Problem 1: Missing claims from QKD proof

(a) In the practice we showed (or will show) that in our QKD protocol, after the Bell test and after measuring the $n$-bit raw key, we have

$$H_\infty(K_A|E)_{\rho_{\text{raw}}} \geq -\log(N2^{-n})$$

where $N := |\{xy \in \{0,1\}^{2n} : |xy| \leq t\}|$. (Note: $|xy|$ does not refer to the Hamming weight of $xy$ here, but to the number of non-00 bitpairs.)

Show that $N \leq (3n + 1)^t$.

**Hint:** Think of how you can compactly describe the bitstring $xy$ with $|xy|$ by only telling where the non-00 pairs are, and then calculate how many such descriptions there are.

Problem 2: Universal hash functions

(a) Let $S$ be the set of all binary $\ell \times m$-matrices. I.e., $S = \mathbb{F}_2^{\ell \times m}$. Let $X$ be the set of all $m$-bit vectors. I.e., $X = \mathbb{F}_2^m$. Let $Y = \mathbb{F}_2^{\ell}$. Let $F : S \times X \to Y$ be defined as $F(s, x) := sx$.

Show that $F$ is a universal hash function.

**Note:** You may use the fact that for any fixed $z \neq 0$, and uniformly distributed $s \in \mathbb{F}_2^{\ell \times m}$, $sz$ is uniformly distributed on $\mathbb{F}_2^{\ell}$. (Bonus points if you prove that fact, too.)

**Note:** This was sketched in the lecture. You only get points if your proof goes beyond the sketch in the lecture in detail/rigor.

(b) (Bonus problem) Let $S := X := \mathbb{F}_{2^m}$ be a finite field (encoded in the standard way as an $\mathbb{F}_2$ vector space). Let $\text{trunc}_\ell(x)$ denote the first $\ell$ bits of $x$. Let $Y := \{0,1\}^{\ell}$. Let $F : S \times X \to Y$ be defined as $F(s, x) := \text{trunc}_\ell(sx)$.

Show that $F$ is a universal hash function.

**Note:** You may use that $\text{trunc}_\ell(a - b) = \text{trunc}_\ell(a) - \text{trunc}_\ell(b)$. (This is immediate from the encoding of $\mathbb{F}_{2^m}$.)