Chaos synchronization of networks with time-delayed couplings

Wolfgang Kinzel

Theoretische Physik, Universität Würzburg

November 2010

Content

- Chaos synchronization with time-delayed couplings
- Semiconductor lasers
- Secure communication
- Analytic results for arbitrary networks,
  master stability function

Coauthors

Uni Würzburg: Anja Englert, Florian Geissler, Sven Heiligenthal, Martin Paulig, WK

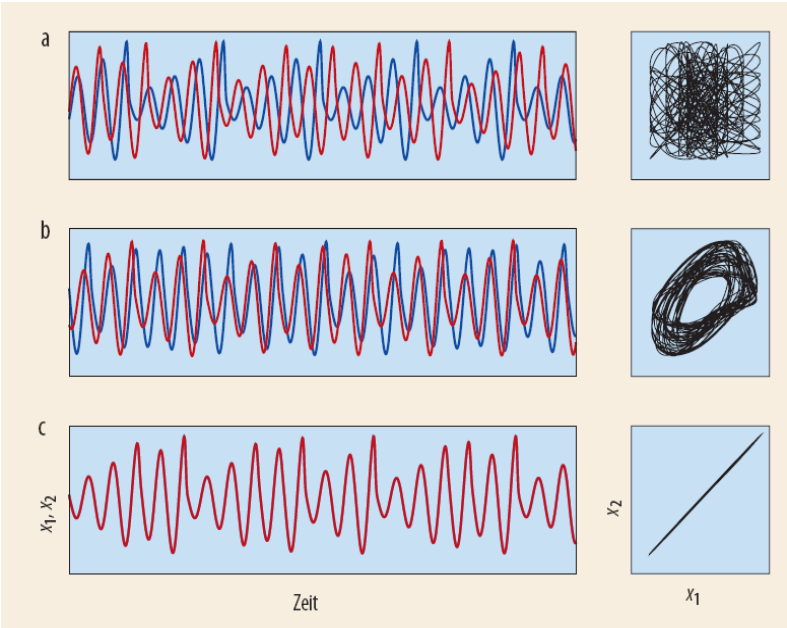
Bar Ilan Uni: Meital Zigzag, Evi Kopelowitz, Ido Kanter, Michael Rosenbluh

Pikovsky 1984, Pecora Carroll 1990:

Chaos synchronization

Two coupled Rössler units :

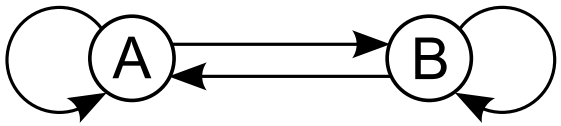
$$\dot{x}_1 = -y_1 - z_1 + k(x_2 - x_1)$$
$$\dot{y}_1 = x_1 + 0.15\, y_1$$
$$\dot{z}_1 = 0.4 + z_1\,(x_1 - 8.5)$$



Time-delayed couplings

Extension to time-delayed couplings:

- Complete synchronization without any time lag (zero lag synchronization)
- The chaotic trajectory is generated/modified by the network

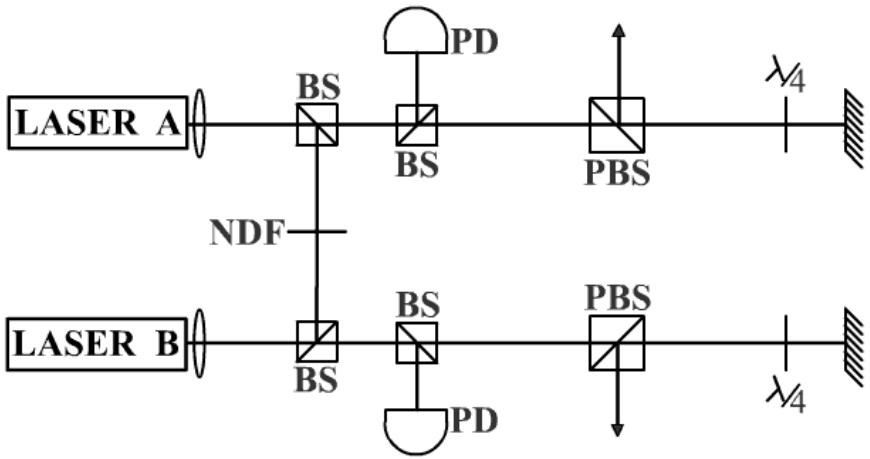


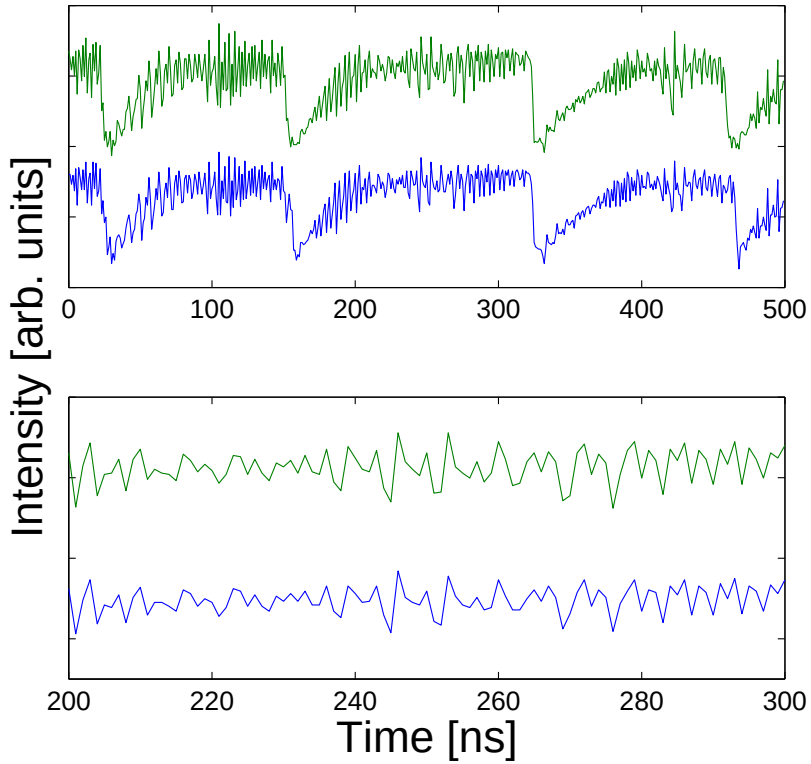
- Chaotic units are coupled by transmitting some of their variables over a long distance,

$$\dot{a}(t) = F\left[a(t), a(t-\tau_f), b(t-\tau_c)\right]$$
$$\dot{b}(t) = F\left[b(t), b(t-\tau_f), a(t-\tau_c)\right]$$

- The delay times are much larger than the internal local time scales Chaotic semiconductors (120 km), Neural networks (few cm)
- Complete synchronization without time lag is possible, $a(t) = b(t)$

Semiconductor lasers with feedback



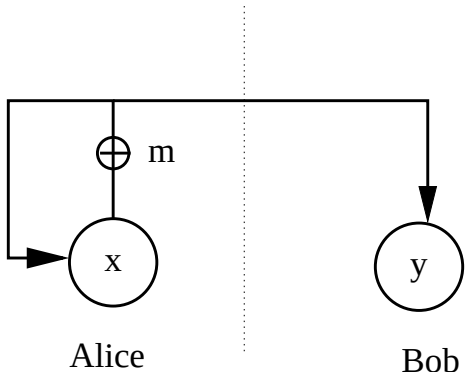


Possible applications: Secure communication over public channels

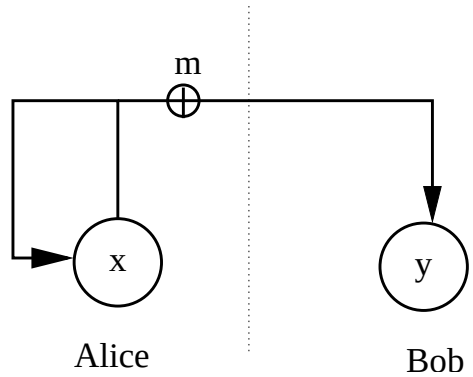
see PRL 2009

Transmission of a secure information

- Sending a tiny message m_t: $s_t = x_t + m_t$
- Recovering the message: $\tilde{m}_t = s_t - y_t$



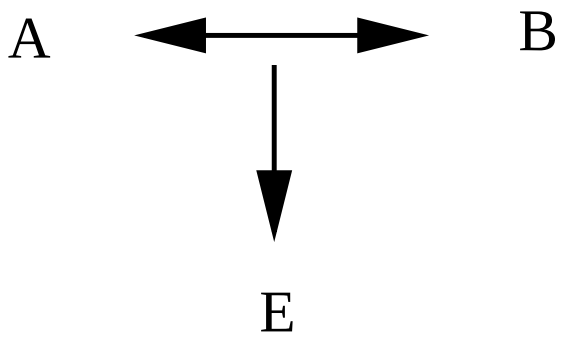
Chaos modulation,
error free transmission



Chaos masking,
chaos pass filter

Nature 2005:
Laser synchronization over 120 km, bit error rates 10^{-7}, Gbits per second

Public key exchange protocol



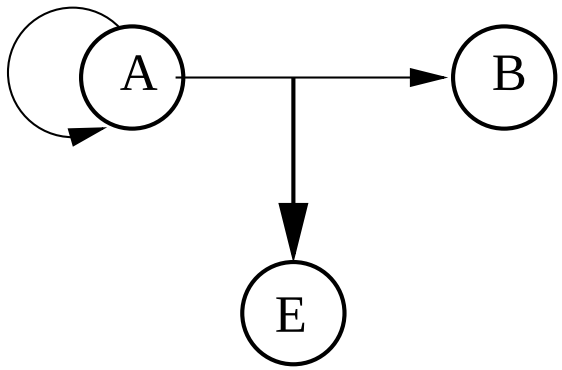
- Two partners A and B generate a common secret, without any previous secret contact.
- An attacker E, listening to the communication, knows everything what A knows about B. But she is not able to find the secret.

Is this possible?

Number theory: Diffie/Hellmann 1976, Rivest/Shamir/Adelman (RSA)

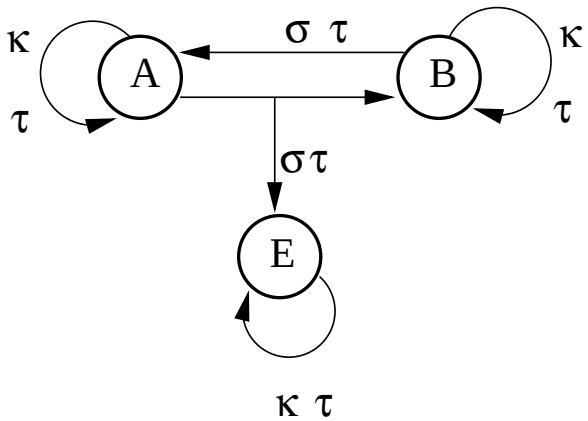
Public secret synchronization

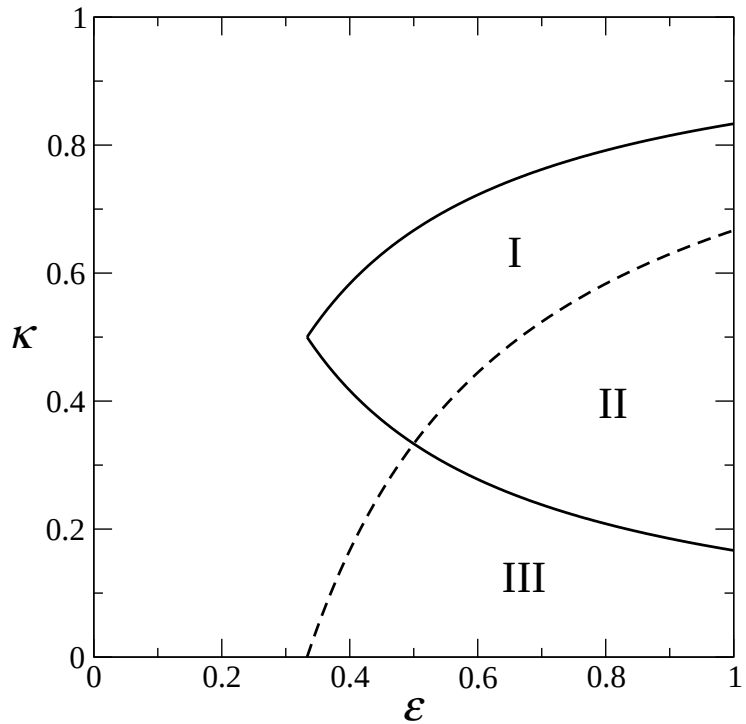
Can two chaotic units synchronize whereas a third unit which is recording all the exchanged signals cannot synchronize?
Master-slave:



No, if Eve knows the parameters of the two units.
Only private key cryptography is possible.

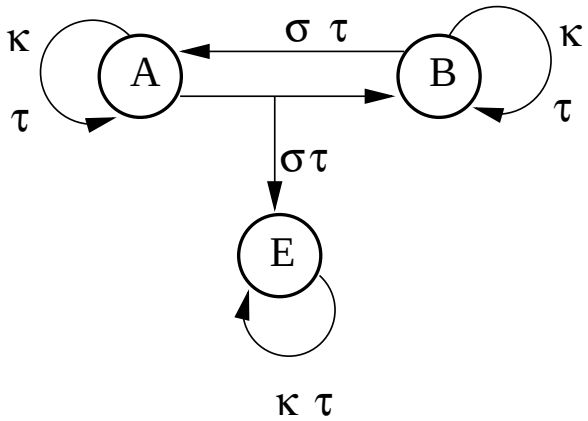
Is two-way more than one-way?

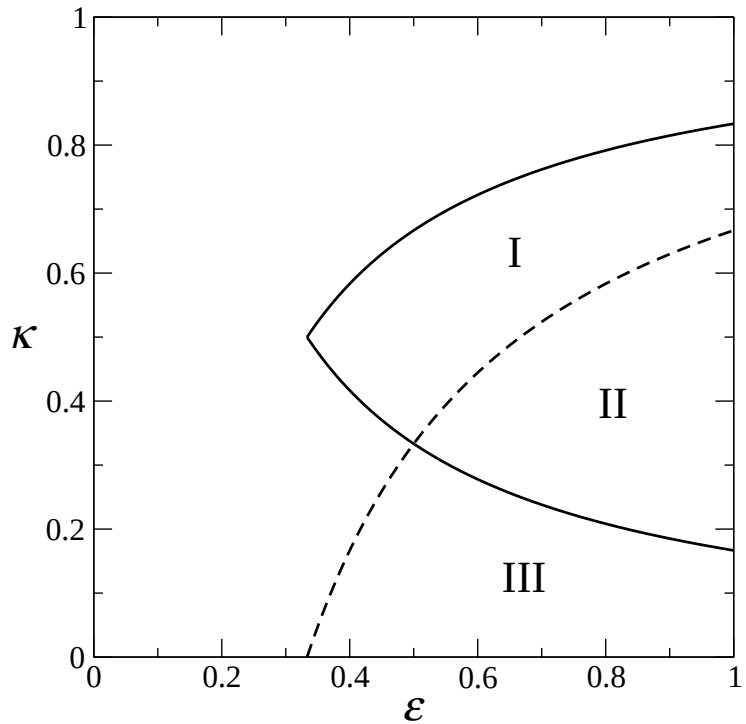




- Yes: Eve cannot synchronize if she has to use an identical system.

Is two-way more than one-way?

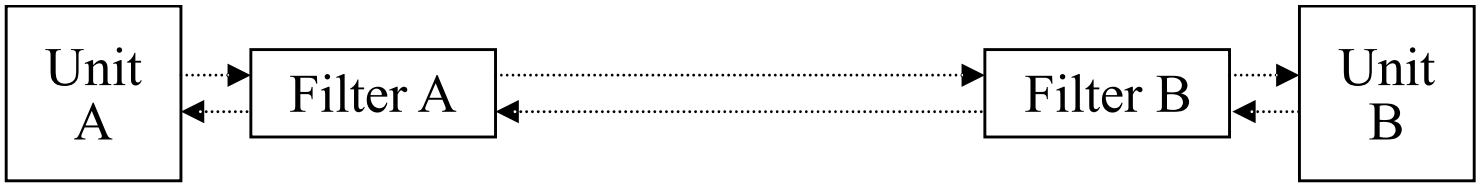




- Yes: Eve cannot synchronize if she has to use an identical system.
- No: Eve can synchronize if she can adjust her parameters

See, however, mutual chaos pass filter, Optics Express 2010

Commutative dynamic filters

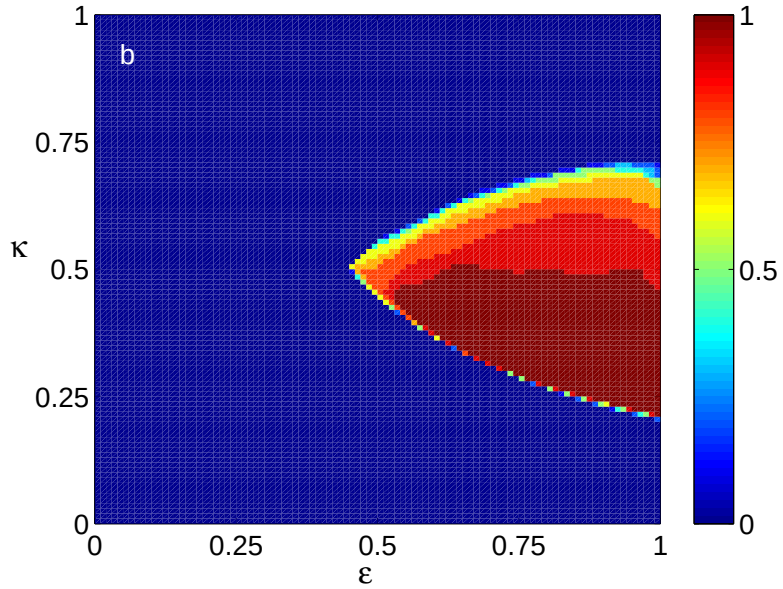


Algorithm:

- A and B use secret filters:

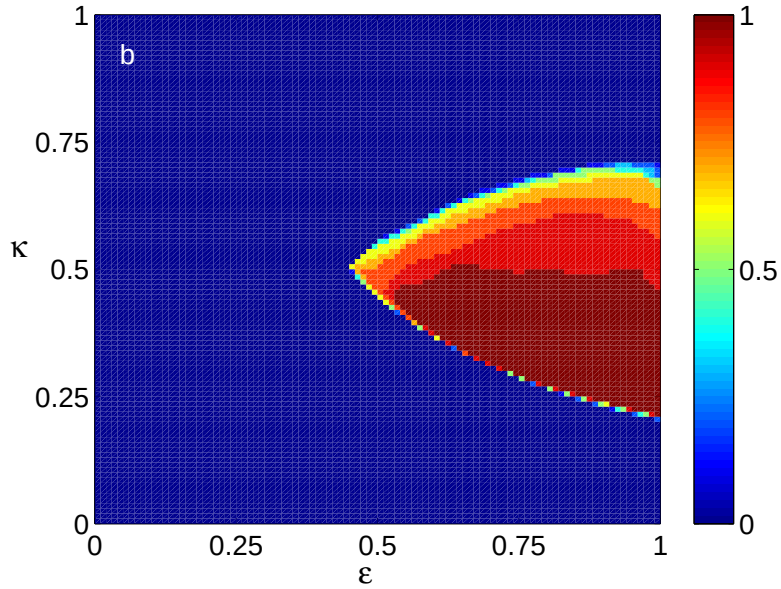
$$s_t = \sum_{k=0}^{N} K_k^A f(a_{t-k}), \quad d_t = \sum_{k=0}^{N} K_k^B f(s_{t-k})$$

- Filters are changed after some time
- Integer values and nonlinearities are used for transmission



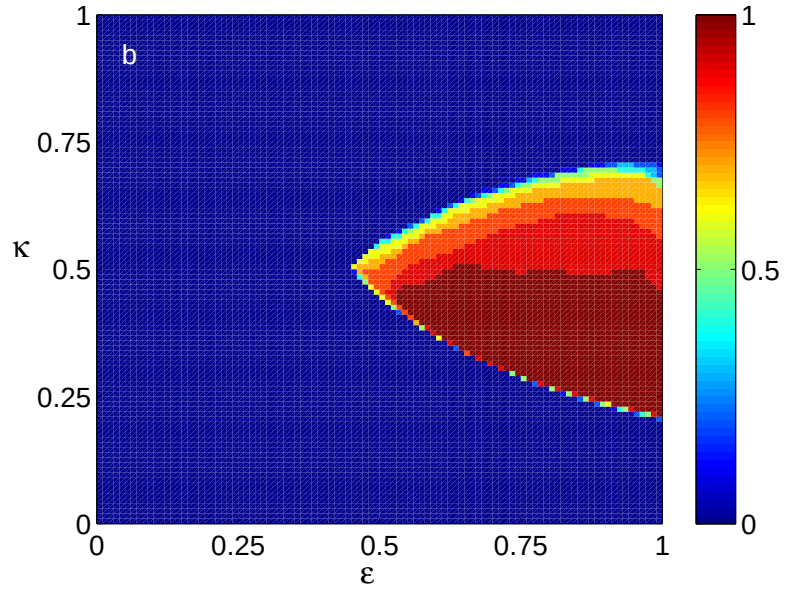
Probability to synchronize:

- Synchronization is possible



Probability to synchronize:

- Synchronization is possible
- A hardware attack is not possible
  E receives $F_A(a_t)$ and $F_B(b_t)$ but not $F_A(F_B(b_t))$



Probability to synchronize:

- Synchronization is possible
- A hardware attack is not possible
  E receives $F_A(a_t)$ and $F_B(b_t)$ but not $F_A(F_B(b_t))$
- A mathematical attack is improbable (NP complete)
- Two-way is more than one-way

Chaos synchronization in networks

Master stability function (Pecora Carroll):

For any network of identical units, the eigenvalues of the coupling matrix determine the stability of the synchronization manifold.

Example: Network of iterated Bernoulli maps, N units with $x_t \in [0,1]$, $f(x) = ax(\mathrm{mod}1)$, $\sum_k G_{j,k} = 1$

$$x_t^j = (1-\epsilon) f(x_{t-1}^j) + \epsilon \sum_k G_{jk} f(x_{t-\tau}^k)$$

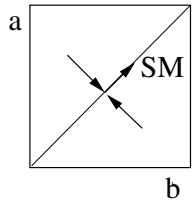
Stability of the synchronized chaotic trajectory against a perturbation belonging to an eigenvector of G with eigenvalue γ_k:

$$z^\tau = (1-\epsilon) a z^{\tau-1} + \epsilon a \gamma_k$$

For each mode γ_k one has a spectrum of τ Lyapunov exponents which are determined by the roots of this polynomial.

Perturbations of the synchronization manifold SM

$\gamma_0 = 1$: Perturbation parallel to SM determines chaos.
$\gamma_{k,k>0}$: Perturbation perpendicular to SM

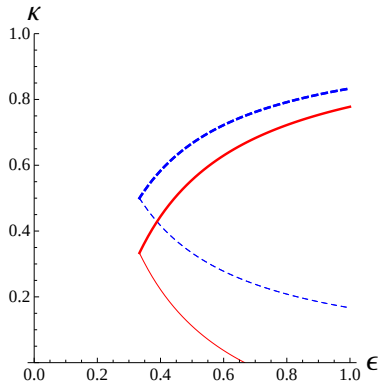


Bernoulli for $\tau \to \infty$:

SM is stable if $\gamma = \max_{k>0}|\gamma_k| < \exp(-\tau\lambda_{\max})$

The eigenvalue gap $1 - \gamma$ determines the region of synchronization. For $\gamma = 1$ synchronization is not possible. For $\gamma < 1$ and $\lambda_{\max} \to 0$, SM is stable.

Two units: $\gamma_1 = -1 \Rightarrow$ No synchronization
Triangle: $\gamma_{1,2} = -1/2 \Rightarrow$ Synchronization



Consequences

- Chaotic units cannot synchronize if the delay time of the coupling is much larger than the internal time scales

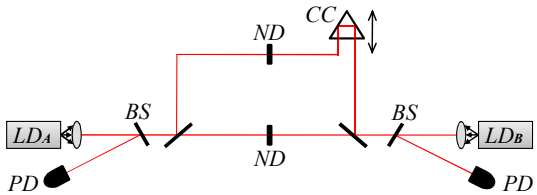
$$z = (1-\epsilon)az^{-1} + \epsilon a\gamma_k z^{-\tau}$$

But: The chaotic trajectory of the network may drive the the local unit non-chaotic.

- Bipartite networks without self-feedback cannot synchronize, since $\gamma = 1$.
- Couplings with multi-delays may synchronize, depending on the ratio of delay times
- Two chaotic networks can synchronize with few couplings
- Complete synchronization of directed graphs
- Classification of general networks by stochastic matrices and loop relations

Symmetries

Pair coupled by two delay times without feedback



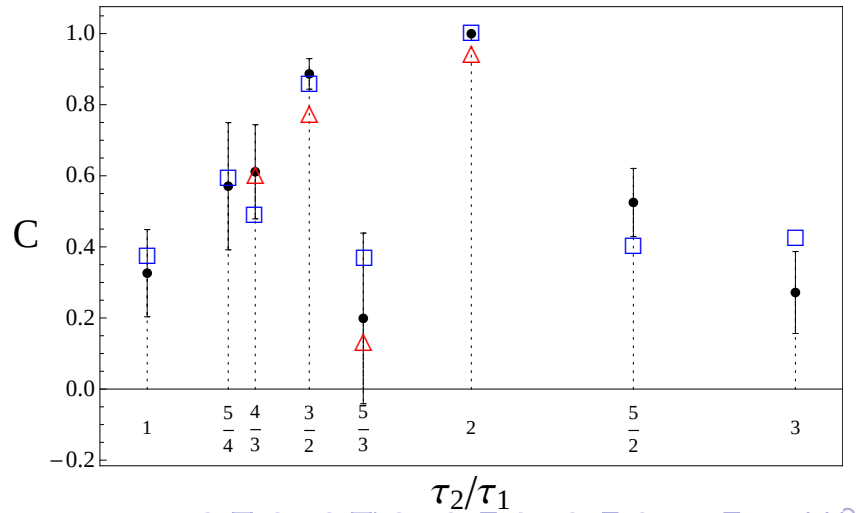
Bernoulli: $z^{\tau_2} = \sigma_0 z^{\tau_2 - 1} + \sigma_1 \gamma_k z^{\tau_2 - \tau_1} + \sigma_2 \gamma_k$

Symmetry $\tilde{z} = -z^n$. For $\gamma_1 = -1$ one finds:

If $\tau_2/\tau_1 = p/q$ with p, q relatively prime and both odd, synchronization is not possible.

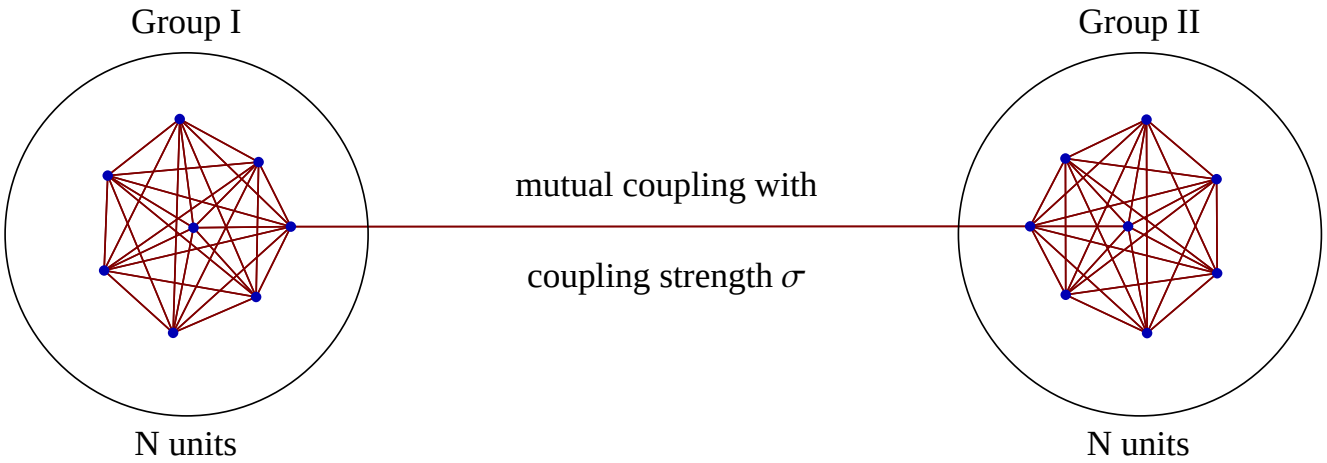
Experiment on two semiconductor lasers:

see: PRL 2010

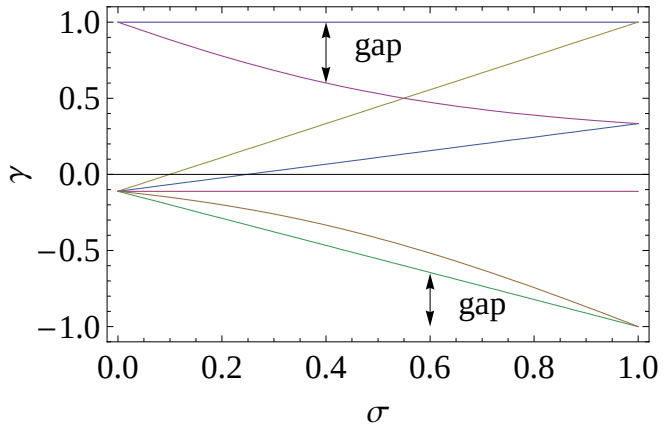


Two chaotic networks

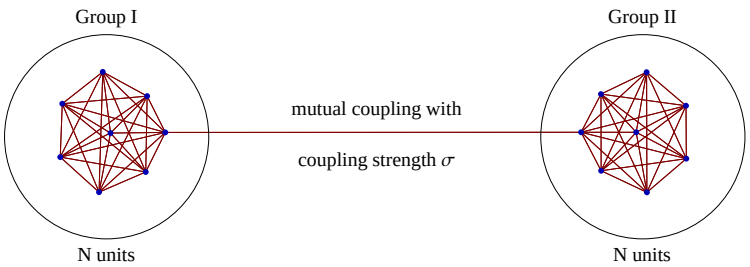
Can two chaotic networks be synchronized by a few couplings?

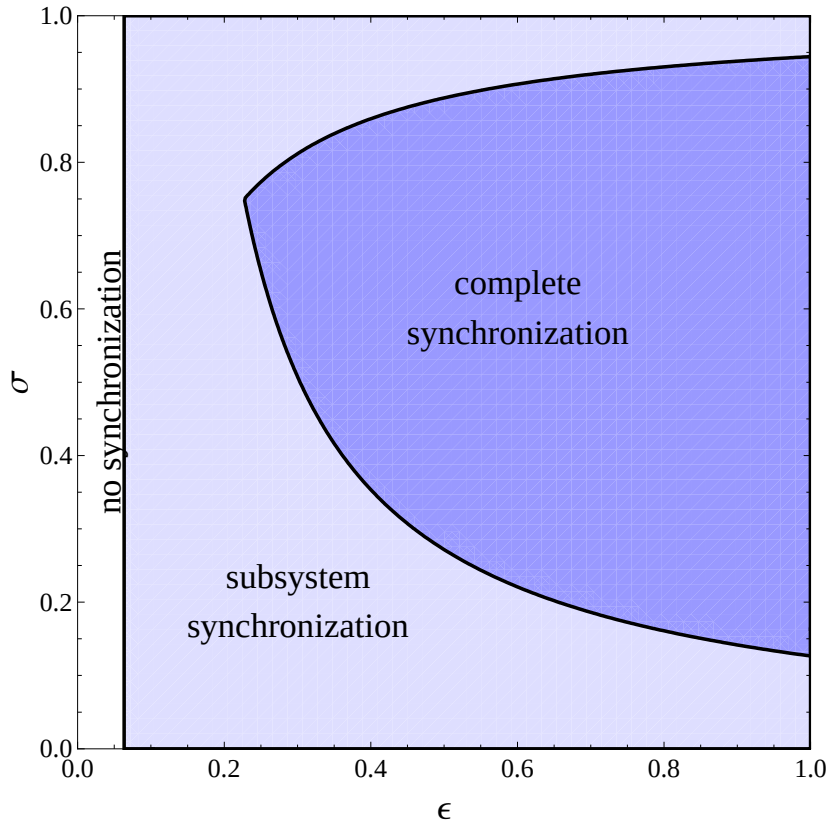


Result for a single bond:
Yes, if N is finite.
Result for αN bonds:
Yes, for $N \longrightarrow \infty$.



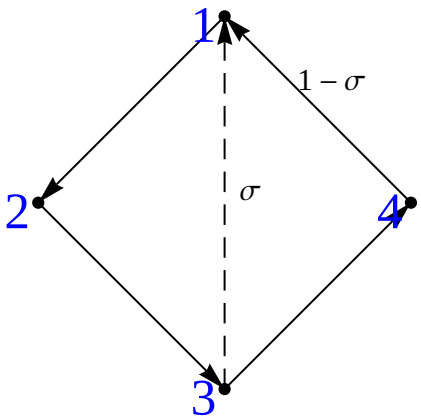
Phase diagram for finite N

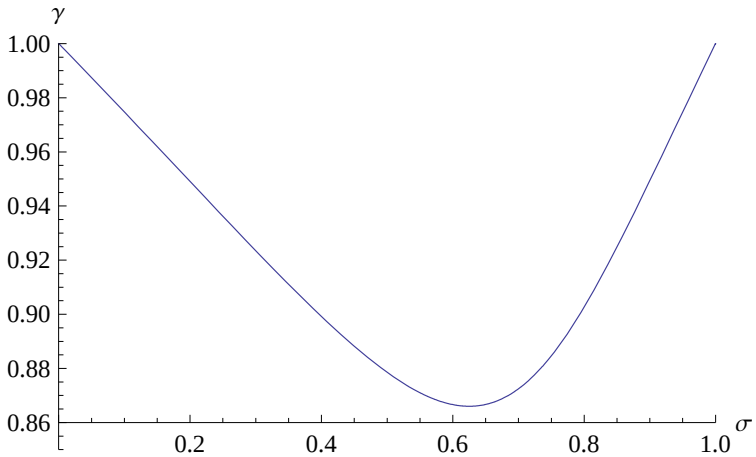


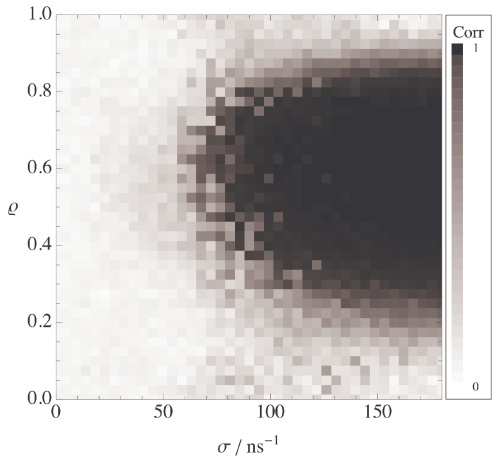


Oriented graph

For a ring: $\gamma_k = \exp ik\pi \Rightarrow$ No synchronization
Ring with additional shortcut:



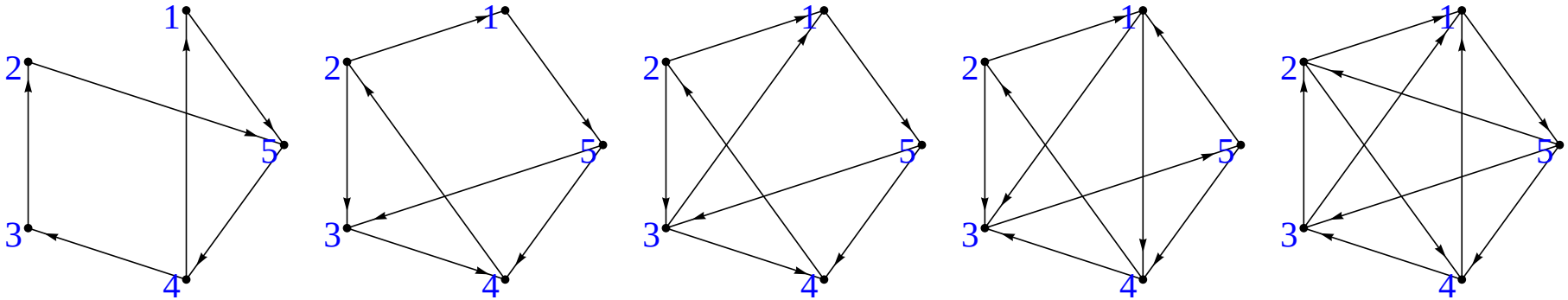




Networks with delayed directed couplings can synchronize without time shift

Optimal oriented graphs

X couplings, 2^X configurations, 2^X values γ,
minimal γ-value gives largest region of synchronization

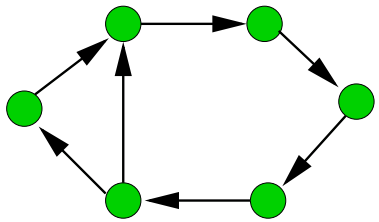


Minimal γ: $0.87,\ 1/\sqrt{2} \simeq 0.707,\ 1/\sqrt{2},\ 0.651,\ 1/\sqrt{2}$

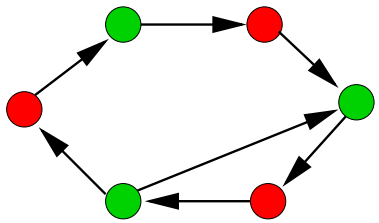
General graphs

Relation to stochastic matrices, ergodic Markov chains:

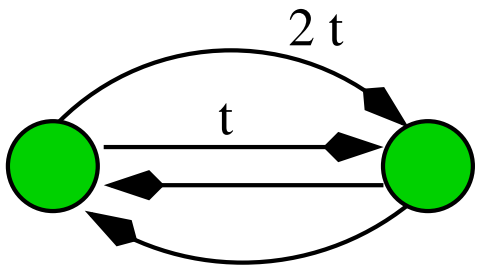
GCD(Two loops) $= 1 \Rightarrow$ Synchronization

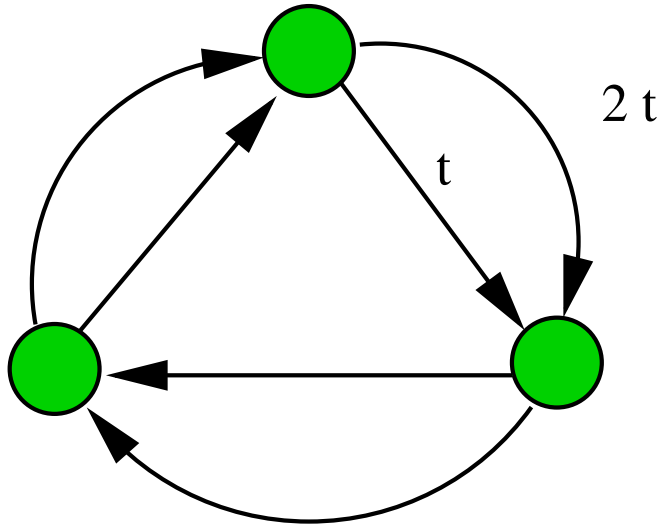


GCD(All loops) $= m \Rightarrow$ Sublattice synchronization



Graphs with multi-delay





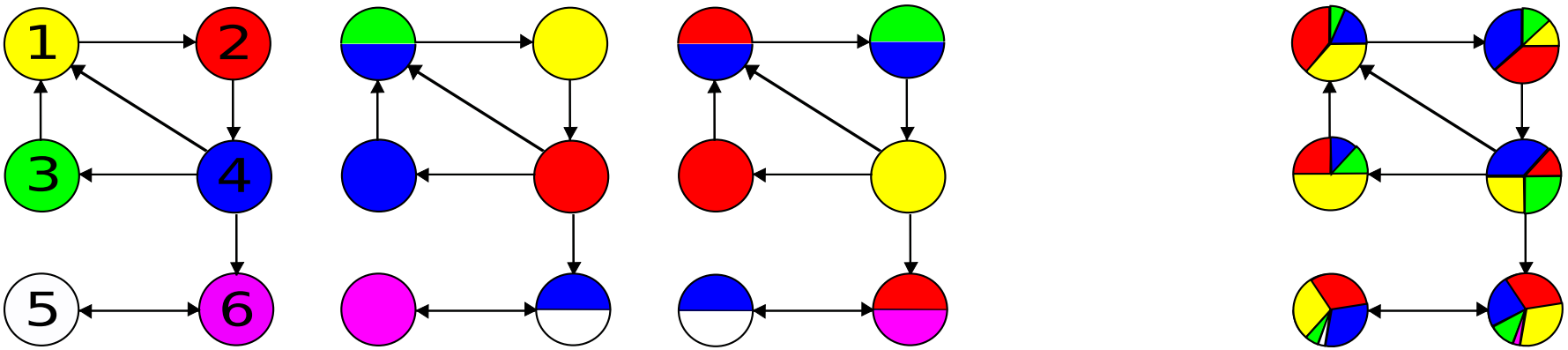
GCD(2,3)=1, GCD(3,4)=1 $\Rightarrow$ Synchronization

General principle: Mixing of information

Mixing information

Synchronization is possible only if the information on the trajectories of all units are mixed together after integer multiples of τ.
Method:

- Color all units with a different color
- Distribute and mix colors according to the links
- If all colors are mixed, synchronization is possible



Conclusion

- Chaotic networks with time-delayed couplings can synchronize without time shift, zero lag synchronization
- Chaos synchronization with bi-directional couplings may be a novel method of public channel cryptography
- If the delay time is large, the eigenvalue gap of the coupling matrix determines synchronization
- Multiple delay times with special ratios enable synchronization, the ratio is given by symmetry
- Two chaotic subnetworks can synchronize with a single bond
- Oriented networks can synchronize
- Complete synchronization with GCD(two loops)=1, sublattice synchronization (clustering) with GCD(all loops)=m