Dr inż. Robert Wójcik, p. 313, C-3, tel. 320-27-40

Katedra Informatyki Technicznej (K30W04ND03)
Wydział Informatyki i Telekomunikacji (W04N)
Politechnika Wrocławska

E-mail: **robert.wojcik@pwr.edu.pl**
Strona internetowa: google: Wójcik Robert

Ochrona danych

Wykład 7_8.

7. Kody korekcyjne

7.1. Problem zakłóceń w systemach transmisji danych

7.2. Rodzaje kodów korekcyjnych

7.3. Struktura kodu blokowego

7.4. Zdolność detekcyjna i korekcyjna kodu

7.5. Kody cykliczne

7.6. Wielomiany generujące kody cykliczne

7.7. Algorytm kodowania – kody cykliczne

7.8. Uproszczony algorytm dekodowania

7.9. Kody cykliczne Hamminga

7.10. Kody maksymalnej długości

7.11. Kody BCH

Kody korekcyjne

Kodowanie korekcyjne zabezpiecza informację przed błędami w systemach transmisyjnych i pamięciach, dzięki czemu zwiększa się niezawodność systemów informatycznych.

Na sygnał w kanale telekomunikacyjnym działają zakłócenia, które powodują błędy transmisyjne. Skutki zakłóceń można opisać, podając stopień zniekształcenia sygnału cyfrowego na wyjściu demodulatora. Stosuje się w tym celu elementową stopę błędów.

Elementowa stopa błędów jest prawdopodobieństwem przekłamania elementarnego sygnału cyfrowego w czasie transmisji.

Przeciętna stopa błędów w istniejących kanałach telekomunikacyjnych bez korekcji błędów wynosi $10^{-2} \div 10^{-5}$.

Z kolei w systemach transmisji danych wymaga się stopy błędów rzędu $10^{-6} \div 10^{-9}$.

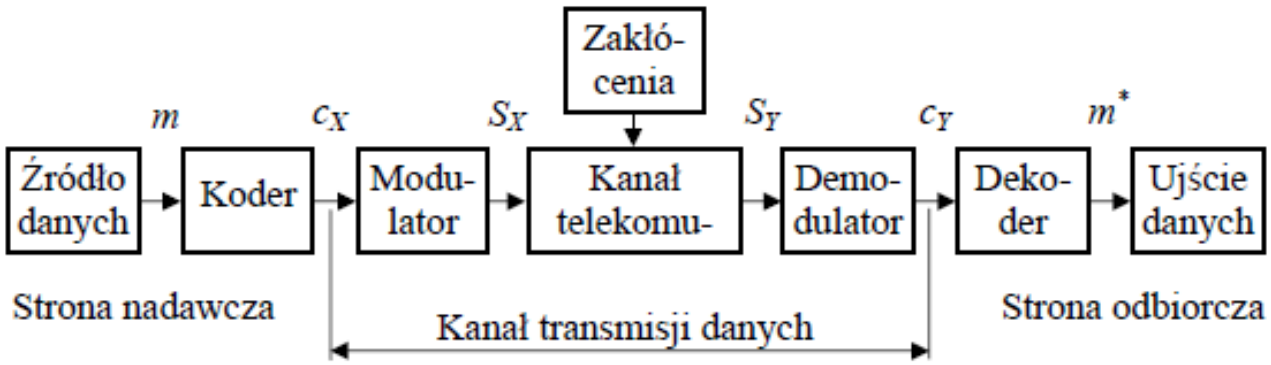
Metody poprawiania elementowej stopy błędów

W kanałach transmisji danych, wykorzystujących standardowe protokoły liniowe, poprawę wierności transmisji osiąga się w wyniku detekcji błędów po stronie odbiorczej i retransmisji błędnych bloków. W tym celu musi być utworzony informacyjny kanał sprzężenia zwrotnego.

Większą efektywność metod poprawy jakości transmisji można uzyskać dzięki zastosowaniu kodów korekcyjnych. Kody korekcyjne są też jedyną metodą poprawienia wierności transmisji wszędzie tam, gdzie są trudności z utworzeniem kanału sprzężenia zwrotnego, np. w łączności satelitarnej.

Za pomocą kodów korekcyjnych można również zabezpieczać dane przechowywane w pamięciach komputerowych.

Na kolejnym rysunku pokazano konfigurację systemu transmisji danych z zastosowaniem kodowego podsystemu korekcyjnego. Do typowego systemu transmisyjnego dodano koder i dekoder. Koder realizuje proces kodowania i jest umieszczony między źródłem danych a łączem transmisji danych. Koder przekształca ciąg wiadomości m w ciąg kodowy c_X, który jest następnie poddawany procesowi modulacji.



Przepływ informacji w kanale transmisji danych

Kanały transmisji danych tworzy się na łączach telekomunikacyjnych, do których dodaje się modulator i demodulator.

Do tworzenia łączy transmisji danych używa się różnych kanałów telekomunikacyjnych takich jak: kanały telefoniczne pojedyncze i grupowe, kanały radiowe i łącza światłowodowe.

Modulator

Modulator przekształca sygnały cyfrowe $\boldsymbol{c}_X$ w sygnały S_X dostosowane do parametrów kanału telekomunikacyjnego pod względem pasma i amplitudy. Najczęściej wykorzystuje się w tym celu dyskretną modulację częstotliwości (FSK) lub fazy (PSK) sygnału nośnego.

Demodulator

Sygnał wyjściowy kanału transmisyjnego S_Y podlega procesowi demodulacji, w czasie której następuje odtworzenie postaci cyfrowej sygnału. W technicznej realizacji do modulacji i demodulacji sygnału służą modemy.

Modemy wraz z łączem telekomunikacyjnym tworzą kanał cyfrowy nazywany *kanałem transmisji danych*.

Cyfrowy sygnał wyjściowy kanału transmisji danych c_Y zwykle różni się od sygnału wejściowego c_X . Miejsca, w których występują różnice, nazywają się *błędami transmisyjnymi*.

Dekoder układu transmisyjnego koryguje te błędy. W tym celu dekoder wykorzystuje określoną metodę korekcji, która zależy od charakterystyki kanału transmisyjnego, i odtwarza sygnał kodowy.

Na podstawie sygnału dekodera estymowany jest sygnał wejściowy *m*. Jeśli sygnał wyjściowy *m** nie ma takiej samej postaci jak sygnał wejściowy *m*, oznacza to, że wystąpiły błędy niekorygowalne.

Głównym problemem inżynierskim jest takie zaprojektowanie pary kodera i dekodera, aby:
• osiągnąć wymaganą stopę błędów transmisyjnych,
• przesyłać dane z możliwie największą szybkością.

W projektowaniu kodera i dekodera musi się uwzględniać parametry kanału transmisyjnego, a przede wszystkim rodzaj występujących w kanale zakłóceń i powodowanych przez nie błędów.

Zakłócenia i błędy w kanałach transmisji danych

Błędy transmisyjne są powodowane zniekształceniami sygnałów w kanale i zakłóceniami wywoływanymi przez czynniki zewnętrzne, np. w przypadku kanałów przewodowych zakłócenia są indukowane przez zewnętrzne pola elektromagnetyczne.

Błędy powstające wskutek działania zakłóceń mają charakter losowy i można je opisać za pomocą funkcji stochastycznych.

W kanałach telekomunikacyjnych występują dwa rodzaje zakłóceń: multiplikatywne Z_M i addytywne Z_A. Sposób oddziaływania zakłóceń na sygnał użyteczny określa zależność:

$$S_Y(t) = Z_M(t)S_X(t) + Z_A \ ,$$

gdzie $S_X(t)$ jest sygnałem wejściowym kanału, a $S_Y(t)$ − sygnałem wyjściowym.

Zakłócenia multyplikatywne

Przyczyną zakłóceń multyplikatywnych są zmiany parametrów kanału. Parametry te można w pewnym stopniu korygować i w ten sposób eliminować błędy przez nie powodowane.

Zakłócenia addytywne

Przyczyną zakłóceń addytywnych są szumy cieplne i sygnały indukowane przez pola zewnętrzne. Zakłócenia addytywne dzielą się na:

- fluktuacyjne: wywołane szumami cieplnymi; mają postać ciągłych w czasie procesów przypadkowych; ich widmo pokrywa zwykle całe pasmo kanału, a rozkład amplitud jest gaussowski;

- impulsowe: pochodzą od czynników zewnętrznych i cechuje je skupienie energii w przypadkowych okresach czasu i pewnym paśmie częstotliwości; rozkład amplitudowy zakłóceń impulsowych w kanałach telefonicznych można aproksymować rozkładem hiperbolicznym; do statystycznego opisu czasu trwania tych zakłóceń i przerw między nimi nadają się stochastyczne procesy Poissona.

Znajomość zjawisk fizycznych w kanale pozwala ocenić, jakie zakłócenia mogą w nim dominować i jakich możemy spodziewać się błędów. Podczas projektowania systemów kodowych ważne są jednak nie same zakłócenia, ale skutki działania zakłóceń w kanale, to jest intensywność błędów i ich rozkład czasowy na wyjściu demodulatora.

Jeśli w kanale dominują błędy spowodowane zakłóceniami fluktuacyjnymi, to rozkład błędów jest zbliżony do prostokątnego i nazywamy je *błędami losowymi* (random errors).

Z kolei zakłócenia impulsowe powodują powstanie *błędów grupowych*, nazywanych też błędami seryjnymi (burst errors).

Aby skonstruować dobry kod, nie wystarcza znajomość elementowej stopy błędów, która nic nie mówi o konfiguracji błędów. Błędy często mają tendencję do grupowania się w pakiety. Wynika to z charakteru zakłóceń impulsowych i przerw w transmisji. W wyniku tego powstają pakiety błędów rozciągające się na przestrzeni od kilku do kilkudziesięciu bitów. Dlatego też, aby zaprojektować efektywny kod, gwarantujący istotną poprawę wierności transmisji, trzeba znać najbardziej prawdopodobne sekwencje błędów.

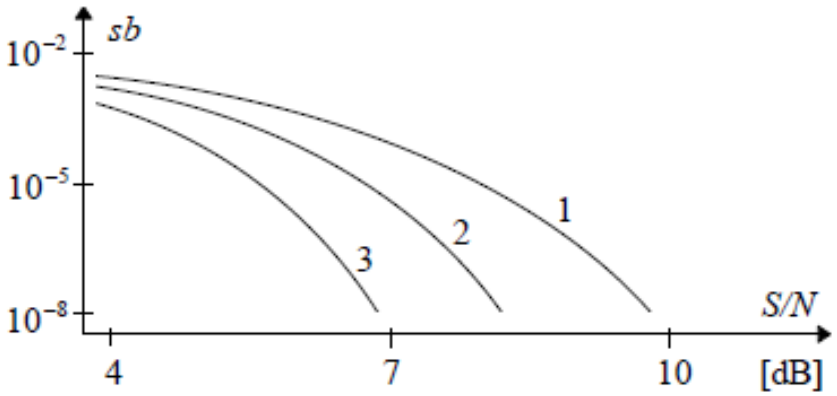
Projektantom systemów kodowych najwygodniej jest posługiwać się wynikami badań statystycznych kanałów. Badania takie obejmują, między innymi, pomiary stopy błędów i prawdopodobieństwa błędów grupowych. Statystyki te mają istotne znaczenie w projektowaniu systemów do korekcji błędów transmisyjnych.

Charakterystyki błędów w kanale transmisyjnym przedstawia się najczęściej w postaci wykresu elementowej stopy błędów *sb* w funkcji *S/N*, gdzie *S* jest mocą sygnału, a *N* mocą zakłóceń. Typowy wykres elementowej stopy błędów dla kanału transmisyjnego z błędami losowymi (gaussowskimi) pokazano na kolejnym rysunku.

W kanale z zakłóceniami gaussowskimi zastosowano modulację częstotliwości FSK (Frequency-Shift Keying).

Na wykresie pokazano charakterystyki dla trzech kanałów:
1. Kanał bez korekcji.
2. Kanał zabezpieczony kodem blokowym Hamminga (n=15, k=11) o zdolności korekcyjnej t = 1);
3. Kanał zabezpieczony kodem blokowym BCH (n=127, k=64) o zdolności korekcyjnej t = 10.

Parametr n jest liczbą bitów wektora kodowego, k jest liczbą bitów informacji, natomiast (n-k) jest liczbą bitów części korekcyjnej.



Rodzaje kodów korekcyjnych

Kodowaniem informacji nazywamy wzajemnie jednoznaczne przyporządkowanie elementów zbioru informacyjnego elementom zbioru sygnałów, za pomocą których informacje te będą albo przesyłane kanałem transmisyjnym, albo zapisywane w pamięciach.

Kod jest zatem zbiorem zakodowanych informacji. Kodowanie stosuje się w celu:
- kompresji informacji,
- szyfrowania informacji,
- przedstawienia informacji w formie odpornej na błędy.

Kody umożliwiające wykrycie lub korekcję błędów nazywają się *kodami korekcyjnymi* lub nadmiarowymi.

Klasyfikacja kodów korekcyjnych została przedstawiona poniżej.

Podział historyczny wyróżnia:

- kody blokowe,

- kody rekurencyjne, nazywane również kodami splotowymi.

Kody blokowe wymagają rozbicia ciągu informacyjnego na bloki *k*-elementowe i wykonania operacji kodowania na każdym bloku niezależnie od innych bloków. Podczas kodowania do bloku informacji jest dołączona *sekwencja kontrolna* umożliwiająca wykrycie lub korekcję błędów.

Kody splotowe nie wymagają podziału informacji na bloki, a kodowanie odbywa się na bieżąco, w takt napływającej informacji. Elementy kodu są uzależnione od bieżącego elementu informacji oraz od pewnej liczby elementów poprzednich. Koder kodu splotowego przyjmuje ciąg informacyjny i przetwarza go na ciąg kodowy o większej liczbie znaków.

Inny podział uwzględnia aparat matematyczny wykorzystywany do konstrukcji kodów korekcyjnych. W tym przypadku rozróżnia się:

- kody liniowe,

- kody cykliczne.

Obie te grupy kodów spełniają kryterium liniowości. Właściwość liniowości oznacza, że suma dwóch dowolnych wektorów kodowych daje wektor należący do zbioru wektorów kodowych tego kodu.

Kody liniowe i cykliczne różnią się konstrukcją i strukturą matematyczną. Do konstrukcji kodów liniowych wykorzystuje się grupy addytywne i wektorowe przestrzenie liniowe, a do konstrukcji kodów cyklicznych – pierścienie wielomianów nad ciałami skończonymi.

W praktyce najczęściej używa się blokowych kodów cyklicznych, które są definiowane z wykorzystaniem wielomianów o współczynnikach nad określonym ciałem. Mogą to być kody cykliczne binarne (np. kody Hamminga) lub kody cykliczne niebinarne (np. kody Reeda Solomona).

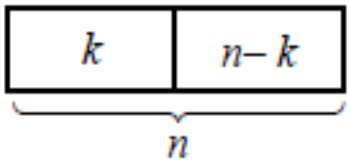
Struktura kodu blokowego

Kodowanie informacji za pomocą kodu blokowego wymaga podziału ciągu informacji na bloki *k*-elementowe.

W wyniku kodowania w koderze powstaje ciąg *n*-elementowy, gdzie *n*>*k*.

Ciąg *n*-elementowy na wyjściu kodera nazywamy *wektorem kodowym* lub słowem kodowym, a *n* jest długością wektora kodowego lub po prostu długością kodu.

Kody blokowe oznaczamy symbolem (*n*,*k*).



Wektor kodowy zawiera *k* elementów informacyjnych i *n* − *k* elementów kontrolnych, zwanych też nadmiarowymi.

W kodach binarnych elementami kodu są bity.

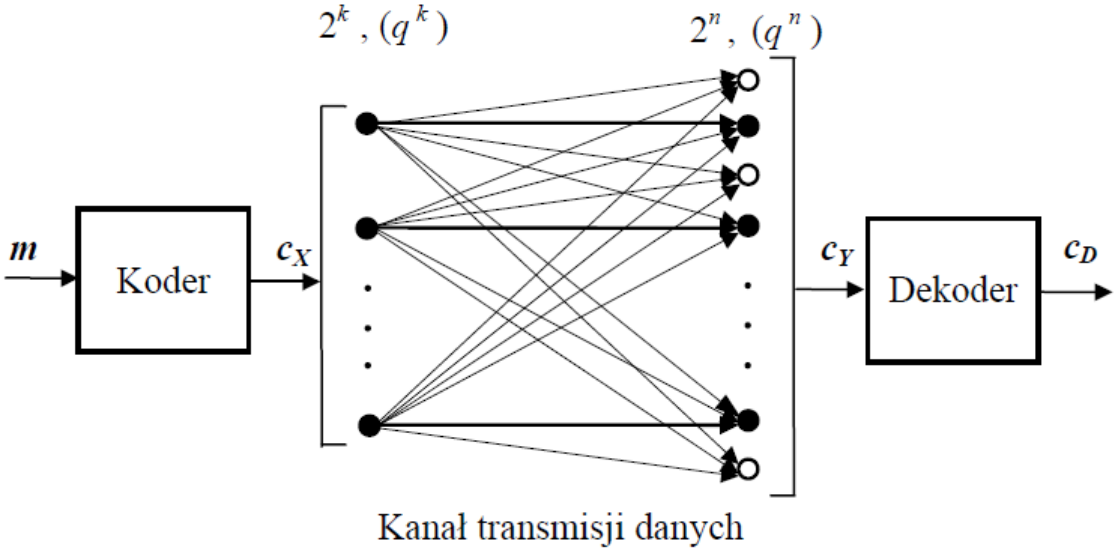
Część kontrolna wektora kodowego zawiera dodatkową informację umożliwiającą korekcję błędów transmisyjnych. Z drugiej strony część kontrolna zwiększa objętość przesyłanej informacji.

Do oceny względnej długości części informacyjnej wektora kodowego stosuje się współczynnik nazywany sprawnością kodu (code rate).

Sprawność kodu R = k / n jest stosunkiem liczby znaków wprowadzonych do kodera *k* do liczby znaków wyjściowych kodera *n*. Im więcej bitów zawiera część kontrolna, tym sprawność kodu jest mniejsza.

Kod blokowy, w którym można odróżnić elementy informacyjne od elementów kontrolnych nazywamy *kodem systematycznym*.

W systemie transmisji z korekcją błędów (kanał transmisji danych) można wyodrębnić podsystem kodowy. Jeśli na wejście kodera są podawane binarne bloki informacji zawierające po k bitów, to koder wygeneruje 2^k różnych wektorów kodowych o długości n, które zostaną podane na wejście kanału transmisyjnego. Ten zbiór wektorów nazywamy *kodem*.



Podczas transmisji może nastąpić zmiana niektórych bitów wektorów kodowych w wyniku działania zakłóceń w kanale. Wskutek tego 2^k-elementowy zbiór wektorów wejściowych kanału transmisyjnego zamieni się w zbiór wyjściowy, zawierający 2^n elementów.

Ten 2^n-elementowy zbiór wyjściowy nazywa się *przestrzenią wektorową* nad ciałem binarnym. Przestrzeń wektorowa oprócz wektorów kodowych zawiera wektory, które nie są wektorami kodowymi. Na rysunku wektory kodowe oznaczono ciemnymi punktami, a wektory niekodowe − punktami jasnymi. W nawiasach podano liczby wektorów nad ciałem rozszerzonym q-elementowym.

Możliwe przypadki działania systemu kodowania

Jeśli przyjmiemy oznaczenia z rysunku pokazującego kanał transmisji danych, to wektor wejściowy dekodera $\boldsymbol{c}_Y$ będzie sumą wektora wyjściowego kodera $\boldsymbol{c}_X$ i wektora błędów $\boldsymbol{e}$.

$$\boldsymbol{c}_Y = \boldsymbol{c}_X + \boldsymbol{e}.$$

W wyniku nałożenia się błędów na wektory kodowe podczas transmisji mogą wystąpić następujące zdarzenia:

1. Wektor kodowy przechodzi przez kanał bez zmiany.

2. Wektor kodowy zostaje zamieniony na inny wektor kodowy.

3. Wektor kodowy zostaje zamieniony na wektor niekodowy.

Przypadek pierwszy ma miejsce, gdy nie ma błędów transmisyjnych, a pozostałe zdarzenia są spowodowane błędami transmisyjnymi.

Gdy wektor kodowy zostanie zmieniony w inny wektor kodowy, wówczas dekoder nie ma możliwości odróżnienia błędnie odebranego wektora i nie może wykryć błędu. Wektor taki powstaje w wyniku nałożenia się wektora błędu na wektor kodowy, gdy wektor błędu ma postać wektora kodowego. Zatem liniowy kod blokowy nie wykrywa tylko takich ciągów błędów, które są same ciągami kodowymi. Błędy takie są niekorygowalne.

Przestrzeń wektorowa oprócz elementów kodu zawiera $2^n - 2^k$ ciągów niekodowych, które nie zostały nadane. Powstają one po stronie odbiorczej w wyniku zdarzenia trzeciego. Dekoder jest tak skonstruowany, że odróżnia ciągi kodowe od ciągów niekodowych. Ciągi niekodowe umożliwiają dekoderowi detekcję błędów transmisyjnych lub ich korekcję.

W przypadku, gdy liczba błędów lub ich rozkład w wektorze odebranym przekracza możliwości korekcyjne kodu, dekoder, analizując ciąg odebrany, może znaleźć ciąg kodowy, różniący się od ciągu odebranego najmniejszą liczbą pozycji, i przyjąć, że ten ciąg został właśnie nadany.

Taka strategia dekodowania nazywa się *dekodowaniem z maksymalną wiarygodnością* (maximum likelihood decoding) i jest powszechnie stosowana w praktyce.

Zdolność detekcyjna i korekcyjna kodu

W celu zdefiniowania podstawowych parametrów kodów wprowadza się pojęcie odległości wektorów kodowych, wagi wektora kodowego oraz odległości minimalnej.

Odległość Hamminga $d_H(u,v)$ między dwoma wektorami kodowymi *u* i *v* jest liczbą pozycji, na których występują różne współrzędne w wektorach. Ilustruje to przykład:

u = [101011011]; v = [100100011]; $d_H(u,v) = 4$.

W tym przypadku wektory różnią się na pozycjach 3, 4, 5, 6, a więc waga wynosi 4.

Waga Hamminga $w(u)$ wektora kodowego *u* jest liczbą niezerowych współrzędnych wektora. Dla powyższego wektora *u* waga Hamminga wynosi: $w(u) = 6$.

Prawdziwa jest własność - odległość między wektorami jest równa wadze sumy wektorów: $d_H(u,v) = w(u + v)$.

Dla podanych wyżej wektorów będzie: u+v = [001111000], stąd w(u+v) = 4, czyli $d_H(u,v) = 4 = w(u+v)$.

Można również zauważyć, że waga wektora kodowego jest równa jego odległości od wektora zerowego.

Odległość Hamminga i wagę Hamminga dla kodów nad ciałami rozszerzonymi oblicza się tak samo jak dla kodów binarnych.

W teorii kodów ważną rolę odgrywa *odległość minimalna* między wektorami kodowymi, oznaczana przez $d = \min d_H(u_i, v_j)$, gdzie u_i, v_j są dowolnymi wektorami danego kodu.

Odległość minimalna decyduje o możliwości detekcji i korekcji błędów kodu blokowego.

Zdolność detekcyjna kodu

Kody mogą być używane do wykrywania błędów transmisyjnych lub do wykrywania i korygowania błędów. Zdolność detekcyjną kodu *l* określa zależność

$$l = d - 1.$$

Kod blokowy o określonym parametrze d może wykryć wszystkie ciągi błędów o wadze d−1 lub mniejszej.

Możliwości korekcji błędów określa zdolność korekcyjna kodu *t*:

t = E[(d-1) / 2] = E[*l* / 2]

gdzie E[ ] oznacza część całkowitą z liczby (np. dla d=5, d-1=4 i t=2; natomiast, dla d=6, d-1=5 i t=E[2.5]=2).

Dla zadanej zdolności korekcyjnej kodu *t* jego odległość minimalna powinna wynosić d ≥ 2 t + 1.

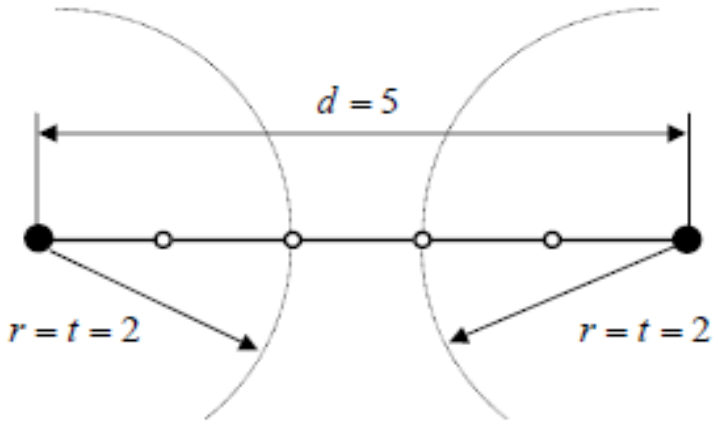
W przypadku, gdy kod jest używany jednocześnie do detekcji *a* błędów i korekcji *b* błędów, jego odległość minimalna powinna wynosić d ≥ *a* + *b* + 1, gdzie *a* ≥ *b*.

Na przykład kod posiadający d = 7 może jednocześnie wykryć i skorygować liczby błędów pokazane w kolumnach poniższej tabeli (a – detekcja, b – korekcja).

a	3	4	5	6
b	3	2	1	0

Zdolność korekcyjną kodu liniowego można zinterpretować graficznie w sposób pokazany na rysunku poniżej.

Na tym rysunku pokazano dwa wektory kodowe w postaci czarnych punktów, między którymi odległość minimalna d = 5. Zdolność korekcyjna takiego kodu t = 2. Jeśli kod koryguje wszystkie błędy w liczbie ≤ 2, oznacza to, że punkty odpowiadające wektorom kodowym można otoczyć w przestrzeni wielowymiarowej „nie przecinającymi się kulami” o promieniu r = 2. Wektory powstające w wyniku błędów, nie przekraczających zdolności korekcyjnej kodu, nie pojawią się na zewnątrz tych kul, co umożliwia przyporządkowanie ich właściwym wektorom kodowym.



Jako przykład obliczania parametrów kodu rozpatrzmy kod z bitem parzystości.

Jest to najprostszy kod detekcyjny. Do ciągów informacyjnych można dodawać jeden lub więcej bitów parzystości.

Kod z jednym bitem parzystości (n, k) = (n, n-1) ma odległość minimalną d = 2 i umożliwia wykrycie jednego błędu oraz wszystkich błędów nieparzystych.

Rozpatrzmy kod z bitem parzystości postaci (n, k) = (3, 2). Kod taki ma dwa bity informacyjne i jeden bit kontrolny.

Mamy $2^k = 4$ wektory informacyjne i jednocześnie 4 wektory kodowe:

00 0, 01 1, 10 1, 11 0.

Pozostałe z możliwych wektorów, tj. 001, 010, 100, 111 nie są wektorami kodu z kontrolą parzystości, gdyż ich waga nie jest liczbą parzystą. Są to wektory niekodowe.

Można zauważyć, że odległość Hamminga $d_H(u_i, v_j) = 2$ dla dowolnych dwóch wektorów u_i, v_j kodu z kontrolą parzystości. Stąd, odległość minimalna d = min $d_H(u_i, v_j) = 2$, gdzie u_i, v_j są dowolnymi wektorami kodu.

Zdolność detekcyjna kodu z kontrolą parzystości (3, 2) wynosi $l = d - 1 = 1$, natomiast jego zdolność korekcyjna t = E[(d-1)/2] = E[1/2] = 0. Tak, więc kod ten może wykryć maksymalnie jeden błąd, ale nie może już skorygować żadnego błędu.

Kody cykliczne

Kody cykliczne stanowią podklasą kodów liniowych. Kody te znalazły największe zastosowania praktyczne ze względu na ich następujące zalety:

- istnieją efektywne algebraiczne metody konstrukcji kodów cyklicznych o wymaganych właściwościach,

- realizacja koderów i dekoderów kodów cyklicznych za pomocą rejestrów przesuwnych ze sprzężeniem zwrotnym jest stosunkowo prosta.

W algebrze kodów cyklicznych ciągi informacyjne i kodowe zapisuje się w postaci wielomianów, a właściwości kodów opisuje się za pomocą pojęć z zakresu pierścieni wielomianów i ciał Galois.

Nazwa kodów cyklicznych pochodzi od właściwości przesunięcia cyklicznego, którą spełniają wektory kodowe.

Kod (*n*, *k*) jest kodem cyklicznym, jeśli każdy wektor kodowy:

$\boldsymbol{c} = [\, a_{n-1} , a_{n-2} , \ldots , a_1 , a_0 \,]$

po *i*-tym przesunięciu cyklicznym daje wektor:

$\boldsymbol{c}_i = [\, a_{n-1-i} , a_{n-2-i} , \ldots , a_1 , a_0 , a_{n-1} , a_{n-2} , \ldots , a_{n-i} \,]$

będący również wektorem kodowym tego kodu.

Czyli przesuwając cyklicznie wektor kodu cyklicznego otrzymujemy tylko i wyłącznie inne wektory tego kodu.

Wektor kodowy $\boldsymbol{c}$ można zapisać w postaci wielomianu:

$c(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x^1 + a_0$.

Właściwość przesunięcia cyklicznego dla wielomianowej postaci słów kodowych definiuje się w następujący sposób.

Jeśli $c(x)$ jest wielomianem kodowym stopnia $n - 1$ kodu cyklicznego, to reszta z dzielenia $x^i c(x)$ przez $x^n - 1$ jest również wektorem kodowym tego kodu. W ciałach binarnych -1 = 1, stąd można rozpatrywać reszty z dzielenia przez $x^n + 1$.

W szczególności po jednokrotnym przesunięciu wektora c otrzymujemy:

$\boldsymbol{c}_1 = [a_{n-2} , a_{n-3} , \ldots , a_1 , a_0 , a_{n-1}]$, czyli wielomian postaci

$c_1(x) = a_{n-2}x^{n-1} + a_{n-3}x^{n-2} + \ldots + a_1x^2 + a_0x^1 + a_{n-1}$.

Można pokazać, że spełniona jest zależność:

$xc(x) = a_{n-1}(x^n+1) + c_1(x)$, a stąd wynika, że

$xc(x) \bmod (x^n+1) = [\, a_{n-1}(x^n+1) + c_1(x) \,] \bmod (x^n + 1) = c_1(x) \bmod (x^n + 1)$.

Ostatecznie spełniona jest zależność zgodnie, z którą przesunięcie cykliczne wektora kodu cyklicznego o jedną pozycję jest równoważne z pomnożeniem wielomianu odpowiadającego temu wektorowi przez x i wyznaczeniu reszty z dzielenia tak otrzymanego wielomianu przez wielomian $x^n + 1$, tj.:

$c_1(x) = xc(x) \bmod (x^n + 1)$.

Podobnie w przypadku *i*-tego przesunięcia cyklicznego wektora nad ciałem charakterystyki dwa otrzymamy:

$c_i(x) = x^i c(x) \bmod (x^n + 1)$.

Tak więc, wszelkie operacje związane z przesuwaniem cyklicznym wektorów kodu cyklicznego są tożsame z odpowiednimi operacjami na wielomianach.

Wielomiany generujące kody cykliczne

Do konstrukcji kodów cyklicznych (n, k) wykorzystywane są odpowiednie wielomiany generujące.

Zasada konstrukcji n-bitowego kodu cyklicznego z wykorzystaniem wielomianu generującego g(x) stopnia nie większego niż n-1 polega na takim przekształceniu k-bitowego ciągu informacyjnego *m* w n-bitowy wektor odpowiedniego kodu cyklicznego *c*, aby otrzymany wielomian c(x) dzielił się bez reszty przez wielomian g(x), czyli aby zachodziła równość

$c(x) = a(x)\, g(x)$,

gdzie a(x) jest pewnym wielomianem stopnia nie większego niż n-1.

Wielomiany generujące kody cykliczne n-bitowe, które dzielą bez reszty wektory kodowe c(x) są wyznaczane jako podzielniki wielomianu $x^n + 1$, gdzie n jest postaci $n = 2^s – 1$, a s jest liczbą naturalną.

Postać liczby $n = 2^s - 1$ wynika z algorytmu faktoryzacji dwumianu $x^n + 1$, gdzie $n = q^s - 1$, nad ciałem rozszerzonym $GF(q^s)$ na iloczyn wielomianów nierozkładalnych.

Z powyższych rozważań wynika, że wielomianem generującym kod cykliczny może być każdy wielomian g(x), który jest podzielnikiem $x^n + 1$, gdzie $n = q^s − 1$, a *s* jest liczbą naturalną.

Jako przykład rozważmy sposób wyznaczania wielomianów generujących oraz parametrów kodów cyklicznych binarnych, w których n = 7, a więc liczba n daje się wyrazić w postaci $n = 7 = 2^3 – 1$.

W tym przypadku można pokazać, że zachodzi:

$x^7 + 1 = x^{2^3-1} + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1).$

Każdy z wielomianów otrzymanych z tego rozkładu lub ich iloczyny mogą być zastosowane do generowania kodu cyklicznego. Możliwe są następujące przypadki:

- $g(x) = x + 1$; wielomian generuje kod z bitem parzystości (n, $n - 1$),
- $g(x) = x^3 + x + 1$; wielomian generuje kod cykliczny Hamminga (7,4),
- $g(x) = x^3 + x^2 + 1$; wielomian generuje kod cykliczny Hamminga (7,4),
- $g(x) = (x + 1)(x^3 + x + 1)$; wielomian generuje kod cykliczny (7,3),
- $g(x) = (x + 1)(x^3 + x^2 + 1)$; wielomian generuje kod cykliczny (7,3),
- $g(x) = (x^3 + x + 1)(x^3 + x^2 + 1)$; wielomian generuje kod cykliczny (7,1).

Kod dualny

Dla każdego kodu cyklicznego (n, k) istnieje *cykliczny kod dualny* (n, $n-k$).

Jeżeli kod cykliczny jest generowany przez wielomian $g(x)$, to wielomianem generującym kod dualny będzie wielomian $g_D(x)$ spełniający zależność:

$$g(x)\, g_D(x) \bmod (x^n + 1) = 0.$$

W najprostszym przypadku, zachodzi: $g(x)\, g_D(x) = 1*(x^n + 1)$, czyli

$g_D(x) = (x^n + 1) / g(x)$.

Na przykład dla kodu Hamminga (n, k) = (7,4), generowanego przez wielomian $g(x) = x^3 + x^2 + 1$, istnieje kod dualny generowany przez wielomian:

$g_D(x) = (x^7 + 1) / (x^3 + x^2 + 1) = (x+1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1.$

Algorytm kodowania – kody cykliczne

Algorytm kodowania ciągu informacyjnego *k*-bitowego m(x) za pomocą wielomianu generującego g(x) stopnia (n-k) sprowadza się do skonstruowania wektora kodowego c(x) stopnia m, w taki sposób, aby dzielił się on bez reszty przez g(x).

Wektor kodowy cyklicznego kodu systematycznego ma postać:

$\boldsymbol{c} = [m_{n-1}, m_{n-2}, \ldots, m_{n-k}, r_{n-k-1}, \ldots, r_0]$

gdzie współrzędne m_i są elementami informacyjnymi, natomiast współrzędne r_i – elementami kontrolnymi.

Gdy mamy wielomian generujący $g(x)$ stopnia $n - k$, to aby obliczyć wektor kodowy systematycznego kodu cyklicznego (n,k), należy wykonać następujące czynności:

1. Wielomian odpowiadający informacji $m(x)$ pomnożyć przez x^{n-k}, tj.

$$x^{n-k}m(x).$$

Można zauważyć, że pomnożenie tego wielomianu przez x^{n-k} jest równoważne z przesunięciem wektora kodowego w lewo o (n−k) pozycji:

$$x^{n-k}m(x) = m_{k-1}x^{n-1} + m_{k-2}x^{n-2} + \ldots + m_1x^{n-k+1} + m_0x^{n-k} .$$

Np. dla wektora informacyjnego m(x) = [1011] i wielomianu $g(x) = x^3 + x^2 + 1$, stopnia n-k = 3, otrzymujemy $x^3m(x)$ = [1011 000].

2. Obliczyć resztę z dzielenia otrzymanego iloczynu przez g(x), tj.

$$r(x) = x^{n-k}m(x) \bmod g(x).$$

3. Obliczyć wielomian c(x), odpowiadający wektorowi kodowemu, dodając $x^{n-k}m(x)$ i resztę r(x) (dodajemy modulo 2 i otrzymamy wektor kodowy podzielny bez reszty przez g(x)):

$$c(x) = x^{n-k}m(x) + r(x) = x^{n-k}m(x) + x^{n-k}m(x) \bmod g(x).$$

Można zauważyć, że w ciałach charakterystyki 2 wielomian c(x) jest podzielny przez g(x), gdyż:

$$x^{n-k}m(x) = w(x)g(x) + r(x),$$

gdzie w(x) jest pewnym wielomianem.

Wynika stąd, że: c(x) = $x^{n-k}m(x)$ + r(x) = w(x)g(x) + r(x) + r(x) = w(x)g(x), gdyż w ciałach charakterystyki 2 zachodzi 2r(x) = 0 (gdyż 2 mod 2 = 0).

W celu ilustracji działania procedury kodowania rozpatrzmy kodowanie informacji za pomocą cyklicznego kodu Hamminga (7,4).

Cykliczne kody Hamminga (n, k) = (2^m - 1, 2^m - 1 - m) są generowane przez wielomiany pierwotne stopnia m. Kody te mają następujące parametry:

• odległość minimalna d = 3,

• zdolność korekcyjna t = 1.

Niech wielomianem generującym kod będzie wielomian pierwotny:

g(x) = x^3 + x + 1, który w zapisie współczynnikowym ma postać :

g(x) = 1011.

Wielomian ten generuje kod kod (n, k) = (7,4).

Obliczmy wektor kodowy dla ciągu informacyjnego m(x)=1101. Obliczenia wykonamy, posługując się ciągami współczynników.

1. Wielomian informacyjny m(x) mnożymy przez x^3 i otrzymujemy

x^3 m(x) = 1101 000.

2. Iloczyn x^3 m(x) dzielimy przez wielomian generujący kod g(x)=1011.

```
                1 1 1 1
1 0 1 1 | 1 1 0 1 0 0 0
          1 0 1 1
          -------
            1 1 0 0
            1 0 1 1
            -------
              1 1 1 0
              1 0 1 1
              -------
                1 0 1 0
                1 0 1 1
                -------
                      1
```

3. Wynik dzielenia możemy zapisać w postaci:

   1101 000 = 1111·1011+1.

Część całkowita z dzielenia wynosi 1111, a reszta r(x) = 1.

4. Resztę otrzymaną z dzielenia r(x) dodajemy do x^3m(x) i otrzymujemy ciąg c(x), odpowiadający wektorowi kodu Hamminga dla m(x)=1101.

   $c(x) = x^3 m(x) + r(x) = 1101\,000 + 1 = 1101001$.

Podobnie można obliczyć pozostałe wektory tego kodu. Za ciągi informacyjne należy przyjąć wszystkie kombinacje liczb zawierających cztery bity. Kod (7,4) będzie miał szesnaście ($2^k = 2^4 = 16$) wektorów kodowych.

Uproszczony algorytm dekodowania

W czasie transmisji wektorów kodowych kanałem transmisyjnym powstają błędy transmisyjne. Zadaniem dekodera jest wykrycie lub wykrycie i usunięcie tych błędów.

Możliwości korekcyjne kodu są określa zdolność korekcyjna kodu *t*.

Każdy kod cykliczny ma swój algorytm dekodowania, który pozwala skorygować wszystkie błędy korygowane przez dany kod, tj. nie przekraczające jego zdolności korekcyjnej *t*.

W praktyce często używa się *algorytmu uproszczonego*, wspólnego dla wszystkich kodów cyklicznych. Algorytm ten umożliwia wykrycie i korekcję wszystkich błędów znajdujących się na (n - k) pozycjach kontrolnych wektora kodowego o ile ich liczba nie przekracza zdolności korekcyjnej kodu. W przypadku, gdy błędy znajdują się również w części informacyjnej wektora kodowego możliwość korekcji błędów zależy od ich rozłożenia w wektorze kodowym, nawet jeśli ich liczba nie przekracza zdolności korekcyjnej kodu. Algorytm ten omówimy szczegółowo.

Etapy algorytmu

W procesie dekodowania oblicza się syndrom wektora odebranego *s*(x), który w przypadku kodów cyklicznych oznacza resztę z dzielenia wielomianu $c_Y(x)$, odpowiadającego wektorowi odebranemu $\boldsymbol{c_Y}$, przez wielomian generujący kod *g*(*x*).

Syndrom $s(x)$ jest więc równy:

$$s(x) = c_Y(x) \bmod g(x).$$

A więc wektor $c_Y(x) = q(x)g(x) + s(x)$.

Syndrom $s(x)$ jest wielomianem stopnia nie większego niż $n - k - 1$.

Jeśli syndrom ma wartość zerową, oznacza to, że wektor odebrany jest wektorem kodowym i w czasie transmisji nie wystąpiły żadne błędy wykrywalne przez kod.

Niezerowa wartość syndromu świadczy o tym, że odebrany wektor nie jest wektorem kodowym i zostały wykryte błędy transmisyjne.

Wektor odebrany $\boldsymbol{c_Y}$, jest sumą wektora nadanego $\boldsymbol{c_X}$ i wektora błędów $\boldsymbol{e}$. Wzór ten zapisujemy w postaci wielomianów:

$$c_Y(x) = c_X(x) + e(x).$$

Wielomian odpowiadający wektorowi kodowemu c_X dzieli się bez reszty przez wielomian generujący kod $g(x)$, można zatem napisać:

$$c_X(x) = n(x)g(x).$$

Podstawiając tę zależność do wzoru poprzedniego, otrzymamy:

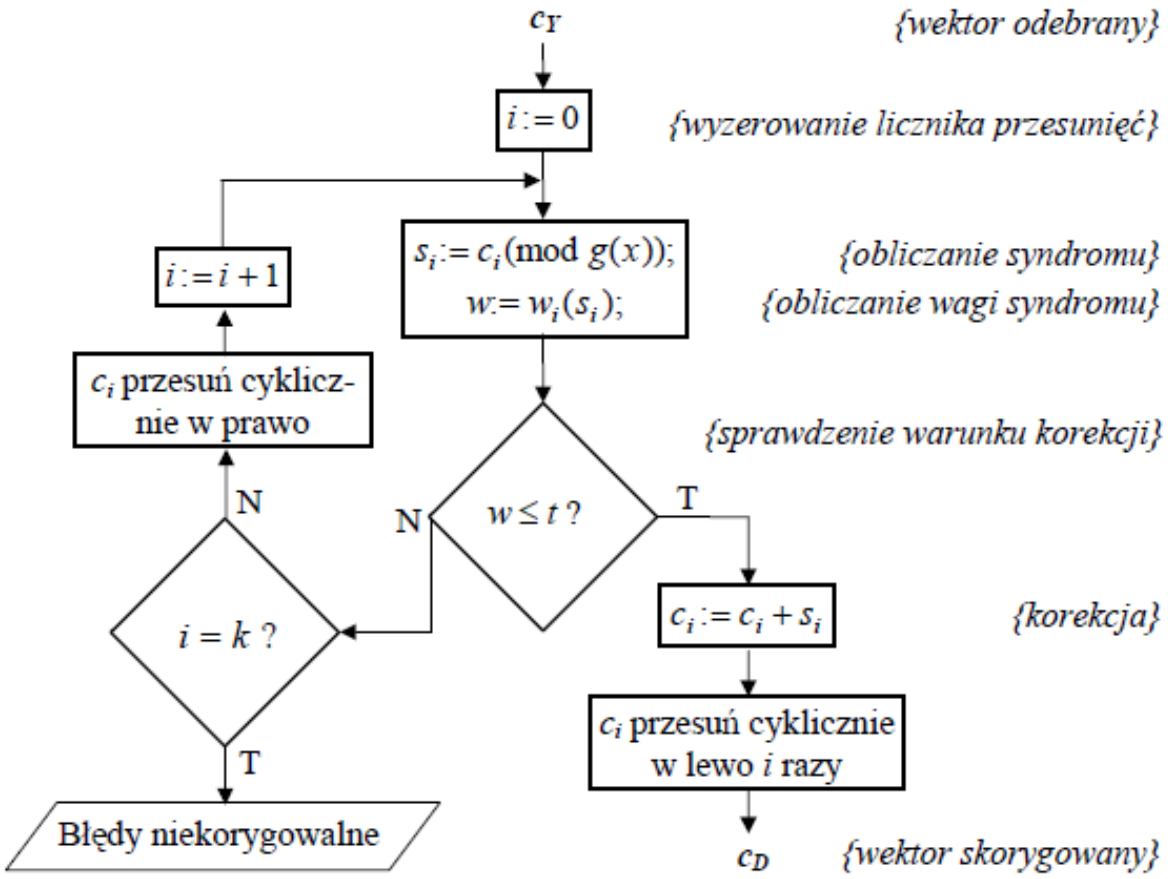
$$c_Y(x) = n(x)g(x) + e(x) .$$

Porównujemy prawą stronę tego wzoru z prawą stroną wzoru
$c_Y(x) = q(x)g(x) + s(x)$ i po przekształceniach, oraz na mocy $-n(x) = n(x)$, mamy:

$$e(x) = (n(x) + q(x))g(x) + s(x).$$

Syndrom jest więc resztą z dzielenia wielomianu odpowiadającego wektorowi błędów $e(x)$ przez wielomian generujący kod $g(x)$. Syndrom zawiera informację o położeniu błędów transmisyjnych, co jest wykorzystywane w trakcie korekcji błędów.

Schemat blokowy algorytmu dekodowania z korekcją błędów pokazano na rysunku. Parametr i oznacza kolejne cykle dekodowania.



Cały proces dekodowania przebiega następująco. Na początku wyznacza się syndrom wektora odebranego *s* a następnie oblicza się jego wagę Hamminga *w*(s). Mogą wówczas wystąpić następujące przypadki:

1. Waga syndromu jest mniejsza lub równa zdolności korekcyjnej kodu, *w*(s) ≤ *t*. Oznacza to, że błędy są położone w części kontrolnej wektora kodowego. Wektor odebrany c_Y może być wtedy skorygowany przez dodanie syndromu do wektora odebranego. W wyniku tego działania otrzymamy wektor wyjściowy dekodera cD:

   $c_D = c_Y + s$.

   Na podstawie tego wektora można wyznaczyć informację odebraną *m**. Będzie ona równa części informacyjnej wektora c_D.

2. Waga syndromu jest większa od zdolności korekcyjnej kodu, *w*(*s*) > *t*. Przypadek ten oznacza, że błędy obejmują część informacyjną wektora kodowego. Należy wówczas przesunąć cyklicznie wektor odebrany tak, aby błędy znalazły się w części kontrolnej, a potem go skorygować.

W tym celu wykonujemy następujące czynności. Przesuwamy wektor odebrany cyklicznie o jedną pozycję w dowolnym kierunku (np. w prawo), obliczamy syndrom i jego wagę oraz sprawdzamy, czy został spełniony warunek podany w punkcie 1, czy też warunek podany w punkcie 2.

- Jeżeli $w(s) \leq t$, należy skorygować wektor odebrany zgodnie z punktem 1, a następnie przesunąć go cyklicznie w odwrotną stronę (w lewo), aby odtworzyć jego pierwotną postać.

- Jeżeli $w(s) > t$, trzeba ponownie przesuwać cyklicznie wektor odebrany w tę samą stronę, obliczając po każdym przesunięciu syndrom i jego wagę aż do momentu, kiedy $w(s) \leq t$. Wtedy należy skorygować wektor odebrany i przesunąć go w odwrotną stronę o taką samą liczbę pozycji.

- W przypadku gdy po k przesunięciach cyklicznych nie uda się skorygować wektora odebranego oznacza to, że wystąpiły błędy niekorygowalne, np. istnieją bity błędne odległe o więcej pozycji w wektorze odebranym niż wynosi liczba bitów części kontrolnej (nie dało się przesunąć bitów błędnych do części kontrolnej).

Algorytm może również zadziałać błędnie jeśli liczba błędnych bitów była większa niż zdolność korekcyjna kodu t.

Algorytm dekodowania ilustruje kolejny przykład.

Przykład.

Dekodowanie wektora odebranego cyklicznego kodu Hamminga (7,4).

Niech wielomianem generującym kod będzie wielomian pierwotny:

$g(x) = x^3 + x + 1$, który w zapisie współczynnikowym ma postać :

g(x) = 1011.

Dla ciągu informacyjnego m(x)=1101 wektor kodowy c(x) = 1101001.

Załóżmy, że na wyjściu kanału odebrano wektor z błędem na pozycji trzeciej

[11**1**1001].

Należy wykonać korekcję tego wektora.

W pierwszej kolejności obliczamy syndrom s(x) wektora odebranego i jego wagę. W tym celu dzielimy wektor odebrany przez wielomian generujący kod. Dzielenie pisemne wykonujemy z wykorzystaniem ciągu współczynników.

```
              1101
1011 | 1111001
          1011
          -------
           1000
           1011
           -------
            0110
            0000
            -------
              1101
              1011
              -------
                110 = s(x)
```

Jest więc: 1111001 = 1101·1011 + 110.

Otrzymaliśmy: s(x) = 110, w(s) = 2. Ponieważ dla cyklicznego kodu Hamminga t = 1, więc w(s) > t, co oznacza, że w wektorze odebranym występuje błąd lub błędy w części informacyjnej, których nie można skorygować.

Przesuwamy cyklicznie wektor odebrany w prawo: $c_1(x)$=1111100, a następnie dzielimy wektor $c_1(x)$ przez g(x).

```
              1101
1011 | 1111100
          1011
          -------
           1001
           1011
           -------
            0100
            0000
            -------
              1000
              1011
              -------
                011 = s1(x)
```

Po wykonaniu dzielenia otrzymamy: 1111100 = 1101·1011 + 011.

Stąd mamy: $s_1(x) = 011$, $w(s_1) = 2$, $w(s_1) > t$.

Przesuwamy ponownie wektor odebrany w prawo: $c_2(x)=0111110$, a następnie dzielimy wektor $c_2(x)$ przez $g(x)$.

```
              0110
1011 | 0111110
       0000
        -------
         1111
         1011
          -------
           1001
           1011
           -------
             0100
             0000
             -------
               100 = s2(x)
```

Po wykonaniu dzielenia otrzymamy:

$0111110 = 110 \cdot 1011 + 100$, a stąd $s_2(x) = 100$, $w(s_2) = 1$.

Ponieważ $w(s_2) = t$, korygujemy przesunięty wektor odebrany $c_{YP}(x)$ dodając do niego syndrom $s_2(x)$, i otrzymujemy wektor skorygowany $c_{DP}(x)$ przesunięty o dwie pozycje w prawo:

$c_{DP}(x) = c_{YP}(x) + s_2(x) = 0111110 + 0000100 = 0111010$.

Przesuwamy otrzymany wektor o dwie pozycje w lewo i otrzymujemy wektor skorygowany 1101001. Wektor ten jest równy wektorowi na wejściu kanału transmisyjnego, czyli $c(x) = 1101001$.

Kody cykliczne Hamminga

Kod cykliczny nazywamy kodem Hamminga, jeżeli jego wielomian generujący jest wielomianem pierwotnym.

Cykliczny kod Hamminga (n, k) generowany przez wielomian pierwotny stopnia m ma następujące parametry:

• długość wektora kodowego $n = 2^m - 1$,

• liczba pozycji informacyjnych $k = 2^m - m - 1$,

• odległość minimalna $d = 3$,

• zdolność korekcyjna $t = 1$.

Kod ten może korygować jeden błąd i wykrywać jeden błąd.

Kody Hamminga można rozszerzyć mnożąc wielomian pierwotny przez czynnik $x + 1$, tj. $g(x) = (x + 1)p(x)$.

Utworzony w ten sposób kod jest cykliczny i charakteryzuje się następującymi parametrami:

• długość wektora kodowego $n = 2^m - 1$,

• liczba pozycji informacyjnych $k = 2^m - m - 2$,

• odległość minimalna $d = 4$,

• zdolność korekcyjna $t = 1$.

Kod ten może korygować jeden błąd i wykrywać dwa błędy.

Kody maksymalnej długości

Kody maksymalnej długości (maximum-length codes) są kodami dualnymi kodów Hamminga utworzonych za pomocą wielomianów pierwotnych $p(x)$. Kody maksymalnej długości istnieją dla każdej liczby całkowitej m ≥ 2. Mają one następujące parametry:

• długość wektora kodowego $n = 2^m - 1$,

• liczba pozycji informacyjnych $k = m$,

• odległość minimalna $d = 2^{m-1}$.

Wielomiany generujące kody maksymalnej długości obliczamy z zależności:

$$g(x) = (x^n + 1) / p(x)$$

gdzie $p(x)$ jest wielomianem pierwotnym stopnia m.

Sposób wyznaczania wielomianu generującego kodu ilustruje przykład.

Kod maksymalnej długości dla $m = 4$ i $p(x) = x^4 + x + 1$.

Dla przyjętych parametrów można skonstruować kod o długości wektora kodowego $n = 15$ i $d = 8$. Wielomian generujący kod będzie następujący:

$g(x) = (x^{16-1} + 1) / p(x) = (x^{15} + 1) / (x^4 + x + 1)$, stąd

$$g(x) = x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1.$$

Kody BCH

Ideałem jest podzbiór wielomianów pierścienia generowany przez pewien wielomian $g(x)$, który jest dzielnikiem $x^n + 1$. Ideał ten stanowi kod, a wielomian $g(x)$ nazywamy *wielomianem generującym kod*. Wielomian $g(x)$ dzieli bez reszty każdy wielomian odpowiadający wektorowi kodowemu. Stopień wielomianu generującego kod określa liczbę elementów kontrolnych wektora kodowego.

Z powyższych rozważań wynika, że wielomianem generującym kod cykliczny może być każdy wielomian, który jest podzielnikiem $x^n + 1$, gdzie $n = q^m - 1$, a m jest liczbą naturalną.

Kody Bose-Chaudhuri-Hocquenghema (BCH) należą do kodów korygujących błędy losowe i mają duże znaczenie praktyczne. Zostały one niezależnie skonstruowane przez Hocquenghema w 1959 r. oraz przez Bose z Chaudhurim w 1960 r.

Kody BCH swoją popularność zawdzięczają następującym zaletom:

- Istnieją efektywne metody konstruowania kodów BCH o zadanych właściwościach detekcyjnych i korekcyjnych.
- Konstrukcja koderów i dekoderów kodów BCH jest prostsza niż dla innych kodów.
-

Kody BCH można konstruować nad ciałem binarnym i ciałami rozszerzonymi. Największe znaczenie mają kody binarne. Udowodniono, że dla każdej liczby całkowitej m i $t < 2^{m-1}$ istnieje kod BCH o długości $n = 2^m - 1$. Może on korygować do t błędów i ma nie więcej niż mt elementów kontrolnych. Kody te mają następujące parametry:

- długość wektora kodowego $n = 2^m - 1,$
- liczba pozycji kontrolnych $n - k \le mt,$
- odległość minimalna $d \ge 2t + 1.$

Wielomiany generujące kody BCH wyznacza się w następujący sposób.

Niech α będzie elementem pierwotnym ciała $GF(2^m)$. Zbiór $\{f(x)\}$ jest zbiorem ciągów kodowych kodu BCH, jeśli pierwiastkami dowolnie wybranego wielomianu $f(x)$ są elementy ciała:

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}.$$

Każdy element ciała o parzystym wykładniku ma w tej sekwencji taką samą funkcję minimalną jak któryś z poprzedzających go elementów o wykładniku nieparzystym. Na przykład α^2 i α^4 są pierwiastkami $m_1(x)$ (pierwiastek α^1), α^6 jest pierwiastkiem $m_3(x)$ (pierwiastek α^3), itd. Uwzględniając ten fakt podczas wyznaczania wielomianu generującego kod BCH, wystarczy wziąć pod uwagę elementy ciała z wykładnikami nieparzystymi.

Wielomian generujący kod BCH o zdolności korekcyjnej *t* jest najmniejszą wspólną wielokrotnością funkcji minimalnych $m_1(x), m_3(x), \ldots, m_{2t-1}(x)$

$$g(x) = NWW\left(m_1(x), m_3(x), \ldots, m_{2t-1}(x)\right).$$

P r z y k ł a d

Wyznaczanie wielomianów generujących kody BCH.

Dla $m = 4$ dwumian $x^{q^m-1} - 1$ ma następujący rozkład:

$$x^{15} + 1 = (x+1)\left(x^4 + x + 1\right)\left(x^4 + x^3 + x^2 + x + 1\right)\left(x^2 + x + 1\right)\left(x^4 + x^3 + 1\right).$$

Wielomiany nierozkładalne z prawej strony znaku równości są wielomianami minimalnymi elementów ciała $GF(2^4)$. Podstawiając symbole wielomianów minimalnych, otrzymamy

$$x^{15} + 1 = m_0(x)\, m_1(x)\, m_3(x)\, m_5(x)\, m_7(x).$$

Korzystając z tego wyrażenia, dla zadanych wartości *t* można wyznaczyć wielomiany generujące kody BCH.

$t = 1,$	$g(x) = m_1(x),$	kod Hamminga (15,11);
$t = 2,$	$g(x) = m_1(x)\, m_3(x),$	kod (15,7);
$t = 3,$	$g(x) = m_1(x)\, m_3(x)\, m_5(x),$	kod (15,5).

Po prawej stronie wielomianów generujących podano parametry kodów (n,k). Na przykład dla $t = 2,\ (n,k) = (15,7).$ Aby obliczyć liczbę pozycji informacyjnych *k* wektora kodowego, należy wyznaczyć stopień wielomianu generującego. Dla kodu $(n,k) = (15,7)$ otrzymamy wielomian generujący ósmego stopnia

$$g(x) = \left(x^4 + x + 1\right)\left(x^4 + x^3 + x^2 + x + 1\right) = x^8 + x^7 + x^6 + x^4 + 1.$$

Wektor kodowy będzie zatem zawierał osiem pozycji kontrolnych i siedem informacyjnych. Odległość minimalna tego kodu jest $d \geq 5$ i może on korygować dwa błędy.

Dla $t = 1$ kod BCH ma wielomian generujący

$$g(x) = m_1(x) = x^4 + x + 1.$$

Kod BCH korygujący jeden błąd jest jednocześnie kodem Hamminga. Generalnie kody Hamminga są podzbiorem kodów BCH.

Tabela kodów cyklicznych

Problem konstrukcji kodów cyklicznych sprowadza się do syntezy wielomianu generującego kod i wyznaczenia jego odległości minimalnej. Zadania te są dość trudne, dlatego też często posługujemy się tablicami zawierającymi wielomiany generujące kody cykliczne i ich parametry.

Wybrany zestaw wielomianów kodów cyklicznych podano w tabeli. Kolejne kolumny tej tabeli zawierają: długość wektora kodowego *n*, liczbę pozycji informacyjnych *k*, odległość minimalną *d* i wielomian generujący kod *g*(*x*).

Wielomian generujący kod podano w postaci współczynników w systemie ósemkowym. Aby na podstawie tabeli wyznaczyć wielomian generujący, należy liczbę ósemkową zamienić na liczbę dwójkową. Na przykład $2467_8 = 10\ 100\ 110\ 111_2$, gdzie współczynnik zmiennej o najwyższej potędze znajduje się z lewej strony ciągu. Stąd wielomianem generującym kod cykliczny (15,5), korygującym trzy błędy (*d* = 7), będzie wielomian 10 stopnia:

$$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Wielomian generujący w zapisie współczynnikowym ma postać: 2 4 6 7.

Tabela. Wielomiany generujące binarnych kodów cyklicznych

n	k	d	$g(x)$	n	k	d	$g(x)$	n	k	d	$g(x)$
7	4	3	13	33	20	6	20741	45	22	8	63335065
	3	4	35		13	10	4172741		21	3	110111011
15	11	3	23		12	10	14217043		20	6	330333033
	10	4	65		11	11	25456465	47	24	11	43073357
	7	5	721		10	12	76563537		23	12	145115461
	6	6	1163	35	25	4	2565	49	28	3	10040001
	5	7	2467		24	4	7637		27	4	30140003
	4	8	7531		23	3	13627		21	4	2010040001
17	9	5	727		20	6	147257	51	43	3	433
	8	6	1171		19	6	251761		35	5	266251
21	16	3	61		18	4	735235		33	6	1403537
	15	4	123		17	6	1532051		32	6	2020213
	12	5	1663		16	7	2433361		27	9	134531443
	11	6	2531		15	8	7455423		26	10	242245105
	10	5	5031		11	5	143676743		24	10	1762776477
	9	8	17053		10	10	244303045		19	14	50112257553
	5	10	214537	39	27	3	13617		18	14	170336760675
23	12	7	5343		26	6	34221		10	18	62066722733023
	11	8	17445		25	3	55263	55	35	5	7164555
25	5	5	4102041		24	6	167725		34	8	11235667
	4	10	14306143		15	10	153651205	57	39	3	1341035
27	9	3	1001001		14	10	274373617		38	6	3443047
	8	6	3003003		13	12	423136633	63	57	3	103
31	26	3	45	41	21	9	6647133		56	4	305
	25	4	157		20	10	13351355		51	5	12471
	21	5	3551	43	29	6	64213		45	7	1701317
	16	7	107657		28	6	134635		39	9	166623567
	15	8	310361		15	13	2607043415		36	11	1033500423
	11	11	5423325		14	14	7211144427		30	13	157464165547
	6	15	313365047	45	35	4	2113		24	15	17323260404441
	5	16	535437151		29	5	230213		18	21	1363026512351725
33	23	3	3043		25	5	7217531		16	23	6331141367235453
	22	6	5145		24	6	11620753		10	27	472622305527250155
	21	3	17537		23	7	21113023		7	31	523104543503271737

Na podstawie danych zawartych w tabeli można skonstruować wybrane kody BCH, np. (7,4) – g(x) = 1 3; (15,7) – g(x) = 7 2 1; (31,21) – g(x) = 3 5 5 1.