, …, fn-2)****, отримане циклічним зсувом елементів* ***fi****, - кодове слово.*

Наведемо ***властивості циклічних кодів***.

1. *Для циклічного* ***(k****,****n)****- коду кожний ненульовий поліном повинен мати степінь принаймні* ***(n-k)****, але не більше* ***n-1***;
2. *Існує тільки один кодовий поліном* ***g(x)=*1*+ g1x +g2x2 +  … + +gn-k-1⋅xn-k- + xn-k*** *степеня* ***(n-k)****, що є дільником кожного* ***кодового полінома******F(x)=A(x)⋅g(x)****, цей поліном називається* ***твірним поліномом коду***.

***Теорема 3***. Циклічний код степеня *n* = 2*r* −1, де *r*>1 – ціле додатнє число, задається породжуючим багаточленом *G*(*x*) степеня *s*<*r* тоді і тільки тоді, коли він ділить двочлен *xn* +1 без остачі.

Припустимо, треба закодувати деяку послідовність ***A=(a0***, ***a1***, ***a2***, ***…***, ***ak-1)***. Відповідний їй поліном матиме вигляд

***A(x)=a0+a1x+a2x2+ … +ak-1xk-1***. (3.17)

Помножимо ***A(x)*** на ***xn-k***, що рівнозначно зсуву двійкової послідовності ***A=(a0, a1, a2, …, ak-1)*** на ***n-k*** розрядів праворуч. У результаті отримаємо поліном степеня ***n-*1** або меншого

***xn-k⋅A(x)=a0xn-k+a1xn-k+1+ … +ak-1xn-1***. (3.18)

Скориставшись теоремою ділення поліномів (3.14), можна записати

***xn-k⋅A(x)=q(x)⋅g(x) + ρ(x)***, (3.19)

де ***q(x)*** і ***ρ(x)*** - частка і остача від ділення полінома ***xn-k*⋅*A(x)*** на твірний поліном ***g(x)***.

Оскільки степінь твірного полінома ***g(x)* *r*=(*n-k*),** то степінь остачі ***ρ*(*x*)** не більше**(*n-k-1*)**, тобто

***ρ(x)=ρ0+ ρ1x+ ρ2x2+…+ ρn-k-1xn-k-1***. (3.20)

Використовуючи правила арифметики з ***GF*(2)**, вираз (3.19) можна записати так:

***ρ(x) + xn-k*⋅*A(x) = q(x)⋅g(x)***. (3.21)

Звідси випливає, що поліном ***ρ(x)+xn-k*⋅*A(x)*** кратний ***g*(*x*)** і має степінь не більше ***n***-**1**.

Отже, поліном ***ρ(x)+xn-k⋅A(x)*** є кодовим поліномом, що відповідає многочлену інформаційної послідовності ***A*(*x*)**.

Розкривши вираз (3.21), отримуємо

***ρ(x)+A(x)xn-k=ρ0+ρ1x+ρ2x2+…+ρn-k-1xn-k-1+a0xn-k+a1xn-k+1 +…+ ak-1xn-1***, (3.22)

що відповідатимемо кодовому слову

***F=***(***ρ0***, ***ρ1***, …, ***ρn-k-1***, ***a0***, ***a1***, ***a2***, …, ***ak-1***),

де ***ρ0***, ***ρ1***, …, ***ρn-k-1*** – перевірні символи; ***a0*, *a1*, *a2*, …, *ak-1* -** інформаційні символи.

Відтак, кодове слово циклічного коду складається з перевірної частини з **(*n-k*)** перевірних символів і інформаційної частини ***m*** завдовжки ***k*** символів. Перевірні символи є коефіцієнтами полінома ***ρ(x)*** – остачі від ділення кодового слова ***u(x)=m(x)*⋅*xn-k*** на твірний поліном ***g(x)***.

**Приклад 2** Закодуємо послідовність ***A=*(0111)** циклічним кодом, заданим твірним поліномом ***g(x)=1+x+x3***.

Вектору ***A*=(0111)** відповідає поліном ***A***(***x***)=***x***+***x***2+***x***3.

Помножимо ***A***(***x***) на ***xn-k=x3***, де ***n-k*** – кількість перевірочних символів: ***A(x) xn-k = A(x)⋅x3=***(***x+x2+x3***) ***x3=x4+x5+x6***, або виконаємо зсув елементів інформаційної послідовності ***A(x)*** на ***r*=3** розряди праворуч: (**0111**)→ (**0000111**).

Розділимо добуток ***A(x)xn-k*** на твірний поліном коду ***g(x)***:

***x6 + x5 + x4 x3+x+1***

**+ *x6 + x4 + x3  x3+x2***

***x5 + x3***

**+ *x5 + x3 + x2***

***x2= ρ(x)***.

Многочлен остачі від ділення має степінь ***n-k-*1** і такий вигляд:

***ρ(x)***= **0**∙***x0+*0**∙***x1+*1⋅*x2***.

Отже, кодовий поліном заданої інформаційної послідовності:

***F(x)=ρ(x) + xn-k*⋅*A(x)=x2****+* ***x4+ x5+ x6***=**0∙*x0 +*0**∙***x1 +*1⋅*x2+*0*∙x3++*1⋅*x4+*1⋅*x5+*1⋅*x6***,

що відповідає кодовому слову ***A***=(**0010111**), де перші три символи перевірні.

Таким чином, *алгоритм побудови циклічного (****k****,****n****)- коду для послідовності* ***A=(a0, a1, a2, … , ak-1)***такий:

*1) многочлен інформаційної послідовності* ***A(x)*** *множиться на* ***xn-k****, тобто зсувається праворуч на* ***n-k*** *розрядів*;

*2) отриманий у такий спосіб поліном ділиться на твірний поліном коду* ***g(x)****;*

*3) остача від ділення* ***xn-k⋅A(x)*** *на* ***g(x)*** *додається до* ***xn-k⋅A(x)****, тобто записується в молодших* ***n-k*** *розрядах.*

Ще однією важливою властивістю циклічного (***k***, ***n***)- коду є те, що твірний поліном ***g(x)*** ділить без остачі двочлен ***xn*+1**, тобто комбінації лінійного коду мають властивість циклічності при виконанні умови

***xn+1=g(x)*⋅*h(x)***. (3.23)

Кожний такий двочлен ***xn*+1** може бути розкладений на декілька *незвідних поліномів* – таких поліномів, які не можуть бути подані як добуток многочленів меншого степеня, тобто вони діляться або самі на себе, або на 1.

Як твірні поліноми різних циклічних кодів використовуються незвідні поліноми і їх добутки, оскільки вони є дільниками двочлена ***xn*+1**. Деякі з твірних поліномів наведені у *табл. 3.4*.

*Таблиця 3.4*

|  |  |
| --- | --- |
| ***Твірний поліном g(x)*** | ***Двійковий запис полінома*** |
| **1*+x*** | **11** |
| **1*+x+x2*** | **111** |
| **1*+x+x3*** | **1101** |
| **1*+x2+x3*** | **1011** |
| **1*+x+x4*** | **11001** |
| **1*+x3+x4*** | **10011** |
| **1*+x+x2+x4*** | **11101** |
| **1*+x2+x3+x4*** | **10111** |
| **1*+x+x2+x3+x4*** | **11111** |

*Продовження табл.3.4*

|  |  |
| --- | --- |
| ***Твірний поліном g(x)*** | ***Двійковий запис полінома*** |
| **1+*x2+x5*** | **101001** |
| **1*+x3+x5*** | **100101** |
| **1*+x+x2+x3+x5*** | **111101** |
| **1*+x+x2+x4+x5*** | **111011** |
| **1*+x4+x5+x6*** | **1000111** |
| **1*+x+x2+x5+x6+x7+x8*** | **111001111** |
| **1*+x3+x5+x9*** | **1001010001** |
| **1*+x+x5+x6+x10+x11*** | **110100100011** |
| **1*+x+x2+x3+x5+x7+x8+x11*** | **111101011001** |
| **1*+x3+x4+x6+x8+x9+x10+x11*** | **100110101111** |
| **1*+x+x2+x3+x4+x12+x13+x14+x15*** | **1111100000001111** |
| **1*+x5+x12+x16*** | **10000100000010001** |

**Визначення*.*** *Поліном* ***h(x)*** *степеня* ***k****, що є часткою від ділення двочлена* ***xn+1*** *на твірний поліном коду* ***g(x)****, називається* ***перевірним поліномом.*** Оскільки ***h(x)*** однозначно зв'язаний з ***g(x)***, то він також визначає код.

Спираючись на вищевикладене, можна дати інше визначення двійкового ***циклічного коду.***

**Визначення*.*** ***Циклічним*** *називається* ***лінійний (k, n)****- код, усі* ***2k*** *кодові комбінації якого подані поліномами степеня* ***n-1*** *і менше, які діляться без остачі на деякий поліном* ***g(x)*** *степеня* ***r=n-k****,**що є дільником двочлена* ***xn+1****.*

12.4 Синдром і виправлення помилок у циклічних кодах

Позначимо через ***F(x)*** та ***у(x)*** поліноми, що відповідають переданому кодовому слову ***F*** і прийнятій послідовності ***у***.

Розділивши поліном прийнятого повідомлення ***у(x)*** на твірний поліном коду ***g(x)***, отримаємо поліноми частки від ділення ***q(x)*** і остачі ***s(x),*** тобто многочлен прийнятого вектора ***у*(*x*)** можна записати так:

***y(x)=q(x)g(x)+s(x)***. (3.24)

*Якщо* ***у(x)*** *є кодовим поліномом, то він ділиться на* ***g(x)*** *без остачі, тобто* ***s(x)=*0**.

Ненульова остача***s(x)≠*0**від ділення полінома прийнятого вектора***у(x)***на твірний поліном коду***g(x*)** є ознакою наявності помилки у прийнятій послідовності, тобто ***кодовим синдромом***.

Поліном синдрому ***s(x)*** має вигляд

***s(x)=s0+s1x+…+sn-k-1xn-k-1***. (3.25)

Покажемо, що многочлен синдрому однозначно зв'язаний з многочленом помилок ***e(x)*** і, отже, за допомогою полінома синдрому можна не тільки виявляти, але й виправляти помилки у прийнятих послідовностях.

Нехай ***e(x)=e0+e1x+…+en-1xn-1*** - многочлен вектора помилок. Тоді поліном прийнятої послідовності

***y(x)=F(x)+e(x)***. (3.26)

Додавши до лівої і правої частин виразу (3.26) кодовий поліном ***u*(*x*)**, отримаємо

***F(x)+y(x)=e(x)***. (3.27)

З урахуванням того, що

***y(x)=q(x)⋅g(x) + s(x)***,

***F(x)=A(x)⋅g(x)***,

вираз (3.27) запишемо так:

***e(x)=*[*A(x)+q(x)*]⋅*g(x)+s(x)=t(x)⋅g(x)+s(x)***, (3.28)

тобто поліном синдрому ***s(x)*** – це остача від ділення многочлена помилки ***e(x)*** на твірний поліном коду ***g(x)***.Звідси випливає, що, *знайшовши поліном синдрому, можна однозначно визначити вектор помилок, і отже, виправити помилку.*

12.5 Твірна і перевірна матриці циклічного коду

Подамо кодове слово циклічного **(*n*, *k*)**- коду таким чином:

***F(x)= ρ(x) + xn-k*⋅*A(x)***, (3.29)

де ***ρ(x)*** – остача від ділення многочлена ***xn-k⋅A*(*x*)** на твірний поліном коду ***g(x)***.

*Твірна матриця* циклічного коду складається з двох частин: *перевірної підматриці* ***Pk×(n-k)*** розмірністю ***k×(n-k)***, щовизначається поліномами остачі ***ρ(x)*** від ділення кодового многочлена ***xn-k⋅A(x)*** на твірний поліном коду ***g*(*x*)** та *одиничної підматриці* ***Ik×k*** розмірністю ***k×k***, що відповідає інформаційній частині кодової послідовності.

*Для побудови* ***твірної матриці*** *циклічного коду беруться тільки ті з комбінацій інформаційних послідовностей* ***ai*(*x*)**, *де* ***i*=1** **.. *k***, *що мають одиницю тільки в одному розряді. Ці комбінації помножують на* ***xn-k*** *і знаходять остачі* *від їх ділення на твірний поліном коду*

, (3.30)

*їм відповідні* ***(n-k-1)****- послідовності**будуть рядками перевірної частини* ***Pk×(n-k)*** *твірної матриці коду*.

***Твірна матриця*** *циклічного коду складається з* ***k*** *лінійно незалежних кодових комбінацій, решта* ***2k-k-1*** *кодових комбінацій, окрім нульової, знаходиться порозрядним додаванням за* ***mod 2*** *усіх пар кодових слів, що утворюють твірну матрицю* *коду*.

**Приклад**  Для циклічного (7, 4)- коду, заданого твірним поліномом ***g(x)=*1*+x2+x3***, побудувати твірну матрицю.

Запишемо чотириелементні одиничні комбінації інформаційних повідомлень ***аi*(*x*)**: **(1000)*→ a1(x)=*1**;**(0100)*→ a2(x)= x***;**(0010)*→ a3(x)= x2***;**(0001)*→ a4(x)= x3***.

Помножимо кожну з них на ***x3*** (кількість перевірних символів ***r=n-k=***7-4***=***3) і розділимо на твірний поліном коду ***g(x)= x3+x2+*1**.

Поліноми остач від ділення ***ρ*(*x*)** мають степінь ***n*-*k*-1**=***2***, на одиницю менший за степінь дільника, і будуть такими:

|  |  |
| --- | --- |
| 1) ***1*⋅*x3  x3+x2+1***  **+ *x3+x2+1 1***  ***x2+1****,*  ***ρ1(x)= 1 + x2 →* (101)**; | 2) ***x∙x3  x3+x2+1***  **+ *x4 + x3 + xx+1***  ***x3 + x***  ***+ x3 + x2 + 1***  ***x2 + x +1***,  ***ρ2(x)= 1+ x + x2→* (111)**; |
| 3) ***x2∙x3 x3+x2+1***  **+ *x5 + x4 + x2  x2+x+1***  ***x4 + x2***  **+ *x4 + x3 + x***  ***x3 + x2 + x***  **+ *x3 + x2 + 1\_\_\_***  ***x + 1***,  ***ρ3(x)= 1+ x →*(110)**; | 4) ***x3∙x3 x3+x2+1***  **+ *x6 + x5 + x3 x3+x2+x***  ***x5 + x3***  **+ *x5 + x4 + x2***  ***x4 + x3 + x2***  **+ *x4 + x3 + x\_\_\_***  ***x2 + x***,  ***ρ4(x)= x + x2 →* (011)**. |

Твірна матриця матиме вигляд

.

 

Відповідно перевірна матриця матиме вигляд

.

 

З перевірної матриці випливає система перевірних рівнянь коду



Кодові слова даного циклічного (7,4)-коду утворюються так:

***F***= (***ρ0***, ***ρ1***, ***ρ2***, ***a0***, ***a1***, ***a2***, ***a3***).

12.6 Способи декодування циклічного коду

Для виправлення помилок циклічним кодом використовують умову, що кількість різних ненульових поліномів синдрому – остач від ділення многочлена прийнятої послідовності на твірний поліном коду – дорівнює кількості елементів ***n*** кодової послідовності, якщо кратність помилки, що виправляється, ***l*=1** або числу сполук з ***n*** по ***l***. Наприклад, при ***n***=15 та ***l***=2 необхідно =105 ненульових остач для однозначного виправлення двох помилок в коді довжини ***n***. Для цього необхідно вибрати поліном ***g*(*x*)** степеня ***r=***7, оскільки ***27***>105, де ***r***=7 – кількість перевірних елементів, ***k=n-r*=**8 – довжина інформаційної послідовності.

Розглянемо способи виправлення поодиноких помилок циклічним кодом (багатократні помилки виправляються так само).

***1-й спосіб*** декодування циклічного коду ґрунтується на побудові гіпотез про наявність помилки у певному розряді кодової комбінації. Цей спосіб декодування такий:

1. *будуємо гіпотезу про наявність помилки у 1-му біті прийнятої комбінації* ***у(x),*** *тобто припускаємо, що вектор помилок* ***(e1=*10 … 00*)****. Знаходимо порозрядну суму* ***у(x)+e(x)*** *і ділимо її на твірний поліном* ***g(x)****: якщо остача від ділення (поліном синдрому)* ***s(x)=0****, то гіпотеза підтверджується, інакше відхиляється*;
2. *будуємо гіпотезу про помилку у 2-му розряді, тобто припускаємо, що* ***e2=*(01 … 00)**. *Знаходимо суму* ***у(x)+e(x)*** *і ділимо на* ***g(x)*** – *у результаті* *підтверджуємо або спростовуємо цю гіпотезу: якщо остача* ***s(x)≠*0***, то гіпотеза відкидається, інакше – приймається і т. д. до того часу, поки не отримаємо остачу* ***s(x)=*0**, *тобто підтвердження гіпотези. Нульовий поліном синдрому* ***s(x)=0*** *свідчить про те, що помилки немає*. *Сума многочленів прийнятої кодованої послідовності і вектора помилок, що відповідає нульовій остачі* ***s(x)=0****, визначає передане кодове слово так:* ***F(x)= y(x) + ei(x)***.

***2-й спосіб*** декодування циклічного коду такий:

1. *визначається вага* ***w*** *вектора синдрому* ***s(x)*** *– остачі від ділення многочлена прийнятої послідовності* ***у(x)*** *на твірний поліном коду* ***g(x)****.* *Якщо* ***w ≤ l****, де* ***l*** *- кратність помилок, що виправляються кодом, то остача* ***s(x)*** *додається до**прийнятої комбінації* ***у(x)****, і у такий спосіб вона виправляється*;
2. *якщо* ***w > l****, то виконується циклічний зсув прийнятої кодової комбінації* ***у(x)*** *на один розряд праворуч, і отримана так комбінація знову ділиться на* ***g(x).*** *Якщо вага вектора остачі* ***s(x) w≤ l****, то циклічно зсунута комбінація додається з цією остачею, а потім циклічно зсовується на один розряд ліворуч (тобто повертається до попереднього положення). Отримана таким чином кодова комбінація вже не містить помилок*;
3. *якщо після першого циклічного зсуву і ділення на твірний поліном вага остачі залишається* ***w > l****, то так само виконується наступний циклічний зсув, ділення на* ***g(x),*** *визначення ваги остачі і т. д. Цей процес продовжується, поки вага остачі не стане* ***w ≤ l****. Кодова комбінація, отримана у результаті послідовного циклічного зсуву, для якої виконуватиметься умова* ***w ≤ l****, додається з остачею* ***s(x)*** *від ділення цієї комбінації на твірний поліном* ***g(x).*** *Після цього виконується циклічний зсув назад на стільки розрядів, на скільки був зсув щодо початкової прийнятої комбінації* ***у(x).*** *У результаті отримуємо виправлену кодову комбінацію* ***F(x).***

Зразки розв'язування задач до розділу 12

**Приклад 1**  Поліноміальний код заданий твірним многочленом ***g(x)=1+x4+x***5. Закодувати двійкові комбінації **1011**, **11001100**. Побудувати твірну матрицю для кожного з одержаних кодів.

***Розв'язання***

1) Закодуємо повідомлення **1011** довжиною ***k***=4 символи.

Цій послідовності відповідає многочлен степеня ***k-1*** ***A***(***x***)=**1*⋅x0+*0*⋅x1+*1*⋅x2+*1*⋅x3=*1*+x2+x3****.*

Поліноміальний код повідомлення утворюється множенням многочлена інформаційної послідовності на твірний поліном коду.

За умовою задачі використовується поліноміальний код з твірним многочленом 5-го степеня і кодується повідомлення, якому відповідає многочлен 3-го степеня. У результаті одержуємо кодовий поліном ***F***(***x***) степеня ***n-1*** – у даному випадку 8-го степеня, що визначає послідовність довжиною ***n=***9 бітів:

***F(x)=A(x)⋅g(x)= (1+x2+x3)⋅(1+x4+x5)= 1+ x2+ x3+ x4+ x5+ x6+ + (1+1)x7+ x8= 1+ x2+ x3+ x4+ x5+ x6+ x8***.

Отриманому многочлену

***F(x)= 1+x2+x3+x4+x5+x6+x8=*** **1**⋅***x****0*+**0**⋅***x****1****+*1**⋅***x****2*+**1**⋅***x3***+**1**⋅***x****4*+**1**⋅***x****5+***1**⋅***x****6*+**0**⋅***x****7+***1**⋅***x****8* відповідає вектор ***F=***(**101111101**), отже, задане інформаційне повідомлення кодується так: (**1011**) **→** (**101111101**).

Твірна матриця коду має розмірність (***n-k***)**×*n*** і таку структуру:

,

де через ***g0***, ***g1***, …, ***gn-k-1*** позначені коефіцієнти твірного многочлена коду.

У даному випадку маємо (*9*, *4*)- код, твірна матриця якого має вигляд

.

Закодуємо задане повідомлення за допомогою твірної матриці:

***F=A***×***G=*** (**1011**)× =(**101111101**).

Одержали кодову послідовність (**1011**) **→** (**101111101**).

2) Закодуємо повідомлення ***m=***(**11001100**).

Кількість інформаційних елементів у повідомленні ***k***=8.

Кількість перевірних елементів ***r=n-k*** визначається степенем твірного полінома коду – у даному випадку ***r***=5.

Довжина кодового слова ***n=k+r=***8+5=13.

Многочлен інформаційного повідомлення ***A=*** (**11001100**) такий: ***A(x)=*** ***1⋅x0+1⋅x1+0⋅x2+0⋅x3+1⋅x4+1⋅x5+0⋅x6+0⋅x7=1+x+x4+x5****.*

Його кодовий поліном ***u(x)*** має степінь ***n-1=***12 і визначається так:

***F(x)=A(x)⋅g(x)=(1+x+x4+x5)( 1+x4+x5)= 1+x+x5+x6+x8+x10***.

Отриманий многочлен ***F(x)=*1**⋅***x****0*+**1**⋅***x****1****+*0**⋅***x****2*+**0**⋅***x3***+**0**⋅***x****4*+**1**⋅***x****5+***1**⋅***x****6*+ +**0**⋅***x****7+***1**⋅***x****8*+**0**⋅***x9***+**1***⋅****x****10* +**0**⋅***x****11+***0**⋅***x****12* визначає кодове слово ***f=***(**1100011010100**).

Отже, задане інформаційне повідомлення кодується так:

(**11001100**)**→**(**1100011010100**).

Твірна матриця даного (*13*, *8*)- коду має вигляд

.

***Відповідь:*** (**1011**)**→** (**101111101**); (**11001100**)**→→**(**1100011010100**).

**Приклад 2** Циклічний (*7*, *4*)- код заданий твірним поліномом ***g(x)=1+x+x***3. Визначити синдром виправлення поодиноких помилок цим кодом. Побудувати перевірну й твірну матриці коду. Декодувати повідомлення (**1001110**).

***Розв'язання***

*Синдром* виправлення поодиноких помилок циклічним кодом визначається діленням многочлена вектора помилок на твірний поліном коду.

Припустимо, що кодується повідомлення ***A*** довжиною ***k*** символів – йому відповідає многочлен ***A***(***x***) степеня ***k*-*1***.

*Кодовим словом* на виході кодера буде послідовність ***f*** довжиною ***n*** символів, якій відповідає многочлен ***F***(***x***) степеня ***n-1***.

Позначимо через ***e***= (***e0***, ***e1***, …, ***en-1***) – вектор помилок в двійковому каналі зв'язку; ***s***=(***s0***, ***s1***, …, ***sn-k-1***) – кодовий синдром, що визначається вектором помилок.

Вектор помилок подається многочленом вигляду ***e(x)=e0+e1x+…+en-1xn-1***, а синдром – многочленом ***s(x)=s0+s1x+…+sn-k-1xn-k-1***.

Знайдемо значення синдрому виправлення поодиноких помилок заданим циклічним (*7*, *4*)- кодом:

1. ***е***=(***1000000***) **→** ***e***(***x***)=***1***,

***1 x****3 +****x****+****1***

***s(x)= 1*** →**(100)**;

1. ***е***=(***0100000***) → ***e***(***x***)=***x***,

***x x****3 +****x****+****1***

***s(x)= x*** →**(010)**;

1. ***е***=(***0010000***) → ***e***(***x***)=***x2***,

***x2 x****3 +****x****+****1***

***s(x)= x2*** →**(001)**;

1. ***e***=(***0001000***) → ***e***(***x***)=***x3***,

***x3 x****3 +****x****+****1***

***+ x****3 +* ***x****+* ***1 1***

***x + 1***

***s(x)= 1+ x*** →**(110)**;

1. ***e***=(***0000100***) → ***e***(***x***)=***x4***,

***x4 x****3 +****x****+****1***

***+ x****4 +****x2****+****x x***

***x2+ x***

***s(x)= x + x2*** →**(011)**;

1. ***e***=(***0000010***) → ***e***(***x***)=***x5***,

***x5 x****3 +****x****+****1***

***+ x****5* +***x3***+***x2 x2+1***

***x3+ x2***

***+ x****3+* ***x***+ ***1***

***x****2*+ ***x***+ ***1***

***s(x)= 1+x+x2*** →**(111)**;

1. ***e***=(***0000001***) → ***e***(***x***)=***x6***,

***x6 x****3 +* ***x*** *+* ***1***

***+x****6 +****x4****+****x3 x3+ x + 1***

***x4+ x3***

***+ x****4+* ***x2****+* ***x***

***x3+ x****2+****x***

***+x****3 +* ***x****+* ***1***

***x****2 +* ***1***

***s(x)= 1+x2*** →**(101)**.

Знайдені комбінації синдрому є стовпцями *перевірної матриці*:

.

*Транспонована перевірна частина* ***PΤ(n-k)×k*** *твірної матриці коду*

*Одинична*

*підматриця* ***IΤ(n-k)×(n-k)***

З перевірної матриці знаходимо *твірну* *матрицю* коду

.

*Перевірна частина* ***Pk×(n-k)***

*Одинична*

*підматриця* ***Ik×k***

Кодове слово утворюється послідовністю ***F***=(***ρ0***, ***ρ1***, ***ρ2***, ***f0***, ***f1***, ***f2***,***f3***), де ***ρ0***, ***ρ1***, ***ρ2*** – перевірочні символи.

Декодуємо задане повідомлення ***y=***(**1001110**).

Даній послідовності відповідає поліном

***y***(***x***)=**1**⋅***x****0*+ **0**⋅***x****1****+*0**⋅***x****2*+ **1**⋅***x3***+ **1**⋅***x****4*+ **1**⋅***x****5+***0**⋅***x****6=****1****+****x3***+ ***x****4*+ ***x****5*.

Скористаємося алгоритмом декодування циклічних кодів:

1. Знайдемо остачу від ділення многочлена прийнятої комбінації на твірний поліном коду і тим самим перевіримо її на наявність помилки:

***x****5+* ***x****4+* ***x****3*+ ***1 x****3* +***x***+***1***

***+ x5*+ *x3*+ *x2*** ***x2***+***x***

***x4+ x****2*+ ***1***

***+ x4*+ *x2*+ *x***

***x***+ ***1***

***s(x)= 1+ x*** →**(110)**.

Ненульова остача ***s***(***x***) свідчить про наявність помилки в прийнятій комбінації.

Вага остачі ***ω***(**110**)= **2**> ***l***, де ***l***=**1** – кратність помилок, що виправляються кодом, отже, необхідно виконати циклічний зсув кодованої послідовності на 1 розряд вправо:

(**1001110**) → (**0100111**)→ ***y***(***x***)=**0**⋅***x****0*+ **1**⋅***x****1****+* 0**⋅***x****2*+ **0**⋅***x3*+**

+**1**⋅***x****4*+ **1**⋅***x****5+* **1**⋅***x****6=****x***+ ***x****4*+ ***x****5***+ *x6****.*

1. Розділимо отриманий у результаті циклічного зсуву многочлен на твірний поліном коду:

***x****6+* ***x****5+* ***x****4*+ ***x x****3* +***x***+***1***

***+x6*+ *x4*+ *x3***  ***x3***+***x2***

***x5 + x****3* ***+ x***

***+x5*+ *x3*+ *x2***

***x2 +x***

***s(x)= x***+ ***x2*** →**(011)**.

Вага остачі ***ω***(**011**)= **2** **> 1**, отже, виконуємо циклічний зсув кодованої послідовності на 1 розряд вправо:

(**0100111**)→ (**1010011**)→ ***y***(***x***)=**1**⋅***x****0*+**0**⋅***x****1****+*1**⋅***x****2+***0**⋅***x3****+* ***+*0**⋅***x****4+* **1**⋅***x****5+***1**⋅***x****6=****1+ x2***+ ***x****5* **+ *x6****.*

1. Розділимо отриманий у результаті циклічного зсуву многочлен на твірний поліном коду:

***x****6+* ***x****5+* ***x****2*+ ***1 x****3* +***x***+***1***

***+x6*+ *x4*+ *x3***  ***x3***+***x2+x***

***x5+ x****4****+ x3+ x2+ 1***

***+x5*+ *x3*+ *x2***

***x4+ 1***

***+x4+ x2+ x***

***x2+ x+ 1***

***s(x)= 1+ x***+ ***x2*** →**(111)**.

Вага остачі ***ω***(**111)= 3 > 1**, знову виконуємо циклічний зсув кодованої послідовності й ділення її многочлена на твірний поліном коду: (**1010011**) → (**1101001**) →

→ ***y***(***x***)=**1**⋅***x****0*+ **1**⋅***x****1****+*0**⋅***x****2*+ **1**⋅***x3***+ **0**⋅***x****4*+ **0**⋅***x****5+***1**⋅***x****6=****1+ x***+ ***x****3***+ *x6****.*

1. Розділимо многочлен циклічно зсуненої послідовності на твірний поліном коду:

***x****6 +* ***x****3+* ***x***+ ***1 x****3*+ ***x***+ ***1***

***+ x6+* *x4* + *x3***  ***x3***+***x***

***x****4****+ x +1***

***+ x4*+ *x2*+ *x***

***x2+ 1***

***s(x)= 1+*** ***x2*** →**(101)**.

Вага остачі ***ω***(**101**)**= 2 > 1**, виконуємо циклічний зсув й ділення на твірний поліном: (**1101001**) → (**1110100**)→ → ***y***(***x***)= **1**⋅***x****0*+ **1**⋅***x****1****+*1**⋅***x****2*+ **0**⋅***x3***+ **1**⋅***x****4*+ **0**⋅***x****5+***0**⋅***x****6=****1+ x***+ ***x****2* **+ *x4****.*

1. Знову розділимо многочлен послідовності, отриманої у результаті останнього циклічного зсуву, на твірний поліном:

***x****4+* ***x****2+* ***x***+***1 x****3* +***x***+***1***

***+ x4* + *x2* + *x x***

***1***

***s(x)=1*** →**(100)**.

Вага отриманої остачі ***ω***(**100**)= **1 ≤ 1**, виконуємо дії з виправлення помилки.

Для цього додаємо до останнього циклічно зсунутого многочлена його остачу від ділення на твірний поліном:

***x****4+* ***x****2+* ***x***+ ***1+ 1 = x+ x****2+* ***x****4* →(**0110100**).

Виконуємо циклічний зсув отриманої кодової комбінації у зворотному напрямку на 4 розряди вліво:

(**0110100**) → (**1000110**).

Одержуємо виправлену кодову комбінацію ***u***=(**1000110**).

Декодуємо передану послідовність, вилучивши перевірні елементи в лівій частині кодового слова: (**1000110**)→(**0110**).