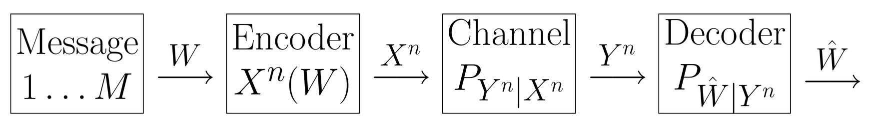
Finite Blocklength Results in Channel Coding

Yury Polyanskiy, H. Vincent Poor and Sergio Verdú

Princeton University, USA

Introduction



- **Object of study:** An (n, M, ϵ)-code is a block code satisfying

$$\mathbb{P}[\hat{W} \neq W] \leq \epsilon$$

- **Fundamental limit:**

$$M^*(n, \epsilon) = \max\{M : \exists (n, M, \epsilon)\text{-code}\}$$

- **Problem:** $M^*(n, \epsilon)$ is impossible to compute exactly even for $n \sim 10$.
- **Solution:** In [PPV08] it was discovered that for various channels, e.g. discrete memoryless (DMC) and additive white Gaussian noise (AWGN), the following expansion [VS64] is notably tight for n, ϵ of interest:

$$\log M^*(n, \epsilon) = nC - \sqrt{nV} Q^{-1}(\epsilon) + O(\log n)\,, \qquad (1)$$

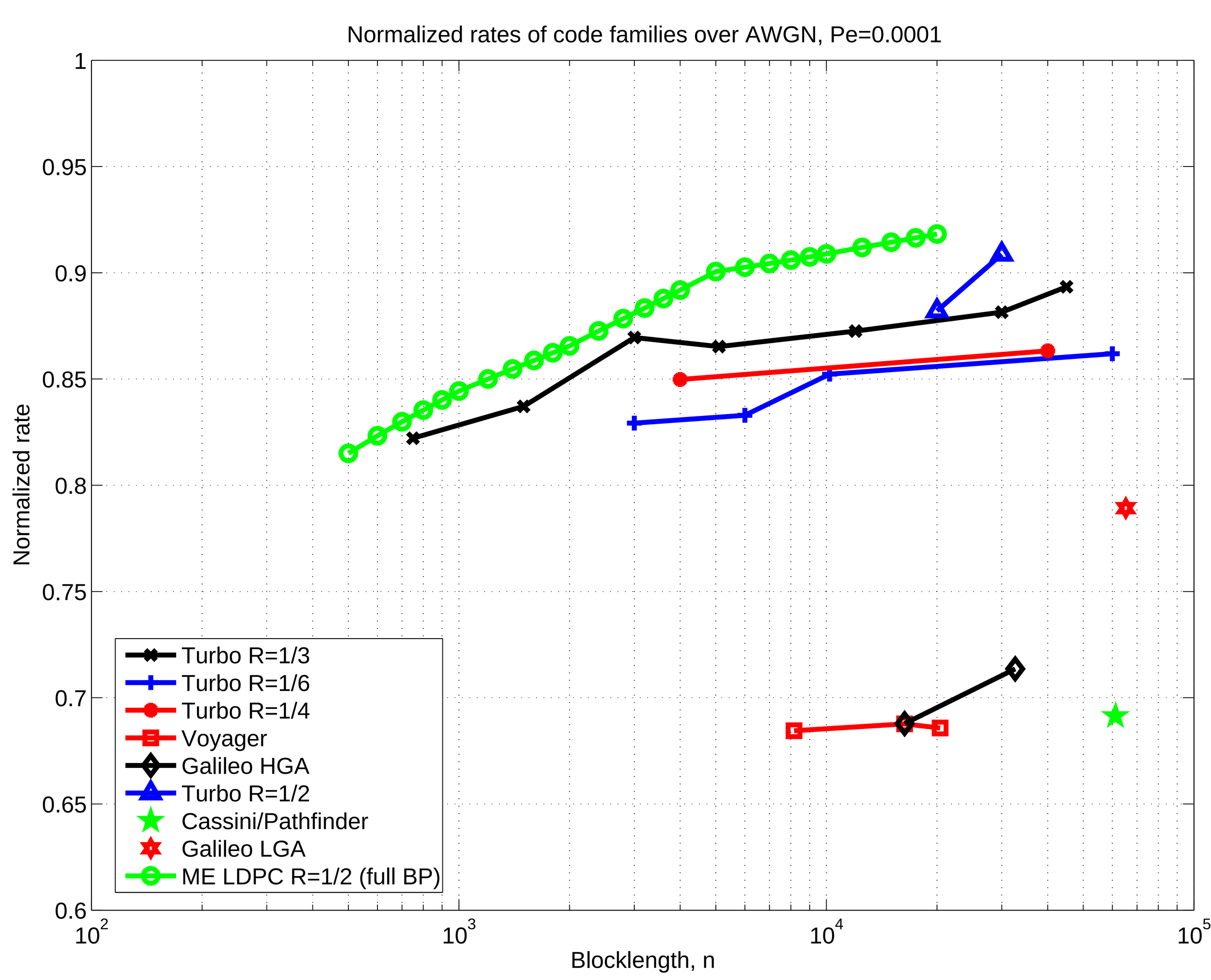
where the **channel capacity** C and **channel dispersion** V are

$$C = \lim_{\epsilon \to 0} \liminf_{n \to \infty} \frac{1}{n} \log M^*(n, \epsilon)\,, \qquad V = \lim_{\epsilon \to 0} \limsup_{n \to \infty} \frac{1}{n} \frac{(nC - \log M^*(n, \epsilon))^2}{2 \ln \frac{1}{\epsilon}}\,.$$

- **Importance:** Many practical questions regarding $M^*(n, \epsilon)$ can be answered by only knowing a pair of numbers: (C, V). For example, according to (1) the minimal blocklength needed to achieve a fraction η of capacity is:

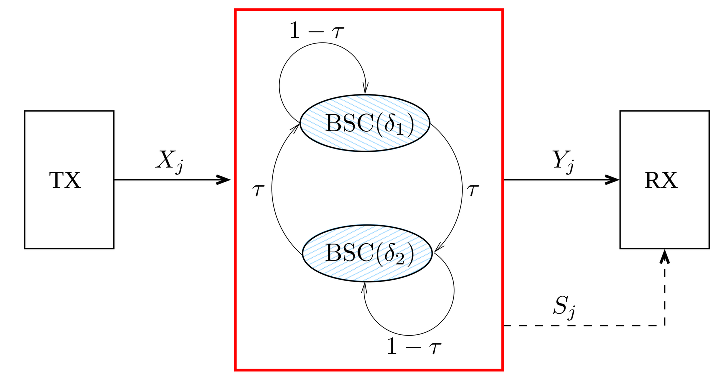
$$n \gtrsim \left(\frac{Q^{-1}(\epsilon)}{1 - \eta}\right)^2 \frac{V}{C^2}\,.$$

- **Practical codes:** We can gauge the efficiency of a given k-to-n code by defining a normalized rate $R_{norm} = \frac{k}{\log M^*(n, \epsilon)}$ and use (1) to compute it. This enables a (more) fair comparison between the codes with different blocklengths and rates.



- **Note:** the ME-LDPC codes were designed and evaluated by Tom Richardson.

Gilbert-Elliott channel (GEC)



- GEC is the first channel with memory for which a finite blocklength analysis is performed. The capacity was found in [MBD89].
- GEC is a channel with dynamics and may serve as a discrete analog of a fading channel.
- GEC can be represented as a binary additive noise channel $Y_j = X_j + Z_j$, with the noise process Z_j being a hidden Markov chain.

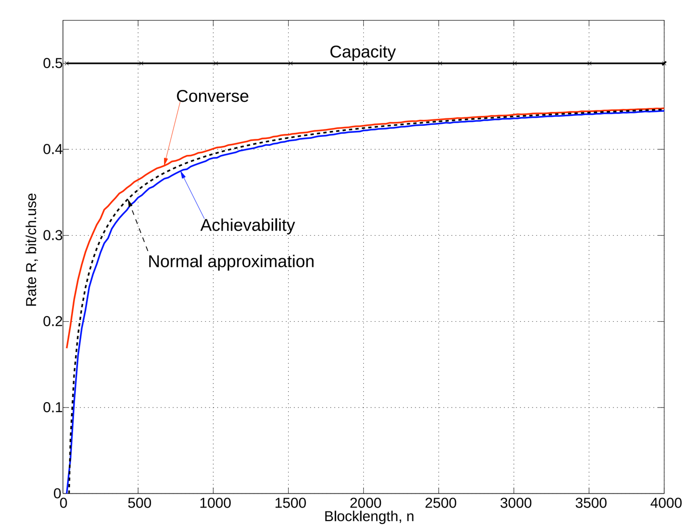
Capacity and dispersion:

S_j known at RX	S_j is not known
$C_1 = \log 2 - \frac{1}{2}[h(\delta_1) + h(\delta_2)]$	$C_0 = \log 2 - \mathbb{E}\left[h(\mathbb{P}[Z_0 = 1 \mid Z_{-\infty}^{-1})\right]$
$V_1 = \frac{V(\delta_1)+V(\delta_2)}{2} + \left(\frac{h(\delta_1)-h(\delta_2)}{2}\right)^2 \left(\frac{1}{\tau} - 1\right)$	$V_0 =$ PSD at zero of $\log P_{Z_j \mid Z_{-\infty}^{j-1}}$

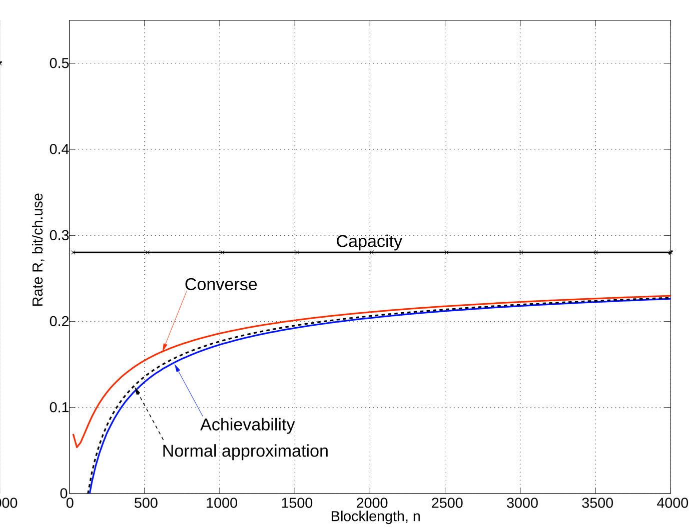
where $h(\delta) = -\delta \log \delta - (1 - \delta)\log(1 - \delta)$ and $V(\delta) = \delta(1 - \delta)\log^2 \frac{1-\delta}{\delta}$ is a dispersion of the BSC.

- **Evaluating the tightness of (1):** $\delta_1 = 1/2, \delta_2 = 0, \tau = 0.1$

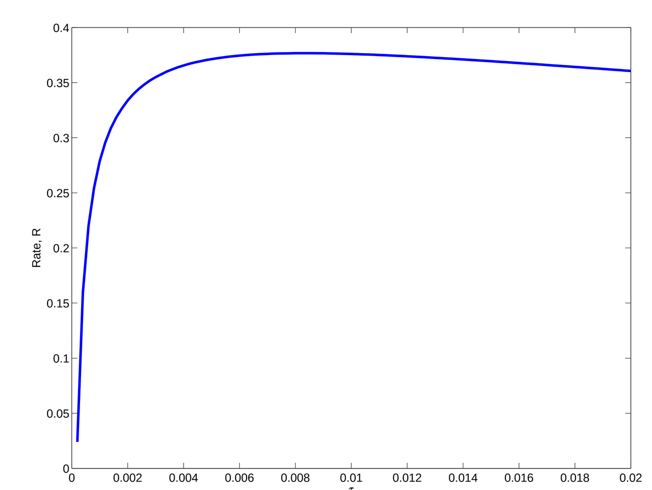
State known



State unknown



- **Observation:** In the state known case the fundamental limit $\log M^*(n, \epsilon)$ depends on the channel dynamics τ only in the dispersion term.
- **New phenomenon:** In the state unknown case, when $\tau \searrow 0$ it is known [MBD89] that $C_0(\tau) \nearrow C_1$. In reality, for a fixed n the behavior of $\frac{1}{n} \log M^*(n, \epsilon)$ is quite the opposite:



- **Slow dynamics**: When $\tau \to 0$ we know that $C_0(\tau) \to C_1$. In addition, we also have $V_0(\tau) = V_1(\tau) + o(1/\tau)$, see [PPV09].

Gaussian channels

AWGN channel

$$Z \sim \mathcal{N}(0, 1)$$
$$X \longrightarrow \bigoplus \longrightarrow Y$$

Power constraint on the codebook $\{\mathbf{c}_i\} \subset \mathbb{R}^n$ is one of the following

- *equal-power*: $||\mathbf{c}_i||^2 = nP$.
- *maximal power*: $||\mathbf{c}_i||^2 \leq nP$.
- *average power*: $\frac{1}{M} \sum ||\mathbf{c}_i||^2 \leq nP$.

Main result: regardless of the power constraint, we have that (1) holds with

$$C(P) = \frac{1}{2}\log(1 + P)$$
$$V(P) = \frac{P}{2} \frac{P + 2}{(P + 1)^2} \log^2 e\,.$$

Parallel AWGN channel

$$Z_j \sim \mathcal{N}(0, \sigma_j^2)$$
$$X_j \longrightarrow \bigoplus \longrightarrow Y_j \qquad j = 1 \ldots L$$

Main result: Given L parallel AWGN channels with noise levels $\sigma_1^2, \ldots \sigma_L^2$ and power constraint P we have that (1) holds with

$$C_L(P) = \sum_{j=1}^{L} C(W_j/\sigma_j^2)$$
$$V_L(P) = \sum_{j=1}^{L} V(W_j/\sigma_j^2)\,,$$

where W_j are water-filling powers:

$$W_j = |\lambda - \sigma_j^2|^+\,, \quad \sum_{j=1}^{L} W_j = P\,.$$

Observation: Note that L parallel codes can achieve at most

$$\log M \approx \sum_{j=1}^{L} nC(W_j/\sigma_j^2) - \sum_{j=1}^{L} \sqrt{nV(W_j/\sigma_j^2)} Q^{-1}(\epsilon) + O(\log n)\,,$$

which is suboptimal in the $\sqrt{n}$ term since $\sum_{j=1}^{L} \sqrt{V(W_j/\sigma_j^2)} > \sqrt{\sum_{j=1}^{L} V(W_j/\sigma_j^2)}$.

References

PPV08 Y. Polyanskiy, H. V. Poor and S. Verdú, "Channel coding rate in the finite blocklength regime," submitted to *IEEE Trans. Inform. Theory*, Nov. 2008.

VS64 V. Strassen, "Asymptotische Abschätzungen in Shannon's Informationstheorie," *Trans. Third Prague Conf. Information Theory*, Czechoslovak Academy of Sciences, Prague, pp. 689-723, 1962.

MBD89 M. Mushkin and I. Bar-David, "Capacity and coding for the Gilbert- Elliott channels," *IEEE Trans. Inform. Theory*, Vol. 35, No. 6, pp. 1277-1290, 1989.

PPV09 Y. Polyanskiy, H. V. Poor and S. Verdú, "Dispersion of the Gilbert-Elliott channel," submitted to *IEEE Trans. Inform. Theory*, Jun. 2009.