Supplementary material: Proofs of Lemmas 1 and 3

Proof of Lemma 1. If $M = m$ but $\widehat{M} \neq m$, then

$$\|\widehat{f}_n - f_m\|_{L_1(\Pi)} \ge \|f_m - f_{\widehat{M}}\|_{L_1(\Pi)} - \|\widehat{f}_n - f_{\widehat{M}}\|_{L_1(\Pi)} \ge 2\varepsilon - \|\widehat{f}_n - f_{\widehat{M}}\|_{L_1(\Pi)}. \tag{28}$$

Thus, if $\|\widehat{f}_n - f_m\|_{L_1(\Pi)} < \varepsilon$, then it must be the case that $\|\widehat{f}_n - f_{\widehat{M}}\|_{L_1(\Pi)} < \varepsilon$, which, in view of (28), is a contradiction. Hence,

$$\mathbb{P}^{\mathsf{S},\pi}(\widehat{M} \neq M) \le \mathbb{P}^{\mathsf{S},\pi}\left(\widehat{f}_n \notin \mathcal{F}_\varepsilon(f_M)\right) \le \delta,$$

and the lemma is proved. □

Proof of Lemma 3. We only prove (16), since the proof of (17) is similar. First note that

$$\frac{\mathbb{P}^{\mathsf{S},m}(x^n, y^n)}{\mathbb{Q}^{\mathsf{S}}(x^n, y^n)} = \prod_{t=1}^{n} \frac{P^m_{Y|X}(y_t|x_t)}{Q_{Y|X}(y_t|x_t)} = \prod_{x \in \mathcal{X}} \prod_{t : x_t = x} \frac{P^m_{Y|X}(y_t|x)}{Q_{Y|X}(y_t|x)}.$$

Then

$$\begin{aligned} D(\mathbb{P}\|\mathbb{Q}) &= \frac{1}{N}\sum_{m=1}^{N}\sum_{x^n, y^n} \mathbb{P}^{\mathsf{S},m}(x^n, y^n) \log \frac{\mathbb{P}^{\mathsf{S},m}(x^n, y^n)}{\mathbb{Q}^{\mathsf{S}}(x^n, y^n)} \\ &= \frac{1}{N}\sum_{m=1}^{N}\sum_{x \in \mathcal{X}} \mathbb{E}_{\mathbb{P}^{\mathsf{S},m}}\left[\sum_{t : X_t = x} \log \frac{P^m_{Y|X}(Y_t|x)}{Q_{Y|X}(Y_t|x)}\right] \\ &= \frac{1}{N}\sum_{m=1}^{N}\sum_{x \in \mathcal{X}} D(P^m_{Y|X}(\cdot|x)\|Q_{Y|X}(\cdot|x))\mathbb{E}_{\mathbb{P}^{\mathsf{S},m}}\left[N(x|X^n)\right], \end{aligned}$$

which gives (16). Eq. (18) follows from the fact that, for a passive strategy, the expectation of $N(x|X^n)$ is equal to $n\Pi(x)$ under both $\mathbb{P}^{\mathsf{S},m}$ and $\mathbb{Q}^{\mathsf{S}}$. The same proof holds with D_{re} replaced by D. □

Proof of Lemma 4. The proof is via the probabilistic method. Specifically, we shall show that if we select N binary strings from $\{0,1\}^k_d$ uniformly at random, then the resulting set will have all three desired properties with probability strictly greater than 0.

For a fixed $\beta \in \{0,1\}^k_d$, let $\mathcal{U}_\beta \triangleq \left\{\beta' \in \{0,1\}^k_d : d_H(\beta, \beta') \le d\right\}$. Then for any $\beta' \in \mathcal{U}_\beta$ $|\{i \in [k] : \beta_i = \beta'_i = 1\}| \ge \frac{d}{2}$. Hence,

$$|\mathcal{U}_\beta| \le \binom{d}{d/2}\binom{k - d/2}{d/2} \le \binom{d}{d/2}\binom{k}{d/2} \le 2^d \binom{k}{d/2},$$

where we have used the fact that $\binom{d}{\ell} \le 2^d$ for any $\ell \le d$. From this we see that if we draw an element of $\{0,1\}^k_d$ uniformly at random, then it will be in $|\mathcal{U}_\beta|$ with probability

$$p = \frac{|\mathcal{U}_\beta|}{\left|\{0,1\}^k_d\right|} \le \frac{2^d\binom{k}{d/2}}{\binom{k}{d}}.$$

Thus, if we select N elements of $\{0,1\}^k_d$ uniformly at random, then the probability that the jth element will be d-close in the Hamming distance to any of the $j-1$ already selected ones is at most $(j-1)p$, and the probability that any two elements are d-close is at most $(N^2/2)p$. Hence, with the choice $N = \lfloor (3k/16d)^{d/4} \rfloor \ge (k/6d)^{d/4}$ we have

$$\frac{N^2 p}{2} \le \frac{1}{2}\left(\frac{3k}{16d}\right)^{d/2} \frac{2^d\binom{k}{d/2}}{\binom{k}{d}} \le \frac{1}{2},$$

where we have used the fact that $\binom{k}{d}/\binom{k}{d/2} \ge \left(\frac{k}{d} - \frac{1}{2}\right)^{k/2}$, as well as the fact that $\frac{3k}{4d} \le \frac{k}{d} - \frac{1}{2}$ for $d \le k/2$. Hence, with probability at least $1/2$, all the N elements will be strictly d-separated.

We now show that the randomly selected set of N elements of $\{0,1\}_d^k$ will also be "well-balanced" in the sense of (19) with probability strictly larger than $1/2$. To that end, let us fix $j \in [k]$ and let $Z_1, \ldots, Z_N$ be the $\{0,1\}$-valued random variables, corresponding to the jth coordinates of the randomly chosen elements. Observe that $\mathbb{E} Z_i = d/k$. Then Bernstein's inequality gives

$$\begin{aligned}\Pr\left(\left|\frac{1}{N}\sum_{i=1}^{N} Z_i - \frac{d}{k}\right| > \frac{d}{2k}\right) &\le 2\exp\left(-\frac{N(d/2k)^2}{2(d/k)(1-d/k) + 2(1-d/k)(d/(2k))/3}\right) \\ &= 2\exp\left(-\frac{Nd}{12k}\right)\end{aligned}$$

This, together with the union bound, shows that the probability of (19) being violated is at most $2k\exp\left(-\frac{Nd}{12k}\right)$, which will be strictly less than $1/2$ for sufficiently large d. Hence, the probability that a set of N elements of $\{0,1\}_d^k$ drawn uniformly at random will fail to satisfy either the separation condition (ii) or the balance condition (iii) is strictly less than 1. This completes the proof. ☐