fn permute_and_flip

Michael Shoemate

September 22, 2025

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

This document proves soundness of `permute_and_flip` [2] in `mod.rs` at commit e62b0aa2 (outdated[1]). `permute_and_flip` noisily selects the index of the greatest score from a vector of input scores.

1 Hoare Triple

Preconditions

Types consistent with pseudocode.

Pseudocode

```
def permute_and_flip(x: list[RBig], scale: RBig):
    if scale.is_zero():  #
        return max(range(x.len()), key=lambda i: x[i])

    # begin nonzero scale
    x_max = max(x)
    permutation = list(range(x.len()))

    for left in range(x.len()):
        right = left + sample_uniform_uint_below(x.len() - left)
        permutation.swap(left, right) # fisher-yates shuffle up to left

        candidate = permutation[left]
        if sample_bernoulli_exp((x_max - x[candidate]) / scale):
            return candidate

    raise "at least one x[candidate] is equal to x_max"
```

Postcondition

Theorem 1.1. Returns the index of the max element z_i, where each $z_i \sim \text{Exp}(\text{shift} = x_i, \text{scale} = \texttt{scale})$.

Lemma 1.2. The permute-and-flip mechanism is equivalent to the report-noisy-max with exponential noise mechanism.

See [1] for proof of Lemma 1.2.

Lemma 1.3. The pseudocode starting from line 5 equivalent to Algorithm 1 in [2], where $\texttt{scale} = \frac{2\Delta}{\epsilon}$.

[1] See new changes with `git diff e62b0aa2..7b6eb5e rust/src/measurements/noisy_top_k/exponential/mod.rs`

Proof. By swapping elements on line 11, an online Fisher-Yates shuffle is applied up to and including index `left`.

Substituting `scale` $= \frac{2\Delta}{\epsilon}$, the argument to `sample_bernoulli_exp` is then $\frac{\epsilon}{2\Delta}(q_* - q_r)$, which is non-negative, satisfying the precondition of `sample_bernoulli_exp`. Therefore by the postcondition of `sample_bernoulli_exp`, the response is a sample from $\text{Bern}(\exp(-x))$, where $x = \frac{\epsilon}{2\Delta}(q_* - q_r)$. Therefore the response is a sample from $\text{Bern}(\exp(\frac{\epsilon}{2\Delta}(q_r - q_*)))$, which is equivalent to Algorithm 1 in [2]. □

Proof of Theorem 1.1. Consider two cases: zero scale and nonzero scale. When scale is zero on line 2, each $z_i = x_i$, so the argmax is returned. Otherwise, by Lemma 1.3 the pseudocode is equivalent to Algorithm 1 in [2], which is in turn equivalent to the postcondition by Lemma 1.2. In all two cases, the postcondition holds. □

References

[1] Zeyu Ding, Daniel Kifer, Thomas Steinke, Yuxin Wang, Yingtai Xiao, Danfeng Zhang, et al. The permute-and-flip mechanism is identical to report-noisy-max with exponential noise. *arXiv preprint arXiv:2105.07260*, 2021.

[2] Ryan McKenna and Daniel R Sheldon. Permute-and-flip: A new mechanism for differentially private selection. *Advances in Neural Information Processing Systems*, 33:193–203, 2020.