The Chaining Lemma and its Application

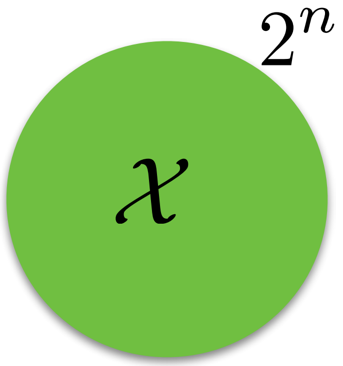
Pratyay Mukherjee
Aarhus University

joint work with

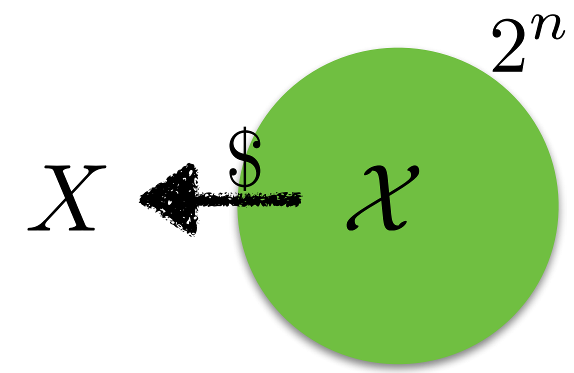
Ivan Damgård(Aarhus), Sebastian Faust (Bochum),
Daniele Venturi (La Sapienza, Rome)

The starting point: A basic question

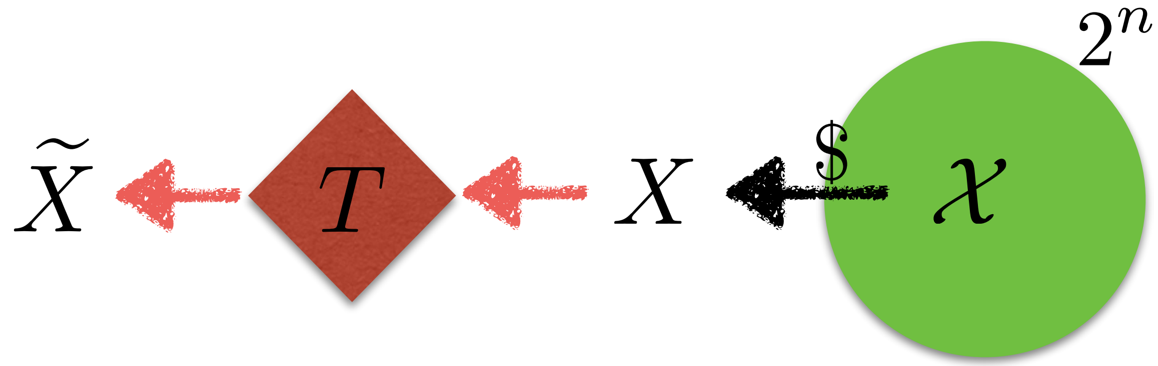
The starting point: A basic question



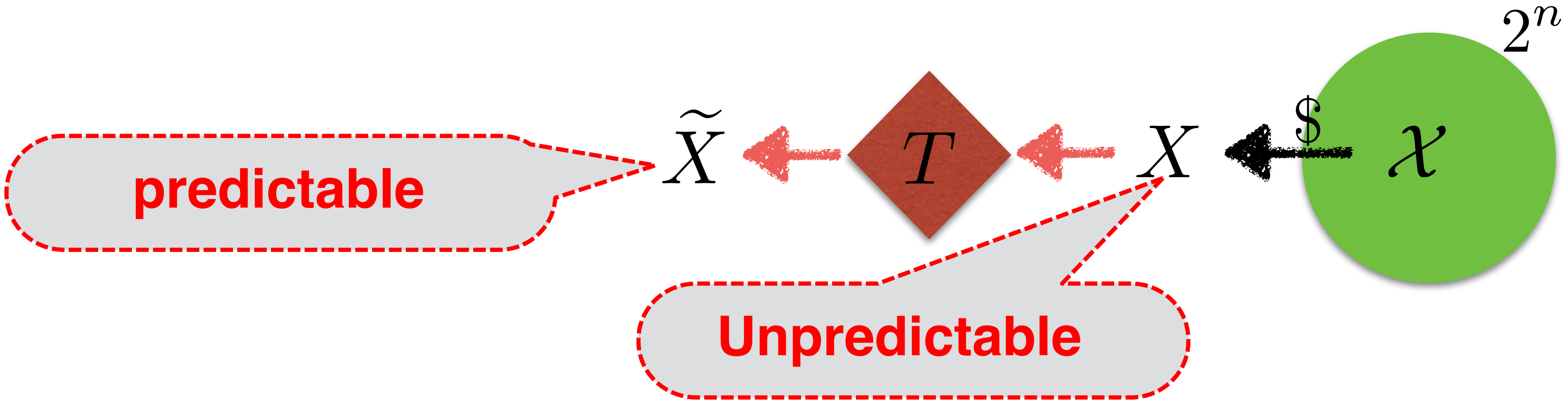
The starting point: A basic question



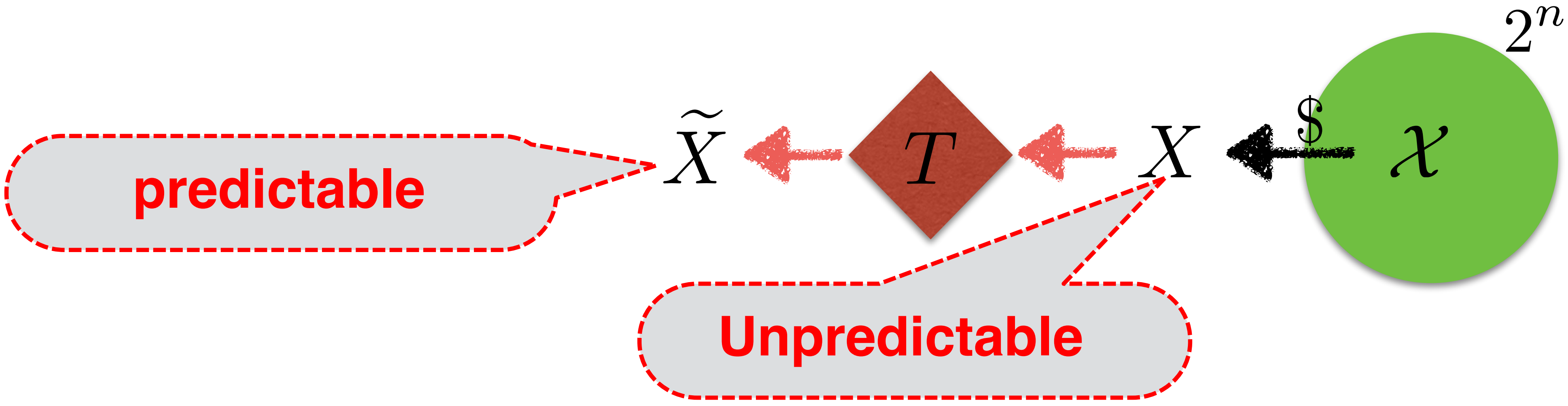
The starting point: A basic question



The starting point: A basic question



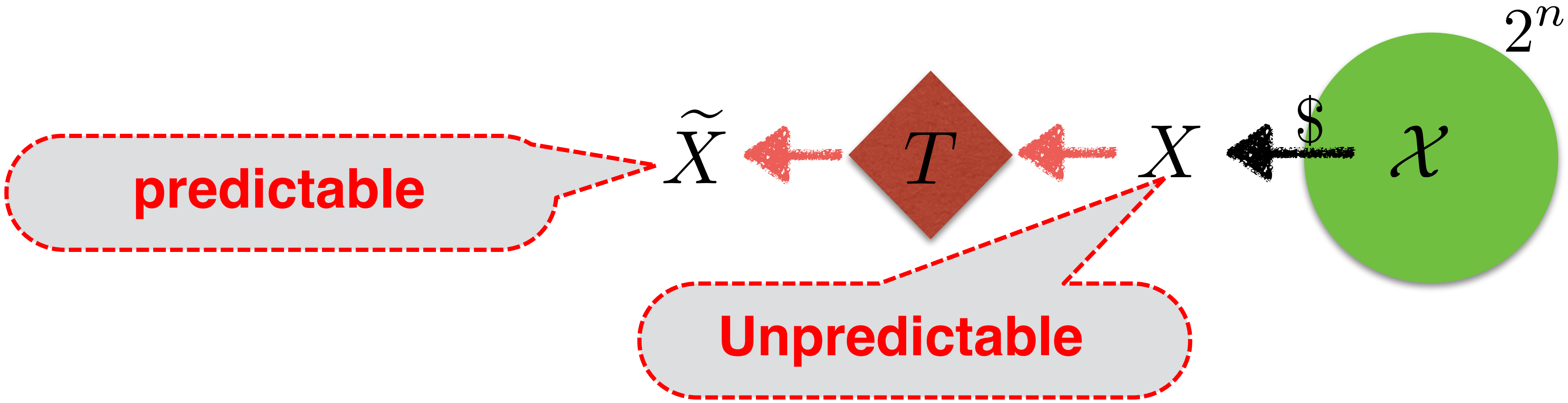
The starting point: A basic question



Natural Question:

How much $\widetilde{X}$ reveals about X ?

The starting point: A basic question

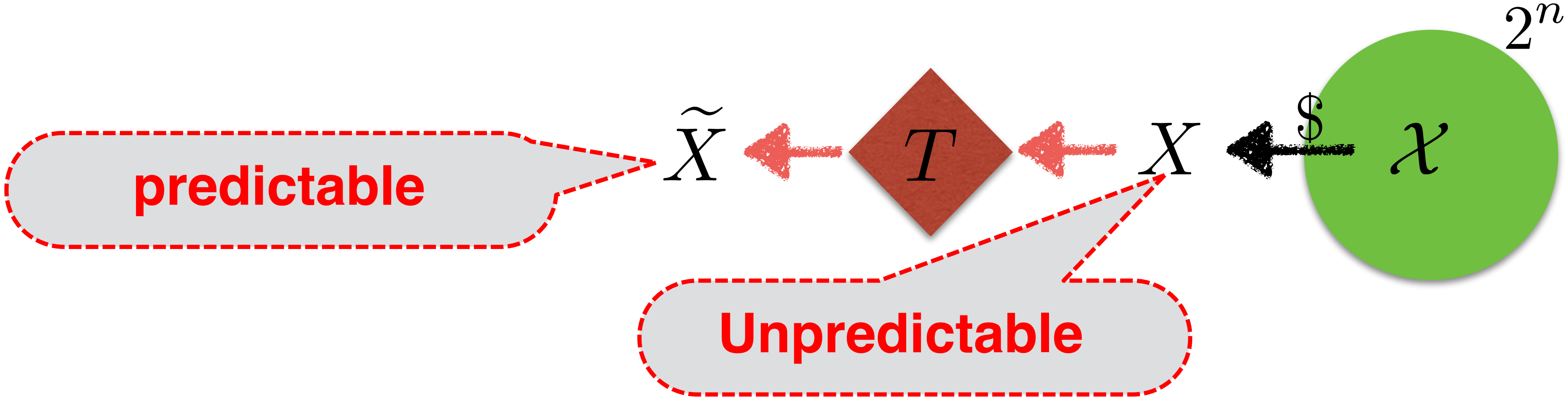


<u>Natural Question:</u>

How much $\widetilde{X}$ reveals about X ?

Naive attempt:
Predictable can't reveal much about unpredictable!

The starting point: A basic question



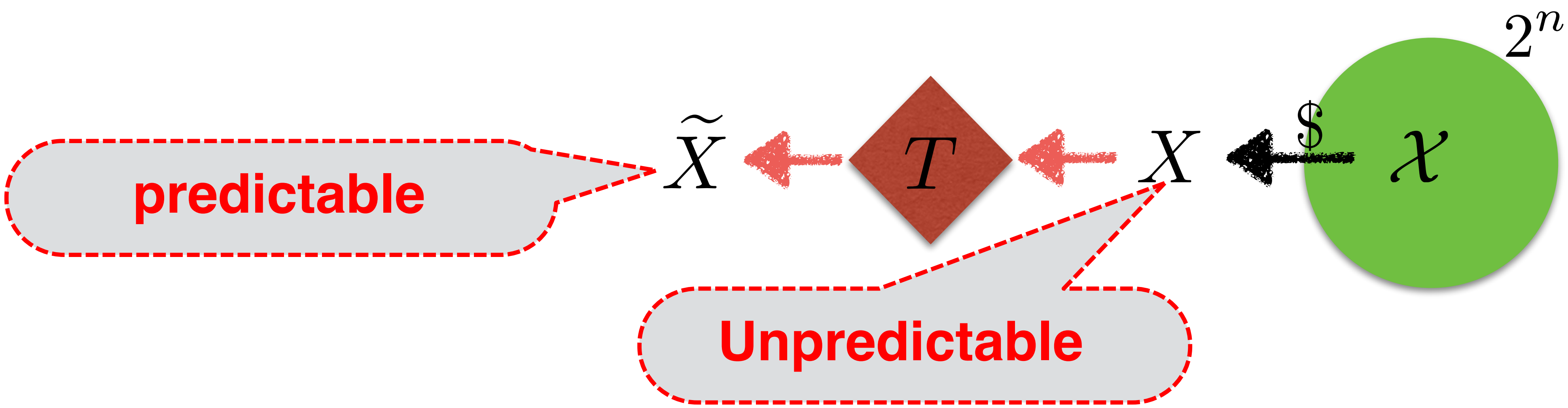
Natural Question:

How much $\widetilde{X}$ reveals about X ?

Naive attempt:
Predictable can't reveal much about unpredictable!

Wrong for min-entropy !

The starting point: A basic question



Natural Question:

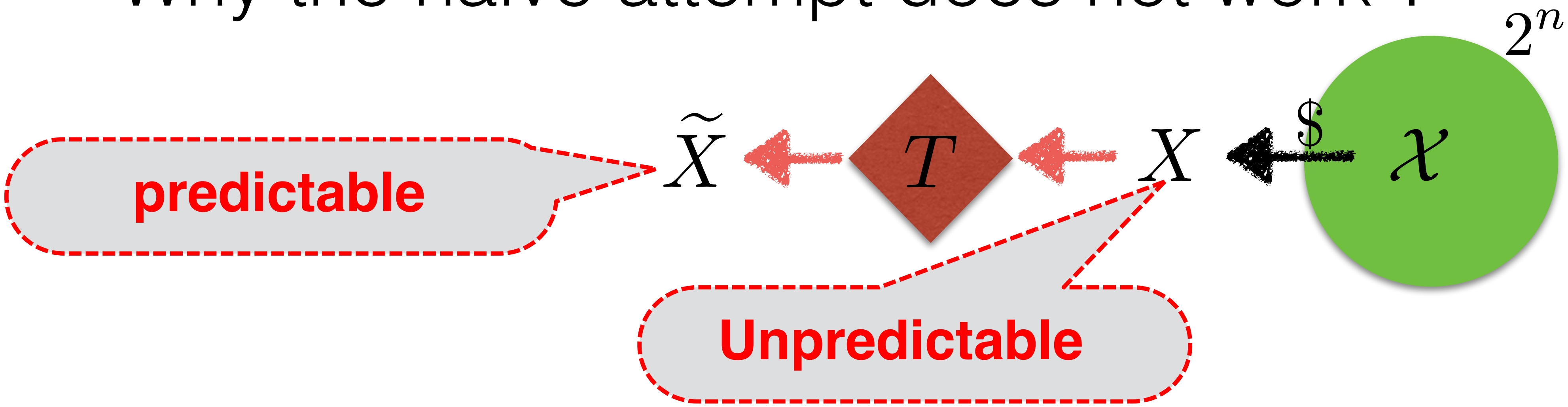
How much $\tilde{X}$ reveals about X ?

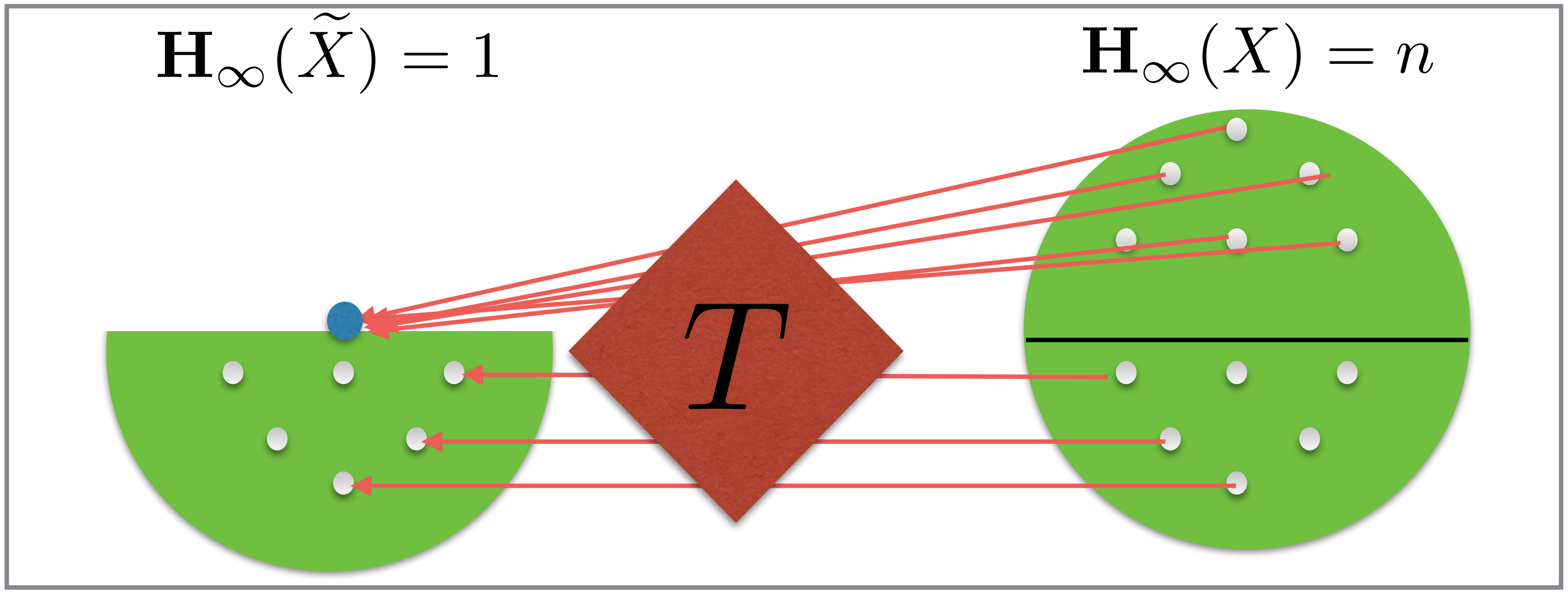
Naive attempt:
Predictable can't reveal much about unpredictable!

Wrong for min-entropy !

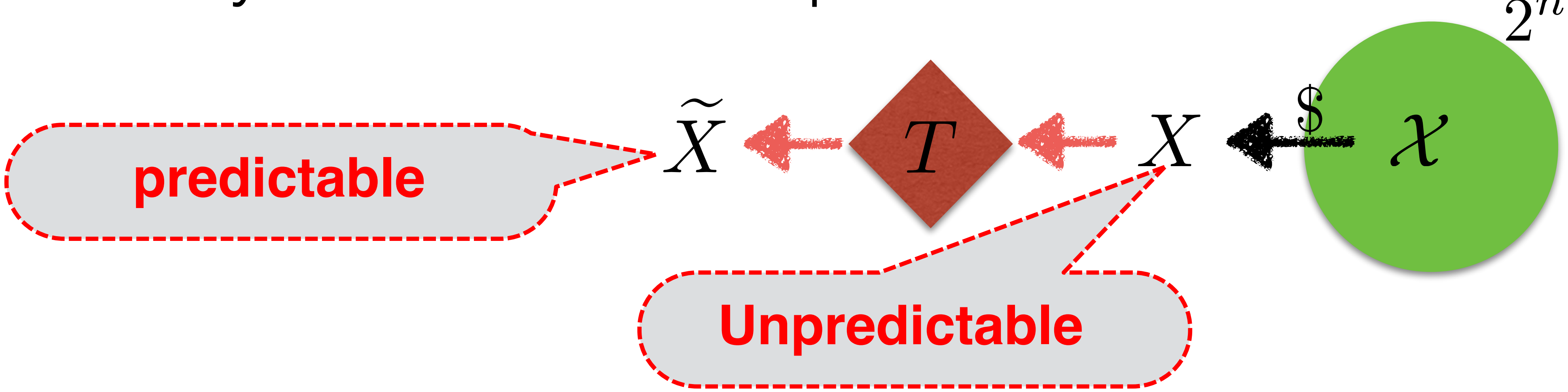
$\mathbf{H}_\infty(X) := -\log \max_x \Pr[X = x]$

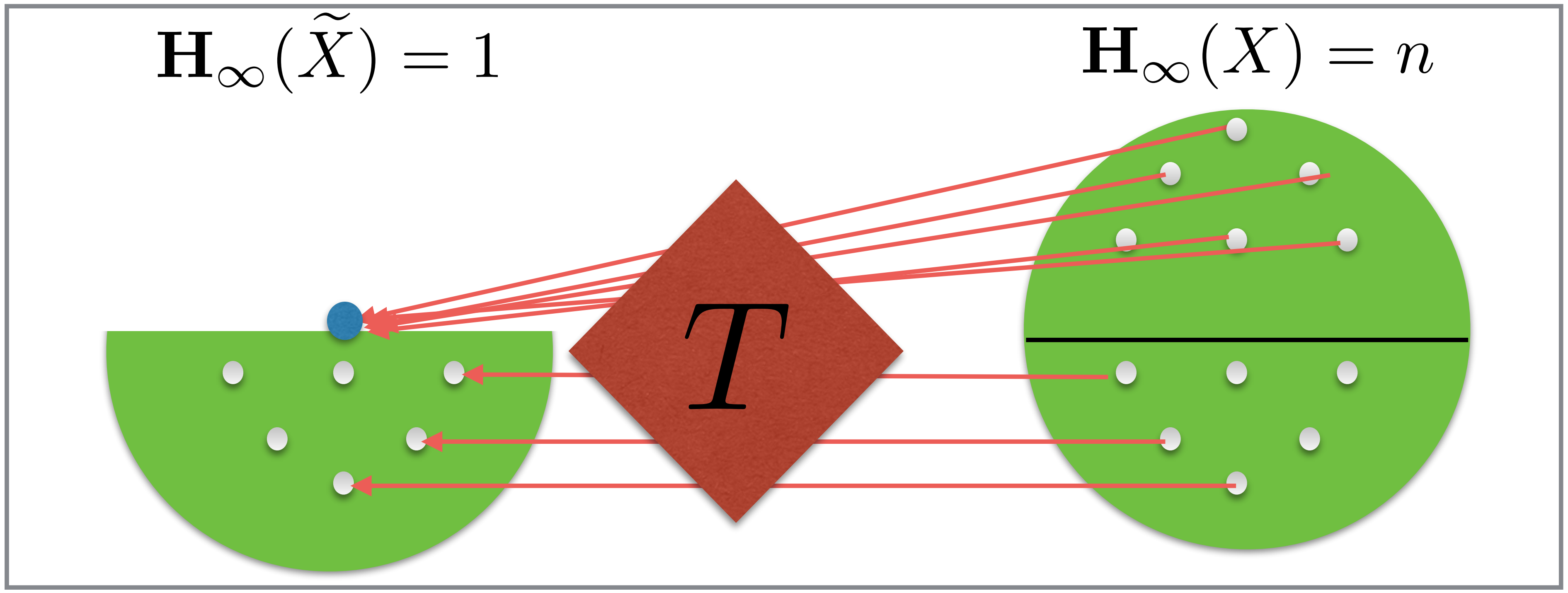
An example T :
Why the naive attempt does not work ?





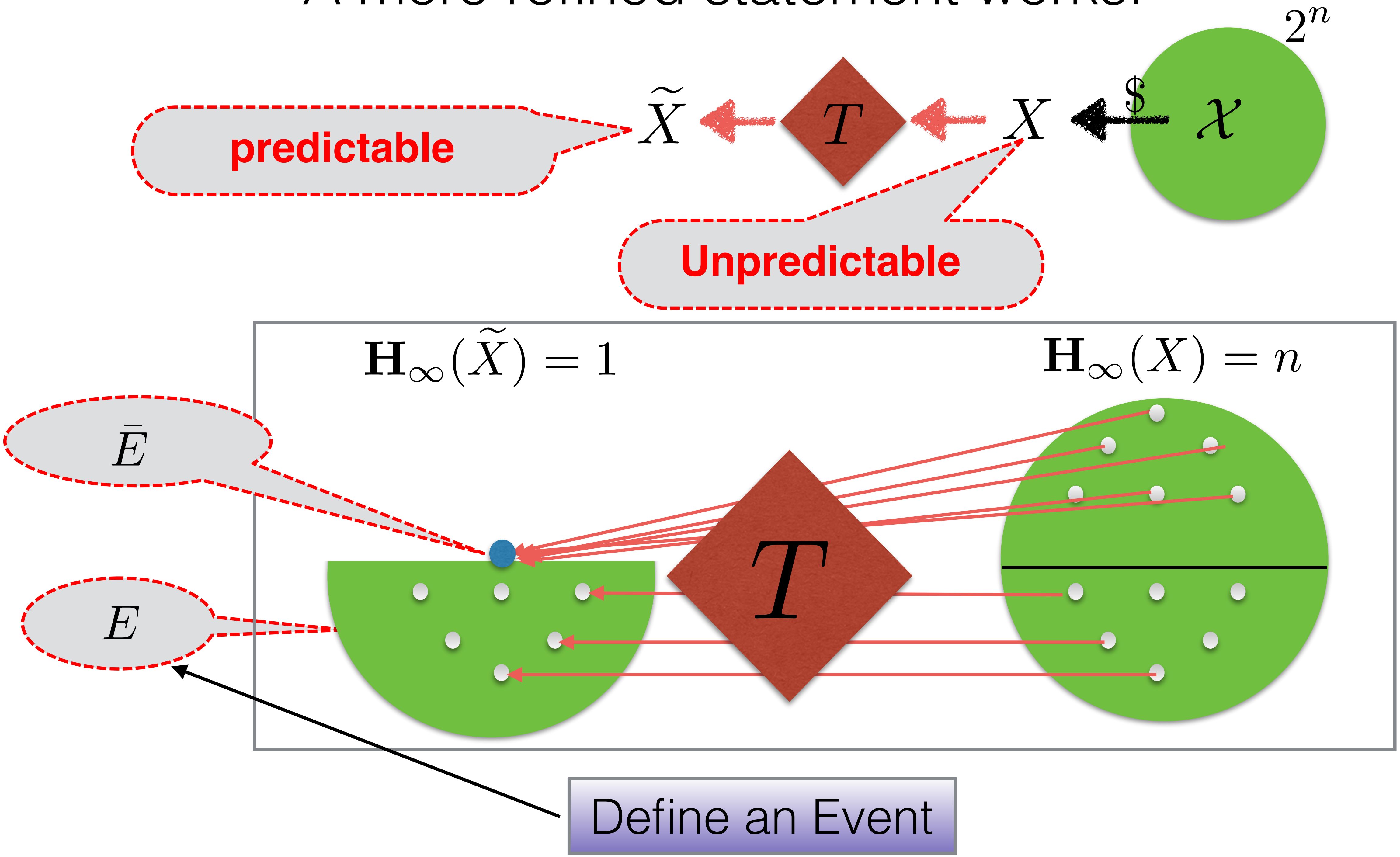
An example T : Why the naive attempt does not work ?



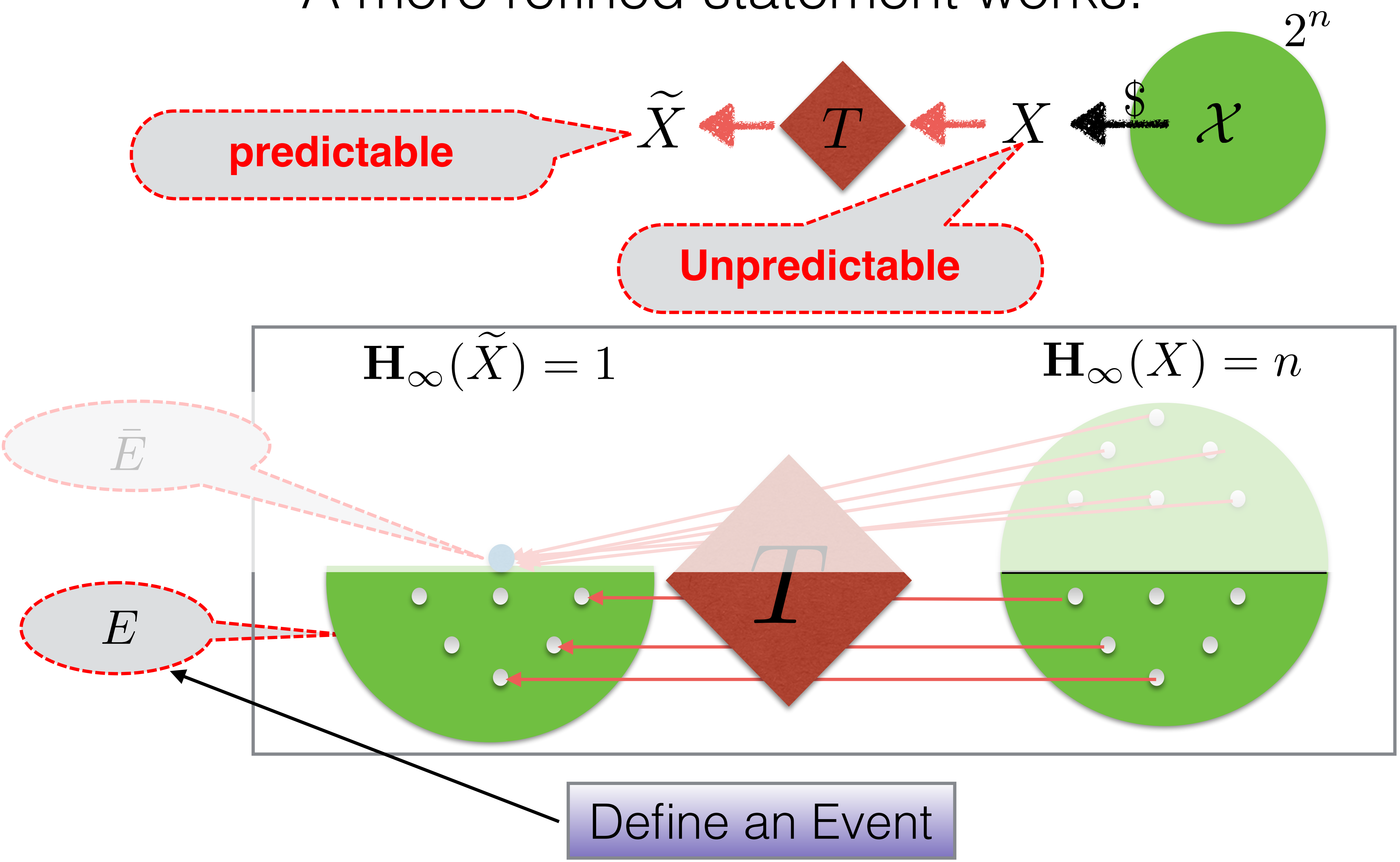


Half the times reveals everything

An example T :
A more refined statement works.

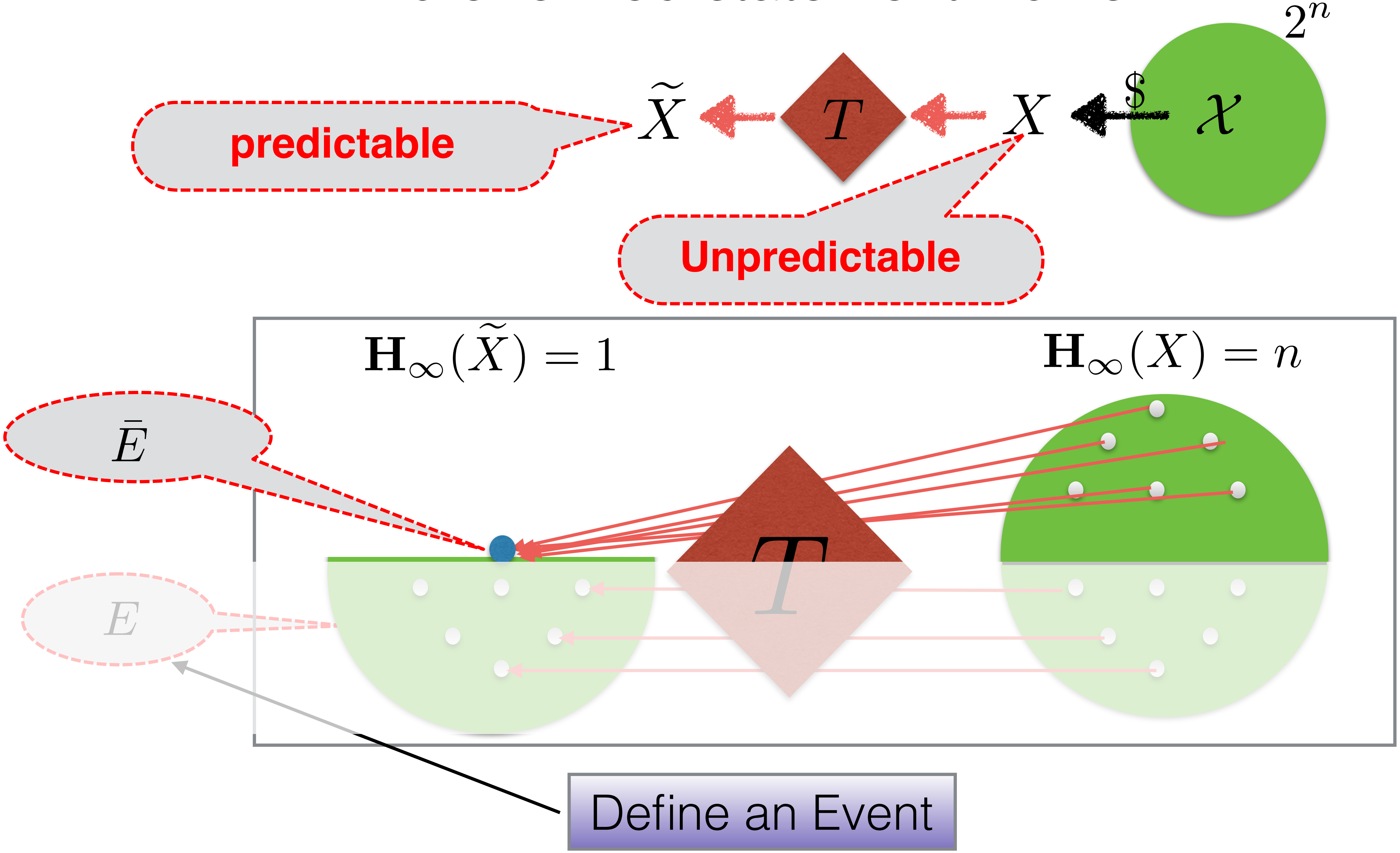


An example T :
A more refined statement works.



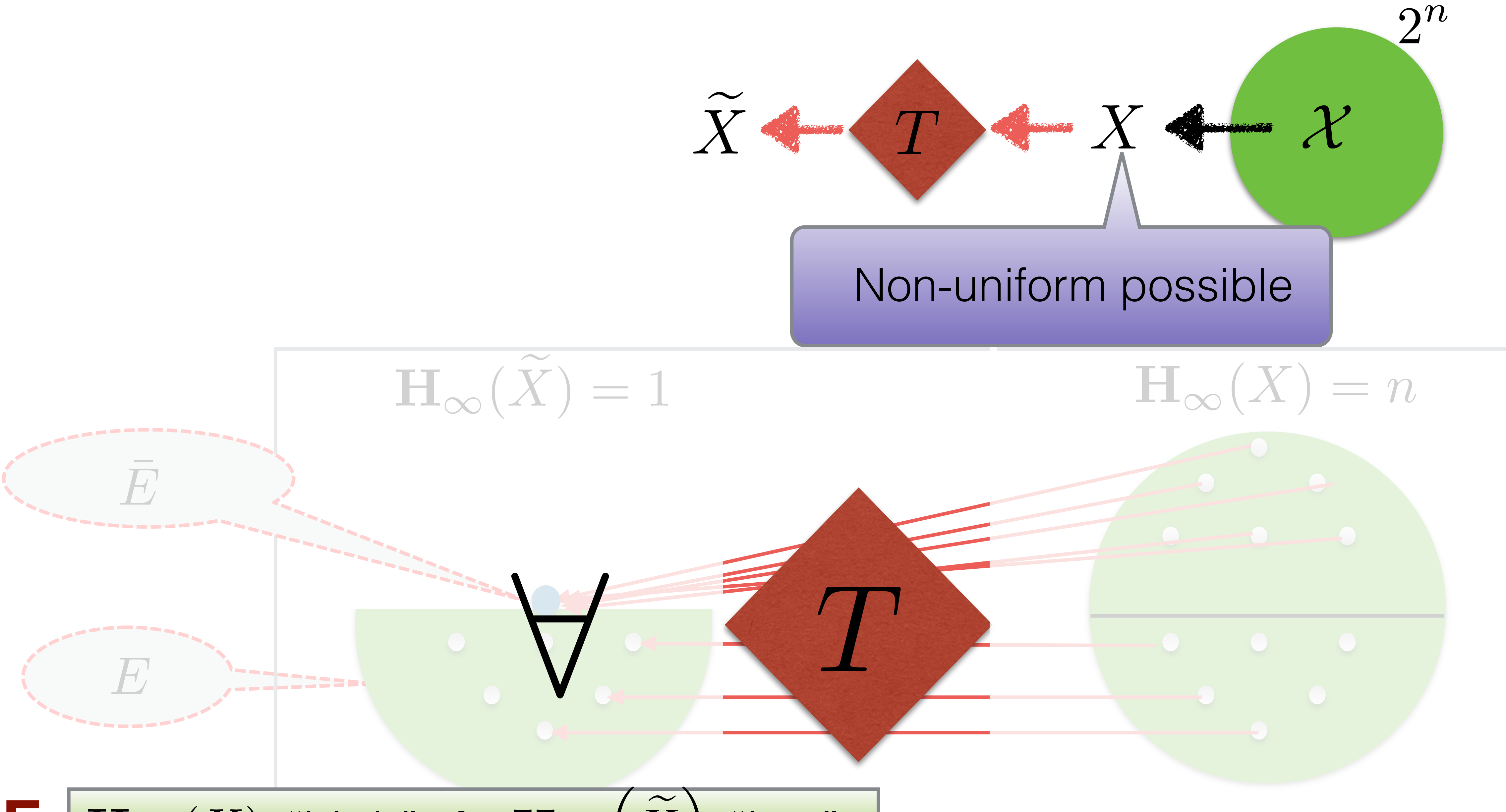
1. When E happens then both $\widetilde{X}|_E$ and $X|_E$ has "high" min-entropy

An example T :
A more refined statement works.



2. When $\bar{E}$ happens then $X|_{\bar{E}} \mid \widetilde{X}|_{\bar{E}}$ has “high” min-entropy.

The basic conjecture



IF $\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low" **THEN** There exists Event E

1. When E happens then both $\widetilde{X}|_E$ and $X|_E$ has "high" min-entropy
2. When $\bar{E}$ happens then $X|_{\bar{E}}$ | $\widetilde{X}|_{\bar{E}}$ has "high" min-entropy.

Generalization over the Chain

Uniform

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

Generalization over the Chain

Uniform

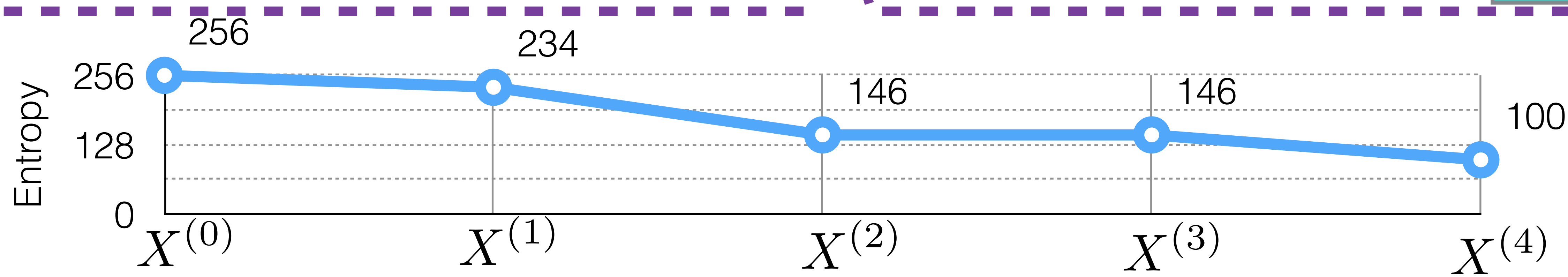
The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

Fact

$$\mathbf{H}_\infty(X^{(i)}) \le \mathbf{H}_\infty(X^{(i-1)})$$

e.g.
$t = 4$
$n = 256$



Generalization over the Chain

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

Fix some threshold $u \ll n$

Generalization over the Chain

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \dots \xrightarrow{T_t} X^{(t)}$$

Fix some threshold $u \ll n$

Case-1: The entire chain is “high” $X^{(t)} \geq u$

Generalization over the Chain

The Chain

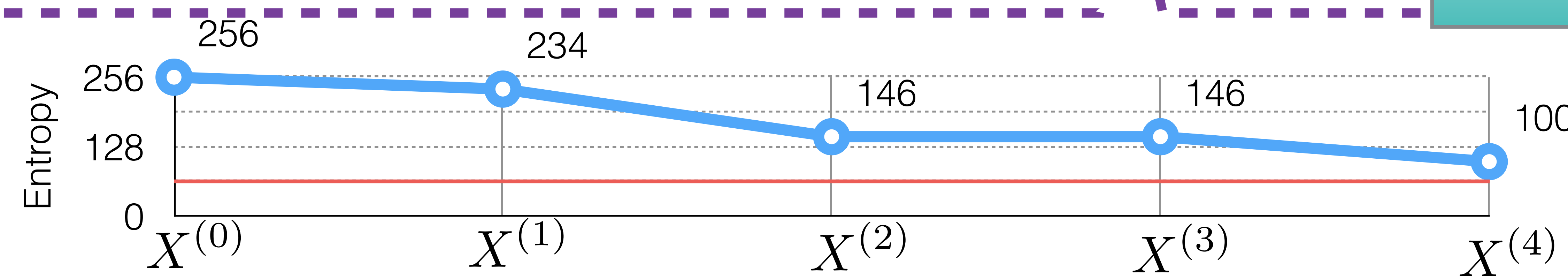
$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \dots \xrightarrow{T_t} X^{(t)}$$

Fix some threshold $u \ll n$

Case-1: The entire chain is "high" $X^{(t)} \geq u$

e.g.

$t = 4$
$n = 256$
$u = 64$



Generalization over the Chain

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

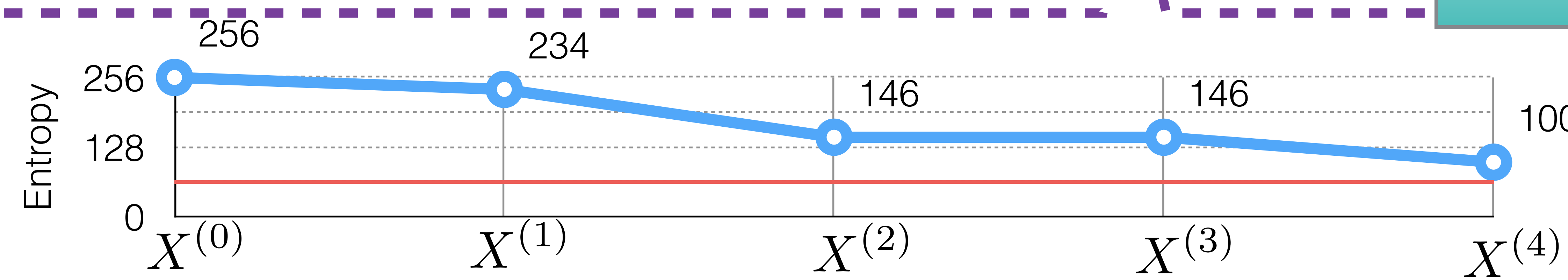
Desired case !

Fix some threshold $u \ll n$

Case-1: The entire chain is "high" $X^{(t)} \geq u$

e.g.

$t = 4$
$n = 256$
$u = 64$



Generalization over the Chain

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

Case-2: At some point the chain goes “low”

$$\exists\ j\ :\ X^{(j-1)} \geq u\ \&\ X^{j} < u$$

Generalization over the Chain

The Chain

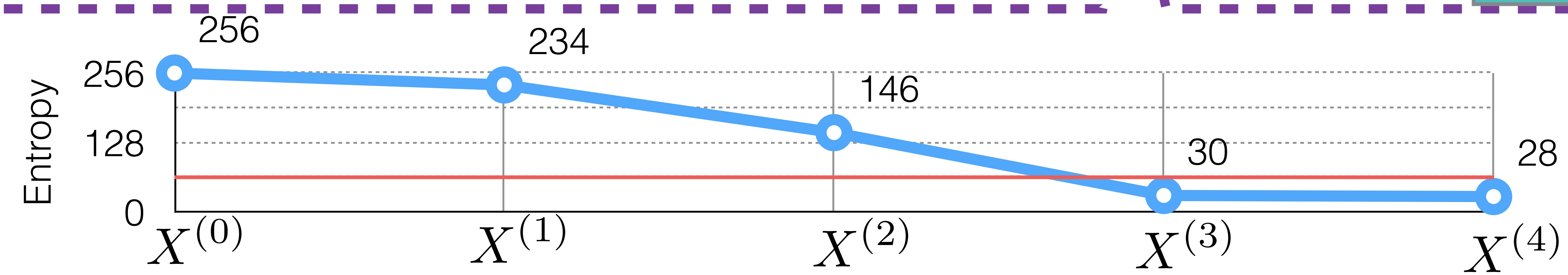
$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \dots \xrightarrow{T_t} X^{(t)}$$

Case-2: At some point the chain goes "low"

$$\exists \ j \ : \ X^{(j-1)} \geq u \ \& \ X^j < u$$

e.g.

$t = 4$
$n = 256$
$u = 64$



Question:

Can we "save" part of the chain ?

The Chain

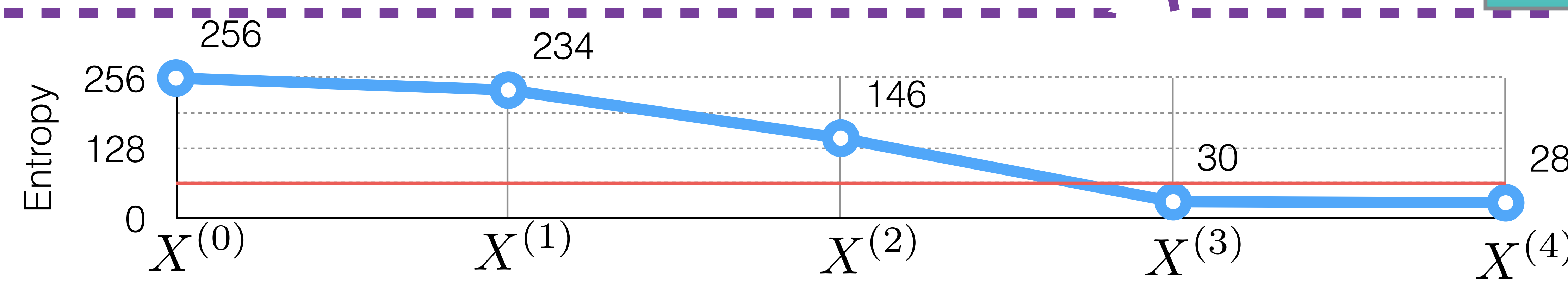
$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

Case-2: At some point the chain goes "low"

$$\exists\ j\ :\ X^{(j-1)} \geq u\ \&\ X^j < u$$

e.g.

$t = 4$
$n = 256$
$u = 64$



Question:

Can we "save" part of the chain ?

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

Note

$i \neq j$ possible

Case-2: At some point the chain goes "low"

$$\exists\, j \;:\; X^{(j-1)} \geq u \;\&\; X^{j} < u$$

Can we find an index i such that given $X^{(i)}$
the part of chain
$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_{i-1}} X^{(i-1)}$$
stays ``high" ?

Question:

Can we "save" part of the chain ?

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \dots \xrightarrow{T_t} X^{(t)}$$

Note

$i \neq j$ possible

Case-2: At some point the chain goes "low"

$$\exists\, j \;:\; X^{(j-1)} \geq u \;\&\; X^{j} < u$$

Can we find an index i such that given $X^{(i)}$
the part of chain
$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \dots \xrightarrow{T_{i-1}} X^{(i-1)}$
stays ``high" ?

Chaining Lemma: Yes!
if t is short enough
than n

Question:

Can we “save” part of the chain ?

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

Note

$i \neq j$ possible

Case-2: At some point the chain goes “low”

$$\exists\ j\ :\ X^{(j-1)} \geq u\ \&\ X^j < u$$

Can we find an index i such that given $X^{(i)}$ the part of chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_{i-1}} X^{(i-1)}$$

stays ``high” ?

$t = O(\sqrt{n})$

Chaining Lemma: Yes! if t is short enough than n

The Chaining Lemma (Informally)

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

The Chaining Lemma (Informally)

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \dots \xrightarrow{T_t} X^{(t)}$$

If t is sufficiently small compare to n then

The Chaining Lemma (Informally)

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

If t is sufficiently small compare to n then

There exists an event E such that

The Chaining Lemma (Informally)

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

If t is sufficiently small compare to n then

There exists an event E such that

1. If E happens then the entire chain is "high" :

$$\mathbf{H}_\infty\left(X^{(t)}_{|E}\right) \geq u$$

2. If $\bar{E}$ happens then there exists an i such that given $X^{(i)}$ the first part of chain stays "high".

$$\widetilde{\mathbf{H}}_\infty\left(X^{(i-1)}_{|\bar{E}} \mid X^{(i)}_{|\bar{E}}\right) \geq u$$

The Chaining Lemma (Informally)

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

If t is sufficiently small compare to n then

There exists an event E such that

1. If E happens then the entire chain is "high" :
$$\mathbf{H}_\infty\left(X^{(t)}_{|E}\right) \geq u$$
2. If $\bar{E}$ happens then there exists an i such that given $X^{(i)}$ the first part of chain stays "high".

$$\widetilde{\mathbf{H}}_\infty\left(X^{(i-1)}_{|\bar{E}} \mid X^{(i)}_{|\bar{E}}\right) \geq u$$

$$\widetilde{\mathbf{H}}_\infty(X|Z) := -\log \mathbb{E}_{z \leftarrow Z}[2^{-\mathbf{H}_\infty(X|Z=z)}]$$

DORS '08

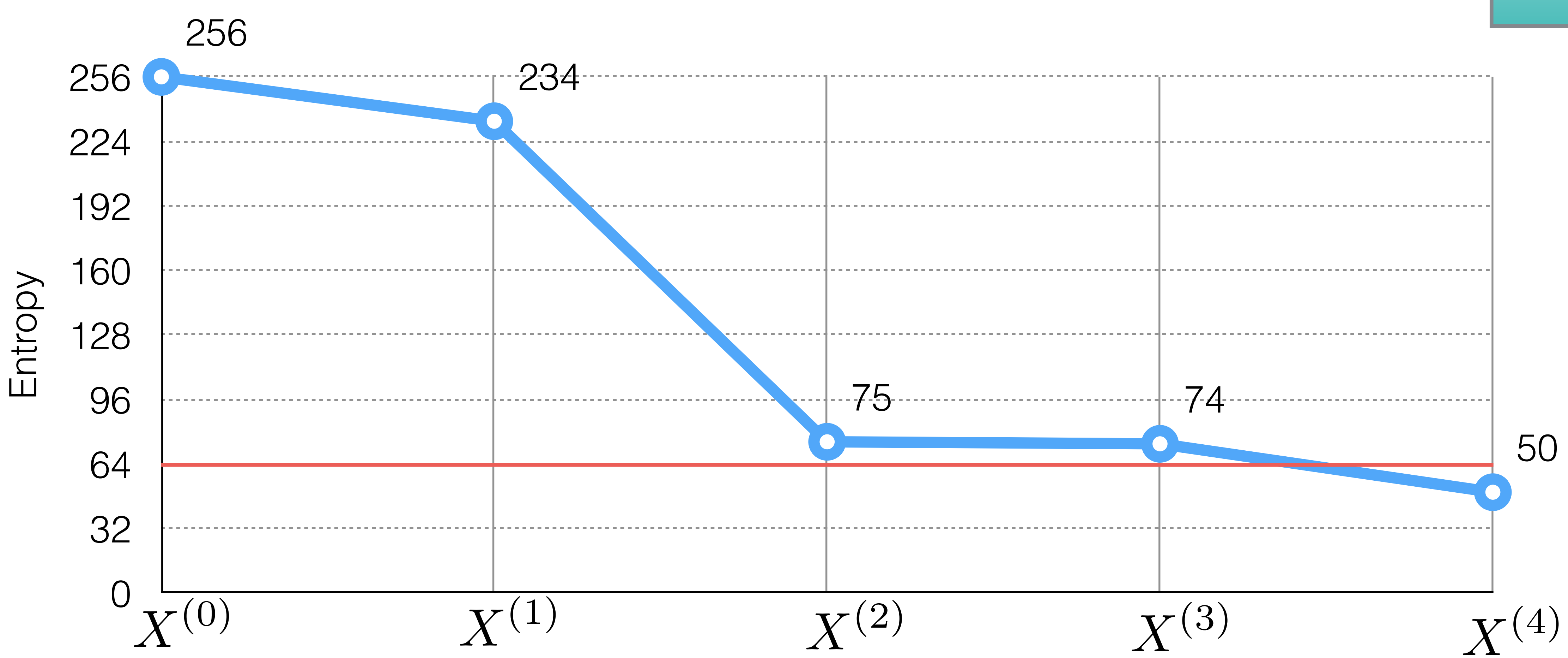
Some intuitions

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

e.g.

$$t = 4$$
$$n = 256$$
$$u = 64$$



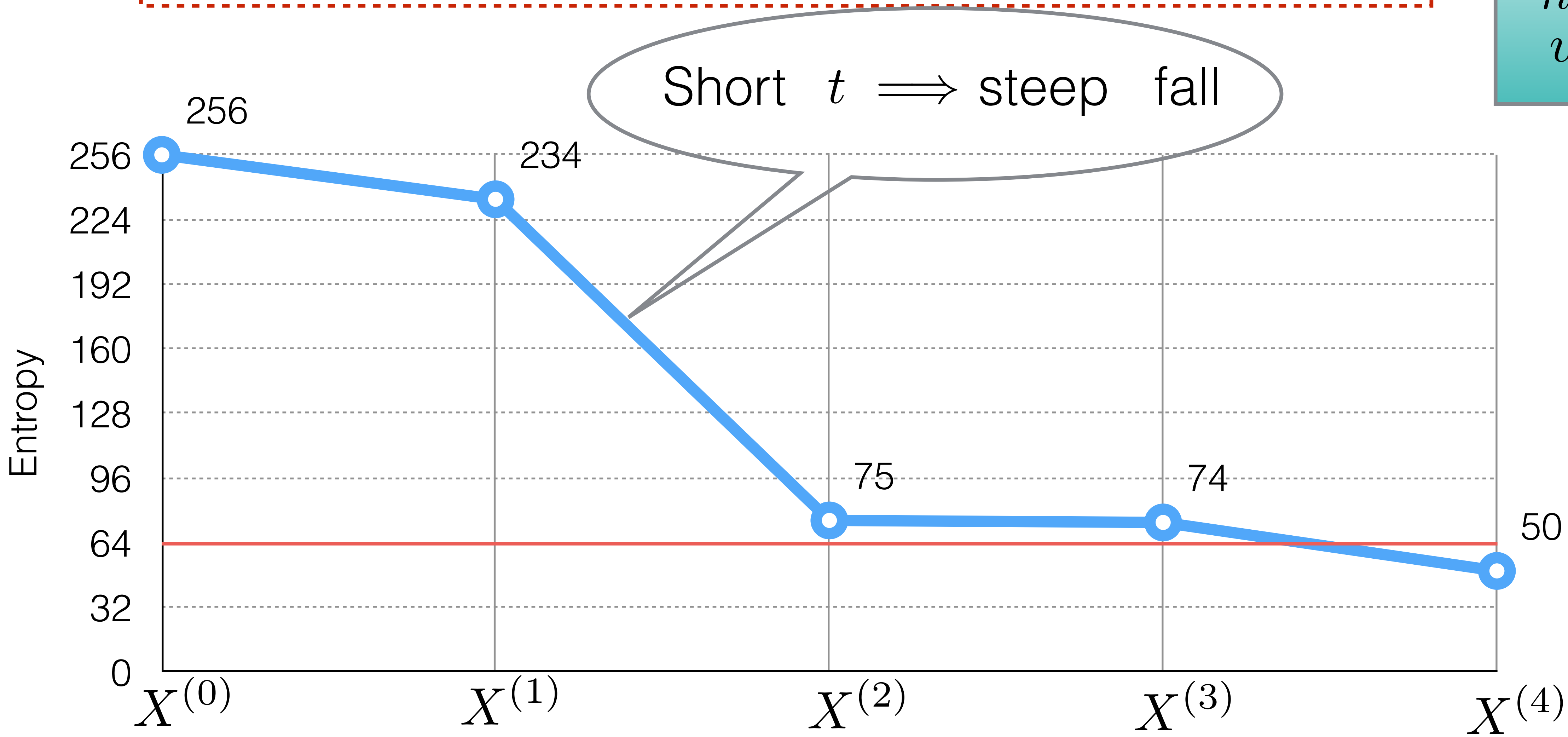
Some intuitions

The Chain

$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \dots \xrightarrow{T_t} X^{(t)}$$

e.g.

$t = 4$
$n = 256$
$u = 64$



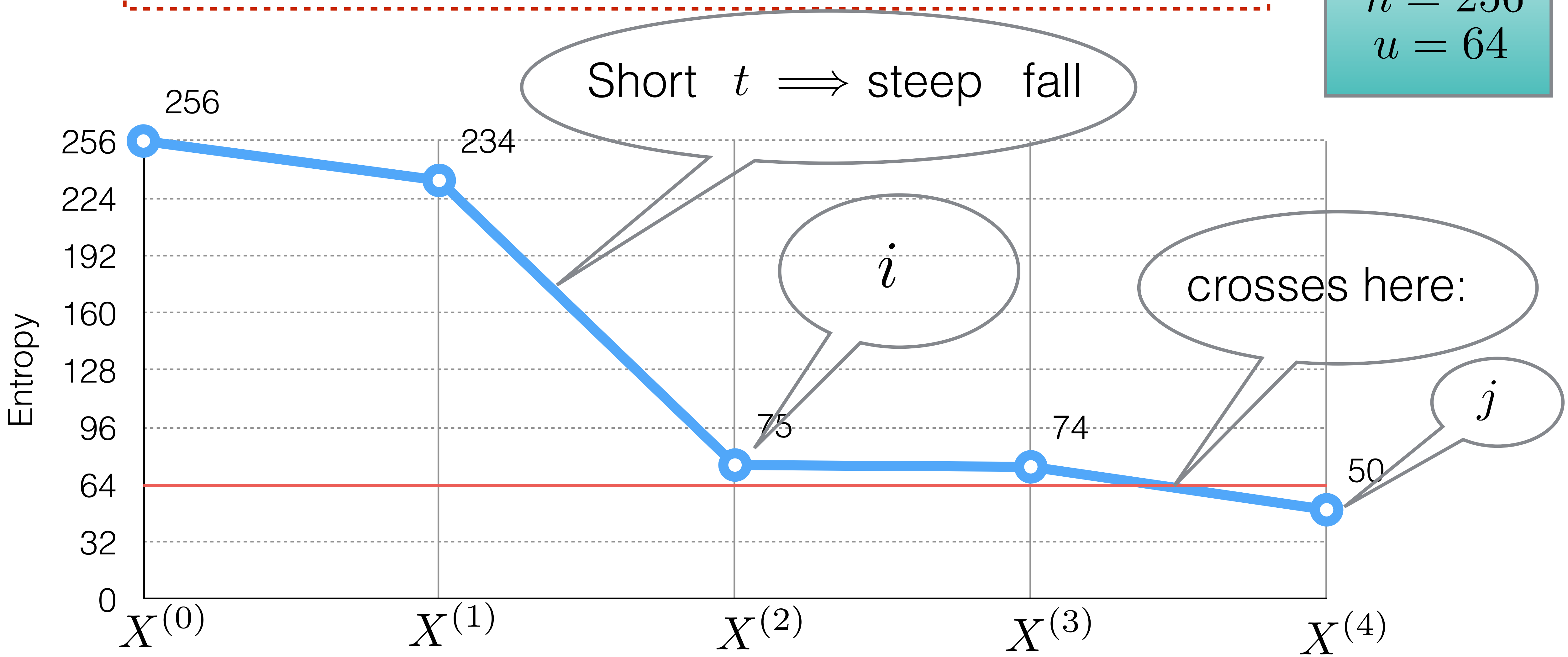
Some intuitions

The Chain

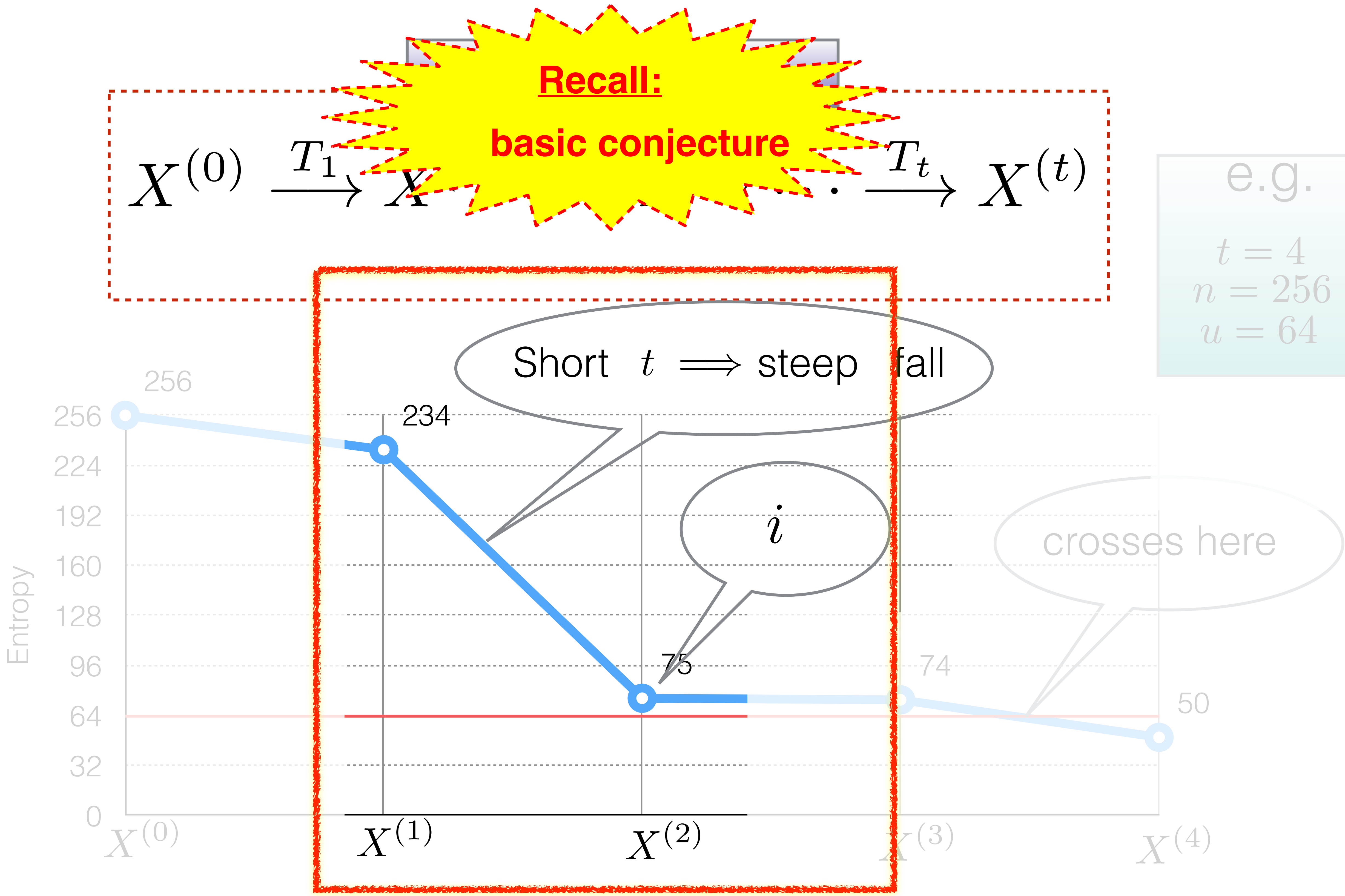
$$X^{(0)} \xrightarrow{T_1} X^{(1)} \xrightarrow{T_2} X^{(2)} \ldots \xrightarrow{T_t} X^{(t)}$$

e.g.

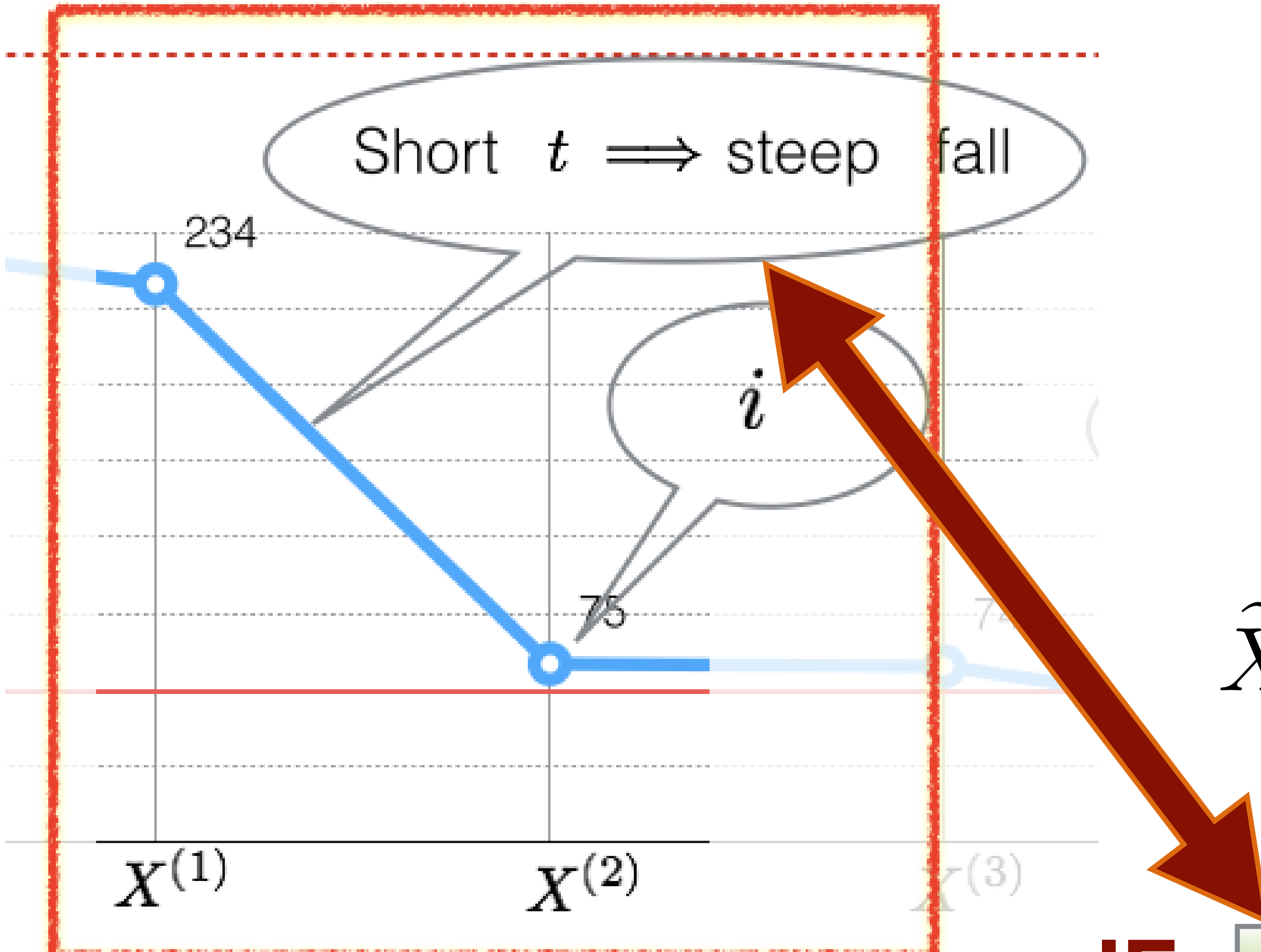
$t = 4$
$n = 256$
$u = 64$

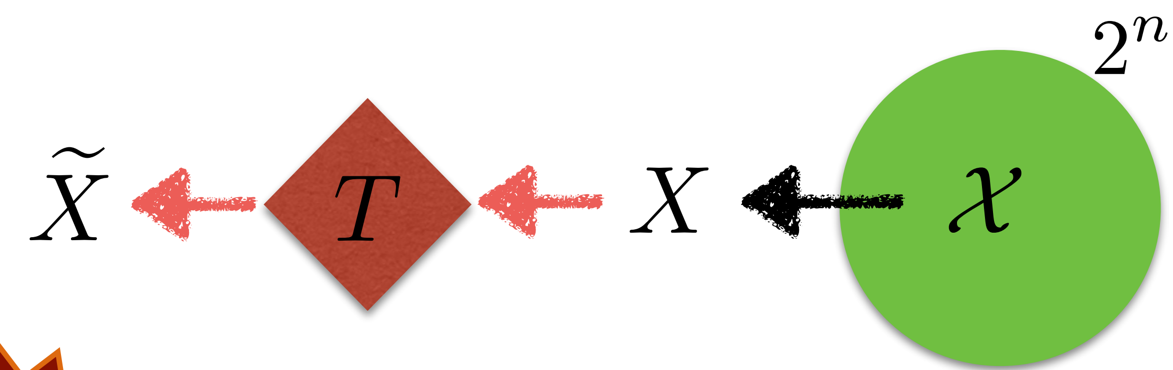


Some intuitions



Recall the basic conjecture





IF $\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

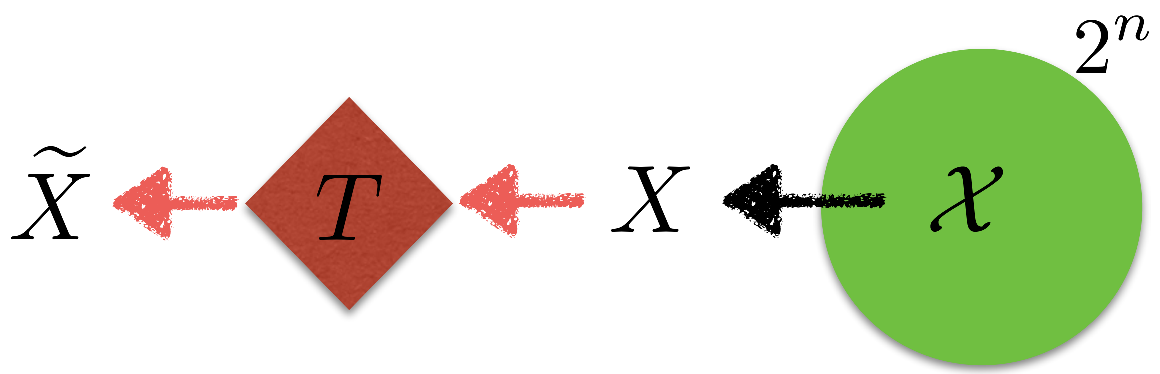
THEN There exists Event E

1. When E happens then both $\widetilde{X}|_E$ and $X|_E$ has "high" min-entropy
2. When $\bar{E}$ happens then $X|_{\bar{E}}$ | $\widetilde{X}|_{\bar{E}}$ has "high" min-entropy.

Proof overview of the basic conjecture

Key-question

how to define such event for any general function ?



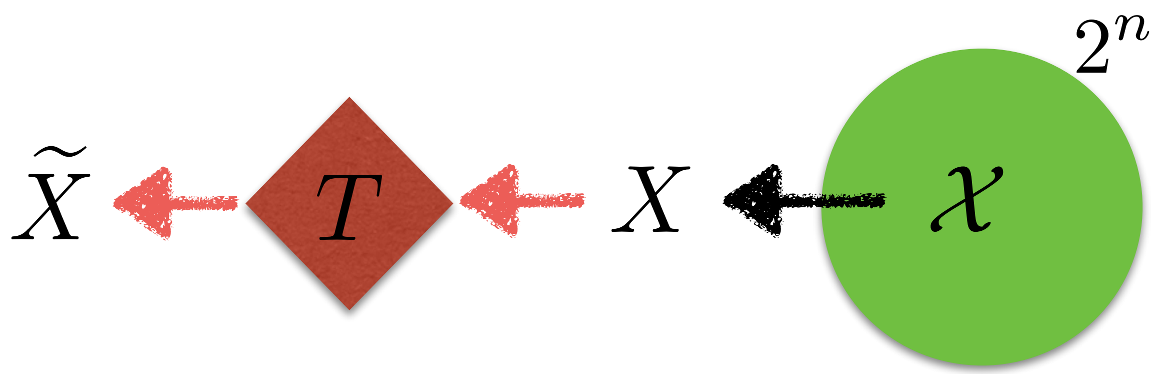
Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Proof overview of the basic conjecture

Key-question

how to define such event for any general function ?



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

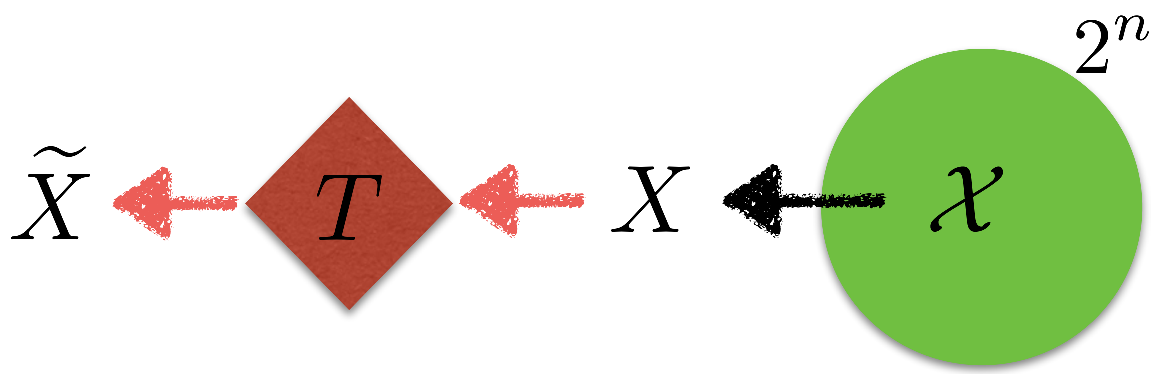
Case-1: $sup(\tilde{X})$ is "small".

Case-2: $sup(\tilde{X})$ is "not small"

Proof overview of the basic conjecture

Key-question

how to define such event for any general function ?



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-1: $sup(\tilde{X})$ is "small".

Case-2: $sup(\tilde{X})$ is "not small"

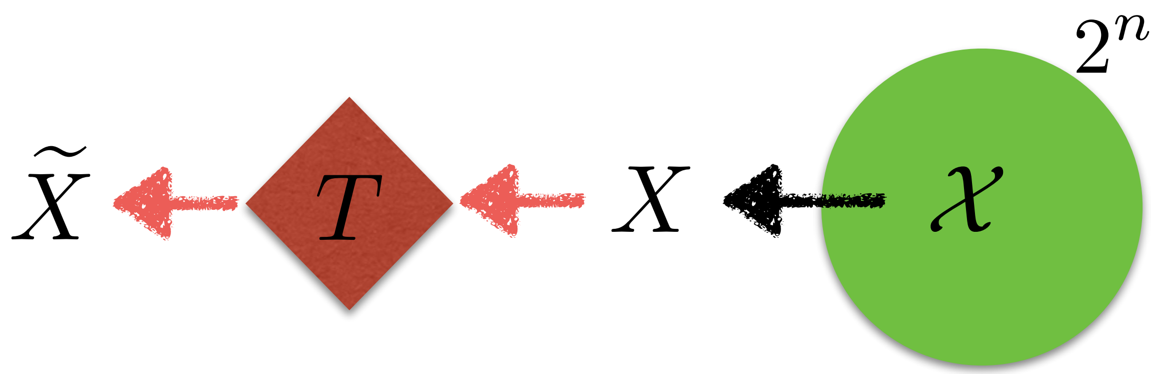
[DORS '08]

$$\widetilde{\mathbf{H}}_\infty\left(X \mid \widetilde{X}\right) \geq \mathbf{H}_\infty(X) - \log(sup(\widetilde{X}))$$

Proof overview of the basic conjecture

Key-question

how to define such event for any general function ?



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-1: $sup(\tilde{X})$ is "small"

Case-2: $sup(\tilde{X})$ is "not small"

[DORS '08]

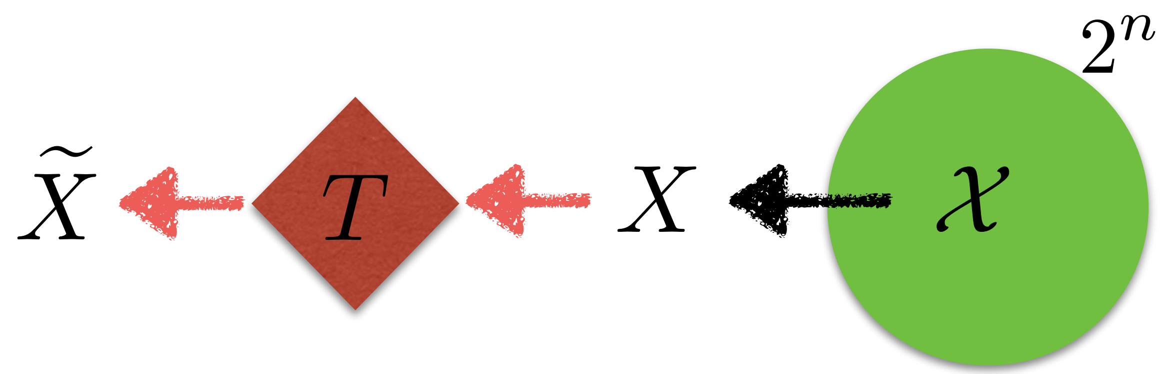
$$\widetilde{\mathbf{H}}_\infty\left(X \mid \widetilde{X}\right) \geq \mathbf{H}_\infty(X) - \log(sup(\widetilde{X}))$$

$\widetilde{\mathbf{H}}_\infty\left(X \mid \tilde{X}\right)$ always "high"

Proof overview of the basic conjecture

Key-question

how to define such event for any general function ?



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-1: $sup(\tilde{X})$ is "small"

Case-2: $sup(\tilde{X})$ is "not small"

[DORS '08]

$$\widetilde{\mathbf{H}}_\infty\left(X \mid \widetilde{X}\right) \geq \mathbf{H}_\infty(X) - \log(sup(\widetilde{X}))$$

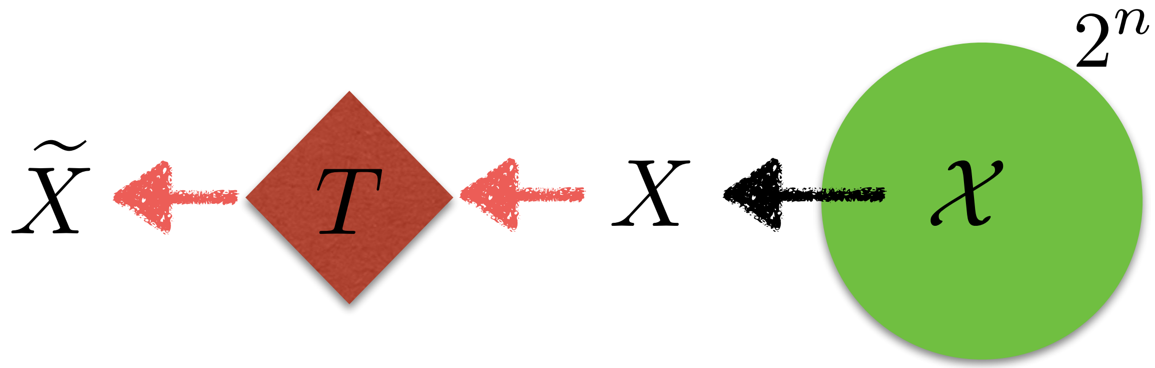
$\widetilde{\mathbf{H}}_\infty\left(X \mid \tilde{X}\right)$ always "high"

Define $E = \emptyset$

Proof overview of the basic conjecture

Key-question

how to define such event for any general function ?



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

- Case-1: $sup(\tilde{X})$ is "small"
- Case-2: $sup(\tilde{X})$ is "not small"

[DORS '08]

$$\widetilde{\mathbf{H}}_\infty\left(X \mid \widetilde{X}\right) \geq \mathbf{H}_\infty(X) - \log(sup(\widetilde{X}))$$

$\widetilde{\mathbf{H}}_\infty\left(X \mid \tilde{X}\right)$ always "high"

Define $E = \emptyset$

Handling case-2 : A basic Lemma

Handling case-2 : A basic Lemma

Lemma (Flat Area)

For any X if $sup(X)$ is "not too small" then $\exists$ E such that:

Handling case-2 : A basic Lemma

Lemma (Flat Area)

For any X if $sup(X)$ is "not too small" then $\exists\ E$ such that:

- E is flat : $\mathbf{H}_\infty\left(X_{|E}\right)$ is "high"

Handling case-2 : A basic Lemma

Lemma (Flat Area)

For any X if $sup(X)$ is "not too small" then $\exists\ E$ such that:

- E is flat : $\mathbf{H}_\infty\left(X_{|E}\right)$ is "high"
- E is large : $|sup(X_{|\bar{E}})| \ll |sup(X)|$

Handling case-2 : A basic Lemma

Lemma (Flat Area)

For any X if $sup(X)$ is "not too small" then $\exists\ E$ such that:

- E is flat : $\mathbf{H}_\infty\left(X_{|E}\right)$ is "high"
- E is large : $|sup(X_{|\bar{E}})| \ll |sup(X)|$

Proof Intuitions:

$$\mathbf{H}_\infty\left(X\right) = 1 \quad sup(X) = 9$$

Handling case-2 : A basic Lemma

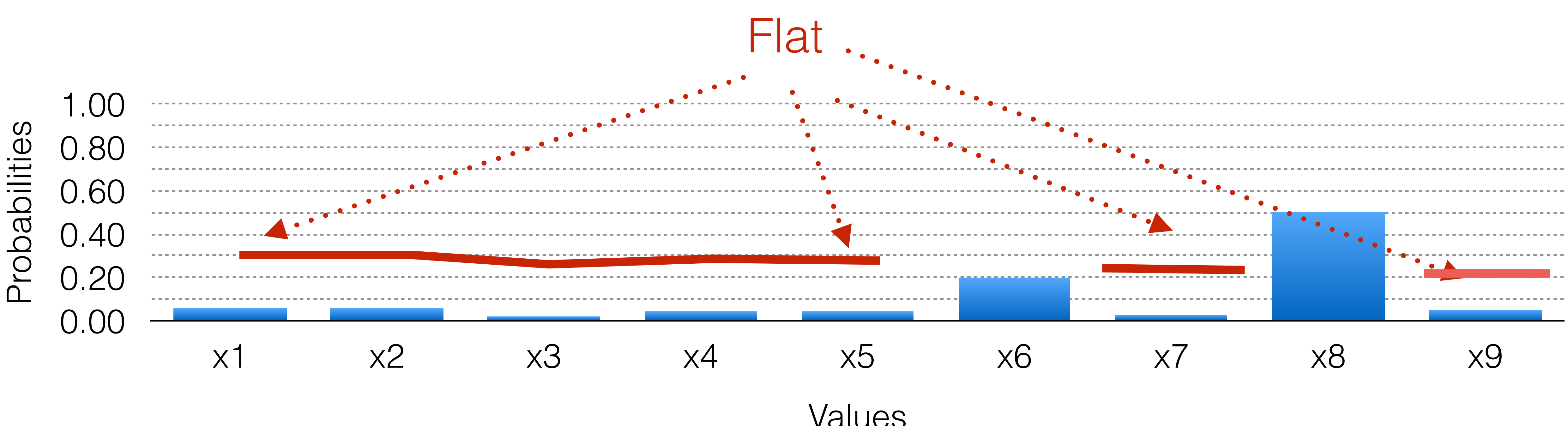
Lemma (Flat Area)

For any X if $sup(X)$ is "not too small" then $\exists\ E$ such that:

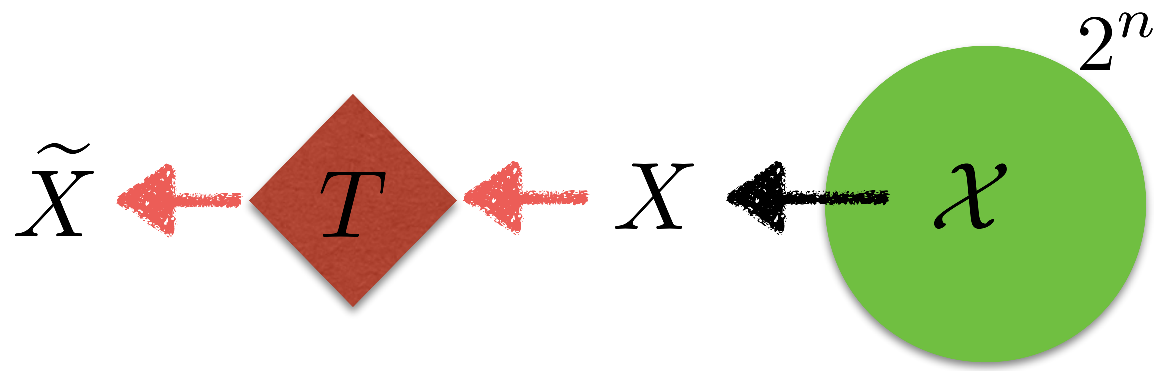
- E is flat : $\mathbf{H}_{\infty}(X_{|E})$ is "high"
- E is large : $|sup(X_{|\bar{E}})| \ll |sup(X)|$

Proof Intuitions:

$$\mathbf{H}_{\infty}(X) = 1 \quad sup(X) = 9$$



….Proof overview: Case-2

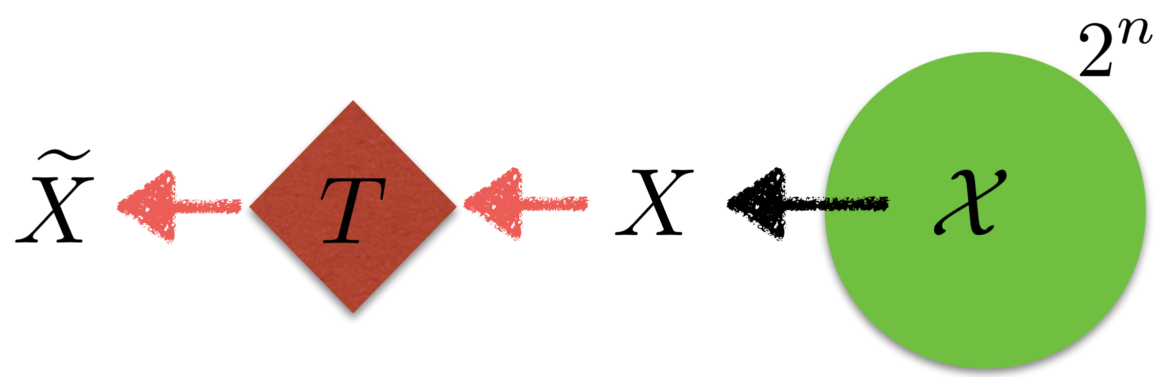


Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-2: $sup(\tilde{X})$ is "not small"

….Proof overview: Case-2



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

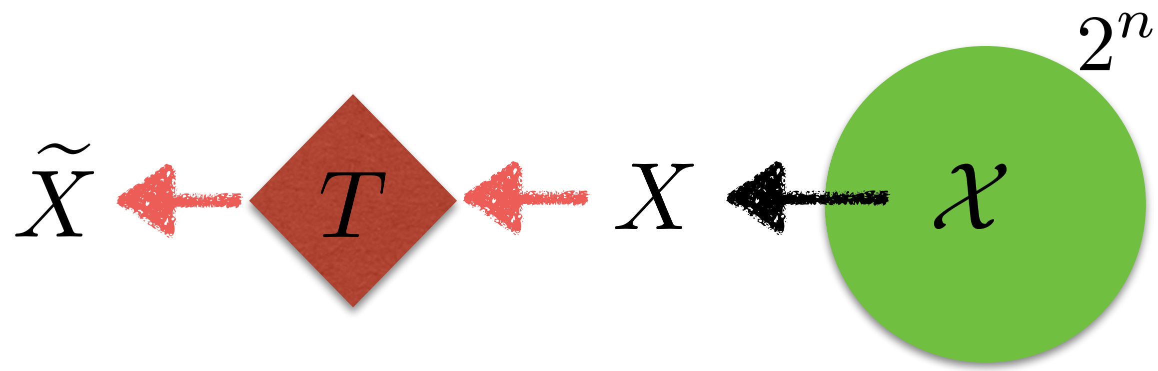
Case-2: $sup(\tilde{X})$ is "not small"

Lemma (Flat Area) ⇒ $\exists\ E\ :\ \mathbf{H}_\infty\left(\widetilde{X}_{|E}\right)$ high

&

$|sup(\widetilde{X}_{|\bar{E}})| \ll |sup(\widetilde{X})|$

….Proof overview: Case-2



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-2: $sup(\tilde{X})$ is "not small"

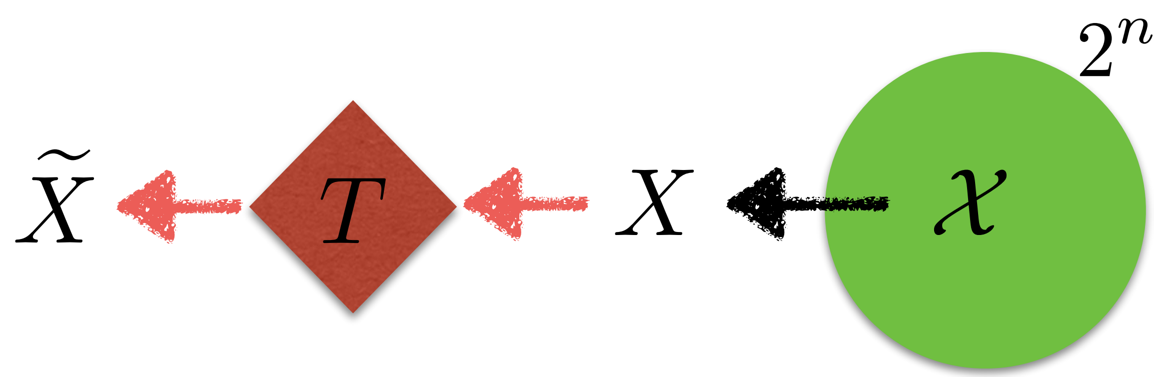
Lemma (Flat Area) ⇒ $\exists\ E\ :\ \mathbf{H}_\infty\left(\widetilde{X}_{|E}\right)$ high

&

$$|sup(\widetilde{X}_{|\bar{E}})| \ll |sup(\widetilde{X})|$$

Check if $|sup(\widetilde{X}_{|\bar{E}})|$ is "small enough"

….Proof overview: Case-2



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-2: $sup(\tilde{X})$ is "not small"

Lemma (Flat Area) ⇒ $\exists\ E : \mathbf{H}_\infty\left(\widetilde{X}_{|E}\right)$ high

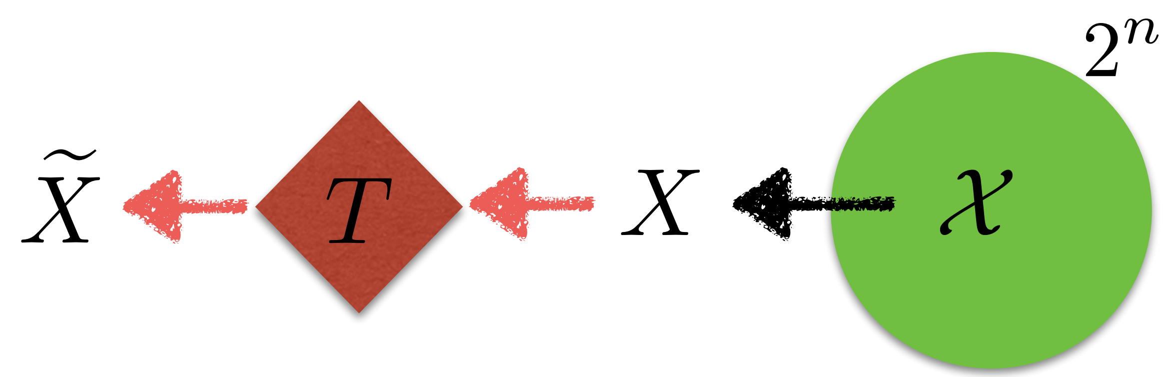
&

$|sup(\widetilde{X}_{|\bar{E}})| \ll |sup(\widetilde{X})|$

Check if $|sup(\widetilde{X}_{|\bar{E}})|$ is "small enough"

NO

….Proof overview: Case-2



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-2: $sup(\tilde{X})$ is "not small"

Lemma (Flat Area) ⇒ $\exists\ E\ :\ \mathbf{H}_\infty\left(\widetilde{X}_{|E}\right)$ high

&

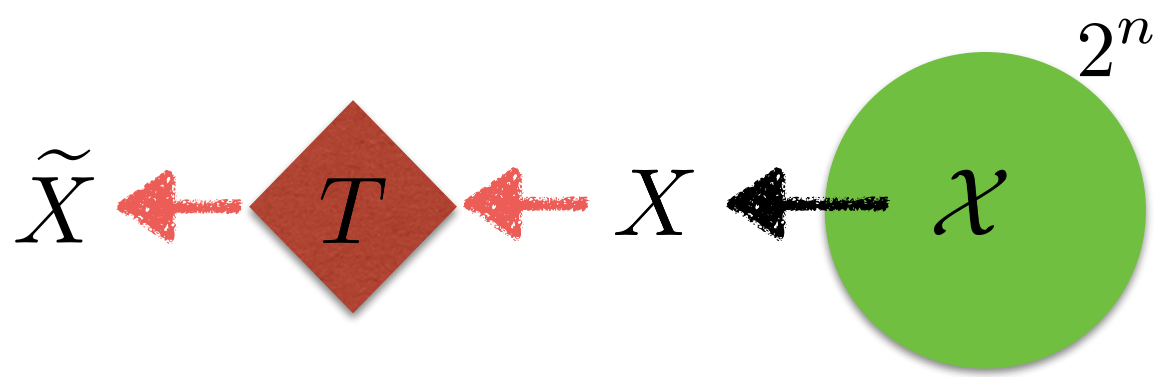
$|sup(\widetilde{X}_{|\bar{E}})| \ll |sup(\widetilde{X})|$

Check if $|sup(\widetilde{X}_{|\bar{E}})|$ is "small enough"

NO

Re-apply Lemma on $\tilde{X}_{|(\bar{E})}$ to get another flat area

….Proof overview: Case-2



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-2: $sup(\tilde{X})$ is "not small"

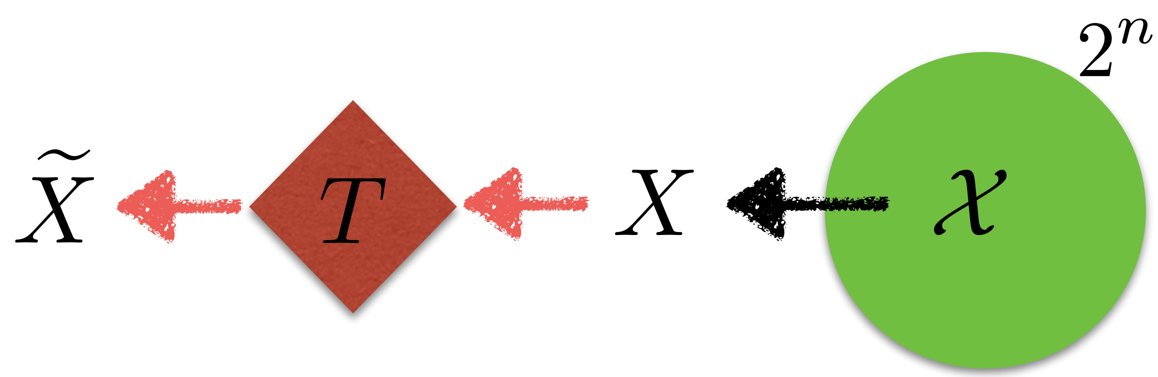
$\exists\ E'\ :\ \widetilde{\mathbf{H}}_\infty(\tilde{X}_{\bar{E}\wedge E'})$ high & $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})| \ll |sup(\widetilde{X}_{|\bar{E}})|$

Re-apply Lemma on $\tilde{X}_{|(\bar{E})}$ to get another flat area

NO

Check if $|sup(\widetilde{X}_{|\bar{E}})|$ is "small enough"

….Proof overview: Case-2



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

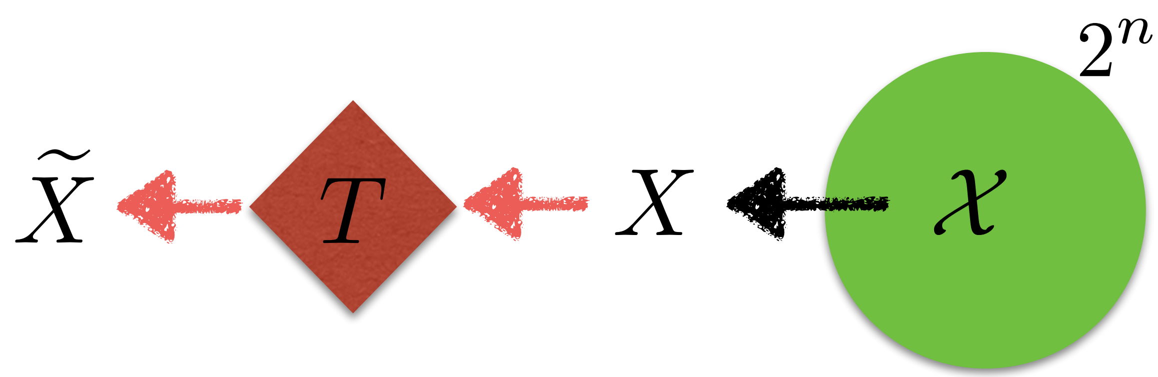
Case-2: $sup(\tilde{X})$ is "not small"

$\exists\ E'\ :\ \widetilde{\mathbf{H}}_\infty(\tilde{X}_{\bar{E}\wedge E'})$ high & $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})| \ll |sup(\widetilde{X}_{|\bar{E}})|$

Re-apply Lemma on $\tilde{X}_{|(\bar{E})}$ to get another flat area

Check if $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})|$ is "small enough"

….Proof overview: Case-2



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-2: $sup(\tilde{X})$ is "not small"

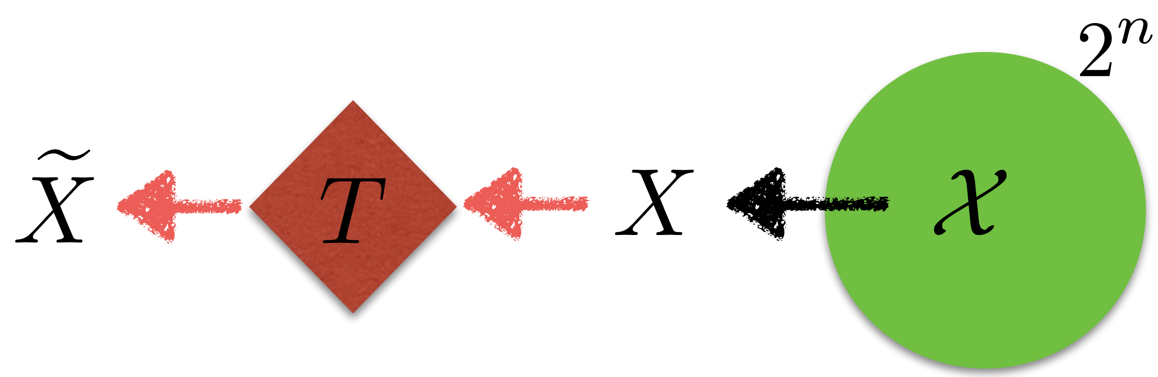
$\exists\ E'\ :\ \widetilde{\mathbf{H}}_\infty(\tilde{X}_{\bar{E}\wedge E'})$ high & $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})| \ll |sup(\widetilde{X}_{|\bar{E}})|$

Re-apply Lemma on $\tilde{X}_{|(\bar{E})}$ to get another flat area

Check if $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})|$ is "small enough"

yes

….Proof overview: Case-2



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-2: $sup(\tilde{X})$ is "not small"

$\exists\ E'\ :\ \widetilde{\mathbf{H}}_\infty(\tilde{X}_{\bar{E}\wedge E'})$ high & $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})| \ll |sup(\widetilde{X}_{|\bar{E}})|$

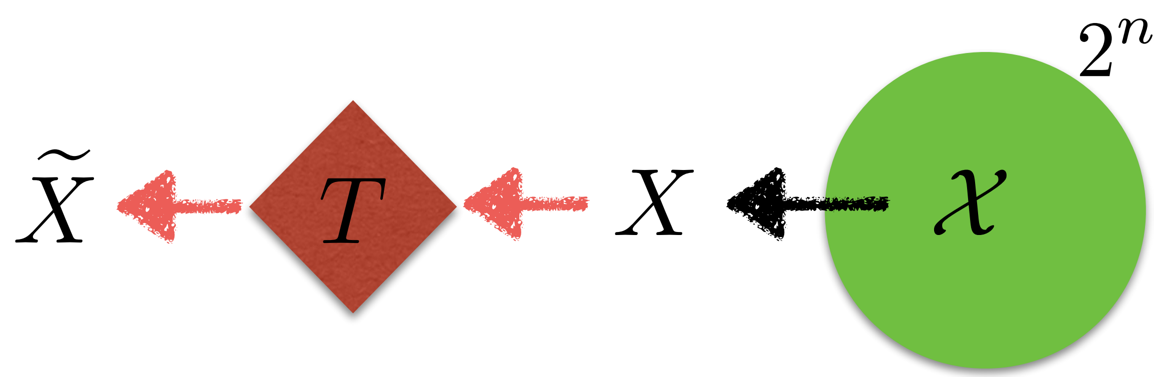
Re-apply Lemma on $\tilde{X}_{|(\bar{E})}$ to get another flat area

Check if $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})|$ is "small enough"

yes

Define $E := E \vee E'$

….Proof overview: Case-2



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-2: $sup(\tilde{X})$ is "not small"

$\exists\ E'\ :\ \widetilde{\mathbf{H}}_\infty(\tilde{X}_{\bar{E}\wedge E'})$ high & $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})| \ll |sup(\widetilde{X}_{|\bar{E}})|$

Re-apply Lemma on $\tilde{X}_{|(\bar{E})}$ to get another flat area

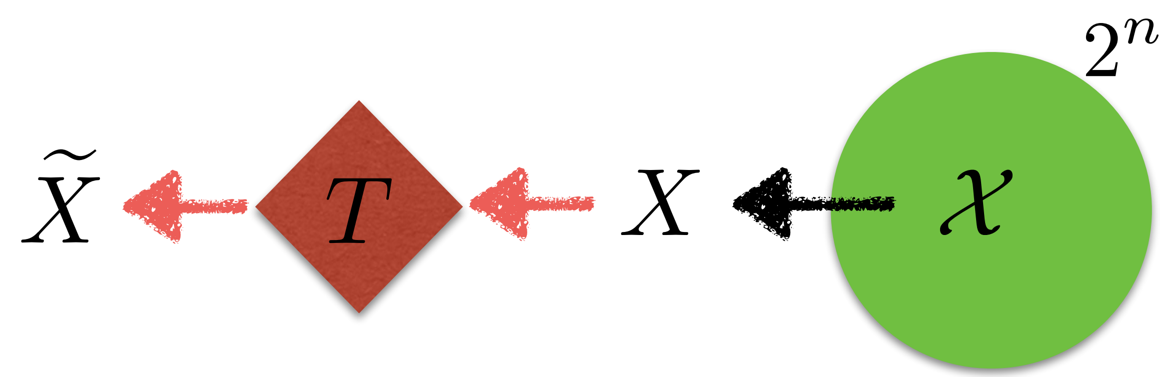
Check if $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})|$ is "small enough"

yes

Define $E := E \vee E'$

Apply DORS'08: $\widetilde{\mathbf{H}}_\infty\left(X_{|\bar{E}\wedge\bar{E}'} \mid \widetilde{X}_{|\bar{E}\wedge\bar{E}'}\right) \geq \mathbf{H}_\infty\left(X_{|\bar{E}\wedge\bar{E}'}\right) - \log(sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'}))$

….Proof overview: Case-2



Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-2: $sup(\tilde{X})$ is "not small"

$\exists\ E'\ :\ \widetilde{\mathbf{H}}_\infty(\tilde{X}_{\bar{E}\wedge E'})$ high & $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})| \ll |sup(\widetilde{X}_{|\bar{E}})|$

Re-apply Lemma on $\tilde{X}_{|(\bar{E})}$ to get another flat area

Check if $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})|$ is "small enough"

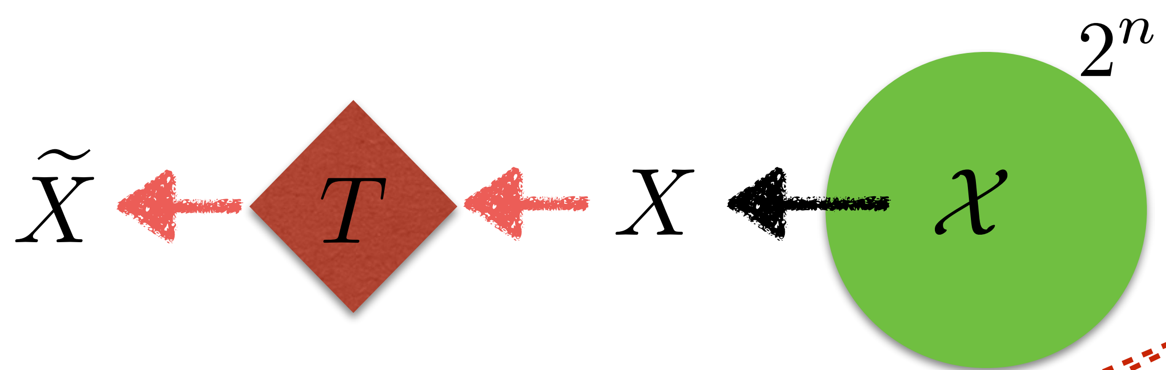
yes

Define $E := E \vee E'$

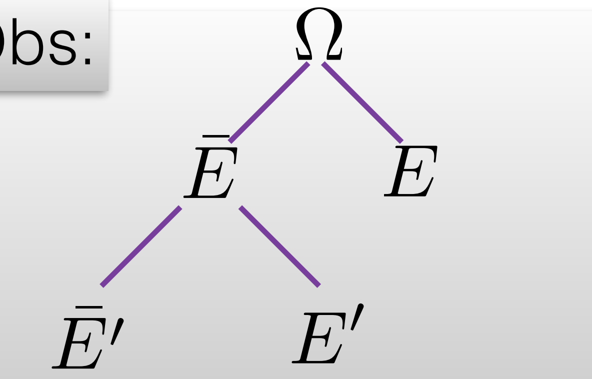
high with some loss

Apply DORS'08: $\widetilde{\mathbf{H}}_\infty\left(X_{|\bar{E}\wedge\bar{E}'} \mid \widetilde{X}_{|\bar{E}\wedge\bar{E}'}\right) \geq \mathbf{H}_\infty\left(X_{|\bar{E}\wedge\bar{E}'}\right) - \log(sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'}))$

….Proof overview: Case-2



Obs:



$\bar{E} \wedge E' \subseteq E \vee E'$

Given:

$\mathbf{H}_\infty(X)$ "high" & $\mathbf{H}_\infty\left(\widetilde{X}\right)$ "low"

Case-2: $sup(\tilde{X})$ is "not small"

$\exists\ E'$: $\widetilde{\mathbf{H}}_\infty(\tilde{X}_{\bar{E}\wedge E'})$ high & $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})| \ll |sup(\widetilde{X}_{|\bar{E}})|$

Re-apply Lemma on $\tilde{X}_{|(\bar{E})}$ to get another flat area

Check if $|sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'})|$ is "small enough"

yes

Define $E := E \vee E'$

high with some loss

Apply DORS'08: $\widetilde{\mathbf{H}}_\infty\left(X_{|\bar{E}\wedge\bar{E}'} \mid \widetilde{X}_{|\bar{E}\wedge\bar{E}'}\right) \geq \mathbf{H}_\infty\left(X_{|\bar{E}\wedge\bar{E}'}\right) - \log(sup(\widetilde{X}_{|\bar{E}\wedge\bar{E}'}))$

Proved

Conclusion

Conclusion

- Application in tamper-resilience: Any crypto-scheme with n-bit key can be protected against $\sqrt{n}$ times tampering.

Conclusion

- Application in tamper-resilience: Any crypto-scheme with n-bit key can be protected against $\sqrt{n}$ times tampering.
  - Use universal hash-function to derive a uniform key from the saved part of the chain (at least the source)

Conclusion

- Application in tamper-resilience: Any crypto-scheme with n-bit key can be protected against $\sqrt{n}$ times tampering.
  - Use universal hash-function to derive a uniform key from the saved part of the chain (at least the source)

Weakness: Tampering is non-adaptive.

Conclusion

- Application in tamper-resilience: Any crypto-scheme with n-bit key can be protected against $\sqrt{n}$ times tampering.
    - Use universal hash-function to derive a uniform key from the saved part of the chain (at least the source)

      Weakness: Tampering is non-adaptive.

- Open: more application(s) ?

Conclusion

- Application in tamper-resilience: Any crypto-scheme with n-bit key can be protected against $\sqrt{n}$ times tampering.
  - Use universal hash-function to derive a uniform key from the saved part of the chain (at least the source)

⚠ Weakness: Tampering is non-adaptive.

- Open: more application(s) ?

Thank You !