

ADS 2 příklady na cvičení

25. 11. 2020

1. Pro odpálení jaderné bomby je potřeba, aby se na tom shodlo alespoň k z celkového počtu n generálů. Vymyslete, jak z odpalovacího kódu odvodit n klíčů pro generály tak, aby libovolná skupina k generálů uměla ze svých klíčů kód vypočítat, ale žádná menší skupina nemohla o kód zjistit nic než jeho délku.
2. Dokažte, že pro každou primitivní n -tou odmocninu z jedničky α platí, že $\alpha = \omega^t$, kde $\omega = e^{2\pi i/n}$ a t je přirozené číslo nesoudělné s n . Kolik primitivních n -tých odmocnin tedy existuje?
3. Dokažte, že pro sudé n a libovolné číslo ω , které je primitivní n -tou odmocninou z jedničky, platí:
 - $\omega^j \neq \omega^k$, kdykoliv $0 \leq j < k < n$.
 - $\omega^{n/2} = -1$
4. DFT je lineární zobrazení. Jde proto zapsat jako násobení nějakou maticí Ω , kde $\Omega_{jk} = \omega^{jk}$. Nalezněte inverzní matici Ω^{-1} . Jelikož $\omega^{-1} = \bar{\omega}$, zkuste, zda hledanou inverzní maticí není $\bar{\Omega}$.
5. Spočítejte Fourierovy obrazy následujících vektorů z \mathbb{C}^n :
 - $(0, \dots, 0)$
 - (x, \dots, x)
 - $(1, -1, 1, -1, \dots, 1, -1)$
 - $(1, 0, 1, 0, 1, 0, 1, 0)$
 - $(\omega^0, \omega^1, \omega^2, \dots, \omega^{n-1})$
 - $(\omega^0, \omega^2, \omega^4, \dots, \omega^{2n-2})$
6. Volba ω : Ve Fourierově transformaci máme volnost v tom, jakou primitivní odmocninu ω si vybereme. Ukažte, že Fourierovy obrazy pro různé volby ω se liší pouze pořadím složek.