Getting lost while hiking in the Boolean wilderness

Renan Gross

Student Probability Day VI, 11/05/17

Weizmann Institute of Science
Joint work with Uri Grupel

Warning

This presentation shows explicit images of graphs.

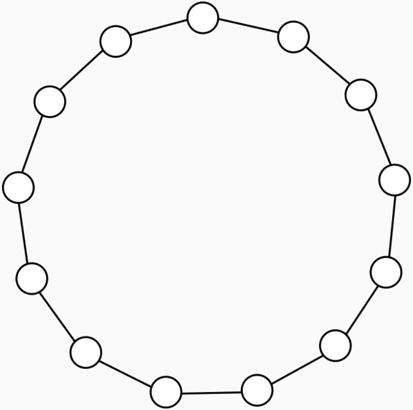
Viewer discretion is advised.

Scenery reconstruction

Suppose we are given a graph G,

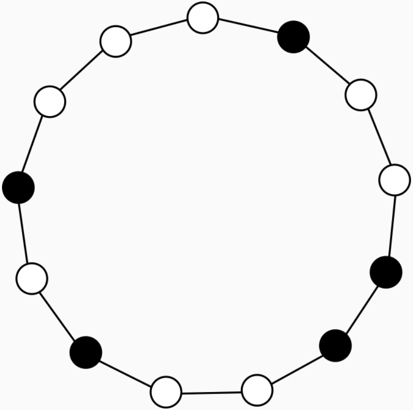
Scenery reconstruction

Suppose we are given a graph G,

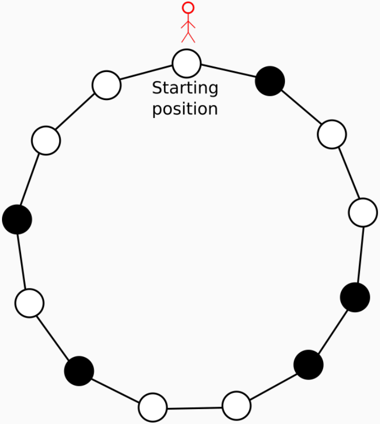


Scenery reconstruction

Suppose we are given a graph G, colored by some function $f(x)$.

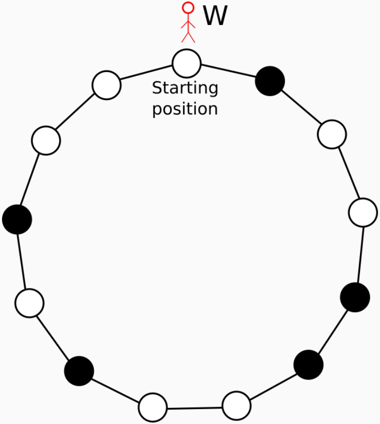


Scenery reconstruction



An agent performs a simple random walk S_t on the graph.

Scenery reconstruction

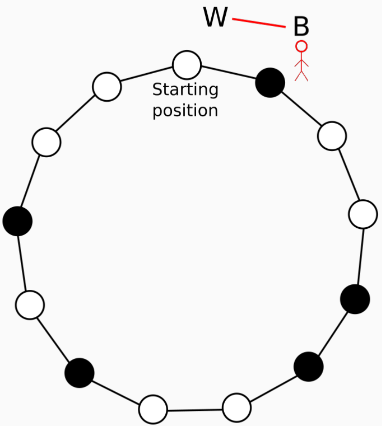


An agent performs a simple random walk S_t on the graph.

Reported scenery:

W

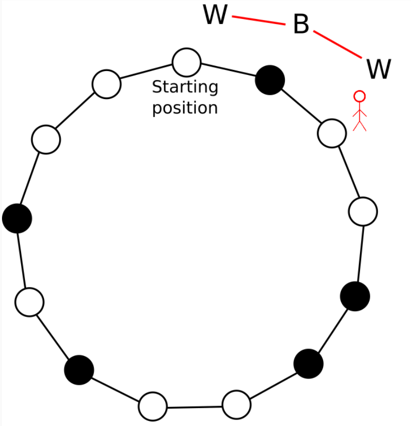
Scenery reconstruction



An agent performs a simple random walk S_t on the graph.

Reported scenery:
W B

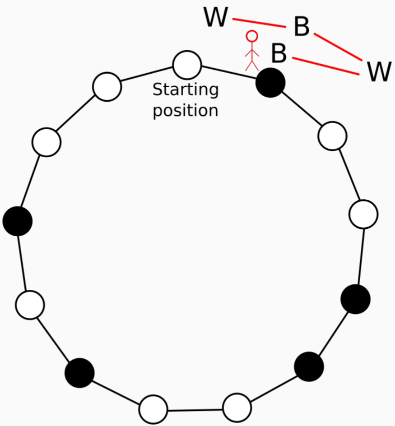
Scenery reconstruction



An agent performs a simple random walk S_t on the graph.

Reported scenery:
W B W

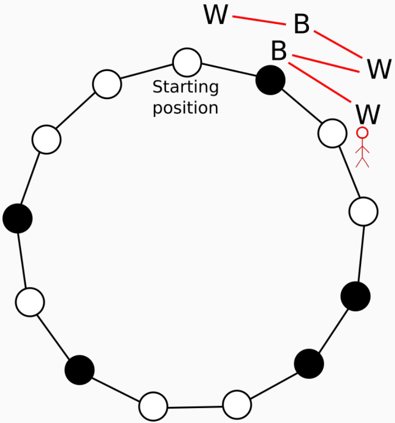
Scenery reconstruction



An agent performs a simple random walk S_t on the graph.

Reported scenery:
W B W B

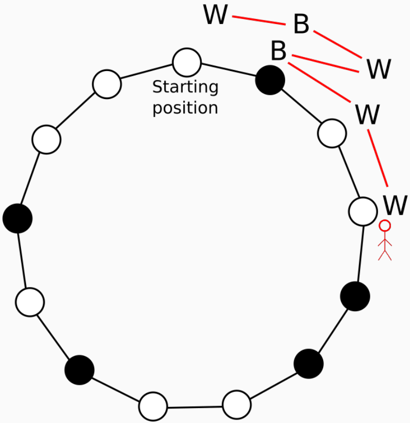
Scenery reconstruction



An agent performs a simple random walk S_t on the graph.

Reported scenery:
W B W B W

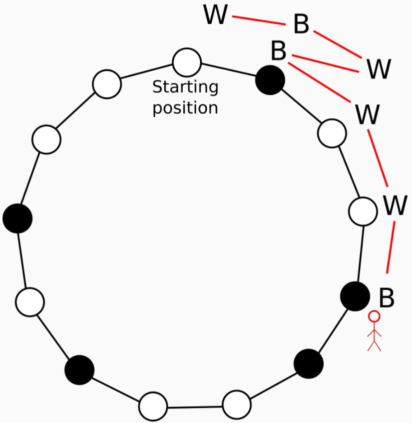
Scenery reconstruction



An agent performs a simple random walk S_t on the graph.

Reported scenery:
W B W B W W

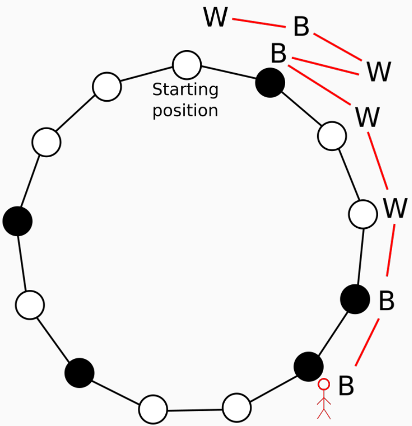
Scenery reconstruction



An agent performs a simple random walk S_t on the graph.

Reported scenery:
W B W B W W B

Scenery reconstruction



An agent performs a simple random walk S_t on the graph.

Reported scenery:
W B W B W W B B

Scenery reconstruction

Question

Suppose we know G. Can we reconstruct the coloring f based only on the trace of the random walk $f(S_t)$?

Scenery reconstruction

Question

Suppose we know G. Can we reconstruct the coloring f based only on the trace of the random walk $f(S_t)$?

Remarks:

- We are given an infinite random walk $\rightarrow$ reconstruction should happen with probability 1

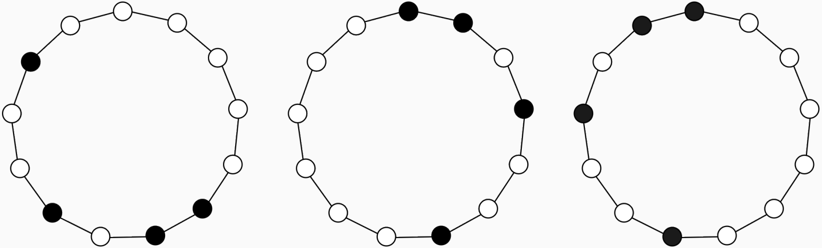
Scenery reconstruction

Question

Suppose we know G. Can we reconstruct the coloring f based only on the trace of the random walk $f(S_t)$?

Remarks:

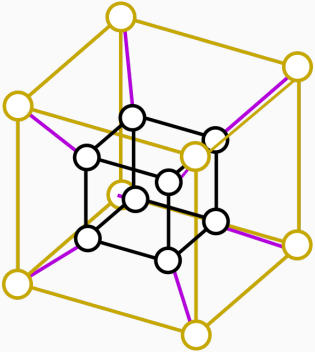
- We are given an infinite random walk $\rightarrow$ reconstruction should happen with probability 1
- Up to isomorphisms of the graph.



Scenery reconstruction

The answer is known for a variety of Abelian Cayley graphs and walks.

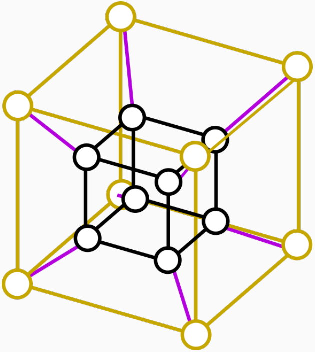
What about the *n*-dimensional Boolean hypercube?



Scenery reconstruction

The answer is known for a variety of Abelian Cayley graphs and walks.

What about the n-dimensional Boolean hypercube?



Vote?

Boolean scenery

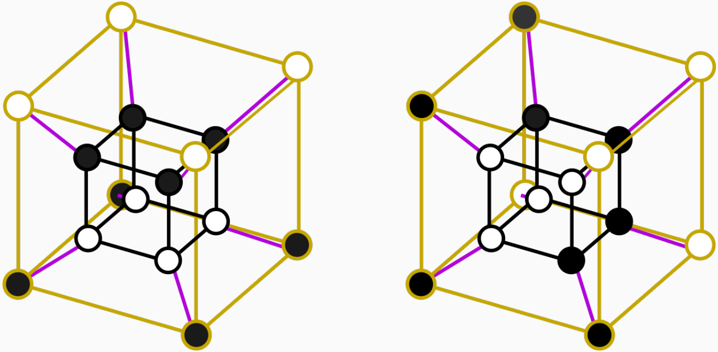
The way to do this is to show that there are two colorings which yield the same distribution of sceneries.

Example:

Boolean scenery

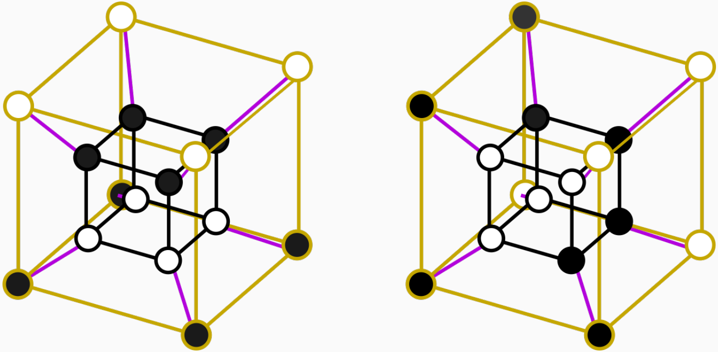
The way to do this is to show that there are two colorings which yield the same distribution of sceneries.

Example:



The way to do this is to show that there are two colorings which yield the same distribution of sceneries.

Example:



The process $f(S_t)$ is Bernoulli IID with success probability $1/2$!

Locally biased functions

So we defined locally biased functions, and started investigating them in their own right.

Definition

Let G be a graph. A Boolean function $f : G \to \{-1, 1\}$ is called *locally p-biased*, if for every vertex $x \in G$ we have

$$\frac{|\{y \sim x;\ f(y) = 1\}|}{deg(x)} = p.$$

In words, f is locally p-biased if for every vertex x, f takes the value 1 on exactly a p-fraction of x's neighbors.

Locally biased functions

So we defined locally biased functions, and started investigating them in their own right.

Definition

Let G be a graph. A Boolean function $f : G \to \{-1, 1\}$ is called *locally p-biased*, if for every vertex $x \in G$ we have

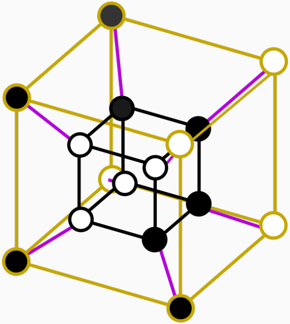
$$\frac{|\{y \sim x;\ f(y) = 1\}|}{deg(x)} = p.$$

In words, f is locally p-biased if for every vertex x, f takes the value 1 on exactly a p-fraction of x's neighbors.

Existence of two non-isomorphic locally biased functions implies that the scenery reconstruction problem cannot be solved.

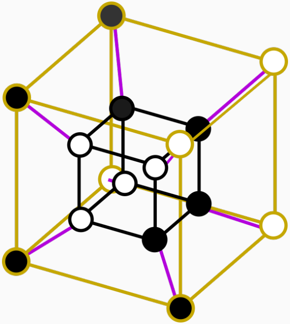
Locally biased functions

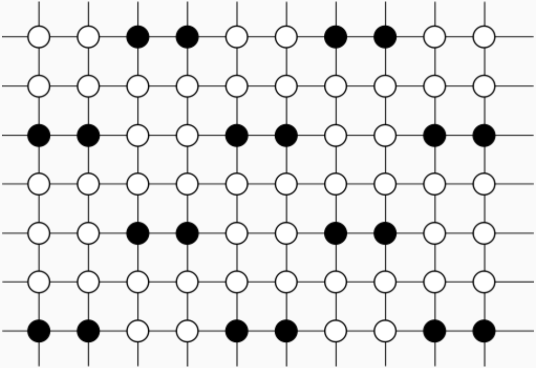
Locally biased functions can be defined for any graph.



Locally biased functions

Locally biased functions can be defined for any graph.





Theorems

We found:

Theorem (characterization)

Let $n \in \mathbb{N}$ be a natural number and $p \in [0,1]$. There exists a locally p-biased function $f : \{-1,1\}^n \to \{-1,1\}$ if and only if $p = b/2^k$ for some integers $b \geq 0, k \geq 0$, and 2^k divides n.

Theorem (size)

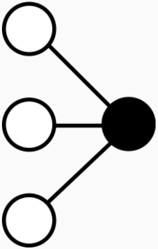
Let n be even. Let $B^n_{1/2}$ be a maximal class of non-isomorphic locally $1/2$-biased functions, i.e every two functions in $B^n_{1/2}$ are non-isomorphic to each other. Then $\left|B^n_{1/2}\right| \geq C2^{\sqrt{n}}/n^{1/4}$, where $C > 0$ is a universal constant.

Proof of theorem 1

We start with locally $1/n$-biased functions.

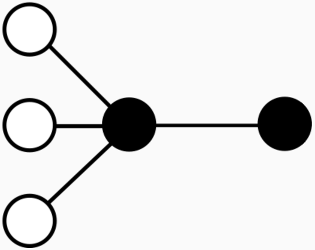
Proof of theorem 1

We start with locally $1/n$-biased functions.



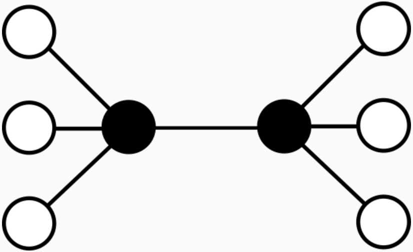
Proof of theorem 1

We start with locally $1/n$-biased functions.



Proof of theorem 1

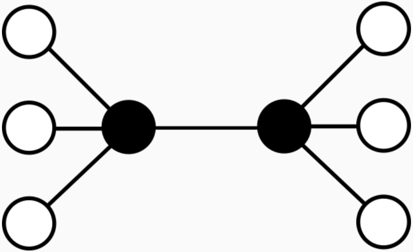
We start with locally $1/n$-biased functions.



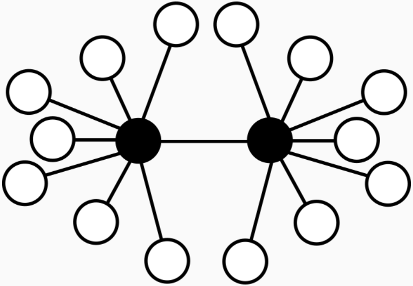
A tile for $n = 4$.

Proof of theorem 1

We start with locally $1/n$-biased functions.



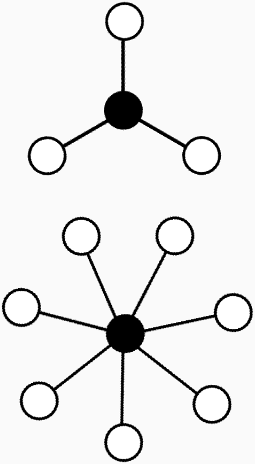
A tile for $n = 4$.



A tile for $n = 8$.

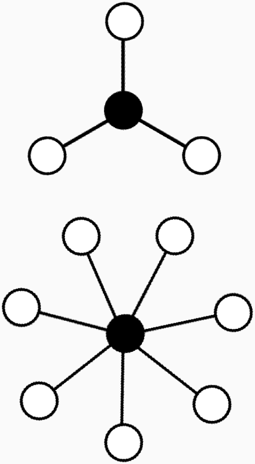
Proof of theorem 1

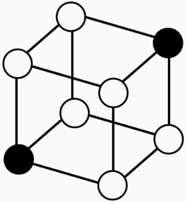
Solution: find a "half-tiling".



Proof of theorem 1

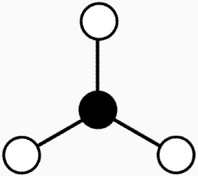
Solution: find a “half-tiling”.

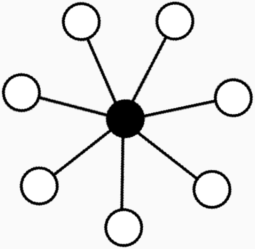


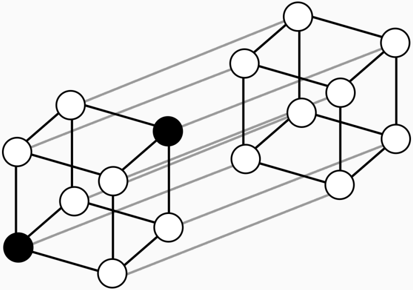


Proof of theorem 1

Solution: find a "half-tiling".

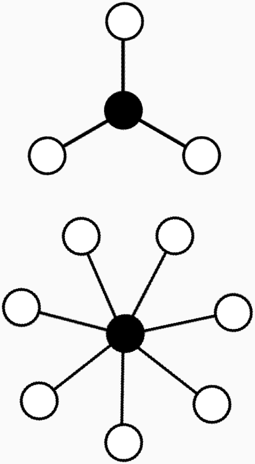


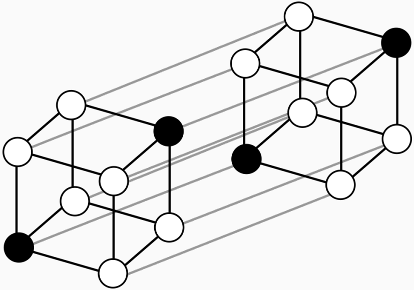




Proof of theorem 1

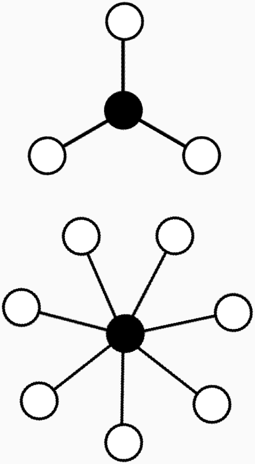
Solution: find a “half-tiling”.

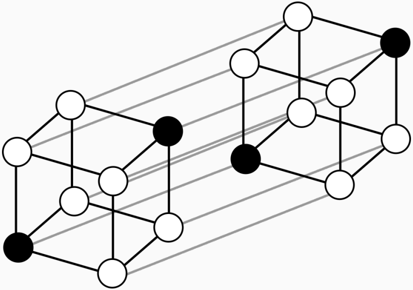




Proof of theorem 1

Solution: find a "half-tiling".

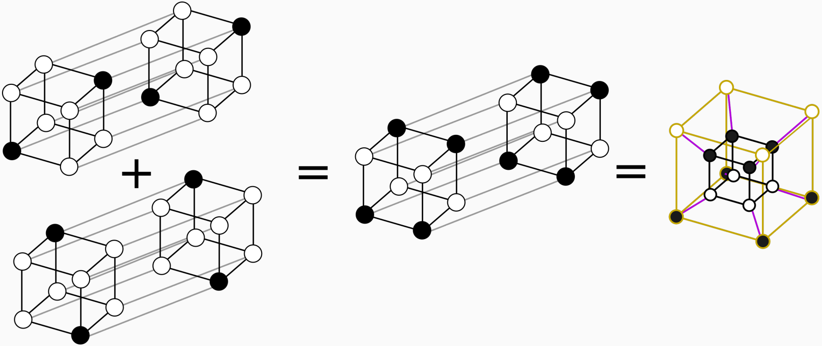




We have a $1/n$ tiling!

Proof of theorem 1

To get m/n instead of $1/n$, combine several disjoint tilings.



Proof of theorem 1

Where do we get half-tilings from? Perfect codes.

Proof of theorem 1

Where do we get half-tilings from? Perfect codes.

Where do we get disjoint half-tilings from? Hamming perfect codes.

A word on the other direction

Let x be a uniformly random element of the cube. Then $f(x) = 1$ with probability $I/2^n$, where $I = |\{x \in \{-1,1\}^n\,;\ f(x) = 1\}|$

A word on the other direction

Let x be a uniformly random element of the cube. Then $f(x) = 1$ with probability $I/2^n$, where $I = |\{x \in \{-1, 1\}^n\,;\ f(x) = 1\}|$

Let y be a uniformly random neighbor of x. Then $f(y) = 1$ with probability p by definition.

A word on the other direction

Let x be a uniformly random element of the cube. Then $f(x) = 1$ with probability $I/2^n$, where $I = |\{x \in \{-1,1\}^n ;\ f(x) = 1\}|$

Let y be a uniformly random neighbor of x. Then $f(y) = 1$ with probability p by definition.

Since both x and y are uniform random vertices,

$$\mathbb{P}(f(x) = 1) = \mathbb{P}(f(y) = 1)$$

A word on the other direction

Let x be a uniformly random element of the cube. Then $f(x) = 1$ with probability $l/2^n$, where $l = |\{x \in \{-1,1\}^n ;\ f(x) = 1\}|$

Let y be a uniformly random neighbor of x. Then $f(y) = 1$ with probability p by definition.

Since both x and y are uniform random vertices,

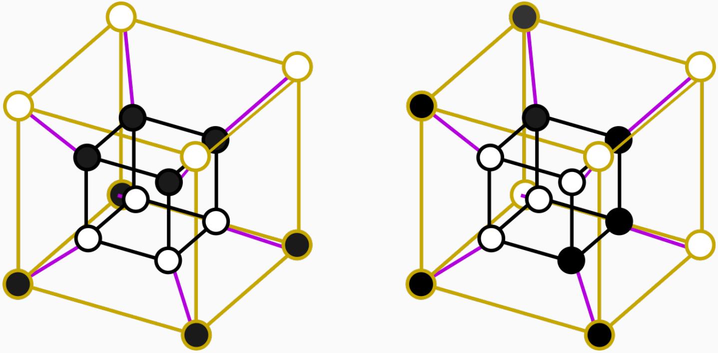
$$\mathbb{P}(f(x) = 1) = \mathbb{P}(f(y) = 1)$$

Denoting $p = m/n$ for some $m \in \{0, 1, \ldots, n\}$, this gives

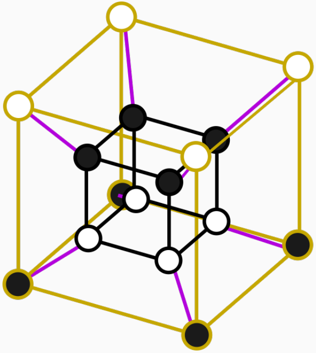
$$p = \frac{l}{2^n} = \frac{m}{n}.$$

Writing $n = c2^k$ gives the desired result.

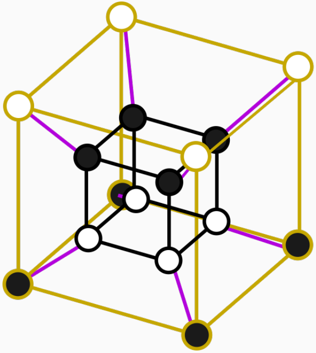
Proof of theorem 2



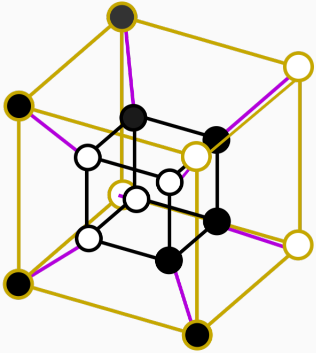
Proof of theorem 2



Proof of theorem 2

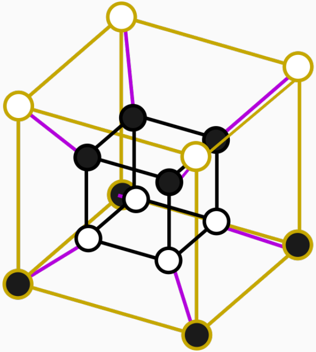


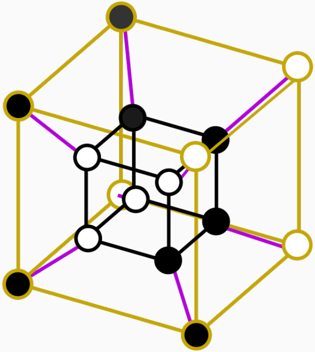
$g(x_1, x_2, x_3, x_4) = x_1x_2$



$h(x_1, x_2, x_3, x_4) =$
$\frac{1}{2}\left(x_1x_2 + x_2x_3 - x_3x_4 + x_1x_4\right)$

Proof of theorem 2





$$g_n(x_1, \ldots, x_n) = x_1 \cdots x_{n/2}$$

$$h_k = h\left(\prod_{i=0}^{k-1} x_{1+4i}, \ldots, \prod_{i=0}^{k-1} x_{4+4i}\right)$$

Proof of theorem 2

Fact

Let $f_i : \{-1, 1\}^{n_i} \to \{-1, 1\}$ *be locally* $1/2$*-biased functions for* $i = 1, 2$ *where* $n_1 + n_2 = n$. *Then*

$$f(x) = f_1(x_1, ..., x_{n_1}) f_2(x_{n_1+1}, ..., x_n)$$

is a locally $1/2$*-biased function on* $\{-1, 1\}^n$.

We can then build up locally $1/2$-biased functions from the building blocks $h_0, h_1, \ldots$ and $g_0, g_2, g_4, \ldots$.

Proof of theorem 2

Fact

Let $f_i : \{-1,1\}^{n_i} \to \{-1,1\}$ *be locally* $1/2$*-biased functions for* $i = 1,2$ *where* $n_1 + n_2 = n$*. Then*

$$f(x) = f_1(x_1, ..., x_{n_1}) f_2(x_{n_1+1}, ..., x_n)$$

is a locally $1/2$*-biased function on* $\{-1,1\}^n$*.*

We can then build up locally $1/2$-biased functions from the building blocks $h_0, h_1, \ldots$ and $g_0, g_2, g_4, \ldots$.

- Every time we pick h_0, we use 4 bits.

Proof of theorem 2

Fact

Let $f_i : \{-1,1\}^{n_i} \to \{-1,1\}$ *be locally* $1/2$*-biased functions for* $i = 1,2$ *where* $n_1 + n_2 = n$*. Then*

$$f(x) = f_1(x_1, ..., x_{n_1}) f_2(x_{n_1+1}, ..., x_n)$$

is a locally $1/2$*-biased function on* $\{-1,1\}^n$*.*

We can then build up locally $1/2$-biased functions from the building blocks $h_0, h_1, \ldots$ and $g_0, g_2, g_4, \ldots$.

- Every time we pick h_0, we use 4 bits.
- Every time we pick h_1, we use 8 bits.

Proof of theorem 2

Fact

Let $f_i : \{-1,1\}^{n_i} \to \{-1,1\}$ *be locally* $1/2$*-biased functions for* $i = 1,2$ *where* $n_1 + n_2 = n$*. Then*

$$f(x) = f_1(x_1, ..., x_{n_1}) f_2(x_{n_1+1}, ..., x_n)$$

is a locally $1/2$*-biased function on* $\{-1,1\}^n$*.*

We can then build up locally $1/2$-biased functions from the building blocks $h_0, h_1, \dots$ and $g_0, g_2, g_4, \dots$.

- Every time we pick h_0, we use 4 bits.
- Every time we pick h_1, we use 8 bits.
- Every time we pick h_2, we use 12 bits.

Proof of theorem 2

Fact

Let $f_i : \{-1,1\}^{n_i} \to \{-1,1\}$ *be locally* $1/2$*-biased functions for* $i = 1,2$ *where* $n_1 + n_2 = n$*. Then*

$$f(x) = f_1(x_1, ..., x_{n_1}) f_2(x_{n_1+1}, ..., x_n)$$

is a locally $1/2$*-biased function on* $\{-1,1\}^n$*.*

We can then build up locally $1/2$-biased functions from the building blocks $h_0, h_1, \ldots$ and $g_0, g_2, g_4, \ldots$.

- Every time we pick h_0, we use 4 bits.
- Every time we pick h_1, we use 8 bits.
- Every time we pick h_2, we use 12 bits.
- ...

Proof of theorem 2

Fact

Let $f_i : \{-1,1\}^{n_i} \to \{-1,1\}$ *be locally* $1/2$*-biased functions for* $i = 1,2$ *where* $n_1 + n_2 = n$. *Then*

$$f(x) = f_1(x_1, ..., x_{n_1}) f_2(x_{n_1+1}, ..., x_n)$$

is a locally $1/2$*-biased function on* $\{-1,1\}^n$.

We can then build up locally $1/2$-biased functions from the building blocks $h_0, h_1, \ldots$ and $g_0, g_2, g_4, \ldots$.

- Every time we pick h_0, we use 4 bits.
- Every time we pick h_1, we use 8 bits.
- Every time we pick h_2, we use 12 bits.
- $\ldots$
- The rest of the bits are filled with g_k.

Proof of theorem 2

- Every time we pick h_0, we use 4 bits.
- Every time we pick h_1, we use 8 bits.
- Every time we pick h_2, we use 12 bits.
- $\ldots$
- The rest of the bits are filled with g_k.

The # of different combinations is the same as the # of solutions to:

$$4a_1 + 8a_2 + \cdots + 4ka_k \leq n$$

which is at least

$$C \cdot 2^{\sqrt{n}}/n^{1/4}$$

for some constant C.

The end of the presentation

- There are other methods of showing that cube scenery cannot be reconstructed.
- But locally biased functions are still cool!
- Try them out for your favorite graphs!