Appendix A

A.1 Proof of Proposition 7.2.1

Proof Given $P_F = P_{F_i}$ and $P_M = P_{M_i}$ for all $i \in \{1, \dots, K\}$, false alarm and miss detection probabilities resulting from γ^K are $P_{F_0} = 1 - B(K/2; K, P_F)$ and $P_{M_0} = B(K/2; K, 1-P_M)$, respectively, where $B(t_0; K, P)$ is a binomial cumulative distribution function with at most t_0 successes out of K trials each having a success probability P. Let $X \sim B(K, P)$ and $Y \sim B(K, 1-P)$ be two Binomial r.v.s with K trials each having a success probability P and $1 - P$, respectively. Then, for two disjoint events $E_1 = X \leq K/2$ and $E_2 = (K - X) \leq K/2$,

$$P(E_1 \cup E_2) = P(E_1) + P(E_2) = 1.$$

Now, by noting that $Y = K - X$ in distribution, we have

$$\begin{aligned} P(E_1) + P(E_2) &= P(X \leq K/2) + P(Y \leq K/2) \\ &= B(K/2; K, P) + B(K/2; K, 1-P) = 1 \end{aligned}$$

which implies that P_{F_0} and P_{M_0} own the same polynomial function f s.t. $P_{F_0} = f(P_F)$ and $P_{M_0} = f(P_M)$. From Proposition 7.4.1, f is monotonically increasing, hence $P_{M_0} = P_{F_0}$ iff $P_M = P_F$. □

A.2 Proof of Proposition 7.2.2

Proof Using the substitution $j = i + 1$, we have

G. Gül, *Robust and Distributed Hypothesis Testing*, Lecture Notes in Electrical Engineering 414, DOI 10.1007/978-3-319-49286-5

$$
\begin{aligned}
P_F P_{F_0}^{2K-1} &= \sum_{i=K}^{2K-1} \binom{2K-1}{i} {P_F}^{i+1} (1-P_F)^{2K-1-i} \\
&= \sum_{j=K+1}^{2K} \binom{2K-1}{j-1} {P_F}^{j} (1-P_F)^{2K-j} \\
&= \left(\sum_{j=K+1}^{2K-1} \binom{2K-1}{j-1} {P_F}^{j} (1-P_F)^{2K-j} \right) + {P_F}^{2K}
\end{aligned} \tag{A.1}
$$

and

$$
\begin{aligned}
(1-P_F) P_{F_0}^{2K-1} &= \sum_{i=K}^{2K-1} \binom{2K-1}{i} {P_F}^{i} (1-P_F)^{2K-i} \\
&= \binom{2K-1}{K} {P_F}^{K} (1-P_F)^{K} \\
&\quad + \sum_{i=K+1}^{2K-1} \binom{2K-1}{i} {P_F}^{i} (1-P_F)^{2K-i}.
\end{aligned} \tag{A.2}
$$

Adding up (A.1) and (A.2), we get

$$
\begin{aligned}
(1-P_F) P_{F_0}^{2K-1} + P_F P_{F_0}^{2K-1} &= \binom{2K-1}{K} P_F^K (1-P_F)^K \\
&\quad + \sum_{i=K+1}^{2K-1} \left(\binom{2K-1}{i-1} + \binom{2K-1}{i} \right) {P_F}^{i} (1-P_F)^{2K-i} + {P_F}^{2K} \\
&= \frac{1}{2} \binom{2K}{K} {P_F}^{K} (1-P_F)^{K} + \sum_{i=K+1}^{2K} \binom{2K}{i} {P_F}^{i} (1-P_F)^{2K-i} \\
&= P_{F_0}^{2K}
\end{aligned}
$$

using the identities

$$
\binom{2K-1}{K} = \frac{1}{2}\binom{2K}{K}, \quad \binom{2K-1}{i} + \binom{2K-1}{i-1} = \binom{2K}{i}
$$

and

$$
{P_F}^{2K} = \binom{2K}{2K} {P_F}^{2K} (1-P_F)^{2K-2K}.
$$

□

A.3 Proof of Lemma 7.3.2

Proof By definition, P_F and P_M are probabilities, hence $(P_F, P_M) \in [0, 1]^2$. Evaluating $P_F = 1 - P_0[l(Y) \leq t]$ and $P_M = P_1[l(Y) \leq t]$ for $\lim_{t\to 0}$ and $\lim_{t\to\infty}$ shows that r_t passes through the points $(1, 0)$ and $(0, 1)$. Let $p_{0,l}$ and $p_{1,l}$ be the density functions of $l(Y)$ for $Y \sim P_0$ and $Y \sim P_1$, respectively. Since r_t is differentiable for every t, i.e.

$$\frac{dP_M}{dP_F} = \frac{dP_M}{dt}\frac{dt}{dP_F} = -\frac{p_{1,l}(t)}{p_{0,l}(t)} \tag{A.3}$$

exists, r_t is continuous. The miss detection probability can also be written as

$$P_M = \int_{\{y:l(y)\leq t\}} p_1(y)\mathrm{d}y = \int_{\{y:l(y)\leq t\}} l(y)p_0(y)\mathrm{d}y = \int_0^t x p_{0,l}(x)\mathrm{d}x,$$

where the last equality follows from

$$p_{0,l}(x) = \left|\frac{\mathrm{d}l^{-1}(x)}{\mathrm{d}x}\right| p_0(l^{-1}(x))$$

with the change of variable $x = l(y)$. Hence,

$$\frac{dP_M}{dt} = tp_{0,l}(t) \overset{\text{(A.3)}}{\Longrightarrow} \frac{dP_M}{dP_F} = -t.$$

As a result,

$$\frac{d^2P_M}{dP_F{}^2} = \frac{d}{dP_F}\left(\frac{dP_M}{dP_F}\right) = -\frac{dt}{dP_F} = \frac{1}{p_{0,l}(t)} \geq 0$$

proves that r_t is convex. □

A.4 Proof of Proposition 7.4.1

Letting $p = p(\theta) = 1 - \theta$ and $q = q(\theta) = \frac{1-2\theta}{1-\theta}$, showing that L_∞^K is negative for sufficiently large K is equivalent to showing that

$$\sum_{i=0}^{K/2} \binom{K}{i} p^i(1-p)^{K-i} < \frac{1}{2}\sum_{i=0}^{K/2}\binom{K}{i} q^i(1-q)^{K-i} \tag{A.4}$$

for sufficiently large K. There are two possible cases:

- Trivial case: For $1/3 \le \theta < 1/2$, the sum on the left converges to zero and the sum on the right converges to a positive number, so the inequality (A.4) is true for large K.
- Remaining case: Suppose $0 < \theta < 1/3$. The inequality of the sums can be proven working term by term. It suffices to show that

$$p^i(1-p)^{K-i} < \frac{1}{2}q^i(1-q)^{K-i} \tag{A.5}$$

for all $0 \le i \le K/2$, when K is large enough. Note that $\frac{p(1-q)}{q(1-p)} = \frac{1-\theta}{1-2\theta} > 1$ and $\frac{p(1-p)}{q(1-q)} = \frac{(1-\theta)^3}{1-2\theta} < 1$. Therefore,

$$\left(\frac{1-p}{1-q}\right)^K \left(\frac{p(1-q)}{q(1-p)}\right)^i \le \left(\frac{1-p}{1-q}\right)^K \left(\frac{p(1-q)}{q(1-p)}\right)^{K/2} = \left(\frac{p(1-p)}{q(1-q)}\right)^{K/2}. \tag{A.6}$$

The right hand side of (A.6) can be made less than $1/2$ by taking K sufficiently large, giving the inequality (A.5) and hence the inequality (A.4).

A.5 Proof of Proposition 7.5.1

Proof To prove that $P_{F_0}(P_F, K, t_0)$ and $P_{M_0}(P_M, K, t_0)$ are increasing functions of P_F and P_M, respectively, it is sufficient to prove it only for $P_{F_0}(P_F, K, t_0)$. Because

$$\frac{\partial P_{M_0}(P_M, K, t_0)}{\partial P_M} = \frac{\partial P_{F_0}(P_F, K, t_0)}{\partial P_F}|_{P_F := 1-P_M}. \tag{A.7}$$

Noting that (A.7) is zero for $P_F = 0$, we have

$$P_{F_0} = \sum_{i=t_0}^{K} \binom{K}{i} P_F^i (1-P_F)^{K-i} = \sum_{i=t_0}^{K} \binom{K-1}{i-1} P_F^i (1-P_F)^{K-i} + \sum_{i=t_0}^{K} \binom{K-1}{i} P_F^i (1-P_F)^{K-i}. \tag{A.8}$$

Since in the second sum, the term is zero when $i = K$, we get

$$\sum_{i=t_0}^{K} \binom{K-1}{i} P_F^i (1-P_F)^{K-i} = \sum_{i=t_0}^{K-1} \binom{K-1}{i} P_F^i (1-P_F)^{K-i}$$
$$< \sum_{i=t_0-1}^{K-1} \binom{K-1}{i} P_F^i (1-P_F)^{K-i}. \qquad \text{(A.9)}$$

Changing the variable $j = i + 1$,

$$\sum_{i=t_0-1}^{K-1} \binom{K-1}{i} P_F^i (1-P_F)^{K-i} = \sum_{j=t_0}^{K} \binom{K-1}{j-1} P_F^{j-1} (1-P_F)^{K-j+1} \qquad \text{(A.10)}$$

and writing (A.10) in (A.8) with (A.9), it follows that

$$\sum_{i=t_0}^{K} \binom{K}{i} {P_F}^i (1-P_F)^{K-i} < \sum_{i=t_0}^{K} \binom{K-1}{i-1} {P_F}^i (1-P_F)^{K-i}$$
$$+ \sum_{j=t_0}^{K} \binom{K-1}{j-1} {P_F}^{j-1} (1-P_F)^{K-j+1}. \qquad \text{(A.11)}$$

Using

$${P_F}^i (1-P_F)^{K-i} + {P_F}^{i-1} (1-P_F)^{K-i+1} = {P_F}^{i-1} (1-P_F)^{K-i}$$

rewrite (A.11),

$$\sum_{i=t_0}^{K} \binom{K}{i} {P_F}^i (1-P_F)^{K-i} < \sum_{i=t_0}^{K} \binom{K-1}{i-1} {P_F}^{i-1} (1-P_F)^{K-i}. \qquad \text{(A.12)}$$

Multiplying (A.12) with $K/(1-P_F)$ and noting that

$$i \binom{K}{i} = K \binom{K-1}{i-1}$$

we finally get

$$\sum_{i=t_0}^{K} \binom{K}{i} {P_F}^{i-1} (1-P_F)^{K-i-1} (i - K P_F) = \frac{\partial P_{F_0}(P_F, K, t_0)}{\partial P_F} > 0.$$

□

A.6 Proof of Proposition 7.5.2

Proof The claim will be proven for odd t_0, while its extension to even t_0 can be accomplished following the same line of arguments. Let the threshold be $t_0 \in \{0, \lfloor K/2 \rfloor - 1\}$ for some K. If $t_0 = \lfloor K/2 \rfloor$, then clearly

$$P_{F_0}(x, K, \lfloor K/2 \rfloor) = P_{M_0}(x, K, \lfloor K/2 \rfloor), \quad \forall x \in [0, 1].$$

One can also see that, cf. Remark 7.4.1,

$$P_{F_0}(x, K, \lfloor K/2 \rfloor - 1) > P_{F_0}(x, K, \lfloor K/2 \rfloor), \quad \forall x \in (0, 1),$$

and

$$P_{M_0}(x, K, \lfloor K/2 \rfloor - 1) < P_{M_0}(x, K, \lfloor K/2 \rfloor), \quad \forall x \in (0, 1).$$

Hence,

$$P_{F_0}(x, K, \lfloor K/2 \rfloor - 1) > P_{M_0}(x, K, \lfloor K/2 \rfloor - 1), \quad \forall x \in (0, 1). \tag{A.13}$$

For a pair (P_F, P_M) to be valid, it should be in $(\mathcal{F} \times \mathcal{M})_{t_0}^K$, i.e.

$$P_{F_0}(P_F, K, \lfloor K/2 \rfloor - 1) = P_{M_0}(P_M, K, \lfloor K/2 \rfloor - 1). \tag{A.14}$$

Assume that (A.14) holds for some (P_F^*, P_M^*) with $P_M^* = P_F^*$ or with $P_M^* < P_F^*$. Then, both cases are obviously a contradiction with (A.13), since both P_{F_0} and P_{M_0} are monotonically increasing functions of P_F and P_M, respectively, cf. Proposition 7.4.1. Therefore, $P_M^* > P_F^*$ must be true for all pairs $(P_F^*, P_M^*) \in (\mathcal{F} \times \mathcal{M})_{t_0}^K$. This proves that $h_{t_0}^K(P_F) > P_F$ for all $P_F \in (0, 1)$. Clearly, when $t_0 \in \{\lfloor K/2 \rfloor + 1, K\}$, due to symmetry, e.g., $P_{M_0}(x, K, \lfloor K/2 \rfloor + 1) = P_{F_0}(x, K, \lfloor K/2 \rfloor - 1)$, the inequalities above change direction and we get $h_{t_0}^K(P_F) < P_F$ for all $P_F \in (0, 1)$. Next, assume that (P_F^*, P_M^*), $(P_F^*, P_M^*) \neq (1, 1)$ is a valid pair that satisfies (A.14) and fix a small positive number δ. Since P_{F_0} is increasing,

$$P_{F_0}\left(P_F^* + \delta, K, \lfloor K/2 \rfloor - 1\right) > P_{F_0}\left(P_F^*, K, \lfloor K/2 \rfloor - 1\right), \quad \forall P_F^* \in [0, 1).$$

This suggests that the left hand side of (A.14) increases by adding δ to P_F^*. In order (A.14) to hold, its right hand side must also increase, which implies an increase of P_M^* by some positive number ϵ, since P_{M_0} is also an increasing function. Then, $(P_F^* + \delta, P_M^* + \epsilon) \in (\mathcal{F} \times \mathcal{M})_{t_0}^K$ for all $(P_F^*, P_M^*) \neq (1, 1)$ implies that $h_{t_0}^K$ is a monotonically increasing function. □

A.7 Proof of (7.18)

Proof Introducing a random variable X_K with a binomial distribution $B(K,\theta)$, it can be shown that

$$\mathcal{L}^K(\theta) = P[X_K > \lfloor K/2 \rfloor] - \frac{1}{1+\hat{\theta}(\theta)^{-K}}.$$

For every $\theta \leq \frac{1}{2}$, $P[X_K > \lfloor K/2 \rfloor] \leq \frac{1}{2}$ hence $P[X_K > \lfloor K/2 \rfloor] < \frac{1}{2}$. Assume that $\theta = \theta_K(x)$ where $\theta_K(x) = \frac{1}{2}\left(1 - \frac{x}{\sqrt{K}}\right)$, for some fixed positive x. Then, $\lfloor K/2 \rfloor = E[X_K] + x_K \sigma(X_K)$ with $x_K = x/\sqrt{4\theta_K(x)(1-\theta_K(x))} \sim x$. The central limit theorem implies that

$$\begin{aligned} P[X_K > \lfloor K/2 \rfloor] &= P\left[X_K > E[X_K] + x_K \sigma(X_K)\right] \\ &= P\left[\frac{X_K - E[X_K]}{\sigma(X_K)} > x_K\right] \\ &= P[X_K^{'} > x] = 1 - F(x) \text{ when } K \to \infty \end{aligned}$$

where $X_K^{'} \sim \mathcal{N}(0,\sigma^2)$. Since $\hat{\theta}(\theta_K(x))^{-K} \to \infty$ when $K \to \infty$, we get,

$$\lim_{K\to\infty} \sup_{\theta \leq 1/2} \mathcal{L}^K(\theta) \geq \lim_{K\to\infty} \mathcal{L}^K(\theta_K(x)) = 1 - F(x).$$

As $F(x) \to \frac{1}{2}$ when $x \to 0^+$, this proves the claim. □