IPAM/UCLA Summer School

Enigma of Arrival

Bud Mishra

Courant Inst., NYU

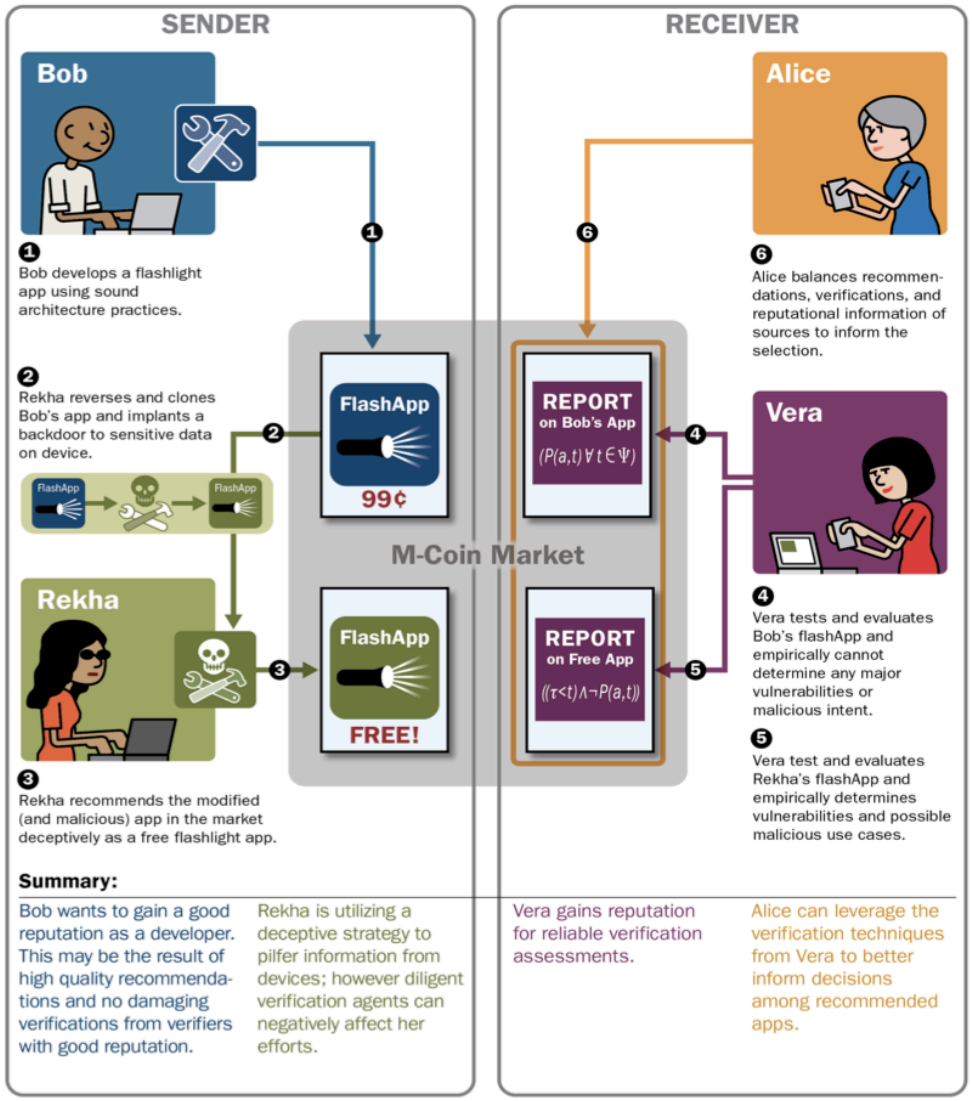
July 10 2015

Outline

Signaling Games

- Two player games with incomplete information...
- One player is informed ... the other player is not...
  1. The informed player's strategy set consists of signals contingent on information
  2. Uninformed player's strategy set consists of actions contingent on signals
- Spence 1973, Zahari 1977, Lewis 2002, Sobel 2009

Complex Signaling



- Games we play.
- Many players...
- How do they get organized?

FLIP IT

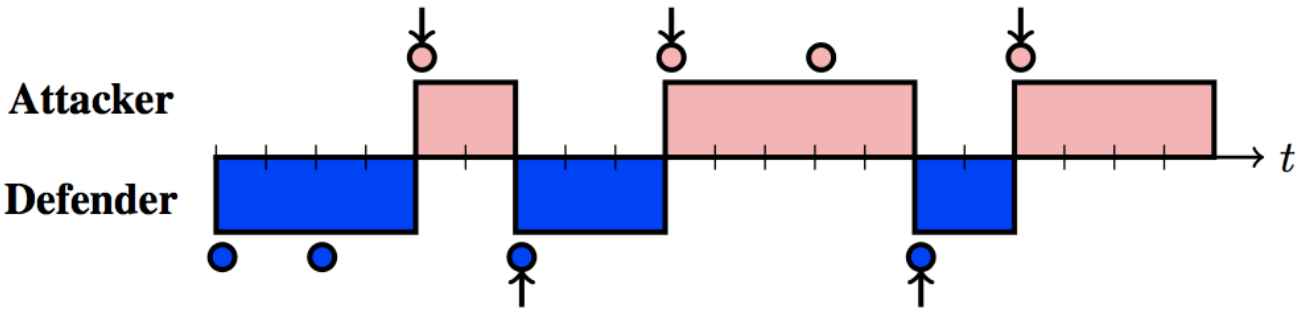


Fig. 1. The FLIPIT game. Blue and red circles represent defender and attacker moves, respectively. Takeovers are represented by arrows. Shaded rectangles show the control of the resource—blue (dark gray in grayscale) for the defender and red (light gray in grayscale) for the attacker. We assume that upon initialization at time 0, the defender has control.

FLIP IT

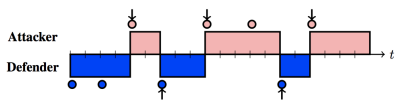


Fig. 1. The FLIPIT game. Blue and red circles represent defender and attacker moves, respectively. Takeovers are represented by arrows. Shaded rectangles show the control of the resource—blue (dark gray in grayscale) for the defender and red (light gray in grayscale) for the attacker. We assume that upon initialization at time 0, the defender has control.

- Sender: Pwner $\mapsto$ Receiver: Owner
- Sender prefers RED state and receiver prefers BLUE state
- Strategic Symmetry: Either player can choose to change the state
- Information Symmetry: The global state is visible to both players

PWN IT

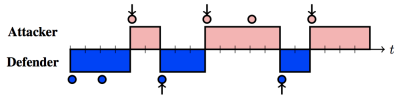


Fig. 1. The FLIPIT game. Blue and red circles represent defender and attacker moves, respectively. Takeovers are represented by arrows. Shaded rectangles show the control of the resource—blue (dark gray in grayscale) for the defender and red (light gray in grayscale) for the attacker. We assume that upon initialization at time 0, the defender has control.

- Sender: Pwner $\mapsto$ Receiver: Owner
- Sender prefers RED state and receiver prefers BLUE state
- Information Asymmetry: The global state is visible only to the sender
- Signaling: Sender can make a **Threat** (e.g., Ransomware), only effective in RED state
- Deception: Bluff – A threat made in a BLUE state

Outline

The Model of Signaling Games

- Two players:

$$S \quad - \quad \text{Sender (Informed)}$$
$$R \quad - \quad \text{Receiver (Uninformed)}$$

- Roles can be shared - partial information, distributed actions
- **TYPE**: Random variable t whose support is given by T (known to Sender S). $\pi(\cdot) =$ Probability distribution over T is a prior belief of R that the sender's type is t.

Game

- Game
  1. Player S learns $t \in T$
  2. S send to R a signal $s \in M$.
  3. R takes an action $a \in A$.
- Payoff function

$$u^{i \in \{S,R\}} : T \times M \times A \to \mathbb{R}.$$

Equilibrium

- **Behavior Strategies**:

1. For S a function $\mu : T \times M \to [0,1]$ such that

$$\sum_{s \in M} \mu(t,s) = 1, \text{ for all } t.$$

$\mu(t,s) =$ Probability that S with type t sends signal s.

2. For R a function $\alpha : M \times A \to [0,1]$ such that

$$\sum_{a \in A} \alpha(s,a) = 1, \text{ for all } s.$$

$\alpha(s,a) =$ Probability that R takes action a following signal s.

- Subjective probability.

$$\beta(t,s) = \frac{\mu(t,s)\pi(t)}{\sum_{t' \in T} \mu(t',s)\pi(t')}.$$

Proposition

Behavior strategies $(\alpha*, \mu*)$ *form a Nash equilibrium iff for all* $t \in T$

$$\mu(t,s) > 0 \text{ implies}$$
$$\sum_{a \in A} U^S(t,s,a)\alpha(s,a)$$
$$= \max_{s' \in S} \sum_{a \in A} U^S(t,s',a)\alpha(s',a);$$

& $s \in S$ *(s.t.* $\sum_{t \in T} \mu(t,s)\pi(t) > 0$*)*

$$\alpha(s,a) > 0 \text{ implies}$$
$$\sum_{t \in T} U^R(t,s,a)\beta(t,a)$$
$$= \max_{a' \in A} \sum_{t \in T} U^R(t,s,a')\beta(t,a'). \quad \square$$

Signaling Games in Nature

- Mapping Types and Actions into Signals:

$$f^S : T \to A; \quad f^R : A \to T.$$

- Sender

$$U^S = I(T, M) + \lambda_S d^S(f^S(t), a).$$

- Receiver

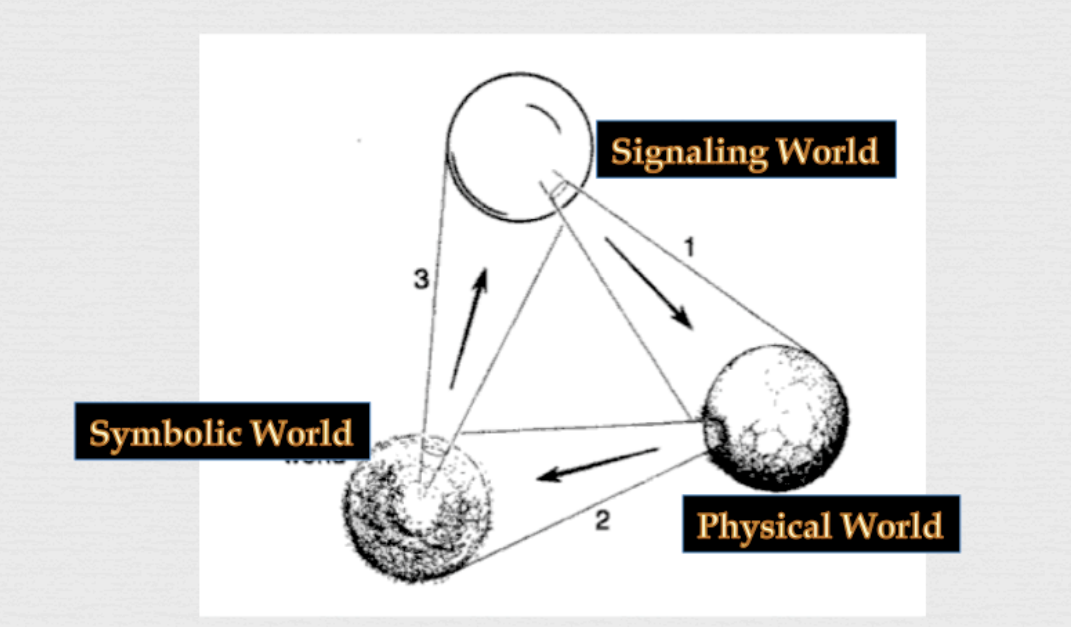
$$U^R = I(A, M) + \lambda_R d^R(t, f^R(a)).$$

Signaling Games

- Separating Equilibrium: Each type t sends a different signal M_t. $f^S : t \mapsto a[M_t]$...
- Pooling Equilibrium: All types t send a single signal $s*$ with probability 1.
- **Convention & Deception**: The divergence between the objective probabilities and the subjective probabilities induced by conventional equilibria.
- **Solution**: Costly Signaling; Credible and Non-credible threat; Aligned Utilities; $2 + m + n$ players

Outline

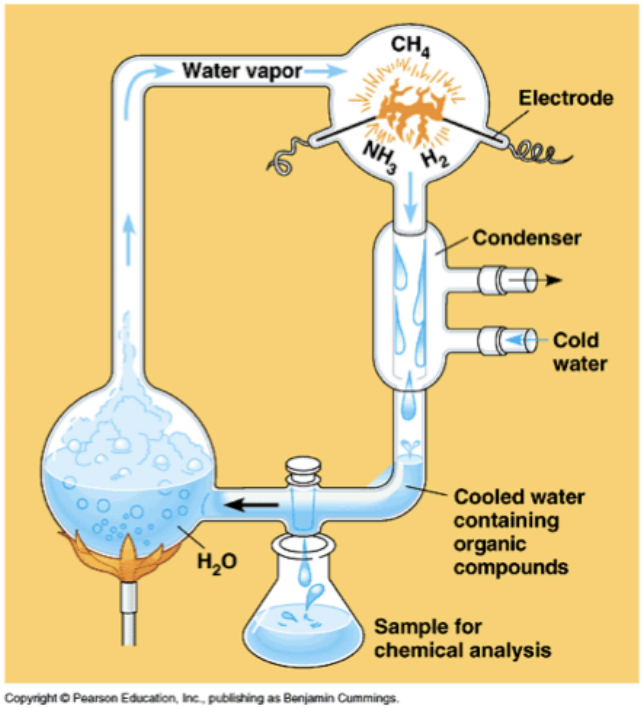
Natural Enigmas



- What contains what?
- Universe, Life and Intelligence
- What came first?

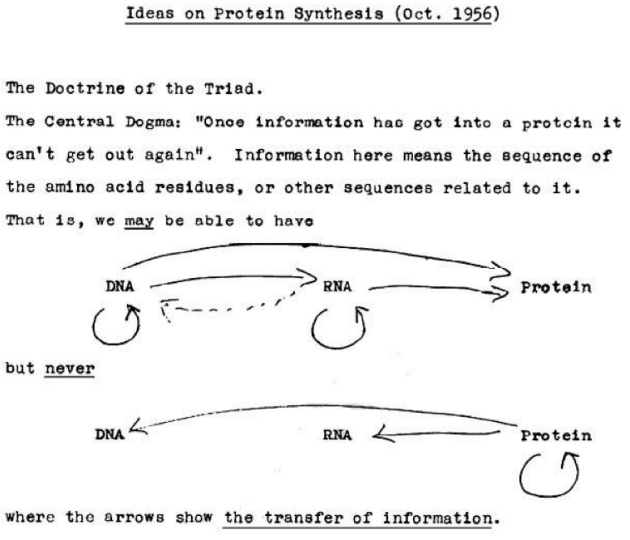
Outline

Origin of Life



- **Four Stages**:
  - Abiotic synthesis of small organic molecules (monomers): ATP
  - Monomers to polymers: RNA World
  - Origin of self-replicating molecules: RNA World/Protein World
  - Mapping Between the Two Worlds
- **The Miller-Urey experiment**:
  After Miller's death in 2007, scientists examining sealed vials preserved from the original experiment

Codons & Anti-Codons



Ideas on Protein Synthesis (Oct. 1956)

The Doctrine of the Triad.

The Central Dogma: "Once information has got into a protein it can't get out again". Information here means the sequence of the amino acid residues, or other sequences related to it.

That is, we may be able to have

DNA RNA Protein

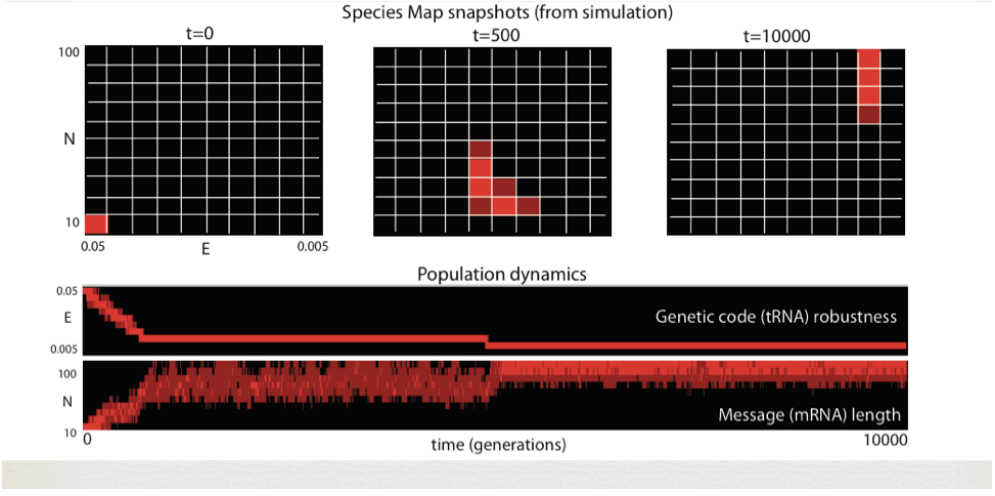
but never

DNA RNA Protein

where the arrows show the transfer of information.

- **A Frozen Accident?**
- **A Signaling Game**:
  - Sender: mRNA $\mapsto$ Receiver: tRNA
  - Evolution of Codons: A conventional Separating Equilibria
  - Codon's **Universality, Immutability and Optimality**
  - Prebiotic Amino Acids & Fitness function

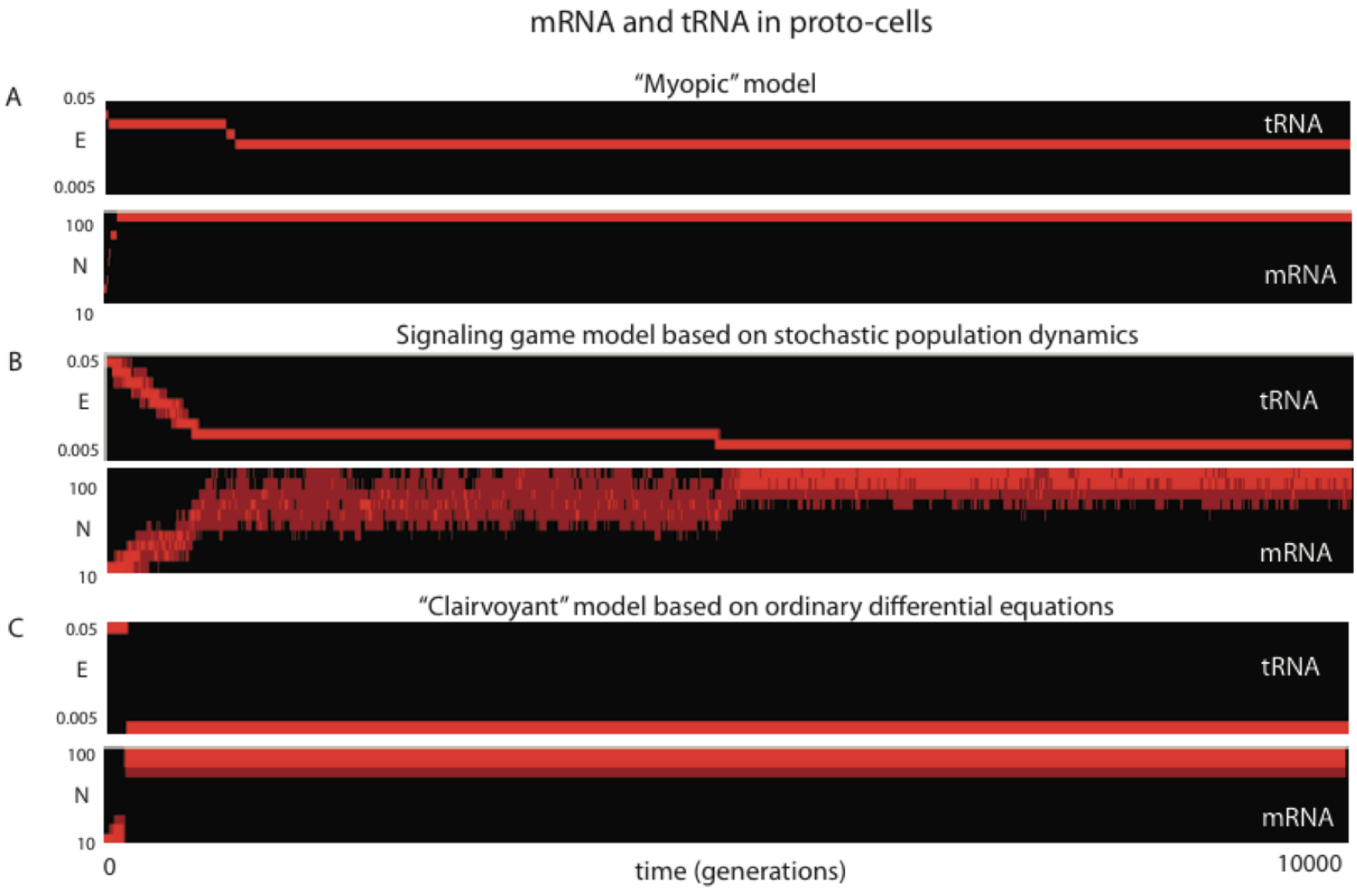
Codon Evolution



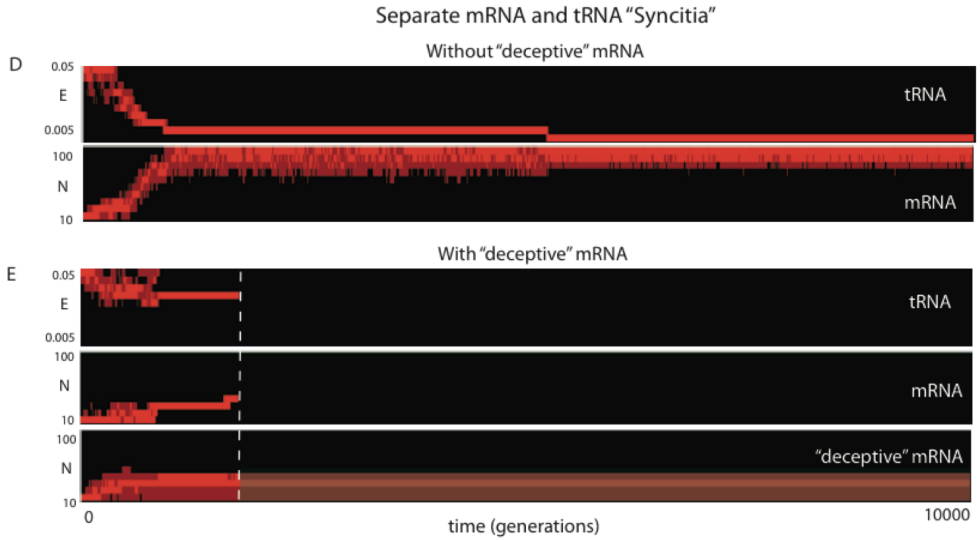
$$\frac{dS}{dt} = S\left(b\left(1-\sum \mu_{\text{out}}\right)-d\right) + \sum S_{\text{others}}\mu_{\text{in}},$$

where b = birthrate (depends on port. length and port. trans. correctly), d = death rate (depends on the carrying capacity and the population size), μ's are the mutation rates (μ_{out} = negatively correlated with port. length), and S = is the size of the population selected.

Simulation of Codon Evolution



Simulation of Codon Evolution



- What about "deception?" (Gene Duplication? Virus?)
- Did they exist inside cells? Syncitia?
- The shortest enzyme is 62 amino acids long... (So what were the first "proteins?")
- What were proto-mRNA and proto-tRNA?

Outline

An Old Debate – Goethe

Protagonists: Biologist Étienne Geoffroy St Hilaire (1772 – 1844) and Anatomist Georges Cuvier (1769–1832)

Time & Place: French Academy – 1830.

Debate between *Philosophical Anatomy* (Geoffroy) vs. *Empirical Anatomy* (Cuvier)

- Geoffroy argued for the unity of animal kingdom.
- Cuvier argued for the existence of four 'embranchments' vertebrates, arthropods, molluscs and echinoderms.

Who was right?

Consider the Lobster

- **Geoffroy's Conjecture**: *The vertebrates were arthropods upside-down; flip the dorsal-ventral morphogenesis.*
- An Anatomical Hurdle: *It seems impossible to map arthropod's ventral nerve cord to vertebrates' dorsal system.*
- It will be few centuries before we'd understand the role of *genes* in the development via control of morphogen gradient. Two genes *sog* and *dpp* (in arthropods) are flipped to the homologous pairs *chordin* and *bmp* (in vertebrates).
- *sog* in the fly, *Drosophila*, determines ventral development: *chordin* in the toad, *Xenopus* , determines dorsal development.

Evo-Devo: Cell-level

We work with an abstraction of a cell that:

- can (noisily) sense some kind of local information $\iota \in \mathcal{I}$, depending on the application
- can produce signals from a set $\mathcal{S}$
- can sense its environment $e \in \mathcal{E} = \mathbb{N}^{\mathcal{S}}$, i.e., the multiset of signals produced by its neighbors
- has a state $\sigma \in \Sigma$, some form of (bounded) memory
- can perform actions $a \in \mathcal{A}$ depending on the application

A strategy is a mapping $s : \Sigma \times \mathcal{I} \times \mathcal{E} \to \Sigma \times 2^{\mathcal{S}} \times \mathcal{A}$.
We denote the individual components as s_Σ, $s_\mathcal{S}$ and $s_\mathcal{A}$.

Evo-Devo: Organism-level (somatic loop)

An organism is a grid of cells. It has a ("germ-line") strategy s.
Under normal circumstances, all its cells have that same strategy s.

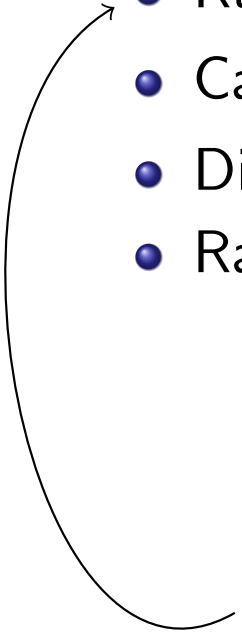
Its dynamics are as follows:

- Chose cells at random; for each cell:
  - Sense local information ι
  - Sense signaling environment e
  - Update state: $\sigma \leftarrow s_\Sigma(\sigma, \iota, e)$
  - Produce signals $s_\mathcal{S}(\sigma, \iota, e)$
  - Perform action $s_\mathcal{A}(\sigma, \iota, e)$

Evo-Devo: Population-level (evolutionary loop)

A population is a set of organisms.

Its dynamics are as follows:



- Run each organism for x steps
- Calculate fitness for each organism (based on rate-distortion)
- Differential reproduction
- Randomly vary each organism's "germ-line" strategy s:
  - Signal duplication: $\mathcal{S} \leftarrow \mathcal{S} \cup \{z_{new}\}$ and update s such that z_{new} is treated like some existing signal
  - Signal removal: $\mathcal{S} \leftarrow \mathcal{S} \setminus \{z\}$ for some $z \in \mathcal{S}$ and update s accordingly
  - Numerical variation, e.g., the dependence of s on $\mathcal{I}$

Rate-distortion based fitness function

Two criteria determine fitness:

- How efficiently is the information communicated?
- How accurately is the information represented?

RDT (rate-distortion theory):

- the former negatively corresponds to the rate R,
- the latter to the distortion D.

We define fitness as $-(R + \lambda D)$ with a Lagrange multiplier λ.

Rate-distortion based fitness function

Given three random variables:

- X over the local information $\mathcal{I}$
- Y over the (combinations of) signals produced
- Z over an interpretation $\hat{\mathcal{I}}$ of these signals (i.e., $\hat{\mathcal{I}} : 2^{\mathcal{S}} \to \mathcal{I}$)

and a distortion measure $d : \mathcal{I} \times \mathcal{I} \to \mathbb{R}$, we get

- $R = I(X; Y)$, the mutual information in X and Y
- $D = \|d(X, Z)\|_p$, the expected distortion between $\mathcal{I}$ and $\hat{\mathcal{I}}$

Segmentation: Instantiations of the general framework

In our segmentation example, we have the following instantiations:

- local information is position ($\mathcal{I} = \{1, \ldots, n\}$)
- information sensed noisily via morphogen gradient
- no actions ($\mathcal{A} = \emptyset$)
- state $\sigma = (U_z)_{z \in \mathcal{S}}$ consists of one "urn" for each signal
- state update: $s_\Sigma(\sigma, \iota, e)$ lets balls in urns decay and adds a new ball to U_z for each signal $z \in e$
- signal selection: $s_\mathcal{S}(\sigma, \iota, e)$ selects signals according to some fixed mapping $\mathcal{I} \to \mathcal{S}$ with additional bias proportional to $|U_z|$ for each signal z

Segmentation: Interpreting signals

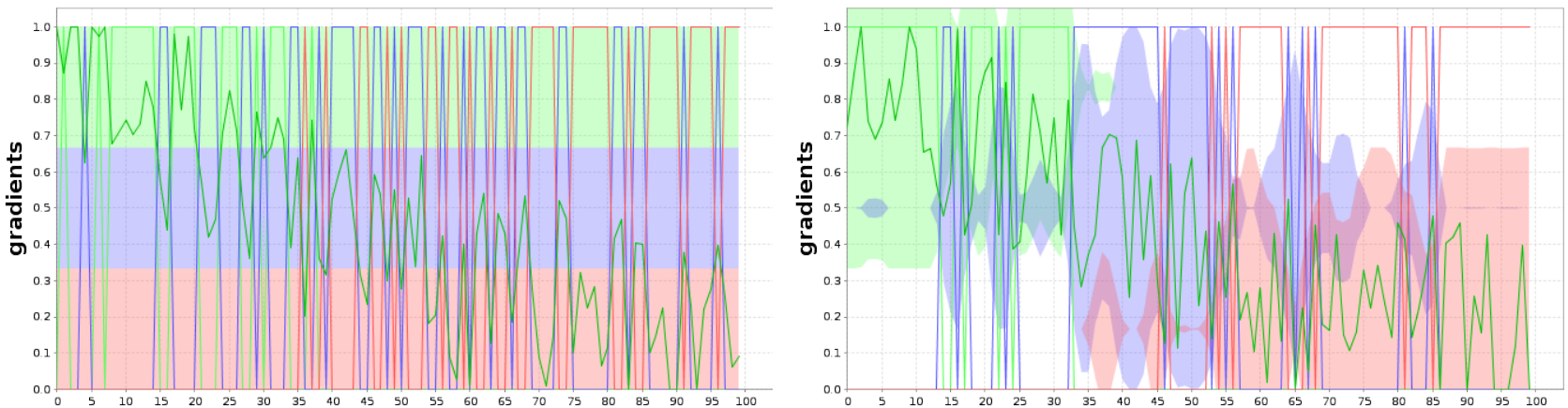
The produced signals can be given meaning (from the perspective of an external observer) as follows.

For each signal combination $z \in 2^{\mathcal{S}}$, the meaning of that combination is the average position of the cells that produce it.

That is, $\hat{\mathcal{I}}(z) = \text{avg}_{\{c|z=z_c\}}\{\mathcal{I}_c\}$, where z_c stands for the (combination of) signals currently produced by cell c, and $\mathcal{I}_c$ for its (true) local information, i.e., position.

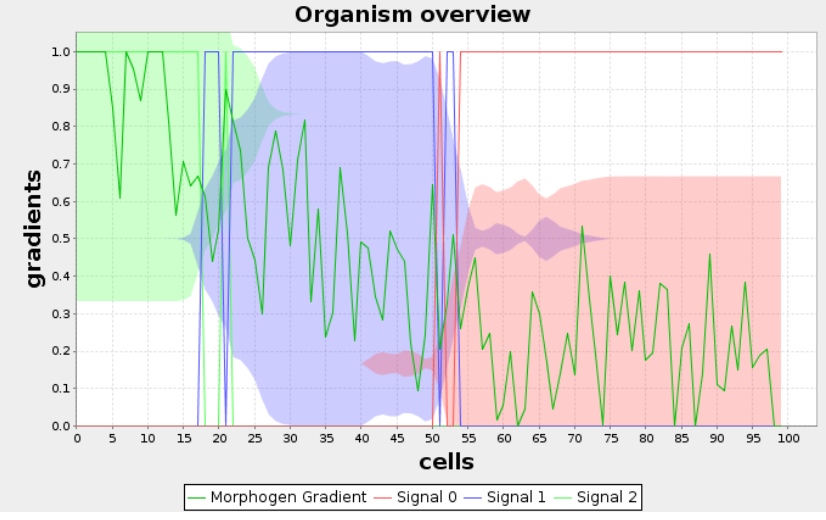
Segmentation: Some screenshots of an organism

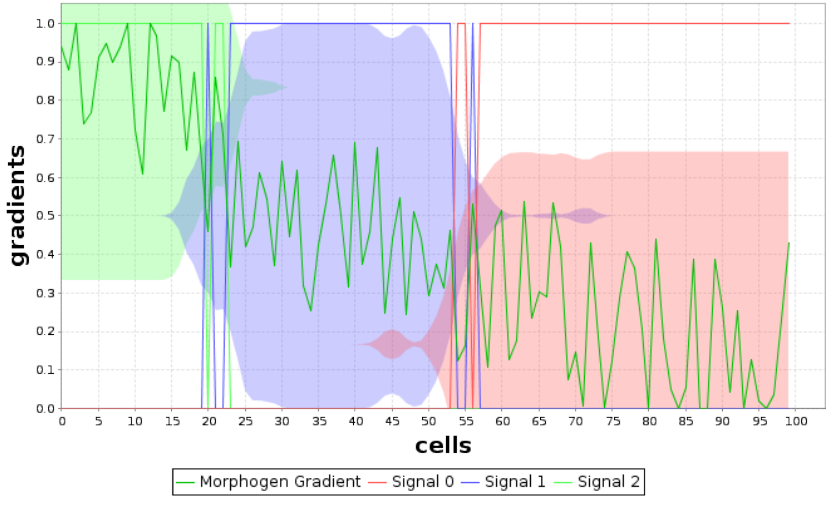
A one-dimensional organism after 0 & 100 steps. $\mathcal{I}$ is normalized to $[0, 1]$. The green line shows the morphogen gradient as currently sensed by the cells (i.e., noisy). The remaining lines depict the currently produced signals. Shaded regions depict $s_{\mathcal{S}}$ after bias has been applied.



Segmentation: More screenshots of an organism

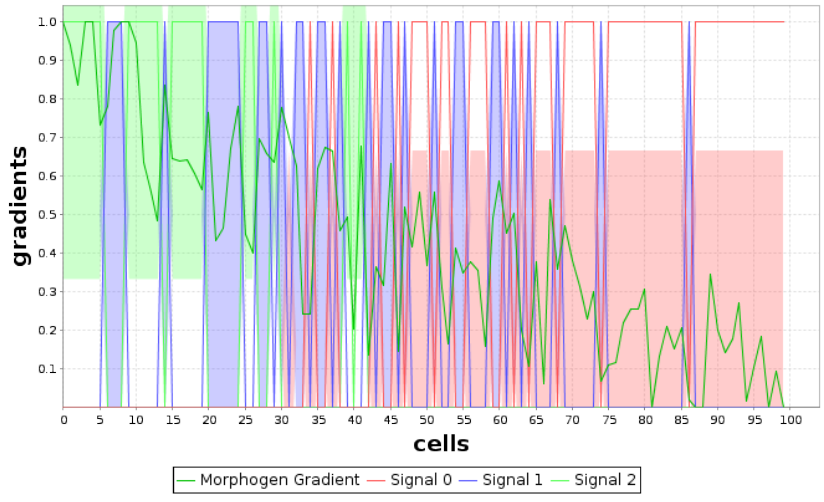
... after 10000 & 15000 steps.

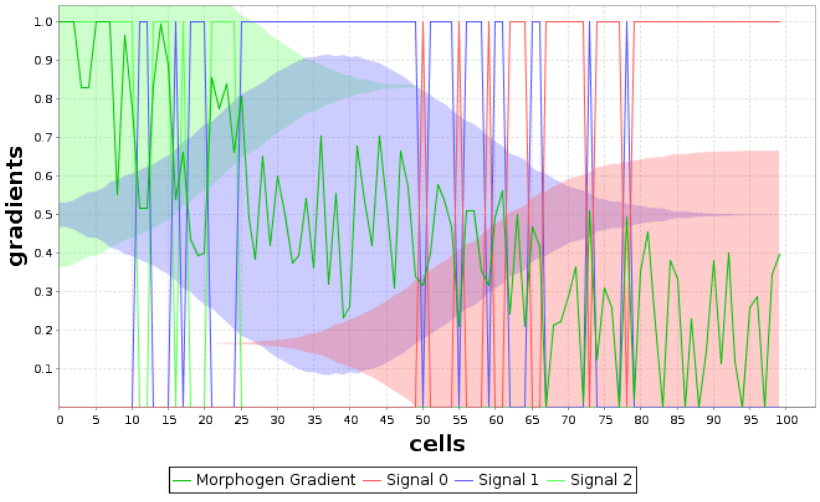




Segmentation: too little or too much sensing

Showing organisms that sense only self, or sense 3 of the 30 nearest neighbors, rather than direct neighbors plus self. After 15000 steps.





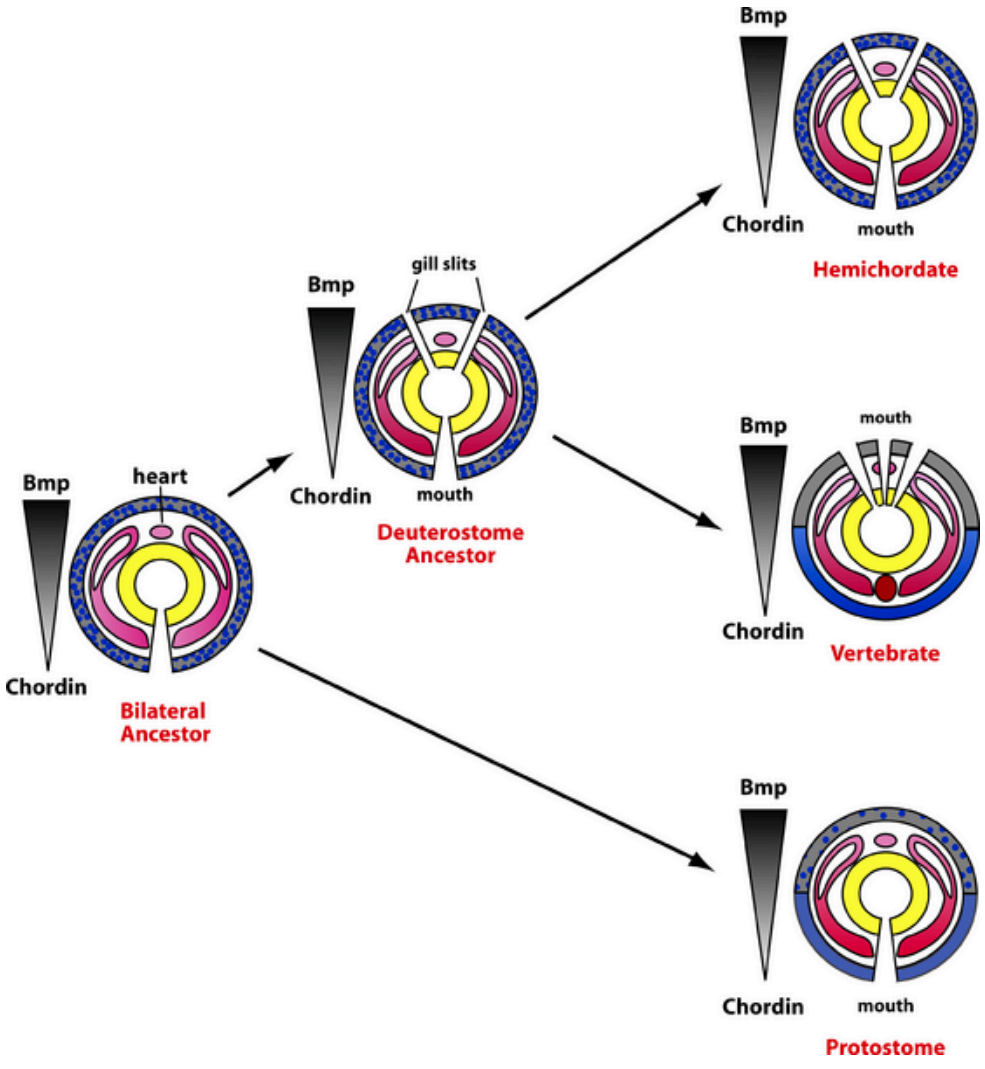
Equilibria

- Separating Equilibrium: Each type t sends a different signal M_t. $f^S : t \mapsto a[M_t]$...
- With two signals $\{\text{BMP}, \text{Anti-BMP}\}$, Arthropods (Protostomes) and Vertebretes (Deuterostomes) represent two different *separating equilibria*. Just as Geoffroy thought!
- Pooling Equilibrium: All types t send a single signal $s*$ with probability 1
- Are there examples of *pooling equilibria* in nature (on earth or some other exoplanet)?

Hemichordates

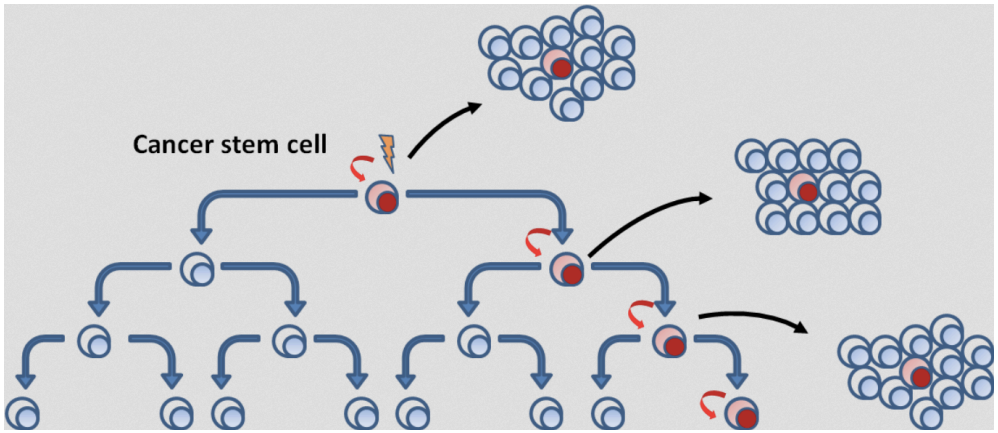
- Saccoglossus kowalevskii (with a diffused CNS; nerve-nets) - Considered a Deuterstome

Signaling Equilibria



- Phylogeny?

Cancer Stem Cells Signaling Games



- Sender: CSC $\mapsto$ Receiver: Progenitors
- Signaling for feedback inhibition.
- Information: Cell density control
- Disregulation in signaling: Information Asymmetry and Deception

Outline

Internet of the Future

- *Signaling on the Internet*
- Sender-Receiver Games:

  Example: User has private data (his Type), Signals Google using meta-data (keywords), Google retrieves a page.
- Examples: Google Game, Netflix Game, Bit-coins Game and AdX Game
- Deception: To be controlled by Recommenders and Verifiers.
- Recommenders ensure *Liveness*: $\forall_A \exists_T \exists_S U_S(T, M, A) \geq \theta^*$.
- Verifiers ensure *Safety*: $\forall_T \exists_A \exists_R U_R(T, M, A) \geq \theta^*$.

Google Game

- - Sender's type = State of ignorance;
  - Receiver's action = Relevant page;
  - Signal = keyword.
- Recommenders are Markovian (static).
- Verifiers are oblivious.
- A simple system, resulting in "Random Surfer with Teleportation."
- Equilibrium results in a Ranking a system: Second Eigenvector of a Graph-Laplacian.

NetFlix Game

- - Sender's type = Choices determined by private state,
  - Receiver's action = Signals = A movie.
- Recommendation system is determined by the receiver's revealed utility, and imputation of his unrevealed utilities (Movie Ranking)
- The utilities are imputed by completing a User $\times$ Movie matrix (Determined by an SVD algorithm)
- Verification is determined by "other users like you."

BitCoin Game

- - Sender's type = Content of S's Bitcoin Wallet,
  - Receiver's action = Update of R's Bitcoin Wallet,
  - Signal = Encrypted Message Signed with S's private key.
- Verifiers are the Bitcoin Miners (with costly signaling, determined by proof-of-work = Computationally hard problem.)
- Block-chains.

AdX Game

- Auction platforms for online ad impressions
  – An impression is an ad shown to a consumer on a website
- Auctions occur when consumers visit websites listed on the exchange in following steps
  1. Consumer visits website
  2. Exchange is notified of available impression
     – Notification includes impression metadata (e.g. website content category, consumer cookies)
  3. Advertisers bid on the impression
     – Impression metadata
     – First and third party data
  4. Winning advertiser's ad appears on the site

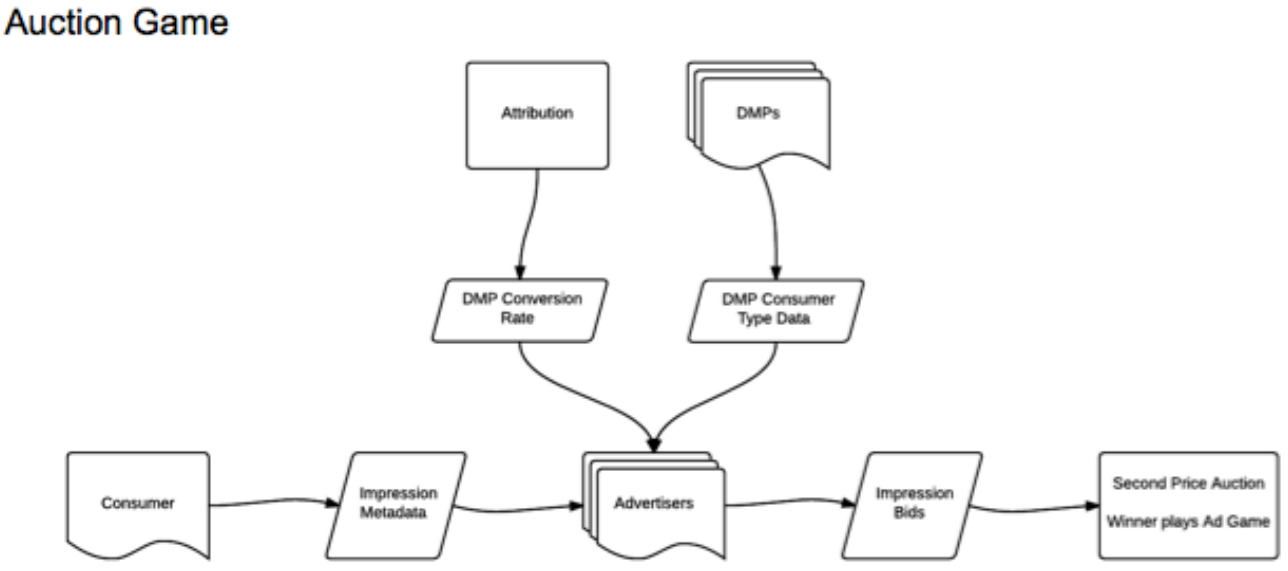
AdX Game

- Audience Targeting
  - bid on specific consumer demographics
  - e.g. women, college students
- Contextual Targeting
  - bid on websites that contain specific content
  - e.g. movies, news
- Complex Boolean Targeting
  - e.g. (men & sports sites & weekday evenings)

AdX Game

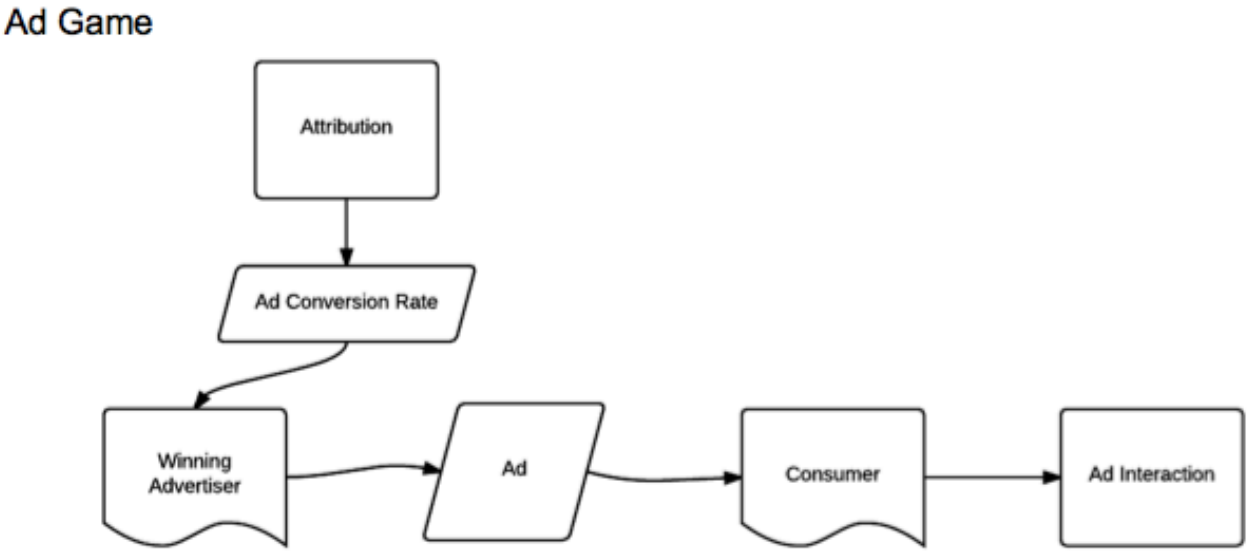
- Consumers and Advertisers send messages
  - consumers send impression metadata
  - advertisers send (drumroll) ads
- Both wish the other to perform certain actions
  - consumers want to be shown suitable ads
  - advertisers want consumers to buy their products
- Both have hidden types

Ad Signaling Consumer → Advertiser



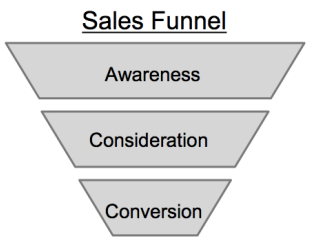
- Sender: Consumer
- Receiver: Advertiser

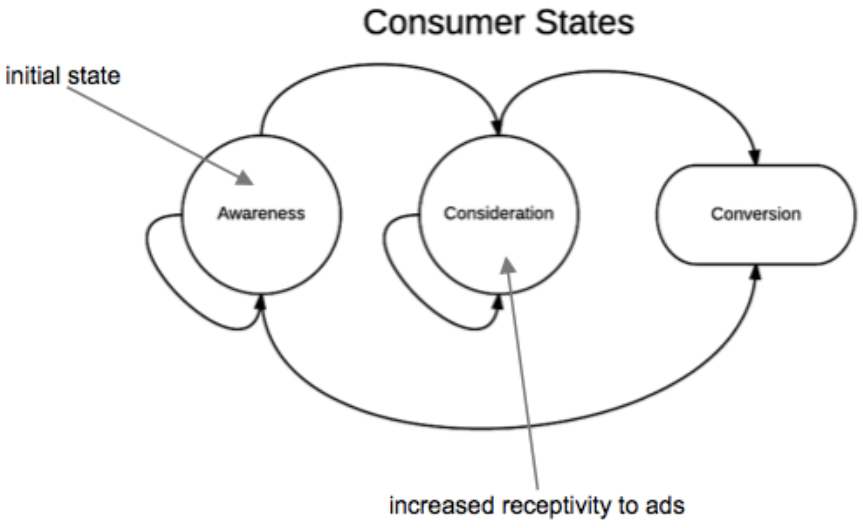
Ad Signaling Advertiser → Consumer



- Sender: Advertiser
- Receiver: Consumer

Complex Signaling





- State evolution

Utilities

- Player Types are unit vectors in R^n
  – consumer types are interpreted as the consumer's affinity for types of products
  – advertiser types are interpreted as the advertiser's products' appeal
- Player Messages are unit vectors in R^n (perturbation of types)
- Player Actions are selected by utilities represented as tensors
  – features are inferred by a Tucker decomposition

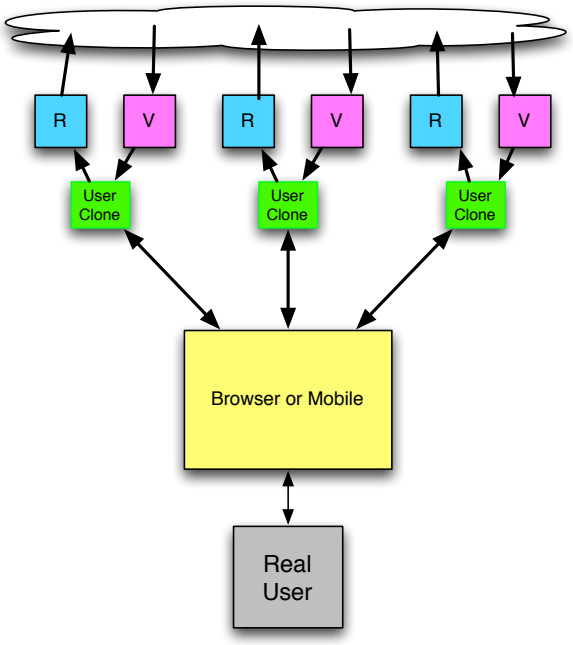
Signaling Game Machine

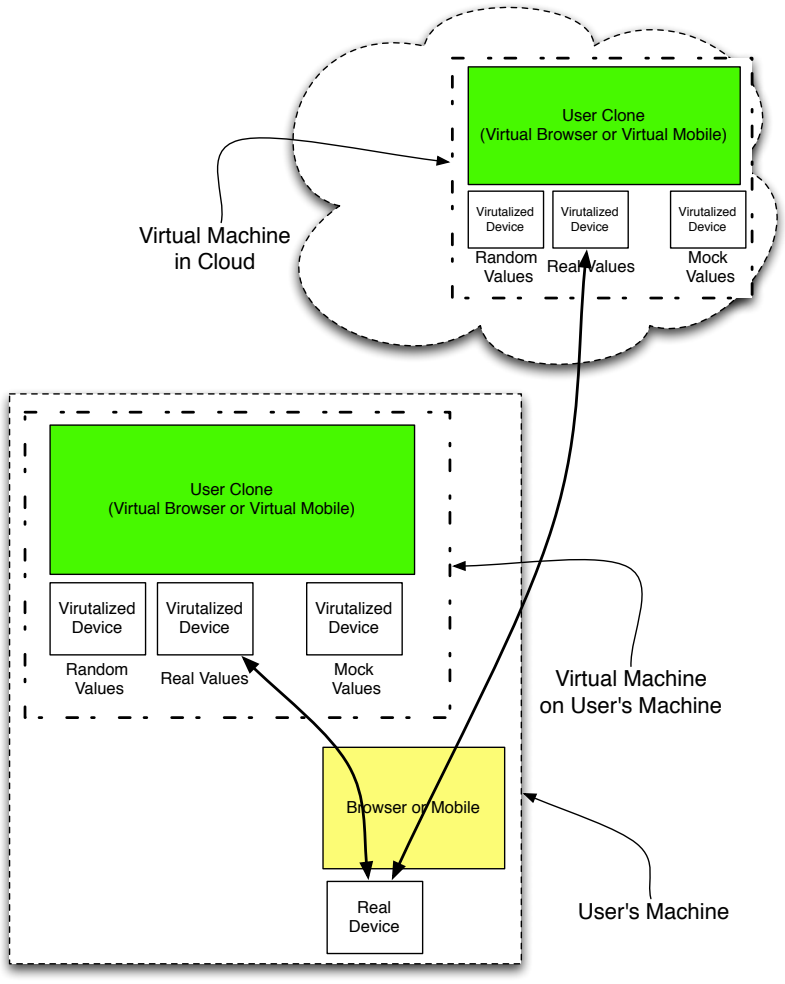
- **Cloud**: Private secure storage, housing sender's (receiver's) types/states and their temporal evolutions.
- **Browser**: Partitioned into several containers, and each container holds a specific clone
  – (e.g., a dumb-clone to surf the web, a financial clone to access the bank, another financial clone to access the investments in risky assets, a healthcare clone, etc.) along with a group of verifiers and recommenders (software agents)
- **VMM (Virtualization)**: Maintains an "approximate bisimulation" relation with the true underlying states and their evolutionary trajectories.
  – any such clone can (with the help of the verifiers and recommenders) generate and emit a suitable signal to its intended receiver.

Signaling Game Machine

- After the signal transmission results in action, the resulting utilities are estimated and reported back to each player, who then respond by modifying their composition of verifiers and recommenders in preparation of the subsequent repetition of signaling games.
- **Anonymization**: A group of clones from many different individuals may form a coalition, to be represented by a virtual meta-clone
  – Meta-clones are implemented using a Mix Network
  – A meta-clone is not anonymous, the meta-clone can be monitored, ranked and penalized.

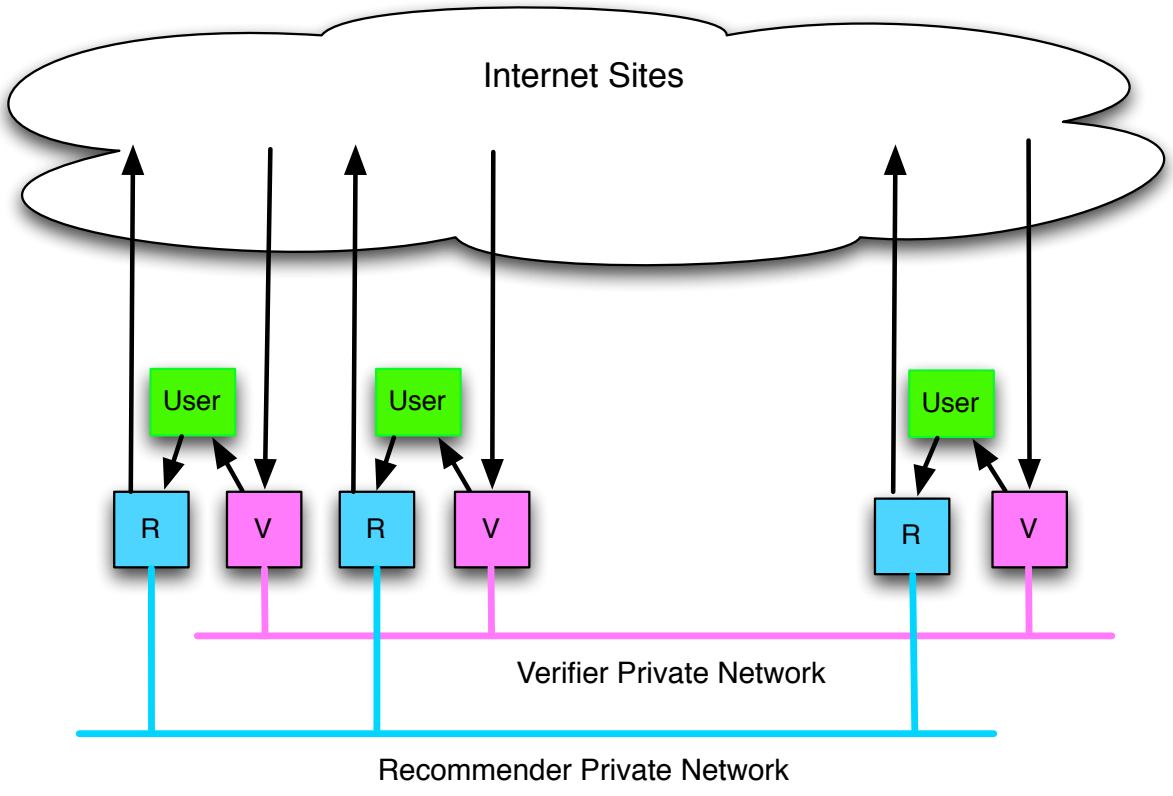
SGM





- Virtualization

SGM: Veras & Rekhas



- Global View

Outline

Cyber Security

- **Traditional (Forensic) Analysis Approaches**:
  - Threat analysis operation centers,
  - Incident response teams,
  - Forensic analysis,
  - Network forensics,
  - Indicator/signature expansions,
  - Reverse engineering malware (configuration discovery),
  - Malware runtime analysis,
  - Design recovery, V
  - Vulnerability enumeration,
  - Fuzz testing,
  - Red/blue penetration testing.

Cyber Security

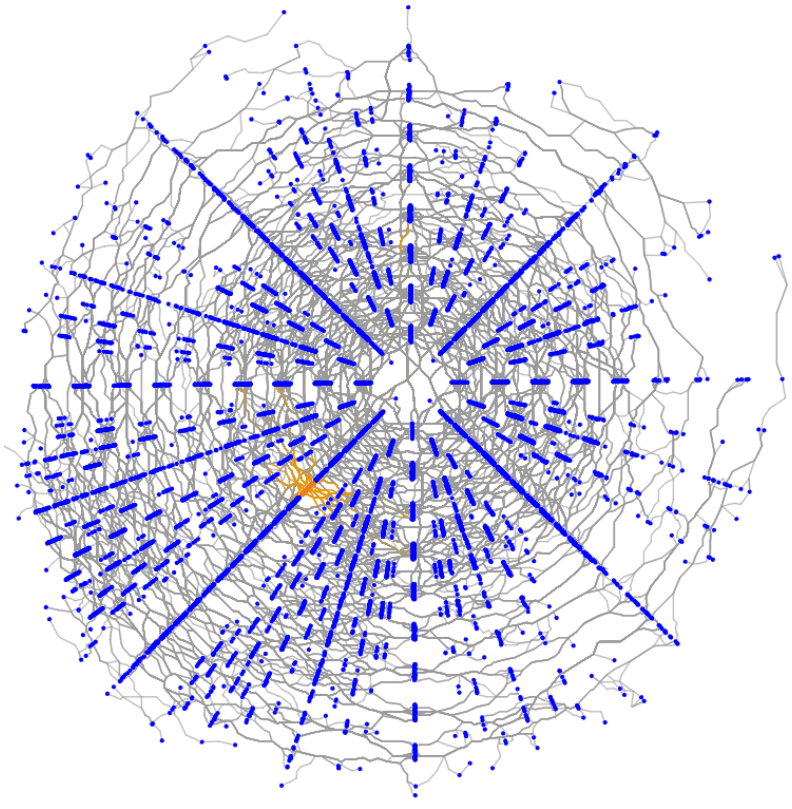
- **Traditional Engineering Approaches**:
  - Secure coding patterns,
  - Security properties/hyper properties and
  - Model checking.

Cyber Security

- Still unclear what approaches may enhance security and privacy (globally).
- **Our (Signaling) Game pproach**:
  - Consider the agent based utilities behind the malicious behavior (cyber deception)
  - Focus the engineering approaches into agent transferable tools.

MBMC (Airforce), NYU, CMU & SEI.

Cyber Evolution



- Sender: App-Store $\mapsto$ Receiver: App-User
- Multi-player Game: with Recommenders-&-Verifiers
- Costly Signaling: M-coins
- Evolutionarily Stable Strategies

Cyber Security

- App-user can receive a free app from an app-store.
- The app-developer knows whether the app is beneficent or malicious; but user doesn't.
- User must decide what action to take:
  - Ignore it
  - Download the App
  - Download and test; give the developer a reputation score, etc.

Cyber Security

- **Avoiding deception?**
- **Credible (and Non-credible) Threats**: Use threats (and promises) to alter other players' expectations of his future actions, and thereby induce them to take actions favorable to him or deter them from making moves that harm him. To succeed, the threats and promises must be credible. (Somewhat Problematic).
- $2 + m + n$-**Players**: (Sender + Receiver + Verifier + Recommenders)...
- **Handicap Principle**: Make signals costly to the signaler, costing the signaler something that could not be afforded by a player with less of a particular trait.

M-Coins

- **A perishable crypto-coin**
- They expire and cannot be reused.
- They are created by a group of trusted authorities; who have the ability to verify an agent's "attack surface."
- They must be used only in a transaction when an agent is challenged.

Asymmetry Breaking

- A sender may act in the "cooperate" behavior mode by sending a useful app honestly or the "defect" behavior mode by sending a malicious app deceptively
- A receiver may act in the "cooperate" behavior mode by accepting trusted or the "defect" behavior mode by responding with a challenge.
- Failing the challenge (namely, in delivering an M-coin in response) results in eviction from the game.

System Parameters

- The payoff-parameters in the next table are as follows:

$$
\begin{aligned}
a &= \text{the } \textit{cost of app}, \\
b &= \text{the } \textit{value of app}, \\
c &= \text{the } \textit{cost of verification}, \\
d &= \text{the } \textit{benefit of hack}, \\
e &= \text{the } \textit{cost of getting caught}, \\
f &= \text{the } \textit{benefit of catching malicious user}, \textit{and} \\
g &= \text{the } \textit{cost of challenging a sender}
\end{aligned}
$$

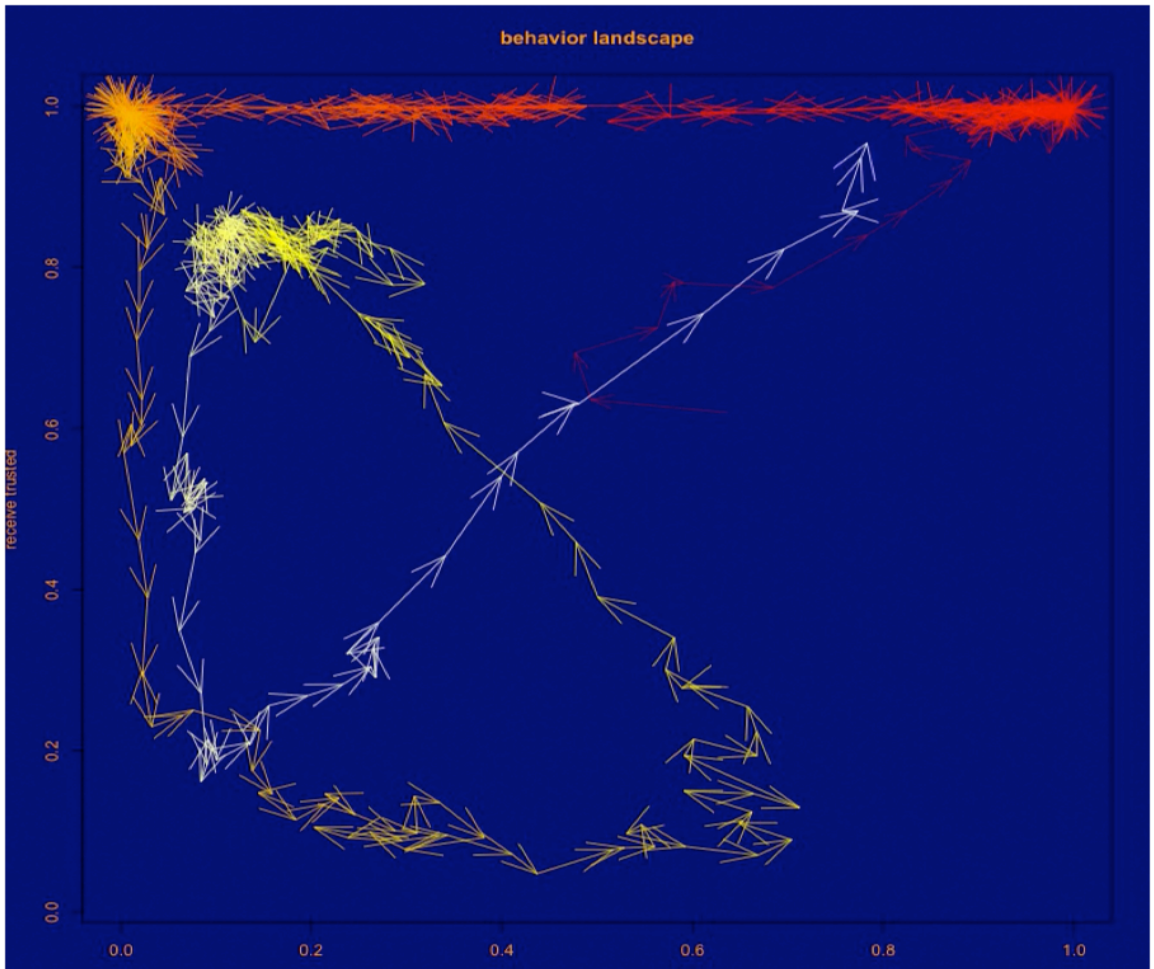
Payoffs

Table: Row player is the sender, column player is the receiver.

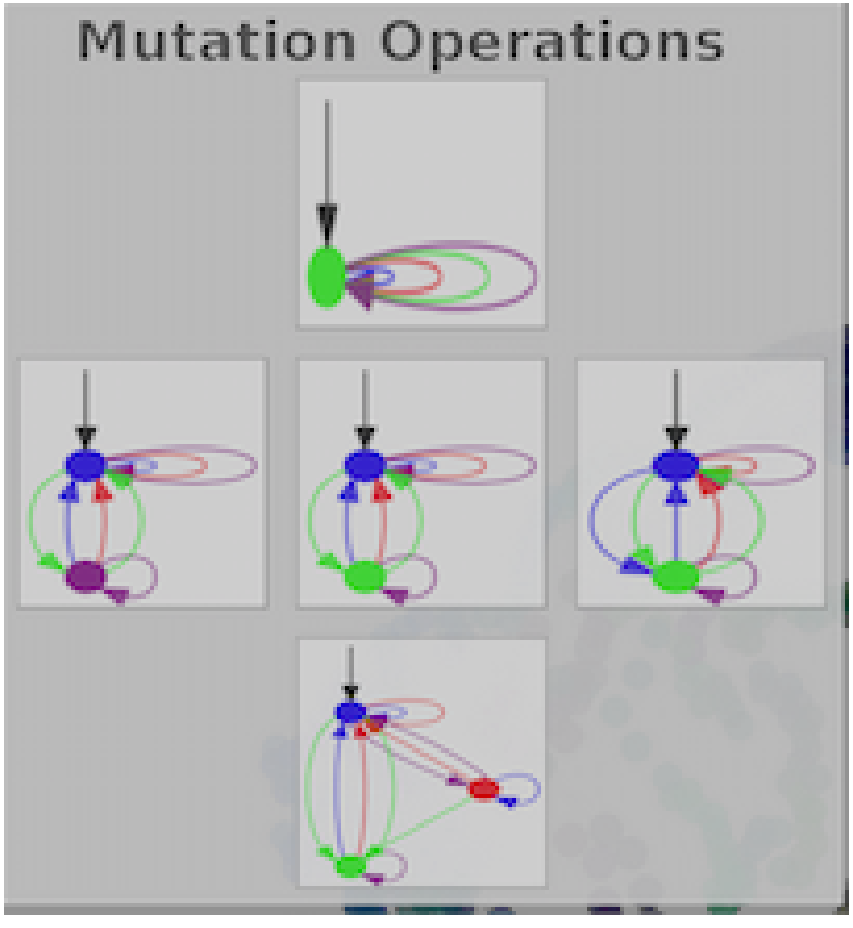
receiver → sender ↓	CC	CD	DC	DD
CC	b b	$b-c$ $-g$	$-d$ $b+d$	$-c-d$ $d-g$
CD	$-g$ $b-c$	$-c-g$ $-c-g$	$f-g$ $b-c-e$	$-c+f-g$ $-c-e-g$
DC	$b+d$ $-d$	$b-c-e$ $f-g$	0 0	$-c-d-e$ $d+f-g$
DD	$d-g$ $-c-d$	$-c-e-g$ $-c+f-g$	$d+f-g$ $-c-d-e$	$-c-e+f-g$ $-c-e+f-g$

.

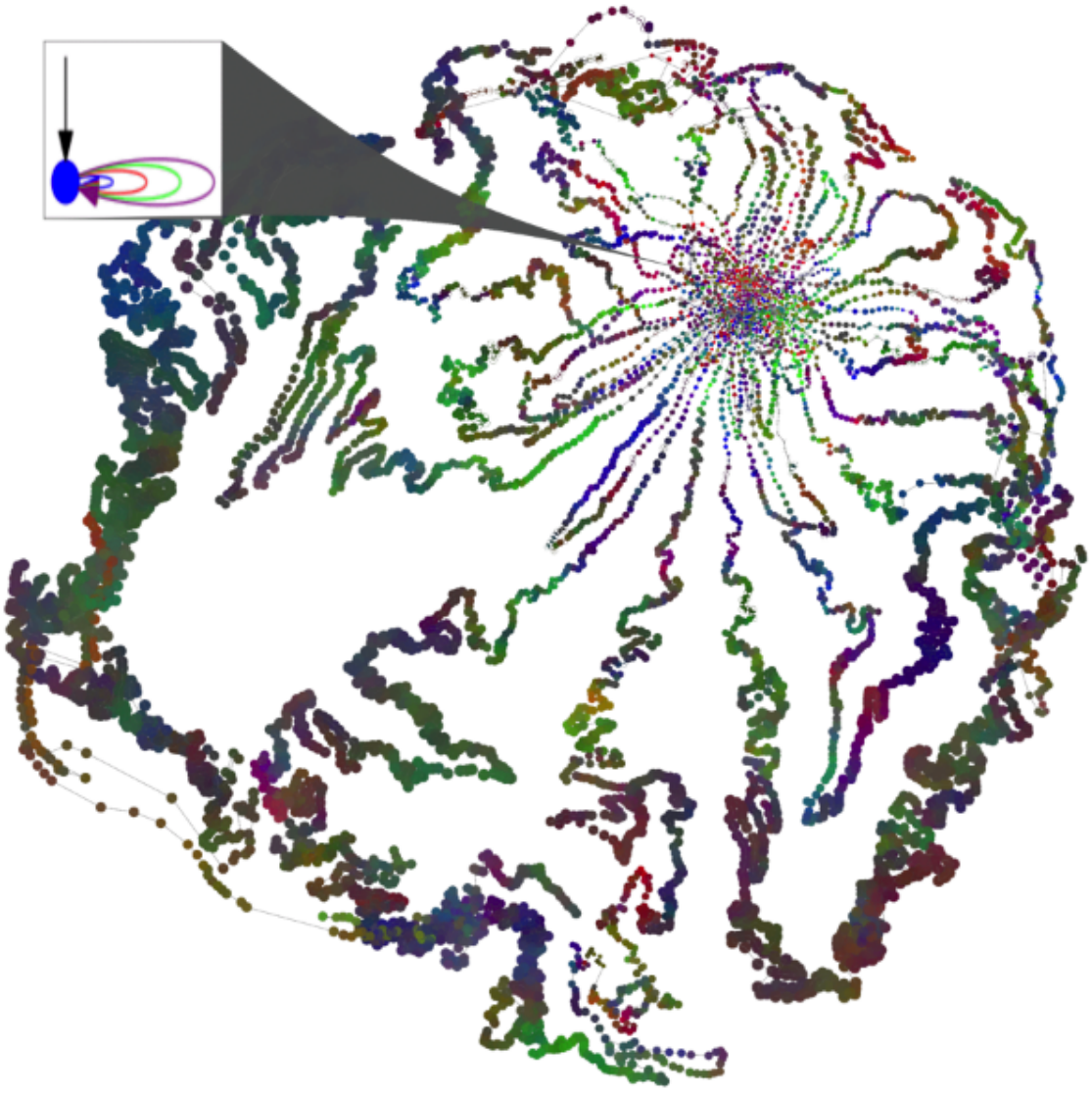
Game Dynamics



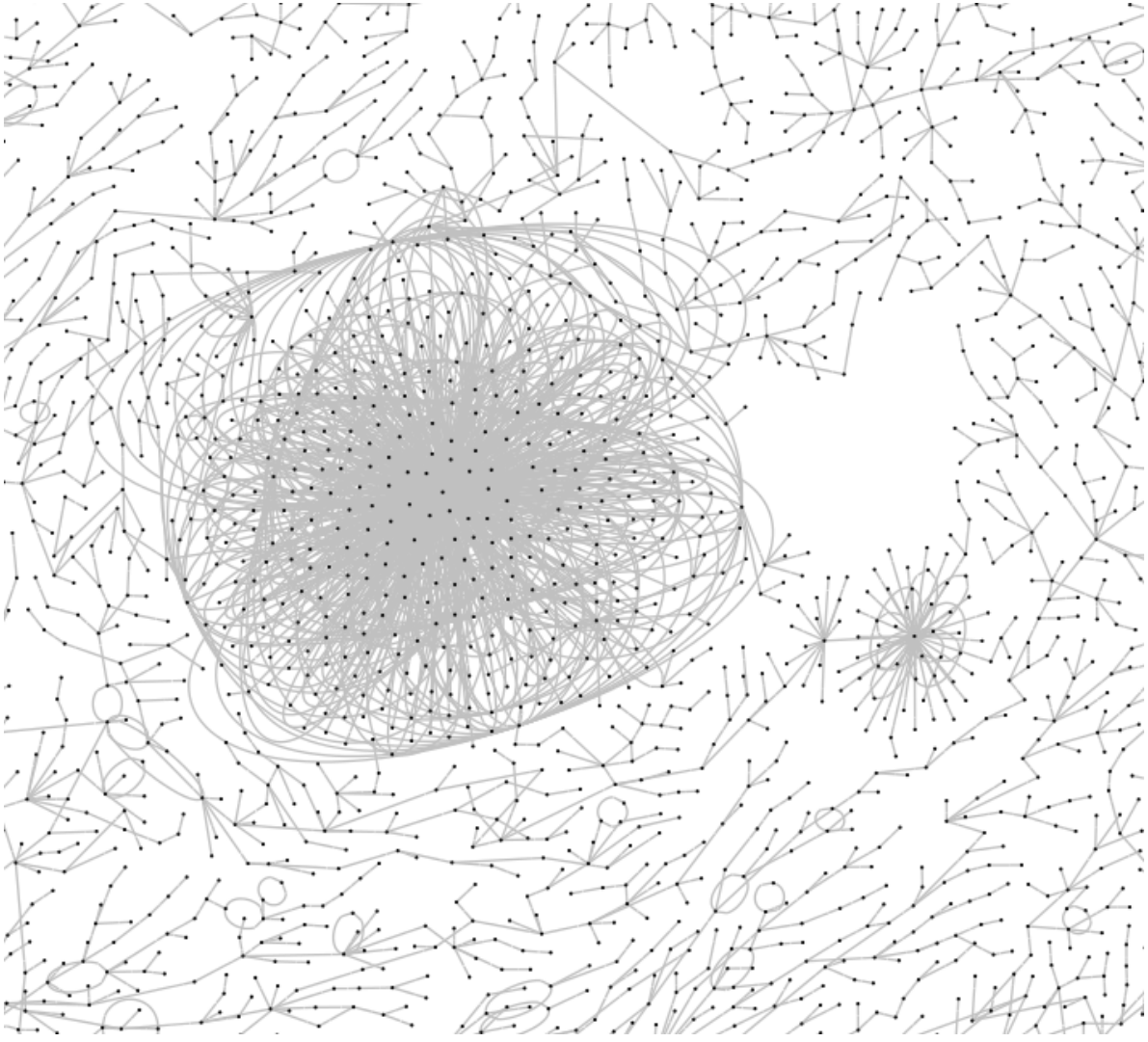
Game Dynamics



Game Dynamics



Game Dynamics



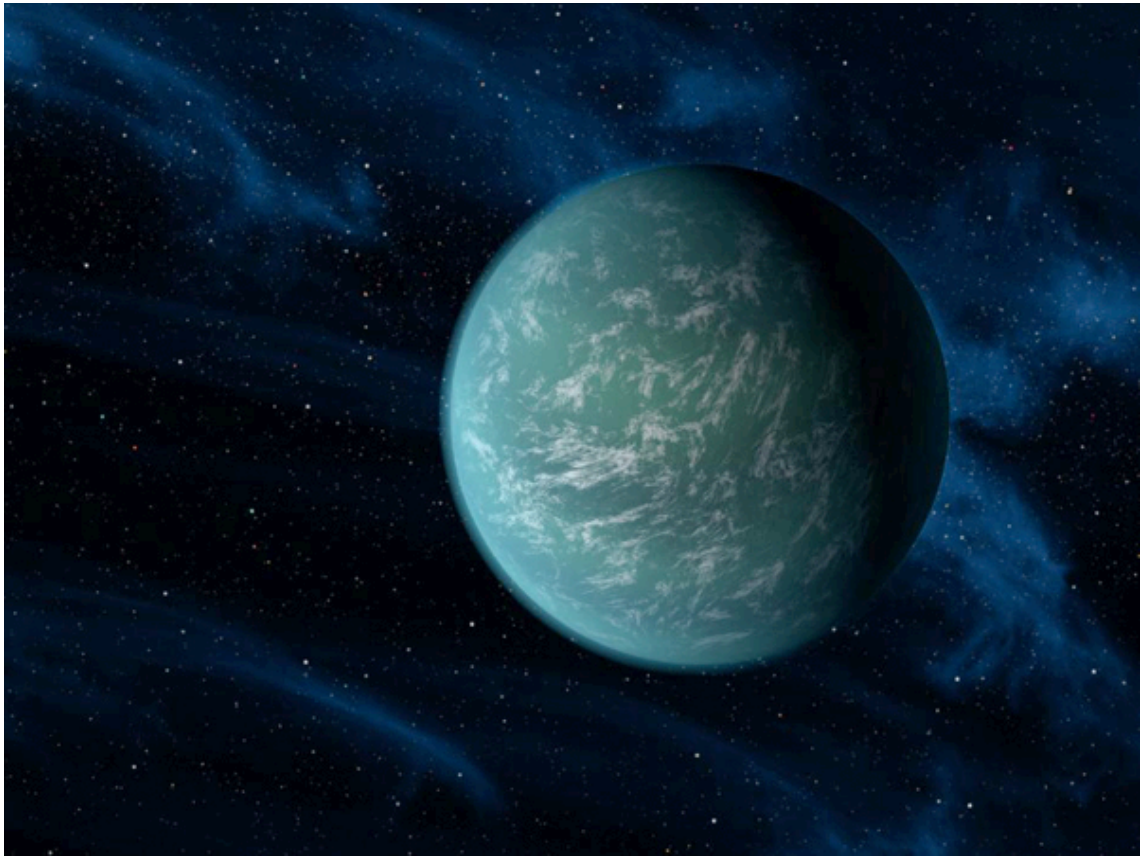
Evolving Evolution

- Cancer: CHA (Cancer Hybrid Automata) and Therapy Design
- Multi-Cellularity and Aging: Neural Systems, Immune Systems
- Internet: Cyber Security, Crypto-Coins, Private Data Markets, Glass Bead Games
- Economics: Financial Markets (Exchanges and Dark Pools)
- Politics: Governance

LEDS: Lab for Entrepreneurship in Data Sciences.

Outline

Another Earth



- Kepler-22b
- An extrasolar planet orbiting G-type star Kepler-22. It is located about 600 light years away from Earth in the constellation of Cygnus.

"Klaatu Barada Nikto"

- Will they have RNA, DNA and Protein? Crick's dogma? Genetic Codes?
- Can we find multi-cellular alien life-forms somewhere else?
- Will they look anything like us? In their body plan, will they have mouth in the front (ventral) and anus in the back (dorsal)?
- Will they have feelings? Will they have a central nervous system (CNS)?
- Will they have limbs? Will they have fingers? How many?
- Will they say, "Klaatu Barada Nikto?"
- Will they trade gold kryptonite?
- In Elohim will they trust?
- Will they have a theory that multi-cellular life could have evolved on earth about 1 bya?

End

- La fin
- Die Ende
- Shuryou
- Slutten
- Wakas
- Sfarsit
- Samapta
- El fin
- Son
- Ukuphela