Problem 8): This **MAC** is *not* secure due to the high probability of collisions. To see this, consider any two messages $m, m^\star \in \mathcal{M}$ such that $m = \{m_1, m_2, \ldots, m_k, \ldots, m_l\}$, $m^\star = \{m_1^\star, m_2^\star, \ldots, m_k^\star, \ldots, m_l^\star\}$, $m_i = m_j^\star$, $m_j = m_i^\star$, and $m_k = m_k^\star$ for all other $k < l$. Then, clearly we have

$$t = F_k(m_1) \oplus F_k(m_2) \oplus \cdots F_k(m_i) \oplus \cdots \oplus F_k(m_j) \oplus \cdots \oplus F_k(m_l)$$

which, by the the of **XOR**, is equivalent to

$$t = F_k(m_1) \oplus F_k(m_2) \oplus \cdots F_k(m_j) \oplus \cdots \oplus F_k(m_i) \oplus \cdots \oplus F_k(m_l)$$

Applying our definitions for m and $m^\star$ from above, we clearly see that

$$\begin{aligned} t &= F_k(m_1) \oplus F_k(m_2) \oplus \cdots F_k(m_j) \oplus \cdots \oplus F_k(m_i) \oplus \cdots \oplus F_k(m_l) \\ &= F_k(m_1^\star) \oplus F_k(m_2^\star) \oplus \cdots F_k(m_i^\star) \oplus \cdots \oplus F_k\left(m_j^\star\right) \oplus \cdots \oplus F_k(m_l^\star) = t^\star \end{aligned}$$

thereby showing collisions for this hash function.

We can calculate the probability of finding a collision here. There are $N_{TOT} = \prod_{i=1}^{l}\{2^n\} = (2^n)^l$ total possible messages with l blocks and block-length n. Out of these, there are $N_{NO-COL} = \prod_{i=1}^{l}\{2^n - i + 1\}$ messages that will have no collisions because one message is removed from the number available for each subsequent block. Therefore, the number of messages with collisions in the *must* be

$$\begin{aligned} N_{COL} = N_{TOT} - N_{NO-COL} &= \prod_{i=1}^{l}\{2^n\} - \prod_{i=1}^{l}\{2^n - i + 1\} \\ &= (2^n)^l - \prod_{i=1}^{l}\{2^n - i + 1\} \end{aligned} \tag{8.1}$$

This allows the probability