László Csirmaz

CEU & Rényi Institute

Secret Sharing on infinite graphs

2006, NyírCrypt

Definition: a *Perfect Secret Sharing on the graph G* is a joint distribution

$$\underbrace{\xi_{v_1}, \xi_{v_2}, \ldots, \xi_{v_n}}_{\text{vertices}}, \underbrace{\quad \xi_s \quad}_{\text{secret}}, \text{ where:}$$

- ξ_v is the *share* of $v \in V$,
- each edge can recover (=determine) the secret s,
- $A \subseteq V$ is independent $\Rightarrow$ $\{\xi_v : v \in A\}$ and ξ_s are independent as random variables.

Definition: $\mathrm{R}(G)$, the *worst case information rate of G* is

$\mathrm{H}(A) =$ entropy of $\{\xi_v : v \in A\}$

$\dfrac{\mathrm{H}(\xi_v)}{\mathrm{H}(\xi_s)} =$ how many bits should v remember.

$$\mathrm{R}(G) \stackrel{\text{def}}{=} \min_{\text{scheme}} \max_{v \in V} \frac{\mathrm{H}(\xi_v)}{\mathrm{H}(\xi_s)}$$

Claim: $\mathsf{R}(G) \geq 1$ *if G is not empty.* ∎

Claim (Shamir): $\mathsf{R}(K_n) = 1$. ∎

Theorem (Stinson): *$G_i \subseteq S$, $\mathcal{S}_i$ is on G_i; $\mathcal{S}_i$ assigns $\mathcal{S}_i(v)$ bits to $v \in V$. Each edge is covered $\geq k$ times. Then there is a scheme which assigns*

$$\frac{1}{k}\sum \mathcal{S}_i(v) \text{ bits to } v.$$ ∎

Claim: *If G' is a* spanned *subgraph of G, then* $\mathsf{R}(G') \leq \mathsf{R}(G)$. ∎

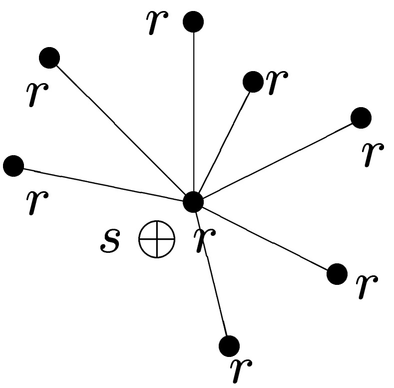
Generally not true for arbitrary subgraphs.

Definition: rate for infinite graphs:

$\mathsf{R}(G) \overset{\text{def}}{=} \sup \{ \mathsf{R}(G') : G'$ is a *finite, spanned* subgraph of $G\}$.

Claim: $\mathrm{R}(K_\infty) = 1$, $\mathrm{R}(\text{star}) = 1$.

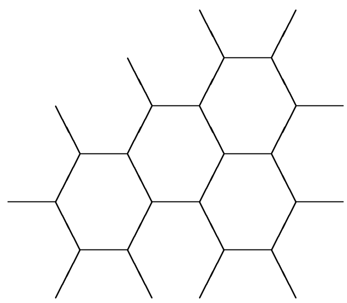
Proof: secret $s \in \{0, 1\}$,
random $r \in \{0, 1\}$



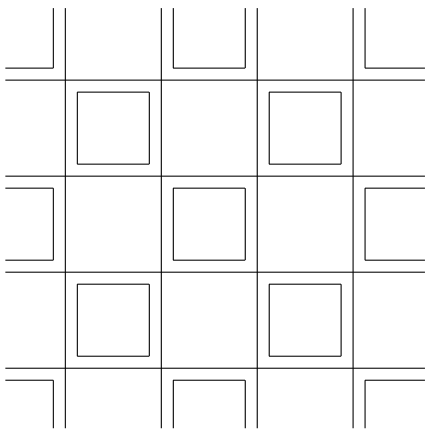
Claim: *If degree* $\leq d$ *then* $\mathrm{R}(G) \leq (d+1)/2$.

Proof: Cover G with starts from each vertex. Edges covered twice; each vertex gets $\leq d+1$ bits.

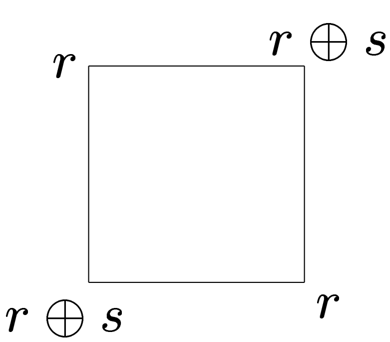
Corollary: R(honeycomb) ≤ 2.



Claim: R(lattice) ≤ 2.

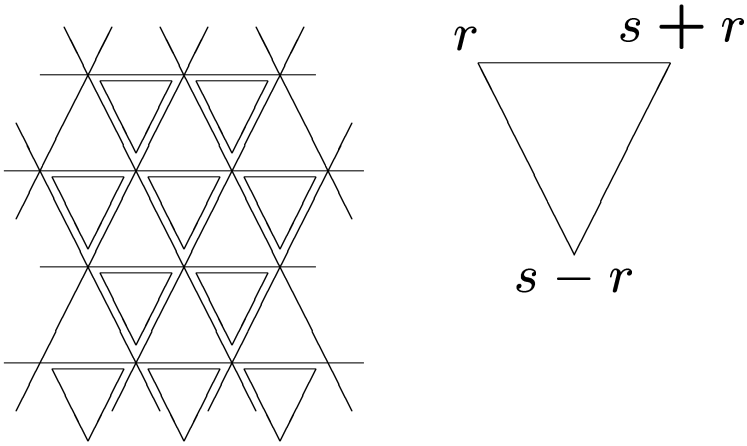


$s \in \{0, 1\}$, $r \in \{0, 1\}$



Claim: R(triangle) ≤ 3.

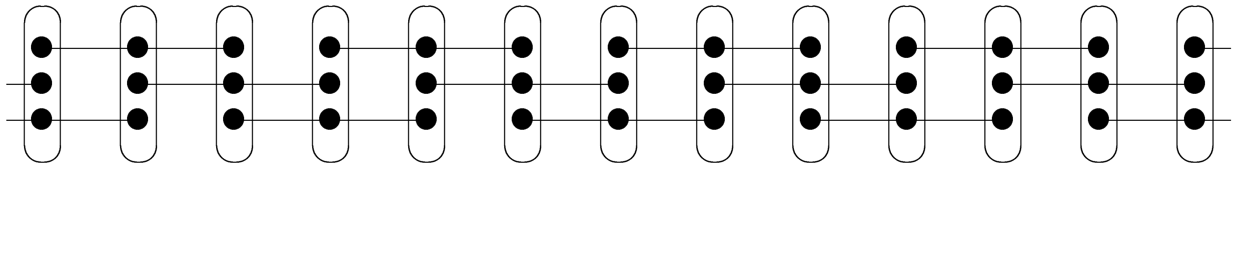
Proof:



$s \in \{0,1,2\}$
$r \in \{0,1,2\}$

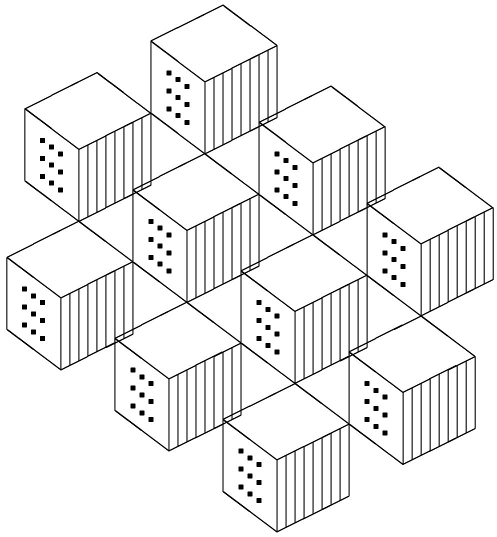
Claim: R(path) ≤ 1.5.

Proof: Each edge is covered twice, each vertex gets 3 bits:



Claim: R(3-dim lattice) ≤ 3.

Proof:



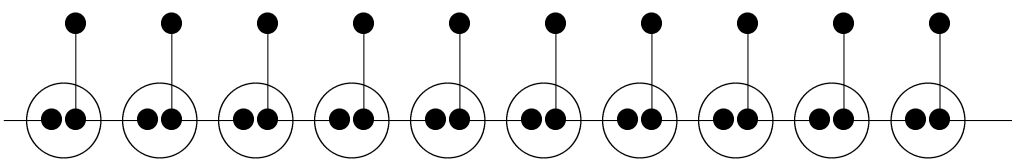
Faces of these cubes: each edge is covered twice; each vertex gets 6 bits. ∎

Claim: R(d-dim lattice) $\leq d$.

Proof: Consider 2-faces. ∎

Claim: R(rake) ≤ 2.

Proof:



Lower Bounds

Reminder: $\mathsf{H}(A) =$ entropy of $\{\xi_v : v \in A\}$

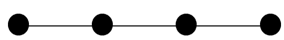
Use known linear inequalities (LP problem)

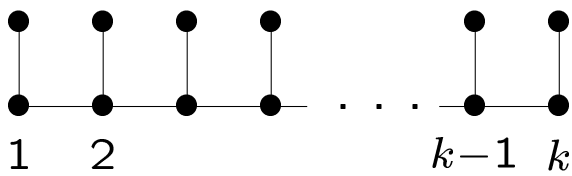
Example: For $G =$  we have $\mathsf{H}(b) + \mathsf{H}(c) \geq \mathsf{H}(bc) \geq 3$ as:

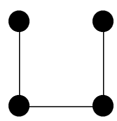
$$\begin{aligned} \mathsf{H}(abcd) &\geq \mathsf{H}(ad) + 1 \\ \mathsf{H}(ad) + \mathsf{H}(ac) &\geq \mathsf{H}(abcd) + \mathsf{H}(a) \\ \mathsf{H}(acd) + \mathsf{H}(abc) &\geq \mathsf{H}(abcd) + \mathsf{H}(ac) + 1 \\ &\vdots \end{aligned}$$

etc.

Claim: R(path) = 1.5

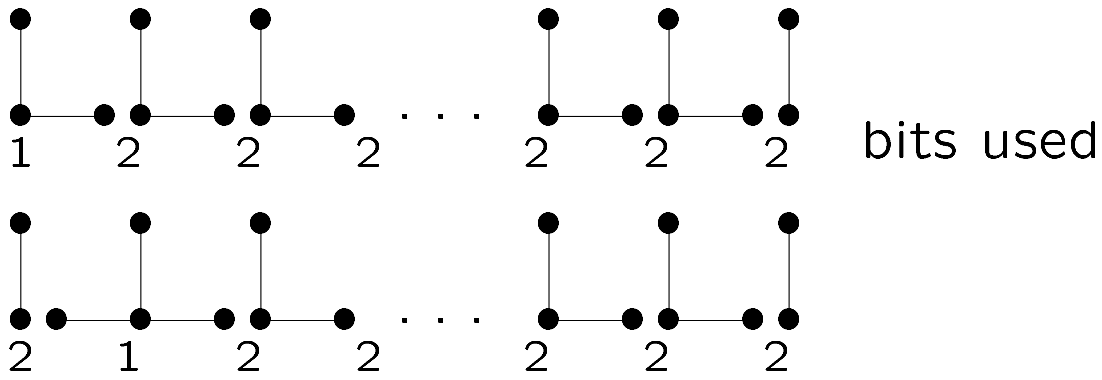
Proof: Contains  as spanned subgraph. ∎

Definition: Rake$_k$: 

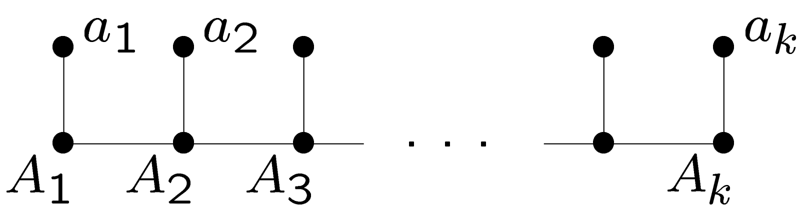
Rake$_2$: 

Theorem: $\mathsf{R}(\mathsf{Rake}_k) = 2 - 1/k$.

Proof: $\leq$ by example. Summing up all k sharings below, 1 bit is missing at every bottom node:



$\geq$:

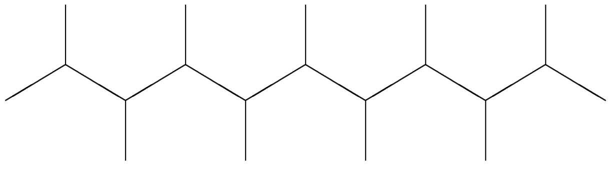


$$\sum_{i=1}^{k} \mathsf{H}(A_i) \geq \mathsf{H}(A_1 A_1 \ldots A_k) + k - 2$$

$$H(A_1 A_1 \ldots A_k) \geq k + 1 \quad \blacksquare$$

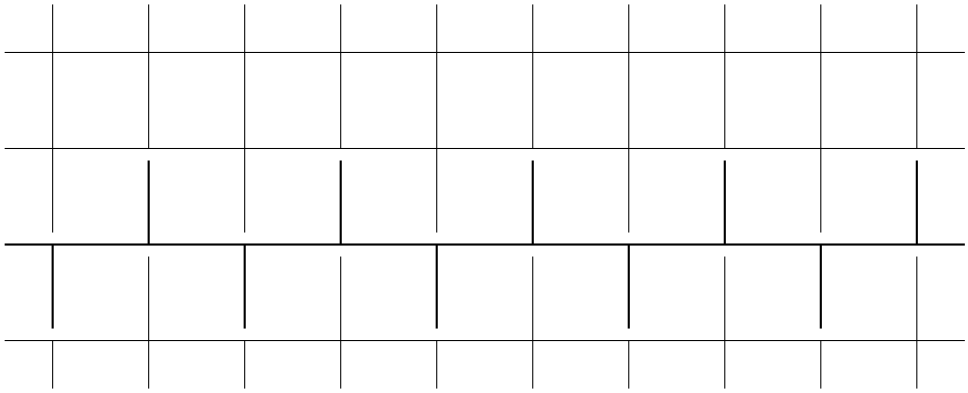
Theorem: $\mathsf{R}(\text{honeycomb}) = 2$.

Proof: Contains the infinite rake as a spanned subraph:



Theorem: R(lattice) = 2.

Proof: The rake can be embedded, too:



Theorem: R(d-dim lattice) = d.

Proof (idea): Vertices of the cube are split as $L_k^d \cup R_k^d$; both are independent.

$$(*) \sum_{v \in \text{cube}} \mathsf{H}(v) \geq f(L_k^d, R_k^d) + \left(d - \frac{1}{2}\right) k^d (1 - o(1))$$

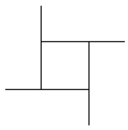
$f(,)$ is a smart expression which allows to prove $(*)$ by induction on k and d. Finally

$$f(L_k^d, R_k^d) \geq \frac{1}{2} k^d. \quad \blacksquare$$

Problems

- $2 \leq$ R(triangle lattice) ≤ 3. Exact value?

- Investigate other nice infinite graphs.

- For the rake R is **not local**, i.e. the sup is not taken. The 2-dimensional lattice **is local**, as R() = 2. What happens in higher dimenions? Is the honeycomb local?

- Limits of the entropy method: for this graph the best lower bound is 7/4. Is it the truth?