The Non-Uniform Hierarchy Theorem

Wolfgang Mulzer

1 The Theorem

Theorem 1.1 (Shannon's theorem)**.** *There exist constants $c_1 \geq 1$ and $c_2 > 0$ such that for all $n \in \mathbb{N}$, (a) every Boolean function $f : \{0,1\}^n \to \{0,1\}$ can be realized by a Boolean circuit of size at most $c_1 2^n/n$; and (b) there exists a Boolean function $g : \{0,1\}^n \to \{0,1\}$ that cannot be realized by a Boolean circuit of size at most $c_2 2^n/n$.*

Theorem 1.2 (Non-uniform Hierarchy Theorem)**.** *There is a constant $c_3 > 0$ such that for any $T, T' : \mathbb{N} \to \mathbb{N}$ with $T(n) \leq c_3 T'(n)$ and $T'(n) \leq c_1 2^n/n$, for $n \in \mathbb{N}$, there exists a language $L \subseteq \{0,1\}^*$ such that L that cannot be decided by a circuit family of size at most $T(n)$, but there is a circuit family of size at most $T'(n)$ that decides L.*

Proof. Set $c_3 = c_2/2c_1$ and define $f(n) = \max\{m \in \mathbb{N} \mid c_1 2^m/m \leq n\}$, for $n \geq 2c_1$. For any $n \geq 2c_1$ and $m = f(n)$, we have $c_1 2^m/m > n/2$, because

$$n < c_1 \frac{2^{m+1}}{m+1} = \frac{2m}{m+1} c_1 \frac{2^m}{m} < 2c_1 \frac{2^m}{m}.$$

Now, fix $n \geq 2c_1$ and let $m = f(T'(n))$. By Theorem 1.1, there exists a Boolean function $g : \{0,1\}^m \to \{0,1\}$ such that g can be realized by a Boolean circuit of size $c_1 2^m/m \leq T'(n)$, but not by a Boolean circuit of size $c_2 2^m/m = (c_2/c_1)c_1 2^m/m \geq (c_2/2c_1)T'(n) \geq T(n)$. Furthermore, since f is monotone,

$$m = f(T'(n)) \leq f(c_1 2^n/n) \leq n.$$

Thus, we can define a language $L_n \subseteq \{0,1\}^n$ by

$$L_n = \{w \circ 0^{n-m} \mid w \in \{0,1\}^m,\ g(w) = 1\}.$$

Now the language $L = \bigcup_{n \geq 2c_1} L_n$ has the desired properties. L has the desired properties. $\square$