CELLULAR AUTOMATA

Pseudo Random Number Generators and Their Resistance to Asynchrony

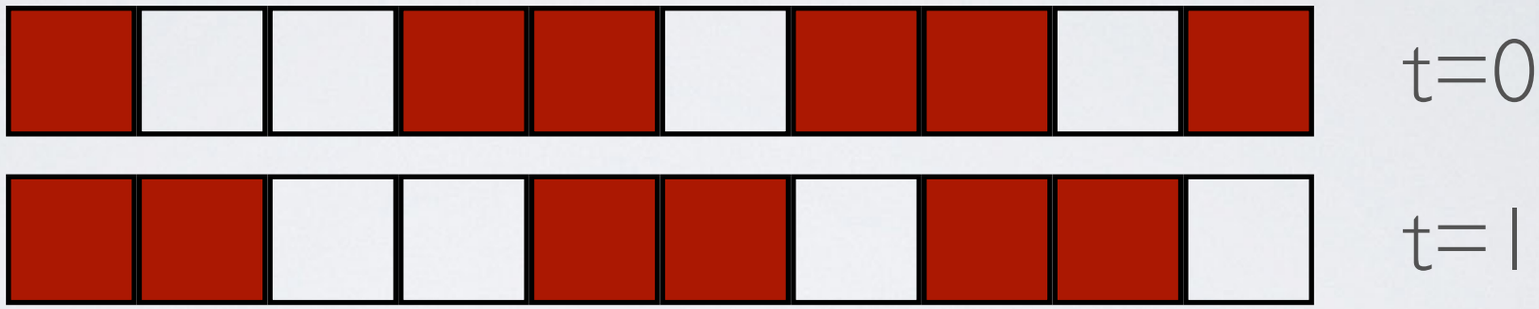
Luca {Manzoni, Mariot}

Università degli Studi di Milano-Bicocca

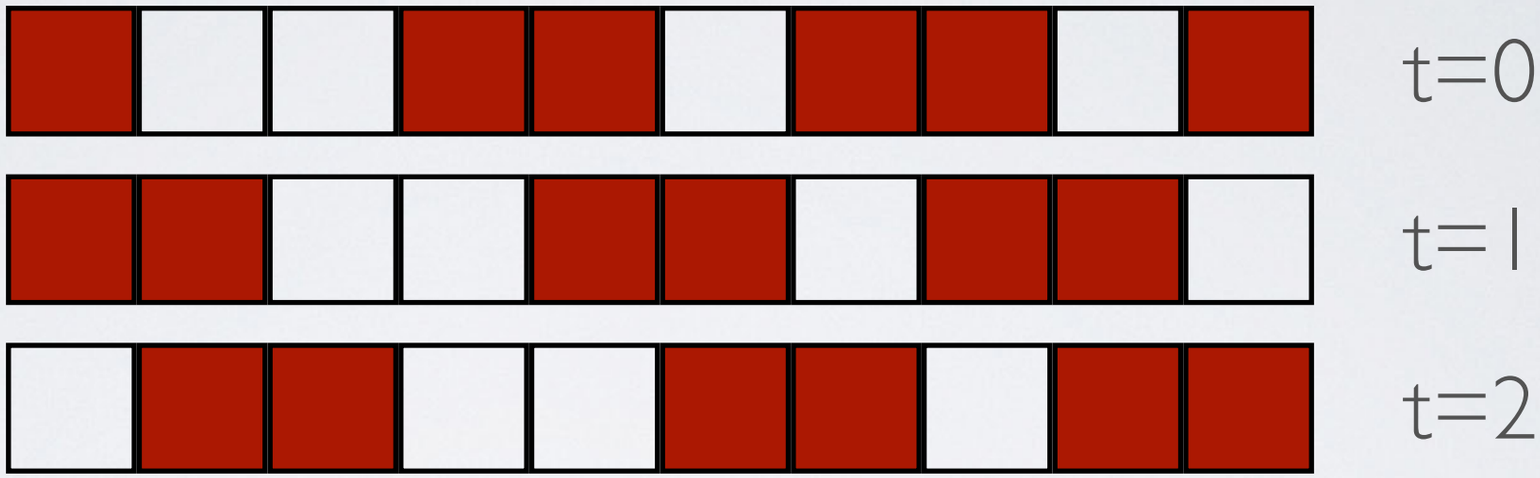
CA AS PRNG

t=0

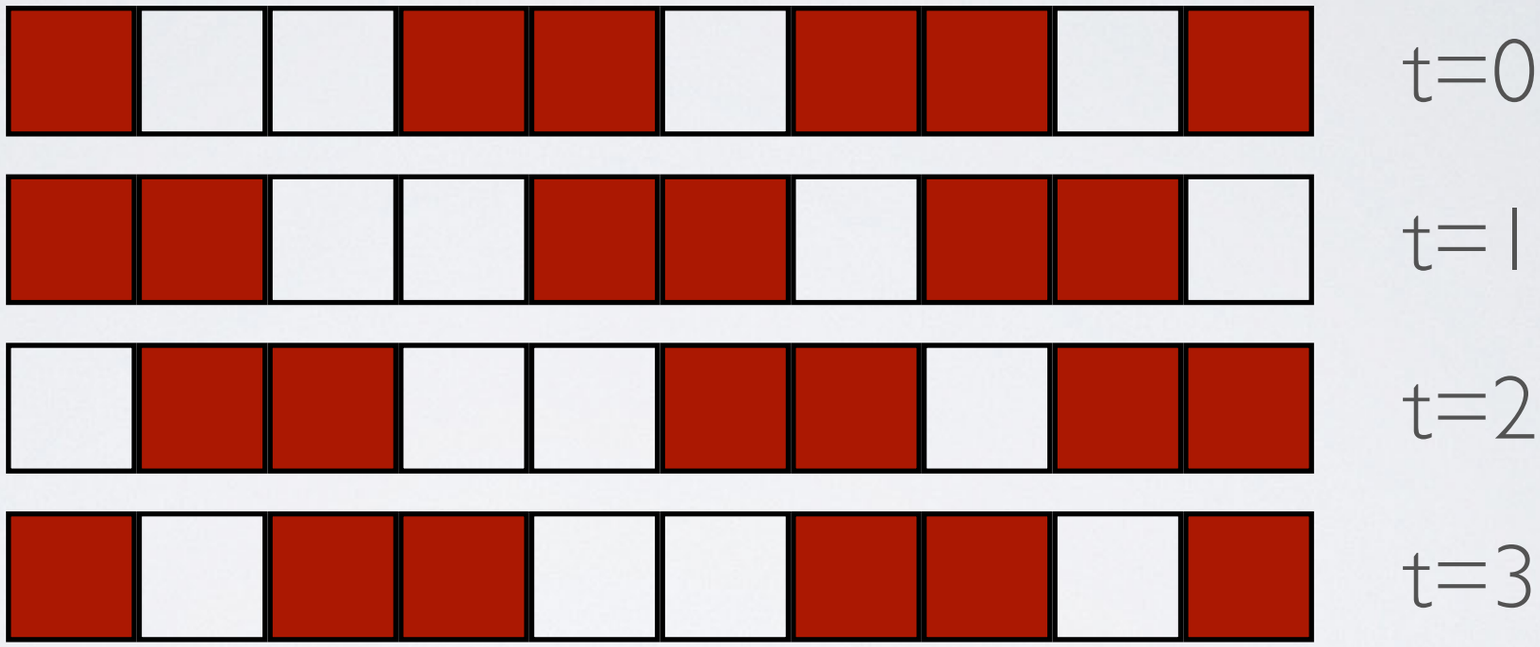
CA AS PRNG



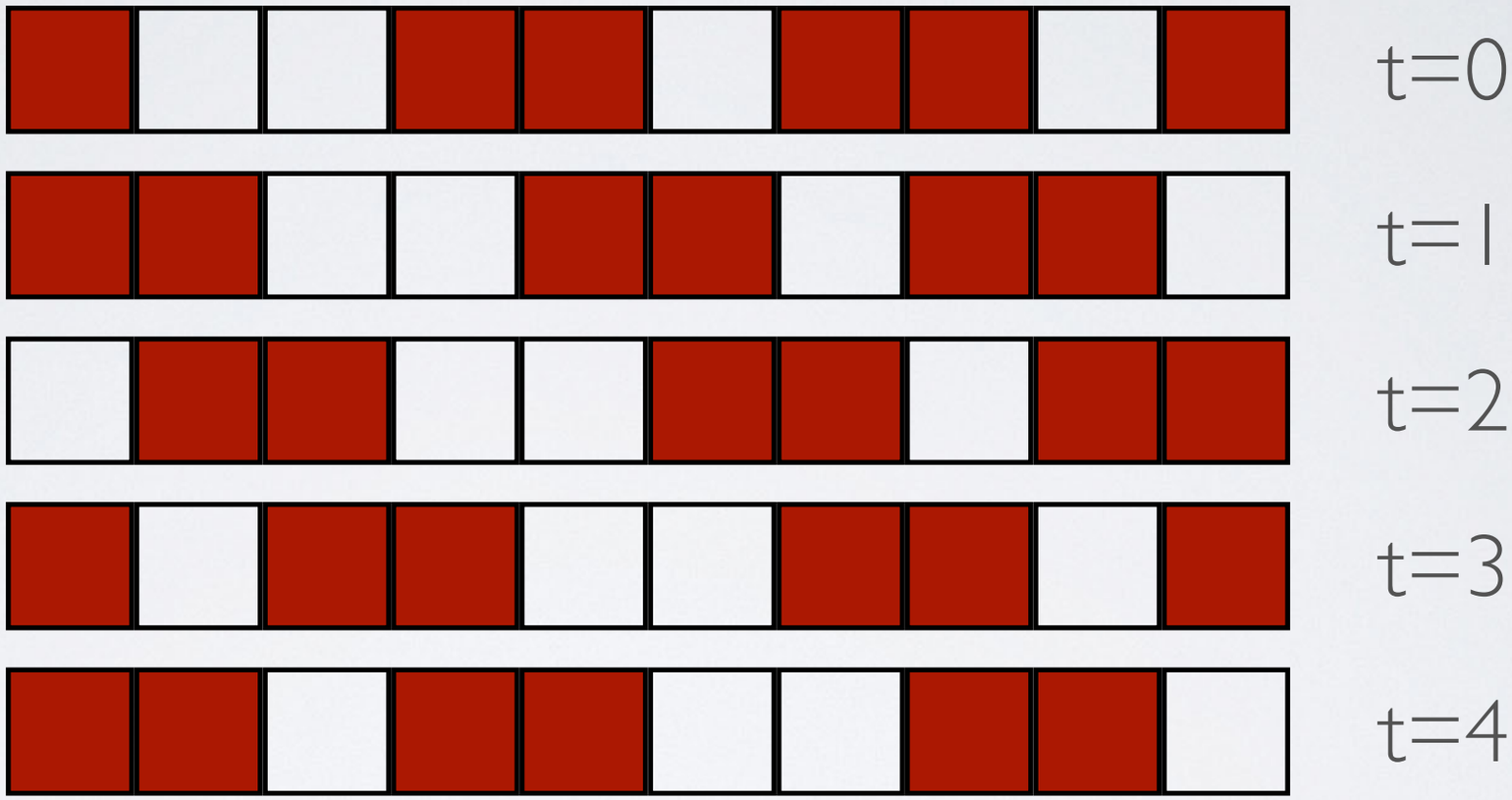
CA AS PRNG



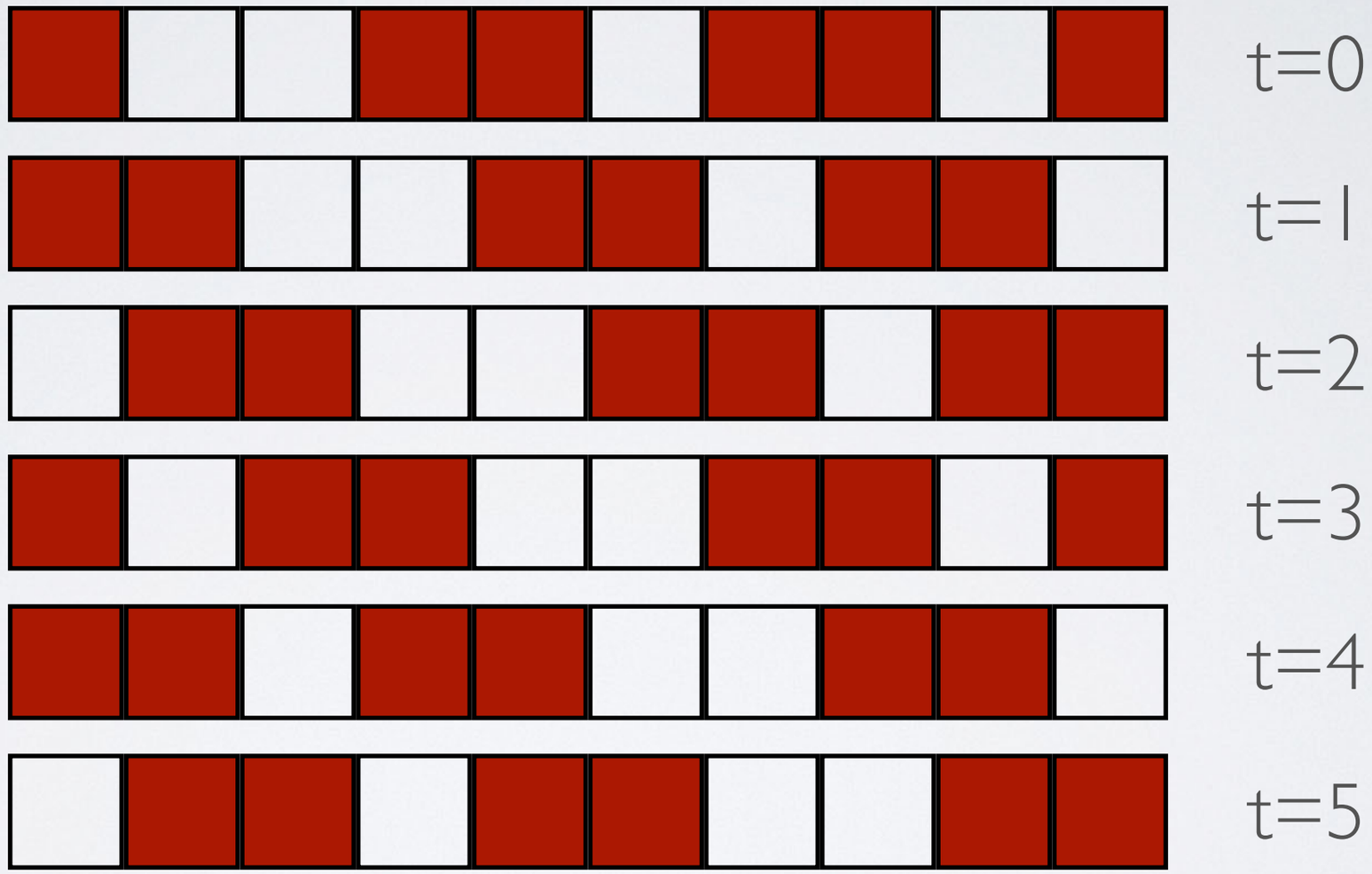
CA AS PRNG



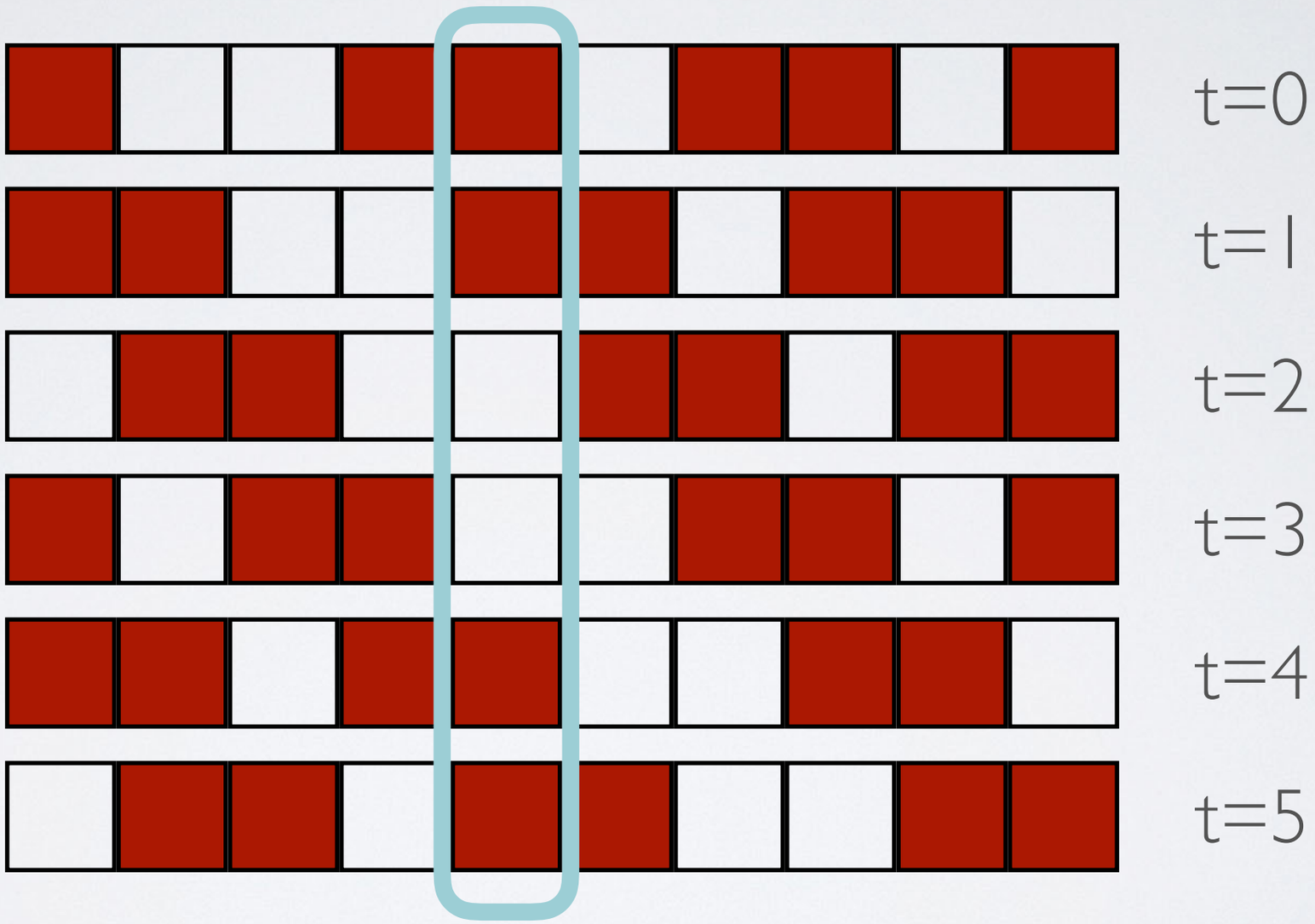
CA AS PRNG



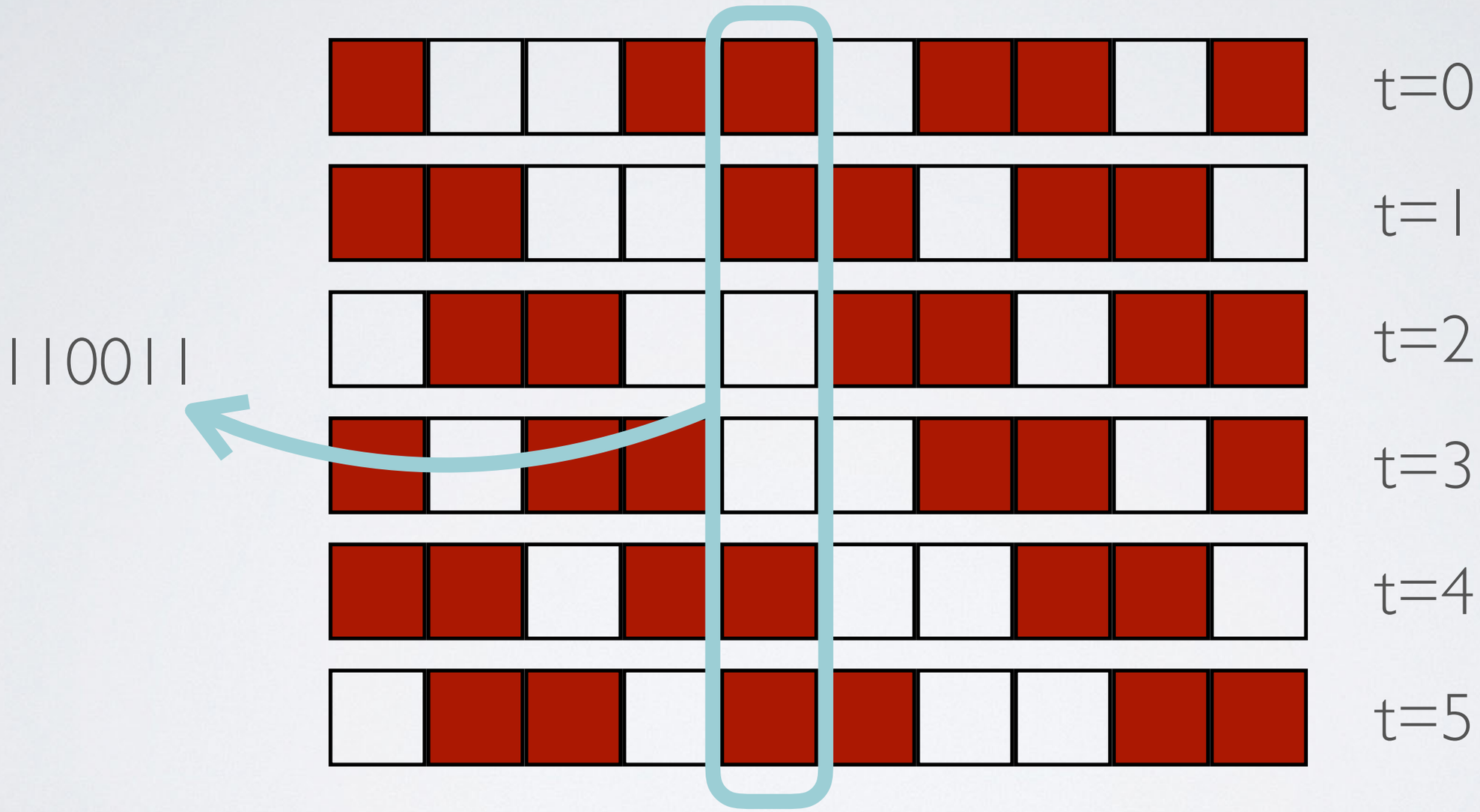
CA AS PRNG



CA AS PRNG



CA AS PRNG



WHY ARE THEY USEFUL?

WHY ARE THEY USEFUL?

- PRNG are essential cryptographic primitives

WHY ARE THEY USEFUL?

- PRNG are essential cryptographic primitives
- CA can be fast!

WHY ARE THEY USEFUL?

- PRNG are essential cryptographic primitives
- CA can be fast!
- But, how can they be attacked?

GOOD RULES FOR PRNG

GOOD RULES FOR PRNG

- Balanced

GOOD RULES FOR PRNG

- Balanced
- Non-linear

GOOD RULES FOR PRNG

- Balanced
- Non-linear
- First order correlation immune

SCENARIO

SCENARIO

CA-based PRNG

SCENARIO

CA-based PRNG

Encrypted Message

SCENARIO

CA-based PRNG

Encrypted Message

SCENARIO

I find your lack of asynchrony disturbing

CA-based PRNG

Encrypted Message

SCENARIO

I find your lack of asynchrony disturbing

ACA-based PRNG

~~CA-based PRNG~~

Encrypted Message

ASYNCHRONY

ASYNCHRONY

- Not all cells update at the same time

ASYNCHRONY

- Not all cells update at the same time
- Many kinds of asynchronous CA

ASYNCHRONY

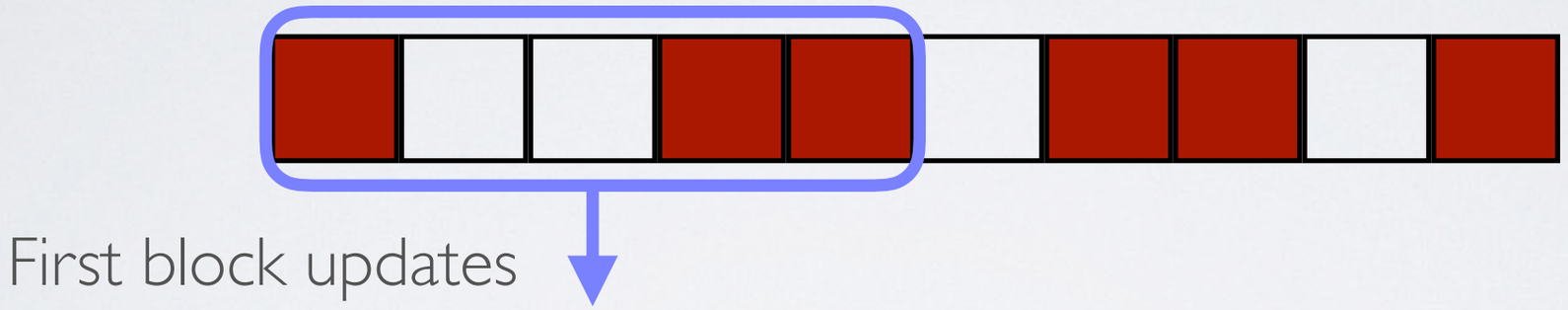
- Not all cells update at the same time
- Many kinds of asynchronous CA
- Here: "block" asynchrony

BLOCK ASYNCHRONY

k=2

BLOCK ASYNCHRONY

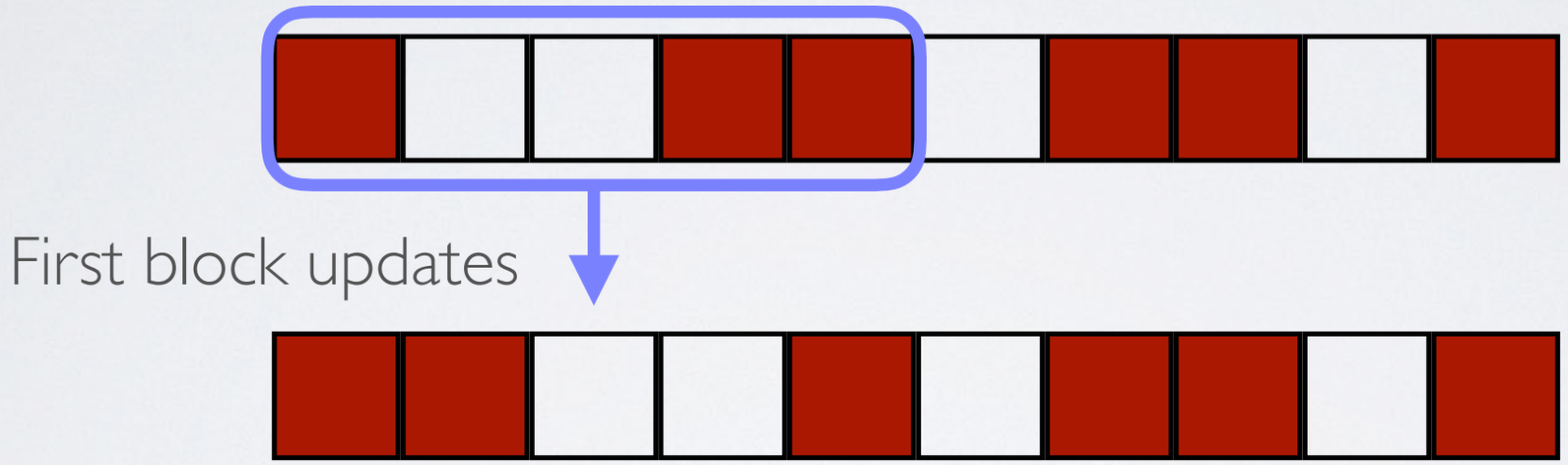
k=2



First block updates

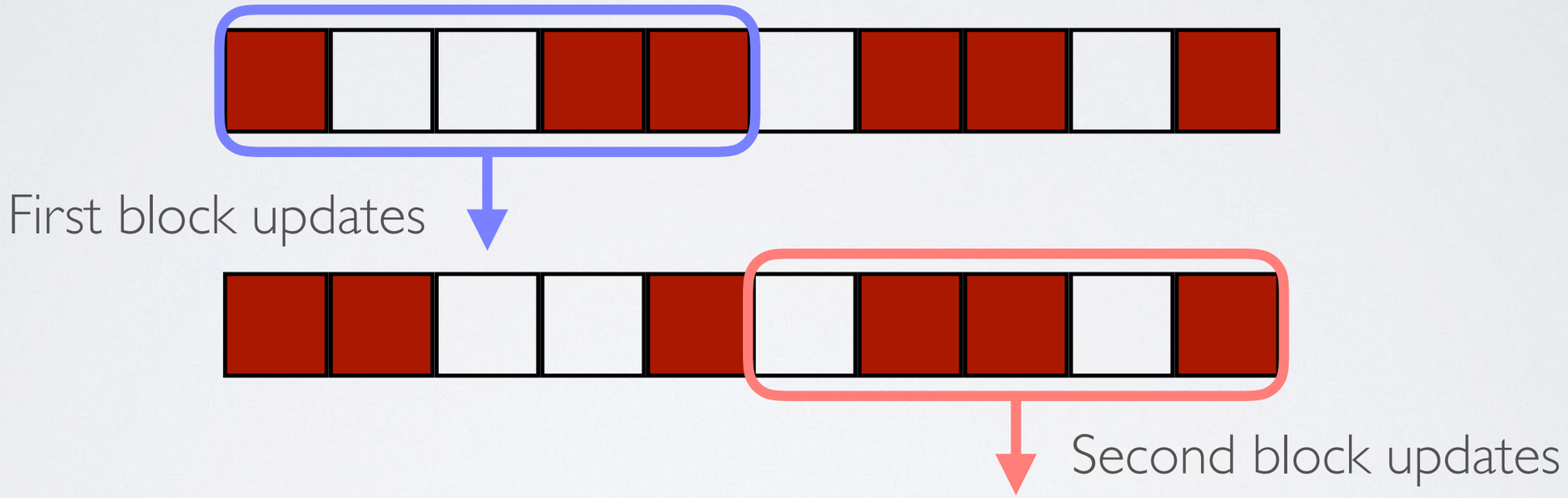
BLOCK ASYNCHRONY

k=2



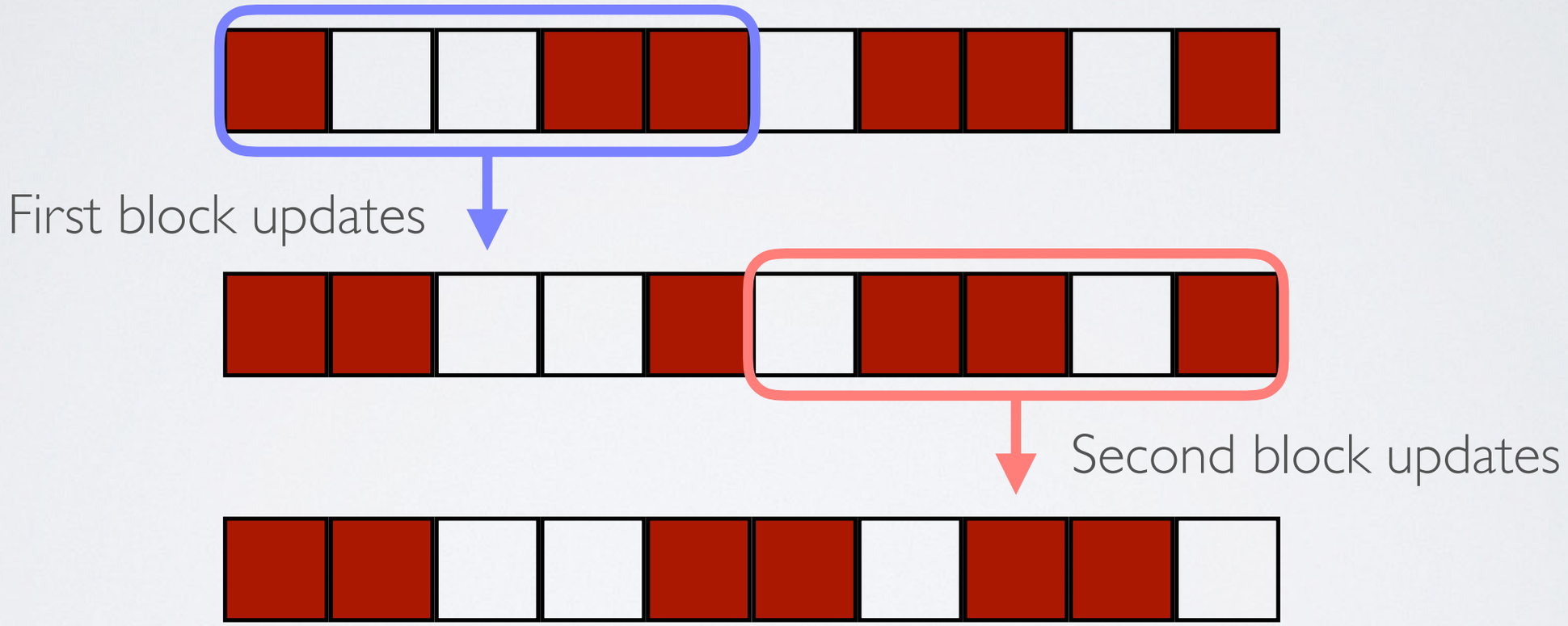
BLOCK ASYNCHRONY

k=2



BLOCK ASYNCHRONY

k=2



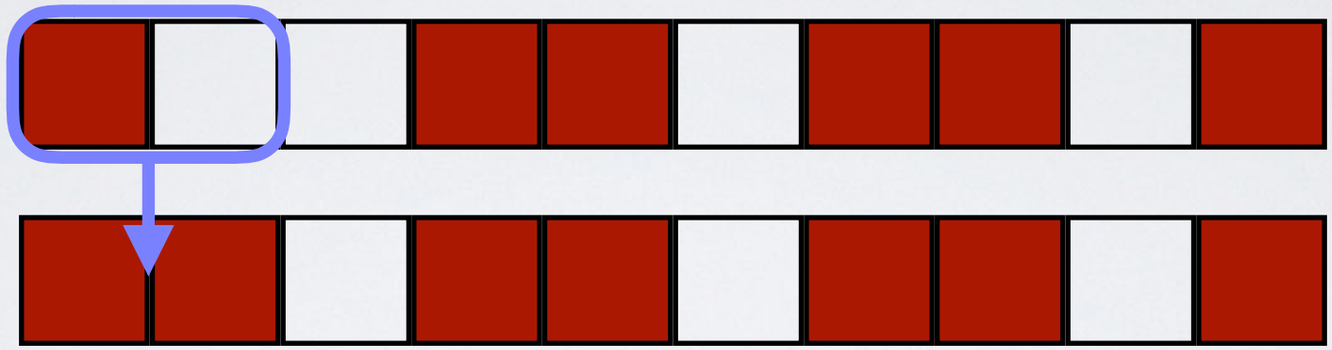
BLOCK ASYNCHRONY

k=5

BLOCK ASYNCHRONY

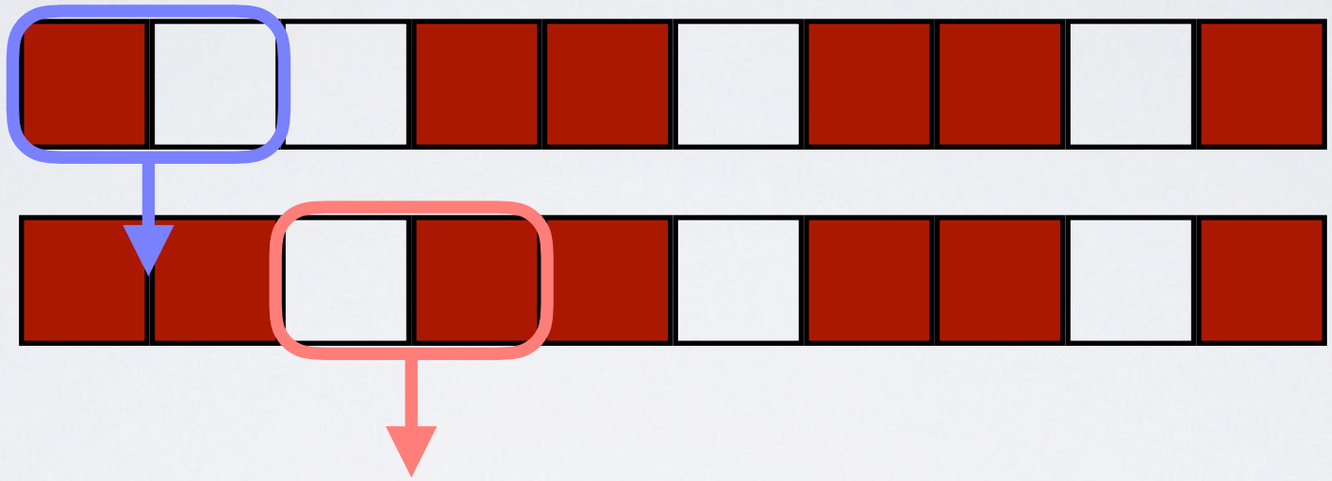
BLOCK ASYNCHRONY

k=5



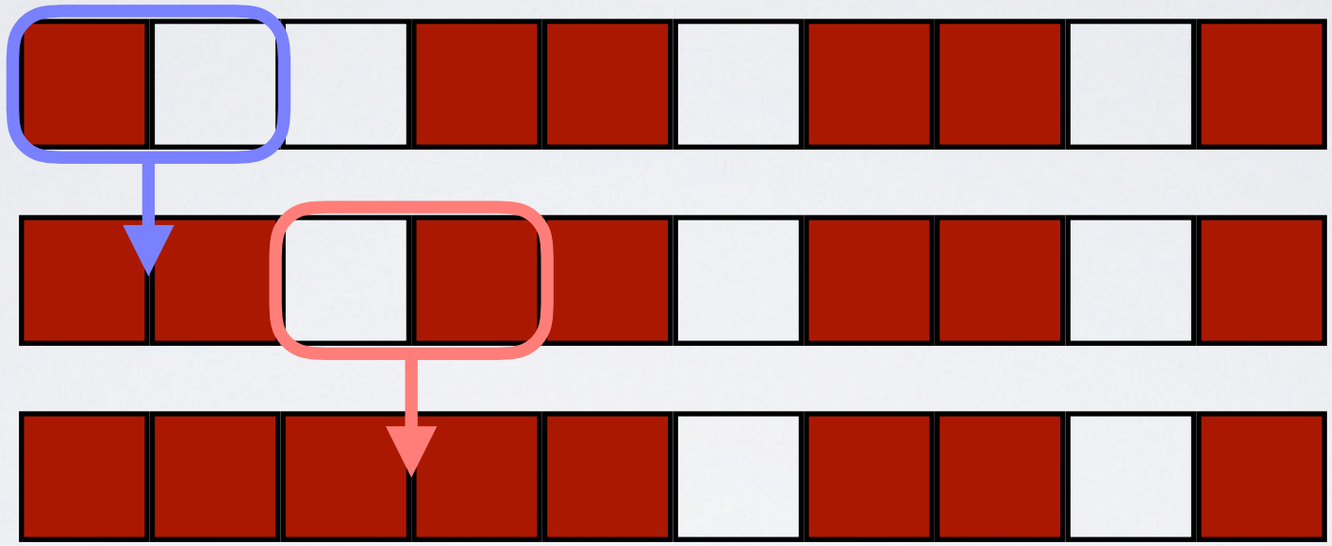
BLOCK ASYNCHRONY

k=5

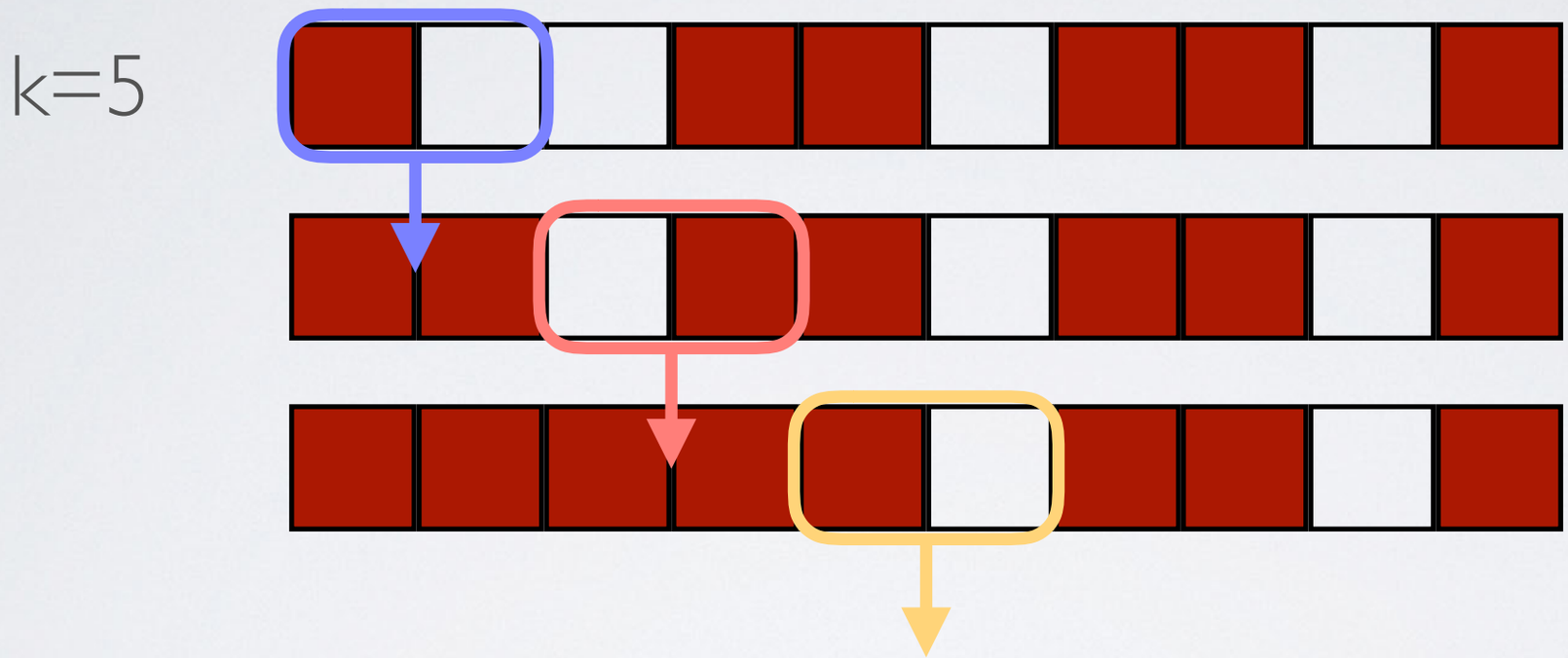


BLOCK ASYNCHRONY

k=5

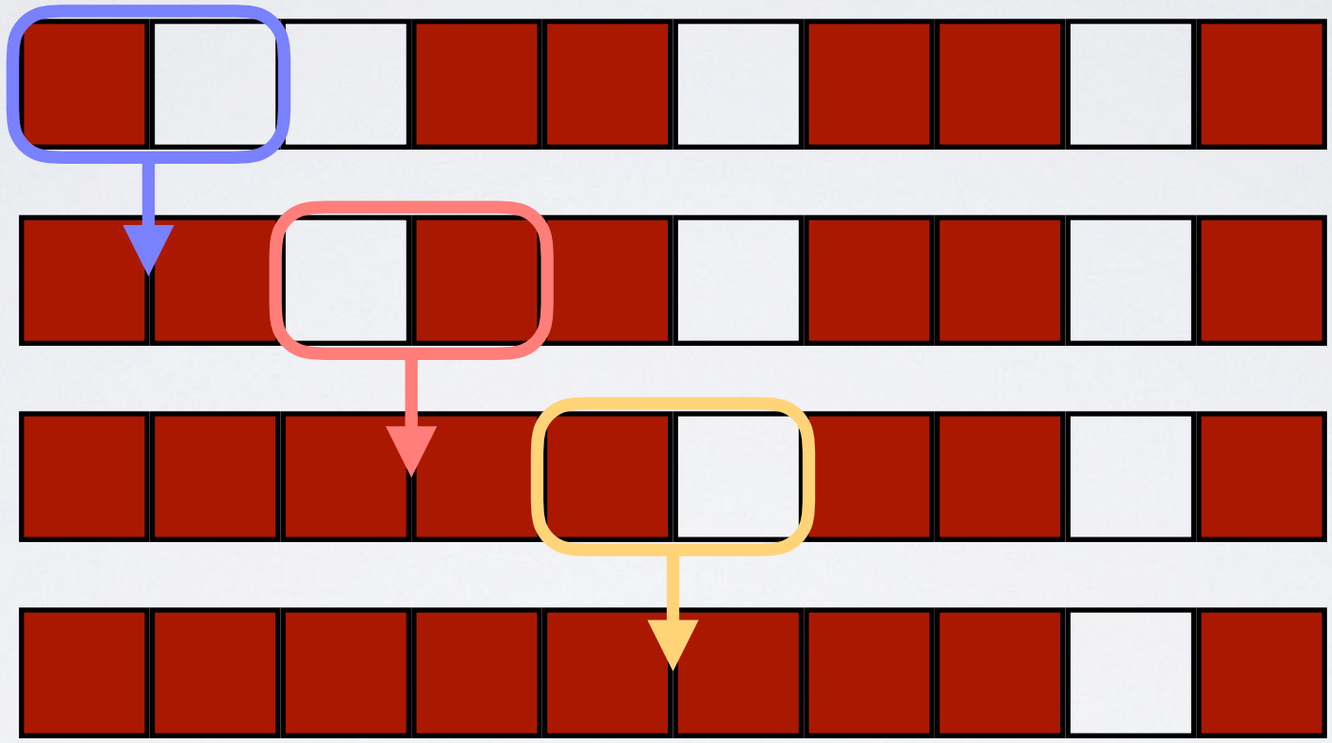


BLOCK ASYNCHRONY



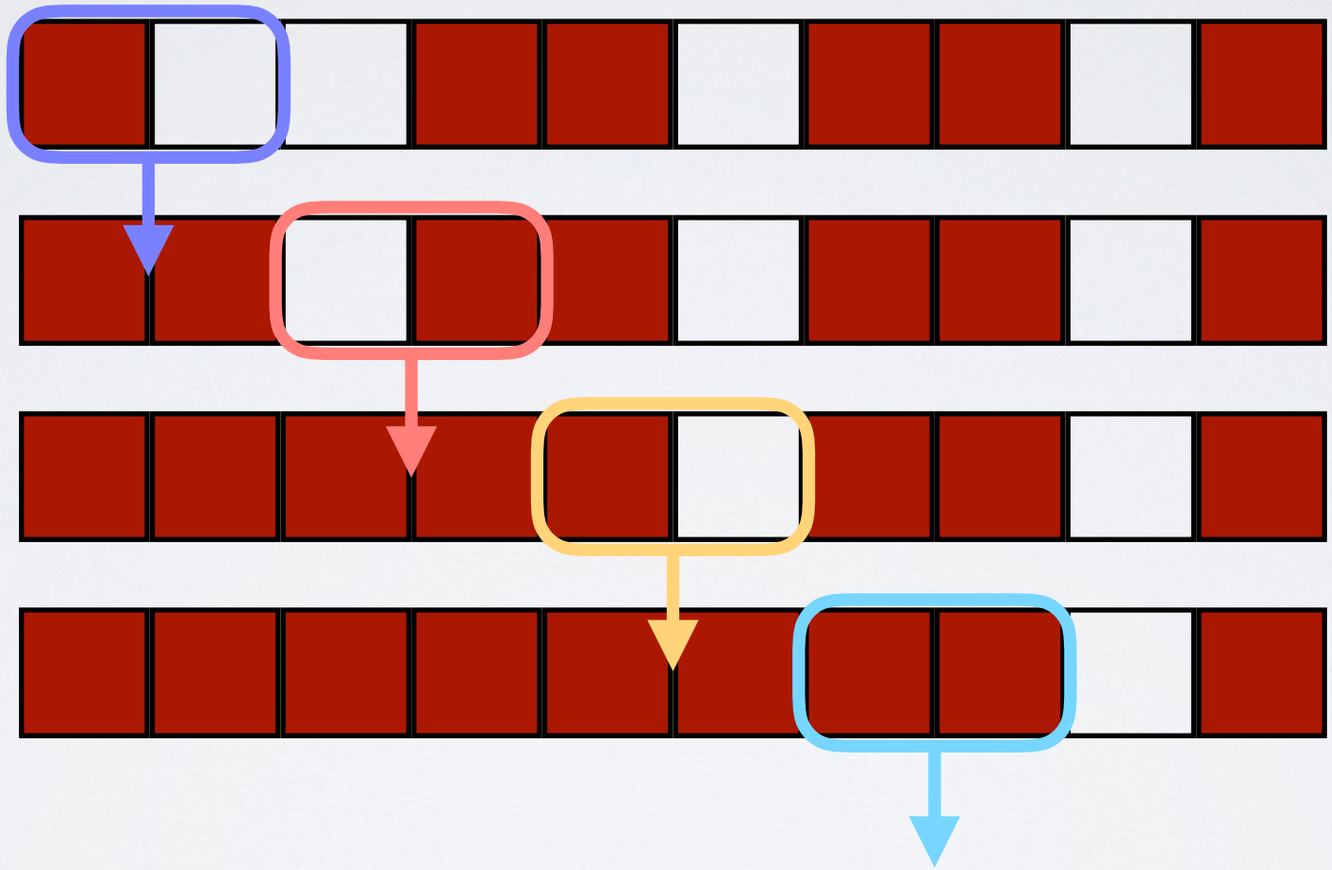
BLOCK ASYNCHRONY

k=5



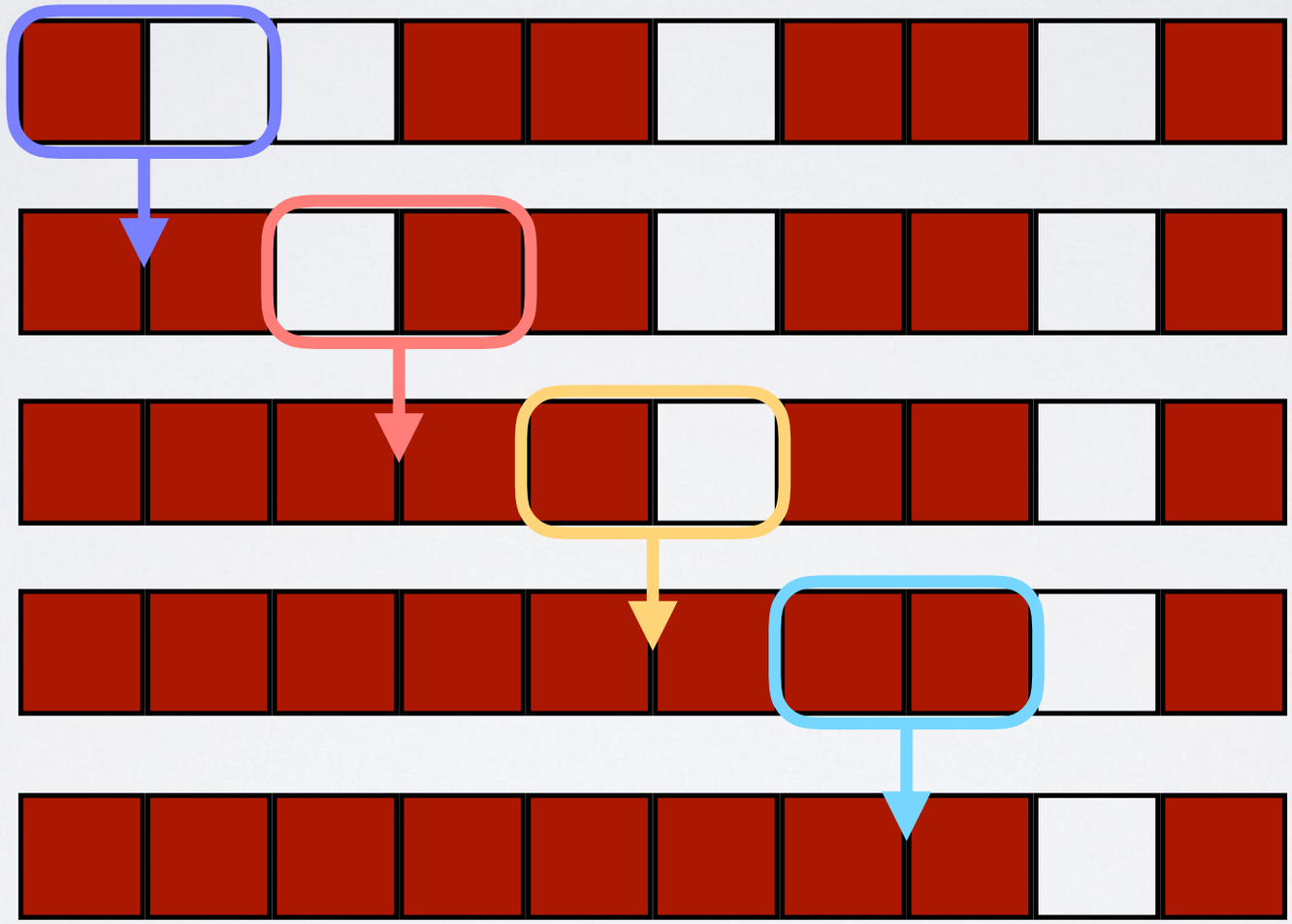
BLOCK ASYNCHRONY

k=5



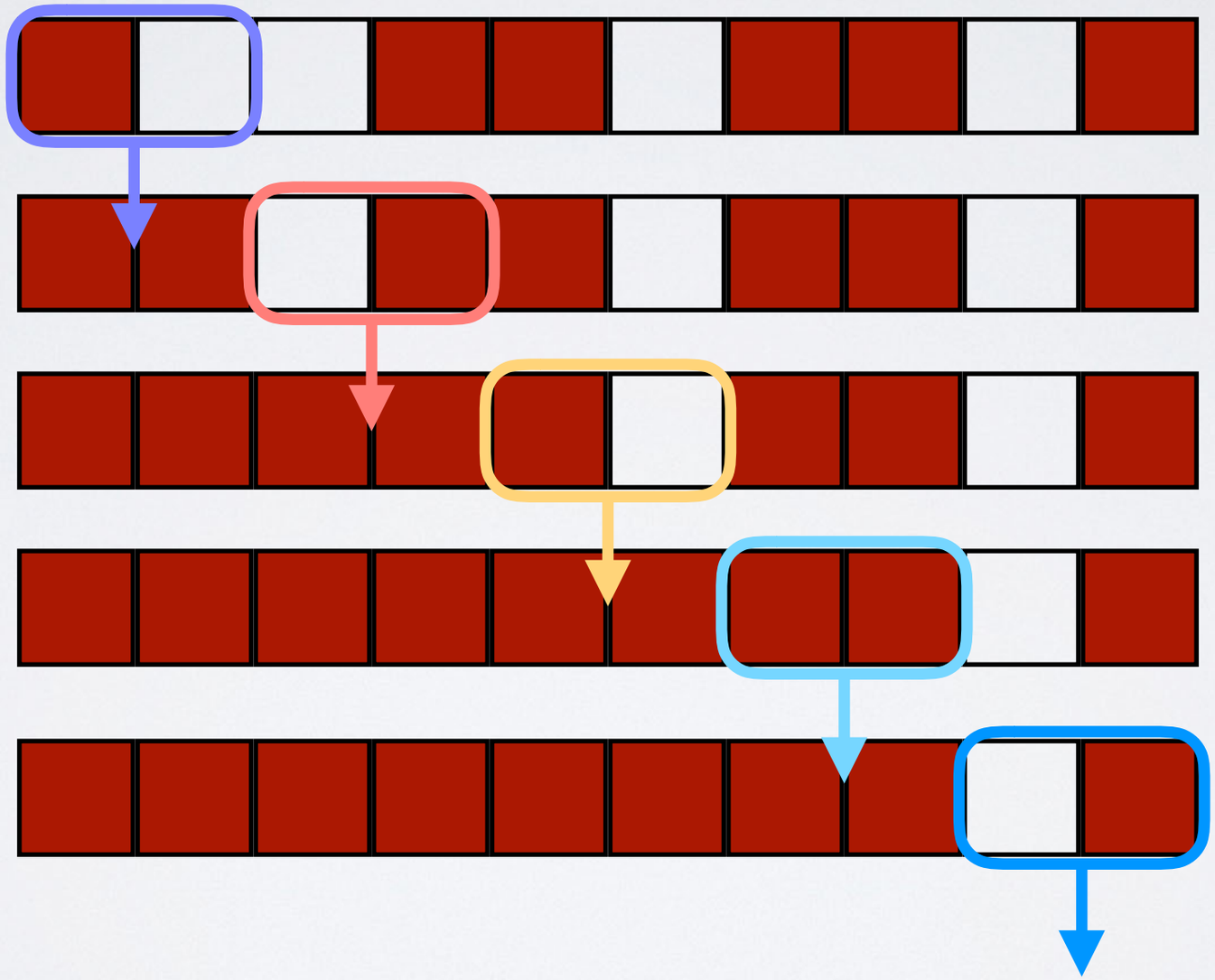
BLOCK ASYNCHRONY

k=5



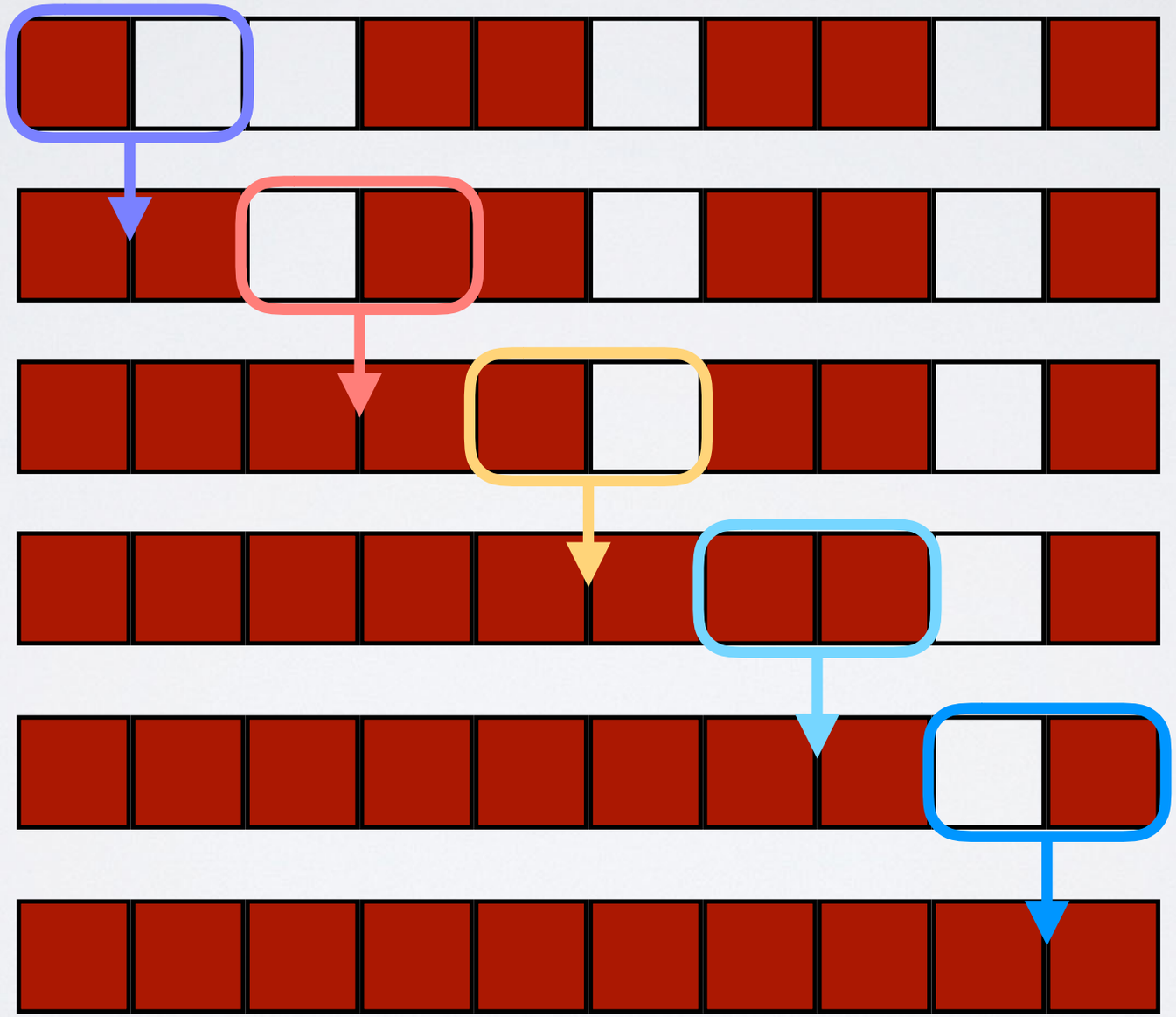
BLOCK ASYNCHRONY

k=5



BLOCK ASYNCHRONY

k=5



THE QUESTIONS

THE QUESTIONS

- How asynchrony influences the PRNG strength?

THE QUESTIONS

- How asynchrony influences the PRNG strength?
- Which CA are resistant to asynchrony?

THE QUESTIONS

- How asynchrony influences the PRNG strength?
- Which CA are resistant to asynchrony?
- Can asynchrony increase PRNG strength?

EXPERIMENTS

EXPERIMENTS

- NIST test suite: 188 statistical tests

EXPERIMENTS

- NIST test suite: 188 statistical tests
- Balanced elementary rules

EXPERIMENTS

- NIST test suite: 188 statistical tests
- Balanced elementary rules
- Initial configuration: 64 bits

EXPERIMENTS

- NIST test suite: 188 statistical tests
- Balanced elementary rules
- Initial configuration: 64 bits
- 10^3 repetitions each producing 10^6 bits

EXPERIMENTS

- NIST test suite: 188 statistical tests
- Balanced elementary rules
- Initial configuration: 64 bits
- 10^3 repetitions each producing 10^6 bits
- Asynchrony k=1, 2, 4, 8, 16, 32, 64

THREE TYPES

THREE TYPES

- **Plateau**: remains strong

THREE TYPES

- **Plateau**: remains strong
- **Hill**: from strong to stronger

THREE TYPES

- **Plateau**: remains strong
- **Hill**: from strong to stronger
- **Mountain**: from weak to strong

THREE TYPES

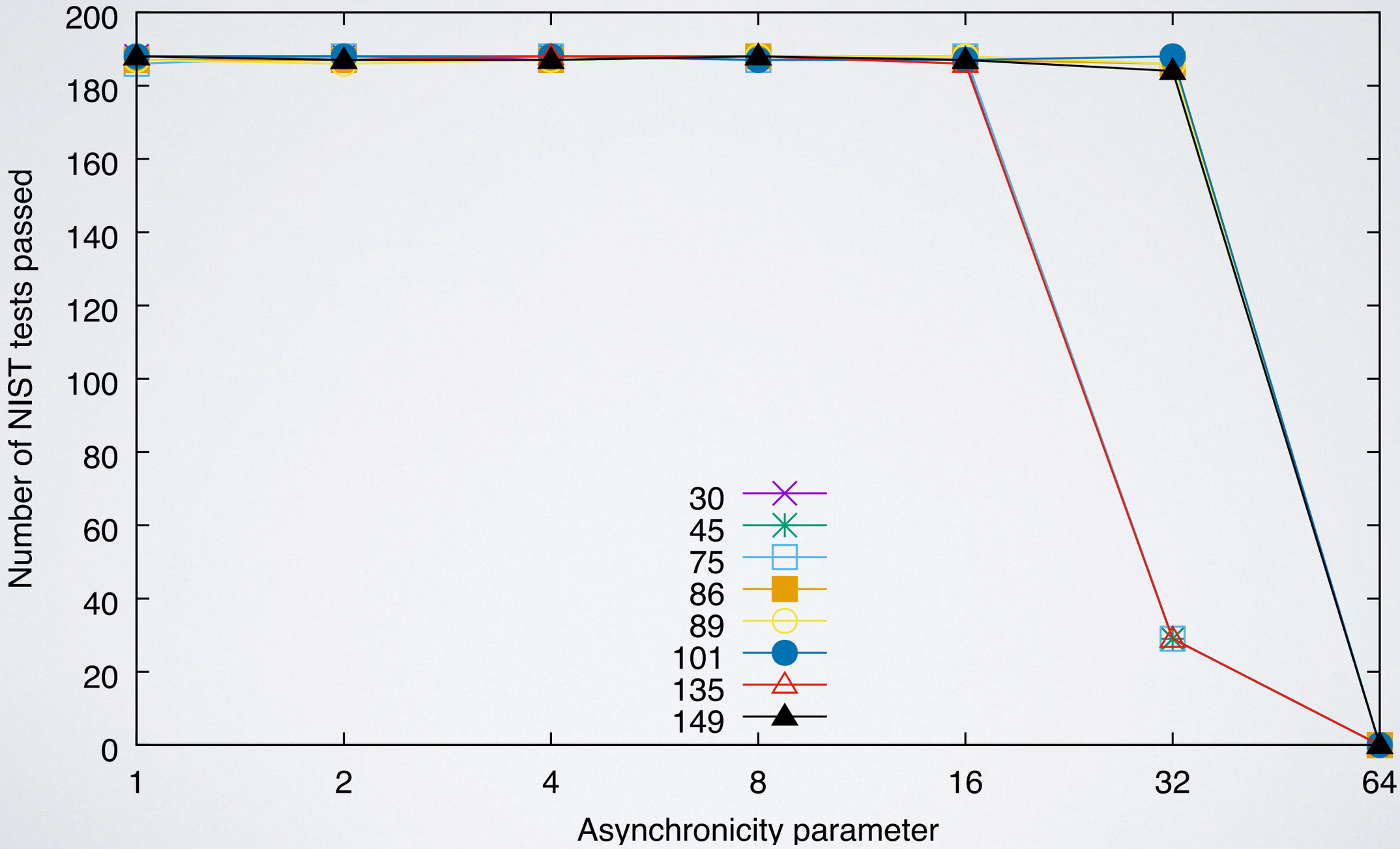
- **Plateau**: remains strong
- **Hill**: from strong to stronger
- **Mountain**: from weak to strong
- Max asynchrony = weak PRNG in all cases

THREE TYPES

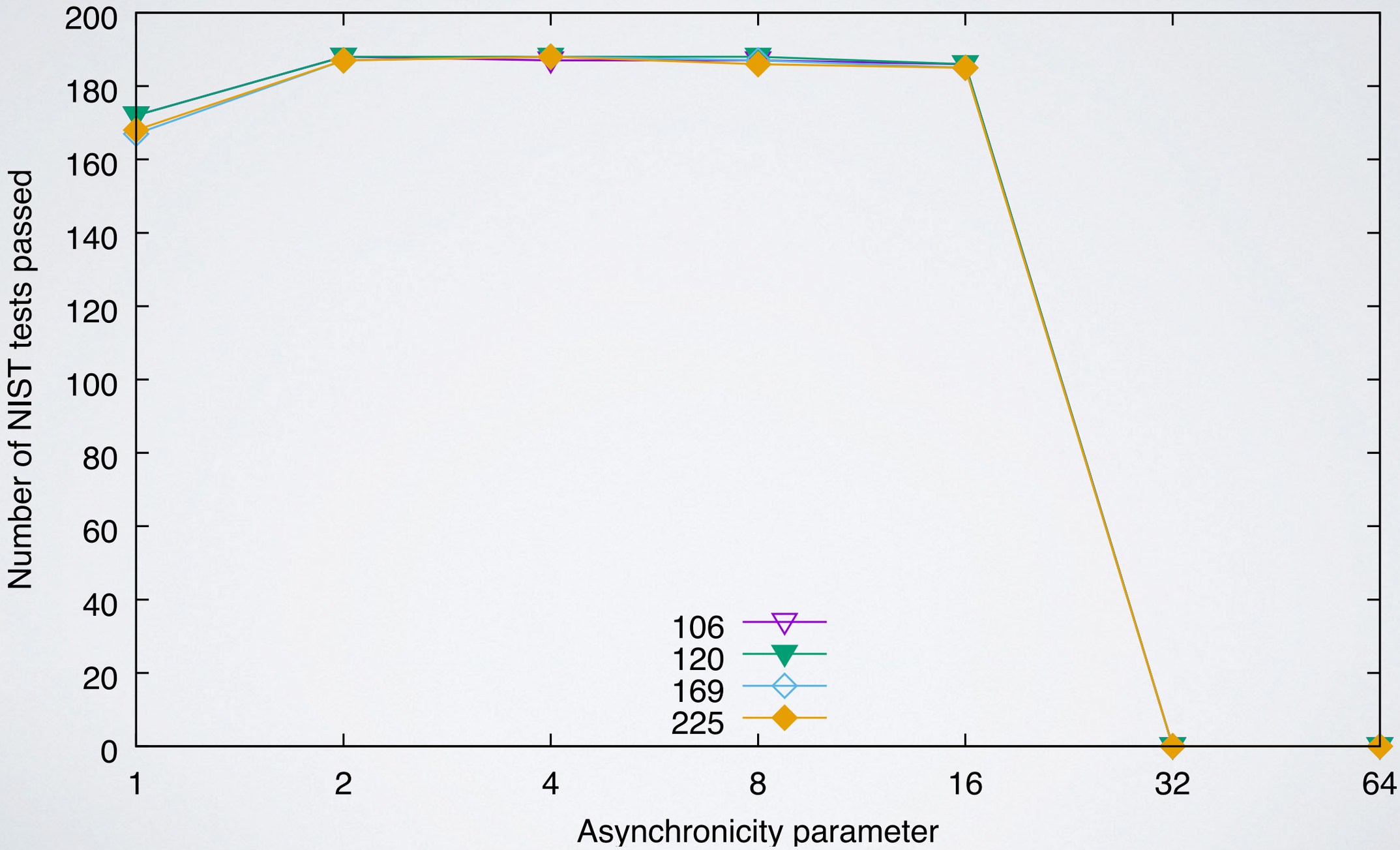
Type 1	Type 2	Type 3
30, 45, 75, 86, 89, 101, 135, 149	106, 120, 169, 225	60, 90, 105, 150, 154, 165, 166, 180, 195, 210

Every other rule is alway weak as a PRNG

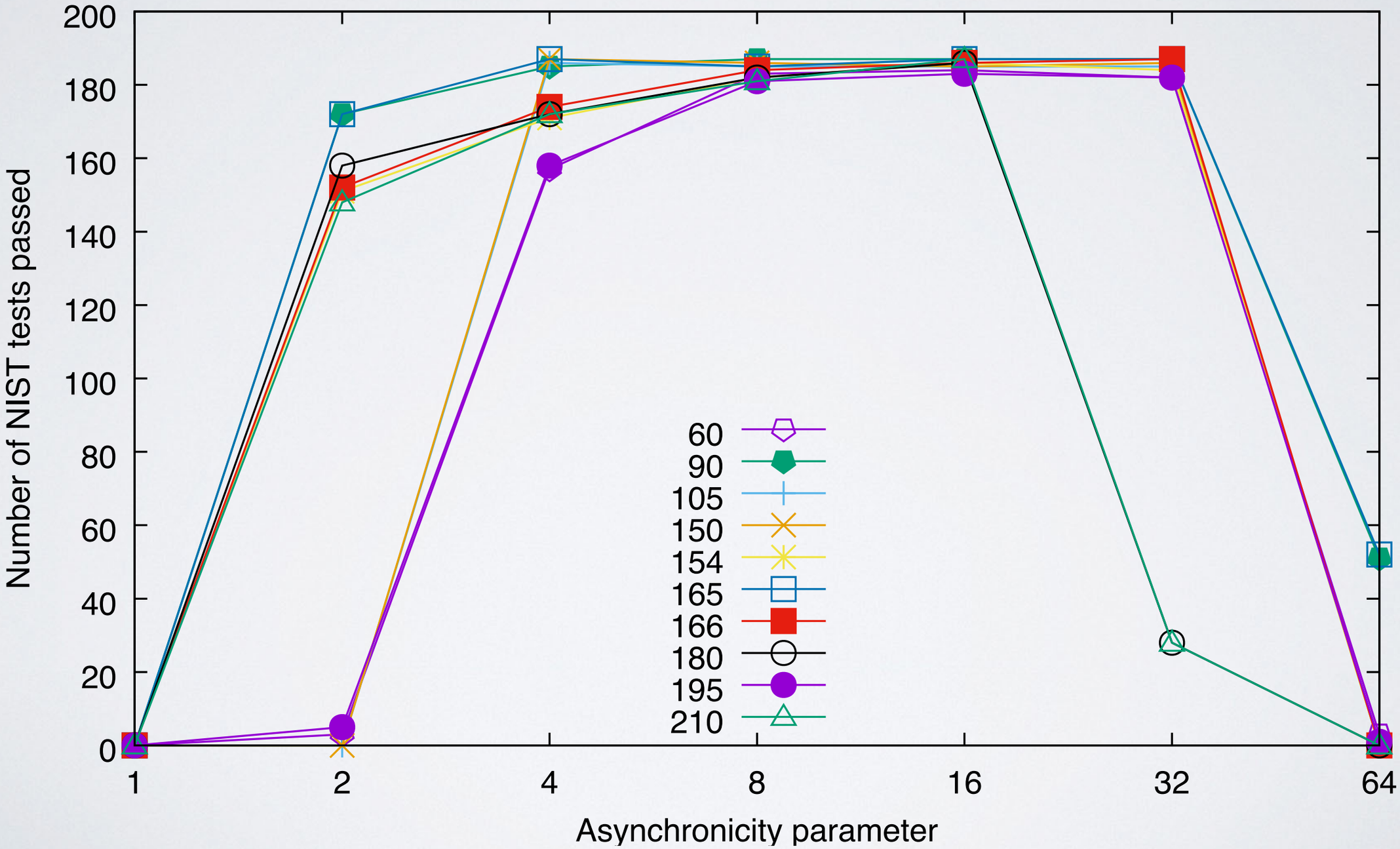
TYPE I


Number of NIST tests passed
200
180
160
140
120
100
80
60
40
20
0
1
2
4
8
16
32
64
Asynchronicity parameter
30
45
75
86
89
101
135
149

TYPE 2


Number of NIST tests passed
200
180
160
140
120
100
80
60
40
20
0
1
2
4
8
16
32
64
Asynchronicity parameter
106
120
169
225

TYPE 3


Number of NIST tests passed
200
180
160
140
120
100
80
60
40
20
0
1
2
4
8
16
32
64
Asynchronicity parameter
60
90
105
150
154
165
166
180
195
210

CONCLUSIONS

CONCLUSIONS

- Always a sudden decrease in strength

CONCLUSIONS

- Always a sudden decrease in strength
- Full asynchrony is destructive for PRNG strength

CONCLUSIONS

- Always a sudden decrease in strength
- Full asynchrony is destructive for PRNG strength
- Limited asynchrony can be beneficial

PERSPECTIVES

PERSPECTIVES

- What happens for CA or radius > 1?

PERSPECTIVES

- What happens for CA or radius > 1?
- What about other ways of introducing asynchrony?

PERSPECTIVES

- What happens for CA or radius > 1?
- What about other ways of introducing asynchrony?
- What formal properties of the rules justify their asynchronous behaviour?

THANK YOU

For Your Attention

Questions?