Locally Sampleable Uniform Symmetric Distributions

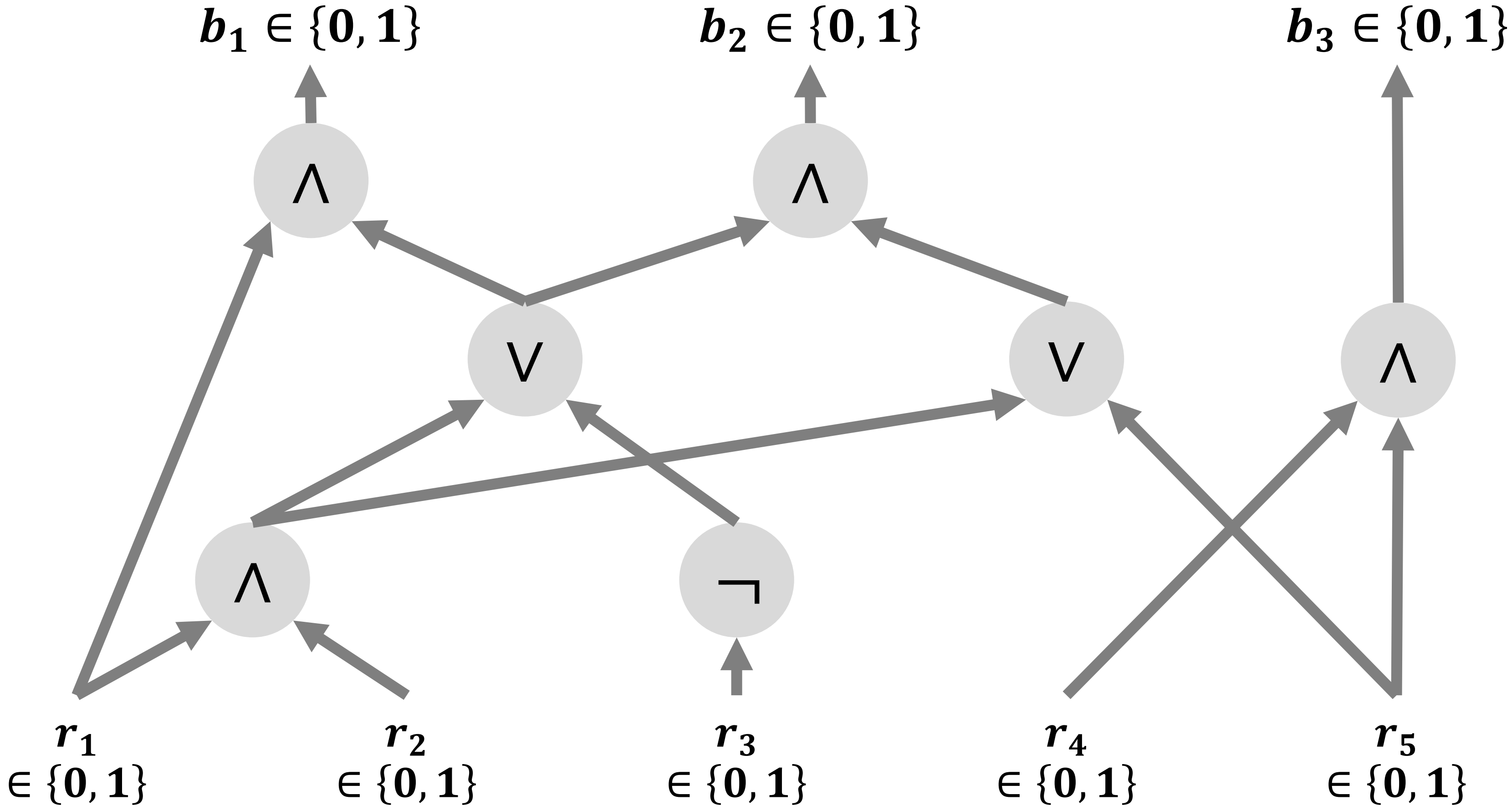
Kewen Wu (UC Berkeley)

Daniel Kane
UCSD

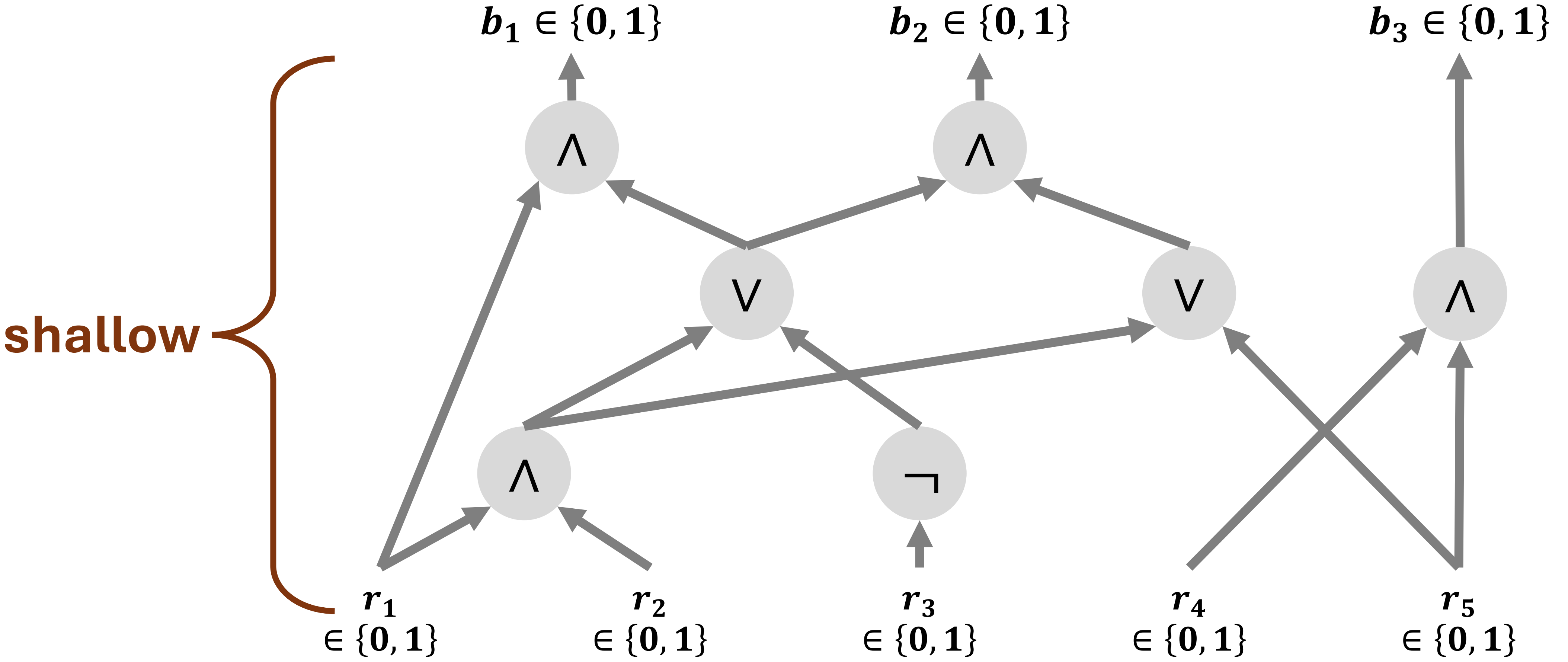
Anthony Ostuni
UCSD

What distributions can a shallow circuit produce?

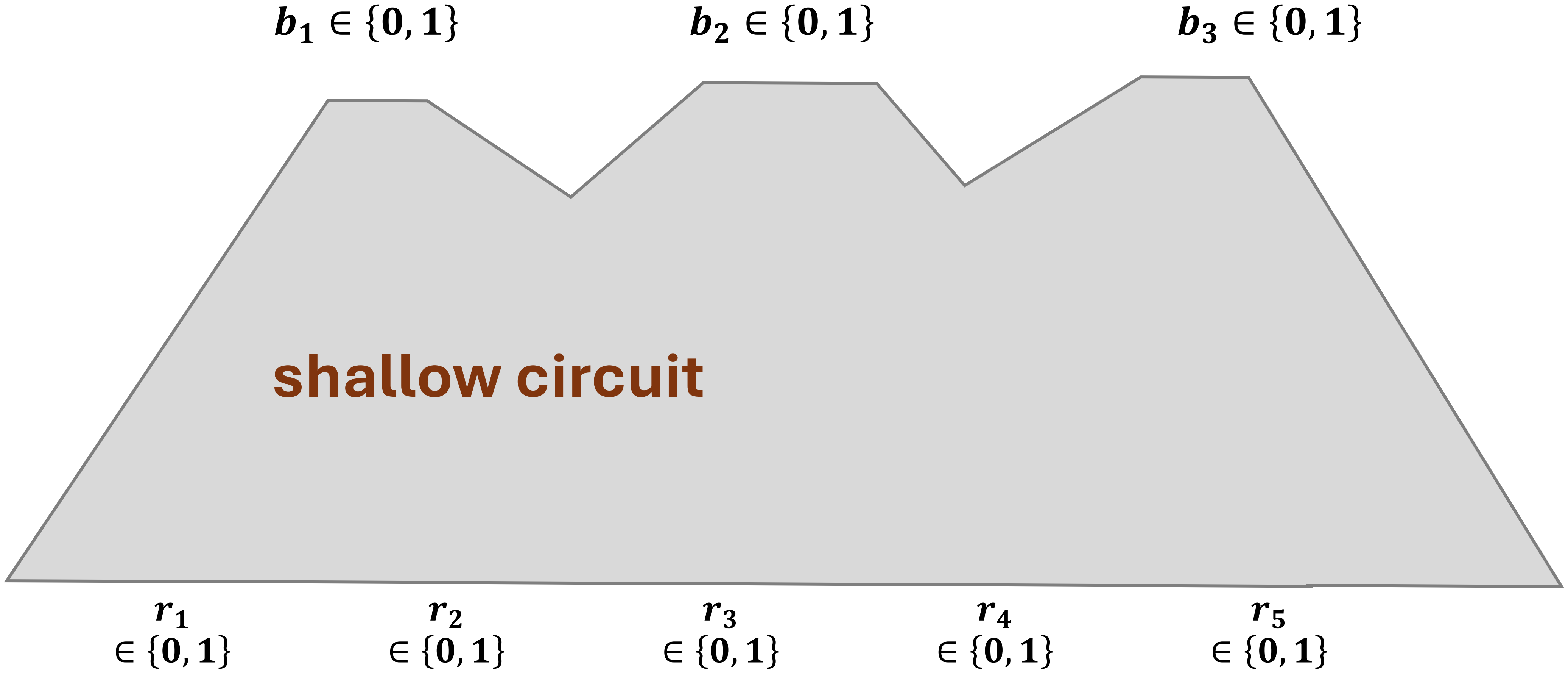
What distributions can a shallow circuit produce?



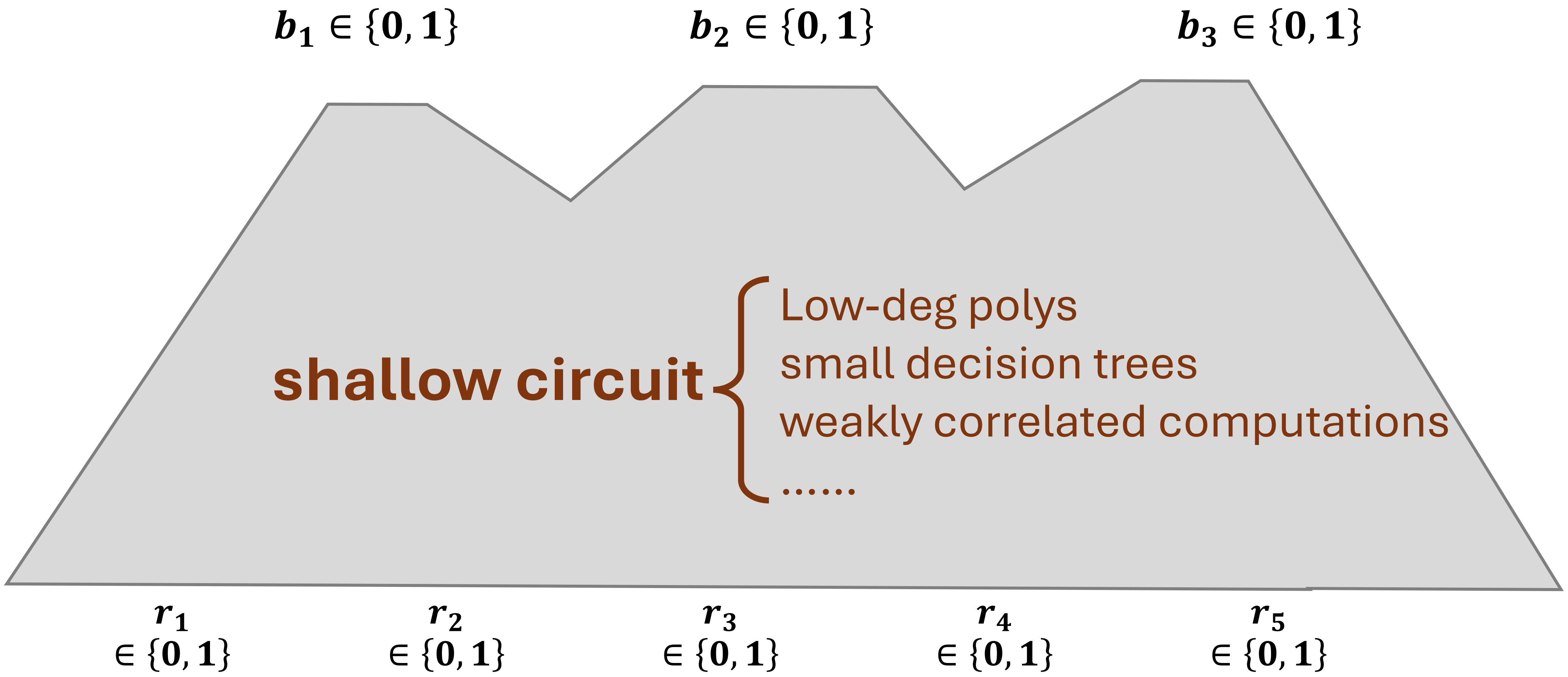
What distributions can a shallow circuit produce?



What distributions can a shallow circuit produce?

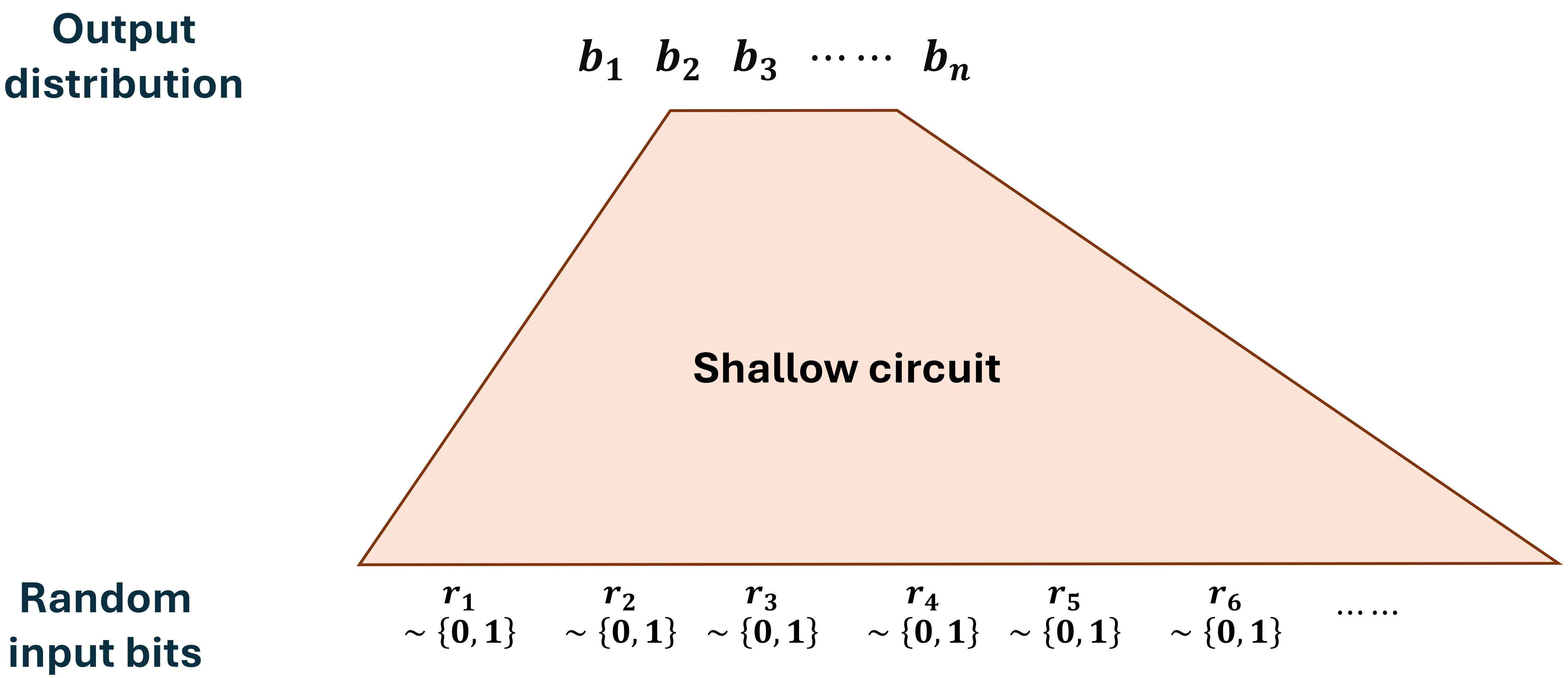


What distributions can a shallow circuit produce?



What distributions can a shallow circuit produce?

What distributions can a shallow circuit produce?



What distributions can a shallow circuit produce?

Output distribution

$D = (b_1, \ b_2, \ b_3, \ \cdots\cdots, \ b_n)$ over $\{0, 1\}^n$

What distributions can a shallow circuit produce?

uniform symmetric

Output distribution $\boldsymbol{D} = (\boldsymbol{b}_1, \ \boldsymbol{b}_2, \ \boldsymbol{b}_3, \ \cdots\cdots, \ \boldsymbol{b}_n)$ over $\{\mathbf{0}, \mathbf{1}\}^n$

What distributions can a shallow circuit produce?

uniform symmetric

Output distribution

$\boldsymbol{D} = (\boldsymbol{b}_1, \ \boldsymbol{b}_2, \ \boldsymbol{b}_3, \ \cdots\cdots, \ \boldsymbol{b}_n)$ over $\{\boldsymbol{0}, \boldsymbol{1}\}^{\boldsymbol{n}}$

Uniform.

$\boldsymbol{D}$ is uniform over its support

What distributions can a shallow circuit produce?

uniform symmetric

Output distribution

$D = (b_1,\ b_2,\ b_3,\ \cdots\cdots,\ b_n)$ over $\{0,1\}^n$

Uniform.

D is uniform over its support

Symmetric.

the support of D is symmetric

x in support iff $\pi(x)$ in support

What distributions can a shallow circuit produce?

uniform symmetric

Output distribution $D = (b_1,\ b_2,\ b_3,\ \cdots\cdots,\ b_n)$ over $\{0,1\}^n$

Uniform.

D is uniform over its support

Symmetric.

the support of D is symmetric

x in support iff $\pi(x)$ in support

Ex / Non-Ex.

Uniform over $\{0,1\}^n$

$1/3$-biased distribution

Uniform string of weight $n/2$

Point distribution on 0^n

What distributions can a shallow circuit produce?

uniform symmetric

Motivations.

Natural question on its own

What distributions can a shallow circuit produce?

uniform symmetric

What can shallow circuits do?

Motivations.

Natural question on its own

What distributions can a shallow circuit produce?

uniform symmetric

What can shallow circuits do?

Motivations.

Natural question on its own

Computation.
It cannot compute

$$f(x_1, \ldots, x_{n-1}) = x_1 \oplus \cdots \oplus x_{n-1}$$

What distributions can a shallow circuit produce?

uniform symmetric

What can shallow circuits do?

Motivations.

Natural question on its own

Computation.
It cannot compute

$$\boldsymbol{f(x_1, \ldots, x_{n-1}) = x_1 \oplus \cdots \oplus x_{n-1}}$$

Sampling.

$$(x_1, \ldots, x_{n-1}, x_1 \oplus \cdots \oplus x_{n-1})$$

What distributions can a shallow circuit produce?

uniform symmetric

What can shallow circuits do?

Motivations.

Natural question on its own

Computation.
It cannot compute

$$f(x_1, \dots, x_{n-1}) = x_1 \oplus \cdots \oplus x_{n-1}$$

Sampling.
It *can* sample

$$(x_1, \dots, x_{n-1}, x_1 \oplus \cdots \oplus x_{n-1})$$
$$\parallel$$
$$(y_1 \oplus y_2, y_2 \oplus y_3, \dots, y_n \oplus y_1)$$

What distributions can a shallow circuit produce?

uniform symmetric

What can shallow circuits do?

Motivations.

Natural question on its own

Computation.
It cannot compute

$$f(x_1, \dots, x_{n-1}) = x_1 \oplus \cdots \oplus x_{n-1}$$

Sampling.
It *can* sample

$$(x_1, \dots, x_{n-1}, x_1 \oplus \cdots \oplus x_{n-1})$$
$$\|$$
$$(y_1 \oplus y_2, y_2 \oplus y_3, \dots, y_n \oplus y_1)$$

Other examples like this?

What distributions can a shallow circuit produce?

uniform symmetric

What can shallow circuits do?

Motivations.

Natural question on its own

Computation.
It cannot compute

$$f(x_1, \dots, x_{n-1}) = x_1 \oplus \cdots \oplus x_{n-1}$$

Sampling.
It *can* sample

$$(x_1, \dots, x_{n-1}, x_1 \oplus \cdots \oplus x_{n-1})$$
$$\parallel$$
$$(y_1 \oplus y_2, y_2 \oplus y_3, \dots, y_n \oplus y_1)$$

Other examples like this? No! [KOW'25+]

What distributions can a shallow circuit produce?

uniform symmetric

Motivations.

Natural question on its own

Data structure lower bounds [Vio’12, FLRS’23, KOW’24]

What distributions can a shallow circuit produce?

uniform symmetric

Dictionary Problem.
Given an $\boldsymbol{n}$-bit string $\boldsymbol{x}$ of weight $\mathbf{0}$ modulo $\mathbf{127}$
Store it as some $\boldsymbol{s}$-bit string $\boldsymbol{h}$ such that
each $\boldsymbol{x_i}$ can be recovered *easily* from $\boldsymbol{h}$

What distributions can a shallow circuit produce?

uniform symmetric

Jan 27

Dictionary Problem.

Given an n-bit string x of weight 0 modulo 127

Store it as some s-bit string h such that

each x_i can be recovered *easily* from h

What distributions can a shallow circuit produce?

uniform symmetric

Dictionary Problem.
Given an n-bit string x of weight 0 modulo 127
Store it as some s-bit string h such that
each x_i can be recovered *easily* from h

Max Efficiency.
Store $h = x$

What distributions can a shallow circuit produce?

uniform symmetric

Dictionary Problem.
Given an $\boldsymbol{n}$-bit string $\boldsymbol{x}$ of weight $\mathbf{0}$ modulo $\mathbf{127}$
Store it as some $\boldsymbol{s}$-bit string $\boldsymbol{h}$ such that
each $\boldsymbol{x_i}$ can be recovered *easily* from $\boldsymbol{h}$

Max Efficiency.
Store $\boldsymbol{h} = \boldsymbol{x}$

$\boldsymbol{s} = \boldsymbol{n}$

$\mathbf{1}$ bit of $\boldsymbol{h}$ to decode $\boldsymbol{x_i}$

What distributions can a shallow circuit produce?

uniform symmetric

Dictionary Problem.
Given an n-bit string x of weight 0 modulo 127
Store it as some s-bit string h such that
each x_i can be recovered *easily* from h

Max Efficiency.
Store $h = x$

$s = n$

1 bit of h to decode x_i

Min Storage.
Only $\approx 2^n/127$ possible x
Store h as the index

What distributions can a shallow circuit produce?

uniform symmetric

Dictionary Problem.
Given an $\boldsymbol{n}$-bit string $\boldsymbol{x}$ of weight $\mathbf{0}$ modulo $\mathbf{127}$
Store it as some $\boldsymbol{s}$-bit string $\boldsymbol{h}$ such that
each $\boldsymbol{x_i}$ can be recovered *easily* from $\boldsymbol{h}$

Max Efficiency.
Store $\boldsymbol{h} = \boldsymbol{x}$

$\boldsymbol{s} = \boldsymbol{n}$

$\mathbf{1}$ bit of $\boldsymbol{h}$ to decode $\boldsymbol{x_i}$

Min Storage.
Only $\approx \mathbf{2}^{\boldsymbol{n}}/\mathbf{127}$ possible $\boldsymbol{x}$
Store $\boldsymbol{h}$ as the index

$\boldsymbol{s} = \log(\mathbf{2}^{\boldsymbol{n}}/\mathbf{127}) = \boldsymbol{n} - \mathbf{6}$

Read entire $\boldsymbol{h}$ to decode $\boldsymbol{x_i}$

What distributions can a shallow circuit produce?

uniform symmetric

Dictionary Problem.
Given an n-bit string x of weight 0 modulo 127
Store it as some s-bit string h such that
each x_i can be recovered *easily* from h

Max Efficiency.

1 bit of h to decode x_i

Min Storage.

$$s = \log(2^n/127) = n - 6$$

Can we achieve both?

What distributions can a shallow circuit produce?

uniform symmetric

Dictionary Problem.
Given an $\boldsymbol{n}$-bit string $\boldsymbol{x}$ of weight $\mathbf{0}$ modulo $\mathbf{127}$
Store it as some $\boldsymbol{s}$-bit string $\boldsymbol{h}$ such that
each $\boldsymbol{x_i}$ can be recovered *easily* from $\boldsymbol{h}$

Max Efficiency.

$\mathbf{1}$ bit of $\boldsymbol{h}$ to decode $\boldsymbol{x_i}$

Min Storage.

$$\boldsymbol{s} = \mathbf{log}(\mathbf{2}^{\boldsymbol{n}}/\mathbf{127}) = \boldsymbol{n} - \mathbf{6}$$

Can we achieve both?

No! [KOW'24]

What distributions can a shallow circuit produce?

uniform symmetric

Dictionary Problem.
Given an $\boldsymbol{n}$-bit string $\boldsymbol{x}$ of weight $\mathbf{0}$ modulo $\mathbf{127}$
Store it as some $\boldsymbol{s}$-bit string $\boldsymbol{h}$ such that
each $\boldsymbol{x_i}$ can be recovered *easily* from $\boldsymbol{h}$

Max Efficiency.

$\mathbf{1}$ bit of $\boldsymbol{h}$ to decode $\boldsymbol{x_i}$

Min Storage.

$\boldsymbol{s} = \log(2^n/127) = \boldsymbol{n} - 6$

Either read $\boldsymbol{\omega(1)}$ bits of $\boldsymbol{h}$
Or $\boldsymbol{h}$ has length $\boldsymbol{n}$

What distributions can a shallow circuit produce?

uniform symmetric

Motivations.

Natural question on its own

Data structure lower bounds [Vio'12, FLRS'23, KOW'24]

What distributions can a shallow circuit produce?

uniform symmetric

Motivations.

Natural question on its own

Data structure lower bounds [Vio’12, FLRS’23, KOW’24]

Quantum-classical separation [BGK’18, WP’23, KOW’24]

What distributions can a shallow circuit produce?

uniform symmetric

Motivations.

Natural question on its own

Data structure lower bounds [Vio'12, FLRS'23, KOW'24]

Quantum-classical separation [BGK'18, WP'23, KOW'24]

Can quantum shallow circuit generate distributions that are classically hard?

What distributions can a shallow circuit produce?

uniform symmetric

Motivations.

Natural question on its own

Data structure lower bounds [Vio'12, FLRS'23, KOW'24]

Quantum-classical separation [BGK'18, WP'23, KOW'24]

Can quantum shallow circuit generate distributions that are classically hard? Yes!

Formal Set-Up

Formal Set-Up

Shallow circuit

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \rightarrow \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Formal Set-Up

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

Formal Set-Up

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \rightarrow \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

When is $\boldsymbol{f}(\boldsymbol{U})$ uniform symmetric?

Example 1

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \rightarrow \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

When is $\boldsymbol{f}(\boldsymbol{U})$ uniform symmetric?

$\boldsymbol{f}(\boldsymbol{U}) \equiv \mathbf{0}^{\boldsymbol{n}}$

zeros

Example 2

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

When is $\boldsymbol{f}(\boldsymbol{U})$ uniform symmetric?

$\boldsymbol{f}(\boldsymbol{U}) \equiv \mathbf{0}^{\boldsymbol{n}}$

zeros

$\boldsymbol{f}(\boldsymbol{U}) \equiv \mathbf{1}^{\boldsymbol{n}}$

ones

Example 3

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

When is $\boldsymbol{f}(\boldsymbol{U})$ uniform symmetric?

$f(U) \equiv 0^n$	$f(U) \equiv 1^n$	$f(U) \sim \{0^n, 1^n\}$
zeros	ones	zeros-or-ones

Example 4

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

When is $\boldsymbol{f}(\boldsymbol{U})$ uniform symmetric?

$|\boldsymbol{f}(\boldsymbol{U})| \equiv \mathbf{0} \bmod \mathbf{2}$

evens

Example 4

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

When is $\boldsymbol{f}(\boldsymbol{U})$ uniform symmetric?

$|\boldsymbol{f}(\boldsymbol{U})| \equiv \mathbf{0} \bmod \mathbf{2}$

$(\boldsymbol{r}_1 \oplus \boldsymbol{r}_2, \boldsymbol{r}_2 \oplus \boldsymbol{r}_3, \boldsymbol{r}_3 \oplus \boldsymbol{r}_4, \dots, \boldsymbol{r}_n \oplus \boldsymbol{r}_1)$

evens

Example 5

Let $\boldsymbol{f}: \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

When is $\boldsymbol{f}(\boldsymbol{U})$ uniform symmetric?

$|\boldsymbol{f}(\boldsymbol{U})| \equiv \mathbf{1} \bmod \mathbf{2}$

odds

$(\boldsymbol{r}_1 \oplus \boldsymbol{r}_2, \boldsymbol{r}_2 \oplus \boldsymbol{r}_3, \boldsymbol{r}_3 \oplus \boldsymbol{r}_4, \dots, \boldsymbol{r}_n \oplus \boldsymbol{r}_1 \oplus \mathbf{1})$

Example 6

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \rightarrow \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

When is $\boldsymbol{f}(\boldsymbol{U})$ uniform symmetric?

$\boldsymbol{f}(\boldsymbol{U}) \sim \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$

evens-or-odds

Examples

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

When is $\boldsymbol{f}(\boldsymbol{U})$ uniform symmetric?

zeros ones zeros-or-ones evens odds evens-or-odds

Examples

Let $\boldsymbol{f}: \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

When is $\boldsymbol{f}(\boldsymbol{U})$ uniform symmetric?

zeros ones zeros-or-ones evens odds evens-or-odds

Uniform over weight $\leq \mathbf{10}$?
Uniform over weight $\boldsymbol{n}/\mathbf{2}$?
Uniform over weight $\mathbf{0}$ modulo $\mathbf{3}$?
……

Examples

Let $\boldsymbol{f}\colon \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

When is $\boldsymbol{f}(\boldsymbol{U})$ uniform symmetric?

zeros ones zeros-or-ones evens odds evens-or-odds

Conjecture [Filmus-Leigh-Riazanov-Sokolov'23]. No other examples

$\boldsymbol{n}$ sufficiently large

Our Result

Let $\boldsymbol{f}: \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$ be a **local** function

each output bit depends on **constant** number of input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

When is $\boldsymbol{f}(\boldsymbol{U})$ uniform symmetric?

zeros ones zeros-or-ones evens odds evens-or-odds

Theorem [KOW'25+]. No other examples

$\boldsymbol{n}$ sufficiently large

Robust and Quantitative

Let $\boldsymbol{f}\colon \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$ be a $\boldsymbol{d}$**-local** function

each output bit depends on $\boldsymbol{d}$ input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

Robust and Quantitative

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \rightarrow \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a $\boldsymbol{d}$**-local** function

each output bit depends on $\boldsymbol{d}$ input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

If $\boldsymbol{f}(\boldsymbol{U})$ is $\boldsymbol{\epsilon}$-close to a uniform symmetric distribution

Robust and Quantitative

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \rightarrow \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a $\boldsymbol{d}$**-local** function

each output bit depends on $\boldsymbol{d}$ input bits

Define $\boldsymbol{U}$ to be the uniform distribution over $\{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}}$

Define $\boldsymbol{f}(\boldsymbol{U})$ be the output distribution of $\boldsymbol{f}$ under $\boldsymbol{U}$

Theorem [KOW'25+].

If $\boldsymbol{f}(\boldsymbol{U})$ is $\boldsymbol{\epsilon}$-close to a uniform symmetric distribution, then $\boldsymbol{f}(\boldsymbol{U})$ is $\boldsymbol{O}_{\boldsymbol{d}}(\boldsymbol{\epsilon})$-close to one of the following six

zeros ones zeros-or-ones evens odds evens-or-odds

$\boldsymbol{n}$ sufficiently large

Takeaway

$f(U) \equiv 0^n$	$f(U) \equiv 1^n$	$f(U) \sim \{0^n, 1^n\}$
zeros	ones	zeros-or-ones
$\lvert f(U) \rvert \equiv 0 \bmod 2$	$\lvert f(U) \rvert \equiv 1 \bmod 2$	$f(U) \sim \{0, 1\}^n$
evens	odds	evens-or-odds

Takeaway

$f(U) \equiv 0^n$

0-local

zeros

$f(U) \equiv 1^n$

0-local

ones

$f(U) \sim \{0^n, 1^n\}$

1-local

zeros-or-ones

$|f(U)| \equiv 0 \bmod 2$

2-local

evens

$|f(U)| \equiv 1 \bmod 2$

2-local

odds

$f(U) \sim \{0, 1\}^n$

1-local

evens-or-odds

Takeaway

$f(U) \equiv 0^n$

0-local

zeros

$f(U) \equiv 1^n$

0-local

ones

$f(U) \sim \{0^n, 1^n\}$

1-local

zeros-or-ones

$|f(U)| \equiv 0 \bmod 2$

2-local

evens

$|f(U)| \equiv 1 \bmod 2$

2-local

odds

$f(U) \sim \{0, 1\}^n$

1-local

evens-or-odds

For uniform symmetric distributions,
*locality of **large constant** is the same as locality of **two***

Proof Overview

zeros ones zeros-or-ones evens odds evens-or-odds

Proof Overview

How to rule out

- Uniform over weight $n/3$
- Uniform over weight $\geq n/2$

zeros ones zeros-or-ones evens odds evens-or-odds

Proof Overview

How to rule out

Uniform over weight $n/3$

Uniform over weight $\geq n/2$

General case

zeros ones zeros-or-ones evens odds evens-or-odds

Weight $\boldsymbol{n/3}$

$\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ is a **local** function

$\boldsymbol{f(U)}$ is the output dist of $\boldsymbol{f}$ under uniform input

Why can't $\boldsymbol{f(U)}$ be uniform over $\boldsymbol{n}$-bit strings of weight $\boldsymbol{n/3}$?

Weight $\boldsymbol{n/3}$

$\boldsymbol{f}: \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$ is a **local** function

$\boldsymbol{f(U)}$ is the output dist of $\boldsymbol{f}$ under uniform input

Why can't $\boldsymbol{f(U)}$ be uniform over $\boldsymbol{n}$-bit strings of weight $\boldsymbol{n/3}$?

Granularity issue!

Weight $n/3$

$f: \{0,1\}^m \to \{0,1\}^n$ is a **local** function

$f(U)$ is the output dist of f under uniform input

Why can't $f(U)$ be uniform over n-bit strings of weight $n/3$?

Granularity issue!

Marginal bias should be $1/3$

Weight $n/3$

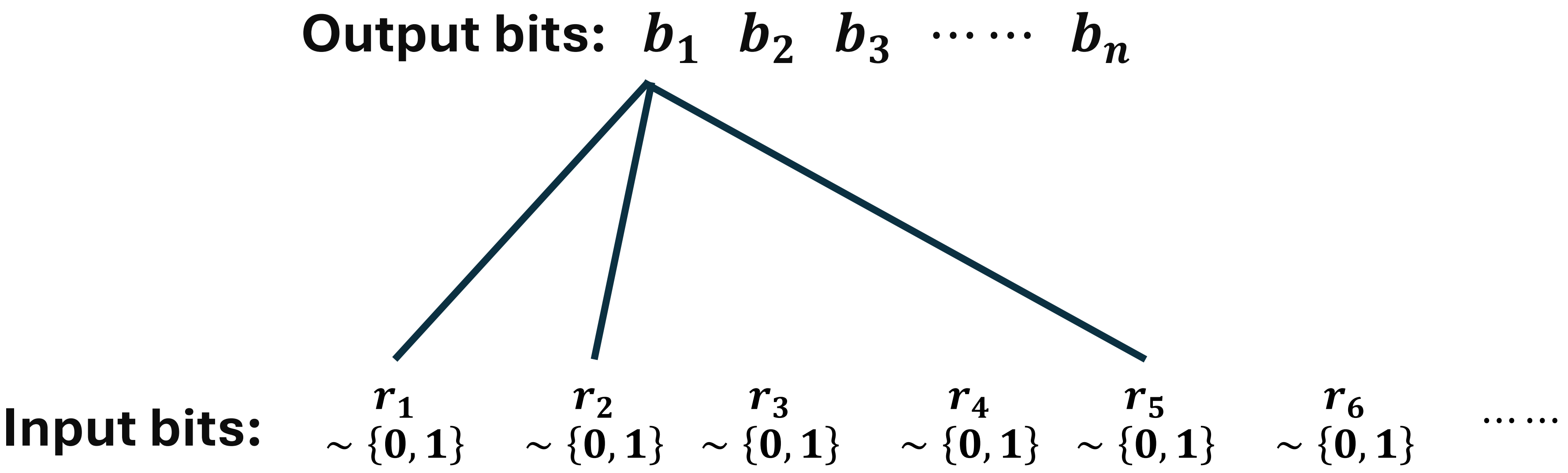
$f: \{0,1\}^m \to \{0,1\}^n$ is a **local** function

$f(U)$ is the output dist of f under uniform input

Why can't $f(U)$ be uniform over n-bit strings of weight $n/3$?

Granularity issue!

Marginal bias should be $1/3$



Weight $n/3$

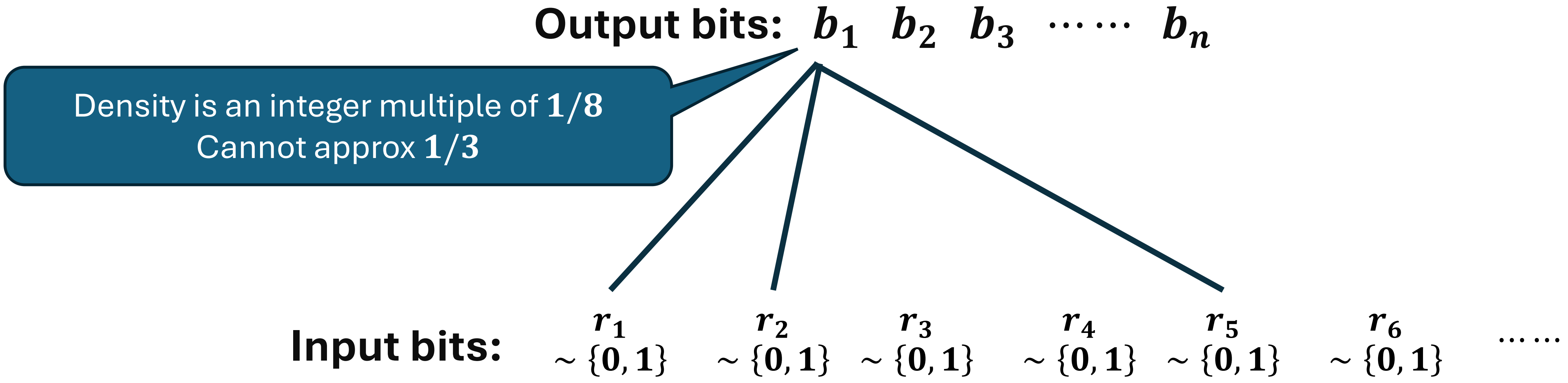
$f: \{0,1\}^m \to \{0,1\}^n$ is a **local** function

$f(U)$ is the output dist of f under uniform input

Why can't $f(U)$ be uniform over n-bit strings of weight $n/3$?

Granularity issue!

Marginal bias should be $1/3$



Weight $n/3$

$f: \{0,1\}^m \to \{0,1\}^n$ is a **local** function

$f(U)$ is the output dist of f under uniform input

By granularity, each output bit produces $\Omega(1)$ distance

Weight $\boldsymbol{n/3}$

$\boldsymbol{f}: \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}} \rightarrow \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$ is a **local** function

$\boldsymbol{f(U)}$ is the output dist of $\boldsymbol{f}$ under uniform input

By granularity, each output bit produces $\boldsymbol{\Omega(1)}$ distance

By concentration, $\boldsymbol{K}$ *independent* output bits produce $\boldsymbol{1-e^{-\Omega(K)}}$ distance

Weight $n/3$

$f: \{0,1\}^m \to \{0,1\}^n$ is a **local** function

$f(U)$ is the output dist of f under uniform input

By granularity, each output bit produces $\Omega(1)$ distance

By concentration, K *independent* output bits produce $1 - e^{-\Omega(K)}$ distance

Structural Lemma.
Conditioning on $o(n)$ input bits, we can find $\Omega(n)$ *independent* output bits.

Weight $\boldsymbol{n/3}$

$\boldsymbol{f}: \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$ is a **local** function

$\boldsymbol{f}(\boldsymbol{U})$ is the output dist of $\boldsymbol{f}$ under uniform input

By granularity, each output bit produces $\boldsymbol{\Omega}(\mathbf{1})$ distance

By concentration, $\boldsymbol{K}$ *independent* output bits produce $\mathbf{1} - \boldsymbol{e}^{-\boldsymbol{\Omega}(\boldsymbol{K})}$ distance

Structural Lemma.
Conditioning on $\boldsymbol{o}(\boldsymbol{n})$ input bits, we can find $\boldsymbol{\Omega}(\boldsymbol{n})$ *independent* output bits.

After conditioning, we have $\mathbf{1} - \boldsymbol{e}^{-\boldsymbol{\Omega}(\boldsymbol{n})}$ distance

Weight $n/3$

$f: \{0,1\}^m \to \{0,1\}^n$ is a **local** function

$f(U)$ is the output dist of f under uniform input

By granularity, each output bit produces $\Omega(1)$ distance

By concentration, K *independent* output bits produce $1 - e^{-\Omega(K)}$ distance

Structural Lemma.
Conditioning on $o(n)$ input bits, we can find $\Omega(n)$ *independent* output bits.

After conditioning, we have $1 - e^{-\Omega(n)}$ distance

By union bound over $2^{o(n)}$ conditioning, the distance is $1 - 2^{o(n)} \cdot e^{-\Omega(n)} = 1 - e^{-\Omega(n)}$

Weight $\geq \boldsymbol{n/2}$

$\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ is a **local** function

$\boldsymbol{f(U)}$ is the output dist of $\boldsymbol{f}$ under uniform input

Why can't $\boldsymbol{f(U)}$ be uniform over $\boldsymbol{n}$-bit strings of weight $\geq \boldsymbol{n/2}$?

Weight $\geq n/2$

$f: \{0,1\}^m \to \{0,1\}^n$ is a **local** function

$f(U)$ is the output dist of f under uniform input

Why can't $f(U)$ be uniform over n-bit strings of weight $\geq n/2$?

Marginal bias should be $1/2$

Weight $\geq n/2$

$f: \{0,1\}^m \to \{0,1\}^n$ is a **local** function

$f(U)$ is the output dist of f under uniform input

Why can't $f(U)$ be uniform over n-bit strings of weight $\geq n/2$?

Granularity argument does not work

Marginal bias should be $1/2$

Weight $\geq \boldsymbol{n}/2$

$\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ is a **local** function

$\boldsymbol{f}(\boldsymbol{U})$ is the output dist of $\boldsymbol{f}$ under uniform input

Why can't $\boldsymbol{f}(\boldsymbol{U})$ be uniform over $\boldsymbol{n}$-bit strings of weight $\geq \boldsymbol{n}/\mathbf{2}$?

Sharp cutoff!

$\boldsymbol{f}(\boldsymbol{U})$ cannot generate strong correlation to produce a sharp cutoff between $< \boldsymbol{n}/2$ and $\geq \boldsymbol{n}/2$

Weight $\geq n/2$

$f: \{0,1\}^m \to \{0,1\}^n$ is a **local** function

$f(U)$ is the output dist of f under uniform input

Why can't $f(U)$ be uniform over n-bit strings of weight $\geq n/2$?

Sharp cutoff!

$f(U)$ cannot generate strong correlation to produce a sharp cutoff between $< n/2$ and $\geq n/2$

Structural Lemma.
Conditioning on $o(n)$ input bits, we can find $\Omega(n)$ *independent* output bits.

Weight $\geq n/2$

$f: \{0,1\}^m \rightarrow \{0,1\}^n$ is a **local** function

$f(U)$ is the output dist of f under uniform input

Why can't $f(U)$ be uniform over n-bit strings of weight $\geq n/2$?

Sharp cutoff!

$f(U)$ cannot generate strong correlation to produce a sharp cutoff between $< n/2$ and $\geq n/2$

Structural Lemma.
Conditioning on $o(n)$ input bits, we can find $\Omega(n)$ *independent* output bits.

Sum of independent bits

Weight $\geq n/2$

$f: \{0,1\}^m \to \{0,1\}^n$ is a **local** function

$f(U)$ is the output dist of f under uniform input

Why can't $f(U)$ be uniform over n-bit strings of weight $\geq n/2$?

Sharp cutoff!

$f(U)$ cannot generate strong correlation to produce a sharp cutoff between $< n/2$ and $\geq n/2$

Structural Lemma.
Conditioning on $o(n)$ input bits, we can find $\Omega(n)$ *independent* output bits.

Sum of independent bits
$\Rightarrow$ Gaussian distribution
$\Rightarrow$ No sharp cutoff

Weight $\geq \boldsymbol{n/2}$: Caveat!

Structural Lemma.
Conditioning on $\boldsymbol{o(n)}$ input bits, we can find $\boldsymbol{\Omega(n)}$ *independent* output bits.

Not always correct!

Sum of independent bits
$\Rightarrow$ Gaussian distribution

Weight $\geq n/2$: Caveat!

Structural Lemma.
Conditioning on $o(n)$ input bits, we can find $\Omega(n)$ *independent* output bits.

Not always correct!

Sum of independent bits
⇒ Gaussian distribution

Independent bits do not necessarily imply Gaussian!

Weight $\geq \boldsymbol{n/2}$: Caveat!

Structural Lemma.
Conditioning on $\boldsymbol{o(n)}$ input bits, we can find $\boldsymbol{\Omega(n)}$ *independent* output bits.

Not always correct!

Sum of independent bits
⇒ Gaussian distribution

Independent bits do not necessarily imply Gaussian!

Ex.

$$\boldsymbol{x_1, \neg x_1, x_2, \neg x_2, x_3, \neg x_3, \ldots, x_{n/2}, \neg x_{n/2}}$$

Weight $\geq n/2$: Caveat!

Not always correct!

Structural Lemma.
Conditioning on $o(n)$ input bits, we can find $\Omega(n)$ *independent* output bits.

Sum of independent bits
$\Rightarrow$ Gaussian distribution

Independent bits do not necessarily imply Gaussian!

Ex.

$$x_1, \neg x_1, x_2, \neg x_2, x_3, \neg x_3, \ldots, x_{n/2}, \neg x_{n/2}$$

Many independent bits, but total weight is always $n/2$

Weight $\geq n/2$: Caveat!

Not always correct!

Structural Lemma.
Conditioning on $o(n)$ input bits, we can find $\Omega(n)$ *independent* output bits.

Sum of independent bits
$\Rightarrow$ Gaussian distribution

Independent bits do not necessarily imply Gaussian!

Ex.

$x_1, \neg x_1, x_2, \neg x_2, x_3, \neg x_3 \ldots, x_{n/2}, \neg x_{n/2}$

Fix.

Weight $\geq \boldsymbol{n/2}$: Caveat!

Structural Lemma.
Conditioning on $\boldsymbol{o(n)}$ input bits, we can find $\boldsymbol{\Omega(n)}$ *independent* output bits.

Not always correct!

Sum of independent bits
⇒ Gaussian distribution

Independent bits do not necessarily imply Gaussian!

Ex.

$$\boldsymbol{x_1, \neg x_1, x_2, \neg x_2, x_3, \neg x_3, \ldots, x_{n/2}, \neg x_{n/2}}$$

Fix.

Each *neighborhood* is far from unbiased
But the "weight $\geq \boldsymbol{n/2}$" distribution is

Weight $\geq \boldsymbol{n/2}$: full argument

Upgraded Structural Lemma.
Conditioning on $\boldsymbol{o(n)}$ input bits, we can find $\boldsymbol{\Omega(n)}$ *independent* output neighborhoods.

Weight $\geq n/2$: full argument

Upgraded Structural Lemma.
Conditioning on $o(n)$ input bits, we can find $\Omega(n)$ *independent* output neighborhoods.

Most neighborhoods are not close to unbiased

Each has $\Omega(1)$ distance

Independence

$1 - e^{-\Omega(n)}$ distance by concentration

Weight $\geq n/2$: full argument

Upgraded Structural Lemma.
Conditioning on $o(n)$ input bits, we can find $\Omega(n)$ *independent* output neighborhoods.

Most neighborhoods are not close to unbiased

Each has $\Omega(1)$ distance

Independence

$1 - e^{-\Omega(n)}$ distance by concentration

Most neighborhoods are close to unbiased

Weight distribution is like Gaussian

Property of Gaussians

Cannot generate sharp cutoff

Weight $\geq \boldsymbol{n/2}$: full argument

Upgraded Structural Lemma.
Conditioning on $\boldsymbol{o(n)}$ input bits, we can find $\boldsymbol{\Omega(n)}$ *independent* output neighborhoods.

Most neighborhoods are not close to unbiased

Each has $\boldsymbol{\Omega(1)}$ distance

Independence

$\boldsymbol{1 - e^{-\Omega(n)}}$ distance by concentration

Most neighborhoods are close to unbiased

Weight distribution is like Gaussian

Property of Gaussians

Cannot generate sharp cutoff

Large distance either way

General Case

To rule out any “weird” uniform symmetric distribution $\boldsymbol{D}$

General Case

To rule out any “weird” uniform symmetric distribution $\boldsymbol{D}$

have $\mathbf{0.5}\boldsymbol{n} \sim \mathbf{0.5}\boldsymbol{n} + \sqrt{\boldsymbol{n}}$, but not $\mathbf{0.5}\boldsymbol{n} - \sqrt{\boldsymbol{n}} \sim \mathbf{0.5}\boldsymbol{n}$

have $\boldsymbol{n}/\mathbf{2}$ and $\boldsymbol{n}/\mathbf{2} + \mathbf{10}$, but not $\boldsymbol{n}/\mathbf{2} + \mathbf{2}$

General Case

To rule out any "weird" uniform symmetric distribution $\boldsymbol{D}$

have $\mathbf{0.5}\boldsymbol{n} \sim \mathbf{0.5}\boldsymbol{n} + \sqrt{\boldsymbol{n}}$, but not $\mathbf{0.5}\boldsymbol{n} - \sqrt{\boldsymbol{n}} \sim \mathbf{0.5}\boldsymbol{n}$

have $\boldsymbol{n}/\mathbf{2}$ and $\boldsymbol{n}/\mathbf{2} + \mathbf{10}$, but not $\boldsymbol{n}/\mathbf{2} + \mathbf{2}$

Design a potential function $\boldsymbol{h}$ to witness the cutoffs

$\mathbf{E}_{x \sim D}[\boldsymbol{h}(|\boldsymbol{x}|)] \approx \mathbf{1}$ for the claimed distribution $\boldsymbol{D}$

$\mathbf{E}_{z \sim G}[\boldsymbol{h}(\boldsymbol{z})] \ll \mathbf{1}$ for Gaussian distributions $\boldsymbol{G}$

General Case

To rule out any “weird” uniform symmetric distribution $\boldsymbol{D}$

have $\mathbf{0.5}\boldsymbol{n} \sim \mathbf{0.5}\boldsymbol{n} + \sqrt{\boldsymbol{n}}$, but not $\mathbf{0.5}\boldsymbol{n} - \sqrt{\boldsymbol{n}} \sim \mathbf{0.5}\boldsymbol{n}$

have $\boldsymbol{n}/2$ and $\boldsymbol{n}/2 + \mathbf{10}$, but not $\boldsymbol{n}/2 + 2$

Design a potential function $\boldsymbol{h}$ to witness the cutoffs

$\mathbf{E}_{x\sim D}[\boldsymbol{h}(|\boldsymbol{x}|)] \approx \mathbf{1}$ for the claimed distribution $\boldsymbol{D}$

$\mathbf{E}_{z\sim G}[\boldsymbol{h}(\boldsymbol{z})] \ll \mathbf{1}$ for Gaussian distributions $\boldsymbol{G}$

Independent neighborhoods

General Case

To rule out any "weird" uniform symmetric distribution $\boldsymbol{D}$

have $\mathbf{0.5}\boldsymbol{n} \sim \mathbf{0.5}\boldsymbol{n} + \sqrt{\boldsymbol{n}}$, but not $\mathbf{0.5}\boldsymbol{n} - \sqrt{\boldsymbol{n}} \sim \mathbf{0.5}\boldsymbol{n}$

have $\boldsymbol{n}/2$ and $\boldsymbol{n}/2 + \mathbf{10}$, but not $\boldsymbol{n}/2 + 2$

Design a potential function $\boldsymbol{h}$ to witness the cutoffs

$\mathbf{E}_{x \sim D}[h(|x|)] \approx \mathbf{1}$ for the claimed distribution $\boldsymbol{D}$

$\mathbf{E}_{z \sim G}[h(z)] \ll \mathbf{1}$ for Gaussian distributions $\boldsymbol{G}$

Independent neighborhoods {

- Close to correct marginal
- Far from correct marginal

General Case

To rule out any "weird" uniform symmetric distribution $\boldsymbol{D}$

have $\mathbf{0.5}\boldsymbol{n} \sim \mathbf{0.5}\boldsymbol{n} + \sqrt{\boldsymbol{n}}$, but not $\mathbf{0.5}\boldsymbol{n} - \sqrt{\boldsymbol{n}} \sim \mathbf{0.5}\boldsymbol{n}$

have $\boldsymbol{n}/2$ and $\boldsymbol{n}/2 + \mathbf{10}$, but not $\boldsymbol{n}/2 + 2$

Design a potential function $\boldsymbol{h}$ to witness the cutoffs

$\mathbf{E}_{x\sim D}[\boldsymbol{h}(|\boldsymbol{x}|)] \approx \mathbf{1}$ for the claimed distribution $\boldsymbol{D}$

$\mathbf{E}_{z\sim G}[\boldsymbol{h}(\boldsymbol{z})] \ll \mathbf{1}$ for Gaussian distributions $\boldsymbol{G}$

Independent neighborhoods

- Close to correct marginal
- Far from correct marginal ⇒ large distance by concentration

General Case

To rule out any "weird" uniform symmetric distribution $\boldsymbol{D}$

have $\mathbf{0.5}\boldsymbol{n} \sim \mathbf{0.5}\boldsymbol{n} + \sqrt{\boldsymbol{n}}$, but not $\mathbf{0.5}\boldsymbol{n} - \sqrt{\boldsymbol{n}} \sim \mathbf{0.5}\boldsymbol{n}$

have $\boldsymbol{n}/\mathbf{2}$ and $\boldsymbol{n}/\mathbf{2} + \mathbf{10}$, but not $\boldsymbol{n}/\mathbf{2} + \mathbf{2}$

Design a potential function $\boldsymbol{h}$ to witness the cutoffs

$\mathbf{E}_{x \sim D}[\boldsymbol{h}(|\boldsymbol{x}|)] \approx \mathbf{1}$ for the claimed distribution $\boldsymbol{D}$

$\mathbf{E}_{z \sim G}[\boldsymbol{h}(\boldsymbol{z})] \ll \mathbf{1}$ for Gaussian distributions $\boldsymbol{G}$

Independent neighborhoods:

- Close to correct marginal ⇒ weight distribution is like Gaussian ⇒ impossible by potential function $\boldsymbol{h}$
- Far from correct marginal ⇒ large distance by concentration

General Case

To rule out any "weird" uniform symmetric distribution D

have $0.5n \sim 0.5n + \sqrt{n}$, but not $0.5n - \sqrt{n} \sim 0.5n$

have $n/2$ and $n/2 + 10$, but not $n/2 + 2$

Design a potential function h to witness th

$\mathbf{E}_{x \sim D}[h(|x|)] \approx 1$ for the claimed distribut

$\mathbf{E}_{z \sim G}[h(z)] \ll 1$ for Gaussian distributions G

Periodicity subtlety that allows evens, odds to be possible

Independent neighborhoods

- Close to correct marginal ⇒ weight distribution is like Gaussian ⇒ impossible by potential function h
- Far from correct marginal ⇒ large distance by concentration

Summary

Locally sampleable uniform symmetric distributions

zeros ones zeros-or-ones evens odds evens-or-odds

Summary

Locally sampleable uniform symmetric distributions

zeros ones zeros-or-ones evens odds evens-or-odds

Locally sampleable symmetric distributions?

Summary

Locally sampleable uniform symmetric distributions

zeros ones zeros-or-ones evens odds evens-or-odds

Locally sampleable symmetric distributions?

In progress: mixture of evens, odds, and $\boldsymbol{p}$-biased

$\boldsymbol{p}$ and the mixing weights should be dyadic rational with constant denominator

Summary

Locally sampleable uniform symmetric distributions

zeros ones zeros-or-ones evens odds evens-or-odds

Locally sampleable symmetric distributions?

In progress: mixture of evens, odds, and $\boldsymbol{p}$-biased

$\boldsymbol{p}$ and the mixing weights should be dyadic rational with constant denominator

Improving quantitative bounds?

Quantitative Bound

Let $f: \{0,1\}^m \to \{0,1\}^n$ be a d**-local** function

Theorem [KOW'25+]. If $n \geq \mathbf{tower}(d)$ and
$f(U)$ is ϵ-close to a uniform symmetric distribution,
then $f(U)$ is $(\epsilon \cdot \mathbf{tower}(d))$-close to one of the following six

zeros ones zeros-or-ones evens odds evens-or-odds

Quantitative Bound

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a $\boldsymbol{d}$**-local** function

Theorem [KOW'25+]. If $\boldsymbol{n} \geq \mathbf{tower}(\boldsymbol{d})$ and $\boldsymbol{f}(\boldsymbol{U})$ is $\boldsymbol{\epsilon}$-close to a uniform symmetric distribution, then $\boldsymbol{f}(\boldsymbol{U})$ is $(\boldsymbol{\epsilon} \cdot \mathbf{tower}(\boldsymbol{d}))$-close to one of the following six

zeros ones zeros-or-ones evens odds evens-or-odds

$\mathbf{tower}(\boldsymbol{d}) = \mathbf{2}^{\mathbf{2}^{\mathbf{2}^{\cdots}}}$ of height $\boldsymbol{d}$

Quantitative Bound

Let $\boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}} \to \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$ be a $\boldsymbol{d}$**-local** function

Theorem [KOW'25+]. If $\boldsymbol{n} \geq \mathbf{tower}(\boldsymbol{d})$ and
$\boldsymbol{f}(\boldsymbol{U})$ is $\boldsymbol{\epsilon}$-close to a uniform symmetric distribution,
then $\boldsymbol{f}(\boldsymbol{U})$ is $(\boldsymbol{\epsilon} \cdot \mathbf{tower}(\boldsymbol{d}))$-close to one of the following six

zeros ones zeros-or-ones evens odds evens-or-odds

Should be $\boldsymbol{\epsilon} \cdot \boldsymbol{O}(\mathbf{1})$
In progress

Quantitative Bound

Let $f: \{0,1\}^m \to \{0,1\}^n$ be a d-**local** function

Necessary for our structural lemma
But should be $\exp(d)$

Theorem [KOW'25+]. If $n \geq \mathbf{tower}(d)$ and
$f(U)$ is ϵ-close to a uniform symmetric distribution,
then $f(U)$ is $(\epsilon \cdot \mathbf{tower}(d))$-close to one of the following six

zeros ones zeros-or-ones evens odds evens-or-odds

Thank you!

kewen_wu@berkeley.edu
https://shlw.github.io