A. Additional proofs

A.1. Local privacy

Proof of Proposition 1. Because ϕ is a sufficient statistic, by definition there exists some channel $Q(y \mid \phi(x,y))$ and a distribution $F_\theta(\phi(x,y) \mid x)$ such that $p_\theta(y \mid x) = Q(y \mid \phi(x,y))F_\theta(\phi(x,y) \mid x)$. If we define

$$S'(o \mid \phi(x,y)) = \sum_y S(o \mid y) Q(y \mid \phi(x,y)), \qquad (18)$$

then (8) follows by substitution and algebra: □

In order to show differential privacy of the two schemes proposed in Section 3, we first note that it suffices to have differential privacy of the observations o with respect to any (possibly random) data $z \in \mathcal{Z}$ processed given the private variable y such that $y \to z \to o$ forms a Markov chain. To see this, suppose Q is an α-differentially private channel taking the intermediate variable z to o and fix any $x \in \mathcal{X}$. Let $R(\cdot \mid y)$ be the distribution of z given $y \in \mathcal{Y}$. Now, for the end-to-end channel S,

$$\begin{aligned}\sup_{o,y,y'} \frac{S(o \mid y)}{S(o \mid y')} &= \sup_{o,y,y'} \frac{\sum_{z\in\mathcal{Z}} Q(o \mid z) R(z \mid y)}{\sum_{z\in\mathcal{Z}} Q(o \mid z) R(z \mid y')} \\ &\le \sup_{o,y,y'} \frac{\max_z Q(o \mid z)}{\min_z Q(o \mid z)} \\ &\le \exp(\alpha).\end{aligned}$$

Differential privacy of the coordinate release mechanism follows immediately from the above observation, together with the fact that, once a coordinate is chosen, it is flipped in the classical way:

$$\begin{aligned}\frac{Q(o_{\text{cr}} \mid \tilde{o}, j)}{Q(o_{\text{cr}} \mid \tilde{o}', j')} &= \exp\left(\frac{\alpha}{2}\left(|o_{\text{cr}} - (1-\tilde{o}[j])| - |o_{\text{cr}} - (1-\tilde{o}'[j'])|\right)\right) \\ &\le \exp(\alpha),\end{aligned}$$

where the final step is by the triangle inequality applied twice. Privacy of per-value ϕ-RR follows similarly:

$$\begin{aligned}\frac{Q(o_{\text{pv}} \mid \tilde{o})}{Q(o_{\text{pv}} \mid \tilde{o}')} &= \exp\left(\frac{\alpha}{2\bar{\delta}}\left(\|o_{\text{pv}} - (\mathbf{1}-\tilde{o})\|_1 - \|o_{\text{pv}} - (\mathbf{1}-\tilde{o}')\|_1\right)\right) \\ &\le \exp(\alpha).\end{aligned}$$