Peer-to-Peer-Netzwerke

Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Christian Schindelhauer

Sommersemester 2006

19. Vorlesung

12.07.2006

schindel@informatik.uni-freiburg.de

III. Zufallsgraphen
C. Regulär, Gerichtet

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Peter Mahlmann, Christian Schindelhauer, *Distributed Random Digraph Transformations for Peer-to-Peer Networks*, erscheint auf 18th ACM Symposium on Parallelism in Algorithms and Architectures, Cambridge, MA, USA. July 30 - August 2, 2006**

Gerichtete Graphen

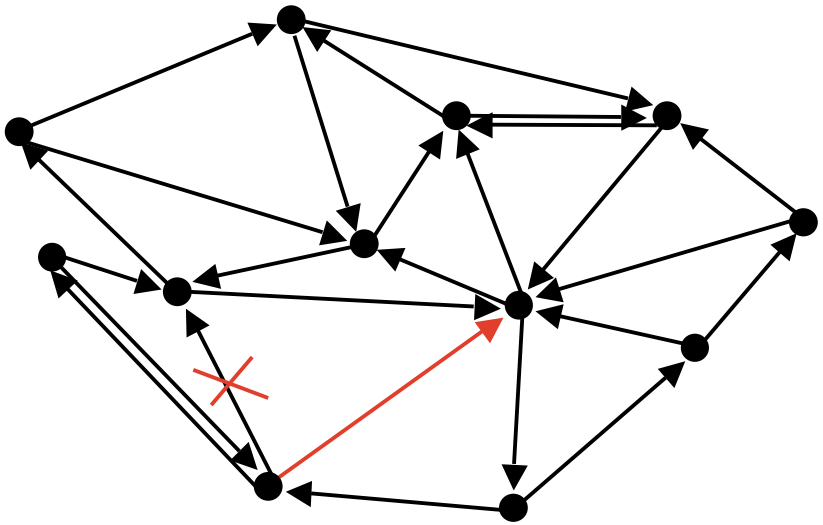
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

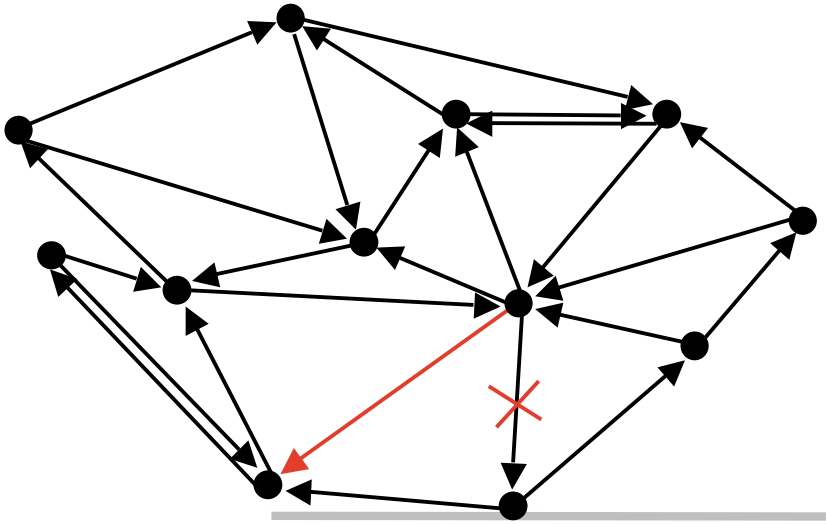
Push Operation:

1. Choose random node *u*
2. Set *v* to *u*
3. While a random event with p= 1/*h* appears
   a) Choose random edge starting at *v* and ending at *v‘*
   b) Set *v* to *v‘*
4. Insert edge (*v*,*v‘*)
5. Remove random edge starting at *v*

Pull Operation:

1. Choose random node *u*
2. Set *v* to *u*
3. While a random event with p= 1/*h* appears
   a) Choose random edge starting at *v* and ending at *v‘*
   b) Set *v* to *v‘*
4. Insert edge (*v‘*,*v*)
5. Remove random edge starting at *v‘*





Simulation der Push-Operation

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

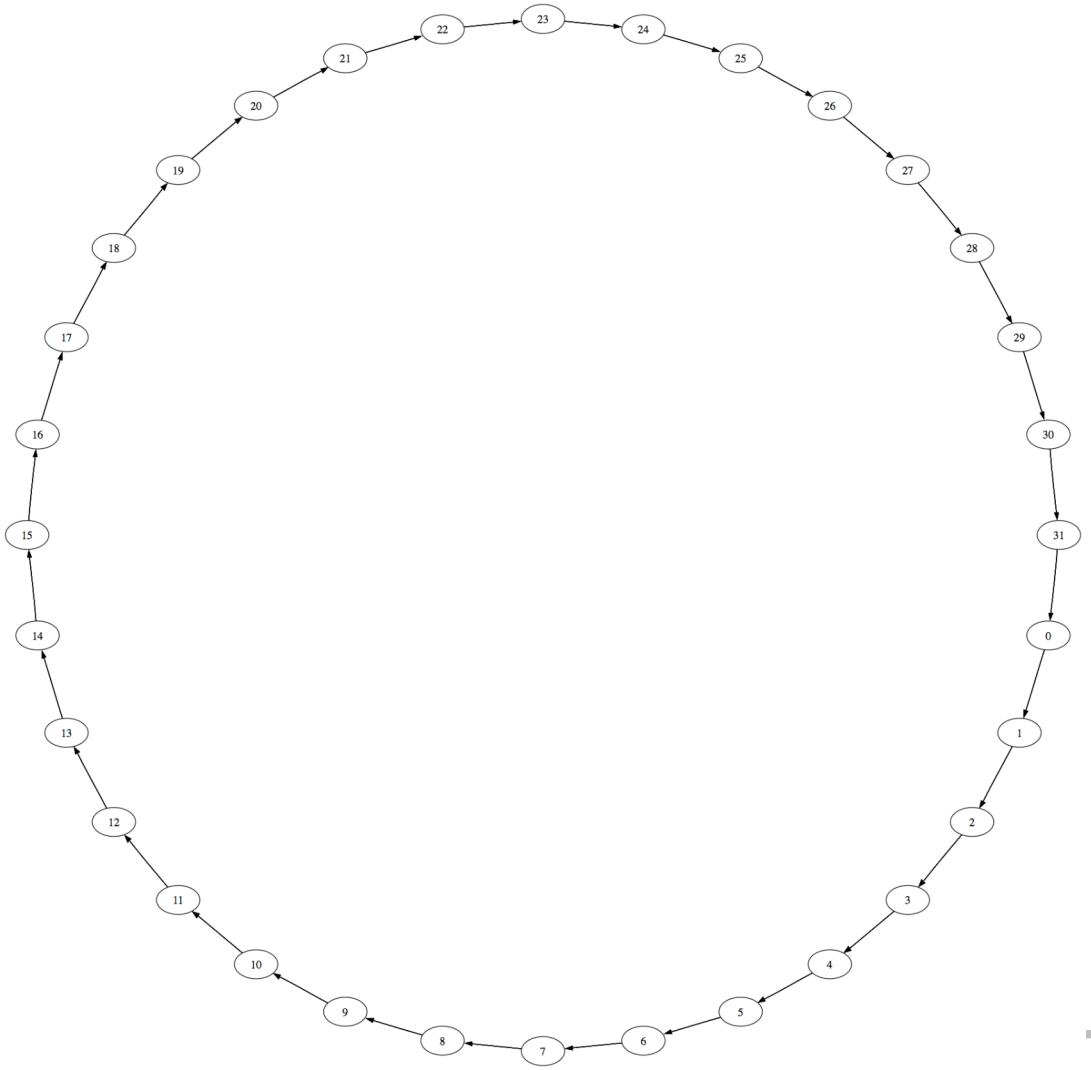
Startsituation

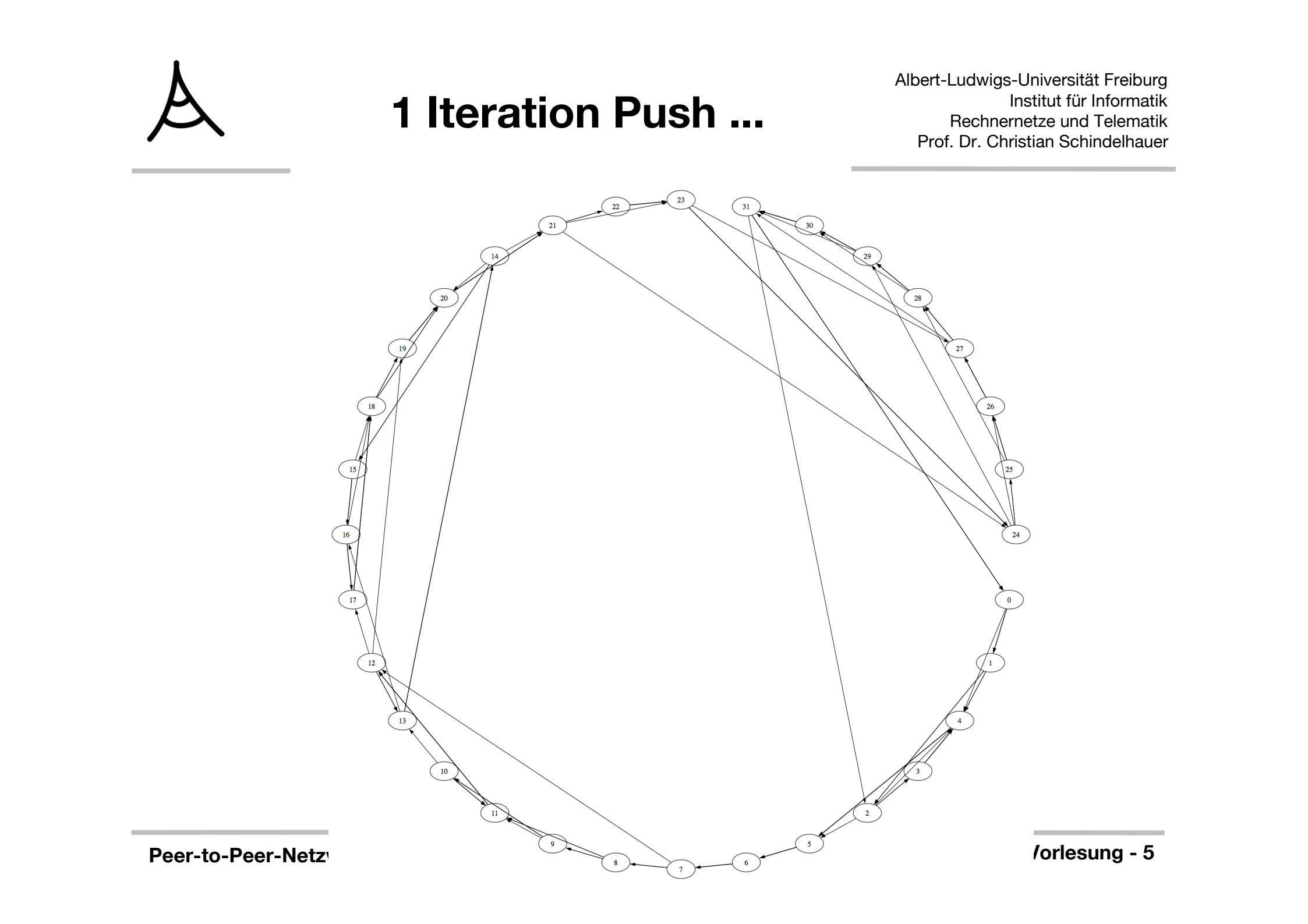
Parameter:

n = 32 Knoten

Ausgrad d = 4

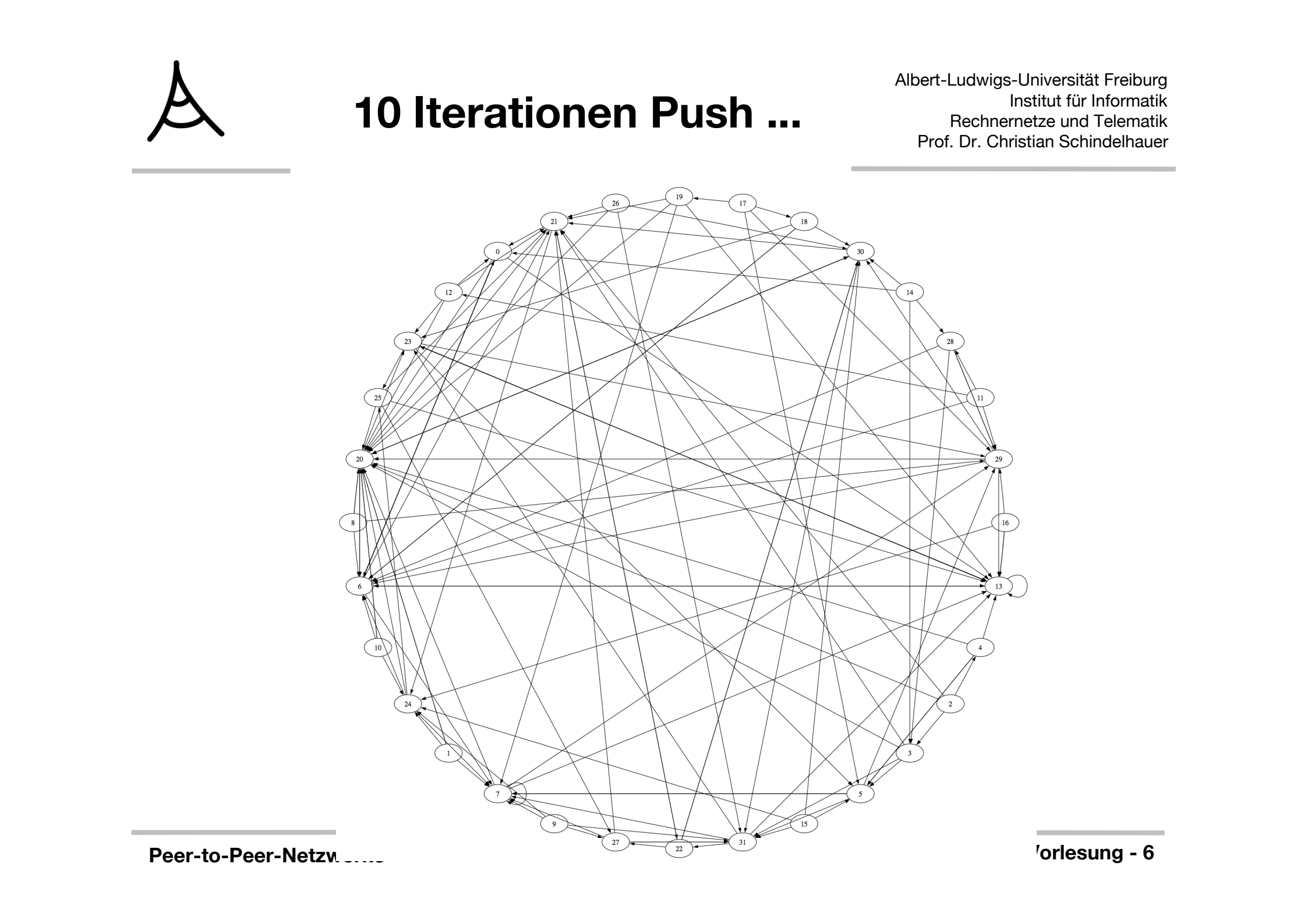
Hop-distanz h = 3





1 Iteration Push ...

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

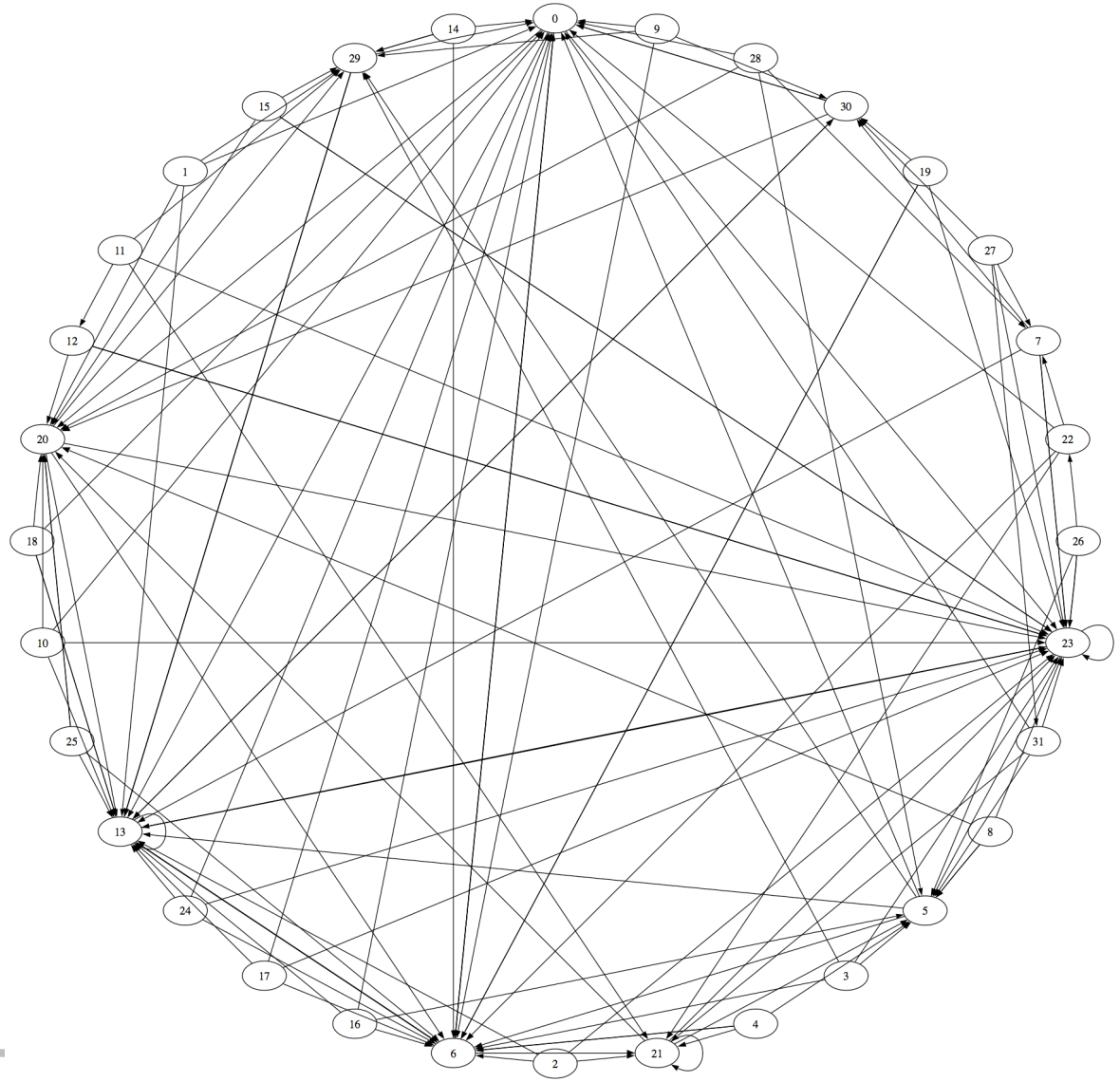


10 Iterationen Push ...

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

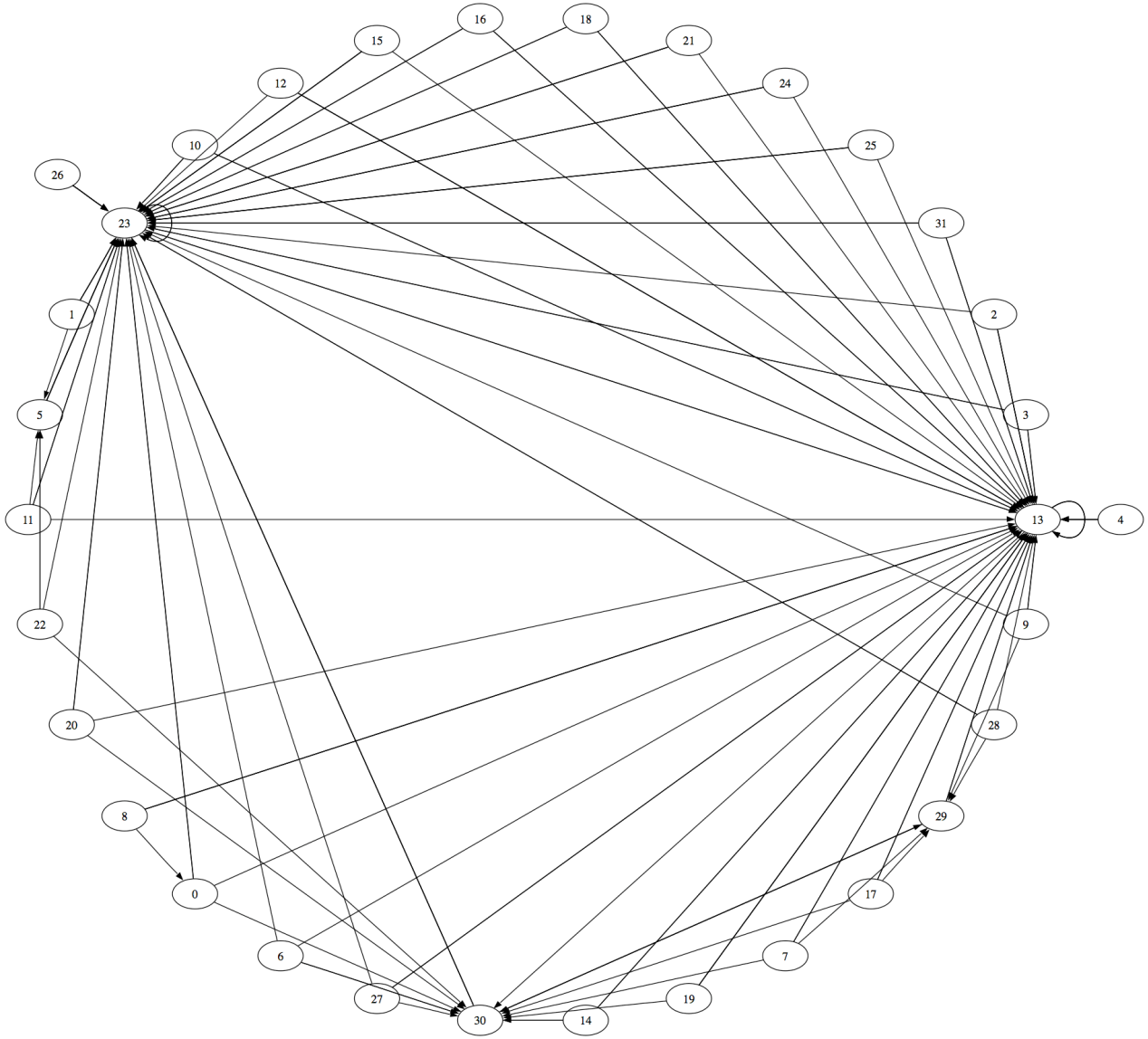
20 Iterationen von Push ...

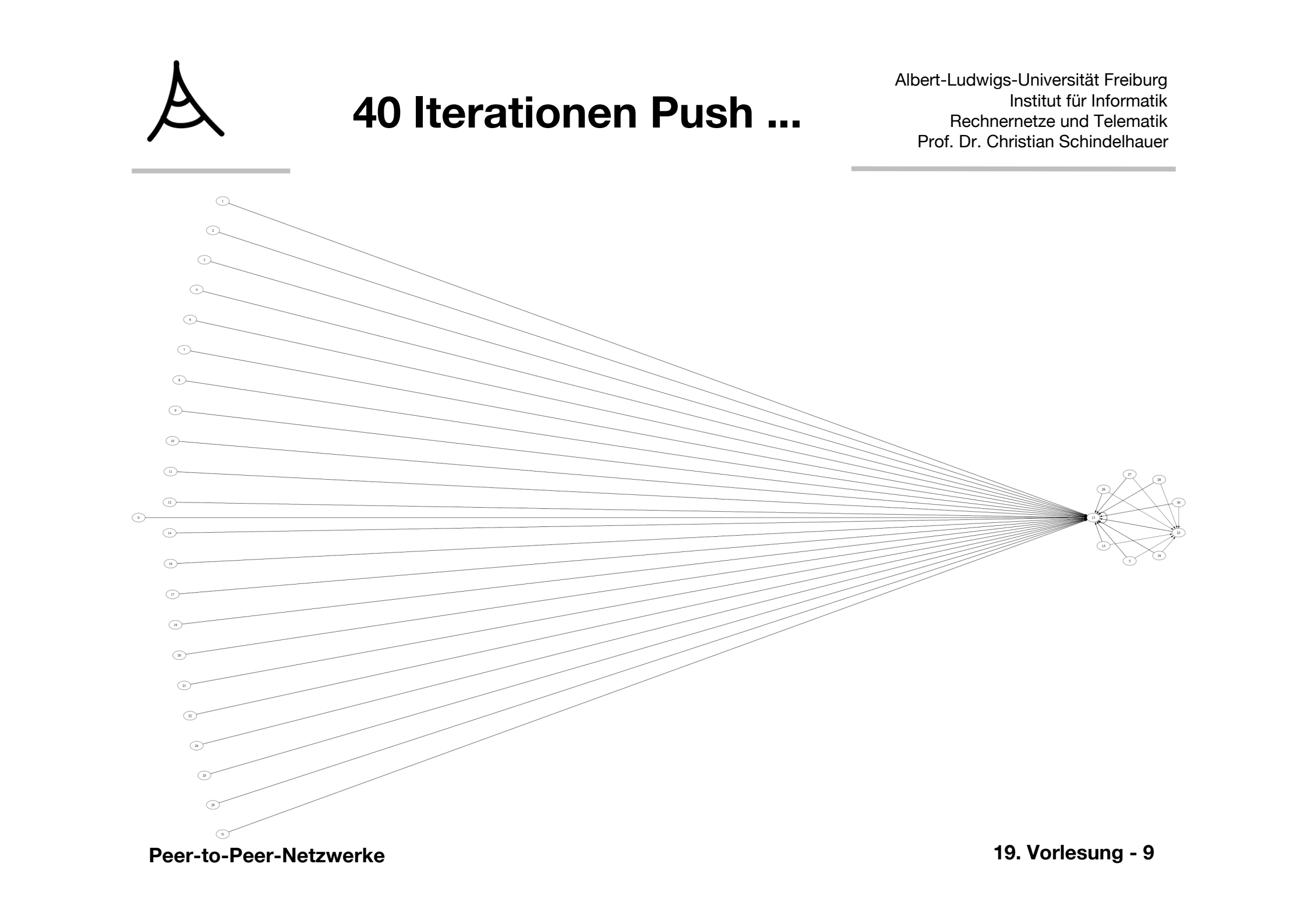
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



30 Iterationen Push ...

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



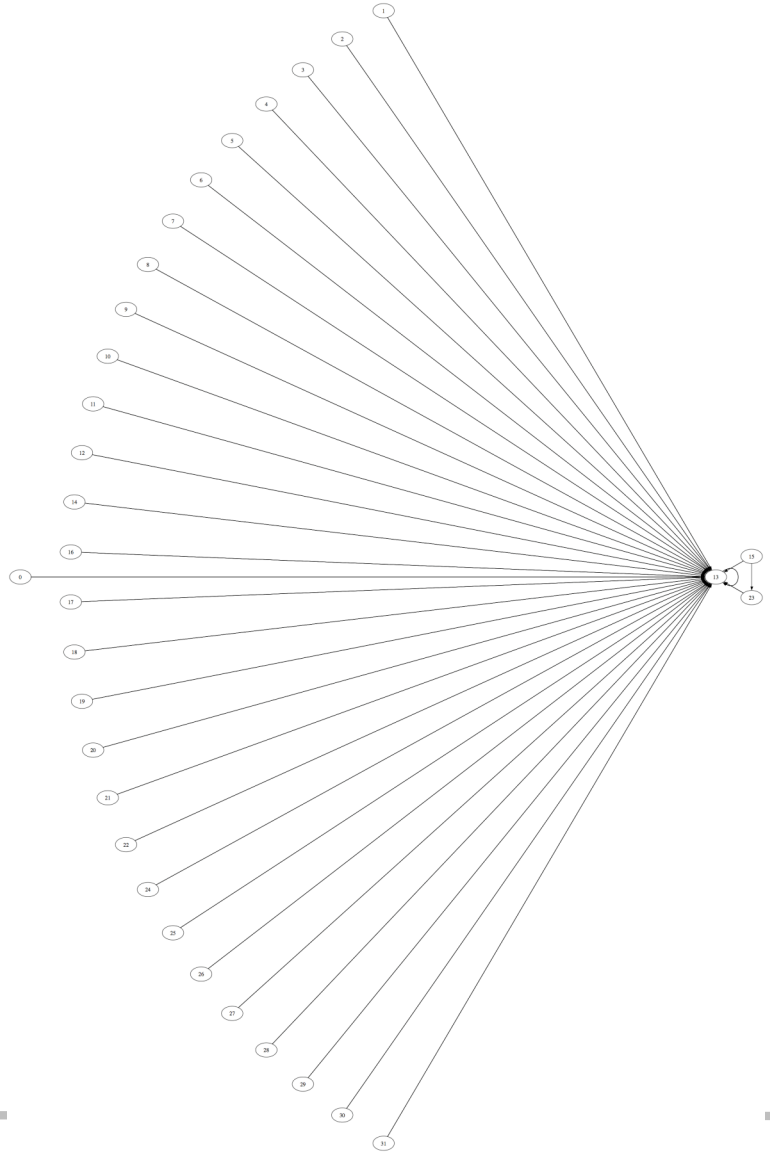


40 Iterationen Push ...

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

50 Iterationen Push ...

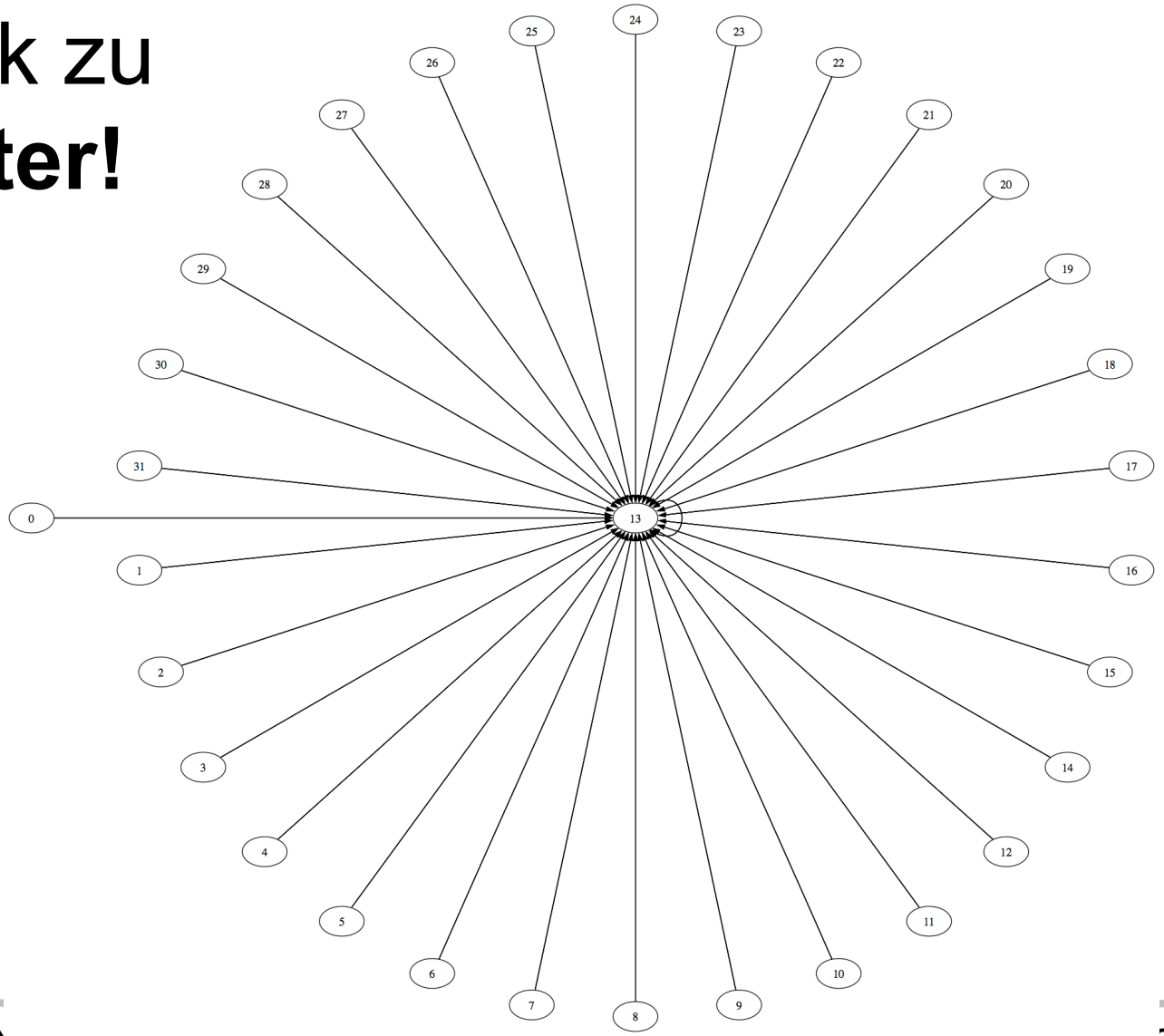
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



70 Iterationen Push ...

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Zurück zu
Napster!



Simulation der Pull-Operation ...

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

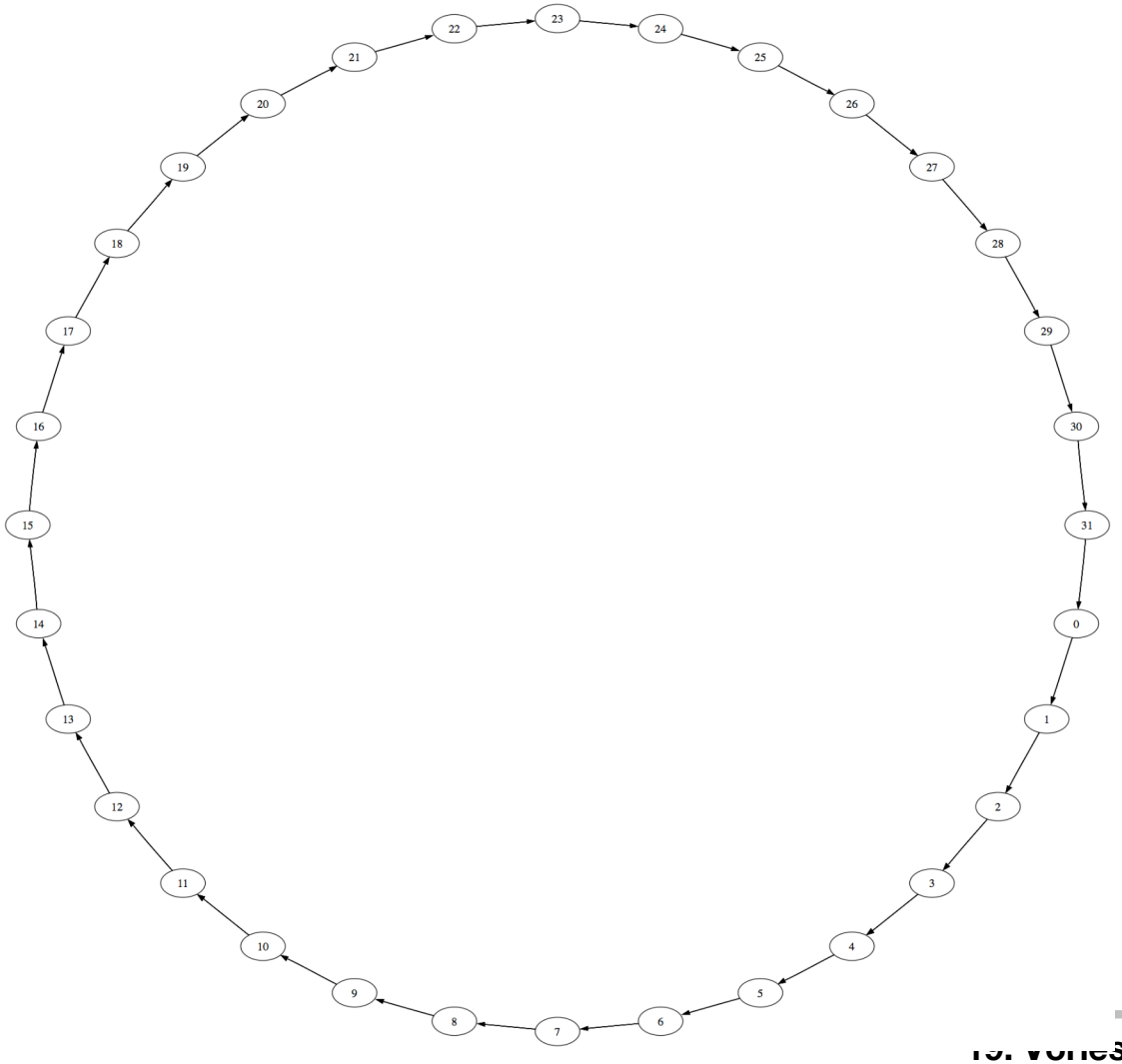
Startsituation

Parameter:

n = 32 Knoten

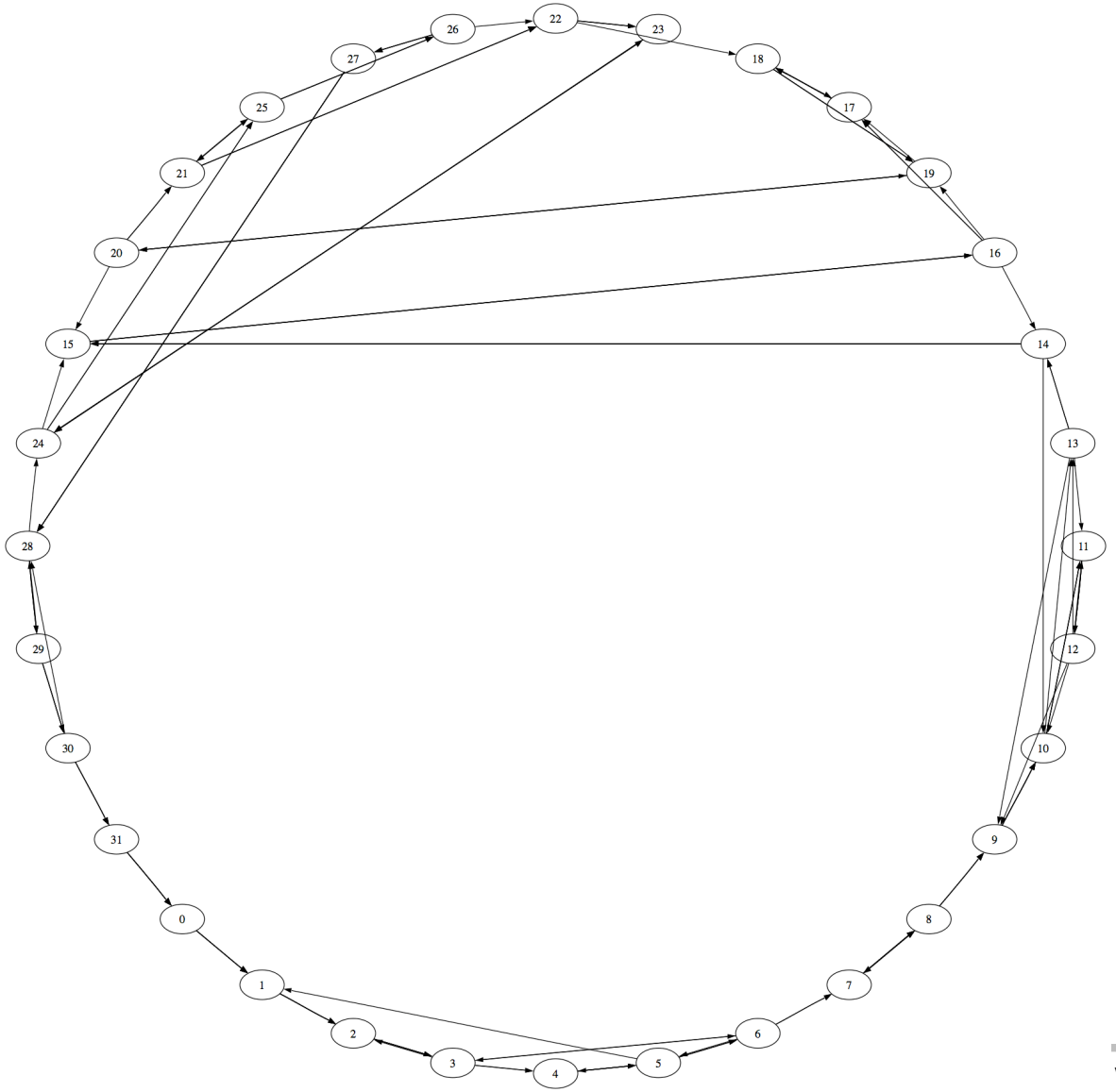
Ausgrad d = 4

Hop-distanz h = 3



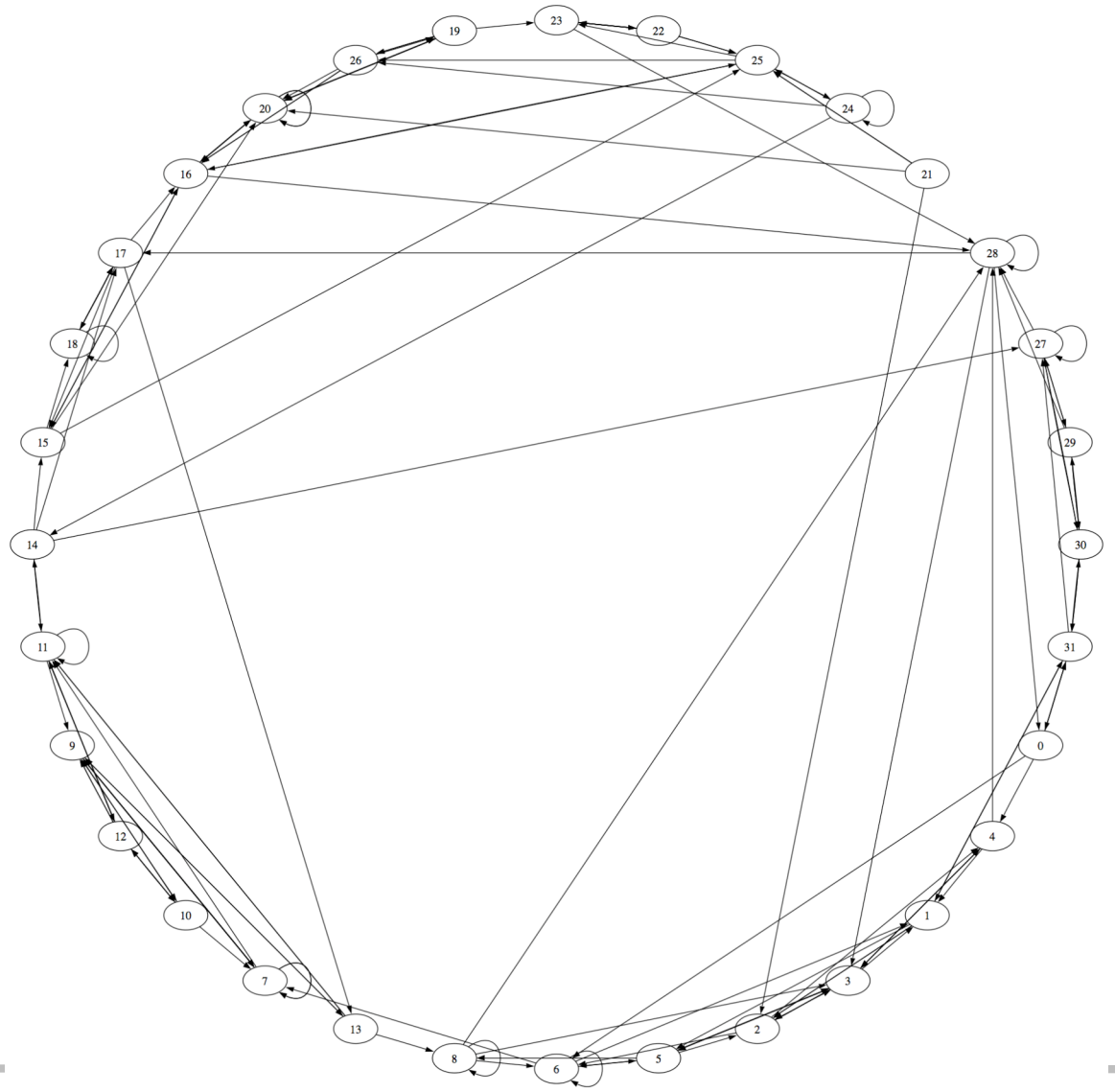
1 Iteration Pull ...

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



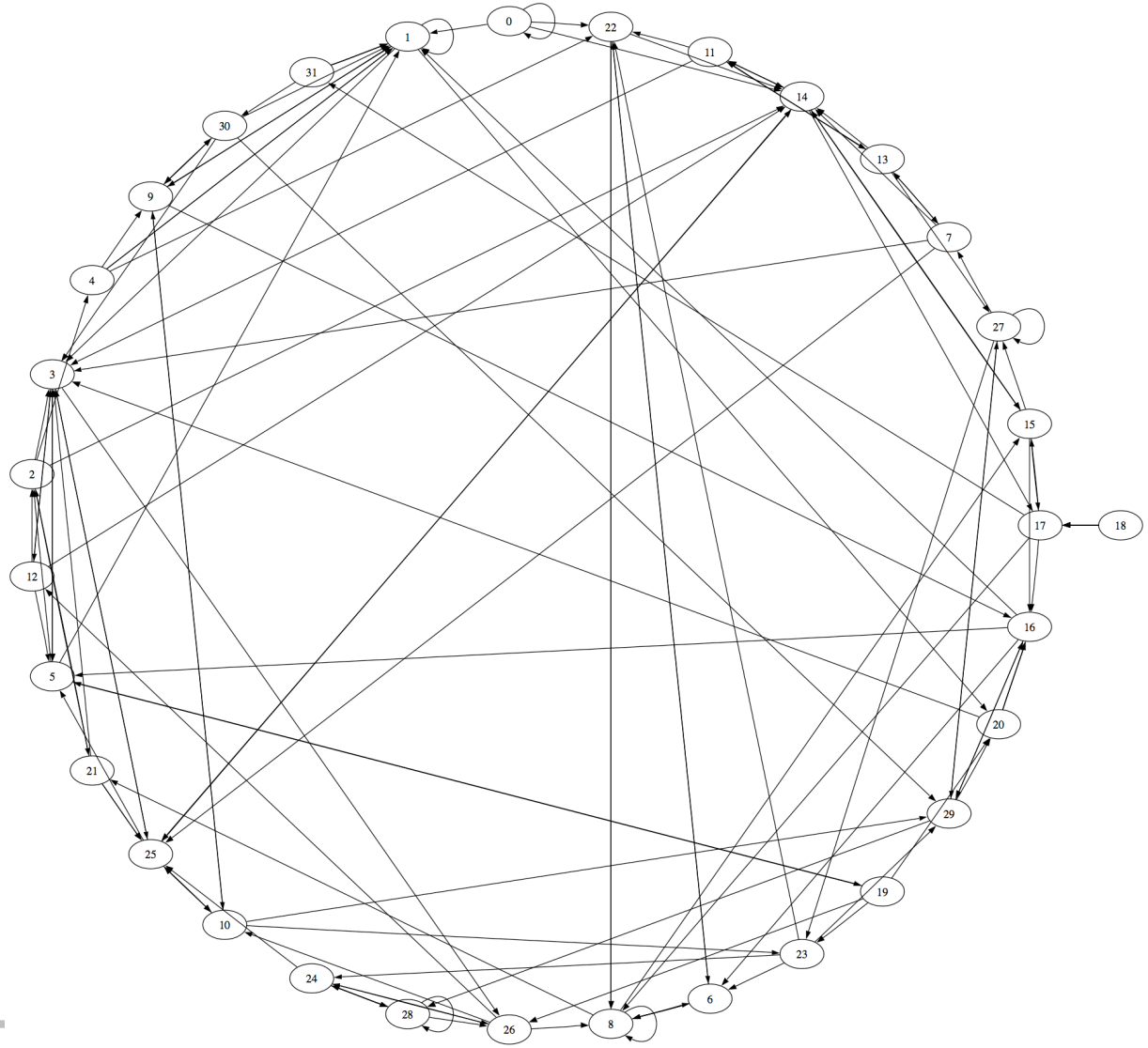
10 Iterationen Pull ...

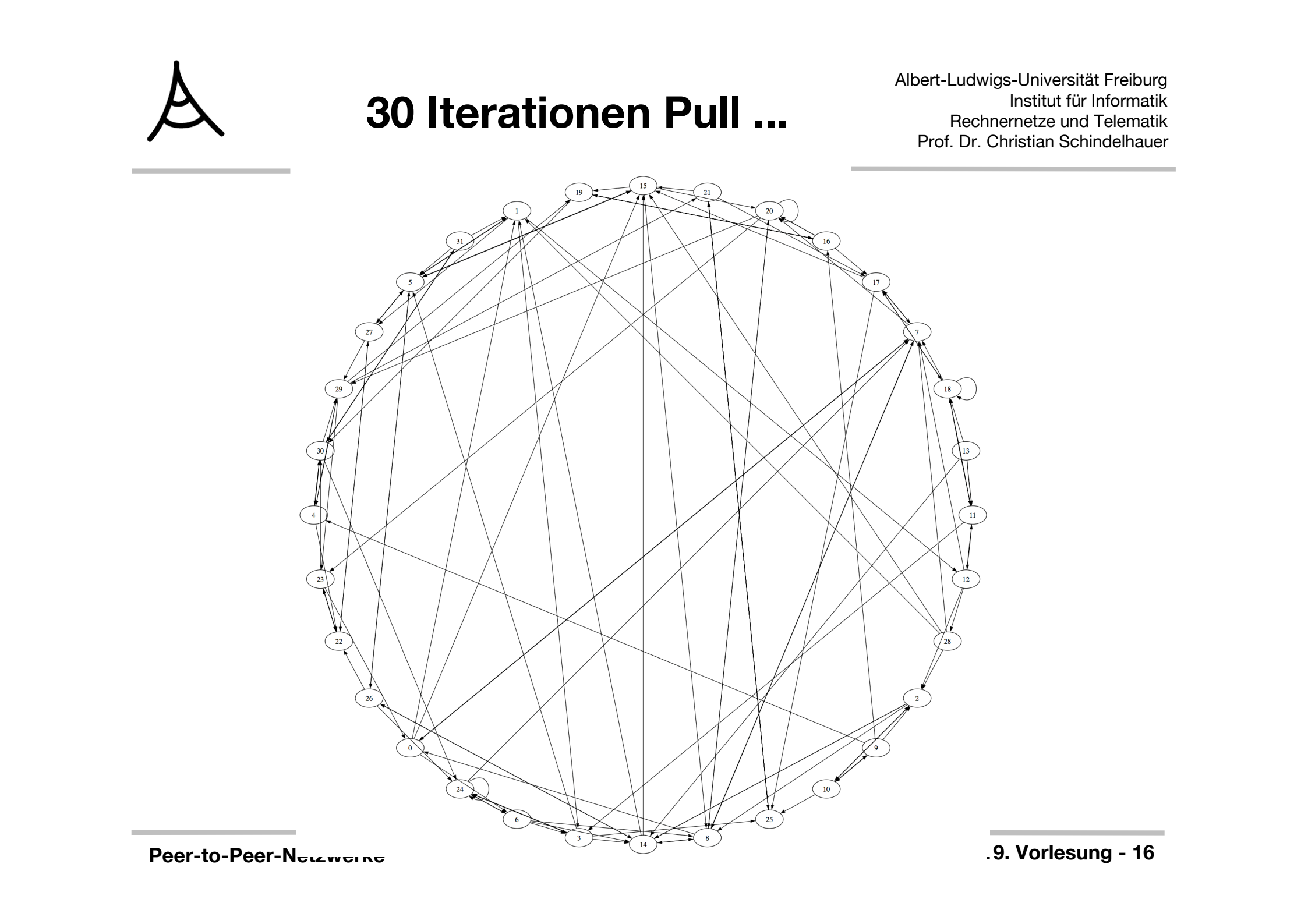
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



20 Iterationen Pull ...

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



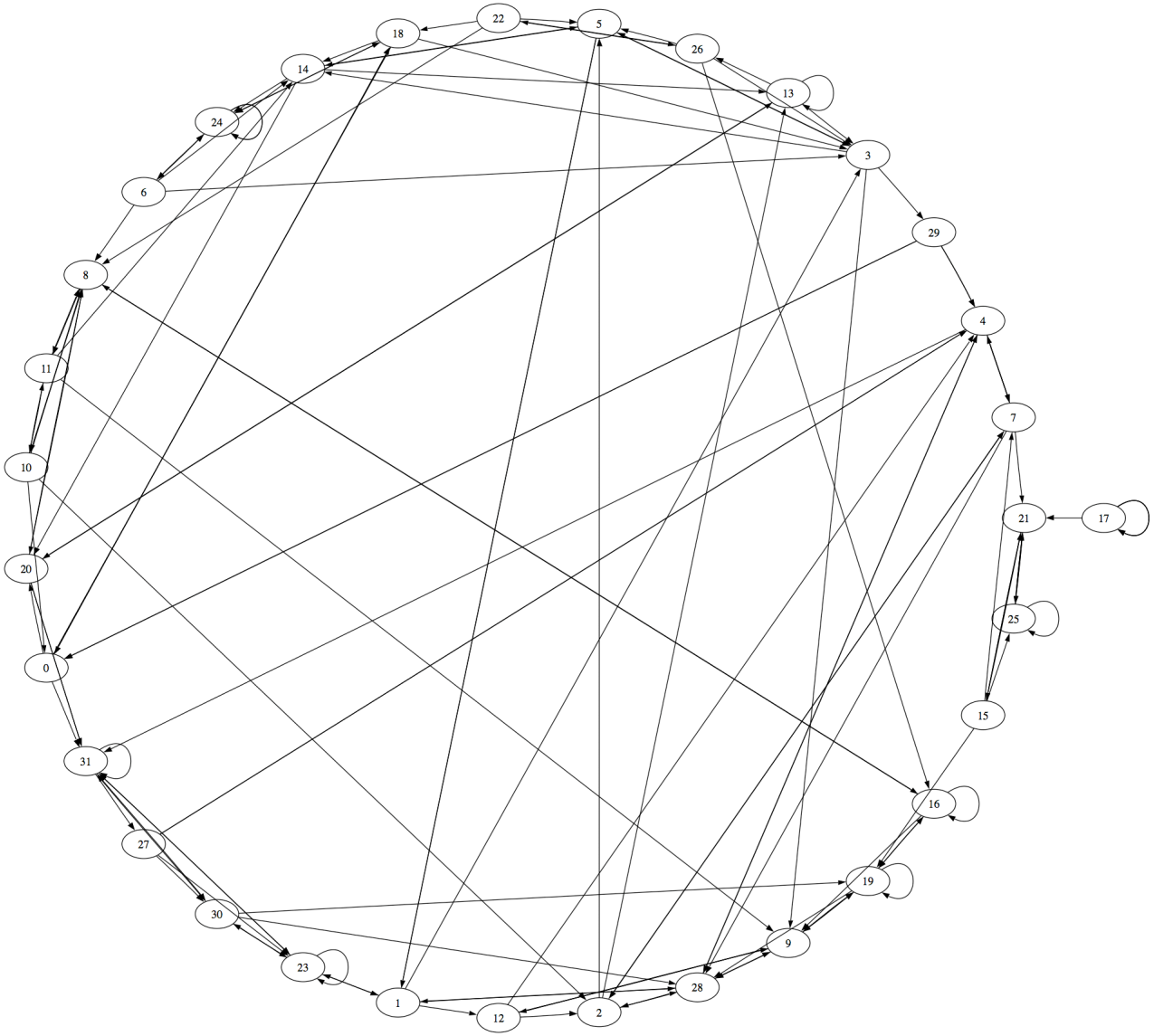


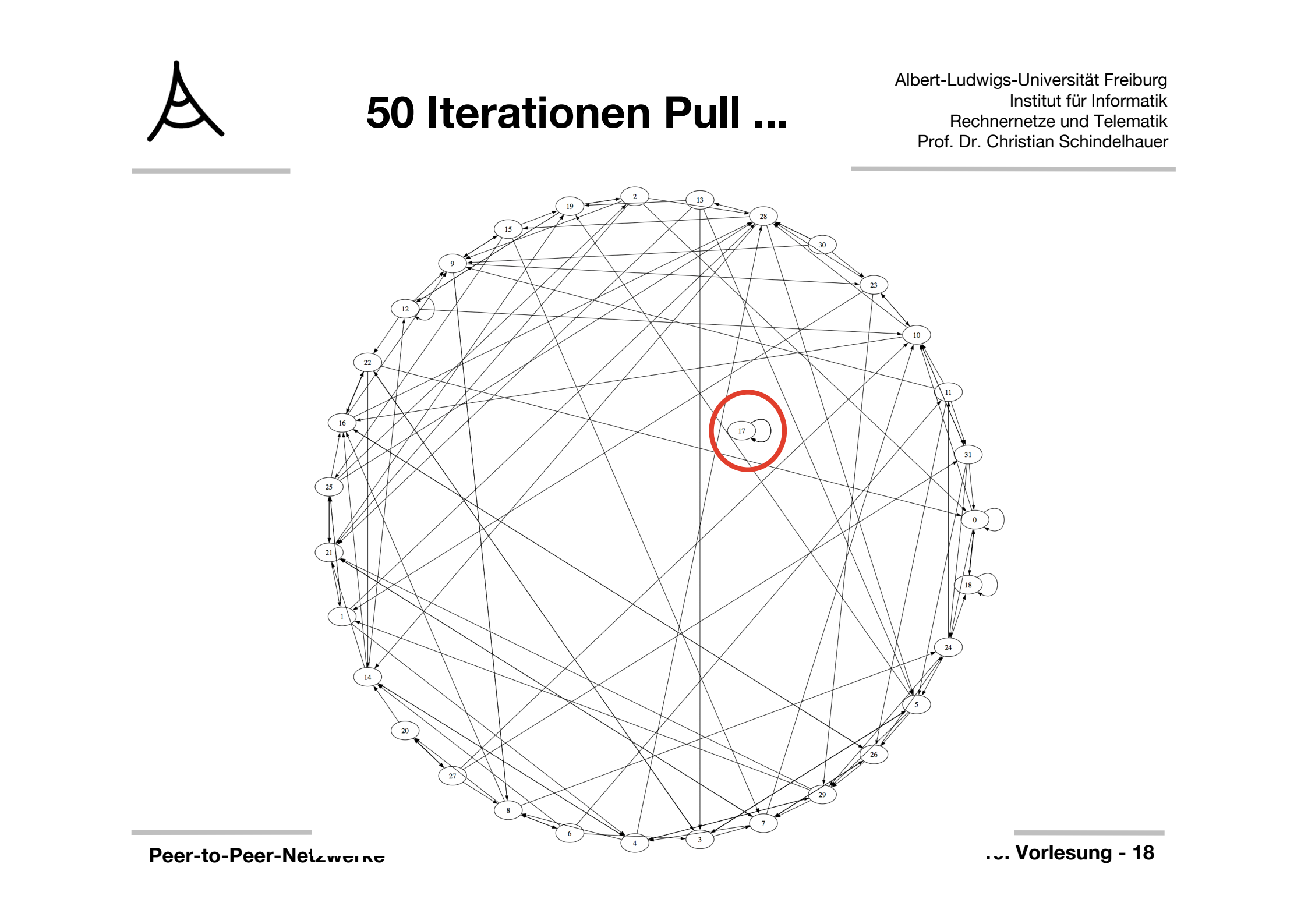
30 Iterationen Pull ...

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

40 Iterationen Pull ...

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



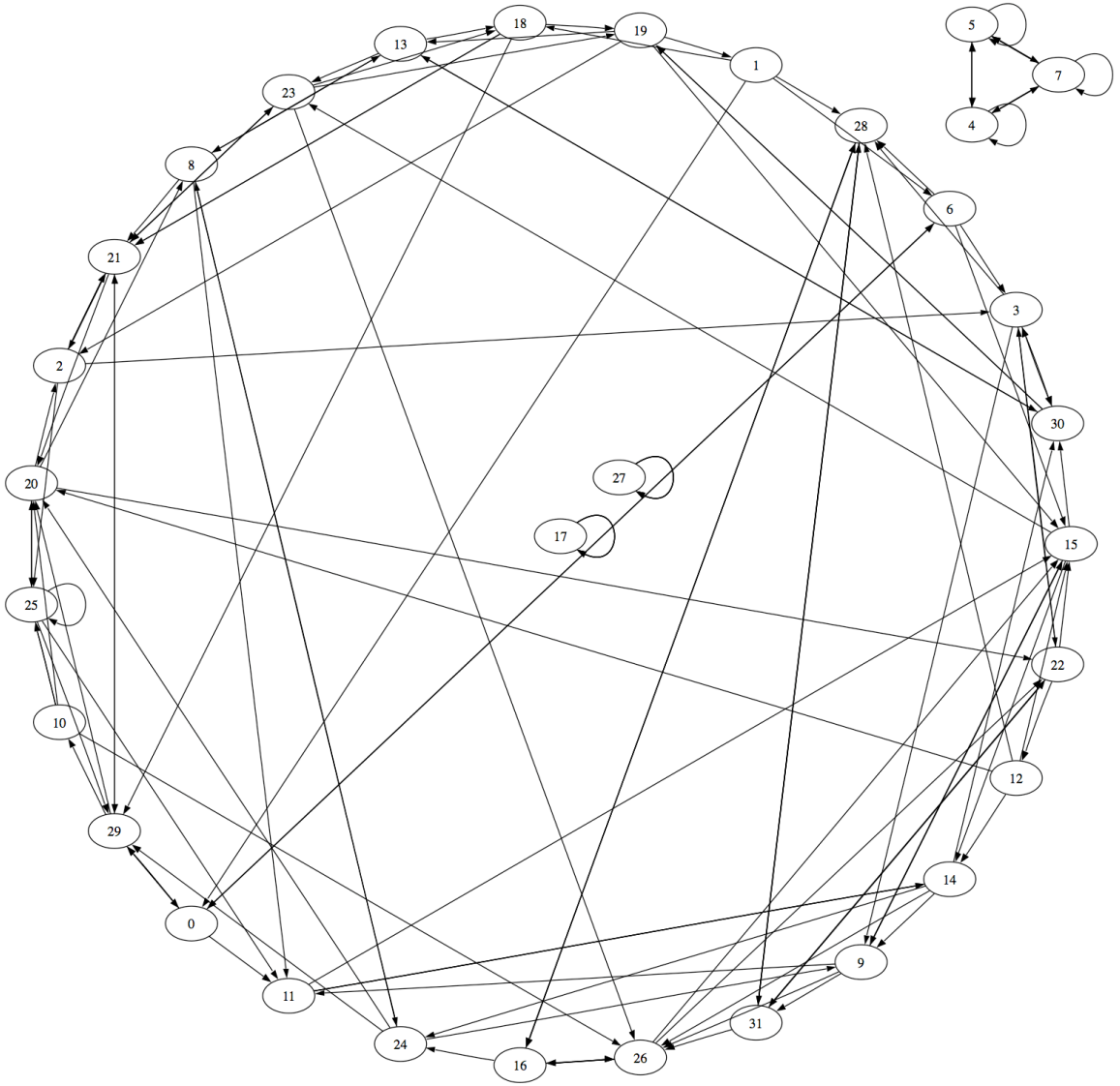


50 Iterationen Pull ...

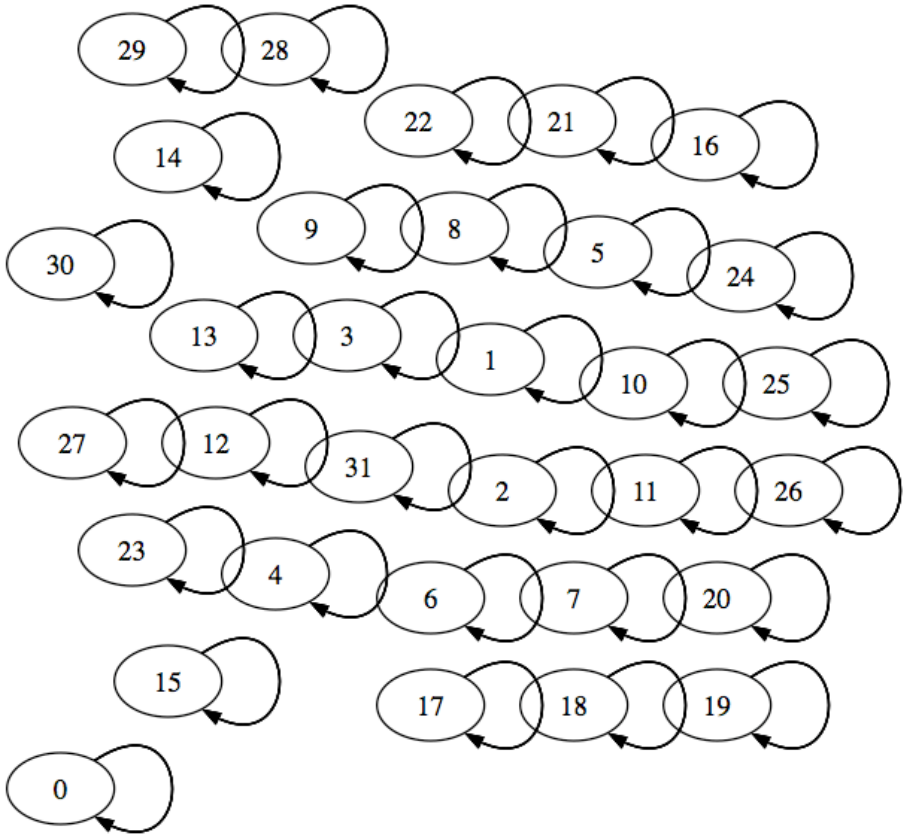
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

500 Iterationen Pull ...

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



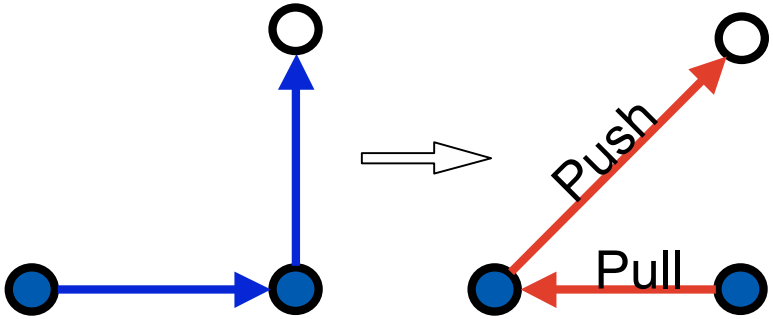
5000 Iterationen Pull ...



Die Kombination von Push und Pull

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Die Lösung: Push&Pull:**



Simulation der Push&Pull-Operationen ...

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

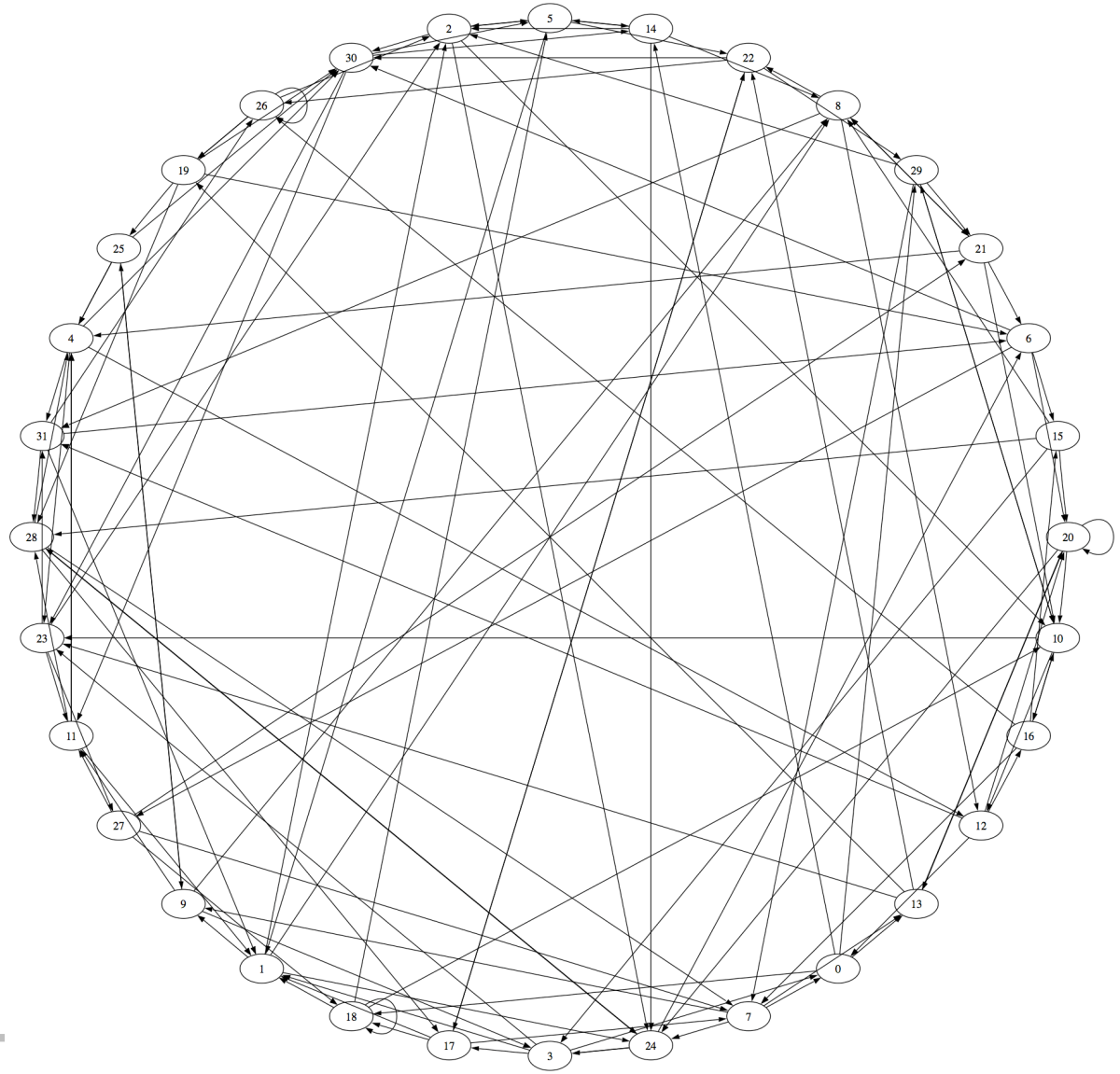
Gleiche Startsituation

Parameter:

n = 32 Knoten

Ausgrad d = 4

Hop-distanz h = 3



Aber

1.000.000 Iterationen

Die Symmetrie von Push&Pull

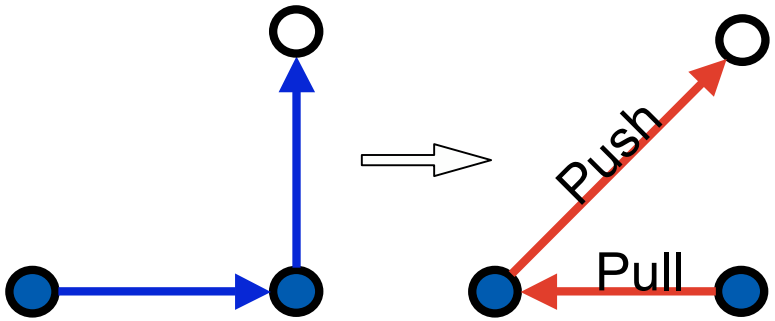
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Lemma (Symmetrie)**
  - Für alle ausgrad-regulären Multigraphen G,G' gilt:

$$P[G \to G'] = P[G' \to G]$$

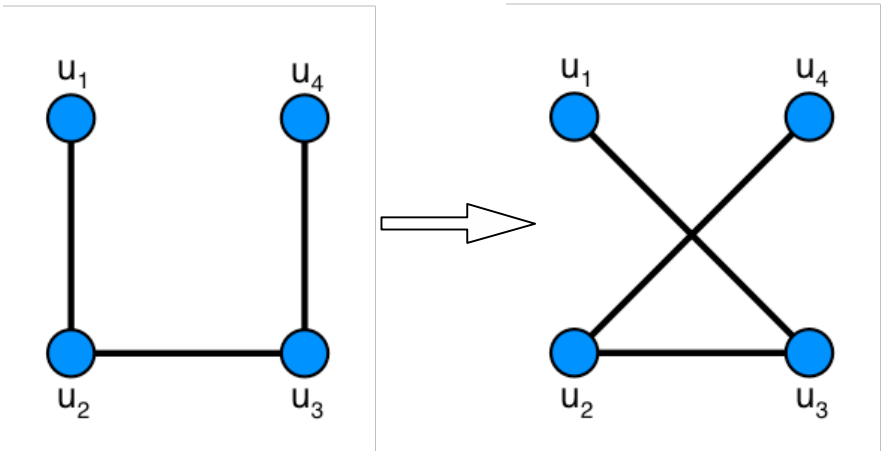
- **Lemma (Erreichbarkeit):**
  - Von jedem schwach zusammenhängenden ausgrad-regulären Graphen G ist jeder andere schwach zusammenhängede ausgrad-reguläre Graph G' mit einer Folge von Push und Pull-Operationen erreichbar

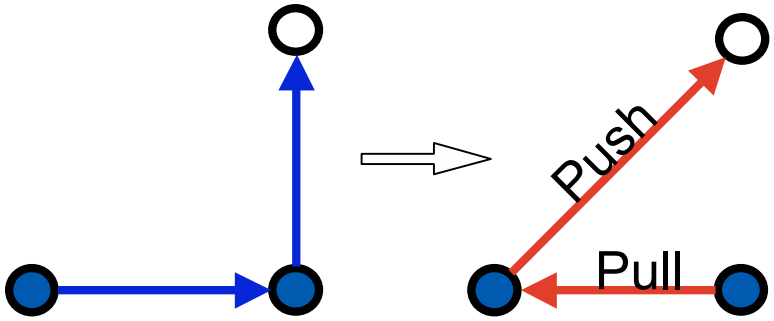
- **Theorem**
  - Aus jedem d-ausgrad-regulären schwach zusammenhängenden Multi-Graph G wird im Limes jeder d-ausgrad-reguläare schwach zusammenhängender Multi-Graph mit gleicher Wahrscheinlichkeit erzeugt



Gute Peer-to-Peer-Operationen

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer





Selbstorganisation in Peer-to-Peer-Netzwerken

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

I. Die Graphstruktur von Gnutella

A. Grad

B. Durchmesser

II. Selbstorganisation von Zufallsgraphen

A. Typen und Eigenschaften von Zufallsgraphen

B. Reguläre ungerichtete zusammenhängende Zufallsgraphen

C. Reguläre gerichtete zusammenhängende Zufallsgraphen

III. Gesteuerte Selbstorganisation

A. Topologie-Management (T-MAN)

B. Selbstorganisierendes Chord

IV. Gesteuerte Selbst-Org.
A. Topologie-Management

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **T-Man: Fast Gossip-based Construction of Large-Scale Overlay Topologies Mark Jelasity Ozalp Babaoglu, 1994**

Verteilte Topologie-Konstruktion

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

do at a random time once in each
consecutive interval of T time units
  $p \leftarrow$ selectPeer()
  myDescriptor $\leftarrow$ (myAddress,myProfile)
  buffer $\leftarrow$ merge(view,{myDescriptor})
  buffer $\leftarrow$ merge(buffer,rnd.view)
  send buffer to p
  receive buffer$_p$ from p
  buffer $\leftarrow$ merge(buffer$_p$,view)
  view $\leftarrow$ selectView(buffer)

(a) active thread

do forever
  receive buffer$_q$ from q
  myDescriptor $\leftarrow$ (myAddress,myprofile)
  buffer $\leftarrow$ merge(view,{myDescriptor})
  buffer $\leftarrow$ merge(buffer,rnd.view)
  send buffer to q
  buffer $\leftarrow$ merge(buffer$_q$,view)
  view $\leftarrow$ selectView(buffer)

(b) passive thread

Fig. 1. The T-MAN protocol.

Aufbau eines Torus

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

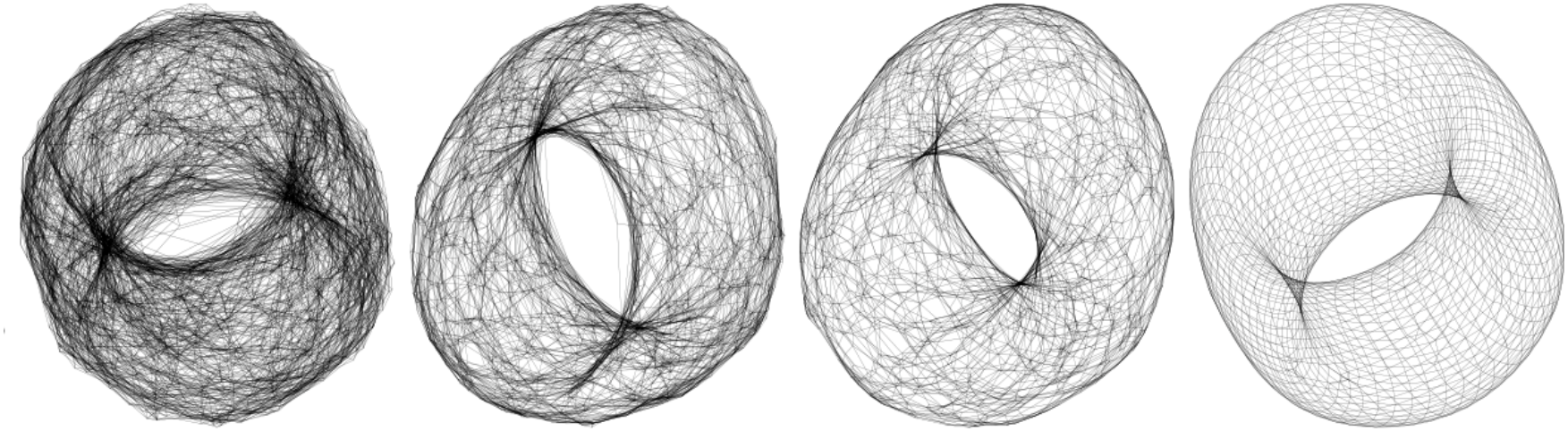
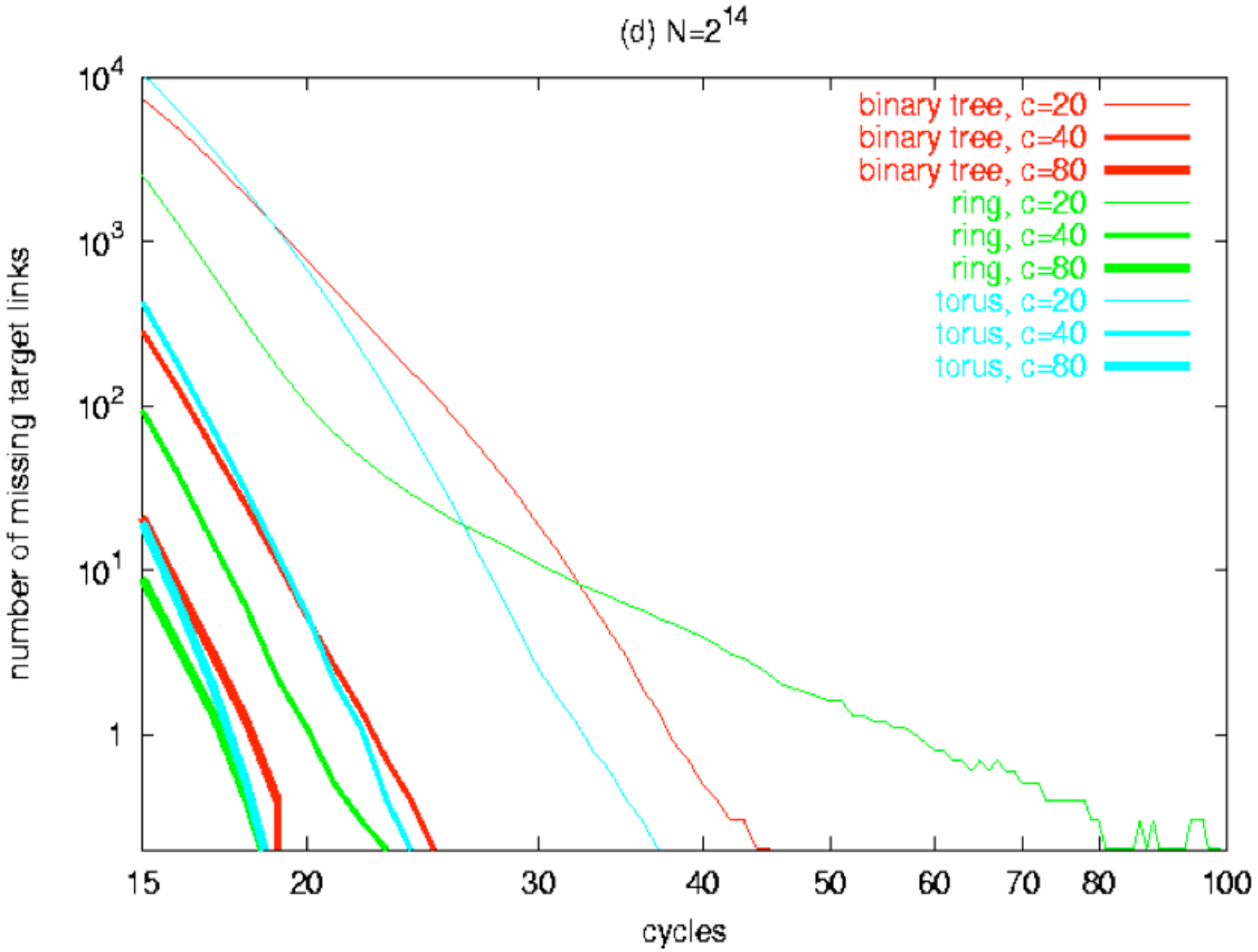


Fig. 2. Illustrative example of constructing a torus over $50 \times 50 = 2500$ nodes, starting from a uniform random topology with $c = 20$. For clarity, only the nearest 4 neighbors (out of 20) of each node are displayed.

Konvergenz von T-MAN

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



IV. Gesteuerte Selbst-Org.
B. T-Chord

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Chord on demand, A Montresor, M Jelasity, O Babaoglu - Peer-to-Peer Computing, 2005. P2P 2005.**

Grundtechnik T-Man

The T-Man algorithm

// *view* is a collection of neighbors

Init: *view* = *rnd.view* ∪ { (*myaddress*, *mydescriptor*) }

```
// active thread
// executed by p
do once every
     δ time units
  q = selectNeighbor(view)
  msg_p = extract(view, q)
  send msg_p to q
  receive msg_q from q
  view = merge(view, msg_q)
```

A "round" of length δ

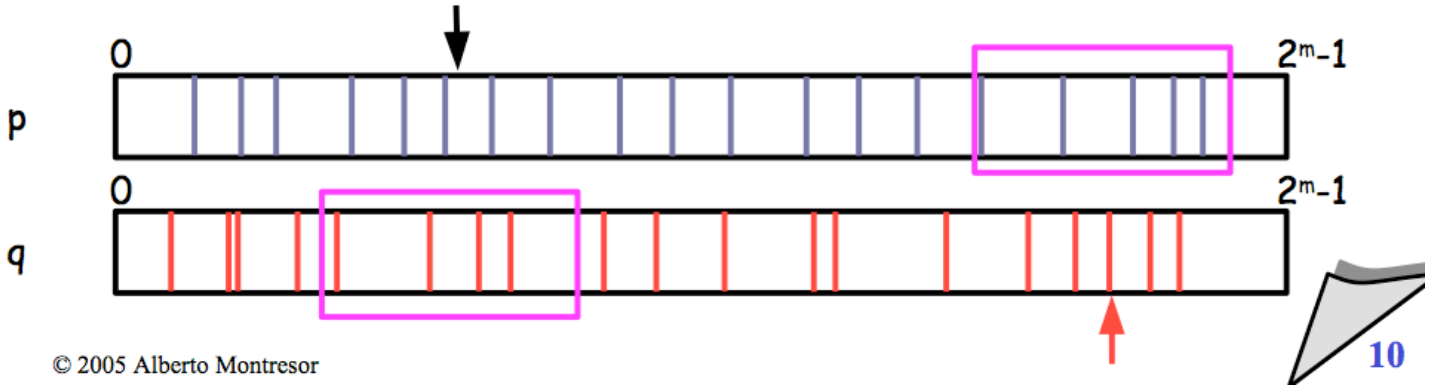
```
// passive thread
// executed by p
do forever
  receive msg_q from *
  msg_p = extract(view, q)
  send msg_p to q
  view = merge(view, msg_q)
```


9

Adaption für Chord

T-Man for T-Chord

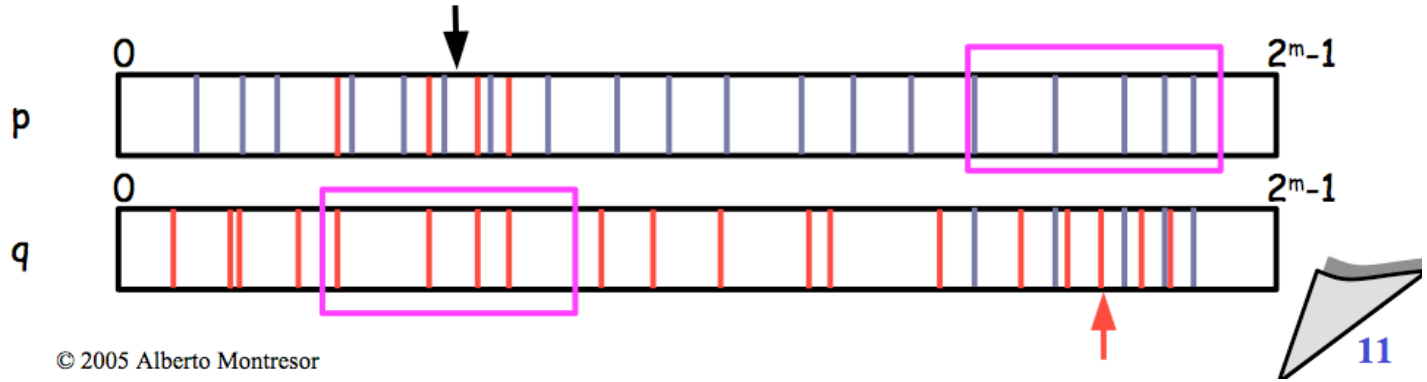
- selectPeer():
  - randomly select a peer ***q*** from the ***r*** nodes in my view that are *nearest to* **p** *in terms of ID distance*
- extract():
  - send to ***q*** the ***r*** nodes in local view that are *nearest to* **q**
  - ***q*** responds with the ***r*** nodes in its view that are *nearest to* **p**
- merge():
  - both ***p*** and ***q*** *merge* the received nodes to their view



Nach Austausch der Links

T-Man for T-Chord

- selectPeer():
  - randomly select a peer ***q*** from the ***r*** nodes in my view that are *nearest to* **p** *in terms of ID distance*
- extract():
  - send to ***q*** the ***r*** nodes in local view that are *nearest to* **q**
  - ***q*** responds with the ***r*** nodes in its view that are *nearest to* **p**
- merge():
  - both ***p*** and ***q*** *merge* the received nodes to their view



Zusammenfassung

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

I. Die Graphstruktur von Gnutella

A. Grad

B. Durchmesser

II. Selbstorganisation von Zufallsgraphen

A. Typen und Eigenschaften von Zufallsgraphen

B. Reguläre ungerichtete zusammenhängende Zufallsgraphen

C. Reguläre gerichtete zusammenhängende Zufallsgraphen

III. Gesteuerte Selbstorganisation

A. Topologie-Management (T-MAN)

B. Selbstorganisierendes Chord

Inhalte

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Kurze Geschichte der Peer-to-Peer-Netzwerke**
- **Das Internet: Unter dem Overlay**
- **Die ersten Peer-to-Peer-Netzwerke**
  - Napster
  - Gnutella
- **CAN**
- **Chord**
- **Pastry und Tapestry**
- **Gradoptimierte Netzwerke**
  - Viceroy
  - Distance-Halving
  - Koorde
- **Netzwerke mit geordneter Speicherung**
  - P-Grid
  - Skip-Net und Skip-Graphs
- **Selbstorganisation**
  - Pareto-Netzwerke
  - Zufallsnetzwerke
  - Topologie-Management
- **Sicherheit in Peer-to-Peer-Netzwerken**
- **Anonymität**
- **Datenzugriff: Der schnellere Download**
- **Peer-to-Peer-Netzwerke in der Praxis**
  - eDonkey
  - FastTrack
  - Bittorrent
- **Juristische Situation**

Verschlüsselungs-methoden

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Symmetrische Verschlüsselungsverfahren

- z.B. Cäsars Code, DES, AES
- Es gibt Funktion f,g, so dass
  - f(schlüssel,text) = code
  - g(schlüssel,code) = text
- Der Schlüssel
  - muss geheim bleiben
  - dem Sender und Empfänger zur Verfügung stehen

Asymmetrische Verschlüsselungsverfahren

- z.B. RSA, Ronald Rivest, Adi Shamir, Lenard Adleman, 1977
  - Diffie-Hellman, PGP
- Geheimer Schlüssel `privat`
  - kennt nur der Empfänger der Nachricht
- Öffentlichen Schlüssel `offen`
  - Ist allen Teilnehmern bekannt
  - Wird erzeugt durch Funktion
    - keygen(`privat`) = `offen`
- Verschlüsselungsfunktion f und Entschlüsselungsfunktion g
  - sind auch allen bekannt
- Verschlüsselung
  - f(offen,text) = code
  - kann jeder berechnen
- Entschlüsselung
  - g(privat,code) = code
  - nur vom Empfänger

Ende der 19. Vorlesung

Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Peer-to-Peer-Netzwerke

Christian Schindelhauer

schindel@informatik.uni-freiburg.de