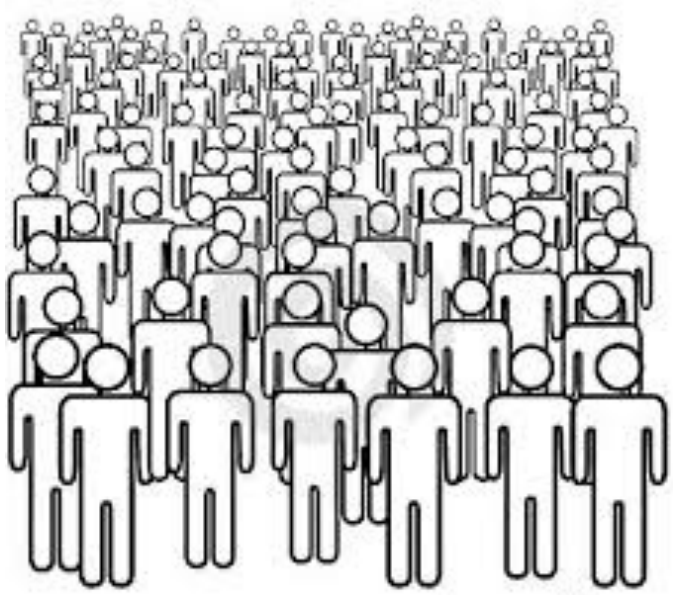
Dynamic Consensus Algorithm in Distributed Proof of Work Network

Analysis & Simulation

Chi Ning, Chou

Recall

Failure of 



Too many participants

Uniformly Fairness on Difficulty

Consensus Algorithm

Consensus Algorithm

Verifier (Winner)

Two Propositions

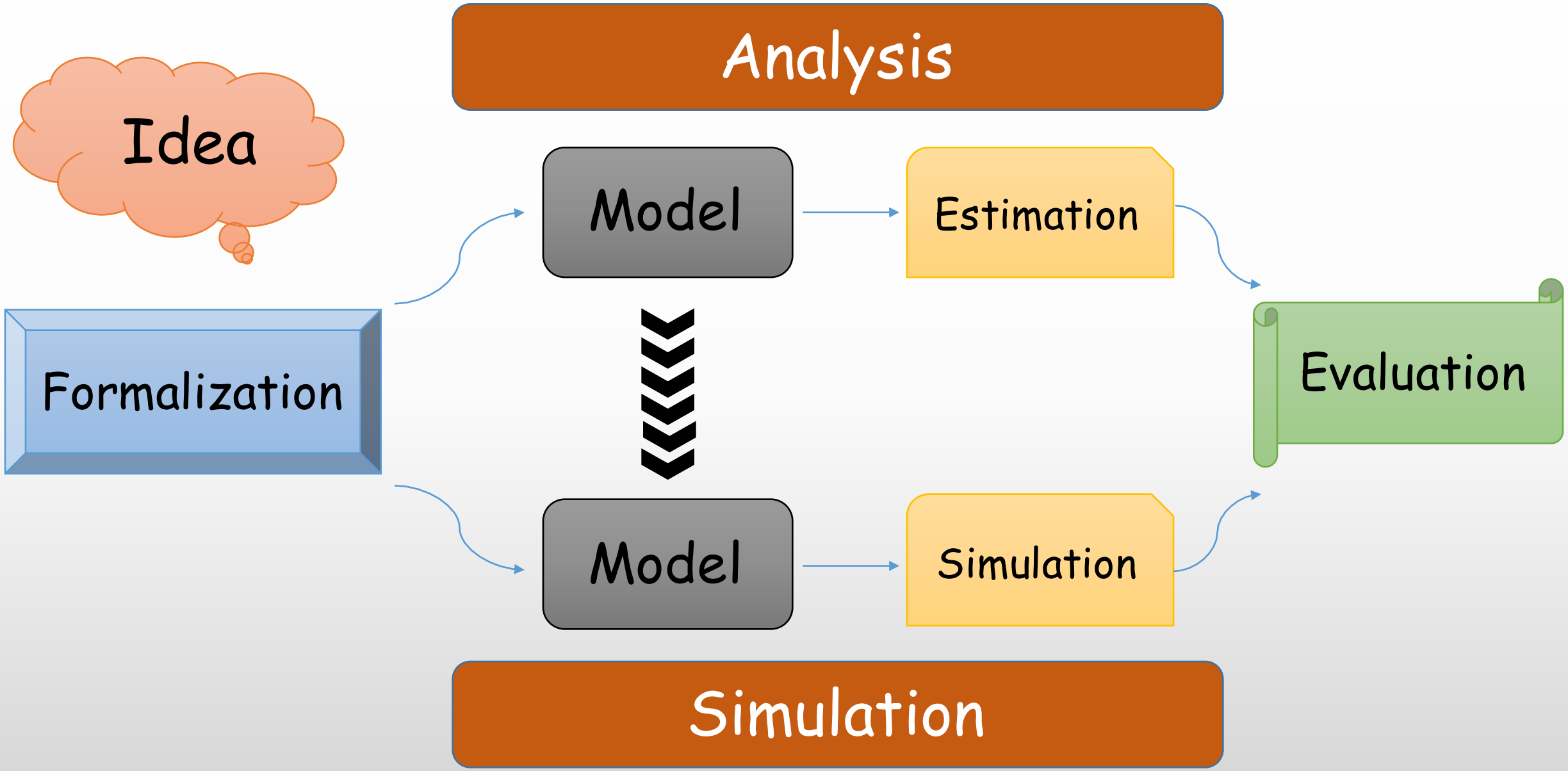
Alias Network

Dynamic Difficulty


HOW
TO...

Goals

- ✓ Efficient
- ✓ Effective
- ✓ Not So Effective


Analysis
Idea
Model
Estimation
Formalization
Evaluation
Model
Simulation
Simulation

Formalization

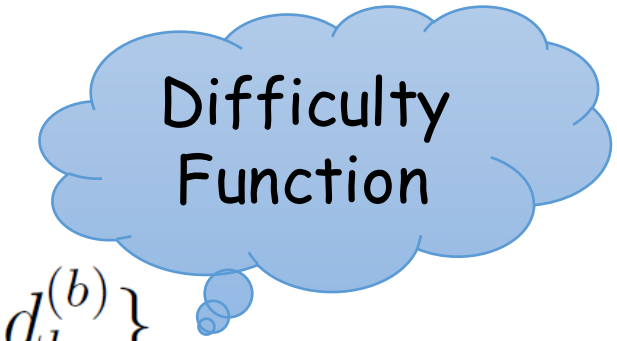
At the bth block,

$$W_k^{(b)} = \{W_{k1}^{(b)}, W_{k2}^{(b)}, ..., W_{kn}^{(b)}\}$$

$$\mathcal{D} : W_k^{(b)} \rightarrow d_k^{(b)} = \{d_{k1}^{(b)}, d_{k2}^{(b)}, ..., d_{kn}^{(b)}\}$$

$$C^{(b)} = \{C_1^{(b)}, C_2^{(b)}, ..., C_n^{(b)}\}$$

$$P^{(b)} = P(W_k^{(b)}, \mathcal{D}, C^{(b)})$$

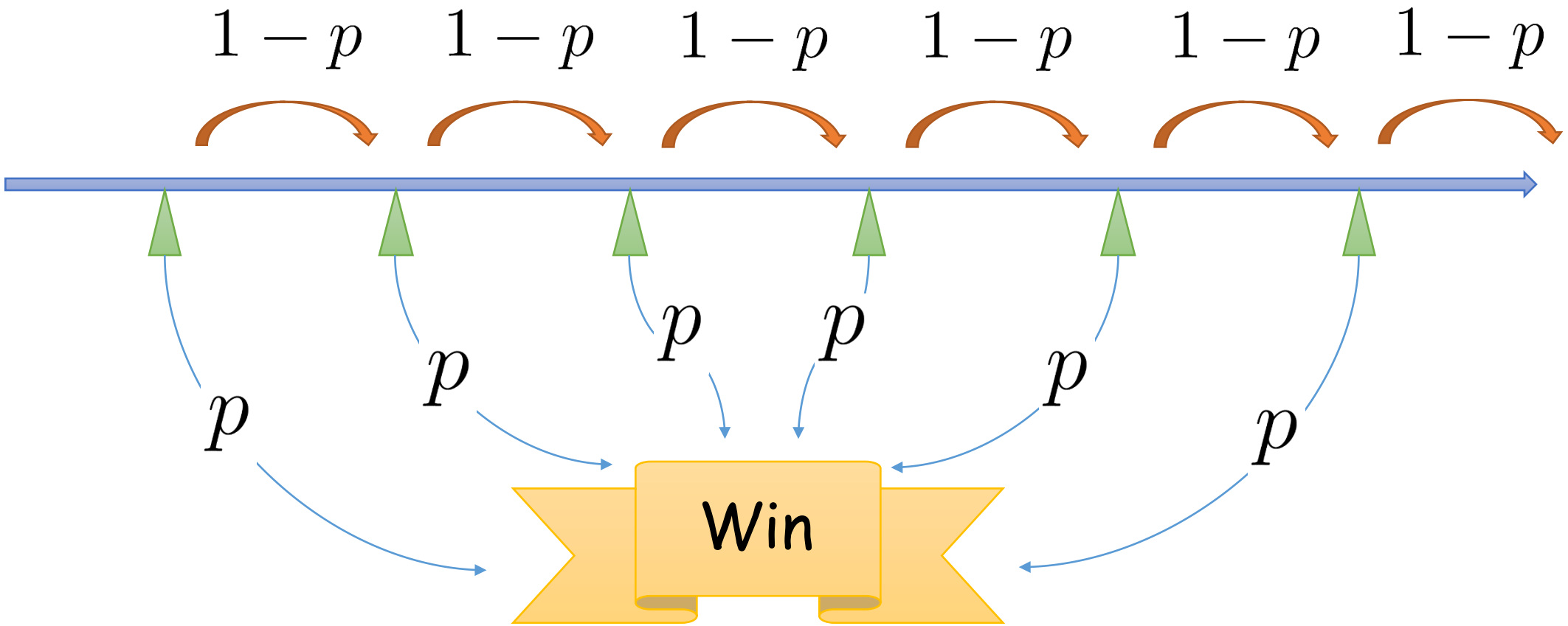


Observation : Single Hash

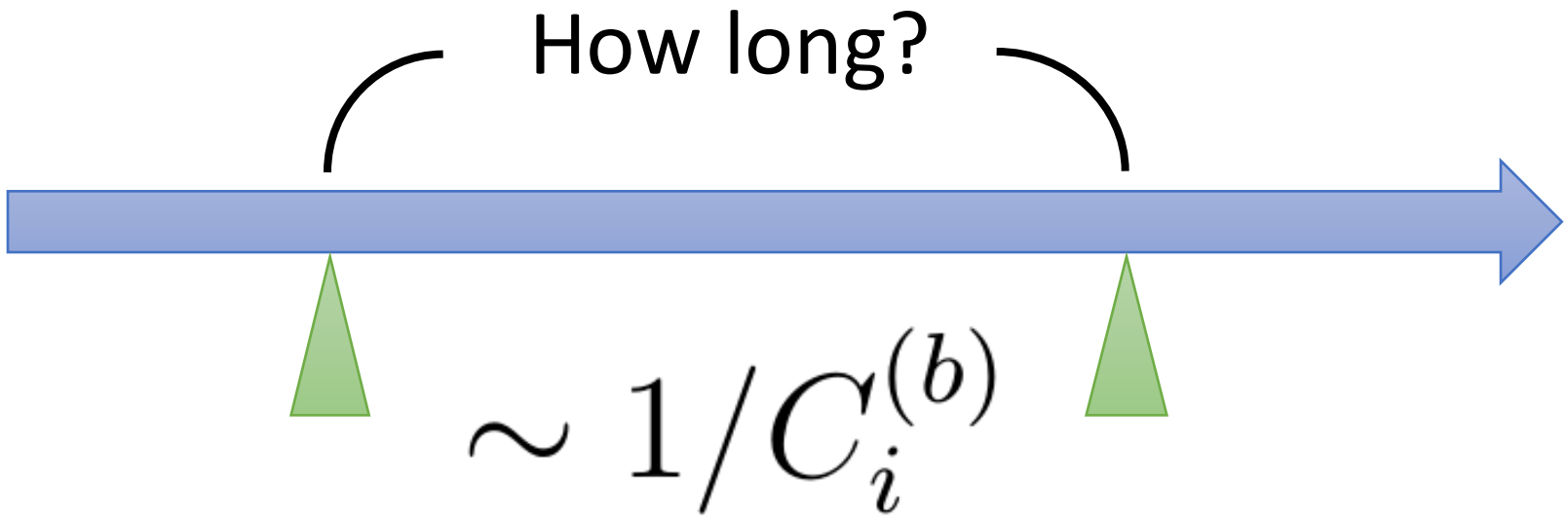
$$\frac{65536}{d \times 2^{48}}$$

$$\approx 4.89 \times 10^{-21}$$

Observation : Single Alias



Observation : Single Interval



=> Computing Power

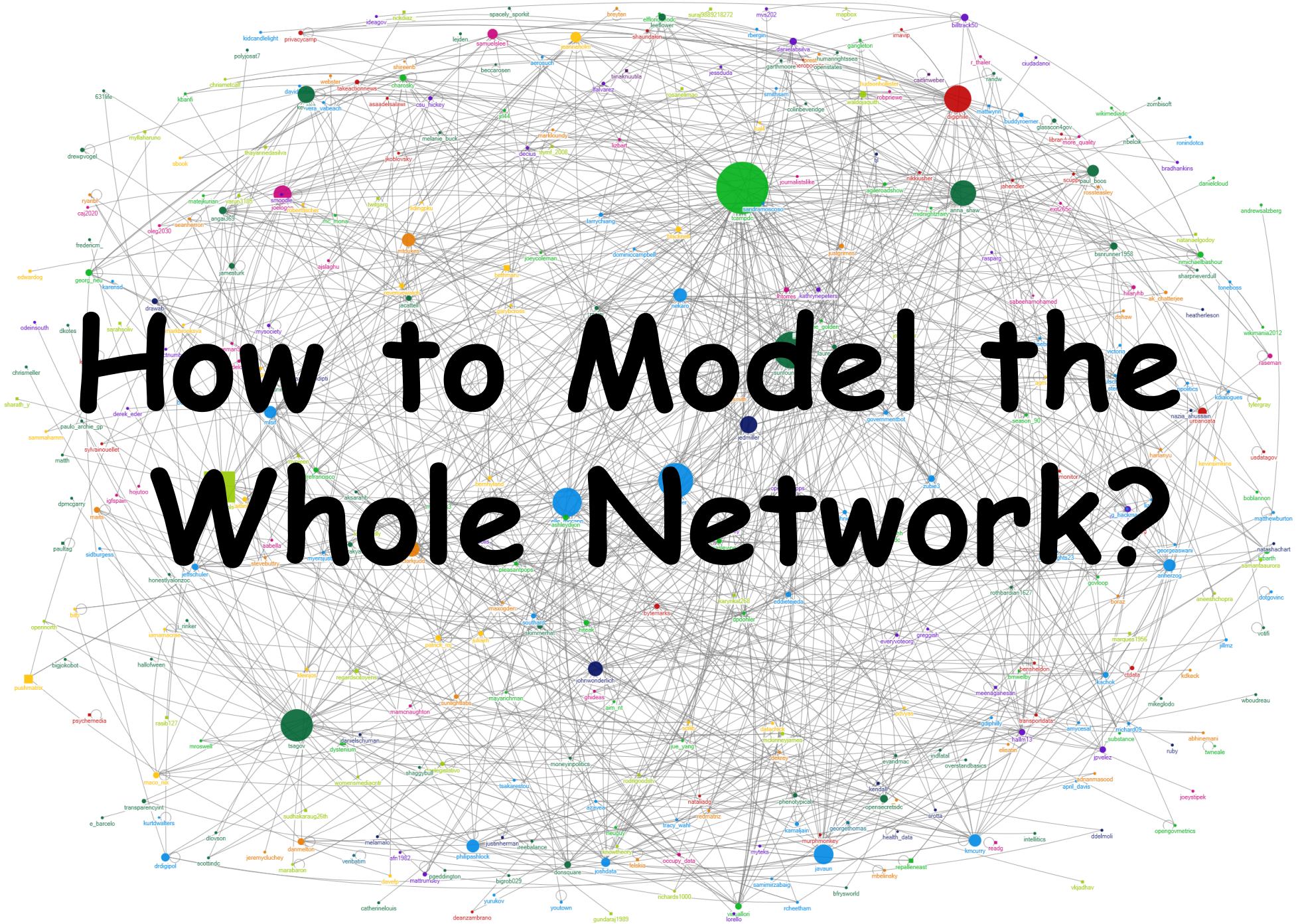
Geometric Distribution

- # blocks to win: $B_i^{(b)}$

$$Pr(B_i^{(b)} = b_i) = P_i^{(b)}(1 - P_i^{(b)})^{b_i - 1}$$

- Time to win: $T_i^{(b)}$

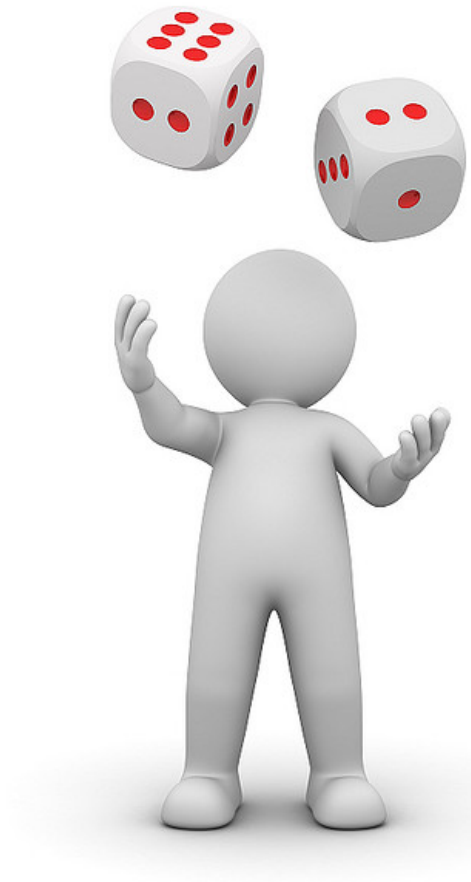
$$B_i^{(b)} / C_i^{(b)}$$


How to Model the Whole Network?

Satoshi Chose Poisson Model

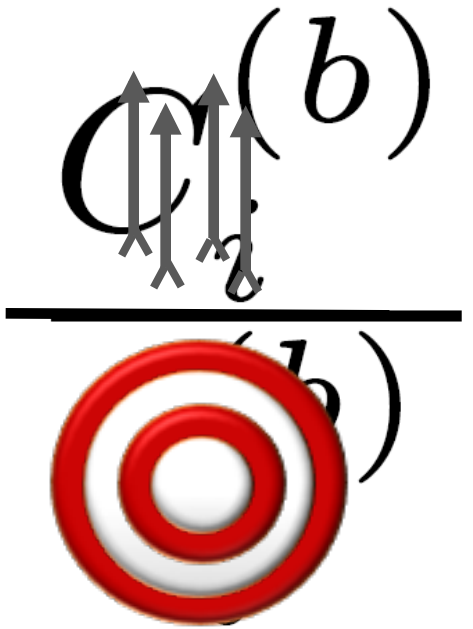
No Physical Meaning!

My Idea



Intuition

Winning Rate



$$Pr(T_i^{(b)} < T^{(b)} - j, \forall j \neq i)$$

Compare with Another Alias

$$Pr(T_i < T_j) = Pr(B_i/C_i < B_j/C_j) = Pr(Bi < \frac{C_i}{C_j} B_j)$$

$$= \sum_{b=1}^{\infty} Pr(B_i = b) Pr(B_j > \frac{C_j}{C_i} b)$$

$$= \sum_{b=1}^{\infty} P_i (1 - P_i)^{b-1} (1 - P_j)^{\frac{C_j}{C_i} b - 1}$$

$$= \frac{P_i}{1 - P_i} \sum_{b=1}^{\infty} [(1 - P_i)(1 - P_j)^{\frac{C_j}{C_i}}]^b$$

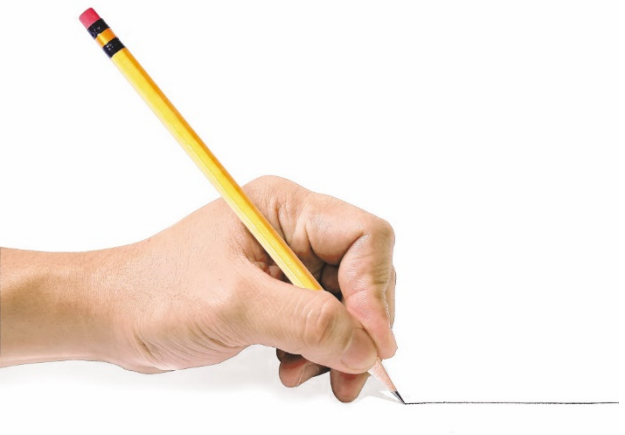
Compare with Another Alias (conti.)

$$Pr(T_i < T_j) = \frac{P_i}{1-P_i} \frac{(1-P_i)(1-P_j)^{\frac{C_j}{C_i}}}{1-(1-P_i)(1-P_j)^{\frac{C_j}{C_i}}}$$

$$= \frac{P_i(1-\frac{C_j}{C_i}P_j)}{1-(1-P_i)(1-\frac{C_j}{C_i}P_j)} \qquad (P_i, P_j \ll 1)$$

$$= \frac{C_iP_i - C_jP_iP_j}{C_iP_i + C_jP_j - C_iC_jP_iP_j}$$

$$= \frac{C_iP_i}{C_iP_i + C_jP_j} \qquad (P_iP_j \ll P_i, P_j)$$



Thus

$$\frac{Pr(T_i<T_j)}{Pr(T_j<T_i)} \approx \frac{C_i P_i}{C_j P_j}$$

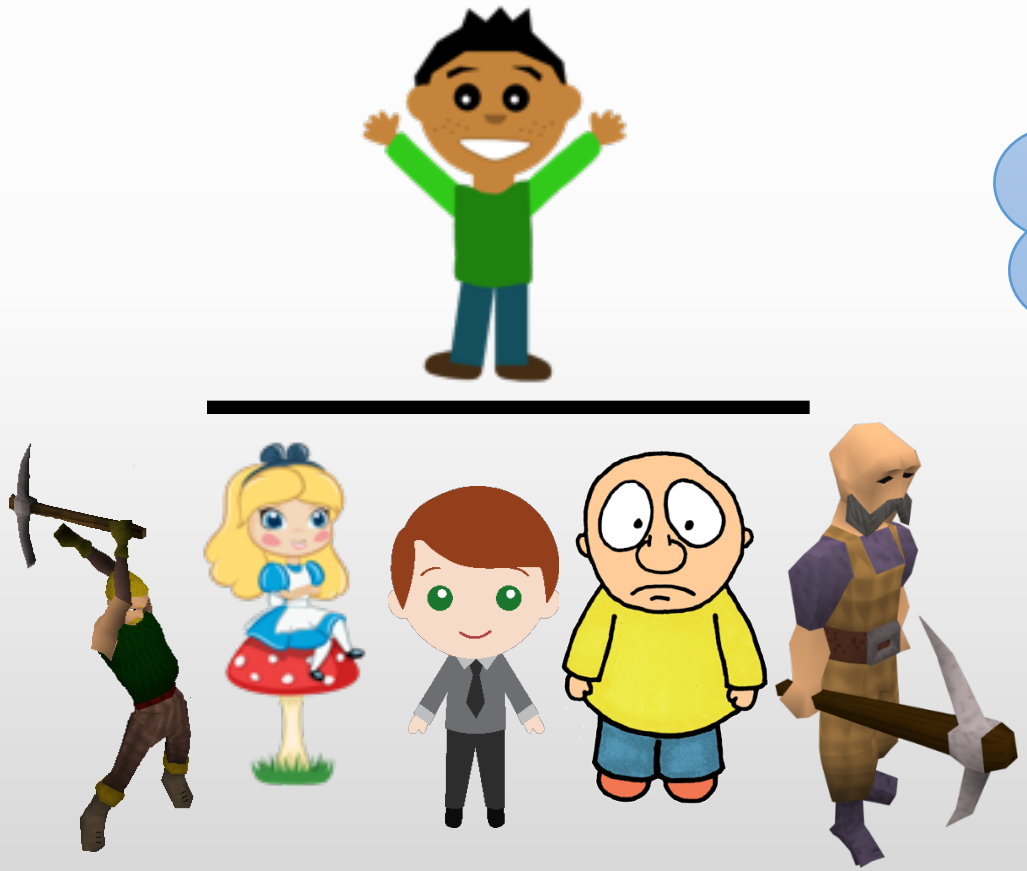
Also,

$$P_i = \frac{65536}{d_i \times 2^{48}}$$

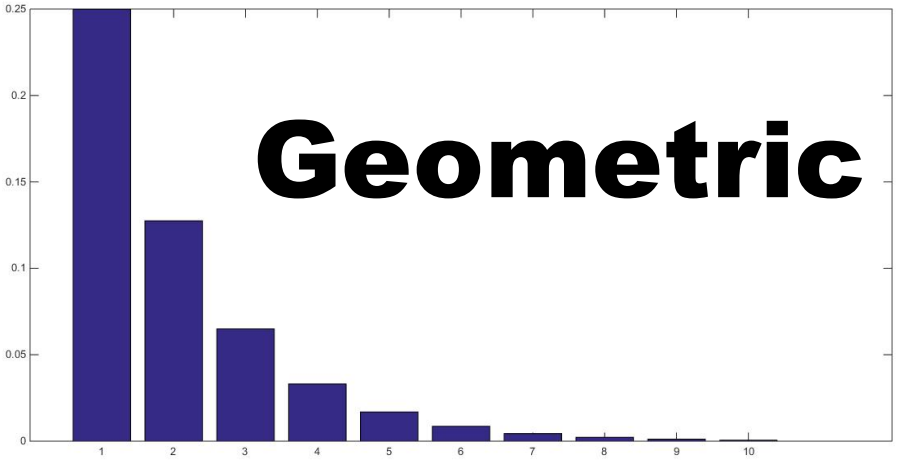
Finally

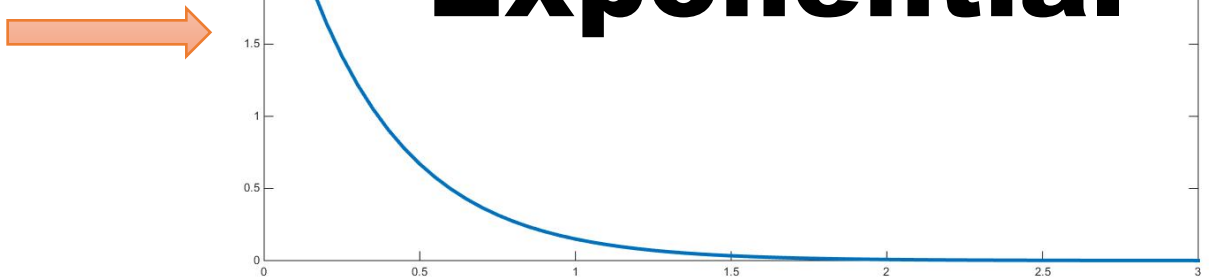
$$\frac{Pr(T_i<T_j)}{Pr(T_j<T_i)} \approx \frac{C_i/d_i}{C_j/d_j}$$

When it Comes to …



Transformation





*Continuous Time

Geometric to Exponential

Consider the cdf of T_i

$$F_{T_i}(t) = \sum_{b=1}^{C_i t} P_i(1-P_i)^{b-1}$$

$$= \sum_{b=1}^{C_i t} \frac{1}{d_i} \frac{65536}{2^{48}} [(1 - \frac{1/d_i}{2^{48}/65536})^{\frac{2^{48}/65536}{1/d_i}}]^{\frac{1}{d_i}\frac{65536}{2^{48}}(b-1)}$$

$$= \sum_{b=1}^{C_i t} \frac{1}{d_i N} [(1 - \frac{1}{d_i N})^{d_i N}]^{\frac{b-1}{d_i N}} \qquad (N = \frac{2^{48}}{65536})$$

$$\approx \sum_{b=1}^{C_i t} \frac{1}{d_i N} \exp(\frac{b-1}{d_i N}) \qquad (N \approx \infty)$$

Geometric to Exponential (conti.)

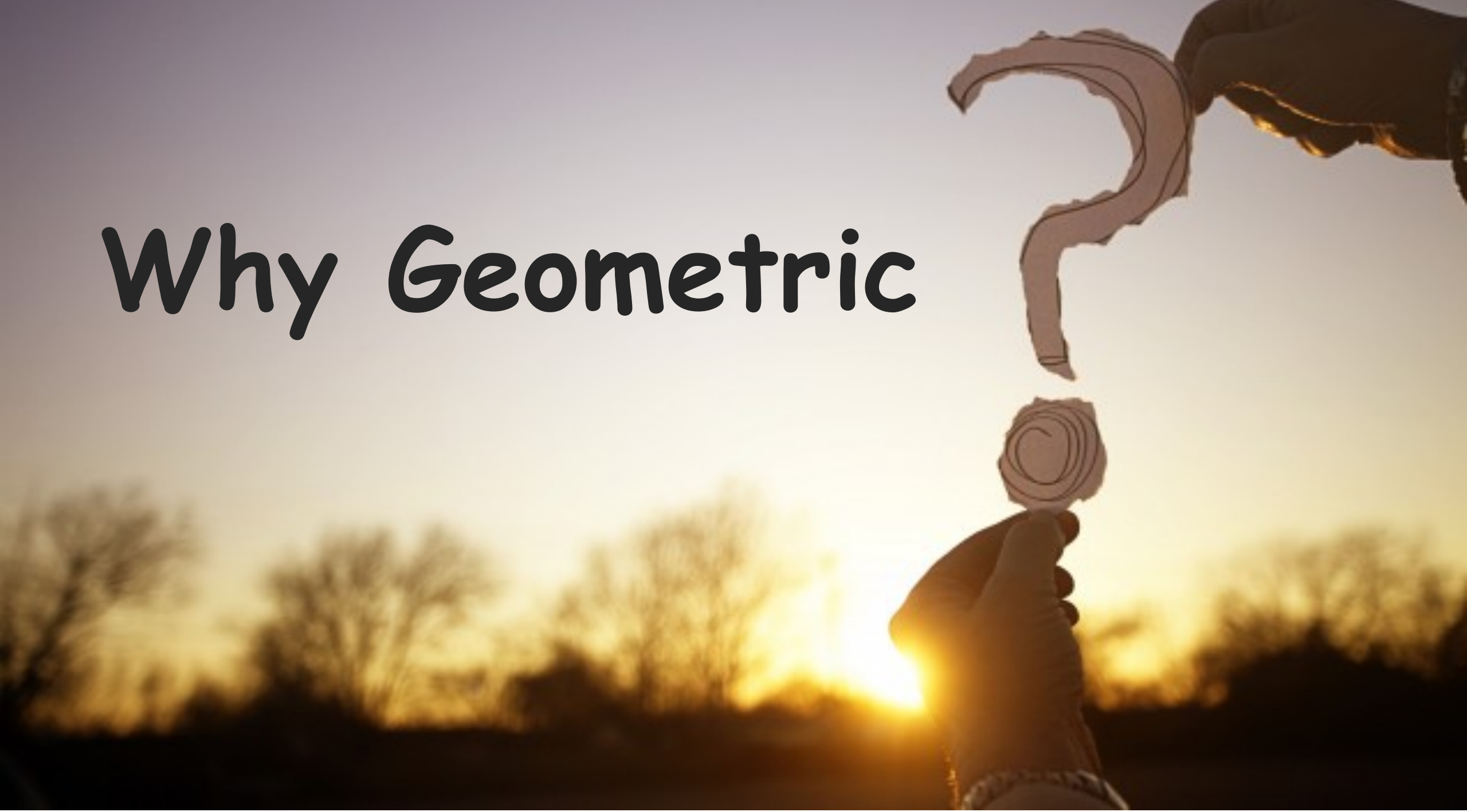
Furthermore,

$$F_{T_i}(t) \approx \sum_{b=1}^{C_i t} \frac{1}{d_i N} \exp(\frac{b-1}{d_i N})$$
$$\approx \int_0^{C_i t} \frac{1}{d_i} \exp(\frac{x}{d_i}) dx = F_{\exp(1/d_i)}(NC_i t)$$

Differentiate $F_{T_i}(t)$ and find the *pdf* of T_i

$$f_{T_i}(t) = \frac{d}{dt} F_{T_i}(t) = \frac{d}{dt}[F_{\exp(1/d_i)}(NC_i t)]$$
$$= NC_i f_{\exp(1/d_i)}(NC_i t)$$
$$= \frac{NC_i}{d_i} \exp(\frac{NC_i t}{d_i}) \sim exp(\frac{NC_i}{d_i})$$

Why Geometric



Good Properties

- Winning Ratio:

$$Pr(exp(\lambda_1) < exp(\lambda_2)) = \frac{\lambda_1}{\lambda_1 + \lambda_2}$$

- Rényi's Representation:

Rényi's Representation

- Moment of the order statistics of inid exponential RVs.

$$\{T_1, T_2, ..., T_n\} \sim \{exp(\lambda_1), exp(\lambda_2), ..., exp(\lambda_n)\}$$

- Extends to Tikov's Representation:

$$\mathbf{X} \stackrel{d}{=} \mathbf{AZ}$$


Simulation

- $Pr(double\ spending)$
- $Winning\ Distribution$

Convergence Theorem

$$\frac{N_{ds}}{n} \xrightarrow{n \to \infty} Pr(double\ spending)$$

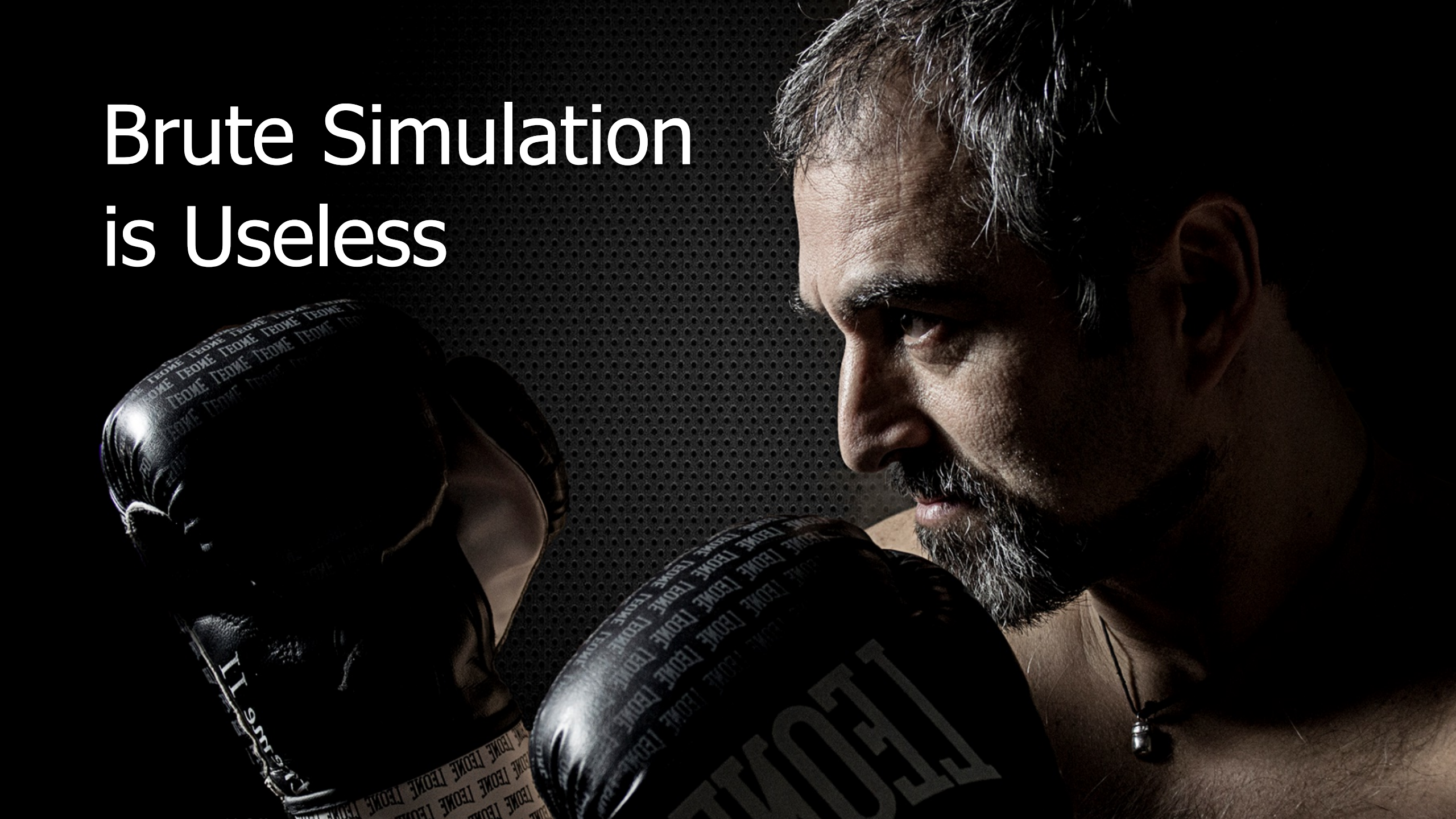
The Bound in Satoshi's Paper is Loose

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012
```

Wrong Model
Wrong Result


Double Spending is ...
An anomaly event
GTGRAPHICS.DE

Brute Simulation is Useless

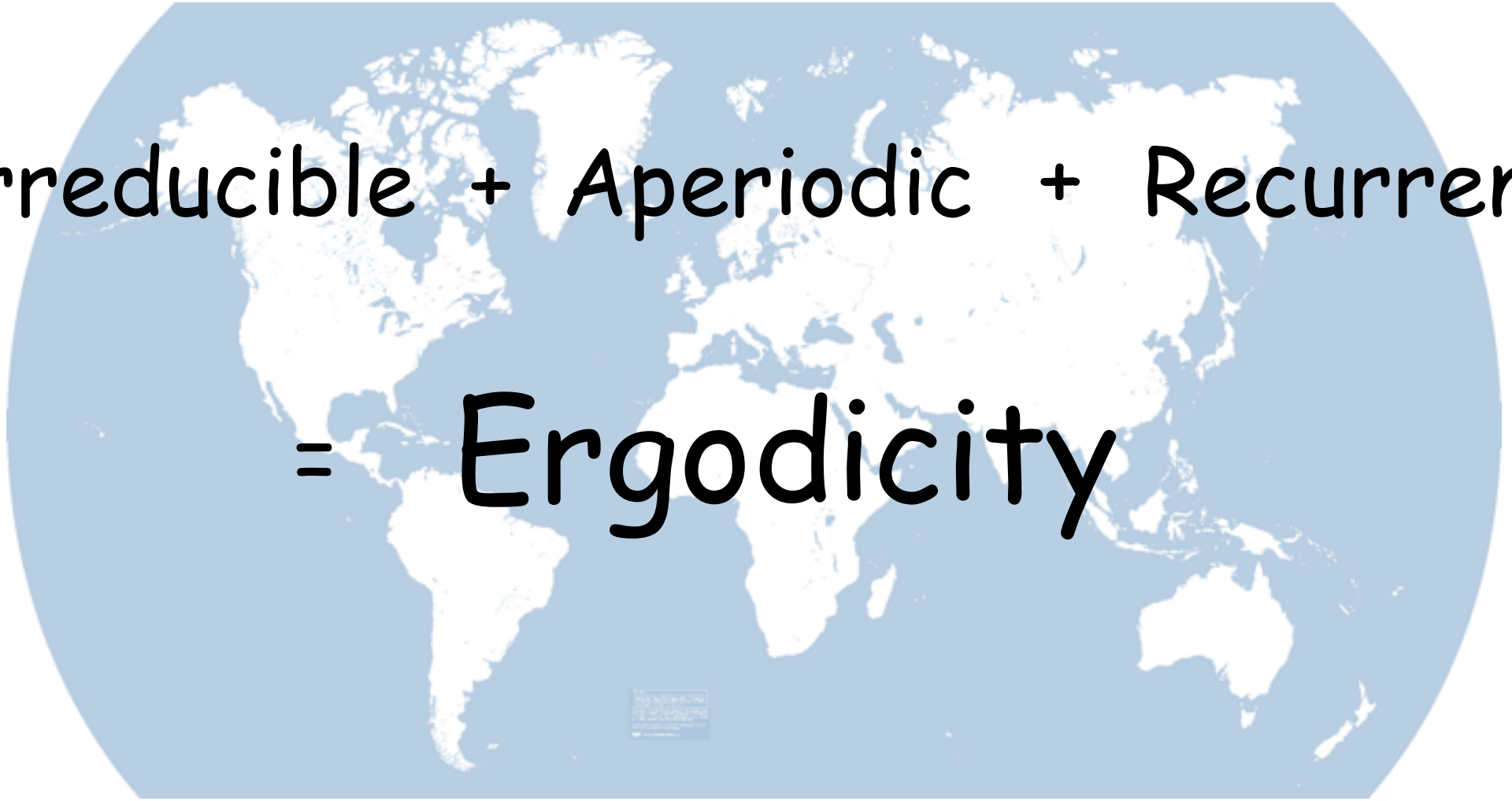


Observation : Markov Property

$$Pr(X_{n+1}|X_n, ...X_1) = Pr(X_{n+1}|X_n)$$

$$Pr(X_{T+n+1}|X_{T+n}, ..., X_{T+1}, A) = Pr(X_{T+n+1}|X_{T+n})$$

More…



Irreducible + Aperiodic + Recurrent

= Ergodicity

Unique Stationary Distribution

$$\pi(dp) = \frac{1}{E(T_{ds})}$$

$$= \lim_{n \to \infty} \frac{N_{ds}}{n}$$

$$= Pr(double\ spending)$$

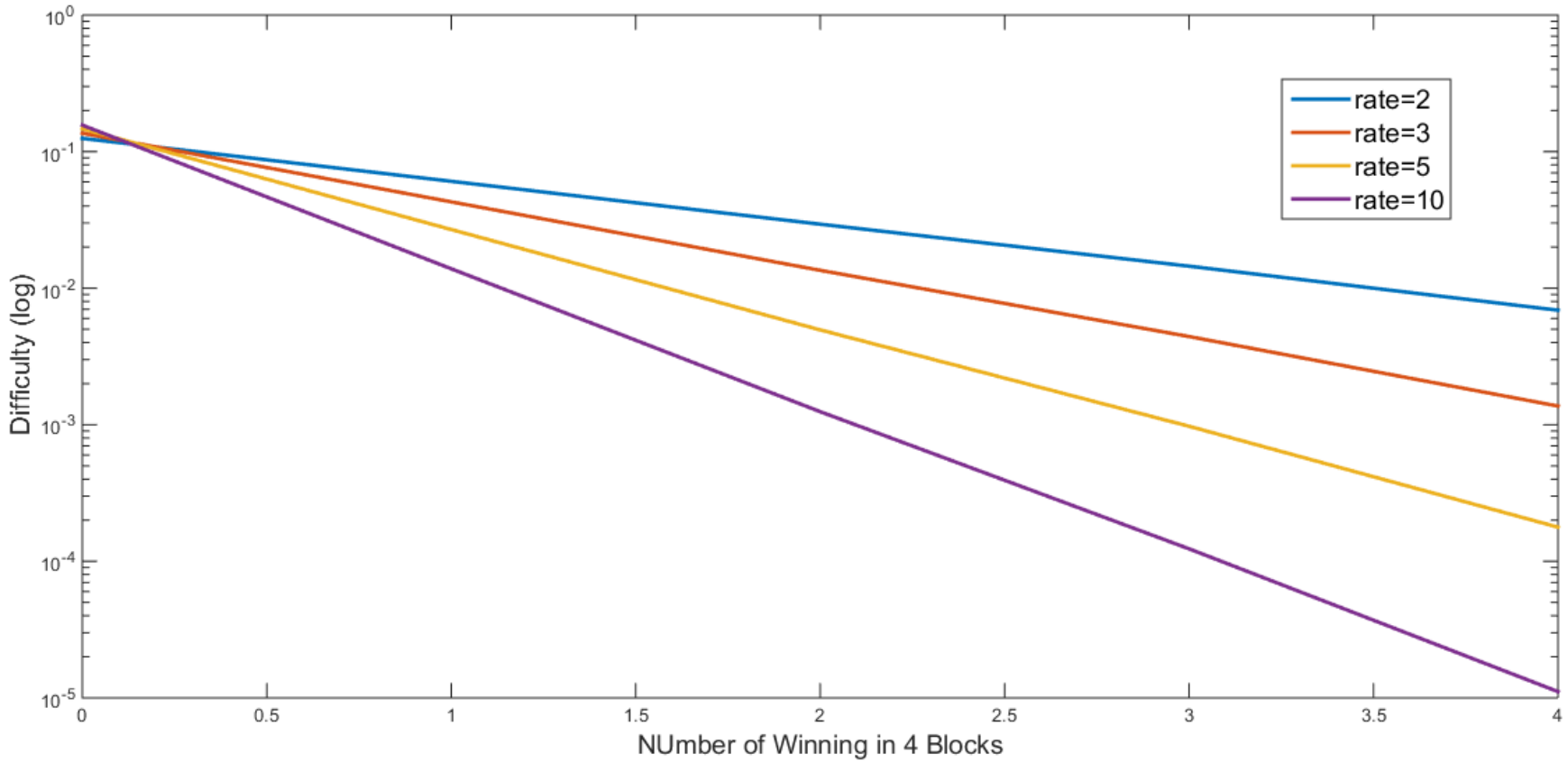
Difficulty Function: Exponential Model

$$D_{exp(r)}(W_k^{(b)}) = \{d_{k1}^{(b)}, \ldots, d_{kn}^{(b)}\}$$

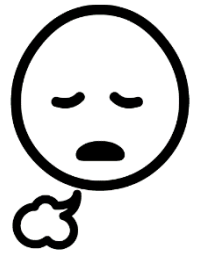
Rate

$$= \{\frac{r^{-W_{k1}^{(b)}}}{\sum_{i=1}^{n} r^{-W_{ki}^{(b)}}}, \ldots, \frac{r^{-W_{kn}^{(b)}}}{\sum_{i=1}^{n} r^{-W_{ki}^{(b)}}}\}$$

Exponential Model Recall



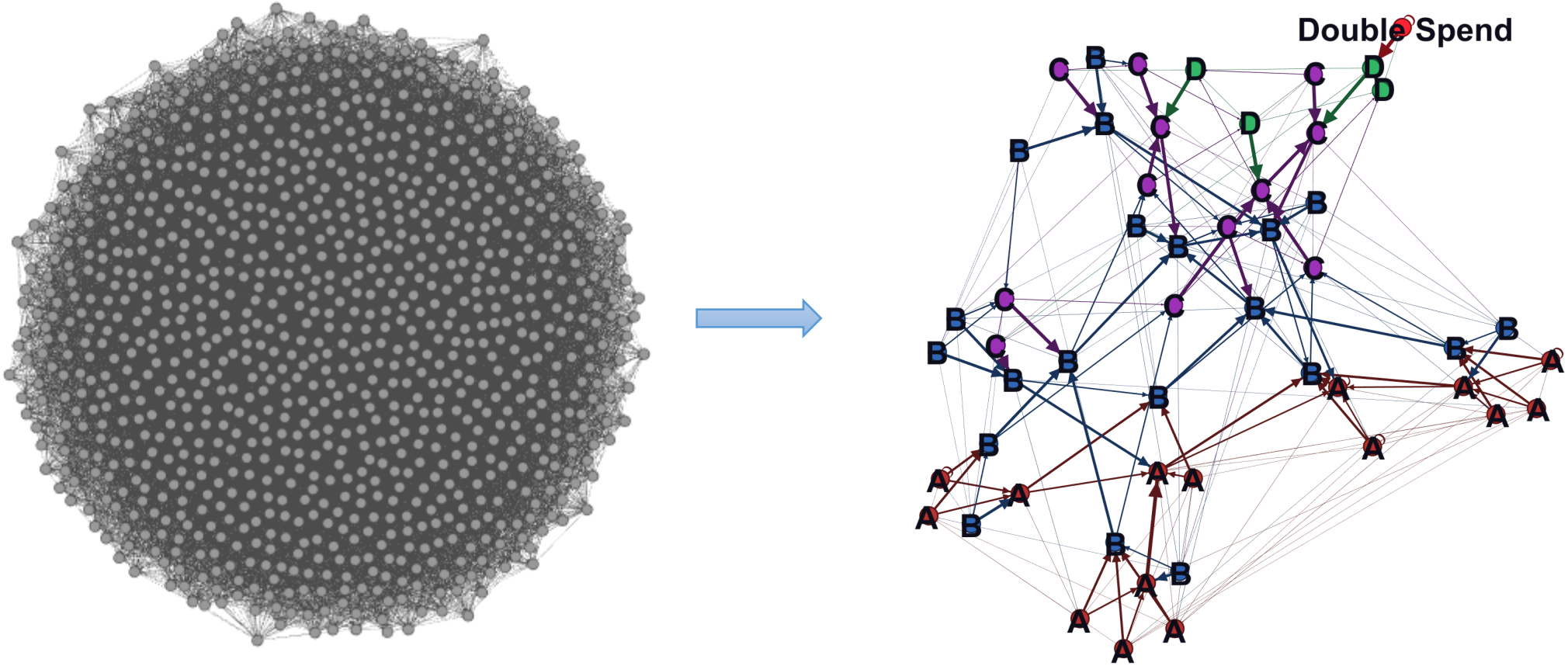
However…



- State: $\mathcal{S} = (W_1, W_2, \ldots, W_{n^k})$
- Transition: $\mathcal{T} = \{Pr(S_i, S_j) \mid \forall i, j\}$

Too Many State! n^k

State Reduction



State Reduction (conti)

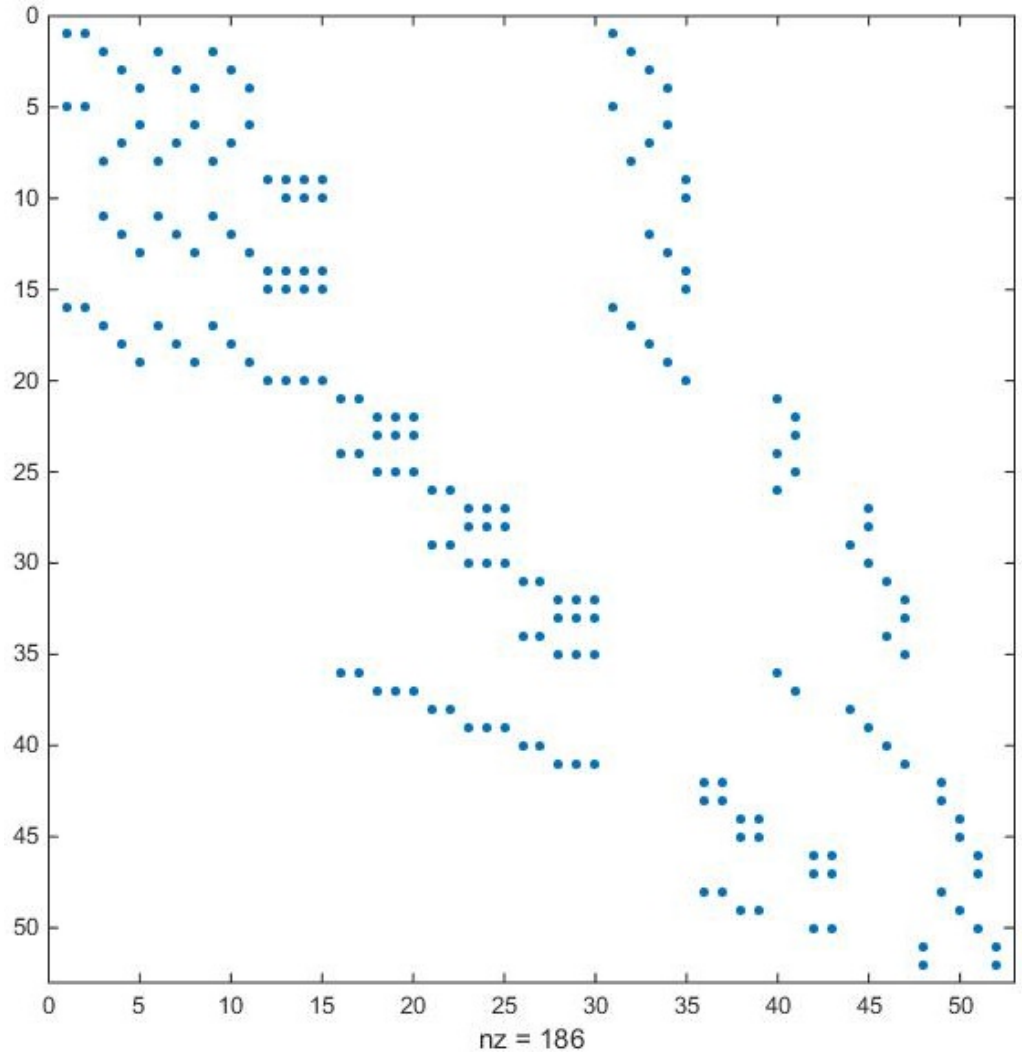
$$\#nodes = \sum_{m=1}^{k} \binom{k}{m} J(m)$$

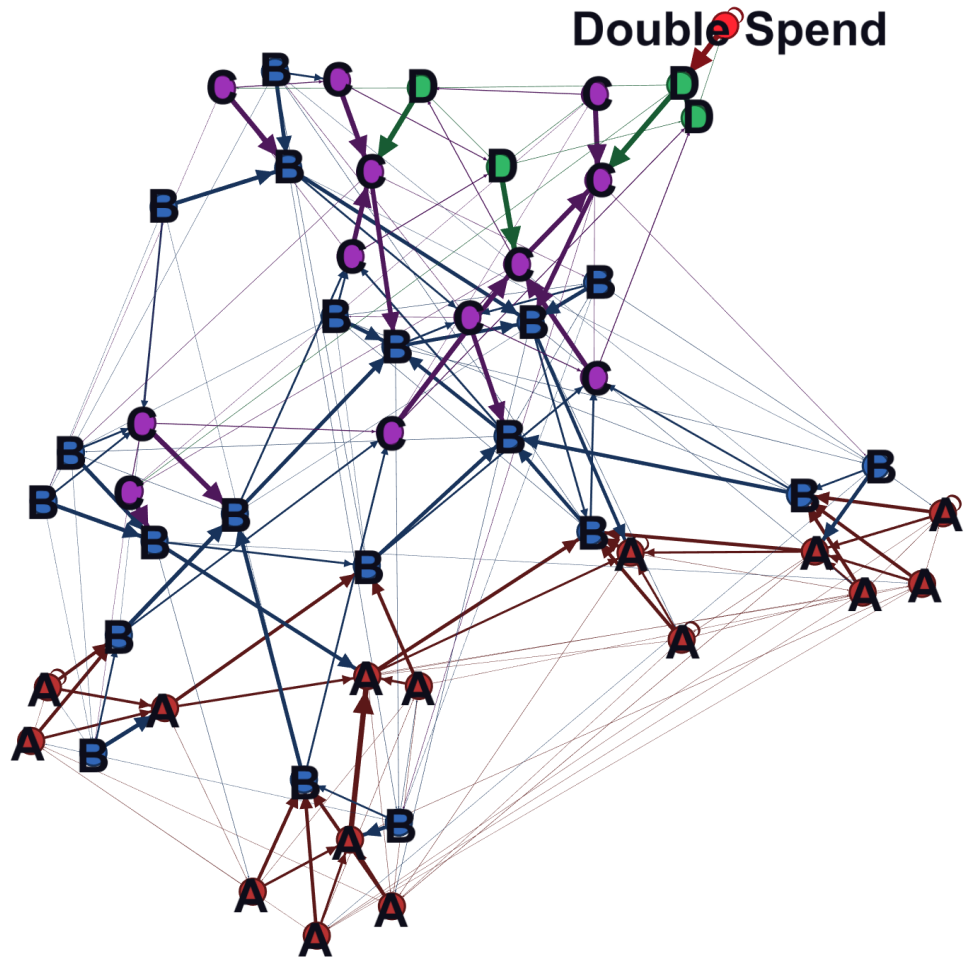
$$J(m) = \begin{cases} \left[\sum_{i=0}^{\frac{m}{2}-1} \binom{m}{i}\right] + \frac{1}{2}\binom{m}{\frac{m}{2}} \\ \sum_{i=0}^{\frac{m-1}{2}} \binom{m}{i} \end{cases}$$

State Reduction: Example

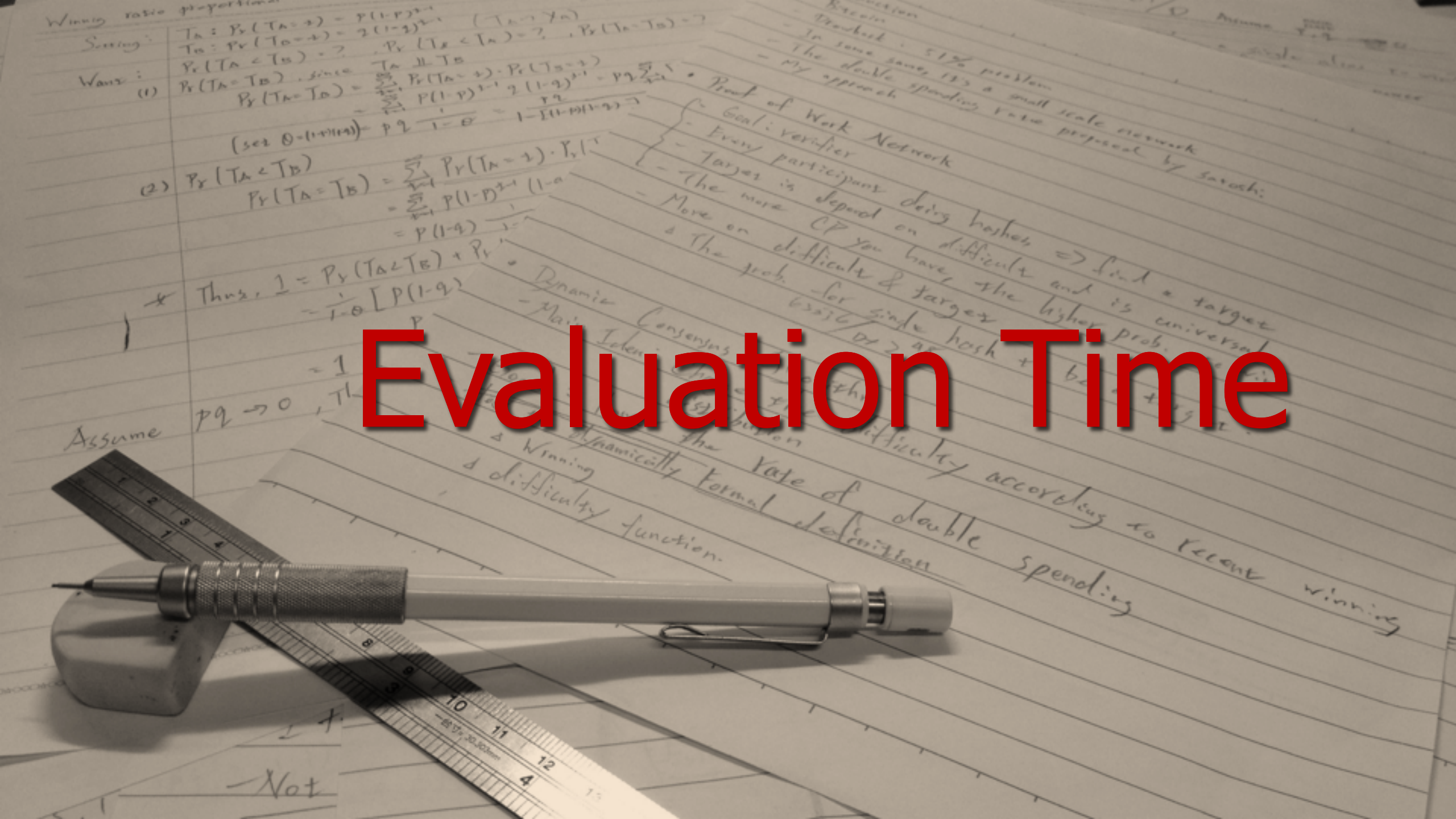
- Rate (k): 4
- # Alias: n

$$52^{n^k}$$

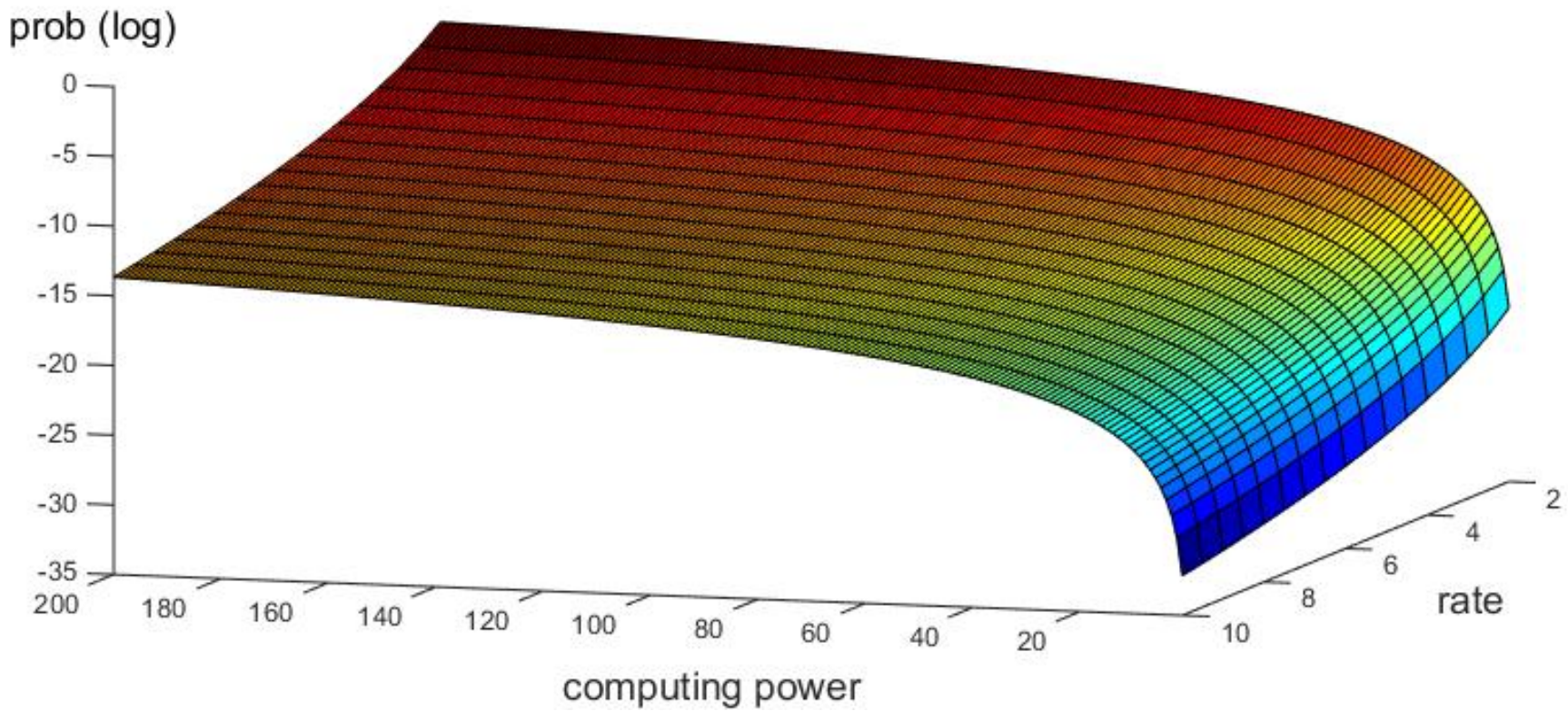

0
5
10
15
20
25
30
35
40
45
50
0
5
10
15
20
25
30
35
40
45
50
nz = 186


Double Spend

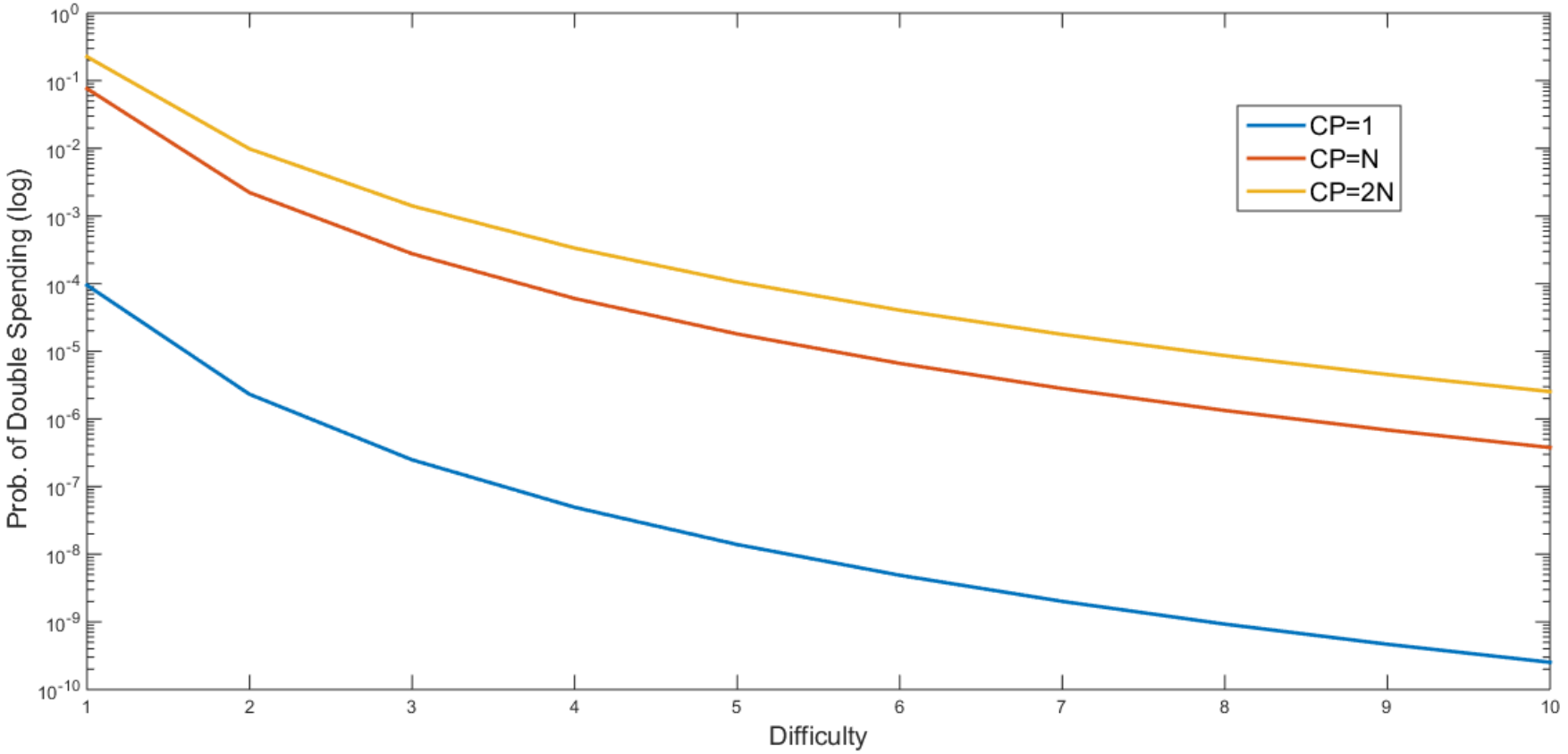
Evaluation Time



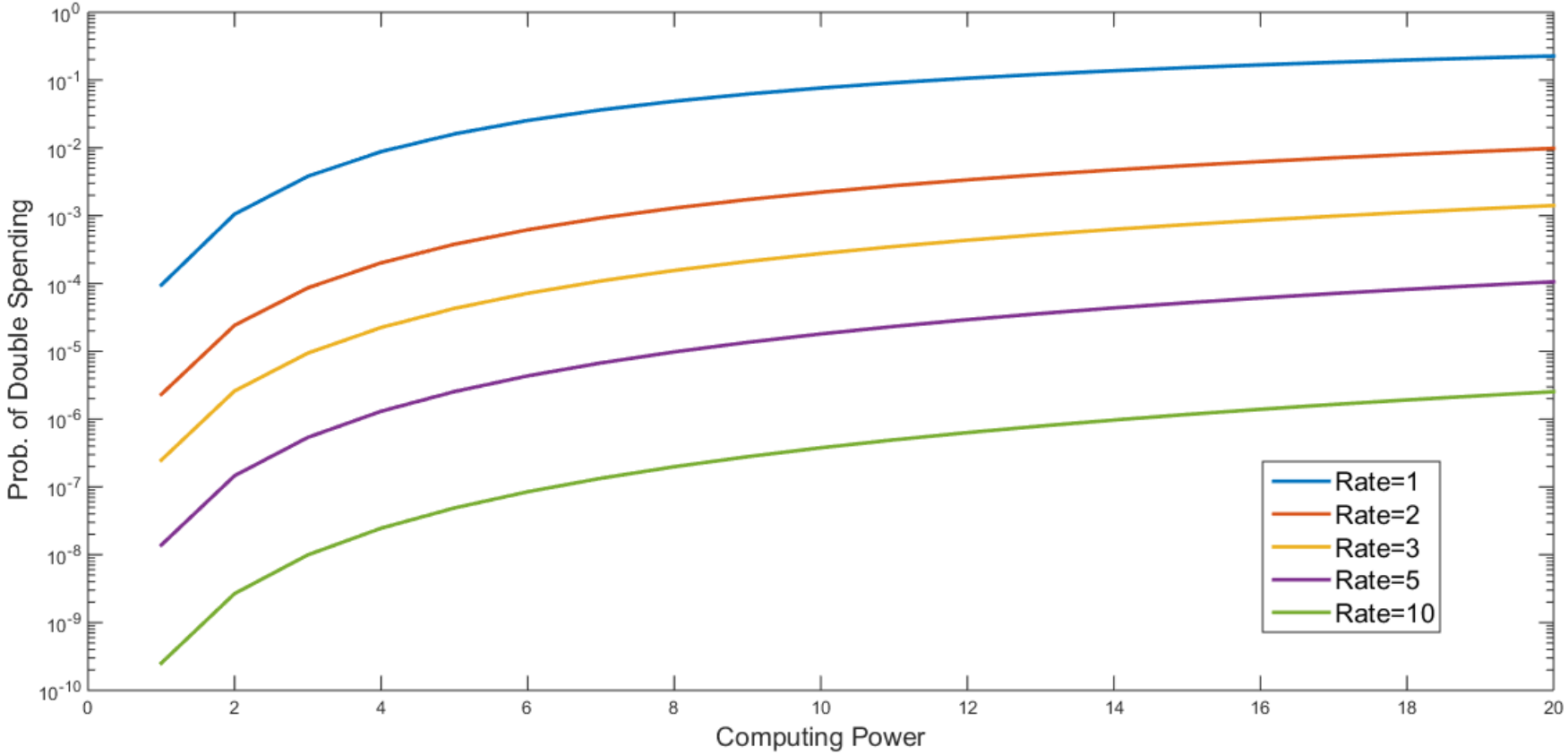
Double Spending



Double Spending: Rate



Double Spending: Computing Power

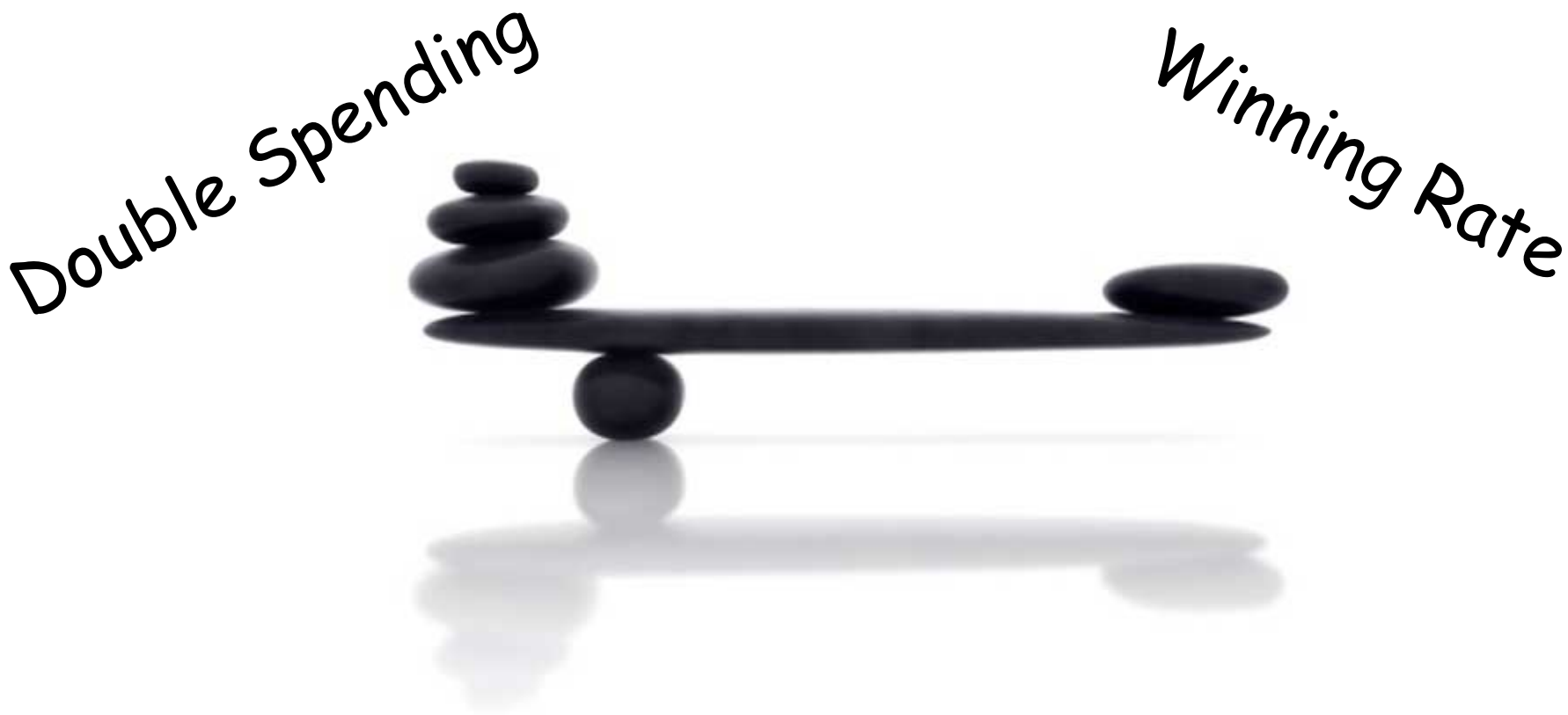


Comparison

		Rate=2	Rate=3	Rate=5
CP = 1	9.46*10^-5	2.31*10^-6	2.49*10^-7	1.39*10^-8
CP = N	7.6*10^-2	2.22*10^-3	2.77*10^-4	1.80*10^-5
CP = 2N	2.2*10^-1	9.8*10^-3	1.4*10^-3	1.06*10^-4

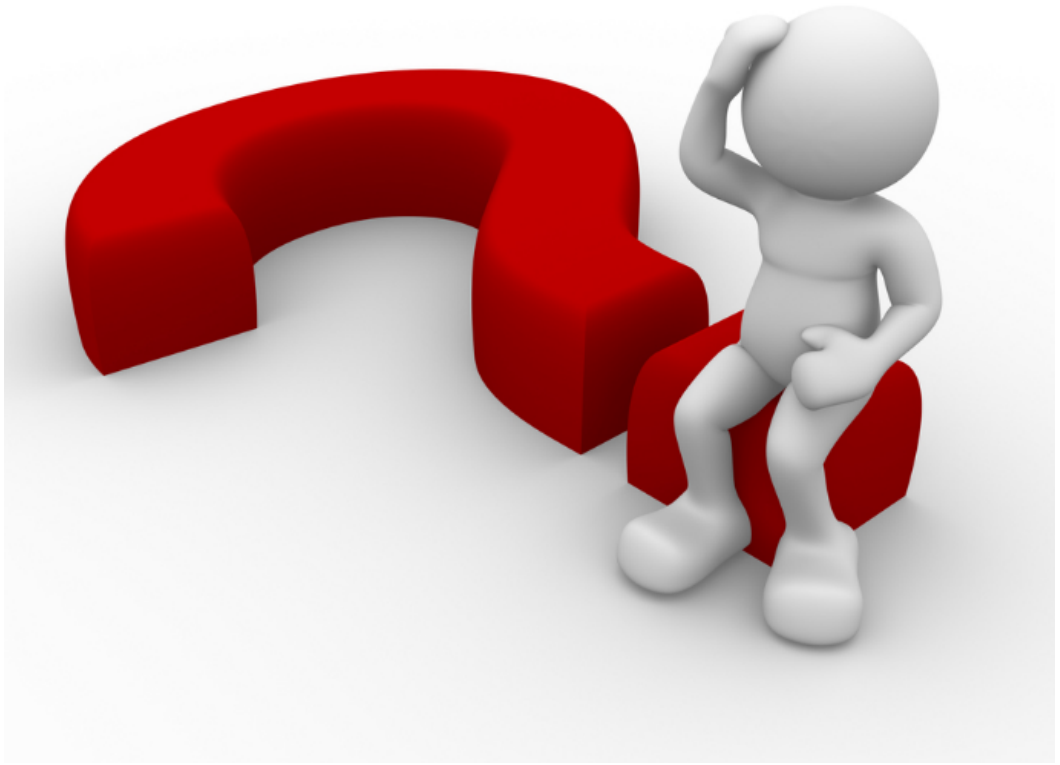

Next…?

Analysis on Winning Distribution



Analysis on Various Difficulty Function

- Different Model
- Updating



Still Lots to Learn!

- Functional Analysis
- Information Theory
- Concentration Inequality
- Approximation Theory


THANK
YOU!