

Lemma

$$b, k, l > 0$$

$$l > \max(8, k)$$

$$C \subseteq \Sigma^k$$

Randomly select  $l$  linear functions  $h_1 \dots h_l: \Sigma^k \rightarrow \Sigma^b$

Randomly select  $l^2$  strings  $z_1 \dots z_{l^2} \in \Sigma^b$

$$H(C) = \{w \mid \text{for some } i, x \in C, h_i(x) = w\}$$

$$\text{if } |C| = \frac{2^b}{4} \text{ then } \Pr(H(C) \cap Z \neq \emptyset) \geq 1 - 2^{-\frac{l}{4}}$$

$$\text{Assume } |C| = 2^b/4$$

$$\Pr(\exists y \in C \text{ s.t. } x \neq y \ \& \ h_i(x) = h_i(y)) \leq |C| \cdot \left(\frac{1}{2}\right)^b = \frac{1}{4}$$

$$\Pr(\forall i \ 1 \leq i \leq l \ \exists y \in C \text{ s.t. } x \neq y \ \& \ h_i(x) = h_i(y)) \leq \left(\frac{1}{4}\right)^l$$

$$\Pr(\exists x \in C \text{ s.t. } \forall i \ \exists y \neq x \in C \text{ s.t. } h_i(x) = h_i(y)) \leq |C| \cdot \left(\frac{1}{4}\right)^l = \frac{2^b}{4} \cdot \left(\frac{1}{4}\right)^l \leq 2^{-l}$$

$$\Pr(H(C) \geq \frac{|C|}{l}) \leq 2^{-l}$$

$$\forall x \in C \exists i \text{ s.t. } \forall y \in C \ h_i(x) \neq h_i(y)$$

$$\text{for } \frac{|C|}{l} \text{ x's } \forall y \in C \ h_i(x) \neq h_i(y)$$

$h_i$  random 0/1 matrix:  $h_i(x) = h_i \cdot x$  over GF(2)

$$h_i(x) \in \Sigma^b$$

$h_i^{(j)}(x)$   $j$ th bit of  $h_i(x)$

$$\text{if } x \neq y \ \Pr(h_i^{(j)}(x) = h_i^{(j)}(y)) = \frac{1}{2}$$

$$\Pr(h_i(x) = h_i(y)) = \Pr(\forall h_i^{(j)}(x) = h_i^{(j)}(y)) = \left(\frac{1}{2}\right)^b$$

$$\text{Assume } H(C) \geq \frac{|C|}{l}$$

$$\Pr(z_j \in H(C)) \geq \frac{1}{2^b} \cdot \frac{|C|}{l} = \frac{1}{4l}$$

$$\Pr(z_j \notin H(C)) \leq \frac{1}{2^b} \cdot \frac{|C|}{l} = 1 - \frac{1}{4l}$$

$$\Pr(\forall i \ z_i \notin H(C)) \leq \left(1 - \frac{1}{4l}\right)^{l^2} + 2^{-l} \leq 2^{-\frac{l}{4}}$$