CMSC818K/ENEE729A. Home assignment 3. **Instructor: A. Barg**

Date due November 29, 8:00pm.

Please submit your work as a **single PDF file** to ELMS/Canvas under the Assignments tab

- Papers submitted as multiple pictures of individual pages are difficult for grading and **will not be accepted**.
- Justification of solutions is required.
- Each problem is worth 10 points. A subset of problems will be graded.

Problem 1. In this problem you will prove that random concatenated codes of rate $R(C) \in (0,1)$ attain the GV bound.

Consider the ensemble $\mathcal{A}$ of binary concatenated codes with an outer $RS[N,K,D]$ Reed-Solomon code over $\mathbb{F}_{2^k}$ and $[n, k=rn]$ linear inner codes $B_i, i=1,\dots,N$ chosen independently from the generator matrix ensemble (HW2). Let $G=(G_1,\dots,G_N)$ be the N-tuple of the inner codes' generator matrices of dimension $k\times n$. Let $C\in\mathcal{A}$ be a concatenated code from this ensemble.

(a) Argue that $P(\dim(C)=kK)\to 1$ as $n\to\infty$.

(b) Given an RS codeword u, we map each symbol $u_i\in\mathbb{F}_{2^k}$ to a binary k-vector and multiply this vector by G_i to obtain a codeword of the inner code $B_i, i=1,\dots,N$. This results in a codeword of the code C, and we use a shorthand notation uG for this operation. Let u be an RS codeword of weight w. Show that for any vector $y\in\mathbb{F}_2^{nN}$ with w nonzero columns

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

(c) Let u be an RS codeword, $\mathrm{wt}(u)=w\ge D$, and consider the vectors of the code C of the form uG. Prove that the expected number $EA_m(w)$ of vectors of weight $m=\mu n$ among them is bounded above as

$$EA_m(w)=\binom{nw}{m}2^{-nw}B_w^{(\mathrm{RS})}$$

where $B_w^{(\mathrm{RS})}$ is the number of vectors of weight w in the RS code.

(d) Let $m=\mu\cdot nN$ and $w=\omega N$. Prove that

$$EA_m(w)\le 2^{Nn[\omega(r-1)+\omega h(\mu/\omega)-r(1-R)](1+o(1))}, \tag{1}$$

where $h(\cdot)$ is the binary entropy function (use the fact that $B_w^{(\mathrm{RS})}\le\binom{N}{w}2^{k(w-D+1)}$ for $w\ge D$).

(e) Which value ω_0 gives the maximum on ω in (1)? Using the computed value of ω_0, find the exponent of the expression for $EA_{\mu nN}(C)$. Note that our optimization is constrained by the condition $\omega_0\le 1$, and this gives rise to two cases depending on the relation between μ and r.

(f) Wrap up the argument, showing that the ensemble of concatenated codes contains codes that attain the GV bound for all rates $R(C)\in(0,1)$. The sufficient condition for this will come out to be $R(C)\le 1-h(1-2^{r-1})$; argue that for any $0<R(C)<1$ there exists the value of r that satisfies this condition.

You will also note that the vectors of minimum weight in the concatenated codes are obtained from RS codewords of weight N (and not of weight D as could be our first guess).

Problem 2. In Lecture 20 we argued that a linear code that achieves capacity of a BSC(p) is equivalent to a procedure of compressing a memoryless Bernoulli source $X(p)$ to the rate $h(p)$. Provide a detailed proof of the equivalence, formalizing the intuition given in the lecture (see notes for Lec. 20 (`ECC Lec.20.pdf`) on Canvas).

Problem 3. (a) Let β be a primitive element of $\mathbb{F}_{11}$ and let $\Omega=\{\beta^i, i=0,\dots,9\}$ be the set of nonzero elements of the field. Consider the $[10,7]$ RS code with evaluation points given by Ω (in this order). A

transposition error in a codeword $x = (x_1, x_2, \ldots, x_{10})$ occurs when exactly one pair of coordinates gets interchanged, e.g.,

$$(x_1, x_2, x_3, x_4, \ldots, x_{10}) \longrightarrow (x_3, x_2, x_1, x_4, \ldots, x_{10}).$$

Prove that the RS code defined above corrects any one transposition error (hint: consider the parity-check equations; write the values of the syndromes in terms of the locations of the transpositions; argue that the locations can be found from these equations).

(b) Does the claim in (a) generalize? Given an RS code of length $n = q - 1$, what are the sufficient conditions for the code to correct a single transposition error?

Problem 4. (a) Write a program to construct a binary polar code of length $N = 64$ and dimension $K = 22$ for the BSC(0.11) channel. As your answer please identify which rows of the matrix $H_2^{\otimes 6}$ you will use to transmit the information, with a justification.

(b) What are the parameters of the RM(6,2) binary Reed-Muller code? Which rows out of the matrix $H_2^{\otimes 6}$ does it use to transmit the information? How does your answer in this part compare with the answer in part (a) of this problem?