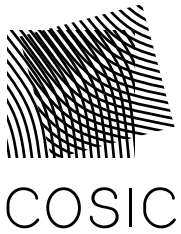
CLASSIFICATION OF BALANCED QUADRATIC FUNCTIONS

Lauren De Meyer & Begül Bilgin

BFA, Loen Norway, June 20th 2018



Research Foundation Flanders
Opening new horizons

¿(Vectorial) Boolean Functions?

Lookup Table (LUT): $0123457689CDEFBA$

Algebraic Normal Form (ANF):

$$S_0(x) = x_0 \oplus x_1x_2$$
$$S_1(x) = x_1 \oplus x_1x_3 \oplus x_2x_3$$
$$S_2(x) = x_2 \oplus x_1x_3$$
$$S_3(x) = x_3$$

Algebraic Degree: 2

Differential Uniformity (Diff): $= \max_{\alpha,\beta\neq 0} \#\{x \in \mathbb{F}_2^p : S(x \oplus \alpha) = S(x) \oplus \beta\} = 16$

Linearity (Lin): $= \max_{\alpha,\beta\neq 0} |\#\{x \in \mathbb{F}_2^p : \alpha \cdot x = \beta \cdot S(x)\} - 2^{p-1}| = 16$

Affine Equivalence

$F_1 \sim F_2$  $F_1 = B \circ F_2 \circ A$

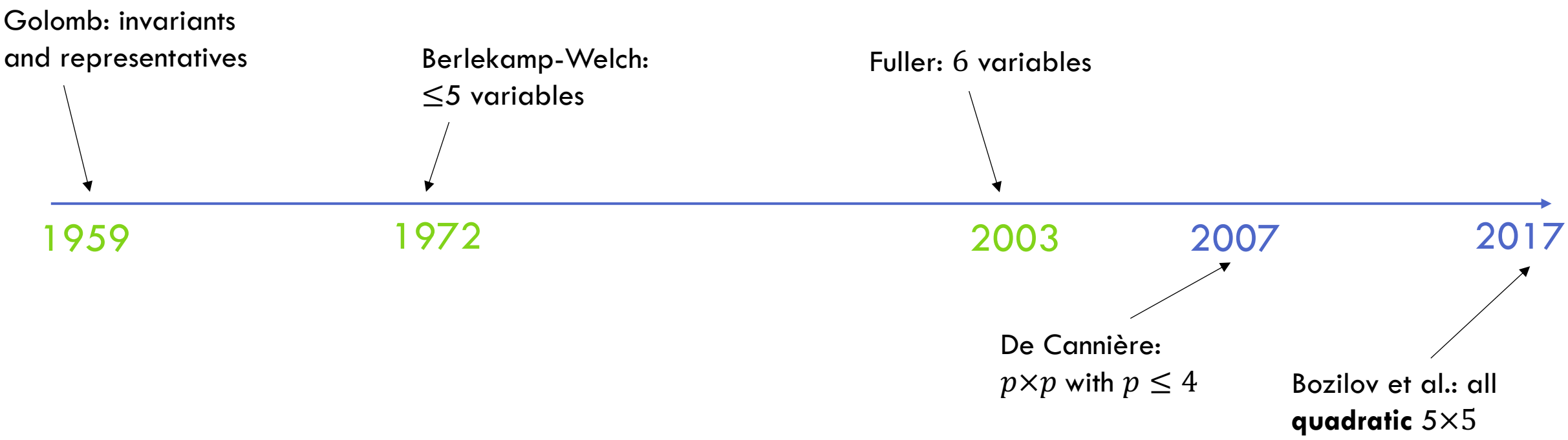
with A, B affine permutations

Invariants:

- Algebraic Degree
- Differential Uniformity
- Linearity
- Multiplicative Complexity

Timeline of Affine Equivalence Classification

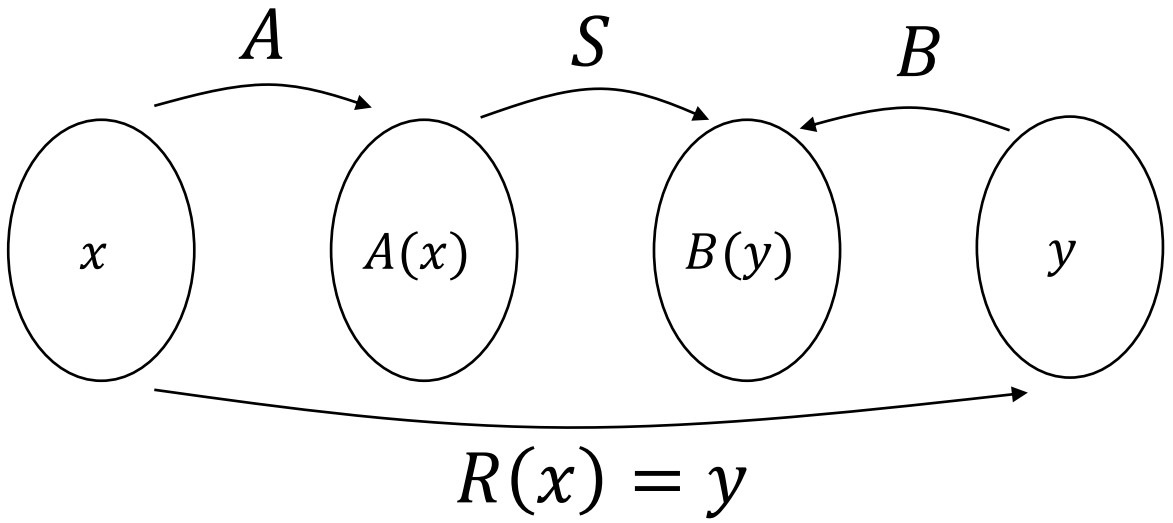
Boolean Functions $f\colon \mathbb{F}_2^p \to \mathbb{F}_2$



Vectorial Boolean Functions: $F\colon \mathbb{F}_2^p \to \mathbb{F}_2^p$

FIND REPRESENTATIVE

- Algorithm by Biryukov et al. [1]
- To find Representative $R = B^{-1} \circ S \circ A$
- for permutations only, i.e. $p \times p$ Boolean Functions S
- Representative is lexicographically smallest of equivalence class



[1] A. Biryukov, C. De Canniere, A. Braeken, and B. Preneel. A toolbox for cryptanalysis: Linear and affine equivalence algorithms. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 33–50. Springer, 2003.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	1	B	9	C	D	6	F	3	E	8	7	4	A	2	5	0

$$x \to A(x) \xrightarrow{S} B(y) \leftarrow y$$

$$0 \to \quad \to \quad \leftarrow 0$$

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$R(x)$	0															

x	**0**	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	**1**	B	9	C	D	6	F	3	E	8	7	4	A	2	5	0

$$x \rightarrow A(x) \quad \overset{S}{\rightarrow} \quad B(y) \leftarrow y$$

Guess $0 \rightarrow 0 \rightarrow 1 \leftarrow 0$

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$R(x)$	0															

x	0	**1**	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	1	**B**	9	C	D	6	F	3	E	8	7	4	A	2	5	0

	$x \to A(x)$	$\overset{S}{\to}$	$B(y) \leftarrow y$
Guess	$0 \to 0$	$\to$	$1 \leftarrow 0$
Guess	$1 \to 1$	$\to$	$B \leftarrow 1$

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$R(x)$	0	1														

x	0	1	**2**	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	1	B	**9**	C	D	6	F	3	E	8	7	4	A	2	5	0

	$x \to A(x)$	$\overset{S}{\to}$	$B(y) \leftarrow y$
Guess	$0 \to 0$	$\to$	$1 \leftarrow 0$
Guess	$1 \to 1$	$\to$	$B \leftarrow 1$
Guess	$2 \to 2$	$\to$	$9 \leftarrow 2$

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$R(x)$	0	1	2													

x	0	1	2	**3**	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	1	B	9	**C**	D	6	F	3	E	8	7	4	A	2	5	0

	$x \to A(x)$	$\overset{S}{\to}$	$B(y) \leftarrow y$	
Guess	$0 \to 0$	$\to$	$1 \leftarrow 0$	
Guess	$1 \to 1$	$\to$	$B \leftarrow 1$	
Guess	$2 \to 2$	$\to$	$9 \leftarrow 2$	
Forward	$3 \to 3$	$\to$	$C \leftarrow 4$	= smallest available power of 2

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$R(x)$	0	1	2	4												

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	1	B	9	C	D	6	F	3	E	8	7	4	A	2	5	0

	$x \to A(x)$	$\overset{S}{\to}$	$B(y) \leftarrow y$	
Guess	$0 \to 0$	$\to$	$1 \leftarrow 0$	
Guess	$1 \to 1$	$\to$	$B \leftarrow 1$	
Guess	$2 \to 2$	$\to$	$9 \leftarrow 2$	
Forward	$3 \to 3$	$\to$	$C \leftarrow 4$	
Bckward	$4 \to 7$	$\leftarrow$	$3 \leftarrow 3$	= smallest y for which $B(y)$ defined

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$R(x)$	0	1	2	4	3											

x	0	1	2	3	4	5	**6**	7	8	9	A	B	C	D	E	F
$S(x)$	1	B	9	C	D	6	**F**	3	E	8	7	4	A	2	5	0

	$x \to A(x)$	$\overset{S}{\to}$	$B(y) \leftarrow y$	
Guess	$0 \to 0$	$\to$	$1 \leftarrow 0$	
Guess	$1 \to 1$	$\to$	$B \leftarrow 1$	
Guess	$2 \to 2$	$\to$	$9 \leftarrow 2$	
Forward	$3 \to 3$	$\to$	$C \leftarrow 4$	
Bckward	$4 \to 7$	$\leftarrow$	$3 \leftarrow 3$	
Forward	$5 \to 6$	$\to$	$F \leftarrow 8$	= smallest available power of 2

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$R(x)$	0	1	2	4	3	8										

x	0	1	2	3	4	**5**	6	7	8	9	A	B	C	D	E	F
$S(x)$	1	B	9	C	D	**6**	F	3	E	8	7	4	A	2	5	0

	$x \to A(x)$	$\overset{S}{\to}$	$B(y) \leftarrow y$
Guess	$0 \to 0$	$\to$	$1 \leftarrow 0$
Guess	$1 \to 1$	$\to$	$B \leftarrow 1$
Guess	$2 \to 2$	$\to$	$9 \leftarrow 2$
Forward	$3 \to 3$	$\to$	$C \leftarrow 4$
Bckward	$4 \to 7$	$\leftarrow$	$3 \leftarrow 3$
Forward	$5 \to 6$	$\to$	$F \leftarrow 8$
Forward	$6 \to 5$	$\to$	$6 \leftarrow 5$
		…	

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$R(x)$	0	1	2	4	3	8	5	…								

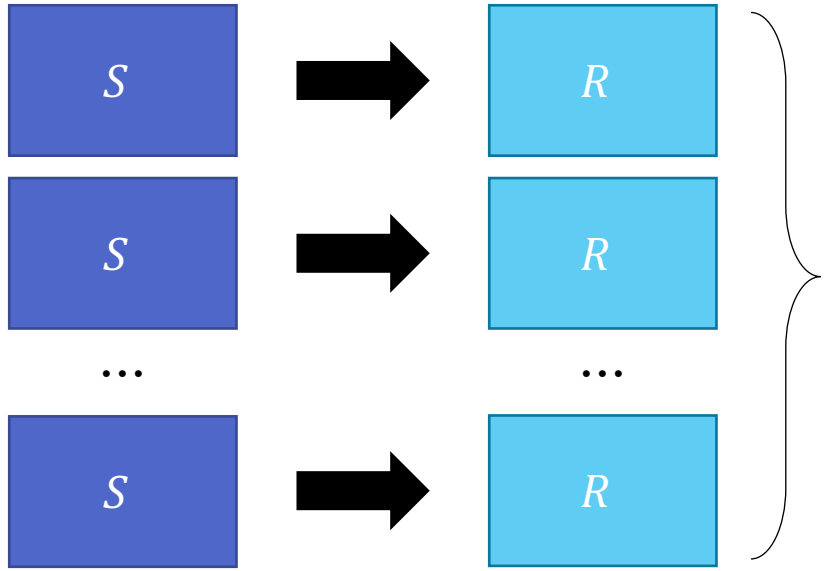
x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	1	B	9	C	D	6	F	3	E	8	7	4	A	2	5	0

	$x \to A(x)$	$\overset{S}{\to}$	$B(y) \leftarrow y$
Guess	$0 \to 0$	$\to$	$1 \leftarrow 0$
Guess	$1 \to 5$	$\to$	$6 \leftarrow 1$
Guess	$2 \to A$	$\to$	$7 \leftarrow 2$
Forward	$3 \to F$	$\to$	$0 \leftarrow 3$
Guess	$4 \to 4$	$\leftarrow$	$\mathrm{D} \leftarrow 4$
Forward	$5 \to 1$	$\to$	$B \leftarrow 6$
Forward	$6 \to E$	$\to$	$5 \leftarrow 8$
		…	

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$R(x)$	0	1	2	3	4	6	8	…								

Classifying 5 × 5 Quadratic S-boxes

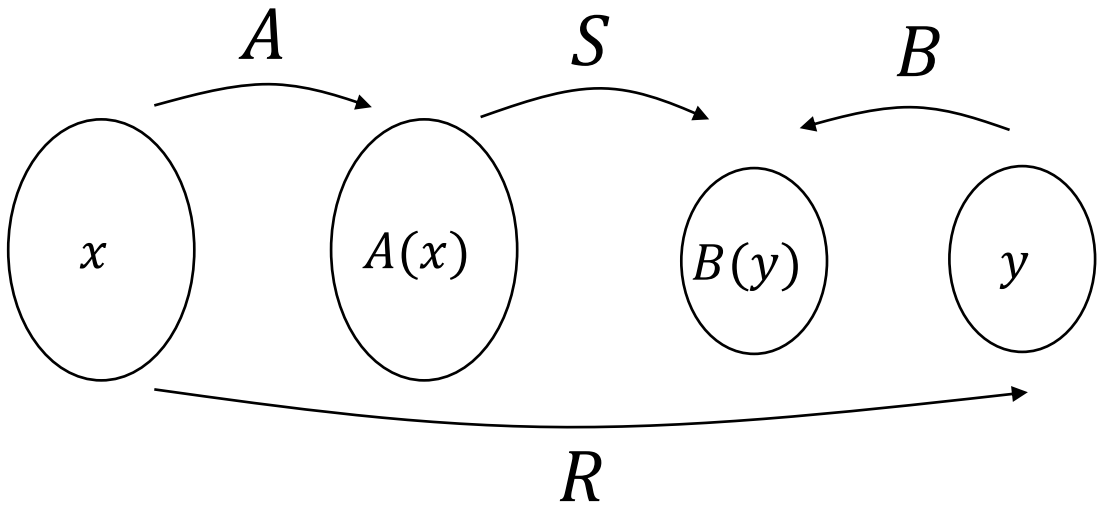
- Previously by Bozilov et al. [2]
- Create list of all ANFs with algebraic degree ≤ 2
- Use AE [1] to get representatives ($\approx 2^{23}$ times)
- Eliminate Doubles
- Result = 76 classes
- 16 threads, $\approx$ 3 hours runtime



[2] D. Bozilov, B. Bilgin, and H. A. Sahin. A Note on 5-bit Quadratic Permutations' Classification. IACR Transactions on Symmetric Cryptology, 2(1):398–404, 2017.

FIND REPRESENTATIVE FOR NON-BIJECTIVE

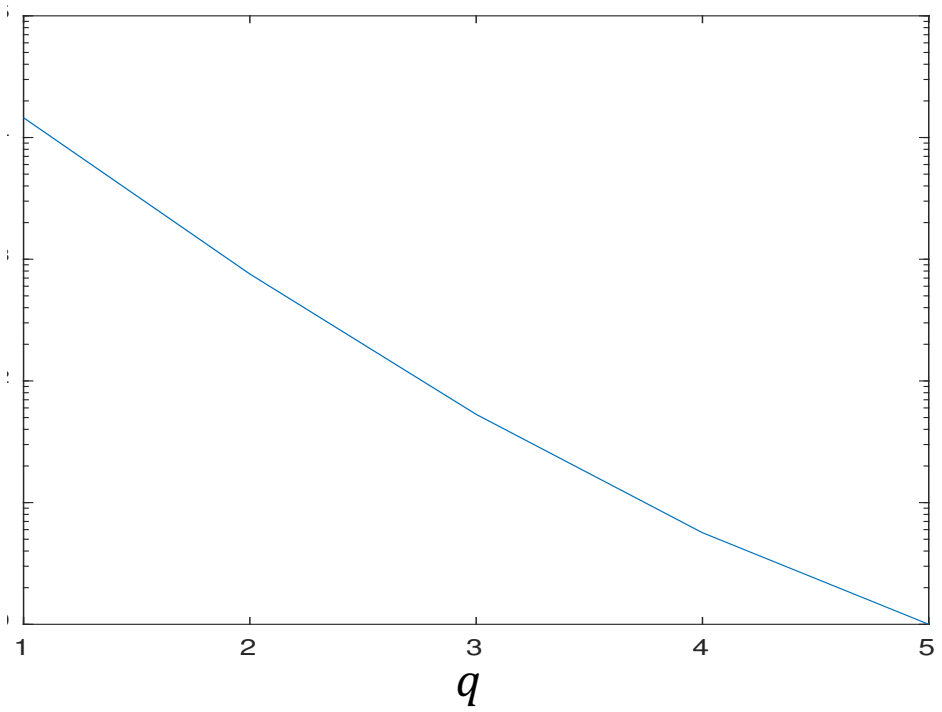
- When $S: \mathbb{F}_2^p \to \mathbb{F}_2^q$ with $q \leq p$ (but still balanced)
- Not invertible
- Backward: 2^{p-q} candidates for $S^{-1}\big(B(y)\big)$



COMPLEXITY

For Finding 1 Representative with this algorithm:

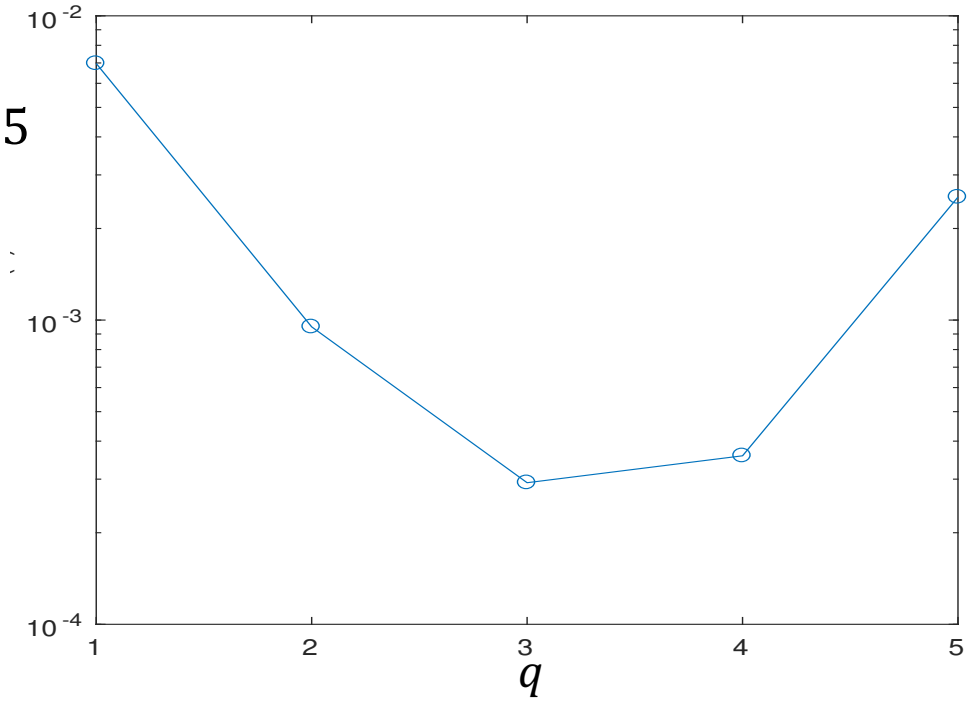
Asymptotically estimated in [1]:



$$p^3 \cdot 2^p \cdot (2^{p-q}!)^{\frac{p}{2^{p-q}}}$$

Our Average Experimental Runtime (s):

$p = 5$



x	**0**	1	**2**	3	**4**	5	6	7	8	9	A	B	C	D	**E**	F
$S(x)$	**1**	3	**1**	0	**1**	2	3	3	2	0	3	0	2	2	**1**	0

	$x \to A(x)$	$\overset{S}{\to}$	$B(y) \leftarrow y$
Guess	$0 \to 0$	$\to$	$1 \leftarrow 0$
Bckward	$1 \to 2$	$\to$	$1 \leftarrow 0$
Bckward	$2 \to 4$	$\to$	$1 \leftarrow 0$
Forward	$3 \to 6$	$\to$	$3 \leftarrow 1$
Bckward	$4 \to E$	$\leftarrow$	$1 \leftarrow 0$
Forward	$5 \to D$	$\to$	$2 \leftarrow 2$
Forward	$6 \to 8$	$\to$	$0 \leftarrow 3$
		…	

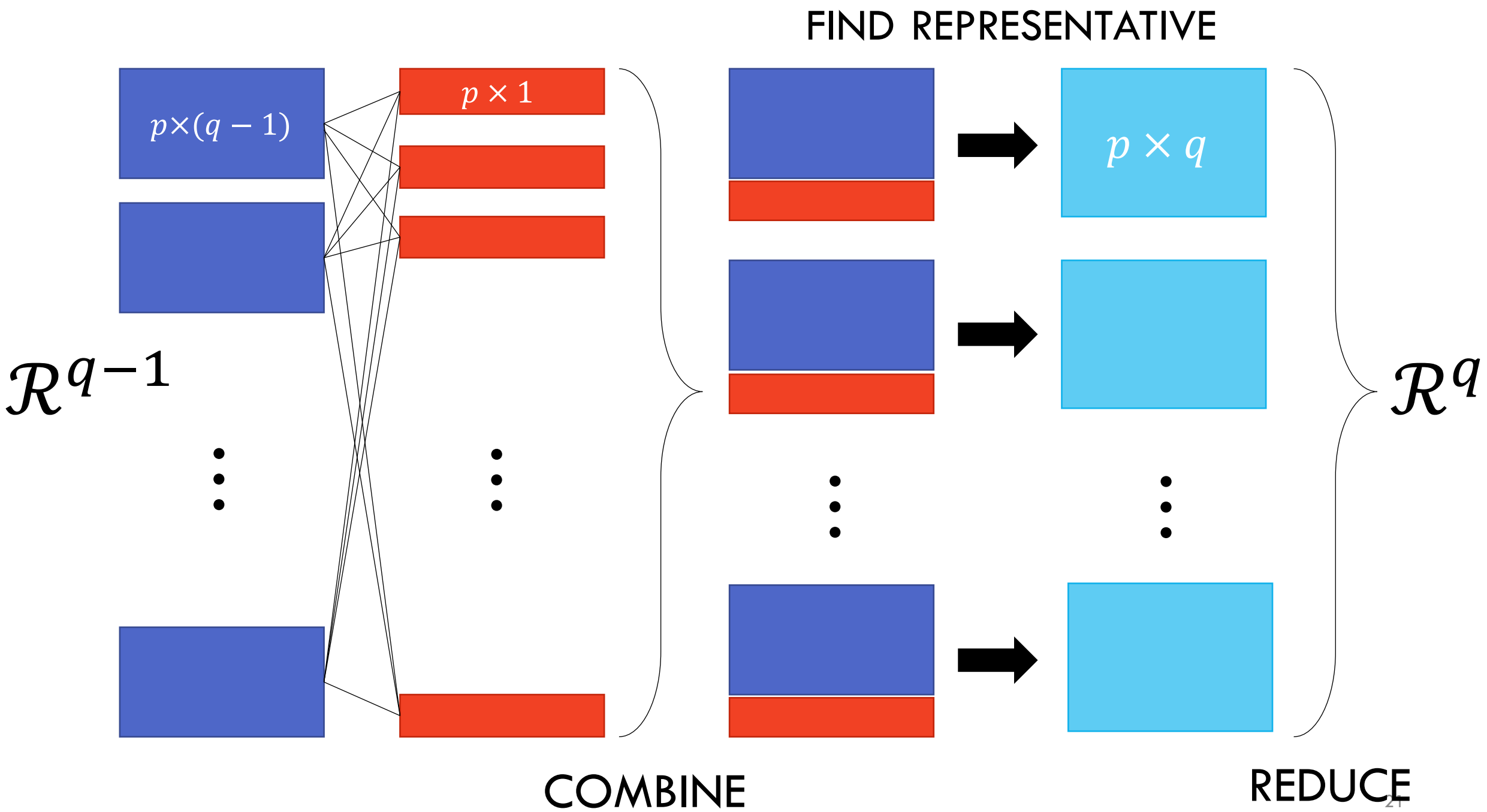
x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$R(x)$	0	0	0	1	0	2	3	…								

Classifying $n \times m$ Balanced Quadratic Functions

Iterative procedure to find all $p \times q$ representatives $\mathcal{R}^q$

- Given all balanced quadratic p-bit Boolean functions $\mathcal{F}$
- Given all $p \times (q-1)$ representatives $\mathcal{R}^{q-1}$

1 $\mathcal{R}^q \leftarrow \phi$
2 $\forall\, r \in \mathcal{R}^{q-1}, \forall\, f \in \mathcal{F}$:
3 Create $p \times q$ function $S(x) = (r(x) \ll 1) \mid f(x)$
4 Find affine eq. representative R
5 $\mathcal{R}^q \leftarrow \mathcal{R}^q \cup R$
6 Sort and eliminate doubles from $\mathcal{R}^q$

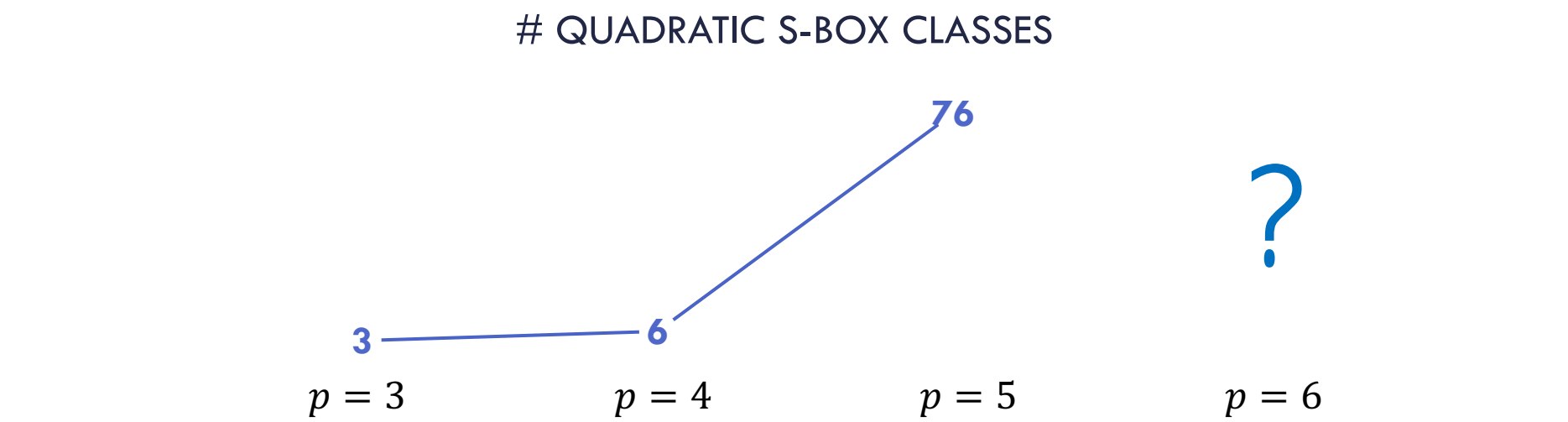

FIND REPRESENTATIVE
$p\times(q-1)$
$p\times 1$
$\mathcal{R}^{q-1}$
$p\times q$
$\mathcal{R}^{q}$
COMBINE
REDUCE

$5 \times q$ Balanced Quadratic Functions

5×1	5×2	5×3	5×4	5×5
3	12	80	166	76

Naïve search: On 4 threads in 50 minutes runtime

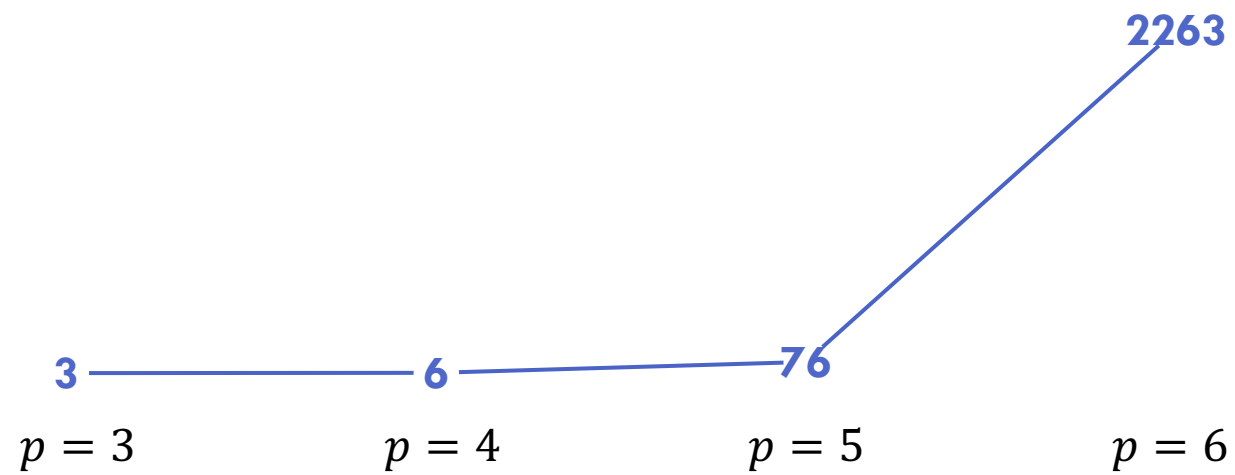
With Optimizations: On 4 threads in 6 minutes runtime



$6 \times q$ Balanced Quadratic Functions

6×1	6×2	6×3	6×4	6×5	6×6
3	24	670	11 891	12 647	2 263

Never been classified before



6 ×6 Quadratic S-boxes

- 2258 even vs. 5 odd
- 70 have quadratic inverses, 2193 have cubic inverses

	Lin = 8	**Lin = 16**	**Lin = 32**
Diff = 4	8	0	0
Diff = 8	0	0	12
Diff = 16	0	49	100
Diff = 32	0	49	1067
Diff = 64	0	200	779

Differentially 6-uniform $n \times n - 2$ functions?

- Open questions of C. Carlet [3]
- 3.10: unkown if for $n \geq 5$, $\exists$ differentially 6-uniform $n \times n - 2$ function?
- 6×4 with algebraic degree 2: no

	Lin = 8	**Lin = 16**	**Lin = 32**
Diff = 8	10	1	0
Diff = 16	1935	845	64
Diff = 32	618	5013	740
Diff = 64	42	2016	607

[3] C. Carlet. Open questions on nonlinearity and on APN functions. In Ç. K. Koç, S. Mesnager, and E. Savas, editors, Arithmetic of Finite Fields - 5th International Workshop, WAIFI 2014, Gebze, Turkey, September 27-28, 2014. Revised Selected Papers, volume 9061 of Lecture Notes in Computer Science, pages 83–107. Springer, 2014.

- Full listings of all $5 \times q$ and $6 \times q$ classes available on http://homes.esat.kuleuven.be/~ldemeyer/
- More details on ePrint Report 2018/113

S-box Decomposition

- Useful for side-channel protected implementations, MPC, …
- A higher-degree S-box H

$$H \sim R_1 \circ A \circ R_2$$

- Goal: Find $F = R_1 \circ A$ and R_2

S-box Decomposition

- Guess R_2 and find F such that $F \circ R_2 \sim H$
- Iteratively (same algorithm!)
  - $\mathcal{F}$ = all quadratic Boolean functions f such that $f \circ R_2$ can be a component of H
  - $\mathcal{R}^q$ = all $p \times q$ representatives r such that $r \circ R_2$ can be a subfunction of H

1 $\mathcal{R}^q \leftarrow \phi$
2 $\forall\, r \in \mathcal{R}^{q-1}, \forall\, f \in \mathcal{F}$:
3 Create $p \times q$ function $S(x) = (r(x) \ll 1) \mid f(x)$
4 Find left affine eq. representative R
5 $\mathcal{R}^q \leftarrow \mathcal{R}^q \cup R$
6 Sort and eliminate doubles from $\mathcal{R}^q$

S-box Decomposition

- Result = compositions with same properties as H (if exists)
- Decompositions:
  - 5-bit cubic AB permutations
  - Inverse of Keccak (SHA-3) nonlinear map χ
- Compositions: "Golden" 5-bit S-boxes:
  - Algebraic Degree 4
  - Diff = 2(APN), 4
  - Lin = 6
  - Quadratic Decomposition length 2

THANK YOU!