01204211: Exercises 8-1

Notes: To avoid confusion, in your answer, you can write vectors with this notation $\vec{u}$.

1. Recall our definition of dot products. Consider vectors over field $\mathbb{F}$. Suppose that $\boldsymbol{u} = [u_1, u_2, \ldots, u_n]$ and $\boldsymbol{v} = [v_1, v_2, \ldots, v_n]$. We define $\boldsymbol{u} \cdot \boldsymbol{v} = \sum_{i=1}^{n} u_i \times v_i$. Using properties of field $\mathbb{F}$, prove that the dot product is commutative, i.e., prove that $\boldsymbol{u} \cdot \boldsymbol{v} = \boldsymbol{v} \cdot \boldsymbol{u}$.

2. *Authentication scheme.* A simple password authentication scheme is not secure against eavesdropping. A more secure scheme is a *challenge-response* scheme, where the system asks a series of questions the user who has the password should provide correct answers. Consider a simple scheme that works with n-vectors over $GF(2)$. The user has an n-bit vector (n-vector over $GF(2)$) $\boldsymbol{p}$ as a password. The system picks k random n-vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$, and for k successive rounds asks the user the following questions.

   - For $i = 1, 2, \ldots, k$, in round i, the server provides $\boldsymbol{u}_i$ to the user.
   - The user replies with $\boldsymbol{r}_i = \boldsymbol{u}_i \cdot \boldsymbol{p}$.
   - The server checks if the anser $\boldsymbol{r}_i$ is in fact the correct answer $\boldsymbol{u}_i \cdot \boldsymbol{p}$.

   Suppose that Eve, the eavesdroper, sees (in clear text) one correct authentication of Alice, i.e., she sees $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ and $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_k$.

   (a) Suppose that Eve tries to log in as Alice. Give the condition on the question $\boldsymbol{v}$ from the server that, given the information that she currently has, Eve can answer correctly.

   (b) Suppose that Eve would like to figure our Alice's password vector $\boldsymbol{p}$. Write down a system of linear equations that she has to solve.

3. *Span test 1.* Consider 3-vectors over $\mathbb{R}$. Let $\boldsymbol{u}_1 = [1, 0, 0], \boldsymbol{u}_2 = [0, 1, 0], \boldsymbol{u}_3 = [0, 0, 1]$.
(a) Show that $\boldsymbol{v} = [10, 13, 29] \in \text{Span } \{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3\}$.

(b) Show that in general $\boldsymbol{v}' = [a, b, c] \in \text{Span}\{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3\}$ for any a, b, c.

4. *Span test 2.* Consider 3-vectors over $\mathbb{R}$. Let $\boldsymbol{u}_1 = [1, 0, 0], \boldsymbol{u}_2 = [0, 1, 0], \boldsymbol{u}_3 = [0, 1, 1]$.
(a) Show that $\boldsymbol{v} = [10, 13, 29] \in \text{Span } \{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3\}$.
Hint: try to find a way to write $[0, 0, 1]$ *as a linear combination of the vectors first.*

(b) Show that in general $\boldsymbol{v}' = [a, b, c] \in \text{Span}\{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3\}$ for any a, b, c.