Presentation for the Quantum Seminar

José Manuel Rodríguez Caballero

University of Tartu

Spring 2020

Subject

My presentation is about the paper[1]:

> *Bouman, Niek J., and Serge Fehr. "Sampling in a quantum population, and applications." Annual Cryptology Conference. Springer, Berlin, Heidelberg, 2010.*

[1] I will not repeat the notation from the paper in this presentation. If someone needs a clarification, either read the paper or ask me during the presentation.

Modifications

My presentation may differ in some points with respect of the presentation given by the authors, not only because of my aesthetic preferences, but also because in some cases there are minor formal problems[2] in the paper, e.g., strictly speaking, definition 1 cannot be applied to what it supposed to be an example[3] of it (I modified this definition in order to avoid this problem).

[2] There are trivial ways to solve these minor problems, but I do not find them elegant. I prefer a presentation without compromising the formalism too much.

[3] Pairwise one-out-of-two sampling, using only part of the sample.

Main definition

Let $\mathcal{I}$ be a finite set of indices, $\mathcal{S}$ be a finite set of seeds and $\mathcal{A}$ be a finite alphabet. Define $\mathcal{T} := 2^{\mathcal{I}}$. A *sampling and estimation strategy* (a *strategy* for short) is given by (P_{TS}, f), where P_{TS} is a probability distribution over $\mathcal{T} \times \mathcal{S}$ and f is a real-valued function over

$$\mathrm{Dom}_f := \bigcup_{(t,s)\in\mathcal{T}\times\mathcal{S}} \left\{(t, q, s) : \quad q \in \mathcal{A}^t\right\}.$$

Main example

Pairwise one-out-of-two sampling, using only part of the sample. Let $\mathcal{I} := [n] \times \{0,1\}$ and $\mathcal{S} := \mathcal{T}$. The probability distribution P_{TS} is given by

$$P_{TS}(t,s) = \frac{1}{2^n \binom{n}{k}}$$

if for some $(j_1, ..., j_n) \in \{0,1\}^n$ we have $t = \{(\ell, j_\ell) : \quad 1 \leq \ell \leq n\}$, $|s| = k$ and $s \subset t$. Otherwise, $P_{TS}(t,s) := 0$.

End of my presentation