Kodowanie

Lista nr 2 (dodatkowa).

Zadanie 1. Czy istnieje binarny kod liniowy długości 8, wymiaru 3, o minimalnej odległości słów kodowych równej 5?

Zadanie 2. Wykaż, że kody Hamminga tej samej długości są równoważne (np. w sensie zadania 8 (poprawionego) z poprzedniej listy).

Zadanie 3. Zadanie dotyczy rozszerzonego kodu Golay'a (kodu Golay'a rozszerzonego o bit kontroli parzystości). Przypuśćmy, że kod liniowy K jest generowany przez wiersze macierzy $[I, B]$, gdzie I jest macierzą jednostkową, a B macierzą kwadratową (o wyrazach z ciała Z_2) taką, że $B^2 = I$ i $B = B^T$. Rozważamy więc kod binarny parzystej długości. Słowa (wektory) z rozważanej przestrzeni będziemy przedstawiać w postaci konkatenacji słów równej długości. Udowodnij, że

1. macierze $[I, B]$ oraz $[B, I]$ są macierzami układów równań definiujących kod K, (w szczególności, K jest kodem dualnym do K),
2. Przypuśćmy, że słowo w zostało przesłane z błędem $u_1 u_2$. Niech $s = [I, B] \cdot w^T$ (s jest więc syndromem). Zauważmy, że $s = u_1 + B \cdot u_2$. Ponadto, jeżeli $u_2 = 0$ (czyli błędy wystąpiły tylko w pierwszej połowie słowa w), to $s = u_1$. Jeżeli natomiast w słowie u_2 znajduje się dokładnie jedna jedynka, a w słowie u_1 – najwyżej dwie, to w słowie s są przynajmniej 4 jedynki. Dla kodu K syndromem może być także słowo $s' = B \cdot s^T = [B, I] \cdot w^T$. Dla tego słowa są prawdziwe analogiczne własności.
3. Przypuśćmy, że kod K koryguje 3 błędy. Opracuj dla kodu K algorytm korygujący $\leqslant 3$ błędy i udowodnij jego poprawność. Wskazówka: w pierwszej lub drugiej połowie otrzymamego słowa występuje 0 lub 1 błąd. Jeżeli występuje 0 błędów, to pozostałe łatwo skorygować korzystając powyższych uwag. Jeżeli występuje 1 błąd, to na wszystkie sposoby próbujemy go skorygować. W jednym przypadku pozostałe błędy powinno się dać łatwo skorygować.
4. Przypuśćmy, że kod K powstaje z kodu K' przez dodanie bitu kontroli parzystości. Opracuj dla kodu K' algorytm korygujący $\leqslant 3$ błędy przy założeniu, że K' koryguje tyle błędów (algorytm korygujący błędy dla kodu Golay'a).

Zadanie 4. (może być nieco żmudne) Znajdź macierz B, o której mowa w poprzednim zadaniu, dla rozszerzonego kodu Golay'a.

Zadanie 5. Udowodnij, że kod długości 2^m, wymiaru $2^m - m - 1$ i minimalnej odległości słów kodowych równej 4 jest (z dokładnością do porządku bitów) rozszerzonym kodem Hamminga.

Zadanie 6. (Metoda szukania kodów cyklicznych, a więc rozkładania wielomianów $x^n + 1$ na czynniki nad ciałem Z_2)

1. Udowodnij, że kwadrat wielomianu dodatniego stopnia nie dzieli wielomianu $x^{2 \cdot n+1} + 1$. Wskazówka: oblicz formalną pochodną podanego wielomianu na dwa sposoby i zauważ, że jest z tym wielomianem względnie pierwsza.
2. Udowodnij, że jeżeli $g(x) \cdot h(x) = x^{2 \cdot n+1} + 1$, to wielomiany $g(x)$ i $h(x)$ są względnie pierwsze.

3. Zauważ, że funkcja $f(x) = 2 \cdot x \bmod (2 \cdot n + 1)$ jest permutacją zbioru $\{k \in N : k < 2 \cdot n + 1\}$, a więc rozbija ten zbiór na rozłączne cykle (minimalne zbiory zamknięte ze względu na f).

4. Niech C będzie cyklem, o którym mowa w poprzednim zadaniu. Zdefiniujmy wielomian I przyjmując $I(x) = \sum_{i \in C} x^i$. Udowodnij, że $x^{2 \cdot n+1} + 1$ dzieli wielomian $I^2(x) - I(x)$. Wielomiany o tej własności będziemy nazywać idempotentami.

5. Udowodnij, że każdy inny idempotent jest sumą idempotentów zdefiniowanych w poprzednim zadaniu (a więc potrafimy znaleźć wszystkie idempotenty).

6. Przypuśćmy, że $g(x) \cdot h(x) = x^{2 \cdot n+1} + 1$. Wtedy $1 = u(x) \cdot g(x) + w(x) \cdot h(x)$ dla pewnych wielomianów $u(x)$ i $w(x)$. Pomnóz podaną równość przez i zauważ, że $u(x) \cdot g(x)$ jest idempotentem. Udowodnij, że ponadto największym wspólnym dzielnikiem wielomianów $u(x) \cdot g(x)$ i $x^{2 \cdot n+1} + 1$ jest $g(x)$.

7. Przedstaw wielomian $x^{100} + 1 \in Z_2[x]$ w postaci iloczynu wielomianów nierozkładalnych.

Zadanie 7. Zauważ, że jeżeli K jest kodem Reeda-Solomona długości n, wymiaru k i minimalnej odległości słów kodowych d, to $d = n - k + 1$ (wiąże się to z zadaniami z dwóch ostatnich list).

Antoni Kościelski, 8 lutego 2001 roku