Oded (June 21, 2022): The simplest yet derandomization of BPP based on HSG

In continuation to my choice Nr. 324, following is my take on the proof presented in Appendix A of the paper of Cheng and Hoza (*ECCC*, TR20-016). Let $\texttt{HSG}(s,n)$ denotes a hitting set (generated) for circuits of size s that take n input bits.

Theorem 1 (the result): *Suppose that* $\texttt{HSG}(s,n)$ *can be computed in time* $T(s) \in [s, 2^{o(n)}]$. *Then,* BPtime(t) *is contained in* Dtime$(T(T(\text{poly}(t))))$.

Actually, the result is meaningful only if $T(T(m)) < 2^m$.

Proof: By standard error reduction, we may assume that, on input x, the BPtime algorithm, denoted A, has error probability $\epsilon = 1/2T(s(|x|) + O(n'))$ and runs in time t', where $n' = t'(n) = O(t(n)\log(1/\epsilon))$ and $s(n) = \text{poly}(t'(n))$ is the size of the circuit $C_x : \{0,1\}^{n'} \to \{0,1\}$ such that $C_x(r) = A(x,r)$. (Formally we set ϵ slightly smaller to avoid a vicious cycle.)[1]

For a generic n-bit input x to the algorithm A, we consider the following $(s(n)+O(n'))$-sized circuits $C'_{x,w} : \{0,1\}^{n'} \to \{0,1\}$ such that $C'_{x,w}(r) \stackrel{\text{def}}{=} \neg C_x(w \oplus r)$, for all $w \in \{0,1\}^{n'}$. Letting $s' = s(n) + O(n')$, we consider the following dichotomy regarding the $C'_{x,w}$'s.

Case of x being a no-instance: For every $\omega \in \{0,1\}^{n'}$ it holds that

$$\Pr_r[C'_{x,\omega}(r)=1] \geq 1 - \epsilon > 1/2.$$

Since each $C'_{x,\omega}$ has size s', it follows that for every ω, there exists $r \in \texttt{HSG}(s',n')$ such that $C'_{x,\omega}(r) = 1$ (equiv., $C_x(\omega \oplus r) = 0$).

Case of x being a yes-instance: For every $r \in \{0,1\}^{n'}$ it holds that

$$\Pr_\omega[C'_{x,r}(\omega)=1] \leq \epsilon.$$

It follows that for every $R \subseteq \{0,1\}^{n'}$ it holds that

$$\Pr_\omega[\exists r \in R \text{ s.t. } C'_{x,r}(\omega)=1] \leq |R| \cdot \epsilon.$$

Equivalently, $\Pr_\omega[\exists r \in R \text{ s.t. } C_x(\omega \oplus r)=0] \leq |R| \cdot \epsilon$.

In particular, for $H \leftarrow \texttt{HSG}(s',n')$, considering $C''_x : \{0,1\}^{n'} \to \{0,1\}$ such that $C''_x(\omega) \stackrel{\text{def}}{=} \bigwedge_{r \in H} C_x(\omega \oplus r)$, we have

$$\Pr_\omega[C''_x(\omega)=1] \geq 1 - T(s') \cdot \epsilon = 1/2,$$

since $|H| < T(s')$. Observing that C''_x has size at most $s'' = T(s') \cdot (s'+1)$, it follows that there exists $\omega \in \texttt{HSG}(s'',n')$ such that $C''_x(\omega) = 1$ (equiv., for every $r \in H$ it holds that $C_x(\omega \oplus r) = 1$).

[1] Recall that $s(n) = \text{poly}(t(n)\log(1/\epsilon))$, whereas we set ϵ to be somewhat smaller than $1/2T(s(n)+O(n'))$. Using $T(s) < 2^{o(n)}$, it follows that $\epsilon \geq \exp(o(s(n)))$, which avoids a vicious cycle. For simplicity, we may just set $\epsilon = 2^{-n}$, and get $s(n) = \text{poly}(t(n))$. However, if both t and T is polynomials, then we may set $\epsilon = 1/\text{poly}(n)$, for a sufficiently large poly.

In contrast, recall that if x is a no-instance, then for every $\omega \in \texttt{HSG}(s'', n')$ there exists $r \in H$ such that $C_x(\omega \oplus r) = 0$.

This dichotomy yields a deterministic decision procedure, which on input $x \in \{0,1\}^n$, determines n', s' and s'', computes $H \leftarrow \texttt{HSG}(s', n')$ and $H' \leftarrow \texttt{HSG}(s'', n')$, and accepts if and only if there exists $\omega \in H'$ such that for every $r \in H$ it holds that $A(x, \omega \oplus r) = 1$. This decision procedure runs in time

$$\begin{aligned} T(s') + T(s'') + T(s') \cdot T(s'') \cdot t'(n) &< 2 \cdot T(s') \cdot T(T(s') \cdot (s'+1)) \cdot t'(n) \\ &= T(\mathrm{poly}(t(n))) \cdot T(T(\mathrm{poly}(t(n))) \cdot \mathrm{poly}(t(n)))) \cdot \mathrm{poly}(t(n)), \end{aligned}$$

since $s' = O(s(n)) = \mathrm{poly}(t'(n))$ and $t'(n) = o(t(n) \cdot n)$. Using $T(m) \geq m$, we get a bound of $T(\mathrm{poly}(t(n))) \cdot T(T(\mathrm{poly}(t(n)))) \cdot \mathrm{poly}(t(n))$, which is upper-bounded by $T(T(\mathrm{poly}(t(n))))$. ■

Corollary 2 (a special case): *Suppose that* $\texttt{HSG}(s, n)$ *can be computed in* $\mathrm{poly}(s)$*-time. Then,* $\mathrm{BPtime}(t)$ *is contained in* $\mathrm{Dtime}(\mathrm{poly}(t))$.

Remark 3 (a finer analysis): *Recall that we used* $|\texttt{HSG}(s, n)| \leq T(s)$*. Using a finer bound of the form* $|\texttt{HSG}(s, n)| \leq N(s)$*, we can use* $s'' = N(s') \cdot (s'+1)$*, and assuming that* $N(s) > s$*, we bound the running-time of the decision procedure by*

$$T(s') + T(s'') + N(s') \cdot N(s'') \cdot t'(n) \leq T(N(\mathrm{poly}(t(n)))),$$

while using $s'' \leq N(s')^2 \leq N(\mathrm{poly}(t(n)))$ *and* $N(N(\mathrm{poly}(t(n))))^3 \leq T(N(\mathrm{poly}(t(n))))$.