Capacity-Achieving Ensembles for the Binary Erasure Channel With Bounded Complexity

Henry Pfister
Qualcomm, Inc.
CA 92121, USA
hpfister@qualcomm.com

Igal Sason
Technion
Haifa 32000, Israel
Sason@ee.technion.ac.il

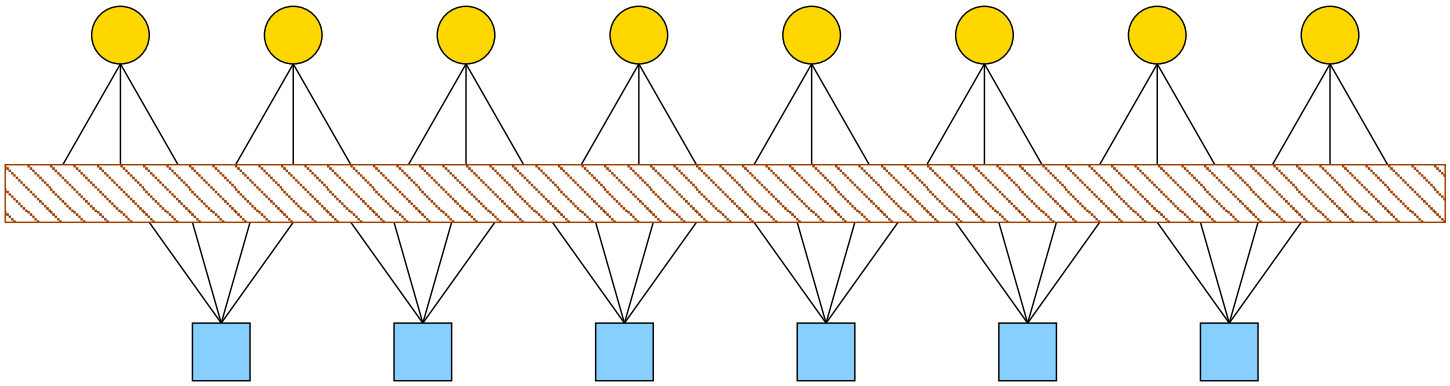
Rüdiger Urbanke
EPFL
Lausanne 1015, Switzerland
Rudiger.Urbanke@epfl.ch

ISIT 2004
Chicago, Illinois

Outline

- Background
  - Codes On Graphs
  - Capacity-Achieving Code Ensembles for the BEC
  - Irregular Repeat Accumulate (IRA) Codes
- Achieving Capacity with Bounded Complexity
  - Check-Regular Construction
  - Bit-Regular Construction
  - Puncturing Rate Versus Complexity
- Simulation Results

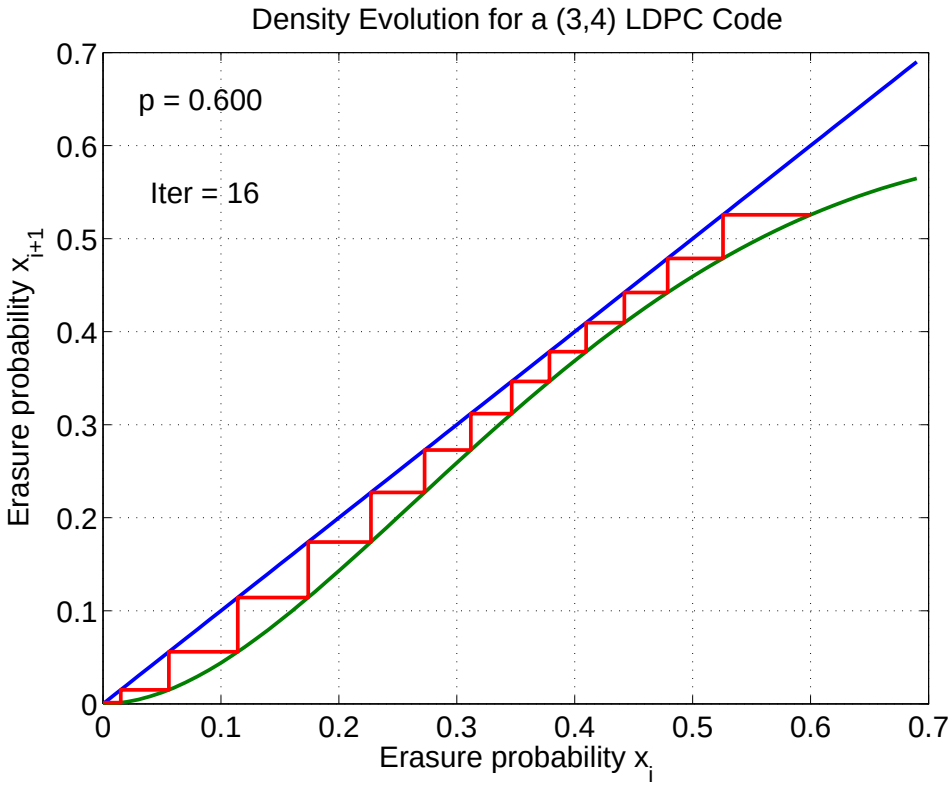
Codes On Graphs (1)



- Low Density Parity Check (LDPC) Codes
  - Message passing iterative (MPI) decoding introduced by Gallager
  - Irregular and capacity-achieving codes for the BEC introduced by Luby et al.
  - An ensemble of irregular codes is defined by the degree distribution (d.d.)
  - Let $\lambda(x) = \sum_{n \geq 2} \lambda_n x^{n-1}$ and $\rho(x) = \sum_{n \geq 2} \rho_n x^{n-1}$, where λ_n and ρ_n are the fraction of edges attached to bit and check nodes of degree n

Codes On Graphs (2)

- Density Evolution (DE)
  - Erasure prob. vs. iteration
  - $x_{i+1} = p\,\lambda\,(1 - \rho(1 - x_i))$
- Successful Decoding Rule
  - $p\,\lambda\,(1 - \rho(1 - x)) < x$
  - Can rewrite for $\lambda(\cdot)$ given $\rho(\cdot)$ as $\lambda(x) < \frac{1}{p}\left(1 - \rho^{-1}(1 - x)\right)$
- Concentration Theorem (R&U)
  - Performance of MPI decoding converges to DE analysis



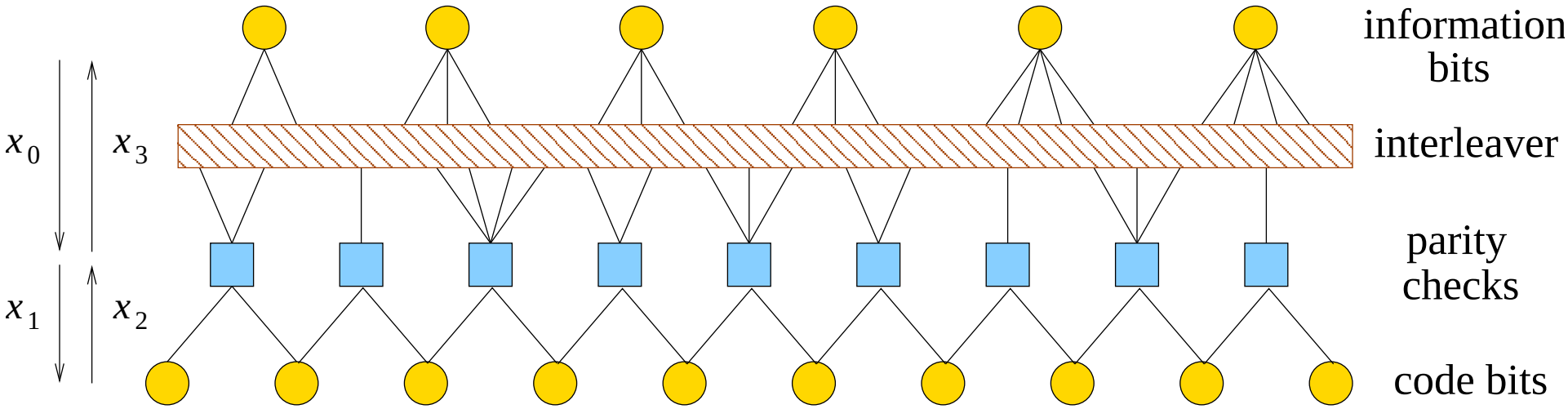
Capacity-Achieving Ensembles (1)

- Sequence of Check-Regular LDPC Codes (Shokrollahi)
  - Check d.d. is regular with degree $k+1$ and given by $\rho^{(k)}(x) = x^k$
  - Bit d.d. given by truncating $\lambda^{(k)}(x) = \frac{1}{p}\left(1-(1-x)^{1/k}\right)$ so that $\widetilde{\lambda}_k(1) = 1$
- Outline of Proof
  1. DE satisfied with equality before truncation: $p\,\lambda^{(k)}\left(1-\rho^{(k)}(1-x)\right) = x$
  2. Power series expansion of $\lambda^{(k)}(x)$ is non-negative
  3. Truncated bit d.d. $\widetilde{\lambda}^{(k)}(x)$ satisfies $\widetilde{\lambda}^{(k)}(1) = 1$ and $\widetilde{\lambda}^{(k)}(x) < \lambda^{(k)}(x)$
  4. Decoding condition satisfied: $p\,\widetilde{\lambda}^{(k)}\left(1-\rho^{(k)}(1-x)\right) < x$ for all $x \in (0,1]$
- Drawback: Achieving $(1-\varepsilon)$ of capacity requires $k \sim \ln\frac{1}{\varepsilon}$

Capacity-Achieving Ensembles (2)

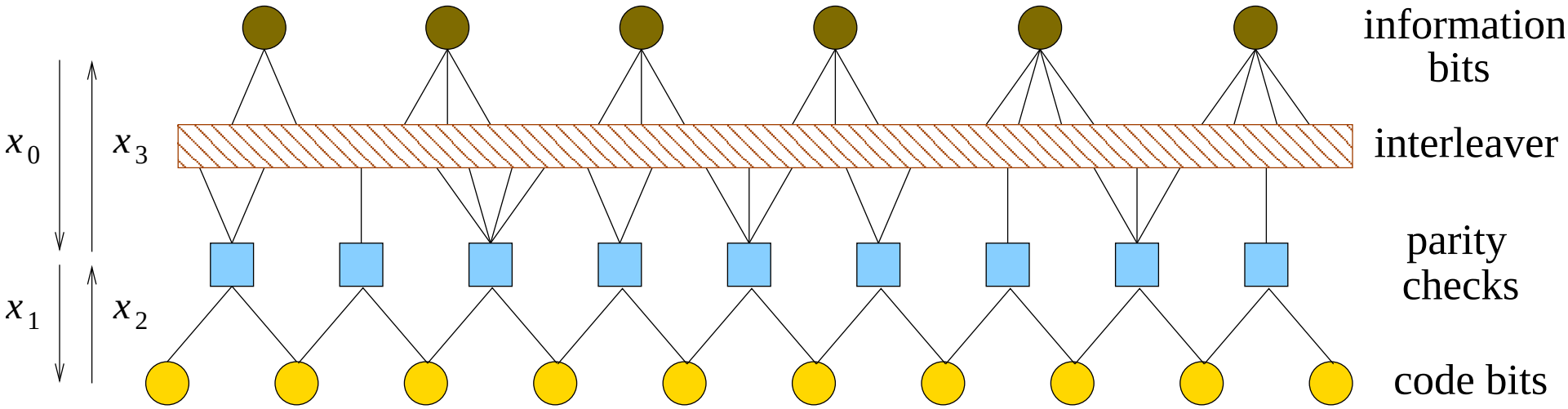
- Complexity to Achieve a Fraction $(1-\varepsilon)$ of BEC Capacity
  - MPI decoding complexity proportional to number of edges in graph
  - Shokrollahi showed number of edges $\sim \ln \frac{1}{\varepsilon}$ for LDPC codes
- Complexity for More General Channels
  - Define minimum complexity of encoding and decoding as $\chi_E(\varepsilon)$ and $\chi_D(\varepsilon)$
  - Based on analysis, Khandekar et al. conjectured: $\chi_D(\varepsilon) = O\left(\frac{1}{\varepsilon} \ln \frac{1}{\varepsilon}\right)$
  - Edges in graph proportional to parity-check matrix density
  - How sparse can the parity-check matrix be in terms of ε ?
  - Sason and Urbanke showed density must grow like $\frac{K_1 + K_2 \ln \frac{1}{\varepsilon}}{1-\varepsilon}$ for LDPC codes
  - Question: Can we get better trade-offs with other graphical models?

Systematic IRA Codes



$$
\begin{aligned}
x_1 &= 1 - (1 - x_2)\, R(1 - x_0), \\
x_2 &= p\, x_1, \\
x_3 &= 1 - (1 - x_2)^2\, \rho(1 - x_0), \\
x_0 &= p\, \lambda(x_3)
\end{aligned}
$$

Non-Systematic IRA Codes



$$
\begin{aligned}
x_1 &= 1 - (1 - x_2)\, R(1 - x_0), \\
x_2 &= p\, x_1, \\
x_3 &= 1 - (1 - x_2)^2\, \rho(1 - x_0), \\
x_0 &= \lambda(x_3)
\end{aligned}
$$

IRA Code Comparison

- Systematic IRA Codes (Jin, Khandekar, McEliece)
  - Capacity-achieving d.d. sequences with complexity $\sim \ln \frac{1}{\varepsilon}$ (S&U)
  - DE fixed point condition for $x \in (0, 1]$

$$p_0 \, \lambda\left(1 - \left[\frac{1-p}{1-pR(1-x)}\right]^2 \rho(1-x)\right) = x \quad \text{where} \quad R(x) = \frac{\int_0^x \rho(t)\, \mathrm{d}t}{\int_0^1 \rho(t)\, \mathrm{d}t}$$

  - If we assume $\rho(0) = 0$, then this implies that $\lambda(1) = 1/p_0$

- Non-Systematic IRA Codes
  - Analysis above implies that a properly normalized $\lambda(\cdot)$ must have $p_0 = 1$
  - Non-sys IRA codes satisfy the DE equation with $\rho(1) = 1$ and $\lambda(1) = 1$

Non-Systematic IRA Code Issues

- Getting Decoding Started
  - DE update has a fixed point at $x = 1$

$$\lambda\left(1 - \left[\frac{1-p}{1-pR(1-x)}\right]^2 \rho(1-x)\right) < x$$

- Solutions
  - Systematic bits, degree 1 checks, and/or pilot bits
  - LT codes and Bi-Regular IRA codes (ten Brink) use degree 1 checks
  - Pilots bits are really the same as doping

Bit-Regular Construction

- Ensemble of bit-regular non-sys IRA codes with $\lambda(x) = x^{q-1}$
  - The parity-check d.d. which satisfies the DE equality for this $\lambda(x)$ is

$$\rho(x) = \frac{1-(1-x)^{\frac{1}{q-1}}}{\left[1-p\left(1-qx+(q-1)\left[1-(1-x)^{\frac{q}{q-1}}\right]\right)\right]^2}$$

  - For $q = 3$, the power series expansion of $\rho(x)$ is non-negative iff $p \in [0, 1/13]$

- Truncating the check d.d. to degree $M(\varepsilon)$ (via degree 1 checks)
  - Let $\rho_\varepsilon(x) = \left(1 - \sum_{n=1}^{M(\varepsilon)} \rho_n\right) + \sum_{n=1}^{M(\varepsilon)} \rho_n x^{n-1}$ where $\sum_{n=M(\varepsilon)+1}^{\infty} \rho_n < \frac{\varepsilon}{q(1-p)}$
  - In this case, DE converges to zero and $R^{IRA} \geq (1-\varepsilon)(1-p)$
  - Complexity (edges per info bit) upper bounded by $q + \frac{2}{(1-p)(1-\varepsilon)}$

Check-Regular Construction

- Ensemble of check-regular non-sys IRA codes with $\rho(x) = x^2$
  - The information-bit d.d. which satisfies the DE equality for this $\rho(x)$ is

$$\lambda(x) = 1 + \sqrt{-\frac{4(1-p)}{3p\sqrt{1-x}}}\sin\left(\frac{1}{3}\arcsin\left(\sqrt{-\frac{27p(1-x)^{3/2}}{4(1-p)^3}}\right)\right)$$

  - Can show the power series expansion of $\lambda(x)$ is non-negative for $p \in [0, 3/4]$

- Truncating the bit d.d. to degree $M(\varepsilon)$ (via pilot bits)
  - Treat all information bits with degree $> M(\varepsilon)$ as pilot bits
  - Effective bit d.d. $\lambda_\varepsilon(x) = \sum_{n=2}^{M(\varepsilon)} \lambda_n x^{n-1}$ where $\sum_{n=M(\varepsilon)+1}^{\infty} \lambda_n/n < \varepsilon(1-p)/3$
  - Again, DE converges to zero and $R^{IRA} \geq (1-\varepsilon)(1-p)$
  - Complexity (edges per info bit) upper bounded by $\frac{5}{1-p}$

Puncturing Rate Versus Complexity

- For any ensemble of systematic IRA codes with puncturing
  - Assume it achieves a fraction $(1-\varepsilon)$ of capacity under MPI decoding
  - Let α be the fraction of punctured info bits and let $p_0 = 1-(1-\alpha)(1-p)$
  - With this, the DE equality can be written as

$$p_0\,\lambda\left(1-\left[\frac{1-p}{1-pR(1-x)}\right]^2\rho(1-x)\right)=x$$

  - Based on similar S&U IRA results, the complexity is lower bounded by

$$\frac{p}{1-p}\cdot\left(\frac{\ln\left(\frac{p_0(1-p)}{\varepsilon}\right)}{\ln\left(\frac{1}{1-p_0}\right)}+2\right)\sim\left(\frac{\ln\frac{1}{\varepsilon}}{\ln\frac{1}{1-\alpha}}\right)$$

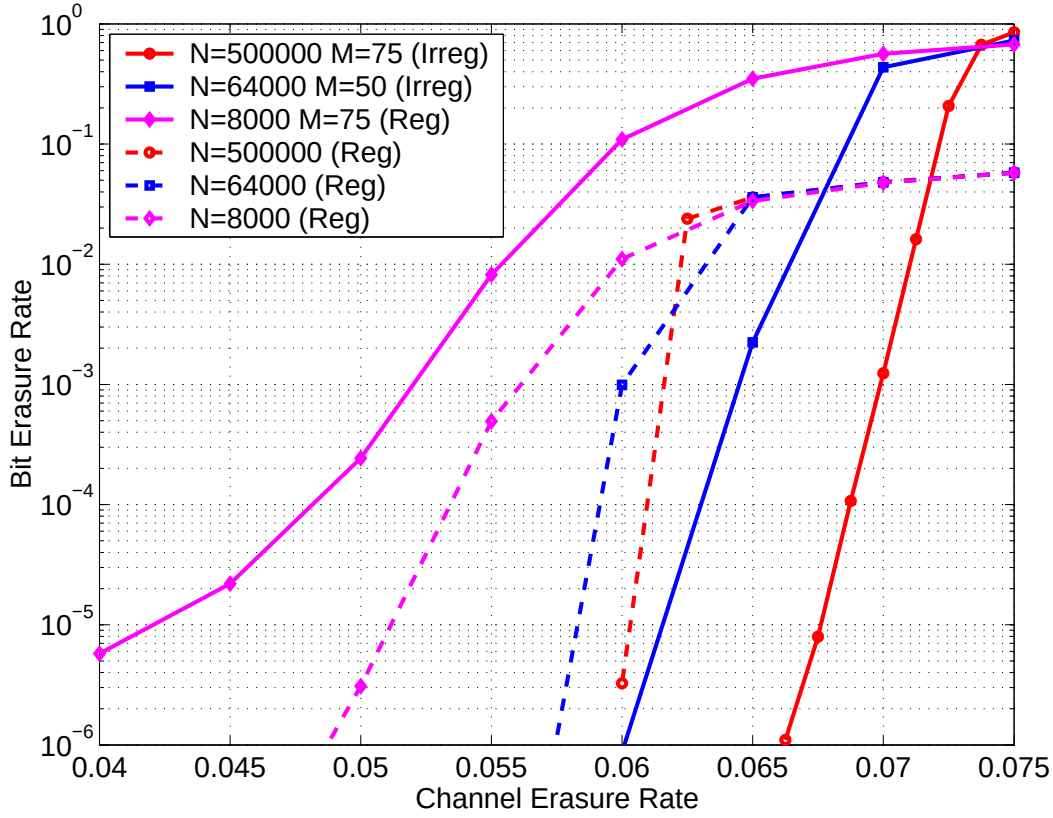
  - To achieve capacity with bounded complexity requires $\alpha = 1-O(\varepsilon)$

Simulation Setup

- Code Design
  - Pick one d.d. and compute the other via power series truncation
  - Bit-regular truncation: Set $\rho_n = 0$ for $n > M$ and renormalize
    Then add some systematic bits to get decoding started (e.g., 100-200)
  - Check-regular truncation: Force bits of degree $> M$ to be pilot bits
  - Vary "design" p to get the desired code rate
- Code Construction
  - Quantize the algebraic d.d. to integers based on block length
  - First, construct by randomly matching bit and check edges
  - Next, swap "bad" edges randomly to remove mult. edges and 4-cycles

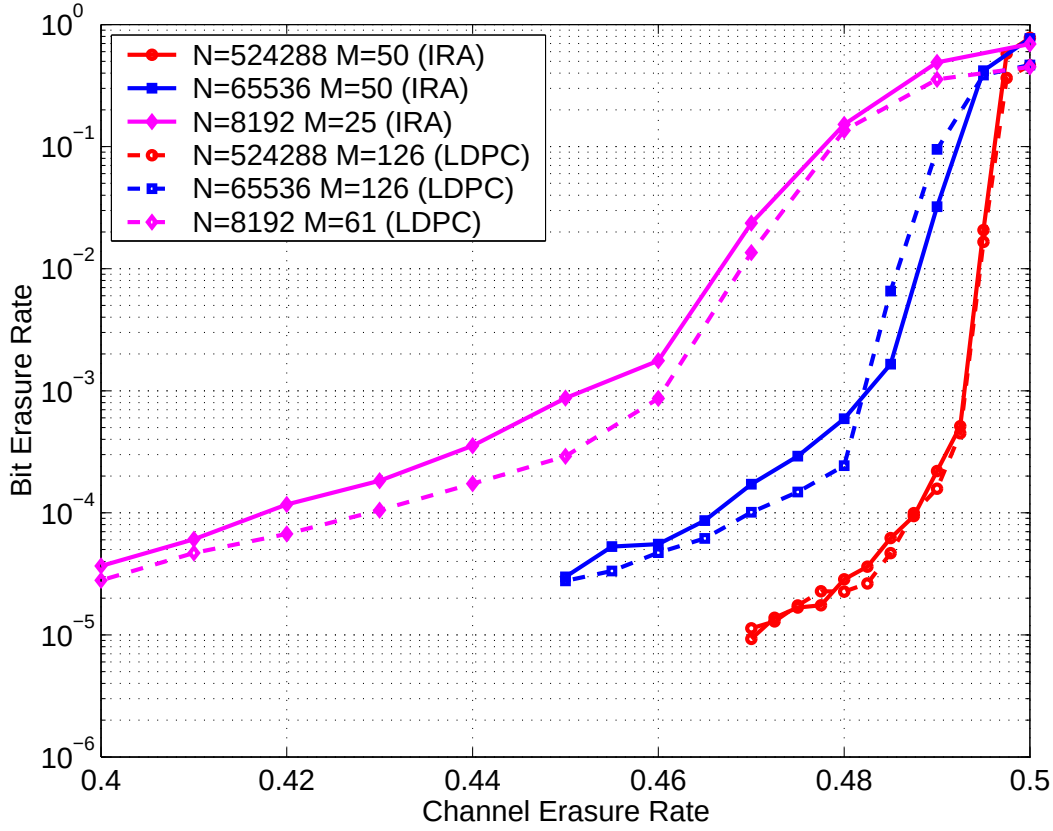
Simulation Results: Bit-Regular

- Design Details (Rate=0.925)
  - "Irreg": Best of $M = 25, 50, 75$
  - "Reg": Sys-IRA d.d. (3,37)
- Observations
  - No apparent error floor
  - Number of sys bits required doesn't grow with length
  - Rate loss is small for large N and large for small N



Simulation Results: Check-Regular

- Design Details (Rate=0.5)
  - "IRA": Best of $M = 25, 50, 75$
  - "LDPC": Check-reg $q = 8, 9$
- Observations
  - Performance very similar
  - Error floor in both ensembles due to marginal stability



Summary

- New Codes that Achieve Capacity with Bounded Complexity
  - Previous constructions have provably unbounded complexity = $O(\ln \frac{1}{\varepsilon})$
  - Our main result is the existence of these codes
  - Simulations show they're not impressive for small to moderate block lengths
  - Is this a fundamental problem with bounded complexity codes?
  - Should beat any fixed complexity LDPC code for "large enough" block length
- Full Paper
  - Full paper is nearly complete
  - Should be at `http://www.ee.technion.ac.il/people/sason` in the next few weeks