Algebraic geometry and Boolean functions

Florian Caullery

Institut de Mathématiques de Marseille
Aix-Marseille Université

International Workshop on Boolean Functions and their Applications, Rosendal, September 2nd-7th 2014

Notations and basic recalls

- Let $q = 2^n$ and $\mathbb{F}_q$ be the finite field with q elements
- $f(x)$ will always denote a function $f : \mathbb{F}_q \mapsto \mathbb{F}_q$ and its associated polynomial
- The set $\mathbb{A}^n(\mathbb{F}_q) := \{(x_1, \ldots, x_n) | x_1, \ldots, x_n \in \mathbb{F}_q\}$ is the affine space of dimension n over $\mathbb{F}_q$
- Define the projective space of dimension n over $\mathbb{F}_q$ by $\mathbb{P}^n(\mathbb{F}_q) := \mathbb{A}^{n+1}(\mathbb{F}_q) - 0/\mathcal{R}$ where $\mathcal{R}$ is the equivalence relation on $\mathbb{A}^{n+1}(\mathbb{F}_q) - 0$

$$x\mathcal{R}y \leftrightarrow \exists \lambda \in \mathbb{F}_q, y = \lambda x$$

- For finite geometers : $\mathbb{P}^2(\mathbb{F}_q) \simeq PG(2, q)$

The Boolean functions we will study

To illustrate our approach, we will take two examples

- O-polynomials
- APN functions

O-polynomials

- A polynomial $f \in \mathbb{F}_q[x]$ of degree at most $q-1$ is an **o-polynomial** if
  1) $f(0) = 0$ and $f(1) = 1$,
  2) f induces a permutation of $\mathbb{F}_q$,
  3) $\begin{pmatrix} 1 & 1 & 1 \\ x & y & z \\ f(x) & f(y) & f(z) \end{pmatrix} \neq 0$ for all distinct $x, y, z \in \mathbb{F}_q$
- Called o-polynomial because they are in 1-1 correspondence with **hyperovals** of $\mathbb{P}^2(\mathbb{F}_q)$.
- An **exceptional** o-polynomial of $\mathbb{F}_q$ is a polynomial defining an o-polynomial **over infinitely many extensions of $\mathbb{F}_q$**.

INSTITUT de MATHÉMATIQUES de MARSEILLE

O-polynomials in term of algebraic geometry

If f is a o-polynomial of $\mathbb{F}_q$, the polynomial

$$\phi_f(x,y,z) = \frac{x(f(y)+f(z)) + y(f(x)+f(z)) + z(f(x)+f(y))}{(x+y)(y+z)(z+x)}$$

vanishes iff $x = y$, $y = z$ or $z = x$.

In terms of algebraic geometry :

If f is a o-polynomial of $\mathbb{F}_q$, the surface X_o in $\mathbb{A}^3(\mathbb{F}_q)$ defined by the equation

$$\phi_f(x,y,z) = 0$$

has all its $\mathbb{F}_q$-rational points on the planes of equation $x + y = 0$, $y + z = 0$ and $z + x = 0$.

s

APN functions

- A polynomial $f \in \mathbb{F}_q[x]$ of degree at most $q-1$ is **Almost Perfectly Nonlinear** if the equation

$$f(x+a)+f(x)=b$$

  has at most two solutions for every nonzero a and every b in $\mathbb{F}_q$.
- An **exceptional** APN polynomial of $\mathbb{F}_q$ is a polynomial which is APN **over infinitely many extensions of $\mathbb{F}_q$**.

APN property in terms of algebraic geometry

f is APN over $\mathbb{F}_q$ if there is no four distinct elements x, y, z and t of $\mathbb{F}_q$ such that

$$\begin{cases} x + y = a, & f(x) + f(y) = b \\ z + t = a & f(z) + f(t) = b \end{cases}$$

Equivalently, the polynomial

$$\phi_f(x, y, z) = \frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(y + z)(z + x)}$$

vanishes iff $x = y$, $y = z$ or $z = x$.

INSTITUT de MATHÉMATIQUES de MARSEILLE

APN property in terms of algebraic geometry

In terms of algebraic geometry :

f is APN over $\mathbb{F}_q$ iff the surface X_apn in $\mathbb{A}^3(\mathbb{F}_q)$ defined by the equation

$$\phi_f = 0$$

has all its $\mathbb{F}_q$-rational points on the planes of equation $x + y = 0$, $y + z = 0$ and $z + x = 0$.

INSTITUT de MATHÉMATIQUES de MARSEILLE

Why doing that - The strategy explained

- Compare the number of $\mathbb{F}_q$-rational points of X and the combination of the planes $x + y = 0$, $y + z = 0$ and $z + x = 0$.
- Discard from the list of potential APN or o-polynomials the polynomials defining a surface with too many points.
- Our main tool : **the Lang-Weil bound** on the number of $\mathbb{F}_q$-rational points of an **absolutely irreducible varieties**(i.e. curves and surfaces).
- But we need to go into the projective space to apply this result (and other useful ones).

Going into the projective space

- We have to work with **homogeneous polynomials**, i.e. polynomials whose nonzero terms all have the same degree :

$$\phi(\lambda x_1, \ldots, \lambda x_k) = \lambda^d \phi(x_1, \ldots, x_k)$$

- Two cases to distinguish :

1. f is a monomial
2. f is not a monomial

INSTITUT de MATHÉMATIQUES de MARSEILLE

The monomial case

- If $f(x) = x^d$, $\phi_{x^d}(x, y, z)$ is already homogenized.
- The equation $\phi_{x^d}(x, y, z) = \phi_d(x, y, z) = 0$ defines **a curve** in $\mathbb{P}^2(\mathbb{F}_q)$.

The Lang-Weil bound for curves

- Let C be an **absolutely irreducible** curve over $\mathbb{P}^2(\mathbb{F}_q)$ defined by a polynomial of degree d.
- Its number $\#C(\mathbb{F}_q)$ of $\mathbb{F}_q$ rational points satisfies

$$|\#C(\mathbb{F}_q) - q| < (d-1)(d-2)q^{1/2} + d^2,$$

(this is a slightly different version of the LW bound due to W. Schmidt).

- The intersection of the curve C and the lines $x + y = 0$, $y + z = 0$ and $z + x = 0$ has at most $3d - 2$ $\mathbb{F}_q$-rational points.
- C has $\mathbb{F}_q$-rational points not on the above lines for q sufficiently large.

The Lang-Weil bound for curves - 2

Theorem (Janwa-Wilson 1993 (APN), Hernando-McGuire 2010(O-polynomial))

If the curve C defined by $\phi_d = 0$ is absolutely irreducible or has an absolutely irreducible component defined over $\mathbb{F}_q$, x^d is ***not*** *an exceptional o-polynomial or APN of $\mathbb{F}_q$.*

INSTITUT de MATHÉMATIQUES de MARSEILLE

When is C absolutely irreducible ?

- If C is not irreducible, it is the combination of two curves C_1 and C_2 defined over $\bar{\mathbb{F}}_q$ respectively by $u(x,y,z)=0$ and $v(x,y,z)=0$.
- Bezout's theorem says

$$\sum_P I(P,u,v) = (\deg u)(\deg v)$$

- Call P a singular point of C if its **multiplicity** is greater than 1.
- Count the singular points of C and apply Bezout's theorem (actually the hard part).

Main results - APN

Theorem (Hernando-McGuire, 2009)

Let d be a positive integer. If d is not of the form $2^i + 1$ (Gold exponent) or $2^{2i} - 2^i + 1$ (Kasami exponent), then the curve defined by

$$\frac{x^d + y^d + z^d + (x + y + z)^d}{(x + y)(y + z)(z + x)}$$

has an absolutely irreducible factor defined over $\mathbb{F}_2$.

Corollary

The only exceptional APN monomial are Gold and Kasami.

Main results - O-polynomial

Theorem (Hernando-McGuire, 2010 ; Zieve 2013)

Let d be a positive integer different from 6 and not a power of 2. The curve defined by

$$\frac{x(y^d+z^d)+y(x^d+z^d)+z(x^d+y^d)}{(x+y)(y+z)(z+x)}$$

has an absolutely irreducible factor defined over $\mathbb{F}_2$.

Corollary

The only exceptional o-monomials are x^6 and x^{2^i}.

The polynomial case

- If $f(x)$ is not a monomial, introduce the homogenization variable w.
- Write $f(x) = \sum_{i=0}^{d} a_i x^i$. It is readily verified that

$$\phi_f(x, y, z) = \sum_{i=2}^{d} a_i \phi_i(x, y, z)$$

and so

$$\bar{\phi}_f(x, y, z, w) = \sum_{i=2}^{d} a_i \phi_i(x, y, z) w^{d-i}.$$

The Lang-Weil bound for surfaces

- Let $\bar{X}$ be an **absolutely irreducible** surface over $\mathbb{P}^3(\mathbb{F}_q)$ defined by a polynomial of degree d.
- Its number $\#\bar{X}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points satisfies

$$|\#\bar{X}(\mathbb{F}_q) - q^2 - q - 1| \leq (d-1)(d-2)q^{3/2} + 18(d+3)^4,$$

  (this is a refinement due to Ghorpade and Lachaud).
- The intersection of $\bar{X}$ with the planes $x + y = 0$, $y + z = 0$, $z + x = 0$ and the plane infinity has at most $4((d-3)q + 1)$ $\mathbb{F}_q$-rational points.
- $\bar{X}$ has $\mathbb{F}_q$-rational points not on the above planes for q sufficiently large.

The Lang-Weil bound for surfaces - 2

Theorem (Rodier, 2008 (APN) Caullery-Schmidt, 2014 (o-polynomial))

*If the surface $\bar{X}$ defined by $\phi_f = 0$ is absolutely irreducible or has an absolutely irreducible component defined over $\mathbb{F}_q$, f is **not** an exceptional o-polynomial or APN of $\mathbb{F}_q$.*

How to prove that $\bar{X}$ is absolutely irreducible

Theorem (Aubry-McGuire-Rodier, 2010)

Let S and P be projective surfaces in $\mathbb{P}^3(\mathbb{F}_q)$ defined over $\mathbb{F}_q$. If $S \cap P$ has a ***reduced*** *absolutely irreducible component defined over $\mathbb{F}_q$, then S has an absolutely irreducible component defined over $\mathbb{F}_q$.*

- Take H_∞ the plane infinity of $\mathbb{P}^3(\mathbb{F}_q)$ (i.e. the plane of equation $w = 0$).
- The equation of $\bar{X} \cap H_\infty$ is given by $\phi_d = 0$!
- We are back to the monomial case **with an extra condition**...
- We have to differentiate cases according to the degree of the f.

Example 1 : Exceptional APN polynomials

- If the degree d of f is odd, $\bar{X}$ has no repeated component (i.e. it is reduced).
- If d is not a Gold or a Kasami exponent $\bar{X} \cap H_\infty$ has a **reduced absolutely irreducible component** defined over $\mathbb{F}_2$.

Corollary

Let f be an exceptional APN polynomial of odd degree, then the degree of f is a Gold or a Kasami exponent.

- Still an open problem for degrees a Gold or Kasami exponent.

INSTITUT de MATHÉMATIQUES de MARSEILLE

Exceptional APN polynomials of even degree

- If the degree d of f is even, write $d = 2^l e$, e odd.
- It is readily verified that

$$\phi_d = ((x+y)(y+z)(z+x))^{2^l-1}\,\phi_e^{2^l}.$$

- The absolutely irreducible component of ϕ_e appears 2^l times in $\bar{X} \cap H_\infty$.

Theorem (Aubry-McGuire-Rodier, 2010)

There is no exceptional APN function of degree $2e$, e odd.

- The case $l \geq 2$ is much more intricate, only partial results exist for $l = 2$.
- The given method leads to overcomplicated computations.

Example 2 : O-polynomials

- An o-polynomial has only terms of even degree so d is even.
- Luckily, ϕ_d is always reduced !
- If d is not 6 or a power of 2, $\bar{X} \cap H_\infty$ has a **reduced absolutely irreducible component** defined over $\mathbb{F}_2$.

Corollary

If f is an exceptional o-polynomial, its degree is either 6 or a power of 2.

INSTITUT de MATHÉMATIQUES de MARSEILLE

Exceptional o-polynomials of degree 6 or a power of 2

Theorem (Hirschfeld, 1971)

If f is an o-polynomial of degree 6, f is either x^6 or $(x+1)^6$.

Theorem (Caullery-Schmidt, 2014)

If f is an o-polynomial of degree a power of 2, f is a linearised polynomial.

Theorem (Payne, 1971 ; Hirschfeld, 1975)

If f is a linearised o-polynomial, then it is of the form x^{2^k}.

Open problems for o-polynomials

Theorem

If f is an o-polynomial of degree less than $\frac{1}{2}q^{1/4}$, then f is either x^6, $(x+1)^6$ or x^{2^k}.

Open problem : what if the degree of f is greater than $\frac{1}{2}q^{1/4}$?

INSTITUT de MATHÉMATIQUES de MARSEILLE

Open problems

- Can we get a tighter bound than the Lang-Weil bound ?
- Can we get a bound which can be applied to not necessarily absolutely irreducible varieties ?
- Can we give a decomposition of ϕ_d for every d ? (This could help for polynomial case)

Informations

Florian Caullery
Institut de Mathematiques de Marseille
Aix Marseille Université
www.univ-amu.fr

Contact : fcaullery@gmail.com
@presquepartout http ://presquepartout.hypotheses.org

INSTITUT
de MATHÉMATIQUES
de MARSEILLE