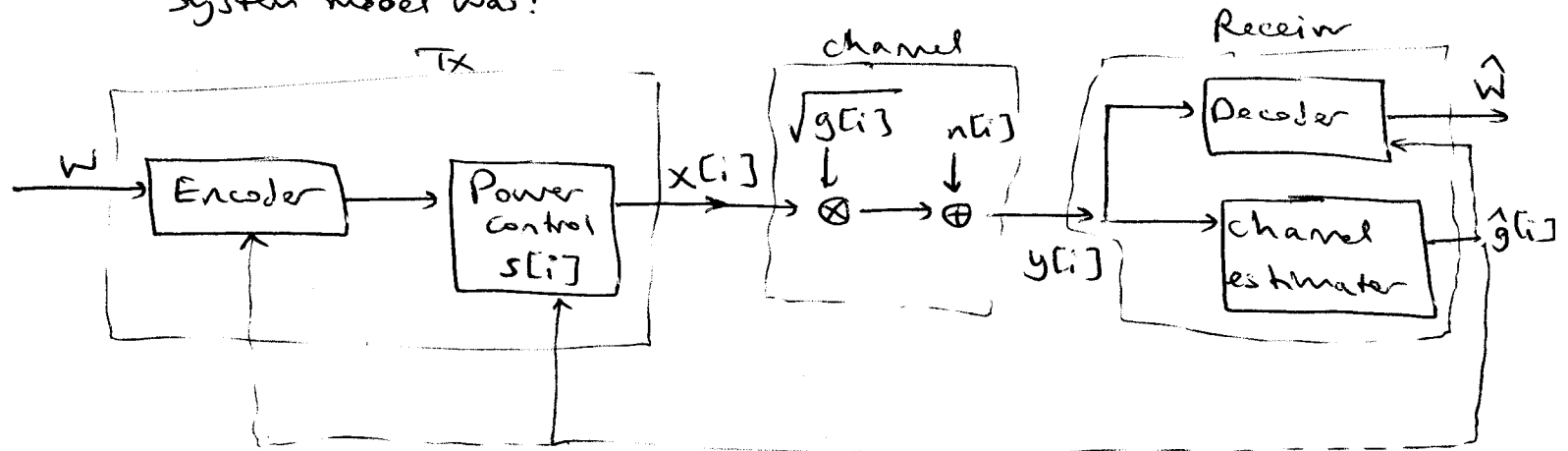


LECTURE #9

— Last time, we examined the capacity of fading channels. under different cases of tx/rx side information, our basic

System model was:

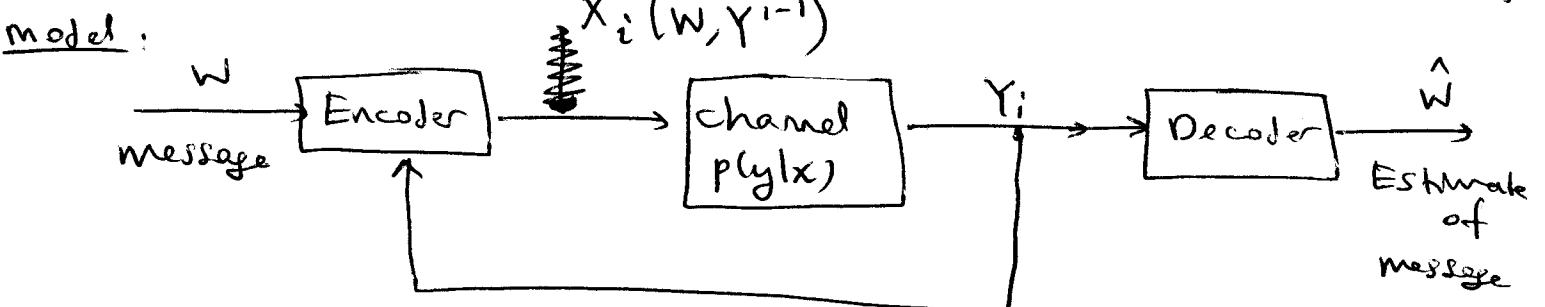


Review of capacity of channels with feedback :

Theorem 1: Feedback does not increase the capacity of discrete memoryless channels, i.e. $C_{FB} = C$.

However, 1) Feedback may lower the complexity of the receiver implementation,

2) Feedback does increase the capacity of correlated channels.



Assumptions:

- Assume that all received symbols are sent back immediately and noiselessly to the Tx.

Pf (Proof of the theorem): ~~Forwards~~

Define a $(2^{nR}, n)$ feedback code as a sequence of

$\uparrow$ $\uparrow$
 # of length of a
~~feedback codes~~ codeword

mappings $x_i(W, Y^{i-1})$. [These mappings are performed at the Tx, (Note that each mapping for symbol i uses the message W and the previous $\{Y^{i-1}\}$ which the Tx received via feedback.] and

$(Y_1^*, \dots, Y_{n-1}^*)$

a sequence of decoding functions $g: Y^n \rightarrow \{1, 2, \dots, 2^{nR}\}$. Thus

$$P_e^{(n)} = \Pr\{g(Y^n) \neq W\}$$

when $W \sim \text{uniform}\{1, \dots, 2^{nR}\}$

Definition: $C_{FB} = \sup\{\text{achievable rates by feedback codes}\}$

Theorem: $C_{FB} = C = \max_{p(x)} I(X; Y)$

Pf (continued):

Note that $C_{FB} \geq C$ (since not using any Y^{i-1} means do a code without feedback)

If $W \sim \text{Uniform} \{1, \dots, 2^{nR}\}$, then

$$\begin{aligned} \boxed{nR} &\stackrel{\text{since } W \sim \text{uniform}}{=} H(W) = H(W|Y^n) + I(W; Y^n) && \text{(by def'n of mutual information)} \\ &\leq [1 + P_e^{(n)} \cdot nR] + I(W; Y^n) && \text{(by Fano's inequality)} \end{aligned}$$

Now,

$$\begin{aligned} I(W; Y^n) &= H(Y^n) - H(Y^n|W) && \text{by def'n of } I(\cdot, \cdot) \\ &= H(Y^n) - \sum_{i=1}^n H(Y_i | Y_1, \dots, Y_{i-1}, W) && \text{[chain rule]} \\ &= H(Y^n) - \sum_{i=1}^n H(Y_i | Y_1, Y_2, \dots, Y_{i-1}, \underbrace{W, X_i}_{\substack{\uparrow \\ (X_i \text{ is a fn of } W \text{ and } Y_1, \dots, Y_{i-1})}}) \\ &= H(Y^n) - \sum_{i=1}^n H(Y_i | X_i) && \text{(since } Y_i \text{ is independent of } W \text{ and } Y_1, \dots, Y_{i-1} \text{ given } X_i) \end{aligned}$$

Then:

$$\begin{aligned} I(W; Y^n) &= H(Y^n) - \sum_{i=1}^n H(Y_i | X_i) \\ &\leq \sum_{i=1}^n H(Y_i) - \sum_{i=1}^n H(Y_i | X_i) && \text{[since } H(Y^n) \leq \sum_{i=1}^n H(Y_i) \text{ if the } Y_i \text{ are independent]} \\ &= \sum_{i=1}^n I(X_i; Y_i) \leq nC. \end{aligned}$$

Then: (from p.3)

$$nR \leq [1 + P_e^{(n)}] nR + nC.$$

$$\Leftrightarrow R \leq \frac{1}{n} + P_e^{(n)} \cdot R + C.$$

$$\Rightarrow R \leq \frac{1}{n} + C$$

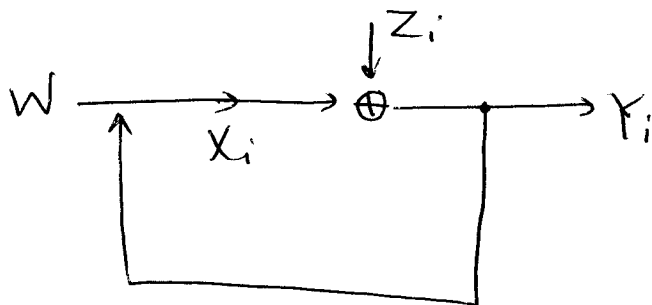
$$n \rightarrow \infty: R \leq C.$$

$$\text{Hence: } C_{FB} = C.$$

Gaussian Channel with feedback:

- For memoryless (PMC) Gaussian channels, we know from the above Theorem 1, that feedback does not increase capacity.
- But: for correlated channels, feedback does increase capacity - we demonstrate this for ^{correlated} GSN channels.

Model:



$$Y_i = X_i + Z_i,$$

$$Z_i \sim \mathcal{N}(0, K_z^{(n)})$$

← covariance matrix
of the noise
process

• A $(2^{nR}, n)$ code for the GSN channel with feedback is:

• a sequence of mappings $x_i: (W, Y^{i-1})$

(where $W \in \{1, 2, \dots, 2^{nR}\}$ is the input message)

Y^{i-1} : sequence of previous values of ~~input~~ output

Power constraint: ↖ power level σ

$$E \left[\frac{1}{n} \sum_{i=1}^n x_i^2(W, Y^{i-1}) \right] \leq P \quad \forall W \in \{1, \dots, 2^{nR}\}$$

↑
over all possible
noise sequences
↑
a fixed W

— Because of feedback, X^n and Z^n are not independent.

(X_i ^{may} depend on the previous values of Z .)

Result:

1. With feedback: $C_{n, FB}$ (bits per transmission of the ~~time-varying~~ ^{correlated} GSN channel)

$$C_{n, FB} = \max_{\frac{1}{n} \text{tr}(K_X^{(n)}) \leq P} \frac{1}{2n} \log_2 \frac{|K_{X+Z}^{(n)}|}{|K_Z^{(n)}|}$$

↑
trace

Where max is taken over all X^n of the form:

$$X_i = \sum_{j=1}^{i-1} b_{ij} Z_j + \tilde{V}_i \quad i=1, 2, \dots, n$$

and $\tilde{V}^n \perp Z^n$.

[That is, the input encoding is done as a linear combination of the past noise samples, and as a linearly additive, independent ~~function~~ ^{sequence} V^n].

[See Cover for the argument that this ~~does not~~ give no p. 258

loss of generality since the channel is GSN.]

Write $X = BZ + V$. $\leftarrow$ (i-dimensional)

$$Y = X + Z$$

$$C_{n,FB} = \max \frac{1}{2n} \log_2 \frac{(B+I) K_Z^{(n)} (B+I)^T + K_V}{|K_Z^{(n)}|}$$

(no feedback $\Rightarrow B=0$)

taken over all ~~non-negative~~ non-negative definite K_V and

~~lower triangular~~ lower triangular B s.t. $\text{tr}(B K_Z^{(n)} + K_V) \leq nP$

2. Without feedback:

$$C_n = \max_{\frac{1}{n} \text{tr}(K_X^{(n)}) \leq P} \frac{1}{2n} \log_2 \frac{|K_X^{(n)} + K_Z^{(n)}|}{|K_Z^{(n)}|}$$

THM: $C_{n,FB} \leq C_n + \frac{1}{2}$ (bits per transmission)

$\therefore$ Feedback increases the capacity of a correlated GSN channel ~~by~~ by at most $\frac{1}{2}$ bit per transmission.

(Recall. feedback channel assumed noiseless)

Now, let us turn to fading channels; in particular

- Side information at the Receiver:

We said last time that:

$$C(S) = \int_0^\infty B \log_2(1+\gamma) p(\gamma) d\gamma$$

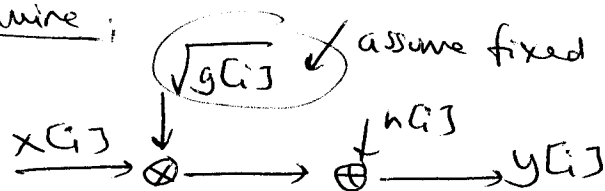
$\Rightarrow$ at Tx:
 [no power adaptation]
 [no rate adaptation]

which is the same expression as if tx had the knowledge of $g[i]$, but could not do power adaptation.

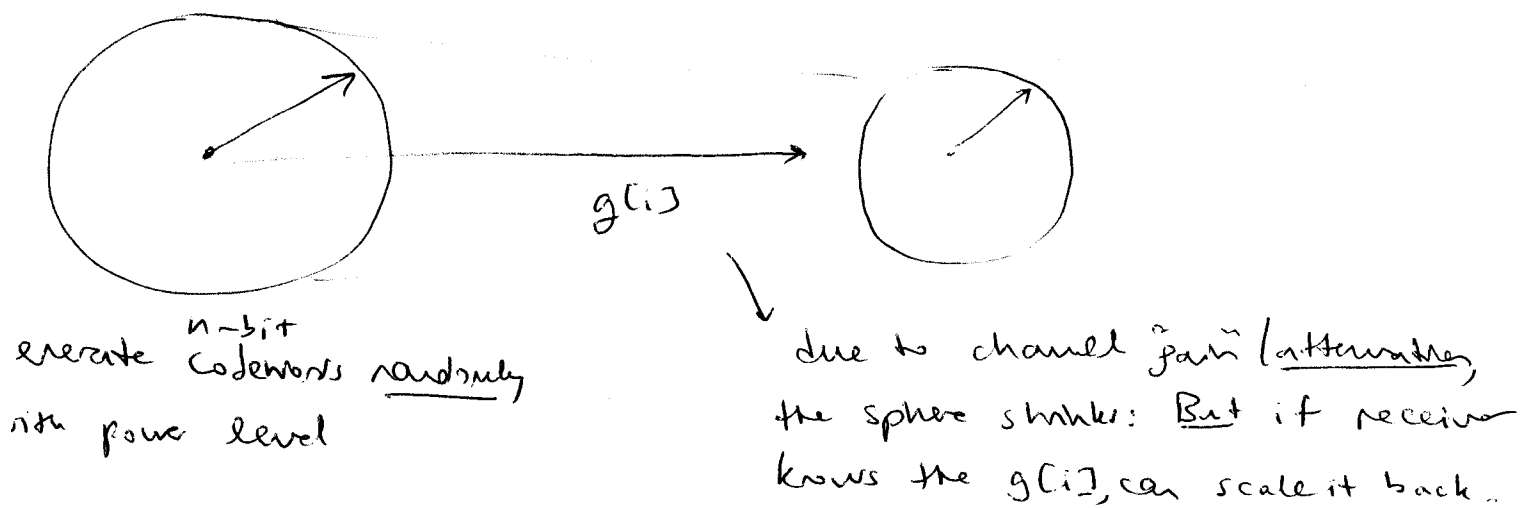
• Why is this the case?

Reason: Note that Pf of Shannon capacity not constructive [does not tell you how to code ~~the~~ except random codes]

Key Scenarios to examine:



Remember, the proof of channel coding theorem for the G_{SN} channel.



Note that the receiver knows the codebook $\{X^n(1), \dots, X^n(2^{nR})\}$, hence, can decode using joint typicality. [Roughly 2^{nI} of the sequences are jointly typical.]

Hence: Capacity of an AWGN channel ^{with gain} with $g[\cdot]$ known only at the receiver is: $B \log_2(1 + \overset{\text{SNR}}{\gamma})$. $\left(\gamma = \frac{g[\cdot] \cdot E_k}{\sigma^2} \right)$

— using Wolfowitz's result gives: $\int_0^\infty B \log_2(1 + \gamma) p(\gamma) d\gamma$.

▲

— Let's go back to Lecture 8, p.13, ~~to~~ to continue our development of Adaptive Modulation with M-QAM constellations.

— Symbol period: T_s

• M-QAM

• Assume ideal Nyquist pulses

Definitions:

$\bar{S} \triangleq$ avg power constant at T_x .

$$\int_0^\infty S(\gamma) p(\gamma) d\gamma \leq \bar{S}$$

$B =$ bandwidth (Hz)

$N_0 =$ noise spectral density

$$\gamma[i] = \frac{\bar{S} \cdot g[i]}{N_0 \cdot B} \quad (\text{SNR of } i\text{th symbol})$$

$$\left[\bar{\gamma} = \frac{\bar{S}}{N_0 \cdot B} \right]$$

$$\left[\frac{\bar{E}_s}{N_0} = \frac{\bar{S} \cdot T_s}{N_0} = \bar{\gamma} \right]$$

For fixed M :

$$R = \frac{\log_2 M}{T_s}$$

M-QAM modulation

(with ideal coherent phase detection)

Bounds:

$$\text{BER} \leq 2 e^{-1.5 \bar{\gamma} / (M-1)} \quad [\text{AWGN channel, M-QAM}]$$

For $M \geq 4$ and $0 \leq \bar{\gamma} \leq 30 \text{ dB}$, a tighter bound:

$$\text{BER} \leq 0.2 e^{-1.5 \bar{\gamma} / (M-1)} \quad [\text{AWGN channel, M-QAM}]$$

Under adaptive modulation:

$$\text{BER}(\gamma) \leq 0.2 e^{-1.5 \left[\gamma \cdot \frac{S(\gamma)}{\bar{S}} \right] / (M-1)}$$

Idea: Adjust $M(\gamma)$ and $S(\gamma)$ to maintain a fixed BER at the receiver.

(Solve for M in terms of BER)

$$\Leftrightarrow M(\gamma) = 1 + \frac{1.5 \gamma}{-\ln(5 \text{BER})} \cdot \frac{S(\gamma)}{\bar{S}}$$

The spectral efficiency for M-QAM is $\log_2 M$.

$$\max \underbrace{E[\log_2 M(\gamma)]}_{\text{avg spectral efficiency}} = \int_0^\infty \log_2 \left(1 + \frac{1.5 \gamma}{-\ln(5 \text{BER})} \cdot \frac{S(\gamma)}{\bar{S}} \right) p(\gamma) d\gamma$$

$$\text{s.t.} \quad \int_0^\infty S(\gamma) p(\gamma) d\gamma \leq \bar{S}$$

Solution, (necessary condition):

$$\frac{S(\gamma)}{\bar{S}} = \begin{cases} \frac{1}{\gamma_K} - \frac{1}{\gamma_{\text{th}}} & \gamma \geq \gamma_K = \boxed{\frac{\gamma_0}{K}} \\ 0 & \gamma < \frac{\gamma_0}{K} (= \gamma_K) \end{cases}$$

where $K = \frac{-1.5}{\ln(5 \text{ BER})}$ and $\gamma_K = \frac{\gamma_0}{K}$.

Then:

$$\max E[\log_2(M)] = \frac{\max R}{B} = \int_{\gamma_K}^{\infty} \log_2 \left[\frac{\gamma}{\gamma_K} \right] p(\gamma) d\gamma.$$



- This shows that uncoded M-QAM under adaptive modulation has an effective power loss of K relative to the optimal transmission scheme, independent of the fading distribution. [i.e. the distribution of the $g(\gamma)$ does not matter ~~in~~ in computing the "gap" but of course $g(\gamma)$ are in determining $p(\gamma)$.]

Recall:

$$\max f = \int_{\gamma_0}^{\infty} \log_2 \left(\frac{\gamma}{\gamma_0} \right) p(\gamma) d\gamma \quad (\text{from p. 6 of lecture 8,})$$

- We also see that K (in dB) is the maximum coding gain.

Channel inversion (using M-QAM).

$$\frac{R}{B} = \log_2 \left(1 + \frac{-1.5}{\ln(\text{BER})} E[\gamma] \right) \quad \text{for } M \geq 4$$

$0 \leq \gamma \leq 3 \sigma^2/B$

$$M(\gamma) = 1 + \frac{1.5}{-\ln(\text{BER})} \cdot \boxed{\frac{\gamma S(\gamma)}{\bar{S}}} \quad \rightarrow \sigma^2 = \text{constant under channel inversion}$$

$$\left[\frac{R}{B} \right] = \log_2 M(\gamma) = \log_2 \left[1 + \frac{1.5}{-\ln(\text{BER})} \cdot \sigma \right]$$

$$= \log_2 \left[1 + \frac{-1.5}{\ln(\text{BER}) \cdot E[\gamma]} \right]$$

(since $\sigma = \frac{1}{E[\gamma]}$)

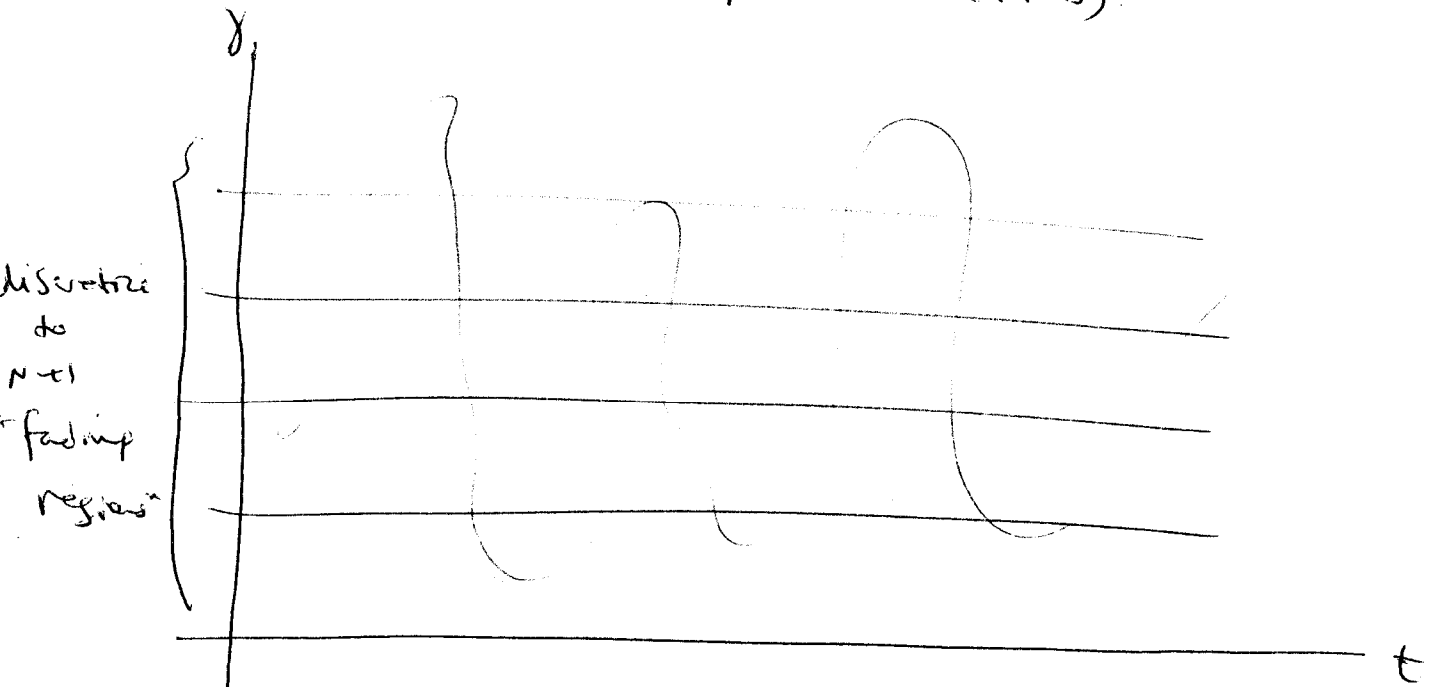
Truncated channel inversion : (M-QAM)

$$\frac{R}{B} = \max_{\gamma_0} \left[\log_2 \left[1 + \frac{-1.5}{\ln(\text{BER}) \cdot \left(\frac{E[\gamma]}{\gamma_0} \right)} \right] \cdot P_r(\gamma > \gamma_0) \right]$$

$$\int_{\gamma_0}^{\infty} \frac{1}{\gamma} p(\gamma) d\gamma$$

Constellation restriction

- Now, we restrict $M \in \{0, 2, 4, 6, 16, 64, 256, \dots\}$
(Square constellations).



- Associate M_j with the j th fading region.

Region boundaries

$$M(\gamma) = \frac{\gamma}{\gamma_k^*} \quad [\gamma = \gamma_k^* \cdot M_j]$$

where γ_k^* is a parameter to be optimized.

Define $M_{N+1} = +\infty$. (we will never use this.)

The M_N constellation will be the largest one used.)

For a fixed γ , transmit the largest constellation size (to maintain the BER) from the set M_j 's $\{0, 3, 4, 16, \dots\}$.

Ex) $2 \leq \frac{\gamma}{\gamma_k^*} < 4 \Rightarrow \text{use 2-QAM.}$

Region boundaries:

$$\gamma = \gamma_k^* \cdot M_j$$

Power control:

To satisfy a target BER ($\forall M_j > 0$).

$$\frac{S_j(\gamma)}{\bar{S}} = \begin{cases} (M_j - 1) \frac{1}{\gamma K} & M_j \leq \frac{\gamma}{\gamma_k^*} \leq M_{j+1} \\ 0 & M_j = 0. \end{cases}$$

Fixed BER, $\forall M_j > 0$:

$$\Rightarrow \left[\frac{E_s(j)}{N_0} = \frac{\gamma S_j(\gamma)}{\bar{S}} = \frac{(M_j - 1)}{K} \right]$$

$\left[\frac{E_s(j)}{N_0} \right] \cdot \frac{1}{\gamma} \quad 15$

Region (j)	γ	M_j	$S_j(\gamma) / \bar{S}$
0	$0 \leq \frac{\gamma}{\gamma_k^*} < 2$	0	0
1	$2 \leq \frac{\gamma}{\gamma_k^*} < 4$	2	$\frac{1}{K \cdot \gamma}$
2	$4 \leq \frac{\gamma}{\gamma_k^*} < 16$	4	$\frac{3}{K \cdot \gamma}$
3	$16 \leq \frac{\gamma}{\gamma_k^*} < 64$	16	$\frac{15}{K \cdot \gamma}$
4	$64 \leq \frac{\gamma}{\gamma_k^*} < +\infty$	64	$\frac{63}{K \cdot \gamma}$

$$\frac{R}{B} = \sum_{j=1}^N \log_2(M_j) \cdot \Pr\left\{M_j \leq \frac{\gamma}{\gamma_k^*} < M_{j+1}\right\}.$$

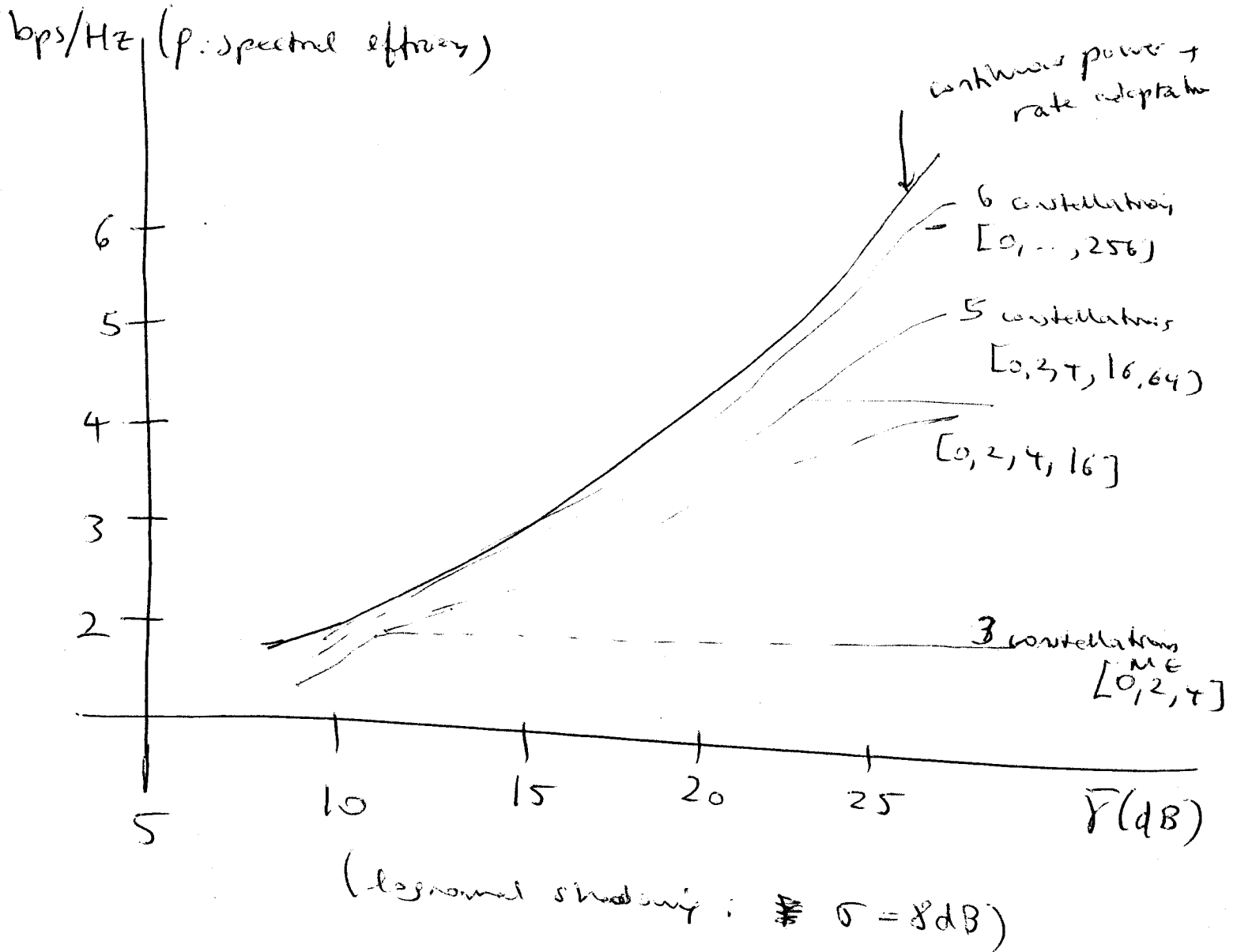
• Maximize $\frac{R}{B}$ w.r.t. γ_k^* .

$$\max \sum_{j=1}^N \log_2(M_j) \cdot \Pr\left\{M_j \leq \frac{\gamma}{\gamma_k^*} < M_{j+1}\right\}.$$

$$\text{s.t.} \quad \sum_{j=1}^{N-1} \int_{\gamma_k^* \cdot M_j}^{\gamma_k^* \cdot M_{j+1}} \frac{S_j(\gamma)}{\bar{S}} p(\gamma) d\gamma = 1.$$

(the total power constraint)

no closed form solution; use numerical search.



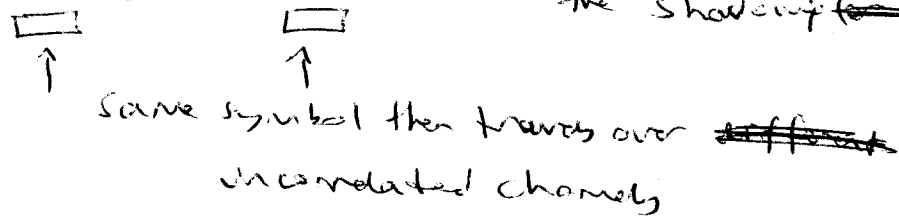
— we see that 6 constellation ME $[0, \dots, 256]$ gets you very close to what you would achieve by cont. power + rate adaptation.

DIVERSITY

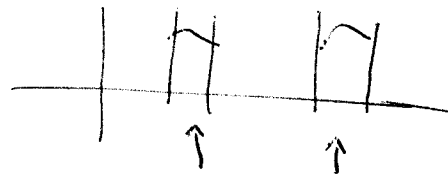
— refers to sending the same signal (info) over several paths (redundancy)

Types of Diversity:

- multiple receive antennas (Space diversity)
- time diversity: continue sending same signal
(for mobile applications) over a period $>$ coherence period of the channel (~~channel~~)



- frequency diversity:



($\Rightarrow$ see uncorrelated channels)

- ~~directional~~

polarization diversity (send same signal over vertical & horizontally polarized components)

- Antenna diversity — (MIMO systems)

o.e. several receive antennas

— Combining techniques :

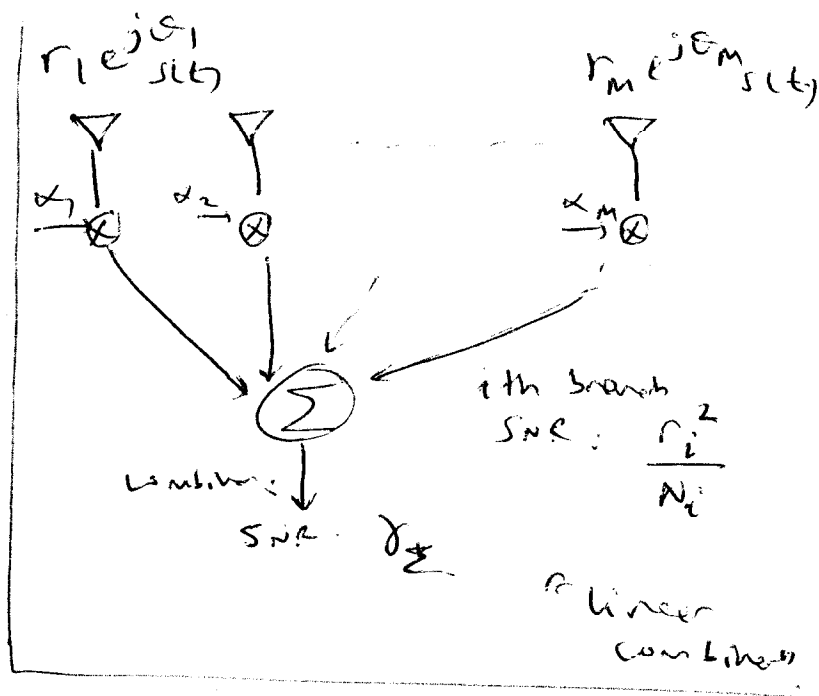
A. Selection

~~B. Threshold~~

B. MRC

C. Equal-gain combining

A. Selection combining :



— Strategy: choose the branch with the highest $SNR = \frac{r_i^2}{N_i}$
 (or practically highest $S+N$, if noise is same on all branches.)

Then: SNR of combiner $\gamma_\Sigma = \max_{1 \leq i \leq M} (\gamma_i)$

• Assume • M branches

• uncorrelated Rayleigh fading amplitudes r_i

$$\gamma_i = \frac{r_i^2}{N} \quad (\text{instantaneous SNR on branch } i)$$

• Assume noise power same on all branches (N)

Let $\bar{\gamma}_i \equiv E[\gamma_i]$

$$p(\gamma_i) = \frac{1}{\bar{\gamma}_i} e^{-\gamma_i/\bar{\gamma}_i} \quad (\text{pdf of SNR on } i\text{th branch})$$

Recall Rayleigh pdf:

$$p(r) = \frac{r}{\sigma^2} e^{-r^2/2\sigma^2}, \quad r \geq 0.$$

Make a change of variables:

$$p(\gamma_b) \cdot d\gamma_b = p(r) \cdot dr \quad \left(p(\gamma_b) = p(r) \cdot \left| \frac{dr}{d\gamma_b} \right| \right)$$

SNR per bit

for a given amplitude $r \equiv \gamma_b = \frac{r^2}{2\sigma_n^2}$

← mean.

σ_n^2 : noise var in in-phase & quadrature branches.

Then:

$$p(\gamma_b) = \frac{\sigma_n^2}{\sigma^2} e^{-\gamma_b \cdot \sigma_n^2 / \sigma^2}$$

$$[\bar{\gamma}_b = \frac{\sigma^2}{\sigma_n^2}]$$

$$p(\gamma_b) = \frac{1}{\bar{\gamma}_b} \cdot e^{-\gamma_b / \bar{\gamma}_b}, \quad \gamma_b \geq 0$$

Hence, when the envelope r has a Rayleigh distribution,

the SNR per bit $\gamma_b \equiv \frac{r^2}{2\sigma_n^2}$ is exponential with

parameter: $\frac{1}{\bar{\gamma}_b}$. (mean $\bar{\gamma}_b$)

Then: in branch

$$p(r_i) = \frac{1}{\bar{r}_i} e^{-r_i/\bar{r}_i}, \quad r_i \geq 0$$

$$P_{out}^{(i)} = P\{r_i < r_0\}$$

$$= \int_0^{r_0} \frac{1}{\bar{r}_i} e^{-r_i/\bar{r}_i} dr_i = 1 - e^{-r_0/\bar{r}_i}$$

$$P_{out}(\text{Gm Line}) = P\{r_\Sigma < r_0\}$$

$$= P\{\max(r_i) \leq r_0\}$$

$$= P\{r_1 \leq r_0, \dots, r_M \leq r_0\}$$

$$= \prod_{i=1}^M P\{r_i < r_0\}$$

(by independence of the branches)

~~(1 - e^{-r_0/\bar{r}_i})^M~~

$$= \prod_{i=1}^M (1 - e^{-r_0/\bar{r}_i})$$

$$= (1 - e^{-r_0/\bar{r}})^M$$

if $\bar{r}_i = \bar{r} \quad \forall i$

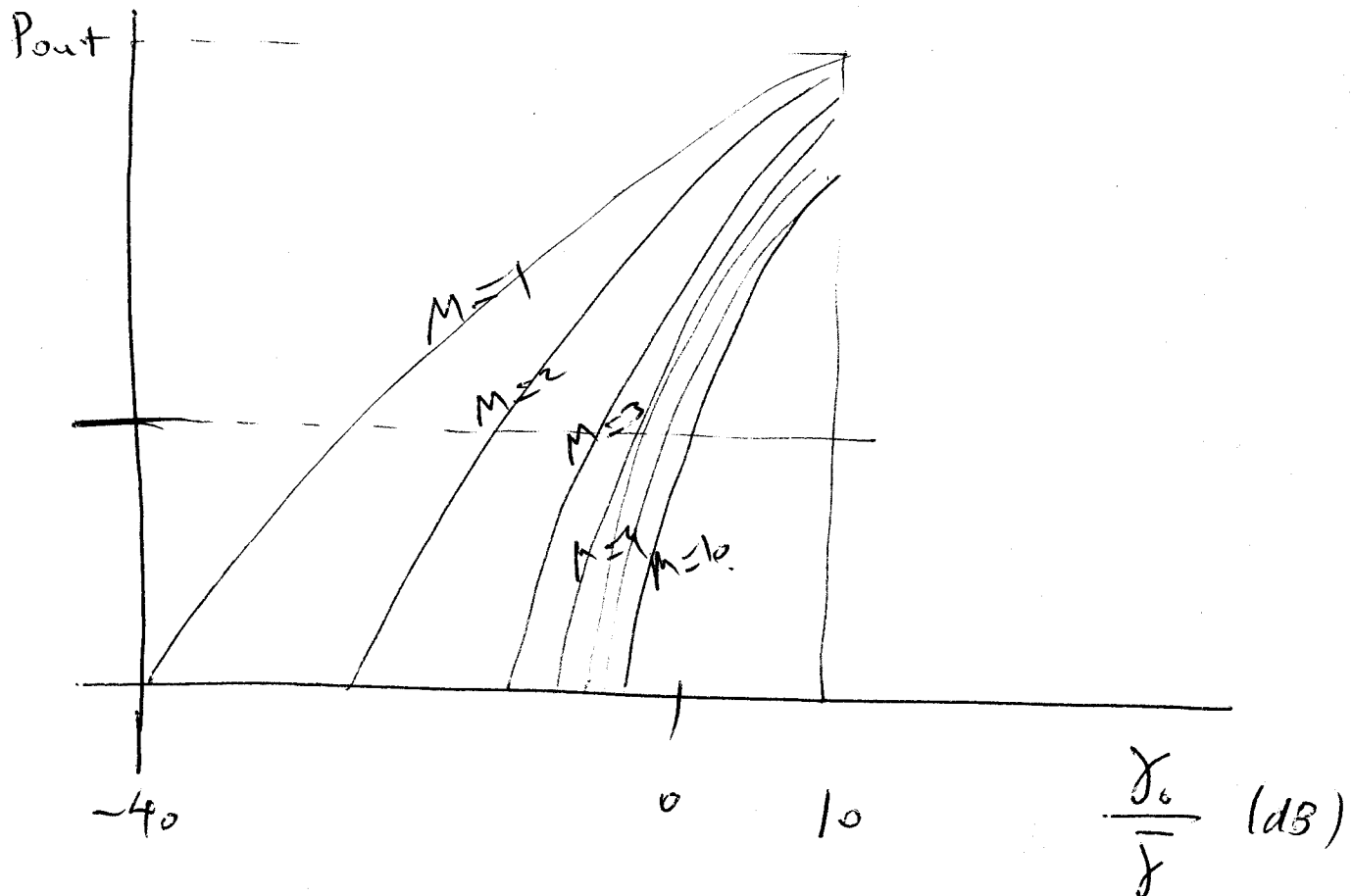
$$P_{r_z}(\gamma) = \frac{d}{d\gamma} P\{\gamma_z < \gamma_0\}$$

$$= \frac{M}{\bar{\gamma}} (1 - e^{-\gamma/\bar{\gamma}})^{M-1} e^{-\gamma/\bar{\gamma}}$$

$$\bar{\gamma}_z = \int_0^{\infty} \gamma \cdot P_{r_z}(\gamma) d\gamma$$

$$\bar{\gamma}_z = \bar{\gamma} \cdot \sum_{i=1}^M \frac{1}{i}$$

— SNR increases with M , but with diminishing returns.



- Note that $M \rightarrow \infty$ gives $\bar{P}_E \rightarrow +\infty$
(harmonic series diverges).

but not physically possible, ~~is~~ - the antennas in a given area will become correlated.

calculation of $\bar{P}_b$:

$$\bar{P}_b = \int_0^\infty \underbrace{P_b(\gamma)}_{\substack{\uparrow \\ \text{the bit error rate of the particular modulation} \\ \text{scheme} \\ \text{(BPSK, etc.)}}} \cdot \underbrace{P_{rE}(\gamma)}_{\substack{\swarrow \\ \text{after combining}}}$$

② Threshold combining.

Idea: scan each of the branches in sequential order & output first signal with a power above a threshold.

- As long as the signal remains above threshold, it outputs that signal.

otherwise - do another seq. search.

- If cannot find

⑧ MRC:

Idea: weight each branch based on its SNR.

- Remove the phase, then combine.

$$r = \sum_{i=1}^M a_i r_i$$

(Assume $N_i = N$),
at i th branch

$$N_{\text{total}} = \sum_{i=1}^M a_i^2 \cdot N$$

$$\gamma_z = \frac{r^2}{N_{\text{total}}} = \frac{\left(\sum_{i=1}^M a_i r_i \right)^2}{\left(\sum_{i=1}^M a_i^2 \right) \cdot N}$$

↑
maximize this

— ^{can be} shown that optimal $a_i^* = \frac{r_i^2}{N}$

$$\boxed{\gamma_z^* = \sum_{i=1}^M \frac{r_i^2}{N} = \sum_{i=1}^M \gamma_i}$$

↑ sum of γ_i

- SNR increases linearly with # of diversity branches.

Let $\bar{\gamma}_i = \bar{\gamma}$ $\forall i$. ($\gamma_i \sim \exp.(1/\bar{\gamma}_i)$)

$\gamma_z \sim \chi^2$ with ~~2M~~ degree of freedom.

~~chi-squared~~

gamma $(\frac{1}{\bar{\gamma}}, M)$

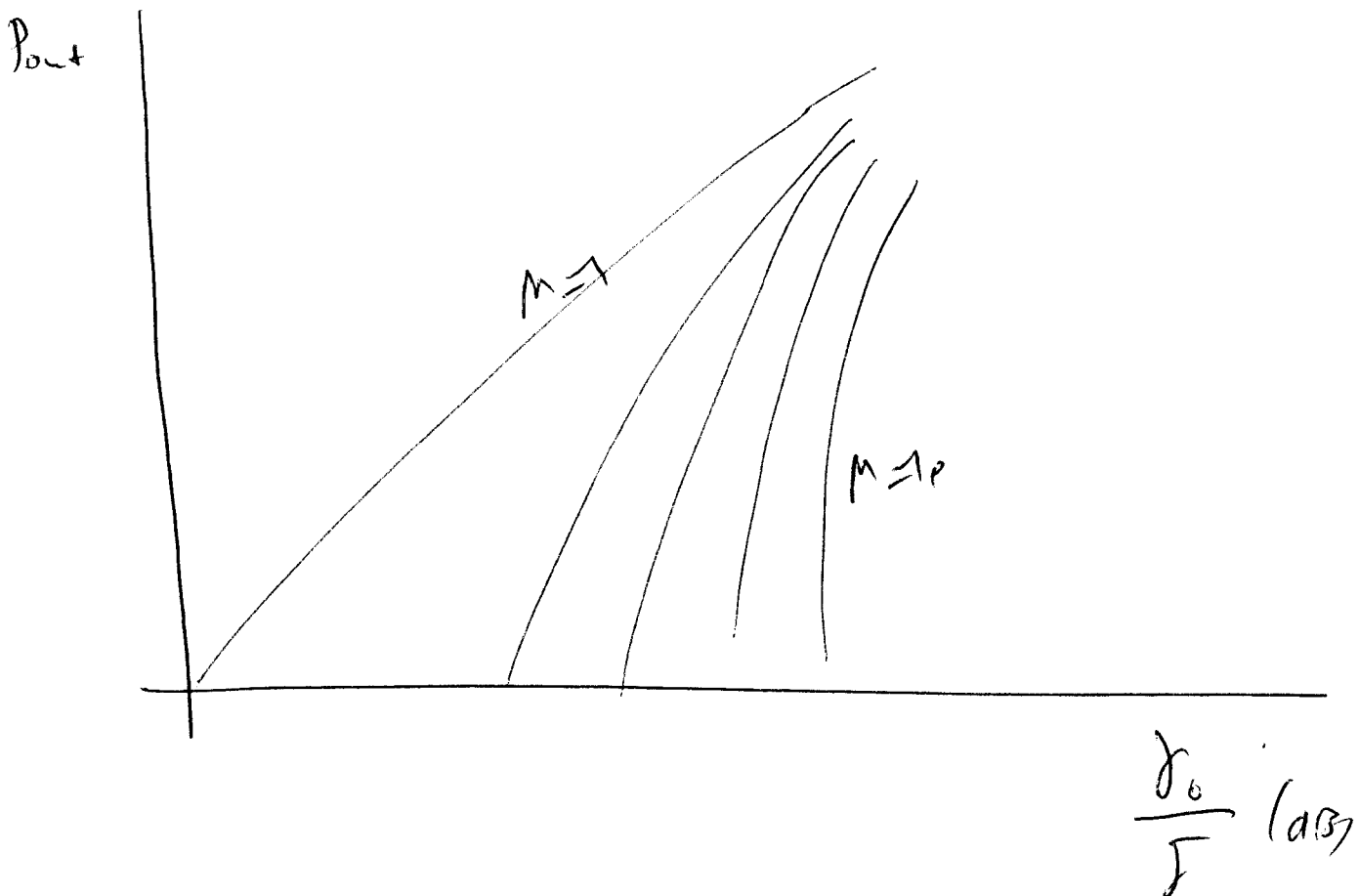
$$\boxed{\bar{\gamma}_2 = M \cdot \bar{\gamma}}$$

$$\text{Var}(\gamma_2) = \frac{\bar{\gamma}}{2}$$

$$P_{\gamma_2}(\gamma) = \frac{\gamma^{M-1} e^{-\gamma/\bar{\gamma}}}{\bar{\gamma}^M (M-1)!}, \quad \gamma \geq 0$$

$$P_{\text{out}} = \Pr\{\gamma_2 < \gamma_0\} = \int_0^{\gamma_0} P_{\gamma_2}(\gamma) d\gamma$$

$$= 1 - e^{-\gamma_0/\bar{\gamma}} \sum_{k=1}^M \frac{(\gamma_0/\bar{\gamma})^{k-1}}{(k-1)!}$$



Equal path combining

Idea: MRC requires knowledge of the $\bar{\gamma}$.

—EGC: sets $a_i = 1$.

$$\gamma_z = \frac{(\sum r_i)^2}{\underbrace{N_{\text{total}}}_{N \cdot M}} = \frac{1}{NM} \left(\sum_{i=1}^M r_i \right)^2.$$

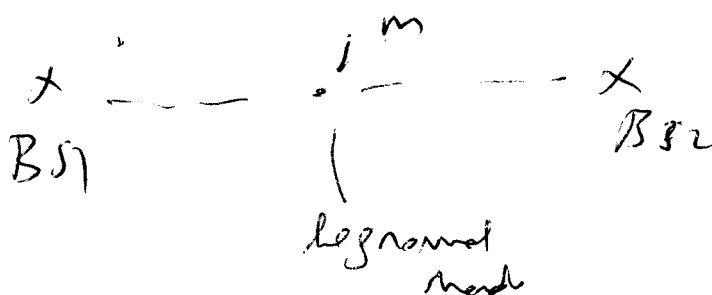
~~For~~ $M=2$ case:

$$P_{\text{out}} = \Pr\{\gamma_z < \gamma_0\}$$

$$= 1 - e^{-2(\gamma_0/\bar{\gamma})} - \sqrt{\pi \left(\frac{\gamma_0}{\bar{\gamma}} \right)} e^{-(\gamma_0/\bar{\gamma})} \text{erf}\left(\sqrt{\gamma_0/\bar{\gamma}}\right)$$

Performance loss $\approx \underline{1.3 \text{ dB}}$ (small)
with r.f. MRC

Macroscopic diversity ($B \times$ diversity)



selection
diversity
(select B) with
best signal at
(instant)

Fano's Inequality:

For a DMC with codebook $\mathcal{C}$ and W (input messages)

uniformly distributed,

$$H(X^n|Y^n) \leq 1 + p_e^{(n)} \cdot nR$$

where $p_e^{(n)} = \Pr(W \neq \hat{g}(Y^n))$

pf Define $E = \begin{cases} 1 & \text{if } \hat{W} \neq W \\ 0 & \text{otherwise} \end{cases}$ (error event)

Then,

$$\begin{aligned} H(E, W|Y^n) &= H(W|Y^n) + H(E|W, Y^n) && \text{(chain rule; conditioning)} \\ &= H(E|Y^n) + H(W|E, Y^n) && \text{[condition the other way]} \end{aligned}$$

• Since $E = \text{function of } \{W, g(Y^n)\}$, $H(E|W, Y^n) = 0$.

• Since E is binary-valued, $H(E) \leq 1$

• Finally,

$$\begin{aligned} H(W|E, Y^n) &= \underbrace{(1-p_e^{(n)})}_{\Pr(E=0)} \underbrace{H(W|E=0, Y^n)}_{\substack{\uparrow 0 \\ \text{since } \hat{W}=W \Rightarrow W = \text{function of } (Y^n)}} + \underbrace{p_e^{(n)}}_{\Pr(E=1)} \cdot \underbrace{H(W|Y^n, E=1)}_{\substack{\leq \log(|W|-1) \\ \text{NR} \\ \text{(since } W \text{ can take on at most } nR \text{ values)}}}} \\ &\leq (1-p_e^{(n)}) \cdot 0 + p_e^{(n)} \cdot nR \\ &= p_e^{(n)} \cdot nR. \end{aligned}$$

Since $W|Y^n$ can take on at most nR values,

Then:

$$H(W|Y^n) + \overset{\nearrow 0}{H(E|W, Y^n)} = \underbrace{H(E|Y^n)}_{\leq 1} + \underbrace{H(W|E, Y^n)}_{\leq P_e^{(n)} \cdot nR}$$

(note that g is known here $g(Y^n)$ known)

$$H(W|Y^n) \leq 1 + P_e^{(n)} \cdot nR.$$

- For a fixed code $X^n(W)$, $X^n(W)$ is a function of W .

$$\Rightarrow \boxed{H(X^n(W)|Y^n) \leq H(W|Y^n) \leq 1 + P_e^{(n)} \cdot nR}$$

i.e. $\boxed{H(X^n|Y^n) \leq 1 + P_e^{(n)} \cdot nR}$