Boolean Functions and Applications (BFA) 2023, Voss, Norway

A new method to represent the inverse map as a composition of quadratics in a binary finite field

Pante Stănică

Department of Applied Mathematics
Naval Postgraduate School
Monterey, CA 93943, USA; pstanica@nps.edu

Joint work with my friends and co-authors:

Florian Luca

Santanu Sarkar

Problem background I

- In **1953**, Carlitz: all permutation polynomials over $\mathbb{F}_q$, $q > 2$ power of a prime, are generated by the special permutation polynomials

$$x^{q-2} \text{ (inversion) and } ax + b \text{ (affine) } a, b \in \mathbb{F}_q.$$

- What is the reason?
- Any permutation is a product of transpositions, so it is sufficient to show (by shifting) that a transposition $(0, \alpha \neq 0)$ can be generated by such a composition:

$$g_\alpha(x) = -\alpha^2 \left(\left((x - \alpha)^{q-2} + \frac{1}{\alpha} \right)^{q-2} - \alpha \right)^{q-2}.$$

Note: $g_\alpha(0) = \alpha, g_\alpha(\alpha) = 0, g_\alpha(\beta) = \beta$, for $\beta \in \mathbb{F}_q \setminus \{0, \alpha\}$.

Problem background II

- Carlitz rank: the smallest number of inversions in such a decomposition;
- *Can the inverse in $\mathbb{F}_{2^n}$ be written as a composition of quadratics, or quadratics and cubics PP?*
- Equiv., we ask if $\exists$ integers $a_1 \geq 0, \ldots, a_r \geq 0, r \geq 1$ s.t.

$$-1 \equiv \prod_{i=1}^{r} (2^{a_i} + 1) \pmod{2^n - 1}.$$

- In **2019**, Nikova, Nikov, Rijmen proposed an algorithm to find such a decomposition, and showed that for $n \leq 16$ any permutation can be decomposed in quadratic PP, when $4 \not| n$ and in cubic PP, when $4 | n$.

Problem background III

- In **2023**, Petrides improved the complexity of the algorithm and gave a computational table of shortest decompositions for $n \leq 32$, allowing also cubic permutations in addition to quadratics.
- He also proved a theoretical result (mentioned later) to find precisely such a decomposition for some special (good) integers.
- Here, we propose a number theoretical approach which allows us to cover all (surely, odd) exponents up to 250 (and beyond).

A theoretical result I

- Let ν_2 be the 2-valuation;
- Petrides (**2023**): if n is odd, some k, and $\frac{n-1}{2^{\nu_2(n-1)}} \equiv 2^k \pmod{2^n-1}$ (Moree (**1997**) calls them good (bad) integers, if they satisfy (do not satisfy) the congr.), then

$$2^n - 2 = 2\left(2^{\frac{n-1}{2^{\nu_2(n-1)}}} - 1\right) \prod_{j=1}^{\nu_2(n-1)} \left(2^{\frac{n-1}{2^j}} + 1\right)$$

$$\equiv 2\left(2^{2^k} - 1\right) \prod_{j=1}^{\nu_2(n-1)} \left(2^{\frac{n-1}{2^j}} + 1\right) = 2\prod_{j=0}^{k-1}\left(2^{2^j} + 1\right) \prod_{j=1}^{\nu_2(n-1)} \left(2^{\frac{n-1}{2^j}} + 1\right)$$

- Thus, for all good integers, one can decompose any permutation polynomial in $\mathbb{F}_{2^n}$ into affine and quadratic power permutations;

A theoretical result II

- Example of **bad** integer: $n = 7$, but $2^7 - 2 = 2(2^6 - 1) = 2(2+1)(2^4 + 2^2 + 1)$, and so, any permutation in F_{2^7} can be decomposed into affine, quadratic and cubic permutations;
- This observati on allows us to extend Petrides' result;

Theorem (Luca, Sarkar, P.S. **2023**)

Let n be an odd integer satisfying

$$\frac{n-1}{2^{\nu_2(n-1)}} \equiv 2^k 3^s \pmod{2^n - 1},$$

for some non-negative integers r, s. Then, the inverse power permutation in $\mathbb{F}_{2^n}$ has a decomposition into affine, quadratic and cubic power permutations of length $k + s + \nu_2(n-1)$.

A theoretical result III

- Let $\mathcal{B}(x)$ be the counting function of such $n \le x$;

Theorem (Luca, P.S. 2023)

We have

$$\#\mathcal{B}(x) \ll \frac{x}{(\log\log x)^{1+o(1)}}, \text{ as } x \to \infty.$$

- In fact, a more general result happens: replace the primes $2, 3$ by an arbitrary set of primes (S-unit), and a similar result will hold ([Luca, P.S. **2023**]).

Our idea:

The equation

$$-1 = \prod_{i=1}^{k} (2^{a_i} + 1)^{x_i} \pmod{2^p - 1}.$$

holds iff it holds one prime q_j at a time, where q_j is a prime divisor of the squarefree $2^p - 1$.

Heuristics I

- Let $N_p = 2^p - 1$, p prime. We know that if a prime $q | N_p$, then $q \equiv 1 \pmod{p}$;
- Can we say anything about the number of distinct prime factors $\omega(N_p)$ of N_p?

Conjecture (Luca, Sarkar, P.S. 2023)

There exists p_0 such that for $p > p_0$, $\omega(N_p) < 1.36 \log p$.

- Similar types of heuristics regarding lower bounds for $\Omega(2^n - 1)$ and $\omega(2^n - 1)$ can be found in Luca, P.S. (**2005**) and Kontorovich, Lagarias (**2021**).
- Our conjecture is based on statistical arguments originating from sieve methods.

Heuristics II

- One could use Túran-Kubilius inequality:

$$\sum_{n\le x}(\omega(n) - \log\log x)^2 = O(x \log\log x),$$

so, if $\delta > 0$ is fixed, the set of $n \le x$ such that

$$\omega(n) \ge (1+\delta)\log\log x$$

is of counting function $O_\delta(x/\log\log x)$.

- We do better via sieves: Hall, Tenenbaum (***Divisors* 1988**) showed that for fixed $\delta > 0$, then

$$\#\{n \le x : \omega(n) \ge (1+\delta)\log\log x\} \ll_\delta \frac{x}{(\log x)^{Q(\delta)}},$$

where

$$Q(\delta) := (1+\delta)\log((1+\delta)/e) + 1.$$

Heuristics III

- We want to apply such heuristics to $N_p = 2^p - 1$. Recall that if $q \mid N_p$, then $2^p \equiv 1 \pmod q$. In particular,

$$\left(\frac{2}{q}\right) = 1, \quad \text{so} \quad q \equiv \pm 1 \pmod 8.$$

- The same proof as in Hall-Tenenbaum shows that

$$\# \{n \le x : q \mid n \Rightarrow q \equiv \pm 1 \pmod 8, \omega(n) \ge (1+\delta) \log\log x\}$$
$$\le \frac{x}{(\log x)^{Q_1(\delta)+o(1)}}, \text{ as } x \to \infty, \text{ where}$$
$$Q_1(\delta) := (1+\delta)\log((1+\delta)/(0.5e)) + 1.$$

Heuristics IV

- Taking $\delta = 0.36$, we get $Q_1(\delta) = 1.00086\ldots$ Thus, the probability that a number n having only prime factors congruent to $\pm 1 \pmod 8$ with $\omega(n) \geq 1.36 \log\log n$ is

$$O\left(\frac{1}{(\log n)^{1.00008}}\right)$$

- Applying this to N_p, we get

$$O\left(\frac{1}{(\log(2^p - 1))^{1.0008}}\right) \ll \frac{1}{p^{1.0008}},$$

and since $\sum_{p\geq 3} \frac{1}{p^{1.0008}}$ is convergent, we are led to believe that perhaps there are at most finitely many primes p s.t.

$$\omega(N_p) \geq 1.36 \log p.$$

Conjecture (Luca, Sarkar, P.S. 2023)

There exists p_0 such that if $p > p_0$, then N_p is squarefree.

- There's some heuristic evidence for the conjecture based upon some results of Murata, Pomerance from **2004**;
- So, assuming the previous two conjectures, let

$$N_p := q_1 \cdots q_k \text{ for some distinct primes } q_1, \ldots, q_k, k \leq 1.36 \log p.$$

- We take numbers of the form $2^a + 1$ with odd $a \in [5, p-2]$, and want to compute $\left(\frac{2^a+1}{2^p-1}\right)$.

- This was done by Rotkiewicz in **1983**: write the Euclidean algorithm with even quotients and signed odd remainders:

$$\begin{aligned} p &= (2k_1)a + \varepsilon_1 r_1, \quad \varepsilon_1 \in \{\pm 1\}, \quad 1 \le r_1 \le a-1 \\ a &= (2k_2)r_1 + \varepsilon_2 r_2, \quad \varepsilon_2 \in \{\pm 1\}, \quad 1 \le r_2 \le r_1 - 1, \\ \ldots &= \ldots \\ r_{\ell-2} &= (2k_\ell) r_{\ell-1} + \varepsilon_\ell r_\ell, \quad \varepsilon_\ell \in \{\pm 1\}, \quad r_\ell = 1, \end{aligned}$$

where $\ell := \ell(a,p)$ is minimal with $r_\ell = 1$.

- Then

$$\left(\frac{2^a+1}{2^p-1}\right) = \left(\frac{2^p-1}{2^a+1}\right) = \left(\frac{(2^a)^{2k_1}\cdot 2^{\varepsilon_1 r_1} - 1}{2^a+1}\right) = \cdots = (-1)^{\ell+1}$$

(the "$\cdots$" needs a bit of work)

- We select the set $\mathcal{A}(p)$ of odd $a \in [5, p-2]$ s.t. $\ell \equiv 0 \pmod 2$.
- We assume that there are a positive proportion of such, namely $\exists c_1 > 0$ s.t. for large p, there are $> c_1 p$ odd numbers $a \in [5, p-2]$ such that $\ell(a, p) \equiv 0 \pmod 2$. So, we have

$$\prod_{i=1}^{k} \left(\frac{2^a + 1}{q_i} \right) = -1 \quad \text{for} \quad a \in \mathcal{A}(p).$$

- We next assume that for such a, the values

$$\left(\left(\frac{2^a + 1}{q_i} \right), 1 \leq i \leq k \right) \tag{1}$$

are uniformly distributed among the vectors $\underbrace{(\pm 1, \ldots, \pm 1)}_{k \text{ times}}$.

- In the full paper we give an argument why that should be so.

- We fix $i \in \{1, \ldots, k\}$ and search for a_i such that

$$\left(\frac{2^{a_i}+1}{q_i}\right) = (-1)^{\delta_{ij}}, \qquad (2)$$

where δ_{ij} is the Kronecker symbol.

- That is, $2^{a_i}+1$ is a quadratic residue modulo q_j for all $j \neq i$ but it is not a quadratic residue modulo q_i.
- Do we expect to find it? Yes!
- The probability that $2^{a_i}+1$ verifies the Legendre conditions given by (2) is $1/2^k$;
- Note that since $\left(\frac{2^{a_i}+1}{N_p}\right) = -1$ we know that an odd number of the $p = p_j$'s satisfy that $\left(\frac{2^{a_i}+1}{p_j}\right) = 1$.

- So, if we assume that this is so for all possible a_i's, and that these events are independent, we get that the probability that this happens is

$$\ll \left(1 - \frac{1}{2^k}\right)^{c_1 p} < \left(1 - \frac{1}{p^{1.36 \log 2}}\right)^{c_1 p} < \left(1 - \frac{1}{p^{0.95}}\right)^{c_1 p} \ll \frac{1}{e^{c_1 p^{0.05}}}.$$

- Of course, this is for i fixed and now we sum up over i from 1 to k introducing another logarithmic factor in the above count, that is, $\sum_p \frac{\log p}{e^{c_1 p^{0.05}}}$, which converges, so we expect that the above event does not occur when $p > p_0$.

- Thus, we have the following conjecture.

Conjecture (Luca, Sarkar, P.S. 2023)

Assume the prior two conjectures. For $p > p_0$ write $2^p - 1 = q_1 \dots q_k$ with prime factors $q_1 < \cdots < q_k$ and $k < 1.36 \log p$. Then for each $i = 1, \dots, k$, there exists an odd $a_i \in [5, p-2]$ such that equalities (2) hold.

- The rest of the proof is unconditional. We show $\exists x_i$ s.t.

$$-1 = \prod_{i=1}^{k} (2^{a_i} + 1)^{x_i} \pmod{2^p - 1}. \qquad (3)$$

- Equation (3) holds iff it holds one prime q_j at a time.
- Write $q_i - 1 =: 2^{\alpha_i} R_i$ for $1 \le i \le k$, R_i odd.
- Let $R := \mathrm{lcm}[R_i : 1 \le i \le k]$ and $x_i = y_i R$ for $1 \le i \le k$. Let ρ_i be a primitive root modulo q_i.

- Write $2^{a_i}+1=\rho_j^{b_{ij}} \pmod{q_j}$. Conditions $\left(\frac{2^{a_i}+1}{q_i}\right)=(-1)^{\delta_{ij}}$ show that $b_{ij}\equiv\delta_{ij} \pmod 2$.
- Thus, we want

$$\rho_j^{(q_j-1)/2}\equiv\rho_j^{R\sum_{i=1}^{k} y_i b_{ij}} \pmod{q_j},$$

which holds (via Fermat Little Thm) provided that

$$\frac{(q_j-1)}{2}\equiv R\sum_{i=1}^{k} y_i b_{ij} \pmod{q_j-1}.$$

- This in turn is equivalent to

$$2^{\alpha_j-1}\equiv(R/R_j)\sum_{i=1}^{k} y_i b_{ij} \pmod{2^{\alpha_j}}.$$

- As R/R_j is odd, it is invertible mod 2^{α_j}, of inverse $(R/R_j)^*$.

- Next, 2^{α_j-1}(since $(R/R_j)^*$ odd) $\equiv 2^{\alpha_j-1}(R/R_j)^* \equiv \sum_{i=1}^{k} y_i b_{ij} \pmod{2^{\alpha_j}}$.
- This is a nondegenerate (the coefficient matrix $\mathcal{B} = (b_{ij})_{1\le i,j\le k}$ modulo 2 is the identity matrix) linear system of modular equations.
- This shows that $\exists$ an integer solution $y_1, \ldots, y_k$. To solve it, we can generate $b_{i,j} \pmod{2^{\alpha_j}}$ (for each i, j) as an integer in the interval $[0, 2^{\alpha_j} - 1]$.
- Then we solve the (nondegenerate) linear system $\sum_{i=1}^{k} y_i b_{ij} = 2^{\alpha_j-1} \quad \text{for} \quad j = 1, 2, \ldots, k$, with rational $(y_1, \ldots, y_k)$ (treating them as residue classes modulo 2^α, where $\alpha = \max\{\alpha_i : 1 \le i \le k\}$, by inverting the odd determinant mod 2^α).

- We have implemented and checked that our algorithm works for most primes (in fact, odd integers) up to 250. But there are a few primes like 47 for which there is no $a_j \in [5, p-2]$ such that $\left(\frac{2^{a_j}+1}{q_i}\right) = (-1)^{\delta_{ij}}$.
- In these cases, we use the following trick: we first take a_i and calculate
$$\left(\frac{2^{a_j}+1}{q_i}\right) = (-1)^{d_{i,j}}.$$
- Ideally, $d_{i,j}$ should be Kronecker symbols, but if they are not, we cannot be certain that the system is solvable because it may have an even determinant;
- However, we observed that in the case of failure, we can always get suitable a_i's such that the corresponding matrix has odd determinant, and is therefore invertible.

Table: Factorization of $2^n - 2 \pmod{2^n - 1}$ for odd $33 \le n \le 250$.

$n = 33$	$(2^5+1)^{599478} \cdot (2^{13}+1)^{299739} \cdot (2^{29}+1)^{1798434}$
$n = 35$	$\left((2+1)(2^{17}+1)\right)^{967995} \cdot (2^{29}+1)^{276570}$
$n = 37$	$(2^5+1)^{77039772} \cdot (2^{13}+1)^{19259943}$
$n = 39$	$\left((2^{11}+1)(2^{21}+1)\right)^{1592955}$
$n = 41$	$(2^9+1)^{20111512782} \cdot (2^{13}+1)^{3351918797}$
$n = 43$	$\left((2^5+1)(2^{17}+1)(2^{23}+1)\right)^{593211015}$
$n = 45$	$(2+1)^{407925} \cdot (2^{13}+1)^{349650} \cdot \left((2^{25}+1)(2^{33}+1)(2^{41}+1)\right)^{116550}$
$n = 47$	$(2^{11}+1)^{1927501725} \cdot (2^{37}+1)^{435242325} \cdot (2^{41}+1)^{1616614350}$
$n = 49$	$(2^9+1)^{34630287489} \cdot (2^{11}+1)^{3393768173922}$
$n = 51$	$(1+2^{29})^{150009615}$
$n = 53$	$(1+2^5)^{6512186850} \cdot (1+2^{15})^{3506562150} \cdot (1+2^{21})^{250468725}$
$n = 55$	$(1+2)^{6588945} \cdot (1+2^{11})^{5856840} \cdot (1+2^{17})^{732105}$ $\cdot (1+2^{25})^{1464210} \cdot (1+2^{33})^{10249470} \cdot (1+2^{47})^{732105}$
$n = 57$	$(1+2^5)^{396029391534} \cdot (1+2^{17})^{1188088174602} \cdot (1+2^{21})^{594044087301}$ $\cdot (1+2^{47})^{198014695767}$
$n = 59$	$(1+2^7)^{3663925098759300} \cdot (1+2^{13})^{305327091563275}$
$n = 61$	$(1+2^9)^{1152921504606846975}$
$n = 63$	$(1+2)^{42958503} \cdot (1+2^5)^{3735522} \cdot (1+2^{39})^{56032830} \cdot$ [illegible]

$n = 103$	$(1+2^5)^{82048582506870378495385411156} \cdot (1+2^9)^{20512145626717594623846352 89}$
$n = 105$	$(1+2^7)^{736412106675} \cdot (1+2^{29})^{6627708960075} \cdot (1+2^{37})^{1472824213350} \cdot$ $(1+2^{55})^{6627708960075} \cdot (1+2^{69})^{15464654240175} \cdot (1+2^{79})^{736412106675} \cdot$ $(1+2^{83})^{4418472640050} \cdot (1+2^{85})^{441847264005} \cdot (1+2^{87})^{13255417920150}$
$n = 107$	$(1+2^5)^{270432128048688938985963350480 21}$
$n = 109$	$(1+2^7)^{74430860831057049021512649980 6} \cdot$ $(1+2^{15})^{37215430415528524510756324990 3}$
$n = 111$	$(1+2^{17})^{207823379439547290711 6} \cdot (1+2^{31})^{742226355141240323970} \cdot$ $(1+2^{39})^{890671626169488388764} \cdot (1+2^{71})^{180254971962872650107} \cdot$ $(1+2^{87})^{519558448598868226779}$
$n = 113$	$(1+2^{15})^{829012262666074828461 90} \cdot (1+2^{25})^{138168710444345804743 65} \cdot$ $(1+2^{29})^{378544412176289876 01} \cdot (1+2^{75})^{138168710444345804743 65} \cdot$ $(1+2^{97})^{829012262666074828461 90}$
$n = 115$	$(1+2^{17})^{235886540414646215 25} \cdot (1+2^{23})^{165120578290252350675} \cdot$ $(1+2^{39})^{235886540414646215 25} \cdot (1+2^{45})^{235886540414646215 25} \cdot$ $(1+2^{75})^{188709232331716972200}$
$n = 117$	$(1+2^5)^{350280341971560} \cdot (1+2^{11})^{481635470210895} \cdot (1+2^{31})^{1225981196900460} \cdot$ $(1+2^{55})^{1269766239646905} \cdot (1+2^{71})^{1225981196900460} \cdot (1+2^{87})^{744345726689565} \cdot$ $(1+2^{93})^{1903697510715} \cdot (1+2^{111})^{1094626068661125} \cdot (1+2^{115})^{1182196154154015}$
$n = 119$	$(1+2^{21})^{121807344007626864485535} \cdot (1+2^{25})^{281093870786831225735 85} \cdot$ $(1+2^{51})^{663541951792519884357 0} \cdot (1+2^{81})^{596855985637371635979121 5} \cdot$ [illegible]

$n = 245$	$(1+2^{69})^{40453428127382698682998734514666380600919326069842116290964 5}\cdot$ $(1+2^{117})^{65247464721584997875804410507526420324063429144906639178975 0}\cdot$ $(1+2^{125})^{10961574073226279643135140965264438614442656096344315382067 80}\cdot$ $(1+2^{141})^{10570089284896769655880314502219280092498275521474875546993 95}\cdot$ $(1+2^{151})^{40453428127382698682998734514666380600919326069842116290964 5}\cdot$ $(1+2^{165})^{15789886462623569485944667342821393718423349853067406681311 95}\cdot$ $(1+2^{167})^{40453428127382698682998734514666380600919326069842116290964 5}$
$n = 247$	$(1+2)^{1340573573884413807045402862803334868907750358289097078156 45}\cdot$ $(1+2^{9})^{13078766574482085922394174271252047501539027885747288567380 0}\cdot$ $(1+2^{35})^{16348458218102607402992717839065059376923784857184110709225}\cdot$ $(1+2^{71})^{85011982734133558495562132763138308760003681257357375687970}\cdot$ $(1+2^{147})^{81742291090513037014963589195325296884618924285920553546125}\cdot$ $(1+2^{195})^{150405815606543988107533004119398546267698820686093818524 87}$
$n = 249$	$(1+2^{97})^{2925277021907294342301024913127710972839014826123103258639378 52070}\cdot$ $(1+2^{119})^{2047693915335106039610717439189397680987310378286172281047564 96449}\cdot$ $(1+2^{137})^{5850554043814588684602049826255421945678029652246206517278757 04140}\cdot$ $(1+2^{173})^{6338100214132471074985553978443373774484532123266723727051986 79485}\cdot$ $(1+2^{199})^{5363007873496706294218545674067470116871527181225689307505527 28795}$

Thank you for your attention!

[Pante Stanica: http://faculty.nps.edu/pstanica]