Lemma 7.5 *Let* P_0 *be the uniform distribution on a finite subgroup* H *of* $\mathbf{C}^\times$ *of order* d*. Let* $\mathcal{D} = \{\mathsf{P}_u : u \in \mathsf{H}\}$ *be a set of* d *distributions on* H *defined by* (7.10)*. The* q*-limited distinguisher between the null hypothesis* $\mathsf{H}_0 : \mathsf{P} = \mathsf{P}_0$ *and the alternate hypothesis* $\mathsf{H}_1 : \mathsf{P} \in \mathcal{D}$ *defined by the distribution acceptance region* $\Pi^\star_q = \Pi^\star \cap \mathcal{P}_q$*, where*

$$\Pi^\star = \left\{ \mathsf{P} \in \mathcal{P} \ : \ \|\mathsf{P}\|_\infty \geq \frac{\log(1-\epsilon)}{\log(1-\epsilon) - \log(1+(d-1)\epsilon)} \right\}, \tag{7.11}$$

is asymptotically optimal and its advantage $\mathrm{BestAdv}_q$ *is such that*

$$1 - \mathrm{BestAdv}_q(\mathsf{H}_0, \mathsf{H}_1) \doteq 2^{q \inf_{0<\lambda<1} \log \frac{1}{d}\left((1+(d-1)\epsilon)^\lambda + (d-1)(1-\epsilon)^\lambda\right)}.$$