Solutions: Homework Set # 4
Principles of Wireless Networks

Problem 1 (Min Cut-Rank Relation)

This proof is essentially based on the capacity characterization of the coherent network, where the channel matrix is known at the receiver. It is shown that in a coherent deterministic network, using random linear mapping at the relays, for any $\varepsilon > 0$, the rate $R = \min_{\Omega} \operatorname{rank}(\mathbf{G}_{\Omega,\Omega^c}) - \varepsilon$ is achievable with probability at least $1 - 2^{-T\varepsilon} 2^{|V|}$. Therefore, there exist at least 2^{TR} vectors in the range space of $\mathbf{H}$ with probability more than $1 - 2^{-T\varepsilon} 2^{|V|}$. The fact that the dimension of the range of a matrix is upper bounded by its rank, implies

$$\Pr[\operatorname{rank}(\mathbf{H}) < T(\min_{\Omega} \operatorname{rank}(\mathbf{G}_{\Omega,\Omega^c}) - \varepsilon)] < 2^{|V|} 2^{-T\varepsilon},$$

Problem 2 (Multi-Sources Deterministic Network)

This problem is a part of a published paper "On Noise Strategies for Wireless Network Secrecy," by E. Perron, S. Diggavi, and E. Telatar.

(a). (i) is true by the symmetry of the code construction.

(ii) holds since if the decoder cannot distinguish between (w_1, w_2) and (w_1', w_2'), it can only choose one of them randomly as the decoded message, and there is a non-zero probability to choose the wrong one. However, if it can distinguish, it never makes a mistake.

(b). (i) is just a union bound (it can be replaced by equality, since the events are disjoint).

(ii) holds because the terms for which $\mathcal{N}(\mathcal{S}_I) \not\subseteq \Omega^c$ are zero. That is because a node in $\mathcal{N}(\mathcal{S}_I)$ does not receive anything from $\mathcal{S}_I$ and therefore cannot distinguish between (W_{I^c}, W_I) and (W_{I^c}, W_I').

(iii) is due to $\Pr[A \& B|C] = \Pr[A|C]\Pr[B|A \& C] \leq \Pr[B|A \& C]$.

(c). The proof of this inequality is similar to the error probability analysis for deterministic network we have seen in the class.

(d). The number of terms in $\sum_{w_1' \neq w_1}$ is the number of different messages can be transmitted by the first source which is $2^{TR_1} - 1$. Similarly, we can show that the number of terms in the second and third summations are $2^{TR_2} - 1$, and $(2^{TR_1} - 1)(2^{TR_2} - 1) < 2^{T(R_1+R_2)}$.

(e). It is shown in part (c) that any inner expectation in (b) is upper bounded by $2^{-TH(Y_{\Omega^c}|X_{\Omega^c})} \leq 2^{-T \min_{\Omega \in \bar{\Lambda}} H(Y_{\Omega^c}|X_{\Omega^c})}$, where the last term does not depend on the particular cut. Therefore the whole summation can be bounded by the number of terms ($|\Lambda|$) times the maximum one. Putting all together we obtain (e).

(f). Note that the upper bound on $\mathbb{E}[\Pr(\text{err})]$ goes to zero, if and only if all three terms go to zero. The number of cuts are constant, and do not increase as $T \to 0$. Here are the constraints on (R_1, R_2) to have vanishing error probability.

$$R_1 < \min_{\Omega \in \tilde{\Lambda}_{\{S_1\}}} H(Y_{\Omega^c} | X_{\Omega^c}) \tag{1}$$

$$R_2 < \min_{\Omega \in \tilde{\Lambda}_{\{S_2\}}} H(Y_{\Omega^c} | X_{\Omega^c}) \tag{2}$$

$$R_1 + R_2 < \min_{\Omega \in \tilde{\Lambda}_{\{S_1, S_2\}}} H(Y_{\Omega^c} | X_{\Omega^c}). \tag{3}$$

(g). Since $\tilde{\Lambda}_I \subseteq \Lambda_I$, the minimization in the LHS is more restricting, and its value can not be less that the value of the RHS. The other inequality follows from the chain as follows.

$$\begin{aligned}
H(Y_{\Omega'^c} | X_{\Omega'^c}) &\overset{(i)}{=} H(Y_{\Omega^{*c}} | X_{\Omega'^c}) + H(Y_{\mathcal{N}(I) \setminus \Omega^{*c}} | Y_{\Omega^{*c}} X_{\Omega'^c}) \\
&\overset{(ii)}{=} H(Y_{\Omega^{*c}} | X_{\Omega'^c}) \\
&\overset{(iii)}{\leq} H(Y_{\Omega^{*c}} | X_{\Omega^{*c}}) \\
&\overset{(iv)}{=} \min_{\Omega \in \Lambda_I} H(Y_{\Omega^c} | X_{\Omega^c}),
\end{aligned}$$

where

(i) is by using chain rule.

(ii) is true because Ω'^c contains $\mathcal{N}(I)$, and since $\mathcal{N}(I)$ is in flow of itself, $Y_{\mathcal{N}(I)}$ is a function of $X_{\mathcal{N}(I)}$.

(iii) holds since $\Omega^{*c} \subseteq \Omega'^c$, and conditioning reduces entropy.

(iv) is due to the assumption that Ω^* is the minimizer cut.

Problem 3 (Typicality in deterministic channels)

(a). Note that we have

$$p(y|x=a) = \begin{cases} 1 & \text{if } y = f(a) \\ 0 & \text{else.} \end{cases}$$

Therefore, $p(x,y) = p(x)p(y|x) = p(x)\mathbf{1}_{[y=f(x)]}$, where $\mathbf{1}_{[.]}$ is the indicator function. For $\underline{x}$ and $\underline{y} = f(\underline{x})$, we have

$$\nu_{\underline{x},\underline{y}}(x,y) = \frac{1}{T} |\{t : (x_t, y_t) = (x, f(x))\}| = \frac{1}{T} |\{t : x_t = x\}| = \nu_{\underline{x}}(x).$$

Therefore we have

$$\begin{aligned}
|\nu_{\underline{x},\underline{y}}(x,y) - p(x,y)| &\leq |\nu_{\underline{x}}(x) - p(x)| \\
&\leq \delta p(x) \\
&= \delta p(x,y),
\end{aligned}$$

where the second inequality holds since $\underline{x} \in T_\delta$.

(b). Let $(\underline{x}, \underline{y})$ be jointly typical. For a pair of (x,y) with $y \neq f(x)$, we have $p(x,y) = p(x)p(y|x) = 0$. Hence definition of jointly typical sequences implies

$$|\nu_{\underline{x},\underline{y}}(x,y) - 0| = |\nu_{\underline{x},\underline{y}}(x,y) - p(x,y)| \leq \delta p(x,y), = 0,$$

and therefore $\nu_{\underline{x},\underline{y}}(x,y) = 0$. We also know that

$$\nu_{\underline{x}}(x) = \sum_{y \in \mathcal{Y}} \nu_{\underline{x},\underline{y}}(x,y) = \nu_{\underline{x},\underline{y}}(x, f(x)),$$

where the last equality holds since there is only one non-zero term in the summation. This implies $\underline{y} = f(\underline{x})$. Moreover,

$$\begin{aligned}
|\nu_{\underline{x}}(x) - p(x)| &= |\nu_{\underline{x},\underline{y}}(x, f(x)) - p(x)p(f(x)|y)| \\
&\leq \delta p(x)p(f(x)|y) \\
&= \delta p(x), \qquad \forall x \in \mathcal{X}
\end{aligned}$$

which is the definition of typicality for $\underline{x}$. Note that the inequality comes from the definition of typicality for $(x,y) = (x, f(x))$.