Kodowanie

Lista nr 1 (dodatkowa).

Uogólnimy pojęcia wykrywania i korygowania błędu. Niech F będzie dowolnym ciałem skończonym. Błędem będziemy teraz nazywać różnicę między słowem odebranym i przesyłanym, a nie pozycję różniącą te dwa słowa.

Zadanie 1. Przyjmujemy, że kod $K \subseteq F^n$ wykrywa błąd $u \in F^n$ wtedy i tylko wtedy, gdy dla każdego $v \in K$ słowo $v + u$ nie należy do K.

1. Udowodnij, że jeżeli kod K wykrywa t błędów, to wykrywa każdy błąd u ze zbioru $S_t(\vec{0}) \setminus \{\vec{0}\}$.
2. Rozważmy kod $K = \{0000, 0101, 1111\}$. Minimalna odległość słów kodu K jest równa 2, a więc ten kod wykrywa 1 błąd. Wobec tego, wykrywa błędy 1000, 0100, 0010 oraz 0001. Wykrywa także błąd 1001, ale nie wykrywa błędu 1010. Opisz błędy wykrywane przez kod K.
3. Znajdź błędy wykrywane przez kod K przy założeniu, że K jest kodem liniowym.

Zadanie 2. Kod K koryguje błąd u wtedy i tylko wtedy, gdy dla dowolnych, różnych $v, v' \in K$ odległość $d(v+u, v)$ jest mniejsza od $d(v+u, v')$. Rozważmy algorytm, który dla danego słowa w zwraca słowo należące do K najmniej różniące się od w, i który nic nie zwraca, jeżeli są dwa słowa najmniej różniące się od w. Udowodnij, że kod K koryguje błąd u wtedy i tylko wtedy, gdy podany algorytm uruchomiony z dowolnym słowem postaci $v + u$ dla $v \in K$ zwraca słowo v.

Zadanie 3. Udowodnij, że jeżeli kod K koryguje t błędów, to koryguje błędy należące do $S_t(\vec{0})$.

Zadanie 4. Przypuśćmy, że mamy słowa $u_1 = a_1 \ldots a_n$ i $u_2 = b_1 \ldots b_n$ takie, że warunek $b_i = 1$ implikuje $a_i = 1$. Udowodnij, że jeżeli kod K koryguje błąd u_1, to koryguje także błąd u_2.

Zadanie 5. Aby przekonać się, które błędy są korygowane, można zbudować tablicę, której kolumny są indeksowane słowami kodu, a wiersze - dowolnymi słowami, wypełnioną sumami odpowiednich indeksów (błędami obliczonymi przy założeniu, że został wysłany indeks kolumny i został odebrany indeks wiersza). Zbuduj taką tablicę dla kodu $K = \{0000, 0001, 1110\}$. Ustal, jakie błędy są korygowane przez ten kod.

Zadanie 6. Niech G będzie macierzą o m liniowo niezależnych wierszach długości n. Udowodnij, że jeżeli A jest macierzą o wymiarach $m \times m$ i niezerowym wyznaczniku, to macierze G i $A \cdot G$ generują ten sam kod liniowy.

Zadanie 7. Niech G będzie macierzą o m liniowo niezależnych wierszach długości n. Udowodnij, że dowolny kod liniowy długości n i wymiaru m jest generowany przez macierz postaci $G \cdot A$ dla macierzy A o wymiarach $n \times n$ i niezerowym wyznaczniku.

Zadanie 8. Niech G będzie macierzą o m liniowo niezależnych wierszach długości n. Udowodnij, że jeżeli A jest macierzą o wymiarach $n \times n$ zawierającą w każdym wierszu i każdej kolumnie dokładnie jedną 1 i poza tym same 0, to macierze G i $G \cdot A$ generują kody liniowe o tej samej minimalnej odległości słów kodowych.

Zadanie 9. Niech K będzie kodem liniowym wymiaru k, długości n o minimalnej odległości słów kodowych d. Udowodnij, że $d - 1 \leqslant n - k$. Wskazówka: przedstaw kod K jako zbiór rozwiązań układu równań liniowych i zastosuj zadanie ze sprawdzianu charakteryzujące kody o minimalnej odległości d.

Zadanie 10. Niech K będzie kodem liniowym wymiaru k, długości n o minimalnej odległości słów kodowych d, generowanym przez macierz G, będącym rozwiązaniem układu równań liniowych z macierzą główną równą H. Udowodnij, że następujące warunki są równoważne:

1. $d = n - k + 1$,
2. każdy zbiór $n - k$ kolumn macierzy H jest liniowo niezależny,
3. każdy zbiór k kolumn macierzy G jest liniowo zależny.

Zadanie 11. Niech K będzie kodem liniowym wymiaru k, długości n o minimalnej odległości słów kodowych $n - k + 1$. Udowodnij, że kod dualny $K^{\perp}$ jest kodem liniowym o minimalnej odległości słów kodowych $k + 1$.

Zadanie 12. Skonstruuj binarny kod liniowy długości 9, wymiaru 2, o minimalnej odległości słów kodowych równej 5. Wskazówka: zbuduj macierz macierz układu równań definiującego ten kod: każde $\leqslant 4$ kolumny tej macierzy powinny być liniowo niezależne, jeżeli wybraliśmy już jakieś kolumny, to nie możemy już do tej macierzy dołączyć sumy $\leqslant 3$ wybranych kolumn, na początku możemy wybierać kolumny z jedną jedynką.

Zadanie 13. Udowodnij, że jeżeli

$$\sum_{i=0}^{d-2} \binom{n-1}{i} < 2^{n-k},$$

to istnieje binarny kod liniowy długości n, wymiaru k, o minimalnej odległości słów kodowych równej d. Wskazówka: zauważ, że podany warunek gwarantuje wykonalność konstrukcji z poprzedniego zadania.

Zadanie 14. Udowodnij, że jeżeli K jest doskonałym kodem długości n o minimalnej odległości słów kodowych $2 \cdot t + 1$, to kod K nie koryguje błędów $u \notin S_t(\vec{0})$.

Antoni Kościelski, 8 lutego 2001 roku