`fn sample_geometric_exp_slow`

Michael Shoemate

August 13, 2024

This proof resides in **"contrib"** because it has not completed the vetting process.

Proves soundness of `fn sample_geometric_exp_slow` in `mod.rs` at commit 0be3ab3e6 (outdated[1]). This proof is an adaptation of subsection 5.2 of [CKS20].

Vetting history

- Pull Request #519

1 Hoare Triple

Precondition

$\texttt{x} \in \mathbb{Q} \land \texttt{x} > 0$

Pseudocode

```python
def sample_geometric_exp_slow(x) -> int:
    k = 0
    while True:
        if sample_bernoulli_exp(x):
            k += 1
        else:
            return k
```

Postcondition

For any setting of the input parameter `x` such that the given preconditions hold, `sample_geometric_exp_slow` either returns `Err(e)` due to a lack of system entropy, or `Ok(out)`, where `out` is distributed as $Geometric(1 - exp(-x))$.

2 Proof

Assume the preconditions are met.

Lemma 2.1. `sample_geometric_exp_slow` only returns `Err(e)` when there is a lack of system entropy.

[1]See new changes with `git diff 0be3ab3e6..95829e1 rust/src/traits/samplers/cks20/mod.rs`

Proof. The preconditions on `x` satisfy the preconditions on `sample_bernoulli_exp`, so by its definition, it only returns an error if there is a lack of system entropy. The only source of errors is from this function, therefore `sample_geometric_exp_slow` only returns `Err(e)` when there is a lack of system entropy. $\square$

Theorem 2.2. [CKS20] If the outcome of `sample_geometric_exp_slow` is `Ok(out)`, then `out` is distributed as $Geometric(1 - exp(-x))$. That is, $P[\texttt{out} = k] = exp(-x)(1 - exp(-x))^k$

Proof. The distribution of the i^{th} boolean returned on line 4 is $B_i \sim Bernoulli(exp(x))$, because the preconditions on `x` satisfy the preconditions for `sample_bernoulli_exp`.

$$
\begin{aligned}
P[\texttt{out} = k] &= P[B_1 = B_2 = ... = B_k = \bot \wedge B_{k+1} = \top] \\
&= P[B_{k+1} = \top] \prod_{i=1}^{k} P[B_i = \bot] && \text{All } B_i \text{ are independent.} \\
&= exp(-x)(1 - exp(-x))^k
\end{aligned}
$$

$\square$

Proof. 1 holds by 2.1 and 2.2. $\square$

References

[CKS20] Clément L. Canonne, Gautam Kamath, and Thomas Steinke. The discrete gaussian for differential privacy. *CoRR*, abs/2004.00010, 2020.