Approximate Counting via Preimage-of-Zero Hashing
Last modified: 11/06/2020
Albert Atserias, UPC Barcelona

Let S be a subset of $\{0,1\}^n$ with short and efficiently verifiable witnesses of membership. We want a $\mathrm{BPP}^{\mathrm{NP}}$-algorithm that, with probability at least $1/2$, outputs a c-approximation of $|S|$ for some constant $c \geq 1$. We will achieve this for $c = 16$. Amplification techniques can improve the approximation guarantee to $c = 1+\epsilon$, for any fixed $\epsilon > 0$, and the success probability to $1-\delta$, for any fixed $\delta > 0$.

Let k be such that $2^{k-1} \leq |S| < 2^k$. Assume $k \geq 1$ since the case $k = 0$ means that $S = \emptyset$ and this fact can be detected with an NP-oracle call. Let $H_{n,t}$ be a 2-universal family of hash functions $h : \{0,1\}^n \to \{0,1\}^t$. Consider the following algorithm:

find largest $t \in \{0,\dots,n\}$ for which some y as below is found:
  choose h in $H_{n,t}$ uniformly at random;
  use NP-oracle to try to find $y \in S$ such that $h(y) = 0^t$;
output 2^t.

Note that for $t = 0$ such a y always exist (since $S \neq \emptyset$). If 2^t is the (random) output of the algorithm, we show that the probability that $|S|/16 < 2^t < 16|S|$ is at least $1/2$. Let X_q be the random variable $|\{y \in S : h(y) = 0^q\}|$ where h is chosen uniformly at random in $H_{n,q}$. We have $\mathbb{E}[X_q] = |S|/2^q$ and, by pairwise independence, also $\mathrm{Var}[X_q] = |S|(1-1/2^q)(1/2^q) \leq \mathbb{E}[X_q]$. Now:

$$\begin{aligned}
\Pr[\, 2^t \geq 16|S| \,] &\leq \Pr[\, 2^t \geq 2^{k-1+4} \,] \\
&= \Pr[\, t = k+3 \text{ or } t = k+4 \text{ or } \cdots \,] \\
&\leq \Pr[\, X_{k+3} \geq 1 \,] + \Pr[\, X_{k+4} \geq 1 \,] + \cdots \\
&\leq |S|/2^{k+3} + |S|/2^{k+4} + \cdots \\
&\leq 1/2^3 + 1/2^4 + \cdots \\
&= 1/4.
\end{aligned}$$

Also

$$\begin{aligned}
\Pr[\, 2^t \leq |S|/16 \,] &\leq \Pr[\, 2^t \leq 2^{k-4} \,] \\
&= \Pr[\, X_{k-3} = 0 \text{ and } X_{k-2} = 0 \text{ and } \cdots \,] \\
&\leq \Pr[\, X_{k-3} = 0 \,] \\
&\leq \mathrm{Var}[X_{k-3}]/\mathbb{E}[X_{k-3}] \\
&\leq 1/\mathbb{E}[X_{k-3}] \\
&= 2^{k-3}/|S| \\
&\leq 2^{k-3}/2^{k-1} \\
&= 1/4.
\end{aligned}$$