Kody wykrywające i korygujące błędy

Agata Pilitowska

22 stycznia 2007

1 Wprowadzenie

Transmisja danych to nic innego jak przesyłanie symboli ustalonego, skończonego alfabetu przez pewien kanał transmisyjny. Niedoskonałość takiego kanału sprawia, że wysłany sygnał może zostać zakłócony i w efekcie wysyłany symbol zostanie błędnie odebrany przez odbiornik. Jeśli, na przykład, przesyłamy wykonane przez satelitę zdjęcia z Marsa na Ziemię, to kanał transmisyjny (przestrzeń między planetarna) jest szczególnie czuły na szum wywołany przez plamy słoneczne, złą pogodę itp. W efekcie elektromagnetyczne sygnały reprezentujące symbole naszego alfabetu zostają zniekształcone i osłabione. Może się więc zdarzyć, że odbiornik popełni błąd interpretując otrzymane sygnały.

Powstające w trakcie transmisji błędy mogą drogo kosztować i dlatego ważne są starania o to, aby błędy te były jak najmniej prawdopodobne. Zastosowanie kodowania w procesie przesyłania informacji umożliwia zwiększenie niezawodności przekazu. Kody korekcyjne są jedyną metodą poprawienia wierności transmisji tam, gdzie retransmisja błędnego sygnału jest niemożliwa, np. w łączności satelitarnej. Za ich pomocą można również zabezpieczać dane przechowywane w pamięciach komputerowych.

Przykład 1.1. Załóżmy, że mamy przesłać wiadomość 1001 i, że wysyłamy ją w niezmienionej postaci. Jeśli w trakcie transmisji powstanie błąd, to nie mamy żadnej możliwości na jego wykrycie. Jeśli natomiast zamiast słowa 1001 prześlemy słowo 10011001 (tzn. powtórzymy je raz jeszcze), wówczas jeśli wystąpi błąd to porównując obie części wiadomości możemy go wykryć.

Gdy na przykład otrzymamy słowo 10010001 to od razu wiemy, że pierwsza cyfra wiadomości może być błędna. Ale cały czas nie wiemy czy błąd powstał w pierwszej czy drugiej części słowa. □

Przykład 1.2. Lepszą metodą do wykrywania pojedynczych błędów jest tzw. binarny kod badania parzystości. Polega on na dodaniu na końcu każdego wysyłanego słowa sumy cyfr *mod* 2. Jeśli suma cyfr przesłanej wiadomości jest nieparzysta, to odbiornik "wie", że przy przesyłaniu musiał wystąpić błąd. Ale nawet, jeśli suma ta jest parzysta, to nie możemy być pewni, że błąd się nie pojawi. □

Początki teorii kodowania przypadają na koniec lat czterdziestych ubiegłego wieku. Opublikowaną w 1948 roku pracą pt."Mathematical theory of communication" C.E.Shannona zainicjował powstanie teorii informacji. Rok później ukazał się artykuł M.J.E.Golay'a pt."Notes on digital coding". Natomiast w 1950 roku R.W.Hamming napisał "Error detecting and error correcting codes".

Zasadnicza idea kodowania polega na przesyłaniu wraz z wiadomością pewnej informacji "nadmiarowej", nie wnoszącej nic do treści samej wiadomości. Odebrana, wydłużona w ten sposób wiadomość odwzorowywana jest za pomocą przekształcenia dekodującego na ciąg pierwotnej długości. Dodatkowa informacja powinna umożliwić w procesie dekodowania bezbłędne odtworzenie wysłanego słowa, jeśli w czasie transmisji wystąpiło "mało" błędów.

Przez analizę informacji zawartych w dodatkowo przesyłanych znakach odbiorca może wykryć, a w niektórych przypadkach nawet skorygować powstały na skutek zakłóceń w kanale transmisyjnym błąd. W związku z tym kody dzielimy na kody wykrywające błędy i na kody korygujące błędy. Kody wykrywające błędy mają po pierwsze na celu ustalenie czy w otrzymanej wiadomości wystąpił błąd pojedynczy, ponieważ takie błędy są najbardziej prawdopodobne. Następnie będą starać się wykrywać błędy podwójne, potrójne i tak dużo jak to będzie możliwe. Natomiast w przypadku kodów korygujących w procesie dekodowania należy błędy wykryć, zlokalizować a następnie poprawić.

Podstawowe definicje i własności

Załóżmy, że informacja jest kodowana przy zastosowaniu symboli należących do skończonego ciała $A = GF(q)$ o $q = p^m$ elementach. Formalnie kod możemy zdefiniować w następujący sposób.

Definicja 1.3. *Podzbiór $\mathcal{C}$ wolnego monoidu A^* nazywamy kodem nad alfabetem A, jeśli dla dowolnych $n, m \in Z^+$, $c_1, \ldots, c_m, d_1, \ldots, d_m \in \mathcal{C} \subseteq A^*$,*

$$c_1 \ldots c_m = d_1 \ldots d_n \Longrightarrow n = m, c_i = d_i.$$

Oznacza to, że jakiekolwiek słowo w wolnej półgrupie nad zbiorem $\mathcal{C}$ może być odczytane jednoznacznie jako konkatenacja słów ze zboru $\mathcal{C}$. Elementy zbioru $\mathcal{C}$ będziemy nazywać *słowami kodowymi.*

Przykład 1.4. Wyróżnijmy pewien element alfabetu A i nazwijmy go *przecinkiem.* Kod przecinkowy nad A złożony jest ze słów, w których przecinek występuje dokładnie raz na końcu słowa. □

Ze względu na sposób dołączania dodatkowych znaków do przesyłanej wiadomości stosowane w praktyce kody dzielimy na dwie klasy: kody blokowe i kody rekurencyjne. W przypadku kodów blokowych przesyłaną informację można podzielić na bloki zawierające k symboli, które mogą być kodowane i dekodowane niezależnie od innych bloków. Po dodaniu symboli dodatkowych słowa kodowe tworzą niepusty podzbiór $\mathcal{C}$ n-wymiarowej przestrzeni wektorowej nad ciałem $A = GF(q)$. Mówimy wówczas, że kod jest długości n. Natomiast w przypadku kodów rekurencyjnych, słowa kodowe nie są stałej długości, lecz nieskończony ciąg symboli informacji przekształcany jest w nieskończony ciąg symboli wiadomości. Elementy kodu uzależnione są od bieżącego elementu informacji oraz od pewnej liczby elementów poprzednich. Na przykład ciąg $i_0, i_1, i_2, \ldots$ zamieniany jest w ciąg $i_0, i_0^{'}, i_1, i_1^{'}, , \ldots,$ gdzie $i_n^{'}$ jest funkcją zmiennych $i_0, i_1, \ldots, i_n$.

Jeśli $|\mathcal{C}| = 1$ to $\mathcal{C}$ nazywamy *kodem trywialnym.* Jeśli $q = 2$ to $\mathcal{C}$ jest kodem binarnym.

Kod blokowy, w którym można odróżnić elementy informacyjne od kontrolnych nazywamy *kodem systematycznym.* Oznacza to, że symbole na pewnych k pozycjach są symbolami informacji oraz istnieje dokładnie jedno słowo kodowe dla każdego możliwego wyboru współrzędnych na tych k pozycjach.

Przykład 1.5. Kod $\mathcal{C} = \{u_1u_2u_3u_4u_5u_6 \in \{0,1\}^6 | u_4 = u_2 + u_3, u_5 = u_1 + u_3, u_6 = u_1 + u_2\}$ jest systematyczny na 3 pozycjach o numerach 1, 2 i 3, ale nie jest systematyczny na pozycjach o numerach 2, 3 i 4. □

Niech $u = u_1 \dots u_n,\ v = v_1 \dots v_n \in \mathcal{C}$ będą słowami kodowymi blokowego kodu $\mathcal{C}$ oraz niech $\mathbf{0}_n := \underbrace{00\dots0}_{n-razy}$ i $\mathbf{1}_n := \underbrace{11\dots1}_{n-razy}$.

Definicja 1.6. ***Odległością Hamming'a*** *(ozn. $d(u,v)$) między dwoma wektorami u i v nazywamy liczba miejsc, na których wektory te się różnią.*

Przykład 1.7.

$$\begin{aligned} d(10111, 00101) &= 2 \\ d(0122, 1220) &= 3 \end{aligned}$$

□

W przypadku binarnym kod $\mathcal{C}$ można interpretować jako podgraf grafu kostki 2^n, którego wierzchołkami są wszystkie słowa kodowe. Wówczas odległość między słowami kodowymi interpretujemy jako minimalną ilości krawędzi między tymi wierzchołkami.

Funkcja odległości jest metryką w przestrzeni $GF(q)^n$, zatem spełnia następujące warunki:

1. $d(u,u) = 0$,
2. $d(u,v) = d(v,u)$,
3. $d(u,w) \leqslant d(u,v) + d(v,w)$ (nierówność trójkąta).

Definicja 1.8. ***Waga*** *(ozn. $wt(u)$) wektora u jest to liczba jego niezerowych współrzędnych, czyli*

$$wt(u) := d(u, \mathbf{0}_n).$$

Przykład 1.9.

$$\begin{aligned} wt(101110) &= 4 \\ wt(01212110) &= 6 \\ wt(\mathbf{0}_n) &= 0 \\ wt(\mathbf{1}_n) &= n \end{aligned}$$

□

Definicja 1.10. *Zbiór*

$$K_r(u) := \{v \in GF(q)^n \mid d(u,v) \leqslant r\}$$

nazywamy ***kulą*** *o promieniu r i środku u.*

Definicja 1.11. ***Minimalną odległością*** *nietrywialnego kodu $\mathcal{C}$ nzaywamy*

$$d := min\{d(u,v) \mid u,v \in \mathcal{C}, u \neq v\}.$$

Ponieważ w praktyce trudno jest dokładnie obliczyć prawdopodobieństwo błędu po dekodowaniu, odległość kodu jest bardzo dobrą miarą "dobroci" kodu. Podczas transmisji wektor kodowy może przejść przez kanał bez zmiany (nie wystąpiły żadne błędy), może zostać zmieniony na inne słowo kodowe lub zostać zmieniony na wektor niekodowy. Dekoder jest tak skonstruowany, że odróżnia słowa kodowe od ciągów niekodowych. Gdy na skutek błędów wektor kodowy zostanie zamieniony na inny wektor kodowy, wówczas dekoder nie ma możliwości odróżnienia błędnie odebranego słowa i nie może wykryć żadnego błędu. Natomiast ciągi niekodowe umożliwiają dekoderowi wykrycie błędów. Na przykład, aby mieć możliwość wykrycia wszystkich pojedynczych błędów odległość kodu musi być co najmniej 2, gdyż inaczej błąd na jednej pozycji może przekształcić jedno słowo kodowe w inne słowo kodowe.

Twierdzenie 1.12. *Warunkiem koniecznym i dostatecznym na to, aby dany kod umożliwiał wykrycie t lub mniej błędów jest, aby odległość kodu była równa co najmniej $t+1$.*

Rolą dekodera jest nie tylko wykrywać, ale także poprawiać zlokalizowane błędy. W praktyce powszechnie stosowana jest strategia dekodowania z maksymalną wiarygodnością. Polega ona na tym, iż dekoder analizując odebrany wektor, znajduje słowo kodowe różniące się od ciągu odebranego najmniejszą liczbą pozycji (najbliższe w sensie odległości słowo kodowe) i przyjmuje, że właśnie taki ciąg został wysłany.

Jeśli odległość kodu $\mathcal{C}$ wynosi d oznacza to, że dowolne dwa słowa kodowe różnią się na co najmniej d miejscach. Stąd kule $K_r(u)$ o promieniu $r = [\frac{1}{2}(d-1)]$ wokół słów kodowych $u \in \mathcal{C}$ są rozłączne. ($[x] := \max\{n \in \mathbb{Z} | n \leqslant x\}$.)

Twierdzenie 1.13. *Kod $\mathcal{C}$ o odległości d może poprawić do $[\frac{1}{2}(d-1)]$ błędów.*

Strategia dekodowania z maksymalną wiarygodnością nie jest jedyną możliwą. Czasami stosuje się niepełną strategię dekodowania. W takim przypadku dekoder poprawia pewną ustaloną liczbę błędów, a gdy wystąpi ich więcej jedynie informuje o tym lub prosi o retransmisję tych danych, w których wystąpiło więcej błędów.

Odległość kodu determinuje ilość błędów, które można wykryć lub poprawić. Często jednak potrzeba więcej informacji na temat odległości między słowami kodowymi.

Definicja 1.14. *Niech $C_i \subseteq \mathcal{C}$ będzie podzbiorem słów kodowych o wadze i. Niech $A_i := |C_i|$. Ciąg $(A_0, A_1, \ldots, A_n)$ nazywamy* ***rozkładem wagi*** *kodu $\mathcal{C}$.*

Definicja 1.15. ***Numeratorem kodu*** $\mathcal{C}$ *nazywamy wielomian*

$$W_{\mathcal{C}}(x, y) := \sum_{i=0}^{n} A_i x^{n-i} y^i = \sum_{u \in \mathcal{C}} x^{n-wt(u)} y^{wt(u)}.$$

Przykład 1.16. Niech $\mathcal{C} = \{00, 11\}$. Wówczas $A_0 = 1$, $A_1 = 0$, $A_2 = 1$ oraz

$$W_{\mathcal{C}}(x, y) = x^2 + y^2.$$

Kod $\mathcal{C} = \{000, 100, 010, 110\}$ ma rozkład $A_0 = 1$, $A_1 = 2$, $A_2 = 1$, $A_3 = 0$ oraz

$$W_{\mathcal{C}}(x, y) = x^3 + 2x^2y + xy^2.$$

□

Definicja 1.17. *Dwa kody $\mathcal{C}_1$ i $\mathcal{C}_2$ długości n nad ciałem $GF(q)$ są* ***równoważne****, jeśli istnieje permutacja $\pi \in S_n$ taka, że $(u_1, \ldots, u_n) \in \mathcal{C}_1$ wtedy i tylko wtedy, gdy $(u_{\pi(1)}, \ldots, u_{\pi(n)}) \in \mathcal{C}_2$.*

Przykład 1.18. Kody $\mathcal{C}_1 = \{0000, 0011, 1100, 1111\}$ oraz $\mathcal{C}_2 = \{0000, 0101, 1010, 1111\}$ są równoważne. □

Kody równoważne zachowują odległość między słowami kodowymi zatem mają dokładnie takie same własności dotyczące zdolności poprawiania i korygowania błędów. Jeśli jeden z nich można odkodować to można i równoważny.

Kod $\mathcal{C}$ długości n, odległości równej d i mający M słów kodowych będziemy nazywali (n, M, d)-kodem.

Załóżmy, że kod $\mathcal{C}$ nad ciałem $GF(q)$ długości n zawierający M słów może poprawić t błędów. Wówczas kule o promieniu t wokół słów kodowych są rozłączne. Każda z takich M kul zawiera $1 + (q-1)\binom{n}{1} + \ldots + (q-1)^t\binom{n}{t}$ wektorów. Ponieważ całkowita liczba elementów przestrzeni $GF(q)^n$ wynosi q^n otrzymujemy następujące ograniczenie na liczbę słów kodowych.

Twierdzenie 1.19. (Ograniczenie Hamming'a.)
Kod długości n nad ciałem $GF(q)$, zawierający M słów kodowych i poprawiający t błędów musi spełniać następującą nierówność

$$M(1 + (q-1)\binom{n}{1} + \cdots + (q-1)^t\binom{n}{t}) \leqslant q^n. \tag{1}$$

W szczególności dla kodów binarnych musi być spełniona nierówność:

$$M(1 + \binom{n}{1} + \cdots + \binom{n}{t}) \leqslant 2^n.$$

Kody, dla których w ograniczeniu (1) zachodzi równość nazywamy *kodami doskonałymi*.

Definicja 1.20. ***Współczynnikiem sprawności*** *(n, M, d)-kodu $\mathcal{C}$ nazywamy liczbę*

$$0 < R := \frac{\log_q M}{n} \leqslant 1.$$

Wartość współczynnika R wskazuje na poziom efektywności kodu. Im większy współczynnik sprawności kodu tym w słowach kodowych jest mniej symboli sprawdzających a więcej symboli informacji. Kod jest tym lepszy im większa jest wartość R. Oznacza to, że dla zadanej długości lepsze kody mają większą liczbę słów kodowych.

W analizie systemów przesyłania stosuje się uproszczone modele kanału transmisyjnego. Najbardziej rozpowszechniony jest model tzw. *kanału symetrycznego*. Z założenia taki kanał nie gubi i nie dodaje symboli do przesyłanej informacji oraz każdy z możliwych błędów jest tak samo prawdopodobny.

Definicja 1.21. ***Binarną funkcją entropii*** *nazywamy funkcję*

$$H_2(0) := 0,$$

$$H_2(x) := -x \log_2 x - (1-x) \log_2 (1-x),$$

gdzie $0 < x \leqslant \mathbf{1}$.

Definicja 1.22. ***Pojemność binarnego kanału symetrycznego*** *z prawdopodobieństwem błędu* $1-p$ *definiujemy jako funkcję*

$$Q_2(1-p) := 1 - H_2(1-p).$$

Przypuśćmy, że wiadomość u jest zakodowana jako słowo v i wysłana przez binarny kanał transmisyjny. Z powodu zakłóceń wektor y, który otrzymujemy może różnić się od wektora wysłanego o wektor błędu

$$e = y - v = e_1 \dots e_n.$$

Jeśli prawdopodobieństwo, że w czasie przesyłania pojedynczego symbolu nie wystąpi błąd wynosi p, wówczas $e_i = 0$ z prawdopodobieństwem p (tzn. i-ty symbol jest poprawny), natomiast $e_i = 1$ z prawdopodobieństwem $1-p$ (tzn. i-ty symbol jest przesłany z błędem). Przyjmujemy, że $0 \leqslant 1-p < \frac{1}{2}$.

Przykład 1.23. Załóżmy, że przesyłamy słowo binarne długości k i kodujemy je za pomocą kodu z potrójnymi powtórzeniami. Otrzymana wiadomość $u_1, \dots, u_k, u_{k+1} \dots, u_{2k}, u_{2k+1}, \dots, u_{3k}$ składa się z $3k$ znaków, które odpowiadają trzykrotnie powtórzonej wiadomości. Przyjmijmy następujący schemat dekodowania: i-ta współrzędna wektora odkodowanego przyjmuje wartość 1, gdy wśród symboli u_i, u_{i+k}, u_{i+2k} wystąpiła ona co najmniej dwukrotnie, w przeciwnym razie przyporządkowujemy jej wartość 0.

Prawdopodobieństwo, iż dowolny symbol otrzymamy trzykrotnie bez błędu jest równe p^3. Prawdopodobieństwo, że dany symbol otrzymamy za pierwszym razem z błędem a pozostałe dwa razy bezbłędnie jest równe $p^2(1-p)$. Prawdopodobieństwo wysłania błędu tylko za drugim razem albo tylko za trzecim razem jest także równe $p^2(1-p)$. Zatem prawdopodobieństwo bezbłędnego odczytania pojedynczego symbolu jest $p^3 + 3p^2(1-p)$, natomiast prawdopodobieństwo odczytania tego symbolu z błędem jest równe $(1-p)^3 + 3p(1-p)^2$.

Przyjmijmy, że prawdopodobieństwo błędu (bez kodowania) dla pojedynczego symbolu jest równe $1-p = 0,1$. Wówczas prawdopodobieństwo trzykrotnego

odczytania symbolu bez błędu jest równe $p^3 = (0,9)^3 = 0,729$, z jednym błędem $3p^2(1-p) = 0,243$, z dwoma błędami $3p(1-p)^2 = 0,027$ a z trzema błędami $(1-p)^3 = 0,001$. Zatem nasz kod redukuje prawdopodobieństwo błędu dla pojedynczego symbolu z 10% do 2,8%, gdyż

$$(1-p)^3 + 3p(1-p)^2 = 0,001 + 0,027 = 0,028.$$

Dla porównania, w kodzie, w którym każdą przesyłaną wiadomość kodujemy przez pięciokrotne powtórzenie i dekodujemy na zasadzie "większości", prawdopodobieństwo błędu dla pojedynczego symbolu jest równe

$$(1-p)^5 + 5p(1-p)^4 + 10(1-p)^3p^2 = 0,00856,$$

czyli mniej niż 1%.

W rezultacie prawdopodobieństwo bezbłędnego przesłania ciągu 10 symboli wzrasta z $(0,9)^{10} \approx 35\%$ do $(0,972)^{10} \approx 74\%$ przy trzykrotnym powtórzeniu i do $(0,99144)^{10} \approx 91,5\%$ przy pięciokrotnym powtórzeniu. □

Korekta błędów polegająca na powtórzeniu wiadomości jest bardzo nieefektywna i daleka od optymalnej. Trzykrotne powtórzenie zapewnia korektę pojedynczego błędu dowolnej pozycji z ciągu kosztem trzykrotnego wydłużenia czasu transmisji. Dla "dobrych" kodów funkcje kodujące i dekodujące powinny być tak określone, aby prawdopodobieństwo odczytania wiadomości z błędem było minimalne. Okazuje się, że istnieją kody, dla których to prawdopodobieństwo jest dowolnie małe.

Niech $\mathcal{C}$ będzie kodem binarnym i niech $P_{\mathcal{C}}$ oznacza dla kodu $\mathcal{C}$ prawdopodobieństwo błędu po dekodowaniu, czyli prawdopodobieństwo, że otrzymane po odkodowaniu słowo jest błędne. Dla ustalonych parametrów n, M i $1-p$ niech

$$P^*(n, M, 1-p) := \min\{P_{\mathcal{C}} |\ \mathcal{C} \text{ jest kodem o parametrach } n, M, 1-p\}.$$

Twierdzenie 1.24. (Shannon)
Jeśli $0 < R < Q_2(1-p)$ *oraz* $M_n := 2^{[Rn]}$, *to* $\lim_{n\to\infty} P^*(n, M_n, d) = 0$.

Zauważmy, iż dla $1-p = 0,001$, $Q_2(1-p) \approx 1$. Zatem, dla dowolnego $\varepsilon > 0$ i dostatecznie dużego n istnieje binarny kod $\mathcal{C}$ długości n, o współczynniku sprawności bliskim 1, dla którego prawdopodobieństwo błędu po dekodowaniu może być dowolnie małe (tzn. $P_{\mathcal{C}} < \varepsilon$).

Podobny rezultat można sformułować dla kodów niebinarnych, ale z nieco inną definicją pojemności kanału.

Niestety, Shannon udowodnił twierdzenie stosując metody probabilistyczne a nie konstrukcyjne. Zatem twierdzenie nie podaje metody jak taki "dobry" kod skonstruować.

Zadania

1. Pokazać, że dla dowolnych wektorów $x = x_1 \dots x_n,\ y = y_1 \dots y_n \in GF(2)^n$
$$\sum_{i=1}^{n}(x_i - y_i)^2 = d(x, y).$$

2. Pokazać, że dla dowolnych wektorów binarnych $x = x_1 \dots x_n$ i $y = y_1 \dots y_n$
$$wt(x + y) = wt(x) + wt(y) - 2wt(x * y),$$
gdzie $x * y := x_1 \cdot y_1 \dots x_n \cdot y_n$.

3. Pokazać, że dla dowolnych wektorów binarnych x i y
$$wt(x + y) \geqslant wt(x) - wt(y).$$

4. Pokazać, że dla kodu binarnego, jeśli $wt(u) = wt(v)$ to $d(u, v)$ jest liczbą parzystą.

5. Z ilu maksymalnie słów kodowch może składać się binarny kod długości 11 poprawiający błędy podwójne?

6. Niech $\mathcal{C}$ będzie binarnym kodem długości 16 i odległości 8 takim, że każde słowo kodowe ma wagę 6. Pokazać, że $\mid \mathcal{C} \mid \leqslant 16$.

7. Niech d będzie liczbą parzystą. Załóżmy, że u, v, w i x są czterema wektorami binarnymi, parami odległymi od siebie o d. Pokazać, że istnieje dokładnie jeden wektor binarny, odległy od u, v i w o $\frac{d}{2}$. Czy zawsze istnieje binarny wektor odległy o $\frac{d}{2}$ od wszystkich czterech wektorów u, v, w i x?

2 Kody liniowe

Niech $I_m \in M_m^m$ oznacza macierz jednostkową o wyrazach z ciała $GF(q)$.

Najbardziej praktyczne w zastosowaniach i łatwe w zrozumieniu są kody liniowe, czyli kody w których słowa kodowe tworzą podprzestrzeń wektorową.

Definicja 2.1. (n,k)***-kodem liniowym*** *nad ciałem $GF(q)$ nazywamy k-wymiarową podprzestrzeń n-wymiarowej przestrzeni $GF(q)^n$.*

Proces kodowania

Wektor $v \in GF(q)^n$ jest słowem kodowym (n,k)-kodu liniowego wtw, gdy jest kombinacją liniową wektorów pewnej bazy przestrzeni k-wymiarowej. Stąd (n,k)-kod liniowy $\mathcal{C} = \{Gu^T | u \in GF(q)^k\}$, gdzie $G \in M_n^k$ jest pewną macierzą o wyrazach należących do ciała $GF(q)$.

Definicja 2.2. *Macierz, której kolumny są wektorami bazowymi k-wymiarowej podprzestrzeni $\mathcal{C}$ nazywamy* ***macierzą kodującą*** *lub* ***macierzą generującą*** *(n,k)-kodu linowego $\mathcal{C}$.*

Ponieważ podprzestrzeń może mieć więcej niż jedną bazę zatem również kod liniowy może mieć więcej niż jedną macierz generującą.

Powiemy, że macierz kodująca G jest w *postaci standardowej*, jeśli $G = \frac{I_k}{-P} \in M_n^k$, gdzie $P \in M_{n-k}^k$. Wówczas w każdym słowie kodowym $v = v_1 \dots v_n \in \mathcal{C}$ pierwszych k symboli to symbole wysyłanej informacji $u = u_1 \dots u_k$, natomiast pozostałe $n-k$ symboli to symbole sprawdzające, będące funkcją symboli informacji:

$$\begin{aligned} v_1 &= u_1, \\ &\vdots \\ v_k &= u_k, \\ v_{k+1} &= -\sum_{i=1}^{k} p_{1i} u_i, \\ &\vdots \\ v_n &= -\sum_{i=1}^{k} p_{(n-k)i} u_i. \end{aligned} \tag{2}$$

Dla każdego kodu liniowego, istnieje równoważny mu kod, którego macierz generująca ma postać standardową.

Przykład 2.3. Macierze

$$G_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ i } G_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$$

są macierzami generującymi (4,2)-kodu $\mathcal{C} = \{0000, 0101, 1011, 1110\}$. □

(n, k)-kod liniowy generowany przez macierz $G = \frac{I_k}{-P} \in M^k_{n-k}$ możemy zdefiniować również nieco inaczej. Z równań (2) otrzymujemy następującą zależność:

$$\begin{aligned} \sum_{i=1}^{k} p_{1i} v_i + v_{k+1} &= 0, \\ &\vdots \\ \sum_{i=1}^{k} p_{(n-k)i} v_i + v_n &= 0. \end{aligned} \tag{3}$$

Stąd dla macierzy $H := P|I_{n-k} \in M^n_{n-k}$, kod $\mathcal{C} = \{v \in GF(q)^n | Hv^T = \mathbf{0}^T_{n-k}\}$. Warunek ten oznacza, że każdy wektor $v \in \mathcal{C}$ jest ortogonalny do każdego wiersza macierzy H. Otrzymane w ten sposób równości (3) noszą nazwę *równości kontroli parzystości.*

Definicja 2.4. *Macierz $H = P|I_{n-k} \in M^n_{n-k}$ nazywamy* ***macierzą kontroli parzystości*** *(n, k)-kodu liniowego generowanego przez macierz $G = \frac{I_k}{-P} \in M^k_{n-k}$.*

Opis (3) daje elegancki układ równań. Każda niewiadoma (symbol sprawdzający) występuje dokładnie raz w każdym równaniu a równań jest tyle, ile symboli sprawdzających.

Lemat 2.5. *Kod liniowy długości n ma wymiar k wtedy i tylko wtedy, gdy jego macierz kontroli parzystości ma rząd $n - k$.*

Macierz generująca i macierz kontroli parzystości (n, k)-kodu linowego są ze sobą ściśle związane, gdyż

$$HG = \mathbf{0}_k \quad \text{oraz} \quad G^T H^T = \mathbf{0}_k.$$

Przykład 2.6. Macierz

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

jest macierzą kontroli parzystości (4,2)-kodu $\mathcal{C} = \{0000, 0101, 1011, 1110\}$ z przykładu 2.3. □

Definicja 2.7. *Wektor Hv^T nazywamy **syndromem** słowa $v \in GF(q)^n$.*

W przypadku kodów liniowych, jeśli wektory $u, v \in \mathcal{C}$ to również wektor $u - v \in \mathcal{C}$. Ponieważ $d(u, v) = wt(u - v)$, gdyż obie strony wyrażają liczbę miejsc na których wektory u i v się różnią, zatem, aby znaleźć odległość kodu liniowego nie trzeba porównywać wszystkich par słów kodowych.

Twierdzenie 2.8. *Odległość kodu liniowego równa jest minimalnej wadze niezerowych słów kodowych.*

Inny sposób określania odległości kodu liniowego daje następujący lemat.

Lemat 2.9. *Niech H będzie macierzą kontroli parzystości liniowego kodu $\mathcal{C}$. Wówczas kod $\mathcal{C}$ ma odległość równą d wtedy i tylko wtedy, gdy każde $d - 1$ kolumn macierzy H jest liniowo niezależnych i pewne d kolumn tej macierzy jest liniowo zależnych.*

Zatem odległość kodu liniowego jest minimalną liczbą liniowo zależnych kolumn macierzy kontroli parzystości natomiast ilość symboli kontrolnych jest maksymalną liczbą liniowo niezależnych kolumn tej macierzy.

Jeśli (n, k)-kod liniowy ma odległość równą d to powiemy o nim, że jest (n, k, d)-kodem liniowym. Zatem (n, k, d)-kody liniowe są $(n, 2^k, d)$-kodami systematycznymi, dla których współczynnik sprawności $R = \frac{k}{n}$.

Jeśli $u \in \mathcal{C}$ jest słowem kodowym kodu liniowego, wówczas liczba słów kodowych $v \in \mathcal{C}$, dla których $d(u, v) = wt(u - v) = i$ równa jest liczbie A_i słów kodowych o wadze i.

Twierdzenie 2.10. (Ograniczenie Singletona.)
Jeśli $\mathcal{C}$ jest (n,k,d)-kodem liniowym to

$$n - k \geqslant d - 1.$$

Twierdzenie 2.11. (Ograniczenie Gilberta - Varshamova.)
Istnieje binarny kod liniowy długości n z co najwyżej r symbolami kontroli parzystości i odległością co najmniej d taki, że

$$1 + \binom{n-1}{1} + \cdots + \binom{n-1}{d-2} < 2^r.$$

Można pokazać, że istnieje kod liniowy nad ciałem $GF(q)$ o tych samych własnościach taki, że

$$\sum_{i=0}^{d-2} (q-1)^i \binom{n-1}{i} < q^r.$$

Twierdzenie (2.11) dowodzi, że istnieją dobre kody liniowe, ale nie wskazuje metody ich konstrukcji.

Twierdzenie 2.12. (Ograniczenie Griesmera.)
Najkrótszy binarny kod liniowy wymiaru k i odległości d ma co najmniej długość $\sum_{i=0}^{k-1} \lceil \frac{d}{2^i} \rceil$. ($\lceil x \rceil$ jest najmniejszą liczbą całkowitą większą od x.)

Przykład 2.13. Najkrótszy kod liniowy wymiaru 5, poprawiający błędy potrójne ma długość równą co najmniej

$$\sum_{i=0}^{4} \lceil \frac{7}{2^i} \rceil = 7 + \lceil \frac{7}{2} \rceil + \lceil \frac{7}{4} \rceil + \lceil \frac{7}{8} \rceil + \lceil \frac{7}{16} \rceil = 15.$$

Istnieje liniowy (15,5,7)-kod BCH. □

Definicja 2.14. *$(n, n-k)$-kod liniowy $\mathcal{C}^\perp := \{u \in A^n \mid uw = 0,\ w \in \mathcal{C}\}$ nazywamy **kodem dualnym** lub **kodem ortogonalnym** do $\mathcal{C}$.*
($uw := \sum_{i=1}^{n} u_i w_i$ w ciele $GF(q)$.)

Jeśli H jest macierzą kontroli parzystości a G macierzą generującą kodu $\mathcal{C}$ to H^T jest macierzą generującą a G^T jest macierzą kontroli parzystości kodu dualnego $\mathcal{C}^\perp$.

Twierdzenie 2.15. (F.J.MacWilliams)
Jeśli $W_{\mathcal{C}}(x,y)$ jest numeratorem (n,k)-kodu linowego $\mathcal{C}$, to wielomian

$$W_{\mathcal{C}^\perp}(x,y) = \frac{1}{q^k} W_{\mathcal{C}}(x+(q-1)y, x-y)$$

jest numeratorem kodu dualnego $\mathcal{C}^\perp$.

W przypadku binarnym,

$$W_{\mathcal{C}^\perp}(x,y) = \frac{1}{2^k} W_{\mathcal{C}}(x+y, x-y).$$

Definicja 2.16. *Kod $\mathcal{C}$ nazywamy **słabo samo-dualnym**, jeśli $\mathcal{C} \subset \mathcal{C}^\perp$.*

W kodach słabo samo-dualnych, dla każdej pary słów kodowych $u, v \in \mathcal{C}$ (niekoniecznie różnych), $uv = 0$.

Przykład 2.17. Dowolny binarny $(n,1)$-kod powtórzeniowy jest słabo samo-dualny, gdy n jest liczbą parzystą. □

Definicja 2.18. *Kod $\mathcal{C}$ nazywamy **samo-dualnym**, jeśli $\mathcal{C} = \mathcal{C}^\perp$.*

Długość n kodów samodualnych musi być parzysta oraz kod $\mathcal{C}$ musi być $(n, n/2)$-kodem.

Przykład 2.19. Binarny (2,1)-kod powtórzeniowy $\mathcal{C} = \{00, 11\}$ jest kodem samodualnym. □

Proces dekodowania

Metoda lidera warstwy. W procesie dekodowania, dekoder musi zdecydować na podstawie otrzymanego po transmisji wektora y jakie słowo kodowe v zostało wysłane. Wystarczy, gdy dekoder znajdzie wektor błędu e, gdyż wówczas $v = y - e$. Ponieważ dla (n,k)-kodów liniowych $\mathcal{C}$ zbiór słów kodowych tworzy k-wymiarową podprzestrzeń n-wymiarowej przestrzeni wektorowej $GF(q)^n$, wektor $y \in GF(q)^n$ musi należeć do jednej z warstw względem $\mathcal{C}$. Niech $y \in a + \mathcal{C}$ dla pewnego $a \in GF(q)^n$, czyli $y = a + u$ dla $u \in \mathcal{C}$. Wówczas

$$e = y - v = a + u - v = a + v' \in a + \mathcal{C}.$$

Zatem wektory y i e należą do tych samych warstw względem podprzestrzeni $\mathcal{C}$.

Stosując strategię dekodowania z maksymalną wiarygodnością odkodujemy wektor y jako najbliższe mu w sensie odległości słowo kodowe u. Wektor błędu będzie miał wtedy najmniejszą możliwą wagę. Zauważmy, że gdy H jest macierzą kontroli parzystości kodu $\mathcal{C}$ to

$$Hy = H(v + e) = Hv + He = He,$$

czyli syndrom Hy wektora y jest taki sam jak syndrom He wektora błędu e. Zatem po otrzymaniu słowa y wybieramy wektor błędu e o minimalnej wadze w tej warstwie do której należy wektor y (tzw. lidera warstwy) i dekodujemy y jako słowo $v = y - e$. Jeśli istnieje więcej niż jeden wektor o minimalnej wadze w danej warstwie, to lidera warstwy wybieramy losowo.

Jeśli słowo $y \in \mathcal{C}$ ma wagę w, to syndrom Hy jest kombinacją liniową pewnych w kolumn macierzy H. Jeśli wektor e jest wektorem błędu to syndrom He jest kombinacją liniową tych kolumn macierzy H, na których został popełniony błąd. Jeśli wystąpił tylko pojedynczy błąd na i-tym miejscu to wektor błędu $e = 0 \dots b \dots 0$ ma wagę 1 i syndrom He jest i-tą kolumną macierzy H pomnożoną przez stałą b. Gdyby i-ta kolumna macierzy H była zerowa to błąd występujący na i-tej pozycji nie zostałby wykryty. Ponadto dla kodów binarnych, jeśli dwie kolumny macierzy H byłyby identyczne, to dwa syndromy dla dwóch różnych błędów pojedynczych byłyby takie same. W obu tych przypadkach nie byłoby możliwe wykrycie błędów pojedynczych. Stąd macierz kontroli parzystości H dla binarnych kodów wykrywających błędy pojedyncze musi mieć kolumny parami różne i niezerowe.

Przykład 2.20. Macierz

$$G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$$

jest macierzą generująca binarnego (4,2)-kodu liniowego $\mathcal{C}$. Wszystkie 16 binarnych wektorów długości 4 możemy podzielić na cztery warstwy względem

podprzestrzeni $\mathcal{C} = \{0000, 1011, 0101, 1110\}$ słów kodowych:

lider warstwy				*syndrom*
0000	1011	0101	1110	$\begin{bmatrix} 0 \\ 0 \end{bmatrix}$
1000	0011	1101	0110	$\begin{bmatrix} 1 \\ 1 \end{bmatrix}$
0100	1111	0001	1010	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$
0010	1001	0111	1100	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$

Niech $y = 1111$ będzie otrzymanym wektorem. Ponieważ syndrom $Hy^T = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ nie jest wektorem zerowym w czasie transmisji zostały popełnione błędy. Dekoder decyduje, że wektorem błędu $e = 0100$ jest lider warstwy, do której należy wektor y. Zatem wektor y zostaje odkodowany jako słowo kodowe $v = y - e = 1011$. □

Kiedy stosujemy metodę dekodowania kodu liniowego opartą na wyborze lidera warstwy, dekodowanie jest poprawne wtedy i tylko wtedy, gdy wektor błędu faktycznie jest liderem warstwy. Jeśli nie, to dekoder popełnia błąd dekodowania.

Niech α_i oznacza liczbę liderów warstw o wadze i. Wówczas prawdopodobieństwo błędu po dekodowaniu dla binarnego (n, k)-kodu linowego $\mathcal{C}$ wynosi:

$$Prawd\{e \neq lider \;\; warstwy\} = 1 - \sum_{i=0}^{n} \alpha_i (1-p)^i p^{n-i}. \tag{4}$$

Ponieważ przyjęta metoda dekodowania zapewnia wybór słowa kodowego z najbliższego sąsiedztwa to dla wszystkich innych metod dekodowania, prawdopodobieństwo $P_{\mathcal{C}}$ błędu po dekodowaniu będzie większe od (4).

Jeśli kod liniowy $\mathcal{C}$ może poprawić t lub mniej błędów oznacza to, że każdy wektor błędu o wadze $\leqslant t$ jest liderem warstwy. Zatem $\alpha_i = \binom{n}{i}$ dla

$0 \leqslant i \leqslant t$.
Dla $i > t$ wartość α_i jest niezwykle trudno obliczyć i jest znana tylko dla kilku kodów.

Jeśli prawdopodobieństwo $(1-p)$ popełnienia błędu przy przesyłaniu pojedynczego symbolu jest małe, to $p \approx 1$ oraz

$$(1-p)^i p^{(n-i)} \gg (1-p)^{(i+1)} p^{(n-i-1)}.$$

W tym przypadku część wzoru (4) dotycząca dużych i jest mało znacząca i wówczas

$$P_{\mathcal{C}} \approx 1 - \sum_{i=0}^{t} \binom{n}{i} (1-p)^i p^{n-i}$$

lub

$$P_{\mathcal{C}} \approx 1 - \sum_{i=0}^{t} \binom{n}{i} (1-p)^i p^{n-i} - \alpha_{t+1}(1-p)^{t+1} p^{n-t-1}$$

są wygodnymi przybliżeniami.

Metoda logicznej większości. Niech dla (n,k)-kodu liniowego równania (3) kontroli parzystości będą takie, że dla pewnego $1 \leqslant i \leqslant k$ zmienna v_i występuje w każdym równaniu układu oraz dla każdego $j \neq i$ zmienna v_j występuje co najwyżej w jednym równaniu.

Załóżmy, że dekoder otrzymuje słowo $x \in GF(q)^n$, w którym wystąpiło $t \leqslant \frac{1}{2}(n-k)$ błędów. Jeśli symbol x_i jest przesłany poprawnie, to co najwyżej t równań układu (3) będzie różnych od zera. Jeśli natomiast zmienna x_i jest niepoprawna, to co najmniej $n-k-(t-1)$ równań jest różnych od zera. Ponieważ $n-k-(t-1) > t$ to liczba równań równych 0 decyduje, czy symbol x_i został przesłany poprawnie czy też nie. Jeśli co najwyżej t równań układu (3) jest różnych od zera to zmienna x_i jest poprawna, jeśli jednak co najmniej $t+1$ równań jest różnych od zera, na pozycji i wystąpił błąd.

Przykład 2.21. Niech $\mathcal{C}$ będzie (7,4)-kodem binarnym o następujących równaniach kontroli parzystości:

$$\begin{aligned} x_1 + x_2 + x_3 &= 0, \\ x_1 + x_4 + x_5 &= 0, \\ x_1 + x_6 + x_7 &= 0. \end{aligned}$$

Jeżeli w otrzymanym słowie x wystąpi jeden błąd, to wszystkie trzy równania będą równe 1, jeśli zmienna x_1 jest niepoprawna. Jeśli dwa z równań będą równe 0 a trzecie 1 to symbol x_1 jest przesłany poprawnie. Natomiast jeśli tylko jedno z równań jest równe 0 to błąd wystąpił na więcej niż jednej pozycji. □

Zadania

1. Znaleźć macierz generującą binarnego (6,3)-kodu liniowego o macierzy kontroli parzystości $H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$.
2. Znaleźć najkrótszy kod linowy wymiaru 3, który poprawia błędy potrójne.
3. Z ilu maksymalnie słów kodowych może składać się binarny kod liniowy długości 11, poprawiający błędy podwójne?
4. Pokazać, że jeśli kolumny macierzy generującej binarnego (ternarnego) (n, k)-kodu linowego $\mathcal{C}$ mają wagę parzystą (podzielną przez 3) i są wzajemnie ortogonalne, to $\mathcal{C}$ jest kodem słabo samo-dualnym.
5. Pokazać, że jeśli kolumny macierzy generującej binarnego (n, k)-kodu linowego $\mathcal{C}$ mają wagę podzielną przez 4 i są wzajemnie ortogonalne, to $\mathcal{C}$ jest kodem słabo samo-dualnym i wszystkie słowa kodowe w $\mathcal{C}$ mają wagę podzielną przez 4.
6. Pokazać, że w liniowym kodzie binarnym albo wszystkie słowa kodowe mają parzystą wagę, albo dokładnie połowa z nich ma wagę parzystą a połowa nieparzystą.
7. Pokazać, że w liniowym kodzie binarnym albo wszystkie słowa kodowe rozpoczynają się 0, albo dokładnie połowa z nich rozpoczyna się 0 a połowa 1.
8. Niech $N(k, d)$ oznacza długość najkrótszego liniowego kodu binarnego wymiaru k i odległości równej d. Pokazać, że
$$N(k, d) \geqslant d + N(k - 1, \lceil \frac{d}{2} \rceil).$$

3 Wybrane metody konstrukcji kodów

Kody rozszerzone. Jeśli $\mathcal{C}$ jest (n, M, d)-kodem nad alfabetem $GF(q)$, wówczas kod rozszerzony $\hat{\mathcal{C}}$ definiujemy następująco:

$$\hat{\mathcal{C}} := \{u_1 \dots u_n u_{n+1} | u_1 \dots u_n \in \mathcal{C},\ \sum_{i=1}^{n+1} u_i \equiv_q 0\}.$$

Przykład 3.1. Jeśli $\mathcal{C}$ jest kodem liniowym o macierzy kontroli parzystości H, to

$$\hat{H} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ & & & & 0 \\ & & H & & 0 \\ & & & & \vdots \\ & & & & 0 \end{bmatrix}$$

jest macierzą kontroli parzystości kodu rozszerzonego $\hat{\mathcal{C}}$. □

Kody skrócone. Usuwając z każdego słowa kodowego (n, M, d)-kodu $\mathcal{C}$ ustaloną współrzędną otrzymujemy skrócony kod $\mathcal{C}^*$ długości $n-1$ o tej samej liczbie M elementów i najczęściej odległości $d-1$.

Przykład 3.2. Usuwając ostatnią współrzędną ze wszystkich słów kodowych (3,2,2)-kodu $\mathcal{C} = \{000, 011, 101, 110\}$ otrzymujemy (2,2,1)-kod skrócony $\mathcal{C}^* = \{00, 01, 10, 11\}$. □

Kody okrojone. Kod okrojony kodu $\bar{\mathcal{C}}$ tworzymy przez wybranie wszystkich słów kodowych należących do $\mathcal{C}$, zakończonych takim samym symbolem i usunięciu tej ostatniej pozycji. Otrzymany kod ma mniejszą długość oraz liczbę słów kodowych, ale zachowuje odległość. Jeśli usuniętym symbolem nie jest 0, wtedy zawsze kod okrojony kodu liniowego nie jest liniowy.

Przykład 3.3. Jeśli $\mathcal{C}$ jest liniowym (n, k, d)-kodem binarnym, to kod okrojony $\bar{\mathcal{C}}$ jest $(n-1, k-1, d')$-kodem, gdzie $d' \geqslant d$. □

Kody powiększone. Kod powiększony $\mathcal{C}^a$ powstaje przez dodanie do kodu $\mathcal{C}$ wektora $\mathbf{1}$ (jeśli nie jest on już elementem tego kodu).

Przykład 3.4. Jeśli $\mathcal{C}$ jest binarnym liniowym (n, k, d)-kodem, który nie zawiera wektora $\mathbf{1}_n$, liniowy kod powiększony $\mathcal{C}^a = \mathcal{C} \cup \{\mathbf{1}_n + \mathcal{C}\}$ składa się ze słów kodu $\mathcal{C}$ oraz wszystkich ich uzupełnień. Wówczas $\mathcal{C}^a$ jest $(n, k+1, d^a)$-kodem, gdzie $d^a = \min\{d, n - d'\}$ i d' jest największą wagą słów kodu $\mathcal{C}$. □

Suma kodów. Niech $\mathcal{C}_1$ i $\mathcal{C}_2$ będą odpowiednio (n, M_1, d_1) i (n, M_2, d_2) kodami binarnymi. Wówczas sumę $\mathcal{C}_\cup$ kodów $\mathcal{C}_1$ i $\mathcal{C}_2$ definiujemy następująco:

$$\mathcal{C}_\cup := \{u|u+v : u \in \mathcal{C}_1, v \in \mathcal{C}_2\},$$

gdzie wektor $u|u+v$ długości $2n$ jest konkatenacją słów $u = u_1 \dots u_n$ i $u+v = u_1+v_1 \dots u_n+v_n$. $\mathcal{C}_\cup$ jest $(2n, M_1M_2, d)$-kodem o odległości $d = \min\{2d_1, d_2\}$. (Jeżeli kody $\mathcal{C}_1$ i $\mathcal{C}_2$ są różnej długości, to aby utworzyć ich sumę należy dodać na końcu każdego słowa w krótszym kodzie odpowiednią ilość zer.)

Przykład 3.5. Jeśli $\mathcal{C}_1$ i $\mathcal{C}_2$ są odpowiednio (n_1, k_1, d_1) i (n_2, k_2, d_2) kodami liniowymi, wówczas suma kodów $\mathcal{C}_\cup$ jest $(2\max\{n_1, n_2\}, k_1+k_2, d = \min\{2d_1, d_2\})$-kodem liniowym. □

Zadania

1. Pokazać, że jeśli $\mathcal{C}$ jest (n, M, d)-kodem binarnym, w którym d jest liczbą nieparzystą, to odległość kodu rozszerzonego $\hat{\mathcal{C}}$ wynosi $d + 1$.

2. Niech $\mathcal{C}$ będzie ternarnym kodem liniowym o macierzy generującej

$$G = \begin{bmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 \end{bmatrix}.$$

   Znaleźć odległość kodu rozszerzonego $\hat{\mathcal{C}}$.

4 Kody nieliniowe i ograniczenia na wielkość kodów

Kody liniowe mają wiele praktycznych zalet. Jednak, gdy chcemy otrzymać kod z największą możliwą liczbę słów kodowych z zadaną minimalną odległością musimy czasami stosować kody nieliniowe.

Przykład 4.1. Załóżmy, że poszukujemy binarnego kodu długości 11, który poprawia błędy podwójne. Z ograniczenia Hamming'a dla kodów liniowych otrzymujemy, iż

$$2^k(1 + \binom{11}{1} + \binom{11}{2}) \leqslant 2^{11}.$$

Zatem $k \leqslant 4$ i największy kod liniowy spełniający zadane warunki może mieć co najwyżej $2^k = 16$ elementów. Natomiast istnieje nieliniowy binarny (11,24,5)-kod składający się z następujących elementów:

00000000000	11011100010
01101110001	10110111000
01011011100	00101101110
00010110111	10001011011
11000101101	11100010110
01110001011	10111000101
00100011101	10010001110
01001000111	10100100011
11010010001	11101001000
01110100100	00111010010
00011101001	10001110100
01000111010	11111111111

□

Niech $A(n, d)$ oznacza maksymalną liczbę słów kodowych w kodzie długości n z odległością d nad alfabetem $GF(q)$. Badanie liczby $A(n, d)$ jest jednym z głównych problemów kombinatorycznych teorii kodowania. Z podstawowych własności kodów wynikają różne ograniczenia na ich wielkość.

Twierdzenie 4.2. (Ograniczenie Singletona.)
Dla dowolnych $q, n, d \in \mathbb{N}$, $q \geqslant 2$

$$A(n, d) \leqslant q^{n-d+1}.$$

Kody, dla których w ograniczeniu Singletona zachodzi równość nazywamy MDS-kodami (kody o maksymalnej odległości).

Twierdzenie 4.3. (Ograniczenie Plotkina.)
Dla dowolnego binarnego kodu o odległości d i długości $n < 2d$,

$$A(n,d) \leqslant 2[\frac{d}{2d-n}]. \tag{5}$$

Wniosek 4.4. *Niech $\mathcal{C}$ będzie kodem binarnym i niech $n, d \in \mathbb{N}$. Jeśli d jest liczbą parzystą, to wówczas*

$$n = 2d \Rightarrow A(2d,d) \leqslant 4d.$$

Jeśli natomiast d jest liczbą nieparzystą, to

$$n < 2d+1 \Rightarrow A(n,d) \leqslant 2[\frac{d+1}{2d+1-n}] \text{ oraz}$$

$$n = 2d+1 \Rightarrow A(2d+1,d) \leqslant 4d+4.$$

Równości w powyższych ograniczeniach osiągane są dla tzw. kodów Hadamarda, które konstruuje się na bazie macierzy Hadamarda.

Przykład 4.5. Macierzą Hadamarda nazywamy macierz kwadratową $H_n \in M_n^n$ o wyrazach 1 i -1 taką, że $H_n H_n^T = nI_n$. Oznacza to, że dwa różne wiersze macierzy H_n są parami ortogonalne, natomiast iloczyn skalarny wiersza przez siebie jest równy n. Ponieważ $H_n^{-1} = \frac{1}{n}H_n^T$, zatem $H_n^T H_n = nI_n$ i kolumny macierzy Hadamarda mają takie same własności. Jeśli H_n jest macierzą Hadamarda to rząd n równy jest 1, 2 lub jest wielokrotnością 4.

Jeśli H_n jest macierzą Hadamarda rzędu n, to macierz

$$H_{2n} := \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix} \tag{6}$$

jest macierzą Hadamarda rzędu $2n$.

Stąd np. $H_1 = \begin{bmatrix} 1 \end{bmatrix}$, $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$ oraz

$$H_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}.$$

Przykładem macierzy Hadamarda, której rząd nie jest potęgą liczby 2 jest macierz

$$H_{12} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 \end{bmatrix}.$$

Niech dla $n \geqslant 1$ H_n będzie macierzą Hadamarda. Zastąpmy w macierzach H_n i $-H_n$ każdy symbol -1 przez 0. Zbór $\mathcal{C}_{H_n}$ złożony ze wszystkich tak zmodyfikowanych wierszy obu macierzy jest binarnym kodem długości n zawierającym $2n$ słów kodowych. Ponieważ dowolne dwa wiersze macierzy Hadamarda są ortogonalne, różnią się zatem na dokładnie połowie pozycji. Stąd kod $\mathcal{C}_{H_n}$ ma odległość równą $\frac{n}{2}$.

Kody utworzone z macierzy Hadamarda postaci (6) i rzędu $n = 2^r$ są kodami liniowymi.

Kod $\mathcal{C}_{H_8}$ otrzymany z macierzy H_8, złożony jest z następujących 16 słów

kodowych:

11111111	00000000
10101010	01010101
11001100	00110011
10011001	01100110
11110000	00001111
10100101	01011010
11000011	00111100
10010110	01101001

□

Kod $\mathcal{C}$ długości n i odległości d, dla którego $|\mathcal{C}| = A(n,d)$ nazywamy *kodem optymalnym.*

Na mocy twierdzenia 1.24 wiemy, że dobre kody są długie (bardziej precyzyjnie, mając kanał transmisyjny z określonym prawdopodobieństwem $1-p$ popełnienia błędu, możemy zredukować ten błąd znajdując ciąg kodów o wzrastającej długości). Ponieważ średnia liczba błędów po transmisji słowa długości n wynosi $n(1-p)$, zatem odległość d kodu musi być co najmniej równa $2n(1-p)$, jeśli chcemy móc te błędy skorygować. Takie wymagania znacznie ograniczają liczbę słów kodowych. Z drugiej strony dla dobrej skuteczności kodu współczynnik R jego sprawności również powinien być duży. Stąd zainteresowanie badaniami nad asymptotycznymi ograniczeniami na wielkość najlepszych kodów. Okazuje się, że najprostsze rezultaty dla kodów binarnych osiągnięto, gdy współczynnik sprawności R wyrażono jako funkcję $\frac{d}{n}$.

Z ograniczenia Plotkina (5) wynika, że jeśli $\frac{d}{n} \geqslant \frac{1}{2}$ to $R \longrightarrow 0$, gdy $n \longrightarrow \infty$. Zatem zakładamy, że $\frac{d}{n} < \frac{1}{2}$.
Niech $f(n) \preceq g(n)$ oznacza, że $f(n) \leqslant g(n)(1+\varepsilon(n))$, gdzie $\mid \varepsilon(n) \mid \rightarrow 0$ przy $n \rightarrow \infty$.

Podane wcześniej dolne ograniczenie Gilberta-Varshamova w postaci asymptotycznej przyjmuje następującą postać.

Twierdzenie 4.6. (Dolne ograniczenie Gilberta-Varshamova)
Niech $0 \leqslant \delta < \frac{1}{2}$. *Istnieje nieskończony ciąg* (n,k,d)*-kodów binarnych liniowych takich, że* $\frac{d}{n} \geqslant \delta$ *i współczynnik sprawności* $R = \frac{k}{n}$ *spełnia warunek:*

$$\frac{k}{n} = R \succeq 1 - H_2(\frac{k}{n}), \text{ gdy } n \rightarrow \infty, \text{ gdy } n \rightarrow \infty.$$

Najlepsze kody (np. kody alternujące) leżą na lub tuż powyżej dolnego ograniczenia Gilberta-Varshamova.

Asymptotyczna wersja górnego ograniczenia Hamming'a ma następującą postać.

Twierdzenie 4.7. (Górne ograniczenie Hamming'a.)
Dla dowolnego (n, M, d)*-kodu*

$$R \preceq 1 - H_2(\frac{d}{2n}), \text{ gdy } n \to \infty.$$

Twierdzenie 4.8. (Górne ograniczenie Elias.)
Dla dowolnego (n, M, d)*-kodu*

$$R \preceq 1 - H_2(\frac{1}{2} - \frac{1}{2}\sqrt{(1 - \frac{2d}{n})}), \text{ gdy } n \to \infty.$$

Lepsze górne ograniczenia podają twierdzenia Mc Eliece, Rodemich, Rumsey i Welch.

Twierdzenie 4.9. (Mc Eliece, Rodemich, Rumsey, Welch)
Dla dowolnego (n, M, d)*-kodu*

$$R \preceq H_2(\frac{1}{2} - \sqrt{\frac{d}{n}(1 - \frac{d}{n})}), \text{ gdy } n \to \infty.$$

Istnieje jeszcze lepsze ograniczenie podane przez tych samych autorów, ale ostateczne górne ograniczenie nie jest znane. Nie jest znany kod, który osiągałby obecnie znane ograniczenia górne.

W tabeli podane są dla porównania przykładowe ograniczenia na wartość $R(\frac{d}{n})$ uzyskane przy zastosowaniu różnych twierdzeń.

$\frac{d}{n}$	$Gil - Var$	Ham	$Elias$	$ERRW - 1$	$ERRW - 2$
0	1	1	1	1	1
0,1	0,531	0,714	0,702	0,722	0,693
0,2	0,278	0,531	0,492	0,469	0,461
0,3	0,119	0,390	0,312	0,250	0,250
0,4	0,029	0,278	0,150	0,081	0,081
0,5	0	0,189	0	0	0

Jak zauważyliśmy optymalne kody powinny charakteryzować się dużym współczynnikiem sprawności (kod jest tym lepszy, im więcej zawiera słów kodowych, gdyż wtedy może przekazać więcej informacji i jest bardziej wydajny), dużą odległością (aby wykrywać i poprawić jak najwięcej błędów) oraz powinny być dostatecznie długie (by zminimalizować prawdopodobieństwo błędu po odkodowaniu). Powinny być również efektywne (przesyłać dane z możliwie największą szybkością). Niestety cele te są wzajemnie sprzeczne. Stąd jednym z zadań teorii kodowania jest uzyskanie skutecznych algorytmów kodowania i dekodowania. Stosowane w praktyce kody nie mają największej możliwej minimalnej odległości, ale za to mogą być łatwo kodowane i dekodowane.

Zadania

1. Pokazać, że dla kodu binarnego i dowolnych $n, d \in \mathbb{N}$:

$$A(n, 2d-1) = A(n+1, 2d),$$

$$A(n, d) \leqslant 2A(n-1, d).$$

   Niech $A(n, d, w)$ oznacza maksymalną liczbę binarnych słów kodowych długości n, odległości co najmniej d i wagi równej w.

2. Pokazać, że dla kodu binarnego $A(n, 2d-1, w) = A(n, 2d, w)$.

3. Pokazać, że dla kodu binarnego, jeśli $w < d$ to $A(n, 2d, w) = 1$.

4. Pokazać, że dla kodu binarnego $A(n, 2d, d) = [\frac{n}{d}]$.

5. Pokazać, że dla kodu binarnego $A(n, 2d, w) \leqslant [\frac{dn}{w^2 - wn + dn}]$.

6. Oszacować możliwie najlepiej liczbę binarnych słów kodowych o wadze równej 4, długości 9 i odległości co najmniej 6.

7. Pokazać, że dla kodu binarnego $A(n, 2d, w) \leqslant [\frac{n}{w} A(n-1, 2d, w-1)]$.

8. Oszacować możliwie najlepiej wartość $A(20, 8, 7)$ dla kodu binarnego.

5 Kody doskonałe

Na mocy twierdzenia 1.13 kule o promieniu $t = [\frac{d-1}{2}]$ wokół słów kodowych kodu o minimalnej odległości d są rozłączne. Zazwyczaj istnieją wektory z przestrzeni $GF(q)^n$, które nie należą do żadnej takiej kuli. Problem zminimalizowania prawdopodobieństwa błędnego dekodowania sprowadza się do umieszczenia w n-wymiarowej kostce $GF(q)^n$ tak wielu nie zachodzących na siebie kul, jak to tylko możliwe.

Definicja 5.1. *Kod $\mathcal{C}$ długości n i odległości d nazywamy kodem doskonałym, jeśli wszystkie wektory przestrzeni $GF(q)^n$ zawarte są w kulach o promieniu $t = [\frac{d-1}{2}]$ i środku będącym słowem kodowym. (Mówimy wówczas, że kule pokrywają całą przestrzeń.)*

Kody doskonałe mogą wykryć i poprawić wszystkie t lub mniej błędów i nie mogą wykryć więcej niż t błędów. Są to najlepsze kody w tym sensie, iż nie istnieją inne kody mogące skorygować większą liczbę błędów.

Dla kodów doskonałych we wzorze na prawdopodobieństwo błędu po odkodowaniu $P_{err} = 1 - \sum_{i=0}^{n} \alpha_i (1-p)^i p^{n-i}$, $\alpha_i = 0$ dla $i > t = [\frac{d-1}{2}]$, czyli dla takich kodów

$$P_{err} = 1 - \sum_{i=0}^{t} \binom{n}{i} (1-p)^i p^{n-i}.$$

Przykład 5.2. Trywialnymi przykładami kodów doskonałych są: kod zawierający dokładnie jedno słowo kodowe (poprawia wszystkie błędy), cała przestrzeń (nie poprawia żadnego błędu) oraz jednowymiarowy binarny kod powtórzeniowy długości n, dla n nieparzystego (zawiera tylko dwa słowa $\mathbf{0}_n$ i $\mathbf{1}_n$ oraz poprawia $\frac{n-1}{2}$ błędów). □

Generalnie konstruowanie kodów doskonałych jest bardzo trudne. Aby wszystkie wektory przestrzeni $GF(q)^n$ zawarte były w kulach o promieniu t i środku w słowie kodowym to korzystając z ograniczenia Hamming'a dla kodu nad ciałem $GF(q)$ musi być spełniona równość:

$$M(1 + (q-1)n + \cdots + (q-1)^t \binom{n}{t}) = q^n,$$

gdzie M jest liczbą elementów kodu.

Lemat 5.3. *Niech $\mathcal{C}$ będzie doskonałym $(n, M, 2t+1)$-kodem nad ciałem $GF(q)$ poprawiającym t błędów. Wówczas liczba słów kodowych M jest potęgą liczby q oraz dla pewnego $l \in \mathbb{Z}$*

$$\sum_{i=0}^{t}(q-1)^i\binom{n}{i} = q^l.$$

W szczególności dla doskonałych binarnych (n, k, d)-kodów liniowych poprawiających $t = [\frac{d-1}{2}]$ błędów musi zachodzić następująca zależność:

$$2^k(1 + n + \cdots + \binom{n}{t}) = 2^n.$$

Istnieje jednak bardzo mało liczb naturalnych $1 \leqslant t < \frac{n-1}{2}$, dla których $1 + n + \cdots + \binom{n}{t}$ jest potęgą liczby 2.

Przykład 5.4. Niech $r \geqslant 1$ będzie liczbą naturalną. Kod liniowy długości $n = \frac{q^r-1}{q-1}$ i wymiaru $n - r$ jest kodem doskonałym nad ciałem $GF(q)$ poprawiającym jeden błąd. W szczególności $(2^r, 2^r - r - 1)$-kod liniowy jest binarnym kodem doskonałym poprawiającym jeden błąd. □

Przykład 5.5. Binarny (23,12,7)-kod liniowy jest kodem doskonałym poprawiającym trzy błędy natomiast ternarny (11,6,5)-kod liniowy jest kodem doskonałym poprawiającym dwa błędy. □

Kody doskonałe mają ciekawe związki z kombinatoryką.

Definicja 5.6. *Systemem Steiner'a $S(a, w, n)$ na n-elementowym zbiorze X nazywamy rodzinę w-elementowych podzbiorów zbioru X (zwanych blokami) taką, że każdy a-elementowy podzbiór zbioru X zawarty jest dokładnie w jednym bloku.*

Niech $\mathcal{C}$ będzie kodem długości n. Powiemy, że wektory o wadze w kodu $\mathcal{C}$ tworzą system Steiner'a $S(a, w, n)$, jeśli każdy zbiór a współrzędnych występuje jako niezerowa pozycja dokładnie w jednym słowie kodowym wagi w.

Twierdzenie 5.7. *Niech $\mathcal{C}$ będzie kodem doskonałym długości n poprawiającym $t = 1$ lub $t = 3$ błędy. Wówczas słowa kodowe o wadze $2t+1 = 3$ lub $2t+1 = 7$ tworzą system Steiner'a $S(t+1, 2t+1, n)$.*

Kody Hamming'a

Kody Hamming'a są ważną rodziną kodów liniowych, doskonałych, poprawiających błędy pojedyncze, które są bardzo łatwe w kodowaniu i w dekodowaniu. Jak już wcześniej zauważyliśmy, macierz kontroli parzystości dla binarnych kodów wykrywających błędy pojedyncze musi mieć kolumny parami różne i niezerowe.

Definicja 5.8. *Niech $r \geqslant 1$ będzie liczbą naturalną. Kolumny macierzy kontroli parzystości $H_r^2 \in M_r^{(2^r-1)}$ liniowego binarnego* ***kodu Hamming'a*** *$\mathcal{H}_r(2)$ są wszystkimi niezerowymi wektorami binarnymi długości r.*

Zatem w macierzy H_r^2, i-ta kolumna jest przedstawieniem liczby i w systemie dwójkowym. Możemy przyjąć, że w każdym słowie kodowym $u = u_1u_2 \dots u_{2^r-1}$ symbole o indeksach 2^i są symbolami kontrolnymi, a pozostałe symbole symbolami słowa źródłowego.

W macierzy H_r^2 każde dwie kolumny są różne i liniowo niezależne. Ponadto istnieją 3 kolumny, które są liniowo zależne. Stąd minimalna odległość kodu $d = 3$. Tak więc binarne kody Hamming'a są $(2^r - 1, 2^r - 1 - r, 3)$-kodami liniowymi dla $r \geqslant 1$.

Jeśli do kodowania zastosujemy macierz H_r^2, w której i-ta kolumna jest binarną reprezentacją liczby i to możemy przyjąć następujący schemat dekodowania dla kodu $\mathcal{H}_r(2)$. Jeśli w przesłanym słowie y wystąpił pojedynczy błąd na l-tej pozycji, to syndrom $H_r^2 e = H_r^2 y$ wektora błędu e będzie l-tą kolumną macierzy H_r^2, czyli binarną reprezentacją liczby l. Pojedynczy błąd korygujemy zamieniając l-ty symbol w otrzymanym słowie y.

Wniosek 5.9. *Słowa kodowe o wadze 3 binarnego $(2^r - 1, 2^r - r - 1, 3)$-kodu Hamming'a tworzą system Steiner'a $S(2, 3, 2^r - 1)$.*

Definicja 5.10. *Kod dualny $\mathcal{H}_r^{\perp}(2)$ do binarnego kodu Hamming'a $\mathcal{H}_r(2)$ nazywamy $(2^r - 1, r)$-kodem sympleksowym $\mathcal{S}_r$.*

Macierzą generującą kodu $\mathcal{S}_r$ jest transponowana macierz kontroli parzystości kodu $\mathcal{H}_r(2)$. Można pokazać indukcyjnie, że każdy kod $\mathcal{S}_r$ zawiera wektor zerowy i wszystkie jego niezerowe słowa kodowe są wagi 2^{r-1}. Stąd kody sympleksowe są to $(2^r - 1, r, 2^{r-1})$-kody liniowe.

Kod $\mathcal{S}_r$ jest nazywany kodem sympleksowym, ponieważ każda para słów kodowych jest w tej samej odległości. Jeśli z wierzchołków n-wymiarowej

kostki wybierzemy tylko te, które są słowami kodowymi, to utworzą one sympleks (zbiór wypukły generowany przez te wierzchołki).

Kody sympleksowe są przykładem kodów, które osiągają ograniczenie Griesmer'a na minimalną długość kodu.

Przykład 5.11. Najkrótszy kod liniowy wymiaru k i odległości $d = 2^{k-1}$ ma długość co najmniej

$$2^{k-1} + 2^{k-2} + \ldots 2 + 1 = 2^k - 1.$$

□

Metody konstrukcji macierzy kontroli parzystości, którą zastosowaliśmy w przypadku binarnym nie można bezpośrednio zastosować do kodów Hamming'a nad innymi ciałami. Jeśli kolumnami macierzy mają być niezerowe wektory długości r o współrzędnych w ciele $GF(q)$, to aby dowolne dwie kolumny takiej macierzy były liniowo niezależne należy usunąć wszystkie te wektory, które są wynikiem mnożenia przez skalary różne od 1. Stąd jako kolumny macierzy należy wybierać po jednym wektorze z każdego zbioru $K = \{v \mid v = aw, a \in GF(q)\}$. Na przykład możemy wybrać tylko te kolumny, dla których pierwsza niezerowa współrzędna równa jest 1. Takich wektorów będzie $\frac{q^r-1}{q-1}$.

Definicja 5.12. *Niech $r \geqslant 1$ będzie liczbą naturalną.* ***Kod Hamming'a*** *$\mathcal{H}_r(q)$ nad ciałem $GF(q)$ ma jako macierz kontroli parzystości macierz $H_r^q \in M_r^{\frac{(q^r-1)}{(q-1)}}$, której kolumny są wszystkimi niezerowymi ciągami długości r o elementach z ciała $GF(q)$, których pierwszy niezerowy element równy jest 1.*

Kody Hamming'a $\mathcal{H}_r(q)$ nad ciałem $GF(q)$ poprawiają pojedyncze błędy. Załóżmy, że do kodowania zastosowaliśmy macierz H_r^q. Aby przeprowadzić proces dekodowania otrzymanego słowa y, w którym został popełniony jeden błąd, obliczamy syndrom $H_r^q y = H_r^q e$ błędu $e = 0 \ldots b \ldots 0$, gdzie b występuje na l-tej pozycji. Jeśli pojedynczy błąd wystąpił w l-tym symbolu, to syndrom błędu będzie l-tą kolumną macierzy H_r^q pomnożoną przez b. Dzieląc syndrom przez b otrzymujemy l-tą kolumnę macierzy H_r^q. Błąd korygujemy odejmując (w ciele $GF(q)$) b od l-tej współrzędnej słowa y.

Kody Golay'a

Kodami Golay'a nazywamy cztery kody liniowe:

1. Binarny $(23, 12, 7)$-kod doskonały $\mathcal{G}_{23}$
2. Binarny $(24, 12, 8)$-kod $\mathcal{G}_{24}$
3. Ternarny $(11, 6, 5)$-kod doskonały $\mathcal{G}_{11}$
4. Ternarny $(12, 6, 6)$-kod $\mathcal{G}_{12}$

Definicja 5.13. *Macierzą generującą $G_{24} \in M_{24}^{12}$ binarnego $(24, 12, 8)$-kodu Golay'a $\mathcal{G}_{24}$ jest macierz*

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1
\end{bmatrix}$$

Binarny $(24, 12, 8)$-kod Golay'a $\mathcal{G}_{24}$ jest kodem wielomianowym generowanym przez wielomian $x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$.

Lemat 5.14. 1. *Każde słowo kodowe kodu $\mathcal{G}_{24}$ ma wagę podzielną przez 4.*
2. *Kod $\mathcal{G}_{24}$ jest samodualny, tzn. $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$.*
3. *Słowa kodowe kodu $\mathcal{G}_{24}$ wagi 8 tworzą system Steiner'a $S(5, 8, 24)$.*
4. *Kod $\mathcal{G}_{24}$ ma następujący rozkład wagi:*

i	0	8	12	16	24
A_i	1	759	2576	759	1

Definicja 5.15. *Binarny $(23, 12, 7)$-kod doskonały $\mathcal{G}_{23}$ jest kodem skróconym kodu $\mathcal{G}_{24}$.*

Lemat 5.16. 1. *Słowa kodowe kodu $\mathcal{G}_{23}$ wagi 7 tworzą system Steiner'a $S(4, 7, 23)$.*
2. *Kod $\mathcal{G}_{23}$ ma następujący rozkład wagi:*

i	0	7	8	11	12	15	16	23
A_i	1	253	506	1288	1288	506	253	1

Definicja 5.17. *Doskonały ternarny $(11, 6, 5)$-kod $\mathcal{G}_{11}$ jest kodem wielomianowym generowanym przez wielomian $x^5 + x^4 - x^3 + x^2 - 1$.*

Lemat 5.18. *Słowa kodowe kodu $\mathcal{G}_{11}$ wagi 5 tworzą system Steiner'a $S(4, 5, 11)$.*

Definicja 5.19. *$(12, 6, 6)$-kod $\mathcal{G}_{12}$ jest kodem rozszerzonym kodu $\mathcal{G}_{11}$.*

Lemat 5.20. 1. *Każde słowo kodowe kodu $\mathcal{G}_{12}$ ma wagę podzielną przez 3.*
2. *Kod $\mathcal{G}_{12}$ jest samodualny, tzn. $\mathcal{G}_{12} = \mathcal{G}_{12}^{\perp}$.*
3. *Słowa kodowe kodu $\mathcal{G}_{12}$ wagi 6 tworzą system Steiner'a $S(5, 6, 12)$.*

Twierdzenie 5.21. *Wszystkie kody Golay'a są jednoznaczne w tym sensie, że każdy kod o parametrach kodów $\mathcal{G}_{11}$, $\mathcal{G}_{12}$, $\mathcal{G}_{23}$ lub $\mathcal{G}_{24}$ jest równoważny z jednym z nich.*

Doskonałe kody Hamming'a i Golay'a skonstruowano w późnych latach 40-tych. W 1973 roku udowodniono, że nie jest możliwe skonstruowanie innych kodów doskonałych korygujących błędy wielokrotne. Dowód tego faktu związany jest z istnieniem całkowitych pierwiastków wielomianów Lloyd'a.

Dla dowolnej liczby $x \in \mathbb{R}$ oznaczmy przez $\binom{x}{m}$ tzw. rozszerzony dwumian, gdzie

$$\binom{x}{m} := \begin{cases} \frac{x(x-1)\cdot\cdots\cdot(x-m+1)}{m} & \text{gdy } m \in \mathbb{Z},\ m > 0, \\ 1 & \text{dla } m = 0, \\ 0 & \text{dla innych } m. \end{cases}$$

Definicja 5.22. *Niech $n \geqslant 0$ będzie liczbą całkowitą i niech $q = p^m$ dla dodatniej liczby pierwszej p. Dla każdego $k = 0, 1, \ldots, n$ wielomian*

$$L_k(x) := P_0(x,n) + \cdots + P_k(x,n) = P_k(x-1, n-1) =$$

$$= \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{x-1}{j} \binom{n-x}{k-j}$$

nazywamy ***wielomianem Lloyda****.*

Twierdzenie 5.23. (Lloyda)
Jeśli istnieje $(n, M, 2t+1)$-kod doskonały nad ciałem $GF(q)$ to wielomian Lloyda

$$L_t(x) = \sum_{j=0}^{t} (-1)^j (q-1)^{t-j} \binom{x-1}{j} \binom{n-x}{t-j}$$

ma t zer całkowitych spełniających warunek $0 < \delta_1 < \cdots < \delta_t < n$.

Lemat 5.24. *Niech $\mathcal{C}$ będzie nietrywialnym $(n, M, 2t+1)$-kodem doskonałym nad ciałem $GF(q)$. Wówczas 0, 1, i 2 nie są pierwiastkami wielomianu Lloyd'a $L_t(x)$.*

Lemat 5.25. *Każdy doskonały kod nad ciałem $GF(q)$ poprawiający błędy pojedyncze ma takie same parametry n, M i d jak kod Hamming'a.*

Lemat 5.26. *Nie ma nietrywialnych binarnych kodów doskonałych poprawiających błędy podwójne.*

Lemat 5.27. *Jedyne nietrywialne kody doskonałe nad ciałem $GF(q)$, dla $q > 2$, poprawiające błędy podwójne mają takie same parametry jak ternarny kod $\mathcal{G}_{11}$.*

Lemat 5.28. *Nie ma nietrywialnych kodów doskonałych nad ciałem $GF(q)$ dla $q > 2$, poprawiających więcej niż dwa błędy.*

Lemat 5.29. *Każdy doskonały kod binarny poprawiający więcej niż dwa błędy ma takie same parametry n, M i d jak kod Golay'a.*

Twierdzenie 5.30. (Tietavainen, Van Lint)
Nietrywialny kod doskonały nad ciałem $GF(q)$ musi mieć dokładnie takie same parametry n, M i d jak kody Hamming'a lub kody Golay'a $\mathcal{G}_{23}$ i $\mathcal{G}_{11}$.

Zatem jedyne nietrywialne kody doskonałe poprawiające błędy wielokrotne są równoważne jednemu z kodów Golay'a: $\mathcal{G}_{23}$ lub $\mathcal{G}_{11}$. Dla doskonałych kodów poprawiających błędy pojedyncze sytuacja jest nieco inna. Nietrywialny liniowy kod doskonały poprawiający błędy pojedyncze jest równoważny z kodem Hamming'a $\mathcal{H}_r(q)$ dla $q \geqslant 2$. W 1962 roku Vasil'ev skonstruował rodzinę nieliniowych binarnych kodów poprawiających błędy pojedyncze z takimi samymi parametrami jak kody Hamming'a. Nieco później Schonheim i Lindstrom znaleźli nieliniowe kody doskonałe nad ciałem $GF(q)$ dla każdego $q = p^m$.

Jednak problem znalezienia wszystkich nieliniowych kodów doskonałych nad ciałem $GF(q)$ poprawiających błędy jednokrotne jest nadal nie rozwiązany.

Kody quasi-doskonałe

Definicja 5.31. *n-wymiarowy kod $\mathcal{C}$ o odległości d nazywamy **kodem quasi-doskonałym**, jeśli wszystkie wektory przestrzeni $GF(q)^n$ zawarte są w kulach o promieniu $t+1 = [\frac{d-1}{2}] + 1$ i środku będącym słowem kodowym.*

Kod quasi-doskonały może poprawić wszystkie błędy o wadze $\leqslant t$, pewne błędy o wadze $t+1$ i żadnego o wadze większej od $t+1$. Kule o promieniu $t+1$ wokół słów kodowych mogą mieć niepuste przecięcie. Ponadto dla kodów quasi-doskonałych $\alpha_i = 0$ dla $i > t+1$. Stąd prawdopodobieństwo błędu po odkodowaniu wynosi:

$$P_{err} = 1 - \sum_{i=0}^{t} \binom{n}{i} (1-p)^i p^{n-i} - \alpha_{t+1}(1-p)^{t+1} p^{n-t-1}.$$

Są to bardzo praktyczne kody i w odróżnieniu od kodów doskonałych istnieje wiele kodów quasi-doskonałych.

6 Kody cykliczne

Niech $F[x]$ oznacza pierścień wielomianów jednej zmiennej o współczynnikach w ciele F i niech $F_n[x] = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \mid a_i \in F\}$ będzie pierścieniem wielomianów jednej zmiennej stopnia nmniejszego niż n.

Definicja 6.1. *Liniowy kod $\mathcal{C}$ nad ciałem $F = GF(q)$ nazywamy **kodem cyklicznym**, jeśli dowolne cykliczne przesunięcie współrzędnych słowa kodowego jest również słowem kodowym. Oznacza to, że*

$$c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \Rightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}.$$

Przykład 6.2. Kod $\mathcal{C} = \{000, 110, 101, 011\}$ jest kodem cyklicznym. □

Aby otrzymać algebraiczny opis kodów cyklicznych nad ciałem $F = GF(q)$ wygodnie jest związać z każdym wektorem $c = (c_0, c_1, \ldots, c_{n-1}) \in F^n$ wielomian $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in F_n[x]$ stopnia $n-1$.

Przykład 6.3. Słowom kodowym kodu $\mathcal{C}$ z przykładu 6.2 odpowiadają wielomiany: 0, $1+x$, $1+x^2$, $x+x^2$. □

Rozważmy następujący pierścień ilorazowy:

$$R_n := F[x]/(x^n - 1) = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + (x^n - 1) \mid a_i \in F\} \cong$$

$$\{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \mid a_i \in F\}.$$

Jeśli $c(x) \in R_n$ to mnożąc wielomian $c(x)$ przez x otrzymujemy

$$xc(x) = c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}x^n.$$

W pierścieniu R_n, $x^n = 1$ stąd

$$xc(x) = c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1}.$$

Otrzymany wielomian odpowiada wektorowi $(c_{n-1}, c_0, \ldots, c_{n-2})$. Zatem mnożenie w pierścieniu R_n wielomianu $c(x)$ przez x odpowiada cyklicznemu przesunięciu współrzędnych wektora c.

Twierdzenie 6.4. *Niech $R_n = F[x]/(x^n - 1)$ i niech $\mathcal{C} \subseteq R_n$. Liniowy kod $\mathcal{C}$ jest kodem cyklicznym wtw, gdy $\mathcal{C}$ jest ideałem w pierścieniu R_n.*

Wniosek 6.5. *Jeśli $\mathcal{C}$ jest kodem cyklicznym to istnieje jednoznacznie wyznaczony unormowany wielomian $g(x) \in \mathcal{C}$ o minimalnym stopniu taki, że $\mathcal{C} = (g(x))$. Ponadto, $g(x) \mid (x^n - 1)$.*

Wielomian $g(x)$ nazywamy *wielomianem generującym kodu cyklicznego* $\mathcal{C} = (g(x))$.

Aby skonstruować kod cykliczny długości n nad ciałem $GF(q)$ należy znaleźć dzielniki wielomianu $x^n - 1$ w tym ciele. W praktyce, dla dużych n, może to być bardzo trudne. Jeśli rozłożymy wielomian $x^n - 1$ na czynniki nierozkładalne nad ciałem $GF(q)$ to skonstruujemy wszystkie kody cykliczne długości n nad tym ciałem.

Schemat kodowania

Zauważmy, że jeżeli $\mathcal{C}$ jest liniowym kodem cyklicznym długości n generowanym przez wielomian $g(x)$ stopnia $n-k$, to wielomiany $g(x), xg(x), \ldots, x^{k-1}g(x) \in \mathcal{C}$ tworzą bazę przestrzeni $\mathcal{C}$.

Twierdzenie 6.6. *Niech $\mathcal{C} = (g(x))$ będzie kodem cyklicznym, generowanym przez wielomian $g(x) = g_0 + g_1 x + \cdots + g_{n-k}x^{n-k}$ stopnia $n - k$ ($g_{n-k} \neq 0$). Wówczas wymiar kodu $\mathcal{C}$ wynosi k a jego macierz generująca $G \in M_n^k$ ma postać:*

$$G = \begin{pmatrix} g_0 & 0 & 0 & \ldots & 0 \\ g_1 & g_0 & 0 & \ldots & 0 \\ g_2 & g_1 & g_0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ g_{n-k} & g_{n-k-1} & g_{n-k-2} & \cdots & \cdots \\ 0 & g_{n-k} & g_{n-k-1} & \cdots & \cdots \\ 0 & 0 & g_{n-k} & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & g_{n-k} \end{pmatrix}.$$

Jednakże kod zdefiniowany przy zastosowaniu tak określonej macierzy generującej nie jest systematyczny. Symbole wiadomości nie występują jawnie na żadnej pozycji w słowach kodowych. Można jednak podać alternatywny schemat kodowania dla kodów cyklicznych, dla którego macierz generująca będzie postaci $\frac{-P}{I_k}$, gdzie $P \in M_{n-k}^k$.

Niech $u(x) = u_0 + u_1 x + \cdots + u_{k-1}x^{k-1}$ będzie wielomianem odpowiadającym przesyłanej wiadomości $u = u_0 u_1 \ldots u_{k-1}$. Ponieważ kod cykliczny $\mathcal{C}$ jest ideałem generowanym przez wielomian $g(x)$, zatem wektor c będzie słowem kodowym wtedy i tylko wtedy, gdy odpowiadający mu wielomian $c(x)$ będzie podzielny przez $g(x)$. Niech

$$c'(x) := x^{n-k}u(x) = u_0 x^{n-k} + \cdots + u_{k-1}x^{n-1}.$$

Wówczas istnieją wielomiany $f(x), r(x) \in R_n$ takie, że

$$c'(x) = g(x)f(x) + r(x), \quad \text{gdzie } 0 \leqslant \mathrm{st}r(x) < \mathrm{st}g(x) = n - k.$$

Stąd

$$c'(x) - r(x) = g(x)f(x) + r(x) - r(x) = g(x)f(x)$$

jest wielomianem podzielnym przez $g(x)$. Jako słowo kodowe dla wiadomości $u(x)$ przyjmujemy wielomian

$$c(x) := c'(x) - r(x) = x^{n-k}u(x) - r(x).$$

Jeśli $\mathcal{C}$ jest kodem cyklicznym długości n generowanym przez wielomian $g(x)$, to $g(x) \mid x^n - 1$ a wielomian

$$h(x) := \frac{x^n - 1}{g(x)} = \sum_{i=0}^{k} h_i x^i,$$

jest stopnia k ($h_k \neq 0$).

Niech $c(x) \in \mathcal{C} = (g(x))$. Stąd $g(x) \mid c(x)$ i istnieje wielomian $f(x) \in R_n$ taki, że $c(x) = f(x)g(x)$. Stąd

$$c(x)h(x) = f(x)g(x)h(x) = f(x)(x^n - 1) \equiv_{R_n} 0.$$

Zatem w pierścieniu R_n wielomian $h(x)$ jest ortogonalny do każdego wielomianu $c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \in \mathcal{C}$. Oznacza to, że współczynniki $\sum_{i=0}^{j} c_{j-i}h_i$ przy x^j w iloczynie $c(x)h(x)$ dla $j = 0, 1, \ldots, n-1$, są równe 0. Ponieważ dla $i > k$, $h_i = 0$, to w szczególności dla $j = k, \ldots, n-1$ współczynniki c_i muszą spełniać następujący układ $n - k$ - równań:

$$\begin{array}{r}c_0h_k + c_1h_{k-1} + \cdots + c_{k-1}h_1 + \cdots + c_kh_0 = 0\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ c_{n-k-2}h_k + c_{n-k-1}h_{k-1} + \cdots + c_{n-3}h_1 + \cdots + c_{n-2}h_0 = 0\\ c_{n-k-1}h_k + c_{n-k-2}h_{k-1} + \cdots + c_{n-2}h_1 + \cdots + c_{n-1}h_0 = 0\end{array} \qquad (7)$$

Układ (7) można zapisać w postaci macierzowej.

$$Hc = \begin{pmatrix} h_k & h_{k-1} & \ldots & \ldots & h_1 & h_0 & 0 & \ldots & 0\\ \ldots & h_k & h_{k-1} & \ldots & \ldots & h_1 & h_0 & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ 0 & \ldots & \ldots & h_k & h_{k-1} & \ldots & h_1 & h_0 & 0\\ 0 & \ldots & \ldots & \ldots & h_k & h_{k-1} & \ldots & h_1 & h_0 \end{pmatrix} \begin{pmatrix} c_0\\ c_1\\ \vdots\\ c_{n-1}\end{pmatrix} = \begin{pmatrix} 0\\ 0\\ \vdots\\ 0\end{pmatrix}.$$

Zatem, jeśli $c \in \mathcal{C}$ to $Hc = \mathbf{0}$. Ponadto, $h_k \neq 0$ czyli rząd macierzy H równy jest $n-k$. Ponieważ stopień wielomianu generującego $g(x)$ równy jest $n-k$ to wymiar kodu wynosi k. Warunek $Hc = \mathbf{0}$ jest więc wystarczający na to, by $c \in \mathcal{C}$. Stąd macierz H jest macierzą kontroli parzystości kodu cyklicznego $\mathcal{C} = (g(x))$. Wielomian $h(x)$ nazywamy *wielomianem sprawdzającym* kodu $\mathcal{C}$.

Jeśli współrzędne $c_{n-k}, \ldots, c_{n-1}$ wektora $c = (c_0, c_1, \ldots, c_{n-k-1}, c_{n-k}, \ldots, c_{n-1})$ przyjmiemy jako symbole wiadomości, to układ (7) jednoznacznie definiuje symbole sprawdzające: $c_0, \ldots, c_{n-k-1}$.

Kody dualne do kodów cyklicznych

Niech $h(x) = h_0 + h_1x + \cdots + h_kx^k$ będzie wielomianem sprawdzającym kodu cyklicznego $\mathcal{C}$ generowanego przez wielomian $g(x)$ stopnia $n-k$ i niech

$$g^{\perp}(x) := x^k h(x^{-1}) = x^k h(x^{-1}) = h_0x^k + h_1x^{k-1} + \cdots + h_k$$

będzie wielomianem generującym kodu cyklicznego $\mathcal{C}^\perp$ wymiaru $n-k$. Wówczas macierz generująca $G^\perp$ kodu $\mathcal{C}^\perp$ ma postać:

$$G^\perp = \begin{pmatrix} h_k & 0 & 0 & \dots & 0 \\ h_{k-1} & h_k & 0 & \dots & 0 \\ h_{k-2} & h_{k-1} & h_k & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ h_0 & h_1 & h_2 & \dots & \dots \\ 0 & h_0 & h_1 & \dots & \dots \\ 0 & 0 & h_0 & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & h_0 \end{pmatrix}.$$

Ponieważ $g \in \mathcal{C}$, na mocy układu (7) współrzędne wielomianu $g(x) = g_0 + g_1 x + \cdots + g_{n-1}x^{n-1}$ spełniają dla każdego $0 \leqslant t \leqslant n-k-1$ równania

$$g_t h_k + g_{t+1}h_{k-1} + \cdots + g_{t+k}h_0 = 0.$$

Oznacza to, że każda kolumna macierzy G jest ortogonalna do każdej kolumny macierzy $G^\perp$. Zatem macierz $G^\perp$ jest macierzą generującą kodu ortogonalnego $\mathcal{C}^\perp$ do kodu $\mathcal{C}$.

Twierdzenie 6.7. *Niech $\mathcal{C} = (g(x))$ będzie kodem cyklicznym generowanym przez wielomian $g(x)$. Kod dualny $\mathcal{C}^\perp$ do kodu $\mathcal{C}$ jest również kodem cyklicznym. Wielomian*

$$g^\perp(x) := x^{\mathrm{st}h(x)}h(x^{-1}),$$

gdzie $x^n - 1 = h(x)g(x)$, jest jego wielomianem generującym.

Cykliczny kod $\mathcal{C}_1 = (h(x))$ jest równoważny z kodem $\mathcal{C}^\perp = (g^\perp(x))$, gdyż zawiera wszystkie słowa kodowe kodu $\mathcal{C}^\perp$ zapisane od tyłu.

Wielomiany minimalne

Twierdzenie 6.8. *Niech L będzie rozszerzeniem ciała F. Jeśli $\alpha \in L$ jest elementem algebraicznym nad F to istnieje unormowany wielomian nierozkładalny $M(x) \in F[x]$, którego pierwiastkiem jest α taki, że dla każdego wielomianu $w(x) \in F[x]$ spełniającego warunek $w(\alpha) = 0$, $M(x) \mid w(x)$.*

Definicja 6.9. *Wielomian $M(x) \in F[x]$ z twierdzenia (6.8) nazywamy* ***wielomianem minimalnym*** *elementu $\alpha \in L$ nad ciałem $F \subseteq L$.*

Lemat 6.10. 1. *Stopień wielomianu minimalnego $M(x) \in GF(p)[x]$ elementu $\beta \in GF(p^m)$ jest mniejszy bądź równy m.*
2. *Wielomian minimalny $M(x) \in GF(p)[x]$ elementu pierwotnego ciała $GF(p^m)$ ma stopień równy m.*
3. *Elementy β i β^p należące do ciała $GF(p^m)$ mają takie same wielomiany minimalne nad ciałem $GF(p)$.*
W szczególności elementy $\beta, \beta^2 \in GF(2^m)$ mają takie same wielomiany minimalne nad ciałem Z_2, .
4. *Jeśli $M(x) \in GF(p)[x]$ jest wielomianem minimalnym elementu $\beta \in GF(p^m)$ to $M(x) \mid x^{p^m} - x$ oraz $M(x) \mid x^{p^m-1} - 1$.*

Jeśli $f(x) \in GF(p)[x]$ jest wielomianem stopnia m nierozkładalnym nad ciałem $GF(p)$, to $GF(p)[x]/(f(x)) = GF(p^m) = GF(p)(\alpha)$, gdzie $f(\alpha) = 0$. Wówczas $f(x) \in GF(p)[x]$ jest wielomianem minimalnym elementu α.

Binarne kody Hamming'a są cykliczne

Niech α będzie generatorem cyklicznej grupy multiplikatywnej $GF^*(2^r)$ ciała $GF(2^r)$. Wówczas wszystkie elementy grupy $GF^*(2^r)$ można zapisać jako odpowiednie potęgi α lub przedstawić jednoznacznie w postaci $\sum_{i=0}^{r-1} a_i \alpha^i$, gdzie $a_i \in GF(2)$. Stąd każde $\alpha^j \in GF(2^r)$ można jednoznacznie reprezentować r-elementowym ciągiem o współczynnikach z ciała $GF(2)$. Zatem każdą z kolumn macierzy kontroli parzystości binarnego kodu Hamming'a $\mathcal{H}_r(2)$ można traktować jako element grupy $GF^*(2^r)$

$$H_r = \left(\ 1, \quad \alpha, \quad \alpha^2, \quad \ldots \quad , \alpha^{2^r-2} \ \right).$$

Wówczas dla $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$

$$c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{H}_r(2) \Leftrightarrow$$

$$H_r c = 0 \Leftrightarrow \sum_{i=0}^{n-1} c_i \alpha^i = 0 \Leftrightarrow c(\alpha) = 0.$$

Niech $M^{(1)}(x)$ będzie wielomianem minimalnym elementu pierwotnego $\alpha \in GF(2^r)$. Ponieważ $c(\alpha) = 0$ to $M^{(1)}(x) \mid c(x)$, a zatem $c(x) \in (M^{(1)}(x))$. Ponadto dla $d(x) \in (M^{(1)}(x))$, $d(\alpha) = 0$, czyli $d \in \mathcal{H}_r$.

Twierdzenie 6.11. *Dla każdego $r \geqslant 1$, binarny kod Hamming'a $\mathcal{H}_r(2)$ jest równoważny z kodem cyklicznym generowanym przez wielomian $g(x) = M^{(1)}(x)$.*

Pierwiastki z 1

Definicja 6.12. *Element $\alpha \in F$ ciała F nazywamy pierwiastkiem n-tego stopnia z 1, jeśli α jest pierwiastkiem wielomianu $x^n - 1$, tzn. $\alpha^n = 1$.*

Niech $\mu_n(F)$ oznacza podzbiór ciała F złożony ze wszystkich pierwiastków n-tego stopnia z 1.

Lemat 6.13. *Podzbiór $\mu_n(F)$ jest podgrupą grupy multiplikatywnej F^*.*

Przykład 6.14. Niech $F = GF(q)$ będzie ciałem skończonym o $q = p^l$ elementach i niech $n = q - 1$. Wówczas grupa multiplikatywna $GF^*(q)$ ciała $GF(q)$ ma rząd $q - 1$ i dla każdego $\alpha \in GF^*(q)$, $\alpha^{q-1} = 1$. Wobec tego $\mu_{q-1}(GF(q)) = GF^*(q)$. Ponieważ rząd tej grupy jest równy stopniu wielomianu $x^n - 1$, $GF(q)$ jest najmniejszym rozszerzeniem ciała $GF(p)$ zawierającym wszystkie pierwiastki tego wielomianu. □

Niech n i q będą liczbami naturalnymi takimi, że $NWD(n, q) = 1$.

Lemat 6.15. *Istnieje najmniejsza liczba całkowita $m \geqslant 0$ taka, że $q^m \equiv_n 1$.*

Liczbę m z lematu 6.15 nazywamy *rzędem liczby q modulo n.*
Niech m będzie rzędem liczby q modulo n. Ponieważ $n \mid q^m - 1$, to z definicji liczby m wynika, że $x^n - 1 \mid x^{q^m-1} - 1$, ale nie dzieli $x^{q^s-1} - 1$, dla $0 < s < m$. Zatem wszystkie pierwiastki wielomianu $x^n - 1$ leżą w rozszerzeniu $GF(q^m)$ ciała $GF(q)$ i w żadnym mniejszym.

Wniosek 6.16. *Najmniejszym rozszerzeniem ciała $GF(q)$, w którym leżą wszystkie pierwiastki wielomianu $x^n - 1$ jest ciało $GF(q^m)$, gdzie m jest rzędem liczby q modulo n.*

Na mocy lematu 6.16, $x^{q^m-1} - 1 = t(x)(x^n - 1)$ dla pewnego wielomianu $t(x)$. Ponieważ w ciele $GF(q^m)$ wielomian $x^{q^m-1} - 1$ ma $q^m - 1$ różnych pierwiastków (każdy element grupy multiplikatywnej ciała $GF(q^m)$ jest pierwiastkiem tego wielomianu) zatem również wielomian $x^n - 1$ ma n różnych pierwiastków w tym ciele. Ponadto każda podgrupa grupy cyklicznej jest grupą cykliczną.

Wniosek 6.17. *Podgrupa $\mu_n(GF(q^m))$ grupy $GF^*(q^m)$ jest grupą cykliczną.*

Definicja 6.18. *Generator grupy $\mu_n(GF(q^m))$ nazywamy pierwotnym n-tym pierwiastkiem z 1.*

Przykład 6.19. Jeśli $n = q^m - 1$, to pierwotny n-ty pierwiastkiem z 1 jest elementem pierwotnym ciała $GF(q^m)$ i $\mu_n(GF(q^m)) = GF^*(q^m)$. □

Twierdzenie 6.20. *Niech $NWD(m, q-1) = 1$ i niech $n = \frac{q^r-1}{q-1}$. Wówczas kod Hamming'a $\mathcal{H}_m(q)$ jest równoważny z kodem cyklicznym $\mathcal{C} = (M(x))$, gdzie $M(x)$ jest wielomianem minimalnym pierwotnego n-tego pierwiastka z 1.*

Niech $\alpha \in GF(q^m)$ będzie pierwotnym n-tym pierwiastkiem z 1. Wówczas

$$x^n - 1 = \prod_{i=0}^{n-1}(x - \alpha^i).$$

Niech $\mathcal{C} = (g(x))$ będzie kodem cyklicznym długości n nad ciałem $GF(q)$, którego $g(x)$ jest wielomianem generującym. Ponieważ $g(x)$ jest podzielnikiem wielomianu $x^n - 1$, zatem w ciele $GF(q^m)$

$$g(x) = \prod_{i \in K}(x - \alpha^i),$$

gdzie $K \subseteq \{0, \ldots, n-1\}$.

Definicja 6.21. *n-ty pierwiastek z jedynki należący do zbioru $\{\alpha^i \mid i \in K\}$ nazywamy zerem kodu $\mathcal{C} = (g(x))$. Pozostałe n-te pierwiastki z 1 nazywamy niezerami tego kodu.*

Niezera kody $\mathcal{C} = (g(x))$ są zerami wielomianu $h(x) = \frac{x^n-1}{g(x)}$. Ponadto, jeśli $c(x) \in R_n$, to $c(x) \in \mathcal{C} \Leftrightarrow c(\alpha^i) = 0$ dla każdego $i \in K$.

Twierdzenie 6.22. *Niech α będzie pierwotnym n-tym pierwiastkiem z 1 w ciele $GF(q^m)$. Niech $\mathcal{C} = (g(x))$ będzie kodem cyklicznym długości n z wielomianem generującym $g(x)$ takim, że dla pewnych liczb całkowitych $b \geqslant 0$ i $\delta \geqslant 1$*

$$g(\alpha^b) = g(\alpha^{b+1}) = \cdots = g(\alpha^{b+\delta-2}) = 0.$$

(tzn. kod ma ciąg $\delta - 1$ kolejnych potęg α jako zera.) Wówczas odległość kodu $\mathcal{C}$ jest większa bądź równa δ.

Wniosek 6.23. *Niech $NWD(r, n) = 1$. Kod cykliczny długości n z zerami α^b, α^{b+r}, α^{b+2r}, $\ldots$, $\alpha^{b+(\delta-2)r}$ ma odległość większą bądź równą δ.*

7 Kody BCH

Kody BCH są rodziną kodów cyklicznych poprawiających błędy wielokrotne. Zostały skonstruowane jako uogólnienie kodów Hamming'a, które poprawiają tylko błędy pojedyncze. Po raz pierwszy opisali je na początku lat 60-tych R.C.Bose i D.K.Ray-Chaudhuri oraz niezależnie A.Hocquenghema. Mają ogromne znaczenie praktyczne, szczególnie w sytuacjach, gdy spodziewana liczba błędów jest niewielka w porównaniu z długością kodu.

Binarny kod Hamming'a długości $n = 2^r - 1$ potrzebował r symboli kontrolnych, aby poprawić jeden błąd. Można przypuszczać, że będzie potrzebnych dwa razy więcej symboli kontrolnych, aby poprawiać błędy podwójne. Skonstruujmy macierz H_{BCH} kontroli parzystości binarnego kodu BCH poprawiającego dwa błędy przez dodanie r wierszy do macierzy H_r kodu Hamming'a $\mathcal{H}_r(2)$. Niech i-ta kolumna nowej macierzy H_{BCH} ma postać:

$$H^i_{BCH} = \begin{pmatrix} \alpha^i \\ \varphi(\alpha^i) \end{pmatrix},$$

gdzie gdzie α jest elementem pierwotnym w ciele $GF(2^r)$ oraz $\varphi(\alpha^i) \in GF(2^r)$.

Jeśli przy przesyłaniu informacji wystąpiły dwa błędy na pozycji i oraz j to syndrom otrzymanego wektora v wynosi:

$$H_{BCH}v = H^i_{BCH} + H^j_{BCH} = \begin{pmatrix} \alpha^i + \alpha^j \\ \varphi(\alpha^i) + \varphi(\alpha^j) \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}.$$

Chcąc wykryć oba błędy musimy tak dobrać funkcję φ, aby dekoder "mógł" obliczyć pozycje i oraz j znając wartość syndromu, czyli z_1 i z_2. Oznacza to, że dla danych $z_1, z_2 \in GF(2^r)$ następujący układ równań:

$$\begin{aligned} \alpha^i + \alpha^j &= z_1 \\ \varphi(\alpha^i) + \varphi(\alpha^j) &= z_2 \end{aligned}$$

ma mieć rozwiązania.

Jeśli na przykład przyjęlibyśmy, że $\varphi(\alpha^i) = c\alpha^i$, gdzie c jest pewną stałą, to układ

$$\begin{aligned} \alpha^i + \alpha^j &= z_1 \\ c(\alpha^i + \alpha^j) &= z_2, \end{aligned}$$

nie miałby rozwiązań dla dowolnych z_1 i z_2.

Jeśli natomiast przyjęlibyśmy, że $\varphi(\alpha^i) = \alpha^{2i}$, to układ

$$\begin{aligned} \alpha^i + \alpha^j &= z_1 \\ \alpha^{2i} + \alpha^{2j} &= z_2, \end{aligned}$$

również nie miałby rozwiązań dla dowolnych z_1 i z_2, gdyż w ciele $GF(2^r)$, $\alpha^{2i} + \alpha^{2j} = (\alpha^i + \alpha^j)^2 = z_1^2$ i równania

$$\begin{aligned} \alpha^i + \alpha^j &= z_1 \\ \alpha^{2i} + \alpha^{2j} &= z_2, \end{aligned}$$

są sprzeczne dla $z_2 \neq z_1^2$.

Niech zatem $\varphi(\alpha^i) = \alpha^{3i}$. Wtedy układ równań

$$\begin{aligned} \alpha^i + \alpha^j &= z_1 \neq 0 \\ \alpha^{3i} + \alpha^{3j} &= z_2 \end{aligned}$$

posiada rozwiązanie. Ponadto

$$z_2 = \alpha^{3i} + \alpha^{3j} = (\alpha^i + \alpha^j)(\alpha^{2i} + \alpha^i\alpha^j + \alpha^{2j}) = z_1(z_1^2 + \alpha^i\alpha^j),$$

a stąd

$$\alpha^i\alpha^j = \frac{z_2}{z_1} + z_1^2.$$

Zauważmy, że α^i oraz α^j są dla $z_1 \neq 0$ pierwiastkami następującego równania:

$$f(x) = (x + \alpha^i)(x + \alpha^j) = x^2 + \alpha^j x + \alpha^i x + \alpha^i\alpha^j = x^2 + z_1 x + \frac{z_2}{z_1} + z_1^2 = 0,$$

a stąd α^{-i} oraz α^{-j} są pierwiastkami równania

$$\sigma(x) := x^2 f(x^{-1}) = 0.$$

Macierz H_{BCH} kontroli parzystości binarnego BCH kodu możemy zapisać następująco:

$$H_{BCH} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^r-2} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(2^r-2)} \end{pmatrix}.$$

Zauważmy, że w drugim wierszu macierzy H_{BCH} nie muszą wystąpić wszystkie elementy ciała, gdyż α^3 nie musi być elementem pierwotnym.

Jeśli w czasie przesyłania nie nastąpił błąd oznacza to, że $z_1 = z_2 = 0$. Jeśli popełniony został jeden błąd na pozycji i ($j = 0$), to $\alpha^i = z_1$ oraz $z_2 = \alpha^{3i} = z_1^3$. Zatem możemy przyjąć następującą strategię dekodowania dla binarnego kodu BCH poprawiającego błędy podwójne. Załóżmy, że po przesłaniu przez kanał transmisyjny otrzymujemy wektor y i obliczamy jego syndrom $H_{BCH}y = \begin{pmatrix} z_1 \\ z_2. \end{pmatrix}$

1. Jeśli $z_1 = z_2 = 0$, przyjmujemy, że w czasie transmisji nie nastąpił żaden błąd a wielomian $\sigma(x) := 0$.

2. Jeśli $z_1 \neq 0$, $z_2 = z_1^3$, poprawiamy pojedynczy błąd na pozycji i, gdzie $\alpha^i = z_1$. Wówczas $\sigma(x) = 1 + z_1 x$.

3. Jeśli $z_1 \neq 0$, $z_2 \neq z_1^3$, tworzymy równanie $\sigma(x) = 1 + z_1 x + (\frac{z_2}{z_1} + z_1^2)x^2 = 0$. Jeśli ma ono dwa różne pierwiastki α^{-i} i α^{-j}, poprawiamy błędy na pozycjach i oraz j.

4. Jeśli równanie $1 + z_1 x + (\frac{z_2}{z_1} + z_1^2)x^2 = 0$ nie ma rozwiązań lub jeśli $z_1 = 0$ i $z_2 \neq 0$, stwierdzamy, że zostały popełnione co najmniej 3 błędy.

Tak skonstruowany binarny BCH kod $\mathcal{C}$ jest kodem cyklicznym. Niech $n = 2^r - 1$ oraz $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. Wówczas

$$c \in \mathcal{C} \Leftrightarrow H'c = 0 \Leftrightarrow \sum_{i=0}^{n-1} c_i \alpha^i = 0 \text{ i } \sum_{i=0}^{n-1} c_i \alpha^{3i} = 0 \Leftrightarrow$$

$$c(\alpha) = 0 \text{ i } c(\alpha^3) = 0 \Leftrightarrow M^{(1)}(x) \mid c(x) \text{ i } M^{(3)}(x) \mid c(x) \Leftrightarrow$$
$$NWW(M^{(1)}(x), M^{(3)}(x)) \mid c(x),$$

gdzie $M^{(1)}(x)$ jest wielomianem minimalnym elementu pierwotnego α natomiast $M^{(3)}(x)$ jest wielomianem minimalnym elementu α^3 w ciele $GF(2^r)$.

Lemat 7.1. *Minimalna odległość binarnego BCH kodu długości $n = 2^r - 1$ poprawiającego dwa błędy równa jest 5.*

Twierdzenie 7.2. *Niech $r \geqslant 3$. Binarny BCH kod długości $n = 2^r - 1$ poprawiający błędy podwójne jest $(n = 2^r - 1, k = n - 2r, 5)$-kodem cyklicznym z wielomianem generującym $g(x) = NWW(M^{(1)}(x), M^{(3)}(x))$, gdzie $M^{(1)}(x)$ jest wielomianem minimalnym elementu pierwotnego $\alpha \in GF(2^r)$ natomiast $M^{(3)}(x)$ jest wielomianem minimalnym elementu $\alpha^3 \in GF(2^r)$.*

Niech jak poprzednio m będzie rzędem q modulo n, α będzie pierwotnym n-tym pierwiastkiem z jedynki w ciele $GF(q^m)$ i niech $M^{(i)}(x)$ będzie wielomianem minimalnym elementu $\alpha^i \in GF(q^m)$.

Definicja 7.3. *Kod cykliczny $\mathcal{C} = (g(x))$ długości n nad ciałem $GF(q)$ jest kodem BCH o zadanej odległości δ jeśli, dla pewnego $b \in \mathbb{Z}$, $b \geqslant 0$,*

$$g(x) = NWW(M^{(b)}(x), M^{(b+1)}(x), \ldots, M^{(b+\delta-2)}(x)).$$

Zatem wielomian generujący $g(x) \in GF(q)[x]$ kodu $\mathcal{C}$ jest unormowanym wielomianem o najniższym stopniu, dla którego α^b, α^{b+1}, $\ldots$, $\alpha^{b+\delta-2}$ są zerami. Czyli BCH kod $\mathcal{C} = (M^{(b)}(x)) \cap (M^{(b+1)}(x)) \cap \cdots \cap (M^{(b+\delta-2)}(x))$ jest największym kodem o tej własności.

Ponieważ

$$c \in \mathcal{C} \Leftrightarrow c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+\delta-2}) = 0 \tag{8}$$

to macierz kontroli parzystości dla kodu $\mathcal{C}$ ma postać:

$$H_{BCH} = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \ldots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \ldots & \alpha^{(n-1)(b+1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \ldots & \alpha^{(n-1)(b+\delta-2)} \end{pmatrix}.$$

Kod $\mathcal{C}$ ma ciąg $\delta - 1$ kolejnych potęg α jako zera. Na mocy twierdzenia 6.22 odległość kodu jest większa bądź równa zadanej odległości δ, czyli taki kod poprawia do $t = [\frac{\delta-1}{2}]$ błędów. Ponieważ stopień wielomianu minimalnego elementu należącego do ciała $GF(q^m)$ jest zawsze mniejszy bądź równy m to $\mathrm{st} g(x) = n - k \leqslant m(\delta - 1)$.

Twierdzenie 7.4. *Kod BCH nad ciałem $GF(q)$ długości n i zadanej odległości δ ma odległość $d \geqslant \delta$ a wymiar większy bądź równy $n - m(\delta - 1)$.*

Jeśli $b = 1$ to takie kody są nazywane kodami BCH w wąskim sensie.

Jeśli $n = q^m - 1$ to takie kody są nazywane pierwotnymi kodami BCH. (W tym przypadku α jest nie tylko pierwotnym n-tym pierwiastkem z 1, ale jest elementem pierwotnym ciała $GF(q^m)$.)

Ponieważ każdy element ciała $GF(q^m)$ można przedstawić jednoznacznie w postaci $\sum_{i=0}^{m-1} a_i\alpha^i$, gdzie $a_i \in GF(q)$, zatem każdy BCH kod nad ciałem $GF(q^m)$ można zdefiniować jako kod nad ciałem $GF(q)$ zastępując każdy element $\alpha^j \in GF(q^m)$ odpowiadającym mu m-elementowym ciągiem o współczynnikach z ciała $GF(q)$.

Binarne kody BCH

W przypadku, gdy $q = 2$ stopień wielomianu $g(x)$ generującego kod BCH można zredukować, gdyż $M^{(2i)}(x) = M^i(x)$.

Dla $b = 1$ możemy zawsze założyć, że zadana odległość δ jest nieparzysta, ponieważ kody z zadaną odległością $2t$ i $2t+1$ pokrywają się. Oba mają taki sam wielomian generujący:

$$g(x) = NWW(M^{(1)}(x), M^{(3)}(x), \ldots, M^{(2t-1)}(x)).$$

Stąd st$g(x) \leqslant mt$ i wymiar kodu jest większy bądź równy $n - mt$ a macierz kontroli parzystości ma postać:

$$H_{BCH} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \ldots & \alpha^{3(n-1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^{2t-1} & \alpha^{2(2t-1)} & \ldots & \alpha^{(n-1)(2t-1)} \end{pmatrix}.$$

Twierdzenie 7.5. *Pierwotny kod BCH w wąskim sensie nad ciałem Z_2 długości $n = 2^m - 1$ i zadanej odległości $\delta = 2t + 1$ ma minimalną odległość $d \geqslant \delta$ a wymiar większy bądź równy $n - mt$.*

Przykład 7.6. *Binarne $(n = 2^r - 1, n - r, 3)$-kody Hamming'a $\mathcal{H}_r(2)$ są szczególnym przypadkiem BCH kodów dla $q = 2$, $b = 1$ i $t = 1$.*

Następujący wniosek pokazuje, dlaczego kody BCH są tak ważne z praktycznego punktu widzenia.

Wniosek 7.7. *Dla dowolnych dodatnich liczb całkowitych m i $t \leqslant 2^{m-1}-1$, istnieje binarny BCH kod długości $n = 2^m - 1$, który koryguje t błędów i ma wymiar większy bądź równy $n - mt$.*

Okazuje się, że faktyczne wartości k i d niewiele odbiegają od podanych ograniczeń.

Twierdzenie 7.8. (Peterson)
Jeśli $n = ab$ to binarny BCH kod w wąskim sensie długości n i zadanej odległości $\delta = a$ ma odległość równą dokładnie a.

Twierdzenie 7.9. *BHC kod długości $n = q^m - 1$ i zadanej odległości $\delta = q^h - 1$ nad ciałem $GF(q)$ ma faktyczną odległość równą δ.*

Znanych jest wiele podobnych twierdzeń, ale nie jest znany warunek konieczny i wystarczający na długość n i zadaną odległość δ, aby faktyczna odległość kodu $d = \delta$. Można natomiast podać górne ograniczenie na rzeczywistą odległość kodu BCH.

Twierdzenie 7.10. *Faktyczna odległość d kodu BCH nad ciałem $GF(q)$, o zadanej odległości δ jest co najwyżej równa $q\delta - 1$.*

Można także sformułować twierdzenia podające faktyczny wymiar kodu.

Twierdzenie 7.11. *Niech $\mathcal{C}$ będzie binarnym BCH kodem długości $n = 2^m - 1$ i zadanej odległości $\delta = 2t + 1$, gdzie*

$$2t - 1 < 2^{\lceil \frac{m}{2} \rceil} + 1.$$

Wówczas wymiar kodu $\mathcal{C}$ wynosi $2^m - 1 - mt$.

Niech $I(n, \delta)$ oznacza wymiar BCH kodu długości n i zadanej odległości δ.

Twierdzenie 7.12. (Mann)
Niech $\mathcal{C}$ będzie BCH kodem w wąskim sensie nad ciałem $GF(q)$ o długości $n = q^m - 1$ i zadanej odległości $\delta = q^\lambda$. Wówczas

$$I(q^m - 1, q^\lambda) \leqslant \sum_{i=0}^{m-\lambda} a_i \varrho_i^m,$$

gdzie liczby całkowite dodatnie $a_0, \ldots, a_{m-\lambda}, \varrho_0, \ldots \varrho_{m-\lambda}$ zależą od $m - \lambda$ (ale nie od m) i spełniają zależność $|\varrho_i| < q$.

Kody BCH dla małych długości, do kilku tysięcy, są wśród najlepszych kodów jakie znamy. Niestety ich skuteczność pogarsza się, gdy długość kodu dąży do nieskończoności.

Definicja 7.13. *Powiemy, że rodzina kodów nad ciałem $GF(q)$, dla ustalonego q, jest dobra, jeśli zawiera nieskończony ciąg $(\mathcal{C}_n)$ liniowych $(n, k(n), d(n))$-kodów $\mathcal{C}_n$ taki, że współczynnik informacji $R_n = \frac{k(n)}{n}$ oraz $\frac{d(n)}{n}$ dążą do niezerowych granic, gdy $n \to \infty$.*

Niestety, pierwotne kody BCH nie mają tej własności.

Twierdzenie 7.14. *Nie istnieje nieskończony ciąg pierwotnych BCH kodów nad ciałem $GF(q)$ taki, że oba współczynniki $\frac{d(n)}{n}$ i $\frac{k(n)}{n}$ są ograniczone z dołu przez wartość niezerową.*

Chociaż długie kody BCH są złe, to niewiele wiadomo o "dobroci" innych długich kodów cyklicznych.

Dekodowanie binarnych kodów BCH

Kody BCH są praktyczne również z tego względu, że istnieją efektywne algorytmy ich dekodowania.

Niech $\mathcal{C}$ będzie binarnym pierwotnym (n, k)-kodem BCH w wąskim sensie z zadaną odległością $\delta = 2t + 1$. Załóżmy, że przesyłamy słowo kodowe $c = c_0c_1 \dots c_{n-1}$ i w wyniku transmisji otrzymujemy wektor $y = c + e$, gdzie $e = e_0e_1 \dots e_{n-1}$ jest wektorem błędu. Proces dekodowania możemy podzielić na 3 etapy:

- Znalezienie syndromu wektora y.
- Znalezienie tzw. wielomianu lokalizacji $\sigma(x)$.
- Znalezienie pierwiastków wielomianu $\sigma(x)$.

Niech jak poprzednio α będzie elementem pierwotnym ciała $GF(2^m)$ i niech $c(x) = \sum_{i=0}^{n-1} c_i x^i$, $e(x) = \sum_{i=0}^{n-1} e_i x^i$ oraz $y(x) = \sum_{i=0}^{n-1} y_i x^i$..

Obliczanie syndromu.
Macierz kontroli parzystości kodu $\mathcal{C}$ ma postać:

$$H_{BCH} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{\delta-2} & \alpha^{2(\delta-2)} & \dots & \alpha^{(n-1)(\delta-2)} \end{pmatrix}.$$

Syndrom wektora y jest zatem równy:

$$H_{BCH}y = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{\delta-2} & \alpha^{2(\delta-2)} & \dots & \alpha^{(n-1)(\delta-2)} \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{pmatrix} =$$

$$\begin{pmatrix} \sum_{i=0}^{n-1} y_i\alpha^i \\ \sum_{i=0}^{n-1} y_i\alpha^{3i} \\ \vdots \\ \sum_{i=0}^{n-1} y_i\alpha^{(\delta-2)i} \end{pmatrix} = \begin{pmatrix} y(\alpha) \\ y(\alpha^3) \\ \vdots \\ y(\alpha^{\delta-2}) \end{pmatrix} = \begin{pmatrix} A_1 \\ A_3 \\ \vdots \\ A_{\delta-2} \end{pmatrix},$$

gdzie $A_l = y(\alpha^l)$. Można łatwo obliczyć wartość A_l znając wektor y. Niech $M^{(l)}(x)$ będzie wielomianem minimalnym elementu α^l. Wówczas

$$y(x) = Q(x)M^{(l)}(x) + R(x),$$

gdzie st$R(x)$ <st$M^{(l)}(x)$. Ponieważ $M^{(l)}(\alpha^l) = 0$, zatem $A_l = y(\alpha^l) = R(\alpha^l)$.

Zauważmy ponadto, że $A_{2r} = y(\alpha^{2r}) = [y(\alpha^r)]^2 = A_r^2$. Stąd $A_2 = A_1^2$, $A_4 = A_2^2$, $\dots$, $A_{\delta-1} = A^2_{\frac{\delta-1}{2}}$.

Szukanie wielomianu lokalizacji.
W przypadku binarnego BCH kodu poprawiającego błędy podwójne, aby obliczyć pozycje i oraz j, na których został popełniony błąd, zdefiniowaliśmy równanie kwadratowe $\sigma(x) = 0$, którego pierwiastkami były α^{-i} oraz α^{-j}. Ogólnie, w przypadku kodu BCH poprawiajacego t błędów również będziemy szukać wielomianu (tzw. wielomianu lokalizacji), którego pierwiastki wskażą pozycje, na których zostały popełnione błędy. Załóżmy, że wektor błędu e ma wagę w i zawiera niezerowe elementy (jedynki) na pozycjach $r_1, \dots, r_w$.

Definicja 7.15. ***Wielomianem lokalizacji*** *nazywamy wielomian*

$$\sigma(x) := \prod_{i=1}^{w}(1 - \alpha^{r_i}x) = \sum_{i=0}^{w}\sigma_i x^i.$$

Zauważmy, że $\sigma_0 = 1$ oraz dla $1 \leqslant l \leqslant \sigma - 1$,

$$A_l = y(\alpha^l) = c(\alpha^l) + e(\alpha^l) = e(\alpha^l).$$

Zatem

$$A_l = \sum_{i=1}^{w}\alpha^{lr_i}.$$

Aby znaleźć wielomian $\sigma(x)$ należy obliczyć współczynniki σ_i. Stosowane są w tym celu różne techniki. Jedną z nich jest wykorzystanie tzw. równań Newtona. Okazuje się bowiem, że współczynniki σ_i i A_l są w przypadku binarnym związane następującym układem równań:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ A_2 & A_1 & 1 & 0 & 0 & \dots & 0 \\ A_4 & A_3 & A_2 & A_1 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ A_{2w-2} & A_{2w-3} & \dots & \dots & \dots & \dots & A_{w-1} \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \\ \vdots \\ \sigma_w \end{pmatrix} = \begin{pmatrix} A_1 \\ A_3 \\ A_5 \\ \vdots \\ A_{2w-1} \end{pmatrix}.$$

Twierdzenie 7.16. (Peterson) *Niech* $A_l = \sum_{i=1}^{w}\alpha^{lr_i}$ *i niech*

$$M_v = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ A_2 & A_1 & 1 & 0 & 0 & \dots & 0 \\ A_4 & A_3 & A_2 & A_1 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ A_{2v-4} & A_{2v-5} & \dots & \dots & \dots & \dots & A_{v-3} \\ A_{2v-2} & A_{2v-3} & \dots & \dots & \dots & \dots & A_{v-1} \end{pmatrix} \in M_v^v.$$

Wówczas:

1. *Jeśli* $w = v$ *lub* $w = v - 1$, *to* $detM_v \neq 0$.
2. *Jeśli* $w < v - 1$, *to* $detM_v = 0$.

Stosując powyższe twierdzenie możemy przyjąć następującą procedurę dekodowania. Załóżmy, że przy transmisji nastąpiło t błędów i w układzie

równań Newtona podstawmy $w = t$. Na mocy twierdzenia Petersona, jeśli wystąpiło t lub $t-1$ błędów, to istnieje rozwiązanie tego układu i możemy próbować je znaleźć. Jeśli jednak wystąpiło mniej niż $t-1$ błędów, układ nie ma rozwiązań. Wtedy zakładamy, że nastąpiły $t-2$ błędy, zastępujemy w układzie równań Newtona w przez $t-2$ i ponownie próbujemy rozwiązać układ. Procedurę należy powtarzać, aż zostanie znalezione rozwiązanie dla pewnego t.

Trudność tej metody polega na tym, że wymaga wielokrotnego wyliczania wyznacznika wysokiego stopnia nad $GF(2^m)$. Jeśli zatem t jest duże, stosuje się inne metody, np. wykorzystuje się inne równania opisujące związki σ_i i A_l.

Znajdywanie pierwiastków wielomianu lokalizacji $\sigma(x)$.
Pierwiastkami wielomianu lokalizacji $\sigma(x) = \prod_{i=1}^{w}(1 - \alpha^{r_i}x)$, gdzie w jest liczbą popełnionych błędów na pozycjach $r_1, \ldots, r_w$ są $x_i = \alpha^{-r_i}$.

Znajdując pierwiastki wielomianu $\sigma(x)$ znajdujemy pozycje, na których został popełniony błąd, gdyż błąd wystąpił na pozycji i wtw, gdy $\sigma(\alpha^{-i}) = 0$.

Jeśli stopień wielomianu $\sigma(x)$ jest równy 1 lub 2 to jego pierwiastki łatwo obliczyć bezpośrednio. W przypadku ogólnym, najprościej jest sprawdzać wszystkie potęgi α.

Algorytm opisany powyżej poprawia tylko t lub mniej błędów w BCH kodzie binarnym o zadanej odległości $2t+1$. Znane są również pełne algorytmy dla wszystkich kodów BCH poprawiających błędy podwójne i dla pewnych poprawiających błędy potrójne. Aby zastosować algorytm dekodowania dla kodów niebinarnych należy w celu znalezienia wielomianu lokalizacji zastosować inne równania opisujące zależności σ_i i A_l. Nadal jednak otwarty pozostaje problem znalezienia pełnego algorytmu dekodującego dla wszystkich kodów BCH.

Rozwiązywanie równań kwadratowych nad ciałem $GF(2^m)$

Ciało $GF(p^m)$ jest przestrzenią wektorową wymiaru m nad ciałem $GF(p)$. Jeśli $f(x)$ jest wielomianem minimalnym elementu pierwotnego α ciała $GF(p^m) = GF(p)[x]/(f(x))$ to bazą jest zbiór $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$. Ale możliwe są także inne postaci bazy.

Twierdzenie 7.17. *Każde ciało $GF(p^m)$ zawiera taki element pierwotny γ, że $\{\gamma, \gamma^p, \gamma^{p^2}, \ldots, \gamma^{p^{m-1}}\}$ jest jego bazą.*

Bazę $\{\gamma, \gamma^p, \gamma^{p^2}, \ldots, \gamma^{p^{m-1}}\}$ nazywamy *bazą normalną* ciała $GF(p^m)$. Wówczas dowolny element $\beta \in GF(p^m)$ można zapisać w postaci:

$$\beta = b_0\gamma + b_1\gamma^2 + b_2\gamma^4 + \cdots + b_{m-1}\gamma^{2^{m-1}},$$

gdzie $b_i \in GF(p)$.

Przykład 7.18. Bazą normalną ciała $GF(4) = Z_2[x]/(x^2+x^1) = \{0, 1, \alpha, \alpha+1\}$ jest zbiór $\{\alpha, \alpha^2\}$. □

Definicja 7.19. *Śladem elementu $\beta \in GF(p^m)$ nazywamy sumę*

$$T_m(\beta) := \beta + \beta^p + \cdots + \beta^{p^{m-1}} = \sum_{j=0}^{m-1} \beta^{p^j} \in GF(p^m).$$

Lemat 7.20. *Niech $\{\gamma, \gamma^p, \gamma^{p^2}, \ldots, \gamma^{p^{m-1}}\}$ będzie bazą normalną ciała $GF(p^m)$ i niech $\beta = b_0\gamma + b_1\gamma^2 + b_2\gamma^4 + \cdots + b_{m-1}\gamma^{2^{m-1}} \in GF(p^m)$, $b_0, \ldots, b_{m-1} \in GF(p)$. Wówczas*

1. $[T_m(\beta)]^p = T_m(\beta^p) = T_m(\beta)$,
2. $T_m(\beta) \in GF(p)$,
3. $T_m(x+y) = T_m(x) + T_m(y)$, dla $x, y \in GF(p^m)$.
   W szczególności w ciele $GF(2^m)$
4. $T_m(\gamma) = 1$,
5. $T_m(\beta) = b_0 + b_1 + \cdots + b_{m-1}$,
6. $T_m(1) \equiv_2 m$.

Twierdzenie 7.21. *Równanie kwadratowe*

$$x^2 + x + \beta = 0, \quad \beta \in GF(2^m)$$

ma w ciele $GF(2^m)$ dwa pierwiastki, jeśli $T_m(\beta) = 0$ i nie ma pierwiastków, jeśli $T_m(\beta) = 1$.

Wniosek 7.22. *Jeśli* $T_m(\beta) = 0$, *to* $x^2 + x + \beta = (x + \xi)(x + \eta)$, *dla pewnych* $\xi, \eta \in GF(2^m)$.
Jeśli $T_m(\beta) = 1$, *to* $x^2 + x + \beta$ *jest wielomianem nierozkładalnym nad ciałem* $GF(2^m)$.

Twierdzenie 7.23. *Pierwotne binarne BCH kody w wąskim sensie są kodami quasi-doskonałymi.*

8 Kody Reed-Solomona (RS-kody)

Niech $q \neq 2$ będzie dodatnią liczbą pierwszą.

Definicja 8.1. *Reed-Solomon (lub krótko RS)* (N, K, D)*-kodem* $\mathcal{RS}$ *nad ciałem* $GF(q)$ *nazywamy BCH kod, dla którego* $N = q - 1$.

Niech α będzie elementem pierwotnym ciała $GF(q)$. Ponieważ w ciele $GF(q)$

$$x^{q-1} - 1 = \prod_{\beta \in GF^*(q)} (x - \beta),$$

wielomian minimalny elementu α^i równy jest

$$M^{(i)}(x) = x - \alpha^i.$$

Stąd RS-kod cykliczny długości $N = q-1$ i zadanej odległości δ ma wielomian generujący:

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \dots (x - \alpha^{b+\delta-2}),$$

stopnia $\delta - 1$ ($\delta - 1$ jest liczbą zer kodu).

Przykład 8.2. Niech $GF(4) = Z_2[x]/(x^2 + x + 1) = Z_2(\alpha) = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$, gdzie $\alpha^2 + \alpha + 1 = 0$ i α jest elementem pierwotnym ciała $GF(4)$. RS kod nad ciałem $GF(4)$, długości $N = q - 1 = 3$ i zadanej odległości $\delta = 2$ ma dla $b = 1$ wielomian generujący $g(x) = x - \alpha$. Stąd $K = N - 1 = 2$. Przyjmując za macierz kontroli parzystości macierz

$$H = [\alpha^2 \ \alpha \ 1]$$

(3,2,2)-kod RS nad ciałem $GF(4)$ składa się z następujących 16 słów kodowych:

0	0	0	1	α	0	β	0	α	β	α	1
0	1	α	α	β	0	1	0	β	1	1	1
0	α	β	β	1	0	1	β	α	α	α	α
0	β	1	α	0	1	α	1	β	β	β	β

□

Przykład 8.3. (4,2,3)-RS kod nad ciałem Z_5 o zadanej odległości 3 ma dla $b = 1$ wielomian generujący $g(x) = (x - 2)(x - 4) = x^2 + 4x + 3$ i składa się z 25 elementów. □

Wymiar RS kodu $\mathcal{RS} = (g(x)$ długości N wynosi $K = N - \mathrm{st}g(x) = N - \delta + 1$. Stąd $\delta = N - K + 1$. Na mocy twierdzenia 6.22, odległość kodu cyklicznego $D \geqslant \delta = N - K + 1$. Z drugiej strony, na mocy ograniczenia Singletona 2.10 odległość kodu liniowego spełnia zależność $N - K \geqslant D - 1$ a stąd $D \leqslant N - K + 1$.

Lemat 8.4. *Niech $\mathcal{RS}$ będzie (N, K, D)-kodem RS. Wówczas*

$$D = N - K + 1.$$

Oznacza to, że kody RS osiągają maksymalną możliwą dla kodów liniowych odległość.

RS-kody są kodami BCH stąd zawsze możemy do ich kodowania i dekodowania zastosować jedną z metod właściwą dla takich kodów. Istnieje także oryginalna metoda kodowania zaproponowana przez Reeda i Solomona.

Algorytm kodowania dla kodów RS

Niech $\mathcal{RS}$ będzie (N, K, D)-RS kodem nad ciałem $GF(q)$ dla $b = 0$ i niech $u = (u_0, u_1, \ldots, u_{K-1})$, gdzie $u_0, \ldots, u_{K-1} \in GF(q)$, będzie wektorem wiadomości. Niech ponadto $u(x) = \sum_{i=0}^{K-1} u_i x^i$.
Jako słowo kodowe przyporządkowane wiadomości u przyjmujemy wektor

$$c = (c_0, c_1, \ldots, c_{N-1}) = (u(1), u(\alpha), \ldots, u(\alpha^{N-1})) =$$

$$= (\sum_{i=0}^{K-1} u_i, \sum_{i=0}^{K-1} u_i \alpha^i, \ldots, \sum_{i=0}^{K-1} u_i \alpha^{(N-1)i}).$$

Otrzymany w ten sposób wektor c jest elementem kodu $\mathcal{RS}$, gdyż wielomian $c(x) = \sum_{i=0}^{N-1} c_i x^i$ ma elementy $1, \alpha, \alpha^2, \ldots, \alpha^{D-1}$ jako zera. Niestety, przedstawiony algorytm nie jest algorytmem systematycznym.

Przykład 8.5. Rozważmy ponownie RS kod $\mathcal{RS} = (x^2 + 4x + 3)$ z przykładu 8.3 i zastosujmy do zakodowania słowa $u = u_0 u_1$ metodę właściwą dla dowolnego kodu wielomianowego. Wówczas wektor wiadomości $u = (u_0, u_1)$ zostaje przekształcony w słowo kodowe $c = (2u_0 + 2u_1, u_0 + 3u_1, u_0, u_1)$.
Stosując natomiast algorytm Reeda-Solomona otrzymujemy wektor kodowy $c' = (c_0, c_1, c_2, c_3) = (u_0 + u_1, u_0 + 2u_1, u_0 + 4u_1, u_0 + 3u_1)$. Jak łatwo zauważyć

żadna ze współrzędnych tego wektora nie jest współrzędną wektora wiadomości. Do ich obliczenia możemy wykorzystać równości:

$$-u_0 = c(1)$$
$$-u_1 = c(\alpha^{-1}).$$

□

Algorytm dekodowania dla kodów RS

Metoda 1. Niech $\mathcal{RS}$ będzie RS kodem. Załóżmy, że słowo kodowe $c = (c_0, c_1, \ldots, c_{N-1}) = (u(1), u(\alpha), \ldots, u(\alpha^{N-1})) \in \mathcal{RS}$ zostało przesłane i w czasie transmisji wystąpił błąd $e = (e_0, e_1, \ldots, e_{N-1})$ w efekcie czego otrzymaliśmy wektor $y = (y_0, y_1, \ldots, y_{N-1}) = c + e$. Spełniony jest wówczas następujący układ N równań z K niewiadomymi $u_0, u_1, \ldots, u_{K-1}$:

$$\begin{aligned}
y_0 = e_0 + c_0 = e_0 + u(1) &= e_0 + u_0 + u_1 + u_2 + \cdots + u_{K-1} \\
y_1 = e_1 + c_1 = e_1 + u(\alpha) &= e_1 + u_0 + \alpha u_1 + \alpha^2 u_2 + \cdots + \alpha^{K-1} u_{K-1} \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
y_{N-1} = e_{N-1} + c_{N-1} &= e_{N-1} + u(\alpha^{N-1}) = \\
= e_{N-1} + u_0 + \alpha^{N-1} u_1 + \alpha^{2(N-1)} u_2 + \cdots + \alpha^{(K-1)(N-1)} u_{K-1}&
\end{aligned}$$

Aby odkodować wysłana wiadomość należy rozwiązać $\binom{N}{K}$ wszystkich możliwych układów K równań. Jeśli w czasie transmisji błąd nie wystąpił, tzn. wektor e jest wektorem zerowym, to dowolne z tych układów ma takie samo rozwiązanie.

Jeśli natomiast wystąpiło w błędów, to pewien zbiór K równań da nam rozwiązania nieprawidłowe. Ponieważ powyższe równości są niezależne, każde K z nich ma dokładnie jedno rozwiązanie $u = (u_0, u_1, \ldots, u_{K-1})$. Niepoprawne u może być rozwiązaniem co najwyżej $w + K - 1$ równań, zawierających w równań z błędem i $K-1$ równań poprawnych. Zatem błędne $u = (u_0, u_1, \ldots, u_{K-1})$ może być rozwiązaniem co najwyżej $\binom{w+K-1}{K}$ układów K równań. Ponadto mamy $\binom{N-w}{K}$ układów równań, których rozwiązaniem jest poprawne u. Zatem wybierając jako rozwiązanie, ten wektor, który jest rozwiązaniem większej ilości równań, wiadomość będzie odczytana poprawnie, jeśli $\binom{N-w}{K} > \binom{w+K-1}{K}$,

tzn. jeśli $D > 2w$. Jeśli liczba $\binom{N}{K}$ jest duża opisana metoda jest niepraktyczna.

Metoda 2. Niech $u(x)$, gdzie $\mathrm{st}u(x) \leqslant K$, będzie wielomianem wiadomości. Wówczas dla każdego $i = 0, \ldots, N-1$

$$u(x) = M^{(i)}(x)f_i(x) + r_i = (x - \alpha^i)f_i(x) + r_i.$$

Stąd dla każdego $i = 0, \ldots, N-1$, $u(\alpha^i) = r_i$. Zatem wektorem kodowym odpowiadającym wiadomości $u(x)$ jest wektor $r = (r_0, r_1, \ldots, r_{N-1})$, gdzie dla każdego $i = 0, \ldots, N-1$, r_i jest resztą z dzielenia wielomianu $u(x)$ przez wielomian minimalny elementu α^i, czyli przez wielomian $x - \alpha^i$. Stosując Chińskie twierdzenie o resztach w odniesieniu do wielomianów możemy znając wektor r odczytać wysłaną wiadomość.

Twierdzenie 8.6. (Chińskie twierdzenie o resztach dla wielomianów) *Niech $m_0(x), \ldots, m_{K-1}(x) \in GF(q)[x]$, które są parami względnie pierwsze i niech $M(x) := m_0(x) \ldots m_{K-1}(x)$. Jeśli $r_0(x), r_1(x), \ldots, r_{K-1}(x) \in GF(q)[x]$, wówczas istnieje dokładnie jeden wielomian $u(x)$, taki że* $\mathrm{st}u(x) < \mathrm{st}M(x)$ *oraz*

$$u(x) \equiv_{m_i(x)} r_i(x),$$

dla $i = 0, \ldots, K-1$.

Zwiększenie długości kodu przez dodanie dodatkowego symbolu sprawdzającego nie zawsze zwiększa odległość kodu. Jest tak dla kodów RS.

Twierdzenie 8.7. *Niech $\mathcal{RS}$ będzie $(N = q-1, K, D)$ kodem RS o wielomianie generującym*

$$g(x) = (x - \alpha)(x - \alpha^2) \ldots (x - \alpha^{D-1}).$$

Dodając do każdego słowa kodowego $c = c_0c_1 \ldots c_{N-1} \in \mathcal{RS}$ dodatkowy symbol kontrolny $c_N := -\sum_{i=0}^{N-1} c_i$, otrzymujemy $(N+1 = q, K, D+1)$-kod rozszerzony $\widehat{\mathcal{RS}}$.

Przykład 8.8. Niech $\mathcal{RS}$ będzie RS kodem z przykładu 8.3. Rozszerzony (4,2,3)-kod $\widehat{\mathcal{RS}}$ składa się z następujących wektorów:

0	0	0	0	1	α	0	β	β	0	α	1	β	α	1	0
0	1	α	β	α	β	0	1	1	0	β	α	1	1	1	1
0	α	β	1	β	1	0	α	1	β	α	0	α	α	α	α
0	β	1	α	α	0	1	β	α	1	β	0	β	β	β	β

□

Kody binarne utworzone z kodów RS

Każdy element ciała $GF(q = p^m)$ jest elementem m-wymiarowej przestrzeni wektorowej nad ciałem $GF(p)$. Niech $\lambda_1, \ldots, \lambda_m$ będzie bazą przestrzeni wektorowej $GF(p^m)$ nad ciałem $GF(p)$ i niech $\beta = \sum_{i=1}^{m} b_i \lambda_i$ będzie dowolnym elementem ciała $GF(p^m)$, dla $b_1, \ldots, b_m \in GF(p)$. Odwzorowanie

$$\varphi : GF(p^m) \to GF^m(p),$$

$$\beta \mapsto (b_1, b_2, \ldots, b_m)$$

przekształca (N, K, D) kod RS nad ciałem $GF(q = p^m)$ w $(n = mN, k = mK, d \geqslant D)$-kod nad ciałem $GF(p)$. Przekształcenie φ przekształca kody liniowe w kody liniowe, ale nie zawsze kody cykliczne w kody cykliczne. Wybór bazy $\lambda_1, \ldots, \lambda_m$ przestrzeni wektorowej $GF(q = p^m)$ może zmienić własności nowo utworzonego kodu. Może np. zmienić rozkład wagi a nawet odległość nowo utworzonego kodu.
Przy konstrukcji kodów RS nad ciałem $GF(q)$ zakładamy, że $q \neq 2$, czyli RS kody nigdy nie są kodami binarnymi. Jeśli natomiast $q = 2^m$ to otrzymany w wyniku przekształcenia φ kod jest kodem binarnym. Takie kody często mają największą możliwą odległość a w wielu sytuacjach mniejsze prawdopodobieństwo popełnienia błędu niż binarne kody BCH z tymi samymi parametrami.

Przykład 8.9. $GF(4) = Z_2(\alpha) = Z_2[x]/(x^2 + x + 1) = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$. Za bazę 2-wymiarowej przestrzeni $GF(4)$ możemy przyjąć $\{1, \alpha\}$. Wówczas przekształcenie $\varphi : GF(2^2) \to Z_2^2$ zdefiniowane jest następująco:

$$0 \mapsto 00$$

$$1 \mapsto 10$$

$$\alpha \mapsto 01$$

$$\beta = \alpha^2 \mapsto 11$$

(3,2,2)-kod RS nad ciałem $GF(4)$ z przykładu 8.3 w wyniku zastosowania przekształcenia φ staje się binarnym (6,4,2)-kodem:

0	0	0	0	0	0		1	0	0	1	0	0		1	1	0	0	0	1		1	1	0	1	1	0
0	0	1	0	0	1		0	1	1	1	0	0		1	0	0	0	1	1		1	0	1	0	1	0
0	0	0	1	1	1		1	1	1	0	0	0		1	0	1	1	0	1		0	1	0	1	0	1
0	0	1	1	1	0		0	1	0	0	1	0		0	1	1	0	1	1		1	1	1	1	1	1

□

Przykład 8.10. Niech $\mathcal{RS} = (g_1(x))$ będzie (7,5,3)-kodem RS nad ciałem $GF(8) = Z_2(\alpha) = Z_2[x]/(x^3 + x + 1) = \{0, 1, \alpha, \alpha^2, \alpha^3 = 1 + \alpha, \alpha^4 = \alpha + \alpha^2, \alpha^5 = 1 + \alpha + \alpha^2, \alpha^6 = 1 + \alpha^2\}$.
Dla $b = 5$ wielomian $g_1(x) = (x + \alpha^5)(x + \alpha^6) = \alpha^4 + \alpha x + x^2$.

Ponieważ $\alpha^2 = 1 + \alpha^6, \alpha^3 = 1 + \alpha, \alpha^4 = 1 + \alpha + \alpha^6, \alpha^5 = \alpha + \alpha^6$ zatem za bazę 3-wymiarowej przestrzeni $GF(2^3)$ możemy przyjąć $\{1, \alpha, \alpha^6\}$. Wówczas przekształcenie $\varphi : GF(2^3) \to Z_2^3$ zdefiniowane jest następująco:

$$\begin{aligned} 0 &\mapsto 000 \\ 1 &\mapsto 100 \\ \alpha &\mapsto 010 \\ \alpha^2 &\mapsto 101 \\ \alpha^3 &\mapsto 110 \\ \alpha^4 &\mapsto 111 \\ \alpha^5 &\mapsto 011 \\ \alpha^6 &\mapsto 001 \end{aligned}$$

Okazuje się, że binarny RS (21,15,3)-kod powstały w wyniku zastosowania przekształcenia φ jest binarnym (21,15,3)-kodem BCH o wielomianie generującym $g_2(y) = 1 + y + y^2 + y^4 + y^6$. Jest to jedyny znany nietrywialny przykład, gdy odwzorowanie φ przekształca kod cykliczny na kod cykliczny. □

Binarne kody otrzymane z kodów RS są szczególnie wygodne do poprawiania błędów seryjnych.

Definicja 8.11. *Serią długości l nazywamy wektor, dla którego wszystkie różne od zera współrzędne występują w ciągu kolejnych l składowych.*

Definicja 8.12. *Błędem seryjnym nazywamy wektor błędu, który jest serią.*

Lemat 8.13. *Każdy (n, k, d)-kod cykliczny może wykryć błąd seryjny o długości $l \leqslant n - k$.*

Twierdzenie 8.14. *Niech $\mathcal{RS}$ będzie RS kodem długości $2^m - 1$, $m \geqslant 2$, który może poprawić t błędów. Powstały z niego kod binarny pozwala skorygować pojedyncze błędy seryjne o długości $l \leqslant (t - 1)m + 1$.*

Przykład 8.15. Niech $\mathcal{C}$ będzie kodem binarnym otrzymanym z $(N = 2^7 - 1, K = 2^7 - 9, D = 9)$ RS kodu $\mathcal{RS}$. Wówczas $\mathcal{C}$ jest $(n = 7(2^7 - 1) = 889, k = 7K = 826, 9)$-kodem. Ponieważ kod $\mathcal{RS}$ pozwala skorygować $t \leqslant \frac{D-1}{2} = 4$ błędy oraz $m = 7$ to kod $\mathcal{C}$ pozwala skorygować pojedyncze błędy seryjne o długości l nie przekraczającej $(t-1)m + 1 = 22$. □

Jeśli wektor $c = c(x) = \sum_{i=0}^{N-1} c_i x^i$ należy do pierwotnego BCH kodu w wąskim sensie o długości N i zadanej odległości D, to $c(\alpha) = \cdots = c(\alpha^{D-1}) = 0$. Zatem $c(x)$ jest podzielny przez wielomian $(x - \alpha) \cdot \cdots \cdot (x - \alpha^{D-1})$, czyli należy również do (N, K, D)-kodu RS. Stąd odległość RS kodów jest co najwyżej taka jak odległość kodów BCH.

Twierdzenie 8.16. *Długie kody binarne otrzymane z kodów RS są złe.*

Jednak bardzo prosta konstrukcja pozwala otrzymać z kodów RS nieskończoną rodzinę dobrych kodów binarnych.

Kody Justesen

Niech $\mathcal{RS}$ będzie $(N = 2^m - 1, K, D = N - K + 1)$-kodem RS nad ciałem $GF(2^m)$ i niech α będzie elementem pierwotnym ciała $GF(2^m)$. Dla każdego elementu $a = (a_0, \ldots, a_{N-1}) \in \mathcal{RS}$, gdzie $a_0, \ldots, a_{N-1} \in GF(2^m)$ zdefiniujmy wektor

$$b := (a_0, a_0, a_1, \alpha a_1, a_2, \alpha^2 a_2, \ldots, a_{N-1}, \alpha^{N-1} a_{N-1}).$$

Następnie każdą składową $b_i \in GF(2^m)$, $0 \leqslant i \leqslant 2N$, wektora b zastąpmy przez odpowiadający jej m-elementowy ciąg binarny. W ten sposób otrzymamy wektor c długości $2mN$.

Definicja 8.17. *$(n = 2mN, k = mK)$-kod zawierający wszystkie wektory c powstałe z wektorów (N, K)- RS kodu $\mathcal{RS}$ w sposób opisany powyżej nazywamy* ***kodem Justesen*** *$\mathcal{J}_{N,K}$.*

Kod $\mathcal{J}_{N,K}$ jest kodem binarnym, którego współczynnik sprawności wynosi:

$$R = \frac{k}{n} = \frac{mK}{2mN} = \frac{K}{2N} < \frac{1}{2}.$$

Twierdzenie 8.18. *Rodzina $\mathcal{J}_{N,K}$ kodów Justesen jest asymptotycznie dobra.*

Kody Justesen są przykładem binarnych kodów konkatenacyjnych długości nN i wymiaru kK. W przypadku takich kodów binarną wiadomość długości kK dzieli się na K ciągów długości k. Każdy z takich ciągów traktuje się jako element ciała $GF(2^k)$ i w ten sposób otrzymuje się wektor długości K nad ciałem $GF(2^k)$. Następnie wiadomość koduje się przy użyciu tzw. (N, K)-kodu zewnętrznego (często wykorzystuje się właśnie do tego celu RS kody). Po zakodowaniu otrzymany wektor $a = a_0 a_1 \dots a_{N-1}$ jest długości N. Każdą współrzędną $a_i \in GF(2^k)$ ponownie traktuje się jako wektor binarny długości k i koduje (innym kodem, tzw. (n, k)-kodem wewnętrznym) w n-elementowy ciąg b_i. W ten sposób otrzymujemy słowo kodowe $b = b_0 b_1 \dots b_{N-1}$ długości N, gdzie każde $b_i \in GF(2^n)$.

9 MDS kody

Definicja 9.1. *(n, k, d)-kod liniowy nazywamy **MDS-kodem**, jeśli $d = n - k + 1$.*

Najważniejszymi przykładami MDS kodów są $(n = q-1, k, d = n-k+1)$ RS kody nad ciałem $GF(q)$, dla wszystkich $k = 1, \ldots, n$ oraz rozszerzone $(n+1, k, d+1 = n-k+2)$ RS kody.

Lemat 9.2. *Niech $\mathcal{C}$ będzie MDS kodem. Wówczas kod dualny $\mathcal{C}^{\perp}$ również jest kodem MDS.*

Przykład 9.3. Niech $\mathcal{C}$ będzie $(4, 2, 3)$- MDS kodem nad ciałem $GF(4) = \{0, 1, \alpha, \beta = \alpha^2\}$ o następującej macierzy generującej:

$$G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & \alpha \\ 1 & \beta \end{bmatrix}$$

Wówczas $H = \begin{bmatrix} 1 & \alpha & 1 & 0 \\ 1 & \beta & 0 & 1 \end{bmatrix}$ oraz

$$H^T = \begin{bmatrix} 1 & 1 \\ \alpha & \beta \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

jest macierzą generującą $(4, 2, 3)$-MDS kodu dualnego $\mathcal{C}^{\perp}$. □

Wniosek 9.4. *Niech $\mathcal{C}$ będzie (n, k, d)-kodem liniowym nad ciałem $GF(q)$. Następujące warunki są równoważne:*

1. *$\mathcal{C}$ jest MDS kodem.*
2. *Każde k wierszy macierzy generującej $G \in M_n^k$ kodu $\mathcal{C}$ jest liniowo niezależnych.*
3. *Każde $n-k$ kolumn w macierzy kontroli parzystości $H \in M_{n-k}^n$ kodu $\mathcal{C}$ jest liniowo niezależnych.*

Z wniosku 9.4 wynika, że dowolne k symboli w słowie kodowym może być przyjęte jako symbole wiadomości.

Dla MDS kodów problem rozkładu wagi jest całkowicie rozwiązany.

Twierdzenie 9.5. *Niech $\mathcal{C}$ będzie $(n, k, d = n - k + 1)$-kodem MDS nad ciałem $GF(q)$. Wówczas liczba A_w słów o wadze w dana jest następującym wzorem:*

$$A_w = \binom{n}{w} \sum_{j=0}^{w-d} (-1)^j \binom{w}{j} (q^{w-d+1-j} - 1).$$

Twierdzenie 9.6. *Jeśli $\mathcal{C}$ jest nietrywialnym $(n, k \geqslant 2, n - k + 1)$-MDS kodem nad ciałem $GF(q)$, to $n \leqslant q + k - 2$.*

Problemem otwartym pozostaje znalezienie dla danych k i q największego n, dla którego istnieje $(n, k, n-k+1)$-MDS kod nad ciałem $GF(q)$. Problem znalezienia najdłuższego MDS kodu można także sformułować jako problem geometryczny. Dla danej k wymiarowej przestrzeni wektorowej nad ciałem $GF(q)$, znaleźć największą liczbę wektorów o tej własności, że każde k z nich tworzy bazę tej przestrzeni.

Rozważmy kod $\mathcal{RS}_2$ o następującej macierzy kontroli parzystości:

$$H_2 = \left(\begin{array}{c|c|c} \mathbf{1} & 1 & 0 \\ \hline H & 0 & 0 \\ \hline 1 = \alpha^{q-1}\ \alpha^{q-k}\ \alpha^{2(q-k)}\ \ldots\ \alpha^{(q-2)(q-k)} & 0 & 1 \end{array}\right),$$

gdzie

$$H = \begin{pmatrix} 1 = \alpha^{q-1} & \alpha & \alpha^2 & \ldots & \alpha^{q-2} \\ 1 = \alpha^{q-1} & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(q-2)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 = \alpha^{q-1} & \alpha^{q-k-1} & \alpha^{2(q-k-1)} & \ldots & \alpha^{(q-2)(q-k-1)} \end{pmatrix}$$

jest macierzą kontroli parzystości RS kodu nad ciałem $GF(q)$, dla $b = 1$ oraz α jest elementem pierwotnym ciała $GF(q)$.

Twierdzenie 9.7. *Kod $\mathcal{RS}_2$ jest $(q + 1, k, q - k + 2)$-MDS kodem.*

Niech $m \geqslant 2$, α będzie elementem pierwotnym ciała $GF(2^m)$ i niech

$$H_3 = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 & 1 & 0 & 0 \\ 1 & \alpha & \alpha^2 & \ldots & \alpha^{q-2} & 0 & 1 & 0 \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(q-2)} & 0 & 0 & 1 \end{pmatrix} \in M_3^{2^m+2}$$

będzie macierzą kontroli parzystości $(2^m+2, 2^m-1, 4)$-kodu $\mathcal{C}_1$ nad ciałem $GF(2^m)$ oraz $G = H^T \in M^3_{2^m+2}$ będzie macierzą generującą $(2^m+2, 3, 2^m)$-kodu dualnego $\mathcal{C}_1^\perp$. Kody $\mathcal{C}_1$ oraz $\mathcal{C}_2 = \mathcal{C}_1^\perp$ są MDS kodami.

Twierdzenie 9.8. *Dla każdego* $1 \leqslant k \leqslant q+1$, *istnieje* $(q+1, k, q-k+2)$*-MDS kod cykliczny nad ciałem* $GF(q)$.

Przykład 9.9. Niech $\mathcal{C}$ będzie kodem cyklicznym długości $n = 9$ nad ciałem $GF(8) = GF(2^3) = Z_2[x]/(x^3+x^2+1) = Z_2(\beta) =$
$\{0, 1 = \beta^7, \beta, \beta^2, \beta^3 = 1+\beta^2, \beta^4 = 1+\beta+\beta^2, \beta^5 = 1+\beta, \beta^6 = \beta+\beta^2\}$,
gdzie $\beta^3+\beta^2+1 = 0$.
Najmniejszym rozszerzeniem ciała $GF(8)$, w którym wielomian x^9-1 rozkłada się na czynniki liniowe jest ciało $GF(64)$, gdyż $8^2 \equiv_9 1$. Niech γ będzie elementem pierwotnym ciała $GF(64)$. Wówczas

$$(\gamma^9)^7 = \gamma^{63} = 1$$

$$((\gamma^9)^2)^7 = \gamma^{126} = 1$$
$$((\gamma^9)^3)^7 = \gamma^{189} = 1$$
$$((\gamma^9)^4)^7 = \gamma^{252} = 1$$
$$((\gamma^9)^5)^7 = \gamma^{315} = 1$$
$$((\gamma^9)^6)^7 = \gamma^{378} = 1$$

Stąd $\beta = \gamma^9$ jest generatorem ośmio-elementowego podciała ciała $GF(64)$, czyli
$GF(8) = \{0, 1, \beta = \gamma^9, \beta^2 = \gamma^{18}, \beta^3 = \gamma^{27}, \beta^4 = \gamma^{36}, \beta^5 = \gamma^{45}, \beta^6 = \gamma^{54}\}$.
Ponadto

$$(\gamma^7)^9 = \gamma^{63} = 1$$

$$((\gamma^7)^2)^9 = \gamma^{126} = 1$$
$$((\gamma^7)^3)^9 = \gamma^{189} = 1$$
$$((\gamma^7)^4)^9 = \gamma^{252} = 1$$
$$((\gamma^7)^5)^9 = \gamma^{315} = 1$$
$$((\gamma^7)^6)^9 = \gamma^{378} = 1$$
$$((\gamma^7)^7)^9 = \gamma^{441} = 1$$

$$((\gamma^7)^8)^9 = \gamma^{504} = 1$$

Zatem $\alpha = \gamma^7$ jest pierwotnym 9-tym pierwiastkiem z 1 oraz elementy $1, \gamma^7, \gamma^{14}, \gamma^{21}, \gamma^{28}, \gamma^{35}, \gamma^{42}, \gamma^{49}, \gamma^{56} \in GF(64)$ są wszystkimi pierwiastkami wielomianu $x^9 - 1$. Nietrudno sprawdzić, że
$\alpha + \alpha^{-1} = \gamma^7 + \gamma^{56} = \beta^5$,
$\alpha^2 + \alpha^{-2} = \gamma^{14} + \gamma^{49} = \beta^3$,
$\alpha^3 + \alpha^{-3} = \gamma^{21} + \gamma^{42} = 1$,
$\alpha^4 + \alpha^{-4} = \gamma^{28} + \gamma^{35} = \beta^6$.
Ponieważ $x^2 + (\alpha^i + \alpha^{-i})x + 1 = (x + \alpha^i)(x + \alpha^{-i})$, zatem
$x^9 + 1 = (x + 1)(x^2 + x + 1)(x^2 + \beta^3 x + 1)(x^2 + \beta^5 x + 1)(x^2 + \beta^6 x + 1)$.
Stąd na przykład $\mathcal{C} = (x^2 + \beta^6 x + 1)$ jest $(9, 7, 3)$-kodem cyklicznym z zerami α^4 oraz α^{-4}, $\mathcal{C} = ((x + 1)(x^2 + \beta^5 x + 1))$ jest $(9, 6, 4)$-kodem cyklicznym z zerami α, α^{-1} oraz 1 natomiast $\mathcal{C} = ((x^2 + x + 1)(x^2 + \beta^6 x + 1))$ jest $(9, 5, 5)$-kodem cyklicznym z zerami α^3, α^4, α^5 oraz α^6. □

10 Kody reszt kwadratowych

Niech $GF(q)$ będzie ciałem o q elementach. Zauważmy, że jeśli q jest liczbą parzystą, czyli $q = 2^m$, to dla każdego $x \in GF(2^m)$

$$(x^{2^{m-1}})^2 = x^{2^m} = x.$$

Zatem każdy element $x \in GF(2^m)$ jest kwadratem elementu $x^{2^{m-1}} \in GF(2^m)$.

Załóżmy teraz, że p jest liczbą pierwszą nieparzystą ($p \neq 2$). Wówczas dla $1 \leqslant x \leqslant p-1$,

$$(p+x)^2 \equiv_p x^2 \equiv_p (p-x)^2.$$

Ponadto, dla $1 \leqslant x, y \leqslant \frac{1}{2}(p-1)$

$$x^2 \equiv_p y^2 \;\Leftrightarrow\; p \mid x^2 - y^2 \;\Leftrightarrow\; p \mid (x-y)(x+y) \;\Leftrightarrow$$

$$\Leftrightarrow\; p \mid x-y \vee p \mid x+y \Leftrightarrow\; x = y \vee x = -y \;\Leftrightarrow\; x = y,$$

gdyż x i y są dodatnie. Zatem wszystkie liczby $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ $(mod p)$ są różne.

Definicja 10.1. *Niech $p \neq 2$ będzie dodatnią liczbą pierwszą i niech $0 \neq a \in Z_p$. Jeśli istnieje liczba $b \in Z_p$ taka, że $a \equiv_p b^2$ to powiemy, że a jest* ***resztą kwadratową*** *modulo p. W przeciwnym razie a nazywamy* ***niereszta kwadratową*** *modulo p.*

Mamy dokładnie $\frac{p-1}{2}$ różnych kwadratowych reszt kwadratowych $mod p$. Niech Q_p oznacza zbiór reszt kwadratowych $mod p$ i niech N_p oznacza zbiór niereszt.

Przykład 10.2. Resztami kwadratowymi $mod 11$ są liczby 1, 3, 4, 5 oraz 9. Pozostałe różne od zera liczby ciała Z_{11} są nieresztami. □

Jeśli β jest elementem pierwotnym ciała $GF(p)$, to $\beta^{\frac{p-1}{2}} \equiv_p -1$. Stąd $\beta^k \in Q_p$ wtedy i tylko wtedy, gdy k jest liczbą parzystą, natomiast $\beta^k \in N_p$ wtedy i tylko wtedy, gdy k jest liczbą nieparzystą. Zatem dowolny element $a = \beta^k \in GF(p)$ należy do zbioru Q_p wtedy i tylko wtedy, gdy

$$a^{\frac{p-1}{2}} \equiv_p \beta^{k\frac{p-1}{2}} \equiv_p (-1)^k \equiv_p 1.$$

Lemat 10.3. 1. *Jeśli* $a, b \in Q_p$ *(*$a, b \in N_p$*) to* $ab \in Q_p$.
2. *Jeśli* $a \in Q_p$ *i* $b \in N_p$ *to* $ab \in N_p$.

Stąd Q_p jest podgrupą cykliczną grupy $GF^*(p)$ generowaną przez β^2.

Lemat 10.4. 1. *Jeśli* $p = 4m + 1$ *to* $-1 \in Q$.
2. *Jeśli* $p = 4m - 1$ *to* $-1 \in N$.

Niech $q \in Q_p$ będzie liczbą pierwszą i niech $GF(q^m)$ będzie rozszerzeniem ciała $GF(q)$ o pierwiastki wielomianu $x^p - 1$. Niech ponadto $\alpha \in GF(q^m)$ będzie pierwotnym p-tym pierwiastkiem z 1 i niech

$$q(x) := \prod_{r \in Q_p} (x - \alpha^r),$$

$$n(x) := \prod_{n \in N_p} (x - \alpha^n).$$

Ponieważ na mocy lematu 10.3 zbiory Q_p i N_p są zamknięte ze względu na mnożenie, można pokazać że wielomiany $q(x)$ i $n(x)$ mają współczynniki należące do ciała $GF(q)$ oraz

$$x^p - 1 = (x - 1)q(x)n(x).$$

Definicja 10.5. ***Kodami reszt kwadratowych*** *nazywamy następujące kody cykliczne długości* p *nad ciałem* $GF(q)$ *(*$q \in Q$*):*

$$\begin{aligned} \mathcal{Q} &= (q(x)), \\ \overline{\mathcal{Q}} &= ((x-1)q(x)), \\ \mathcal{N} &= (n(x)), \\ \overline{\mathcal{N}} &= ((x-1)n(x)). \end{aligned}$$

Kody $\mathcal{Q}$ i $\mathcal{N}$ nazywamy kodami resztowymi rozszerzonymi a kody $\overline{\mathcal{Q}}$ i $\overline{\mathcal{N}}$ nazywamy kodami resztowymi okrojonymi. Kody $\mathcal{Q}$ i $\mathcal{N}$ są wymiaru $\frac{1}{2}(p+1)$, gdyż st$n(x)$=st$q(x) = \frac{p-1}{2}$. Stąd $k = p - \frac{p-1}{2} = \frac{2p-p+1}{2} = \frac{p+1}{2}$. Natomiast kody $\overline{\mathcal{Q}}$ i $\overline{\mathcal{N}}$ są wymiaru $\frac{1}{2}(p-1)$, gdyż st$(x-1)n(x)$=st$(x-1)q(x) = \frac{p-1}{2} + 1$ oraz $k = p - \frac{p-1}{2} - 1 = \frac{p+1}{2} - 1 = \frac{p-1}{2}$. Oczywiście $\overline{\mathcal{Q}} \subset \mathcal{Q}$ oraz $\overline{\mathcal{N}} \subset \mathcal{N}$.

Przykład 10.6. Dla $p = 7$ mamy $Q_7 = \{1, 2, 4\}$ oraz $N_7 = \{3, 5, 6\}$. Niech $q = 2 \in Q_7$. Najmniejszym rozszerzeniem ciała $GF(2)$ o pierwiastki wielomianu $x^7 - 1$ jest ciało $GF(8)$. Niech α będzie elementem pierwotnym ciała $GF(8) = Z_2[x]/(x^3 + x + 1)$ (jest on jednocześnie pierwotnym 7-ym pierwiastkiem z 1). Wówczas

$$\mathcal{Q} = (\prod_{r \in Q_7} (x - \alpha^r)) = ((x + \alpha)(x + \alpha^2)(x + \alpha^4)) = (x^3 + x + 1).$$

Ponieważ $x^3 + x + 1$ jest wielomianem minimalnym elementu α, kod $\mathcal{Q}$ jest $(7, 4, 3)$-kodem Hamminga.
Ponadto $\overline{\mathcal{Q}} = ((x+1)(x^3+x+1))$ jest $(7, 3, 4)$-podkodem kodu $\mathcal{Q}$, natomiast kod $\mathcal{N}$ jest kodem równoważnym z $\mathcal{Q}$ o wielomianie generującym

$$n(x) = \prod_{n \in N_7} (x - \alpha^n) = (x + \alpha^3)(x + \alpha^5)(x + \alpha^6) = x^3 + x^2 + 1.$$

Inny wybór elementu pierwotnego w ciele $GF(8)$ zamienia wielomiany generujące kodów $\mathcal{Q}$ i $\mathcal{N}$. □

Ponieważ binarny kod cykliczny $\mathcal{C} = (g(x))$ zawiera tylko wektory wagi parzystej wtw, gdy $(1+x) \mid g(x)$ to binarne kody resztowe okrojone zawierają dokładnie wszystkie słowa o parzystej wadze kodów resztowych rozszerzonych.

Twierdzenie 10.7. *Kody $\mathcal{Q}$ i $\mathcal{N}$ oraz $\overline{\mathcal{Q}}$ i $\overline{\mathcal{N}}$ są parami równoważne.*

Przykład 10.8. $(23, 12, 7)$-binarny kod Golay'a $\mathcal{G}_{23}$ jest kodem reszt kwadratowych dla $p = 23$ oraz $q = 2$. W ciele $GF(2)$

$$x^{23}+1 = (x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)(x^{11}+x^9+x^7+x^6+x^5+x+1),$$

stąd

$$\mathcal{G}_{23} = (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1) = (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1).$$

$(11, 6, 5)$-ternarny kod Golay'a $\mathcal{G}_{11}$ jest kodem reszt kwadratowych dla $p = 11$ oraz $q = 3$. W ciele $GF(3)$

$$x^{11} - 1 = (x - 1)(x^5 + x^4 - x^3 + x^2 - 1)(x^5 - x^3 + x^2 - x - 1),$$

stąd

$$\mathcal{G}_{11} = (x^5 + x^4 - x^3 + x^2 - 1) = (x^5 - x^3 + x^2 - x - 1).$$

□

Twierdzenie 10.9. *Niech d będzie odległością kodu $\mathcal{Q}$ (lub $\mathcal{N}$). Wówczas*

$$d^2 \geqslant p.$$

Ponadto, jeśli $p = 4k - 1$ to $d^2 - d + 1 \geqslant p$.

Przykład 10.10. $(7, 4, d)$-kod reszt kwadratowych nad ciałem $GF(q)$ ma odległość $d \geqslant \sqrt{p} = \sqrt{7}$, czyli $d \geqslant 3$.
Ponadto dla $p = 7 = 4 \cdot 2 - 1$, $d^2 - d + 1 = 9 - 3 + 1 = 7 \geqslant p = 7$. □

Współczynnik sprawności kodów reszt kwadratowych wynosi

$$R = \frac{\frac{1}{2}(p+1)}{p} = \frac{1}{2} + \frac{1}{2p} \to \frac{1}{2}, \text{ gdy } p \to \infty.$$

Generalnie są to dobre kody.

Twierdzenie 10.11. *Jeśli $p = 4k - 1$ to $\mathcal{Q}^\perp = \overline{\mathcal{Q}}$ oraz $\mathcal{N}^\perp = \overline{\mathcal{N}}$.*
Jeśli $p = 4k + 1$ to $\mathcal{Q}^\perp = \overline{\mathcal{N}}$ oraz $\mathcal{N}^\perp = \overline{\mathcal{Q}}$.

Ponieważ binarne kody $\mathcal{Q}$ i $\mathcal{N}$ zawierają słowa wagi nieparzystej to muszą zawierać wektor jednostkowy $\mathbf{1}$. Można pokazać, że kod $\mathcal{Q}$ jest generowany przez kod $\overline{\mathcal{Q}}$ i $\mathbf{1}$ natomiast kod $\mathcal{N}$ jest generowany przez kod $\overline{\mathcal{N}}$ i $\mathbf{1}$.

Następujące twierdzenie podaje warunek na istnienie binarnych i ternarnych kodów reszt kwadratowych.

Twierdzenie 10.12. 1. *Jeśli $p = 8m \pm 1$ to $2 \in Q_p$.*
2. *Jeśli $p = 8m \pm 3$ to $2 \in N_p$.*
3. *Jeśli $p = 12m \pm 1$ to $3 \in Q_p$.*

Grupa automorfizmów kodu

Niech $\mathcal{C}$ będzie kodem binarnym długości n. Jak wiemy, dowolna permutacja n współrzędnych zamienia kod $\mathcal{C}$ w kod równoważny.

Definicja 10.13. *Permutacje współrzędnych kodu $\mathcal{C}$, które przekształcają kod $\mathcal{C}$ w ten sam kod, tworzą podgrupę $Aut(\mathcal{C})$ grupy S_n zwaną* ***grupą automorfizmów kodu*** *$\mathcal{C}$.*

Przykład 10.14. 1. Jeśli $\mathcal{C} = Z_2[x]/(x^n - 1)$ to $Aut(\mathcal{C}) = S_n$.
2. Jeśli $\mathcal{C} = \{\mathbf{0}_n\}$ to $Aut(\mathcal{C}) = S_n$. □

Przykład 10.15. Grupa automorfizmów kodu $\mathcal{C} = \{0000, 0011, 1100, 1111\}$ składa się z następujących 8 permutacji:

$$Aut(\mathcal{C}) = \{(1), (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}.$$

□

Szczególnie interesujące są grupy automorfizmów kodów cyklicznych. Zgodnie z definicją kodu cyklicznego grupa automorfizmów takiego kodu zawiera wszystkie permutacje cykliczne długości n (tzn. permutację $(123 \ldots n)$ i wszystkie jej złożenia). Ponadto, jeśli n jest liczbą nieparzystą to grupa $Aut(\mathcal{C})$ zawiera prócz wszystkich permutacji cyklicznych długości n również permutację taką, że $\sigma_2 : x \mapsto x^2$, gdyż wówczas σ_2 jest przekształceniem różnowartościowym (przekształaca bazę $\{1, x, x^2, \ldots, x^{n-1}\}$ w bazę $\{1, x^2, x^4, x^6, \ldots, x^{n-1}, x^{n+1} = x, x^{n+3} = x^3, \ldots, x^{2n-2} = x^{n-2}\}$) oraz dla każdego $a(x) \in \mathcal{C}$, $\sigma_2(a(x)) = a(x^2) = (a(x))^2 \in \mathcal{C}$ $(g(x) \mid a(x) \Rightarrow g(x) \mid (a(x))^2)$.

Przykład 10.16. Grupa automorfizmów (7,3,4)-kodu sympleksowego $\mathcal{S}_3 = \{0000000, a = 1110100, b = b^8 = 0111010, b^2 = 0011101, b^4 = 0100111, c = C^8 == 1001110,$
$c^2 = 1101001, c^4 = 1010011\}$ zawiera permutację $\sigma_2 : x \to x^2$, gdyż $\sigma_2(a(x)) = a(x)$. □

Algorytm dekodowania permutacyjnego dla binarnych kodów cyklicznych

Metoda dekodowania permutacyjnego jest stosowana do kodów z dużą grupą automorfizmów, np. do kodów cyklicznych a szczególnie do kodów reszt kwadratowych.

Niech $\mathcal{C}$ będzie (n, k, d)- cyklicznym kodem binarnym. Załóżmy, że do kodowania zastosowaliśmy metodę właściwą dla kodów wielomianowych. Wówczas macierz generująca kodu $\mathcal{C}$ ma postać $G = (\frac{P}{I})$ a macierz kontroli parzystości $H = (I \mid P)$. Zatem dla słowa $c = c_0c_1 \dots c_{n-k} \dots c_{n-1} \in \mathcal{C}$, współrzędne $c_0, \dots, c_{n-k-1}$ są symbolami sprawdzającymi, natomiast $c_{n-k}, \dots, c_{n-1}$ są k symbolami wiadomości.

Twierdzenie 10.17. *Niech $y = y_0y_1 \dots y_{n-1}$ będzie wektorem otrzymanym w procesie kodowania o syndromie $s = Hy$ i niech $e = e_0e_1 \dots e_{n-1}$ będzie wektorem błędu o wadze t, gdzie $2t + 1 \leqslant d$. Jeśli $wt(s) \leqslant t$, to symbole informacji $y_{n-k}, \dots, y_{n-1}$ są przesłane bez błędu a $s0 \dots 0 = e_0 \dots e_{n-k-1}0 \dots 0$ jest wektorem błędu. Jeśli natomiast $wt(s) > t$, to co najmniej jeden symbol informacji y_i $(n - k \leqslant i \leqslant n - 1)$ w wektorze y jest niepoprawny.*

W oparciu o twierdzenie 10.17 możemy zastosować następującą metodę dekodowania. Załóżmy, że chcemy poprawić wszystkie błędy o wadze mniejszej lub równej t, dla ustalonego $t \leqslant [\frac{d-1}{2}]$. Niech $P = \{\pi_1 = 1, \pi_2, \dots, \pi_s\}$ będzie zbiorem permutacji, które zachowują kod i mają tę własność, że dla dowolnego wektora e wagi mniejszej lub równej t istnieje w zbiorze P permutacja π_i, która przenosi wszystkie 1 w wektorze e poza pozycje informacji.

Aby odkodować otrzymany wektor y, należy obliczyć dla każdej permutacji $\pi_i \in P$ wektor $\pi_i y$ oraz jego syndrom $s^i := H(\pi_i y)$. Jeśli istnieje takie $1 \leqslant i \leqslant s$, że $wt(s^i) \leqslant t$, to na mocy twierdzenia 10.17, wszystkie błędy, które zostały popełnione znajdują się na pierwszych $n - k$ pozycjach wektora $\pi_i y$ i dane są przez wektor $s^i = e_0 \dots e_{n-k-1}$. Zatem wektor y możemy odkodować jako słowo

$$c = \pi_i^{-1}(\pi_i y + e_0 \dots e_{n-k-1}0 \dots 0).$$

Jeśli natomiast $wt(s^i) > t$ dla wszystkich $1 \leqslant i \leqslant s$, wnioskujemy, że w słowie y zostało popełnionych więcej niż t błędów.

Przykład 10.18. Jeśli za zbiór P przyjmiemy zbiór generowany przez jedną permutację cykliczną $S = (123 \dots n)$ długości n, to wówczas $P = \{1, S, S^2, \dots, S^{n-1}\}$.

W tym przypadku metoda dekodowania permutacyjnego poprawia wszystkie błędy wagi t, gdzie $t \leqslant [\frac{n-1}{k}]$. Jednak jest użyteczna jedynie w przypadku wystąpienia małej ilości błędów lub błędów seryjnych. □

Przykład 10.19. Niech $\mathcal{C}$ będzie $(31, 21, 5)$-BCH kodem poprawiajacym błędy podwójne. Ponieważ $[\frac{30}{21}] = 1$, to metoda z przykładu 10.18 pozwala poprawić jedynie błędy pojedyncze. Niech $S = (12 \ldots 31)$ oraz $\gamma : \mathcal{C} \to \mathcal{C}$ będzie permutacją zachowującą kod taką, że

$$y_0 y_1 \ldots y_{30} \mapsto z_0 z_1 \ldots z_{30},$$

gdzie $z_{2i} \equiv_{31} y_i$ dla $i = 0, 1, \ldots, 30$. Wówczas $P = \{S^i \gamma^j \mid 0 \leqslant i \leqslant 30, 0 \leqslant j \leqslant 4\}$ jest zbiorem 155 permutacji, które dla wszystkich wektorów wagi 2 przenoszą 1 poza symbole informacji, zatem mogą być zastosowane w metodzie dekodowania permutacyjnego. □

Przykład 10.20. Niech $\mathcal{C}$ będzie $(23, 12, 7)$-kodem Golay'a $\mathcal{G}_{23}$ poprawiajacym błędy potrójne. Ponieważ $[\frac{22}{12}] = 1$, to metoda z przykładu 10.18 pozwala poprawić jedynie błędy pojedyncze. Niech $S = (12 \ldots 23)$. Wówczas $P = \{S^i \sigma_2^j \mid 0 \leqslant i \leqslant 22, j = 0, 1, 2 \text{ lub } 11\}$ jest zbiorem 92 permutacji, które dla wszystkich wektorów wagi mniejszej bądź równej 3 przenoszą 1 poza symbole informacji, zatem mogą być zastosowane w metodzie dekodowania permutacyjnego. □

Żaden ze zbiorów permutacji P znalezionych w przykładach 10.19 oraz 10.20 nie jest zbiorem minimalnym.

11 Kody alternujące

Kody alternujące są dużą rodziną kodów otrzymaną przez niewielką modyfikację macierzy kontroli parzystości dla kodów BCH. Ta niewielka modyfikacja powoduje, że w przeciwieństwie do kodów BCH, niektóre długie kody alternujące są dobre i osiągają ograniczenie Gilberta - Varshamova.

Definicja 11.1. *Niech* $\alpha = (\alpha_1, \ldots, \alpha_N) \in [GF(q^m)]^N$, $\alpha_i \neq \alpha_j$ *dla* $i \neq j$ *i* $v = (v_1, \ldots, v_N) \in [GF^*(q^m)]^N$. ***Uogólniony RS*** (N, K)***-kod liniowy*** $GRS_K(\alpha, v)$ ***nad ciałem*** $GF(q^m)$ *składa się ze wszystkich wektorów postaci:*

$$(v_1 F(\alpha_1), \ldots, v_N F(\alpha_N)),$$

gdzie $F(z) \in GF(q^m)[z]$ *jest wielomianem stopnia mniejszego niż* K *odpowiadającym wektorowi wiadomości.*

Przykład 11.2. Niech β będzie elementem pierwotnym w ciele $GF(q^m)$. (N, K)-RS kod nad ciałem $GF(q^m)$ jest kodem $GRS_K(\alpha, v)$ dla $\alpha = (1, \beta, \ldots, \beta^{N-1})$ oraz $v = (1, \ldots, 1)$. □

Niech $F(z) = a_0 + a_1 z + \ldots + a_{K-1} z^{K-1}$ będzie wielomianem wiadomości. Wówczas i-ta współrzędna wektora kodowego odpowiadającego wiadomości $F(z)$ równa jest

$$v_i F(\alpha_i) = v_i(a_0 + \alpha_i a_1 + \ldots + \alpha_i^{K-1} a_{K-1}) = v_i a_0 + \alpha_i v_i a_1 + \ldots + \alpha_i^{K-1} v_i a_{K-1}.$$

Zatem wektor

$$c = \begin{pmatrix} v_1 & \alpha_1 v_1 & \ldots & \alpha_1^{K-1} v_1 \\ \vdots & \vdots & & \vdots \\ v_i & \alpha_i v_i & \ldots & \alpha_i^{K-1} v_i \\ \vdots & \vdots & & \vdots \\ v_N & \alpha_N v_N & \ldots & \alpha_N^{K-1} v_N \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ \vdots \\ a_{K-1} \end{pmatrix}$$

jest słowem kodowym należącym do $GRS_K(\alpha, v)$ oraz

$$G_K = \begin{pmatrix} v_1 & \alpha_1 v_1 & \ldots & \alpha_1^{K-1} v_1 \\ \vdots & \vdots & & \vdots \\ v_i & \alpha_i v_i & \ldots & \alpha_i^{K-1} v_i \\ \vdots & \vdots & & \vdots \\ v_N & \alpha_N v_N & \ldots & \alpha_N^{K-1} v_N \end{pmatrix}$$

jest macierzą generującą tego kodu.

Twierdzenie 11.3. *Kod $GRS_K(\alpha, v)$ jest liniowym MDS kodem.*

Twierdzenie 11.4. *Kodem dualnym do kodu $GRS_K(\alpha, v)$ jest kod $GRS_{N-K}(\alpha, y)$, dla pewnego wektora $y = (y_1, \ldots, y_N) \in [GF^*(q^m)]^N$.*

Z twierdzenia 11.4 wynika, że macierz kontroli parzystości H_K kodu $GRS_K(\alpha, v)$ równa jest transponowanej macierzy generującej kod dualny $GRS_K^{\perp}(\alpha, v) = GRS_{N-K}(\alpha, y)$, gdzie $y = (y_1, y_2, \ldots, y_N) \in [GF^*(q^m)]^N$. Stąd

$$H_K = G_{K-N}^T = \begin{pmatrix} y_1 & y_2 & \ldots & y_N \\ \alpha_1 y_1 & \alpha_2 y_2 & \ldots & \alpha_N y_N \\ \alpha_1^2 y_1 & \alpha_2^2 y_2 & \ldots & \alpha_N^2 y_N \\ \vdots & \vdots & & \vdots \\ \alpha_1^{N-K-1} y_1 & \alpha_2^{N-K-1} y_2 & \ldots & \alpha_N^{N-K-1} y_N \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_N \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_N^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{N-K-1} & \alpha_2^{N-K-1} & \ldots & \alpha_N^{N-K-1} \end{pmatrix} \begin{pmatrix} y_1 & \ldots & \ldots & 0 \\ 0 & y_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & \ldots & y_N \end{pmatrix}.$$

Definicja 11.5. ***Kod alternujący*** *$\mathcal{A}(\alpha, y)$ nad ciałem $GF(q)$ składa się ze wszystkich słów kodowych kodu $GRS_K(\alpha, v)$ nad ciałem $GF(q^m)$, których współrzędne należą do ciała $GF(q)$. (Kod $\mathcal{A}(\alpha, y)$ jest ograniczeniem kodu $GRS_K(\alpha, v)$ do ciała $GF(q)$.)*

Zatem kod alternujący $\mathcal{A}(\alpha, y)$ zawiera wszystkie wektory $c \in [GF(q)]^N$ takie, że $H_K c = 0$, gdzie $H_K = (H_{ij})$, $H_{ij} \in GF(q^m)$, jest macierzą kontroli parzystości kodu $GRS_K(\alpha, v)$.

Przykład 11.6. Macierz kontroli parzystości kodu BCH nad ciałem $GF(q)$ ma postać

$$\begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \ldots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \ldots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \ldots & \alpha^{(n-1)(b+\delta-2)} \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{(n-1)} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{\delta-2} & \alpha^{2(\delta-2)} & \dots & \alpha^{(n-1)(\delta-2)} \end{pmatrix} = \begin{pmatrix} 1 & \dots & \dots & 0 \\ 0 & \alpha^b & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & \alpha^{(n-1)b} \end{pmatrix},$$

gdzie $\alpha \in GF(q^m)$ jest n-tym pierwotnym pierwiastkiem z 1.
Zatem jest to kod alternujący o parametrach: $\alpha = (1, \alpha, \alpha^2, \dots, \alpha^{n-1})$ oraz $y = (1, \alpha^b, \alpha^{2b}, \dots, \alpha^{(n-1)b})$. □

Kod alternujący $\mathcal{A}(\alpha, y)$ można zdefiniować również nieco inaczej. Ponieważ ciało $GF(q^m)$ jest m-wymiarową przestrzenią wektorową nad ciałem $GF(q)$, zatem każdy element H_{ij} macierzy

$$H_K = \begin{pmatrix} H_{11} & \dots & H_{1N} \\ H_{21} & \dots & H_{2N} \\ \vdots & & \vdots \\ H_{(N-K)1} & \dots & H_{(N-K)N} \end{pmatrix}$$

jest postaci

$$H_{ij} = \sum_{l=1}^{m} H_{ijl}\beta_l,$$

gdzie $H_{ijl} \in GF(q)$ oraz $\beta_1, \dots, \beta_m$ są wektorami bazowymi.

Macierz $\overline{H}_K$ o elementach w ciele $GF(q)$ otrzymujemy zastępując każdy element H_{ij} macierzy H_K przez odpowiedni wektor $(H_{ij1}, \dots, H_{ijm})$ długości m nad ciałem $GF(q)$. Wówczas

$$\overline{H}_K = \begin{pmatrix} H_{111} & H_{121} & \dots & H_{1N1} \\ H_{112} & H_{122} & \dots & H_{1N2} \\ \vdots & \vdots & & \vdots \\ H_{11m} & H_{12m} & \dots & H_{1Nm} \\ H_{211} & H_{221} & \dots & H_{2N1} \\ \vdots & \vdots & & \vdots \\ H_{(N-K)1m} & H_{(N-K)2m} & \dots & H_{(N-K)Nm} \end{pmatrix}.$$

Stąd dla wektora $a = (a_1, \ldots, a_N) \in [GF(q)]^N$

$$a \in \mathcal{A}(\alpha, y) \;\Leftrightarrow\; H_K a = 0 \;\Leftrightarrow\; \sum_{j=1}^{N} H_{ij} a_j = 0, \;\text{ dla }\; i = 1, \ldots, N-K \;\Leftrightarrow$$

$$\Leftrightarrow\; \sum_{j=1}^{N} H_{ijl} a_j = 0, \;\text{ dla }\; i = 1, \ldots, N-K, \;\; l = 1, \ldots, m \;\Leftrightarrow \overline{H}_K a = 0.$$

Rząd macierzy $\overline{H}_K$ nad ciałem $GF(q)$ wynosi co najwyżej $(N-K)m$, zatem zakładając, że długość N kodu alternującego musi być większa od ilości symboli kontrolnych, wymiar k kodu $\mathcal{A}(\alpha, y)$ spełnia zależność:

$$N - (N-K)m \leqslant k \leqslant N - (N-K).$$

Przykład 11.7. Niech β będzie elementem pierwotnym ciała $GF(2^3) = Z_2[x]/(x^3 + x + 1)$ i niech $\alpha = (1, \beta, \beta^2, \ldots, \beta^6)$ oraz $y = (1, 1, 1, \ldots, 1)$. Macierz H_5 kodu alternującego długości $N = 7$ ma postać:

$$H_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \end{pmatrix}.$$

Zastępując każdy element tej macierzy binarnym wektorem długości 3 otrzymujemy macierz

$$\overline{H}_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Ponieważ drugi i trzeci wiersz macierzy $\overline{H}_5$ są zerowe, zatem poszukiwaną macierzą kontroli parzystości jest

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

i binarny kod alternujący $\mathcal{A}(\alpha, y)$ jest $(7, 3)$-kodem. □

Przykład 11.8. Jeśli w przykładzie 11.7 jako y przyjmiemy wektor $(1, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6)$ to macierz H_5 przyjmie postać

$$\begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta & \beta^3 & \beta^5 \end{pmatrix}.$$

Stąd dla wektora $c = (c_0, c_1, \ldots, c_6) \in Z_2^7$,

$$c \in \mathcal{A}(\alpha, y) \;\Leftrightarrow\; H_5 c = 0 \;\Leftrightarrow\; \sum_{i=0}^{6} \beta^i c_i = 0 \;\wedge\; \sum_{i=0}^{6} \beta^{2i} c_i = 0.$$

Ponieważ $\sum\limits_{i=0}^{6} \beta^{2i} c_i = (\sum\limits_{i=0}^{6} \beta^i c_i)^2$, stąd drugi rząd macierzy H_5 jest zbędny i macierzą kontroli parzystości kodu $\mathcal{A}(\alpha, y)$ jest

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

co oznacza, że jest to binarny $(7, 4, 3)$-kod Hamming'a. □

Twierdzenie 11.9. *Niech d będzie odległością kodu $\mathcal{A}(\alpha, y)$. Wówczas*

$$d \geqslant N - K + 1.$$

Definicja 11.10. *Niech $\mathcal{C}$ będzie kodem nad ciałem $GF(q^m)$ i niech $T_m(\beta)$ będzie śladem elementu $\beta \in GF(q^m)$. Kodem śladowym $T_m(\mathcal{C})$ nad ciałem $GF(q)$ kodu $\mathcal{C}$ nazywamy kod złożony ze wszystkich różnych wektorów postaci $(T_m(c_1), \ldots, T_m(c_n))$, gdzie $(c_1, \ldots, c_n) \in \mathcal{C}$.*

Twierdzenie 11.11. *Kodem dualnym do kodu alternującego $\mathcal{A}(\alpha, y)$ jest kod śladowy kodu dualnego $GRS_K^{\perp}(\alpha, v)$, czyli*

$$\mathcal{A}^{\perp}(\alpha, y) = T_m(GRS_{N-K}(\alpha, y)) = T_m(GRS_K^{\perp}(\alpha, v)).$$

Twierdzenie 11.12. *Długie kody alternujące są dobre.*

Niestety, z twierdzenia nie wynika, które kody alternujące są dobre.

Klasa kodów alternujących jest bardzo obszerna. Ze względu na ograniczenia nakładane na wektory α i y możemy wyróżnić następujące klasy kodów alternujących:

- kody Goppa
- kody Srivastava
- uogólnione kody Srivastava
- kody Chien-Choy (do tej klasy należą kody BCH)

Literatura

[1] N.J.A. Sloane, F.J. MacWilliams, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[2] J.H. van Lint, *Introduction to Coding Theory*, Springer, 1999.

[3] V.Pless, *Introduction to the Theory of Error-Correcting Codes*, John Wiley & Sons, 1982.

[4] E.R. Berlekamp, *Algebraic Coding Theory*, Aegean Park Press, Laguna Hills, 1984.

[5] W. Lipski, W. Marek, *Analiza kombinatoryczna*, PWN, Warszawa 1986.