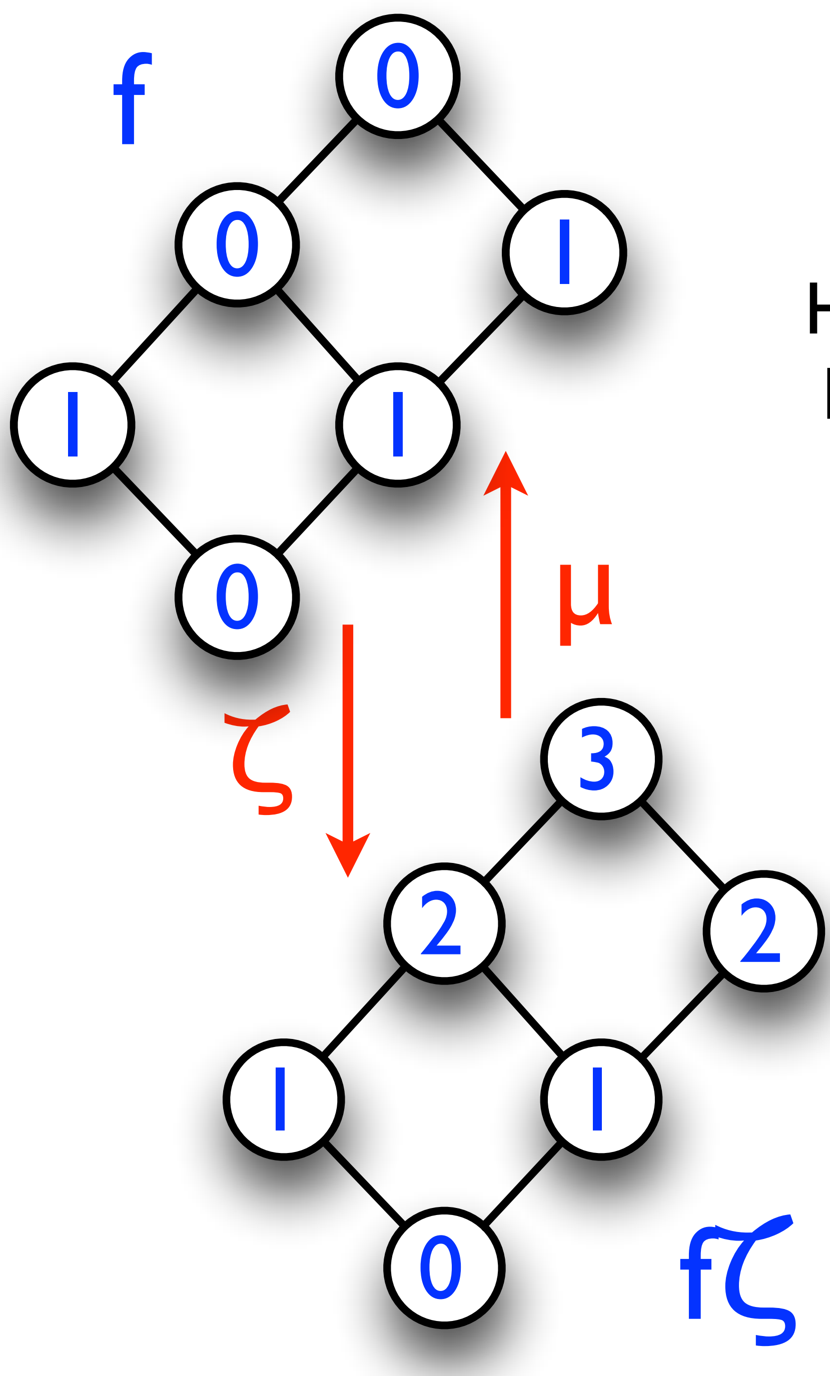
Fast Möbius inversion with applications



Petteri Kaski

Helsinki Institute for Information Technology HIIT &
Department of Information and Computer Science
Aalto University, Helsinki

Joint Estonian–Latvian
Theory Days at Medzābaki, Lidaste
30 September 2012

Aalto University
School of Science

Joint work with

Andreas Björklund (Lund),
Thore Husfeldt (Copenhagen),
Mikko Koivisto (Helsinki),
Jesper Nederlof (Utrecht) &
Pekka Parviainen (Stockholm)

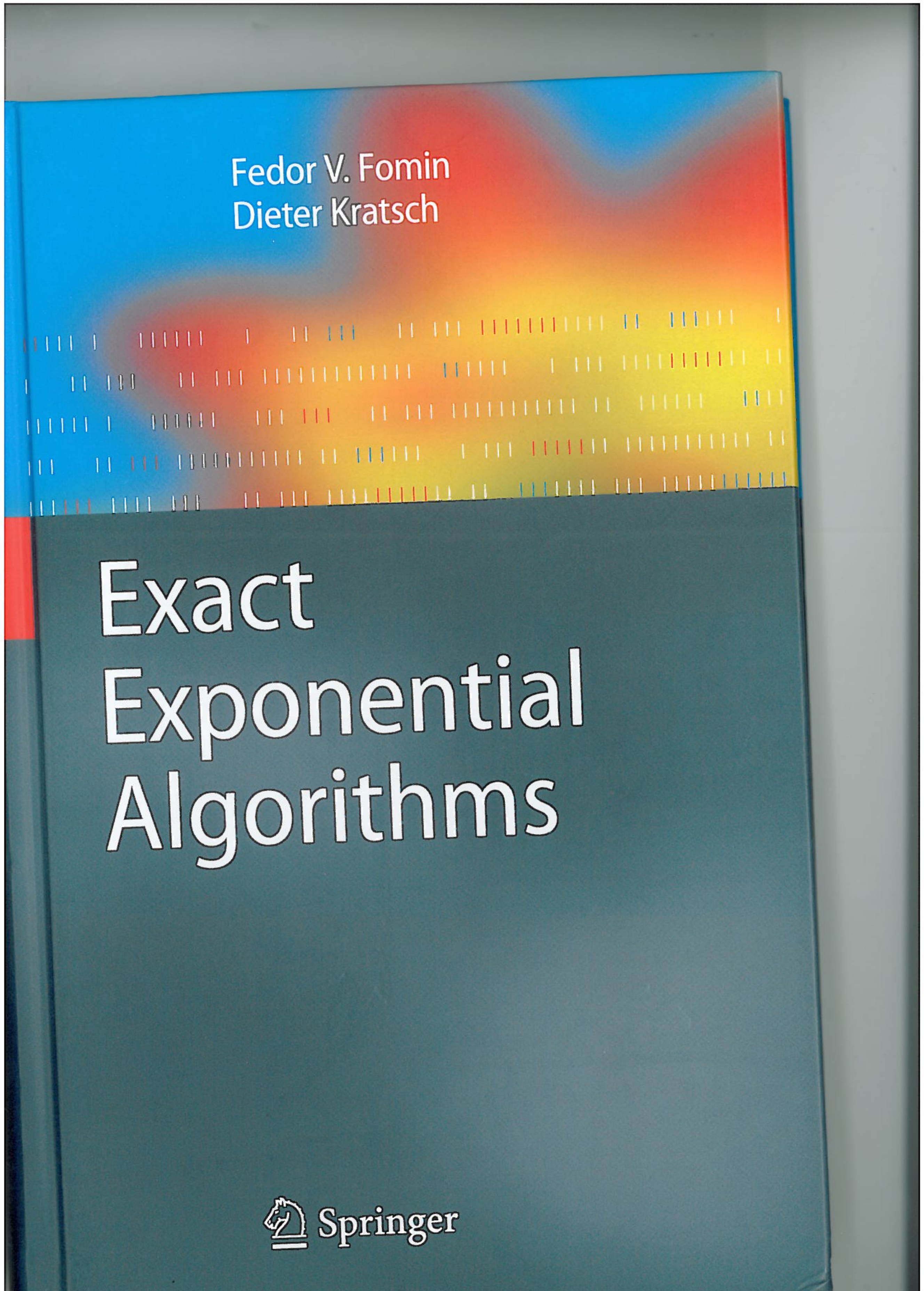
Background

“The main argument in favor of $P \neq NP$ is the total lack of fundamental progress in the area of exhaustive search. This is, in my opinion, a very weak argument. The space of algorithms is very large and we are only at the beginning of its exploration.”

— Moshe Vardi

[Lane A. Hemaspaandra,
SIGACT News Complexity Theory Column 36,
SIGACT News 33:34–47, June 2002.]

- Take your favorite NP-complete problem
- Is there an algorithm that
  - ... perhaps does not run in polynomial time ...
  - ... *but still beats exhaustive search?*
- E.g. k-coloring an n-vertex graph
  — can one do better than $O^*(k^n)$ time,
  in the worst case, on arbitrary graphs?



[Fomin & Kratsch, Springer 2010]

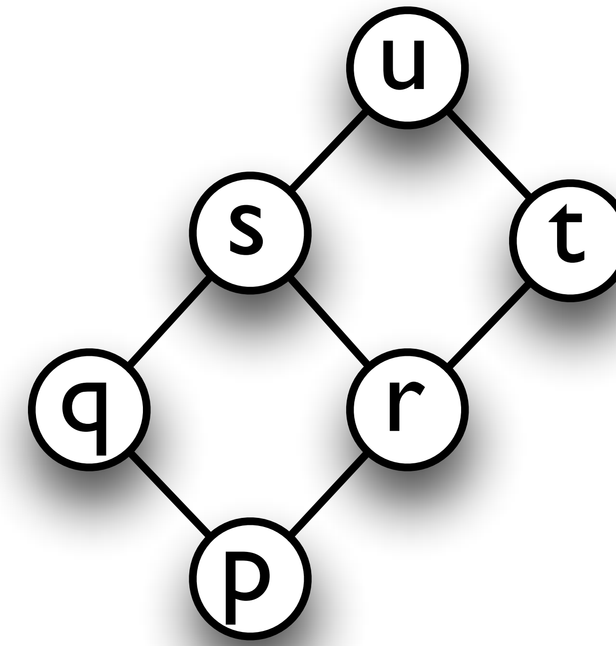
"Bad, but better" algorithms for hard problems

- For many NP-complete graph problems, currently the fastest known exact algorithms rely on algebraic techniques
- Examples:
graph coloring, k-path, Steiner tree, Hamilton cycle, k-clique, triangle packing, ...
- **This talk** — one technique and one problem
  - fast Möbius inversion on lattices
  - ... illustrated with graph coloring and the subset lattice

Fast Möbius inversion on lattices

(Finite) lattices

- *Combinatorial definition:*
  A (finite) partially ordered set $(L,\leq)$ such that
  1) there is a minimum element; and
  2) any two elements $x,y \in L$ have a least upper bound (**join**) $x \vee y$

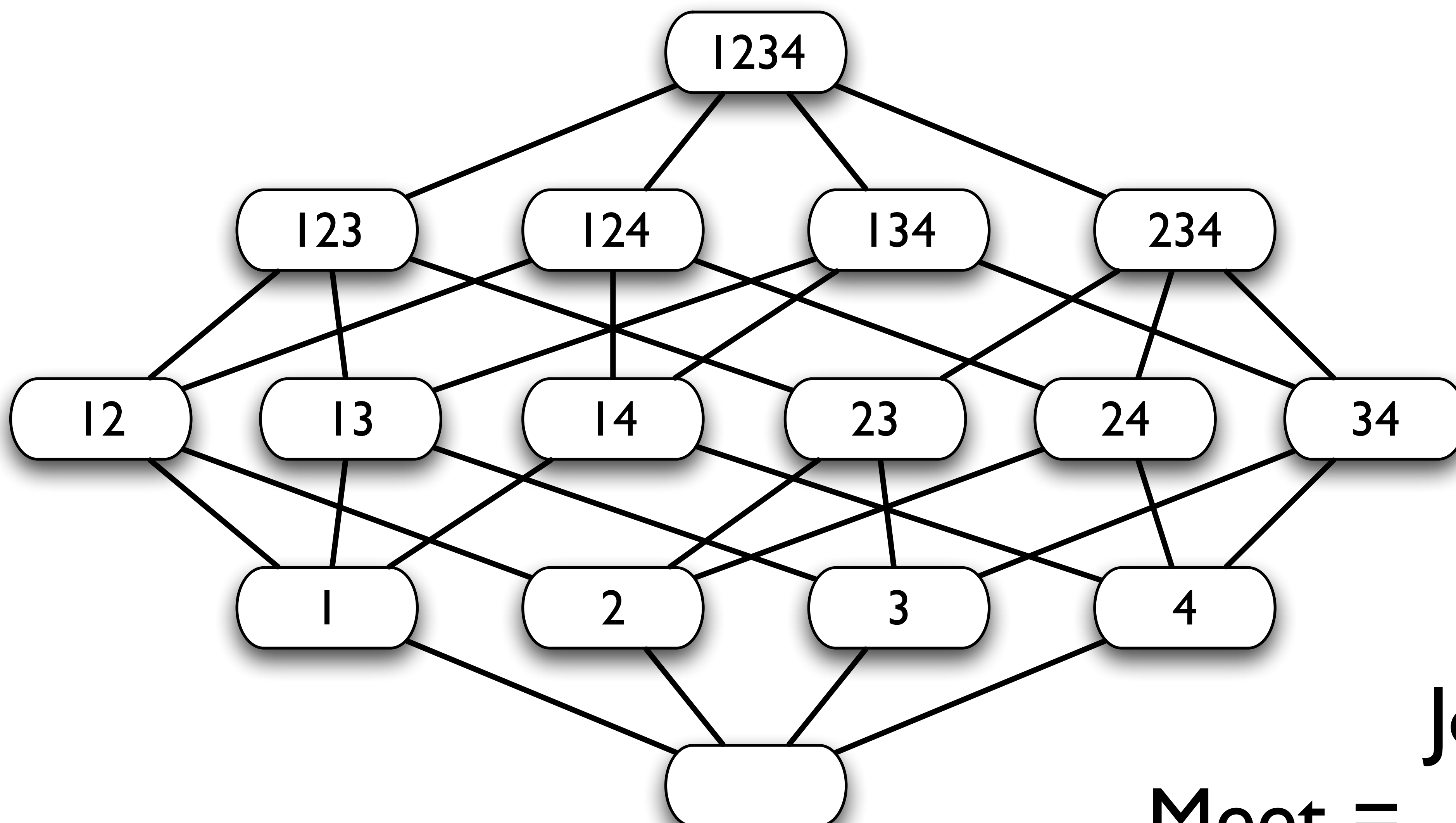


- *Algebraic definition:*
  A (finite) commutative idempotent semigroup $(L,\vee)$ with identity

$\vee$	p	q	r	s	t	u
p	p	q	r	s	t	u
q	q	q	s	s	u	u
r	r	s	r	s	t	u
s	s	s	s	s	u	u
t	t	u	t	u	t	u
u	u	u	u	u	u	u

Example: Subset lattice

- The set of all 2^n subsets of an n-element set
- Partially ordered by subset inclusion

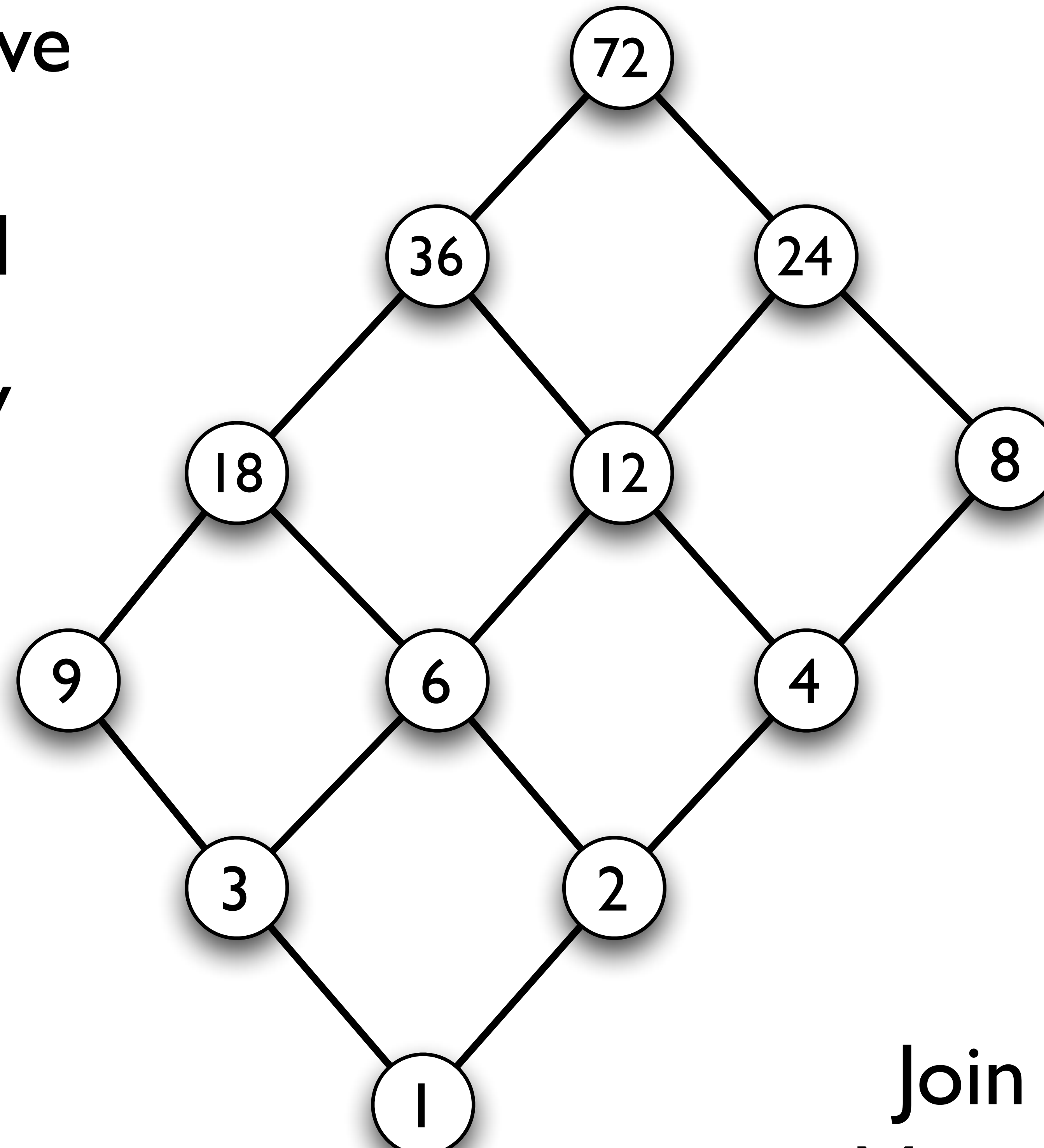


Join = Union

Meet = Intersection

Example: Divisor lattice

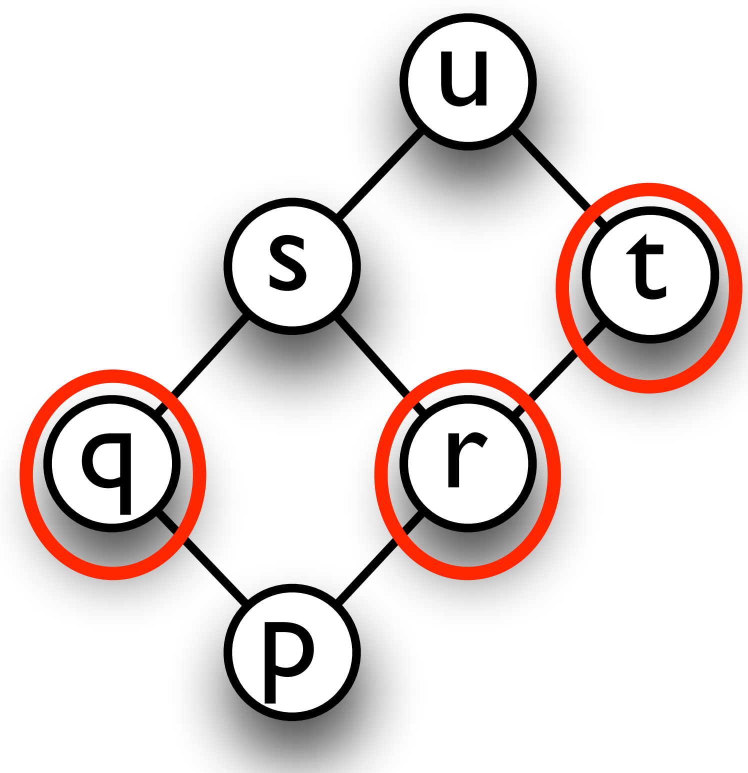
- The set of all positive divisors of a positive integer M
- Partially ordered by divisibility



Join = lcm
Meet = gcd

Join-irreducible elements

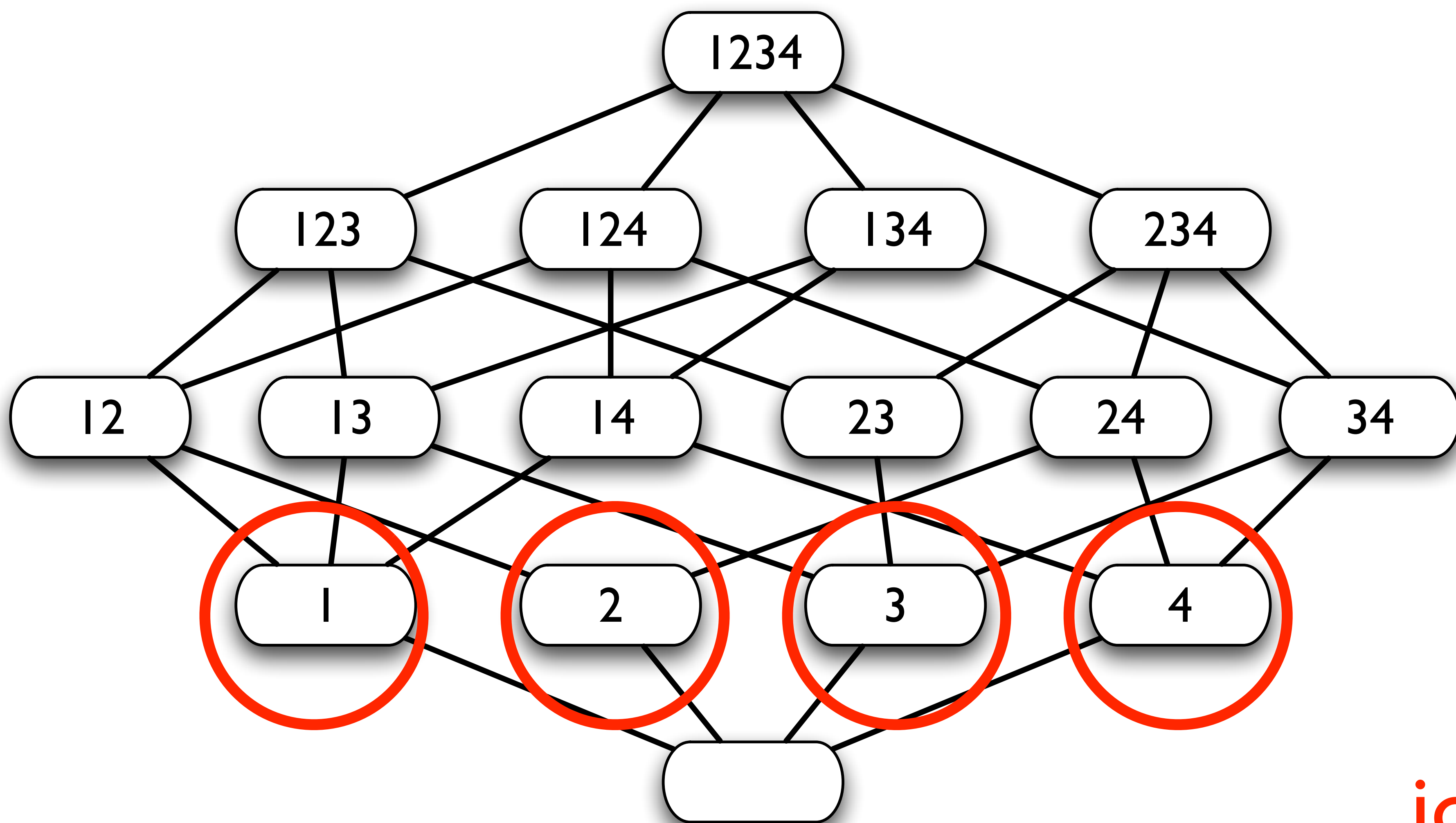
- An element $z \in L$ is **join-irreducible** if $z = x \vee y$ implies $z = x$ or $z = y$
- The minimum ("zero") element is always join-irreducible
- *Algebraic view:* The set of nonzero join-irreducibles is a minimal set of generators for $(L, \vee)$



= "down-degree one" in the lattice diagram

Example: Subset lattice

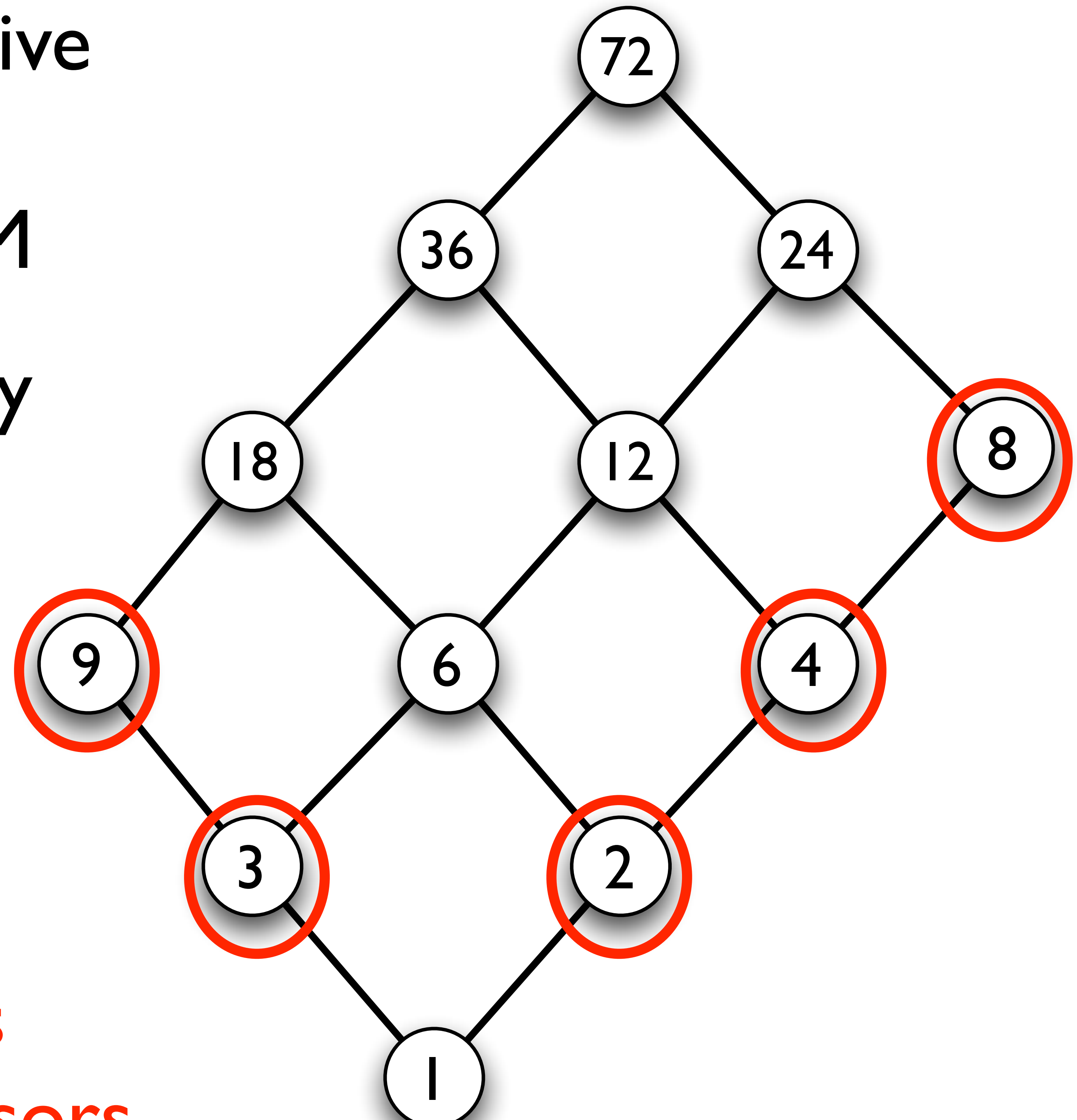
- The set of all subsets of an n-element set
- Partially ordered by subset inclusion



Nonzero join-irreducibles = singletons

Example: Divisor lattice

- The set of all positive divisors of
  a positive integer M
- Partially ordered by divisibility



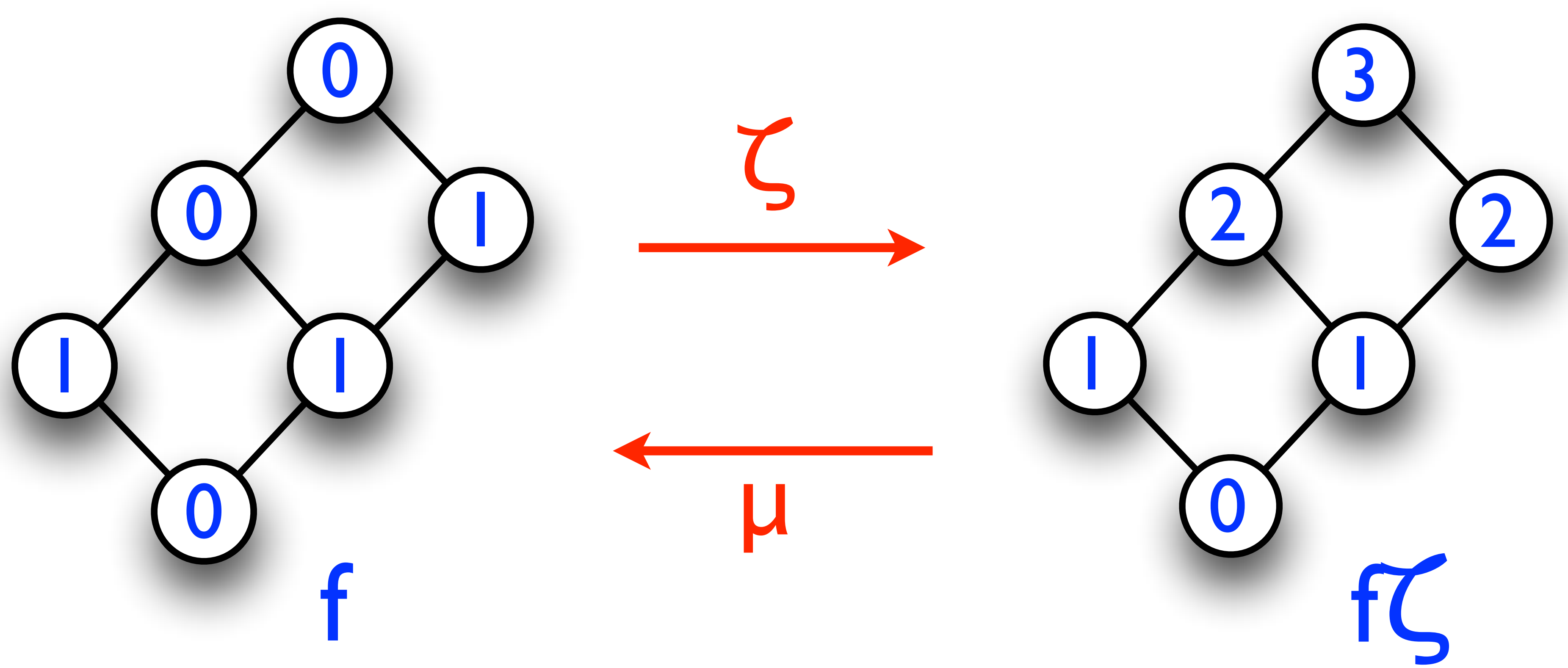
Nonzero
join-irreducibles
= prime power divisors

Möbius inversion [Rota]

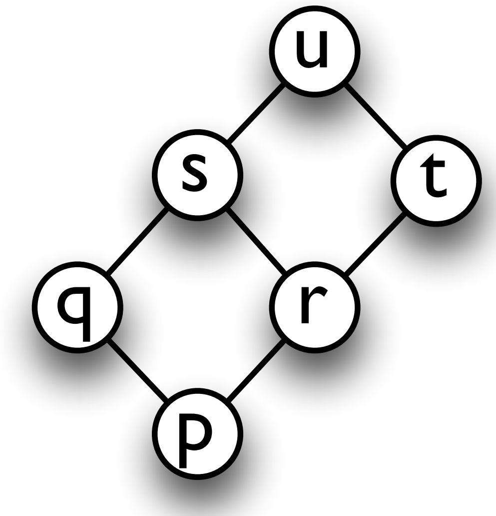
- Let $(L, \leq)$ be a lattice
- Let R be a ring

Analogy:
Zeta transform
~ Fourier transform
Möbius transform
~ inv. Fourier transform

- For $f : L \to R$, define the **zeta transform** $f\zeta : L \to R$ for all $y \in L$ by $f\zeta(y) = \sum_{x \in L : x \leq y} f(x)$
- The inverse of ζ is the **Möbius transform** μ



In the language of linear algebra

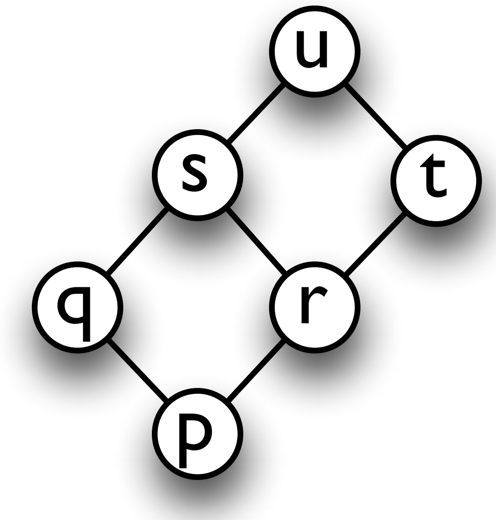


- Suppose L has v elements
- f is a row vector of length v with positions indexed by L
- ζ is a v by v matrix with $\zeta(x,y)=1$ if $x \leq y$; $\zeta(x,y)=0$ otherwise
- Zeta transform: Right-multiply f with ζ

	p	q	r	s	t	u
f	0	0	1	1	1	0
$f\zeta$	0	1	1	2	2	3

ζ	p	q	r	s	t	u
p	1	1	1	1	1	1
q	0	1	0	1	0	1
r	0	0	1	1	1	1
s	0	0	0	1	0	1
t	0	0	0	0	1	1
u	0	0	0	0	0	1

Complexity of evaluation



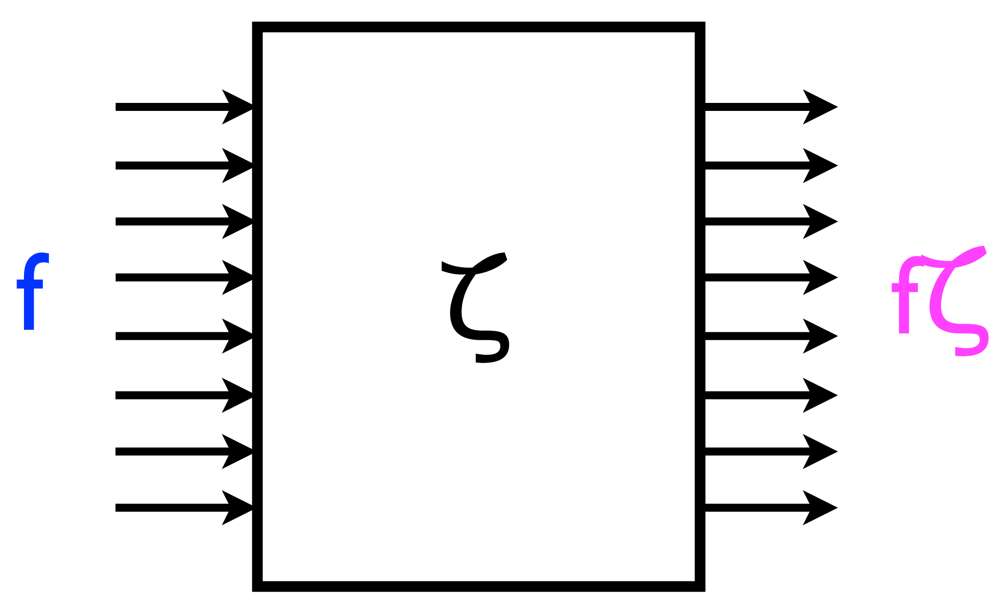
- Assume that L is fixed, $|L| = v$
- Task:
  Given $f : L \to R$ as input,
  compute $f\zeta : L \to R$
- $f\zeta$ can clearly be computed in $O(v^2)$ arithmetic operations in R
- ***But can we go faster?***

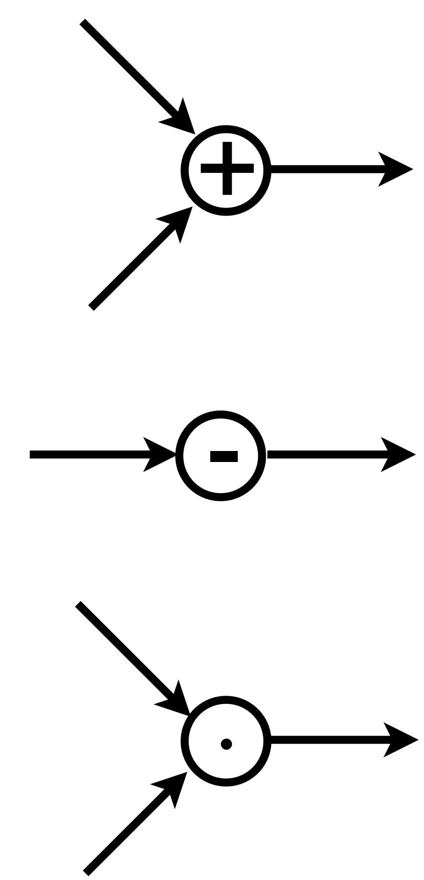
	p	q	r	s	t	u
f	0	0	1	1	1	0
fζ	?	?	?	?	?	?

ζ	p	q	r	s	t	u
p	1	1	1	1	1	1
q	0	1	0	1	0	1
r	0	0	1	1	1	1
s	0	0	0	1	0	1
t	0	0	0	0	1	1
u	0	0	0	0	0	1

Arithmetic circuits

- How many gates are sufficient / necessary in an arithmetic circuit that computes $f\zeta$ from f ?
- Trivial circuit has $O(v^2)$ gates
  ——***but do there exist smaller circuits?***





Why?

- Polynomial multiplication:

$$(1x^0+1x^1+3x^2)\cdot(1x^0+2x^1) = 1x^0+3x^1+5x^2+6x^3$$

- ... *fast* multiplication via the fast Fourier transform (FFT)

- "Lattice polynomial" multiplication:

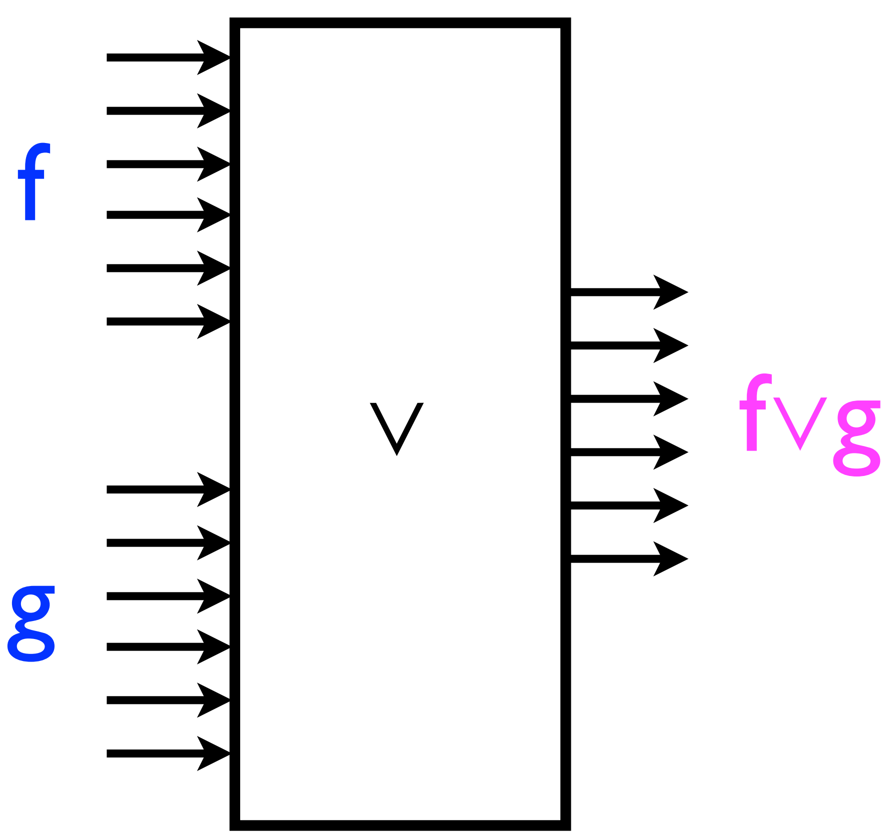
$$(1\{a,b\} + 3\{c,d\}) \cup (1\{b,c\} + 2\{d\}) =$$
$$= 1\{a,b,c\} + 3\{b,c,d\} + 2\{a,b,d\} + 6\{c,d\}$$

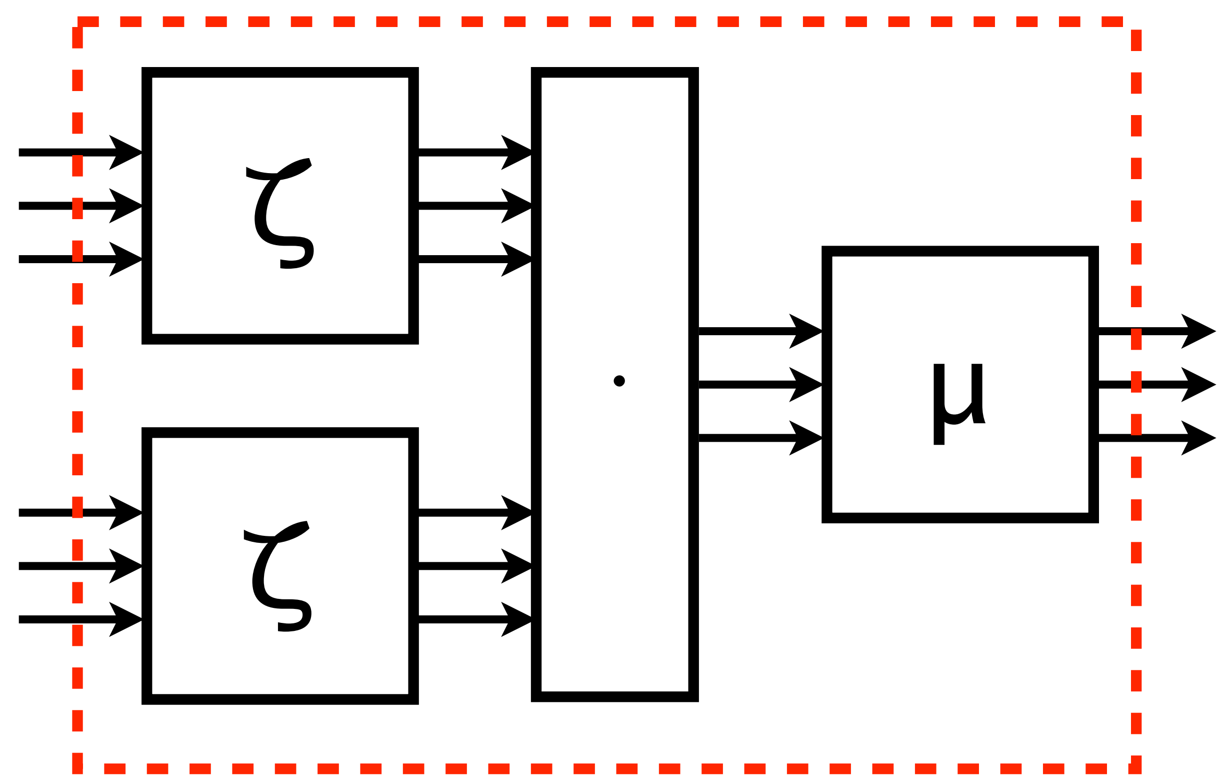
- ... *fast* multiplication via the fast zeta transform & fast Möbius transform (FZT/FMT)

Fast multiplication in the semigroup algebra of $(L,\leq)$

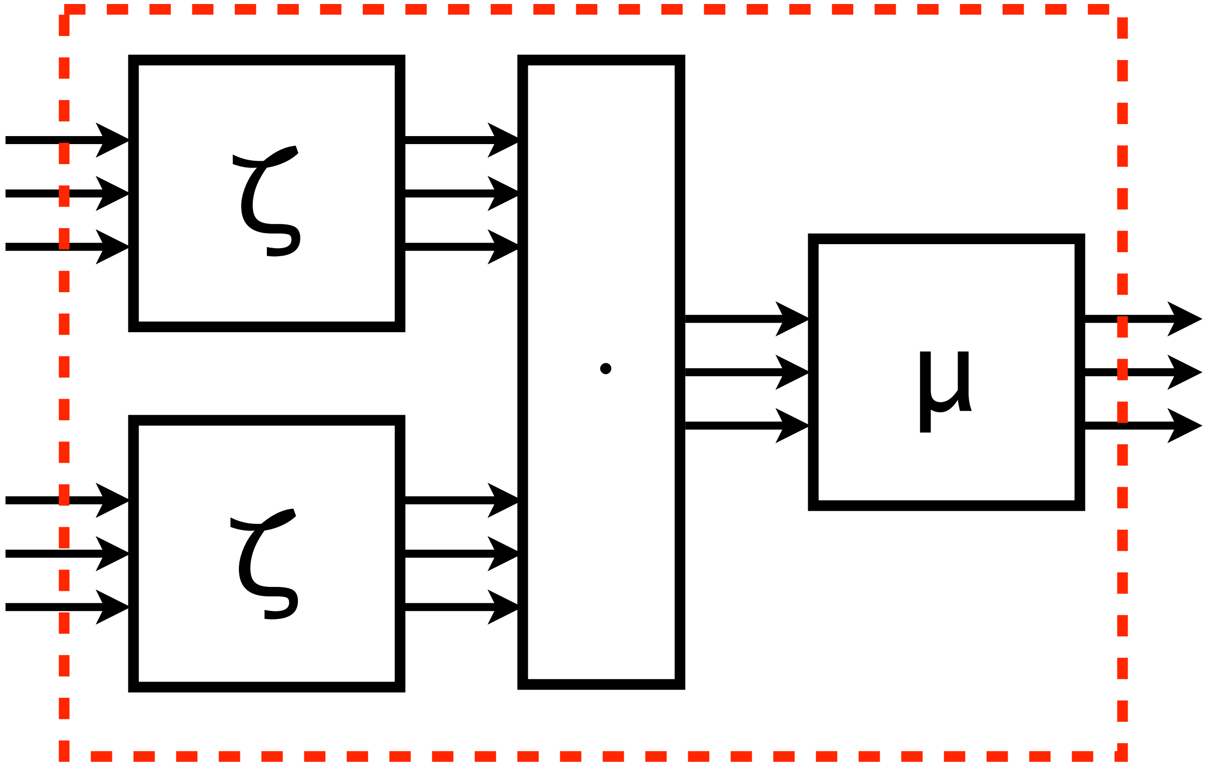
- Given $f : L \to R$ and $g : L \to R$ as input
- The product $f \vee g : L \to R$ is defined for all $z \in L$ by $f \vee g(z) = \sum_{x,y \in L\,:\,x \vee y = z} f(x)g(y)$

[Solomon 1967; Kennes 1992]





[Solomon 1967; Kennes 1992]



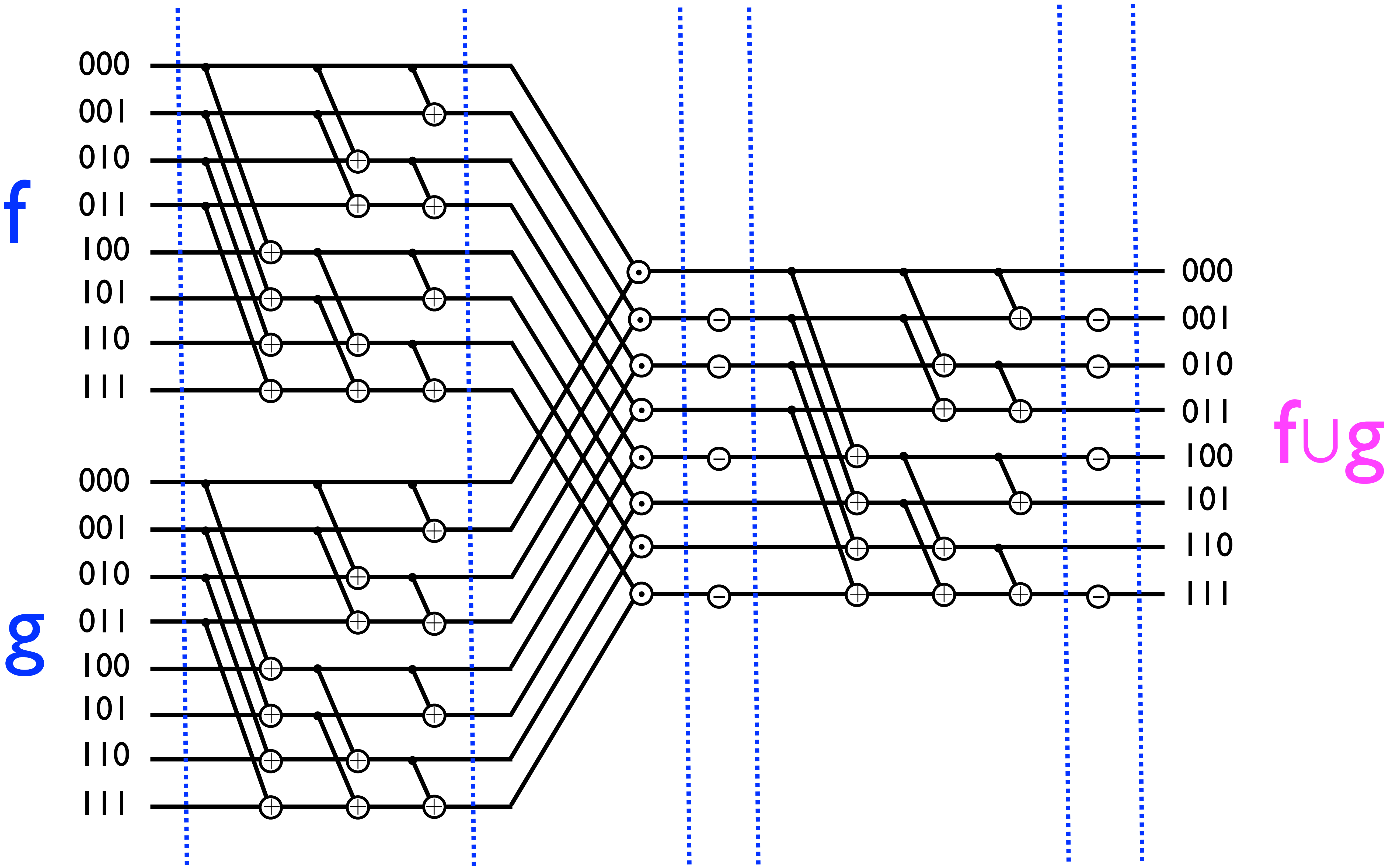
- **Claim.**

$$(f \vee g)\zeta = (f\zeta) \cdot (g\zeta)$$

- **Proof.**

$$
\begin{aligned}
(f \vee g)\zeta(u) &= \textstyle\sum_{z \in L \,:\, z \leq u} (f \vee g)(z) \\
&= \textstyle\sum_{z \in L \,:\, z \leq u} \sum_{x,y \in L \,:\, x \vee y = z} f(x)g(y) \\
&= \textstyle\sum_{x,y \in L \,:\, x \vee y \leq u} f(x)g(y) \\
&= \textstyle\sum_{x,y \in L \,:\, x \leq u,\, y \leq u} f(x)g(y) \\
&= \textstyle\sum_{x \in L \,:\, x \leq u} f(x) \sum_{y \in L \,:\, y \leq u} g(y) \\
&= f\zeta(u) \cdot g\zeta(u)
\end{aligned}
$$

Example (subset lattice, n=3)



Earlier work

- The semigroup algebra of a lattice decomposes into a direct sum of 1-dimensional subalgebras [Schwarz 1954; Hewitt & Zuckerman 1955]
- The zeta transform is an algebra isomorphism from standard representation to the direct sum [Solomon 1967]
- Algorithmic significance: Fast multiplication algorithm (for the subset lattice), discovered in the context of automating Dempster–Schafer theory [Kennes 1992; Yates 1937]

Applications

- (Currently fastest) exact algorithms for many hard problems such as graph colouring
  [Björklund, Husfeldt & Koivisto 2009]
- Constructing FFTs for inverse semigroups
  [Malandro & Rockmore 2010]
- Analysis of Markov chains on semigroups
  [Bidigare, Hanlon & Rockmore 1999; Brown 2000; Brown & Diaconis 1998]

Earlier work (upper bounds)

- Trivial upper bound $O(v^2)$
- There exists an arithmetic circuit of size $O(v \log v)$ for the zeta transform on the subset lattice of an n-element set, $v = 2^n$ [Yates 1937]
- There exists an arithmetic circuit of size $O(v \log^3 v)$ for the zeta transform on the poset structure of the rook monoid R_n, $v = |R_n|$ [Malandro 2010]

Earlier work (lower bounds)

- Trivial lower bound $\Omega(v)$
- Most lattices with v elements have zeta circuits of size $\Omega(v^{3/2} / \log v)$ [Klotz and Lucht 1971]
- Every monotone circuit for the zeta transform on a lattice L with e edges in the lattice diagram has $\Omega(e)$ gates [Kennes 1992]

Main result



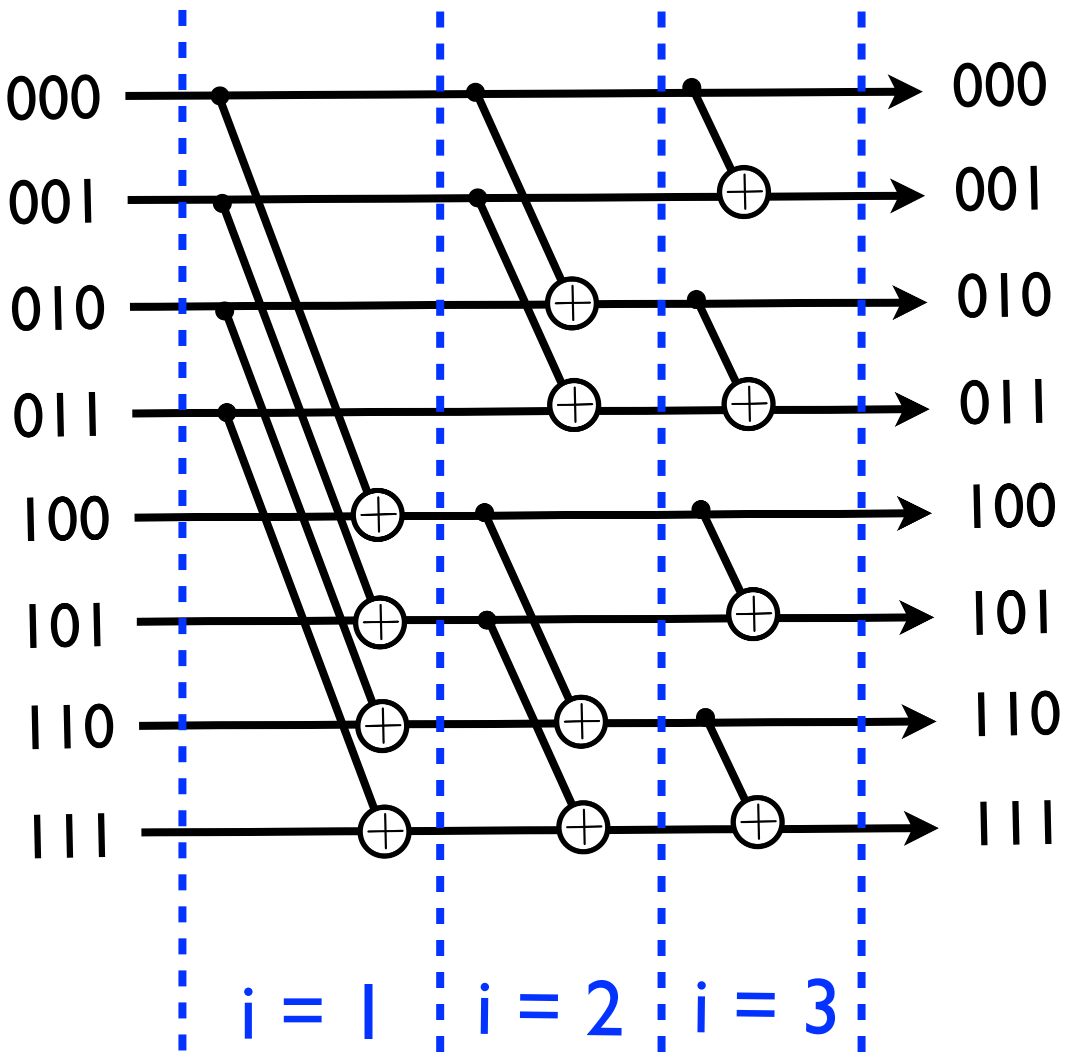



- Let $(L, \leq)$ be a lattice with v elements, n of which are *nonzero* and *join-irreducible*
- Then, there exist arithmetic circuits of size $O(vn)$ both for the zeta transform on L and for the Möbius transform on L
- (The claim holds also if *join-irreducible* is replaced with *meet-irreducible*)

Motivation: Many combinatorially useful lattices have $n = O(\text{polylog } v)$

Yates's circuit for ($\{0,1\}^n$,$\subseteq$)

Example: n = 3



- The output at $y \in \{0,1\}^n$ is the sum of values at all inputs $x \in \{0,1\}^n$ with $x \subseteq y$
- Idea:
  There is a unique "ordered walk" from x to y in n steps, where step i = 1,2,...,n changes coordinate i (if necessary)

Graph coloring

Graph coloring

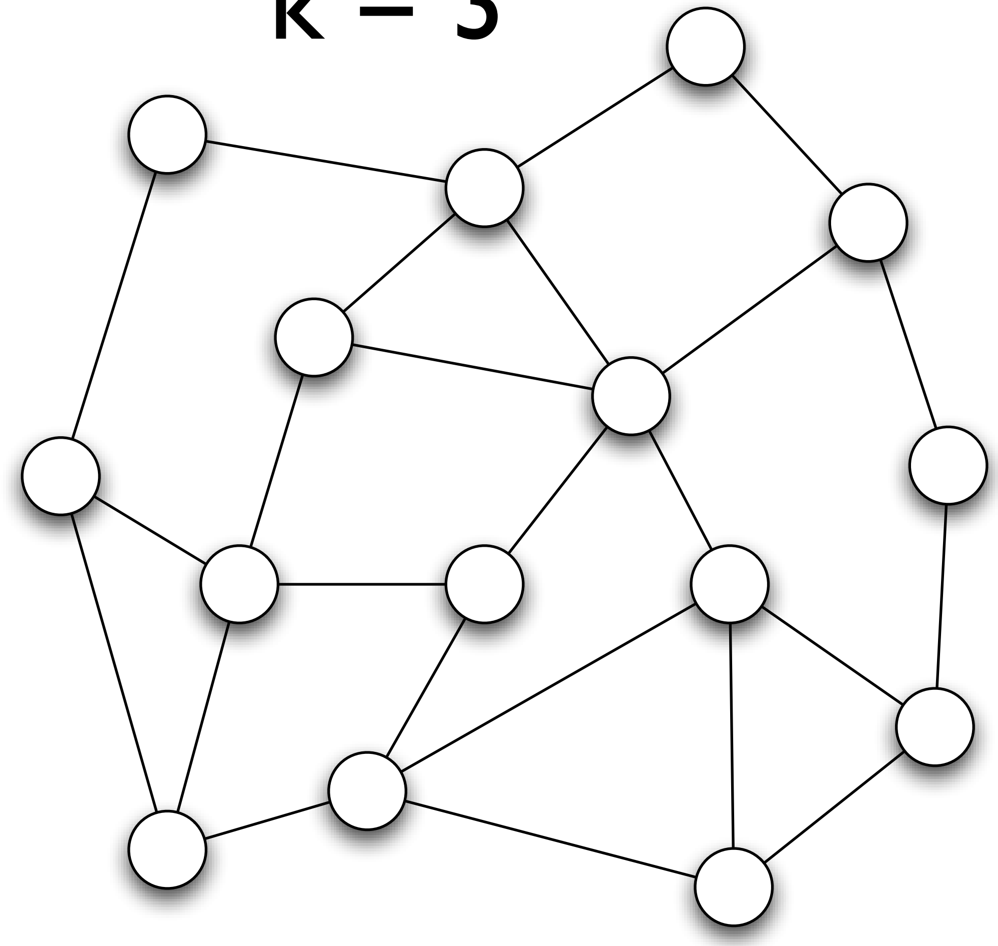
Input:

1. A graph G with n vertices
2. An integer k

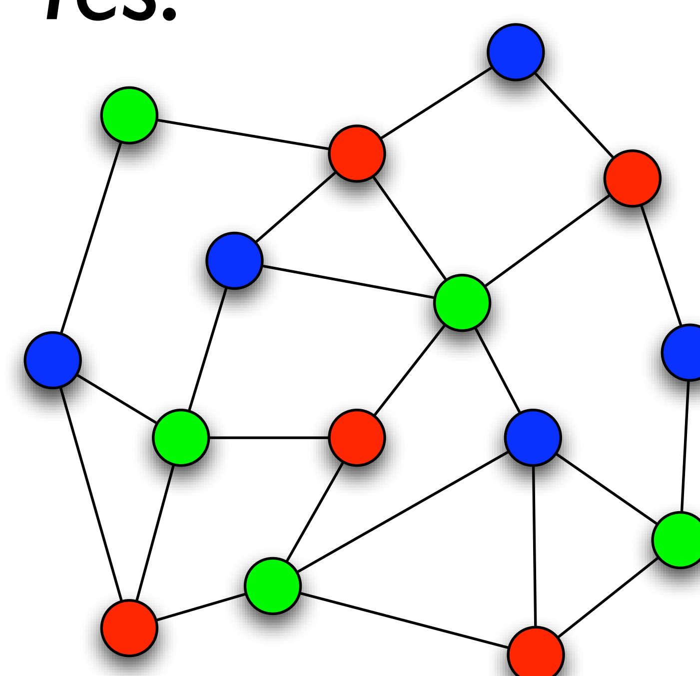
Question:

Can the vertices of G be colored with k colors such that no edge is monochromatic?

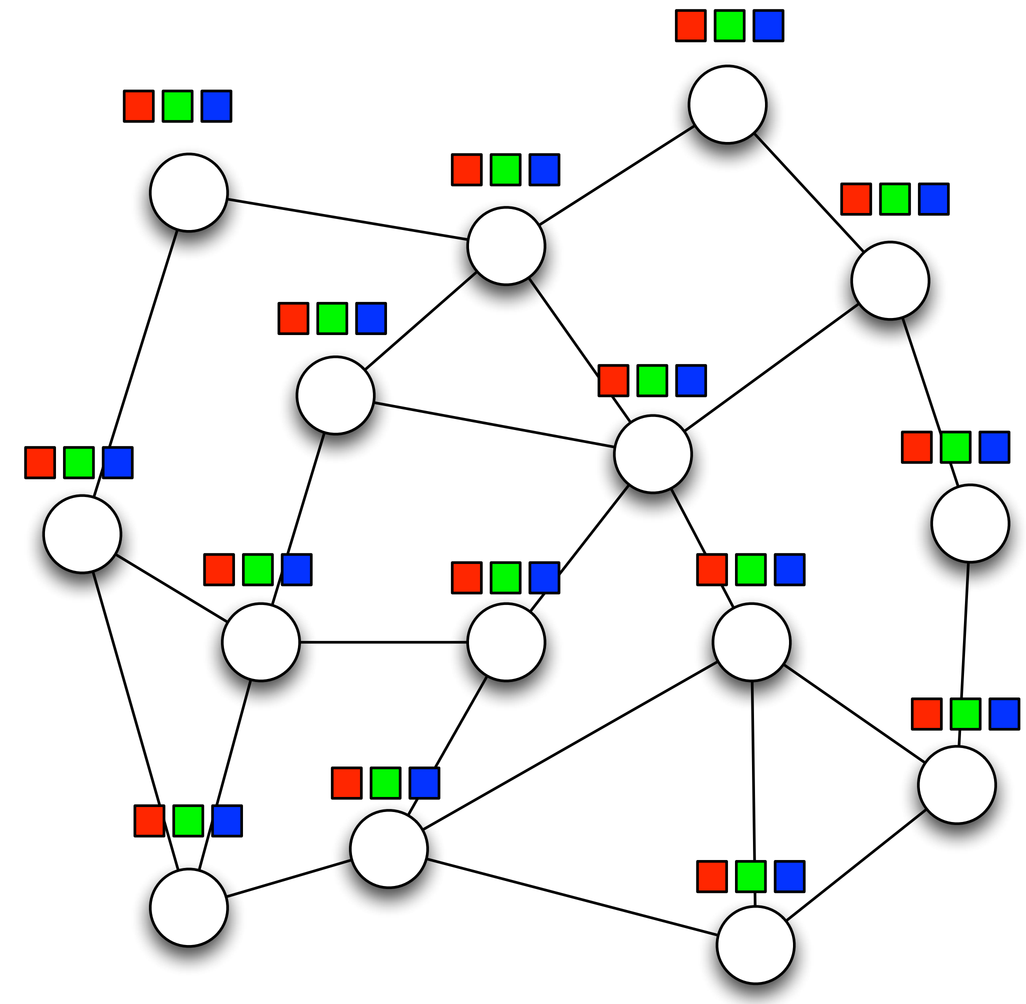
k = 3



Yes:



Coloring by brute force



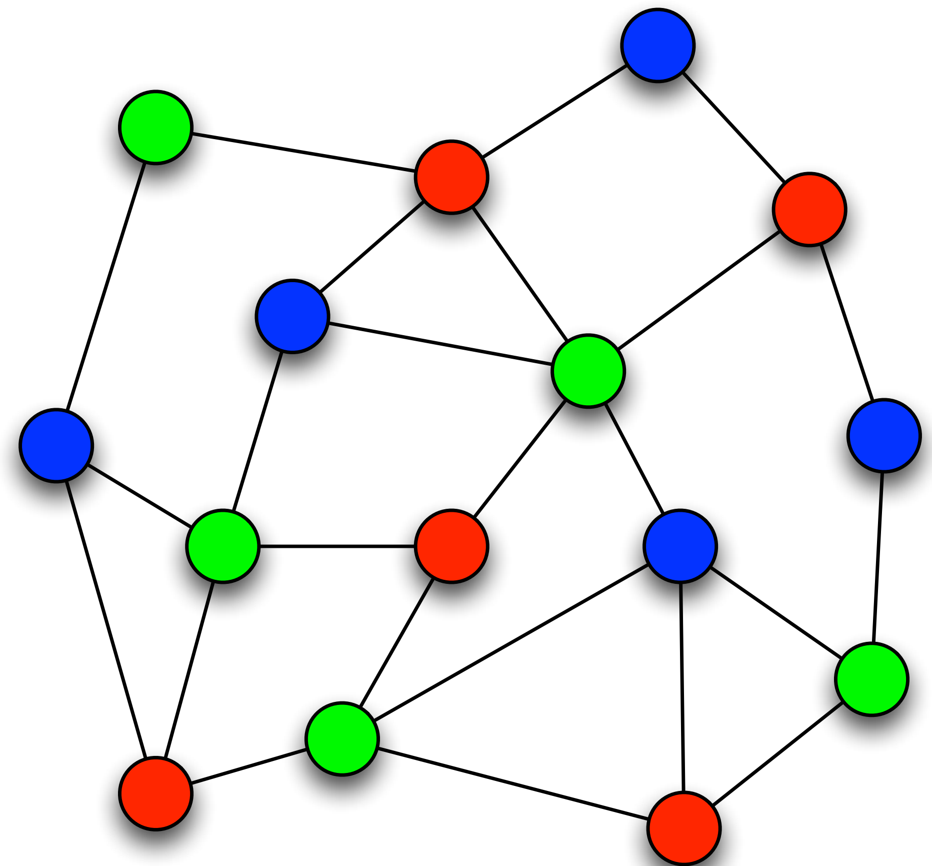
There are k^n ways to color the vertices
— try out all possible colorings in time $O^*(k^n)$

[The $O^*(\ )$-notation suppresses factors polynomial in the input size, e.g. $O^*(k^n) = O(k^n \mathrm{poly}(n))$.]

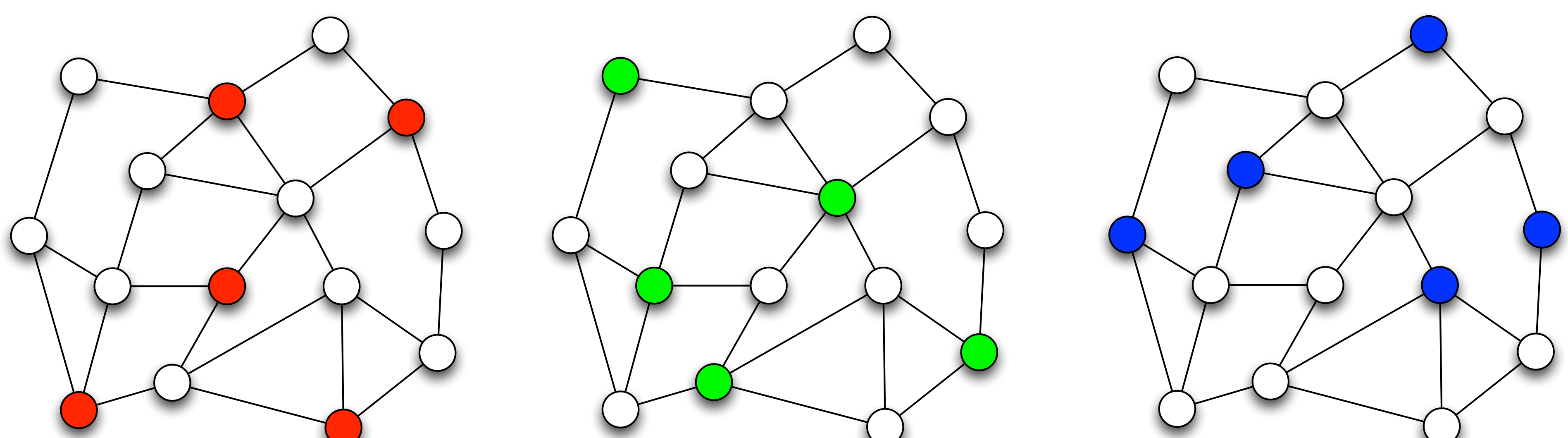
Current best
for graph coloring:

$O^*(2^n)$ time

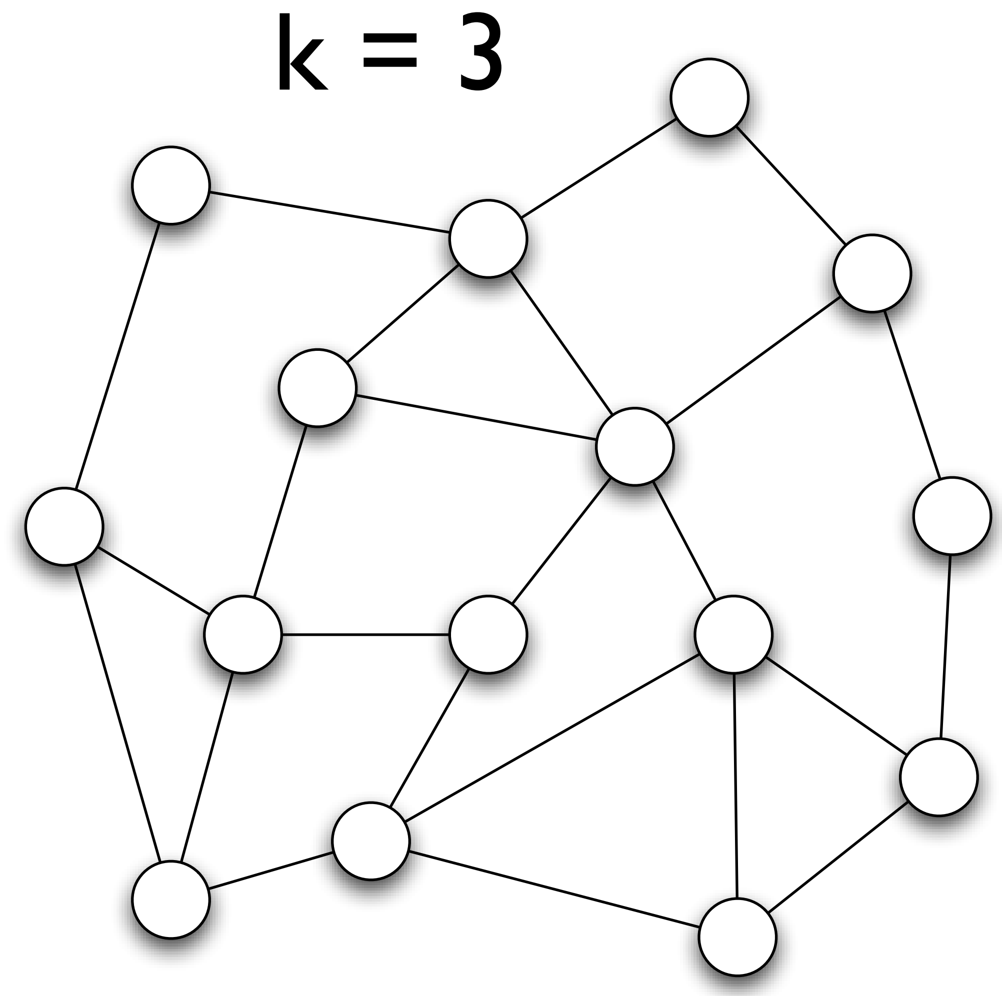
[Björklund–Husfeldt–
Koivisto 2009]



Every k-coloring partitions the vertices of G into k sets (S_1, S_2, ..., S_k), each of which is an independent set in G



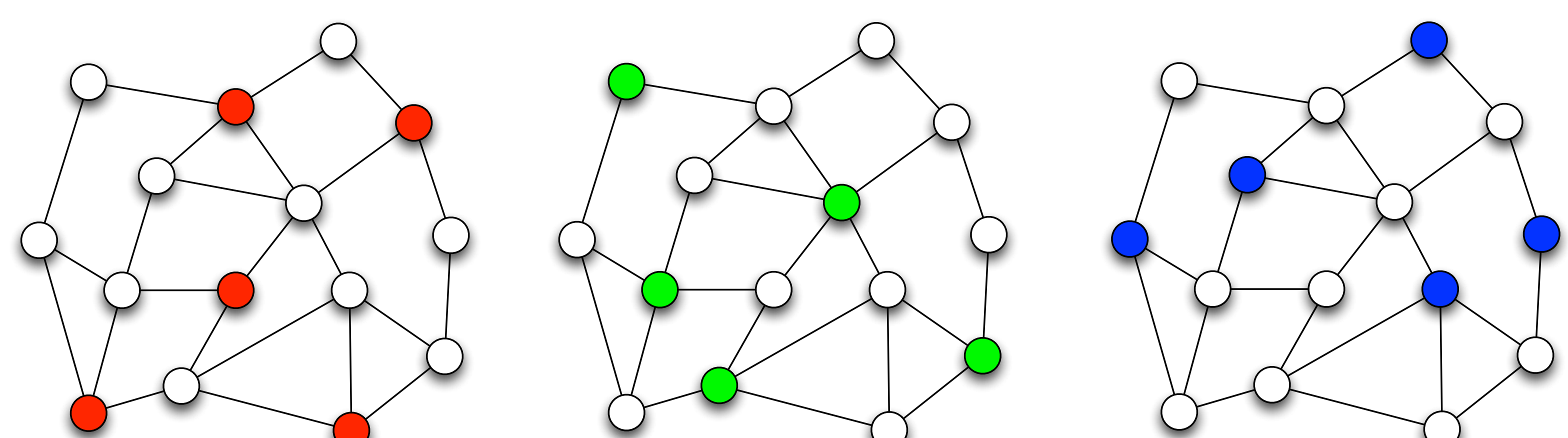
Graph coloring (restated)



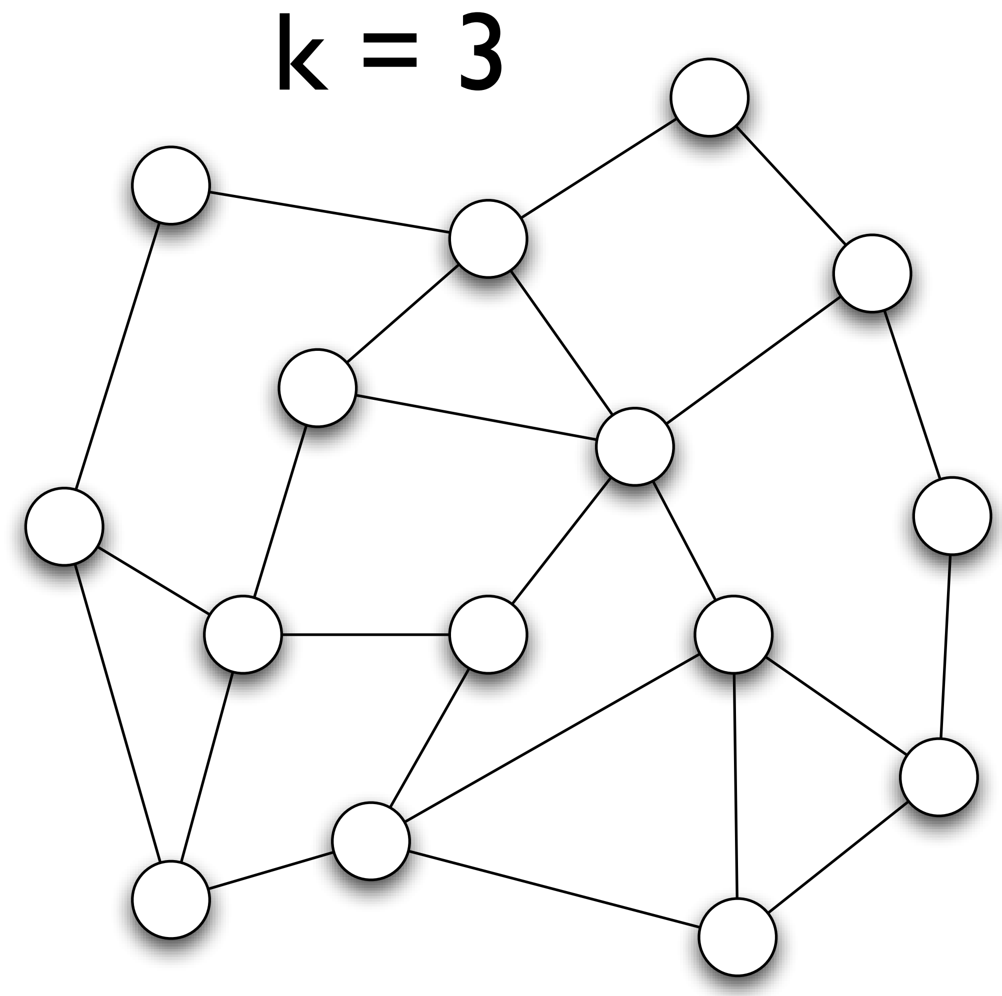
Question:

Can the vertices of G be partitioned into k sets (S_1, S_2, ..., S_k), each of which is an independent set?

Yes:



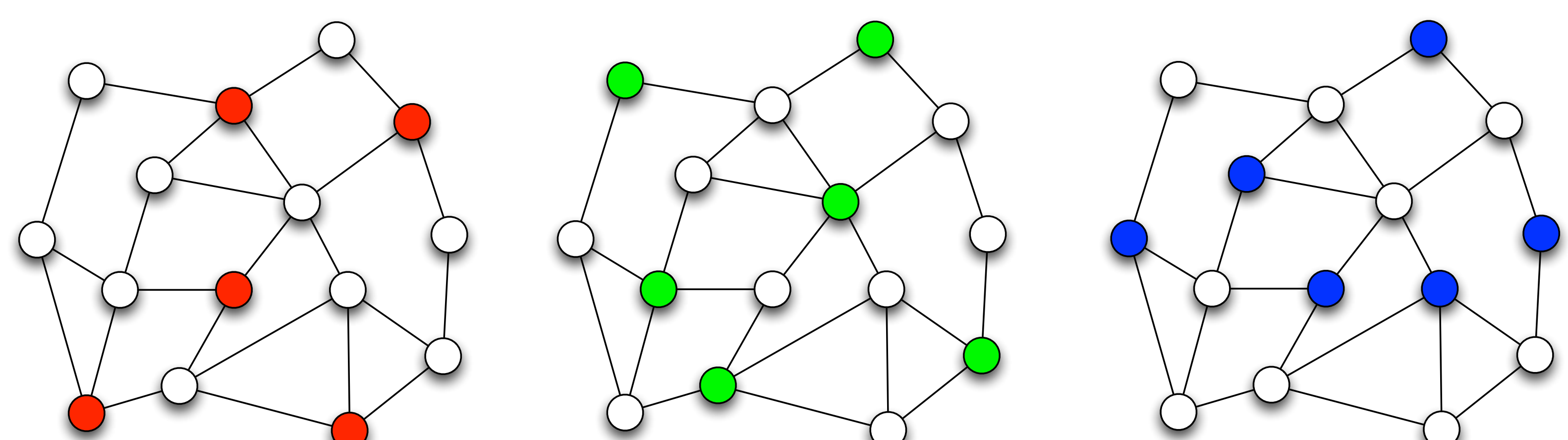
Graph coloring (restated again)



Question:

Do there exist independent sets $(S_1, S_2, \ldots, S_k)$ with $S_1 \cup S_2 \cup \ldots \cup S_k = V$?

Yes:



Set Cover (Dense)

Input:

1. A family $\mathcal{F}$ of subsets of $[n]=\{1,2,\ldots,n\}$
2. An integer k

Question:

Does there exist a k-tuple $(S_1, S_2, \ldots, S_k) \in \mathcal{F}^k$ such that $S_1 \cup S_2 \cup \ldots \cup S_k = [n]$?

Note:

To solve graph coloring, let $\mathcal{F}$ consist of the independent sets of G — we have $|\mathcal{F}| \leq 2^n$

#Subset Cover (Dense)

Input:

1. A family $\mathcal{F}$ of subsets of $[n]=\{1,2,\ldots,n\}$
2. An integer k

Output:

For each $Z \subseteq [n]$, the number $c_k(Z)$ of k-tuples $(S_1, S_2, \ldots, S_k) \in \mathcal{F}^k$ such that $S_1 \cup S_2 \cup \ldots \cup S_k = Z$

Idea:

Assume $c_{k-1}(Z)$ is available for each $Z \subseteq [n]$

— using this data, compute $c_k(Z)$ for each $Z \subseteq [n]$

The union product

- Identify subsets of $[n]$ with binary strings in $\{0,1\}^n$
- Let R be a ring (e.g. the integers)
- Let $f : \{0,1\}^n \to R$ and $g : \{0,1\}^n \to R$
- Define the **union product** $f \cup g : \{0,1\}^n \to R$ for all $Z \subseteq [n]$ by

$$f \cup g(Z) = \sum_{X,Y \in \{0,1\}^n \,:\, X \cup Y = Z} f(X) g(Y)$$

To solve #Subset Cover:

1) Let f be an indicator function for $\mathcal{F} \subseteq \{0,1\}^n$
2) Then $c_1 = f$, and $c_k = c_{k-1} \cup f$ for $k = 2,3,\ldots$

- Given $f : \{0,1\}^n \to R$ and $g : \{0,1\}^n \to R$ as input, the union product $f \cup g : \{0,1\}^n \to R$ can be computed in $O(2^n n)$ operations in R [Kennes 1992, Yates 1937]

- #Subset Cover can be solved in time $O^*(2^n)$ #Subset Partition can be solved in time $O^*(2^n)$ [Björklund–Husfeldt–Koivisto 2009]

- #Graph Coloring can be solved in time $O^*(2^n)$ [Björklund–Husfeldt–Koivisto 2009]

The proof in more detail

Main result

- Let (L,≤) be a lattice with v elements,
  n of which are *nonzero* and *join-irreducible*
- Then, there exist arithmetic circuits of size O(vn)
  both for the zeta transform on L
  and for the Möbius transform on L
- (The claim holds also if *join-irreducible*
  is replaced with *meet-irreducible*)

Motivation: Many combinatorially useful
lattices have n = O(polylog v)

Proof outline

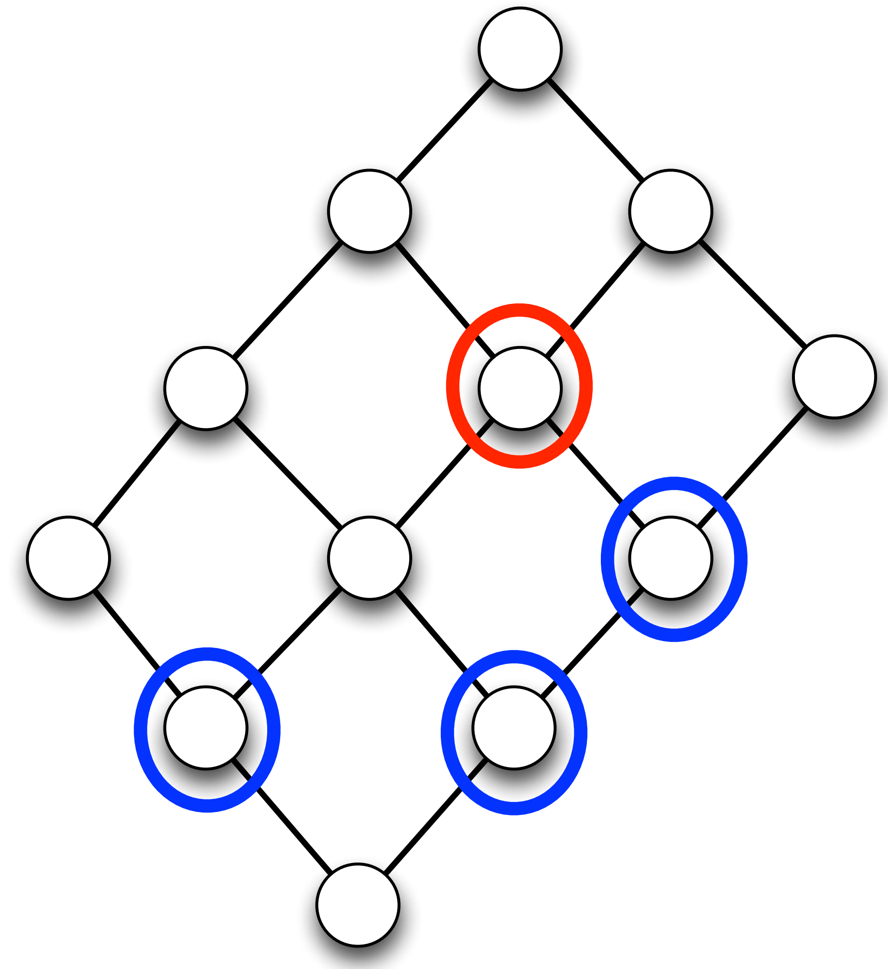
- Let (L,≤) be a lattice with v elements,
and let N⊆L be the n nonzero join-irreducibles
- Denote by $\mathcal{P}$(N) the set of all subsets of N
- Step 1 (basic lattice theory):
Embed (L,≤) into ($\mathcal{P}$(N),⊆) via the "spectrum map" $\mathcal{S}$
- Step 2 (basic lattice theory):
Because the image $\mathcal{F}=\mathcal{S}$(L) is intersection-closed in $\mathcal{P}$(N), there is a unique closure operator on $\mathcal{P}$(N) with image $\mathcal{F}$
- Step 3 (novel circuits for ∩- or ∪-closed set families):
Construct circuits for the zeta & Möbius transforms on ($\mathcal{F}$,⊆) by taking closure of ordered walks on ($\mathcal{P}$(N),⊆)

1.

- Define the **spectrum map** $\mathcal{S} : \mathrm{L} \to \mathcal{P}(\mathrm{N})$ for all $x \in \mathrm{L}$ by

$$\mathcal{S}(x) = \{\, i \in \mathrm{N} : i \leq x \,\}$$

- **a)** $x = \vee \mathcal{S}(x)$ for all $x \in \mathrm{L}$
- **b)** $x \leq y$ iff $\mathcal{S}(x) \subseteq \mathcal{S}(y)$ for all $x,y \in \mathrm{L}$
- **c)** $\mathcal{S}(x \wedge y) = \mathcal{S}(x) \cap \mathcal{S}(y)$ for all $x,y \in \mathrm{L}$



$\mathcal{S}(x)$ = "nonzero join-irreducibles below x"

- $\mathcal{S}$ is an order-isomorphism from $(\mathrm{L},\leq)$ to $(\mathcal{S}(\mathrm{L}),\subseteq)$
- The image $\mathcal{F}=\mathcal{S}(\mathrm{L})$ is *intersection-closed:* $\mathrm{N} \in \mathcal{F}$ and for all $A,B \in \mathcal{F}$ it holds that $A \cap B \in \mathcal{F}$

2.

- A **closure operator** on $(\mathcal{P}(N), \subseteq)$ is a map $\perp : \mathcal{P}(N) \to \mathcal{P}(N)$ such that for all A,B $\subseteq$ N it holds that
  1) $A \subseteq \perp(A)$,
  2) $A \subseteq B$ implies $\perp(A) \subseteq \perp(B)$, and
  3) $\perp(A) = \perp(\perp(A))$
- The image $\perp(\mathcal{P}(N))$ of a closure operator is intersection-closed
- Conversely, every intersection-closed family $\mathcal{F} \subseteq \mathcal{P}(N)$ defines a unique closure operator $\perp$ whose image is $\mathcal{F}$

3. Construction (1/2)

- Let $\mathcal{F} \subseteq \{0,1\}^n$ be intersection-closed
- Key ideas:
  – Imitate Yates's construction on $\{0,1\}^n$
  – "Project" the construction using $\perp$: $\{0,1\}^n \rightarrow \mathcal{F}$
- Let $x,y \in \mathcal{F}$ with $x \subseteq y$ and let

$$x = w(0) \subseteq w(1) \subseteq \ldots \subseteq w(n) = y$$

be the ordered walk from x to y in $\{0,1\}^n$

- Then, the "projection"

$$x = \perp(w(0)) \subseteq \perp(w(1)) \subseteq \ldots \subseteq \perp(w(n)) = y$$

is a walk from x to y in $\mathcal{F}$

3. Construction (2/2)

- An analysis of the projected walks gives a recurrence on $\mathcal{F}$ that can be evaluated in n steps i = 1,2,...,n analogously to Yates's circuit

- Circuit for the Möbius transform on $(\mathcal{F},\subseteq)$
  — The recurrence for the zeta transform on $(\mathcal{F},\subseteq)$ can be inverted by proceeding in order of increasing size through the sets in $\mathcal{F}$

- Dual result (for a union-closed family $\mathcal{F}$):
  — Elementwise complement of $\mathcal{F}$ is intersection-closed
  — Traverse the walk from x to y with x⊆y in reverse order from y to x

Summary & Further work

- **Main result:**
  There exist arithmetic circuits of size $O(vn)$ for the zeta & Möbius transforms on $(L,\leq)$ with v elements and n nonzero join-irreducibles
- Can we go faster?
  —Are there smaller circuits?
- Is there a family of lattices L that does not admit (monotone) circuits of size $O(e)$, where e is the number of edges in the diagram of L ?
- Further parallels between Möbius inversion and Fourier analysis?