Binomials that do not produce permutations

Dylan Cruz, Andrés Ramos, Ivelisse Rubio (Advisor)

Department of Computer Science
University of Puerto Rico, Río Piedras

Abstract

Permutations have important applications in fields such as coding theory and cryptography. We study binomials of the form $x^m(x^{\frac{q-3}{2}} + B)$ over finite fields $\mathbb{F}_q$. In this research we prove that this class of binomials never permutes a finite fields when: (a) $A = \alpha^k$, where k is odd and α is a primitive root of the field, (b) $A = \alpha^k$, where k is even, α is a primitive root of the field and $q = 4h+1$, $h \in \mathbb{N}$. We are left with the case $A = \alpha^k$ where k is even and $q = 4h + 3$, $h \in \mathbb{N}$. We conjecture that the remaining class of polynomials do not permute $\mathbb{F}_q$.

Preliminaries

Definition. A **finite field** is an algebraic strucure that consists of a finite set A with the operations $+, *$ that satisfy the following axioms:

- A is an abelian group under $+$.
- $A^* = A/\{0\}$ is an abelian group under $*$.
- $*$ distributes over $+$.

Every finite field has $q = p^r$ elements, where p is prime and it's denoted $\mathbb{F}_q$.

Definition. An element $\alpha \in \mathbb{F}_q$ is said to be a **primitive root** of $\mathbb{F}_q$ if α generates $\mathbb{F}_q^*$. This is, $\mathbb{F}_q^* = < \alpha > = \{\alpha^0, \alpha^1, \alpha^3, ..., \alpha^{q-2}\}$.

Definition. A **permutation** of a set A is a reordering of its elements. A function $f : A \to A$ defines a permutation of A if and only if it is a bijection.

Definition. A polynomial $p \in \mathbb{F}_q[x]$ is said to be a **permutation polynomial** of $\mathbb{F}_q$ if $p : \mathbb{F}_q \to \mathbb{F}_q$ defines a permutation.

Example.
Let $A = \mathbb{F}_7$ and $f : A \to A$, $f(x) = x^4 + 3x$
Then, f defines the permutation $0, 4, 1, 6, 2, 3, 5$ of A.

Theorem 1 ([4]) *Let $f(x) = x^m + ax^n$ over $\mathbb{F}_p$ with $m > n > 0$ and $a \in \mathbb{F}_p^*$. If $gcd(m - n, p - 1) \in \{2, 4\}$, then f does not permute $\mathbb{F}_p$.*

Theorem 2 ([2]) *(Hermite's Criterion) A polynomial $f \in \mathbb{F}_q[x]$ permutes $\mathbb{F}_q$ if and only if the following two conditions hold:*

- *f has exactly one root in $\mathbb{F}_q$.*
- *For each integer t with $1 \leq t \leq q - 2$ and $t \not\equiv 0$ (mod p), the reduction of $f(x)^t$ mod$(x^q - x)$ has degree $\leq q - 2$.*

Results

Theorem 3 *The binomial $x(x^{\frac{q-3}{2}} + B)$ is not a permutation polynomial of $\mathbb{F}_q$.*

Theorem 4 *The binomial $x^m(x^{\frac{q-3}{2}} + B)$ is not a permutation polynomial of $\mathbb{F}_p$*

Theorem 5 *The binomial $x^m(x^{\frac{q-3}{2}} + B)$ is not a permutation polynomial of $\mathbb{F}_q$, $q \neq 2^r$, if:*

- *$B = \alpha^k$, where k is an odd number.*
- *$B = \alpha^k$, where k is an even number and $q = 4h + 1$.*

Conjecture. The binomial $x^m(x^{\frac{q-3}{2}} + B)$ is not a permutation polynomial of $\mathbb{F}_q$

Summary

$x^m(x^{\frac{q-3}{2}} + B)$	$m = 1$	$m > 1$
$q = p$	Theorem 2 & Theorem 3	Theorem 4
$q = p^r$	Theorem 2	Theorem 5*

*This proof is still missing the case where $q = 4h + 3$ and $B = \alpha^k$ where k is odd.

Conclusion

In many cases permutation polynomials over finite fields have to be found by exhaustive searches. To reduce the search time it is useful to know which classes of polynomials do not permute the field. We conjecture that the binomials of the form $x^m(x^{\frac{q-3}{2}} + B)$ never permute $\mathbb{F}_q$, $q \neq 2^r$. Our future work consists of proving that the case $q = 4h + 3$ and $B = \alpha^k$ where k is odd never permutes $\mathbb{F}_q$ and finding other general families.

Acknowledgements

This research is supported by the Puerto Rico Louis Stokes Alliance for Minority Participation.

References

[1] David M. Burton , *Elementary Number Theory*, International series in pure and applied mathematics, McGraw-Hill Higher Education, 2007.

[2] Rudolf Lidl and Harald Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Applications. Cambridge University Press, 2nd edition, 1996

[3] L. González, *Involuciones de Cuerpos Finitos Obtenidas por Binomios, Manuscript*, UPR-RP, (2016)

[4] Ariane Masuda and Michael Zieve *Nonexistance of permutation binomials of a certain shape*, Electronic Journal of Combinatorics, 2007