On defining and verifying the Jacobian condition for Boolean maps in two variables

Virendra Sule
Department of EE
IIT Bombay
(vrs@ee.iitb.ac.in)

August 18, 2011

1 Introduction

The well known Jacobian problem [2] is defined for polynomial maps $F : \mathbb{C}^n \to \mathbb{C}^n$ described by n-tuples of polynomials $f_i, i = 1 \dots n$ in the polynomial ring $\mathbb{C}[X_1, \dots, X_n]$. Such an F is said to be invertible as a polynomial map (henceforth simply called *invertible*) if there is an n-tuple of polynomials g_i in $\mathbb{C}[X_1, \dots, X_n]$ such that

$$f_i(g_1, \dots, g_n)(X_1, \dots, X_n) = X_i$$

for $i = 1, \dots, n$. Compactly the above polynomial compositional relation can be written as

$$F \circ G = Id$$

The Jacobian of F is the matrix of formal partial derivatives

$$JF = [\partial_{X_i} f_j]$$

The Jacobian problem is unresolved for $n \geq 2$ stated as

Conjecture 1 (Jacobian conjecture (JC))**.** Let $n \geq 2$. Then the map F is invertible if

$$\det JF = c \neq 0$$

where c is a constant.

The condition above is known as Jacobian condition. The problem has remained unresolved for rational, real or the complex field. The questions we want to explore in this note are, how to define a finite field case of this problem, what computational problems arise when the complex field is replaced by a finite field and whether the problem of verifying Jacobian condition on finite fields is computationally fieasible. The idea of defining the Jacobian condition and stating an analogous problem over finite fields appeared in [1] which formed a motivation for this article. On closer examination it appeared that the problem of defining analogous JC on finite fields involved subtleties. In this article we proceed with defining the JC only on prime fields and analyze the computational feasibility of verifying the analogus conjecture on binary fields for only two variables.

One difference created due to such a change of field is that over the complex field the polynomial functions $f : \mathbb{C}^n \to \mathbb{C}$ correspond one to one with polynomials in the polynomial ring in n variables with co-efficients in $\mathbb{C}$ on the other hand if K is a prime field the polynomial ring $K[X_1, \ldots, X_n]$ is infinite while the ring of functions $f : K^n \to K$ is finite. For $K = \mathbb{F}_p$ this ring corresponds to $K[X_1, \ldots, X_n]/I$ where I is the ideal generated by $(X_i^p - X_i)$. By Lagrange interpolation every function $f : K \to K$ is equal to a polynomial function $f(x)$ of degree at most $p - 1$. We shall call $f(x)$ as a *representative* of f.

This raises the question, how do we define the partial derivatives of $\mathbb{F}_p$-valued functions with arguments in $\mathbb{F}_p$ and the Jacobian condition so that we can state an analogue of JC? One way of resolving this question is to define a notion of differential of the function by analogy with differential of a map in real variable calculus. We shall call this a formal differential of a function f. It turns out that a formal derivative of a polynomial representative of f also represents the formal differential of f.

2 Function in a prime field and its formal differential

Consider a prime field $\mathbb{F}_p$ and a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$. By interpolation, such a function is equal to a polynomial function with $\mathbb{F}_p$ co-efficients called a representative of f. Let this be denoted as $f(x_1, \ldots, x_n)$ where arguments x_i take values in $\mathbb{F}_p$. Clearly the highest power with which any of the arguments appear in $f(x_1, \ldots, x_n)$ is $p - 1$ since these satisfy the equation $x^p - x = 0$. We say that f has lowest degree d if f evaluates all monomials in x_i of degree $< d$ to zero while at least one degree d monomial has assignments of x_i in $\mathbb{F}_p$ such that f has nonzero value. It follows that a function has nonzero lowest degree d iff any polynomial representative of f has a nonzero co-efficient for at least one d degree term and all co-efficients of terms of degree $< d$ are zero.

Definition 1 (Formal differential and the Jacobian)**.** Let f be a function $f : \mathbb{F}_p \to \mathbb{F}_p$. The differential of f is the function $Df : \mathbb{F}_p \to \mathbb{F}_p$ such that for any y in $\mathbb{F}_p$, the function

$$f(x + y) - f(x) - Df(x)y = \theta(y^2)$$

where $\theta(y^2)$ is a function with lowest degree ≥ 2.

For a function of several variables $f(x_1, x_2, \ldots, x_n)$ (denoted as $f(x)$), the differential of f is the n-tuple of functions $Df_i : \mathbb{F}_p^n \to \mathbb{F}_p$ such that for any n-tuple y_i in $\mathbb{F}_p^n$,

$$f(x + y) - f(x) - \sum_i Df_i(x)y_i = \theta(y_i^2)$$

where $\theta(y_i^2)$ is a $\mathbb{F}_p$-valued function on $\mathbb{F}_p^n$ with lowest degree ≥ 2. The functions $Df_i(x)$ are called the i-th component of formal partial differentials of f (or i-th partial differential of f).

For a function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ let $f_i(x)$, $i = 1, 2, \ldots, n$ denote the component functions such that $F = [f_1, \ldots, f_n]$ for all values of the arguments. Then the Jacobian of F is the matrix function

$$JF(x) = [\phi_{(i,j)}(x)]$$

where $\phi_{(i,j)}(x)$ is the j-th partial differential of f_i.

From this definition it follows that if $f(x)$ is a polynomial function in $\mathbb{F}_p$ of the form

$$f(x) = \sum_{i=0}^{p-1} a_i x^i$$

then

$$Df(x) = a_1 + \sum_{i=2}^{p-1} a_i i x^{i-1} \mod p$$

Hence given $f : \mathbb{F}_p \to \mathbb{F}_p$ the formal differential Df exists. These computations can be carried out for functions of n variables. The composition of two functions $f, g : \mathbb{F}_p \to \mathbb{F}_p$ denoted $f \circ g = f(g(x))$ is well defined as a function in $\mathbb{F}_p$. In terms of polynomial representations the resulting composite function is a composition of the polynomials reduced modulo $x^p - x$ for the arguments while co-efficients are reduced modulo p. Since the formal differential Df of a polynomial $f(x_1, \ldots, x_n)$ satisfies the chain rule

$$Df(g(x)) = Df.Dg$$

if $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$, $G : \mathbb{F}_p^k \to \mathbb{F}_p^m$ are maps then we have

$$D(F \circ G \mod I) = DF.DG \mod I$$

where I is the ideal $(x_1 - x_1, x_2 - x_2, \ldots, x_n - x_n)$.

With the above definition of the Jacobian of a function we now restate an analogue of JC on prime fields as follows.

Conjecture 2 (JC on $\mathbb{F}_p$)**.** The function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is invertible if

$$\det JF = c \neq 0 \tag{1}$$

where c is a constant (in $\mathbb{F}_p$).

We call (1) the Jacobian condition on $\mathbb{F}_p$.

2.1 Single variable case of JC

First we explore whether this modified definition of a derivative has a chance of getting the JC to be true at least for $n = 1$. Let f be a function in $\mathbb{F}_p$. Then f can be represented by a polynomial function of degree at most $p - 1$. Let this be denoted

$$f(x) = a_0 + a_1 x + \ldots + a_{p-1} x^{p-1}$$

where a_i and x belong to $\mathbb{F}_p$. The formal differential of f is then represented by

$$Df(x) = a_1 + a_i i x^{i-1} \mod p$$

Hence the Jacobian condition $Df = c \neq 0$, forces co-efficients a_i to satisfy

$$a_1 \neq 0 \qquad a_i i \mod p = 0$$

for $i = 2, \ldots, (p-1)$. However this implies $a_i \mod p = 0$ since $i < p$. Hence all functions satisfying the Jacobian condition are affine with $a_1 \neq 0$. Consider the function g whose polynomial representative is

$$g(X) = -a_0 a_1^{-1} + a_1^{-1} X$$

which is also affine. Then it can be easily verified by composing the polynomial function $f(g(x))$ representing $f \circ g$ that

$$f(g(x)) = g(f(x)) = x$$

Hence g is the (unique) inverse of f. We have thus proved

Proposition 1. JC is true for $n = 1$ over prime fields.

Invertible polynomial functions in $\mathbb{F}_q$ are studied in [3] and are called "permutation polynomials". Necessary and sufficient conditions are known for such polynomials. However these conditions are purely algebraic equivalences of transformational properties of invertible polynomials and none of these appear to result in an analogous condition such as the Jacobian condition. The statement of the Jacobian condition on the other hand is a in terms of co-efficients of the polynomial. Such a statement is very important from the point of view of computational verifiability and complexity hence is of a different nature. The JC is also a generalized restatement of the Roll's theorem in real analysis. The studies relating to JC such as in [2] dont seem to have crossed paths or have anything common with the theory of permutation polynomials.

2.2 Computational problems

Apart from the theoretical problem of proving the JC in the prime field case, there is the computational problem of verifying the JC on finite fields as well as what is the complexity of computing the inverse function. We formally state these computational problems.

Problem 1 (Verifying JC)**.** Develop a computational algorithm to verify the JC over $\mathbb{F}_p^n$. Develop analysis of complexity of this problem as a function of p and n. Determine the complexity class of this problem. If this problem is in complexity class P we can say that verifying the JC is a feasible problem.

Problem 2 (Construction of invertible functions)**.** Give an algorithm to output a complete classification of invertible functions F and their inverses G. Develop an algorithm which will output all functions F which satisfy JC and their inverses G when the such exist. Analyze the complexities of these algorithms. If the former is in P we can consider the problem of constructing invertible functions to be solvable.

3 Defining JC over the ring of Boolean functions

Let B be the two element binary field (or the Boolean algebra). The Boolean functions $f : B^n \to B$ correspond to the ring $R = \mathbb{F}_2[X_1, \ldots, X_n]/I$ where $I = (X_1^2 \oplus X_1, \ldots, X_n^2 \oplus X_n)$. R is a Boolean ring (elements satisfy the equation $w^2 = w$) under the operation of addition modulo 2 (XOR) denoted $\oplus$, multiplication (AND) denoted by . and with 0 and

1 as respective identities. The composition of Boolean functions is obtained by composing polynomial representatives and reducing modulo I. For $n = 2$, ring R has only functions represented by $a_0 \oplus a_1X \oplus a_2Y \oplus XY$ where a_i are 0 or 1. The only constant function in R is the constant 1.

3.1 Case $n = 2$

We now show the verification of JC for the simplest case $n = 2$. The Boolean functions in this case have representatives $a_0 \oplus a_1X \oplus a_2Y \oplus a_3XY$. Let $F = [f_1, f_2]$ where

$$\begin{array}{rcl} f_1(X,Y) & = & a \oplus bX \oplus cY \oplus dXY \\ f_2(X,Y) & = & e \oplus fX \oplus gY \oplus hXY \end{array}$$

The Jacobian matrix is

$$JF = \left[\begin{array}{cc} b \oplus dY & c \oplus dX \\ f \oplus hY & g \oplus hX \end{array}\right]$$

Hence $\det JF = 1$ iff

$$\begin{array}{rcl} bg \oplus fc & = & 1 \\ bh \oplus fd & = & 0 \\ ch \oplus gd & = & 0 \end{array}$$

Solving these equations over B it turns out that only the following pair of functions are possible for f_i for F satisfying the JC. (Maps F obtained by permuting f_i are treated as identical). The JC does not depend on constant terms so a, e can be arbitrary. So we list the other three co-efficients.

$$\left[\begin{array}{ccc} b & c & d \\ f & g & h \end{array}\right] = \left[\begin{array}{ccc} 0 & 1 & 0 \\ 1 & 0 & 0 \end{array}\right] \left[\begin{array}{ccc} 1 & 0 & 0 \\ * & 1 & 0 \end{array}\right]$$

In effect the above computation proves

Proposition 2. If a function $F : B^2 \to B^2$ satisfies the Jacobian condition

$$\det JF = 1$$

then F is affine (i.e. the representatives of the components f_i are affine) of the form

$$F = \left[\begin{array}{c} a \\ e \end{array}\right] \oplus A \left[\begin{array}{c} X \\ Y \end{array}\right]$$

where

$$\det A = 1$$

Hence such functions F have inverses

$$G = \ A^{-1} \left[\begin{array}{c} a \oplus X \\ e \oplus Y \end{array}\right]$$

The proposition shows that JC is true for $K = \mathbb{F}_2$ and $n = 2$. However this is verification of the JC in this special case and was possible due to the fact that the constraint $\det JF = 1$ could be solved easily as a computational problem. For $n > 2$ such a computation is a satisfiability problem of rapidly increasing complexity and has not been achieved even for $n = 3$.

4 Conclusion

The JC is proved for functions $F : B^n \to B^n$ for $n = 1, 2$ and for functions $F : \mathbb{F}_p \to \mathbb{F}_p$ for p prime. In all these cases functions F satisfying the Jacobian condition $\det JF = \text{const} \neq 0 \mod p$ are affine.

References

[1] R. J. Lipton. Post on the Jacobian problem `http://rjlipton.wordpress.com`

[2] Arno van den Essen, Polynomial automorphisms and the Jacobian conjecture. Birkhauser, 2000.

[3] R. Lidl and H. Niederreiter, Finite fields. Cambridge University Press, 1997.