Slide #4. Proof sketch that $|C| = |C + u|$ where u is any word in K^n (as usual, $|A|$ denotes the number of elements of the set A). Let $\psi : C \to C + u$ be the map given by $\psi(c) = c + u$. Show that:

1. ψ is injective (i.e., one-to-one):
$$\psi(c_1) = \psi(c_2) \Longleftrightarrow c_1 = c_2.$$
2. ψ is surjective (onto): Let y be an arbitrary element of $C+u$, i.e., $y = c+u$ for some $c \in C$. Then $\psi(y+u) = y$.

Thus, ψ is bijective. The existence of a bijection between two finite sets shows that they have the same number of elements.

* * *

Proof sketch of that either
$$C + u = C + v \;\text{ or }\; (C + u) \cap (C + v) = \emptyset :$$
Suppose there exists $z \in (C + u) \cap (C + v)$. Then $z = c_1 + u = c_2 + v$ for some $c_1, c_2 \in C$. Thus,
$$u = c_1 + c_2 + v = c_3 + v$$
where $c_3 \in C$. That is, $u = c_3 + v$ for some $c_3 \in C$. Now, one has
$$C + u = C + (c_3 + v) = \{c + c_3 + v \,|\, c \in C\} = C + v.$$
The above means that if cosets $C + u$ and $C + v$ have one element in common, then they must coincide.

* * *

Proof sketch of consequence #4 regarding the *number of cosets of an (n, k) linear code* C. Let M be the number of such cosets. The cosets partition the space K^n, meaning that K^n is a *disjoint* union of the M cosets of C:

$$K^n = \text{coset}_1 \sqcup \text{coset}_2 \sqcup \cdots \sqcup \text{coset}_M.$$

Each coset has the same number of elements as C, namely, 2^k. Thus,

$$2^n = 2^k \cdot M,$$

whence $M = 2^n/2^k = 2^{n-k}$. This is an important result to remember!