1. Proof of Theorem 9.1

Proof. Assume for contradiction that there exists a circuit C of size $s = 2^{o(t\sqrt{\log n})}$ computing $\mathrm{SearchSAT}^t$.

By Lemma~[lemma:component-independence], with high probability the adversarial distribution $\mathcal{D}_C$ preserves a set S of components with $|S| \geq t/2 - \sqrt{t \log t}.

For each preserved component $i \in S$, the restricted function $f_i|_{\rho_i}$ requires circuits of size $2^{\Omega(\sqrt{\log n})}$ (by the base Tseitin lower bound).

By the product bound in Lemma~[lemma:component-independence], the composed restricted function requires circuits of size:

$$\mathrm{Csize}(f|_\rho) \geq \prod_{i \in S} \mathrm{Csize}(f_i|_{\rho_i}) \geq \left(2^{\Omega(\sqrt{\log n})}\right)^{|S|} = 2^{\Omega(|S| \cdot \sqrt{\log n})}$$

Since $|S| = \Omega(t)$, we have:

$$\mathrm{Csize}(f|_\rho) \geq 2^{\Omega(t \cdot \sqrt{\log n})}$$

However, the restricted circuit $C|_\rho$ has size at most s, leading to the contradiction:

$$2^{\Omega(t \cdot \sqrt{\log n})} \leq s = 2^{o(t\sqrt{\log n})}$$

This contradiction proves the theorem. □