fn quantile_cnd

Aishwarya Ramasethu, Yu-Ju Ku, Jordan Awan, Michael Shoemate

January 28, 2025

Compute the quantile of a canonical noise distribution, as specified by a tradeoff function `f`.

1 Hoare Triple

Preconditions

Compiler-verified

- Argument `uniform` of type `RBig`
- Argument `f`, a function from `RBig` to `RBig`
- Argument `c` of type `RBig`

User-verified

- Argument `uniform` is in $[0, 1]$
- Argument `f` is a symmetric nontrivial tradeoff function
- Argument `c` is the fixed point of `f`, where `f(c) = c`

Pseudocode

```python
def quantile_cnd(
    uniform: RBig, f: Callable[[RBig], RBig], c: RBig
) -> RBig | None:
    if uniform < c:
        return quantile_cnd(RBig(1) - f(uniform), f, c) - RBig(1)
    elif uniform <= RBig(1) - c:  # the linear function
        num = uniform - RBig(1, 2)
        den = RBig(1) - RBig(2) * c
        if den.is_zero():
            return
        return num / den
    else:
        return quantile_cnd(f(RBig(1) - uniform), f, c) + RBig(1)
```

Postcondition

Theorem 1.1. Evaluates the quantile function $F_f^{-1}(u)$ as defined in Proposition F.6 of Awan and Vadhan 2023.

Proof. We start by defining $F_f(\cdot)$:

Definition 1.2 (Awan and Vadhan 2023, Definition 3.7)**.** Let f be a symmetric nontrivial tradeoff function, and let $c \in [0, 1/2)$ be the unique fixed point of f: $f(c) = c$. We define $F_f : \mathbb{R} \to \mathbb{R}$ as

$$F_f(x) = \begin{cases} f(1 - F_f(x+1)) & x < -1/2 \\ c \cdot (1/2 - x) + (1-c)(x + 1/2) & -1/2 \le x \le 1/2 \\ 1 - f(F_f(x-1)) & x > 1/2. \end{cases} \tag{1}$$

The preconditions for `quantile_cnd` satisfy the preconditions for this definition. The quantile function $F_f^{-1}(u)$ is defined in the following lemma.

Proposition 1 (Awan and Vadhan 2023, Proposition F.6)**.** The quantile function $F_f^{-1} : (0, 1) \to \mathbb{R}$ for F_f can be expressed as

$$F_f^{-1}(u) = \begin{cases} F_f^{-1}(1 - f(u)) - 1 & u < c \\ \frac{u - 1/2}{1 - 2c} & c \le u \le 1 - c \\ F_f^{-1}(f(1-u)) + 1 & u > 1 - c, \end{cases} \tag{2}$$

where c is the unique fixed point of f. Furthermore, for any $u \in (0, 1)$, the expression $Q_f(u)$ takes a finite number of recursive steps to evaluate. Thus, if $U \sim U(0, 1)$, then $F_f^{-1}(U) \sim F_f$.

The pseudocode implements 1 with exact arithmetic via fractions, as it involves no transcendental functions.

□

References

Awan, Jordan and Salil Vadhan (2023). "Canonical Noise Distributions and Private Hypothesis Tests". In: *The Annals of Statistics* 51.2, pp. 547–572.