fn score_candidates_map

Michael Shoemate

April 15, 2025

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

Proves soundness of `score_candidates_map` in `mod.rs` at commit f5bb719 (outdated[1]). `score_candidates_map` returns a specific function that can be used to prove stability of the quantile scoring transformation.

1 Hoare Triple

Precondition

$\texttt{alpha\_den} > \texttt{alpha\_num}$.

Function

```
def score_candidates_map(alpha_num, alpha_den, known_size) -> Callable[[int], int]:
    if known_size:

        def stability_map(d_in: u32) -> u64:
            return T.inf_cast(d_in // 2).inf_mul(2).inf_mul(alpha_den)

    else:
        abs_dist_const: u64 = max(alpha_num, alpha_den - alpha_num) #
        stability_map = T.exact_int_cast(d_in).alerting_mul(abs_dist_const)

    return stability_map
```

Postcondition

Theorem 1.1. If `known_size` is set, then returns a function that computes $\texttt{d\_in}//2 \cdot 2 \cdot \texttt{alpha\_den}$ for argument `d_in` or an error.

Otherwise, returns a function that computes $\texttt{d\_in} \cdot \max(\texttt{alpha\_num}, \texttt{alpha\_den} - \texttt{alpha\_num})$, for argument `d_in` or an error.

Proof. Recall the definitions of `ExactIntCast` and `AlertingMul`. These traits have no preconditions, and guarantee exact arithmetic or an error.

In addition, by the precondition, the subtraction cannot overflow. Therefore, the postcondition is met. □

[1] See new changes with `git diff f5bb719..781be61f rust/src/transformations/quantile_score_candidates/mod.rs`