NOTE TO ODED (Roei Tell, MIT) August 8, 2021

The following two results assert that any improvement over the brute-force algorithm for quantified derandomization of polynomial-sized circuits, for any parametric setting of quantified derandomization, implies that $\mathcal{NEXP} \not\subset \mathcal{P} / \text{poly}$. For small values of the parameters (i.e., a polynomial number of exceptional inputs) we can get a stronger conclusion, namely that $\mathcal{NP} \not\subset \mathcal{SIZE}[n^k]$ for any fixed $k \in \mathbb{N}$.

Specifically, recall that the brute-force algorithm for quantified derandomization evaluates the circuit over $2B(n) + 1$ inputs. The results assert that solving the problem in time noticeably less than $B(n)$ implies circuit lower bounds. As pointed out by Ryan Williams, this is a generalization of his result [Wil13], which is the special case of $B(n) = 2^{n/3}$. (The proofs rely on his result as well as on the extension in [MW18], and benefit from the standard relaxations of the hypothesis – the algorithm only needs to solve the one-sided error version of the problem, and may be non-deterministic.)

**Definition 1** (quantified derandomization). The Quantified Derandomization problem with error bound $B$ (QD$_B$, in short) is the following promise problem:

1. The set of “yes” instances $Y \subseteq \{0, 1\}^*$ consists of descriptions of $n$-bit circuits that accept all but $B(n)$ of their input strings.
2. The set of “no” instances $N \subseteq \{0, 1\}^*$ consists of descriptions of $n$-bit circuits that reject all but $B(n)$ of their input strings.

When the given circuit is also promised to belong to a certain restricted class of circuits denoted by $C$, we denote the problem by QD$_B[C]$.

**Theorem 2** (beating the brute-force quantified derandomization implies circuit lower bounds). Suppose that for some $B(n) < 2^n$ and all $k \in \mathbb{N}$ there exists a non-deterministic machine $M$ that gets as input an $n$-bit circuit $C$ of size $n^k$, runs in time $B(n) \cdot (\log(B(n)))^{-\omega(1)}$, accepts if $C$ accepts all its inputs, and rejects if $C$ rejects all but at most $B(n)$ of its inputs. Then $\mathcal{NEXP} \not\subset \mathcal{P} / \text{poly}$.

There is a slight gap between the ideal threshold result, which would assert that any improvement over $B(n) \cdot O(s)$ implies lower bounds (where $s$ is the circuit size), and Theorem 2, which requires an improvement over $B(n)$. This gap is immaterial when $B(n) \geq 2^{n^{1/2}}$ (e.g., as in Williams’ parameter setting), whereas for $B(n) = 2^{n^{o(1)}}$ the proof below shows that the circuit size $s$ is actually a fixed universal polynomial, so the gap is small (with ideal dispersers this polynomial would be near-linear in $n$).

**Proof.** We will rely on the result of Williams [Wil13], which asserts that if for all $k_0 \in \mathbb{N}$ there exists a non-deterministic machine solving CAPP$_{1,2}$ for $m$-bit circuits of size $m^{k_0}$ in time $2^m / m^{o(1)}$ then $\mathcal{NEXP} \not\subset \mathcal{P} / \text{poly}$. The proof amounts to a reduction of CAPP$_{1,2}$ to QD$_B$ with $B = B(n)$ as in the hypothesis, using a near-optimal disperser-based error-reduction computable by general circuits, from [TSUZ07].

We are given a circuit $C_0: \{0, 1\}^m \rightarrow \{0, 1\}$ of size $m^{k_0}$ that either accepts all its inputs, or rejects all but at most $2^m / 2$ of its inputs. We will use the disperser
Disp: \( \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^m \) from [TSUZ07, Theorem 1.4] for error-reduction, instantiated with input length \( n \) such that \( m = \log(B(n)) \) (i.e., \( n = B^{-1}(2^m) \)), error \( \epsilon = .01 \), min-entropy \( k = \log(B(n)) \), and seed length \( O(\log(n)) \). Then, the circuit \( C: \{0,1\}^n \rightarrow \{0,1\}^m \) defined by \( C(z) = \bigwedge_{s \in \{0,1\}^\ell} C_0(\text{Disp}(z,s)) \) satisfies the following:

1. The circuit size is \( 2^\ell \cdot T_{\text{Disp}}(n) \cdot m^{k_0} \leq n^{k_0+\epsilon} \), where \( T_{\text{Disp}} \) is the polynomial time complexity of \( \text{Disp} \) and \( c \in \mathbb{N} \) is a universal constant.

2. If \( C_0 \) accepts all its inputs then \( C \) accepts all of its inputs, and if \( C_0 \) rejects all but at most \( 2^m/2 \) of its inputs then \( C \) rejects all but at most \( B(n) \) of its inputs.

Using the hypothesized non-deterministic machine for \( \text{QD}_B \) we can distinguish between the two latter cases in time \( B(n) \cdot (\log(B(n)))^{-\omega(1)} = 2^m/m^{\omega(1)} \).

**Theorem 3** (beating the brute-force quantified derandomization for \( B(n) = \text{poly}(n) \) implies stronger circuit lower bounds). There exists a universal constant \( c \in \mathbb{N} \) such that the following holds. Suppose that for some \( B(n) = \text{poly}(n) \) there exists \( \epsilon > 0 \) and a non-deterministic machine \( M \) that gets as input an \( n \)-bit circuit \( C \) of size \( n^\epsilon \), runs in time \( B(n)^{1-\epsilon} \), accepts if \( C \) accepts all its inputs, and rejects if \( C \) rejects all but at most \( B(n) \) of its inputs. Then, for all \( k \in \mathbb{N} \) it holds that \( \text{NP} \nsubseteq SIZE[n^k] \).

**Proof.** The proof is similar to the proof of Theorem 2, except that we use the result of Murray and Williams [MW18] instead of that of [Wil13]: They proved that if for some \( \delta \in (0,1) \) there exists a non-deterministic machine solving \( \text{CAPP}_{1,1/2} \) for \( m \)-bit circuits of size \( 2^\delta \cdot m \) in time \( 2^{(1-\delta) \cdot m} \), then for all \( k \in \mathbb{N} \) it holds that \( \text{NP} \nsubseteq SIZE[n^k] \).

Let \( B(n) = n^\delta \) and let \( \delta = \delta(\epsilon,a) \) be sufficiently small. We are given a circuit \( C_0: \{0,1\}^m \rightarrow \{0,1\} \) of size \( 2^\delta \cdot m \), and we reduce its error using the disperser of [TSUZ07] with the same parameters as in the proof of Theorem 2 (i.e., \( n = B^{-1}(2^m) \), min-entropy \( \log(B(n)) \), small constant error, and seed length \( O(\log(B(n))) \)). The resulting circuit \( C \) is of size \( 2^\ell \cdot n^{k_1} \cdot 2^\delta \cdot m \), which is bounded by \( n^c \) for a universal \( c > k_1 \) (since \( m = \log(B(n)) = a \cdot \log(n) \) and \( \delta = \delta(\epsilon,a) > 0 \) is sufficiently small). The hypothesized algorithm for \( \text{QD}_B \) of \( C \) runs in time \( B(n)^{1-\epsilon} = 2^{(1-\epsilon) \cdot m} < 2^{(1-\delta) \cdot m} \), where the inequality relies on \( \delta > 0 \) being sufficiently small.

**References**

