Recent results on the nonlinearity of Boolean functions

Kai-Uwe Schmidt

Paderborn University

Outline

Asymptotic results on the nonlinearity of

Outline

Asymptotic results on the nonlinearity of Boolean functions

Outline

Asymptotic results on the nonlinearity of

Boolean functions and more general functions

Outline

Asymptotic results on the nonlinearity of

Boolean functions and more general functions

Nonasymptotic results

Outline

Asymptotic results on the nonlinearity of Boolean functions and more general functions

Nonasymptotic results

Autocorrelations of Boolean functions

Nonlinearity of Boolean functions

$$f : \mathbb{F}_2^3 \to \mathbb{F}_2$$

$$f(x, y, z) = xy + yz + z$$

Nonlinearity of Boolean functions

$$f : \mathbb{F}_2^3 \to \mathbb{F}_2$$

$$f(x, y, z) = xy + yz + z$$

(x, y, z)	000	001	010	011	100	101	110	111
$f(x, y, z)$	0	1	0	0	0	1	1	1

Nonlinearity of Boolean functions

$$f : \mathbb{F}_2^3 \to \mathbb{F}_2$$

$$f(x,y,z) = xy + yz + z$$

(x,y,z)	000	001	010	011	100	101	110	111
$f(x,y,z)$	0	1	0	0	0	1	1	1
z	0	1	0	1	0	1	0	1

Nonlinearity of Boolean functions

$$f : \mathbb{F}_2^3 \to \mathbb{F}_2$$

$$f(x, y, z) = xy + yz + z$$

(x, y, z)	000	001	010	011	100	101	110	111
$f(x, y, z)$	0	1	0	0	0	1	1	1
z	0	1	0	1	0	1	0	1
$x + y$	0	0	1	1	1	1	0	0

Nonlinearity of Boolean functions

$$f : \mathbb{F}_2^3 \to \mathbb{F}_2$$

$$f(x, y, z) = xy + yz + z$$

(x, y, z)	000	001	010	011	100	101	110	111
$f(x, y, z)$	0	1	0	0	0	1	1	1
z	0	1	0	1	0	1	0	1
$x + y$	0	0	1	1	1	1	0	0
$x + y + z$	1	0	0	1	0	1	1	0

Nonlinearity of Boolean functions

$$f : \mathbb{F}_2^3 \to \mathbb{F}_2$$

$$f(x, y, z) = xy + yz + z$$

(x, y, z)	000	001	010	011	100	101	110	111
$f(x, y, z)$	0	1	0	0	0	1	1	1
z	0	1	0	1	0	1	0	1
$x + y$	0	0	1	1	1	1	0	0
$x + y + z$	1	0	0	1	0	1	1	0

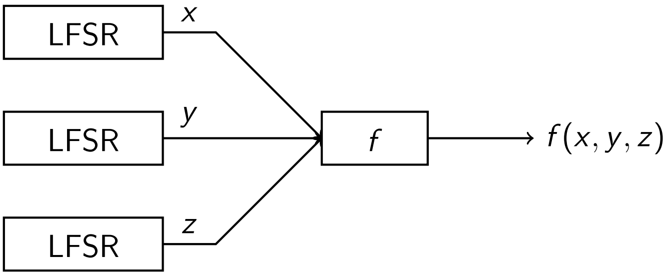
The Hamming distance of f to the 16 affine Boolean functions is either 2, 4, or 6. Therefore the nonlinearity of f is 2.

Cryptography

Boolean functions with large nonlinearity are difficult to approximate by linear functions and so provide resistance against linear cryptanalysis.

Cryptography

Boolean functions with large nonlinearity are difficult to approximate by linear functions and so provide resistance against linear cryptanalysis.



Cryptography

Boolean functions with large nonlinearity are difficult to approximate by linear functions and so provide resistance against linear cryptanalysis.

Main question

What is the largest nonlinearity of a Boolean function on $\mathbb{F}_2^n$?

Cryptography

Boolean functions with large nonlinearity are difficult to approximate by linear functions and so provide resistance against linear cryptanalysis.

Main question

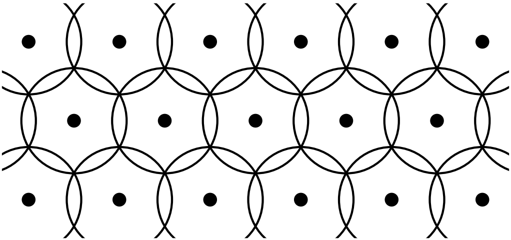
What is the largest nonlinearity of a Boolean function on $\mathbb{F}_2^n$?

A related question

What is the largest nonlinearity of a balanced Boolean function on $\mathbb{F}_2^n$?

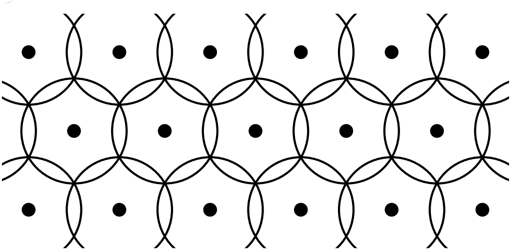
Coding theory

The covering radius of a code $\mathcal{C} \subseteq \mathbb{F}_2^N$ is the smallest number r, such that the spheres of radius r centred at the points of $\mathcal{C}$ cover the whole space $\mathbb{F}_2^N$.



Coding theory

The covering radius of a code $\mathcal{C} \subseteq \mathbb{F}_2^N$ is the smallest number r, such that the spheres of radius r centred at the points of $\mathcal{C}$ cover the whole space $\mathbb{F}_2^N$.



Main question (restated)

What is the covering radius of the first order Reed-Muller code $R(1, n)$?

Fourier transforms

The Fourier transform of $f : \mathbb{F}_2^n \to \mathbb{F}_2$:

$$\hat{f}(a) = \frac{1}{2^{n/2}} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)} \, (-1)^{\langle a,y \rangle}.$$

Fourier transforms

The Fourier transform of $f : \mathbb{F}_2^n \to \mathbb{F}_2$:

$$\hat{f}(a) = \frac{1}{2^{n/2}} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)} \, (-1)^{\langle a,y \rangle}.$$

The nonlinearity of f equals $2^{n-1} - \mu(f)\, 2^{n/2-1}$, where

$$\mu(f) = \max_{a \in \mathbb{F}_2^n} |\hat{f}(a)|$$

is the spectral radius of f.

Fourier transforms

The Fourier transform of $f : \mathbb{F}_2^n \to \mathbb{F}_2$:

$$\hat{f}(a) = \frac{1}{2^{n/2}} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)} \, (-1)^{\langle a,y \rangle}.$$

The nonlinearity of f equals $2^{n-1} - \mu(f)\, 2^{n/2-1}$, where

$$\mu(f) = \max_{a \in \mathbb{F}_2^n} |\hat{f}(a)|$$

is the spectral radius of f.

Main question (restated)

What is the smallest spectral radius $\mu(n)$ of a Boolean function on $\mathbb{F}_2^n$?

Parseval's identity

Parseval's identity is

$$\sum_{a \in \mathbb{F}_2^n} \hat{f}(a)^2 = 2^n,$$

so that the spectral radius of a Boolean function is at least 1 and the covering radius of $R(1, n)$ is at most $2^{n-1} - 2^{n/2-1}$.

Parseval's identity

Parseval's identity is

$$\sum_{a \in \mathbb{F}_2^n} \hat{f}(a)^2 = 2^n,$$

so that the spectral radius of a Boolean function is at least 1 and the covering radius of $R(1, n)$ is at most $2^{n-1} - 2^{n/2-1}$.

The extremal functions are called bent functions.

Parseval's identity

Parseval's identity is

$$\sum_{a \in \mathbb{F}_2^n} \hat{f}(a)^2 = 2^n,$$

so that the spectral radius of a Boolean function is at least 1 and the covering radius of $R(1,n)$ is at most $2^{n-1} - 2^{n/2-1}$.

The extremal functions are called bent functions. They exist precisely when n is even.

Parseval's identity

Parseval's identity is

$$\sum_{a \in \mathbb{F}_2^n} \hat{f}(a)^2 = 2^n,$$

so that the spectral radius of a Boolean function is at least 1 and the covering radius of $R(1, n)$ is at most $2^{n-1} - 2^{n/2-1}$.

The extremal functions are called bent functions. They exist precisely when n is even.

This answers the main question for even n:

- The smallest spectral radius is 1.

Parseval's identity

Parseval's identity is

$$\sum_{a \in \mathbb{F}_2^n} \hat{f}(a)^2 = 2^n,$$

so that the spectral radius of a Boolean function is at least 1 and the covering radius of $R(1, n)$ is at most $2^{n-1} - 2^{n/2-1}$.

The extremal functions are called bent functions. They exist precisely when n is even.

This answers the main question for even n:

- The smallest spectral radius is 1.
- The largest nonlinearity is $2^{n-1} - 2^{n/2-1}$.

Parseval's identity

Parseval's identity is

$$\sum_{a \in \mathbb{F}_2^n} \hat{f}(a)^2 = 2^n,$$

so that the spectral radius of a Boolean function is at least 1 and the covering radius of $R(1,n)$ is at most $2^{n-1} - 2^{n/2-1}$.

The extremal functions are called bent functions. They exist precisely when n is even.

This answers the main question for even n:

- The smallest spectral radius is 1.
- The largest nonlinearity is $2^{n-1} - 2^{n/2-1}$.
- The covering radius of $R(1,n)$ equals $2^{n-1} - 2^{n/2-1}$.

What happens for odd n?

- $\sqrt{2} = \mu(1) \geq \mu(3) \geq \mu(5) \geq \ldots$
  (Helleseth-Kløve-Mykkeltveit 1978)

What happens for odd n?

- $\sqrt{2} = \mu(1) \geq \mu(3) \geq \mu(5) \geq \dots$
  (Helleseth-Kløve-Mykkeltveit 1978)
- $\mu(3) = \sqrt{2}$ (easy to check)

What happens for odd n?

- $\sqrt{2} = \mu(1) \geq \mu(3) \geq \mu(5) \geq \ldots$
  (Helleseth-Kløve-Mykkeltveit 1978)
- $\mu(3) = \sqrt{2}$ (easy to check)
- $\mu(5) = \sqrt{2}$ (Berlekamp-Welch 1972)

What happens for odd n?

- $\sqrt{2} = \mu(1) \geq \mu(3) \geq \mu(5) \geq \dots$
  (Helleseth-Kløve-Mykkeltveit 1978)
- $\mu(3) = \sqrt{2}$ (easy to check)
- $\mu(5) = \sqrt{2}$ (Berlekamp-Welch 1972)
- $\mu(7) = \sqrt{2}$ (Mykkeltveit 1980), (Hou 1996)

What happens for odd n?

- $\sqrt{2} = \mu(1) \geq \mu(3) \geq \mu(5) \geq \ldots$
  (Helleseth-Kløve-Mykkeltveit 1978)
- $\mu(3) = \sqrt{2}$ (easy to check)
- $\mu(5) = \sqrt{2}$ (Berlekamp-Welch 1972)
- $\mu(7) = \sqrt{2}$ (Mykkeltveit 1980), (Hou 1996)

Whether $\mu(2m+1) = \sqrt{2}$ in general remains an open question.

— Helleseth, Kløve & Mykkeltveit 1978

What happens for odd n?

- $\sqrt{2} = \mu(1) \geq \mu(3) \geq \mu(5) \geq \ldots$
  (Helleseth-Kløve-Mykkeltveit 1978)
- $\mu(3) = \sqrt{2}$ (easy to check)
- $\mu(5) = \sqrt{2}$ (Berlekamp-Welch 1972)
- $\mu(7) = \sqrt{2}$ (Mykkeltveit 1980), (Hou 1996)

Whether $\mu(2m+1) = \sqrt{2}$ in general remains an open question.

— Helleseth, Kløve & Mykkeltveit 1978

- $\mu(n) \leq \frac{27}{32}\sqrt{2} = 1.19\ldots$ for all $n \geq 15$
  (Patterson-Wiedemann 1983)

What happens for odd n?

- $\sqrt{2} = \mu(1) \geq \mu(3) \geq \mu(5) \geq \ldots$
  (Helleseth-Kløve-Mykkeltveit 1978)
- $\mu(3) = \sqrt{2}$ (easy to check)
- $\mu(5) = \sqrt{2}$ (Berlekamp-Welch 1972)
- $\mu(7) = \sqrt{2}$ (Mykkeltveit 1980), (Hou 1996)

Whether $\mu(2m+1) = \sqrt{2}$ in general remains an open question.

— Helleseth, Kløve & Mykkeltveit 1978

- $\mu(n) \leq \frac{7}{8}\sqrt{2} = 1.23\ldots$ for all $n \geq 9$ (Kavut-Yücel 2010)
- $\mu(n) \leq \frac{27}{32}\sqrt{2} = 1.19\ldots$ for all $n \geq 15$
  (Patterson-Wiedemann 1983)

What did Patterson-Wiedemann do?

For a subgroup $H \leq \mathrm{GL}_n(\mathbb{F}_2)$ consider *H-invariant functions*:

$$f(hx) = f(x) \quad \text{for all } x \in \mathbb{F}_2^n \text{ and all } h \in H.$$

What did Patterson-Wiedemann do?

For a subgroup $H \leq \mathrm{GL}_n(\mathbb{F}_2)$ consider H-invariant functions:

$$f(hx) = f(x) \quad \text{for all } x \in \mathbb{F}_2^n \text{ and all } h \in H.$$

The Fourier transform of f is also H-invariant.

What did Patterson-Wiedemann do?

For a subgroup $H \leq \mathrm{GL}_n(\mathbb{F}_2)$ consider *H-invariant functions*:

$$f(hx) = f(x) \quad \text{for all } x \in \mathbb{F}_2^n \text{ and all } h \in H.$$

The Fourier transform of f is also H-invariant.

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \{1, \theta^5, \theta^{10}\}$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

What did Patterson-Wiedemann do?

For a subgroup $H \leq \mathrm{GL}_n(\mathbb{F}_2)$ consider *H-invariant functions*:

$$f(hx) = f(x) \quad \text{for all } x \in \mathbb{F}_2^n \text{ and all } h \in H.$$

The Fourier transform of f is also H-invariant.

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \{1, \theta^5, \theta^{10}\}$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

What did Patterson-Wiedemann do?

For a subgroup $H \leq \mathrm{GL}_n(\mathbb{F}_2)$ consider *H-invariant functions*:

$$f(hx) = f(x) \quad \text{for all } x \in \mathbb{F}_2^n \text{ and all } h \in H.$$

The Fourier transform of f is also H-invariant.

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \{1, \theta^5, \theta^{10}\}$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

What did Patterson-Wiedemann do?

For a subgroup $H \leq \mathrm{GL}_n(\mathbb{F}_2)$ consider *H-invariant functions*:

$$f(hx) = f(x) \quad \text{for all } x \in \mathbb{F}_2^n \text{ and all } h \in H.$$

The Fourier transform of f is also H-invariant.

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \{1, \theta^5, \theta^{10}\}$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

What did Patterson-Wiedemann do?

For a subgroup $H \leq \mathrm{GL}_n(\mathbb{F}_2)$ consider H-invariant functions:

$$f(hx) = f(x) \quad \text{for all } x \in \mathbb{F}_2^n \text{ and all } h \in H.$$

The Fourier transform of f is also H-invariant.

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \{1, \theta^5, \theta^{10}\}$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

What did Patterson-Wiedemann do?

For a subgroup $H \leq \mathrm{GL}_n(\mathbb{F}_2)$ consider H-invariant functions:

$$f(hx) = f(x) \quad \text{for all } x \in \mathbb{F}_2^n \text{ and all } h \in H.$$

The Fourier transform of f is also H-invariant.

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \{1, \theta^5, \theta^{10}\}$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \mathrm{Gal}(\mathbb{F}_{2^4}/\mathbb{F}_2)$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

What did Patterson-Wiedemann do?

For a subgroup $H \leq \mathrm{GL}_n(\mathbb{F}_2)$ consider *H-invariant functions*:

$$f(hx) = f(x) \quad \text{for all } x \in \mathbb{F}_2^n \text{ and all } h \in H.$$

The Fourier transform of f is also H-invariant.

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \{1, \theta^5, \theta^{10}\}$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \mathrm{Gal}(\mathbb{F}_{2^4}/\mathbb{F}_2)$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

What did Patterson-Wiedemann do?

For a subgroup $H \leq \mathrm{GL}_n(\mathbb{F}_2)$ consider *H-invariant functions*:

$$f(hx) = f(x) \quad \text{for all } x \in \mathbb{F}_2^n \text{ and all } h \in H.$$

The Fourier transform of f is also H-invariant.

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \{1, \theta^5, \theta^{10}\}$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \mathrm{Gal}(\mathbb{F}_{2^4}/\mathbb{F}_2)$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

What did Patterson-Wiedemann do?

For a subgroup $H \le \mathrm{GL}_n(\mathbb{F}_2)$ consider H-invariant functions:

$$f(hx) = f(x) \quad \text{for all } x \in \mathbb{F}_2^n \text{ and all } h \in H.$$

The Fourier transform of f is also H-invariant.

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \{1, \theta^5, \theta^{10}\}$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ that are H-invariant for $H = \mathrm{Gal}(\mathbb{F}_{2^4}/\mathbb{F}_2)$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

The case $n = 15$

$$2^{n-1} - 2^{(n-1)/2} = 16\,256 \qquad \lfloor 2^{n-1} - 2^{n/2-1} \rfloor = 16\,293$$

The case $n = 15$

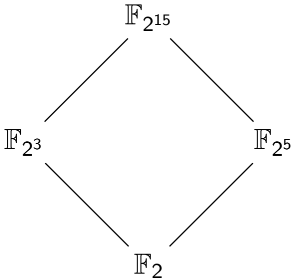
$$2^{n-1} - 2^{(n-1)/2} = 16\,256 \qquad \lfloor 2^{n-1} - 2^{n/2-1} \rfloor = 16\,293$$

$\mathrm{GL}_{15}(\mathbb{F}_2)$ has a subgroup

$$H \cong \mathbb{F}_{2^3}^* \times \mathbb{F}_{2^5}^* \times \mathrm{Gal}(\mathbb{F}_{2^{15}}/\mathbb{F}_2)$$

of order $7 \cdot 31 \cdot 15 = 3255$.

This group partitions $\mathbb{F}_2^{15}$ into 10 orbits of size 3255 and one orbit of size 217.



The case $n = 15$

$$2^{n-1} - 2^{(n-1)/2} = 16\,256 \qquad \lfloor 2^{n-1} - 2^{n/2-1} \rfloor = 16\,293$$

$\mathrm{GL}_{15}(\mathbb{F}_2)$ has a subgroup

$$H \cong \mathbb{F}_{2^3}^* \times \mathbb{F}_{2^5}^* \times \mathrm{Gal}(\mathbb{F}_{2^{15}}/\mathbb{F}_2)$$

of order $7 \cdot 31 \cdot 15 = 3255$.

This group partitions $\mathbb{F}_2^{15}$ into 10 orbits of size 3255 and one orbit of size 217.

$$\begin{tikzcd}[column sep=small]
 & \mathbb{F}_{2^{15}} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{F}_{2^3} \arrow[dr, dash] & & \mathbb{F}_{2^5} \arrow[dl, dash] \\
 & \mathbb{F}_2 &
\end{tikzcd}$$

The search space is reduced from $2^{32\,768}$ to 2^{11}.

The case $n = 15$

$$2^{n-1} - 2^{(n-1)/2} = 16\,256 \qquad \lfloor 2^{n-1} - 2^{n/2-1} \rfloor = 16\,293$$

$GL_{15}(\mathbb{F}_2)$ has a subgroup

$$H \cong \mathbb{F}_{2^3}^* \times \mathbb{F}_{2^5}^* \times \mathrm{Gal}(\mathbb{F}_{2^{15}}/\mathbb{F}_2)$$

of order $7 \cdot 31 \cdot 15 = 3255$.

This group partitions $\mathbb{F}_2^{15}$ into 10 orbits of size 3255 and one orbit of size 217.

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{F}_{2^{15}} \arrow[dl] \arrow[dr] & \\
\mathbb{F}_{2^3} \arrow[dr] & & \mathbb{F}_{2^5} \arrow[dl] \\
 & \mathbb{F}_2 &
\end{tikzcd}$$

The search space is reduced from $2^{32\,768}$ to 2^{11}. This gives functions with nonlinearity $16\,276$ and spectral radius

$$\tfrac{27}{32}\sqrt{2} = 1.1932\ldots.$$

The case $n = 9$

$$2^{n-1} - 2^{(n-1)/2} = 240 \qquad \lfloor 2^{n-1} - 2^{n/2-1} \rfloor = 244$$

The case $n = 9$

$$2^{n-1} - 2^{(n-1)/2} = 240 \qquad \lfloor 2^{n-1} - 2^{n/2-1} \rfloor = 244$$

The search space is 2^{512}.

The case $n = 9$

$$2^{n-1} - 2^{(n-1)/2} = 240 \qquad \lfloor 2^{n-1} - 2^{n/2-1} \rfloor = 244$$

The search space is 2^{512}.

subgroup	# orbits	nonlinearity	spectral radius
$\mathbb{F}_{2^3}^* \times \mathrm{Gal}(\mathbb{F}_{2^9}/\mathbb{F}_2)$	8	< 240	$> \sqrt{2}$

Patterson-Wiedemann 1983

The case $n = 9$

$$2^{n-1} - 2^{(n-1)/2} = 240 \qquad \lfloor 2^{n-1} - 2^{n/2-1} \rfloor = 244$$

The search space is 2^{512}.

subgroup	# orbits	nonlinearity	spectral radius
$\mathbb{F}_{2^3}^* \times \mathrm{Gal}(\mathbb{F}_{2^9}/\mathbb{F}_2)$	8	< 240	$> \sqrt{2}$
$\mathrm{Gal}(\mathbb{F}_{2^9}/\mathbb{F}_2)$	60	$= 241$	$= 1.3258\ldots$

Patterson-Wiedemann 1983

Kavut-Maitra-Yücel 2007

The case $n = 9$

$$2^{n-1} - 2^{(n-1)/2} = 240 \qquad \lfloor 2^{n-1} - 2^{n/2-1} \rfloor = 244$$

The search space is 2^{512}.

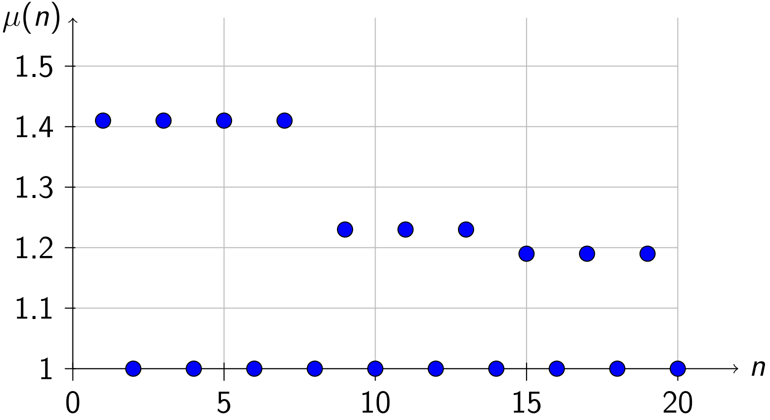
subgroup	# orbits	nonlinearity	spectral radius
$\mathbb{F}_{2^3}^* \times \mathrm{Gal}(\mathbb{F}_{2^9}/\mathbb{F}_2)$	8	< 240	$> \sqrt{2}$
$\mathrm{Gal}(\mathbb{F}_{2^9}/\mathbb{F}_2)$	60	$= 241$	$= 1.3258\ldots$
$\mathrm{Gal}(\mathbb{F}_{2^9}/\mathbb{F}_{2^3})$	176	≥ 242	$\leq 1.2374\ldots$

Patterson-Wiedemann 1983

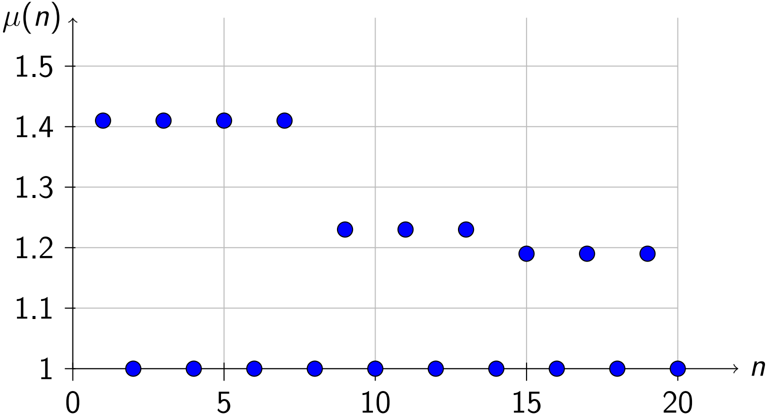
Kavut-Maitra-Yücel 2007

Kavut-Yücel 2010

Best known nonlinearities

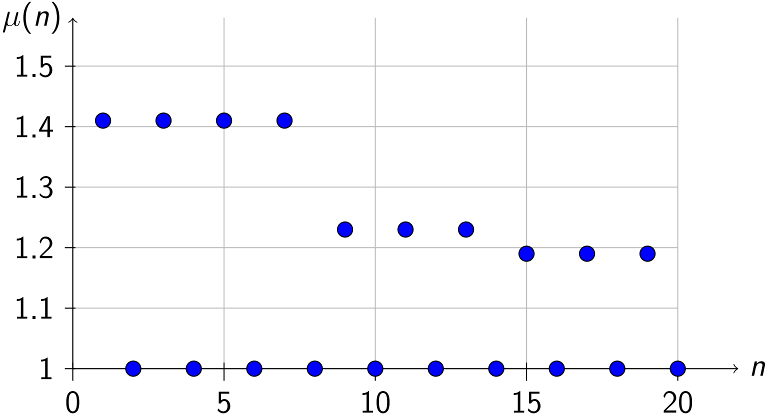


Best known nonlinearities



Conjecture (Patterson-Wiedemann 1983). $\lim_{n\to\infty} \mu(n) = 1$.

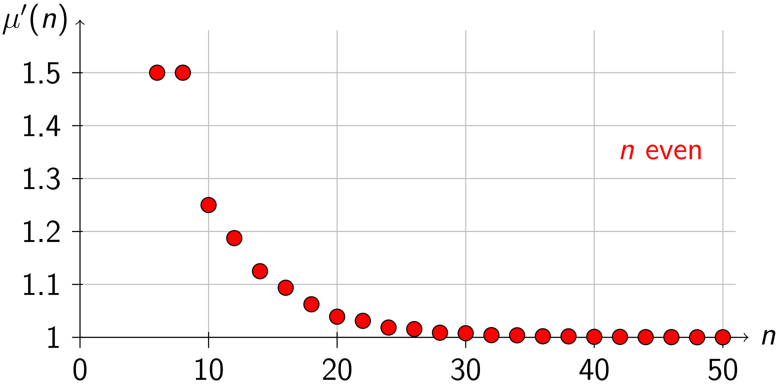
Best known nonlinearities



Conjecture (Patterson-Wiedemann 1983). $\lim_{n\to\infty} \mu(n) = 1$.

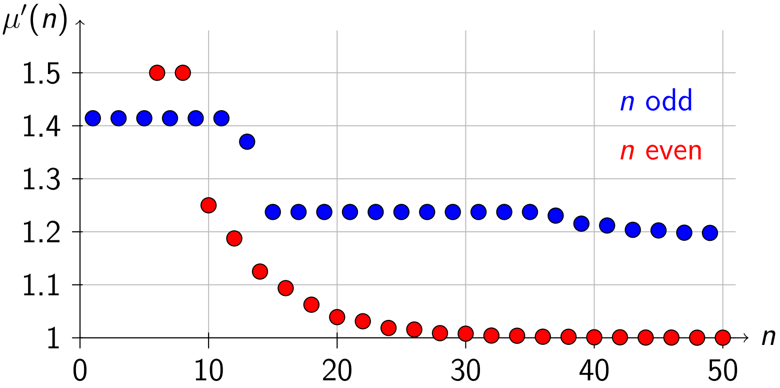
Theorem (S. 2019). This conjecture is true.

Nonlinearities of balanced functions



Theorem (Dobbertin 1995). $\lim_{m\to\infty} \mu'(2m) = 1$.

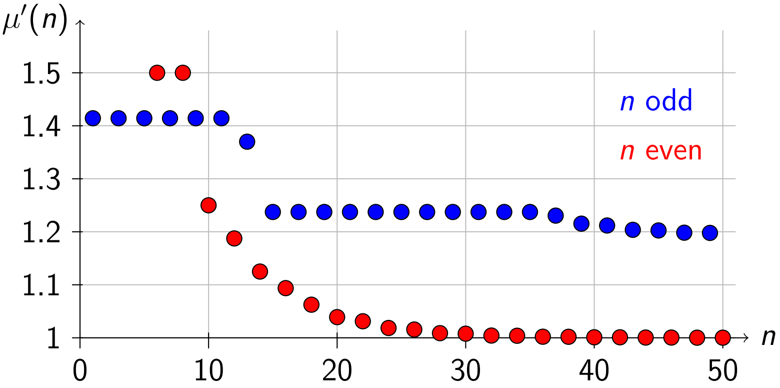
Nonlinearities of balanced functions



Theorem (Dobbertin 1995). $\lim_{m\to\infty} \mu'(2m) = 1$.

Conjecture (Dobbertin 1995). $\lim_{n\to\infty} \mu'(n) = 1$.

Nonlinearities of balanced functions



Theorem (Dobbertin 1995). $\lim_{m\to\infty} \mu'(2m) = 1$.

Conjecture (Dobbertin 1995). $\lim_{n\to\infty} \mu'(n) = 1$.

Corollary (S. 2019). This conjecture is also true.

The functions: An example

Take a subgroup H of $\mathbb{F}_{2^n}^*$ and consider functions

$$f : \mathbb{F}_{2^n} \to \{-1, 1\}$$

that are constant on the cosets of H, except for H itself.

The functions: An example

Take a subgroup H of $\mathbb{F}_{2^n}^*$ and consider functions

$$f : \mathbb{F}_{2^n} \to \{-1, 1\}$$

that are constant on the cosets of H, except for H itself.

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ with $H = \{1, \theta^5, \theta^{10}\}$:

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

The functions: In general

- H is a subgroup of $\mathbb{F}_{2^n}^*$ of index v.

The functions: In general

- H is a subgroup of $\mathbb{F}_{2^n}^*$ of index v.
- T is a complete system of coset representatives of H.

The functions: In general

- H is a subgroup of $\mathbb{F}_{2^n}^*$ of index v.
- T is a complete system of coset representatives of H.
- $g : T \to \{0, -1, 1\}$ is balanced with $g(z) = 0 \Leftrightarrow z \in H$.

The functions: In general

- H is a subgroup of $\mathbb{F}_{2^n}^*$ of index v.
- T is a complete system of coset representatives of H.
- $g : T \to \{0, -1, 1\}$ is balanced with $g(z) = 0 \Leftrightarrow z \in H$.
- $h : H \to \{-1, 1\}$ is some function.

The functions: In general

- H is a subgroup of $\mathbb{F}_{2^n}^*$ of index v.
- T is a complete system of coset representatives of H.
- $g : T \to \{0, -1, 1\}$ is balanced with $g(z) = 0 \Leftrightarrow z \in H$.
- $h : H \to \{-1, 1\}$ is some function.

Consider functions $f : \mathbb{F}_{2^n} \to \{-1, 1\}$ with $f(0) = 1$ and

$$f(y) = \mathbb{1}_H(y)\, h(y) + \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \text{for } y \in \mathbb{F}_{2^n}^*.$$

The functions: In general

- H is a subgroup of $\mathbb{F}_{2^n}^*$ of index v.
- T is a complete system of coset representatives of H.
- $g : T \to \{0, -1, 1\}$ is balanced with $g(z) = 0 \Leftrightarrow z \in H$.
- $h : H \to \{-1, 1\}$ is some function.

Consider functions $f : \mathbb{F}_{2^n} \to \{-1, 1\}$ with $f(0) = 1$ and

$$f(y) = \mathbb{1}_H(y)\, h(y) + \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \text{for } y \in \mathbb{F}_{2^n}^*.$$

Proposition (S. 2019). Let $v = 7^e$. Then, for some odd n, there is a function $h : H \to \{-1, 1\}$ such that f satisfies

$$\max_{a \in \mathbb{F}_{2^n}} |\hat{f}(a)| \le 1 + 12\sqrt{\log(2v)/v}.$$

The functions: In general

- H is a subgroup of $\mathbb{F}_{2^n}^*$ of index v.
- T is a complete system of coset representatives of H.
- $g : T \to \{0, -1, 1\}$ is balanced with $g(z) = 0 \Leftrightarrow z \in H$.
- $h : H \to \{-1, 1\}$ is some function.

Consider functions $f : \mathbb{F}_{2^n} \to \{-1, 1\}$ with $f(0) = 1$ and

$$f(y) = \mathbb{1}_H(y)\, h(y) + \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \text{for } y \in \mathbb{F}_{2^n}^*.$$

Proposition (S. 2019). Let $v = 7^e$. Then, for some odd n, there is a function $h : H \to \{-1, 1\}$ such that f satisfies

$$\max_{a \in \mathbb{F}_{2^n}} |\hat{f}(a)| \leq 1 + 12\sqrt{\log(2v)/v}.$$

The main result follows by letting e tend to infinity.

Fourier Near-Eigenfunctions

If $\mathbb{1}_H$ is an eigenfunction for the Fourier transform, then on $\mathbb{F}_{2^n}^*$,

$$f(y) = \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \longleftrightarrow \quad \hat{f}(a) = f(a^{-1}).$$

Fourier Near-Eigenfunctions

If $\mathbb{1}_H$ is an eigenfunction for the Fourier transform, then on $\mathbb{F}_{2^n}^*$,

$$f(y) = \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \longleftrightarrow \quad \hat{f}(a) = f(a^{-1}).$$

Let χ be a multiplicative character of $\mathbb{F}_{2^n}$ of order v. Then

$$\mathbb{1}_H(y) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(y) \quad \longleftrightarrow \quad \widehat{\mathbb{1}_H}(a) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(a)\, \frac{\overline{G(\chi^j)}}{2^{n/2}}.$$

Fourier Near-Eigenfunctions

If $\mathbb{1}_H$ is an eigenfunction for the Fourier transform, then on $\mathbb{F}_{2^n}^*$,

$$f(y) = \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \longleftrightarrow \quad \hat{f}(a) = f(a^{-1}).$$

Let χ be a multiplicative character of $\mathbb{F}_{2^n}$ of order v. Then

$$\mathbb{1}_H(y) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(y) \quad \longleftrightarrow \quad \widehat{\mathbb{1}_H}(a) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(a)\, \frac{\overline{G(\chi^j)}}{2^{n/2}}.$$

Then $G(\chi^j) \in \mathbb{Q}(\sqrt{-7})$

Fourier Near-Eigenfunctions

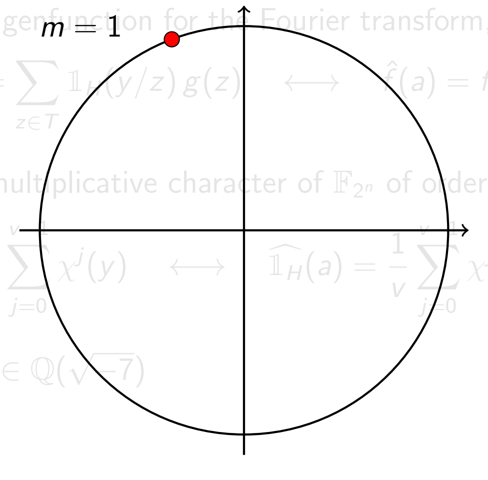
If $\mathbb{1}_H$ is an eigenfunction for the Fourier transform, then on $\mathbb{F}_{2^n}^*$,

$$f(y) = \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \longleftrightarrow \quad \hat{f}(a) = f(a^{-1}).$$

Let χ be a multiplicative character of $\mathbb{F}_{2^n}$ of order v. Then

$$\mathbb{1}_H(y) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(y) \quad \longleftrightarrow \quad \widehat{\mathbb{1}_H}(a) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(a)\, \frac{\overline{G(\chi^j)}}{2^{n/2}}.$$

Then $G(\chi^j) \in \mathbb{Q}(\sqrt{-7})$



Distribution of $\frac{G(\chi)}{2^{n/2}}$, $v = 7$, $n = 3m$

Fourier Near-Eigenfunctions

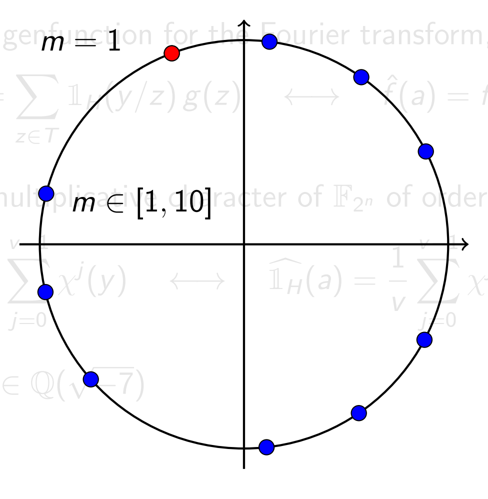
If $\mathbb{1}_H$ is an eigenfunction for the Fourier transform, then on $\mathbb{F}_{2^n}^*$,

$$f(y) = \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \longleftrightarrow \quad \hat{f}(a) = f(a^{-1}).$$

Let χ be a multiplicative character of $\mathbb{F}_{2^n}$ of order v. Then

$$\mathbb{1}_H(y) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(y) \quad \longleftrightarrow \quad \widehat{\mathbb{1}_H}(a) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(a)\, \frac{\overline{G(\chi^j)}}{2^{n/2}}.$$

Then $G(\chi^j) \in \mathbb{Q}(\sqrt{-7})$



Distribution of $\frac{G(\chi)}{2^{n/2}}$, $v = 7$, $n = 3m$

Fourier Near-Eigenfunctions

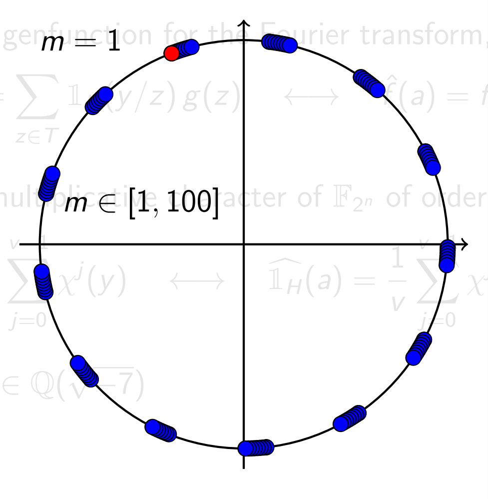
If $\mathbb{1}_H$ is an eigenfunction for the Fourier transform, then on $\mathbb{F}_{2^n}^*$,

$$f(y) = \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \longleftrightarrow \quad \hat{f}(a) = f(a^{-1}).$$

Let χ be a multiplicative character of $\mathbb{F}_{2^n}$ of order v. Then

$$\mathbb{1}_H(y) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(y) \quad \longleftrightarrow \quad \widehat{\mathbb{1}_H}(a) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(a)\, \frac{\overline{G(\chi^j)}}{2^{n/2}}.$$

Then $G(\chi^j) \in \mathbb{Q}(\sqrt{-7})$



Distribution of $\frac{G(\chi)}{2^{n/2}}$, $v = 7$, $n = 3m$

Fourier Near-Eigenfunctions

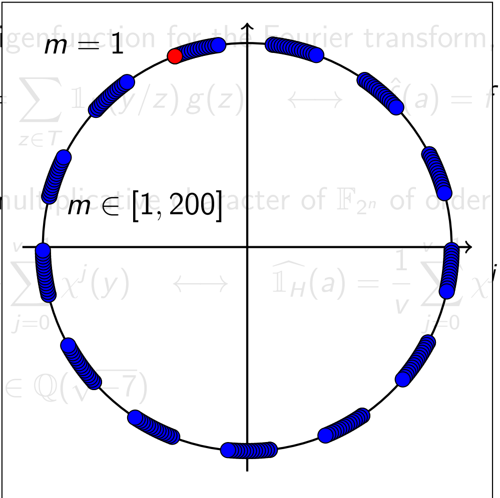
If $\mathbb{1}_H$ is an eigenfunction for the Fourier transform, then on $\mathbb{F}^*_{2^n}$,

$$f(y) = \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \longleftrightarrow \quad \hat{f}(a) = f(a^{-1}).$$

Let χ be a multiplicative character of $\mathbb{F}_{2^n}$ of order v. Then

$$\mathbb{1}_H(y) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(y) \quad \longleftrightarrow \quad \widehat{\mathbb{1}_H}(a) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(a)\, \frac{\overline{G(\chi^j)}}{2^{n/2}}.$$

Then $G(\chi^j) \in \mathbb{Q}(\sqrt{-7})$



Distribution of $\frac{G(\chi)}{2^{n/2}}$, $v = 7$, $n = 3m$

Fourier Near-Eigenfunctions

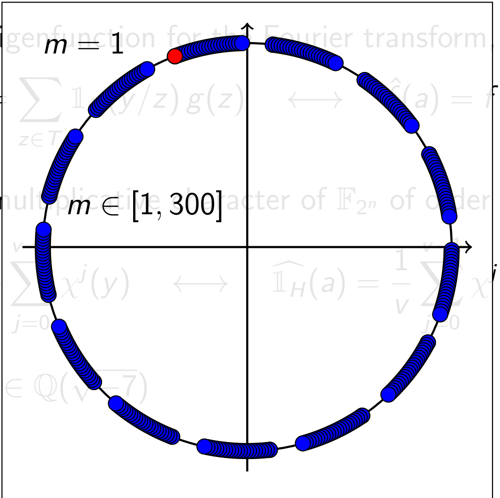
If $\mathbb{1}_H$ is an eigenfunction for the Fourier transform, then on $\mathbb{F}^*_{2^n}$,

$$f(y) = \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \longleftrightarrow \quad \hat{f}(a) = f(a^{-1}).$$

Let χ be a multiplicative character of $\mathbb{F}_{2^n}$ of order v. Then

$$\mathbb{1}_H(y) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(y) \quad \longleftrightarrow \quad \widehat{\mathbb{1}_H}(a) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(a)\, \frac{\overline{G(\chi^j)}}{2^{n/2}}.$$

Then $G(\chi^j) \in \mathbb{Q}(\sqrt{-7})$



Distribution of $\frac{G(\chi)}{2^{n/2}}$, $v = 7$, $n = 3m$

Fourier Near-Eigenfunctions

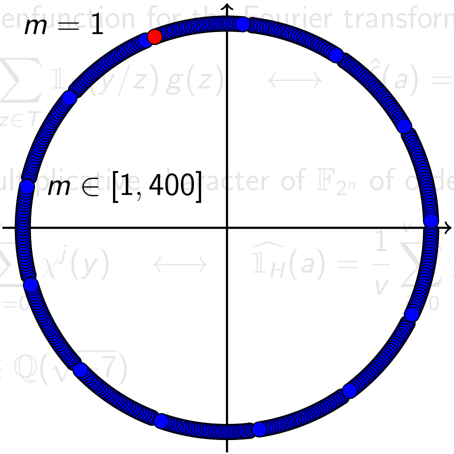
If $\mathbb{1}_H$ is an eigenfunction for the Fourier transform, then on $\mathbb{F}^*_{2^n}$,

$$f(y) = \sum_{z \in T} \mathbb{1}(y/z)\, g(z) \quad \longleftrightarrow \quad \hat{f}(a) = f(a^{-1}).$$

Let χ be a multiplicative character of $\mathbb{F}_{2^n}$ of order v. Then

$$\mathbb{1}_H(y) = \frac{1}{v}\sum_{j=0}^{v} \chi^j(y) \quad \longleftrightarrow \quad \widehat{\mathbb{1}_H}(a) = \frac{1}{v}\sum_{j=0}^{v} \chi^j(a)\, \frac{\overline{G(\chi^j)}}{2^{n/2}}.$$

Then $G(\chi^j) \in \mathbb{Q}(\sqrt{-7})$



Distribution of $\frac{G(\chi)}{2^{n/2}}$, $v = 7$, $n = 3m$

Fourier Near-Eigenfunctions

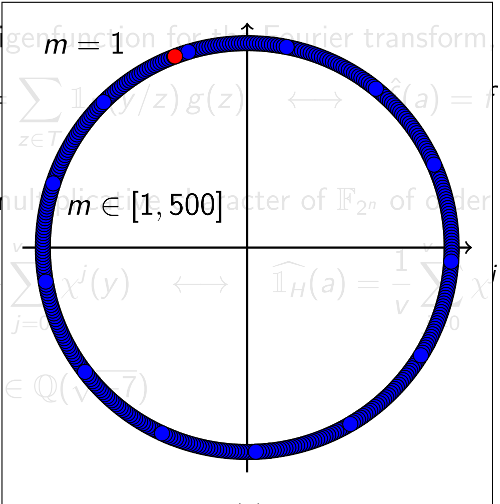
If $\mathbb{1}_H$ is an eigenfunction for the Fourier transform, then on $\mathbb{F}_{2^n}^*$,

$$f(y) = \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \longleftrightarrow \quad \hat{f}(a) = f(a^{-1}).$$

Let χ be a multiplicative character of $\mathbb{F}_{2^n}$ of order v. Then

$$\mathbb{1}_H(y) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(y) \quad \longleftrightarrow \quad \widehat{\mathbb{1}_H}(a) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(a)\, \frac{\overline{G(\chi^j)}}{2^{n/2}}.$$

Then $G(\chi^j) \in \mathbb{Q}(\sqrt{-7})$



Distribution of $\frac{G(\chi)}{2^{n/2}}$, $v = 7$, $n = 3m$

Fourier Near-Eigenfunctions

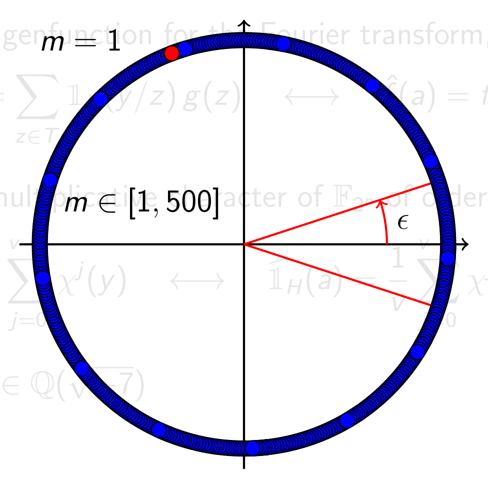
If $\mathbb{1}_H$ is an eigenfunction for the Fourier transform, then on $\mathbb{F}^*_{2^n}$,

$$f(y) = \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \longleftrightarrow \quad \hat{f}(a) = f(a^{-1}).$$

Let χ be a multiplicative character of $\mathbb{F}_{2^n}$ of order v. Then

$$\mathbb{1}_H(y) = \frac{1}{v} \sum_{j=0}^{v} \chi^j(y) \quad \longleftrightarrow \quad \widehat{\mathbb{1}_H}(a) = \frac{1}{v} \sum_{j=0}^{v} \chi^j(a)\, \frac{\overline{G(\chi^j)}}{2^{n/2}}.$$

Then $G(\chi^j) \in \mathbb{Q}(\sqrt{-7})$



Distribution of $\frac{G(\chi)}{2^{n/2}}$, $v = 7$, $n = 3m$

Fourier Near-Eigenfunctions

If $\mathbb{1}_H$ is an eigenfunction for the Fourier transform, then on $\mathbb{F}_{2^n}^*$,

$$f(y) = \sum_{z \in T} \mathbb{1}_H(y/z)\, g(z) \quad \longleftrightarrow \quad \hat{f}(a) = f(a^{-1}).$$

Let χ be a multiplicative character of $\mathbb{F}_{2^n}$ of order v. Then

$$\mathbb{1}_H(y) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(y) \quad \longleftrightarrow \quad \widehat{\mathbb{1}_H}(a) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(a)\, \frac{\overline{G(\chi^j)}}{2^{n/2}}.$$

Then $G(\chi^j) \in \mathbb{Q}(\sqrt{-7})$ and by the Davenport-Hasse Theorem

$$\frac{G(\chi^j)}{2^{n/2}} \approx 1 \quad \text{for some odd } n \text{ and all } 0 < j < v.$$

Six standard deviations suffice

Take an $M \times N$ matrix A with $M \geq N$ and real entries of magnitude at most 1.

Is there a $u \in \{-1, 1\}^N$ such that $\|Au\|_\infty$ is "small"?

Six standard deviations suffice

Take an $M \times N$ matrix A with $M \geq N$ and real entries of magnitude at most 1.

Is there a $u \in \{-1, 1\}^N$ such that $\|Au\|_\infty$ is "small"?

Standard probabilistic method:

$$\|Au\|_\infty < \sqrt{2N \log(2M)} \quad \text{for almost all } u \in \{-1, 1\}^N.$$

Six standard deviations suffice

Take an $M \times N$ matrix A with $M \geq N$ and real entries of magnitude at most 1.

Is there a $u \in \{-1, 1\}^N$ such that $\|Au\|_\infty$ is "small"?

Standard probabilistic method:

$$\|Au\|_\infty < \sqrt{2N \log(2M)} \quad \text{for almost all } u \in \{-1, 1\}^N.$$

Theorem (Spencer 1985). For all sufficiently large N, there exists $u \in \{-1, 1\}^N$ such that

$$\|Au\|_\infty < 11\sqrt{N \log(2M/N)}.$$

Six standard deviations suffice

Take an $M \times N$ matrix A with $M \geq N$ and real entries of magnitude at most 1.

Is there a $u \in \{-1, 1\}^N$ such that $\|Au\|_\infty$ is "small"?

Standard probabilistic method:

$$\|Au\|_\infty < \sqrt{2N \log(2M)} \quad \text{for almost all } u \in \{-1, 1\}^N.$$

Theorem (Spencer 1985). For all sufficiently large N, there exists $u \in \{-1, 1\}^N$ such that

$$\|Au\|_\infty < 11\sqrt{N \log(2M/N)}.$$

This shows the existence of $h : H \to \{-1, 1\}$ such that

$$f(y) = \mathbb{1}_H(y)h(y) \quad \longleftrightarrow \quad |\hat{f}(a)| \leq 11\sqrt{\log(2v)/v}.$$

More general functions

$$f : \mathbb{F}_3^2 \to \mathbb{F}_3, \quad f(x,y) = x^2 + xy - y^2$$

(x,y)	00	01	02	10	11	12	20	21	22
$f(x,y)$	0	2	2	1	1	2	1	2	1

More general functions

$$f : \mathbb{F}_3^2 \to \mathbb{F}_3, \quad f(x,y) = x^2 + xy - y^2$$

(x,y)	00	01	02	10	11	12	20	21	22
$f(x,y)$	0	2	2	1	1	2	1	2	1
$x+y+1$	1	2	0	2	0	1	0	1	2

More general functions

$$f : \mathbb{F}_3^2 \to \mathbb{F}_3, \quad f(x, y) = x^2 + xy - y^2$$

(x, y)	00	01	02	10	11	12	20	21	22
$f(x, y)$	0	2	2	1	1	2	1	2	1
$x + y + 1$	1	2	0	2	0	1	0	1	2
$x - y + 1$	1	0	2	2	1	0	0	2	1

More general functions

$$f : \mathbb{F}_3^2 \to \mathbb{F}_3, \quad f(x,y) = x^2 + xy - y^2$$

(x,y)	00	01	02	10	11	12	20	21	22
$f(x,y)$	0	2	2	1	1	2	1	2	1
$x+y+1$	1	2	0	2	0	1	0	1	2
$x-y+1$	1	0	2	2	1	0	0	2	1

The Hamming distance of f to each of the 27 affine functions is either 5 or 8. Therefore the nonlinearity of f is 5.

More general functions

$$f : \mathbb{F}_3^2 \to \mathbb{F}_3, \quad f(x,y) = x^2 + xy - y^2$$

(x,y)	00	01	02	10	11	12	20	21	22
$f(x,y)$	0	2	2	1	1	2	1	2	1
$x+y+1$	1	2	0	2	0	1	0	1	2
$x-y+1$	1	0	2	2	1	0	0	2	1

The Hamming distance of f to each of the 27 affine functions is either 5 or 8. Therefore the nonlinearity of f is 5.

A more general question

What is the largest nonlinearity of a function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$?

More general functions

$$f : \mathbb{F}_3^2 \to \mathbb{F}_3, \quad f(x,y) = x^2 + xy - y^2$$

(x,y)	00	01	02	10	11	12	20	21	22
$f(x,y)$	0	2	2	1	1	2	1	2	1
$x+y+1$	1	2	0	2	0	1	0	1	2
$x-y+1$	1	0	2	2	1	0	0	2	1

The Hamming distance of f to each of the 27 affine functions is either 5 or 8. Therefore the nonlinearity of f is 5.

A more general question

What is the largest nonlinearity of a function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$?

Equivalently, what is the covering radius of the generalised first order Reed-Muller code $R_q(1,n)$?

A more general conjecture

Writing the nonlinearity as

$$q^{n-1}(q-1) - \mu(f)q^{n/2-1}$$

A more general conjecture

Writing the nonlinearity as

$$q^{n-1}(q-1) - \mu(f)q^{n/2-1}$$

and letting $\mu_q(n)$ be the minimum of $\mu(f)$, we have

$$1 \leq \mu_q(n) \leq \sqrt{q}.$$

Moreover $\mu_q(n) = 1$ for all even n.

A more general conjecture

Writing the nonlinearity as

$$q^{n-1}(q-1) - \mu(f)q^{n/2-1}$$

and letting $\mu_q(n)$ be the minimum of $\mu(f)$, we have

$$1 \leq \mu_q(n) \leq \sqrt{q}.$$

Moreover $\mu_q(n) = 1$ for all even n.

It was shown by (Leducq 2013) that

- $\sqrt{q} = \mu_q(1) \geq \mu_q(3) \geq \mu_q(5) \geq \dots$

A more general conjecture

Writing the nonlinearity as

$$q^{n-1}(q-1) - \mu(f)q^{n/2-1}$$

and letting $\mu_q(n)$ be the minimum of $\mu(f)$, we have

$$1 \leq \mu_q(n) \leq \sqrt{q}.$$

Moreover $\mu_q(n) = 1$ for all even n.

It was shown by (Leducq 2013) that

- $\sqrt{q} = \mu_q(1) \geq \mu_q(3) \geq \mu_q(5) \geq \dots$
- $\mu_3(n) \leq \frac{2}{3}\sqrt{3}$ for each $n \geq 3$ with equality for $n = 3$ and 5

A more general conjecture

Writing the nonlinearity as

$$q^{n-1}(q-1) - \mu(f)q^{n/2-1}$$

and letting $\mu_q(n)$ be the minimum of $\mu(f)$, we have

$$1 \leq \mu_q(n) \leq \sqrt{q}.$$

Moreover $\mu_q(n) = 1$ for all even n.

It was shown by (Leducq 2013) that

- $\sqrt{q} = \mu_q(1) \geq \mu_q(3) \geq \mu_q(5) \geq \ldots$
- $\mu_3(n) \leq \frac{2}{3}\sqrt{3}$ for each $n \geq 3$ with equality for $n = 3$ and 5

The generalised Patterson-Wiedemann Conjecture

.

$$\lim_{n\to\infty} \mu_q(n) = 1 \quad \text{for all prime powers } q.$$

Asymptotic nonlinearities

Theorem (S. 2020). Let q be a power of a prime p and suppose that there is another prime $r > 3$ such that $r \equiv 3 \pmod 4$ and $-p$ is a primitive root modulo r^2. Then $\lim_{n\to\infty} \mu_q(n) = 1$.

Asymptotic nonlinearities

Theorem (S. 2020). Let q be a power of a prime p and suppose that there is another prime $r > 3$ such that $r \equiv 3 \pmod 4$ and $-p$ is a primitive root modulo r^2. Then $\lim_{n\to\infty} \mu_q(n) = 1$.

Prime pairs (p, r) satisfying the condition

p	2	3	5	7	11	13	17	19	23	29	31	37
r	7	23	11	31	7	23	19	31	7	23	11	7

Asymptotic nonlinearities

Theorem (S. 2020). Let q be a power of a prime p and suppose that there is another prime $r > 3$ such that $r \equiv 3 \pmod 4$ and $-p$ is a primitive root modulo r^2. Then $\lim_{n\to\infty} \mu_q(n) = 1$.

Prime pairs (p, r) satisfying the condition

p	2	3	5	7	11	13	17	19	23	29	31	37
r	7	23	11	31	7	23	19	31	7	23	11	7

Corollary (S. 2020). We have $\lim_{n\to\infty} \mu_q(n) = 1$ for all powers q of a prime p lying in a subset of the primes with density 1.

Asymptotic nonlinearities

Theorem (S. 2020). Let q be a power of a prime p and suppose that there is another prime $r > 3$ such that $r \equiv 3 \pmod 4$ and $-p$ is a primitive root modulo r^2. Then $\lim_{n\to\infty} \mu_q(n) = 1$.

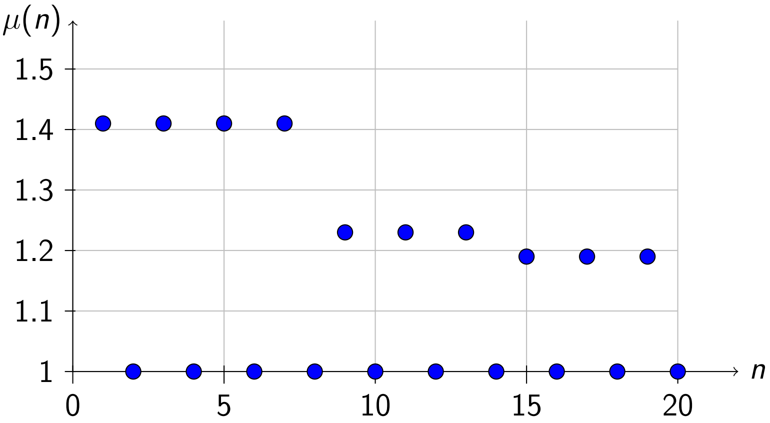
Prime pairs (p, r) satisfying the condition

p	2	3	5	7	11	13	17	19	23	29	31	37
r	7	23	11	31	7	23	19	31	7	23	11	7

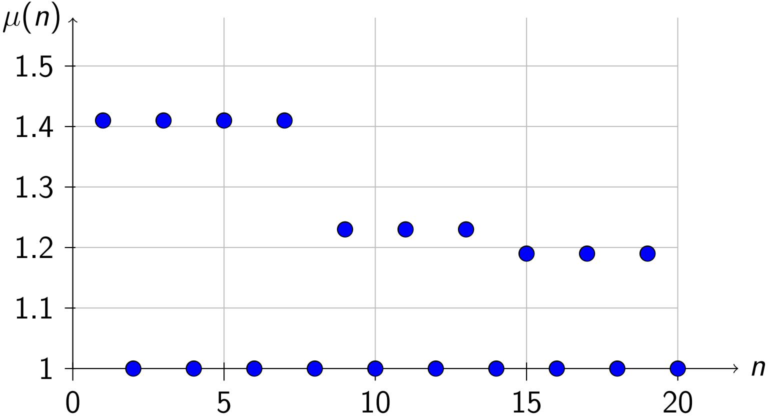
Corollary (S. 2020). We have $\lim_{n\to\infty} \mu_q(n) = 1$ for all powers q of a prime p lying in a subset of the primes with density 1.

Theorem (S. 2020). Assume GRH. Then $\lim_{n\to\infty} \mu_q(n) = 1$ for all prime powers q.

Best known nonlinearities



Best known nonlinearities



We now know that $\lim_{n\to\infty} \mu(n) = 1$,

however without improving any specific value of $\mu(n)$.

The quadratic residue construction

This idea goes back to (Bringer-Gillot-Langevin 2005).

The quadratic residue construction

This idea goes back to (Bringer-Gillot-Langevin 2005).

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ with $H = \{1, \theta^5, \theta^{10}\}$, so that $v = 5$:

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 4, \quad 4^2 \equiv 1 \pmod 5.$$

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

The quadratic residue construction

This idea goes back to (Bringer-Gillot-Langevin 2005).

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ with $H = \{1, \theta^5, \theta^{10}\}$, so that $v = 5$:

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 4, \quad 4^2 \equiv 1 \pmod 5.$$

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

In general, v is prime and $f(0) = 1$ and

$$f(y) = \mathbb{1}_H(y)h(y) + \sum_{k=0}^{v-1} \mathbb{1}_H(y/\theta^k)(k \,|\, v) \quad \text{for } y \in \mathbb{F}_{2^n}^*.$$

The quadratic residue construction

This idea goes back to (Bringer-Gillot-Langevin 2005).

Functions $\mathbb{F}_{2^4} \to \mathbb{F}_2$ with $H = \{1, \theta^5, \theta^{10}\}$, so that $v = 5$:

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 4, \quad 4^2 \equiv 1 \pmod 5.$$

0	θ^0	θ^1	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}	θ^{11}	θ^{12}	θ^{13}	θ^{14}

In general, v is prime and $f(0) = 1$ and

$$f(y) = \mathbb{1}_H(y)h(y) + \sum_{k=0}^{v-1} \mathbb{1}_H(y/\theta^k)(k \,|\, v) \quad \text{for } y \in \mathbb{F}_{2^n}^*.$$

We still have to choose $h : H \to \{-1, 1\}$.

The Fourier transform

Choose v prime, such that $v \equiv 3 \pmod 4$ and such that -2 is a primitive root modulo v. For example, $v = 7, 23, 47, 71, 79$.

The Fourier transform

Choose v prime, such that $v \equiv 3 \pmod 4$ and such that -2 is a primitive root modulo v. For example, $v = 7, 23, 47, 71, 79$.

If χ is a multiplicative character of $\mathbb{F}_{2^n}$ of order v, then

$$G(\chi) = a + b\sqrt{-v}$$

for some unique $a, b \in \mathbb{Z}$ satisfying $a^2 + vb^2 = 2^n$.

The Fourier transform

Choose v prime, such that $v \equiv 3 \pmod 4$ and such that -2 is a primitive root modulo v. For example, $v = 7, 23, 47, 71, 79$.

If χ is a multiplicative character of $\mathbb{F}_{2^n}$ of order v, then

$$G(\chi) = a + b\sqrt{-v}$$

for some unique $a, b \in \mathbb{Z}$ satisfying $a^2 + vb^2 = 2^n$.

Then the Fourier transform of $\sum_{k=1}^{v-1} \mathbb{1}_H(y/\theta^k)(k \,|\, v)$ takes on the four values in the set

$$\frac{1}{2^{n/2}} \,\{0,\, a-b,\, -a-b,\, (v-1)b\}\,.$$

The Fourier transform

Choose v prime, such that $v \equiv 3 \pmod 4$ and such that -2 is a primitive root modulo v. For example, $v = 7, 23, 47, 71, 79$.

If χ is a multiplicative character of $\mathbb{F}_{2^n}$ of order v, then

$$G(\chi) = a + b\sqrt{-v}$$

for some unique $a, b \in \mathbb{Z}$ satisfying $a^2 + vb^2 = 2^n$.

Then the Fourier transform of $\sum_{k=1}^{v-1} \mathbb{1}_H(y/\theta^k)(k \,|\, v)$ takes on the four values in the set

$$\frac{1}{2^{n/2}}\ \{0,\ a-b,\ -a-b,\ (v-1)b\}\,.$$

The maximum modulus is close to 1 if and only if $\frac{G(\chi)}{2^{n/2}} \approx \pm 1$.

Improving Spencer's theorem

Take an $M \times N$ matrix A with $M \geq N$ and real entries of magnitude at most 1.

Theorem (Spencer 1985). For all sufficiently large N, there exists $u \in \{-1, 1\}^N$ such that

$$\|Au\|_\infty < 11\sqrt{N \log(2M/N)}.$$

Improving Spencer's theorem

Take an $M \times N$ matrix A with $M \geq N$ and real entries of magnitude at most 1.

Theorem (Spencer 1985). For all sufficiently large N, there exists $u \in \{-1,1\}^N$ such that

$$\|Au\|_\infty < 11\sqrt{N\log(2M/N)}.$$

Theorem (Goldammer-S. 2020). There exists $u \in \{-1,1\}^N$ such that

$$\|Au\|_\infty < 6\sqrt{N\log(2M/N)}.$$

Improving Spencer's theorem

Take an $M \times N$ matrix A with $M \geq N$ and real entries of magnitude at most 1.

Theorem (Spencer 1985). For all sufficiently large N, there exists $u \in \{-1, 1\}^N$ such that

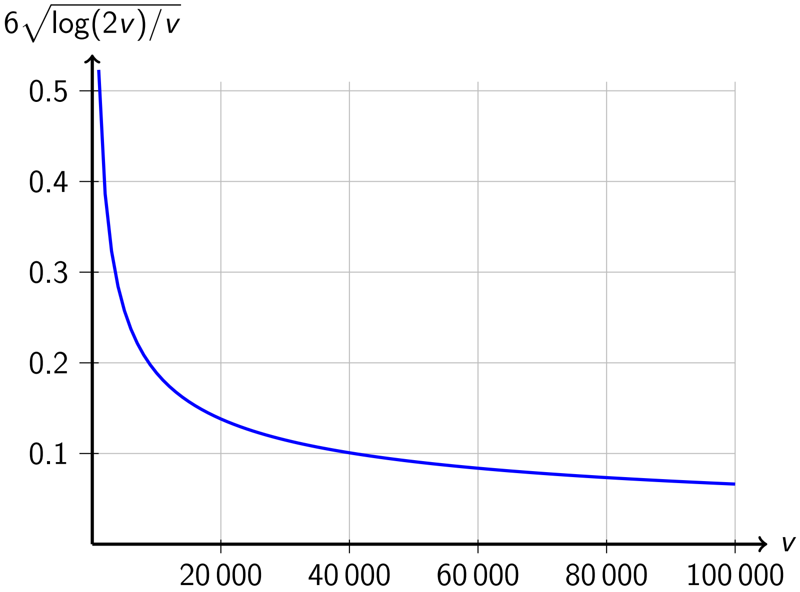
$$\|Au\|_\infty < 11\sqrt{N \log(2M/N)}.$$

Theorem (Goldammer-S. 2020). There exists $u \in \{-1, 1\}^N$ such that

$$\|Au\|_\infty < 6\sqrt{N \log(2M/N)}.$$

This shows the existence of $h : H \to \{-1, 1\}$ such that

$$f(y) = \mathbb{1}_H(y)h(y) \quad \longleftrightarrow \quad |\hat{f}(a)| \leq 6\sqrt{\log(2v)/v}.$$


$6\sqrt{\log(2v)/v}$
0.5
0.4
0.3
0.2
0.1
20 000
40 000
60 000
80 000
100 000
v

Smallest known nonlinearities

- $\mu(3) = \sqrt{2}$ (easy to check)
- $\mu(5) = \sqrt{2}$ (Berlekamp-Welch 1972)
- $\mu(7) = \sqrt{2}$ (Mykkeltveit 1980), (Hou 1996)
- $\mu(n) \leq 1.237\ldots$ for all $n \geq 9$ (Kavut-Yücel 2010)
- $\mu(n) \leq 1.193\ldots$ for all $n \geq 15$ (Patterson-Wiedemann 1983)

Smallest known nonlinearities

- $\mu(3) = \sqrt{2}$ (easy to check)
- $\mu(5) = \sqrt{2}$ (Berlekamp-Welch 1972)
- $\mu(7) = \sqrt{2}$ (Mykkeltveit 1980), (Hou 1996)
- $\mu(n) \leq 1.237\ldots$ for all $n \geq 9$ (Kavut-Yücel 2010)
- $\mu(n) \leq 1.193\ldots$ for all $n \geq 15$ (Patterson-Wiedemann 1983)
- $\mu(n) \leq 1.157\ldots$ for all $n \geq 7\,515$ (Goldammer-S. 2020)

Smallest known nonlinearities

- $\mu(3) = \sqrt{2}$ (easy to check)
- $\mu(5) = \sqrt{2}$ (Berlekamp-Welch 1972)
- $\mu(7) = \sqrt{2}$ (Mykkeltveit 1980), (Hou 1996)
- $\mu(n) \leq 1.237\ldots$ for all $n \geq 9$ (Kavut-Yücel 2010)
- $\mu(n) \leq 1.193\ldots$ for all $n \geq 15$ (Patterson-Wiedemann 1983)
- $\mu(n) \leq 1.157\ldots$ for all $n \geq 7\,515$ (Goldammer-S. 2020)
- $\ldots$
- $\mu(n) \leq 1.056\ldots$ for all $n \geq 1\,211\,811$ (Goldammer-S. 2020)

Autocorrelations

The autocorrelation of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ at shift $u \in \mathbb{F}_2^n$ is

$$C_u(f) = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)+f(y+u)}.$$

Autocorrelations

The autocorrelation of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ at shift $u \in \mathbb{F}_2^n$ is

$$C_u(f) = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)+f(y+u)}.$$

The absolute indicator of f is

$$\delta(f) = \frac{1}{2^{n/2}} \max_{u \neq 0} |C_u(f)|.$$

Autocorrelations

The autocorrelation of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ at shift $u \in \mathbb{F}_2^n$ is

$$C_u(f) = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)+f(y+u)}.$$

The absolute indicator of f is

$$\delta(f) = \frac{1}{2^{n/2}} \max_{u \neq 0} |C_u(f)|.$$

This measures the resistance of a Boolean function against differential cryptanalysis.

Autocorrelations

The autocorrelation of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ at shift $u \in \mathbb{F}_2^n$ is

$$C_u(f) = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)+f(y+u)}.$$

The absolute indicator of f is

$$\delta(f) = \frac{1}{2^{n/2}} \max_{u \neq 0} |C_u(f)|.$$

This measures the resistance of a Boolean function against differential cryptanalysis.

A related question

What is the smallest absolute indicator $\delta(n)$ of a Boolean function on $\mathbb{F}_2^n$?

Small autocorrelations

The autocorrelations can be computed from the Fourier transform:

$$C_u(f) = \sum_{a \in \mathbb{F}_2^n} \widehat{f}(a)^2 \, (-1)^{\langle a,u \rangle}.$$

Small autocorrelations

The autocorrelations can be computed from the Fourier transform:

$$C_u(f) = \sum_{a\in\mathbb{F}_2^n} \widehat{f}(a)^2\,(-1)^{\langle a,u\rangle}.$$

For example, every bent function f satisfies $\delta(f) = 0$. Hence

$$\delta(n) = 0 \quad \text{for all even } n.$$

Small autocorrelations

The autocorrelations can be computed from the Fourier transform:

$$C_u(f) = \sum_{a \in \mathbb{F}_2^n} \widehat{f}(a)^2 \, (-1)^{\langle a,u \rangle}.$$

For example, every bent function f satisfies $\delta(f) = 0$. Hence

$$\delta(n) = 0 \quad \text{for all even } n.$$

The best known general result is (Zhang-Zheng 1996)

$$\delta(n) \le \sqrt{2} \quad \text{for all odd } n.$$

The Zhang-Zheng conjecture

(Zhang-Zheng 1996) constructed balanced Boolean functions f on $\mathbb{F}_2^n$ satisfying

$$\delta(f) \le \begin{cases} 2 & \text{for even } n \\ \sqrt{2} & \text{for odd } n. \end{cases}$$

The Zhang-Zheng conjecture

(Zhang-Zheng 1996) constructed balanced Boolean functions f on $\mathbb{F}_2^n$ satisfying

$$\delta(f) \leq \begin{cases} 2 & \text{for even } n \\ \sqrt{2} & \text{for odd } n. \end{cases}$$

Conjecture (Zhang-Zheng 1996). For every balanced Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ we have

$$\delta(f) \geq \sqrt{2}.$$

The Zhang-Zheng conjecture

(Zhang-Zheng 1996) constructed balanced Boolean functions f on $\mathbb{F}_2^n$ satisfying

$$\delta(f) \le \begin{cases} 2 & \text{for even } n \\ \sqrt{2} & \text{for odd } n. \end{cases}$$

Conjecture (Zhang-Zheng 1996). For every balanced Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ we have

$$\delta(f) \ge \sqrt{2}.$$

This conjecture has been disproved for several small values of n by using the Patterson-Wiedemann approach together with heuristic search techniques.

Infinitely many counterexamples

Theorem (Tang-Maitra 2018). For each $n \geq 46$ with $n \equiv 2 \pmod 4$ there is a balanced function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that

$$\delta(f) \leq 1 - o(1) \quad \text{and} \quad \mu(f) \leq \tfrac{7}{4} + o(1).$$

Infinitely many counterexamples

Theorem (Tang-Maitra 2018). For each $n \geq 46$ with $n \equiv 2 \pmod 4$ there is a balanced function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that

$$\delta(f) \leq 1 - o(1) \quad \text{and} \quad \mu(f) \leq \tfrac{7}{4} + o(1).$$

Theorem (S. 2020). For each even $n \geq 6$ there exists a balanced function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that

$$\delta(f) \leq \frac{8\sqrt{(n+3)\log(2)}}{2^{n/4}} \quad \text{and} \quad \mu(f) \leq 1 + o(1).$$

Infinitely many counterexamples

Theorem (Tang-Maitra 2018). For each $n \geq 46$ with $n \equiv 2 \pmod 4$ there is a balanced function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that

$$\delta(f) \leq 1 - o(1) \quad \text{and} \quad \mu(f) \leq \tfrac{7}{4} + o(1).$$

Theorem (S. 2020). For each even $n \geq 6$ there exists a balanced function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that

$$\delta(f) \leq \frac{8\sqrt{(n+3)\log(2)}}{2^{n/4}} \quad \text{and} \quad \mu(f) \leq 1 + o(1).$$

Moreover there is a probabilistic algorithm that constructs such a function with probability at least $1/2$.

Infinitely many counterexamples

Theorem (Tang-Maitra 2018). For each $n \geq 46$ with $n \equiv 2 \pmod 4$ there is a balanced function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that

$$\delta(f) \leq 1 - o(1) \quad \text{and} \quad \mu(f) \leq \tfrac{7}{4} + o(1).$$

Theorem (S. 2020). For each even $n \geq 6$ there exists a balanced function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that

$$\delta(f) \leq \frac{8\sqrt{(n+3)\log(2)}}{2^{n/4}} \quad \text{and} \quad \mu(f) \leq 1 + o(1).$$

Moreover there is a probabilistic algorithm that constructs such a function with probability at least $1/2$.

This gives counterexamples for all even $n \geq 20$.

Tweaking bent functions

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent function. Then f is perfect:

$$\delta(f) = 0 \quad \text{and} \quad \mu(f) = 1,$$

but not balanced. Suppose that there are more 1's than 0's.

Tweaking bent functions

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent function. Then f is perfect:

$$\delta(f) = 0 \quad \text{and} \quad \mu(f) = 1,$$

but not balanced. Suppose that there are more 1's than 0's.

Flip every 1 with probability

$$\frac{2^{n/2-1}}{2^{n-1} + 2^{n/2-1}}.$$

Tweaking bent functions

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent function. Then f is perfect:

$$\delta(f) = 0 \quad \text{and} \quad \mu(f) = 1,$$

but not balanced. Suppose that there are more 1's than 0's.

Flip every 1 with probability

$$\frac{2^{n/2-1}}{2^{n-1} + 2^{n/2-1}}.$$

Show that this does typically not change $\delta(f)$ and $\mu(f)$ by much and that we typically get a nearly balanced function. Then only a few more bit flips make the function balanced.

New conjectures

Let $\delta'(n)$ be the smallest absolute indicator of a balanced Boolean functions on $\mathbb{F}_2^n$.

New conjectures

Let $\delta'(n)$ be the smallest absolute indicator of a balanced Boolean functions on $\mathbb{F}_2^n$.

Corollary (S. 2020). We have

$$\lim_{m\to\infty} \delta'(2m) = 0.$$

New conjectures

Let $\delta'(n)$ be the smallest absolute indicator of a balanced Boolean functions on $\mathbb{F}_2^n$.

Corollary (S. 2020). We have

$$\lim_{m\to\infty} \delta'(2m) = 0.$$

It is tempting to conjecture that

$$\lim_{n\to\infty} \delta'(n) = 0$$

and hence also

$$\lim_{n\to\infty} \delta(n) = 0.$$

New conjectures

Let $\delta'(n)$ be the smallest absolute indicator of a balanced Boolean functions on $\mathbb{F}_2^n$.

Corollary (S. 2020). We have

$$\lim_{m \to \infty} \delta'(2m) = 0.$$

It is tempting to conjecture that

$$\lim_{n \to \infty} \delta'(n) = 0$$

and hence also

$$\lim_{n \to \infty} \delta(n) = 0.$$

It seems that the functions used in the proof of the Patterson-Wiedemann Conjecture can be used to prove this.

Recent results on the nonlinearity of Boolean functions

Kai-Uwe Schmidt

Paderborn University