Blocklength Scaling of Polar Codes

David Burshtein
Based on joint work with Dina Goldin

School of Electrical Engineering
Tel Aviv University

February 2015

Problem Definition

- $W(\cdot \mid \cdot)$ – DMC.
- $C = I(W)$ – symmetric capacity.
- Goal: Communicate at rate R with error probability $P_e \leq P_e^0$.
- Capacity achieving family of codes: For any $R < C$, can find code with rate R and blocklength N, such that $P_e \leq P_e^0$.
- How does N scale with respect to $C - R$?
- Without complexity considerations: $N = \beta/(C-R)^2$ (best possible and is achievable).
- What about finite length scaling of computationally efficient capacity achieving codes?

Blocklength Scaling of Binary Polar Codes

- Polar codes [Arikan, 2009] are capacity achieving.
- Computational complexity is $O(N \log N)$.
- Blocklength scales polynomially: $N = \frac{\beta}{(C-R)^{\mu}}$ [Guruswami and Xia, 2013], [Hassani et al., 2014]. How small can we set μ?
  - $3.55 \leq \mu \leq 6$ [Hassani et al., 2014].
  - $\mu \leq 5.7$ [Goldin and Burshtein, 2014].
  - $\mu \leq 4.7$ [Mondelli et al., 2015].
- Similar scaling of N in lossy source coding, w.r.t. $R(D) - R$ [Goldin and Burshtein, 2014] and various problems in multiuser information theory.

How can we generalize / improve results?

- General polarization kernels, or nonbinary polar codes.
- Recent result for q-ary polar codes when q is prime: N scales polynomially with respect to $\frac{1}{C-R}$: $N = \frac{\beta}{(C-R)^{\mu}}$ [Guruswami and Velingker, 2014].
- However, in the proof, μ is very large. Can we do better?
- We show that for $q = 3$ much lower values of μ can be obtained [Goldin and Burshtein, 2015].
- The technique can be applied to other values of prime q.

Polarization

Proposed in [Arikan, 2009]

- Blocklength $N = 2^n$
- *Generator matrix* G_N, size $N \times N$
- Message vector $\mathbf{u} = u_1^N$, $\mathbf{x} = x_1^N = \mathbf{u}G_N$
- B-DMC channel $W : \mathcal{X} \to \mathcal{Y}$, $\mathcal{X} = \{0, 1\}$
- Channel output $\mathbf{y} = y_1^N$
- Probability distribution: $P(\mathbf{u}, \mathbf{x}, \mathbf{y}) = \frac{1}{2^N} \mathbb{1}_{\{\mathbf{x}=\mathbf{u}G_N\}} \prod_{i=1}^N W(y_i \mid x_i)$
- For $i = 1, 2, \ldots, N$, define the N sub-channels

$$W_N^{(i)}(\mathbf{y}, u_1^{i-1} \mid u_i) \triangleq P(\mathbf{y}, u_1^{i-1} \mid u_i) = \frac{1}{2^{N-1}} \sum_{u_{i+1}^N} P(\mathbf{y} \mid \mathbf{u})$$

- *Polarization*: Typically, either $I(W_N^{(i)}) \approx 1$ or $I(W_N^{(i)}) \approx 0$.

Polar codes, Encoding

- Code rate $R < I(W)$.
- Let $Z(W) \triangleq \sum_{y\in\mathcal{Y}} \sqrt{W(y \mid 0)W(y \mid 1)}$.
- The frozen set F is the set of $N(1-R)$ sub-channels with highest $Z(W_N^{(i)})$.

Algorithm (Encoding)

- If $i \in F$, fix to frozen $\mathbf{u}_F$.
- If $i \in F^c$ use it for information.
- Transmit $\mathbf{x} = \mathbf{u}G_N$.

Polar codes, Decoding

Algorithm (Decoding)

For $i = 1, 2, \ldots, N$:

1. If $i \in F$, $\hat{u}_i = u_i$
2. If $i \in F^c$, $\hat{u}_i = \begin{cases} 0 & \text{if } L_N^{(i)} > 1 \\ 1 & \text{if } L_N^{(i)} \le 1 \end{cases}$ where $L_N^{(i)} = \frac{W_N^{(i)}(\mathbf{y}, \hat{u}_1^{i-1} \mid u_i = 0)}{W_N^{(i)}\left(\mathbf{y}, \hat{u}_1^{i-1} \mid u_i = 1\right)}$

- For $R < I(W)$, error probability, P_e, satisfies [Arikan and Telatar, 2009]:

$$P_e = O\left(2^{-N^\beta}\right) \quad , \quad \text{for any } \beta < 1/2$$

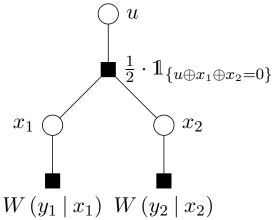
- Encoding and decoding complexity $O(N \log N)$.

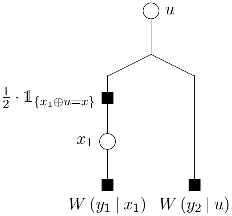
Analysis of Polarization

Sub-channels can be described using the following random process:

- $B_1, B_2 \dots$ i.i.d $\Pr\{B_n = 0\} = \Pr\{B_n = 1\} = 1/2$
- $W_0 = W$, $W_{n+1} = \begin{cases} W_n^-, & \text{if } B_{n+1} = 0 \\ W_n^+ & \text{if } B_{n+1} = 1. \end{cases}$
  - $W^-(y_1, y_2 \mid u) \triangleq (W \boxast W)(y_1, y_2 \mid u) \triangleq \frac{1}{2} \sum_x W(y_1 \mid u \oplus x) W(y_2 \mid x)$
  - $W^+(y_1, y_2, x \mid u) \triangleq (W \circledast W)(y_1, y_2, x \mid u) \triangleq \frac{1}{2} W(y_1 \mid x \oplus u) W(y_2 \mid u)$

$W^-(y_1, y_2 \mid u)$ $\qquad$ $W^+(y_1, y_2, x \mid u)$





Analysis of Polarization (CONT'D)

- W_n uniformly distributed over $\left\{ W_N^{(i)} \right\}_{i=1}^{N}$.
- Hence, for $Z_n = Z(W_n)$, $I_n = I(W_n)$,

$$P\left[Z_n \in (a,b)\right] = \left| \left\{ i \; : \; Z\left(W_N^{(i)}\right) \in (a,b) \right\} \right| / \; N$$

$$P\left[I_n \in (a,b)\right] = \left| \left\{ i \; : \; I\left(W_N^{(i)}\right) \in (a,b) \right\} \right| / \; N$$

- It was shown [Arikan, 2009], for any fixed small $\delta > 0$,
  - $\lim_{n\to\infty} \Pr\left(Z_n \le \delta\right) = I(W)$
  - $\lim_{n\to\infty} \Pr\left(Z_n \ge 1-\delta\right) = 1 - I(W)$
  - $\lim_{n\to\infty} \Pr\left(I_n \le \delta\right) = 1 - I(W)$
  - $\lim_{n\to\infty} \Pr\left(I_n \ge 1-\delta\right) = I(W)$

How can finite length scaling be derived?

Following [Hassani et al., 2014] and the variations in [Goldin and Burshtein, 2014]:

- It is known that

$$Z(W^+) = Z^2(W)$$
$$Z(W)\sqrt{2 - Z^2(W)} \le Z(W^-) \le 2Z(W) - Z^2(W)$$

- For some $f_0(z) > 0$, $z \in (0,1)$, $f_0(0) = f_0(1) = 0$, define $f_k(z)$ recursively:

$$f_k(z) \triangleq \sup_{y \in \left[z\sqrt{2-z^2}, z(2-z)\right]} \frac{f_{k-1}\left(z^2\right) + f_{k-1}(y)}{2}$$

- Also define $L_k(z) \triangleq f_k(z)/f_0(z)$, $L_k \triangleq \sup_{z\in(0,1)} L_k(z)$.
- It can be shown that $\mathrm{E}[f_0(Z_n)] \le A \cdot \left(\sqrt[k]{L_k}\right)^n \cdot f_0\left[Z(W)\right]$ for constant A.

How can finite length scaling be shown? (CONT'D)

- Using appropriately chosen $f_0(z)$ it can now be shown:

$$P\left(Z_n \in (\delta, 1-\delta)\right) \leq \frac{A}{\delta}\left(\sqrt[k]{L_k}\right)^n \leq \frac{A}{\delta}2^{-\rho n}$$

  for constant A and $\rho = 0.2127$.

- Proceed by showing, given m_0, for constant $\tilde{A}$, that

$$P\left(\omega \in \Omega \,:\, Z_n(\omega) \notin (\delta, 1-\delta)\, \forall n \geq m_0\right) \geq 1 - \frac{\tilde{A}}{\delta}2^{-\rho m_0}$$

$$P\left(\omega \in \Omega \,:\, Z_n(\omega) \leq \delta \;\, \forall n \geq m_0\right) \geq I(W) - \frac{\tilde{A}}{\delta}2^{-\rho m_0}$$

How can finite length scaling be shown? (CONT'D)

- Following [Arikan, 2009] it can now be shown that for

$$R \leq I(W) - \left(1 + \frac{A}{\delta}\right) \cdot 2^{-\alpha n}$$

we have

$$P_e = O\left(N^{-a}\right)$$

where $a > 0$ for $\alpha = 1/(1 + 1/\rho) = 5.702^{-1}$.

- This proves the following scaling result:

Theorem

For $P_e \leq P_e^0$, sufficient to set $N = \beta / \left(I(W) - R\right)^{5.702}$.

Outline of analysis of q-ary polarization

- Instead of $Z(W_n)$ use $I(W_n)$.
- Given q-ary input channel W, $W^- = W \boxast W$ and $W^+ = W \circledast W$ obtain a bound
$$I(W) - I(W^-) \geq \epsilon_l\left[I(W)\right]$$
for some $\epsilon_l\left[I(W)\right]$.
- For some $f_0(x) > 0$, $x \in (0,1)$, $f_0(0) = f_0(1) = 0$, define $f_k(x)$, for $k = 1, 2, \ldots$, recursively
$$f_k(x) \triangleq \sup_{\epsilon_l(x) \leq \epsilon \leq \epsilon_h(x)} \frac{f_{k-1}(x+\epsilon) + f_{k-1}(x-\epsilon)}{2}$$
for $\epsilon_h(x) \triangleq \min(x, 1-x)$.
- The rest of the analysis is very similar to the binary case.

Outline of analysis of q-ary polarization (CONT'D)

- In particular $L_k(x) \triangleq f_k(x)/f_0(x)$, $L_k \triangleq \sup_{x\in(0,1)} L_k(x)$.
- Hence

$$
\begin{aligned}
&\mathrm{E}[f_k(I_{n+1})] \\
&= \mathrm{E}\left[\frac{f_k(I_n^+) + f_k(I_n^-)}{2}\right] \\
&\leq \mathrm{E}\left[\sup_{\epsilon_l(x)\leq\epsilon\leq\epsilon_h(x)} \frac{f_k(I_n+\epsilon) + f_k(I_n-\epsilon)}{2}\right] \\
&\leq \mathrm{E}\left[f_{k+1}(I_n)\right]
\end{aligned}
$$

- Hence $\mathrm{E}\left[f_0(I_n)\right] \leq \mathrm{E}\left[f_k(I_{n-k})\right] \leq L_k \mathrm{E}\left[f_0(I_{n-k})\right]$.
- Hence $\mathrm{E}[f_0(I_n)] \leq A \cdot \left(\sqrt[k]{L_k}\right)^n \cdot f_0\left[I(W)\right]$ for constant A.
- Rest is almost identical to the binary case when using Z_n.

The main difficulty

- In the binary case $q = 2$, a tight bound $\epsilon_l \left[I(W)\right]$ such that $I(W) - I(W^-) \geq \epsilon_l \left[I(W)\right]$ is well known, e.g. [Richardson and Urbanke, 2008].
- This is not the case for $q > 2$.
- We show how good bounds can be obtained numerically.

Our approach to obtain $\epsilon_l(x)$

- Following notation in [Karzand and Telatar, 2010], given q-ary channel $W(y|x)$

$$W(y) \triangleq (1/q) \sum_{x=0}^{q-1} W(y \mid x)$$

$$\mathbf{v}(y) \triangleq [v_0(y), v_1(y), \ldots, v_{q-1}(y)]^T$$

$$v_x(y) \triangleq \frac{W(y \mid x)}{qW(y)} \quad , \quad \sum_{x=0}^{q-1} v_x(y) = 1$$

- Then: $I(W) = \sum_y W(y) [1 - H[\mathbf{v}(y)]] = \sum_G \hat{W}(G) \cdot G$ where $\hat{W}(G) \triangleq \sum_{y \,:\, H[\mathbf{v}(y)]=1-G} W(y)$

Our approach to obtain $\epsilon_l(x)$ (CONT'D)

- Given two channels, W_a and W_b, let $W_{a\circledast b} \triangleq W_a \circledast W_b$, i.e.

$$W_{a\circledast b}\left(y_1, y_2 \mid u\right) \triangleq \frac{1}{q}\sum_{u'=0}^{q-1} W_b\left(y_2 \mid u'\right) W_a\left(y_1 \mid u+u'\right)$$

- Hence $W_{a\circledast b}\left(y_1, y_2\right) = W_a\left(y_1\right) W_b\left(y_2\right)$ and [Karzand and Telatar, 2010]

$$\mathbf{v}_{a\circledast b}\left(y_1, y_2\right) = \mathbf{v}_b\left(y_2\right) \star \mathbf{v}_a\left(y_1\right)$$

  where $\star$ denotes q-circular cross-correlation.

- Also define

$$g\left(G_1, G_2\right) \triangleq 1 - \min_{\substack{H[\mathbf{v}_a(y_1)]=1-G_1 \\ H[\mathbf{v}_b(y_2)]=1-G_2}} H\left[\mathbf{v}_b\left(y_2\right) \star \mathbf{v}_a\left(y_1\right)\right]$$

Our approach to obtain $\epsilon_l(x)$ (CONT'D)

$$
\begin{aligned}
I\left(W_{a\circledast b}\right) &= \sum_{y_1,y_2} W_{a\circledast b}\left(y_1,y_2\right)\left\{1-H\left[\mathbf{v}_{a\circledast b}\left(y_1,y_2\right)\right]\right\} \\
&\leq \sum_{G_1,G_2} \sum_{\substack{y_1:H[\mathbf{v}_a(y_1)]=1-G_1 \\ y_2:H[\mathbf{v}_b(y_2)]=1-G_2}} W_a\left(y_1\right) W_b\left(y_2\right) g\left(G_1,G_2\right) \\
&= \sum_{G_1,G_2} \hat{W}_a\left(G_1\right) \hat{W}_b\left(G_2\right) g\left(G_1,G_2\right)
\end{aligned}
$$

If $g\left(G_1,G_2\right)$ concave (separately!) in G_1, G_2 (otherwise replace by concave upper bound)

$$
I\left(W_{a\circledast b}\right) \leq g\left[\sum_{G_1} \hat{W}_a\left(G_1\right) G_1, \sum_{G_2} \hat{W}_a\left(G_2\right) G_2\right] = g\left[I\left(W_a\right), I\left(W_b\right)\right]
$$

Our approach to obtain $\epsilon_l(x)$ (CONT'D)

- In our case $W^- = W \circledast W$. Hence $I(W^-) \le g[I(W), I(W)]$.
- Hence $I(W) - I(W^-) \ge I(W) - g[I(W), I(W)] \triangleq \epsilon_l[I(W)]$.
- Recall

$$g(G_1, G_2) \triangleq 1 - \min_{\substack{H[\mathbf{v}_a(y_1)]=1-G_1 \\ H[\mathbf{v}_b(y_2)]=1-G_2}} H[\mathbf{v}_b(y_2) \star \mathbf{v}_a(y_1)]$$

- At lease for $q = 3$, a *QSC* channel provides an excellent approximation to the solution!
- A QSC with error prob. p:

$$W(y \mid x) = \begin{cases} 1-p & y = x \\ p/(q-1) & y \ne x \end{cases}.$$

Properties of $g(G_1, G_2)$

$$g\left(G_1, G_2\right) \triangleq 1 - \min_{\substack{H[\mathbf{v}_a(y_1)]=1-G_1 \\ H[\mathbf{v}_b(y_2)]=1-G_2}} H\left[\mathbf{v}_b\left(y_2\right) \star \mathbf{v}_a\left(y_1\right)\right]$$

Lemma

If W_a and W_b are QSC, then $W_{a \boxast b}$ is QSC, and $I\left(W_{a \boxast b}\right) = g_{QSC}\left[I\left(W_a\right), I\left(W_b\right)\right]$.

Lemma

Using QSC channels W_a and W_b yields extreme point in Lagrangian of definition of $g(G_1, G_2)$, $\forall G_1, G_2 > 0$.

Properties of $g(G_1, G_2)$ (CONT'D)

Lemma

$$g\left(G_1, G_2\right) = 1 - \min_{\substack{H[\mathbf{v}_a(y_1)] \geq 1-G_1 \\ H[\mathbf{v}_b(y_2)] \geq 1-G_2}} H\left[\mathbf{v}_b\left(y_2\right) \star \mathbf{v}_a\left(y_1\right)\right]$$

Lemma

Define $f\left(\mathbf{u}\right) \triangleq \min_{H(\mathbf{v}) \geq 1-G} H\left(\mathbf{u} \star \mathbf{v}\right)$. *Then,* $f\left(\mathbf{u}\right)$ *is concave.*

$g(G_1, G_2)$ can be computed efficiently using algorithms for concave minimization over convex region.

Properties of $g(G_1, G_2)$ (CONT'D)

Lemma

1. $g(G_1, G_2) = g(G_2, G_1)$
2. $g(x_1, y_1) \leq g(x_2, y_2)$ *for* $x_1 \leq x_2$ *and* $y_1 \leq y_2$.
3. $g(1, G_2) = G_2$
4. $g(G_1, G_2) \leq \min(G_1, G_2)$.
5. $\lim_{x \to 1} \frac{\partial g(x, G_2)}{\partial x} = 0$

Lemma

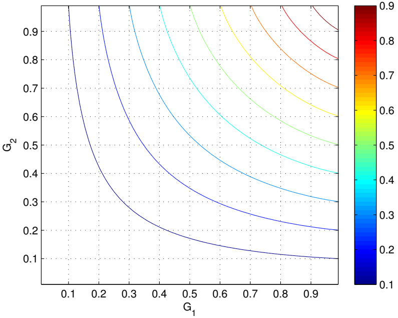
For sufficiently small G_1, G_2 *and* $q = 3$, $g(G_1, G_2) = \ln 3 \cdot G_1 G_2$.

Lemma

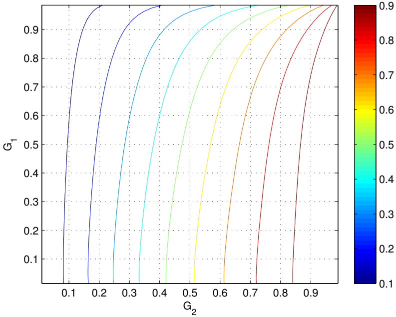
For G_1, G_2 *sufficiently close to* 1, *and* $q = 3$, $g(G_1, G_2) = G_1 + G_2 - 1$

Numerical Results

$g\left(G_1, G_2\right)$ for $q = 3$

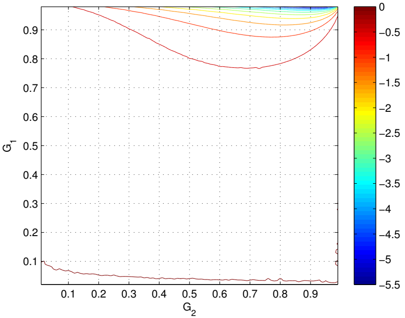


$\frac{\partial g(G_1, G_2)}{\partial G_1}$ for $q = 3$



Numerical Results (CONT'D)

$\frac{\partial^2 g(G_1,G_2)}{\partial G_1^2}$ for $q = 3$



We can find a concave upper bound on $g(G_1, G_2)$.

A concave upper bound on $g(G_1, G_2)$

- For a given G_2, concave hull of $g(G_1, G_2)$ is obtained by passing a tangent line:

$$\max_{x \in [G_1, 1]} \frac{G_1}{x} g(x, G_2)$$

- In order to obtain upper bound on $g(G_1, G_2)$, concave in G_1 and G_2 (separately):

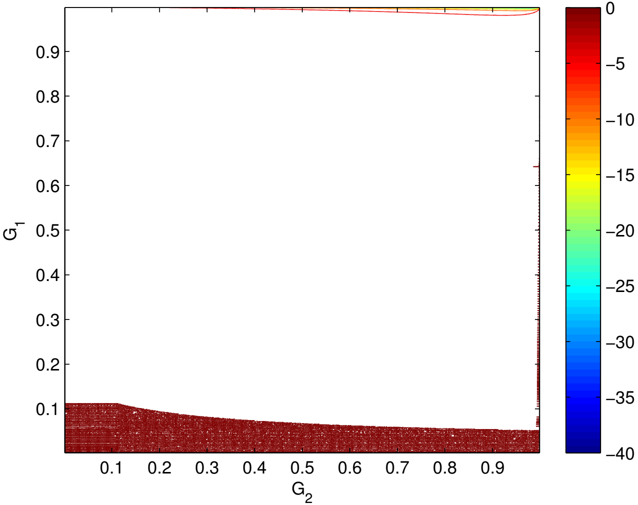
$$g^*(G_1, G_2) = \max_{x_1 \in [G_1, 1], x_2 \in [G_2, 1]} \frac{G_1 G_2}{x_1 x_2} g(x_1, x_2)$$

- We can also obtain closed form concave upper bound on $g(G_1, G_2)$ given by

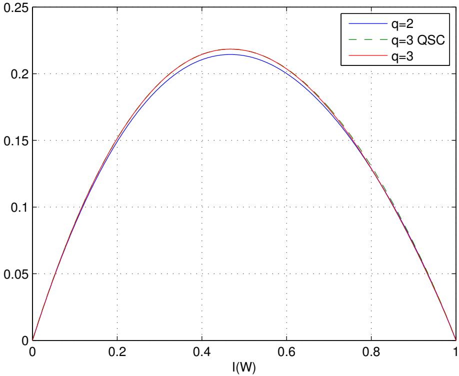
$$g^*_{QSC}(G_1, G_2) + 0.0104[G_1(1 - G_2) + G_2(1 - G_1)]$$

  However this solution produces a slightly worse bound on the scaling.

$\frac{\partial^2 g^*_{QSC}(G_1,G_2)}{\partial G_1^2}$ for $q = 3$



Lower bound on $I(W) - I(W^-)$



Using this bound (with $g^*(G_1, G_2)$), can be shown that scaling of N is $N = \frac{\beta}{(I(W)-R)^{6.504}}$ (or better), $\beta = \beta(P_e^0)$.

Conclusion

- The blocklength of polar codes scales polynomially with respect to the inverse gap between code rate and capacity.
- For binary and ternary polar codes this polynomial has low degree.
- The numerical technique presented may also work for other nonbinary polar codes.
- May be interesting to examine the dependence of the scaling parameter in the bound w.r.t. the alphabet size (q). Does it decrease w.r.t. q?

References I

Arikan, E. (2009).
Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels.
IEEE Transactions on Information Theory, 55(7):3051–3073.

Arikan, E. and Telatar, E. (2009).
On the rate of channel polarization.
In *Proc. IEEE International Symposium on Information Theory (ISIT)*, pages 1493–1495, Seoul, Korea.

Goldin, D. and Burshtein, D. (2014).
Improved bounds on the finite length scaling of polar codes.
IEEE Transactions on Information Theory, 60(11):6966–6978.

Goldin, D. and Burshtein, D. (2015).
On the finite length scaling of ternary polar codes.
In *Proc. IEEE International Symposium on Information Theory (ISIT)*.
submitted for presentation.

References II

Guruswami, V. and Velingker, A. (2014).
An entropy sumset inequality and polynomially fast convergence to Shannon capacity over all alphabets.
arXiv preprint arXiv:1411.6993.

Guruswami, V. and Xia, P. (2013).
Polar codes: speed of polarization and polynomial gap to capacity.
In *IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 310–319.

Hassani, S., Alishahi, K., and Urbanke, R. (2014).
Finite-length scaling for polar codes.
IEEE Transactions on Information Theory, 60(10):5875–5898.

Karzand, M. and Telatar, E. (2010).
Polar codes for q-ary source coding.
In *Proc. IEEE International Symposium on Information Theory (ISIT)*, pages 909–912, Austin, Texas.

References III

Mondelli, M., Hassani, S. H., and Urbanke, R. (2015).
Unified scaling of polar codes: error exponent, scaling exponent, moderate deviations, and error floors.
arXiv preprint arXiv:1501.02444.

Richardson, T. and Urbanke, R. (2008).
Modern Coding Theory.
Cambridge University Press, Cambridge, UK.