Permutations with special properties

Claude Gravel

Tutte Institute for Mathematics and Computing

Friday, September 29th, 2017

Finite Fields Day @ Carleton

Notation

1. $Q(X) \in \mathbb{Z}_2[X]$
2. $n = \deg(Q(X))$ (n is odd during all this presentation)
3. $a \in \mathbb{Z}_2^n$
4. $P_a(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} \in \mathbb{Z}_2[X]/(Q(X)) \cong \mathbb{F}_{2^n}$

Powers and boolean functions

For $a \in \mathbb{Z}_2^n$, and $t \in \mathbb{Z}_{2^n-1}$, φ_j's are the boolean functions s.t.

$$\begin{aligned} P_a(X) \mapsto \left(P_a(X)\right)^t & \mod Q(X) \\ \equiv \left(\sum_{j=0}^{n-1} a_j X^j\right)^t & \mod Q(X) \\ \equiv \sum_{j=0}^{n-1} \varphi_j(a) X^j & \mod Q(X). \end{aligned}$$

In vector space notation:

$$\begin{aligned} a &\mapsto (\varphi_0(a), \ldots, \varphi_{n-1}(a)) \\ &\stackrel{\text{def}}{=} \sigma(a) \text{ and } \sigma \in S_{2^n}. \end{aligned}$$

Each φ_j is a sum of products of the form $a_{i_1} \cdots a_{i_j}$. There are no more than 2^n such products.

Irreducible polynomials

For $n \in \mathbb{N}$, the number of irreducible polynomials of degree n is

$$\frac{1}{n} \sum_{d|n} 2^d \mu\Big(\frac{n}{d}\Big).$$

Let Q_1 and Q_2 be two irreducible polynomials. For a given $t \in \mathbb{Z}_{2^n-1}$, there is at least one a such that

$$\big(P_a(X)\big)^t \bmod Q_1(X) \not\equiv \big(P_a(X)\big)^t \bmod Q_2(X).$$

Q_1 and Q_2 lead to two different permutations σ_1 and σ_2.

List of some interesting properties

Given an irreducible polynomial Q, we consider

$$\sigma(a) = (\varphi_0(a), \ldots, \varphi_{n-1}(a)).$$

Some properties of interest (not an exhaustive list) are:

1. The algebraic degrees w.r.t. a of the boolean functions φ_j.
2. The cycle structure of σ.
3. The (average) number of products in the φ_j's.

Example I

Take an $n \in \mathbb{N}$, and $t = 2^n - 2$. Given an irreducible polynomial Q of degree n, we have

$$\left(P_a(X)\right)^{2^n-2} \equiv \left(P_a(X)\right)^{-1} \equiv \sum_{j=0}^{n-1} \varphi_j(a) X^j \mod Q(X).$$

The permutation has two fixed points and only cycles of length 2.

The algebraic degree of the outputs is $n - 1$.

The average number of products in φ_j is (empirically) about 2^{n-1}.

Example II

As before, take $n \in \mathbb{N}$, and any $t = -2^k \bmod (2^n - 1)$ with $k = 0, \ldots, n-1$.

The algebraic degree of the outputs $n - 1$.

There is a cycle with length larger than 2 if $k \neq 0$, and there are two fixed points.

The average number of products in φ_j is (empirically) about 2^{n-1}.

About the algebraic degree

The algebraic degree of the output boolean functions have been well-studied.

For a given $n \in \mathbb{N}$, it is shown that the powers that produce maximal degree output boolean functions are of the form $2^n - 2^k - 1 \equiv -2^k \bmod (2^n - 1)$ for $k \in \{0, \ldots, n-1\}$.

About the period

We recall that for $a \in \mathbb{Z}_2^n$ and for some $t \in \mathbb{Z}_{2^n-1}$,

$$P_a(X) \mapsto \left(P_a(X)\right)^t \equiv \sum_{j=0}^{n-1} \varphi_j(a) X^j \mod Q(X).$$

Under the t^{th}-power map, the period is the minimal value of k such that

$$P_a(X) \mapsto \left(P_a(X)\right)^t \mapsto \left(P_a(X)\right)^{t^2} \ldots \mapsto \left(P_a(X)\right)^{t^k} = P_a(X).$$

For $t = 2^n - 2$, the permutation has period 2 since

$$(2^n - 2)^2 \equiv (-1)^2 \equiv 1 \mod (2^n - 1).$$

For $t = -2^k$ and $1 < k < n$, the period is $2n$ since

$$(-2^k)^{2n} \equiv 2^{2kn \bmod n} \mod (2^n - 1) \equiv 1 \mod (2^n - 1).$$

Some remarks about previous slides

It seems impossible to get the algebraic degree right, i.e., all output bits with degree $n-1$, and a long cycle.

To keep the algebraic degree alive, combine maps with powers of the form -2^k for $k=0,\ldots,n-1$.

Taking consecutive powers (the order does not matter actually)

$$-2^0 \to -2^1 \to \ldots \to -2^{n-1}$$

does not increase the lenght of the cycles since

$$\prod_{j=0}^{n-1} -2^j \equiv (-1)^n 2^{n(n-1)/2} \equiv -1 \mod (2^n-1).$$

Idea

Idea: Perturb the input at every step, shift by a power of two, and invert.

Choose $b \in \mathbb{Z}_2^n \quad (b \neq 0)$ and let $a^{(j)} \in \mathbb{Z}_2^n$ be the sequence defined by

$$\begin{aligned} P_{a^{(0)}}(X) &= P_a(X) \\ P_{a^{(j)}}(X) &= \left(P_{a^{(j-1)}}(X) + P_b(X)\right)^{-2^{j-1}} \text{ for } j = 1, \ldots, n, \end{aligned}$$

with input $a \in \mathbb{Z}_2^n$, and output $a^{(n)} \in \mathbb{Z}_2^n$.

Note: For a given $b \in \mathbb{Z}_{2^n} \quad (b \neq 0)$, not all irreducible polynomials of degree n lead to the desired permutations.

Remarks and intuition for the construction

Note: Easy to implement, i.e., perturbation (bit flips), and powers of $2^n - 1 - 2^k$ for $k = 0, \dots, n-1$.

Note: If the block length is increased by 1 from n to $n+1$ bits, then one more round is added. The number of rounds is logarithmic and hence bits are well "shook". There are exactly $n = \log_2(2^n)$ powers of the form 2^k.

Note: Analogy with continued fractions over finite field, but it is the power that changes.

A counting (empirical) experiment

Let $\mathcal{I}_n \subset \mathbb{Z}_2[X]$ be the set of irreducible polynomials.
Let $\mathcal{J}_n \subset \mathcal{I}_n$ be the set of irreducible polynomial which lead to the desired permutations such that the perturbation polynomial is $P(X) = X^{n-1} + 1$. (In the following table, $\mathcal{P}_n \subset \mathcal{I}_n$ is the set of primitive and irreducible polynomials.

n	$\|\mathcal{J}_n\|$	$\|\mathcal{I}_n\|$	$\|\mathcal{J}_n\|/\|\mathcal{I}_n\|$	$\|\mathcal{P}_n\|$
3	1	2	0.5	2
5	2	6	0.333333	6
7	6	18	0.333333	18
9	10	56	0.178571	48
11	30	186	0.16129	176
13	87	630	0.138095	630
15	259	2182	0.118698	1800
17	1130	7710	0.146563	7710
19	3805	27594	0.137892	27594

Illustrated rounds - Example I

	0	1	2
0	2	6	4
1	7	7	3
2	4	1	5
3	3	5	0
4	1	3	7
5	0	4	1
6	6	2	2
7	5	0	6

$$P(X) = X^2 + 1, Q(X) = 1 + X + X^3$$

ILLUSTRATED ROUNDS - EXAMPLE II

	0	1	2	3	4
0	12	13	9	16	1
1	7	18	12	11	30
2	5	11	17	0	19
3	29	8	18	14	21
4	9	2	8	13	2
5	15	26	29	3	22
6	2	17	0	26	20
7	27	3	20	10	25
8	11	5	27	17	0
9	31	30	22	2	3
10	22	9	4	4	16
11	3	6	16	1	28
12	18	19	7	15	14
13	4	31	3	25	12
14	24	24	23	27	8
15	10	29	30	29	5
16	1	21	21	24	7
17	0	14	28	22	4
18	26	22	31	5	13
19	23	15	19	21	23
20	19	28	25	19	24
21	28	20	14	7	11
22	16	1	24	28	29
23	13	16	1	23	18
24	21	7	13	31	17
25	14	23	11	8	15
26	25	10	6	9	9
27	30	25	26	6	31
28	6	4	2	30	6
29	17	0	10	20	26
30	20	12	15	12	27
31	8	27	5	18	10

$$P(X) = X^4 + 1, Q(X) = 1 + X + X^2 + X^3 + X^5$$

Illustrated rounds - Example III

	0	1	2	3	4
0	7	5	28	6	13
1	10	17	0	22	5
2	4	25	23	28	20
3	26	20	21	12	24
4	14	28	26	23	18
5	8	22	25	26	26
6	28	23	13	20	22
7	3	6	11	13	31
8	30	12	16	1	19
9	12	4	3	31	7
10	5	13	6	8	21
11	18	27	24	4	17
12	2	16	1	29	15
13	23	8	27	2	2
14	13	26	31	27	4
15	25	31	22	3	23
16	1	9	19	9	9
17	0	21	9	10	3
18	22	14	18	21	29
19	29	2	15	17	0
20	27	15	5	18	30
21	19	19	10	25	6
22	17	0	30	19	12
23	11	11	8	7	25
24	15	3	20	30	10
25	20	7	17	0	27
26	6	18	7	14	8
27	16	1	12	15	14
28	31	30	29	16	1
29	24	24	2	24	16
30	9	29	4	5	11
31	21	10	14	11	28

$$P(X) = X^4 + 1, Q(X) = 1 + X + X^3 + X^4 + X^5$$

Counterexample (even degree)

	0	1	2	3	4	5
0	10	38	39	23	19	39
1	13	5	29	53	34	48
2	46	13	17	17	63	30
3	38	40	53	43	27	36
4	48	24	12	14	50	10
5	18	43	59	36	48	55
6	47	10	6	39	43	14
7	34	55	46	2	6	21
8	43	19	47	45	57	17
9	21	53	23	33	0	25
10	41	60	62	31	29	8
11	20	9	50	56	28	60
12	59	62	30	44	26	49
13	3	6	40	61	49	29
14	39	42	3	46	4	11
15	35	29	8	42	17	12
16	19	21	61	10	46	16
17	37	26	56	59	2	20
18	23	27	16	27	13	37
19	7	22	63	30	55	38
20	60	16	28	9	39	34
21	8	34	57	3	51	13
22	5	58	10	20	9	7
23	28	52	7	35	32	1
24	17	3	20	60	36	44
25	27	4	55	51	62	31
26	45	48	11	41	60	2
27	2	51	4	57	5	32
28	9	47	49	18	42	63
29	53	35	26	25	59	4
30	24	63	31	58	45	24
31	15	23	14	47	54	46

	0	1	2	3	4	5
32	1	36	24	37	18	35
33	0	49	32	1	16	33
34	44	18	34	24	3	41
35	58	25	33	0	56	27
36	55	20	52	21	53	22
37	29	61	25	19	40	53
38	50	45	44	29	61	45
39	22	17	5	26	10	51
40	61	56	19	50	25	28
41	52	39	35	15	22	3
42	12	28	60	13	12	19
43	33	0	45	55	41	9
44	32	1	2	38	21	61
45	11	46	36	11	38	47
46	62	31	18	22	37	58
47	25	14	21	8	35	18
48	57	12	27	62	30	57
49	26	54	38	7	23	59
50	49	15	43	28	52	50
51	36	57	37	32	1	62
52	40	8	22	12	33	0
53	42	37	15	34	11	6
54	51	2	41	52	47	56
55	6	50	54	6	7	43
56	14	7	42	5	15	42
57	63	30	48	48	44	15
58	56	33	0	54	20	52
59	16	59	13	63	31	26
60	4	44	58	49	58	54
61	54	41	9	40	8	23
62	30	11	51	16	14	40
63	31	32	1	4	24	5

$P(X) = X^5 + 1, Q(X) = 1 + X + X^4 + X^5 + X^6$

Profile matrix and differentials

For each of the 259 cases found for $n = 15$ (among 2182 irreducible polynomials) with $P(X) = X^{14} + 1$, the largest entries worth $\frac{6}{2^{15}}$ (about 60 out of 2^{30} entries for each case).

Recall that if P denotes the profiles matrix, the (a, b)-entry of P is given by

$$\frac{1}{2^n} \sum_{x \in \mathbb{Z}_2^n} \mathbb{1}\{F(x \oplus a) \oplus F(x) = b\},$$

where F is a permutation over $\{0,1\}^n$, a is an input approximator to x, and b is an output approximator to $F(x)$ for a given input $x \in \{0,1\}^n$.

See text file for results.

Goals

Goal: Clarifying the relation between the choice perturbation and irreducible polynomials.

Goal: Characterizing the set $\mathcal{J}_n$ for a given $P(X) \in \mathbb{Z}_2[X]$ with $1 \leq \deg P \leq n-1$. Have an algorithm to construct it, and then from which we could sample randomly.

Goal: The more important perhaps would be to show at least that

$$\lim_{n\to\infty} \frac{|\mathcal{J}_n|}{|\mathcal{I}_n|} \neq 0.$$

We recall that

$$|\mathcal{I}_n| = \frac{1}{n}\sum_{d|n} 2^d \mu(n/d) \in O\left(\frac{2^n}{n}\right).$$

Also the number of primitive irreducible polynomial is given by

$$|\mathcal{P}_n| = \frac{1}{n}\phi\big(2^n - 1\big).$$

ACKNOWLEDGEMENT

Special thanks to David Thomson, Daniel Panario and Steven Wang for the invitation. Thanks to Gilles Brassard, and Luc Devroye for the discussions we had during my phd period.

Bibliography I

[1] C. Carlet, Boolean functions for cryptography and error correcting codes. Technical report, Universités Paris 8 and Paris 13, CNRS

[2] C. Carlet, Vectorial boolean functions for cryptography. Technical report, Universités Paris 8 and Paris 13, CNRS

[3] P. Flajolet, and A. M. Odlyzko, Random mapping statistics. *Advances In Cryptography*, pages 329-354. Springer Verlag, 1990.

[4] P. Flajolet, and R. Sedgewick, *Analytic Combinatorics.* Cambridge University Press. 2009.

[5] R. Lidl, and H. Niederreiter, *Finite Fields*, Number v.20 pt. 1, in EBL-Schweitzer. Cambridge University Press, 1997.

[6] G. L. Mullen, and D. Panario, *Handbook of Finite Fields*. Chapman & Hall/CRC, 1st edition, 2013.