Problem 1.

(a) Length $= rN$; as long as $r<1$, w.h.p. $\dim(C) = kK$ for $n \to \infty$.

(b) Let $y = (y_1, \dots, y_N)$, where $y_i \in \mathbb{F}_2^n$ is the i^{th} column of y.

Since $P(uG_i = y_i) = \left(\frac{1}{2}\right)^n$ for every i with $y_i \neq 0$, by independence

$$P(uG = y) = 2^{-nw}.$$

(c) Obvious from the definition.

(d)
$$EA_m(w) \leq \binom{nw}{m} 2^{-nw} \binom{N}{w} 2^{k(w-D+1)} \qquad \left(\text{using } \binom{n}{\alpha n} \leq 2^{nh(\alpha)}\right)$$

$$= 2^{Nn\left(\omega(r-1) + \omega h\left(\frac{\mu}{\omega}\right) - r(1-R)\right)(1+o(1))}$$

(e) The unconstrained maximum of 'this expression' on ω is attained for $\omega_0 = \frac{\mu}{1-2^{r-1}}$ (using $h'(x) = \log_2 \frac{1-x}{x}$). We obtain:

$$EA_{\mu nN} \leq 2^{nNF}, \text{ where}$$

$$F = \begin{cases} R(C) - 1 + h(\mu) & \text{if } \mu \geq 1 - 2^{r-1} \\ R(C) - \mu \log\left(2^{1-r} - 1\right) - r & \text{if } 0 < \mu < 1 - 2^{r-1} \end{cases}$$

(f). The first case above corresponds to the GV bound: indeed, using Markov's inequality, we find that

$$EA_{\mu nN} < 1 \quad \text{if} \quad R(C) < 1 - h(\mu)$$

i.e., there exists a code with no codewords of weight $\leq \mu nN$ which means that it attains the GV bound.

The condition for attainment of the GV bound is

$$1 - 2^{r-1} \leq \mu = \delta_{GV}(R(C)), \quad \text{where } \delta_{GV}(z) = h^{-1}(1-z).$$

This is the same as $R(C) \leq 1 - h(1 - 2^{r-1})$

Finally, let us show that for any $0<R<1$ it is possible to find the value of r such that $h(1-2^{r-1}) \leq 1-R$, i.e. that for any $R \in (0,1)$ concatenated codes attain the GV bound.

For any $0<R<1$ this equation has a unique solution for r. In more detail,

$$\Leftrightarrow \quad 1-2^{r-1} \leq h^{-1}(1-R) \quad \text{where } h^{-1}: [0,1] \to [0,\tfrac{1}{2}]$$

$$\Leftrightarrow \quad 2^{r-1} \geq 1-\delta_{GV}(R)$$

$$\Leftrightarrow \quad r \geq \log_2 2(1-\delta_{GV}(R))$$

Since $\delta_{GV}(R) \in (0, \tfrac{1}{2})$, the R.H.S. here is between 0 and 1, and we are done.

Note that the codewords of (relative) weight $\delta_{GV}(R)$ are obtained for $w_0 = 1$, i.e., from RS codewords of weight $Nw_0 = N$.

Problem 2 (assuming $p<\tfrac{1}{2}$)

1. Let C be an $[n,k]$ linear binary code. Consider the set $\mathcal{Z} = \mathbb{F}_2^n / C$ of cosets of C in $\mathbb{F}_2^n$. Let H be an $(n-k)\times n$ parity-check matrix of C.

Let $Z \in \mathcal{Z}$ be a coset, then for any $y_1, y_2 \in Z$ we have

$$Hy_1^T = Hy_2^T \quad \text{because } (y_1 - y_2) \in C.$$

Thus we can label the cosets with syndrome vectors $s = Hz$, where $z \in Z$ is any vector in the coset.

2. Given a coset Z_s with syndrome s, let $z(s)$ be a vector in Z_s of the lowest Hamming weight among the vectors i

2a. Consider a coset $Z_s = (z(s) \ldots)$, where the vectors in Z_s are noise vectors in $BSC(p)$; then

$$P_{Bern^n(p)}(z(s)) \geq P_{Bern^n(p)}(y) \qquad \forall y \in Z_s$$

Thus the maximum likelihood decoder $Dec(C)$ can be defined as

$$\mathrm{Dec}(C): \mathbb{F}_2^n \to C$$
$$y \mapsto c = y - z(s), \text{ where } y \in Z_s$$

2b. For a Bernoulli(p) source define a compression procedure

$$S: \mathbb{F}_2^n \to \mathbb{F}_2^{n-k}$$
$$y \mapsto s = Hy^T$$

where H is the above parity-check matrix.

The inverse (decompression) mapping U is given by $U(s) = z(s)$.

3. Let $P_e(C)$ be the probability of error

$$P_e(C) := P(\mathrm{Dec}(y) \neq 0 \mid \text{transmitted } 0)$$

*) $P_e(C)$ does not depend on the transmitted vector

Let $P_U(s) = P(U(s) \neq y \mid \text{source output} = y)$
$$= P(\text{source output} \neq z(s))$$

It is rather clear that $P_e(C) < \varepsilon$ iff $P_U(s) < \varepsilon$ because the two events coincide.

({typical errors} = {typical source outputs})

4. Suppose there is a sequence of linear codes $C_i\,[n_i, k_i]$, $i = 1, 2, \dots$ s.t. $\frac{k_i}{n_i} \to 1 - h(p)$ and $P_e(C_i) \xrightarrow[i\to\infty]{} 0$.

The number of distict syndromes is $2^{n_i - k_i}$, so the compression rate is $\frac{n_i - k_i}{n_i} \to h(p)$. Together with Part 3. this completes our argument.

Problem 3.

(a) Consider the parity-check matrix of the code:

$$H=\begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 & \beta^9 \\ 1 & \beta^2 & \beta^{2\cdot 2} & \beta^{3\cdot 2} & \beta^{4\cdot 2} & \beta^{5\cdot 2} & \beta^{6\cdot 2} & \beta^{7\cdot 2} & \beta^{8\cdot 2} & \beta^{9\cdot 2} \\ 1 & \beta^3 & \beta^{2\cdot 3} & \beta^{3\cdot 3} & \beta^{4\cdot 3} & \beta^{5\cdot 3} & \beta^{6\cdot 3} & \beta^{7\cdot 3} & \beta^{8\cdot 3} & \beta^{9\cdot 3} \end{bmatrix}$$

Suppose that coordinates x_{j_1} and x_{j_2} of the transmitted vector $(x_0\, x_1 \cdots x_9)$ are transposed

We know that $\sum_{j=0}^{n} x_j \beta^{ij} = 0, \quad i=1,2,3$

Thus $S_1 = \sum_{j\neq i_1,i_2} x_j\beta^j + x_{j_2}\beta^{j_1} + x_{j_1}\beta^{j_2} = \beta^{j_1}(x_{j_2}-x_{j_1}) + \beta^{j_2}(x_{j_1}-x_{j_2}), \quad j_1\neq j_2$

$$= (\beta^{j_1}-\beta^{j_2})(x_{j_2}-x_{j_1})$$

$$S_2 = (\beta^{2j_1}-\beta^{2j_2})(x_{j_2}-x_{j_1})$$

$$S_3 = (\beta^{3j_1}-\beta^{3j_2})(x_{j_2}-x_{j_1})$$

So

$$\frac{S_2}{S_1} = \beta^{j_1}+\beta^{j_2}$$

$$\frac{S_3}{S_1} = \beta^{2j_1}+\beta^{j_1+j_2}+\beta^{2j_2}$$

Call $\beta^{j_1}=X$; $\beta^{j_2}=Y$; $\frac{S_2}{S_1}=A$; $\frac{S_3}{S_1}=B$

We have $\left.\begin{array}{l} X+Y=A \\ X^2+XY+Y^2=B \end{array}\right\} \Rightarrow Y^2-AY+(A^2-B)=0 \quad (*)$

If X and Y come from a single transposition error (as described), then Eq. (*) has 2 roots in $\mathbb{F}_{11}$; they are the locations of the transposed coordinates. Note: Generally a quadratic equation doesn't always have roots in $\mathbb{F}_q$; so if (*) does not, this means that in addition to the transposition there were other errors.

(b) The above procedure works for any $[q-1, q-4]$ RS code. If the dimension $k < n-3$, then the distance $d \geq 5$, and the code corrects arbitrary 2 errors.

Problem 4. You could do one of the following things:

compute $Z(W_i)$, $i = 1, \dots, 64$ from the definition

or compute directly the capacity of the virtual channels $I(W_i)$

and choose 22 channels with the smallest Z or the largest I.

It is not an optimal idea to run simulations of the virtual channels and it is simply incorrect to apply the BEC expressions for $I(W_i)$ for the case of the BSC.

The RM(6,2) code has dimension 22, and its basis vectors are the rows in $H_2^{\otimes 6}$ with the largest Hamming weights.

This subset of rows does not coincide with the set of rows chosen by the polar code.