Teoretyczne podstawy informatyki
Wykłady XI, XII. Teoria kodów.

Wprowadzone pojęcia: Kody, rozstęp kodu, kod doskonały, kody liniowe, $[n, k]$-kod, $[n, k, d]$-kod, kody Hamminga.

Podstawowe definicje i twierdzenia

Twierdzenie 1. *Dla każdego kodu C nad ciałem $\mathbb{F}_q$ o długości n i rozstępie $2r + 1$ zachodzi*

$$q^n \geqslant |C| \sum_{i=0}^{r} \binom{n}{i} (q-1)^i .$$

Ponadto, w powyższej nierówności wystepuje równość wtedy i tylko wtedy, gdy C jest kodem doskonałym.

Twierdzenie 2. *Jeśli macierz generująca $[n, k]$-kodu C ma postać $\mathbf{G} = [\mathbf{I}_k \mathbf{P}]$, to $\mathbf{H} = [-\mathbf{P}^T \mathbf{I}_{n-k}]$ jest macierzą (sprawdzania) parzystości tego kodu. W powyższym zapisie $\mathbf{I}_\ell$ oznacza macierz jednostkową o wymiarze ℓ, a $\mathbf{P}^T$ macierz transponowaną do $\mathbf{P}$.*

Twierdzenie 3. *Niech C będzie kodem o macierzy parzystości $\mathbf{H}$. Aby znaleźć słowo kodu najbliższe słowu $\mathbf{x}$, należy znaleźć słowo $\mathbf{y}$ takie, by zachodziło*

$$\mathbf{Hy} = \mathbf{Hx} \qquad (*)$$

i spośród słów spełniających powyższą równość $(*)$ słowo $\mathbf{y}$ miało najmniej wyrazów niezerowych. Wtedy $\mathbf{z} = \mathbf{x} - \mathbf{y}$ jest szukanym słowem z kodu C leżącym najbliżej $\mathbf{x}$.