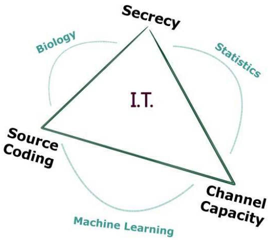
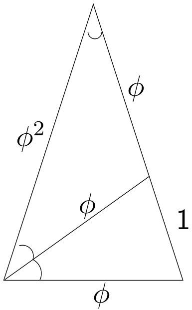
Communication in Networks for Coordinating Behavior

Paul Cuff

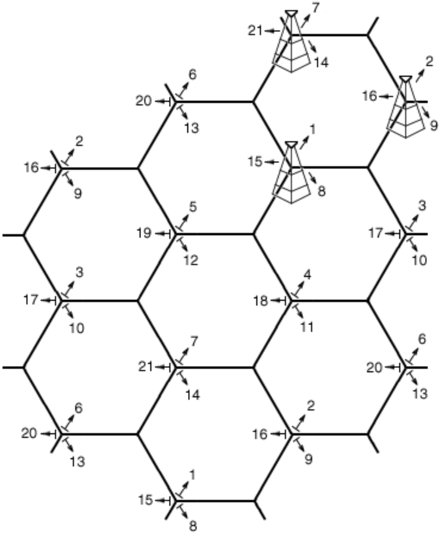
Stanford University

June 5, 2009

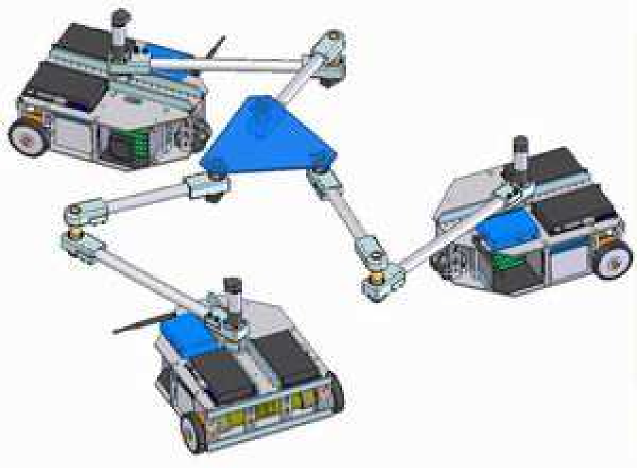




Cellular Communication Systems

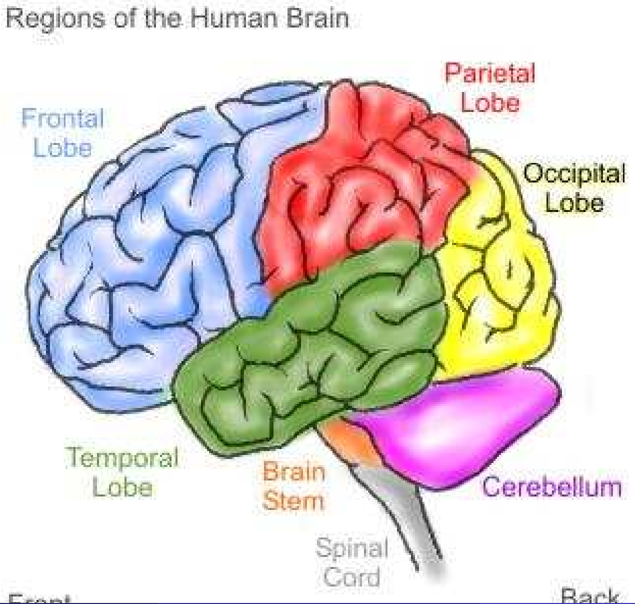


Distributed Sensing and Control



Competitive Settings

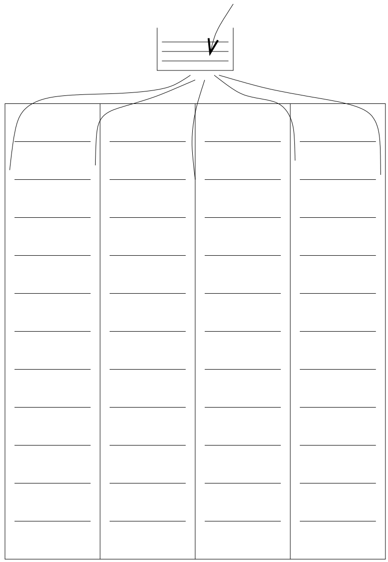
Parallel Processing in the Brain



Data Centers

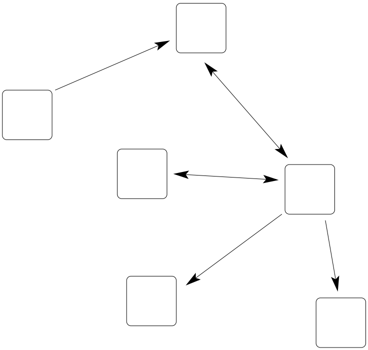
Data Center

Computations can be divided among computers in a data center.



Overview - Coordinating Actions in a Network

Network of nodes with communication:

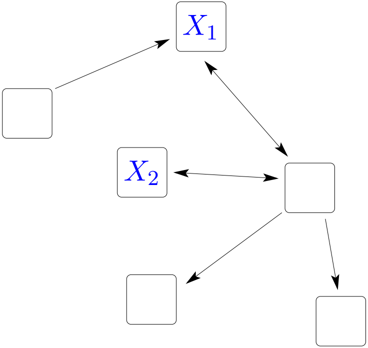


Other work moving information in networks:

- The Gossiping Dons Problem [Bollobas, The Art of Mathematics]
- Distributed Average Consensus [Tsitsiklis, Bertsekas, Athans 84]
- Communication Complexity [Yao 79]
- Function Computation [Ayaso, Shah, & Dahleh 08]

Overview - Coordinating Actions in a Network

Network of nodes with communication:

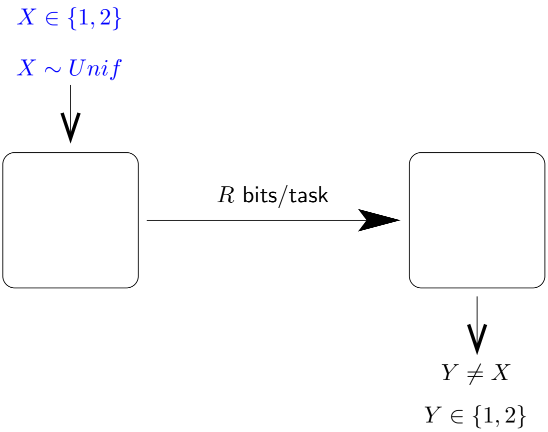


Other work moving information in networks:

- The Gossiping Dons Problem [Bollobas, The Art of Mathematics]
- Distributed Average Consensus [Tsitsiklis, Bertsekas, Athans 84]
- Communication Complexity [Yao 79]
- Function Computation [Ayaso, Shah, & Dahleh 08]

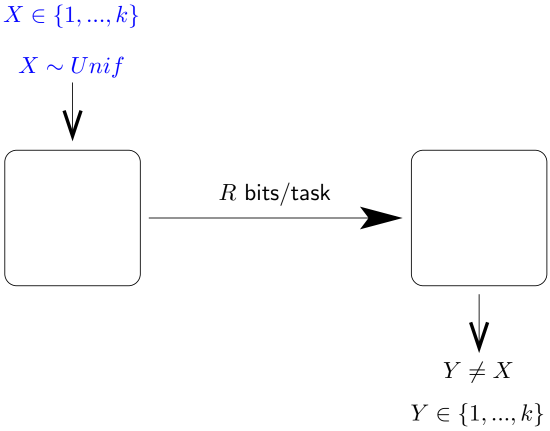
Two Nodes

Tasks are identified by numbers.



Two Nodes

Tasks are identified by numbers.



Buffer of Tasks

Example ($R = \frac{1}{4}$, $k = 5$):

Tasks assigned to X: X_1 X_2 ... each independent

Sample realization: 3 1 2 5 3 5 2 4

Buffer of Tasks

Example ($R = \frac{1}{4}$, $k = 5$):

Tasks assigned to X:	X_1 X_2 ...	each independent
Sample realization:	3 1 2 5 3 5 2 4	
Message bits:	$b_1 b_2 = 01$	

Buffer of Tasks

Example ($R = \frac{1}{4}$, $k = 5$):

Tasks assigned to X: X_1 X_2 ... each independent

Sample realization: 3 1 2 5 3 5 2 4

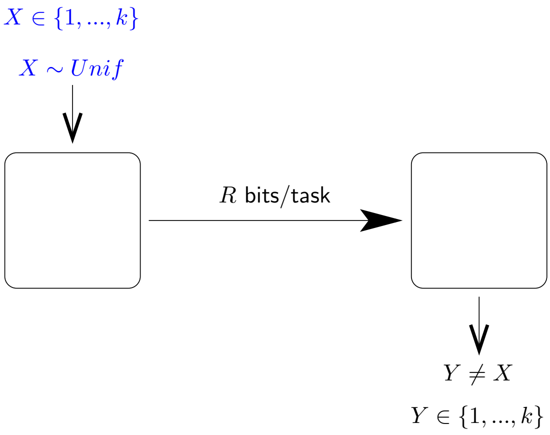
Message bits: $b_1 b_2 = 01$

Codebook:

b_1 b_2	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8
0 0	1	2	3	4	5	1	2	3
0 1	2	4	1	3	5	2	4	1
1 0	...							
1 1	...							

Two Nodes

Tasks are identified by numbers.



Concept from Rate-distortion Theory

To generate correlated actions $\sim p(x,y)$,

$R \geq I(X;Y)$ is required.

$$
\begin{aligned}
I(X;Y) &= H(X) + H(Y) - H(X,Y), \\
H(X) &= \mathbb{E} \log \frac{1}{p(X)}.
\end{aligned}
$$

To generate correlated actions $\sim p(x, y)$,

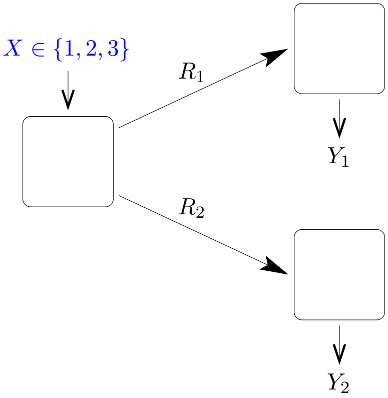
$R \geq I(X;Y)$ is required.

$$
\begin{aligned}
I(X;Y) &= H(X) + H(Y) - H(X,Y), \\
H(X) &= \mathbb{E} \log \frac{1}{p(X)}.
\end{aligned}
$$

Choose $(X,Y) \sim Unif\{(i,j) \ : \ i \neq j\}$.

$R_{min} = \log\left(\frac{k}{k-1}\right)$.

Three Node Network



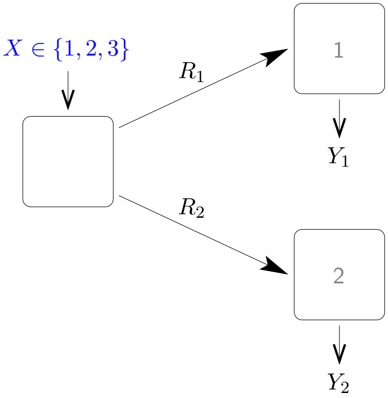
Ideas for assigning tasks uniquely (i.e. $X \neq Y_1 \neq Y_2 \neq X$).

Assign Y_1 first: $R_1 = \log\left(\frac{3}{2}\right)$.

Assign Y_2 using full rate: $R_2 = \log 3$.

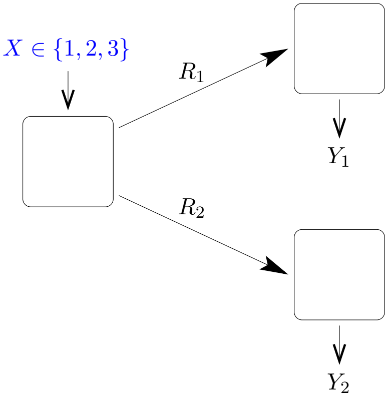
$R_{ave} = \log_2 3 - 1/2$.

Three Node Network



Ideas for assigning tasks uniquely (i.e. $X \neq Y_1 \neq Y_2 \neq X$).
Assign $Y_1 \in \{1, 3\}$: $R_1 = H\left(\frac{1}{3}\right)$.
Assign $Y_2 \in \{2, 3\}$: $R_2 = H\left(\frac{1}{3}\right)$.
$R_{ave} = \log_2 3 - 2/3$.

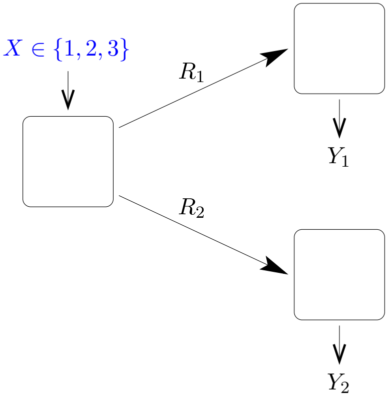
Three Node Network



Techniques so far:

$$
\begin{aligned}
R_1 &\geq I(X;Y_1), \\
R_2 &\geq I(X;Y_2), \\
R_1 + R_2 &\geq I(X;Y_1) + I(X,Y_2) + I(Y_1;Y_2|X).
\end{aligned}
$$

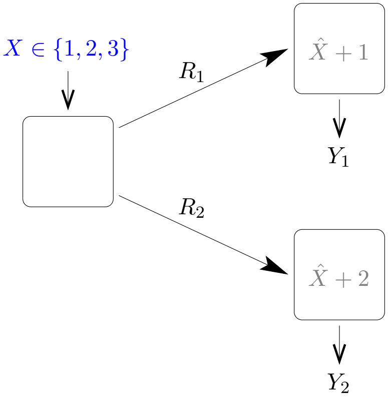
Three Node Network



Common message to both:
(similar to Berger-Zhang scheme for Multiple Descriptions)

$$\begin{aligned} R_1 &\geq I(X;U,Y_1), \\ R_2 &\geq I(X;U,Y_2), \\ R_1 + R_2 &\geq I(X;U,Y_1) + I(X;U,Y_2) + I(Y_1;Y_2|X,U). \end{aligned}$$

Three Node Network



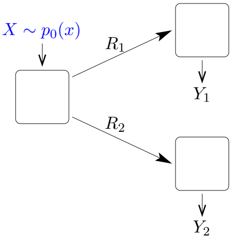
Rates for optimized common message quality $\hat{X}$.

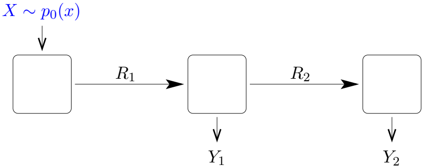
Communication rate with common message: $R_{ave} = \log 3 - \log \phi$.

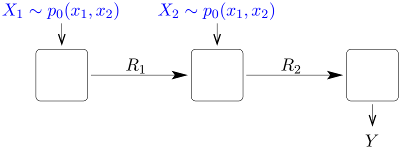
The golden ratio $\phi = \frac{\sqrt{5}+1}{2}$.

[Cuff, Permuter, Cover 09]

Three Node Networks



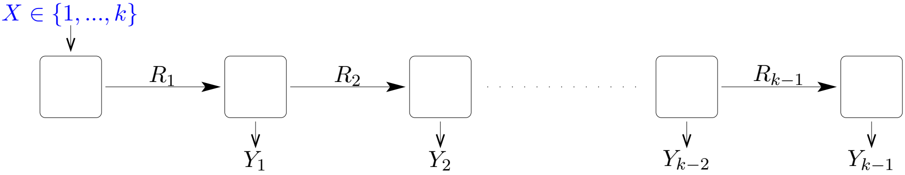




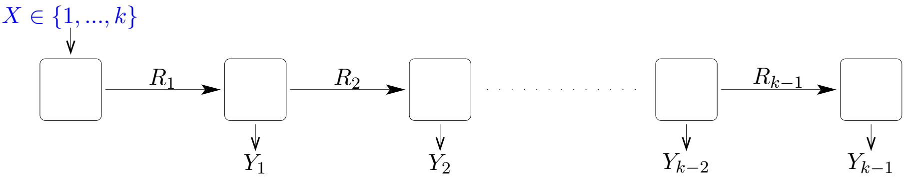
Each of these networks benefits from a common message.

Large Networks

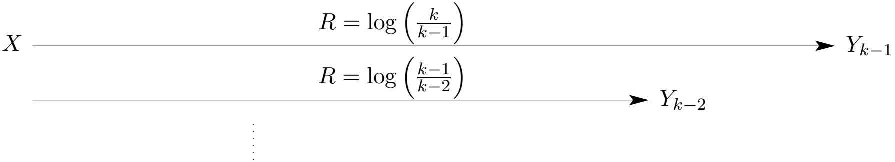
Cascade - One Assigned

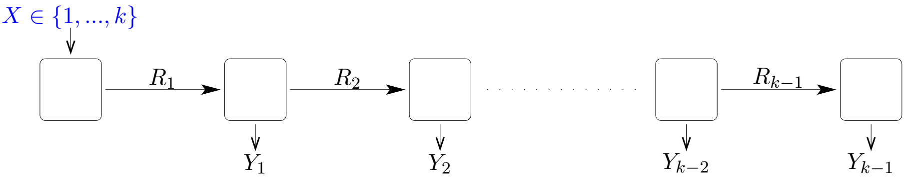


Cascade - One Assigned

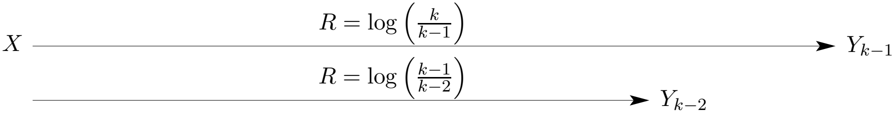


Optimal Communication:



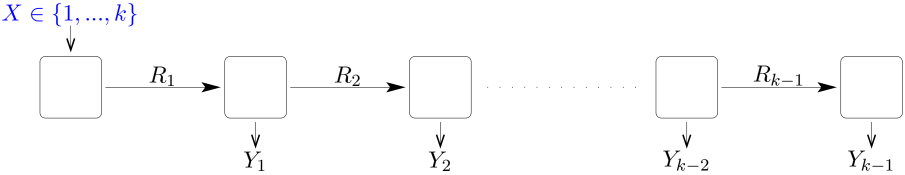


Optimal Communication:



$$
\begin{aligned}
R_{k-1} &= \log\left(\frac{k}{k-1}\right), \\
R_{k-2} &= \log\left(\frac{k}{k-1}\right) + \log\left(\frac{k-1}{k-2}\right) = \log\left(\frac{k}{k-2}\right), \\
R_i &= \log\left(\frac{k}{i}\right).
\end{aligned}
$$

Cascade - One Assigned

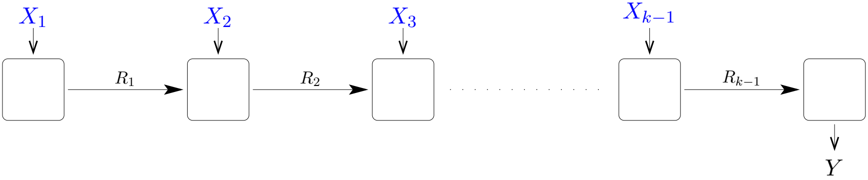


Sum rate:

$$
\begin{aligned}
R &= \sum_{i=1}^{k-1} \log\left(\frac{k}{i}\right) \\
&= k \log k - \sum_{i=1}^{k} \log i \\
&= k \log k - \log k! \\
&\approx k \log k - \log\left(\frac{k}{e}\right)^k \\
&= k \log e.
\end{aligned}
$$

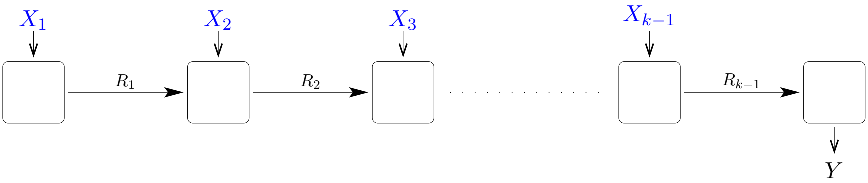
Linear in k

Cascade - All But One Assigned



X_i unique in $\{1, ..., k\}$ for all i.
Y must be the remaining task.

Cascade - All But One Assigned

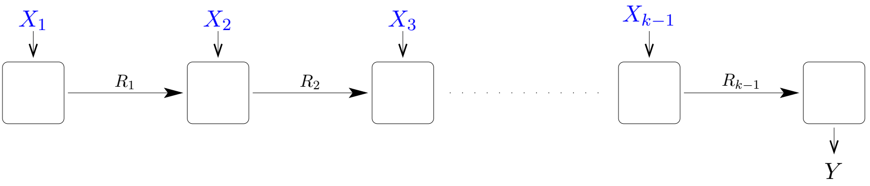


X_i unique in $\{1, ..., k\}$ for all i.
Y must be the remaining task.

Idea - Accumulate information:

$$\begin{aligned} R_1 &= \log(k-1), \\ R_2 &= \log(k-1) + \log(k-2) - \log 2, \\ R_i &= \log \binom{k-1}{i}. \end{aligned}$$

Cascade - All But One Assigned

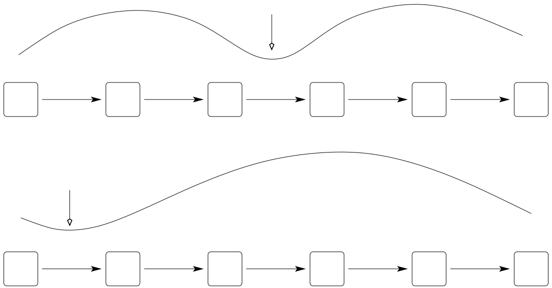


X_i unique in $\{1, ..., k\}$ for all i.
Y must be the remaining task.

Better Idea - Accumulate mod k sum: $\quad R_i < \log k$, for all i.

Sum rate: $\quad R < (k-1)\log k.$

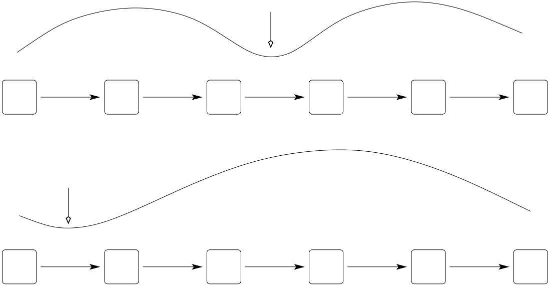
Cascade - Lower Bounds



$R_i \;\geq\; \log(i+1).$

Sum rate: $R \;=\; \sum_{i=1}^{k-1} R_i \;\gtrsim\; k \log \frac{k}{e}.$

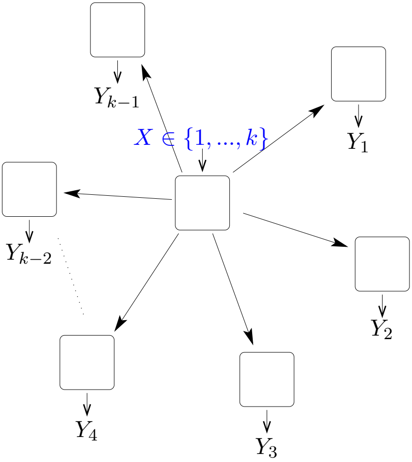
Cascade - Lower Bounds



$R_i \;\; \geq \;\; \log(i+1).$ Sum rate: $R \;\; = \;\; \sum_{i=1}^{k-1} R_i \;\; \geq\approx \;\; k \log \frac{k}{e}.$

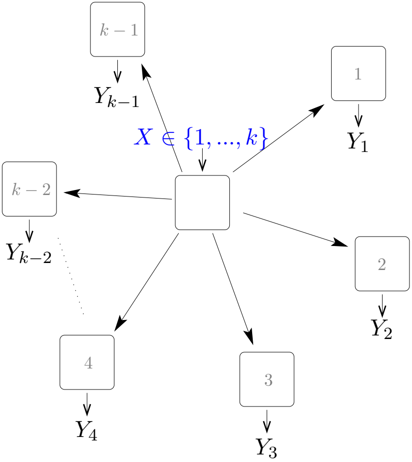
Upper and lower bounds both scale like $k \log k$.

Star Network



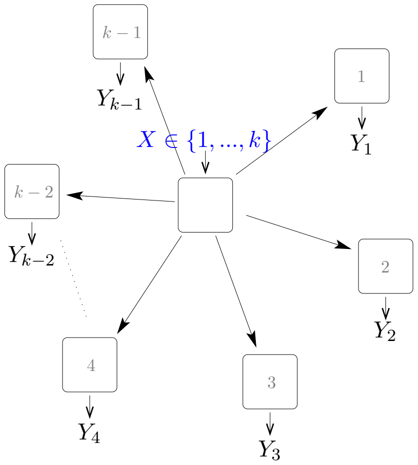
Try $R_i = \log \frac{k}{k-1}$ for all i. (Doesn't work)

Star Network



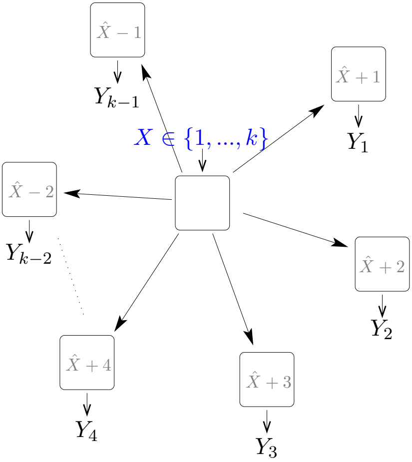
Assign Default Tasks: $R_i = h\left(\frac{1}{k}\right) \approx \frac{\log k}{k}$. Sum rate: $R \approx \log k + \log e$.

Star Network



Lower bound: $R \;\geq\; I(X; Y_1, ..., Y_{k-1}) \;=\; H(X) \;=\; \log k.$

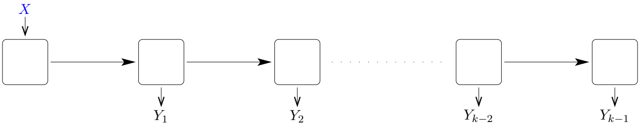
Star Network



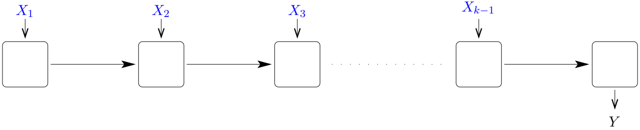
Two phase: Specify low-rate estimate $\hat{X}$. Choose defaults to exclude $\hat{X}$.

Task Assignment Summary

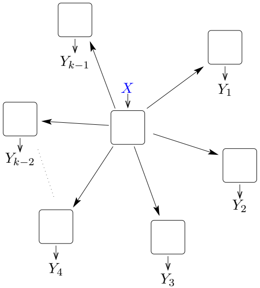
Sum rate:



$R_{min} \approx k \log e$ (linear)



$$R_{min} \approx k \log k.$$



$$R_{min} \approx \log k.$$

[Cuff, Permuter, Cover 09]

$\varsigma\upsilon\kappa\varrho\varepsilon\varsigma\upsilon$

Adversarial Settings

Coordination in the presence of an adversary engages with two frameworks:

1. Cryptography
2. Game Theory

Other work connecting these fields:

[Dodis, Halevi, Rabin 2000]

Game Theory

Payoff Matrix for a zero-sum game:

		Enemy 0	Enemy 1
Me $p(x)$	0	1	2
	1	3	-1

Game Theory

Payoff Matrix for a zero-sum game:

			Enemy	
			0	1
My team $p(x,y)$	00		1	2
	01		3	-1
	10		0	1
	11		-1	0

Team Action

Isolated Participants:

$$p(x)p(y)$$

Team Action

Isolated Participants:

$$p(x)p(y)$$

With Communication:

$$p(x, y)$$

To generate correlated actions $\sim p(x, y)$,

$R \geq I(X;Y)$ is required.

$$
\begin{aligned}
I(X;Y) &= H(X) + H(Y) - H(X,Y), \\
H(X) &= \mathbb{E} \log \frac{1}{p(X)}.
\end{aligned}
$$

To generate correlated actions $\sim p(x, y)$,

$R \geq I(X;Y)$ is required.

$$\begin{aligned} I(X;Y) &= H(X) + H(Y) - H(X,Y), \\ H(X) &= \mathbb{E} \log \frac{1}{p(X)}. \end{aligned}$$

This does not produce independent actions in the sequence.

To generate correlated actions $\sim p(x, y)$,

$R \geq I(X;Y)$ is required.

$$
\begin{aligned}
I(X;Y) &= H(X) + H(Y) - H(X,Y), \\
H(X) &= \mathbb{E} \log \frac{1}{p(X)}.
\end{aligned}
$$

This does not produce independent actions in the sequence.

What is the price of independence?

Billy and the Bully

Billy hopes to avoid the Bully:

Billy, $P(\text{home}) = 3/4$ \ Bully	out	home
home	1	0
out	0	3

Billy and the Bully

Billy hopes to avoid the Bully:

Bully

Billy

$P(\text{home}) = 3/4$

	out	home
home	1	0
0	0	3
1	0	0

If friends go to hangout 0, Billy gets no enjoyment by going to 1.
How much information about hangout choice do friends need to give?

Erasure Challenge

Person A

0 1 0 0 1 1 1 1

Erasure Challenge

Person A	Person B
0 1 0 0 1 1 1 1	0 e e e e 1 e e

Erasure Challenge

Person A	Person B
0 1 0 0 1 1 1 1	0 e e e e 1 e e

How much must Person A tell Person B?

Erasure Challenge

Person A								Person B							
0	1	0	0	1	1	1	1	0	e	e	e	e	1	e	e

How much must Person A tell Person B?

- Tell all the bits
  8 bits

Erasure Challenge

Person A

0 1 0 0 1 1 1 1

Person B

0 e e e e 1 e e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits

Erasure Challenge

Person A

0 1 0 0 1 1 1 1

Person B

0 e e e e 1 e e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits

Erasure Challenge

Person A

0 1	0 0	1 1	1 1

Person B

0 e e e e 1 e e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits
- Split the randomization

Erasure Challenge

Person A							
0	1	0	0	1	1	1	1

Person B

0 e e e e 1 e e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits
- Split the randomization

Erasure Challenge

Person A							
0	1	0	0	1	1	1	1

Person B							
0	1	e	e	1	1	e	e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits
- Split the randomization

Erasure Challenge

Person A							
0	1	0	0	1	1	1	1

Person B							
0	e	e	e	e	1	e	e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits
- Split the randomization

Erasure Challenge

Person A							
0	1	0	0	1	1	1	1

Person B							
0	e	e	e	e	1	e	e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits
- Split the randomization
  $\log_2 \binom{4}{2} + 4$ bits

Erasure Challenge

Person A

0	1	0	0	1	1	1	1

Person B

0	e	e	e	e	1	e	e

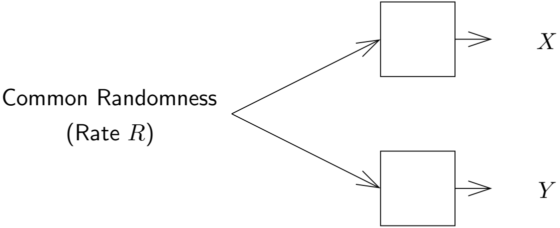
How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  $\log_2 \binom{8}{2} + 2$ bits $= \log_2 112 = 6.81$ bits
- Split the randomization
  $\log_2 \binom{4}{2} + 4$ bits $= \log_2 96 = 6.58$ bits

Wyner's Common Information

[Wyner 75]: $$C(X;Y) \triangleq \min_{X-U-Y} I(X,Y;U).$$

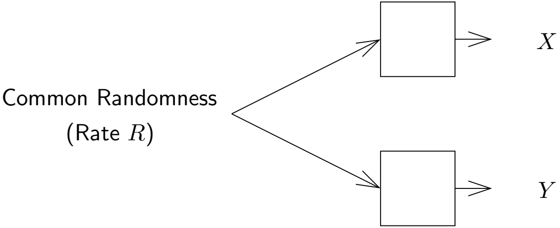
Amount of common randomness needed to generate X and Y?



Wyner's Common Information

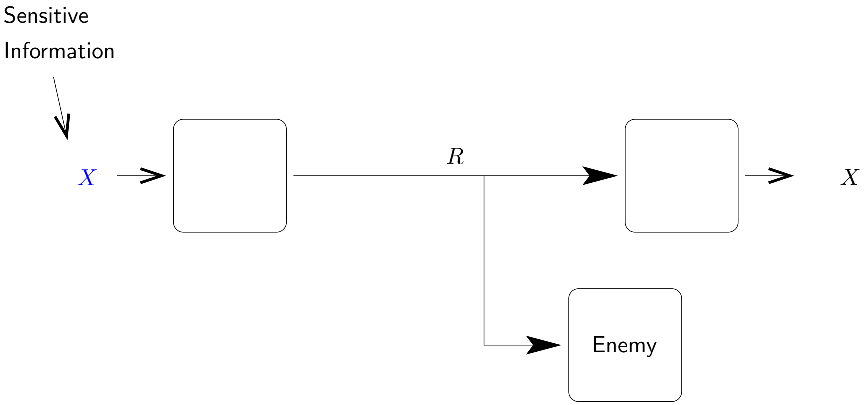
[Wyner 75]: $$C(X;Y) \triangleq \min_{X-U-Y} I(X,Y;U).$$

Amount of common randomness needed to generate X and Y?

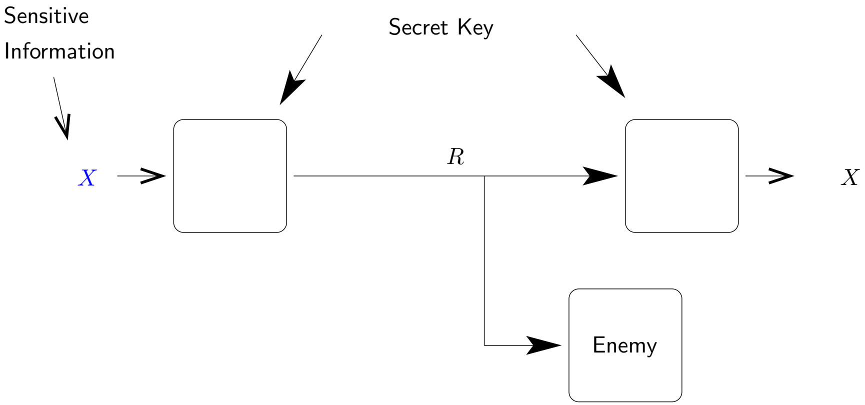


[Cuff 08]: Best use of common randomness in repeated zero-sum game.

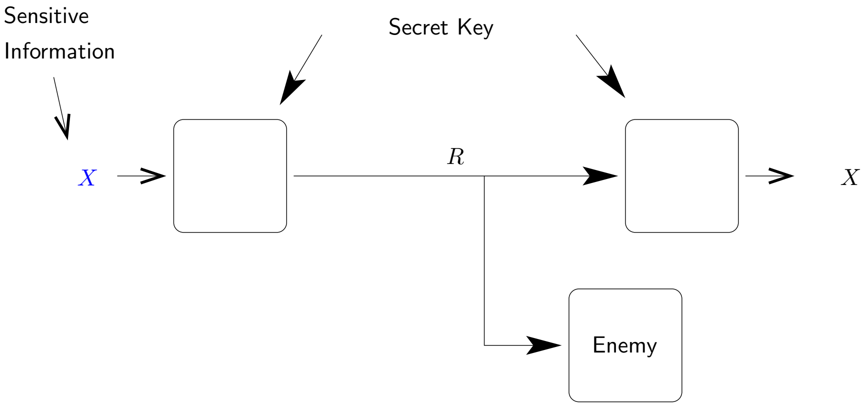
Encryption



Encryption



Encryption



$$R_1 = R_2 = H(X).$$ [Shannon 45]

One-time Pad

Message:

01011011101

Secret Key (random):

11100101101

One-time Pad

Message:

$$01011011101$$

Secret Key (random):

$$11100101101$$

$\bigoplus$

Transmission:

$$10111110000$$

One-time Pad

Message:

01011011101

Secret Key (random):

11100101101

$\oplus$

Transmission:

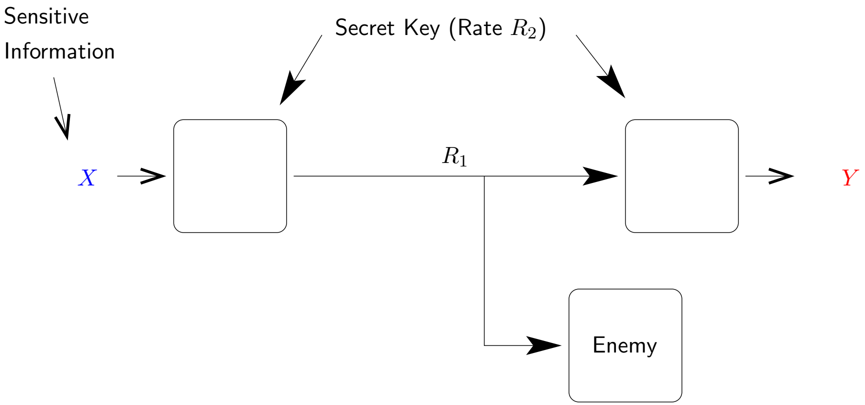
10111110000

$\oplus$

Decoded Message:

01011011101

Correlation Encryption

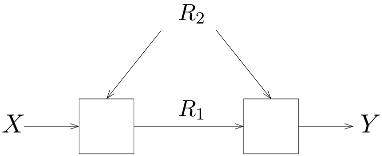


Goals:

1. Y correlated with X according to desired $p(y|x)$.
2. Enemy knows nothing about X or Y.

Correlation Encryption Rate Region

$$S \triangleq Cl\{\text{ encryption achievable } (R_1, R_2)\}$$



Theorem: Encryption Rate Region

$S = \{(R_1, R_2)$:

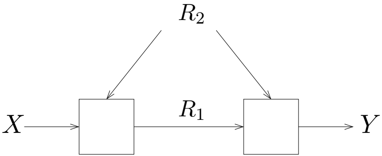
$$\begin{aligned} R_1 &\geq I(X;U), \\ R_2 &\geq I(X,Y;U), \end{aligned}$$

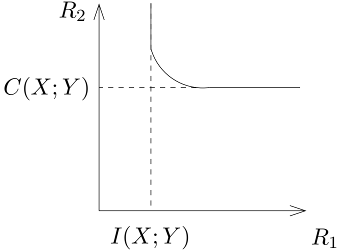
for some U such that $X - U - Y$ forms a Markov chain and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1.\}$

[Cuff 08]

Correlation Encryption Rate Region

$$S \triangleq Cl\{\text{ encryption achievable } (R_1, R_2)\}$$





Theorem: Encryption Rate Region

$S = \{(R_1, R_2)$:

$$\begin{aligned} R_1 &\geq I(X;U), \\ R_2 &\geq I(X,Y;U), \end{aligned}$$

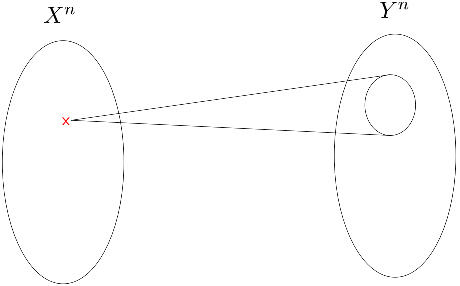
for some U such that $X - U - Y$ forms a Markov chain and $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 1.\}$

[Cuff 08]

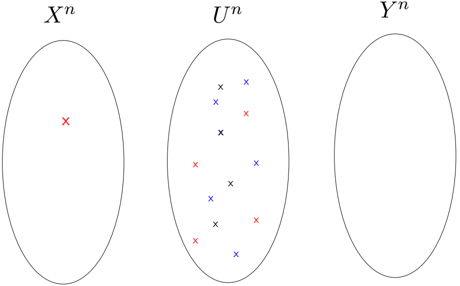
Achievability

Achievability

Achievability

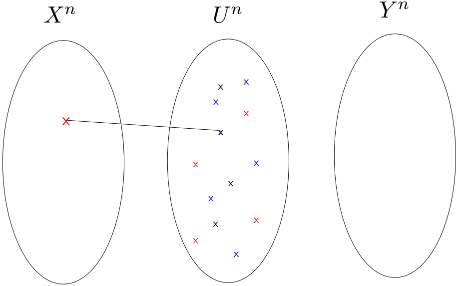


Achievability



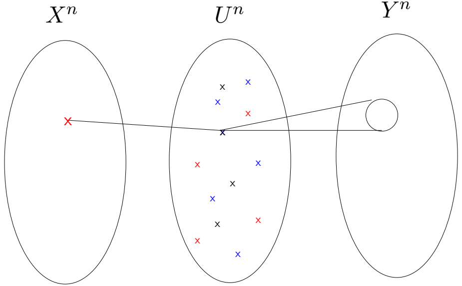
- Generate many codebooks of u^n sequences $\sim \prod_{i=1}^{n} p(u_i)$.
- The secret key specifies the codebook to use.

Achievability



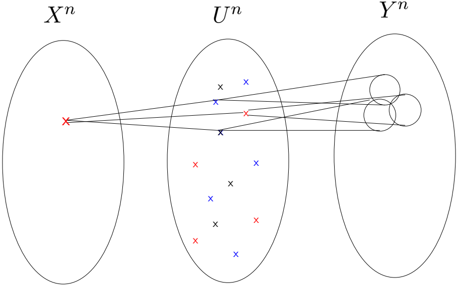
- Generate many codebooks of u^n sequences $\sim \prod_{i=1}^{n} p(u_i)$.
- The secret key specifies the codebook to use.
- Encoder finds a u^n sequence correlated with x^n and sends the index i.

Achievability



- Generate many codebooks of u^n sequences $\sim \prod_{i=1}^{n} p(u_i)$.
- The secret key specifies the codebook to use.
- Encoder finds a u^n sequence correlated with x^n and sends the index i.
- Decoder generates y^n randomly conditioned on $u^n(i)$.

Achievability



$$
\begin{aligned}
R_1 &\geq I(X;U), \\
R_2 &\geq I(X;U) + {\color{red} I(U;Y|X)}.
\end{aligned}
$$

Resolvability: [Wyner 75] [Han, Verdú 93]

Converse

M is the message.
W is the secret key.

$$
\begin{aligned}
nR_1 &\geq H(M) \\
&\geq H(M|W) \\
&\geq I(X^n; M|W) \\
&\geq I(X^n; M, W) \ldots
\end{aligned}
$$

Converse

M is the message.
W is the secret key.

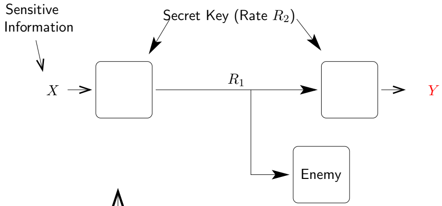
$$\begin{aligned} nR_1 &\geq H(M) \\ &\geq H(M|W) \\ &\geq I(X^n;M|W) \\ &\geq I(X^n;M,W)... \end{aligned}$$

$$\begin{aligned} nR_2 &= H(W) \\ &\geq H(W|M) \\ &\geq H(X^n,Y^n;W|M) \\ &= I(X^n,Y^n;W,M) - I(X^n,Y^n;M)... \end{aligned}$$

Example

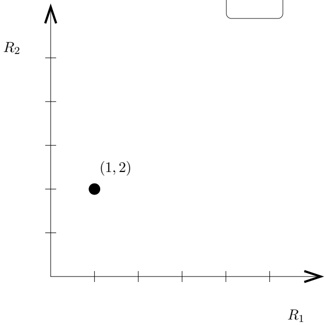
Task assignment in an adversarial setting.

System Monitor



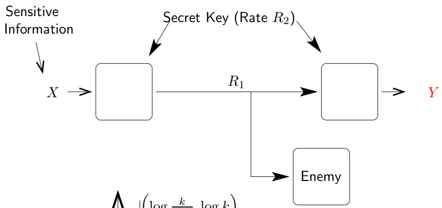
$X \sim Unif\{1, ..., k\}$.

Y needs to be different from X and **random among the choices**.



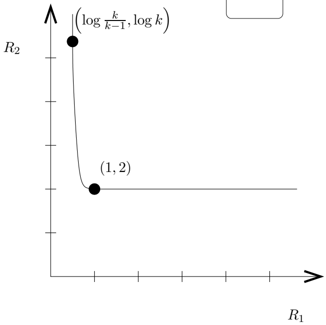
Task assignment in an adversarial setting.

System Monitor



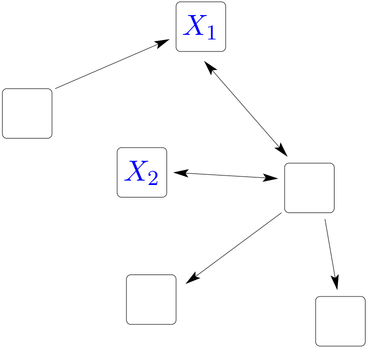
$X \sim Unif\{1, ..., k\}$.

Y needs to be different from X and **random among the choices**.



Recap

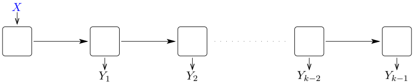
Network of nodes with communication:

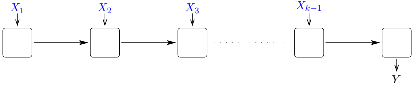


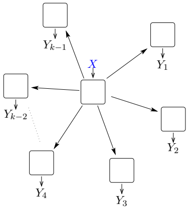
Observations:

- Tools: Random coding, auxiliary variables, common randomness.
- Different networks require very different techniques.

Non-adversarial:







Adversarial:

Two Nodes:

- Secret key required
- Tradeoff between communication and secret key
- Game theory perspective

Fundamental Limits:

- Communication: $R_1 > I(X;Y)$.
- Secret key: $R_2 > C(X;Y)$.

Acknowledgments

M W V P U E C R L I A P O B N H D S A G V S Y A R K E M I O A S R Y N L A W

Acknowledgments

M W V P U E C R L I A P O B N H D S A G V S Y A R K E M I O A S R Y N L A W

Acknowledgments

M W V P U E C R L I A P O B N H D S A G V S Y A R K E M I O A S R Y N L A W

Acknowledgments

M W V P U E C R L I A P O B N H D S A G V S Y A R K E M I O A S R Y N L A W

Acknowledgments

M W V P U E C R L I A P O B N H D S A G V S Y A R K E M I O A S R Y N L A W

Acknowledgments

M W V P U E C R L I A P O B N H D S A G V S Y A R K E M I O A S R Y N L A W

Acknowledgments

M W V P U E C R L I A P O B N H D S A G V S Y A R K E M I O A S R Y N L A W

Acknowledgments

M W V P U E C R L I A P O B N H D S A G V S Y A R K E M I O A S R Y N L A W

Acknowledgments

M W V P U E C R L I A P O B N H D S A G V S Y A R K E M I O A S R Y N L A W

Acknowledgments

M W V P U E C R L I A P O B N H D S A G V S Y A R K E M I O A S R Y N L A W

Acknowledgments

M W V P U E C R L I A P O B N H D S A G V S Y A R K E M I O A S R Y N L A W

And many more!

Acknowledgments

S J D Q P O E W N Z M X C N Z H B A H G J A K S D F X P I U C I O P U Q R E
T Y Q W J R H X C M N B C V H A V B C N Z M X M Q P W E O I R E Y W O Z X
C V N B C M L A S D F K G J H Y S T E U Q S J D Q P O E W N Z M X C N Z J D
Q P O E W N Z M X C N Z H B A H G J A K S D F X P I U C I O P U Q R E T Y Q
W J R H X C M N B C V H A V B C N Z M X M Q P W E O I R E Y W O Z X C V N
B C M L A S D F K G J H Y S T E U Q S J D Q P O E W N Z M X C N Z J D Q P O
E W N Z M X C N Z H B A H G J A K S D F X P I U C I O P U Q R E T Y Q W J R
H X C M N B C V H A V B C N Z M X M Q P W E O I R E Y W O Z X C V N B C M
L A S D F K G J H Y S T E U Q S J D Q P O E W N Z M X C N Z