

**Lemma 2.** Let  $V$  be a finite vector space and let  $\alpha \in (0, 1)$  be a real number. Let  $A$  be a random uniformly chosen subset of  $V$  of size  $|V|(1 - \alpha)$  and  $v$  be a random uniformly chosen vector of  $V$  independent of  $A$ . Then

$$\mathbf{E}(1 - \frac{|A \cup (v + A)|}{|V|}) = \alpha^2.$$

*Proof.* For a fixed vector  $u \in V$ , let  $X_u = |A \cup (u + A)|$  be a random variable where  $A$  is a random uniformly chosen subset of  $V$  of size  $|V|(1 - \alpha)$ . Let  $v$  be a random uniformly chosen vector  $v \in V$ . Then

$$\mathbf{E}(1 - \frac{|A \cup (v + A)|}{|V|}) = (1 - \frac{\sum_{u \in V} \mathbf{P}(v = u) \mathbf{E}(X_u)}{|V|}) = \frac{\sum_{u \in V} (1 - \frac{\mathbf{E}(X_u)}{|V|})}{|V|}$$

because  $\mathbf{P}(v = u) = \frac{1}{|V|}$ .

First we compute  $\mathbf{E}(X_u)$  for a fixed vector  $u$ . For a random vector  $v$  we have that probability  $v \in A$  is  $|V|(1 - \alpha)|V|^{-1} = 1 - \alpha$ . Thus probability of  $v \notin A$  is  $\alpha$  and also probability that  $v \notin u + A$  is  $\alpha$  because  $|A| = |(u + A)|$ . Hence

$$\begin{aligned} \mathbf{E}(X_u) &= \sum_{v \in V} 1 \mathbf{P}((v \in A) \vee (v \in (u + A))) = \\ &= \sum_{v \in V} 1 - \mathbf{P}((v \notin A) \wedge (v \notin (u + A))) = \\ &= \sum_{v \in V} 1 - \mathbf{P}(v \notin A) \mathbf{P}(v \notin (u + A)) = \\ &= \sum_{v \in V} 1 - \alpha^2 = |V|(1 - \alpha^2). \end{aligned}$$

If we substitute the value  $\mathbf{E}(X_u)$  we obtain

$$\begin{aligned} \mathbf{E}(1 - \frac{|A \cup (v + A)|}{|V|}) &= \frac{\sum_{u \in V} (1 - \frac{\mathbf{E}(X_u)}{|V|})}{|V|} = \frac{\sum_{u \in V} (1 - \frac{|V|(1 - \alpha^2)}{|V|})}{|V|} = \\ &= \frac{\sum_{u \in V} (1 - (1 - \alpha^2))}{|V|} = \frac{\sum_{u \in V} \alpha^2}{|V|} = \alpha^2 \quad \square. \end{aligned}$$