Egzamin z Teorii informacji. Rozwiązanie zadania 1.

1. Niech C_i, dla $i = 1, 2$, będzie kodem liniowym nad ciałem $\mathbb{F}_2$ o minimalnej odległości słów kodowych d_i. Niech ponadto d_0 oznacza minimalną odległość słów kodowych kodu $C_1 \cap C_2$ oraz d_3 oznacza minimalną odległość słów kodowych kodu $C_1 + C_2 = \{a + b : a \in C_1,\ b \in C_2\}$. Niech d oznacza minimalną odległość słów kodowych kodu $\{(a + b, a' + b, a + a' + b) : a, a' \in C_1,\ b \in C_2\}$. Wykaż, że $d \geq \min(d_0, 2 \cdot d_1, 3 \cdot d_3)$.
Rozwiązanie.

Zauważmy najpierw, że skoro C_i są kodami liniowymi, to kody $C_1 + C_2$ oraz $C = \{(a + b, a' + b, a + a' + b) : a, a' \in C_1,\ b \in C_2\}$ również są kodami liniowymi (dowód bardzo prosty — pomijamy). W związku z tym, aby obliczyć minimalną odlegość słów kodowych dla C, wystarczy obliczyć najmniejszą wagę Hamminga $wt(c)$ niezerowego słowa kodowego $c \in C$, $c \neq (0, 0, 0)$.

Uwaga: w zadaniu mamy pokazać, że $d \geq \min(d_0, 2 \cdot d_1, 3 \cdot d_3)$, czyli że dla każdego $c \in C$, $c \neq (0, 0, 0)$ zachodzi $wt(c) \geq d_0$ lub $wt(c) \geq 2d_1$ lub $wt(c) \geq 3d_3$. Większość osób pokazywało np., że dla *pewnych* $c_a, c_b, c_c \in C$ mamy $wt(c_a) \geq d_0$, $wt(c_b) \geq 2d_1$ oraz $wt(c_c) \geq 3d_3$ (często twierdząc, że pokazują coś innego), z czego niewiele wynika (albo też rozważano tylko $c = (x_1, x_2, x_3)$ dla których $x_1 \neq 0, x_2 \neq 0, x_3 \neq 0$).

Weźmy zatem $c = (x_1 = a + b, x_2 = a' + b, x_3 = a + a' + b) \in C, c \neq 0$, czyli $(x_1, x_2, x_3) \neq (0, 0, 0)$. Rozważmy 3 przypadki: a) $x_1 \neq 0, x_2 \neq 0, x_3 \neq 0$, b) $x_1 = 0, x_2 \neq 0, x_3 \neq 0$, a) $x_1 = 0, x_2 = 0, x_3 \neq 0$, Zauważmy, że $C = \{(a + b, a' + b, a'' + b) : a, a', a'' \in C_1$, takie że $a + a' + a'' = 0,\ b \in C_2\}$. W związku z tym pozostałe przypadki są symetryczne, więc nie musimy ich osobno rozważać.

a) $x_1 \neq 0, x_2 \neq 0, x_3 \neq 0$, zatem dla $i = 1, 2, 3$ mamy $wt(x_i) \geq d_3$ (gdyż $x_i \in C_1 + C_2$), stąd $wt(c) = wt(x_1) + wt(x_2) + wt(x_3) \geq 3d_3$.

b) $x_1 = a + b = 0, x_2 = a' + b \neq 0, x_3 = a + a' + b \neq 0$, stąd $b = a \in C_1$. Zatem $0 \neq x_2, x_3 \in C_1$, więc dla $i = 2, 3$ mamy $wt(x_i) \geq d_1$, czyli $wt(c) \geq 2d_1$.

c) $x_1 = a + b = 0, x_2 = a' + b = 0, x_3 = a + a' + b \neq 0$, zatem $a = b = a' = x_3 \in C_1 \cap C_2$, więc $wt(c) \geq d_0$.

Stąd zawsze dla $c \in C, c \neq 0$ mamy $wt(c) \geq \min(d_0, 2d_1, 3d_3)$, czyli minimalna odległość słów kodowych kodu C wynosi co najmniej $\min(d_0, 2d_1, 3d_3)$.