PROBLEM 1. Consider the sequence $M_0, M_1, \ldots$ of matrices constructed recursively as follows:

$$M_0 = [+1] \quad \text{and} \quad M_{r+1} = \begin{bmatrix} +M_r & +M_r \\ +M_r & -M_r \end{bmatrix} \text{ for } r = 0, 1, \ldots$$

For example, we have,

$$M_1 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}, \quad M_2 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}, \quad \ldots$$

Note that M_r is a $2^r \times 2^r$ matrix with elements taking values in $\{+1, -1\}$. Each row (and each column) has squared Euclidean norm 2^r.
Now fix $r > 0$ and let $n = 2^r$. Let x be a row of M_r and write $x = [x'\, x'']$ where x' is the left half of x and x'' is the right half (for example, with $r = 2$ and $x = [+1, +1, -1, -1]$ being the 3rd row of M_2, we have $x' = [+1, +1]$ and $x'' = [-1, -1]$). As $\tilde{x} = [\tilde{x}'\, \tilde{x}'']$ steps through all the n rows of M_r, compute the inner products $p' = \langle x', \tilde{x}' \rangle$ and $p'' = \langle x'', \tilde{x}'' \rangle$. (For the example above (p', p'') takes the values $(2, -2)$, $(0, 0)$, $(2, 2)$ and $(0, 0)$ as $\tilde{x}$ steps through $[+1, +1, +1, +1]$, $[+1, -1, +1, -1]$, $[+1, +1, -1, -1]$ and $[+1, -1, -1, +1]$.)

(a) Show that for any row x of M_r, (p', p'') equals $(n/2, n/2)$ once, the value $(n/2, -n/2)$ once, and the value $(0, 0)$ for the remaining $n - 2$ times. Use this to conclude that the rows of M_r are orthogonal to each other.
Hint: One way is by induction on r.

Let $B_r = \begin{bmatrix} +M_r \\ -M_r \end{bmatrix}$. The $m = 2n$ rows of B_r consists of the rows of M_r and their negatives. Let $x = [x'\, x'']$ be a row of B_r. As $\tilde{x} = [\tilde{x}'\, \tilde{x}'']$ steps through all the m rows of B_r compute $p' = \langle x', \tilde{x}' \rangle$ and $p'' = \langle x'', \tilde{x}'' \rangle$.

(b) Show that for any row x of B_r, (p', p'') takes the value $(n/2, n/2)$ once, the value $(-n/2, -n/2)$ once, the value $(n/2, -n/2)$ once, the value $(-n/2, n/2)$ once, and the value $(0, 0)$ the remaining $m - 4$ times.
Hint: Use (a).

(c) Conclude that for any row x of B_r, $p' + p''$ takes the value n once, the value $-n$ once, and the value 0 the remaining $m - 2$ times.
Hint: Use (b).

PROBLEM 2. Suppose we have a channel whose input $x = [x'\, x'']$ is a real vector of even dimension n (so that x' and x'' are of dimension $n/2$). The channel has two behaviors determined by an internal state $s \in \{1, 2\}$. The output $Y = [Y'\, Y'']$ is given by

$$(Y',\, Y'') = \begin{cases} \left(\sqrt{g}x' + Z',\, x'' + Z''\right) & \text{if } s = 1, \\ \left(x' + Z',\, \sqrt{g}x'' + Z''\right) & \text{if } s = 2, \end{cases}$$

where $g \geq 1$ is a non-negative constant and $Z = [Z'\, Z'']$ has i.i.d. $\mathcal{N}(0, \sigma^2)$ components. In other words, the channel subjects either the first half (if $s = 1$) or the second half (if $s = 2$) of the input vector to an energy gain g, and adds Gaussian noise.
Suppose $c_1, \ldots, c_m$ are the codewords for m equally likely messages for transmission over the channel above. Thus, each c_i is a real vector of (even) dimension n. Write $c_i = [c_i'\, c_i'']$ so that c_i' and c_i'' are real vectors of dimension $n/2$.

(a) Suppose the value of s is known to the receiver. What is the decision rule that minimizes the probability of error?

(b) Suppose $\|c_1'\| = \cdots = \|c_m'\|$ and $\|c_1''\| = \cdots = \|c_m''\|$. Let

$$\text{score}(i, Y, s) = \begin{cases} \sqrt{g}\langle Y', c_i'\rangle + \langle Y'', c_i''\rangle & s = 1, \\ \langle Y', c_i'\rangle + \sqrt{g}\langle Y'', c_i''\rangle & s = 2. \end{cases}$$

Show that

$$\hat{\imath} = \arg\max_i \text{score}(i, Y, s)$$

is an optimum decision rule for a receiver that observes $Y = [Y'\, Y'']$ and is aware of the value of s.

Now suppose that the receiver is *not* aware of the value of s. Still supposing that the codewords c_i are as in (b) (i.e., all have equal norms of their first halves, and equal norms of their second halves), consider the following way to assign a score to each message i based on the observation $Y = [Y'\, Y'']$:

$$\text{score}(i, Y) = \max_{s \in \{1,2\}} \text{score}(i, Y, s)$$

and the following two decoding rules. The first rule chooses the message with the highest score, i.e.,

$$\hat{\imath}_1 = \arg\max_i \text{score}(i, Y).$$

The second is based on a threshold t, and chooses the message $\hat{\imath}_2$ if $\hat{\imath}_2$ is the only i for which $\text{score}(i, Y) > t$. If there is no such i, or two or more such i's, it sets $\hat{\imath}_2 = 0$ — note that when $\hat{\imath}_2 = 0$ this decoding rule has certainly made an error.

(c) Argue that when $\hat{\imath}_2 \neq 0$, we have $\hat{\imath}_1 = \hat{\imath}_2$, and thus the probability of error of the second decoding rule is an upper bound to the probability of error of the first decoding rule.

PROBLEM 3. Let $r \geq 0$. Let the codewords for m messages, $c_1, \ldots, c_m$ be the rows of the matrix $\sqrt{\alpha}[B_r\, B_r]$, where B_r is as in Problem 1 above and $\alpha \geq 0$ is chosen to make the energy per bit to equal $\mathcal{E}_b$.

(a) With n denoting the dimension of the c_i's, express n, m and α in terms of r and $\mathcal{E}_b$.

Suppose the codewords above are used to communicate over the channel in Problem 2. Let s denote the channel state and $\bar{s}$ denote the 'other' state (i.e., $\bar{s} = 3 - s$).

(b) Fix a threshold t. Show that, conditional on i being the transmitted message, the probability of error of the second decoding rule that uses the threshold t is upper bounded by

$$\Pr\big(\text{score}(i, Y, s) \leq t\big) + \sum_{i' \neq i} \sum_{s' \in \{1,2\}} \Pr\big(\text{score}(i', Y, s') > t\big).$$

(c) Let $\beta = \frac{1}{2}\alpha(g+1)n$. Show that, conditional on i being the transmitted message, with s being the channel state,

$$\text{score}(i, Y, s) \sim \mathcal{N}(\beta, \sigma^2\beta).$$

(d) Conditional on i being the transmitted message, with s being the channel state, show that

(i) there is one value of $i' \neq i$ for which

$$\text{score}(i', Y, s) \sim \mathcal{N}(-\beta, \sigma^2\beta) \quad \text{and} \quad \text{score}(i', Y, \bar{s}) \sim \mathcal{N}(-\alpha\sqrt{g}n, \sigma^2\beta);$$

(ii) for the remaining $m-2$ values of $i' \neq i$,

$$\text{score}(i', Y, s) \sim \mathcal{N}(0, \sigma^2\beta) \quad \text{and} \quad \text{score}(i', Y, \bar{s}) \sim \mathcal{N}(0, \sigma^2\beta).$$

Hint: Use 1(c).

(e) For a threshold $t \geq 0$, show that the error probability of the second decoding rule is upper bounded by

$$Q\left(\frac{\beta - t}{\sqrt{\sigma^2\beta}}\right) + (2m-2)Q\left(\frac{t}{\sqrt{\sigma^2\beta}}\right).$$

Hint: Use (b), (c) and (d) and the fact that $Q(\cdot)$ is a decreasing function.

(f) Fix $0 < \epsilon < 1$ and set $t = (1-\epsilon)\beta$. Show that the error probability of the second decoding rule is upper bounded by

$$Q\left(\epsilon\sqrt{\beta/\sigma^2}\right) + (2m-2)Q\left((1-\epsilon)\sqrt{\beta/\sigma^2}\right).$$

(g) Show that as r grows, the first term above approaches zero, and if $(1+g)(1-\epsilon)^2\mathcal{E}_b > \sigma^2 4\ln 2$, the third term approaches zero too.
Hint: For the last claim, use the fact that for $x \geq 0$, $Q(x) \leq \frac{1}{2}\exp(-x^2/2)$.

(h) Conclude that if $\mathcal{E}_b/\sigma^2 > (4\ln 2)/(1+g)$, the error probability of the first decoding rule approaches zero as r grows.