On the Degree of Boolean Functions as Polynomials over $\mathbb{Z}_m$

Xiaoming Sun[1] Yuan Sun[1] Jiaheng Wang[2] Kewen Wu[2]
Zhiyu Xia[1] Yufan Zheng[1]

[1]Institute of Computing Technology, Chinese Academy of Sciences

[2]Peking University

ICALP 2020

Power of Modular Counting

$\mathbf{AC}^0$: Unbounded fan-in constant-depth circuits with AND, OR and NOT gates.

Power of Modular Counting

$\mathbf{AC}^0[m]$: Unbounded fan-in constant-depth circuits with AND, OR, NOT and MOD^m gates.

Power of Modular Counting

$\mathbf{AC}^0[m]$: Unbounded fan-in constant-depth circuits with AND, OR, NOT and MOD^m gates.

Razborov-Smolensky: $\mathsf{MOD}^3_n \notin \mathbf{AC}^0[2]$.

Power of Modular Counting

$\mathbf{AC}^0[m]$: Unbounded fan-in constant-depth circuits with AND, OR, NOT and MOD^m gates.

Razborov-Smolensky: $\mathsf{MOD}_n^3 \notin \mathbf{AC}^0[2]$.

What about $\mathbf{AC}^0[6]$?

Power of Modular Counting

$\mathbf{AC}^0[m]$: Unbounded fan-in constant-depth circuits with AND, OR, NOT and MOD^m gates.

Razborov-Smolensky: $\text{MOD}_n^3 \notin \mathbf{AC}^0[2]$.

What about $\mathbf{AC}^0[6]$? We do not know whether $\mathbf{AC}^0[6] \supseteq \mathbf{NP}$ or not!

Power of Modular Counting

$\mathbf{AC}^0[m]$: Unbounded fan-in constant-depth circuits with AND, OR, NOT and MOD^m gates.

Razborov-Smolensky: $\mathrm{MOD}_n^3 \notin \mathbf{AC}^0[2]$.

What about $\mathbf{AC}^0[6]$? We do not know whether $\mathbf{AC}^0[6] \supseteq \mathbf{NP}$ or not!

Currently best upper bound of modular counting circuits: $\mathbf{ACC}^0 \not\supseteq \mathbf{NEXP}$, which builds on Williams' breakthrough algorithmic method for circuit lower bounds **[Williams, 2011]**.

Polynomial Representation and Degree

Represent every Boolean function $f : \{0,1\}^n \to \{0,1\}$ by polynomial:

$$\sum_{a\in\{0,1\}^n} f(a) \left(\prod_{i:a_i=1} x_i\right) \left(\prod_{i:a_i=0} (1-x_i)\right) =: \sum_{S\subseteq[n]} c_S \prod_{i\in S} x_i.$$

Polynomial Representation and Degree

Represent every Boolean function $f : \{0,1\}^n \to \{0,1\}$ by polynomial:

$$\sum_{a \in \{0,1\}^n} f(a) \left(\prod_{i : a_i = 1} x_i \right) \left(\prod_{i : a_i = 0} (1 - x_i) \right) =: \sum_{S \subseteq [n]} c_S \prod_{i \in S} x_i .$$

Over $\mathbb{Z}_m$:

$$\sum_{S \subseteq [n]} (c_S \bmod m) \prod_{i \in S} x_i .$$

Polynomial Representation and Degree

Represent every Boolean function $f : \{0,1\}^n \to \{0,1\}$ by polynomial:

$$\sum_{a \in \{0,1\}^n} f(a) \left(\prod_{i : a_i = 1} x_i \right) \left(\prod_{i : a_i = 0} (1 - x_i) \right) =: \sum_{S \subseteq [n]} c_S \prod_{i \in S} x_i.$$

Over $\mathbb{Z}_m$:

$$\sum_{S \subseteq [n]} (c_S \bmod m) \prod_{i \in S} x_i.$$

Definition (Degree)

The degree (resp. modulo-m degree) of a Boolean function f, denoted by $\deg(f)$ (resp. $\deg_m(f)$), is the degree of the polynomial that represents f over $\mathbb{Z}$ (resp. $\mathbb{Z}_m$).

Polynomial Representation and Degree

Represent every Boolean function $f : \{0,1\}^n \to \{0,1\}$ by polynomial:

$$\sum_{a \in \{0,1\}^n} f(a) \left(\prod_{i: a_i = 1} x_i \right) \left(\prod_{i: a_i = 0} (1 - x_i) \right) =: \sum_{S \subseteq [n]} c_S \prod_{i \in S} x_i.$$

Over $\mathbb{Z}_m$:

$$\sum_{S \subseteq [n]} (c_S \bmod m) \prod_{i \in S} x_i.$$

Definition (Degree)

The degree (resp. modulo-m degree) of a Boolean function f, denoted by $\deg(f)$ (resp. $\deg_m(f)$), is the degree of the polynomial that represents f over $\mathbb{Z}$ (resp. $\mathbb{Z}_m$).

$\deg(f)$ is polynomially related to many other complexity measures, e.g., block sensitivity, decision tree depth, and sensitivity **[Huang, 2019]**.

Polynomial Representation and Degree

Represent every Boolean function $f : \{0,1\}^n \to \{0,1\}$ by polynomial:

$$\sum_{a \in \{0,1\}^n} f(a) \left(\prod_{i : a_i = 1} x_i \right) \left(\prod_{i : a_i = 0} (1 - x_i) \right) =: \sum_{S \subseteq [n]} c_S \prod_{i \in S} x_i.$$

Over $\mathbb{Z}_m$:

$$\sum_{S \subseteq [n]} (c_S \bmod m) \prod_{i \in S} x_i.$$

Definition (Degree)

The degree (resp. modulo-m degree) of a Boolean function f, denoted by $\deg(f)$ (resp. $\deg_m(f)$), is the degree of the polynomial that represents f over $\mathbb{Z}$ (resp. $\mathbb{Z}_m$).

$\deg(f)$ is polynomially related to many other complexity measures, e.g., block sensitivity, decision tree depth, and sensitivity **[Huang, 2019]**.

What about $\deg_m(f)$?

Polynomial Representation and Degree

Consider $f = \mathsf{PARITY}_n$.

Polynomial Representation and Degree

Consider $f = \text{PARITY}_n$. The polynomial representing it is

$$\text{PARITY}_n(x) = \frac{1}{2} - \frac{1}{2}\prod_{i=1}^{n}(1 - 2x_i).$$

Polynomial Representation and Degree

Consider $f = \mathsf{PARITY}_n$. The polynomial representing it is

$$\mathsf{PARITY}_n(x) = \frac{1}{2} - \frac{1}{2}\prod_{i=1}^{n}(1 - 2x_i).$$

We have $\deg(f) = n$

Polynomial Representation and Degree

Consider $f = \mathsf{PARITY}_n$. The polynomial representing it is

$$\mathsf{PARITY}_n(x) = \frac{1}{2} - \frac{1}{2}\prod_{i=1}^{n}(1 - 2x_i).$$

We have $\deg(f) = n$ but $\deg_2(f) = 1$. Unbounded!

Polynomial Representation and Degree

Consider $f = \mathsf{PARITY}_n$. The polynomial representing it is

$$\mathsf{PARITY}_n(x) = \frac{1}{2} - \frac{1}{2}\prod_{i=1}^{n}(1 - 2x_i).$$

We have $\deg(f) = n$ but $\deg_2(f) = 1$. Unbounded!

Also $\deg_3(f) = n$.

Polynomial Representation and Degree

Consider $f = \mathsf{PARITY}_n$. The polynomial representing it is

$$\mathsf{PARITY}_n(x) = \frac{1}{2} - \frac{1}{2}\prod_{i=1}^{n}(1 - 2x_i).$$

We have $\deg(f) = n$ but $\deg_2(f) = 1$. Unbounded!

Also $\deg_3(f) = n$.

A function is *non-degenerated*, if it depends on all n input bits.

Theorem ([Gopalan, Lovett and Shpilka, 2009])

For all non-degenerated $f : \{0,1\}^n \to \{0,1\}$ *and different primes* p, q,

$$\deg_q(f) \geq \frac{n}{\lceil \log_2 p \rceil \deg_p(f) p^{2\deg_p(f)}}.$$

Polynomial Representation and Degree

Consider $f = \mathsf{PARITY}_n$. The polynomial representing it is

$$\mathsf{PARITY}_n(x) = \frac{1}{2} - \frac{1}{2}\prod_{i=1}^{n}(1-2x_i).$$

We have $\deg(f) = n$ but $\deg_2(f) = 1$. Unbounded!

Also $\deg_3(f) = n$.

A function is *non-degenerated*, if it depends on all n input bits.

Theorem ([Gopalan, Lovett and Shpilka, 2009])

For all non-degenerated $f : \{0,1\}^n \to \{0,1\}$ and different primes p, q,

$$\deg_q(f) \geq \frac{n}{\lceil \log_2 p \rceil \deg_p(f) p^{2\deg_p(f)}}.$$

i.e., Low $\deg_p(f)$ implies high $\deg_q(f)$.

Polynomial Representation and Degree

Consider $f = \mathsf{PARITY}_n$. The polynomial representing it is

$$\mathsf{PARITY}_n(x) = \frac{1}{2} - \frac{1}{2}\prod_{i=1}^{n}(1-2x_i).$$

We have $\deg(f) = n$ but $\deg_2(f) = 1$. Unbounded!

Also $\deg_3(f) = n$.

A function is *non-degenerated*, if it depends on all n input bits.

Theorem ([Gopalan, Lovett and Shpilka, 2009])

For all non-degenerated $f : \{0,1\}^n \to \{0,1\}$ and different primes p, q,

$$\deg_q(f) \geq \frac{n}{\lceil \log_2 p \rceil \deg_p(f) p^{2\deg_p(f)}}.$$

i.e., Low $\deg_p(f) = o(\log n)$ implies high $\deg_q(f) = \Omega(n^{1-o(1)})$.

Polynomial Representation and Degree

Consider $f = \text{PARITY}_n$. The polynomial representing it is

$$\text{PARITY}_n(x) = \frac{1}{2} - \frac{1}{2}\prod_{i=1}^{n}(1 - 2x_i).$$

We have $\deg(f) = n$ but $\deg_2(f) = 1$. Unbounded!

Also $\deg_3(f) = n$.

A function is *non-degenerated*, if it depends on all n input bits.

Theorem ([Gopalan, Lovett and Shpilka, 2009])

For all non-degenerated $f : \{0,1\}^n \to \{0,1\}$ and different primes p, q,

$$\deg_q(f) \geq \frac{n}{\lceil \log_2 p \rceil \deg_p(f) p^{2\deg_p(f)}}.$$

i.e., Low $\deg_p(f) = o(\log n)$ implies high $\deg_q(f) = \Omega(n^{1-o(1)})$.
By Chinese Remainder Theorem,

$$\deg_{pq}(f) = \max\{\deg_p(f), \deg_q(f)\}$$

Polynomial Representation and Degree

Consider $f = \mathsf{PARITY}_n$. The polynomial representing it is

$$\mathsf{PARITY}_n(x) = \frac{1}{2} - \frac{1}{2}\prod_{i=1}^{n}(1 - 2x_i).$$

We have $\deg(f) = n$ but $\deg_2(f) = 1$. Unbounded!

Also $\deg_3(f) = n$.

A function is *non-degenerated*, if it depends on all n input bits.

Theorem ([Gopalan, Lovett and Shpilka, 2009])

For all non-degenerated $f : \{0,1\}^n \to \{0,1\}$ and different primes p, q,

$$\deg_q(f) \geq \frac{n}{\lceil \log_2 p \rceil \deg_p(f) p^{2\deg_p(f)}}.$$

i.e., Low $\deg_p(f) = o(\log n)$ implies high $\deg_q(f) = \Omega(n^{1-o(1)})$.
By Chinese Remainder Theorem,

$$\deg_{pq}(f) = \max\{\deg_p(f), \deg_q(f)\} = \Omega(\log n).$$

$\deg_{pq}(f)$ vs $\deg(f)$

Conjecture

For any Boolean function f,

$$\deg(f) = O\left(\text{poly}\left(\deg_{pq}(f)\right)\right).$$

$\deg_{pq}(f)$ **vs** $\deg(f)$

Conjecture

For any Boolean function f,

$$\deg(f) = O\left(\text{poly}\left(\deg_{pq}(f)\right)\right).$$

Best separation so far is quadratic **[Li and Sun, 2017]**.

- There exists a sequence of Boolean functions $\{f_n\}$ with $\deg_{pq}(f_n) = O(\deg(f_n)^{1/2})$.

$\deg_{pq}(f)$ **vs** $\deg(f)$

Conjecture

For any Boolean function f,

$$\deg(f) = O\left(\text{poly}\left(\deg_{pq}(f)\right)\right).$$

Best separation so far is quadratic **[Li and Sun, 2017]**.

- There exists a sequence of Boolean functions $\{f_n\}$ with $\deg_{pq}(f_n) = O(\deg(f_n)^{1/2})$.

We call a function *symmetric* if its value only depends on the Hamming weight of the input.

$\deg_{pq}(f)$ **vs** $\deg(f)$

Conjecture

For any Boolean function f,

$$\deg(f) = O\left(\text{poly}\left(\deg_{pq}(f)\right)\right).$$

Best separation so far is quadratic **[Li and Sun, 2017]**.

- There exists a sequence of Boolean functions $\{f_n\}$ with $\deg_{pq}(f_n) = O(\deg(f_n)^{1/2})$.

We call a function *symmetric* if its value only depends on the Hamming weight of the input.

This conjecture is true for symmetric functions **[Lee et al., 2015]**.

Our Results

Theorem ([Li and Sun, 2017])

For any positive integer m with at least two different prime factors p, q and any non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$, we have

$$\deg_m(f) \geq \frac{1}{p+q} \cdot n.$$

Our Results

Theorem

For any positive integer m *with at least two different prime factors* p, q *and any non-trivial symmetric function* $f : \{0,1\}^n \to \{0,1\}$*, we have*

$$\deg_m(f) \geq \frac{1}{2 + \frac{1}{p-1} + \frac{1}{q-1}} \cdot n.$$

The factor cannot be improved to any constant larger than $1/2$.

Our Results

Theorem

For any positive integer m with at least two different prime factors p, q and any non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$, we have

$$\deg_m(f) \geq \frac{1}{2 + \frac{1}{p-1} + \frac{1}{q-1}} \cdot n.$$

The factor cannot be improved to any constant larger than $1/2$.

Theorem

For any prime p, positive integer k, and non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$ with sufficiently large n, we have

$$\deg_{p^k}(f) \geq (p-1) \cdot k.$$

The bound $(p-1) \cdot k$ is tight.

Our Results

Theorem

For any positive integer m with at least two different prime factors p, q and any non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$, we have

$$\deg_m(f) \geq \frac{1}{2 + \frac{1}{p-1} + \frac{1}{q-1}} \cdot n.$$

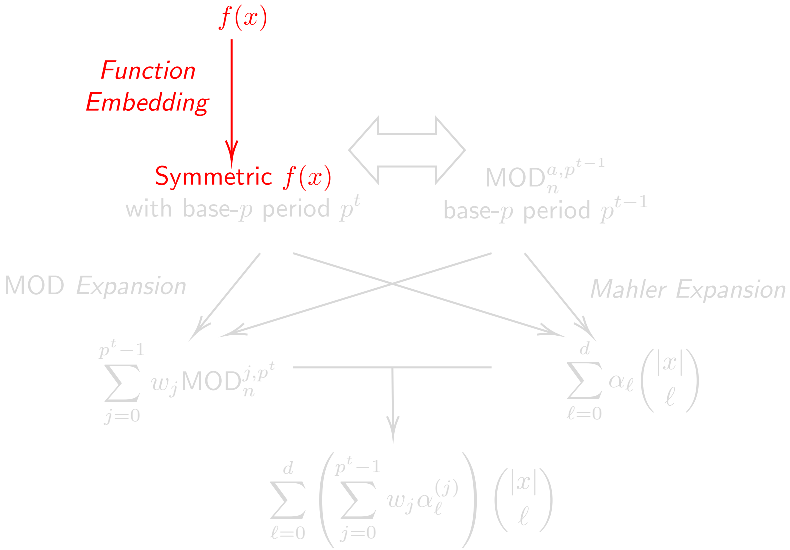
The factor cannot be improved to any constant larger than $1/2$.

Theorem

For any prime p, positive integer k, and non-degenerated function $f : \{0,1\}^n \to \{0,1\}$ with sufficiently large n, we have

$$\deg_{p^k}(f) \geq (p-1) \cdot k.$$

The bound $(p-1) \cdot k$ is tight.



$f(x)$
Function Embedding
Symmetric $f(x)$
with base-p period p^t
$\mathsf{MOD}_n^{a,p^{t-1}}$
base-p period p^{t-1}
MOD *Expansion*
Mahler Expansion
$\sum_{j=0}^{p^t-1} w_j \mathsf{MOD}_n^{j,p^t}$
$\sum_{\ell=0}^{d} \alpha_\ell \binom{|x|}{\ell}$
$\sum_{\ell=0}^{d} \left(\sum_{j=0}^{p^t-1} w_j \alpha_\ell^{(j)} \right) \binom{|x|}{\ell}$

Symmetric Function Embedding

Lemma

Let $f : \{0,1\}^n \to \{0,1\}$ be a non-degenerate Boolean function. Then there exists a set of indices $S \subseteq [n]$ with $|S| = \omega(1)$, and a restriction $\sigma : [n] \setminus S \to \{0,1\}$ such that $f|_\sigma$ is a non-trivial symmetric Boolean function.

$$f(x_1, x_2, x_3, x_4, x_5, x_6, \cdots, x_{n-1}, x_n)$$

Symmetric: $f(x_1,\ 1, x_3,\ 0,\ 0,\ 1, \cdots, x_{n-1},\ 1)$

$\#$ Free variables $= \omega(1)$.

Symmetric Function Embedding

Lemma

Let $f : \{0,1\}^n \to \{0,1\}$ be a non-degenerate Boolean function. Then there exists a set of indices $S \subseteq [n]$ with $|S| = \omega(1)$, and a restriction $\sigma : [n] \setminus S \to \{0,1\}$ such that $f|_\sigma$ is a non-trivial symmetric Boolean function.

$$f(x_1, x_2, x_3, x_4, x_5, x_6, \cdots, x_{n-1}, x_n)$$

Symmetric: $f(x_1,\ 1, x_3,\ 0,\ 0,\ 1, \cdots, x_{n-1},\ 1)$

$\#$ Free variables $= \omega(1)$.

Proved by hypergraph Ramsey theory.

Symmetric Function Embedding

Lemma

Let $f : \{0,1\}^n \to \{0,1\}$ be a non-degenerate Boolean function. Then there exists a set of indices $S \subseteq [n]$ with $|S| \geq r(n) = \omega(1)$, and a restriction $\sigma : [n]\backslash S \to \{0,1\}$ such that $f|_\sigma$ is a non-trivial symmetric Boolean function.

Suppose $M(f)$ is a complexity measure. If M is non-increasing w.r.t. restrictions (i.e., $M(f) \geq M(f|_\sigma)$), then

$$\forall \text{ symmetric } f,\ M(f) \geq h(n)$$
$$\implies \forall \text{ non-degenerated } f,\ M(f) \geq h(r(n)).$$

Symmetric Function Embedding

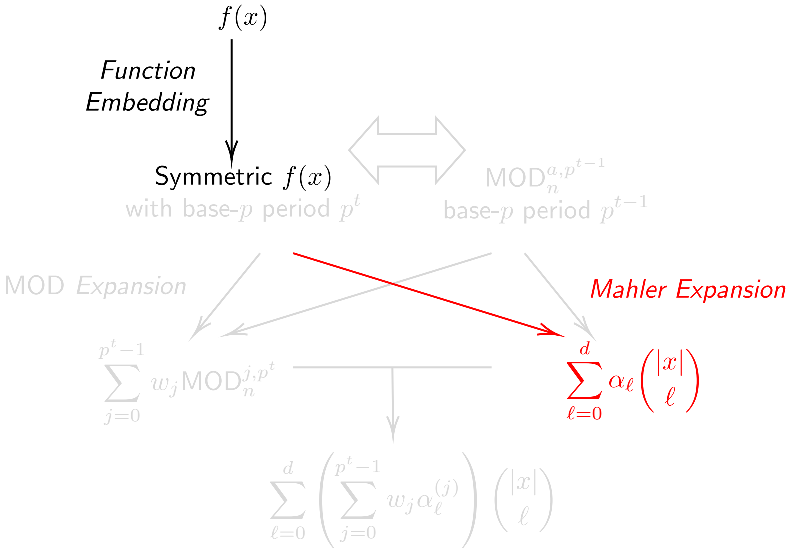
Lemma

Let $f : \{0,1\}^n \to \{0,1\}$ be a non-degenerate Boolean function. Then there exists a set of indices $S \subseteq [n]$ with $|S| \geq r(n) = \omega(1)$, and a restriction $\sigma : [n] \backslash S \to \{0,1\}$ such that $f|_\sigma$ is a non-trivial symmetric Boolean function.

Suppose $M(f)$ is a complexity measure. If M is non-increasing w.r.t. restrictions (i.e., $M(f) \geq M(f|_\sigma)$), then

$$\forall \text{ symmetric } f,\ M(f) \geq h(n)$$
$$\implies \forall \text{ non-degenerated } f,\ M(f) \geq h(r(n)).$$

$r(n) \approx \sqrt{\log^*(n)}$ grows extremely slow, but suffices for our purpose.


$f(x)$
Function Embedding
Symmetric $f(x)$
with base-p period p^t
$\mathsf{MOD}_n^{a,p^{t-1}}$
base-p period p^{t-1}
MOD *Expansion*
Mahler Expansion
$\sum_{j=0}^{p^t-1} w_j \mathsf{MOD}_n^{j,p^t}$
$\sum_{\ell=0}^{d} \alpha_\ell \binom{|x|}{\ell}$
$\sum_{\ell=0}^{d} \left(\sum_{j=0}^{p^t-1} w_j \alpha_\ell^{(j)} \right) \binom{|x|}{\ell}$

Mahler Expansion

For any symmetric f, let F be its univariate version, i.e., $F(|x|) = f(x)$.

Mahler Expansion

For any symmetric f, let F be its univariate version, i.e., $F(|x|) = f(x)$.

Several ways to represent $F(t)$:

Mahler Expansion

For any symmetric f, let F be its univariate version, i.e., $F(|x|) = f(x)$.

Several ways to represent $F(t)$:

- expanding by t^j (aka standard form);

Mahler Expansion

For any symmetric f, let F be its univariate version, i.e., $F(|x|) = f(x)$.

Several ways to represent $F(t)$:

- expanding by t^j (aka standard form);
- expanding by $\binom{t}{j}$ (aka Mahler expansion);

Mahler Expansion

For any symmetric f, let F be its univariate version, i.e., $F(|x|) = f(x)$.

Several ways to represent $F(t)$:

- expanding by t^j (aka standard form);
- expanding by $\binom{t}{j}$ (aka Mahler expansion);
- ...

Mahler Expansion

For any symmetric f, let F be its univariate version, i.e., $F(|x|) = f(x)$.

Several ways to represent $F(t)$:

- expanding by t^j (aka standard form);
- expanding by $\binom{t}{j}$ (aka Mahler expansion);
- ...

Theorem (Mahler expansion)

Assume that $f : \{0,1\}^n \to \{0,1\}$ is a symmetric Boolean function, and F is the corresponding univariate version. Let $d := \max\{n, m-1\}$. Then there exists a unique sequence $\alpha_0, \alpha_1, \cdots, \alpha_d \in \mathbb{Z}_m$ such that

$$\sum_{j=0}^{d} \alpha_j \binom{t}{j} = \begin{cases} F(t), & 0 \le t \le n; \\ 0, & n < m-1 \text{ and } n < t < m. \end{cases}$$

We call $\sum_{j=0}^{d} \alpha_j \binom{t}{j}$ the *Mahler expansion* of F over $\mathbb{Z}_m$, and α_j the j-th *Mahler coefficient*.

Mahler Expansion

For any symmetric f, let F be its univariate version, i.e., $F(|x|) = f(x)$.

Several ways to represent $F(t)$:

- expanding by t^j (aka standard form);
- expanding by $\binom{t}{j}$ (aka Mahler expansion);
- ...

Let $n = 2$ and $f(x) = x_0 \vee x_1$. On $\mathbb{Z}_5$, its Mahler expansion is

$$F(x) = \binom{|x|}{1} + 4\binom{|x|}{2} + 2\binom{|x|}{4}.$$

But $\deg_5(f) = 2$.

Mahler Expansion

For any symmetric f, let F be its univariate version, i.e., $F(|x|) = f(x)$.

Several ways to represent $F(t)$:

- expanding by t^j (aka standard form);
- expanding by $\binom{t}{j}$ (aka Mahler expansion);
- ...

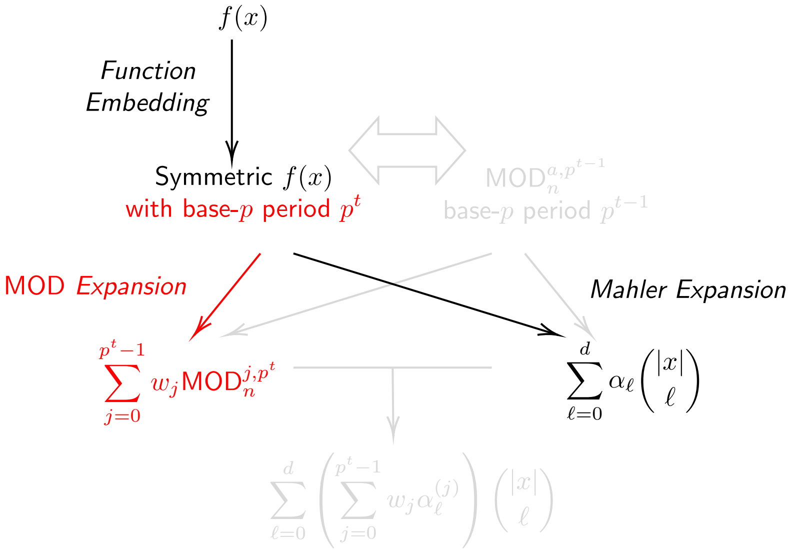
Let $n = 2$ and $f(x) = x_0 \vee x_1$. On $\mathbb{Z}_5$, its Mahler expansion is

$$F(x) = \binom{|x|}{1} + 4\binom{|x|}{2} + 2\binom{|x|}{4}.$$

But $\deg_5(f) = 2$.

Fact

$\deg_m(f) = \max\{\ell : \alpha_\ell \not\equiv 0 \pmod{m}, \ell \leq n\}$.


$f(x)$
Function Embedding
Symmetric $f(x)$
with base-p period p^t
$\mathsf{MOD}_n^{a,p^{t-1}}$
base-p period p^{t-1}
MOD Expansion
Mahler Expansion
$\sum_{j=0}^{p^t-1} w_j \mathsf{MOD}_n^{j,p^t}$
$\sum_{\ell=0}^{d} \alpha_\ell \binom{|x|}{\ell}$
$\sum_{\ell=0}^{d} \left(\sum_{j=0}^{p^t-1} w_j \alpha_\ell^{(j)} \right) \binom{|x|}{\ell}$

MOD **Function**

For any symmetric f, let F be its univariate version, i.e., $F(|x|) = f(x)$.

Several ways to represent $F(t)$:

- expanding by t^j (aka standard form);
- expanding by $\binom{t}{j}$ (aka Mahler expansion);
- expanding by MOD functions, provided F is *periodic*.
  - m-periodic: $F(a) = F(a+m), \forall a \in \{0, 1, \cdots, n-m\}$

MOD **Function**

For any symmetric f, let F be its univariate version, i.e., $F(|x|) = f(x)$.

Several ways to represent $F(t)$:

- expanding by t^j (aka standard form);
- expanding by $\binom{t}{j}$ (aka Mahler expansion);
- expanding by MOD functions, provided F is *periodic*.
  - m-periodic: $F(a) = F(a+m), \forall a \in \{0, 1, \cdots, n-m\}$

If $n \geq m-1$, define

$$\mathsf{MOD}_n^{c,m}(x) := \begin{cases} 0, & |x| \not\equiv c \pmod{m}; \\ 1, & |x| \equiv c \pmod{m}. \end{cases}$$

MOD **Function**

For any symmetric f, let F be its univariate version, i.e., $F(|x|) = f(x)$.

Several ways to represent $F(t)$:

- expanding by t^j (aka standard form);
- expanding by $\binom{t}{j}$ (aka Mahler expansion);
- expanding by MOD functions, provided F is *periodic*.
  - m-periodic: $F(a) = F(a+m), \forall a \in \{0, 1, \cdots, n-m\}$

If $n \geq m - 1$, define

$$\mathsf{MOD}_n^{c,m}(x) := \begin{cases} 0, & |x| \not\equiv c \pmod{m}; \\ 1, & |x| \equiv c \pmod{m}. \end{cases}$$

Every m-periodic function can be spanned by $\{\mathsf{MOD}_n^{a,m}(x)\}_{a=0}^{m-1}$.

MOD **Function**

If f is m^t-periodic but not m^{t-1}-periodic, then we call $\pi_m(f) := m^t$ the *base-m period* of f.

MOD Function

If f is m^t-periodic but not m^{t-1}-periodic, then we call $\pi_m(f) := m^t$ the *base-m period* of f.

- Example: The not-all-equal NAE function is defined as $\mathsf{NAE}_n(x_1, \ldots, x_n) := \mathbb{I}[\exists i, j \text{ s.t. } x_i \neq x_j]$. Then $\pi_3(\mathsf{NAE}_3) = 3$ while $\pi_3(\mathsf{NAE}_4) = 9$.

MOD **Function**

If f is m^t-periodic but not m^{t-1}-periodic, then we call $\pi_m(f) := m^t$ the *base-m period* of f.

- Example: The not-all-equal NAE function is defined as $\mathsf{NAE}_n(x_1, \ldots, x_n) := \mathbb{I}[\exists i, j \text{ s.t. } x_i \neq x_j]$. Then $\pi_3(\mathsf{NAE}_3) = 3$ while $\pi_3(\mathsf{NAE}_4) = 9$.

Theorem ([Wilson, 2006])

For prime p and positive integers t, k, denote $d := (k-1) \cdot \varphi(p^t) + p^t - 1$. Then for any $n \geq d$, we have $\deg_{p^k}(\mathsf{MOD}_n^{0,p^t}) = d$.

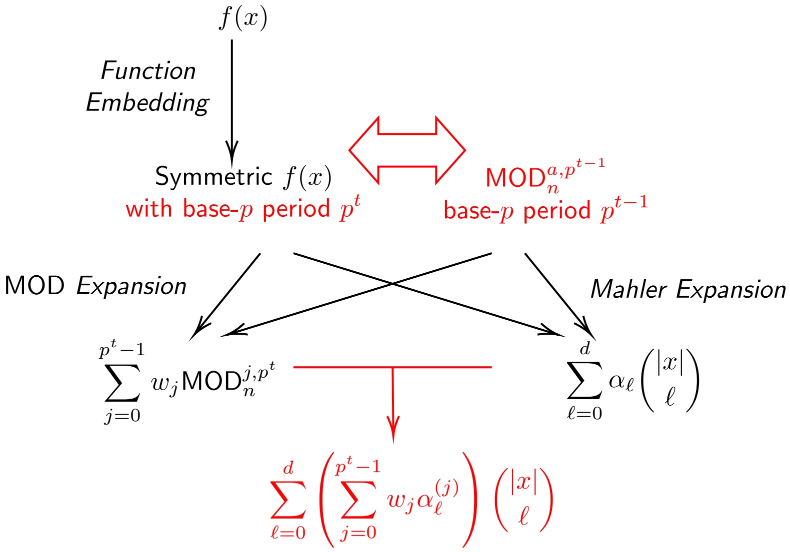
MOD **Function**

If f is m^t-periodic but not m^{t-1}-periodic, then we call $\pi_m(f) := m^t$ the *base-m period* of f.

- Example: The not-all-equal NAE function is defined as $\mathsf{NAE}_n(x_1, \dots, x_n) := \mathbb{I}[\exists i, j \text{ s.t. } x_i \neq x_j]$. Then $\pi_3(\mathsf{NAE}_3) = 3$ while $\pi_3(\mathsf{NAE}_4) = 9$.

Corollary

For prime p and positive integers t, k, denote $d := (k-1) \cdot \varphi(p^t) + p^t - 1$. Then for any $n \geq d$ and a, we have $\deg_{p^k}(\mathsf{MOD}_n^{a,p^t}) = d$.


$f(x)$
Function Embedding
Symmetric $f(x)$
with base-p period p^t
$\mathsf{MOD}_n^{a,p^{t-1}}$
base-p period p^{t-1}
MOD *Expansion*
Mahler Expansion
$\sum_{j=0}^{p^t-1} w_j \mathsf{MOD}_n^{j,p^t}$
$\sum_{\ell=0}^{d} \alpha_\ell \binom{|x|}{\ell}$
$\sum_{\ell=0}^{d} \left(\sum_{j=0}^{p^t-1} w_j \alpha_\ell^{(j)} \right) \binom{|x|}{\ell}$

Combination of Different Expansions

The MOD expansion of f:

$$f(x) = \sum_{j=0}^{p^t-1} w_j \mathsf{MOD}_n^{j,p^t}(x).$$

Let $\boldsymbol{w} := (w_0, \cdots, w_{p^t-1})^\top$.

Combination of Different Expansions

The MOD expansion of f:

$$f(x) = \sum_{j=0}^{p^t-1} w_j \mathsf{MOD}_n^{j,p^t}(x). \qquad \text{Let } \boldsymbol{w} := (w_0, \cdots, w_{p^t-1})^\top.$$

The MOD expansion of $\mathsf{MOD}_n^{i,p^{t-1}}$:

$$\mathsf{MOD}_n^{i,p^{t-1}}(x) = \sum_{j=0}^{p^t-1} v_j^{(i)} \mathsf{MOD}_n^{j,p^t}(x). \quad \text{Let } \boldsymbol{v}^{(i)} := \left(v_0^{(i)}, \cdots, v_{p^t-1}^{(i)}\right)^\top.$$

Combination of Different Expansions

The MOD expansion of f:

$$f(x) = \sum_{j=0}^{p^t-1} w_j \mathsf{MOD}_n^{j,p^t}(x). \qquad \text{Let } \boldsymbol{w} := \left(w_0, \cdots, w_{p^t-1}\right)^\top.$$

The MOD expansion of $\mathsf{MOD}_n^{i,p^{t-1}}$:

$$\mathsf{MOD}_n^{i,p^{t-1}}(x) = \sum_{j=0}^{p^t-1} v_j^{(i)} \mathsf{MOD}_n^{j,p^t}(x). \quad \text{Let } \boldsymbol{v}^{(i)} := \left(v_0^{(i)}, \cdots, v_{p^t-1}^{(i)}\right)^\top.$$

$f(x)$ is not p^{t-1} periodic $\implies \boldsymbol{w} \notin \operatorname{span}\left\{\boldsymbol{v}^{(0)}, \cdots, \boldsymbol{v}^{(p^{t-1}-1)}\right\}$.

Combination of Different Expansions

$f(x)$ is not p^{t-1} periodic $\implies \boldsymbol{w} \notin \operatorname{span}\left\{\boldsymbol{v}^{(0)}, \cdots, \boldsymbol{v}^{(p^{t-1}-1)}\right\}$.

Apply Mahler expansion to MODs, where $\alpha_\ell^{(j)}$ is the ℓ-th Mahler coefficient of MOD_n^{j,p^t}:

$$f(x) = \sum_{j=0}^{p^t-1} w_j \mathsf{MOD}_n^{j,p^t}(x) = \sum_{\ell=0}^{d} \left(\left(\sum_{j=0}^{p^t-1} w_j \alpha_\ell^{(j)} \right) \binom{|x|}{\ell} \right),$$

where d is the degree of MOD_n^{j,p^t}.

Combination of Different Expansions

$f(x)$ is not p^{t-1} periodic $\implies \boldsymbol{w} \notin \operatorname{span}\left\{\boldsymbol{v}^{(0)}, \cdots, \boldsymbol{v}^{(p^{t-1}-1)}\right\}$.

Apply Mahler expansion to MODs, where $\alpha_\ell^{(j)}$ is the ℓ-th Mahler coefficient of MOD_n^{j,p^t}:

$$f(x) = \sum_{j=0}^{p^t-1} w_j \mathsf{MOD}_n^{j,p^t}(x) = \sum_{\ell=0}^{d} \left(\left(\sum_{j=0}^{p^t-1} w_j \alpha_\ell^{(j)} \right) \binom{|x|}{\ell} \right),$$

where d is the degree of MOD_n^{j,p^t}.

- Construct $\boldsymbol{S} \in \mathbb{F}_p^{\varphi(p^t) \times p^t}$ s.t. $\boldsymbol{S}_{i,j} = (\alpha_{d-i}^{(j)}/p^{k-2}) \bmod p$.

Combination of Different Expansions

$f(x)$ is not p^{t-1} periodic $\implies \boldsymbol{w} \notin \operatorname{span}\left\{\boldsymbol{v}^{(0)}, \cdots, \boldsymbol{v}^{(p^{t-1}-1)}\right\}$.

Apply Mahler expansion to MODs, where $\alpha_\ell^{(j)}$ is the ℓ-th Mahler coefficient of MOD_n^{j,p^t}:

$$f(x) = \sum_{j=0}^{p^t-1} w_j \mathsf{MOD}_n^{j,p^t}(x) = \sum_{\ell=0}^{d} \left(\left(\sum_{j=0}^{p^t-1} w_j \alpha_\ell^{(j)} \right) \binom{|x|}{\ell} \right),$$

where d is the degree of MOD_n^{j,p^t}.

- Construct $\boldsymbol{S} \in \mathbb{F}_p^{\varphi(p^t) \times p^t}$ s.t. $\boldsymbol{S}_{i,j} = (\alpha_{d-i}^{(j)}/p^{k-2}) \bmod p$.
- Verify that $\ker \boldsymbol{S} = \operatorname{span}\left\{\boldsymbol{v}^{(0)}, \cdots, \boldsymbol{v}^{(p^{t-1}-1)}\right\}$.

Combination of Different Expansions

$f(x)$ is not p^{t-1} periodic $\implies \boldsymbol{w} \notin \operatorname{span}\left\{\boldsymbol{v}^{(0)}, \cdots, \boldsymbol{v}^{(p^{t-1}-1)}\right\}$.

Apply Mahler expansion to MODs, where $\alpha_\ell^{(j)}$ is the ℓ-th Mahler coefficient of MOD_n^{j,p^t}:

$$f(x) = \sum_{j=0}^{p^t-1} w_j \mathsf{MOD}_n^{j,p^t}(x) = \sum_{\ell=0}^{d} \left(\left(\sum_{j=0}^{p^t-1} w_j \alpha_\ell^{(j)} \right) \binom{|x|}{\ell} \right),$$

where d is the degree of MOD_n^{j,p^t}.

- Construct $\boldsymbol{S} \in \mathbb{F}_p^{\varphi(p^t) \times p^t}$ s.t. $\boldsymbol{S}_{i,j} = (\alpha_{d-i}^{(j)}/p^{k-2}) \bmod p$.
- Verify that $\ker \boldsymbol{S} = \operatorname{span}\left\{\boldsymbol{v}^{(0)}, \cdots, \boldsymbol{v}^{(p^{t-1}-1)}\right\}$.
- So $\boldsymbol{S}\boldsymbol{w} \neq 0$, implying a high-order Mahler coefficient of f.

From Primes to Their Product

Theorem

For any prime p, positive integer k, and non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$ with sufficiently large n,

$$\deg_{p^k}(f) \geq (p-1) \cdot k.$$

From Primes to Their Product

Lemma

For any prime p and non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$,

$$\deg_p(f) \geq \min\left\{\frac{n}{2}, \left(1 - \frac{1}{p}\right)\pi_p(f)\right\}.$$

From Primes to Their Product

Lemma

For any prime p and non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$,

$$\deg_p(f) \geq \min\left\{\frac{n}{2}, \left(1 - \frac{1}{p}\right)\pi_p(f)\right\}.$$

Lemma (Periodicity Lemma)

Let g be an a-periodic and b-periodic function on domain $\{0,1,\ldots,n\}$ with $gcd(a,b) = 1$ and $n \geq a + b - 2$. Then g is a constant function.

From Primes to Their Product

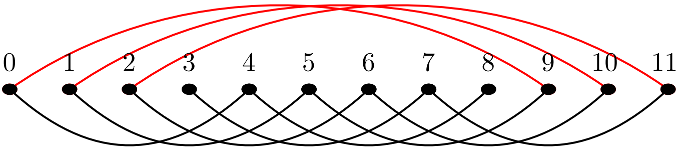
Lemma

For any prime p and non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$,

$$\deg_p(f) \geq \min\left\{\frac{n}{2}, \left(1 - \frac{1}{p}\right)\pi_p(f)\right\}.$$

Lemma (Periodicity Lemma)

Let g be an a-periodic and b-periodic function on domain $\{0, 1, \ldots, n\}$ with $gcd(a, b) = 1$ and $n \geq a + b - 2$. Then g is a constant function.



$a = 4$, $b = 9$ and $n = a + b - 2$

From Primes to Their Product

Lemma

For any prime p and non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$,

$$\deg_p(f) \geq \min\left\{\frac{n}{2}, \left(1 - \frac{1}{p}\right)\pi_p(f)\right\}.$$

Goal:

$$\deg_m(f) \geq \frac{1}{2 + \frac{1}{p-1} + \frac{1}{q-1}} \cdot n.$$

From Primes to Their Product

Lemma

For any prime p and non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$,

$$\deg_p(f) \geq \min\left\{\frac{n}{2}, \left(1 - \frac{1}{p}\right)\pi_p(f)\right\}.$$

Goal:

$$\deg_m(f) \geq \frac{1}{2 + \frac{1}{p-1} + \frac{1}{q-1}} \cdot n.$$

If $\max\{\deg_p(f), \deg_q(f)\} \geq \frac{n}{2}$, the inequality follows naturally.

From Primes to Their Product

Lemma

For any prime p and non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$,

$$\deg_p(f) \geq \min\left\{\frac{n}{2}, \left(1 - \frac{1}{p}\right)\pi_p(f)\right\}.$$

Goal:

$$\deg_m(f) \geq \frac{1}{2 + \frac{1}{p-1} + \frac{1}{q-1}} \cdot n.$$

If $\max\{\deg_p(f), \deg_q(f)\} \geq \frac{n}{2}$, the inequality follows naturally.

Otherwise,

$$\deg_{pq}(f) = \max\{\deg_p(f), \deg_q(f)\} \geq \max\left\{\left(1 - \frac{1}{p}\right)\pi_p(f), \left(1 - \frac{1}{q}\right)\pi_q(f)\right\}.$$

From Primes to Their Product

Lemma

For any prime p and non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$,

$$\deg_p(f) \geq \min\left\{\frac{n}{2}, \left(1 - \frac{1}{p}\right)\pi_p(f)\right\}.$$

Goal:

$$\deg_m(f) \geq \frac{1}{2 + \frac{1}{p-1} + \frac{1}{q-1}} \cdot n.$$

If $\max\{\deg_p(f), \deg_q(f)\} \geq \frac{n}{2}$, the inequality follows naturally.

Otherwise,

$$\deg_{pq}(f) = \max\{\deg_p(f), \deg_q(f)\} \geq \max\left\{\left(1 - \frac{1}{p}\right)\pi_p(f), \left(1 - \frac{1}{q}\right)\pi_q(f)\right\}.$$

By periodicity lemma, $\pi_p(f) + \pi_q(f) > n + 2$.

From Primes to Their Product

Lemma

For any prime p and non-trivial symmetric function $f : \{0,1\}^n \to \{0,1\}$,

$$\deg_p(f) \geq \min\left\{\frac{n}{2}, \left(1 - \frac{1}{p}\right)\pi_p(f)\right\}.$$

Goal:

$$\deg_m(f) \geq \frac{1}{2 + \frac{1}{p-1} + \frac{1}{q-1}} \cdot n.$$

If $\max\{\deg_p(f), \deg_q(f)\} \geq \frac{n}{2}$, the inequality follows naturally.

Otherwise,

$$\deg_{pq}(f) = \max\{\deg_p(f), \deg_q(f)\} \geq \max\left\{\left(1 - \frac{1}{p}\right)\pi_p(f), \left(1 - \frac{1}{q}\right)\pi_q(f)\right\}.$$

By periodicity lemma, $\pi_p(f) + \pi_q(f) > n + 2$.

Combine both to get $\deg_{pq}(f) > \frac{n+2}{2+\frac{1}{p-1}+\frac{1}{q-1}} > \frac{n}{2+\frac{1}{p-1}+\frac{1}{q-1}}$.

Instance with Factor $1/2$

Lemma

If $1, a_1, \cdots, a_k$ are linearly independent over $\mathbb{Q}$, then for any $\varepsilon > 0$, there exist infinitely many $\ell \in \mathbb{N}_+$ such that $\ell a_i \bmod 1 \in (1-\varepsilon, 1)$ for all i.

Instance with Factor $1/2$

Lemma

If $1, a_1, \cdots, a_k$ are linearly independent over $\mathbb{Q}$, then for any $\varepsilon > 0$, there exist infinitely many $\ell \in \mathbb{N}_+$ such that $\ell a_i \bmod 1 \in (1 - \varepsilon, 1)$ for all i.

Suppose $m = p_1 \cdots p_k$. Select another prime q. Let $a_i := \log q / \log p_i$.

Instance with Factor $1/2$

Lemma

If $1, a_1, \cdots, a_k$ are linearly independent over $\mathbb{Q}$, then for any $\varepsilon > 0$, there exist infinitely many $\ell \in \mathbb{N}_+$ such that $\ell a_i \bmod 1 \in (1-\varepsilon, 1)$ for all i.

Suppose $m = p_1 \cdots p_k$. Select another prime q. Let $a_i := \log q / \log p_i$.

Then $1, a_1, \cdots, a_k$ are linearly independent over $\mathbb{Q}$.

Instance with Factor $1/2$

Lemma

If $1, a_1, \cdots, a_k$ are linearly independent over $\mathbb{Q}$, then for any $\varepsilon > 0$, there exist infinitely many $\ell \in \mathbb{N}_+$ such that $\ell a_i \bmod 1 \in (1 - \varepsilon, 1)$ for all i.

Suppose $m = p_1 \cdots p_k$. Select another prime q. Let $a_i := \log q / \log p_i$.

Then $1, a_1, \cdots, a_k$ are linearly independent over $\mathbb{Q}$.

Thus, we have infinitely many ℓ s.t. $\ell \cdot \log q / \log p_i \bmod 1 \in (1 - \varepsilon, 1)$.

Instance with Factor $1/2$

Lemma

If $1, a_1, \cdots, a_k$ are linearly independent over $\mathbb{Q}$, then for any $\varepsilon > 0$, there exist infinitely many $\ell \in \mathbb{N}_+$ such that $\ell a_i \bmod 1 \in (1-\varepsilon, 1)$ for all i.

Suppose $m = p_1 \cdots p_k$. Select another prime q. Let $a_i := \log q / \log p_i$.

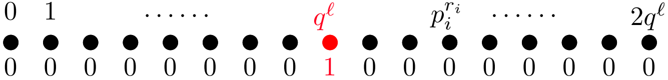
Then $1, a_1, \cdots, a_k$ are linearly independent over $\mathbb{Q}$.

Thus, we have infinitely many ℓ s.t. $\ell \cdot \log q / \log p_i \bmod 1 \in (1-\varepsilon, 1)$.

Therefore, $p_i^{r_i}/q^\ell \in (1, p_i^\varepsilon)$ where $r_i = \lceil \ell \cdot \log q / \log p_i \rceil$.

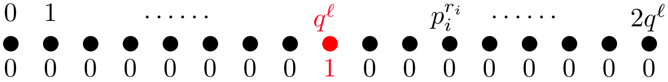
Instance with Factor $1/2$

For fixed ℓ, take $n = 2q^\ell$, and consider the following symmetric function f:



Instance with Factor $1/2$

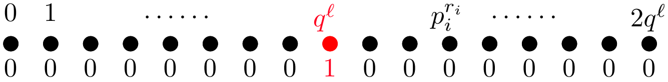
For fixed ℓ, take $n = 2q^\ell$, and consider the following symmetric function f:



f is $p_i^{r_i}$-periodic, and hence $\deg_{p_i}(f) \leq p_i^{r_i} - 1$ **[Wilson, 2006]**.

Instance with Factor $1/2$

For fixed ℓ, take $n = 2q^\ell$, and consider the following symmetric function f:



f is $p_i^{r_i}$-periodic, and hence $\deg_{p_i}(f) \le p_i^{r_i} - 1$ **[Wilson, 2006]**.

Finally,

$$\deg_m(f) \overset{\text{CRT}}{=} \max\{\deg_{p_i}(f)\} \le \max\{p_i^{r_i}\} \le \frac{n}{2} \max\{p_i^{\varepsilon}\}.$$

Then let $\varepsilon \to 0$.

Concluding Remarks

- Ramsey-type argument requires super large $n \geq \mathrm{tower}(\mathrm{poly}(p, k))$. Could it be improved to something like $n \geq \exp(\mathrm{poly}(p, k))$?

Concluding Remarks

- Ramsey-type argument requires super large $n \geq \mathrm{tower}(\mathrm{poly}(p,k))$. Could it be improved to something like $n \geq \exp(\mathrm{poly}(p,k))$?
- Is it true that $\deg(f) = O\left(\mathrm{poly}\left(\deg_{pq}(f)\right)\right)$ for all non-trivial Boolean functions?

Concluding Remarks

- Ramsey-type argument requires super large $n \geq \mathrm{tower}(\mathrm{poly}(p, k))$. Could it be improved to something like $n \geq \exp(\mathrm{poly}(p, k))$?
- Is it true that $\deg(f) = O\left(\mathrm{poly}\left(\deg_{pq}(f)\right)\right)$ for all non-trivial Boolean functions?
- Conjecture: $\deg_m(f) \geq n/2 - o(n)$ for all non-trivial symmetric Boolean functions when m contains two different prime factors.

Concluding Remarks

- Ramsey-type argument requires super large $n \geq \text{tower}(\text{poly}(p, k))$. Could it be improved to something like $n \geq \exp(\text{poly}(p, k))$?
- Is it true that $\deg(f) = O\left(\text{poly}\left(\deg_{pq}(f)\right)\right)$ for all non-trivial Boolean functions?

- Conjecture: $\deg_m(f) \geq n/2 - o(n)$ for all non-trivial symmetric Boolean functions when m contains two different prime factors.
- A related conjecture: $\deg(f) \geq n - O(1)$ for all non-trivial symmetric Boolean functions. **[Gathen and Roche, 1997]**
  - Best lower bound: $\deg(f) \geq n - O(n^{0.525})$.
  - Best instance: $\deg(f) = n - 3$.

Thank you!