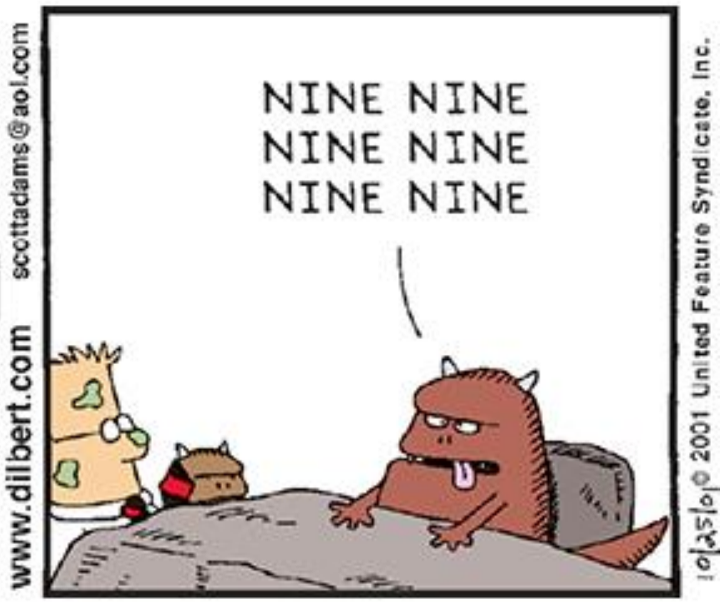
Extractors

Low Entropy Requirements Colliding with Non-Malleability

Divesh Aggarwal Eldon Chung Maciej Obremski

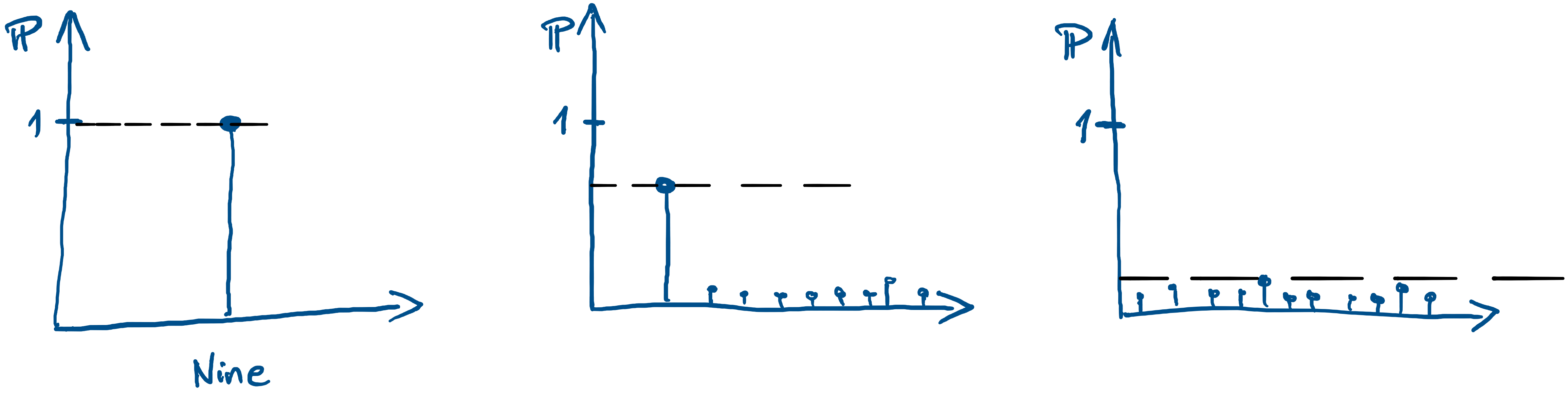
National University of Singapore

Randomness



All processes are random
but some processes are
more random than others.

Min-Entropy

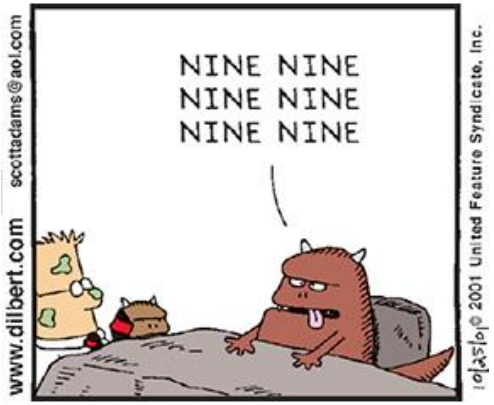


$$H_\infty(X) = -\log \max_x \mathbb{P}(X=x)$$

$X \sim \text{uniform}\{0,1\}^n$

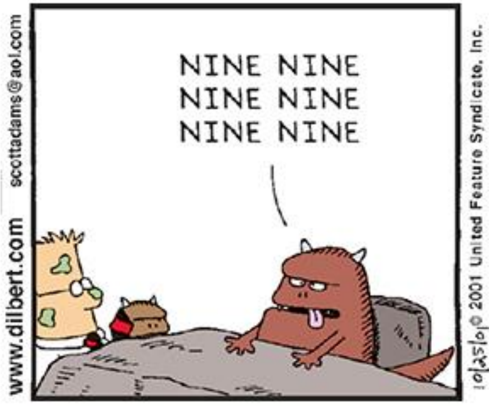
$H_\infty(X) = n$ ← this is maximum possible.

Extractors

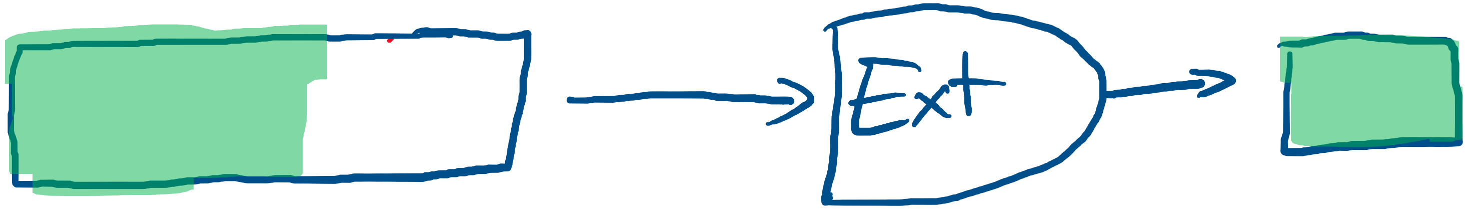


$\xrightarrow{?}$

Extractors

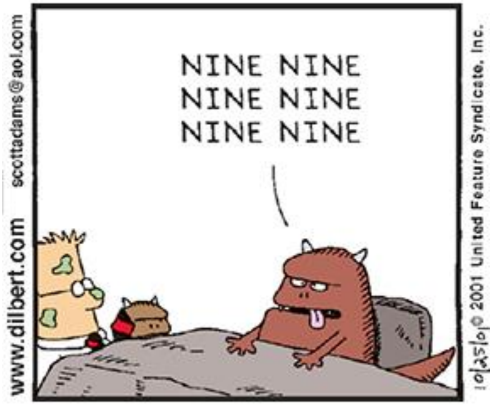

NINE NINE
NINE NINE
NINE NINE
www.dilbert.com scottadams@aol.com
10/25/01 © 2001 United Feature Syndicate, Inc.

?

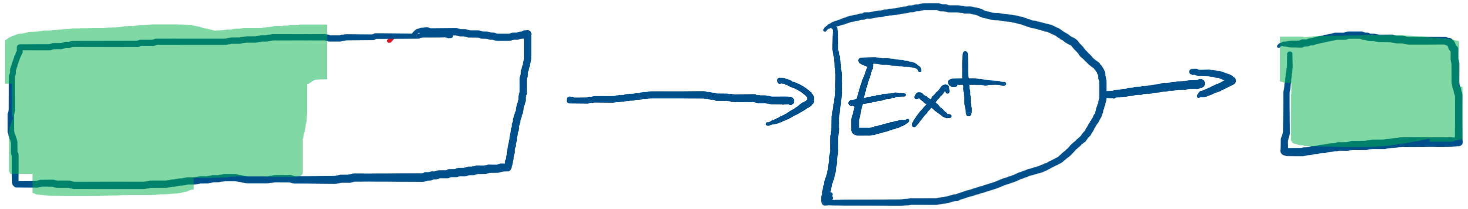


Nope

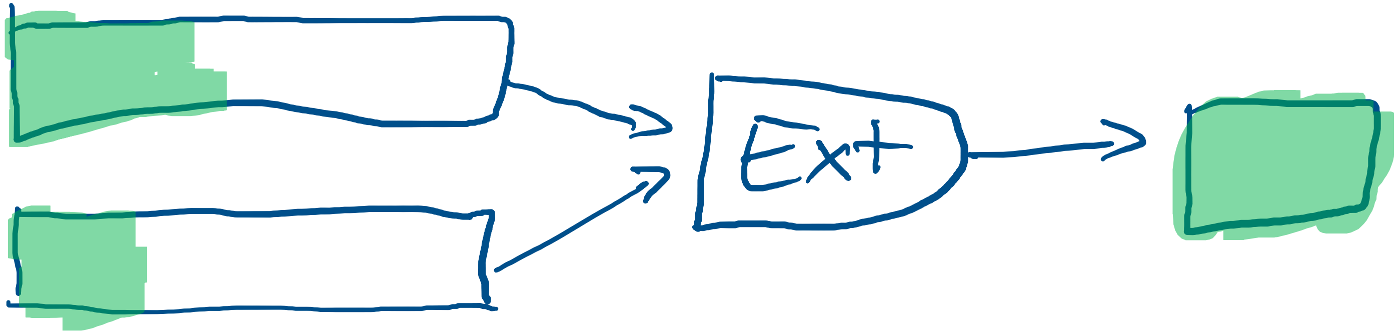
Extractors


NINE NINE
NINE NINE
NINE NINE
www.dilbert.com scottadams@aol.com
© 2001 United Feature Syndicate, Inc.

?

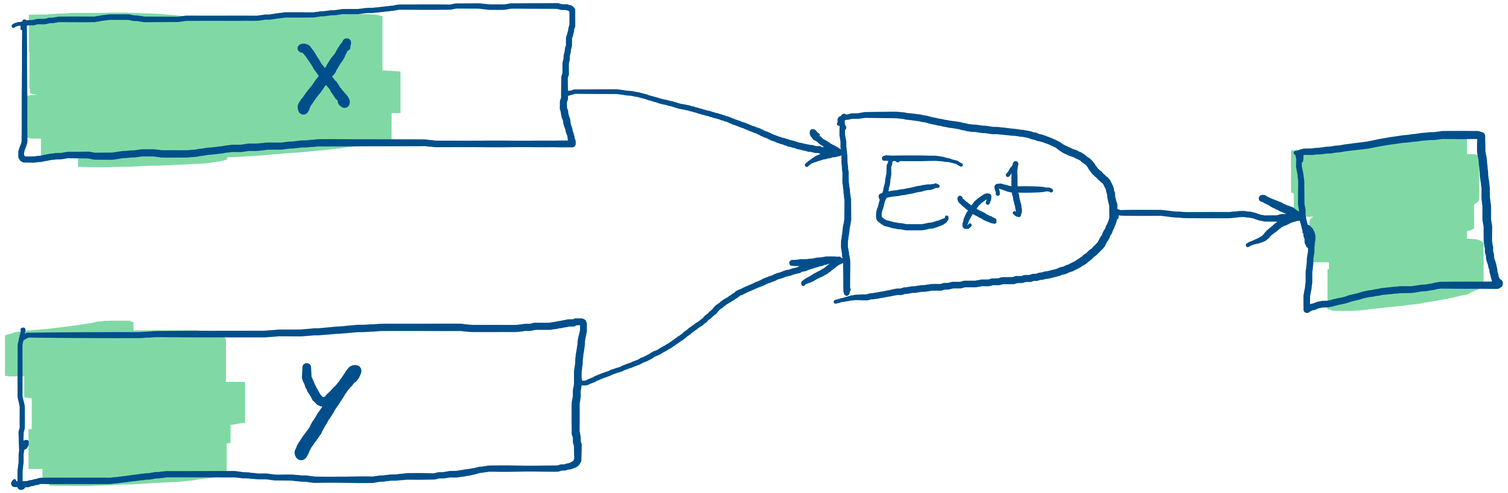


Nope

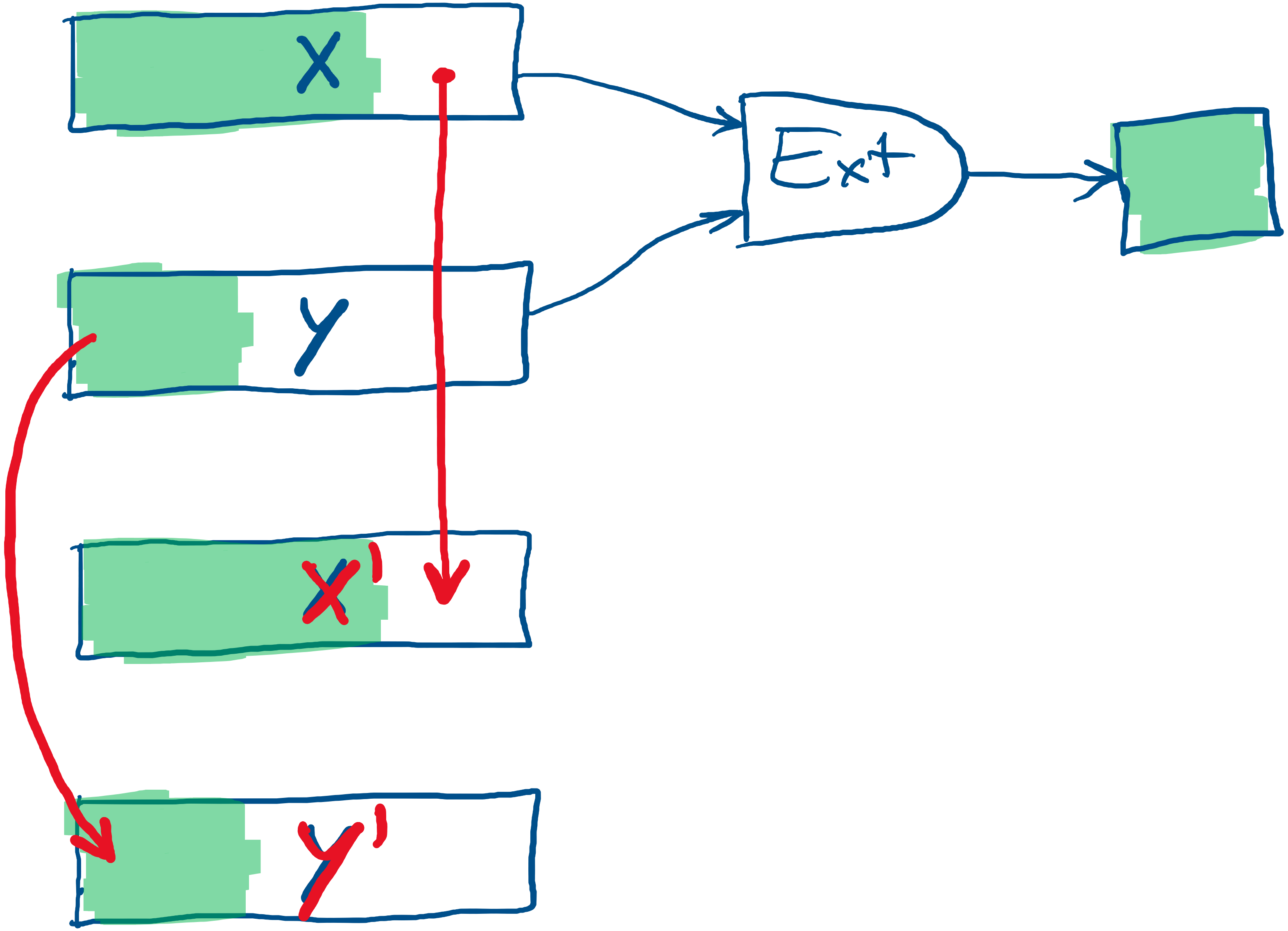


Yey

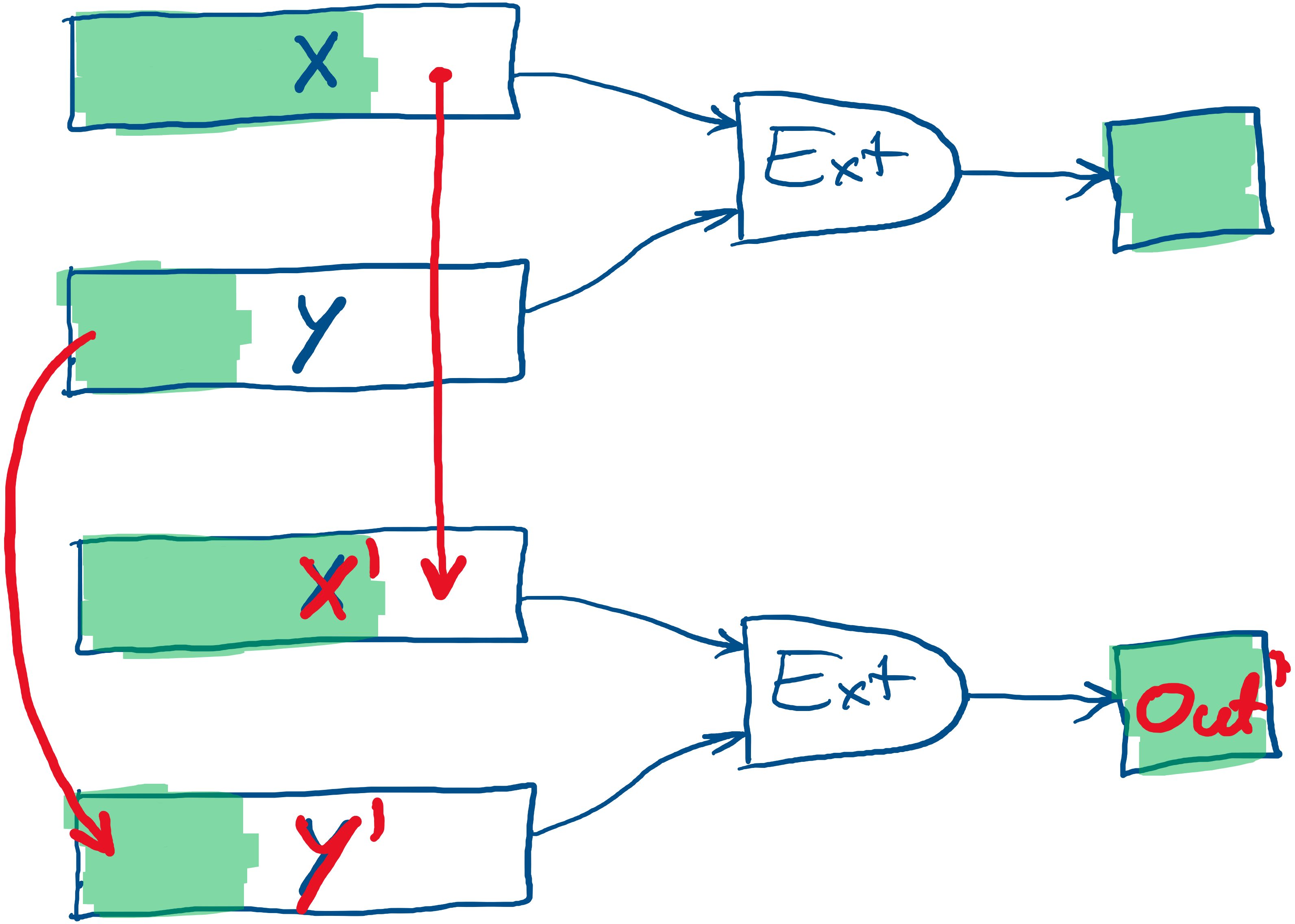
Non-Malleability



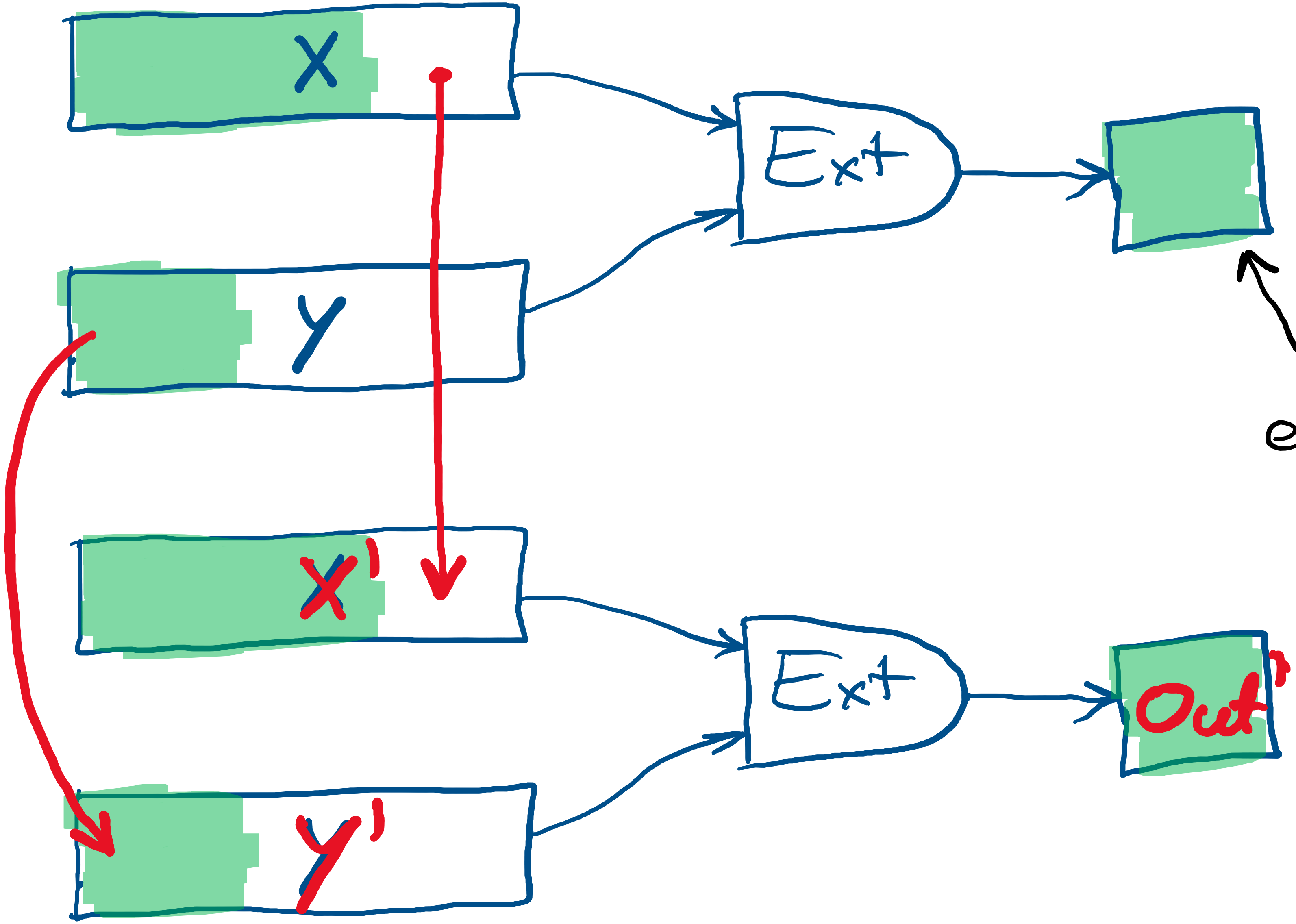
Non-Malleability



Non-Malleability

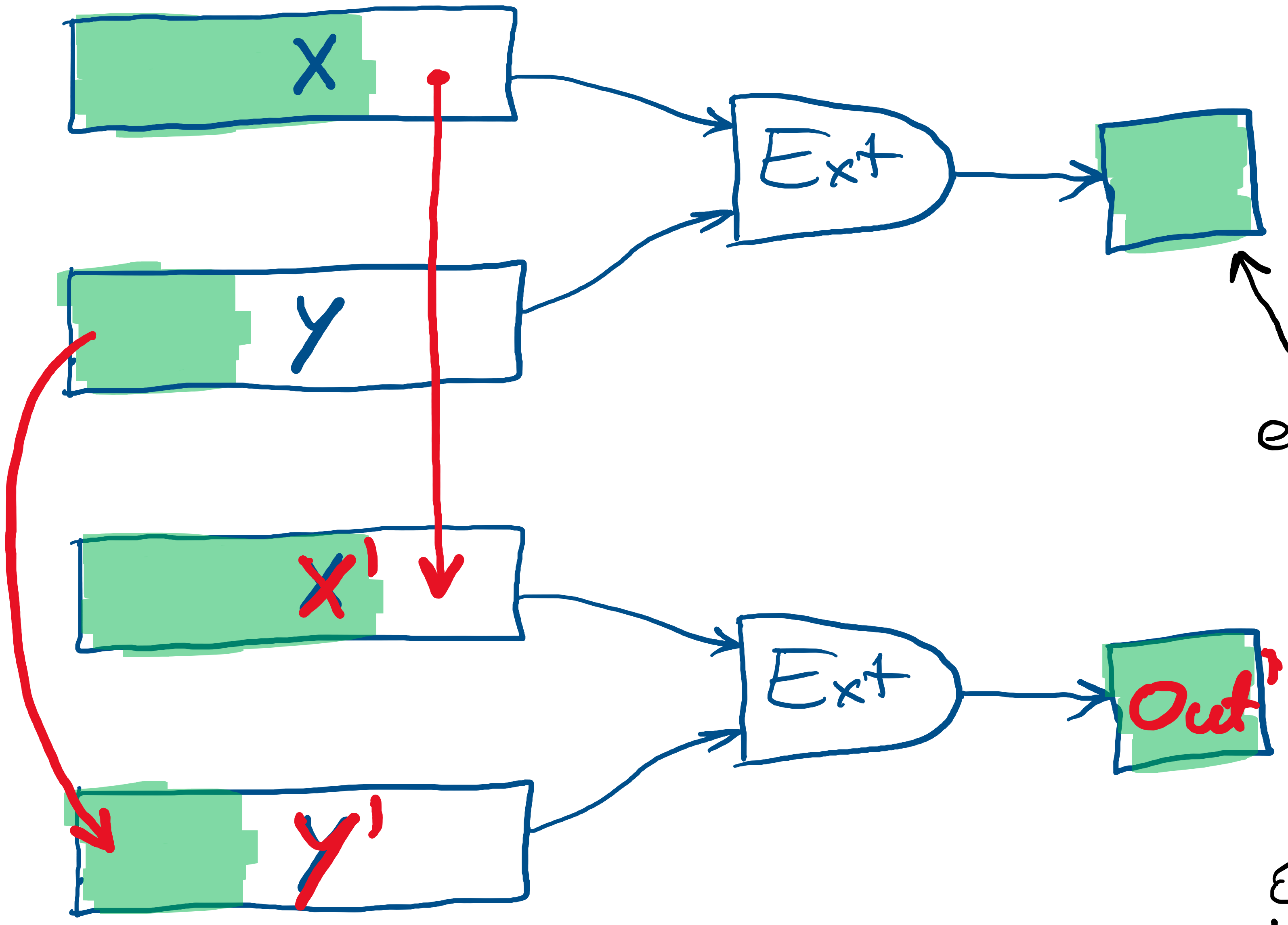


Non-Malleability



Remains uniform even given Out'

Non-Malleability



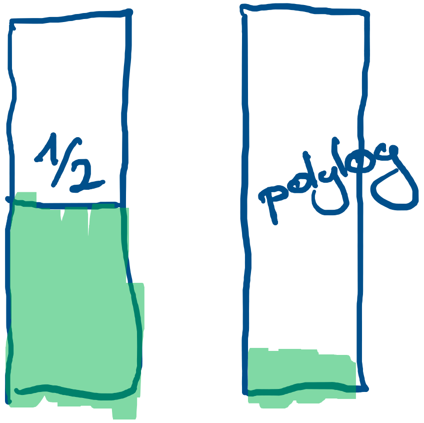
Remains uniform even given Out'

Even if X and X' are correlated, and Y, Y' are correlated Out and Out' are Independent.

What we Know (negligible error)

What we know (negligible error)

Raz

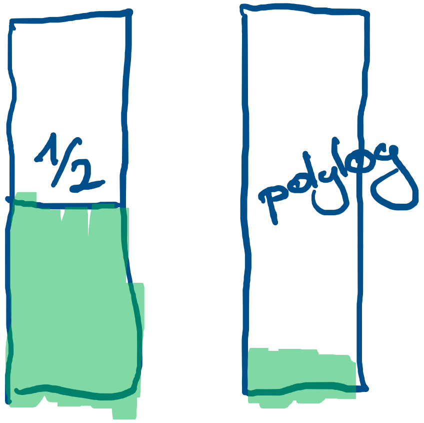


Not

NM

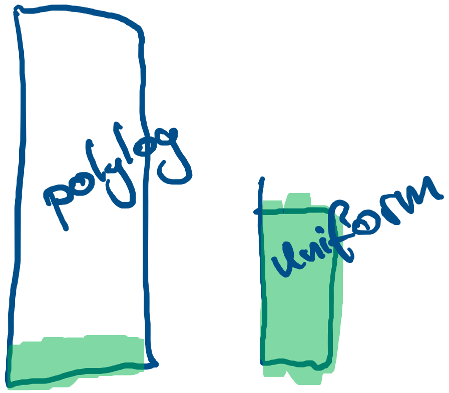
What we know (negligible error)

Raz



Not NM

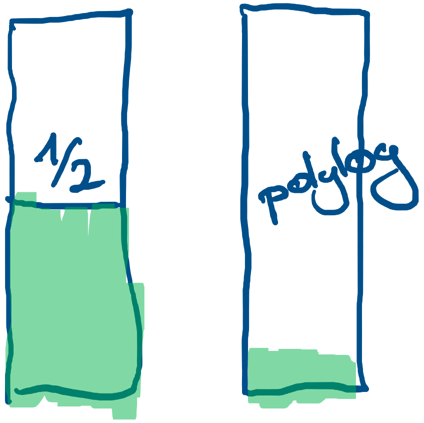
Seeded nmExt



NM with respect to seed

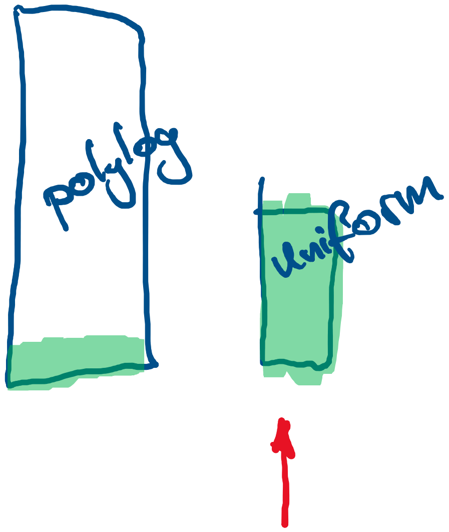
What we Know (negligible error)

Raz



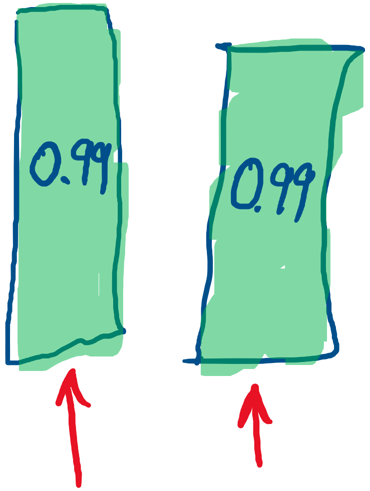
Not NM

Seeded nmExt



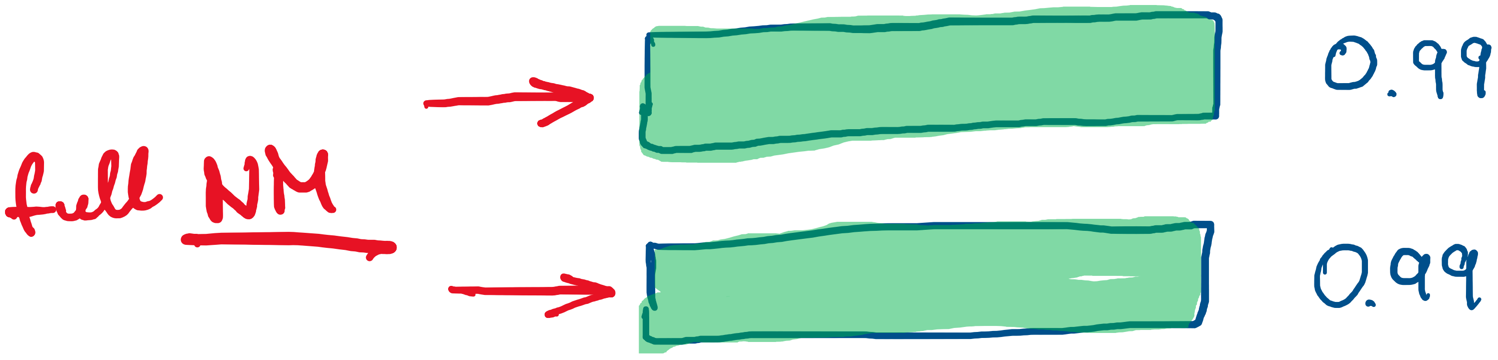
NM with respect to seed

2 nmExt

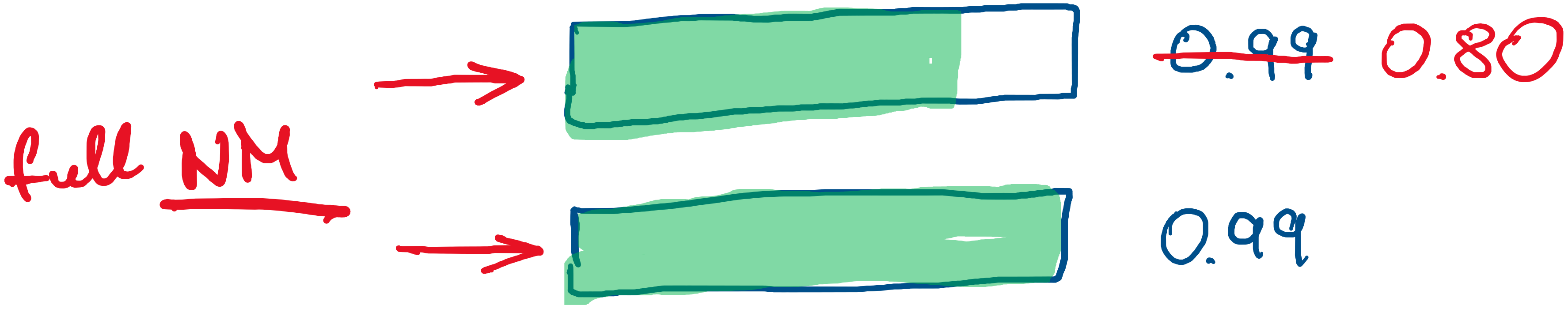


full NM

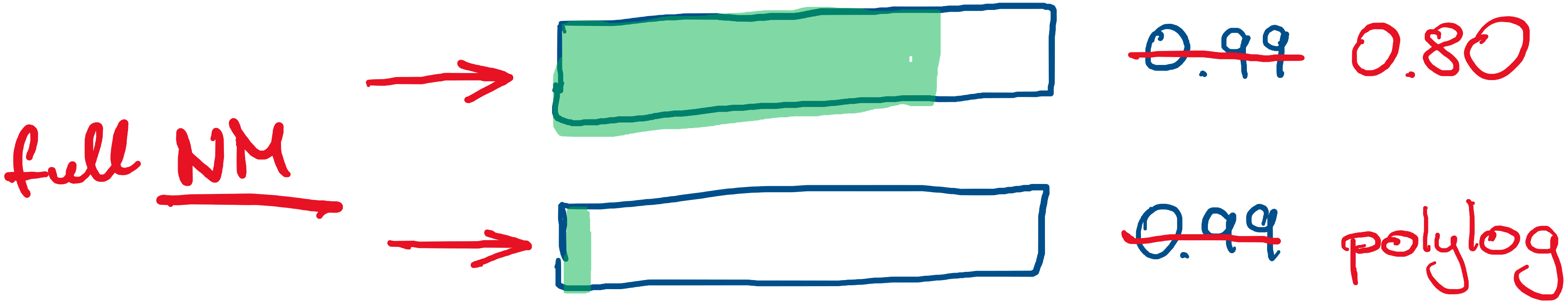
What we know NOW



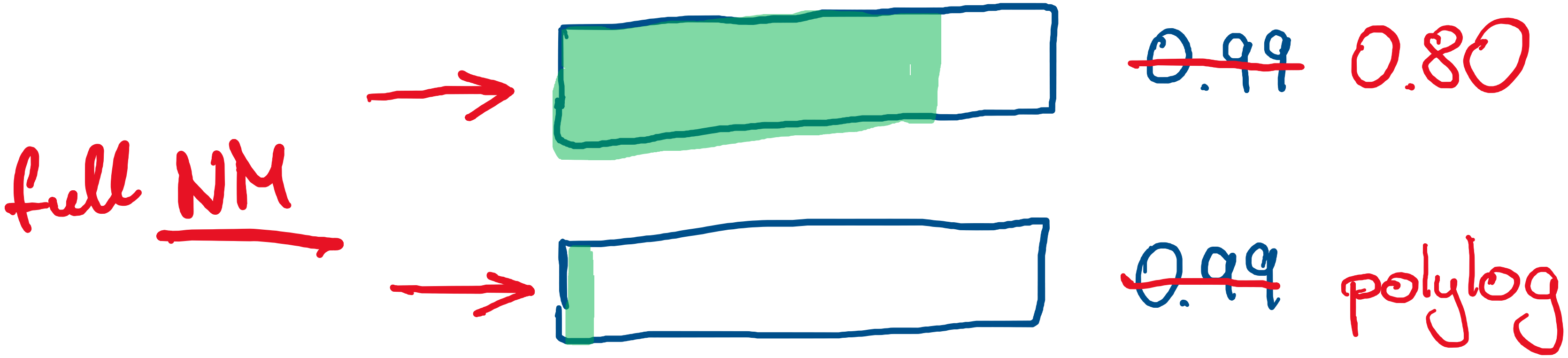
What we Know NOW



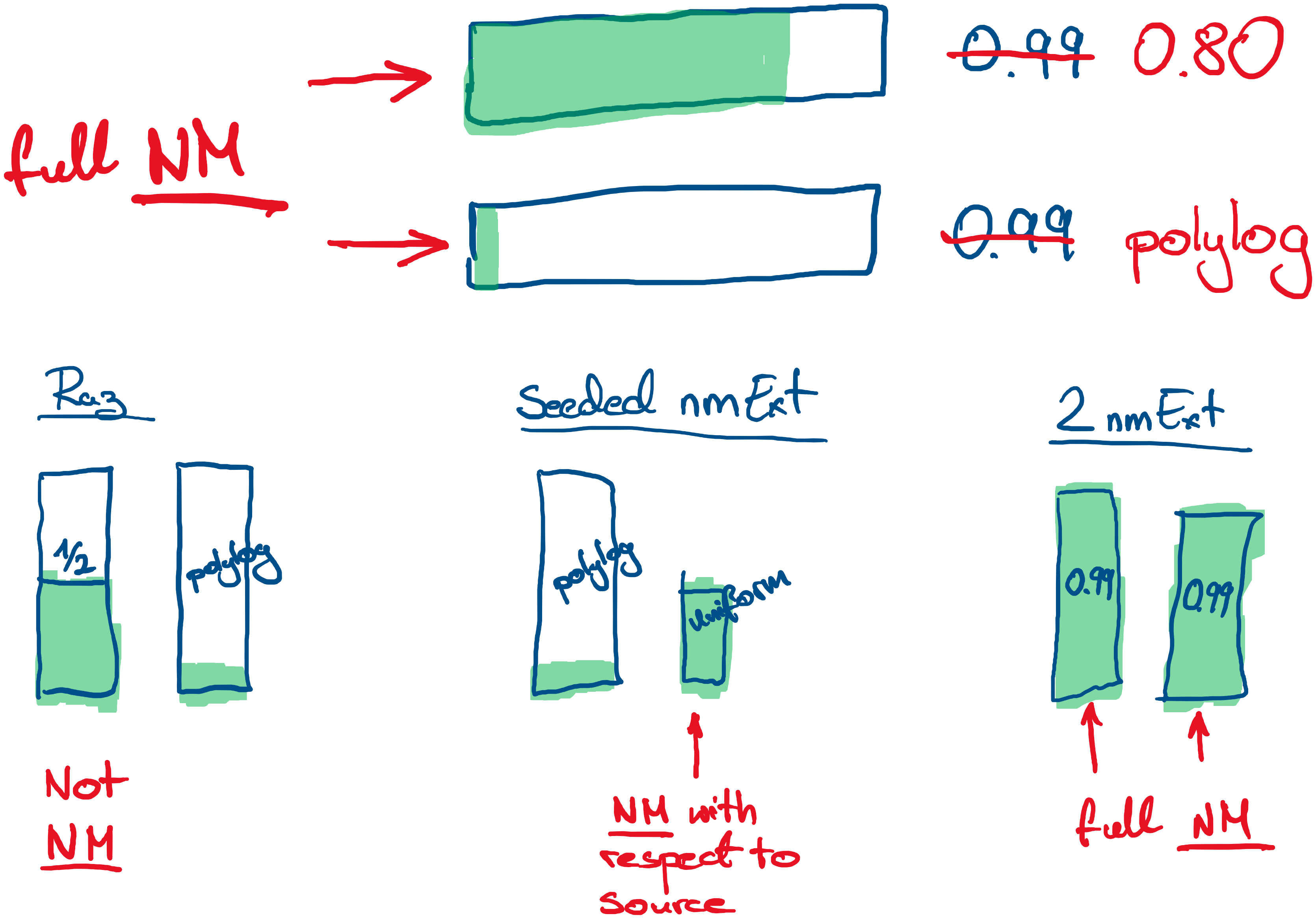
What we know NOW



Best of all Worlds



Best of all Worlds



A bit more history

Goyal, Srinivasan, Zhu '21 considered following

$$2\mathrm{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) =$$

A bit more history

Goyal, Srinivasan, Zhu '21 considered following

$$2\mathrm{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \mathrm{Li}(\qquad\qquad ; \boxed{Y_2})$$

A bit more history

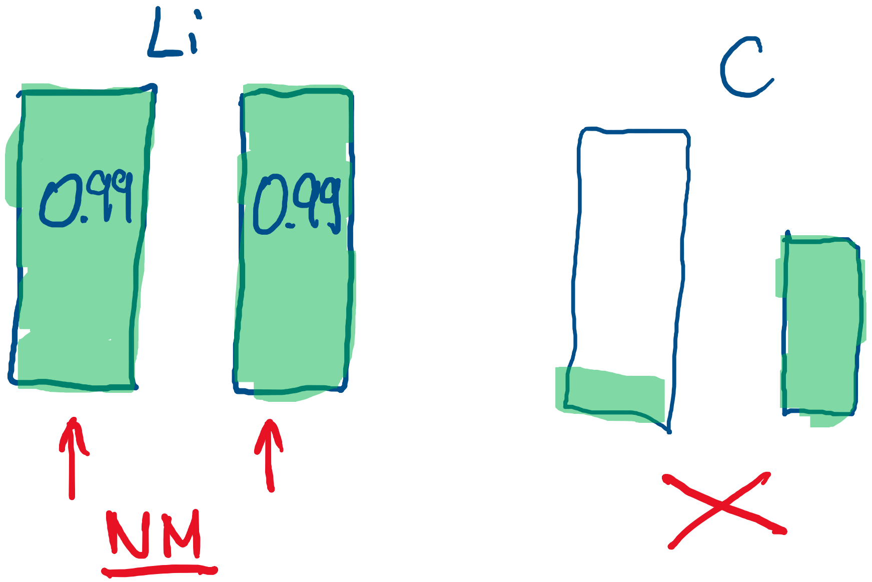
Goyal, Srinivasan, Zhu '21 considered following

$$2\mathrm{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \mathrm{Li}(C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2})$$

A bit more history

Goyal, Srinivasan, Zhu '21 considered following

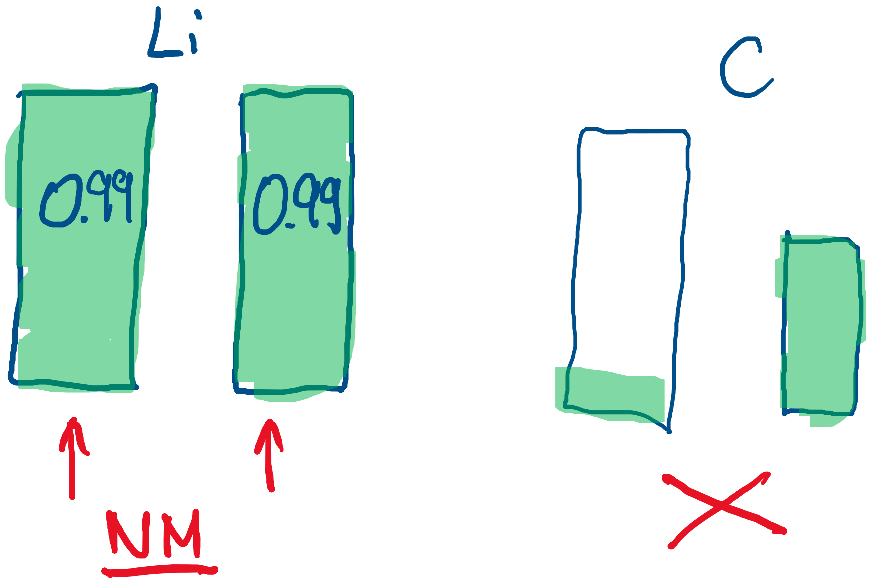
$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{Li}\left(C\left(\boxed{X}, \boxed{Y_1}\right); \boxed{Y_2}\right)$$



A bit more history

Goyal, Srinivasan, Zhu '21 considered following

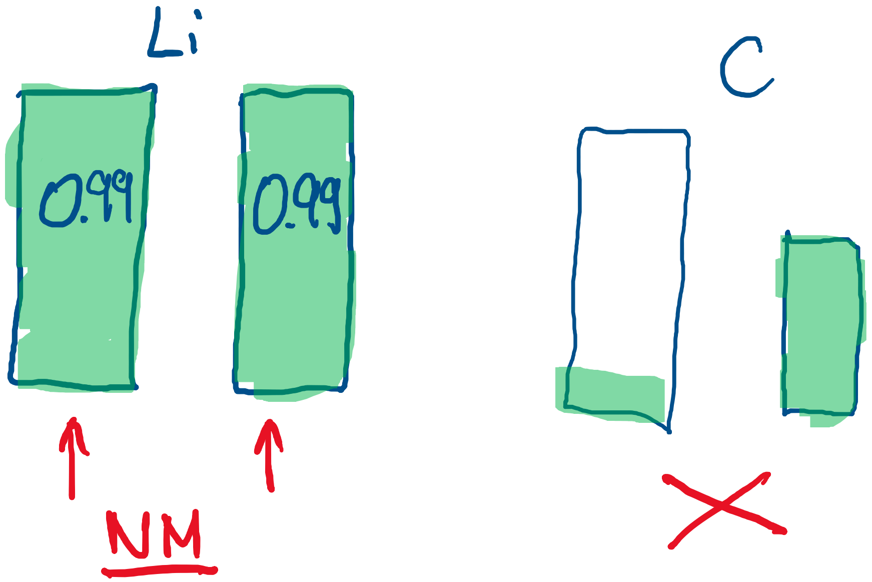
$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{Li}\left(C\left(\boxed{X}, \boxed{Y_1}\right); \boxed{Y_2}\right)$$



A bit more history

Goyal, Srinivasan, Zhu '21 considered following

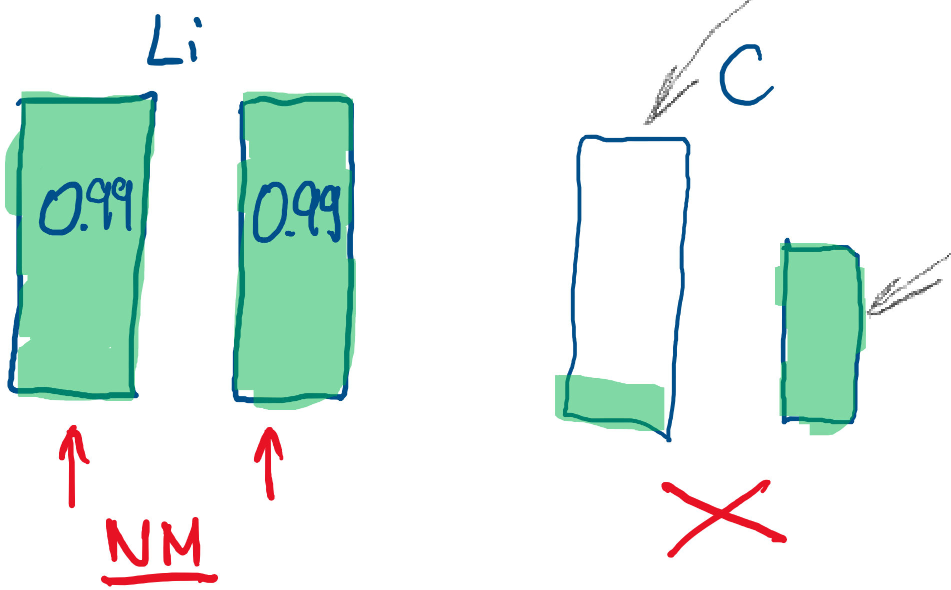
$$2\mathrm{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \mathrm{Li}(C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2})$$



A bit more history

Goyal, Srinivasan, Zhu '21 considered following

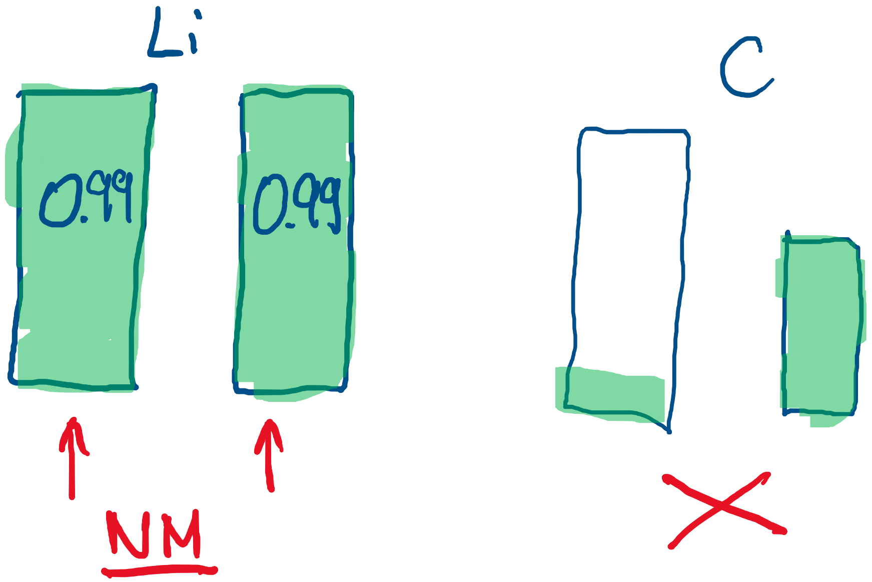
$$2\mathrm{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \mathrm{Li}(C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2})$$



A bit more history

Goyal, Srinivasan, Zhu '21 considered following

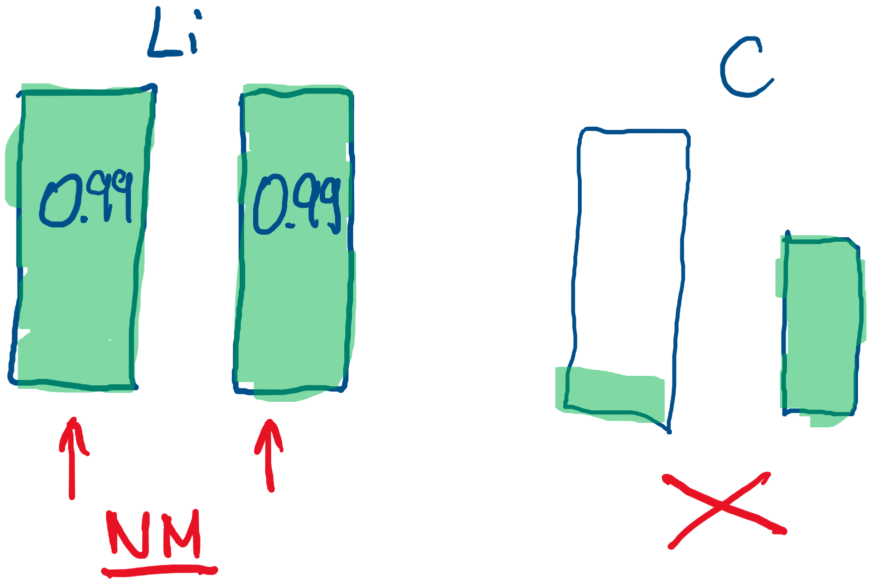
$$2\mathrm{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \mathrm{Li}(C(\boxed{X}, \boxed{Y_1}) ; \boxed{Y_2})$$



A bit more history

Goyal, Srinivasan, Zhu '21 considered following

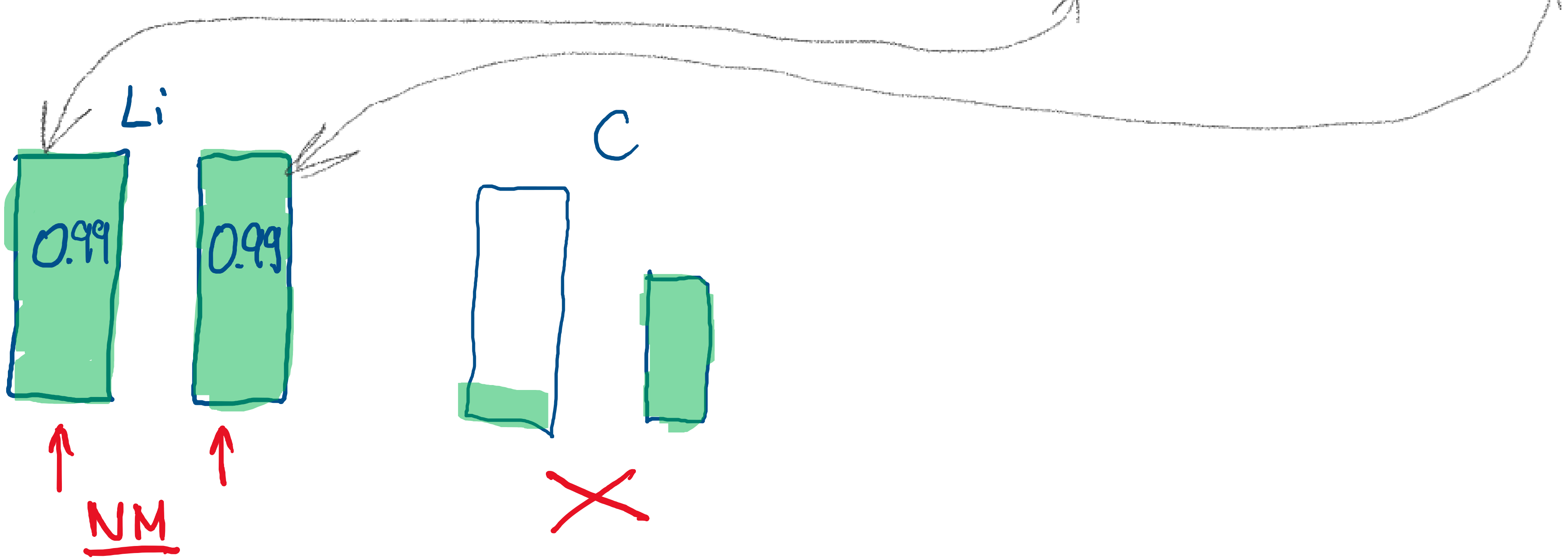
$$2\mathrm{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \mathrm{Li}(C(\boxed{X}, \boxed{Y_1}) ; \boxed{Y_2})$$



A bit more history

Goyal, Srinivasan, Zhu '21 considered following

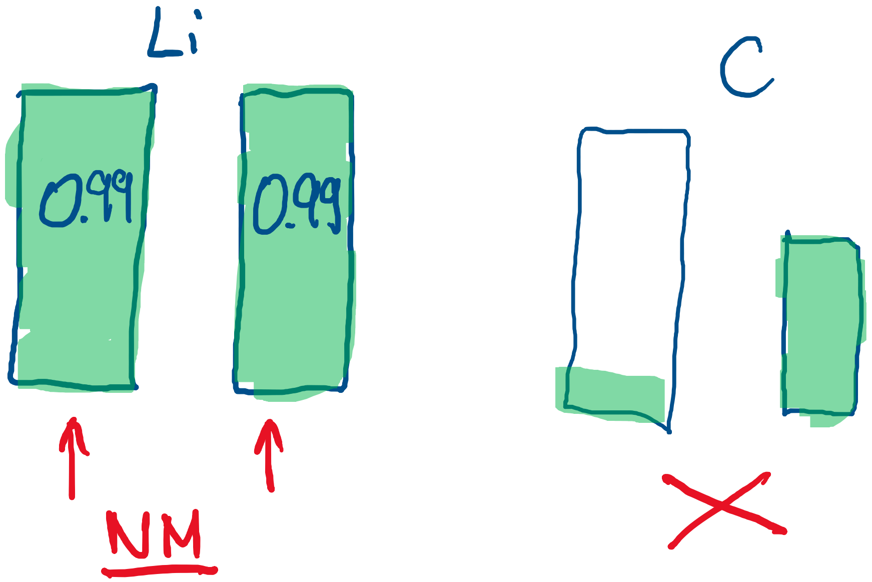
$$2\mathrm{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \mathrm{Li}(\boxed{C(\boxed{X}, \boxed{Y_1})}; \boxed{Y_2})$$



A bit more history

Goyal, Srinivasan, Zhu '21 considered following

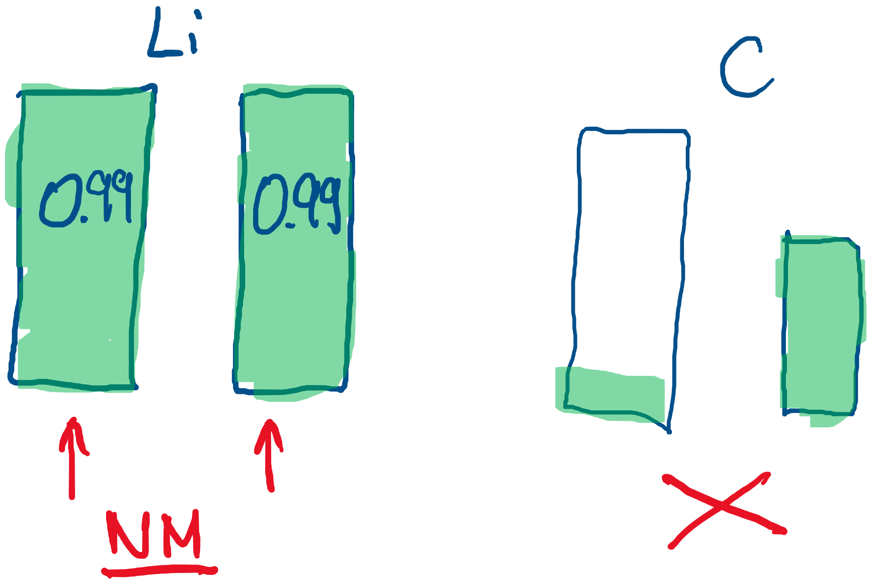
$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{Li}\left(C\left(\boxed{X}, \boxed{Y_1}\right); \boxed{Y_2}\right)$$



A bit more history

Goyal, Srinivasan, Zhu '21 considered following

$$2\mathrm{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \mathrm{Li}(C(\boxed{X}, \boxed{Y_1}) ; \boxed{Y_2})$$



Problem

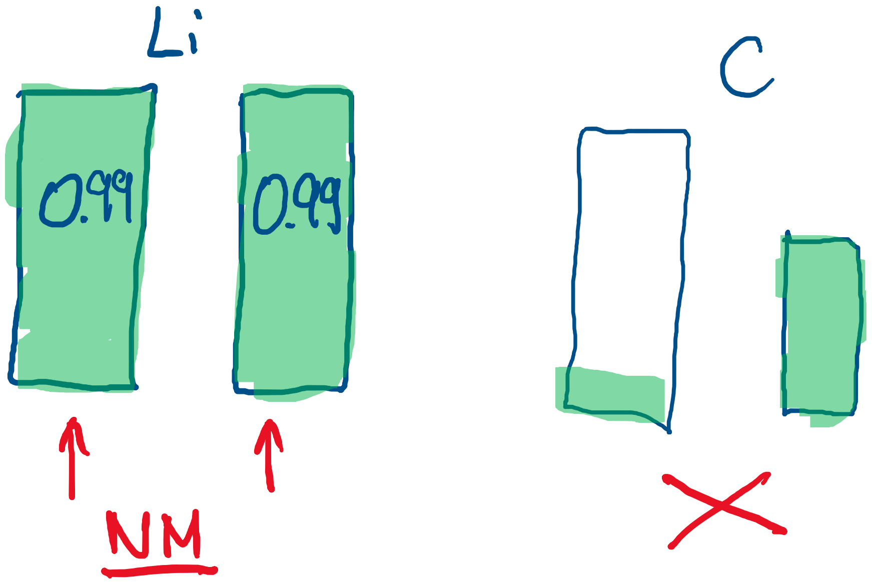
if $Y_1' \neq Y_1$

$X' \neq X$

A bit more history

Goyal, Srinivasan, Zhu '21 considered following

$$2\text{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \text{Li}\left(C(\boxed{X}, \boxed{Y_1}) ; \boxed{Y_2} \right)$$



Problem

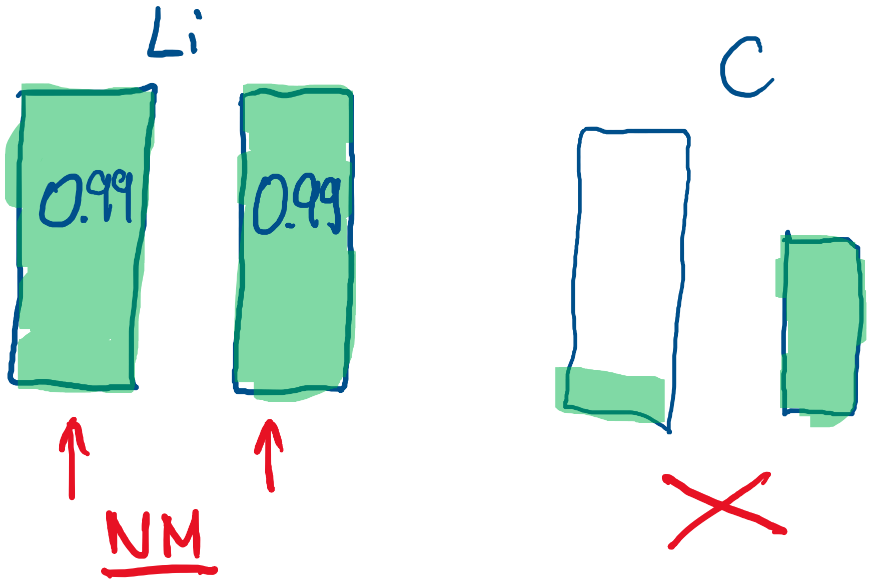
if $Y_1' \neq Y_1$ but $C(X', Y_1') = C(X, Y_1)$

$X' \neq X$ then

A bit more history

Goyal, Srinivasan, Zhu '21 considered following

$$2\text{NMExt}\left(\boxed{X},\ \boxed{Y_1 \| Y_2}\right) = \text{Li}\left(C\left(\boxed{X}, \boxed{Y_1}\right);\ \boxed{Y_2}\right)$$



Problem

if $Y_1' \neq Y_1$ but $C(X', Y_1') = C(X, Y_1)$

$X' \neq X$ then

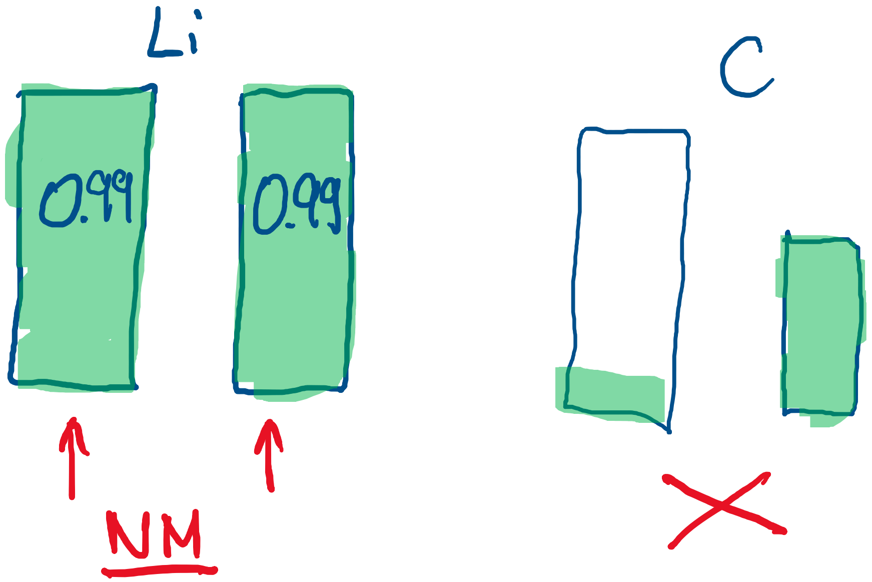
$Out' = Out.$

A bit more history

Goyal, Srinivasan, Zhu '21 considered following

also has to be uniform since Li doesn't tollerate low entropy.

$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{Li}\left(C\left(\boxed{X}, \boxed{Y_1}\right); \boxed{Y_2}\right)$$



Problem

if $Y_1' \neq Y_1$ but $C(X', Y_1') = C(X, Y_1)$

$X' \neq X$

then

$\mathrm{Out}' = \mathrm{Out}.$

GSZ transform with a twist(s)

Original

$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{Li}\left(C\left(\boxed{X}, \boxed{Y_1}\right); \boxed{Y_2} \right)$$

GSZ transform with a twist(s)

Original

$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{Li}\left(C\left(\boxed{X}, \boxed{Y_1}\right); \boxed{Y_2}\right)$$

Twist

$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = E\left(\qquad\qquad\qquad \right)$$

GSZ transform with a twist(s)

Original

$$\mathrm{2NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{Li}\left(C\left(\boxed{X}, \boxed{Y_1}\right); \boxed{Y_2}\right)$$

Twist

$$\mathrm{2NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = E\left(C\left(\boxed{X}, \boxed{Y_1}\right), \qquad \right)$$

GSZ transform with a twist(s)

Original

$$2\text{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \text{Li}\left(C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2}\right)$$

Twist

$$2\text{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = E\left(C(\boxed{X}, \boxed{Y_1}), \boxed{Y_1 \| Y_2}\right)$$

GSZ transform with a twist(s)

Original

$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{Li}\left(C\left(\boxed{X}, \boxed{Y_1}\right); \boxed{Y_2}\right)$$

Twist

Problem $C(X', Y_1') = C(X, Y_1)$

$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = E\left(C\left(\boxed{X}, \boxed{Y_1}\right), \boxed{Y_1 \| Y_2}\right)$$

GSZ transform with a twist(s)

Original

$$2NMExt(\boxed{X}, \boxed{Y_1 \| Y_2}) = Li(C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2})$$

Twist

Problem $C(X', Y_1') = C(X, Y_1)$

$$2NMExt(\boxed{X}, \boxed{Y_1 \| Y_2}) = E(C(\boxed{X}, \boxed{Y_1}), \boxed{Y_1 \| Y_2})$$

if $Y_1' \neq Y_1$ E will see it!

GSZ transform with a twist(s)

Original

$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{Li}\left(C\left(\boxed{X}, \boxed{Y_1}\right); \boxed{Y_2}\right)$$

Twist

Problem $C(X', Y_1') = C(X, Y_1)$

$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = E\left(C\left(\boxed{X}, \boxed{Y_1}\right), \boxed{Y_1 \| Y_2}\right)$$

Problem $C(X', Y_1) = C(X, Y_1)$

GS2 transform with a twist(s)

Original

$$2NMExt(\boxed{X}, \boxed{Y_1 \| Y_2}) = Li(C(\boxed{X}, \boxed{Y_1}); \boxed{Y_2})$$

Twist

Problem $C(X', Y_1') = C(X, Y_1)$

$$2NMExt(\boxed{X}, \boxed{Y_1 \| Y_2}) = E(C(\boxed{X}, \boxed{Y_1}), \boxed{Y_1 \| Y_2})$$

Problem

$$C(X', Y_1) = C(X, Y_1)$$

All we need is ~~love~~ Collision Resistance

Leftover Hash Lemma

- if $\mathbb{P}_{Y \leftarrow \$}\big(C(x_0, Y) = C(x_1, Y) \big)$ is tiny for all $x_0 \neq x_1$

  then C is a good Extractor!

Leftover Hash Lemma

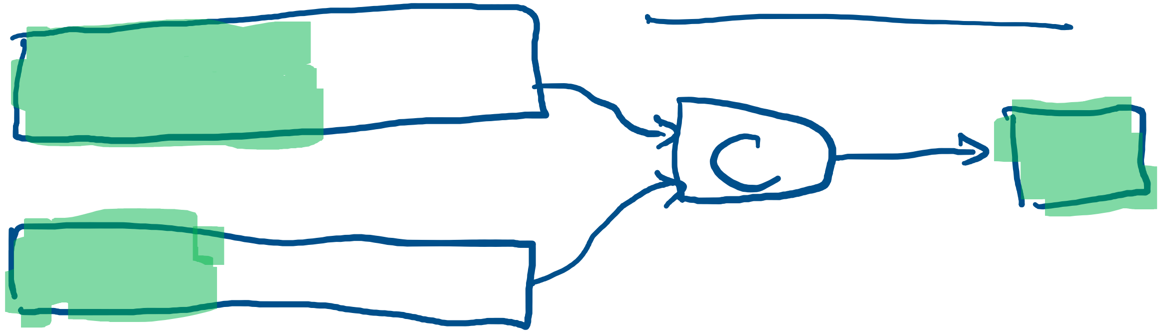
- if $\underset{Y \leftarrow \$}{\mathbb{P}}\big(C(x_0, Y) = C(x_1, Y) \big)$ is tiny for all $x_0 \neq x_1$

  then C is a good Extractor!

- Infact in [OS'18] we showed inverse is almost true too.

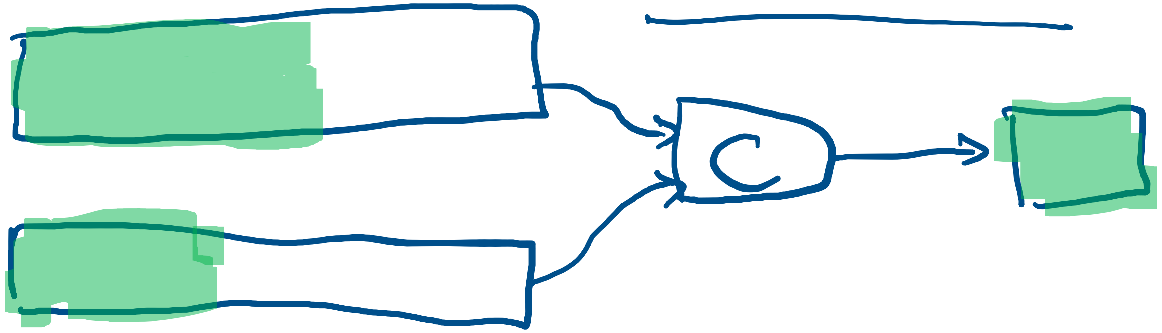
Collision Resilient Extractors.

Extraction



Collision Resilient Extractors.

Extraction



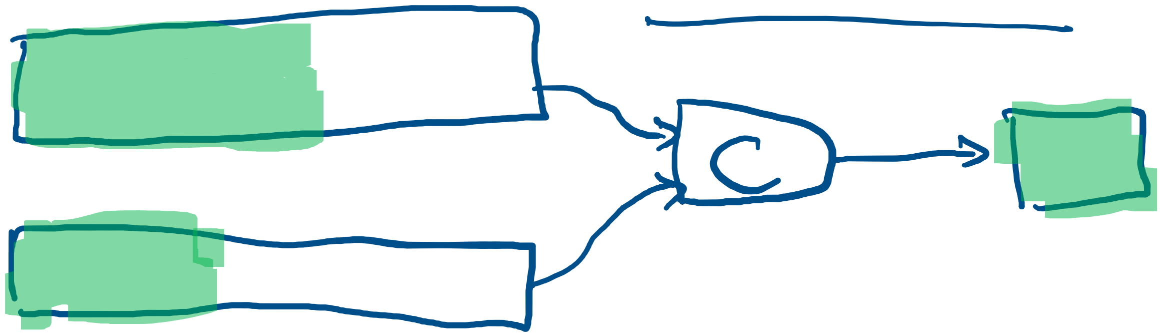
CR

$$\mathbb{P}_{Y \leftarrow \$}\left(C(X, Y) = C(X', Y)\right) \leq \text{tiny}$$

X and X'
are arbitrarly
correlated

Collision Resilient Extractors.

Extraction



CR

$$\mathbb{P}_{Y \leftarrow \$}\left(C(X,Y)=C(X',Y)\right) \le \text{tiny}$$

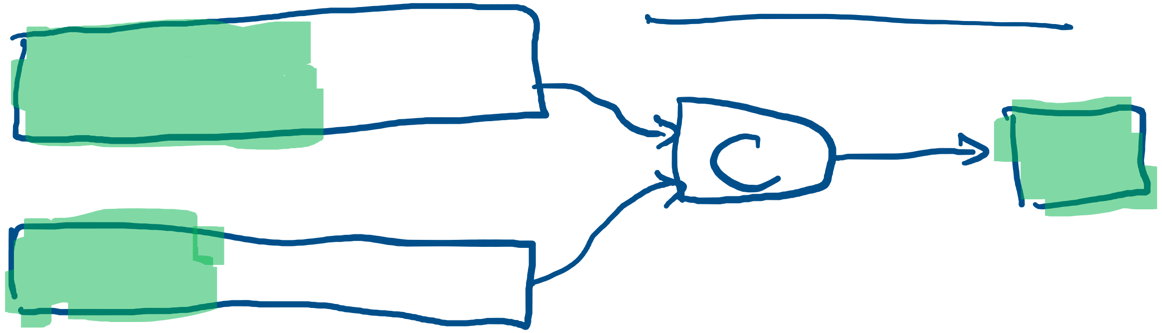
X

makes it even easier.

X and X' are arbitrarly correlated

Collision Resilient Extractors.

Extraction



CR

$$\mathbb{P}_{Y \leftarrow \$}\Big(C(X, Y) = C(X', Y)\Big) \leq \text{tiny}$$

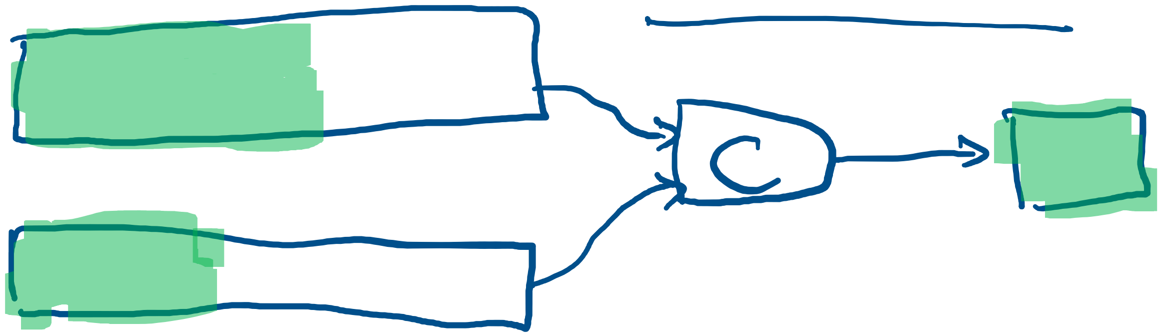
makes it even easier.

X and X' are arbitrarly correlated

What is CR:

Collision Resilient Extractors.

Extraction



CR

$$\mathbb{P}_{Y \leftarrow \$}\Big(C(X,Y)=C(X',Y)\Big) \leq \text{tiny}$$

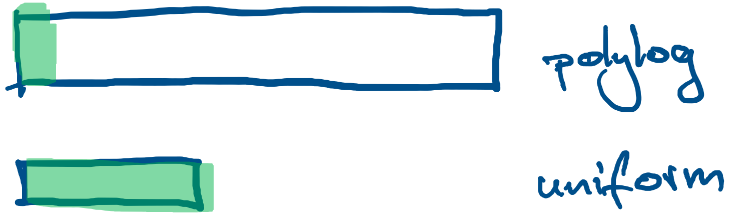
X

makes it even easier.

X and X' are arbitrarly correlated

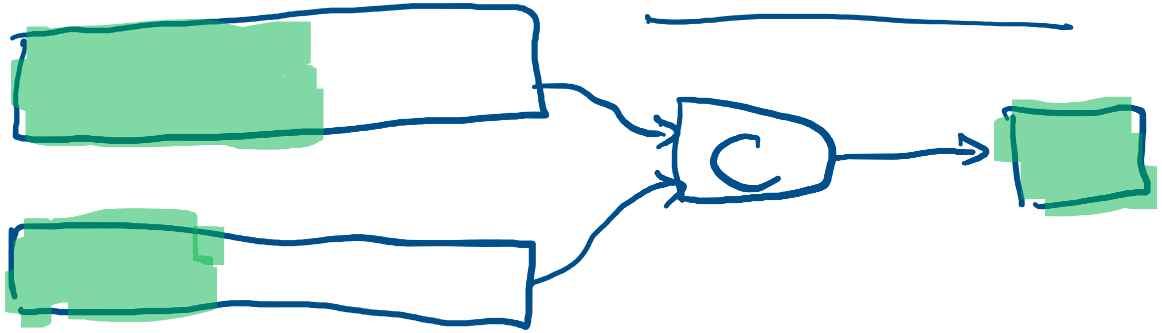
What is CR:

- Seeded Ext (can be compiled)



Collision Resilient Extractors.

Extraction



CR

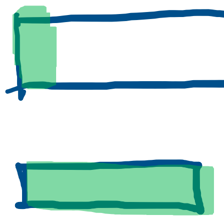
$$\mathop{\mathbb{P}}_{Y\leftarrow\$}\Big(C(X,Y)=C(X',Y)\Big)\le\text{tiny}$$

X makes it even easier.

X and X' are arbitrarly correlated

What is CR:

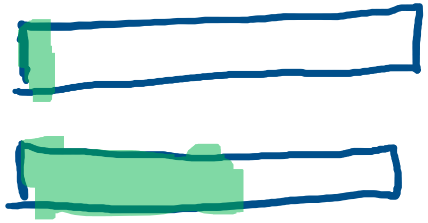
- Seeded Ext (can be compiled)



polylog

uniform

- Raz



polylog

$\frac{1}{2}$

Construction

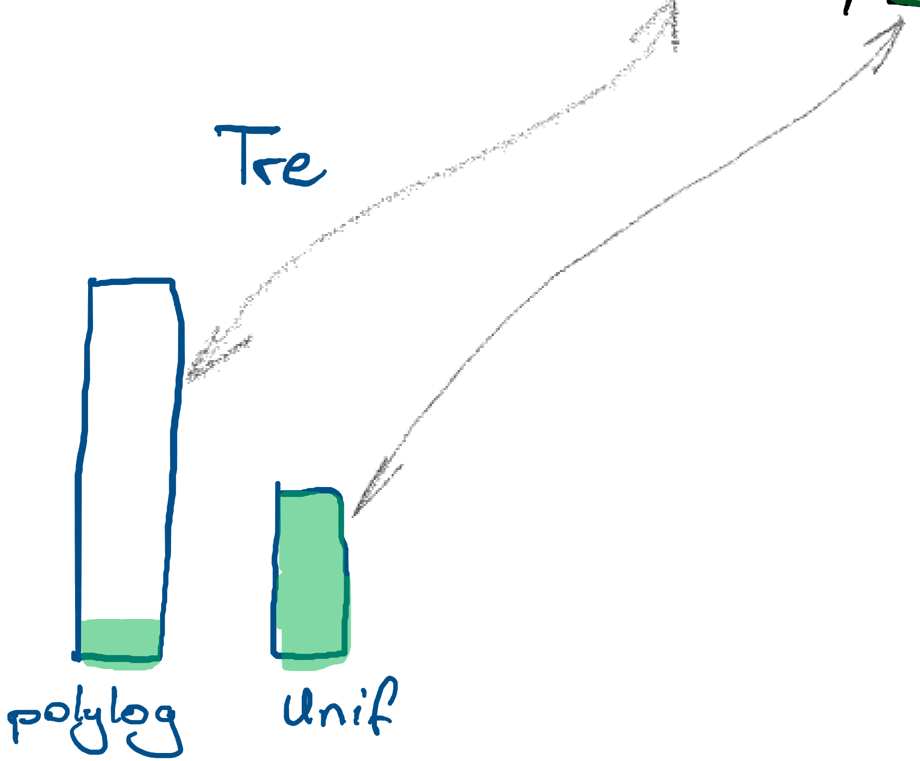
$$\underline{\mathrm{FNMExt}}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \underline{\mathrm{Li}}\left(\underline{\mathrm{Tre}}\left(\boxed{X}, \boxed{Y_1}\right), \boxed{Y_1 \| Y_2}\right)$$

Construction

$$\underline{\mathrm{FNMExt}}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \underline{\mathrm{Li}}\left(\underline{\mathrm{Tre}}\left(\boxed{X}, \boxed{Y_1}\right), \boxed{Y_1 \| Y_2}\right)$$

Construction

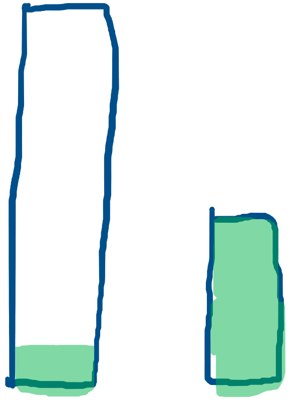
$$\mathrm{FNMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{Li}\left(\mathrm{Tre}\left(\boxed{X}, \boxed{Y_1}\right), \boxed{Y_1 \| Y_2}\right)$$



Construction

$$\underline{\mathrm{FNMExt}}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \underline{\mathrm{Li}}\left(\underline{\mathrm{Tre}}\left(\boxed{X}, \boxed{Y_1}\right), \boxed{Y_1 \| Y_2}\right)$$

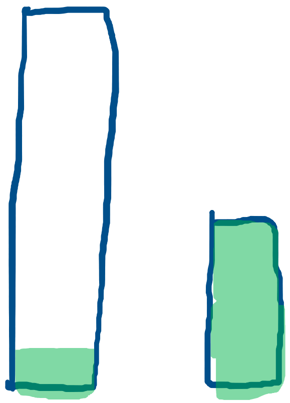
Tre



Construction

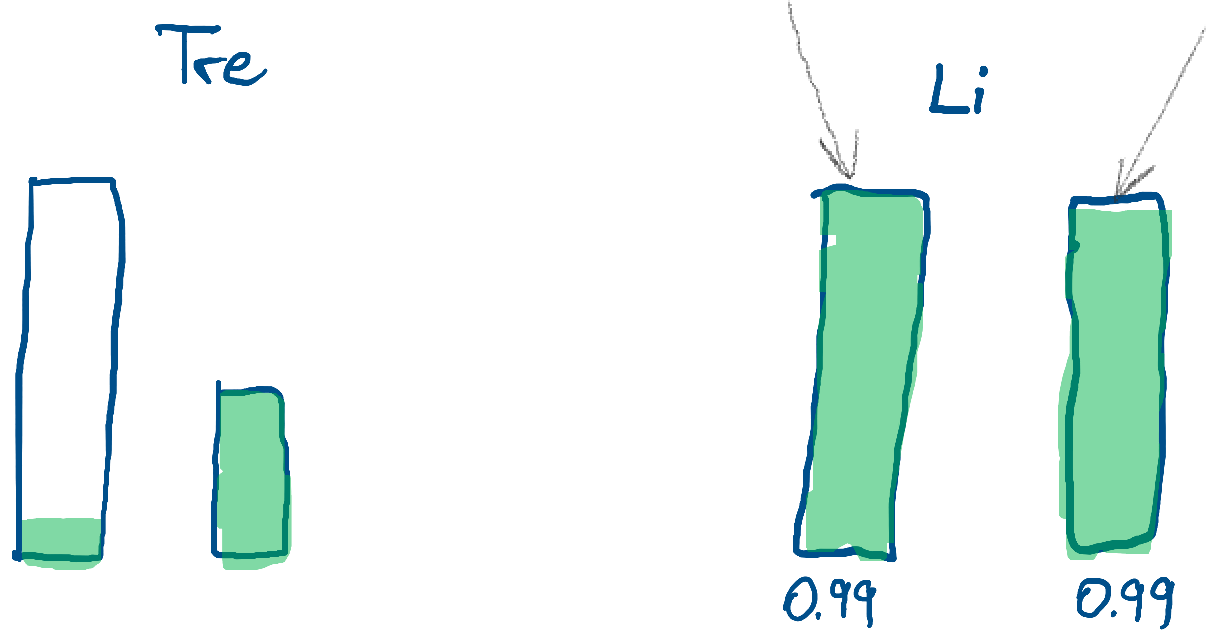
$$\underline{\mathrm{FNMExt}}\left(\boxed{x}, \boxed{Y_1 \| Y_2}\right) = \underline{\mathrm{Li}}\left(\underline{\mathrm{Tre}}\left(\boxed{x}, \boxed{Y_1}\right), \boxed{Y_1 \| Y_2}\right)$$

Tre



Construction

$$\underline{\mathrm{FNMExt}}\left(\boxed{x}, \boxed{Y_1 \| Y_2}\right) = \underline{\mathrm{Li}}\left(\underline{\mathrm{Tre}}\left(\boxed{x}, \boxed{Y_1}\right), \boxed{Y_1 \| Y_2}\right)$$

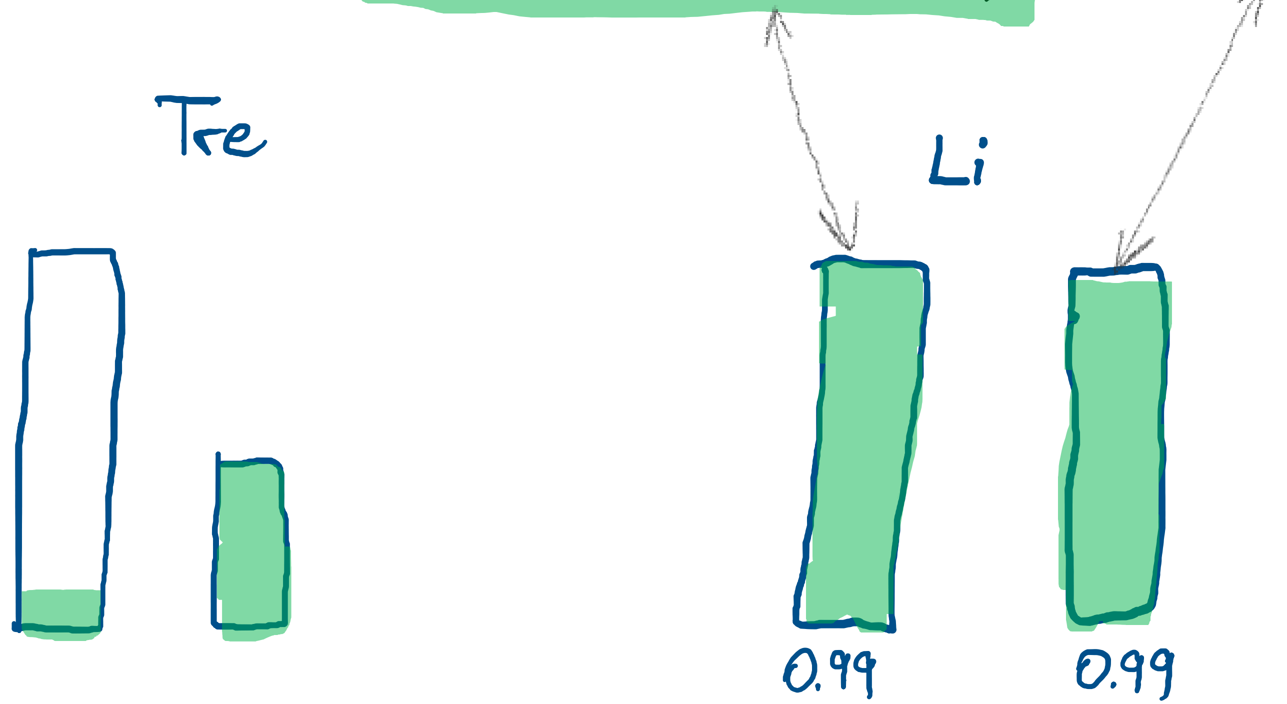


Construction

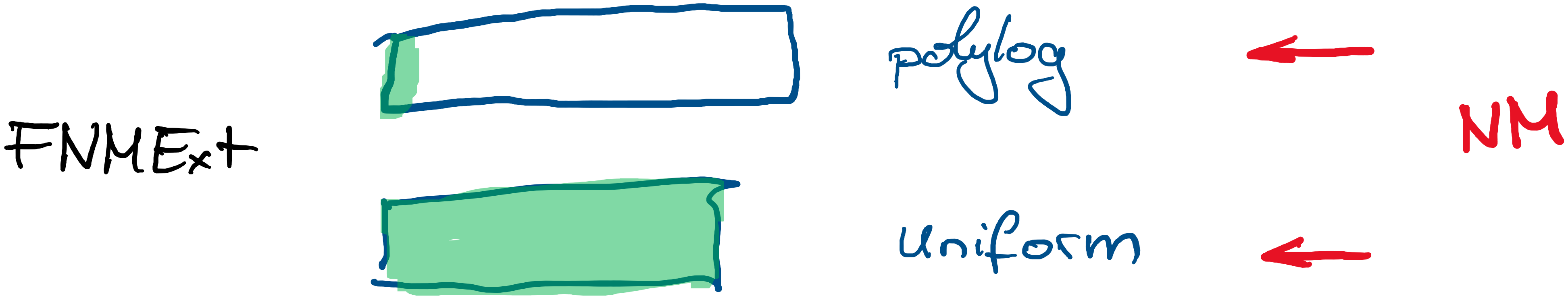
$$\underline{\mathrm{FNMExt}}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \underline{\mathrm{Li}}(\underline{\mathrm{Tre}}(\boxed{X}, \boxed{Y_1}), \boxed{Y_1 \| Y_2})$$

gives NonMalleability

gives low entropy of X.



Construction



Construction

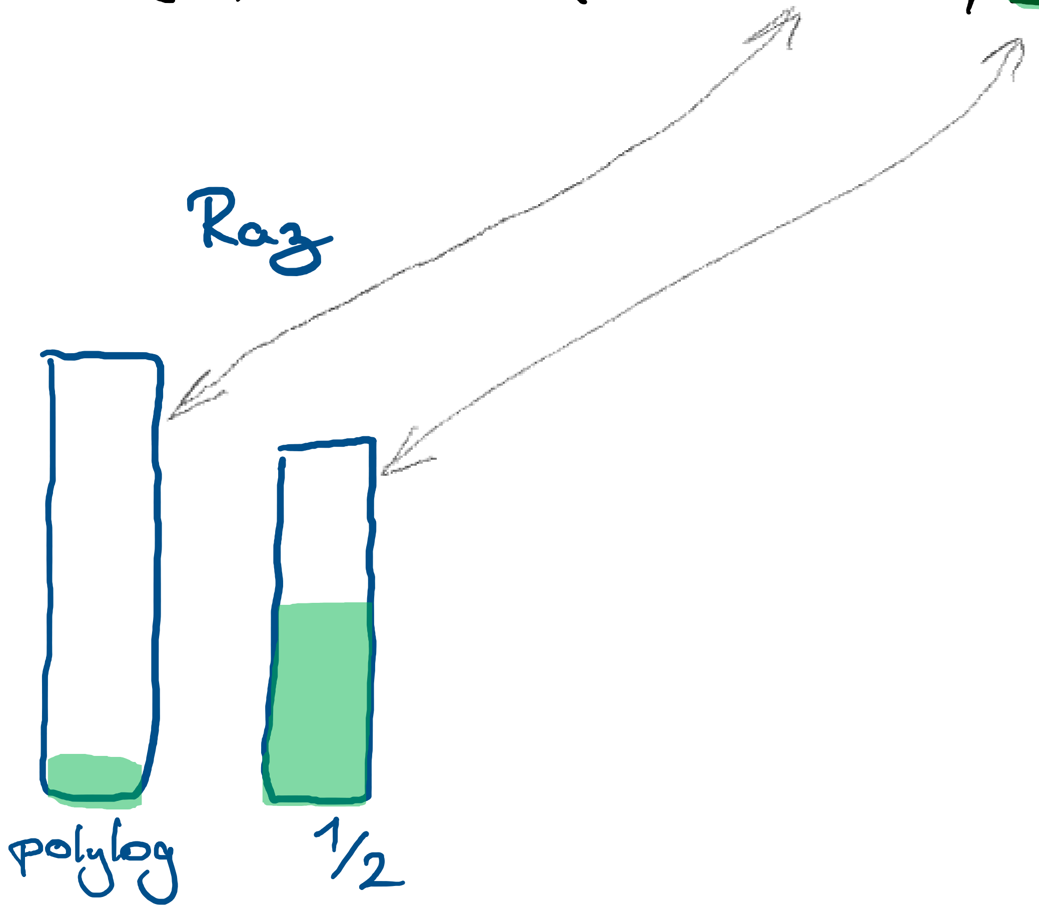
$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{FNMExt}\left(\mathrm{Raz}\left(\boxed{X}, \boxed{Y_1}\right), \boxed{Y_1 \| Y_2}\right)$$

Construction

$$\mathrm{2NMExt}\left(\boxed{X},\ \boxed{Y_1 \| Y_2}\right) = \mathrm{FNMExt}\left(\mathrm{Raz}\left(\boxed{X},\ \boxed{Y_1}\right),\ \boxed{Y_1 \| Y_2}\right)$$

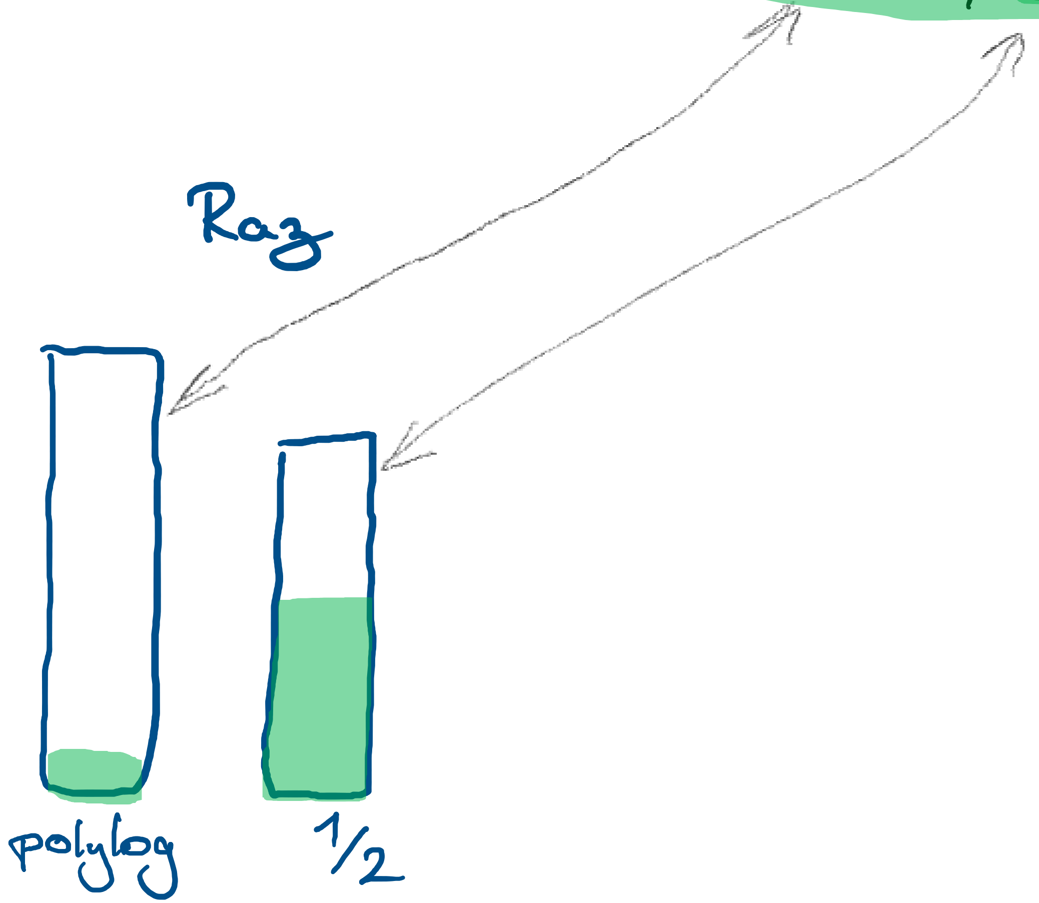
Construction

$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{FNMExt}\left(\mathrm{Raz}\left(\boxed{X}, \boxed{Y_1}\right), \boxed{Y_1 \| Y_2}\right)$$



Construction

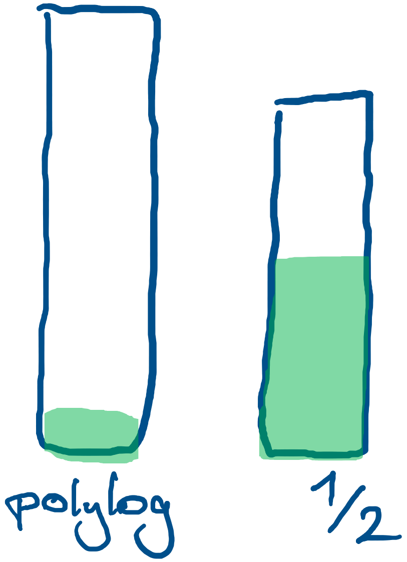
$$2\mathrm{NMExt}\left(\boxed{\;X\;},\ \boxed{Y_1 \| Y_2}\right) = \mathrm{FNMExt}\left(\mathrm{Raz}\left(\boxed{\;X\;},\ \boxed{Y_1\;}\right),\ \boxed{Y_1 \| Y_2}\right)$$



Construction

$$2\mathrm{NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{FNMExt}\left(\mathrm{Raz}\left(\boxed{X}, \boxed{Y_1}\right), \boxed{Y_1 \| Y_2}\right)$$

Raz

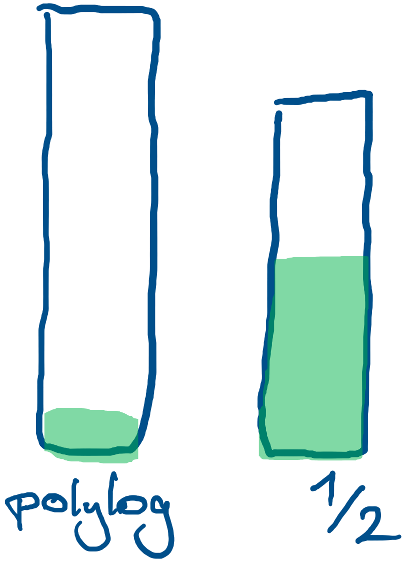


Construction

$$2\text{NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \text{FNMExt}(\text{Raz}(\boxed{X}, \boxed{Y_1}), \boxed{Y_1 \| Y_2})$$

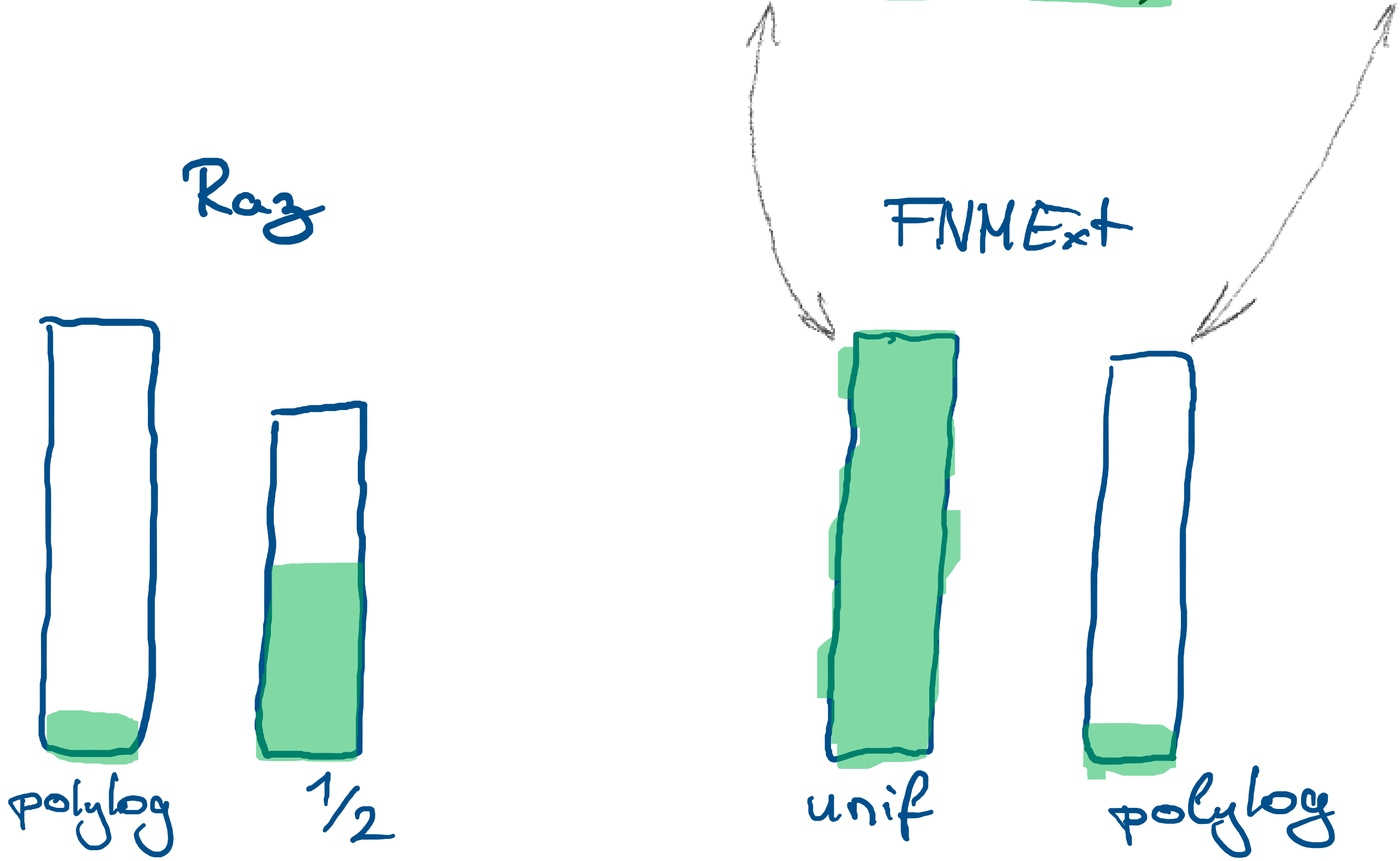
Entropy in Y_1 has been „used up" so there is little left.

Raz



Construction

$$\mathrm{2NMExt}\left(\boxed{X}, \boxed{Y_1 \| Y_2}\right) = \mathrm{FNMExt}\left(\mathrm{Raz}\left(\boxed{X}, \boxed{Y_1}\right), \boxed{Y_1 \| Y_2}\right)$$

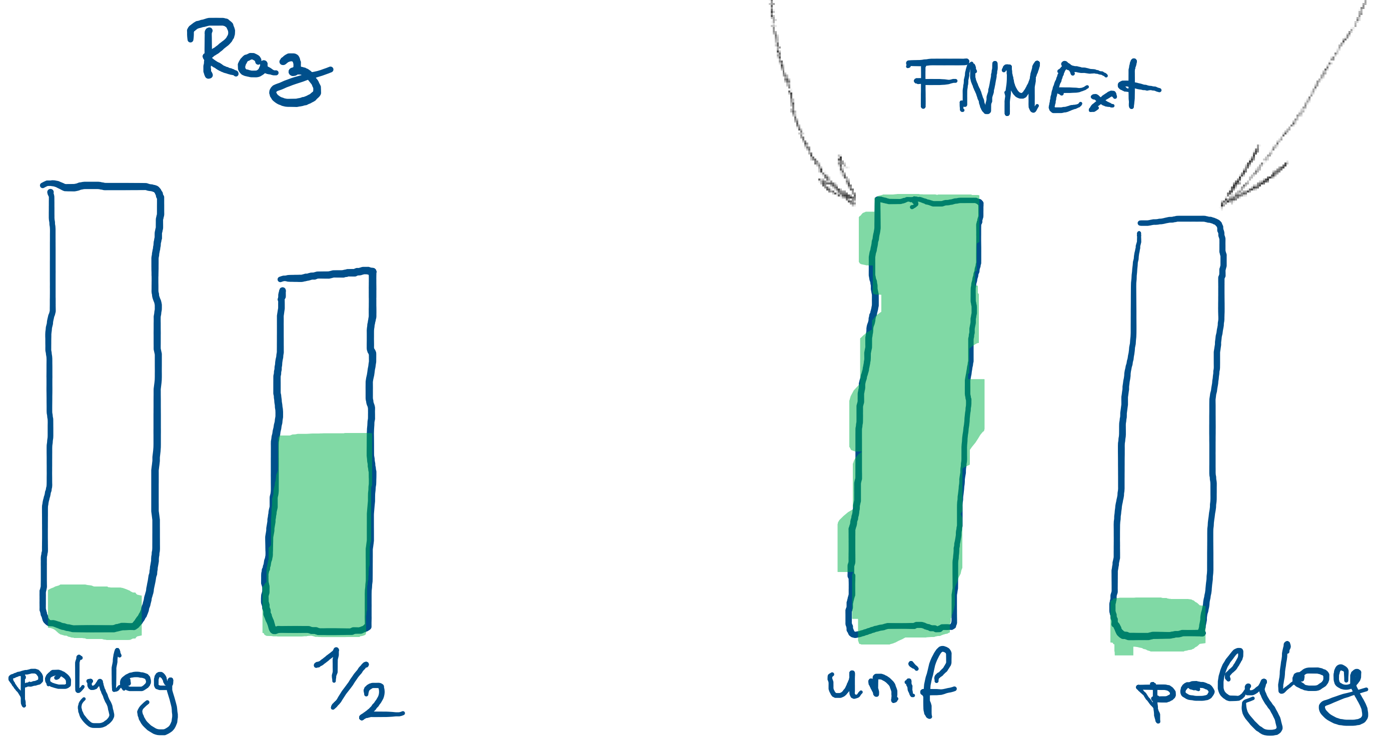


Construction

gives NonMalleability

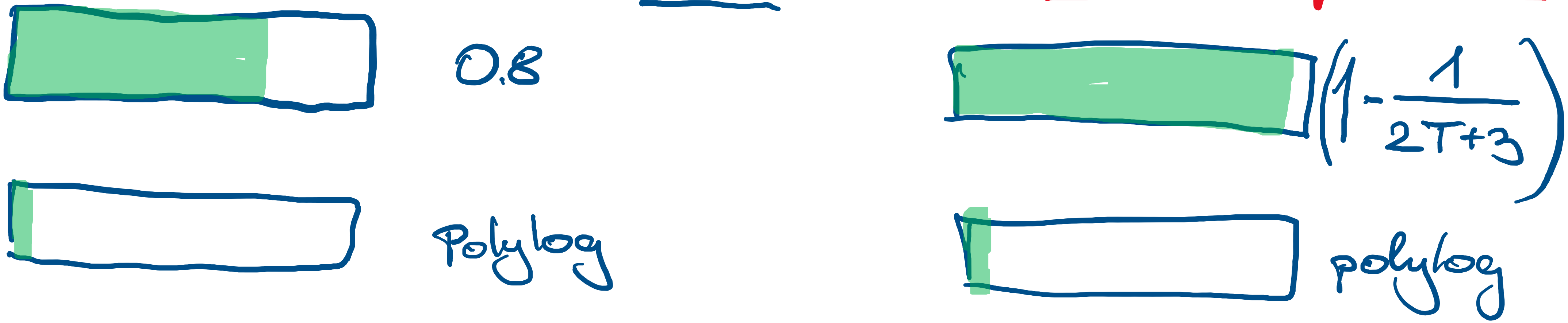
allows for lower entropies

$$\mathrm{2NMExt}(\boxed{X}, \boxed{Y_1 \| Y_2}) = \mathrm{FNMExt}(\mathrm{Raz}(\boxed{X}, \boxed{Y_1}), \boxed{Y_1 \| Y_2})$$



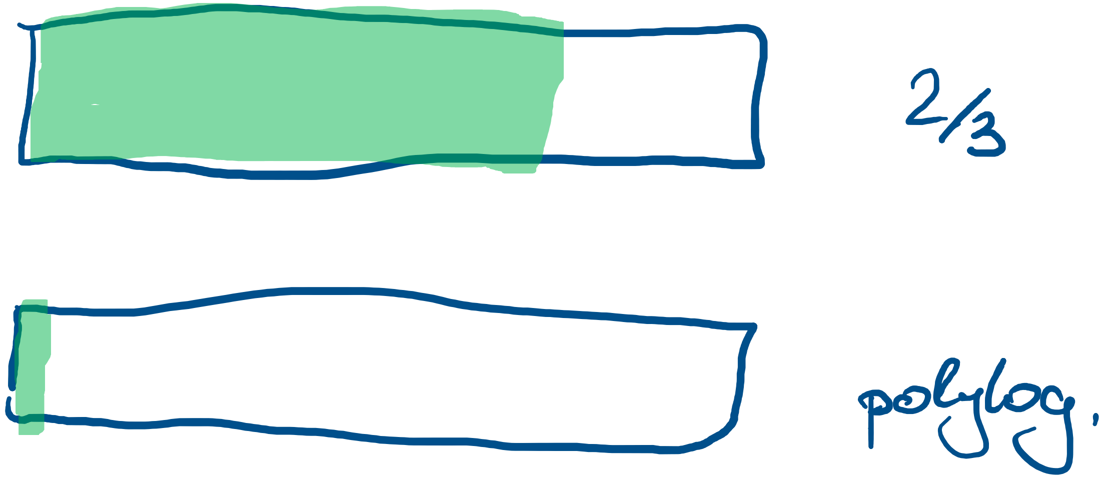
Final Result

Full NM — And — T-Multitamper NM



Subsequent Work

Li :



single tampering.

Why Care?

Why Care ?

2NMExt are cool tools:

NMC

Privacy Amplification

Network Extraction

Leak Resi
Tamper Resi

NM Secret Sharing

Why Care?

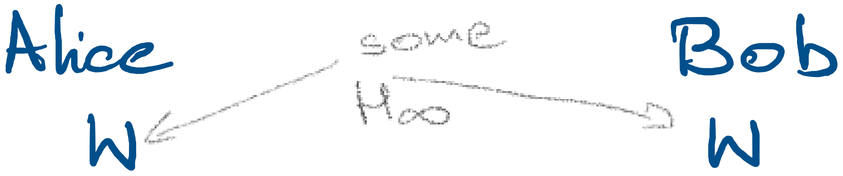
2NMExt are cool tools:

Privacy Amplification

Why Care ?

2NMExt are cool tools:

Privacy Amplification



Alice

Bob

W

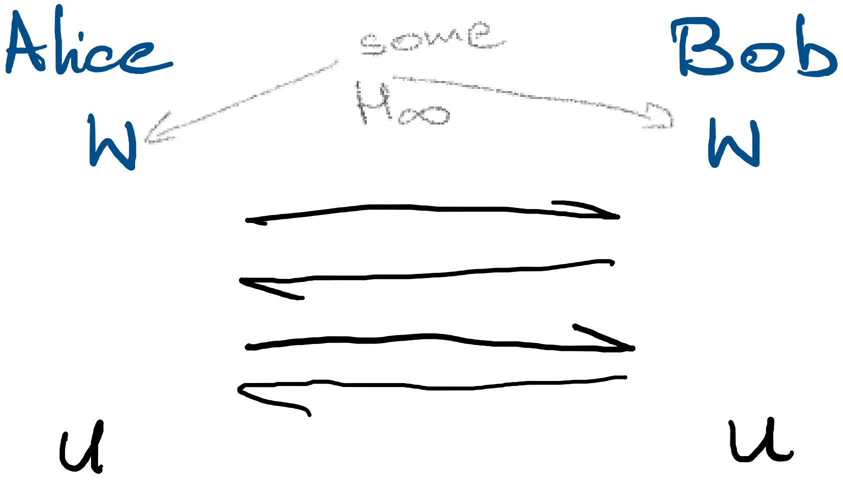
some H_∞

W

Why Care?

2NMExt are cool tools:

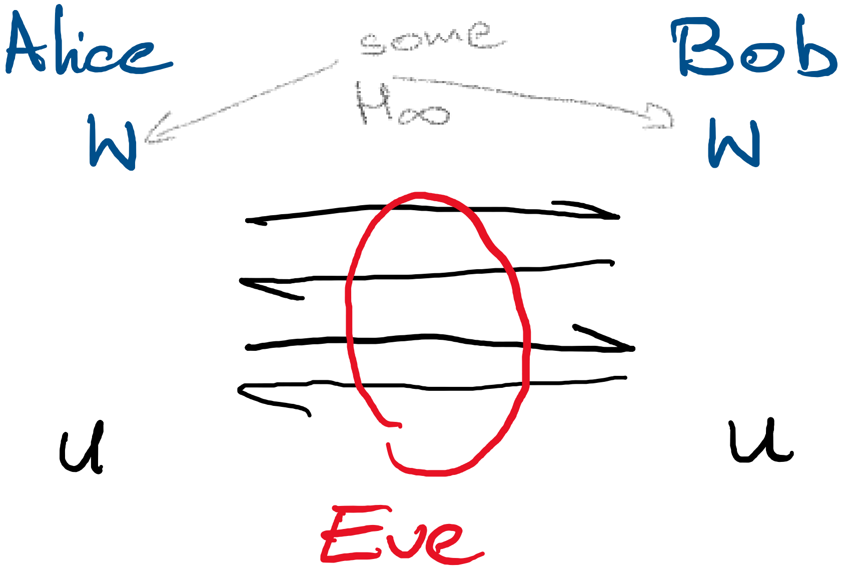
Privacy Amplification



Why Care?

2NMExt are cool tools:

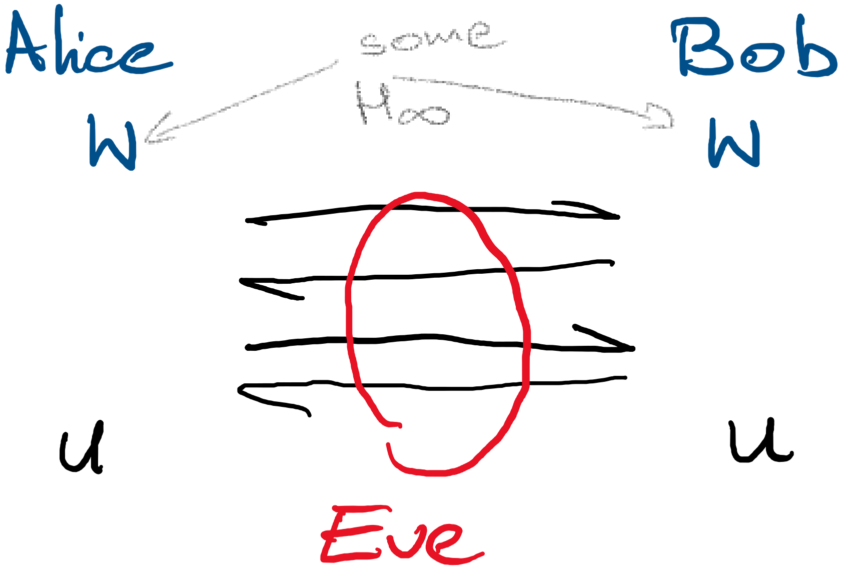
Privacy Amplification



Why Care?

2NMExt are cool tools:

Privacy Amplification

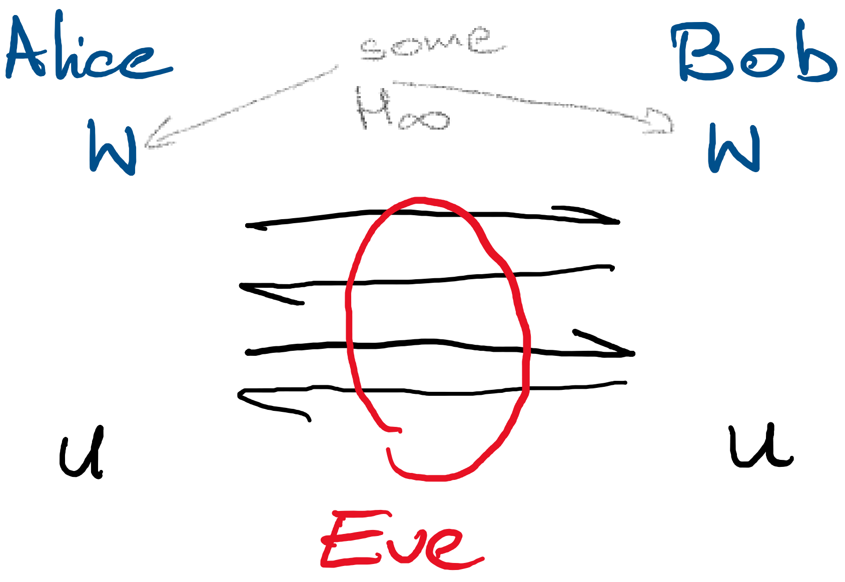


Seeded nmExt

Why Care ?

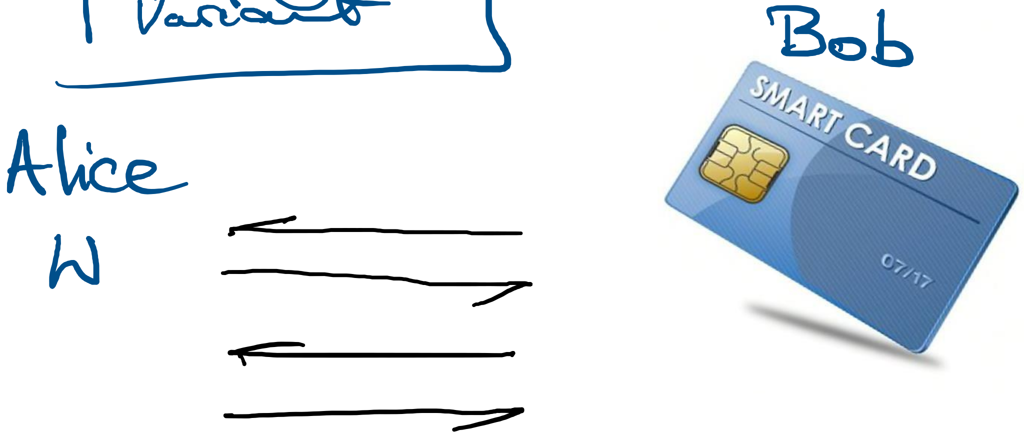
2NMExt are cool tools:

Privacy Amplification



Seeded nmExt

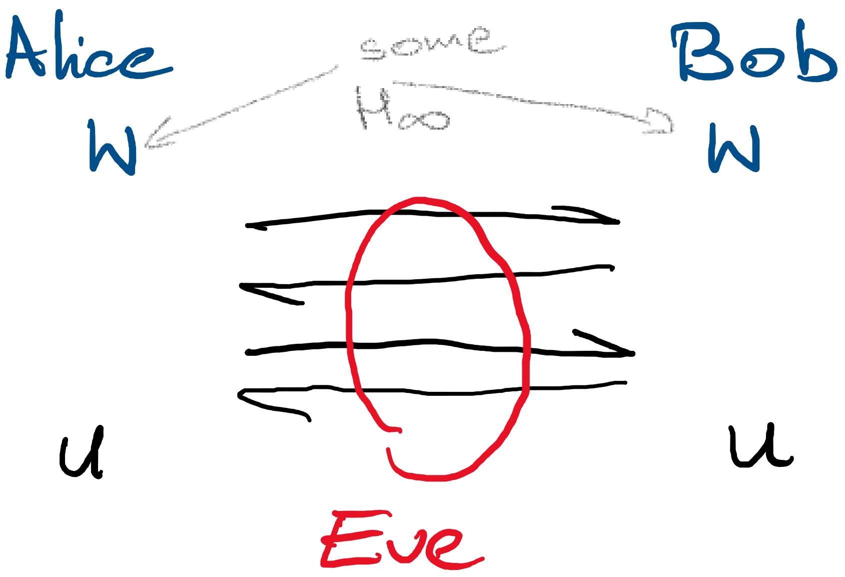
Stronger Variant



Why Care?

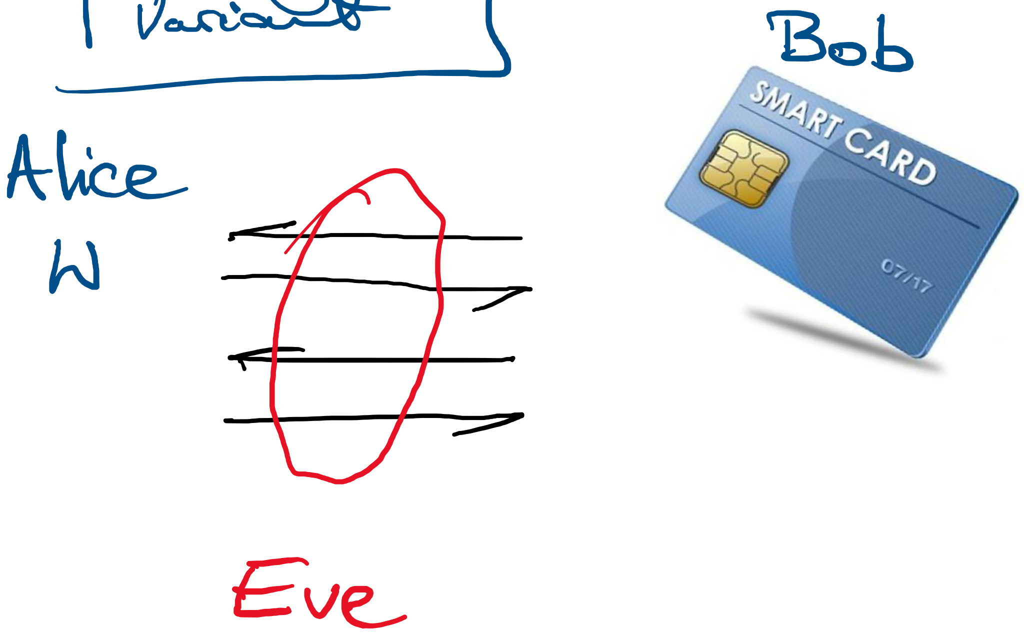
2NMExt are cool tools:

Privacy Amplification



Seeded nmExt

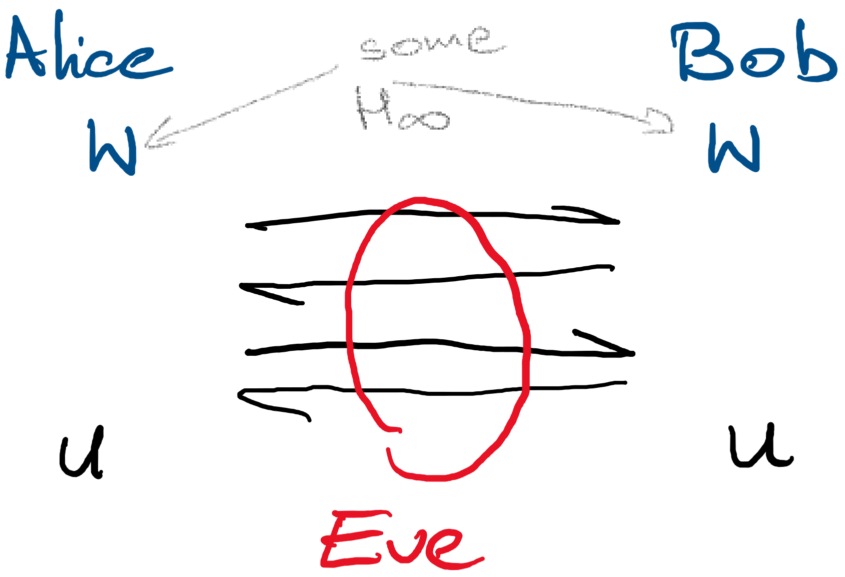
Stronger Variant



Why Care?

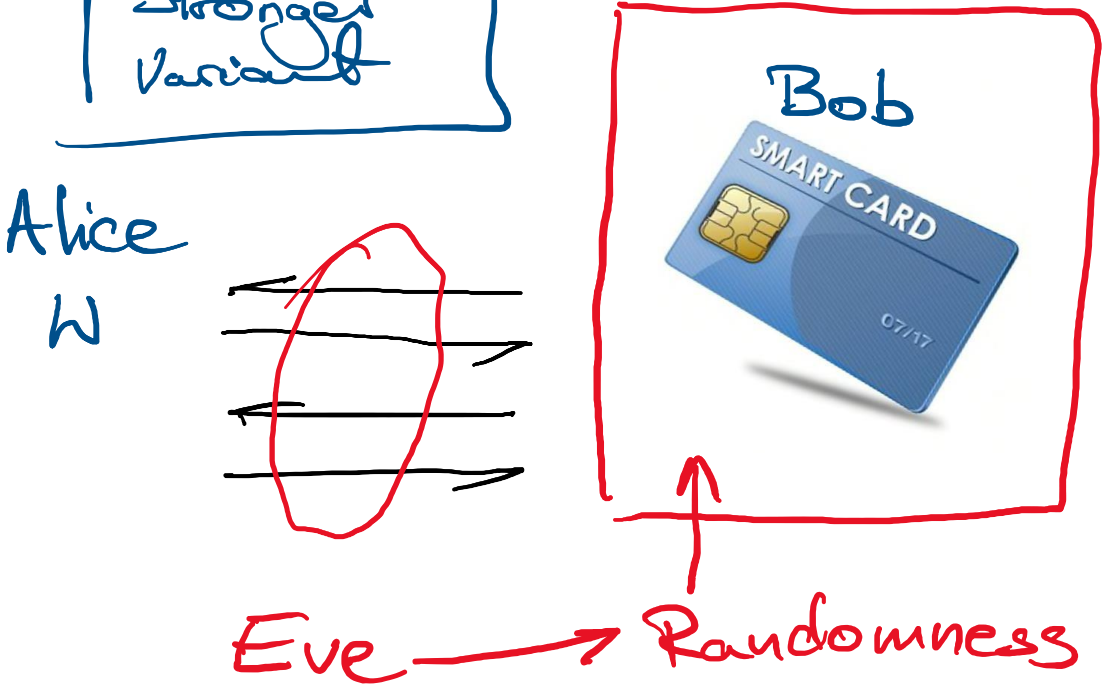
2NMExt are cool tools:

Privacy Amplification



Seeded nmExt

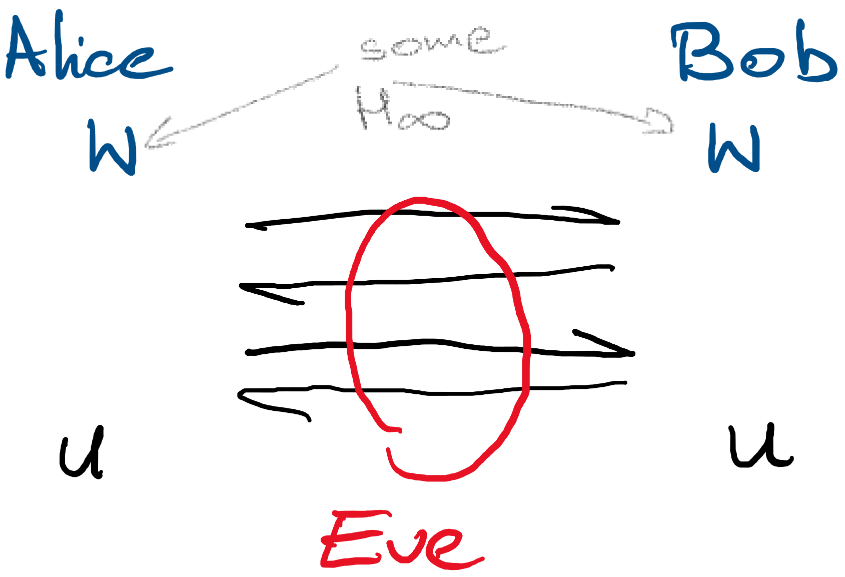
Stronger Variant



Why Care ?

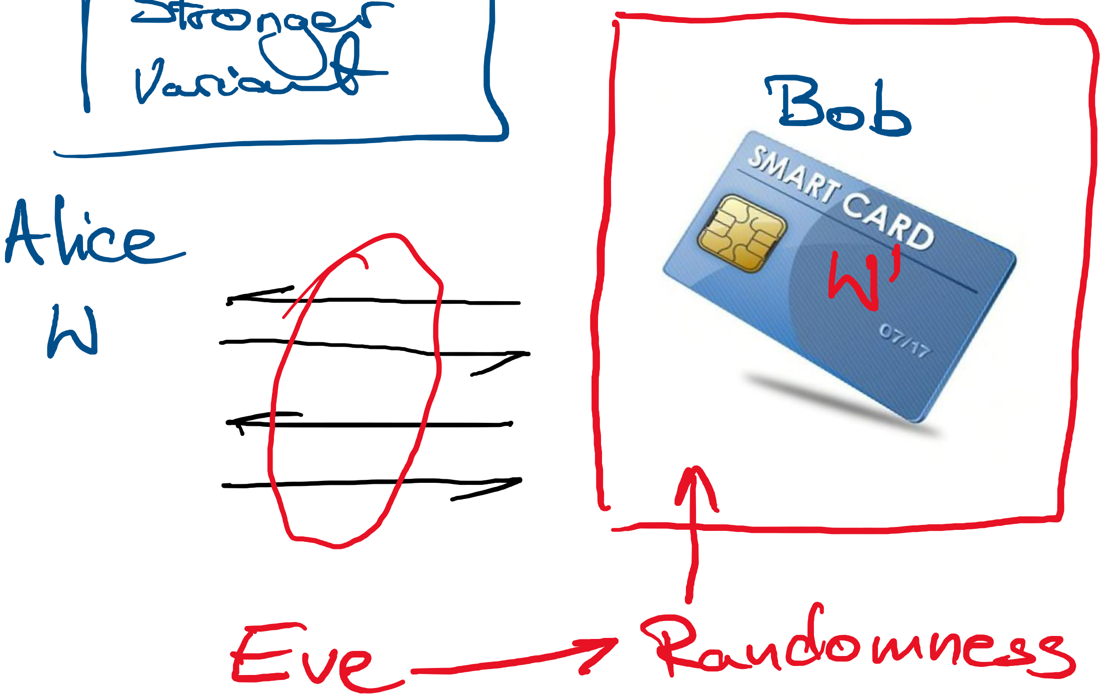
2NMExt are cool tools:

Privacy Amplification



Seeded nmExt

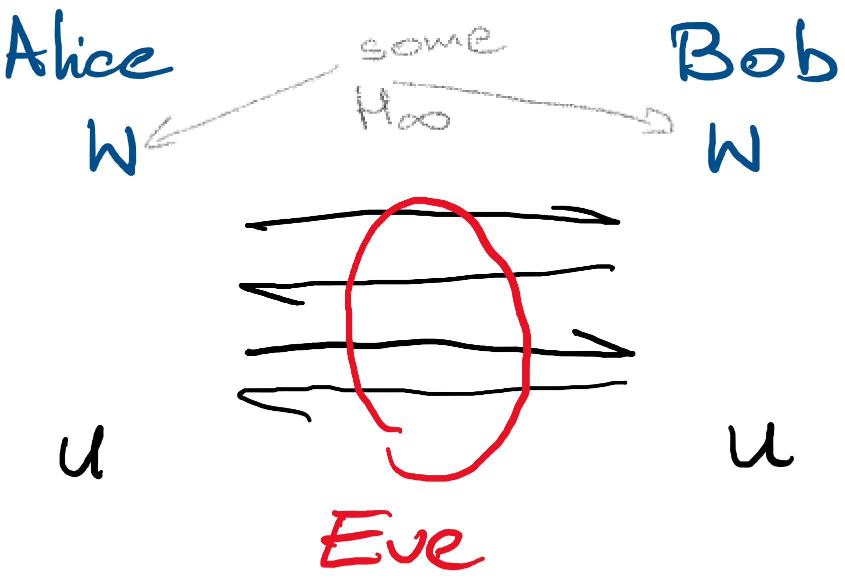
Stronger Variant



Why Care?

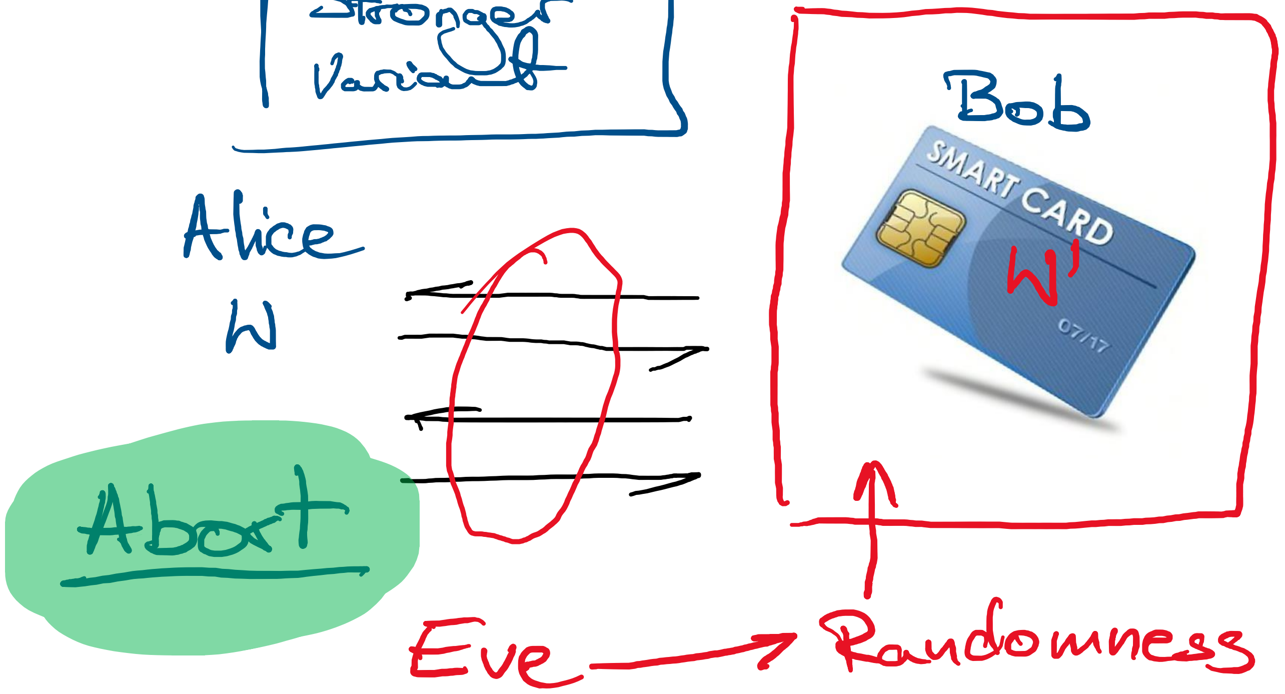
2NMExt are cool tools:

Privacy Amplification



Seeded nmExt

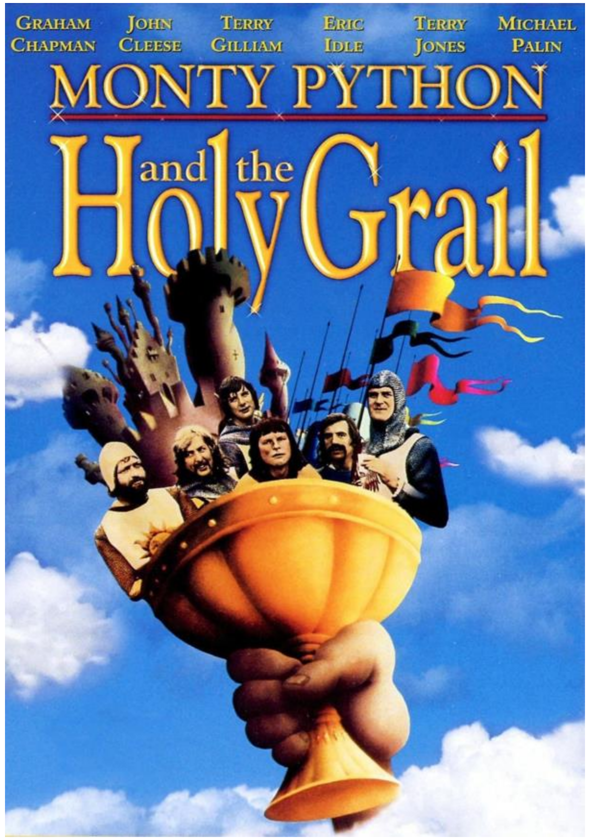
Stronger Variant



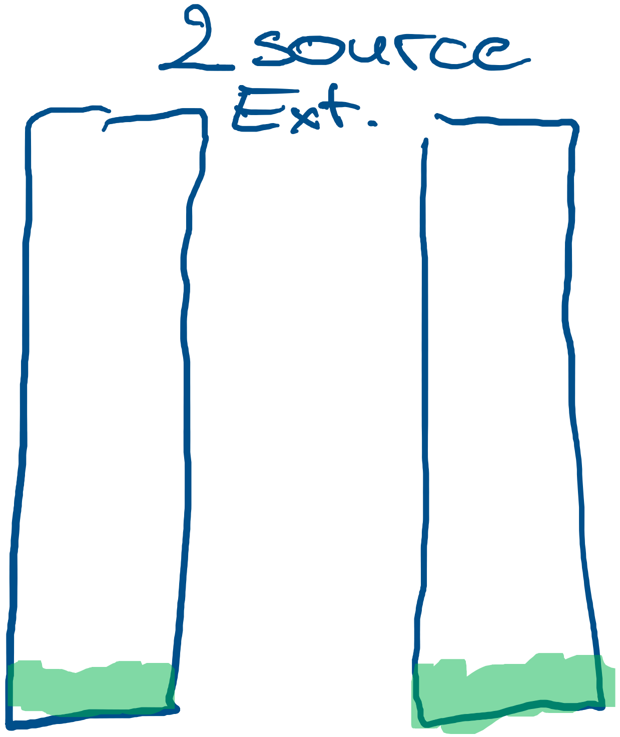
2nmExt

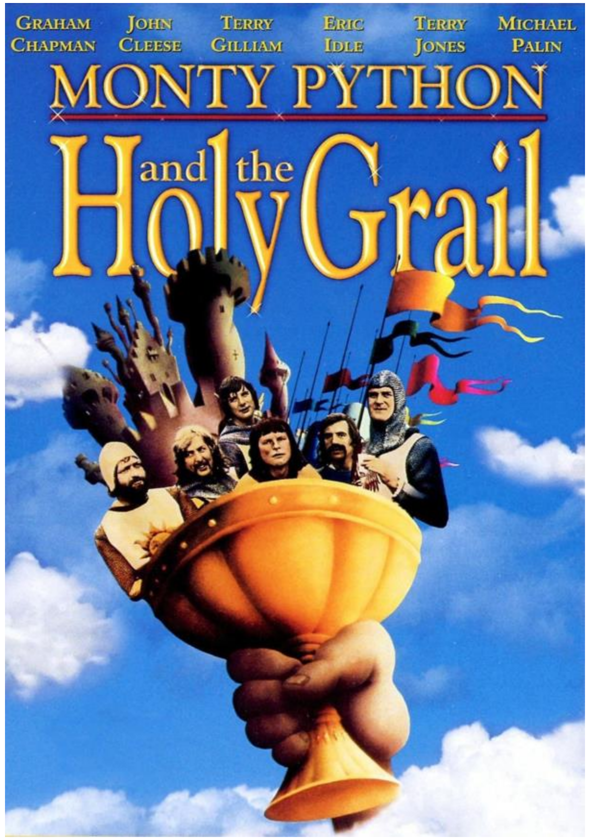
Why I care

Why I care


GRAHAM CHAPMAN
JOHN CLEESE
TERRY GILLIAM
ERIC IDLE
TERRY JONES
MICHAEL PALIN
MONTY PYTHON
and the Holy Grail

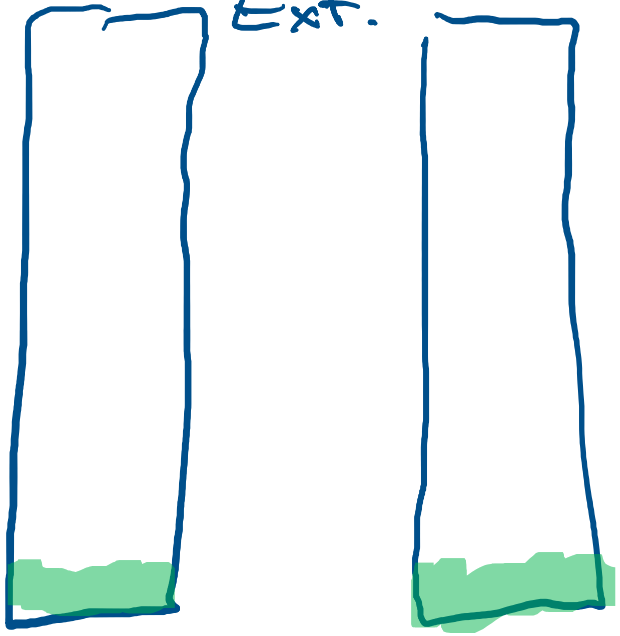
Why I care

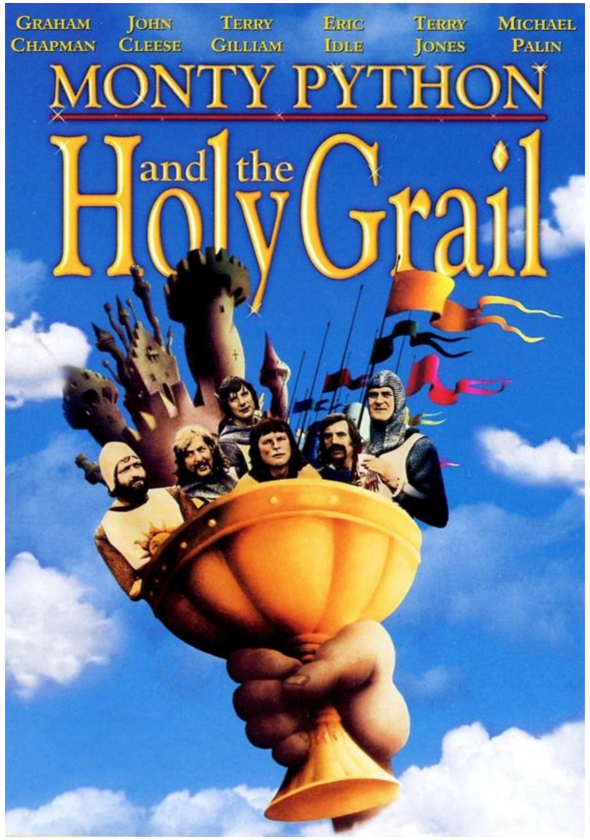

2 source
Ext.


GRAHAM CHAPMAN
JOHN CLEESE
TERRY GILLIAM
ERIC IDLE
TERRY JONES
MICHAEL PALIN
MONTY PYTHON
and the Holy Grail

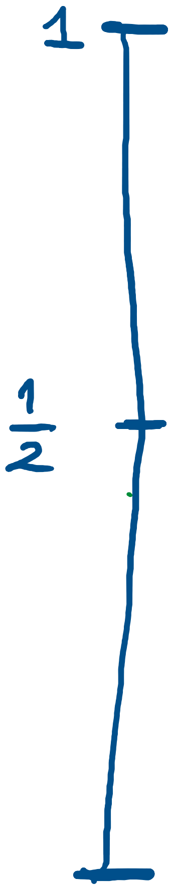
Why I care

2 source Ext.



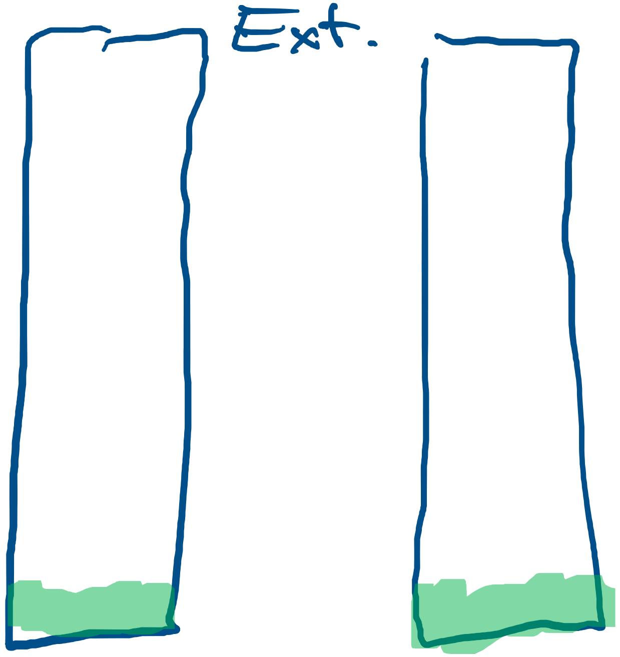


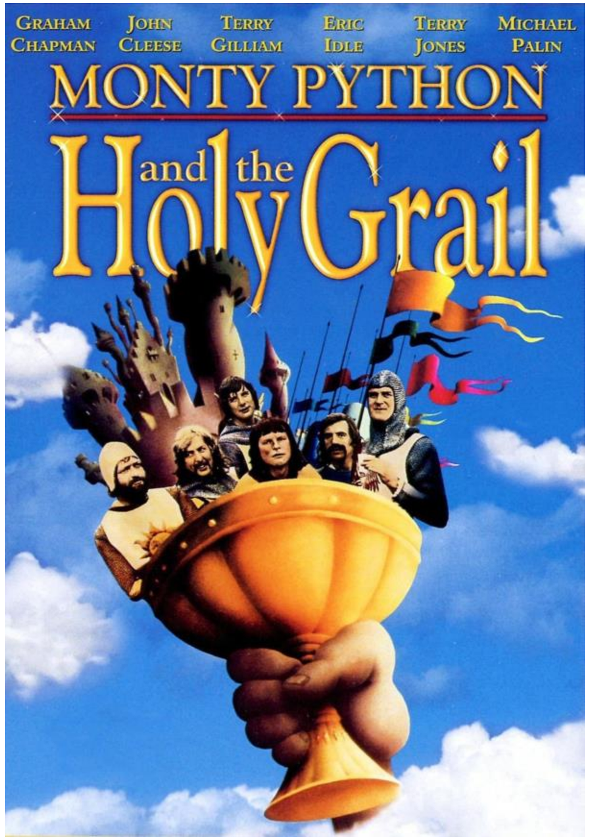
Entropy Rate



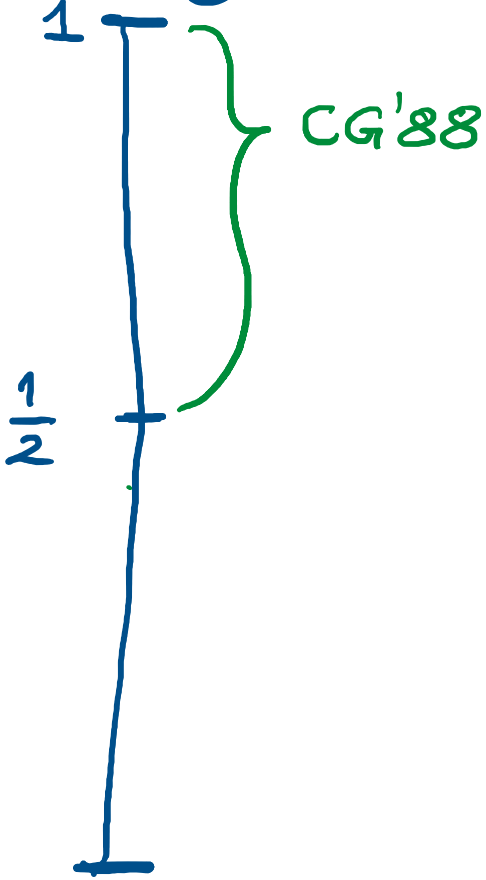
Why I care

2 source Ext.



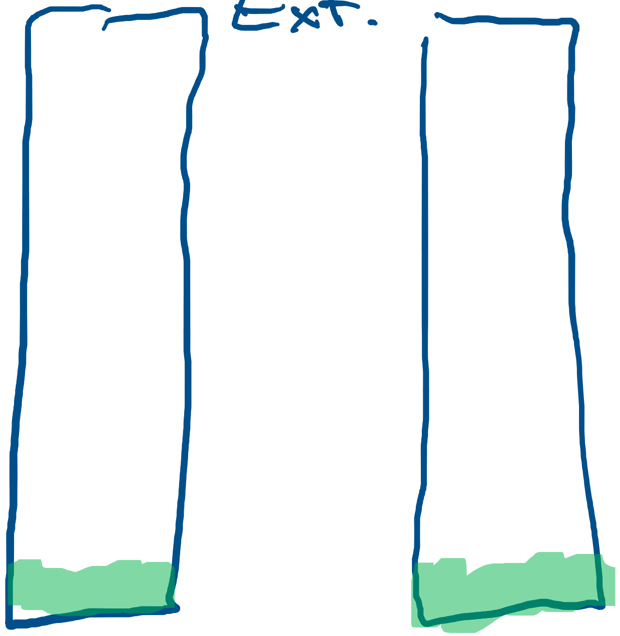


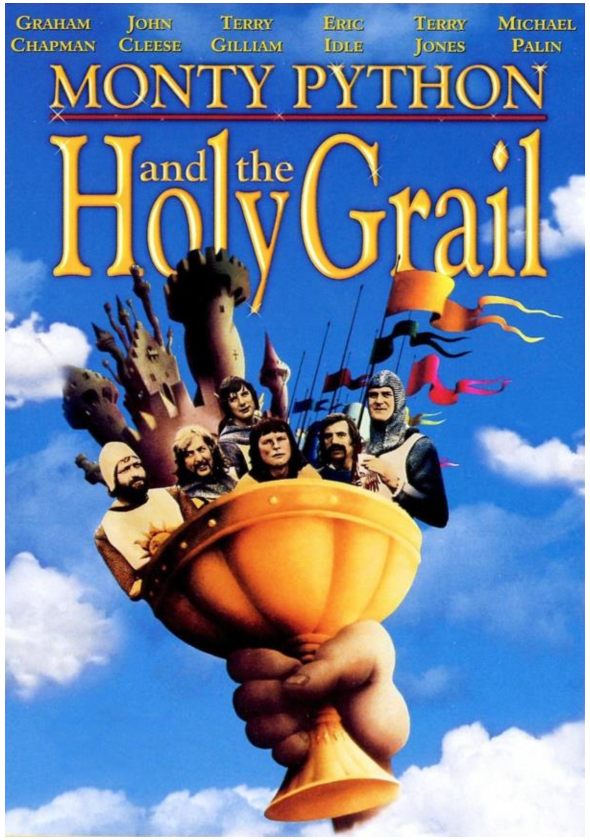
Entropy Rate



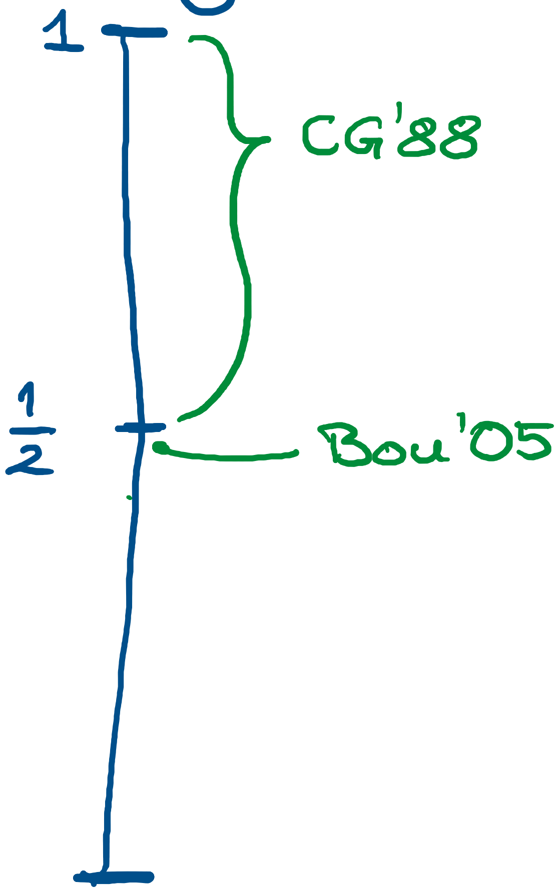
Why I care

2 source Ext.



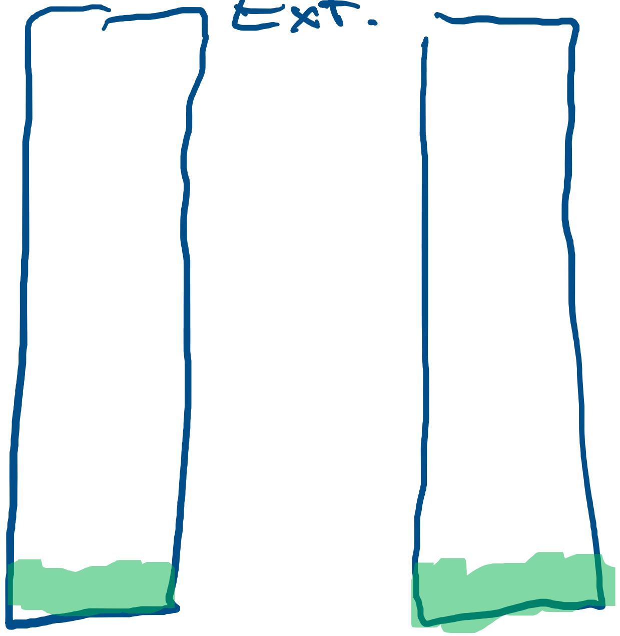


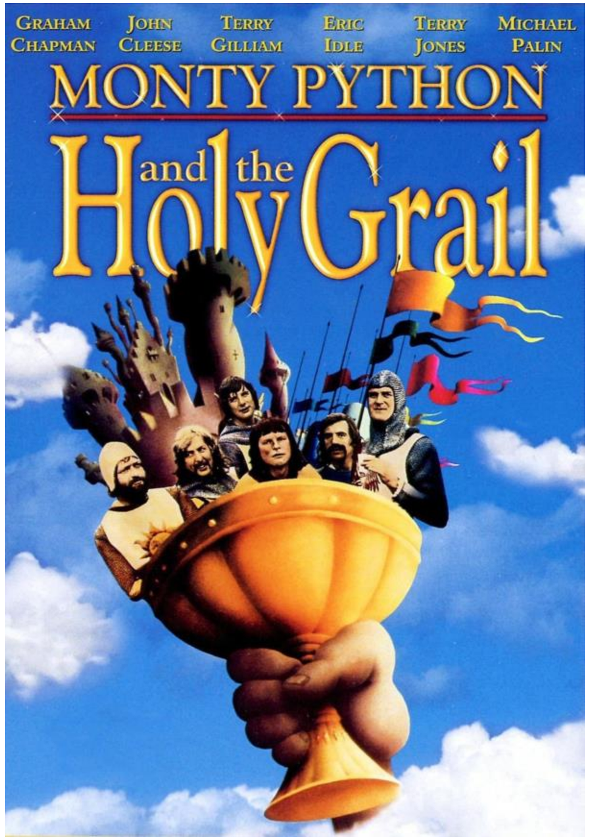
Entropy Rate



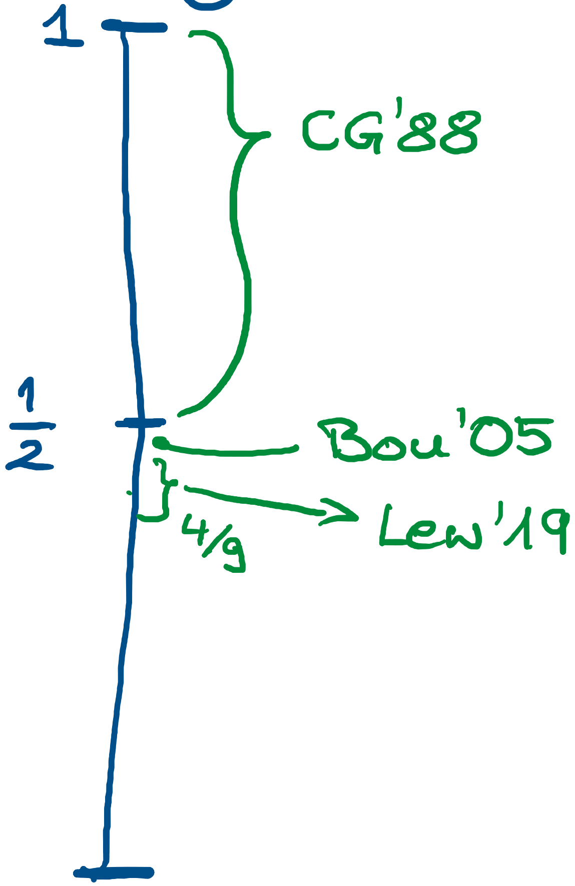
Why I care

2 source Ext.



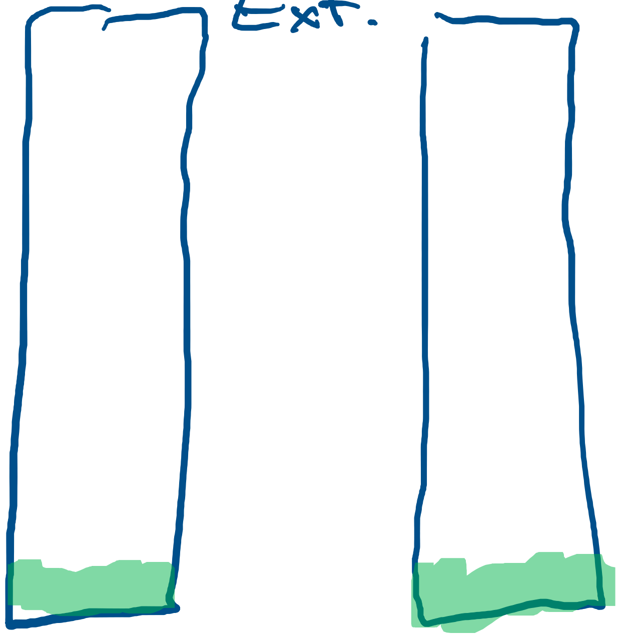


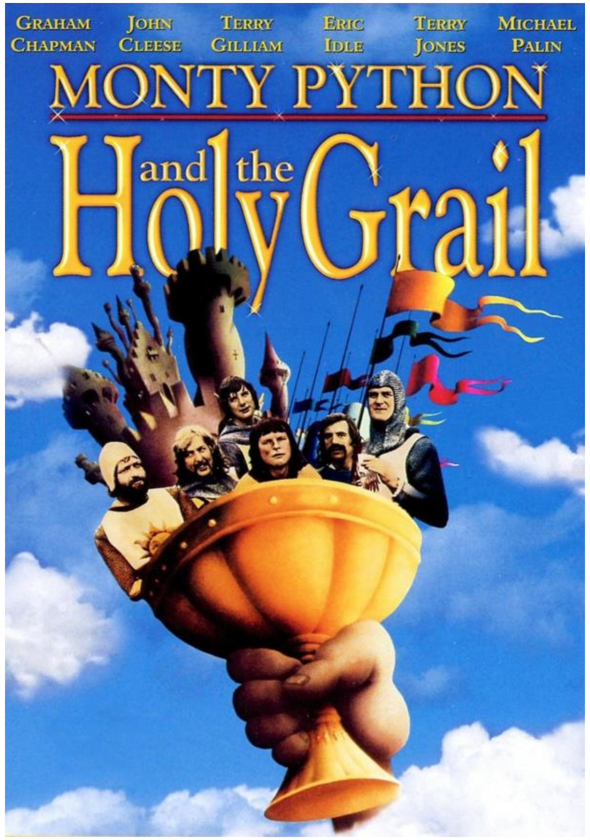
Entropy Rate



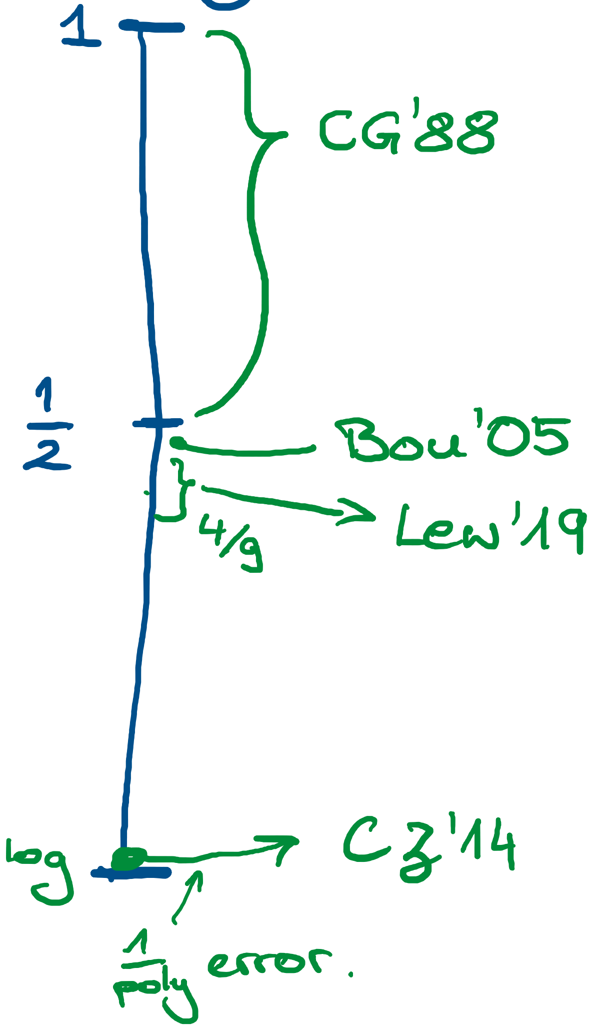
Why I care

2 source Ext.



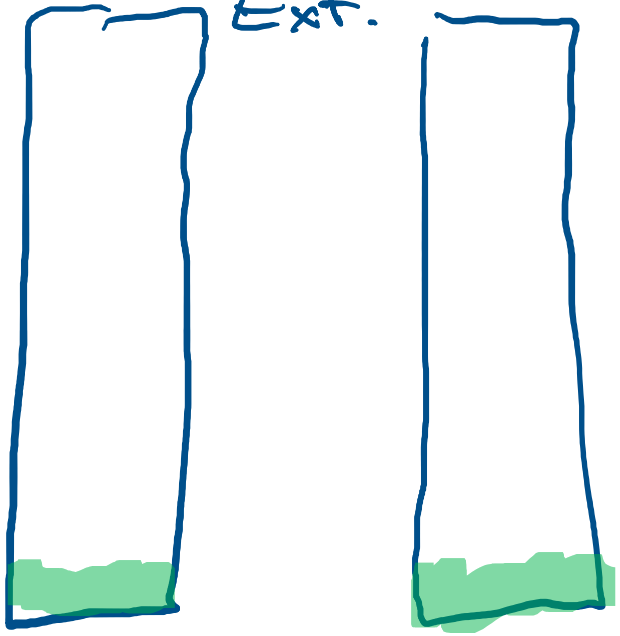


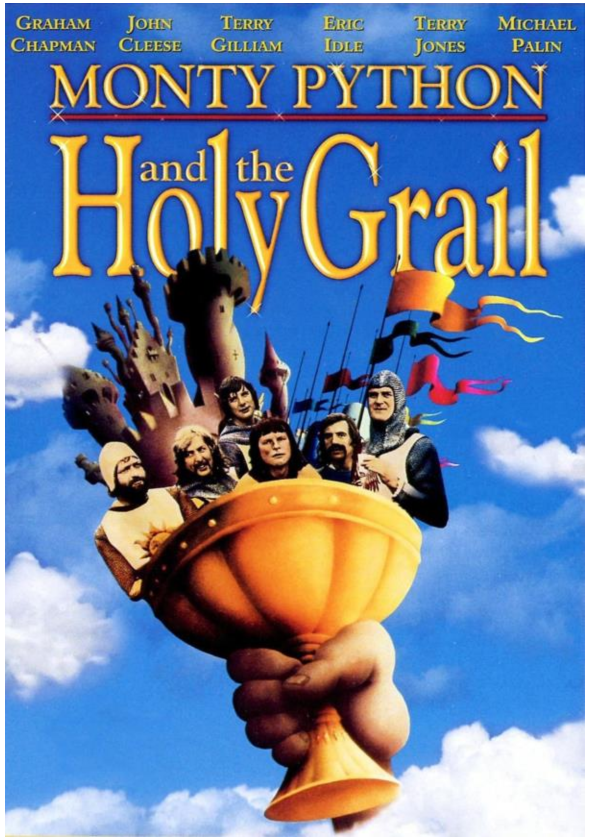
Entropy Rate



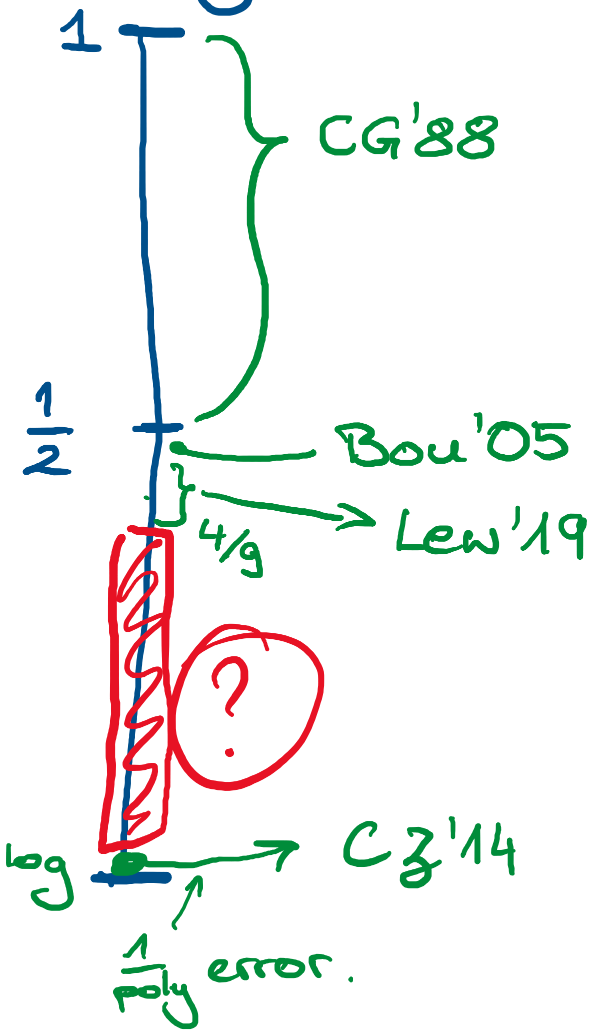
Why I care

2 source Ext.

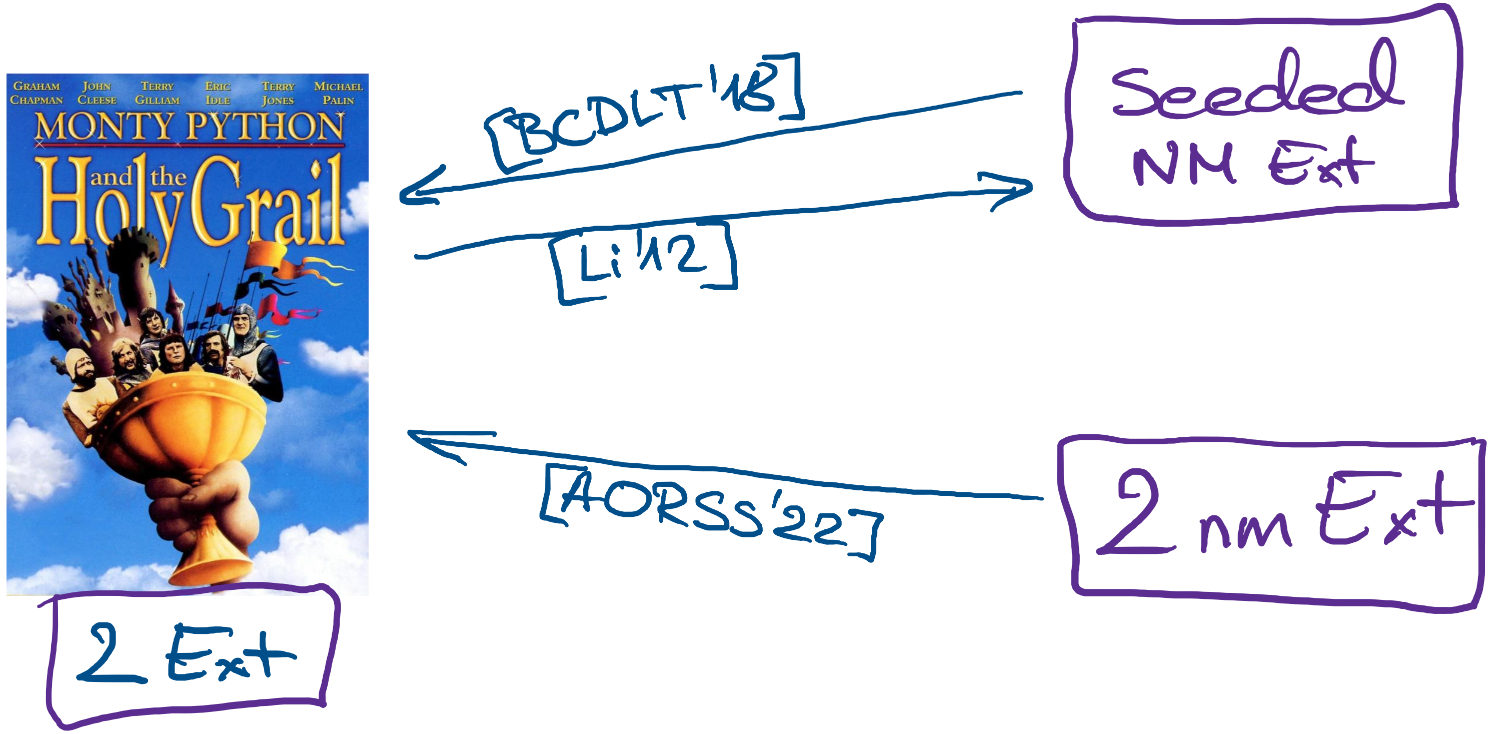




Entropy Rate



Connections



GRAHAM CHAPMAN JOHN CLEESE TERRY GILLIAM ERIC IDLE TERRY JONES MICHAEL PALIN
MONTY PYTHON
and the Holy Grail

Seeded NM Ext

[BCDLT'18]

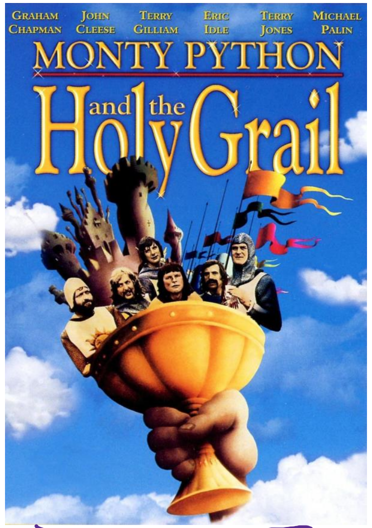
[Li'12]

2 nm Ext

[AORSS'22]

2 Ext

Connections



2 Ext

[BCDLT'18]

Seeded NM Ext

[Li'12]

[AORSS'22]

2 nm Ext

$(1-\frac{1}{T})$ entropy threshold

this paper gets $\left(1-\frac{1}{2T+3}\right)$

Thank You

22.30