

# fn quantile\_cnd

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

December 18, 2025

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

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

```
1 def quantile_cnd(  
2     uniform: RBig, f: Callable[[RBig], RBig], c: RBig  
3 ) -> RBig | None:  
4     if uniform < c:  
5         return quantile_cnd(RBig(1) - f(uniform), f, c) - RBig(1)  
6     elif uniform <= RBig(1) - c: # the linear function  
7         num = uniform - RBig(1, 2)  
8         den = RBig(1) - RBig(2) * c  
9         if den.is_zero():  
10             return  
11         return num / den  
12     else:  
13         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  $F_f : \mathbb{R} \rightarrow \mathbb{R}$  as

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

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  $F_f^{-1} : (0, 1) \rightarrow \mathbb{R}$  for  $F_f$  can be expressed as

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

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  $F_f^{-1}(U) \sim F_f$ .

`quantile_cnd` is the quantile function  $F_f^{-1}(u)$ , `f` is the tradeoff function  $f$ , `uniform` is  $u$ , and `c` is the fixed point of  $f$ , as guaranteed in the precondition.

Since the pseudocode uses exact arithmetic, `quantile_cnd` implements 1, satisfying the postcondition.  $\square$

## References

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