

Erdős, Dissociated sets, and Lattices

Thomas Bloom

Manchester University

VANTAGE

29th September 2026

- The actual result I will talk about is entirely generated by AI, just given the problem as a prompt.
- The exposition/presentation I will present here is 'joint work' from myself and GPT.
- (GPT's involvement in the latter has been largely explaining the AI proof, which was written in Lean, and fact-checking. Everything in these slides is written by me.)

- 1931: Charlie Chaplin's 'City Lights' premieres; the Empire State Building is opened; Al Capone is put on trial; and an 18 year old Paul Erdős is a student at the University of Budapest.



- In this year he asked maybe the first 'Erdős problem'.

Definition

A finite set A of positive integers is called dissociated if all the 2^n possible subset sums are distinct.

- For example, $A = \{1, 2, 4, \dots, 2^{n-1}\}$ is dissociated.
- This is a dissociated set of size n in $[1, 2^n)$.
- This is not always the best possible: for example in $[1, 8)$ instead of $\{1, 2, 4\}$ we also have $\{3, 5, 6, 7\}$.
- But Erdős conjectured that, at least up to constants, the powers of 2 are as dense as possible.
- In later life Erdős dated this question to 1931, and called it 'perhaps my first serious problem'.

Conjecture (Erdős)

If $A \subseteq [1, X]$ is a dissociated set of size n then $X \gg 2^n$.

- $A = \{1, \dots, 2^{n-1}\}$ show that $X \leq 2^{n-1}$ is possible.

Conjecture (Erdős)

If $A \subseteq [1, X]$ is a dissociated set of size n then $X \gg 2^n$.

- Erdős repeated this question many times; he offered \$500 for a solution.
- He seemed confident that $X \gg 2^n$. Some experimentation justifies this – it is computationally hard to find dissociated sets substantially denser than the powers of 2!

Lemma

If $A \subseteq [1, X]$ is a dissociated set of size n then $X \gg 2^n/n$.

Proof.

There are 2^n distinct subset sums of A , all integers in the interval $[0, nX]$. Therefore $nX \gg 2^n$. □

Lemma (Erdős-Moser)

If $A \subseteq [1, X]$ is a dissociated set of size n then $X \gg 2^n / \sqrt{n}$.

Proof.

Consider

$$\sum_{c \in \{-1, 1\}^n} \left(\sum_{a \in A} c_a a \right)^2.$$

Expanding the square and rearranging, this is equal to

$2^n \sum_{a \in A} a^2 \ll 2^n n X^2$. But it is the sum of 2^n distinct integers, so is $\gg 2^{3n}$. Rearranging gives the result. □

- There are now a number of different proofs of $X \gg 2^n/\sqrt{n}$ (with some improvements in the explicit constant): Guy, Elkies, Bae, Aliev, Elkies-Gleason, and most recently Dubroff, Fox, and Xu, who proved in fact

$$X \geq \binom{n}{\lfloor n/2 \rfloor} = (\sqrt{2/\pi} - o(1)) \frac{2^n}{\sqrt{n}}.$$

- But progress stalled there for a long time – far from Erdős' (nearly 100 year old) conjecture that $X \gg 2^n$.

- The trivial $A = \{1, \dots, 2^{n-1}\}$ achieves $X \leq \frac{1}{2}2^n$.
- Previous improvements to this upper bound have come from blowing up small examples: if $A \subseteq [1, X]$ is a dissociated set then $2 \cdot A \cup \{1\} \subseteq [1, 2X]$ is a dissociated set of size $n + 1$, so the minimal ratio $X/2^n$ is non-increasing as a function of n .
- Conway-Guy gave a sequence which allows for $X \leq \frac{1}{4}2^n$ (for large n).
- Best previous bound, by Bohman, was $X \leq 0.2202 \cdot 2^n$.

Theorem

There exists, for all large n , a dissociated set of size n in $[1, X]$ where

$$X \ll n^{-1/3}2^n.$$

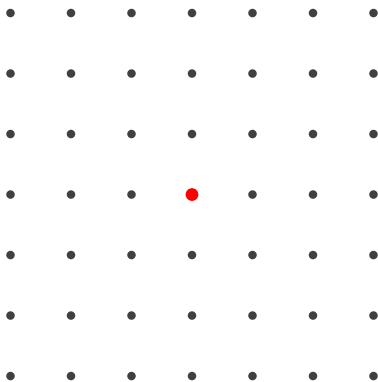
Theorem

There exists, for all large n , a dissociated set of size n in $[1, X]$ where

$$X \ll n^{-1/3} 2^n.$$

- This was proved by GPT Astra a few weeks ago.
- Actual construction/proof can be written down in a couple of pages; I can verify this line by line, but it seems very 'magical' to me, and I didn't really understand what was going on.
- Work in progress: reinterpret this in terms of lattices.

- A lattice is a discrete subgroup of $\mathbb{R}^d$ – or, if you prefer, all integer linear combinations of some set of linearly independent vectors.



- The covolume of a lattice is the area of the ‘fundamental parallelepiped’ (AKA the determinant of the matrix of the generating set of vectors). Basically how ‘dense’ the lattice is.
- Here is a natural question: given some nice set $K \subset \mathbb{R}^d$ (say convex, bounded, closed), centred at the origin, how dense a lattice can one find which intersects K only at the origin?
- (Basically equivalent to the packing question of how can one most efficiently pack translates of K in a periodic pattern.)
- The smallest covolume we can achieve for K is denoted by $\Delta(K)$ (called the critical determinant for Δ).

- ‘Easy’ general bounds are

$$2^{-n} |K| \leq \Delta(K) \leq |K|.$$

- Upper bound is basically from choosing a random lattice; this seems to have first been noted by Hlawka in 1944. (For many ‘nice’ K this can be improved to $\leq \frac{1}{2\zeta(n)} |K|$.)

- ‘Easy’ general bounds are

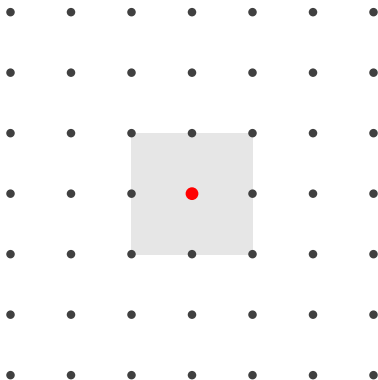
$$2^{-n} |K| \leq \Delta(K) \leq |K|.$$

- The lower bound follows from Minkowski’s theorem:

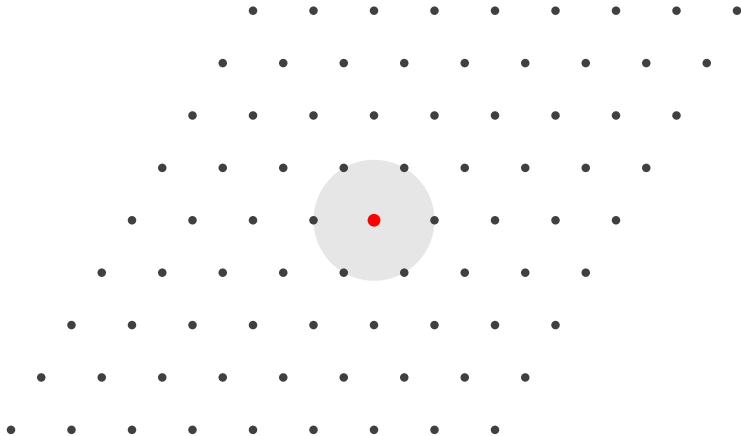
Theorem (Minkowski)

If K is a symmetric convex set with volume $> 2^n \text{covol}(\Lambda)$ then K contains a non-zero point of Λ .

- If $K = (-1, 1)^n = C_n$, the n -dimensional cube, then the lower bound is achieved: $\Delta(C_n) = 1 = 2^{-n} |C_n|$.



- If $K = S_n$ is the n -dimensional ball then this is the famous sphere-packing problem.



- We currently know

$$2^{-0.395 \dots n} |S_n| \ll \Delta(S_n) \ll n^{-2} |S_n|.$$

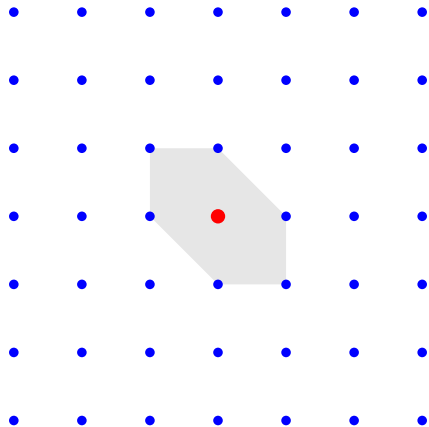
- The upper bound is due to Klartag (2026); improving on work of many others previously (all of which proved a bound of the shape $n^{-1+o(1)} |S_n|$).
- The lower bound was recently established by OpenAI, building on previous work by many others, most notably Cohn and Elkies.
- (Upper bound maybe sharp, up to logarithmic factors?)

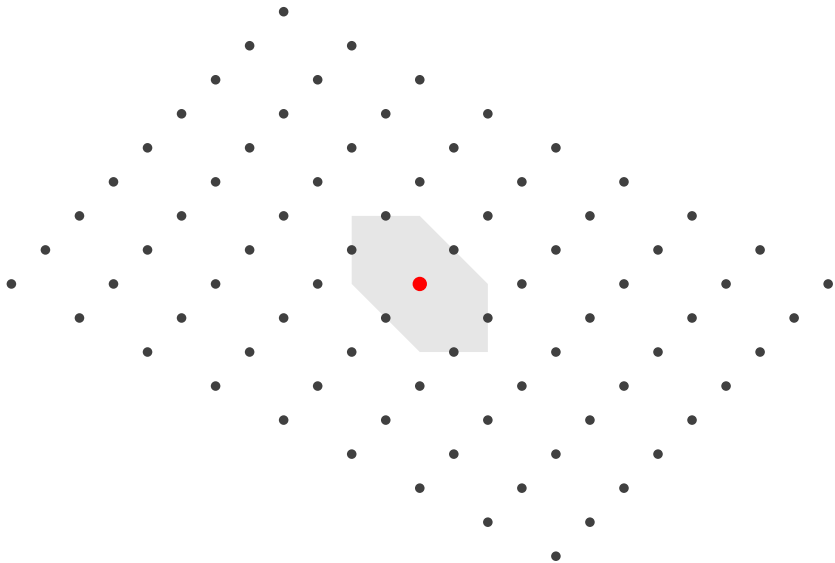
- What's this got to do with dissociated sets?
- Schinzel (perhaps) first noted the connection between dissociated sets and the 'generalised hexagon': if $\alpha \in [-1, 1]^n$ then let

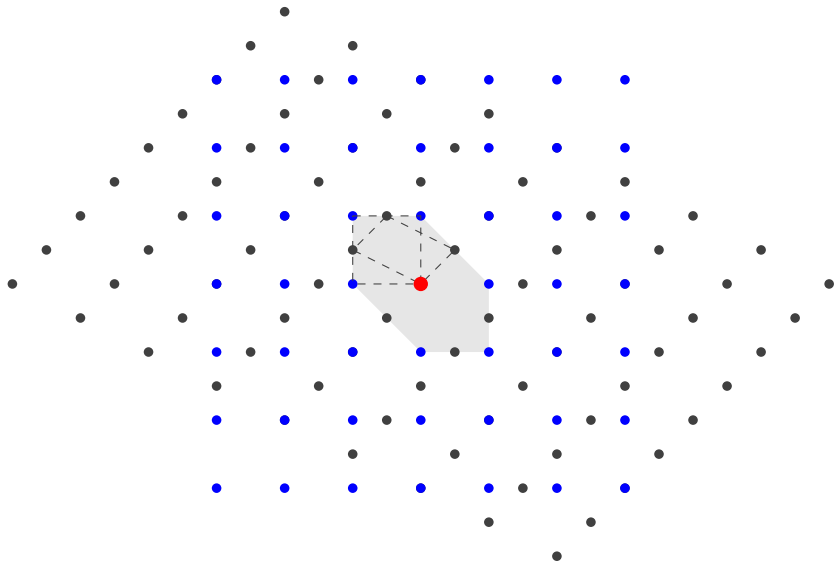
$$H_\alpha^n = \{x \in (-1, 1)^n : |\alpha \cdot x| < 1\}.$$

- We will investigate $\Delta(H_\alpha)$ – note that Schinzel conjectured that

$$\Delta(H_\alpha) \geq \Delta(H_{(1, \dots, 1)}).$$







Theorem (Aliev-Schinzel)

If $A \subseteq [1, X]$ is a dissociated set of n integers then there exists $\alpha \in \mathbb{R}^{n-1}$ such that $\|\alpha\|_\infty \leq 1$ and

$$X \geq \Delta(2 \cdot H_\alpha^{n-1}).$$

- The volume of H_α can be calculated exactly: it is $\asymp 2^n / \|\alpha\|_2 \gg 2^n / \sqrt{n}$.
- So the earlier Minkowski lower bound $\Delta(K) \geq 2^{-n} |K|$ gives an alternative proof of $X \gg 2^n / \sqrt{n}$:

$$X \gg 2^{-n} \cdot 2^n \cdot 2^n / \sqrt{n} \gg 2^n / \sqrt{n}.$$

Theorem (Aliev-Schinzel)

If $A \subseteq [1, X]$ is a dissociated set of n integers then there exists $\alpha \in \mathbb{R}^{n-1}$ such that $\|\alpha\|_\infty \leq 1$ and

$$X \geq \Delta(2 \cdot H_\alpha^{n-1}).$$

Proof.

Let $A \subseteq [1, X]$ be a dissociated set of integers of size n . Note that, without loss of generality, we can assume that $X \in A$, and that the a_i have no mutual common divisor. We use this to build a lattice $\Lambda \subset \mathbb{R}^{n-1}$ of covolume X which avoids $2 \cdot H_\alpha^{n-1}$ for some α , proving the claim. □

Proof.

Consider the lattice

$$\Lambda = \left\{ \mathbf{z} \in \mathbb{Z}^{n-1} : \sum_{i < n} a_i z_i \equiv 0 \pmod{X} \right\}.$$

This lattice has covolume X – indeed, since there is no common divisor, the map $\mathbb{Z}^{n-1} \rightarrow \mathbb{Z}/X\mathbb{Z}$ given by

$$(z_1, \dots, z_{n-1}) \mapsto \sum_{i < n} a_i z_i$$

is surjective, and hence $\mathbb{Z}^{n-1}/\Lambda \cong \mathbb{Z}/X\mathbb{Z}$. □

Proof.

Now let $\alpha = (a_1/X, \dots, a_{n-1}/X)$ and suppose $z \in \Lambda \cap 2 \cdot H_\alpha$. We know that $|z_i| < 2$ for all i , and also $z_i \in \mathbb{Z}$, and hence $z_i \in \{-1, 0, 1\}$. Now

$$z_n = -\frac{1}{X} \sum_{i < n} a_i z_i$$

is also an integer, which must be < 2 , so is also in $\{-1, 0, 1\}$. We therefore have $z_1, \dots, z_n \in \{-1, 0, 1\}$ such that

$$\sum a_i z_i = 0,$$

whence by dissociativity $z_i \equiv 0$ for all i , and so $\Lambda \cap 2 \cdot H_\alpha = \{0\}$. □

- So we know that lower bounds for Erdős' dissociated sets problem are closely related to the critical determinant of the hexagon – what about upper bounds?
- We have proved that $X \gg \Delta(2 \cdot H_{\alpha}^{n-1})$. Does the converse hold? Is it true that there exist dissociated sets of size n in $[1, X]$ where

$$X \ll \Delta(2 \cdot H_{\alpha}^{n-1})$$

for some α ? I don't know.

- ...but if we modify the definition of the critical determinant slightly then such a connection can be extracted from Astra's proof.

- Recall that $\Delta(K)$ is defined as the infimum covolume over all lattices which only intersect K at the origin.
- In the previous lemma, we constructed a lattice from a dissociated set to give an upper bound for $\Delta(K)$.
- This was not a completely generic lattice: it satisfied
 1. $\Lambda \subset \mathbb{Z}^{n-1}$, and
 2. the quotient $\mathbb{Z}^{n-1}/\Lambda$ was a cyclic group.
- Let us call such lattices ‘cyclic’.

- With this observation, consider now the modified $\Delta^C(K)$, where we only take the infimum over all *cyclic* lattices which only intersect K at the origin.
- Trivially $\Delta(K) \leq \Delta^C(K)$, so we still have $\Delta^C(K) \geq 2^{-n} |K|$.
- The Aliev-Schinzel lemma actually proved that, if we had a dissociated set of size n in $[1, X]$, then

$$X \geq \Delta^C(2 \cdot H_{\alpha}^{n-1})$$

for some α .

- This inequality can be reversed.

Theorem

For any n there exists $t = O(\log n)$ and a dissociated set of size $n + t$ in $[1, X]$, where

$$X \ll 2^t \Delta^C(2 \cdot H_{(1, \dots, 1)}^{n-1}).$$

- In other words, morally the best possible $X/2^n$ for the dissociated set problem satisfies

$$X/2^n \asymp 2^{-n} \Delta^C(2 \cdot H_{(1, \dots, 1)}^{n-1}).$$

- (Only ‘morally’ since the upper bound loses $O(\log n)$, and the lower bound is assuming a cyclic version of Schinzel’s conjecture that $\Delta(H_\alpha) \geq \Delta(H_{(1, \dots, 1)})$)

Theorem

For any n there exists $t = O(\log n)$ and a dissociated set of size $n + t$ in $[1, X]$, where

$$X \ll 2^t \Delta^C(2 \cdot H_{(1, \dots, 1)}^{n-1}).$$

Proof.

Pick a lattice Λ which realises the right-hand side. There is a surjection $\phi : \mathbb{Z}^{n-1} \rightarrow \mathbb{Z}/q\mathbb{Z}$ with $\ker \phi = \Lambda$. Let $c_i = \phi(e_i)$ and $c_n = 0$. Since Λ avoids $2 \cdot H$, if $\sum_i \beta_i c_i = 0$ where $\beta_i \in \{-1, 0, 1\}$ and $\sum \beta_i = 0$ then $\beta_i = 0$, so the set of c_i is weakly dissociated mod q (restricting to $\sum \beta_i = 0$). □

Theorem

For any n there exists $t = O(\log n)$ and a dissociated set of size $n + t$ in $[1, X]$, where

$$X \ll 2^t \Delta^C(2 \cdot H_{(1, \dots, 1)}^{n-1}).$$

Proof.

Now consider

$$A = \{q, 2q, \dots, 2^{t-1}q\} \cup (\{(2^t + n)q\} + C).$$

This set is dissociated, has size $n + t$, and is in $[1, X]$ where $X = (2^t + n + 1)q$. The claim follows from $q = \text{covol}(\Lambda) \gg \Delta^C(2 \cdot H)$. □

- In the remainder of the talk I will focus on an upper bound for $\Delta(H)$ – the critical determinant of the generalised hexagon

$$H = \left\{ x \in (-1, 1)^n : \left| \sum x_i \right| < 1 \right\}.$$

- As we have seen, to turn this into a bound for dissociated sets we actually need to do this for $2 \cdot H$, and also need to make sure the lattice is cyclic.

Theorem

$$\Delta(H) \ll n^{-1/3}.$$

- Compare this to the trivial lower bound from Minkowski's theorem,

$$\Delta(H) \gg 2^{-n} |H| \asymp n^{-1/2}.$$

- Note a lot less surprising now that Erdős' conjecture is false – we need to understand lattice packing problems, which are hard!

Theorem

There exists a full-rank lattice $\Lambda \subset \mathbb{R}^n$ of covolume $\ll n^{-1/3}$ such that $\Lambda \cap H = \{0\}$.

- Our lattice is built as the Laplacian lattice of a directed graph.
- Lots of theory around these – see ‘sandpile’ models and ‘chip-firing’.

- Let G be a directed graph on $n + 1$ vertices.
- There is exactly one 'sink' vertex, with no outgoing edges, such that every other vertex has a directed path going to the sink.
- There is also one designated 'source' vertex – this can have in-edges also, but is such that every cycle goes through the source eventually.
- The Laplacian lattice in $\mathbb{R}^{n+1}$ is generated by the n vectors (one for each non-sink vertex)

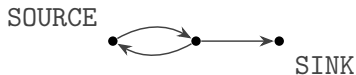
$$\gamma_v = e_v - \frac{1}{d^+(v)} \sum_{v \rightarrow w} e_w.$$

- Note these vectors are all in the hyperplane $\sum x_i = 0$. Restricting to the first n coordinates gives a lattice of full rank in $\mathbb{R}^n$, say Λ_G (the reduced Laplacian).

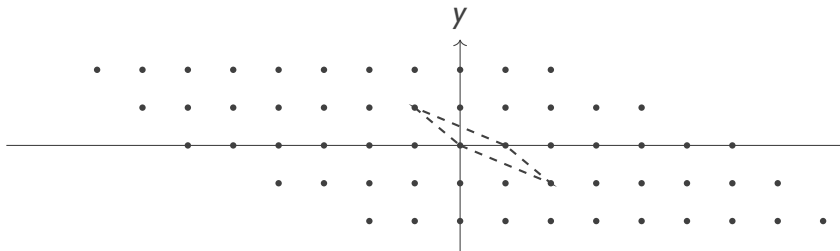
- This construction belongs to algebraic graph theory, of which the matrix tree theorem is a central result.
- This allows us to calculate the covolume of the lattice.

Theorem (Matrix tree theorem/Kirchhoff's theorem)

If G is a directed graph with one sink and one source then the covolume of Λ_G is the probability that, beginning at the source and choosing out-edges uniformly at random, we end at the sink rather than back at the source.



- The reduced Laplacian is generated by $(1, -1)$ and $(-1/2, 1)$ – this is equal to the lattice generated by $(1, 0)$ and $(0, 1/2)$, and the covolume of this lattice is $1/2$.

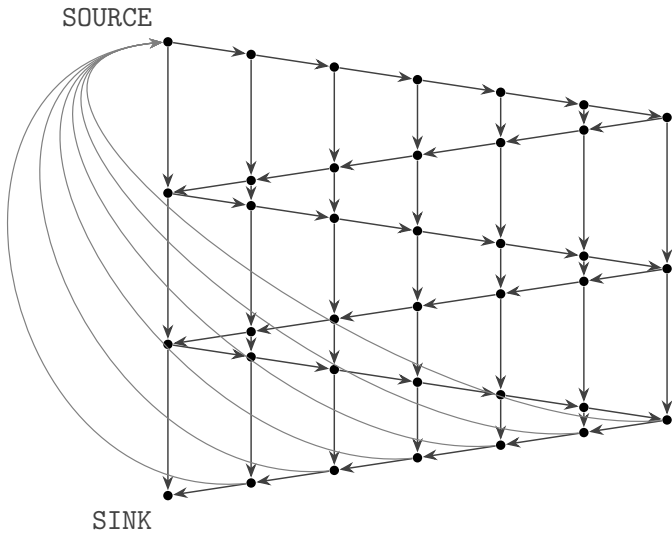


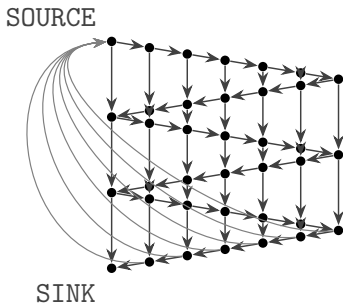
- The probability that we arrive at the sink before the source is $1/2$.

Theorem

There exists a full-rank lattice $\Lambda \subset \mathbb{R}^n$ of covolume $\ll n^{-1/3}$ such that $\Lambda \cap H = \{0\}$.

- So we want a one source/one sink directed graph G with n non-sink vertices, such that $\Lambda_G \cap H = \{0\}$, and the probability that starting at the source and walking randomly we get to the sink is $\ll n^{-1/3}$.





- The 'zigzag graph' – each row has k vertices, and there are s rows in total altogether. (So this example has $k = 7$ and $s = 6$.) This means there are $n = s(k - 1)$ non-sink vertices.
- Every non-sink vertex has out-degree exactly 2.

- There are $n = s(k - 1)$ non-sink vertices.
- The sink-probability (so covolume of the lattice) is $\ll 1/k + k/s$. Optimising this one takes $k \approx n^{1/3}$ and $s \approx n^{2/3}$, so covolume at the end is $\ll n^{-1/3}$ as claimed.
- Proof idea: say $s \asymp k^2$. Think of the walk as just wandering in $[1, k]$ – the expected number of steps before we ‘saturate’ this is $\asymp k^2$, so we need $s \asymp k^2$ many steps. After this many steps, expect to be uniformly distributed over the width, so probability $\approx 1/k$ that we’re at the origin/sink.

- But why $\Lambda \cap H = \{O\}$?
- Suppose that $y \in \Lambda \cap H$, say

$$y = \sum_{v \neq \text{SINK}} z_v \gamma_v \in (-1, 1)^n$$

with $z_v \in \mathbb{Z}$ and $z_{\text{SINK}} = 0$.

- Looking at the coordinates, this means that for all non-sink vertices v ,

$$\left| z_v - \frac{1}{2} \sum_{u \rightarrow v} z_u \right| < 1.$$

- If $z_v > 0$ is positive this inequality implies there must exist some $u \rightarrow v$ with $z_u > 0$. Similarly if $z_v < 0$.
- Since every cycle in G contains the SOURCE, this implies that either $z_v \geq 0$ for all v or ≤ 0 . Suppose the former.

- Let S be the set of v for which $z_v > 0$. If this is empty then $z_v = 0$ for all v , and we have the origin. Suppose not.
- As we have seen, if $v \in S$ there must exist a predecessor of v in S (in particular SOURCE must be in S).
- The inequality

$$\left| z_v - \frac{1}{2} \sum_{u \rightarrow v} z_u \right| < 1,$$

and the fact that $z_v \geq 0$ for all v , also implies that if there are ≥ 2 predecessors of v in S then $v \in S$.

- These facts together can be used to prove that S occupies a non-empty left-interval in each row.
- In particular, on the last row, $\text{SOURCE} \in S$. But we know $z_{\text{SOURCE}} = 0$, a contradiction.

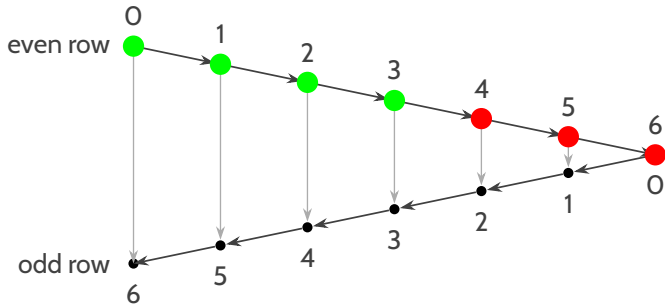


Figure: The green vertices are in S , the red are not.

- Two rules: if $v \in S$ there must be a predecessor of v in S , and if both predecessors of v are in S then $v \in S$.
- Also: if non-empty S must contain a cycle, so has at least one vertex on every row.

- In summary: dissociated sets are equivalent to lattice packing of hexagons; subtle geometric behaviour, not surprising that the initial guess of Erdős was wrong, and more efficient packings do exist.
- So far, I cannot find examples of this zigzag graph being used before in lattice constructions – what else can they be used for?
- Can be viewed as some kind of adaptation of the Conway-Guy sequence (which in hindsight arises from a related pyramid structure; cf. Boustrophedon transform).