Kodowanie

Lista nr 7.

Zadanie 1. Opracuj algorytm korygujący błędy dla kodu Golay'a oparty o następującą ideę: w danym słowie szukamy jednego z błędów, jeżeli błąd znajdziemy, to pozostałe korygujemy stosując algorytm error-trapping.

Zadanie 2. Niech F będzie ciałem skończonym o $n+1$ elementach Oczywiście, w F istnieje element β taki, że $\beta^n = 1$ oraz $\beta^i \neq 1$ dla i takich, że $0 < i < n$. Niech t będzie liczbą spełniającą nierówność $2 \cdot t < n$. Rozważmy

$$K = \{w \in F^{n-1}[x] : \forall i\ 0 < i \leqslant 2 \cdot t \Rightarrow w(\beta^i) = 0\}.$$

Udowodnij, że zbiór K jest kodem cyklicznym. Znajdź generator kodu K. Udowodnij, że minimalna odległość Hamminga słów kodu K jest równa $2 \cdot t + 1$. Kody tej postaci nazywamy kodami Reeda-Solomona.

Zadanie 3. Zbadaj kody Reeda-Solomona dla $n = 6$.

Zadanie 4. Niech F będzie ciałem o $2^m = 8$ elementach (ciałem $Z_2^2[x]$ z mnożeniem modulo $1 + x + x^3$). Zbadaj kod K Reeda-Solomona otrzynamy dla $n = 7$ (i, wobec tego, ciała F) oraz dla $t = 2$. Dla każdego $a \in F$ niech $p(a)$ oznacza słowo $a_0a_1a_2 \in Z_2^3$ takie, że $a = a_0 + a_1 \cdot x + a_2 \cdot x^2$. Niech

$$K_b = \{p(w_0) \dots p(w_6) : \sum_{i=0}^{6} w_i \cdot x^i \in K\}.$$

Udowodnij, że K_b jest kodem korygującym pęknięcia długości $(t-1) \cdot m + 1$, czyli długości 4. Zauważ, że konstrukcję z tego zadania można uogólnić zachowując podaną własność.

Zadanie 5. Niech F będzie podciałem ciała F', $r(x) \in F'[x]$ – wielomianem stopnia $t \geqslant 2$, a $a_1, \dots, a_n \in F'$ – wybranymi elementami, które nie są pierwiastkami równania $r(x) = 0$. Jeżeli a nie jest pierwiastkiem równania $r(x) = 0$, to wprowadzamy oznaczenie

$$\frac{1}{x-a} = \frac{1}{r(a)} \cdot \frac{r(x) - r(a)}{x - a} \in F'[x].$$

Niech

$$K = \{v_1 \dots v_n \in F^n : \sum_{i=1}^{n} \frac{v_i}{x - a_i} = 0\}.$$

Zauważ, że K jest kodem liniowym. (Nazywamy go kodem Goppa.) Udowodnij, że K jest zbiorem rozwiązań jednorodnego układu równań liniowych, którego macierzą główną jest $H = (h_{i,j})_{i=1,\dots,n, j=1,\dots,t}$, gdzie $h_{i,j} = \frac{a_i^{j-1}}{r(a_i)}$.

Zadanie 6. Sprawdź, że jeżeli $F = Z_2$, F' ma 8 elementów, to wielomian $r(x) = x^2 + x + 1$ jest nierozkładalny nad F'. Znajdź kod K opisany w poprzednim zadaniu dla podanych F, F' i r oraz ciągu $a_1, \dots, a_8$ parami różnych elementów F'.

Zadanie 7. Niech F' będzie ciałem o $n+1$ elementach, $r(x) = x^{2 \cdot t}$ i niech $\beta^n, \beta^{n-1}, \dots, \beta$ będzie ciągiem wszystkich niezerowych elementów F'. Udowodnij, że w tym przypadku kod Goppa jest kodem BCH.

Zadanie 8. Udowodnij, że dla kodu Goppa wyznaczonego przez wielomian stopnia t minimalna odległość słów kodowych od 0 jest $\geqslant t+1$. Wskazówka: dowodzi się to tak, jak analogiczne twierdzenie dla kodów BCH. Można też dowieść, że binarny kod Goppa wyznaczony przez nieredukowalny wielomian stopnia t koryguje t błędów.

Antoni Kościelski, 25 stycznia 2001 roku