On the Fast Algebraic Immunity of Majority Functions

Pierrick MÉAUX

ICTEAM/ELEN/Crypto Group, Université catholique de Louvain, Belgium

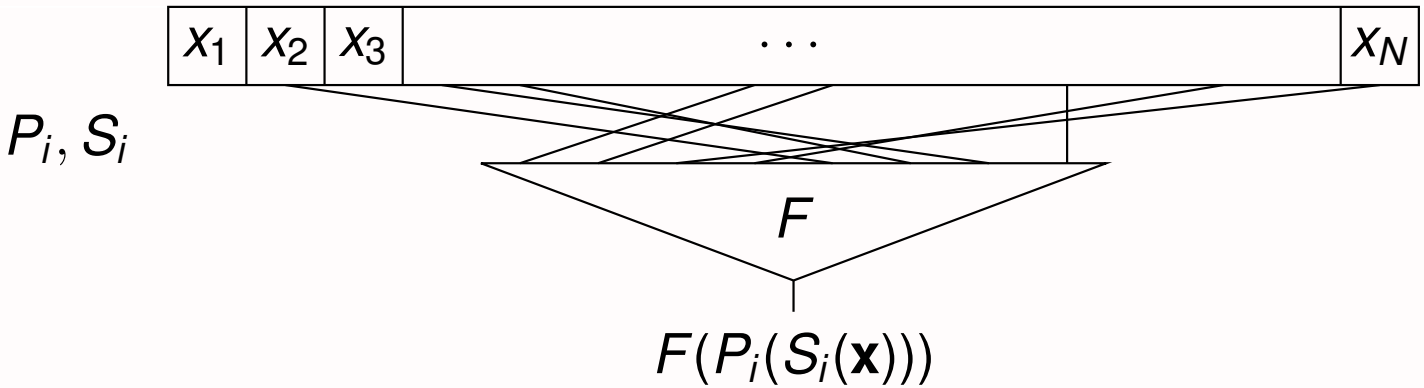
Latincrypt 2019— Santiago de Chile
Wednesday October 2

Table of Contents

Summary

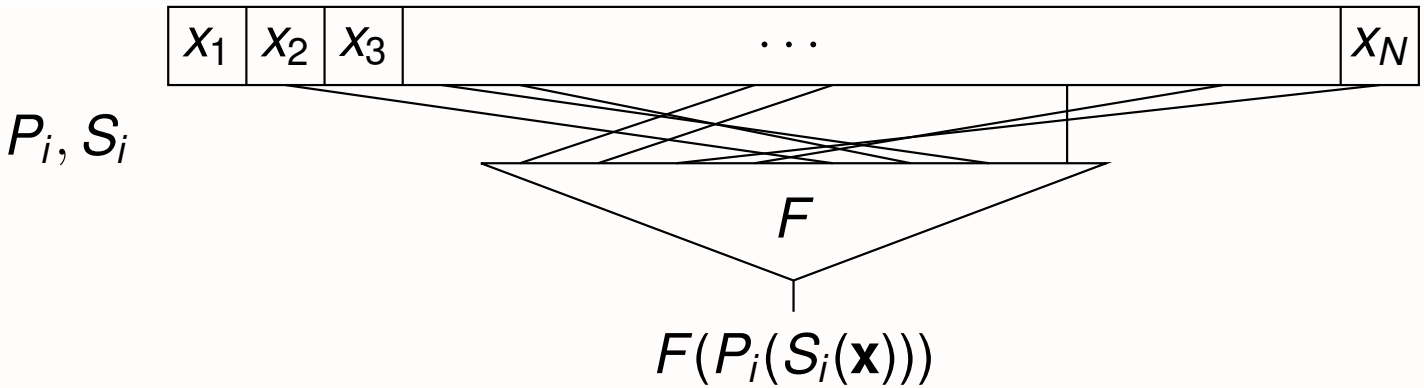
Motivation: Why FAI and Majority Functions?

A conceptually simple design:



Motivation: Why FAI and Majority Functions?

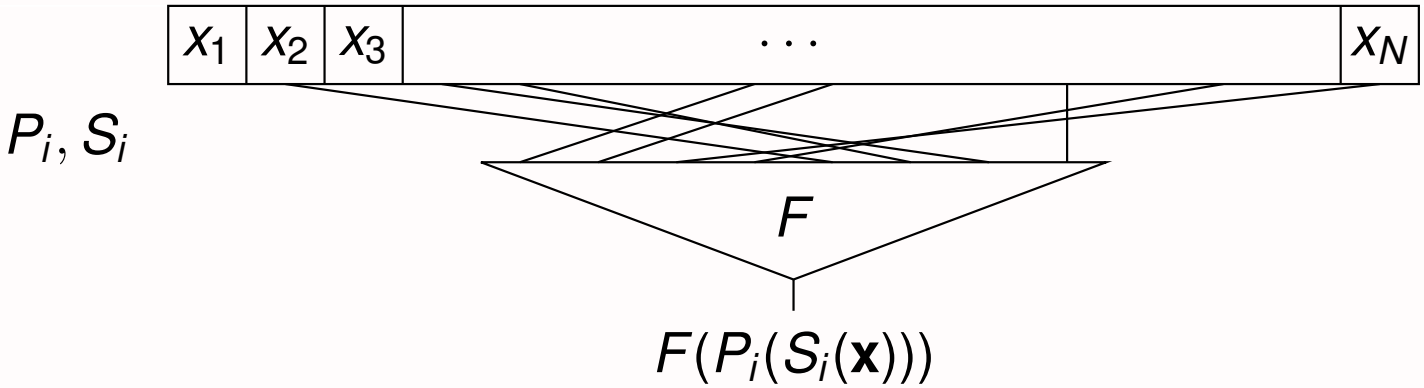
A conceptually simple design:



- Goldreich's PRG [Gol01]: Pseudorandom generators with polynomial stretch and small locality. Local functions.
- FLIP cipher [MJSC16]: stream cipher adapted to frameworks using fully homomorphic encryption.

Motivation: Why FAI and Majority Functions?

A conceptually simple design:



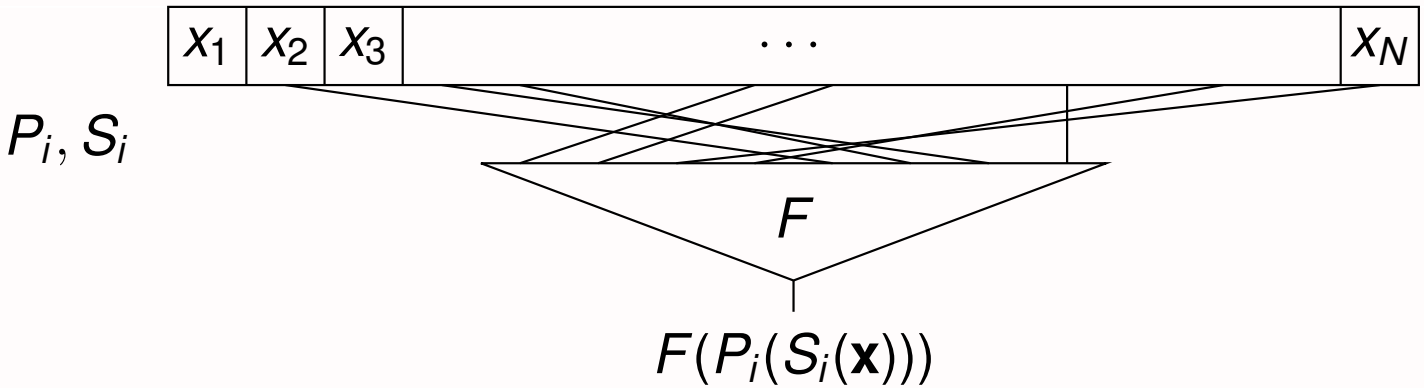
- Goldreich's PRG [Gol01]: Pseudorandom generators with polynomial stretch and small locality. Local functions.
- FLIP cipher [MJSC16]: stream cipher adapted to frameworks using fully homomorphic encryption.

Fast Algebraic Immunity?

Majority functions?

Motivation: Why FAI and Majority Functions?

A conceptually simple design:



- Goldreich's PRG [Gol01]: Pseudorandom generators with polynomial stretch and small locality. Local functions.
- FLIP cipher [MJSC16]: stream cipher adapted to frameworks using fully homomorphic encryption.

Fast Algebraic Immunity? Cryptographic criterion on Boolean functions.
$\rightarrow$ bound on complexity best knowns attacks.

Majority functions? Easy to compute, good algebraic properties.
$\rightarrow$ XOR-MAJ predicates of [AL18], filtering function in FiLIP [MCJS19].

Algebraic System and Attacks

$$\begin{cases} b_1 = F(P_1(S_1(\mathbf{x}))) \\ b_2 = F(P_2(S_2(\mathbf{x}))) \\ b_3 = F(P_3(S_3(\mathbf{x}))) \\ \vdots \end{cases}$$

Resolution:

- SAT solvers , Grobner bases approaches.
- Linearization techniques. Example: all equations have the degree of F.

Algebraic System and Attacks

$$\begin{cases} b_1 = F(P_1(S_1(\mathbf{x}))) \\ b_2 = F(P_2(S_2(\mathbf{x}))) \\ b_3 = F(P_3(S_3(\mathbf{x}))) \\ \vdots \end{cases}$$

Resolution:

- SAT solvers , Grobner bases approaches.
- Linearization techniques. Example: all equations have the degree of F.

Algebraic Attacks [CM03]

Let F be the filtering function

1. find g a low algebraic degree function s.t. g and gF has low degree,
2. create T equations with monomials of degree $\leq deg(g)$,
3. linearize the system of T equations in $D = \sum_{i=0}^{deg(g)} \binom{N}{i}$ variables,
4. solve the system in $\mathcal{O}(D^{\omega})$.

Algebraic System and Attacks

Algebraic Attacks [CM03]

Let F be the filtering function

1. find g a low algebraic degree function s.t. g and gF has low degree,
2. create T equations with monomials of degree $\leq deg(g)$,
3. linearize the system of T equations in $D = \sum_{i=0}^{deg(g)} \binom{N}{i}$ variables,
4. solve the system in $\mathcal{O}(D^\omega)$.

Algebraic Immunity

Let $F : \mathbb{F}_2^N \to \mathbb{F}_2$, we define:

$$\begin{aligned} \mathrm{AI}(F) &= \min\{ \max(\deg(g), \deg(gF), g \neq 0) \} \\ &= \min\{\deg(g), g \neq 0 \mid gF = 0 \text{ or } g(F+1) = 0\} \end{aligned}$$

Algebraic System and Attacks

Algebraic Attacks [CM03]

Let F be the filtering function

1. find g a low algebraic degree function s.t. g and gF has low degree,
2. create T equations with monomials of degree $\leq deg(g)$,
3. linearize the system of T equations in $D = \sum_{i=0}^{deg(g)} \binom{N}{i}$ variables,
4. solve the system in $\mathcal{O}(D^{\omega})$.

Fast Algebraic Attacks [Cou03]

Let F be the filtering function:

1. find g and h of low degree such that $gF = h$, $\deg(g) \leq \mathrm{AI}(F) < \deg(h)$.
2. search linear relations in the system to cancel the monomials of degree more that $\deg(g)$,
3. linearize and solve the system of degree $\deg(g) \leq \mathrm{AI}(F)$.

Algebraic System and Attacks

Fast Algebraic Attacks [Cou03]

Let F be the filtering function:

1. find g and h of low degree such that $gF = h$, $\deg(g) \leq \mathrm{AI}(F) < \deg(h)$.
2. search linear relations in the system to cancel the monomials of degree more that $\deg(g)$,
3. linearize and solve the system of degree $\deg(g) \leq \mathrm{AI}(F)$.

Fast Algebraic Immunity

Let $F : \mathbb{F}_2^N \to \mathbb{F}_2$, we define:

$$\mathrm{FAI}(F) = \min\left\{2\mathrm{AI}(F), \min_{1 \leq \deg(g) < \mathrm{AI}(F)} [\deg(g) + \deg(Fg)]\right\}.$$

Majority Functions

Majority function

$$x = (x_1, \cdots, x_n) \in \mathbb{F}_2^n, \quad \mathrm{MAJ}_n(x) = \begin{cases} 0 & \text{if } \mathrm{w_H}(x) \leq \frac{n}{2}, \\ 1 & \text{otherwise.} \end{cases}$$

Majority Functions

Majority function

$$x = (x_1, \cdots, x_n) \in \mathbb{F}_2^n, \quad \mathrm{MAJ}_n(x) = \begin{cases} 0 & \text{if } \mathrm{w_H}(x) \leq \frac{n}{2}, \\ 1 & \text{otherwise.} \end{cases}$$

- Symmetric function, easy to compute.
  $\rightarrow$ homomorphic evaluation with multiplexers, quasi additive noise [MCJS19].
- Optimal algebraic immunity [BP05,DMS06], $\mathrm{AI}(\mathrm{MAJ}_n) = \lfloor (n+1)/2 \rfloor$.
  $\rightarrow$ direct sum $F = g + \mathrm{MAJ}_n$ provides $\mathrm{AI}(F) \geq \mathrm{AI}(\mathrm{MAJ}_n)$ and $\mathrm{FAI}(F) \geq \mathrm{FAI}(\mathrm{MAJ}_n)$.

Majority Functions

Majority function

$$x = (x_1, \cdots, x_n) \in \mathbb{F}_2^n, \quad \mathrm{MAJ}_n(x) = \begin{cases} 0 & \text{if } \mathrm{w_H}(x) \leq \frac{n}{2}, \\ 1 & \text{otherwise.} \end{cases}$$

- Symmetric function, easy to compute.
  $\rightarrow$ homomorphic evaluation with multiplexers, quasi additive noise [MCJS19].
- Optimal algebraic immunity [BP05,DMS06], $\mathrm{AI}(\mathrm{MAJ}_n) = \lfloor (n+1)/2 \rfloor$.
  $\rightarrow$ direct sum $F = g + \mathrm{MAJ}_n$ provides $\mathrm{AI}(F) \geq \mathrm{AI}(\mathrm{MAJ}_n)$ and $\mathrm{FAI}(F) \geq \mathrm{FAI}(\mathrm{MAJ}_n)$.

Algebraic properties of MAJ_n:

- deg, known for all n.
- AI, known for all n.
- FAI, only bounds.

Related Works and Main Result

Notation:

$$n = 2^m + 2k + \varepsilon,$$

$m \in \mathbb{N}^*, k \in \mathbb{N}, k < 2^{m-1}, \varepsilon \in \{0, 1\}$.

Related Works and Main Result

Notation:

$$n = 2^m + 2k + \varepsilon,$$

$m \in \mathbb{N}^*, k \in \mathbb{N}, k < 2^{m-1}, \varepsilon \in \{0, 1\}$.

- [ACGKMR06] Theorem 2, for $n \geq 2$:

$$\mathrm{FAI}(\mathrm{MAJ}_n) \leq 2^{m-1} + 2k + 2.$$

- [TLD16], exact FAI when $n = 2^m$ and $n = 2^m + 1$.
- [CGZ19], exact FAI when $n = 2^m + 2$ and $n = 2^m + 3$, since $m \geq 2$.

Related Works and Main Result

Notation:

$$n = 2^m + 2k + \varepsilon,$$

$m \in \mathbb{N}^*, k \in \mathbb{N}, k < 2^{m-1}, \varepsilon \in \{0, 1\}$.

- [ACGKMR06] Theorem 2, for $n \geq 2$:

$$\mathrm{FAI}(\mathrm{MAJ}_n) \leq 2^{m-1} + 2k + 2.$$

- [TLD16], exact FAI when $n = 2^m$ and $n = 2^m + 1$.
- [CGZ19], exact FAI when $n = 2^m + 2$ and $n = 2^m + 3$, since $m \geq 2$.

This work:
Let $m \geq 2$, $0 \leq k < 2^{m-2}$, $\varepsilon \in \{0, 1\}$,

$$\mathrm{FAI}(\mathrm{MAJ}_n) = 2^{m-1} + 2k + 2.$$

Summary

Bounding the FAI

Threshold Function

$$x = (x_1, \cdots, x_n) \in \mathbb{F}_2^n, d \in \{0, \cdots, n\}, \quad \mathrm{T}_d(x) = \begin{cases} 0 & \text{if } \mathrm{w_H}(x) < d, \\ 1 & \text{otherwise.} \end{cases}$$

n even: $\mathrm{MAJ}_n = \mathrm{T}_{\frac{n}{2}+1}$, for n odd $\mathrm{MAJ}_n = \mathrm{T}_{\frac{n+1}{2}}$.

Bounding the FAI

Threshold Function

$$x = (x_1, \cdots, x_n) \in \mathbb{F}_2^n, d \in \{0, \cdots, n\}, \quad \mathrm{T}_d(x) = \begin{cases} 0 & \text{if } \mathrm{w_H}(x) < d, \\ 1 & \text{otherwise.} \end{cases}$$

n even: $\mathrm{MAJ}_n = \mathrm{T}_{\frac{n}{2}+1}$, for n odd $\mathrm{MAJ}_n = \mathrm{T}_{\frac{n+1}{2}}$.

Threshold and Annihilators

Annihilators: $\mathrm{AN}(f) = \min_{g \neq 0}[\deg(g) \mid fg = 0]$.

$$\mathrm{AN}(\mathrm{T}_d) = n - d + 1, \text{ and } \mathrm{AN}(1 + \mathrm{T}_d) = d.$$

Multiplicative property: $0 < \deg(g) < \mathrm{AN}(f) \Rightarrow \deg(fg) \geq \mathrm{AN}(f + 1)$.

Bounding the FAI

Threshold and Annihilators

Annihilators: $\mathrm{AN}(f) = \min_{g \neq 0}[\deg(g) \mid fg = 0]$.

$$\mathrm{AN}(\mathrm{T}_d) = n - d + 1, \text{ and } \mathrm{AN}(1 + \mathrm{T}_d) = d.$$

Multiplicative property: $0 < \deg(g) < \mathrm{AN}(f) \Rightarrow \deg(fg) \geq \mathrm{AN}(f + 1)$.

Lower Bound

Let $n = 2^m + 2k + \varepsilon$, $m \geq 1$, $0 \leq k < 2^{m-1}$, and $\varepsilon \in \{0, 1\}$, then:

$$\mathrm{FAI}(\mathrm{MAJ}_n) \geq 2^{m-1} + k + 2.$$

Bounding the FAI

Threshold and Annihilators

Annihilators: $\mathrm{AN}(f) = \min_{g \neq 0}[\deg(g) \mid fg = 0]$.

$$\mathrm{AN}(\mathrm{T}_d) = n - d + 1, \text{ and } \mathrm{AN}(1 + \mathrm{T}_d) = d.$$

Multiplicative property: $0 < \deg(g) < \mathrm{AN}(f) \Rightarrow \deg(fg) \geq \mathrm{AN}(f + 1)$.

Lower Bound

Let $n = 2^m + 2k + \varepsilon$, $m \geq 1$, $0 \leq k < 2^{m-1}$, and $\varepsilon \in \{0, 1\}$, then:

$$\mathrm{FAI}(\mathrm{MAJ}_n) \geq 2^{m-1} + k + 2.$$

$$2^{m-1} + k + 2 \leq \mathrm{FAI}(\mathrm{MAJ}_n) \leq 2^{m-1} + 2k + 2.$$

Corollary: for $n = 2^m + \varepsilon$, $\quad \mathrm{FAI}(\mathrm{MAJ}_n) = 2^{m-1} + 2$.

Algebraic Normal Form of Threshold Functions

Algebraic Normal Form

n-variable polynomial representation over $\mathbb{F}_2$ *i.e.* belonging to $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$:

$$F(x) = \sum_{I \subseteq [n]} a_I \left(\prod_{i \in I} x_i \right) = \sum_{I \subseteq [n]} a_I x^I, \qquad \text{where } a_I \in \mathbb{F}_2.$$

Simplified Algebraic Normal Form for T_d:

λ_0	λ_1	λ_2	$\cdots$	λ_n

F symmetric: all, or none, monomials of the same degree in the ANF.

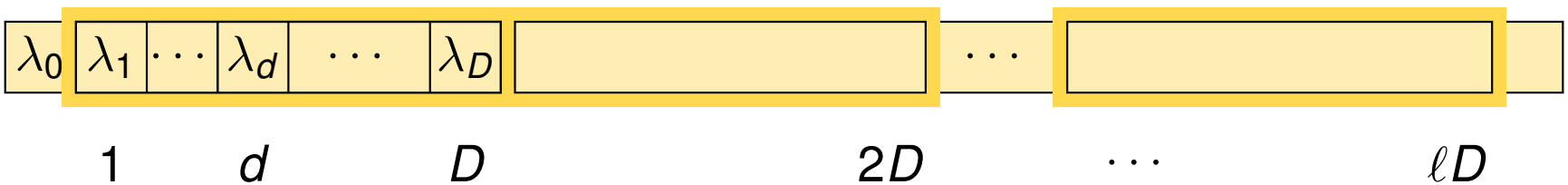
Algebraic Normal Form of Threshold Functions

Algebraic Normal Form

n-variable polynomial representation over $\mathbb{F}_2$ *i.e.* belonging to $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$:

$$F(x) = \sum_{I \subseteq [n]} a_I \left(\prod_{i \in I} x_i \right) = \sum_{I \subseteq [n]} a_I x^I, \qquad \text{where } a_I \in \mathbb{F}_2.$$

Simplified Algebraic Normal Form for T_d:



Periodicity, $D = 2^{\lceil \log d \rceil}$

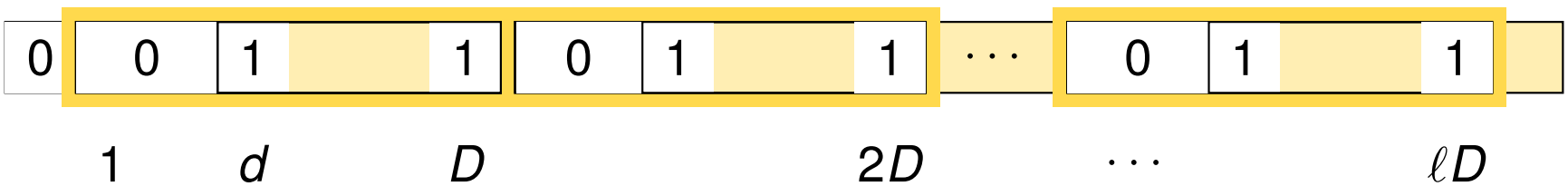
Algebraic Normal Form of Threshold Functions

Algebraic Normal Form

n-variable polynomial representation over $\mathbb{F}_2$ *i.e.* belonging to $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$:

$$F(x) = \sum_{I \subseteq [n]} a_I \left(\prod_{i \in I} x_i \right) = \sum_{I \subseteq [n]} a_I x^I, \qquad \text{where } a_I \in \mathbb{F}_2.$$

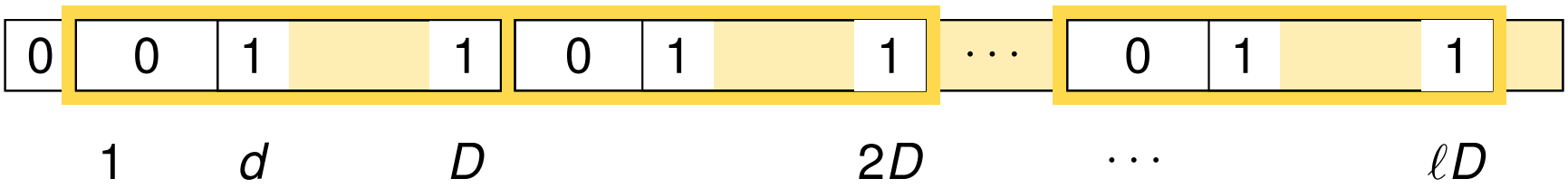
Simplified Algebraic Normal Form for T_d:



Smaller set of interest

Algebraic Normal Form of Threshold Functions

Simplified Algebraic Normal Form for T_d:



Algebraic Normal Form of all Threshold Functions

$n \in \mathbb{N}^*$, $0 < d \leq n+1$, $D = 2^{\lceil \log d \rceil}$, the sets S_d and S'_d are:

$$S_d = \{v \in \{0, D-1\} \mid v \preceq D-d\}, \text{ and } \quad S'_d = \{kD + d + v \mid v \in S_d\} \cap \{1, n\}.$$

The SANF of T_d is such that: $\lambda_{i'} = 1 \Leftrightarrow i' \in S'_d$.
Equivalently:

$$\mathrm{T}_d = \sum_{i \in S'_d} \sigma_i.$$

Algebraic Normal Form of Threshold Functions

Algebraic Normal Form of all Threshold Functions

$n \in \mathbb{N}^*$, $0 < d \leq n+1$, $D = 2^{\lceil \log d \rceil}$, the sets S_d and S'_d are:

$$S_d = \{v \in \{0, D-1\} \mid v \preceq D-d\}, \text{ and } \quad S'_d = \{kD + d + v \mid v \in S_d\} \cap \{1, n\}.$$

The SANF of T_d is such that: $\lambda_{i'} = 1 \Leftrightarrow i' \in S'_d$.
Equivalently:

$$\mathrm{T}_d = \sum_{i \in S'_d} \sigma_i.$$

Example: $d = 3$,
$S_d = \{v \in \{0,1,2,3\} \mid v \preceq 001\} = \{0,1\}$,
$S'_d = \{\{4k+3\} \cup \{4k+4\}\} \cap \{1, n\}$,
$\mathrm{T}_3 = \sigma_3 + \sigma_4 + \sigma_7 + \sigma_8 + \cdots$

Algebraic Normal Form of Threshold Functions

Algebraic Normal Form of all Threshold Functions

$n \in \mathbb{N}^*$, $0 < d \leq n+1$, $D = 2^{\lceil \log d \rceil}$, the sets S_d and S'_d are:

$$S_d = \{v \in \{0, D-1\} \mid v \preceq D-d\}, \text{ and } \quad S'_d = \{kD + d + v \mid v \in S_d\} \cap \{1, n\}.$$

The SANF of T_d is such that: $\lambda_{i'} = 1 \Leftrightarrow i' \in S'_d$.
Equivalently:

$$\mathrm{T}_d = \sum_{i \in S'_d} \sigma_i.$$

Example: $d = 3$,
$S_d = \{v \in \{0,1,2,3\} \mid v \preceq 001\} = \{0,1\}$,
$S'_d = \{\{4k+3\} \cup \{4k+4\}\} \cap \{1, n\}$,
$\mathrm{T}_3 = \sigma_3 + \sigma_4 + \sigma_7 + \sigma_8 + \cdots$
Corollary: φ_d indicator of Hamming weight d:

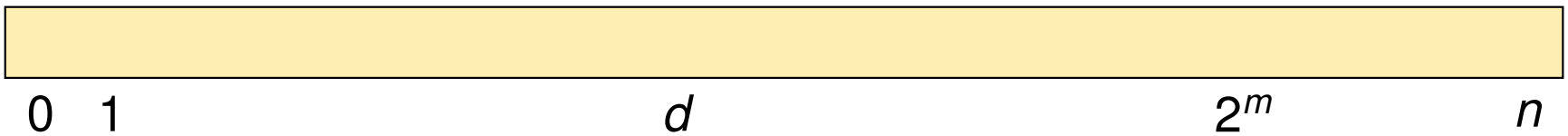
$$\varphi_d = \sum_{i \in S'_d \triangle S'_{d+1}} \sigma_i.$$

Summary

Proof Overview (1)

$n = 2^m + 2k + \varepsilon, \quad m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}.$

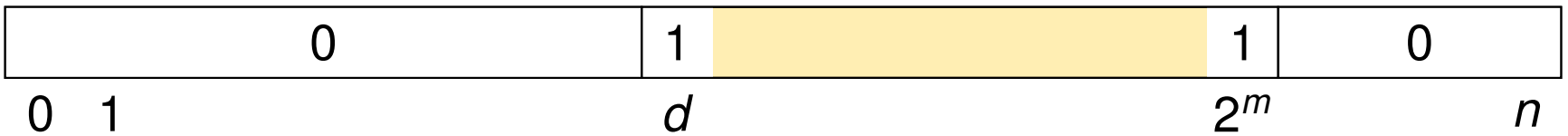
$$\mathrm{MAJ}_n = \mathrm{T}_{2^{m-1}+k+1}.$$



Proof Overview (1)

$n = 2^m + 2k + \varepsilon, \quad m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}.$

$$\mathrm{MAJ}_n = \mathrm{T}_{2^{m-1}+k+1}.$$

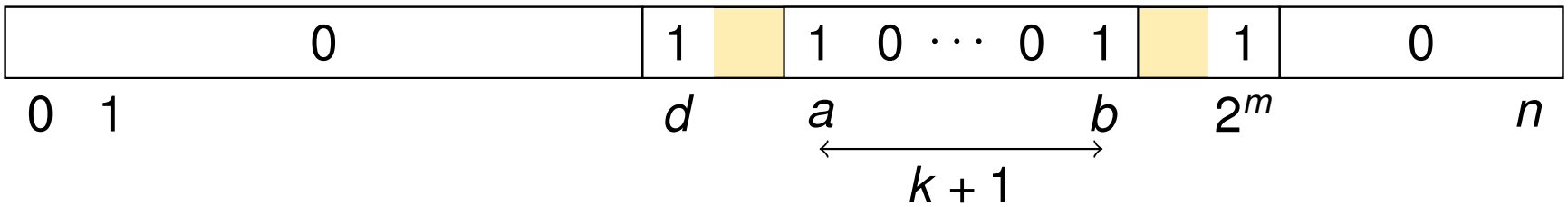


Set of interest: $\{d, \cdots, D\}$

Proof Overview (1)

$n = 2^m + 2k + \varepsilon, \quad m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}.$

$$\mathrm{MAJ}_n = \mathrm{T}_{2^{m-1}+k+1}.$$

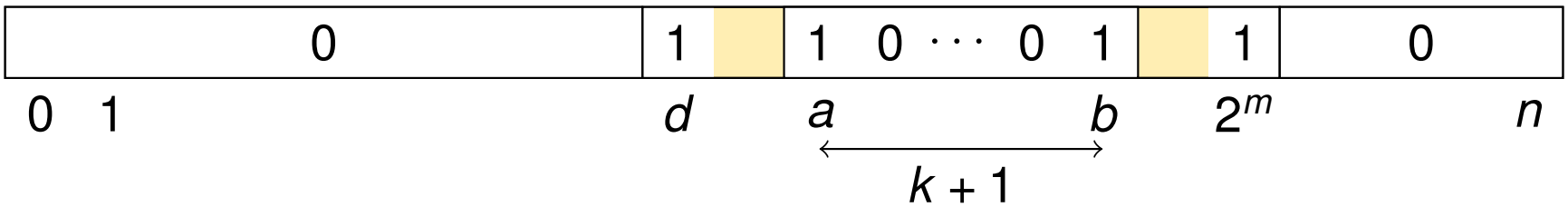


Set of interest: $\{d, \cdots, D\}$
Gap: $a = 2^m - 2^{m-2}$, $b = 2^m - 2^{m-2} + k + 1$, and $\{a, \cdots, b\} \cap S'_d = \{a, b\}$.

Proof Overview (1)

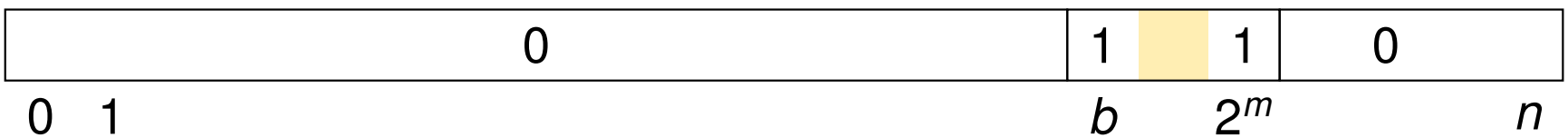
$n = 2^m + 2k + \varepsilon, \quad m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}.$

$$\mathrm{MAJ}_n = \mathrm{T}_{2^{m-1}+k+1}.$$



Set of interest: $\{d, \cdots, D\}$
Gap: $a = 2^m - 2^{m-2}$, $b = 2^m - 2^{m-2} + k + 1$, and $\{a, \cdots, b\} \cap S'_d = \{a, b\}$.

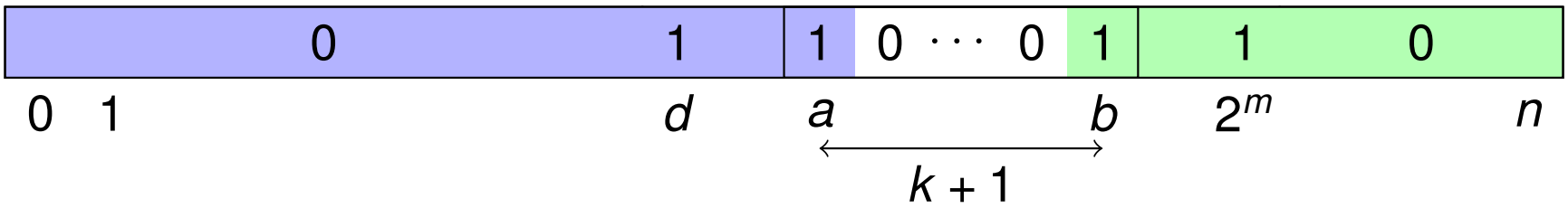
$$\mathrm{T}_b = \mathrm{T}_{2^m - 2^{m-2}+k+1}.$$



Proof Overview (1)

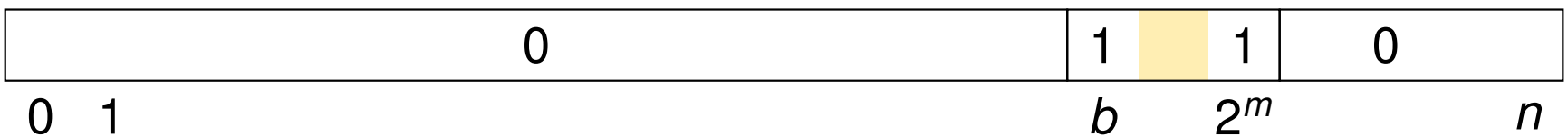
$n = 2^m + 2k + \varepsilon, \quad m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}.$

$$\mathrm{MAJ}_n = \mathrm{T}_{2^{m-1}+k+1}.$$



Set of interest: $\{d, \cdots, D\}$
Gap: $a = 2^m - 2^{m-2}$, $b = 2^m - 2^{m-2} + k + 1$, and $\{a, \cdots, b\} \cap S'_d = \{a, b\}$.

$$\mathrm{T}_b = \mathrm{T}_{2^m - 2^{m-2}+k+1}.$$

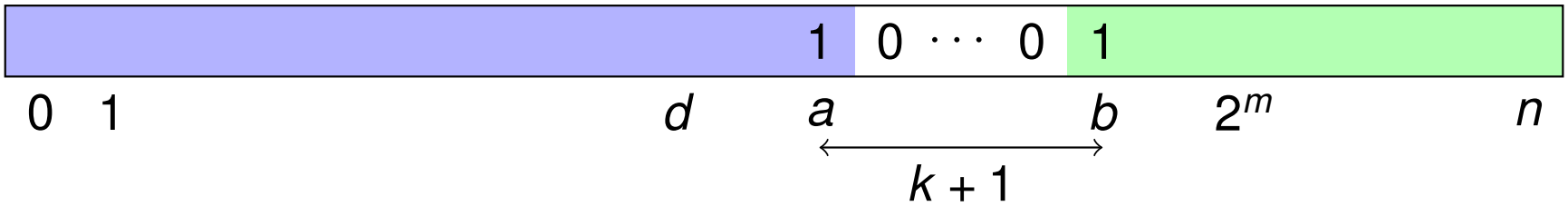


Partition: $\mathrm{MAJ}_n = f_a + \mathrm{T}_b$

Proof Overview (2)

Consider $n = 2^m + 2k + \varepsilon$; $\quad m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}$.

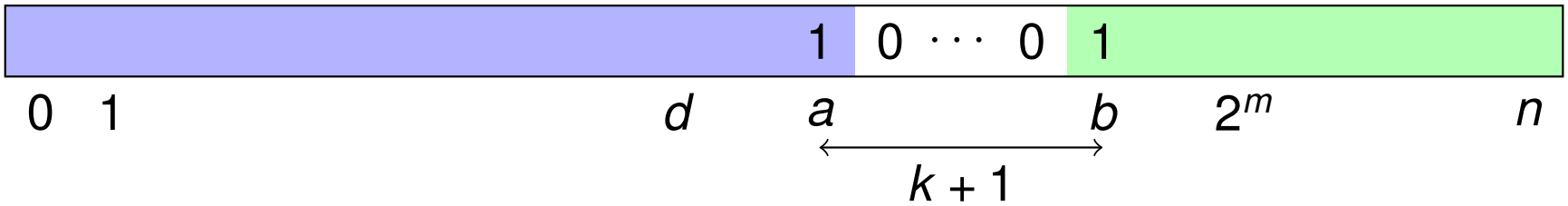
$$\mathrm{MAJ}_n = \mathrm{T}_{2^{m-1}+k+1} = f_a + \mathrm{T}_b.$$



Proof Overview (2)

Consider $n = 2^m + 2k + \varepsilon$; $\quad m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}$.

$$\mathrm{MAJ}_n = \mathrm{T}_{2^{m-1}+k+1} = f_a + \mathrm{T}_b.$$



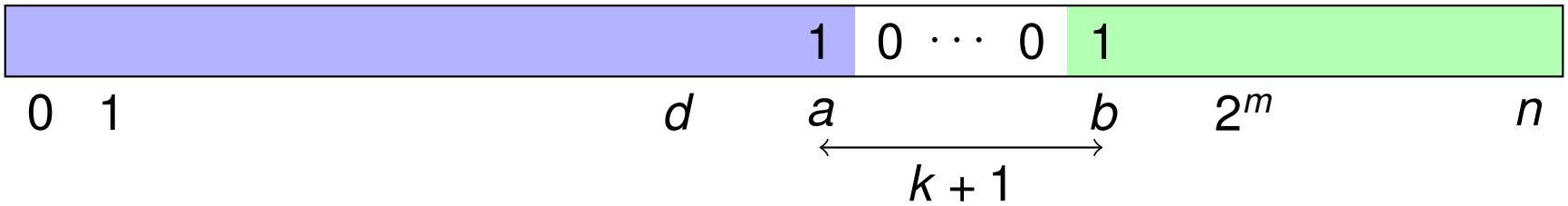
Recall: $\mathrm{FAI}(F) = \min\left\{2\mathrm{AI}(F), \min_{1 \leq \deg(g) < \mathrm{AI}(F)}[\deg(g) + \deg(Fg)]\right\}$

Since $2\mathrm{AI}(\mathrm{MAJ}_n) \geq n$, we focus on the degree of $\mathrm{MAJ}_n g$:

Proof Overview (2)

Consider $n = 2^m + 2k + \varepsilon$; $\quad m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}$.

$$\mathrm{MAJ}_n = \mathrm{T}_{2^{m-1}+k+1} = f_a + \mathrm{T}_b.$$



Recall: $\mathrm{FAI}(F) = \min\left\{2\mathrm{AI}(F), \min_{1 \leq \deg(g) < \mathrm{AI}(F)}[\deg(g) + \deg(Fg)]\right\}$

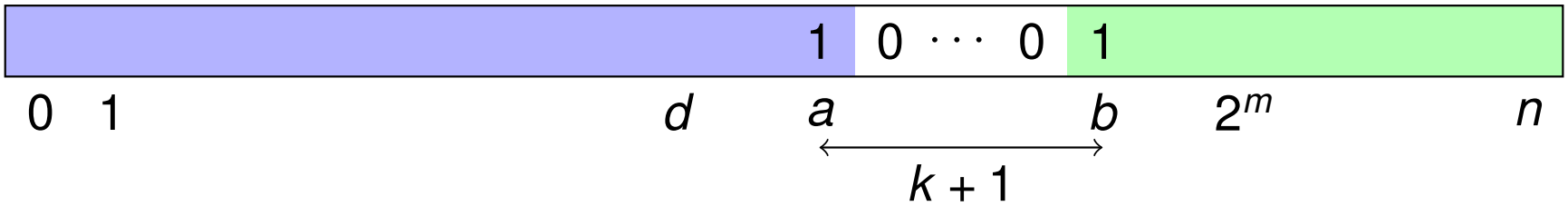
Since $2\mathrm{AI}(\mathrm{MAJ}_n) \geq n$, we focus on the degree of $\mathrm{MAJ}_n g$:

- If $1 \leq \deg(g) \leq k$:
  since $k < \mathrm{AI}(\mathrm{T}_b) \leq \mathrm{AN}(1 + \mathrm{T}_b) = b$, then $\deg(g\mathrm{T}_b) \geq b$
  $\deg(gf_a) \leq a + k < b$
  then $\deg(g(f_a + \mathrm{T}_b))+ \geq b \geq 2^{m-1} + 2k + 2 \quad$ (using $2^{m-2} > k$).

Proof Overview (2)

Consider $n = 2^m + 2k + \varepsilon$; $\quad m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}$.

$$\mathrm{MAJ}_n = \mathrm{T}_{2^{m-1}+k+1} = f_a + \mathrm{T}_b.$$



Recall: $\mathrm{FAI}(F) = \min\left\{2\mathrm{AI}(F), \min_{1 \leq \deg(g) < \mathrm{AI}(F)}[\deg(g) + \deg(Fg)]\right\}$

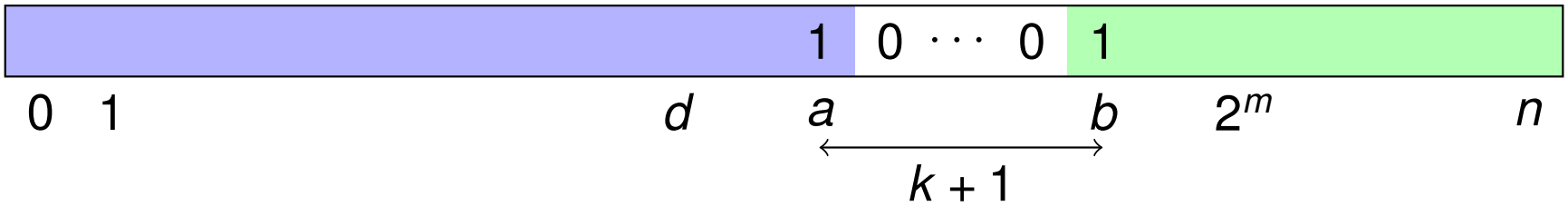
Since $2\mathrm{AI}(\mathrm{MAJ}_n) \geq n$, we focus on the degree of $\mathrm{MAJ}_n g$:

- If $1 \leq \deg(g) \leq k$:
  since $k < \mathrm{AI}(\mathrm{T}_b) \leq \mathrm{AN}(1 + \mathrm{T}_b) = b$, then $\deg(g\mathrm{T}_b) \geq b$
  $\deg(gf_a) \leq a + k < b$
  then $\deg(g(f_a + \mathrm{T}_b))+ \geq b \geq 2^{m-1} + 2k + 2 \quad$ (using $2^{m-2} > k$).
- If $k < \deg(g) < \mathrm{AI}(\mathrm{MAJ}_n)$:
  $\deg(g\mathrm{MAJ}_n) \geq \mathrm{AN}(\mathrm{MAJ}_n + 1) \quad$ (multiplicative property)
  $\deg(g\mathrm{MAJ}_n) \geq 2^{m-1} + k + 1 \quad$ (AN threshold functions)
  then $\deg(g) + \deg(Fg) \geq 2^{m-1} + 2k + 2$.

Proof Overview (2)

Consider $n = 2^m + 2k + \varepsilon$; $\quad m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}$.

$$\mathrm{MAJ}_n = \mathrm{T}_{2^{m-1}+k+1} = f_a + \mathrm{T}_b.$$



Recall: $\mathrm{FAI}(F) = \min\left\{2\mathrm{AI}(F), \min_{1 \leq \deg(g) < \mathrm{AI}(F)}[\deg(g) + \deg(Fg)]\right\}$

Since $2\mathrm{AI}(\mathrm{MAJ}_n) \geq n$, we focus on the degree of $\mathrm{MAJ}_n g$:

- If $1 \leq \deg(g) \leq k$:
  since $k < \mathrm{AI}(\mathrm{T}_b) \leq \mathrm{AN}(1 + \mathrm{T}_b) = b$, then $\deg(g\mathrm{T}_b) \geq b$
  $\deg(gf_a) \leq a + k < b$
  then $\deg(g(f_a + \mathrm{T}_b))+ \geq b \geq 2^{m-1} + 2k + 2 \quad$ (using $2^{m-2} > k$).
- If $k < \deg(g) < \mathrm{AI}(\mathrm{MAJ}_n)$:
  $\deg(g\mathrm{MAJ}_n) \geq \mathrm{AN}(\mathrm{MAJ}_n + 1) \quad$ (multiplicative property)
  $\deg(g\mathrm{MAJ}_n) \geq 2^{m-1} + k + 1 \quad$ (AN threshold functions)
  then $\deg(g) + \deg(Fg) \geq 2^{m-1} + 2k + 2$.

$\Rightarrow$ reaching upper bound,

$$\mathrm{FAI}(\mathrm{MAJ}_n) = 2^{m-1} + 2k + 2.$$

Summary

Conclusion and open questions

Conclusion:

◇ ANF of threshold functions.

→ Simple formulation with sets, basis for all symmetric functions.

◇ Exact fast algebraic immunity of MAJ_n, $n = 2^m + 2k + \varepsilon$, where $m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}$.

→ Better bounds for XOR-MAJ functions.

Conclusion and open questions

Conclusion:

◇ ANF of threshold functions.

→ Simple formulation with sets, basis for all symmetric functions.

◇ Exact fast algebraic immunity of MAJ_n, $n = 2^m + 2k + \varepsilon$, where $m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}$.

→ Better bounds for XOR-MAJ functions.

Open questions:

◇ Remaining cases?

- $m < 2$ solved, $\mathrm{FAI}(\mathrm{MAJ}_2) = 2$, and $n = 3$ from corollary.
- $m \geq 2$, $2^{m-2} < k < 2^{m-1}$. Upper bound $B = 2^{m-1} + 2k + 2$ unreachable.
- $m \geq 2$, $k = 2^{m-2}$. B reachable (ex $n = 6$).

◇ Extending techniques for all threshold function? all symmetric functions?

Conclusion and open questions

Conclusion:

◇ ANF of threshold functions.

→ Simple formulation with sets, basis for all symmetric functions.

◇ Exact fast algebraic immunity of MAJ_n, $n = 2^m + 2k + \varepsilon$, where $m \geq 2, 0 \leq k < 2^{m-2}, \varepsilon \in \{0, 1\}$.

→ Better bounds for XOR-MAJ functions.

Open questions:

◇ Remaining cases?

- $m < 2$ solved, $\mathrm{FAI}(\mathrm{MAJ}_2) = 2$, and $n = 3$ from corollary.
- $m \geq 2$, $2^{m-2} < k < 2^{m-1}$. Upper bound $B = 2^{m-1} + 2k + 2$ unreachable.
- $m \geq 2$, $k = 2^{m-2}$. B reachable (ex $n = 6$).

◇ Extending techniques for all threshold function? all symmetric functions?

Thanks for your attention!