Combinatorics, Probability and Computing (2019) 28, 46–60. © Cambridge University Press 2018
doi:10.1017/S0963548318000305

Indistinguishable Sceneries on the Boolean Hypercube

RENAN GROSS and URI GRUPEL[†]

Faculty of Mathematics and Computer Science, Weizmann Institute of Science, Herzl Street, Rehovot 7610001, Israel
(e-mail: renan.gross@weizmann.ac.il, uri.grupel@weizmann.ac.il)

Received 20 February 2017; revised 4 April 2018; first published online 5 June 2018

We show that the scenery reconstruction problem on the Boolean hypercube is in general impossible. This is done by using locally biased functions, in which every vertex has a constant fraction of neighbours coloured by 1, and locally stable functions, in which every vertex has a constant fraction of neighbours coloured by its own colour. Our methods are constructive, and also give super-polynomial lower bounds on the number of locally biased and locally stable functions. We further show similar results for $\mathbb{Z}^n$ and other graphs, and offer several follow-up questions.

2010 *Mathematics subject classification*: Primary 05C60
Secondary 68P30, 68R05

1. Introduction

Let $f : \{-1,1\}^n \to \{-1,1\}$ be a Boolean function on the n-dimensional hypercube, and let S_i be a random walk on the hypercube. Can we reconstruct the function f (with probability 1, up to the hypercube's symmetries) by only observing the scenery process $\{f(S_i)\}_i$?

Similar questions have been raised for other graphs. For example, it was shown in [1] that when G is a cycle graph, the answer is yes: it is possible to reconstruct the function f (which is a string up to choice of origin) up to rotation and reflection with probability 1. It is still an open question whether any such string can be reconstructed in polynomial time. When $G = \mathbb{Z}$, reconstruction is generally impossible [6]; for random sceneries on $\mathbb{Z}$ see [9].

When G is the hypercube, such a process was studied for a specific Boolean function, the *percolation* crossing, under the notion of dynamical percolation; see [3] for details.

In the general case, however, we show that for $n \geqslant 4$ the answer is no. We do this by considering a pair of non-isomorphic functions f and g such that if S_i and T_i are random walks on the hypercube, then $f(S_i)$ and $g(T_i)$ have exactly the same distribution. We discuss two different classes of such functions.

[†] Supported by the European Research Council (ERC).

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

- *Locally p-biased functions.* 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 neighbours. If f is a locally p-biased function, then the random variables $\{f(S_i)\}_i$ have the same distribution as independent Bernoulli random variables with $\mathbb{P}(f(S_i) = 1) = p$.
- *Locally p-stable functions.* Let G be a graph. A Boolean function $f : G \to \{-1,1\}$ is called *locally p-stable* if, for every vertex $x \in G$, we have
$$\frac{|\{y \sim x;\ f(x) = f(y)\}|}{\deg(x)} = p.$$
In words, f is locally p-stable if, for every vertex x, f retains its value on exactly a p-fraction of x's neighbours. If f is locally p-stable, then the random variables $\{f(S_i)f(S_{i+1})\}_i$ have the same distribution as independent Bernoulli random variables with $\mathbb{P}(f(S_i)f(S_{i+1}) = 1) = p$.

We say that two Boolean functions $f, g : \{-1,1\}^n \to \{-1,1\}$ are *isomorphic* if there exists an automorphism of the hypercube $\psi : \{-1,1\}^n \to \{-1,1\}^n$ such that $f \circ \psi = g$. Two functions are *non-isomorphic* if no such ψ exists.

The existence of two non-isomorphic locally p-biased functions or two non-isomorphic locally p-stable functions thus render scenery reconstruction on the hypercube impossible.

It is not immediately obvious that pairs of non-isomorphic locally p-biased and pairs of non-isomorphic locally p-stable functions exist. It is then natural to ask, for which p values do they exist? If they do exist, how many of them are there?

In this paper, we characterize the possible p values on the n-dimensional hypercube, give bounds on the number of non-isomorphic pairs, and discuss results on other graphs. The paper is organized as follows.

In Section 2 we give a full characterization of the connection between the dimension of the hypercube n and the permissible p values of locally p-biased functions, as expressed in the following theorem.

Theorem 1.1. *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 $b \geqslant 0, k \geqslant 0$, and 2^k divides n.*

Our construction is based on the Hamming code. In this code, some of the bits of an n-bit word are designated as parity bits, and their value is a linear combination of the rest of the word such that all the words in the code have a minimum distance of 3. Combining different translations of Hamming codes, we can construct functions for all p of the above form.

In Section 3 we inspect the class size of non-isomorphic locally p-biased functions on the hypercube. We show that the class size for $p = 1/2$ is at least $C2^{\sqrt{n}}/n^{1/4}$ for some constant $C > 0$, and for $p = 1/n$ it is super-exponential in n, when such p values are permissible. Thus reconstruction is impossible for such functions. We conjecture that the number of non-isomorphic locally p-biased functions scales quickly for all permissible p values.

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

Conjecture 1.2. *Let $n > 0$ be even. Let $p = b/2^k$, where $1 \leqslant b \leqslant 2^k$, $k \geqslant 1$ and 2^k divides n. Let B_p^n be the set of non-isomorphic locally p-biased functions. Then $|B_p^n|$ is super-exponential in n.*

In Section 4 we briefly discuss locally p-stable functions. We show that they exist for all possible p values, and that for most p values there are many non-isomorphic pairs; however, for every n, there are p values for which there is a single unique locally p-stable function. The results in this section are based on those of Section 3.

In Section 5 we discuss locally p-biased functions on other graphs. First, we show that when G is a regular tree of degree n, then all $p = a/n$ are permissible. Second, we show that for $G = \mathbb{Z}^n$ all the results for the hypercubes hold true. This gives us a partial answer for permissible p values for $\mathbb{Z}^n$, but there are additional values that cannot be achieved through the hypercube construction: for example, for $n = 1$ we can define a function with $p = 1/2$ and when $n = 2$ we can find a function with $p = 1/4$. We also discuss other Cayley graphs of $\mathbb{Z}$, and suggest further questions on scenery reconstruction.

Throughout most of this paper we treat the Boolean hypercube as the set $\{-1,1\}^n$. We identify it with the $\{0,1\}^n$ hypercube by considering -1 in the first to correspond to 0 in the second. In this context, for two functions $f, g : \{-1,1\}^n \to \{-1,1\}$, the support of f is the set $\{x \in \{-1,1\}^n; f(x) = 1\}$, and the union of f and g is the function supported on the union of the supports of f and g.

2. Characterization of permissible p values for locally p-biased functions

In this section we prove Theorem 1.1. The 'only if' part is achieved by a double-counting argument.

Proof (of the 'only if' statement of Theorem 1.1). Let $f : \{-1,1\}^n \to \{-1,1\}$ be a locally p-biased Boolean function. For a given vertex, p represents both the fraction of neighbours on which f obtains the value 1, and also the fraction of vertices of the entire graph on which f obtains the value 1. Thus $p = m/n$ for some $m \in \{0,1,\ldots,n\}$, and also $p = l/2^n$ where $l = |\{x \in \{-1,1\}^n;\ f(x) = 1\}|$:

$$p = \frac{l}{2^n} = \frac{m}{n}. \tag{2.1}$$

Decompose n into its prime powers, writing $n = c2^k$, where c is odd. Then by (2.1), we have that

$$l = \frac{2^{n-k} \cdot m}{c}$$

is an integer, and so c must divide m, *i.e.* $m = bc$ for some b. But then

$$p = \frac{m}{n} = \frac{b}{2^k},$$

as stated by the theorem. □

The 'if' part of Theorem 1.1 is given by an explicit construction, performed in three steps. First, we use perfect codes (introduced below) in order to obtain a locally $1/n$-biased function

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

for n that is a power of two. Second, we extend the result to a locally m/n-biased function by taking the union of m locally $1/n$-biased functions with disjoint support. Finally, given a locally p-biased function on n bits, we show how to manipulate its Fourier representation in order to yield a locally p-biased function on cn bits for any c.

We begin with a brief review of binary codes. We omit proofs and simply state definitions and known results; for a more thorough introduction, see *e.g.* [7, 8].

A binary code C on the n-dimensional hypercube is simply a subset of $\{-1,1\}^n$; its elements are called *codewords*. The *distance* of a code C is defined as $\min_{x\neq y\in C}\delta_H(x,y)$, where $\delta_H(x,y) = |\{i\in\{1,\ldots,n\}; x_i \neq y_i\}|$ is the Hamming distance between x and y, that is, the number of coordinates in which x and y differ. A code of odd distance d is called *perfect* if the Hamming balls of radius $(d-1)/2$ around each codeword completely tile the hypercube without overlaps. A code is called *linear* if its codewords form a vector space over $\mathbb{F}_2$.

A particularly interesting code is the Hamming code with k parity bits, denoted H_k. It is a linear, distance-3 perfect code on the hypercube of dimension $n = 2^k - 1$. Its codewords are structured as follows. For $x \in H_k$ and $i \in \{1,\ldots,n\}$, the bit x_i is called a *parity bit* if i is a power of 2 and a *data bit* otherwise. Thus every codeword contains k parity bits and $2^k - k - 1$ data bits. The data bits range over all possible bit-strings on $2^k - k - 1$ bits, while the parity bits are a function of the data bits:

$$x_i = \bigoplus_{j:i\wedge j\neq 0} x_j \quad \text{for all } i = 2^l,\ l \geqslant 0$$

where $\oplus$ denotes exclusive bitwise OR (XOR), and $\wedge$ denotes bitwise AND. Thus there are $2^k - k - 1$ codewords in H_k.

Armed with perfect codes, we are ready to start our proof.

Lemma 2.1. *Let $n = 2^k$ be a power of two. Then there exists a locally $1/n$-biased function on $\{-1,1\}^n$.*

Proof. In a locally $1/n$-biased function f, every point in the hypercube must have exactly 1 neighbour which is given the value 1, and $n-1$ neighbours which are given the value -1.

Let C be a distance-3 perfect code on the $(n-1 = 2^k - 1)$-dimensional hypercube. That is, every two codewords in C are at a Hamming distance of at least 3 from each other, and the Hamming balls of radius 1 centred around each codeword completely tile the hypercube. Such codes exist for dimension $2^k - 1$; for example, as mentioned above and shown in [7], the Hamming code is such a code. Define $f : \{-1,1\}^n \to \{-1,1\}$ to be the following function:

$$f(x) = \begin{cases} 1 & x \in C \times \{-1,1\}, \\ -1 & \text{otherwise.} \end{cases} \tag{2.2}$$

In words, $f(x)$ takes the value of 1 whenever the first $n-1$ coordinates of x are a codeword in C, and otherwise takes the value of -1. Then f is a locally $1/n$-biased function:

- If $f(x) = 1$, then $x = (y,b) \in C \times \{-1,1\}$. Thus $x' = (y,-b)$ is the only neighbour of x on which $f(x') = 1$; any other neighbour differs from x in the first $n-1$ coordinates, and since C is a distance-3 code, these coordinates are not a codeword in C.

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

- If $f(x) = -1$, then $x = (y, b)$ where $b \in \{-1, 1\}$ and y is not a codeword of C. Since C is perfect, y must fall inside some radius-1 ball of a codeword z. Then $x' = (z, b)$ is the only neighbour of x such that $f(x') = 1$; any other codeword differs from z in at least three coordinates since C is a distance-3 code, and so differs from y in at least two. □

Lemma 2.2. *Let $n = 2^k$ be a power of two. Then there exists a locally m/n-biased function on $\{-1, 1\}^n$ for any $m = 0, 1, \ldots, n$.*

Proof. For $m = 0$ the statement is trivial. Let $m \in \{1, \ldots, n\}$. In order to construct a locally m/n-biased function, it is enough to find m locally $1/n$-biased functions $f_1, \ldots, f_m$ with pairwise disjoint support, that is,

$$\{x : f_i(x) = 1\} \cap \{x : f_j(x) = 1\} = \emptyset \quad \text{for all } i \neq j.$$

With these functions, we can define f in the following manner:

$$f(x) = \begin{cases} 1 & f_i(x) = 1 \text{ for some } i, \\ -1 & \text{otherwise.} \end{cases}$$

Then f is a locally m/n-biased function. For every $x \in \{1, -1\}^n$, consider its neighbours on which f takes the value 1, *i.e.* the set $\{y;\ d(x, y) = 1, \exists i \text{ s.t. } f_i(y) = 1\}$. Each f_i contributes exactly one element to this set, since it is a locally$1/n$-biased function; further, these elements are all distinct, since the f_i have pairwise disjoint supports. So x has m neighbours on which f takes the value 1.

Recall that the Hamming code on $2^k - 1$ bits uses $2^k - k - 1$ data bits (these range over all possible bit-strings on $2^k - k - 1$ bits) and k parity bits (these are a function of the data bits). Let C be the Hamming code on $2^k - 1$ bits, and rearrange the order of the bits so that the parity bits are all on the right-hand side of the codeword, that is, each codeword x can be written as $x = (y, z)$, where y is a word of length $2^k - k - 1$ constituting the data bits and z is a word of length k constituting the parity bits.

Now, for all $1 \leqslant i \leqslant n$, define the sets $C_i = \{x \oplus (i-1);\ x \in C\}$, where $\oplus$ denotes the exclusive OR (XOR) operator. Then the sets C_i are all pairwise disjoint: in order for two words $x = (y, z) \in C_i$ and $x' = (y', z') \in C_j$ to be the same, we need to have both $y = y'$ and $z = z'$. But if $y = y'$ then the data bits are the same, and by construction $z \oplus z' = (i-1) \oplus (j-1)$, so $z \neq z'$ if $i \neq j$. Further, since XORing by a constant only amounts to a rotation of the hypercube, each C_i is still a perfect code.

Let f_i be the function which uses C_i as its perfect code as defined in (2.2). Then, $f_1, \ldots, f_n$ are n locally $1/n$-biased functions with pairwise disjoint supports. The combination of any m of these functions yields a locally m/n-biased function. □

Lemma 2.3. *Let $f : \{-1, 1\}^n \to \{-1, 1\}$ be a locally p-biased function on the n-dimensional hypercube. Let $c \in \mathbb{N}$, and define a new function $f' : \{-1, 1\}^{cn} \to \{-1, 1\}$ by*

$$f'(x) = f\left(\prod_{j=0}^{c-1} x_{1+jn}, \ldots, \prod_{j=0}^{c-1} x_{n+jn}\right). \tag{2.3}$$

Then f' is a locally p-biased function.

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

Proof. Let $x' \in \{-1,1\}^{cn}$ and let $i \in \{1,2,\ldots,n\}$. The number of neighbours of x' that change the sign of the ith coordinate of $\left(\prod_{j=0}^{c-1} x_{1+jn}, \ldots, \prod_{j=0}^{c-1} x_{n+jn}\right)$ is exactly c. Since the coordinates are independent and f is locally p-biased, the fraction of neighbours of x' where f' obtain the value 1 is pcn. □

We are now ready to prove that the condition on p is sufficient in Theorem 1.1.

Proof (of the 'if' statement of Theorem 1.1). All that is left is to stitch the above lemmas together. Let $n = c2^k$. Using Lemma 2.2, create a locally p-biased function $g : \{-1,1\}^{2^k} \to \{-1,1\}$ on 2^k variables; then, using Lemma 2.3, extend it to a function f on n variables. □

3. Non-isomorphic locally p-biased functions

In this section we discuss the classes of non-isomorphic locally p-biased function. We show that for the hypercube of dimension n, the growth rate with respect to n is at least $\Omega(2^{\sqrt{n}}/\sqrt{n})$ for $p = 1/2$ and super-exponential for $p = 1/n$, when such p are permissible. We conjecture that for any permissible p the growth rate is super-polynomial.

The proof for $p = 1/2$ is based on an explicit construction of non-isomorphic locally $1/2$-biased functions. In order to define these functions we use the following simple observation.

Observation 3.1. *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*

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

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

The above proposition allows us to construct examples for locally $1/2$-biased functions, by combinations of such functions on lower dimensions.

We have two basic examples for locally $1/2$-biased functions.

(1) In any even dimension n,

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

(2) In dimension $n = 4$,

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

The Fourier decomposition of a Boolean function is its expansion as a real multilinear polynomial: any Boolean function $f : \{-1,1\}^n \to \mathbb{R}$ can be written as a sum

$$f(x_1, \ldots, x_n) = \sum_{S \subseteq \{1,\ldots,n\}} \hat{f}_S \prod_{i \in S} x_i,$$

where the $\hat{f}_S$ are real coefficients. Such a representation is unique; for a proof and other properties of the Fourier decomposition, see *e.g.* [10, Chapter 1].

Automorphisms of the hypercube are manifested on the Fourier decomposition of a Boolean function either by permutation or by a sign change to a subset of indices. Hence, we can show

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

that two Boolean functions are not isomorphic by showing that their Fourier decompositions cannot be mapped into one another by such permutations and sign changes.

In this section, a tensor product of two functions $f(x_1,\dots,x_n)$ and $g(x_1,\dots,x_m)$ is a function on disjoint indices, that is,

$$h(x_1,\dots,x_{n+m}) = f(x_1,\dots,x_n)\cdot g(x_{n+1},\dots,x_{n+m}).$$

Proposition 3.2. *There exists $h_1,h_2,\dots$ such that for any k the function h_k is locally $1/2$-biased on the $4k$-dimensional hypercube and h_k is not isomorphic to any tensor product of $h_1,\dots,h_{k-1},g_2,g_4,g_6,\dots$.*

Proof. We define $h_1 = h$, and

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

where h is the function from example (2). By Lemma 2.3, h_k is locally $1/2$-biased on $\{-1,1\}^{4k}$. Assume that h_k is isomorphic to a tensor product of $h_1,\dots,h_{k-1},g_2,\dots,g_{n-2}$. If there exists $1 \leqslant i \leqslant j < k$ such that both h_i and h_j appear in a product that is isomorphic to h_k, then the Fourier decomposition of the product would have at least 16 different monomials. But h_k has only four different monomials, and the functions cannot be isomorphic. Similarly, if we do not use any of the functions $h_1,\dots,h_{k-1}$, then we get the parity function, which has only one monomial in its Fourier decomposition. Hence, we may assume that there is only one $1 \leqslant i < k$ such that h_i is in the product. Then, up to an automorphism, this function is of the form

$$f(x) = h_i(x_1,\dots,x_{4i})g_{4k-4i}(x_{4i+1},\dots,x_{4k}).$$

On the one hand, by definition of h_k, its Fourier decomposition has pairs of monomials with no shared indices (*e.g.* the monomials that replace x_1x_2 and x_3x_4 in h_1). On the other hand, in the decomposition of f, all monomials have shared indices; for example x_{4i+1} appears in all monomials. Hence they are not isomorphic. □

Using the functions $h_1,h_2,\dots$ we can give a lower bound for the class of non-isomorphic locally $1/2$-biased functions.

Lemma 3.3. *The number of non-negative integer solutions to*

$$a_1 + 2a_2 + \cdots + ka_k \leqslant k \tag{3.1}$$

is at least $C4^{\sqrt{k}}/k^{1/4}$, where $C > 0$ is a universal constant.

Proof. For any $1 \leqslant \ell \leqslant k$, the number of solutions to (3.1) is at least the number of solutions to

$$\ell a_1 + \ell a_2 + \cdots + \ell a_\ell \leqslant k.$$

It is well known that the number of solutions to this inequality is

$$\binom{\ell + k/\ell}{\ell}.$$

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

This term is maximized when $\ell^2 = k$. Hence, a lower bound for the number of solutions to (3.1) is

$$\binom{2\sqrt{k}}{\sqrt{k}}.$$

By Stirling's formula, the asymptotic of this is $(1/\sqrt{\pi})4^{\sqrt{k}}/k^{1/4}$. □

Remark. The number of integer solutions to the equality case is the famous partition function $p(n)$. Hardy and Ramanujan [4] showed precise asymptotics. Using their result it is possible to show that the number of integer solutions is

$$\sum_{j=1}^{k} p(j) \sim Ce^{c\sqrt{k}}/\sqrt{k},$$

with explicit constants $C, c > 0$. While this result gives better bounds than Lemma 3.3, our simple estimation is enough for our purposes.

Proposition 3.4. *Let n be even. Let $B^n_{1/2}$ be a maximal class of non-isomorphic locally $1/2$-biased functions. Then $|B^n_{1/2}| \geqslant C2^{\sqrt{n}}/n^{1/4}$, where $C > 0$ is a universal constant.*

Proof. Let $k = \lfloor n/4 \rfloor$. By Observation 3.1, we can construct locally $1/2$-biased functions by tensor products of $h_1, \ldots, h_k$ and $g_1, \ldots, g_n$, as follows. Choose functions $\{h_{i_j}\}$ such that $m := \sum 4i_j \leqslant n$. Then the tensor product $\otimes h_{i_j}$ uses m variables. This can be completed to n variables by tensoring with g_{n-m}.

If two functions use the same h_i, then they are isomorphic (by change of indices). And if they have a different decomposition of h_i, then by the same arguments used in Proposition 3.2, they have a different Fourier decomposition and are therefore non-isomorphic. Thus, the isomorphic class of such a function is determined by the number of times each h_i appears in the product.

Hence, the number of non-isomorphic functions we can construct in this manner is the number of solutions to

$$4a_1 + 8a_2 + \cdots + 4ka_k \leqslant n, \tag{3.2}$$

where the $a_1, \ldots, a_k$ are non-negative integers that represent the number of copies of h_i in the product. Using Lemma 3.3, this number is at least $C4^{\sqrt{k}}/k^{1/4} = C'2^{\sqrt{n}}/n^{1/4}$ □

For a Boolean function f with Fourier coefficients $\hat{f}_S$, the Fourier weight at degree d is defined as

$$W_d(f) = \sum_{|S|=d} \hat{f}_S^2.$$

As the following proposition shows, the Fourier decomposition of a locally $1/2$-biased function contains only monomials of degree $n/2$. It might be possible to obtain better bounds on the number of non-isomorphic functions using this condition.

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

Proposition 3.5. *Let $f:\{-1,1\}^n \to \{-1,1\}$ be a locally $1/2$-biased function. Then the Fourier weight at degree $n/2$ is* 1.

It is an interesting question to find a general connection between p and the weight distribution of a locally p-biased function.

Proof. Let A_n be the adjacency matrix of the hypercube. The map

$$\varphi : f \mapsto (f(a_1),\dots,f(a_{2^n})),$$

where $a_1,\dots,a_{2^n}$ are the vertices of the hypercube, is a bijection between locally $1/2$-biased functions and the null space of A_n. Since

$$A_n = \begin{pmatrix} A_{n-1} & I \\ I & A_{n-1} \end{pmatrix},$$

we have

$$P_n(t) = P_{n-1}(t-1)P_{n-1}(t+1),$$

where P_n is the characteristic polynomial of A_n. For A_2 the eigenvalue 0 has multiplicity 2 and ± 2 has 1. Continuing by induction, the eigenvalues of A_m are $-m,-m+2,\dots,m$ with multiplicities $\binom{m}{0},\binom{m}{2},\dots,\binom{m}{m}$. Hence, for even n the dimension of the null space is $\binom{n}{n/2}$. For any $S \subseteq \{1,2,\dots,n\}$ with $|S| = n/2$ we denote $\chi_S(x) = \prod_{i\in S} x_i$ and $v_S = \varphi(\chi_S)$. Since the functions χ_S are all locally $1/2$-biased, the vectors v_S are in the null space of A_n. Note that there are $\binom{n}{n/2}$ such vectors, and they form an independent set. Hence the set $\{v_S\}_S$ is a basis of the null set. By the bijection we get that every locally $1/2$-biased function is a linear combination of χ_S. □

Class sizes for locally $1/n$-biased functions can also be achieved via the following proposition.

Proposition 3.6. *Let $n = 2^k$, and let C_1 and C_2 be two non-isomorphic distance-3 perfect codes on the $(n-1)$-dimensional hypercube. Then the two functions f_1 and f_2 defined by equation* (2.2) *using the perfect codes C_1 and C_2 are non-isomorphic.*

The proof shows that in any isomorphism between two functions constructed using equation (2.2), the last coordinate must be preserved. However, this will imply that the remaining coordinates are isomorphic, in contradiction to the assumption.

Proof. Suppose to the contrary that f_1 and f_2 are isomorphic, that is, there is an automorphism $\varphi:\{-1,1\}^n \to \{-1,1\}^n$ such that for all $x \in \{-1,1\}^n$, we have $f_1(x) = f_2(\varphi(x))$. Denote by $B = \{(y,1);\, y \in \{-1,1\}^{n-1}\}$ the $(n-1)$-dimensional hypercube obtained by fixing the last coordinate to 1, denote $C = \{(y,1);\, y \in C_2\}$ and note that $\text{support}(f_2|_B) = C$ by construction. Consider $\varphi|_B$, the restriction of φ to B. This restriction is an isomorphism between B and some $(n-1)$-dimensional hypercube A contained within the n-dimensional hypercube. Any sub-hypercube of dimension $n-1$ is obtained from $\{-1,1\}^n$ by fixing one of the coordinates to be either 1 or -1, and taking the span of all other coordinates. Then A must be spanned by the first $n-1$ coordinates, leaving the last coordinate fixed: otherwise, by equation (2.2), the set A would

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

contain two neighbouring points x and x' that differ only in their last coordinate such that $f_1(x) = f_1(x') = 1$. This means there are $y, y' \in C$ obeying $\varphi(y) = x, \varphi(y') = x'$; but this is a contradiction, since φ should preserve distances, and the distance between x and x' is 1 while the distance between y and y' is 3. So $A = \{(y,b);\ y \in \{-1,1\}^{n-1}\}$ for some $b \in \{-1,1\}$. But then $\varphi|_B$ is an isomorphism between C_1 and C_2, since C_1 is a perfect code in A and C_2 is a perfect code in B, a contradiction. □

Corollary 3.7. *Let $n = 2^k$. Let $B^n_{1/n}$ be the class of non-isomorphic locally $1/n$-biased functions. Then $|B^n_{1/n}|$ is super-exponential in n.*

Proof. By Proposition 3.6, any lower bound on the number of non-isomorphic perfect codes on the $(n-1)$-dimensional hypercube gives a lower bound to the number of locally $1/n$-biased functions on the n-dimensional hypercube. Recent constructions, such as in [5], give a super-exponential lower bound on the number of such perfect codes. □

We would have liked to apply the same argument to locally m/n-biased functions, as given by the construction in Lemma 2.2. Our argument there used the explicit construction of the Hamming code which, being linear, was easy to modify in order to obtain functions with disjoint supports. Such is not the case for the construction of non-linear codes. However, we still believe that similar estimates are true for any permissible p.

Corollary 3.8. *By Proposition 3.4, scenery reconstruction is impossible for even-dimensional hypercubes.*

For odd dimensional hypercubes, on which there are no non-trivial locally biased functions, we use locally stable functions instead, as described in the next section.

4. Locally p-stable functions

Unlike locally p-biased functions, there is no restriction on permissible p values for locally p-stable functions.

Observation 4.1. *Let $p = m/n$ for some $m \in \{0,1,\ldots,n\}$. Then the parity function on $n-m$ variables,*

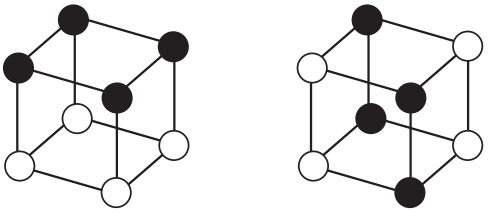
$$f(x_1,\ldots,x_n) = x_{m+1}x_{m+2}\ldots x_n,$$

is locally p-stable.

Thus we will focus on the number of non-isomorphic pairs of locally stable functions. A negative result is attainable by a simple examination.

Proposition 4.2. *If $p = 1/n$ or $p = (n-1)/n$, then the parity function is the only locally stable p-function on the hypercube, up to isomorphisms. See Figure 1.*

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press



(a) (b)

Figure 1. (a) The only locally $(n-1)/n$-stable function is the parity function on 1 variable. (b) The only locally $1/n$-stable function is the parity function on $n-1$ variables.

Proof. We prove only for $p=(n-1)/n$; the proof for $p=1/n$ is similar.

We will show that f depends only on a single coordinate. Let x be an initial point in the hypercube and y its unique neighbour such that $f(x)\neq f(y)$. Denote the coordinate in which they differ by i. By local stability, every other neighbour x' of x has $f(x')=f(x)$, and every other neighbour y' of y has $f(y')=f(y)$.

Let $j\neq i$, let $\tilde{x}$ be the neighbour of x that differs from x in coordinate j, and let $\tilde{y}$ be the neighbour of y that differs y in coordinate j. Then $\tilde{x}$ is a neighbour of $\tilde{y}$, since $\tilde{x}$ and $\tilde{y}$ differ only in the ith coordinate. Also, since $f(x)=f(\tilde{x})$ and $f(y)=f(\tilde{y})$ but $f(x)\neq f(y)$, we have $f(\tilde{x})\neq f(\tilde{y})$.

Since f is locally $(n-1)/n$-stable, each of x's neighbours x' has exactly one neighbour y' on which f attains the opposite value. By the above, for each such x', the corresponding y' differs from it in the ith coordinate. This reasoning can be repeated, choosing a neighbour of x as the initial starting point, showing that for all x' with the same ith coordinate as x, $f(x)=f(x')$, while for all x' that differ in the ith coordinate from x, $f(x)\neq f(x')$. This means that either $f(x)=x_i$ or $f(x)=-x_i$. □

Many other p values, however, have larger classes of non-isomorphic locally p-stable functions, since locally stable functions can be built out of locally $1/2$-biased functions.

Proposition 4.3. *There is an injection φ between locally $1/2$-biased functions on $\{-1,1\}^n$ and locally $(n/2)/(n+1)$-stable functions on $\{-1,1\}^{n+1}$. Further, if f and g are two non-isomorphic locally $1/2$-biased functions, then $\varphi(f)$ and $\varphi(g)$ are also non-isomorphic.*

Proof. Define φ by

$$(\varphi(f))(x_1,\ldots,x_{n+1})=f(x_1,\ldots,x_n)\cdot x_{n+1}.$$

Then $\varphi(f)$ is locally $(n/2)/(n+1)$-stable, since for every $x\in\{-1,1\}^{n+1}$, $\varphi(f)$ retains its value on exactly half of the neighbours which differ in the first n coordinates, but flips its value on the neighbour that differs in the last coordinate. The claim about non-isomorphism follows directly from the functions' Fourier decomposition. □

Observe that unlike locally biased functions, locally stable functions can be easily extended to higher dimension.

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

Observation 4.4. *Let f be a locally $(n-m)/n$-stable function. Then f can be extended to hypercubes of size $n' \geqslant n$ by simply ignoring all but the first n coordinates. This gives a locally $(n'-m)/n'$-stable function.*

We can use this observation to give a lower bound on the number of locally $(n'-m)/n'$-stable functions for a fixed m and any $n' \geqslant 2m-2$. This works as follows. First, pick any fixed $m > 1$. Using Proposition 4.3, we obtain a locally $(n-m)/n = (n/2)/(n+1)$-stable with $n = 2m-2$. This can be extended by Observation 4.4 to any $n' \geqslant n$, and together with Proposition 3.4 we get a lower bound of $C2^{\sqrt{2m-2}}/(2m-2)^{1/4}$ different locally $(n'-m)/n'$-stable functions.

This observation also provides us with a pair of non-isomorphic locally stable functions for all hypercubes of dimension $n \geqslant 5$, showing the following.

Corollary 4.5. *Scenery reconstruction is impossible for n-dimensional hypercubes for $n \geqslant 5$.*

5. Other directions and open questions

In this section we discuss similar results and questions for other graphs. We also list some further questions regarding locally biased and locally stable functions on the hypercube. For other excellent open problems see [2].

5.1. Hypercube reconstruction

Our work shows that in general, Boolean functions on the hypercube cannot be reconstructed.

Question 5.1. *Under which conditions is it possible to reconstruct Boolean functions on the hypercube?*

Question 5.2. *Is a random Boolean function reconstructible with high probability?*

Remark. Using the techniques of [1], it can be shown that reconstruction is always possible in the hypercube of dimension at most 3.

5.2. Other graphs

Note that the necessity condition on p of Theorem 1.1 can be applied to any finite regular graph, ruling out functions based on the relation between the graph degree and the number of vertices.

Trees. Let G be an n-regular infinite tree. Then for any $p = b/n$, $b = 0, 1, \ldots, n$ there exists a locally p-biased function. Such a function can be found greedily by picking a root vertex $v \in G$, setting $f(v) = 1$, and iteratively assigning values to vertices further away in any way that meets the constraints.

Notice that the method above requires picking some initial vertex, and that the method yields many possible functions on labelled trees (all of which are isomorphic when we remove the labels). Once the initial vertex v has been fixed, it is possible to generate a distribution on locally p-biased functions, by setting $f(v)$ to be 1 with probability b/n, and randomly expanding from there.

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

Question 5.3. *For an n-regular tree G, find an invariant probability measure on locally p-biased functions that commutes with the automorphisms of the tree.*

The standard lattice. The following propositions show that there is a one-to-one mapping of locally p-biased functions from the hypercube to $\mathbb{Z}^n$. Since automorphisms of the lattice can be pulled back to automorphisms of the hypercube, we get lower bounds for the size of non-isomorphic locally p-biased functions on $\mathbb{Z}^n$.

Proposition 5.4. *Let $f : \{-1,1\}^n \to \{-1,1\}$ be a locally p-biased function. Then there exists a locally p-biased extension $\tilde{f} : \mathbb{Z}^n \to \{-1,1\}$ such that $f\big|_{\{-1,1\}^n} = f$. In addition, if f and g are non-isomorphic locally p-biased functions on the hypercube, then $\tilde{f}$ and $\tilde{g}$ are non-isomorphic.*

Proof. Here we think of the hypercube as $\{0,1\}^n$ instead of $\{-1,1\}^n$. For any $x \in \mathbb{Z}^n$, define

$$\psi(x_1,\ldots,x_n) = (x_1 \bmod 2,\ldots,x_n \bmod 2)$$

and

$$\widetilde{f}(x) = f(\psi(x)).$$

Let $x \in \mathbb{Z}^n$, and let e_i be the ith vector in the standard basis. Denote $y = \psi(x)$ and write y^i for the neighbour of y in $\{0,1\}^n$ which differs from y in the ith direction. Then $\widetilde{f}(x+e_i) = \widetilde{f}(x-e_i) = f(y^i)$, showing that $\widetilde{f}$ is a locally p-biased function.

Note that the automorphisms of $\mathbb{Z}^n$ are those of the hypercube with the addition of translations. But under the map ψ, translations in $\mathbb{Z}^n$ amount to reflections in $\{0,1\}^n$. Thus any automorphism between $\widetilde{f}$ and $\widetilde{g}$ would induce one between f and g. □

The above extension procedure gives us lower bounds on the growth rate of some classes of non-isomorphic locally p-biased functions.

Corollary 5.5. *Let $\widetilde{B}_p^n$ be the class of non-isomorphic locally p-biased functions on $\mathbb{Z}^n$.*

(1) *If n is even, then $|\widetilde{B}_{1/2}^n| \geqslant C2^{\sqrt{n}}/n^{1/4}$, where $C > 0$ is a universal constant.*

(2) *If $n = 2^k$, then $|\widetilde{B}_{1/n}^n|$ is super-exponential.*

Unlike for the hypercube, we do not have a characterization theorem for the lattice $\mathbb{Z}^n$. In fact, we have found a locally $1/2$-biased function for $\mathbb{Z}$ and a locally $1/4$-biased function for $\mathbb{Z}^2$; see Figure 2. Neither of these are the result of embedding the relevant hypercube in the lattice via Proposition 5.4.

Question 5.6. *Give a complete characterization of permissible p values for locally p-biased functions on $\mathbb{Z}^n$. When such functions exist, count how many there are.*

Cayley graphs. In general, for a given group with a natural generating set, it is interesting to ask whether its Cayley graph admits locally biased or locally stable functions, and if so, how many. Specific examples which spring to mind for such groups are the group of permutations S_n with all

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

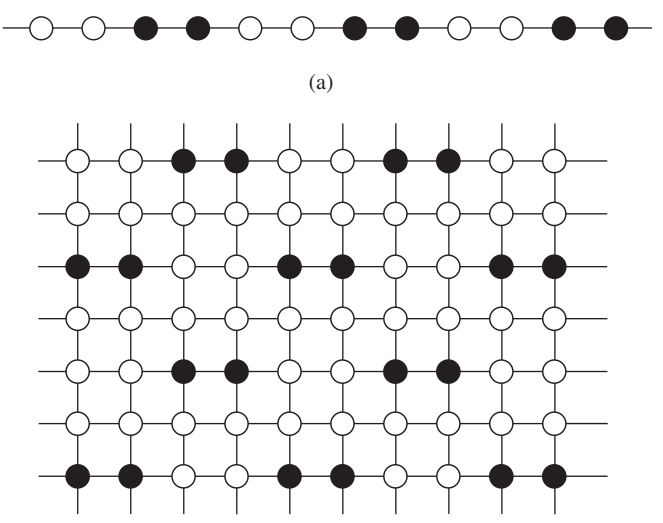


Figure 2. (a) A locally $1/2$-biased function on $\mathbb{Z}$. (b) A locally $1/4$-biased function on $\mathbb{Z}^2$.

transpositions $\{\sigma_{ij}\}_{i<j}$, and $\mathbb{Z}$ with any number of generators. For the latter case, the following observation shows that for any two generators, $\mathbb{Z}$ has a locally $1/2$-biased function.

Observation 5.7. *Let $a > 1$ and $b > 1$ generate $\mathbb{Z}$. Then the function f defined by*

$$f(x) = \begin{cases} 1 & 0 \leqslant (x \mod 2(a+b)) < a+b, \\ -1 & a+b \leqslant (x \mod 2(a+b)) < 2(a+b) \end{cases}$$

is locally $1/2$-biased.

Computer search shows that for some generators, other locally biased functions exist; see Figure 3 for an example.

Question 5.8. *Characterize the locally biased and locally stable functions on S_n as a function of its generating set.*

Question 5.9. *Characterize the locally biased and locally stable functions on $\mathbb{Z}$ as a function of its generating set.*

5.3. Locally biased and locally stable functions

Section 3 only gives lower bounds on the number of locally biased functions, and applies only for $p = 1/2$ and $p = 1/n$ (and $1 - 1/n$ by taking negation of functions).

Question 5.10. *What are the exact asymptotics for the number of non-isomorphic locally biased functions, for all permissible p?*

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press

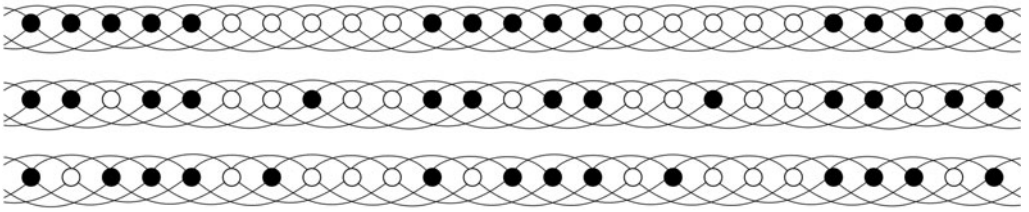


Figure 3. Three non-isomorphic locally $1/2$-biased functions for $\mathbb{Z}$ with the generators $\{2,3\}$. Computer search shows that these are the only ones.

We can also ask about the robustness of the locally biased property.

Question 5.11. *How do the characterization and counting theorems for locally biased functions change, when we relax the locally biased demand for $2^{o(n)}$ of the vertices (i.e. a small number of vertices can have their neighbours labelled arbitrarily)?*

The uniqueness of locally $1/n$-stable functions is in stark contrast to the exponential size of locally $1/n$-biased functions. Our bounds in Section 4 for the number of $(n-m)/n$-locally stable functions are exponential in m, but not in n. We seek a better understanding of these functions.

Question 5.12. *What are the exact asymptotics for the number of non-isomorphic locally stable functions?*

Acknowledgements

We thank Itai Benjamini for proposing the question of indistinguishability and for his advice, Ronen Eldan for his suggestions on locally stable functions, and David Ellis for his comments on perfect codes. We also thank Noga Alon and Peleg Michaeli for some useful discussions.

References

[1] Benjamini, I. and Kesten, H. (1996) Distinguishing sceneries by observing the scenery along a random walk path. *J. Anal. Math.* **69** 97–135.
[2] Finucane, H., Tamuz, O. and Yaari, Y. (2014) Scenery reconstruction on finite abelian groups. *Stochastic Process. Appl.* **124** 2754–2770.
[3] Garban, C. and Steif, J. E. (2015) *Noise Sensitivity of Boolean Functions and Percolation*, Institute of Mathematical Statistics Textbooks, Cambridge University Press.
[4] Hardy, G. H. and Ramanujan, S. (1918) Asymptotic formulæ in combinatory analysis. *Proc. London Math. Soc.* **s2-17** 75–115.
[5] Krotov, D. S. and Avgustinovich, S. V. (2008) On the number of 1-perfect binary codes: A lower bound. *IEEE Trans. Inform. Theor.* **54** 1760–1765.
[6] Lindenstrauss, E. (1999) Indistinguishable sceneries. *Random Struct. Alg.* **14** 71–86.
[7] van Lint, J. H. (1975) A survey of perfect codes. *Rocky Mountain J. Math.* **5** 199–224.
[8] van Lint, J. H. (1998) *Introduction to Coding Theory*, third edition, Springer.
[9] Matzinger, H. and Rolles, S. W. (2003) Reconstructing a piece of scenery with polynomially many observations. *Stochastic Process. Appl.* **107** 289–300.
[10] O'Donnell, R. (2014) *Analysis of Boolean Functions*, Cambridge University Press.

https://doi.org/10.1017/S0963548318000305 Published online by Cambridge University Press