Channel Manipulation as a Coding Technique

Hsin-Po Wang (EECS, UC Berkeley)

J = 74 M = 77 S = 83 F = 70 O = 79

The “JMMSFO” polynomial:

$$f(x) = 74 + 77x + 77x^2 + 83x^3 + 70x^4 + 79x^5$$

J = 74 M = 77 S = 83 F = 70 O = 79

The “JMMSFO” polynomial:

$f(x) =$ 

$f(-3) = 232 \quad f(-2) = 844 \quad f(-1) = -18 \quad f(0) = 74$

$f(1) = 460 \quad f(2) = 848 \quad f(3) = 706 \quad f(4) = 742$

J = 74 M = 77 S = 83 F = 70 O = 79

The “JMMSFO” polynomial:

$f(x) =$ 

$f(-3) = 232$ $f(-2) = 844$ $f(-1) = -18$ $f(0) =$ 

$f(1) = 460$ $f(2) = 848$ $f(3) = 706$ $f(4) = 742$

J = 74 M = 77 S = 83 F = 70 O = 79

The “JMMSFO” polynomial:

$f(x) =$ 

$f(-3) = 232$ $f(-2) = 844$ $f(-1) = -18$ $f(0) =$ 

$f(1) = 4$  $f(2) = 848$ $f(3) = 706$ $f(4) = 742$

J = 74   M = 77   S = 83   F = 70   O = 79

The "JMMSFO" polynomial:

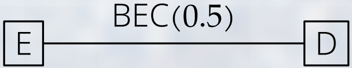
$f(x) =$ 

$f(-3) = 232$ $f(-2) = 844$ $f(-1) = -18$ $f(0) =$ 

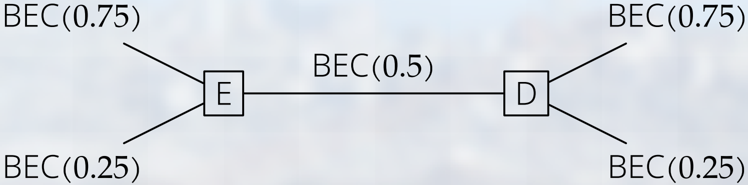
$f(1) = 4$  $f(2) = 848$ $f(3) =$  $f(4) = 742$

New Idea

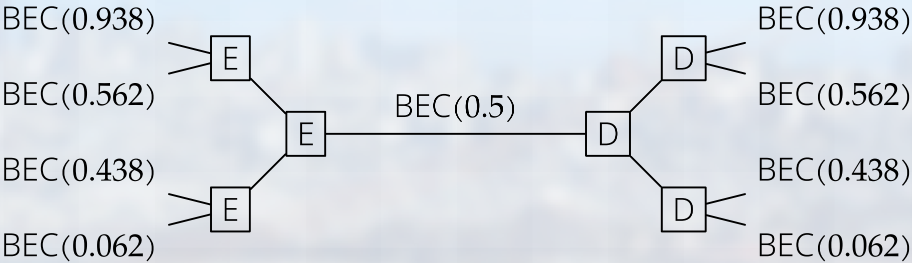
Polar Codes



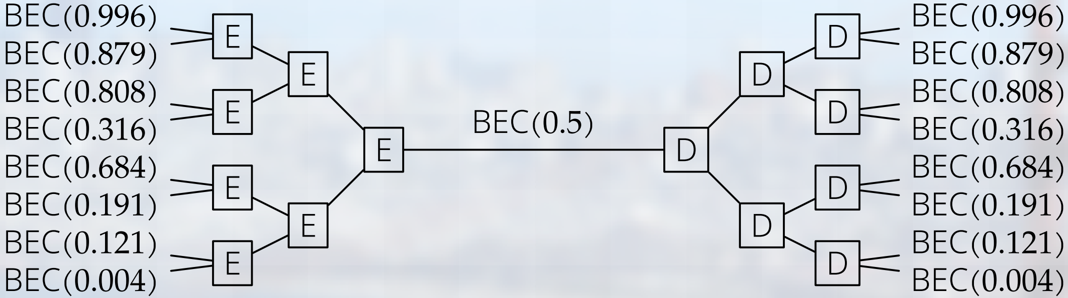
Suppose there are magic devices $\boxed{\text{E}}$ and $\boxed{\text{D}}$ that turns BEC(x) into BEC(x^2) and BEC$(2x - x^2)$.



Suppose there are magic devices $\boxed{\mathrm{E}}$ and $\boxed{\mathrm{D}}$ that turns $\mathrm{BEC}(x)$ into $\mathrm{BEC}(x^2)$ and $\mathrm{BEC}(2x - x^2)$.



What if we apply apply more magic devices?



What if we apply apply more magic devices?
And more and more and more???

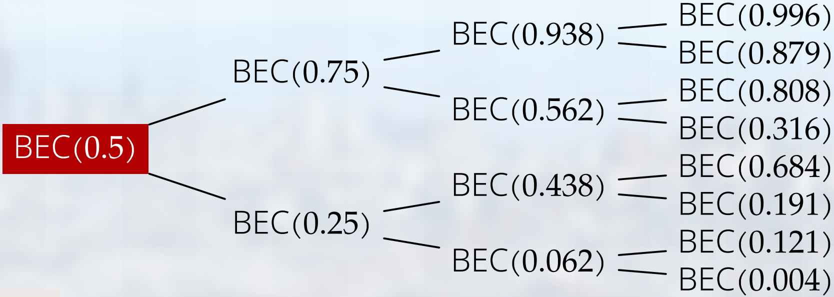
- $\mathrm{BEC}(0.5)$
  - $\mathrm{BEC}(0.75)$
    - $\mathrm{BEC}(0.938)$
      - $\mathrm{BEC}(0.996)$
      - $\mathrm{BEC}(0.879)$
    - $\mathrm{BEC}(0.562)$
      - $\mathrm{BEC}(0.808)$
      - $\mathrm{BEC}(0.316)$
  - $\mathrm{BEC}(0.25)$
    - $\mathrm{BEC}(0.438)$
      - $\mathrm{BEC}(0.684)$
      - $\mathrm{BEC}(0.191)$
    - $\mathrm{BEC}(0.062)$
      - $\mathrm{BEC}(0.121)$
      - $\mathrm{BEC}(0.004)$

This is a tree

- BEC(0.5)
  - BEC(0.75)
    - BEC(0.938)
      - BEC(0.996)
      - BEC(0.879)
    - BEC(0.562)
      - BEC(0.808)
      - BEC(0.316)
  - BEC(0.25)
    - BEC(0.438)
      - BEC(0.684)
      - BEC(0.191)
    - BEC(0.062)
      - BEC(0.121)
      - BEC(0.004)

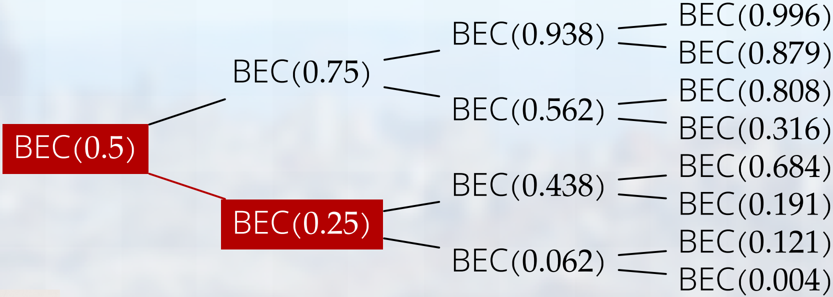
E. Arıkan: This is a martingale

$$M_{n+1} := \begin{cases} 2M_n - M_n^2 & \text{with prob. } 1/2, \\ M_n^2 & \text{with prob. } 1/2. \end{cases}$$



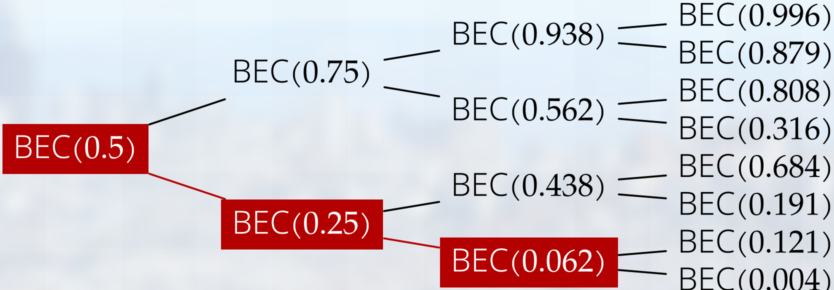
E. Arıkan: This is a martingale

$$M_{n+1} := \begin{cases} 2M_n - M_n^2 & \text{with prob. } 1/2, \\ M_n^2 & \text{with prob. } 1/2. \end{cases}$$



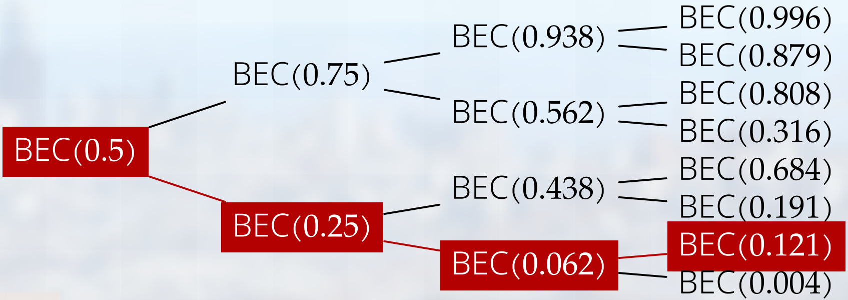
E. Arıkan: This is a martingale

$$M_{n+1} := \begin{cases} 2M_n - M_n^2 & \text{with prob. } 1/2, \\ M_n^2 & \text{with prob. } 1/2. \end{cases}$$



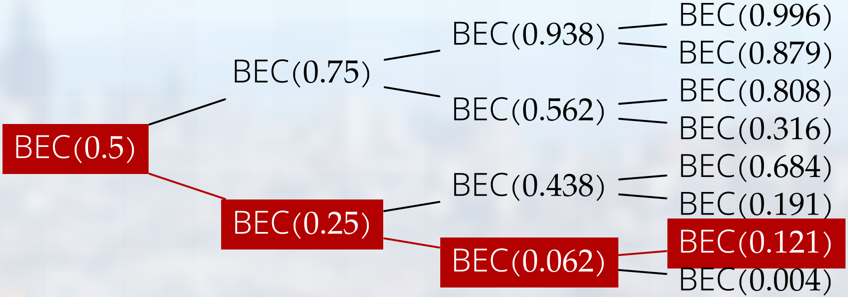
E. Arıkan: This is a martingale

$$M_{n+1} := \begin{cases} 2M_n - M_n^2 & \text{with prob. } 1/2, \\ M_n^2 & \text{with prob. } 1/2. \end{cases}$$



E. Arıkan: This is a martingale

$$M_{n+1} := \begin{cases} 2M_n - M_n^2 & \text{with prob. } 1/2, \\ M_n^2 & \text{with prob. } 1/2. \end{cases}$$



:Study martingale to study code

$$M_{n+1} := \begin{cases} 2M_n - M_n^2 & \text{with prob. } 1/2, \\ M_n^2 & \text{with prob. } 1/2. \end{cases}$$

Martingale–Code Rate Thm []

Martingale–Code Rate Thm []

$$\text{Prob}\{4^{-n} < M_n < 1 - 4^{-n}\} < \varepsilon$$

implies code rate

$(1/2 - \varepsilon)N$ bits / N channel uses.

$(1/2 - N^{-\rho})N$ bits / N channel uses

History of ρ over BMS Channels: 0 $1/2$

$(1/2 - N^{-\rho})N$ bits / N channel uses

History of ρ over BMS Channels: 0 $1/2$

2015 Guruswami–Xia

2012 Goli–Hassani–Urbanke

2014 Hassani–Alishahi–Urbanke

2014 Goldin–Burshtein

2016 Mondelli–Hassani–Urbanke

2022 –Lin–Vardy–Gabrys

Improve ρ over BEC: 0 $1/2$

Improve ρ over BEC: 0 $1/2$

2010 Hassani–Alishahi–Urbanke 2×2

2010 Korada–Montanari–Telatar–Urbanke 2×2

2014 Fazeli–Vardy 8×8

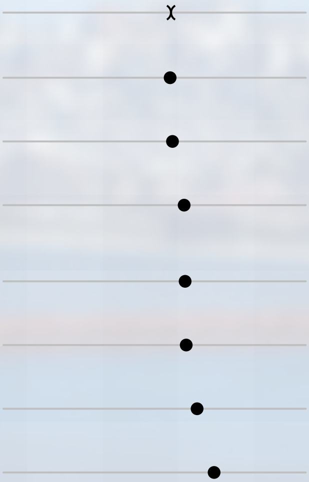
2021 Trofimiuk–Trifonov 16×16

2022 Duursma–Gabrys–Guruswami–Lin– $2 \times 2/F_4$

2021 Trofimiuk 24×24

2021 Yao–Fazeli–Vardy 32×32

2021 Yao–Fazeli–Vardy 64×64



The optimal ρ: 0 $\qquad$ $1/2$

The optimal ρ: 0 $1/2$

2019 Pfister–Urbanke
q-ary erasure channel, $q \to \infty$

2021 Fazeli–Hassani–Mondelli–Vardy
binary erasure channel

2022 Guruswami–Riazanov–Ye
binary symmetric memoryless channel

2021 –Duursma
discrete memoryless channel

2011 Alamdar-Yazdi–Kschischang:
Prune the tree to reduce complexity.

2017 El-Khamy–Mahdavifar–Feygin–Lee–Kang:
Pruning reduces complexity by a scalar; still $O(N \log N)$.

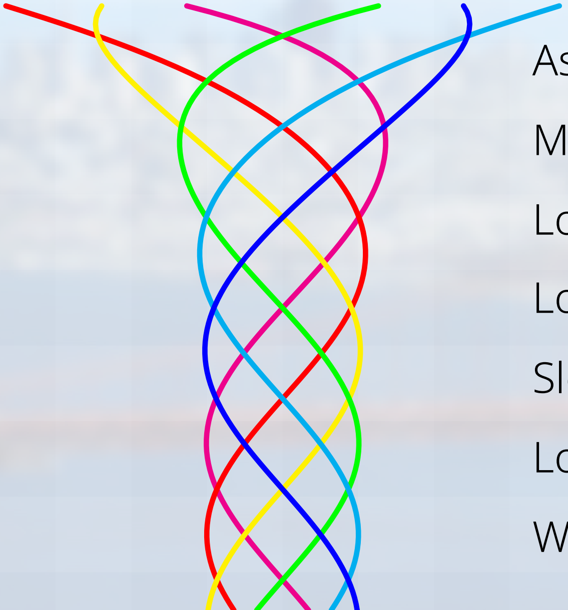
2021 –Duursma: $O(N \log \log N)$
Trade-off: complexity $\approx O(N \log(-\log(\text{decode error})))$.

2021 Mondelli–Hashemi–Cioffi–Goldsmith,
2021 Hashemi–Mondelli–Fazeli–Vardy–Cioffi–Goldsmith:
Study parallelism vs latency.

Polar code is a mathy code

Polar code is a mathy code

Polar achieves the capacity of



Asymmetric channel

Multiple access channel

Lossless compression

Lossy compression

Slepian–Wolf

Lossless compression w/ helper

Wiretap channel (degradation)

Deletion channel … (good error prob)

Broadcast channel … (good error prob)

Channel with memory … (good error prob)

Wiretap channel (no degradation) … (good error prob)

Hidden Markov chain channel state … (good error prob)

Non-stationary channel … (good gap to capacity)

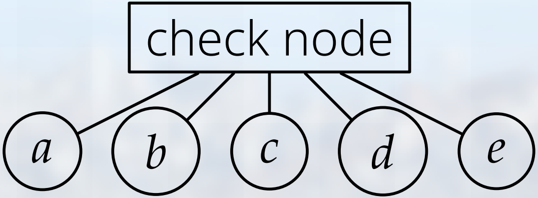
Classical–Quantum channel … (yes)

Quantum–Quantum channel … (?)

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

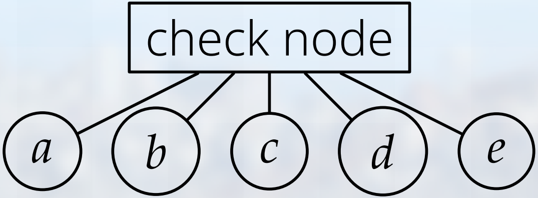
Wikipedia

Low-Density Parity-Check (LDPC) Codes

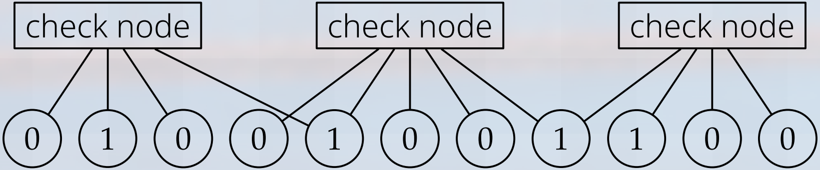
Rule: Every 

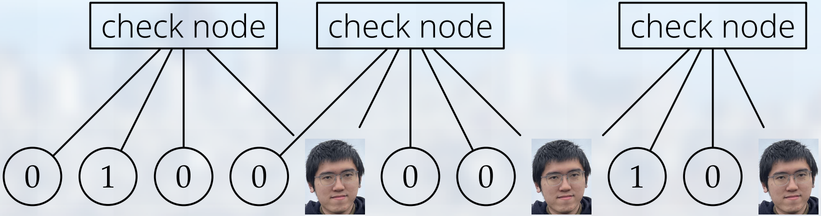
Sum to an even number

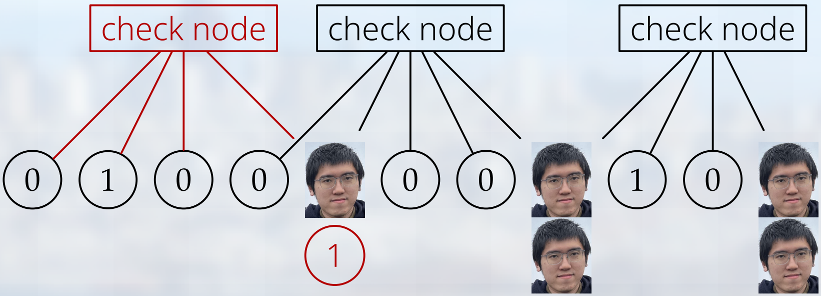
Rule: Every

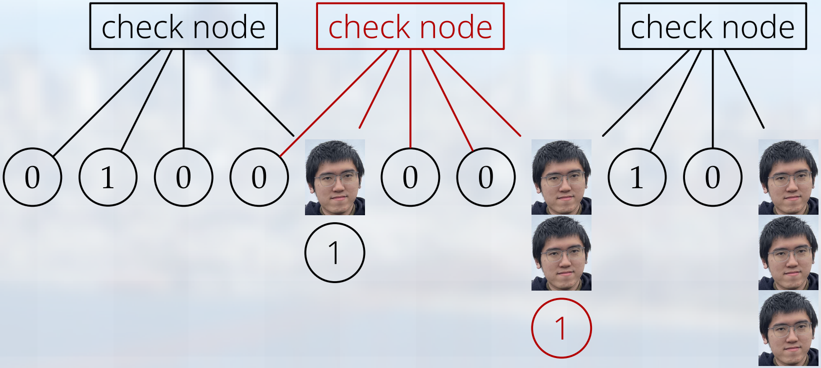


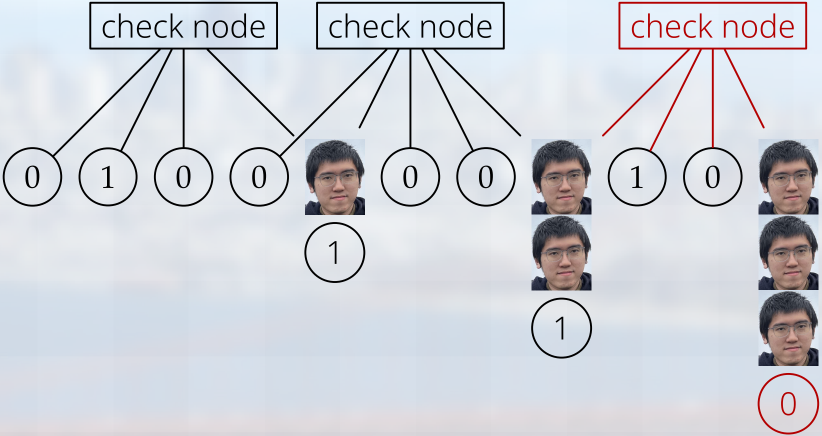
Sum to an even number

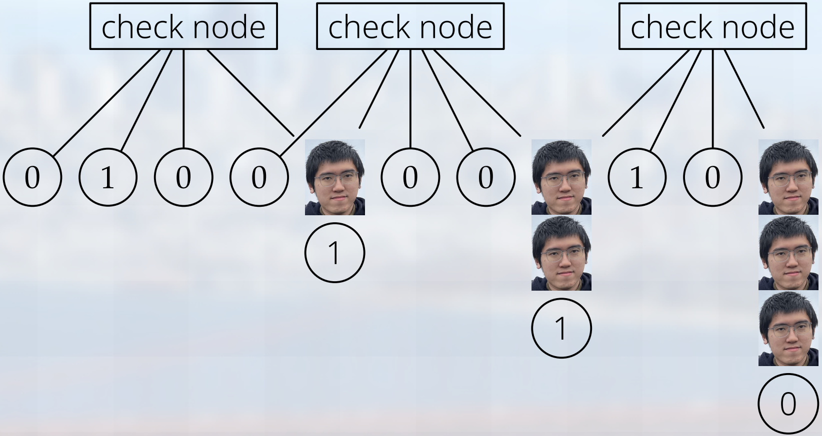



check node
check node
check node
0
1
0
0
0
0
1
0

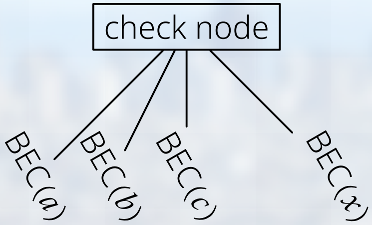

check node
check node
check node
0
1
0
0
0
0
1
0
1

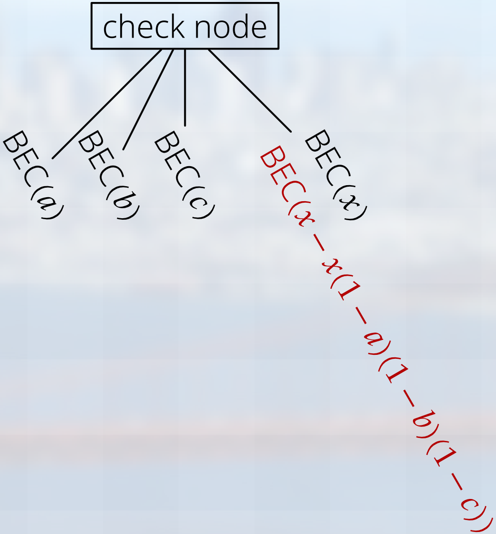

check node
check node
check node
0
1
0
0
0
0
1
0
1
1

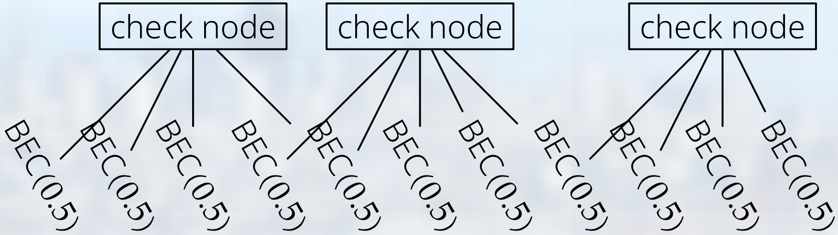

check node
check node
check node
0
1
0
0
1
0
0
1
1
0
0

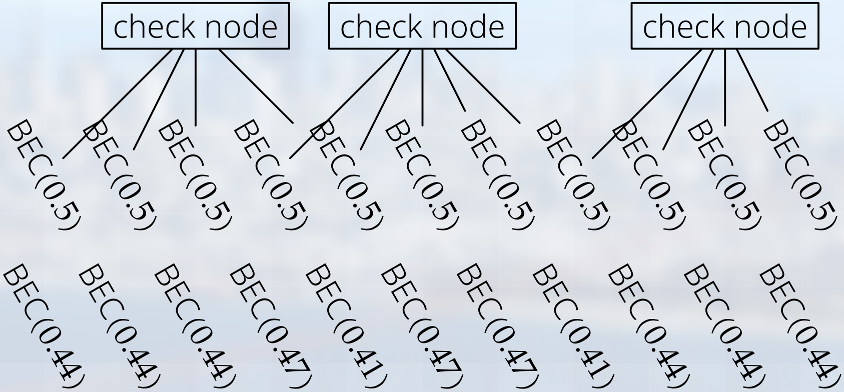


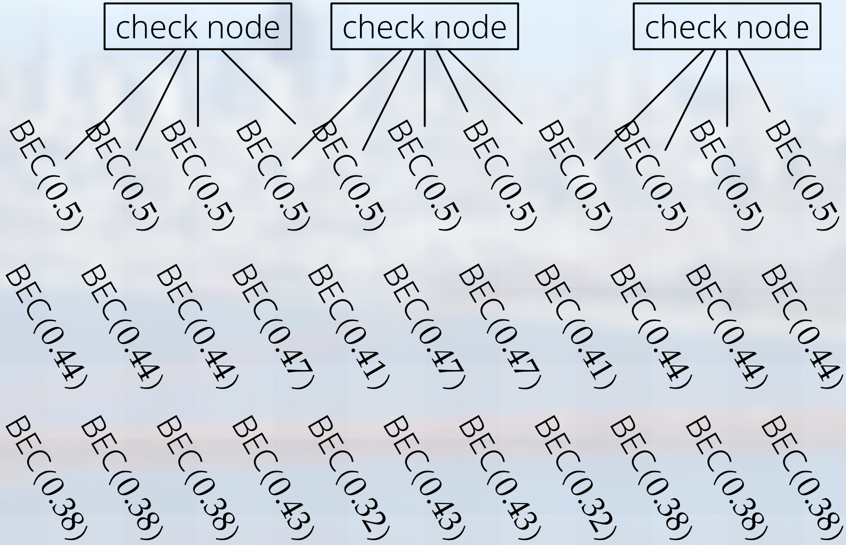
How to analyze, mathematically?


check node
BEC(a)
BEC(b)
BEC(c)
BEC(x)


check node
BEC(a)
BEC(b)
BEC(c)
BEC(x)
BEC($x - x(1-a)(1-b)(1-c)$)


check node
check node
check node
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)


check node
check node
check node
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.5)
BEC(0.44)
BEC(0.44)
BEC(0.44)
BEC(0.47)
BEC(0.41)
BEC(0.47)
BEC(0.47)
BEC(0.41)
BEC(0.44)
BEC(0.44)
BEC(0.44)

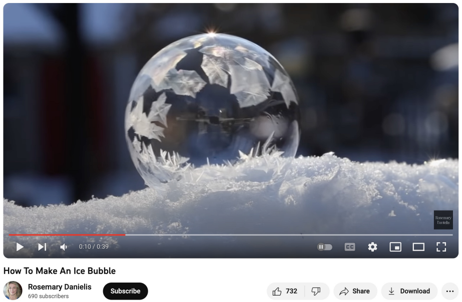

check node
check node
check node
BEC(0.5) BEC(0.5) BEC(0.5) BEC(0.5) BEC(0.5) BEC(0.5) BEC(0.5) BEC(0.5) BEC(0.5) BEC(0.5) BEC(0.5)
BEC(0.44) BEC(0.44) BEC(0.44) BEC(0.47) BEC(0.41) BEC(0.47) BEC(0.47) BEC(0.41) BEC(0.44) BEC(0.44) BEC(0.44)
BEC(0.38) BEC(0.38) BEC(0.38) BEC(0.43) BEC(0.32) BEC(0.43) BEC(0.43) BEC(0.32) BEC(0.38) BEC(0.38) BEC(0.38)


0:05 / 0:39
How To Make An Ice Bubble
Rosemary Danielis
690 subscribers
Subscribe
732
Share
Download


0:05 / 0:39
How To Make An Ice Bubble
Rosemary Danielis
690 subscribers
Subscribe
732
Share
Download


0:10 / 0:39
How To Make An Ice Bubble
Rosemary Danielis
690 subscribers
Subscribe
732
Share
Download


0:05 / 0:39
How To Make An Ice Bubble
Rosemary Danielis
690 subscribers
Subscribe
732
Share
Download


0:10 / 0:39
How To Make An Ice Bubble
Rosemary Danielis
690 subscribers
Subscribe
732
Share
Download


0:15 / 0:39
How To Make An Ice Bubble
Rosemary Danielis
690 subscribers
Subscribe
732
Share
Download


0:05 / 0:39
How To Make An Ice Bubble
Rosemary Danielis
690 subscribers
Subscribe
732
Share
Download
0:10 / 0:39
How To Make An Ice Bubble
Rosemary Danielis
690 subscribers
Subscribe
732
Share
Download
0:15 / 0:39
How To Make An Ice Bubble
Rosemary Danielis
690 subscribers
Subscribe
732
Share
Download
0:20 / 0:39
How To Make An Ice Bubble
Rosemary Danielis
690 subscribers
Subscribe
732
Share
Download

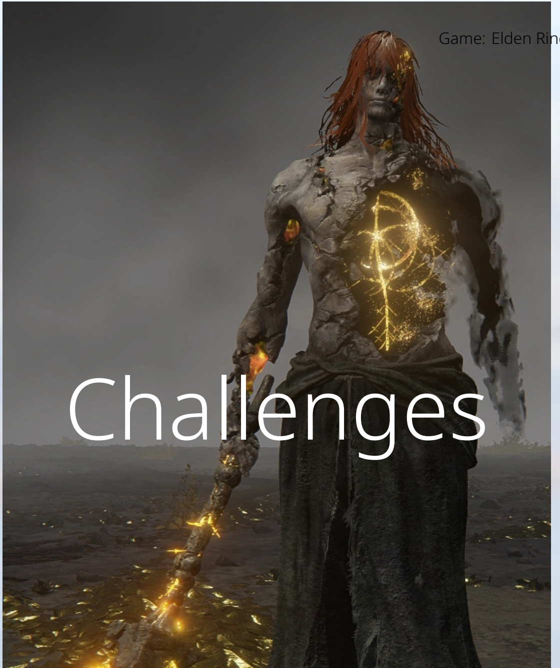
LDPC code is a physics code

LDPC code is a physics code

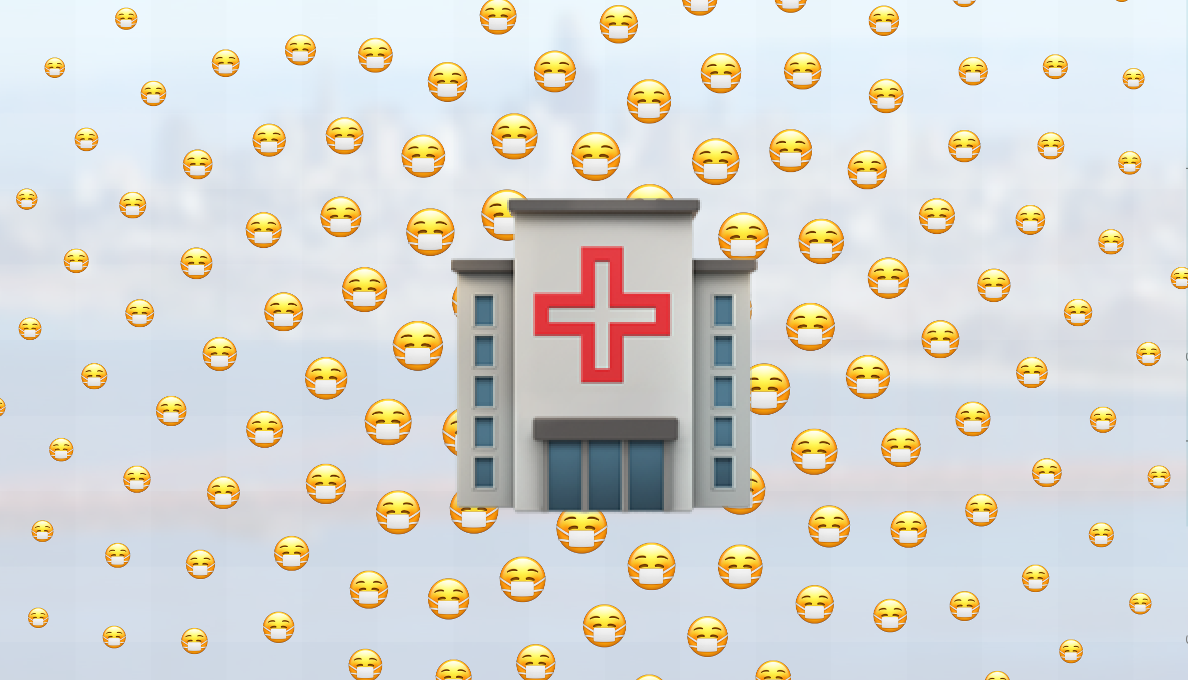
Works well but hard to analyze


Wikipedia
Society
LDPC
Turbo
Polar
Reed–Muller
Channel Evolution

Challenges



Game: Elden Ring



Problem	There are n	k of them	To solve, use m
Radio protocol	cellphones	want to talk	frequencies
Disease control	people	are sick	virus tests
Search engine	webpages	contain keywords	bits per keyword

Problem	There are n	k of them	To solve, use m
Radio protocol	cellphones	want to talk	frequencies
Disease control	people	are sick	virus tests
Search engine	webpages	contain keywords	bits per keyword
Radio protocol	messages	will be sent	frequencies
Genotyping	genes	cause cancer	gene tests
Computer forensics	files	will be modified	bits of storage
Property-preserving hash	properties	appears in a file	bits per file
Image compression	wavelet coefficients	are nonzero	bits per digit
Traitor tracing	users	resell keys	keys
Heavy hitter / DoS	users	are spamming	virtual servers

Proposal: Prove the following

Proposal: Prove the following.

Lemma [Your Name Here]

If we can solve (n, k)-RAC
(RAC = random access channel),

then we can solve $(3n, 2k)$-RAC.

CHALLENGES

Game: Elden Ring

DNA Coding

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

ATTCCG

ATTACG

DNA Coding

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

DNA Coding

ATT CCG

⬆️

G

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

DNA Coding

- Substitution
- Insertion
- Deletion
- Transposition
- Amplification
- Permutation

ATT~~C~~CG

DNA Coding

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

ATTCCG

ATCTCG

DNA Coding

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

DNA Coding

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

DNA Coding

Traditional coding problem

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

DNA Coding

Synchronization problem

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

DNA Coding

Channels
with
memory

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

DNA Coding

Polar code
OK

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

DNA Coding

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

Trace reconstruction problem

DNA Coding

Substitution

Insertion

Deletion

Transposition

Amplification

Use empirical distribution as codeword

Permutation

DNA Coding

Network coding

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

DNA Coding

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation

Clustering problem

DNA Coding

Substitution

Insertion

Deletion

Transposition

Amplification

Permutation