The Dissertation Committee for David Charles Jedlicka certifies that this is the approved version of the following dissertation:

On the Suitability of Power Functions as S-boxes for Symmetric Cryptosystems

Committee:

_____

José Felipe Voloch, Supervisor

_____

Fernando Rodriguez-Villegas

_____

David J. Saltman

_____

John Tate

_____

David Zuckerman

On the Suitability of Power Functions as S-boxes for Symmetric Cryptosystems

by

David Charles Jedlicka, B.A.

Dissertation

Presented to the Faculty of the Graduate School of

the University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Doctor of Philosophy

The University of Texas at Austin

May 2006

Acknowledgments

My appreciation and thanks is owed to many people. First, I would like to thank my adviser Felipe Voloch for his insight, encouragement, and patience. The computer programming assistance and editing of Gregory Stoll was invaluable. I am also greatly indebted to my family and friends for their love and support. Finally, a special note of thanks is due to my entire dissertation committee.

On the Suitability of Power Functions as S-boxes for Symmetric Cryptosystems

Publication No. _____

David Charles Jedlicka, Ph.D.

The University of Texas at Austin, 2006

Supervisor: José Felipe Voloch

I present some results towards a classification of power functions that are Almost Perfect Nonlinear (APN), or equivalently differentially 2-uniform, over $\mathbb{F}_{2^n}$ for infinitely many positive integers n. APN functions are useful in constructing S-boxes in AES-like cryptosystems. An application of a theorem by Weil [20] on absolutely irreducible curves shows that a monomial x^m is not APN over $\mathbb{F}_{2^n}$ for all sufficiently large n if a related two variable polynomial has an absolutely irreducible factor defined over $\mathbb{F}_2$. I will show that the latter polynomial's singularities imply that except in five cases, all power functions have such a factor. Three of these cases are already known to be APN for infinitely many fields. The last two cases are still unproven. Some specific cases of power functions have already been known to be APN over only finitely many fields, but they also follow from the results below.

Contents

Chapter 1

Introduction

1.1 Research Summary

Functions that are Almost Perfect Nonlinear (APN), or equivalently differentially 2-uniform, are useful in constructing S-boxes for symmetric key-iterated block ciphers like the Advanced Encryption Standard (AES). The functions considered are typically polynomial mappings over a finite field of characteristic 2, i.e. $\mathbb{F}_{2^n}$. Three classes of power functions have already been shown to be APN over $\mathbb{F}_{2^n}$ for infinitely many n. Also, two classes have been shown to be APN for only finitely many n.

I present some results towards a classification of all power functions that are APN over $\mathbb{F}_{2^n}$ for infinitely many n. Almost all power functions are only APN over finitely many fields. A theorem by Weil [20] bounds the number of rational points on an absolutely irreducible projective curve over $\mathbb{F}_{2^n}$. An easy application of this bound shows that a function x^m is not APN over $\mathbb{F}_{2^n}$ for all sufficiently large n if a related two variable polynomial has an absolutely irreducible factor defined over $\mathbb{F}_2$. I will show that for most power functions the associated two variable polynomial will have too few singularities to factor. Thus, most power functions will be APN over only finitely many fields. Only two classes of power functions remain unclassified although both appear to also be APN over $\mathbb{F}_{2^n}$ for only finitely many n. All fields in this paper will be of characteristic 2.

1.2 The Advanced Encryption Standard

In 2000, the US National Institute for Standards and Technology (NIST) chose Rijndael [8] to be the new Advanced Encryption Standard (AES) to replace DES. Like DES, AES is a symmetric key-iterated block cipher. A symmetric cipher uses the same key for both encryption and decryption. As a block cipher, AES encrypts the plaintext in 128-bit blocks. The blocks are treated as a 4 x 4 matrix of 8-bit entries. Key-iterated means that the encryption takes place over a number of identical rounds each ending with the addition of the key. AES applies 10, 12 or 14 virtually identical rounds where the number of rounds is dependent on the size of the key. Each round is composed of four operations: Byte Substitution, Row Shift, Column Mix, and Round Key Addition. See Figure 1.1.

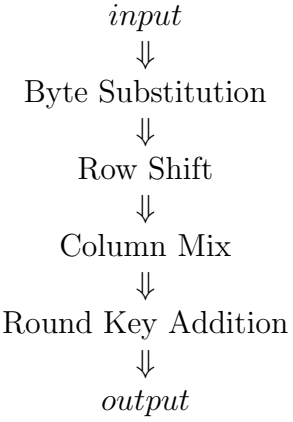

Figure 1.1: One round of AES

The Byte Substitution is the only nonlinear step. In this step, each byte in the block matrix is transformed by an S-box function and then an affine transformation is applied to ensure that algebraic expression of this step is complicated. The S-box function used by AES is $s(x) = x^{-1}$ where x is treated as an element of $\mathbb{F}_{2^8}$ and 0^{-1} is defined as 0.

The next two steps, the Row Shift and Column Mix, provide the diffusion, i.e. the property that each byte in the ciphertext depends on every byte in the plaintext. They are $\mathbb{F}_2$-linear.

Lastly, the round key is added to the ciphertext. The round key is a function of

the entire encryption key. The secrecy of the encrypted text resides in the encryption key. The round is then repeated a total of 10-14 times, with the last round varying slightly.

1.3 Differential Cryptanalysis

One serious attack on iterative block ciphers is differential cryptanalysis. The easiest way to gain security against this attack is to simply perform enough rounds of encryption. The challenge in creating an efficient and secure cipher however lies in trying to make each round as resistant as possible so that fewer rounds need to be performed.

Differential cryptanalysis is based on following a chain of differences between ciphertexts through each round of the cipher. Consider two n-bit plaintexts α and $\hat{\alpha}$ that have a difference of $\alpha' = \alpha - \hat{\alpha}$. Let $\beta = E(\alpha)$ be the encryption of α by the cipher E. Likewise $\hat{\beta} = E(\hat{\alpha})$. The difference α' propagates then to a difference $\beta' = \beta - \hat{\beta}$. The value of β' depends on more than α' of course.

The **difference propagation probability**, $Prob(\alpha', \beta')$, is the probability that a given α' propagates to a given β'. Here α is not considered fixed, but rather we sum over all possible plaintexts. $Prob(\alpha', \beta') = 2^{-n} \sum_{\alpha} \delta(\beta' - (E(\alpha) - E(\alpha - \alpha')))$, where $\delta(x) = 1$ if $x = 0$ and is 0 otherwise. Differential cryptanalysis exploits difference propagations that have large probabilities. To prove resistance against this attack we must be able to show that $Prob(\alpha', \beta')$ is as small as possible for all α', β'.

From [19], the difference propagation probability can be bounded above by twice the square of the probability of any c' being mapped to any d' over any round of the encryption, i.e. $Prob(\alpha', \beta') \leq 2(\max_{c',d'} Prob_i(c', d'))^2$. This motivates the following definition.

Definition 1. *A function $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is said to be APN (Almost Perfect Non-linear) or differentially 2-uniform if it has the following property: For all $\alpha \in \mathbb{F}_{2^n}^*$, $\beta \in \mathbb{F}_{2^n}$,*

$$\#\{x \in \mathbb{F}_{2^n} | \phi(x+\alpha) - \phi(x) = \beta\} \leq 2 \qquad (*)$$

If the S-box function is APN, then $\max_{c',d'} Prob_i(c', d') = \frac{2}{2^n}$. Note that over a field of characteristic 2, a function cannot be differentially 1-uniform as the difference between x and $x + \alpha$ is the same as the difference between $x + \alpha$ and x. Thus, the strongest resistance to differential cryptanalysis occurs with an APN S-box function.

More can be found in [8] pp. 113-122 as well as [18] and [19].

1.4 Known Results

Known Results		
Function	APN for large n?	Reference
x^{2^j+1} for $\gcd(n, j) = 1$	Yes	Gold [12], Janwa and Wilson [14]
$x^{4^j-2^j+1}$ for $\gcd(n, j) = 1$	Yes	Kasami [15] and Dobbertin [9]
x^{-1} for odd n	Yes	Nyberg [18], Beth and Ding [2]
x^m for $m \equiv 3 \pmod 4$ and $m > 3$	No	Janwa, McGuire and Wilson [13]
x^m for $d = 1$, h_+ has no singularities off the lines $y = x$ and $y = x + 1$	No	Janwa, McGuire and Wilson [13]
x^m for $d < \frac{m-1}{2^l}$, $m > 5$	No	Jedlicka
x^{-m} for $m \equiv 1 \pmod 4$, $m > 5$	No	Jedlicka

Table 1.1: All known results including this paper

Two classes of monomials are already known to be APN over $\mathbb{F}_{2^n}$ for infinitely many n. $\phi(x) = x^{2^j+1}$ is APN over $\mathbb{F}_{2^n}$ provided $(n, j) = 1$. This class was shown to be maximally nonlinear by Gold [12] for odd n which implies APN according to Chabaud and Vaudenay [7, Theorem 4]. This class was shown to be APN for all n provided $(n, j) = 1$ by Janwa and Wilson [14] as well as Nyberg [18].

The other class of monomials, Kasami power functions, $\phi(x) = x^{4^j-2^j+1}$, is known to be APN over $\mathbb{F}_{2^n}$ also provided $(n, j) = 1$. They were shown to be maximally nonlinear (and hence APN) for odd n by Kasami [15]. The even case was addressed by Dobbertin [9].

The equivalence of this problem to finding double-error-correcting cyclic codes with minimum distance 5 is discussed in Carlet et al. [6] in 1998. Thus, the work done by Baker, Lint, and Wilson [1] in 1983 on cyclic codes also showed the first class of monomials to be APN. Likewise, the Kasami power functions were studied by van Lint and Wilson [17] in the case of odd n in 1986 and by Janwa and Wilson [14] in the case of even n in 1993.

For power functions with negative exponents, one class is already known to be APN over infinitely many fields. $g(x) = x^{-1}$ is APN over $\mathbb{F}_{2^n}$ provided n is odd; see Nyberg [18] and Beth and Ding [2].

Composing these functions with the Frobenius automorphism (giving functions of the form $x^{(2^b)(2^j+1)}$, $x^{(2^b)(4^j-2^j+1)}$, or $x^{(2^b)(-1)}$) also produces APN monomials. See Lemma 4.

Two large cases of monomials have already been known to not be APN over $\mathbb{F}_{2^n}$ for infinitely many n. When $m \equiv 3 \pmod 4$ and $m > 3$ then x^m is APN over only finitely many fields. Also, in the case that $d = 1$ and h_+ has no singular points off the lines $y = x$ and $y = x + 1$, then x^m is APN over only finitely many fields (see the next section for definitions of d and h_+). These results are proven in Janwa, McGuire and Wilson [13] and also follow from Theorem 1.

1.5 My Results

For a function ϕ to be APN over $\mathbb{F}_{2^n}$, there cannot be an α, x, and y such that $\phi(x+\alpha)+\phi(x) = \phi(y+\alpha)+\phi(y)$ where $y \neq x, x+\alpha$. This is equivalent to asking that $\phi(x+\alpha)+\phi(x)+\phi(y+\alpha)+\phi(y) = 0$ has no solutions outside of $y = x$ and $y = x+\alpha$. According to Lemma 3 in Section 2.2, we may assume $\alpha = 1$ in the case that ϕ is a power function. This motivates the following definition.

Definition 2. *For the case of power functions with positive exponents, let $\phi_+(x) = x^m$ for a positive integer m. Define $f_+(x, y) = (x+1)^m + x^m + (y+1)^m + y^m$ and*

$h_+(x,y) = \frac{f_+(x,y)}{(x+y)(x+y+1)}$.

For the case of negative exponents, let $\phi_-(x) = x^{-m}$ *where* $m > 0$. *Define* $\eta(x,y) = (x+1)^{-m} + x^{-m} + (y+1)^{-m} + y^{-m}$. *Note that* 0^{-1} *is defined as 0.* η *can be transformed into* $\eta = \frac{x^m(x+1)^m(y^m+(y+1)^m)+y^m(y+1)^m(x^m+(x+1)^m)}{x^m y^m (x+1)^m (y+1)^m}$. *Zeros of the numerator are also zeros of* η. *Let* $f_-(x,y)$ *be the numerator of* η. *Then as above define* $h_-(x,y) = \frac{f_-(x,y)}{(x+y)(x+y+1)}$.

Thus, ϕ_+ is APN over $\mathbb{F}_{2^n}$ for a positive integer n if and only if h_+ has no zeros off the lines $y = x$ and $y = x+1$. The same applies to ϕ_- and h_-. Also, while f_+, f_-, h_+ and h_- explicitly depend on the parameter m, for simplicity I shall suppress the m in the notation. The following definition will be used throughout the paper, and you can also refer to the symbol reference page in Section 2.4.

Definition 3. *Define* l *to be the largest integer such that* 2^l *divides* $m-1$. *Also, let* $m' = \frac{m-1}{2^{l-1}} + 1$. *Let* $d = gcd(m-1, 2^l-1) = gcd(\frac{m'-1}{2}, 2^l-1)$. *Also let* k *be the largest integer such that* 2^k *divides* $m+1$.

Note that $l = 1$ is equivalent to $m \equiv 3 \pmod 4$.

Theorem 1. *Let* m *be an odd integer,* $m > 5$ *and* $m \neq 2^j + 1$ *for any positive integer* j. *Then,* h_+ *has an absolutely irreducible factor defined over* $\mathbb{F}_2$ *provided* $d < \frac{m'-1}{2}$.

Theorem 2. *Let* $m \equiv 1 \pmod 4$ *and* $m > 5$. *Then,* h_- *has an absolutely irreducible factor defined over* $\mathbb{F}_2$.

Corollary 1. *For odd integers* m *such that* $m > 5$ *and* $m \neq 2^j + 1$ *for any positive integer* j, *the power function* x^m *is not APN over* $\mathbb{F}_{2^n}$ *for large enough* n. *Similarly, for integers* $m > 5$ *where* $m \equiv 1 \pmod 4$, *the function* x^{-m} *is not APN over* $\mathbb{F}_{2^n}$ *for large enough* n.

Proof. This follows from Theorem 1 and Theorem 2 according to Lemma 2. □

Chapter 2

Background Material and Proof Strategy

2.1 Algebraic Geometry over Finite Fields

Let $f(x, y)$ be a polynomial with coefficients in the field $\mathbb{F}_q$. If $f(x, y)$ is irreducible over $\mathbb{F}_q$ but factors over an extension, then the factors will be conjugates. If $f(x, y)$ does not factor over any extension of $\mathbb{F}_q$ we say it is absolutely irreducible. We can consider $f(x, y)$ to be a curve over the affine plane $\mathbb{A}^2(\mathbb{F}_q)$. Points on the curve correspond to zeros of the function.

Definition 4. *A point $p = (x_0, y_0)$ on f is singular if $\frac{\partial f}{\partial x}(p) = \frac{\partial f}{\partial y}(p) = 0$. The multiplicity of p on f, denoted $m_p(f)$, is the degree of the smallest degree term with non-zero coefficients in $F(x, y) = f(x - x_0, y - y_0)$. Any point on a curve will have multiplicity at least 1, while a singular point has multiplicity at least 2. For any nonnegative integer T, define F_T to be the homogeneous polynomial composed of the terms of degree T in F. Then the tangent lines to f at p are the factors of F_{m_p}.*

Any two plane curves, call them u and v, defined over the finite field $\mathbb{F}_{2^n}$ that intersect at a point p are said to intersect transversally if they have no tangent lines in common at p. An intersection point of u and v will be a singular point of the curve uv. Each intersection point can be assigned a number indicating approximately the "multiplicity of intersection." The intersection number, $I_p(u, v)$, is defined as

$\dim_K(O_p(\mathbb{A}^2)/(u,v))$, where K is the field $\mathbb{F}_{2^n}$ and $O_p(\mathbb{A}^2)$ is the ring of rational functions over the affine plane that are defined at p. We will not be calculating intersection numbers from the definition but rather using a few simple properties from Fulton [11] pp 74-75. First, if u and v intersect transversally then $I_p(u,v) = m_p(u) \cdot m_p(v)$. Also, if u and v do not intersect at p at all, then $I_p(u,v) = 0$. One extra property I will need which is proven in Janwa, McGuire and Wilson [13] is:

Lemma 1. *Let $J(x,y) = 0$ be an affine curve defined over $\mathbb{F}_q$ and let $J(x,y) = u(x,y) \cdot v(x,y)$. Write $J(x+a, y+b) = J_m + J_{m+1} + ...$ where $p = (a,b)$ is a point on J of multiplicity m. Suppose J_m and J_{m+1} are relatively prime. Then, u and v intersect transversely implying that $I_p(u,v) = m_p(u) \cdot m_p(v)$. In addition, if J has only one tangent direction at p, then $I_p(u,v) = 0$, and p falls on only one of the curves u and v.*

Now consider $f(x,y)$ as a projective curve over $\mathbb{P}^2(\mathbb{F}_q)$. Weil's Bound [20] states that the number of rational points, N, over $\mathbb{F}_{q^m}$ on an absolutely irreducible projective curve that is defined over $\mathbb{F}_q$ satisfies $|N - (q^m + 1)| \leq c\sqrt{q^m}$, where the constant c is independent of the field. Also, recall that for a function γ to be APN, there cannot be any solutions to $\gamma(x+\alpha) + \gamma(x) + \gamma(y+\alpha) + \gamma(y) = 0$ outside of $y = x$ and $y = x + \alpha$.

Lemma 2. *For a polynomial function $\gamma : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_2$ and a constant $\alpha \in \mathbb{F}_{2^n}^*$, if the function $g(x,y) = \frac{\gamma(x+\alpha)+\gamma(x)+\gamma(y+\alpha)+\gamma(y)}{(x+y)(x+y+\alpha)}$ has an absolutely irreducible factor over $\mathbb{F}_2$, then γ is not APN over $\mathbb{F}_{2^n}$ for large enough n.*

Proof. Following Lidl and Niederreiter [16] page 365, let $p(x,y)$ be the absolutely irreducible factor of g, and let d be its degree. Then there are at most $2d$ rational points on p with either $y = x$ or $y = x + \alpha$. Weil's Bound [20] states that the number of rational points, N, over $\mathbb{F}_{2^n}$ on an absolutely irreducible projective curve satisfies $|N - (2^n + 1)| \leq c\sqrt{2^n}$ for some constant c. For sufficiently large n, the total number of points will exceed $2d$. Therefore, g will have a zero off the lines $y = x$ and $y = x + \alpha$ and so γ will not be APN. □

Definition 5. *Let $\hat{f}$ be the usual homogenized, projective form of f. Define $\tilde{f}$ to be the dehomogenized form of $\hat{f}$ relative to y, redefining $x = \frac{x}{y}$ and $z = \frac{z}{y}$. As in*

the affine case, for any nonnegative integer T, define $\tilde{F}_T$ to be the homogeneous polynomial composed of the terms of degree T in $\tilde{F}$.

Bezout's Theorem states that for two projective plane curves, u and v, of degree d_u and d_v respectively, $\sum_p I_p(u,v) = d_u \cdot d_v$ where the sum runs over all points of intersection. For a proof, see Fulton [11] pp 112-115. This theorem shows that the intersection number is the proper way to count the multiplicity of an intersection point.

One last definition that we will need is a discrete valuation ring. A ring, R, which is Noetherian, local, and whose maximal ideal is principal is called a discrete valuation ring. Such a ring has an irreducible element t, called a uniformizing parameter, such that every nonzero $r \in R$ can be written uniquely as $r = ut^n$ for some unit u and nonnegative integer n. The exponent n is called the order of r, $\text{ord}(r)$. The order satisfies the property that if $\text{ord}(a) < \text{ord}(b)$ then $\text{ord}(a+b) = \text{ord}(a)$.

Lucas's Theorem gives a useful formula for computing $\binom{a}{b}$ mod 2. Writing $a = a_j 2^j + a_{j-1}2^{j-1} + ... + a_1 2 + a_0$ and $b = b_j 2^j + b_{j-1}2^{j-1} + ... + b_1 2 + b_0$, then $\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_j}{b_j}$ mod 2. Note that this is congruent to 0 if and only if the binary expansion of b has a 1 in a place that the binary expansion of a has a 0, i.e. $b_i = 1$ and $a_i = 0$ for some i. By the definition of l in Definition 3, the first nonzero digit after the units digit in the binary expansion of m occurs at the 2^l place. Thus $\binom{m}{q} = 0$ for $1 < q < 2^l$. Also, $(x+1)^m$ has a nice expansion; the only nonzero terms are those whose exponents' binary expansions are subsets of the binary expansion of m. For example $(x+1)^5 = x^5 + x^4 + x + 1$ because the only possible subsets of $5 = 2^2 + 2^0$ are $2^2 + 2^0 = 5$, $2^2 = 4$, $2^0 = 1$, and 0.

2.2 Initial Lemmas

Lemma 3. *If x^m is not differentially 2-uniform over $\mathbb{F}_{2^n}$ for some positive integer n then there exists a β such that x^m fails to satisfy inequality $(*)$ in Definition 1 for β and $\alpha = 1$ over $\mathbb{F}_{2^n}$.*

Proof. As x^m is not differentially 2-uniform over $\mathbb{F}_{2^n}$, then there exists an $\alpha \neq 0$ and a β such that x^m fails to satisfy inequality $(*)$ in Definition 1. This mean that

there are multiple x_i values that satisfy $(x_i+\alpha)^m + x_i^m = \beta$. Dividing the equation $(x+\alpha)^m - x^m = \beta$ by α^m yields $(\frac{x_i}{\alpha}+1)^m + (\frac{x_i}{\alpha})^m = \frac{\beta}{\alpha^m}$. Thus for $\alpha' = 1$ and $\beta' = \frac{\beta}{\alpha^m}$, there are multiple values $x_i' = \frac{x_i}{\alpha}$ that satisfy the differentially uniform equation. Thus, x^m fails to satisfy inequality $(*)$ when $\alpha = 1$ as well. □

Lemma 4. *x^{a2^b} with a odd is APN if and only if x^a is.*

Proof. The squaring map is an automorphism of $\mathbb{F}_{2^n}$. Thus, $(x+\alpha)^m - x^m = \beta$ if and only if $(x+\alpha)^{2m} - x^{2m} = \beta^2$. Therefore, if an α propagates to a β for more than 2 choices of plaintext x under the encryption function x^m, then clearly α propagates to β^2 for more than 2 choices of plaintext under the encryption function x^{2m}. □

We will assume for the rest of the paper that m is odd, $m > 5$, and that for the positive case $m \neq 2^j + 1$ for any integer j as these monomials are already well studied. Also, all calculations in the paper take place over a field extension of $\mathbb{F}_2$ large enough to contain all the singularities of f_+, f_-, h_+, and h_-.

2.3 Proof Strategy

The method I will use of proving that h_+ and h_- have absolutely irreducible factors defined over $\mathbb{F}_2$ will be to bound the intersection number above for all possible intersection points in the projective plane. I will thus calculate a bound for the global intersection number regardless of the choice of factorization. The lemma below will show that we can find factorization whose global intersection number is at least a certain size. These two bounds will often lead to a contradiction. This method first appears in the literature in Janwa, McGuire and Wilson [13] although I derived it independently.

Lemma 5. *If h_+ or h_- has no absolutely irreducible factors over $\mathbb{F}_2$, then $e = \frac{I_{tot}}{\frac{(deg(h))^2}{4}} \geq \frac{8}{9}$ where I_{tot} is any upper bound on the global intersection number of u and v for all factorizations $h = u \cdot v$ over the algebraic closure of $\mathbb{F}_2$. Equivalently, if h_+ or h_- has no absolutely irreducible factors over $\mathbb{F}_2$, then there exists a factoring into u and v such that $\sum_p I_p(u,v) \geq \frac{2(deg(h))^2}{9}$.*

Proof. For simplicity I will just use h without specifying h_+ or h_-. Assume that h factors over $\mathbb{F}_2$ as $h = e_1 e_2 ... e_r$ where each e_i is irreducible over $\mathbb{F}_2$ and $r \geq 1$. Let c_i be the number of factors of e_i when it splits over the algebraic closure of $\mathbb{F}_2$. Then over the algebraic closure of $\mathbb{F}_2$ each e_i factors into c_i conjugates each of degree $\frac{(\deg(e_i))}{c_i}$.

Now, partition the factors of each e_i into two polynomials, u_i, v_i such that $\deg(u_i) = \deg(v_i)$ if c_i is even and $\deg(u_i) = \deg(v_i) + \frac{(\deg(e_i))}{c_i}$ if c_i is odd. Setting $u = \prod u_i$ and $v = \prod v_i$, we can produce a factorization of h such that $\deg(u) - \deg(v) \leq \frac{\deg(h)}{3}$. Given that $\deg(u) + \deg(v) = \deg(h)$, we have that $\deg(u)\deg(v) \geq \frac{(\deg(h))^2}{4}(\frac{8}{9})$. Since $I_{tot} \geq \deg(u)\deg(v)$ by Bezout's Theorem and $e = \frac{I_{tot}}{\frac{(\deg(h))^2}{4}}$, we get that $e \geq \frac{8}{9}$. □

2.4 Symbol Reference Page

a	The largest power of 2 less than m', i.e. $2^{\lfloor \log_2(m') \rfloor}$
d	$\gcd(m-1, 2^l - 1) = \gcd(\frac{m'-1}{2}, 2^l - 1)$
e	$\frac{I_{tot}}{\frac{(\deg(h))^2}{4}}$
ϕ_+	x^m where $m \neq 2^j + 1$ for any integer j
ϕ_-	x^{-m}
f_+	$(x+1)^m + x^m + (y+1)^m + y^m$
f_-	$x^m(x+1)^m(y^m + (y+1)^m) + y^m(y+1)^m(x^m + (x+1)^m)$
F_T	The polynomial composed of the terms of degree T in $f(x+x_0, y+y_0)$
h_+	$\frac{f_+(x,y)}{(x+y)(x+y+1)}$
h_-	$\frac{f_-(x,y)}{(x+y)(x+y+1)}$
H_T	The polynomial composed of the terms of degree T in $h(x+x_0, y+y_0)$
$I_p(u,v)$	The multiplicity of an intersection point of u and v. More precisely, $\dim_K(O_p(\mathbb{A}^2)/(u,v))$. See Section 2.1
I_{tot}	Any upper bound on the global intersection number of u and v for all factorizations $h = u \cdot v$ over the algebraic closure of $\mathbb{F}_2$
k	The largest positive integer such that 2^k divides $m+1$
l	The largest positive integer such that 2^l divides $m-1$
m	An odd positive integer greater than 5
m'	$\frac{m-1}{2^{l-1}} + 1$

Chapter 3

Positive Exponents

3.1 Easy Base Cases

For a few classes of m, we can easily show that h_+ is smooth. With no singularities, h_+ must clearly be absolutely irreducible. Note that the lemma below depends on Lemma 9 and Corollary 2 as well as Lemma 10 from Section 3.2 of this chapter.

Lemma 6. *Assume $m \equiv 3$ (mod 4). If all of the affine singularities of f_+ lie only on the lines $y = x$ and $y = x + 1$, then h_+ is smooth and thus absolutely irreducible.*

Proof. If all the affine singularities of f_+ lie only on the lines $y = x$ and $y = x + 1$, then the same applies to h_+. By Lemma 9 and Corollary 2 from Section 3.2, the singular points have multiplicity 2 on f_+. Thus, they would have multiplicity one less on h_+. A singular point of multiplicity 1 is not a singular point - it is just a normal point on the curve. Thus, h_+ has no affine singular points. Lemma 10 from Section 3.2 shows that h_+ has no singular points at infinity and thus it is smooth hence absolutely irreducible. □

Theorem 3. *For $m = 2^j + 3$ where $j > 2$, h_+ is smooth and thus absolutely irreducible.*

Proof. As $m = 2^j + 3$, f_+ expands to

$$f_+ = x^{2^j+2} + x^{2^j+1} + x^{2^j} + x^3 + x^2 + x + y^{2^j+2} + y^{2^j+1} + y^{2^j} + y^3 + y^2 + y.$$

Now, $\frac{\partial f_+}{\partial x} = x^{2^j} + x^2 + 1$ and $\frac{\partial f_+}{\partial y} = y^{2^j} + y^2 + 1$. Assume that (x, y) is a singular point. Use that $x^{2^j} = x^2 + 1$ and $y^{2^j} = y^2 + 1$ in the equation $f_+(x, y) = 0$ to get

$$\begin{aligned} 0 &= (x^4 + x^2) + (x^3 + x) + (x^2 + 1) + x^3 + x^2 + x + \\ &\quad + (y^4 + y^2) + (y^3 + y) + (y^2 + 1) + y^3 + y^2 + y \\ &= x^4 + x^2 + y^4 + y^2 \\ &= (x + y)^2(x + y + 1)^2. \end{aligned}$$

Thus, all affine singular points of $f_+(x, y)$ satisfy either $x = y$ or $x = y + 1$. Since $h_+ = \frac{f_+}{(x+y)(x+y+1)}$, all affine singular points for h_+ also occur only on these two lines.

Lemma 6 shows that as $m \equiv 3 \pmod 4$, if h_+ has no singular points outside these two lines, then it is smooth hence absolutely irreducible. □

Lemma 7. *The singular points of f_+ are precisely the points (x_0, y_0) that satisfy $(x_0 + 1)^{m-1} = x_0^{m-1} = y_0^{m-1} = (y_0 + 1)^{m-1}$.*

Proof. First, $\frac{\partial f_+}{\partial x} = (x + 1)^{m-1} + x^{m-1}$ and $\frac{\partial f_+}{\partial y} = (y + 1)^{m-1} + y^{m-1}$. Assume that (x_0, y_0) is a zero of these two partial derivatives. Thus,

$$(x_0 + 1)^{m-1} = x_0^{m-1} \tag{3.1}$$
$$(y_0 + 1)^{m-1} = y_0^{m-1}. \tag{3.2}$$

Now, take equations (3.1) and (3.2) and multiply them by $x_0 + 1$ and $y_0 + 1$ respectively to get

$$(x_0 + 1)^m = x_0^m + x_0^{m-1} \tag{3.3}$$
$$(y_0 + 1)^m = y_0^m + y_0^{m-1}. \tag{3.4}$$

Substituting these two equations into

$$0 = f_+(x_0, y_0) = (x_0+1)^m + x_0^m + (y_0+1)^m + y_0^m$$

yields the equation $0 = x_0^{m-1} + y_0^{m-1}$. This shows that all singular points satisfy $(x_0+1)^{m-1} = x_0^{m-1} = y_0^{m-1} = (y_0+1)^{m-1}$. The fact that only singular points satisfy these equations follows similarly.

□

Lemma 8. *For $m = 2^j - 2^p - 1, j \geq 4, j > p > 1$, all singular points $p = (x_0, y_0)$ of f_+ must satisfy $x_0^{2^{p-1}} + x_0 = y_0^{2^{p-1}} + y_0$.*

Proof. We can manipulate $\frac{\partial f_+}{\partial x} = (x+1)^{m-1} + x^{m-1}$ as follows

$$\frac{\partial f_+}{\partial x}(x_0, y_0) = (x_0+1)^{2^j - 2^p - 2} + x_0^{2^j - 2^p - 2} = 0$$

$$(x_0+1)^{2^j} + x_0^{2^j-2^p-2}(x_0+1)^{2^p+2} = 0$$

$$x_0^{2^j} + 1 + x_0^{2^j-2^p-2}(x_0+1)^{2^p+2} = 0$$

$$x_0^{2^j-2^p-2}(x_0^{2^p+2} + (x_0+1)^{2^p+2}) = 1$$

$$x_0^{2^j-2^p-2} = \frac{1}{(x_0^{2^p+2} + (x_0+1)^{2^p+2})}$$

$$x_0^{2^j-2^p-2} = \frac{1}{(x_0^{2^p} + x_0^2 + 1)}$$

Likewise, $y_0^{2^j-2^p-2} = \frac{1}{(y_0^{2^p}+y_0^2+1)}$. Now, $x_0^{m-1} = y_0^{m-1}$ by Lemma 7. This is the same as $x_0^{2^j-2^p-2} = y_0^{2^j-2^p-2}$ so

$$\frac{1}{(x_0^{2^p} + x_0^2 + 1)} = \frac{1}{(y_0^{2^p} + y_0^2 + 1)}.$$

Over $\mathbb{F}_2$ this simplifies to $x_0^{2^{p-1}} + x_0 + 1 = y_0^{2^{p-1}} + y_0 + 1$ which implies $x_0^{2^{p-1}} + x_0 = y_0^{2^{p-1}} + y_0$. □

Theorem 4. *For $m = 2^j - 5, j \geq 4$, h_+ is smooth hence absolutely irreducible.*

Proof. From Lemma 8 with $p = 2$, we have that all singular points satisfy $x_0^2 + x_0 = y_0^2 + y_0$. This simplifies to $(x_0 + y_0)(x_0 + y_0 + 1) = 0$. Thus, all singular points of h_+ occur on the lines $x = y$ or $x = y + 1$.

As $m \equiv 3 \pmod 4$ and all affine singular points of f_+ occur on the two lines $x = y$ and $x = y + 1$, Lemma 6 shows that h_+ is smooth hence absolutely irreducible. □

Theorem 5. *For $m = 2^j - 9, j \geq 5$, h_+ is smooth hence absolutely irreducible.*

Proof. From Lemma 8 with $p = 3$, we have that all singular points of f_+ satisfy $x_0^4 + x_0 = y_0^4 + y_0$. This simplifies to $(x_0+y_0)(x_0+y_0+1)(x_0+y_0+w)(x_0+y_0+w^2) = 0$, where w is a root of $x^2 + x + 1$. Thus, all singular points occur on the lines $y = x$, $y = x + 1$, $y = x + w$, or $y = x + w^2$.

Consider the case of singular points on the line $y = x + w$. In this case, the singular points must satisfy $x^{m-1} = (x + 1)^{m-1} = (x + w)^{m-1}$. As no affine singular point has an x-value of 0, we may divide by x^{m-1} yielding

$$1 = (1 + u)^{m-1} = (1 + wu)^{m-1} \tag{3.5}$$

where $u = x^{-1}$.

Remembering $m - 1 = 2^j - 10 = 2(2^{j-1} - 5)$, we can substitute this in and take the square root of both equations to get the simultaneous equations $1 = (1+u)^{2^{j-1}-5}$ and $1 = (1 + wu)^{2^{j-1}-5}$. Moving the negative exponents to the other side gives

$$(1 + u)^5 = 1 + u^{2^{j-1}}, \text{ and} \tag{3.6}$$

$$(1 + wu)^5 = 1 + w^{2^{j-1}} u^{2^{j-1}}. \tag{3.7}$$

There are two cases, $w^{2^{j-1}} = w$ or $w^{2^{j-1}} = w^2$.

First assume $w^{2^{j-1}} = w$. Then take equation (3.6), multiply both sides by w, and add it to equation (3.7) to get

$$w(1 + u)^5 + (1 + wu)^5 = w + wu^{2j-1} + 1 + wu^{2^{j-1}} \tag{3.8}$$

$$w(1+u+u^4+u^5)+(1+wu+wu^4+w^2u^5)=w+1$$

$$(w+w^2)u^5=0$$

This implies $u=0$. However, u was defined as the inverse of x and cannot be zero, a contradiction.

Next assume that $w^{2^{j-1}}=w^2$. Then take equation (3.6), multiply both sides by w^2, and add it to equation (3.7) to get

$$w^2(1+u)^5+(1+wu)^5=w^2+w^2u^{2^{j-1}}+1+w^2u^{2^{j-1}}$$

$$w^2(1+u+u^4+u^5)+(1+wu+wu^4+w^2u^5)=w^2+1$$

$$(w^2+w)u+(w^2+w)u^4=0$$

$$u^3=1$$

which implies $u=1,w$, or w^2. As $x\neq 1$, $u\neq 1$. Likewise, from equation (3.5), $u\neq w^2$, so u must be w. This implies $x=u^{-1}=w^2$ which implies $y=x+w=w^2+w=1$ which is impossible as all singular points must satisfy $(y+1)^{m-1}=y^{m-1}$.

Therefore, there are no singular points on the line $y=x+w$. Since $y=x+w^2$ is conjugate to this line (squaring points on one line gives points on the other), there are no singular points on $y=x+w^2$ either. Therefore, all singular points must lie on $y+x$ or $x+y+1$.

As all affine singular points of f_+ occur on the two lines $x=y$ and $x=y+1$, Lemma 6 shows that h_+ is smooth hence absolutely irreducible. □

The following theorem is a generalization of the previous one; however, in generalizing, we must strengthen the assumptions to be able to still prove that h_+ is smooth.

Theorem 6. *For $m = 2^j - 2^p - 1$ where $j \geq p+2, p \geq 2$, and $j \equiv 1 \pmod{p-1}$, h_+ is smooth hence absolutely irreducible.*

Proof. From Lemma 8 we have that all singular points of f_+ satisfy $x_0^{2^{p-1}} + x_0 = y_0^{2^{p-1}} + y_0$. This factors as $(x_0+y_0)(x_0+y_0+1)(x_0+y_0+w)(x_0+y_0+w^2)...(x_0+y_0+w^{(2^{p-1}-2)}) = 0$, where w is a generator of $\mathbb{F}^*_{2^{p-1}}$. Thus, all singular points occur on the lines $y = x$, $y = x+1$, $y = x+w$, ..., $y = x + w^{(2^{p-1}-2)}$.

Consider the case of singular points on the line $y = x + w^a$ for $0 < a < 2^{p-1} - 1$. In this case, the singular points must satisfy $x^{m-1} = (x+1)^{m-1} = (x+w^a)^{m-1}$. As $x = 0$ is not a root, we may divide by x^{m-1} yielding

$$1 = (1+u)^{m-1} = (1+w^a u)^{m-1}$$

where $u = x^{-1}$.

Remembering $m - 1 = 2^k - 2^p - 2 = 2(2^{j-1} - 2^{p-1} - 1)$, we can substitute this in and take the square root of both equations to get the simultaneous equations

$$1 = (1+u)^{2^{j-1}-2^{p-1}-1} \text{ and } 1 = (1+w^a u)^{2^{j-1}-2^{p-1}-1}.$$

Moving the negative exponents to the other side gives

$$(1+u)^{2^{p-1}+1} = 1 + u^{2j-1} \tag{3.9}$$

$$(1+w^a u)^{2^{p-1}+1} = 1 + w^{a2^{j-1}} u^{2^{j-1}}. \tag{3.10}$$

As $j \equiv 1 \pmod{p-1}$ we know that $w^{a2^{j-1}} = w^a$ in $\mathbb{F}_{2^{p-1}}$.

Take equation (3.9), multiply both sides by w^a, and add this to equation (3.10) to get

$$w^a(1+u)^{2^{p-1}+1} + (1+w^a u)^{2^{p-1}+1} = w^a + w^a u^{2j-1} + 1 + w^a u^{2^{j-1}}$$

$$w^a(1+u+u^{2^{p-1}} + u^{2^{p-1}+1}) + (1 + w^a u + w^a u^{2^{p-1}} + w^{a+1} u^{2^{p-1}+1}) = w^a + 1$$

$$(w^a + w^{a+1})u^{2^{p-1}+1} = 0$$

which implies $u = 0$. However, u was defined as the inverse of x and cannot be zero, a contradiction. Therefore, there are no singular points on the line $y = x + w^a$. Thus, all singular points must lie on $y + x$ or $x + y + 1$.

As all affine singular points of f_+ occur on the two lines $x = y$ and $x = y + 1$, Lemma 6 shows that h_+ is smooth hence absolutely irreducible. □

3.2 Singularities of h_+

Theorem 7. *The singular points of h_+ are described by Table 3.1. If $m \equiv 3$ (mod 4), then h_+ has no singularities at infinity (Type III).*

Singularities of h_+				
Type	Description	m_p	I_p Bound	Max Number of Points
I a	Affine, on a line, $x_0, y_0 \in \mathbb{F}_{2^l}^*$	2^l	$(2^{l-1})^2$	$2(d-1)$
I b	Affine, on a line, $x_0, y_0 \notin \mathbb{F}_{2^l}^*$	$2^l - 1$	0	$m' - 3$
II a	Affine, off both lines, $x_0, y_0 \in \mathbb{F}_{2^l}^*$	$2^l + 1$	$2^{l-1}(2^{l-1}+1)$	$(d-1)(d-3)$
II b	Affine, off both lines, exactly one of $x_0, y_0 \in \mathbb{F}_{2^l}^*$	2^l	0	Not important
II c	Affine, off both lines, $x_0, y_0 \notin \mathbb{F}_{2^l}^*$	2^l	2^l if $l > 1$ 0 if $l = 1$	$(\frac{m'-3}{2})(m'-a-3)$ − $(d-1)(d-3)$
III a	(1:1:0)	$2^l - 2$	$(\frac{2^l-2}{2})^2$	1
III b	$(w:1:0)$, $w^d = 1$, $w \neq 1$	2^l	$(2^{l-1})^2$	$d-1$
III c	$(w:1:0)$, $w^d \neq 1$	$2^l - 1$	0	Not important

Table 3.1: All singularities of h_+

The proof will follow from Lemmas 9-16 and their corollaries. Recall the symbols from Definition 3. Note that if $m \equiv 3 \pmod 4$, then $d = l = 1$. Note that "on a line" means that the singular point falls on one of the two lines $x_0 = y_0 + 1$ or

$x_0 = y_0$ and "off both lines" means the point is on neither line. a is the largest power of 2 less than m', i.e. $a = 2^{\lfloor \log_2(m') \rfloor}$. Also, w is a root of $x^{\frac{m'-1}{2}} = 1$.

Lemma 9. *The total number of affine singularities of f_+ (Type I and II) is at most $(\frac{m'-3}{2})(m'-1-a)$ where a is the largest power of 2 less than m', i.e. $a = 2^{\lfloor \log_2(m') \rfloor}$. On f_+, each affine singularity has multiplicity 2^l or 2^l+1. A singularity has multiplicity exactly 2^l+1 on f_+ if and only if both $x_0, y_0 \in \mathbb{F}_{2^l}^*$. On h_+, singularities on either of the lines $y = x$ or $y = x+1$ will have multiplicity one less than they have on f_+; all other singularities will have the same multiplicity on both curves.*

Proof. First let us calculate the singularities of f_+. By Lemma 7, the singular points (x_0, y_0) of f_+ are precisely the solutions to the following three equations.

$$x_0^{m-1} = y_0^{m-1} \tag{3.11}$$
$$(x_0+1)^{m-1} = x_0^{m-1} \tag{3.12}$$
$$(y_0+1)^{m-1} = y_0^{m-1} \tag{3.13}$$

Note that this implies $x_0 \neq 0, 1$ and $y_0 \neq 0, 1$. Since $2^l | (m-1)$, we can take the square root of both sides of each of these equations l times giving

$$x_0^{\frac{m'-1}{2}} = y_0^{\frac{m'-1}{2}} \tag{3.14}$$
$$(x_0+1)^{\frac{m'-1}{2}} = x_0^{\frac{m'-1}{2}} \tag{3.15}$$
$$(y_0+1)^{\frac{m'-1}{2}} = y_0^{\frac{m'-1}{2}}. \tag{3.16}$$

Interestingly, this shows that the singular points are the same for m and m'.

Equation (3.15) has at most $\frac{m'-3}{2}$ roots. Now for any root, x_0, of (3.15) if we let $y_0 = x_0$ or $y_0 = x_0+1$ then (x_0, y_0) is a singular point of f_+, but there may be more choices for y_0. Fix an x_0 and let us count the number of possible values of y_0 for which (x_0, y_0) is a singular point. Let $\alpha = x_0^{\frac{m'-1}{2}}$ and substitute this into equation (3.14) to get $y_0^{\frac{m'-1}{2}} = \alpha$. Write m in the form $m = (\sum_{j=1}^{b} 2^{i_j}) + 2^l + 1$ for some

integer b where $i_j > i_{j-1}$ and $i_j > l$ for all j. Thus $m' = (\sum_{j=1}^{b} 2^{i_j - l + 1}) + 2 + 1$ and $(\frac{m'-1}{2}) = (\sum_{j=1}^{b} 2^{i_j - l}) + 1$.

In this context we can write equation (3.16) as $(\sum_{\nu} y_0^{\nu}) + y_0^{\frac{m'-1}{2}} = 0$, where the sum runs over all possible partial sums (combinations) of the terms in the binary expansion of $\frac{m'-1}{2}$. We can cancel out the two top degree terms to get

$$\sum_{\nu}^{*} y_0^{\nu} = 0 \tag{3.17}$$

where the asterisk indicates that this sum runs over all possible partial sums except $\nu \neq \frac{m'-1}{2}$.

Now multiply equation (3.17) by $y_0^{\frac{m'-1}{2} - 2^{i_b - l}}$ substituting in $y_0^{\frac{m'-1}{2}} = \alpha$ for any terms of degree greater than or equal to $\frac{m'-1}{2}$ and call the resulting equation E. I claim equation E has degree $m' - 1 - 2^{i_b - l + 1} = m' - 1 - a$ where a is the largest power of 2 less than m', i.e. $a = 2^{\lfloor \log_2(m') \rfloor}$.

Proof of claim: Any term in (3.17) with degree c where c is greater than or equal to $2^{i_b - l}$ is, after the multiplication and substitution, dropped to a term of degree $c - 2^{i_b - l}$ in E. Thus, its degree in E is at most $\frac{m'-1}{2} - 1 - 2^{i_b - l}$. By Lucas's Theorem, the next largest degree in (3.17) below $2^{i_b - l}$ is $\frac{m'-1}{2} - 2^{i_b - l}$. To be more specific, since $2^{i_b - l}$ is the largest power of 2 that occurs in the binary expansion of $\frac{m'-1}{2}$, the next largest exponent (composed only of powers of 2 that occur in the binary expansion) in equation (3.17) would be the sum of all other powers of 2 that occur, i.e. $\frac{m'-1}{2} - 2^{i_b - l}$. That next largest exponent then becomes a term of degree $m' - 1 - 2^{i_b - l + 1}$ in E. Since $\frac{m'-1}{2} - 1 - 2^{i_b - l} < m' - 1 - 2^{i_b - l + 1}$, this is the largest degree term in E as the claim stated.

Thus, we have at most $m' - 1 - a$ choices for y_0 and the maximum number of affine singularities for f_+ and h_+ is $(\frac{m'-3}{2})(m' - 1 - a)$.

Next we must calculate the multiplicity of the singular points. Consider

$$f_+(x + x_0, y + y_0) = (x + x_0 + 1)^m + (x + x_0)^m + (y + y_0 + 1)^m + (y + y_0)^m.$$

Recall that the multiplicity of a singular point is the degree of the smallest

nonzero term in the above expression. By the definition of l and Lucas's Theorem, over any extension of $\mathbb{F}_2$, $\binom{m}{q} = 0$ for $1 < q < 2^l$ so there are no nonzero terms with degree between 1 and 2^l. Also, as p is a singular point, it will have multiplicity at least 2. Therefore, the multiplicity is at least 2^l on f_+. Consider the terms of degree $2^l + 1$ in x. They will have the coefficient $(x_0+1)^{m-2^l-1} + x_0^{m-2^l-1}$. Assume for contradiction that this is zero. Then,

$$0 = ((x_0+1)^{m-2^l-1} + x_0^{m-2^l-1})(x_0+1)^{2^l} = x_0^{m-2^l-1}$$

This implies $x_0 = 0$, a contradiction. Thus, the coefficient of x^{2^l+1} is non-zero, and so the multiplicity of (x_0, y_0) is at most $2^l + 1$.

$h_+ = \frac{f_+}{(x+y)(x+y+1)}$ will have at most the same number of singularities as f_+ each with either the same multiplicity as on f_+ or one less.

Next, we will show when the singularities have multiplicity exactly 2^l+1. Recall that $x_0 \neq 0, 1$ and $y_0 \neq 0, 1$. Assume that there are no terms in $f_+(x + x_0, y + y_0)$ of degree 2^l, i.e. that the coefficients of x^{2^l} and y^{2^l} are 0 for some singular point (x_0, y_0). Thus,

$$\begin{aligned} 0 &= ((x_0+1)^{m-2^l} + x_0^{m-2^l}) \\ &= ((x_0+1)^{m-2^l} + x_0^{m-2^l})(x_0+1)^{2^l} \\ &= (x_0+1)^{m-1}(x_0+1) + x_0^{m-2^l}({x_0}^{2^l} + 1) \\ &= x_0^{m-1} + x_0^{m-2^l} = x_0^{m-2^l-1}(x_0^{2^l-1} + 1) \end{aligned}$$

implying $x_0^{2^l-1} = 1$ which is equivalent to $x_0 \in \mathbb{F}_{2^l}^*$. The same must apply to y_0. Every step is reversible, so the implication is if and only if. □

Corollary 2. *The singular points of f_+ all have multiplicity 2^l if and only if $d = gcd(2^l-1, m'-1) = 1$. There are $2(d-1)$ singularities of Type I a and $(d-1)(d-3)$ singularities of Type II a. Therefore, there are at most $(\frac{m'-3}{2})(m'-a-3) - (d-1)(d-3)$ singularities of Type II c.*

Proof. A point (x_0, y_0) is singular if and only if it satisfies the following three equations.

$$(x_0+1)^{\frac{m'-1}{2}} = x_0^{\frac{m'-1}{2}}, \qquad x_0^{\frac{m'-1}{2}} = y_0^{\frac{m'-1}{2}}, \text{ and } \qquad (y_0+1)^{\frac{m'-1}{2}} = y_0^{\frac{m'-1}{2}}$$

Assume first that there exists a singular point (x_0, y_0) with multiplicity of 2^l+1. I shall show the $\gcd(2^l-1, m'-1) > 1$. Lemma 9 shows that a singular point having multiplicity of exactly 2^l+1 implies that $x_0, y_0 \in \mathbb{F}_{2^l}^*$. Thus x_0 also satisfies $x_0^{2^l-1} = 1$ and $(x_0+1)^{2^l-1} = 1$. Note that $x_0 \neq 0, 1$.

Let $j \equiv \frac{m'-1}{2} \bmod (2^l-1)$. Then x_0 must satisfy $(x_0+1)^j = x_0^j$. Divide this by x_0^j to get $(1+\frac{1}{x_0})^j = 1$. Now let $z_0 = \frac{1}{x_0}$ and we can rewrite the equation as $(z_0+1)^j = 1$. Note that $z_0, z_0+1 \in \mathbb{F}_{2^l}^*$ and so $(z_0+1)^{2^l-1} = 1$. Thus the order of z_0+1, $\mathrm{ord}(z_0+1)$, divides 2^l-1 and j. This implies that $\mathrm{ord}(z_0+1) | \frac{m'-1}{2}$. Since the order divides both 2^l-1 and $\frac{m'-1}{2}$, it divides their gcd. However, $\mathrm{ord}(z_0+1) > 1$ and so $\gcd(2^l-1, \frac{m'-1}{2}) > 1$.

Now assume that $\gcd(2^l-1, \frac{m'-1}{2}) = d > 1$. Again, let $j \equiv \frac{m'-1}{2} \bmod (2^l-1)$. Then, $d|j$. Let $w_0 \neq 1$ be an element in the subgroup of order d in $\mathbb{F}_{2^l}^*$. Thus $w_0^j = 1$. Let $z_0 = w_0 + 1$ to get $(1+z_0)^j = 1$. Now let $x_0 = \frac{1}{z_0}$ to get the equation $(1+\frac{1}{x_0})^j = 1$ which is equivalent to $(x_0+1)^j = x_0^j$. This means that our constructed x_0 satisfies the equation for the x-coordinates of singular points. Let $y_0 = x_0$. Then (x_0, y_0) is a singular point of f. As $x_0, y_0 \in \mathbb{F}_{2^l}^*$, this singular point has multiplicity 2^l+1.

We have thus proven the contrapositive of the if and only if statement. Clearly there are only $2(d-1)$ singularities of Type I a as the subgroup of order d in $\mathbb{F}_{2^l}^*$ discussed above has order d and for a given choice of x_0 there are 2 choices for y_0 such that (x_0, y_0) falls on one of the lines $y = x$ and $y = x+1$. Likewise, as there are $d-1$ choices for x_0 and $d-3$ choices for a y_0 that does not satisfy $y = x$ nor $y = x+1$, there are $(d-1)(d-3)$ singularities of Type II a. Given the bound in the total number of affine singularities in Lemma 9, there are at most $(\frac{m'-3}{2})(m'-a-3) - (d-1)(d-3)$ singularities of Type II c. This bound may be able to be improved, but it is sufficient for our purposes. □

Lemma 10. *If $m \equiv 3$ (mod 4), then $\hat{h}_+$ has no singularities at infinity. Otherwise, h_+ has $\frac{m'-1}{2}$ singular points at infinity. Let w be a root of $x^{\frac{m'-1}{2}} = 1$.*

On h_+ the singular point $(w:1:0)$ has multiplicity

$$m_p = \begin{cases} 2^l - 2 & \text{if } w = 1 \text{ (Type III a)} \\ 2^l & \text{if } w \neq 1, w^d = 1 \text{ (Type III b)} \\ 2^l - 1 & \text{else (Type III c)} \end{cases}$$

Proof. First, we will use an unusual projective form of f_+. Let $\hat{j} = (x+z)^m + x^m + (y+z)^m + y^m$. This is the usual projective form of f_+ multiplied by z.

$$\begin{aligned} \frac{\partial \hat{j}}{\partial x} &= (x+z)^{m-1} + x^{m-1} \\ \frac{\partial \hat{j}}{\partial y} &= (y+z)^{m-1} + y^{m-1} \\ \frac{\partial \hat{j}}{\partial z} &= (x+z)^{m-1} + (y+z)^{m-1} \end{aligned}$$

We are only interested in singular points at infinity so for $(x_0 : y_0 : z_0)$, we may assume $z_0 = 0$. Also, as $y_0 = 0$ implies $x_0 = 0$, we may assume $y_0 \neq 0$ and scale so that $y_0 = 1$. Under these simplifications, $\frac{\partial \hat{j}}{\partial x} = 0$, $\frac{\partial \hat{j}}{\partial y} = 0$ and $\frac{\partial \hat{j}}{\partial z} = x_0^{m-1} + 1$. We may take the 2^lth root of this last equation so it becomes $x_0^{\frac{m'-1}{2}} = 1$.

Clearly, as $\frac{m'-1}{2}$ is odd, there are exactly $\frac{m'-1}{2}$ roots to this. There is one special root out of these, $x_0 = 1$, as this is the only root on the lines $y = x$ and $y = x + z$, and it is on both.

For multiplicity, dehomogenize $\hat{f}_+$ relative to y. Redefine x as $\frac{x}{y}$ and z as $\frac{z}{y}$. Now shift by $(x_0, 0)$ to get

$$\tilde{f}_+(x + x_0, z + 0) = \frac{(x + x_0 + z)^m + (x + x_0)^m + (z+1)^m + 1}{z}.$$

There are no non-zero terms of degree q in the numerator where $q < 2^l$ as $\binom{m}{q} = 0$. Consider the terms of degree $2^l - 1$ (they have degree 2^l in the numerator)

$$\frac{\binom{m}{2^l}(x+z)^{2^l} x_0^{m-2^l} + \binom{m}{2^l} x^{2^l} x_0^{m-2^l} + \binom{m}{2^l} z^{2^l}}{z} = z^{2^l - 1}(x_0^{m-2^l} + 1).$$

This term is zero if and only if ${x_0}^{m-2^l} = 1$ if and only if ${x_0}^{\gcd(m-2^l, m-1)} = 1$ if

and only if ${x_0}^d = 1$.

If $d = 1$, then only the point $(1 : 1 : 0)$ has multiplicity greater than $2^l - 1$. All the rest have multiplicity exactly $2^l - 1$. In the case $(1 : 1 : 0)$, looking at the terms of degree 2^l in $\tilde{f}_+(x + 1, z)$, we can see it has multiplicity 2^l on $\tilde{f}_+$.

$$\frac{(x+z)^{2^l+1}(1) + x^{2^l+1} + z^{2^l+1}}{z} = x^{2^l} + xz^{2^l-1} \neq 0$$

If $d > 1$ then for the d numbers that satisfy ${x_0}^d = 1$, the points $(x_0 : 1 : 0)$ have multiplicity greater than $2^l - 1$. The others have multiplicity exactly $2^l - 1$.

To show that the points with ${x_0}^d = 1$ have multiplicity 2^l, look at the the terms of degree 2^l in $\tilde{f}_+(x + x_0, z)$:

$$\frac{(x+z)^{2^l+1}x_0^{m-2^l-1} + x^{2^l+1}x_0^{m-2^l-1} + z^{2^l+1}}{z}$$

$$= x^{2^l}{x_0}^{m-2^l-1} + xz^{2^l-1}{x_0}^{m-2^l-1} + z^{2^l}(1 + {x_0}^{m-2^l-1}) \neq 0 \text{ as } x_0 \neq 0.$$

Thus, the multiplicity of these points is exactly 2^l on $\tilde{f}_+$.

This describes the singular points of f_+ at infinity. $\hat{h}_+ = \frac{\hat{f}_+}{(x+y)(x+y+z)}$, and the only singular point at infinity on the two projective lines $x + y$ and $x + y + z$ is $(1 : 1 : 0)$. Thus all the other singular points at infinity have the same multiplicity on $\hat{h}_+$ except $(1 : 1 : 0)$ has multiplicity 2 less.

The last case is when $m \equiv 3 \pmod 4$. Here, $d = 1$ and the work above shows that all the singular points of f have multiplicity at most $2^l - 1$ on $\hat{h}_+$ which is 1 (i.e. nonsingular) as $l = 1$. Thus there are no singular points at infinity in this case. □

3.3 I_p Bounds of Singularities of h_+

To calculate the intersection number of a singularity we need to know the tangent lines. These are the factors of $H_{m_p(h)}$ as discussed in Definition 4.

Lemma 11. *Let $p = (x_0, y_0)$ be a singular point of h_+ which is on one of the lines $y = x$ and $y = x + 1$. Then $F_{m_p+2} = H_{m_p+1}(x + y) + H_{m_p}(x + y)^2$ and*

$F_{m_p+1} = H_{m_p}(x+y)$. *Also, the tangent lines to* h *at* p *are the factors of* $\frac{(x^{m_p+1}+y^{m_p+1})}{(x+y)}$, *where* m_p *is the multiplicity of* p *on* h_+.

Proof. The tangent lines to h_+ at p are the factors of the homogeneous polynomial, H_{m_p}, composed of the lowest degree terms of $h_+(x + x_0, y + y_0)$.

Write $h_+(x+x_0, y+y_0) = R+H_{m_p+1}+H_{m_p}$ where R is the polynomial composed of the terms of degree greater than $m_p + 1$. Then,

$$\begin{aligned} f_+(x + x_0, y + y_0) &= h_+(x + x_0, y + y_0)[((x + x_0 + y + y_0)(x + x_0 + y + y_0 + 1))] \\ &= [R + H_{m_p+1} + H_{m_p}][(x + y)^2 + (x + y)] \\ &= [R\{(x + y)^2 + (x + y)\} + H_{m_p+1}(x + y)^2] + \\ &\quad + [H_{m_p+1}(x + y) + H_{m_p}(x + y)^2] + [H_{m_p}(x + y)]. \end{aligned}$$

The terms of degree m_p+2 in $f(x+x_0, y+y_0)$ are the terms in the second set of brackets in the last equation. Thus, $F_{m_p+2} = H_{m_p+1}(x+y)+H_{m_p}(x+y)^2$. The terms of degree $m_p + 1$ are those in the last set of brackets, and thus $F_{m_p+1} = H_{m_p}(x+y)$.

The lowest degree terms of $f_+(x+x_0, y+y_0)$ must be of the form $b_1x^{m_p+1}+b_2y^{m_p+1}$ for constants b_1, b_2 constants. However, since the terms must be divisible by $(x+y)$, clearly $b_1 = b_2 \neq 0$. Thus, $H_{m_p} = \frac{b_1(x^{m_p+1}+y^{m_p+1})}{(x+y)}$ and so the tangent lines to h_+ at p are the factors of $\frac{(x^{m_p+1}+y^{m_p+1})}{(x+y)}$. □

Corollary 3. *For Type I a singularities,* $I_p(u, v) \leq (2^{l-1})^2$.

Proof. These singular points have multiplicity 2^l on h_+ and $x_0, y_0 \in \mathbb{F}^*_{2^l}$. Lemma 11 shows that the tangent lines to h_+ at p are the factors of $\frac{(x^{2^l+1}+y^{2^l+1})}{(x+y)}$ which are all distinct. Recall from the background material section that when the tangent lines are all distinct then the intersection multiplicity of that point is the product of the singularity multiplicities, $m_p(u)$ and $m_p(v)$, of the two factors. Since the sum of their singularity multiplicities is 2^l, their product is bounded above by $(\frac{2^l}{2})^2$. Therefore, $I_p(u, v) \leq (2^{l-1})^2$. □

Corollary 4. *For Type I b singularities,* $I_p(u, v) = 0$.

Proof. By Lemma 9 and Corollary 2, Type I b singularities have multiplicity $2^l - 1$ on h_+. By Lemma 11, the tangent lines of h_+ at an affine singular point $p = (x_0, y_0)$ are the factors of $(x+y)^{2^l-1}$. From Lemma 9, $H_{2^l} \neq 0$ as $x_0, y_0 \notin \mathbb{F}_{2^l}^*$. We already know $H_{2^l-1} = b_1(x+y)^{2^l-1}$ for some constant b_1. By Lemma 11, $F_{2^l+1} = H_{2^l}(x+y) + H_{2^l-1}(x+y)^2$. Thus, $\gcd(H_{m_p+1}, H_{m_p}) = \gcd(H_{2^l}, H_{2^l-1}) = \gcd(H_{2^l} + H_{2^l-1}(x+y), H_{2^l-1}) = \gcd\left(\frac{F_{2^l+1}}{(x+y)}, H_{2^l-1}\right)$. From $f_+(x+x_0, y+y_0)$, we can easily calculate F_{2^l+1}.

$$f_+(x+x_0, y+y_0) = (x+(x_0+1))^m + (x+x_0)^m + (y+(y_0+1))^m + (y+y_0)^m$$

$$\begin{aligned} F_{2^l+1} &= x^{2^l+1}(x_0+1)^{m-2^l-1} + x^{2^l+1}x_0^{m-2^l-1} + y^{2^l+1}(y_0+1)^{m-2^l-1} + y^{2^l+1}y_0^{m-2^l-1} \\ &= [(x_0+1)^{m-2^l-1} + x_0^{m-2^l-1}](x^{2^l+1} + y^{2^l+1}) \end{aligned}$$

as either $y_0 = x_0$ or $y_0 = x_0 + 1$. Let $c = [(x_0+1)^{m-2^l-1} + x_0^{m-2^l-1}]$ and $c \neq 0$ as $F_{2^l+1} \neq 0$. Thus, $F_{2^l+1} = c[x^{2^l+1} + y^{2^l+1}]$.

Note that since $H_{2^l-1} = b_1(x+y)^{2^l-1}$, we know that $\gcd\left(\frac{F_{2^l+1}}{(x+y)}, H_{2^l-1}\right) = 1$.

Therefore, by Lemma 1 since $\gcd(H_{m_p}, H_{m_p+1}) = 1$ and there is only one tangent direction at p, $I_p(u,v) = 0$ for all affine singular points p of Type I b. □

Lemma 12. *Let p be a singular point of h_+ which is on neither of the lines $y = x$ and $y = x+1$. Then, $F_{m_p} = cH_{m_p}$ and $F_{m_p+1} = cH_{m_p+1} + H_{m_p}(x+y)$ where $c = (x_0+y_0)(x_0+y_0+1)$.*

Proof. Write $h_+(x+x_0, y+y_0) = R + H_{m_p+1} + H_{m_p}$ where R is the polynomial composed of all the terms of degree greater than $m_p + 1$. Then,

$$\begin{aligned} f_+(x+x_0, y+y_0) &= h_+(x+x_0, y+y_0)[(x+x_0+y+y_0)(x+x_0+y+y_0+1)] \\ &= [R + H_{m_p+1} + H_{m_p}][(x+y)^2 + (x+y) + c] \\ &= \{R[(x+y)^2 + (x+y) + c] + H_{m_p+1}[(x+y)^2 + (x+y)] + \\ &\quad + H_{m_p}[(x+y)^2]\} + \{cH_{m_p+1} + H_{m_p}[x+y]\} + cH_{m_p} \end{aligned}$$

Note that the terms in the last set of braces compose the polynomial F_{m_p+1}, and $F_{m_p} = cH_{m_p}$. □

Corollary 5. *For Type II a singularities,* $I_p(u,v) \leq (2^{l-1})(2^{l-1}+1)$.

Proof. These singular points have multiplicity 2^l+1 on h_+ and $x_0, y_0 \in \mathbb{F}_{2^l}^*$. From Lemma 12, $cH_{m_p} = F_{m_p}$ implying the tangent lines to h_+ at p are the same as f_+ at p. The lowest degree terms of f_+ must be of the form $c_1x^{m_p} + c_2y^{m_p}$ for some constants c_1, c_2. As $m_p = 2^l+1$, the tangent lines are all distinct. Therefore, $I_p(u,v) \leq (2^{l-1})(2^{l-1}+1)$. □

Corollary 6. *For Type II b singularities,* $I_p(u,v) = 0$.

Proof. These singular points have multiplicity 2^l on h_+ and without loss of generality (by the symmetry of x and y) we may assume that $y_0 \in \mathbb{F}_{2^l}^*$ but x_0 is not. From Lemma 12, $cH_{m_p} = F_{m_p}$ implying the tangent lines to h_+ at p are the same as f_+ at p. The lowest degree terms of f_+ must be of the form $c_1x^{m_p} + c_2y^{m_p}$ for some constants c_1, c_2. As $y_0 \in \mathbb{F}_{2^l}^*$ then $c_2 = 0$ from the proof of Lemma 9; see the discussion as to when the coefficients of x^{2^l} and y^{2^l} are zero. Thus, the tangent lines are 2^l copies of x.

However, by Lemma 9, $F_{2^l+1} = c_1x^{2^l+1} + c_2y^{2^l+1}$ for some $c_1, c_2 \neq 0$. Thus

$$1 = \gcd(F_{2^l+1}, F_{2^l}) = \gcd(cH_{2^l+1} + H_{2^l}(x+y), cH_{2^l}) = \gcd(H_{2^l+1}, H_{2^l}).$$

Therefore Lemma 1 implies $I_p = 0$. □

Lemma 13. *For Type II c singularities,* $I_p(u,v) \leq 2^l$. *If* $l = 1$, *then* $I_p(u,v) = 0$. *Also, there are at most* $\left(\frac{m'-3}{2}\right)(2^l-2)(2^l+1) - (d-1)(d-3)$ *of these singularities with nonzero intersection number.*

Proof. As $y_0 \neq x_0, x_0+1$, then $p = (x_0, y_0)$ has multiplicity of 2^l on both f_+ and on h_+. The lowest degree terms of f_+ must be of the form $c_1x^{m_p} + c_2y^{m_p}$ for some constants c_1, c_2 and $m_p = 2^l$. As the multiplicity is 2^l, Lemma 9 shows that $x_0, y_0 \notin \mathbb{F}_{2^l}^*$. The proof of that lemma actually proves the stronger result that the

coefficients c_1 and c_2 are nonzero. As $m_p = 2^l$, the tangent lines are 2^l copies of the same line $c_3x + c_4y$.

From Lemma 12 and the proof of Corollary 6, $\gcd(H_{2^l}, H_{2^l+1}) = \gcd(F_{2^l}, F_{2^l+1})$. Now,

$$\begin{aligned} F_{2^l+1} &= [(x_0+1)^{m-2^l-1} + x_0^{m-2^l-1}]x^{2^l+1} + [(y_0+1)^{m-2^l-1} + y_0^{m-2^l-1}]y^{2^l+1} \\ &= c_1x^{2^l+1} + c_2y^{2^l+1} \\ F_{2^l} &= [(x_0+1)^{m-2^l} + x_0^{m-2^l}]x^{2^l} + [(y_0+1)^{m-2^l} + y_0^{m-2^l}]y^{2^l} = d_1x^{2^l} + d_2y^{2^l} \end{aligned}$$

Now the factors of F_{2^l+1} are equivalent to the factors of $(c_3z)^{2^l+1}+1$ where $z = \frac{x}{y}$ and $c_3 = \sqrt[2^l+1]{\frac{c_1}{c_2}}$. The factors of F_{2^l} are equivalent to the factors of $(d_3z)^{2^l}+1$ where $d_3 = \sqrt[2^l]{\frac{d_1}{d_2}}$.

The only factor they could have in common then is d_3z+1 (equivalently, d_3x+y). By Lemma 14 below, they have this factor in common precisely when the singular point $p = (x_0, y_0)$ satisfies

$$(x_0+1)^{2^l}y_0(y_0^{2^l-1}+1)^{2^l+1} = (y_0+1)^{2^l}x_0(x_0^{2^l-1}+1)^{2^l+1} \tag{3.18}$$

If $l = 1$, then p cannot satisfy equation (3.18) as $y_0 \neq x_0$ and $y_0 \neq x_0 + 1$. Therefore $\gcd(F_{2^l+1}, F_{2^l}) = 1$ which implies $\gcd(H_{2^l+1}, H_{2^l}) = 1$. As there is only one tangent direction at p, $I_p(u, v) = 0$ by Lemma 1.

If $l > 1$, then there may exist singular points off of the lines $y = x, y = x+1$ that satisfy equation (3.18) above. From Lemma 15 below, we can bound the intersection number of these singular points by 2^l. Also there are at most $\binom{m'-3}{2}(2^l-2)(2^l+1)$ singularities with nonzero intersection number that satisfy equation (3.18). However, if $x_0, y_0 \in \mathbb{F}_{2^l}^*$, we get a solution to equation (3.18), and there are $(d-1)(d-3)$ such solutions. As $x_0, y_0 \notin \mathbb{F}_{2^l}^*$, we can actually bound the number of these singularities with nonzero intersection number by $\binom{m'-3}{2}(2^l-2)(2^l+1)-(d-1)(d-3)$. □

Lemma 14. *The polynomials $S = c_1x^{2^l+1}+c_2y^{2^l+1}$ and $T = d_1x^{2^l}+d_2y^{2^l}$ as defined in Lemma 13 have a common factor precisely when there exists a singular point (x_0, y_0) of f_+ that satisfies $(x_0+1)^{2^l}y_0(y_0^{2^l-1}+1)^{2^l+1} = (y_0+1)^{2^l}x_0(x_0^{2^l-1}+1)^{2^l+1}$.*

Proof. Singular points satisfy the equations

$$x_0^{m-1} = y_0^{m-1} \tag{3.19}$$
$$(x_0+1)^{m-1} = x_0^{m-1} \tag{3.20}$$
$$(y_0+1)^{m-1} = y_0^{m-1} \tag{3.21}$$

Since T is just 2^l copies of the same line, S and T have a common line if and only if $\sqrt[2^l]{T}$ is also a factor of S. This is equivalent to

$$\left(\frac{c_1}{c_2}\right)^{2^l} = \left(\frac{d_1}{d_2}\right)^{2^l+1}. \tag{3.22}$$

From the proof of Lemma 13, we have that $c_1 = (x_0+1)^{m-2^l-1} + x_0^{m-2^l-1}$ and $c_2 = (y_0+1)^{m-2^l-1} + y_0^{m-2^l-1}$. Using equations (3.20) and (3.21), we can easily write them as $c_1 = \frac{x_0^{m-2^l-1}}{(x_0+1)^{2^l}}$ and $c_2 = \frac{y_0^{m-2^l-1}}{(y_0+1)^{2^l}}$. Thus,

$$\begin{aligned}\frac{c_1}{c_2} &= \frac{x_0^{m-2^l-1}(y_0+1)^{2^l}}{y_0^{m-2^l-1}(x_0+1)^{2^l}} = \frac{x_0^{m-2^l-1}(y_0+1)^{2^l}x_0^{2^l}y_0^{2^l}}{y_0^{m-2^l-1}(x_0+1)^{2^l}x_0^{2^l}y_0^{2^l}} \\ &= \frac{x_0^{m-1}(y_0+1)^{2^l}y_0^{2^l}}{y_0^{m-1}(x_0+1)^{2^l}x_0^{2^l}} = \frac{(y_0+1)^{2^l}y_0^{2^l}}{(x_0+1)^{2^l}x_0^{2^l}}\end{aligned}$$

Next, from the proof of Lemma 13, $d_1 = (x_0+1)^{m-2^l} + x_0^{m-2^l}$. We can rewrite it as

$$d_1 = [(x_0+1)^{m-2^l} + x_0^{m-2^l}]\frac{(x_0+1)^{2^l}}{(x_0+1)^{2^l}} = \frac{(x_0+1)(x_0+1)^{m-1} + x_0^{m-2^l}(x_0+1)^{2^l}}{(x_0+1)^{2^l}}$$

$$= \frac{(x_0+1)x_0^{m-1} + x_0^{m-2^l}(x_0^{2^l}+1)}{(x_0+1)^{2^l}} = \frac{x_0^{m-1} + x_0^{m-2^l}}{(x_0+1)^{2^l}} = \frac{x_0^{m-2^l}(x_0^{2^l-1}+1)}{(x_0+1)^{2^l}}$$

Similarly $d_2 = \frac{y_0^{m-2^l}(y_0^{2^l-1}+1)}{(y_0+1)^{2^l}}$. Thus,

$$\frac{d_1}{d_2} = \frac{x_0^{m-2^l}(x_0^{2^l-1}+1)(y_0+1)^{2^l}}{y_0^{m-2^l}(y_0^{2^l-1}+1)(x_0+1)^{2^l}} \frac{(x_0^{2^l-1}y_0^{2^l-1})}{(x_0^{2^l-1}y_0^{2^l-1})} = \frac{(x_0^{2^l-1}+1)(y_0+1)^{2^l}y_0^{2^l-1}}{(y_0^{2^l-1}+1)(x_0+1)^{2^l}x_0^{2^l-1}}$$

Substituting what we know into equation (3.22) gives the equivalent

$$\frac{y_0^{2^{2l}}(y_0+1)^{2^{2l}}}{x_0^{2^{2l}}(x_0+1)^{2^{2l}}} = \frac{y_0^{(2^{2l}-1)}(y_0+1)^{(2^{2l}+2^l)}(x_0^{2^l-1}+1)^{(2^l+1)}}{x_0^{(2^{2l}-1)}(x_0+1)^{(2^{2l}+2^l)}(y_0^{2^l-1}+1)^{(2^l+1)}}$$

which, as desired, simplifies to

$$(x_0+1)^{2^l}y_0(y_0^{2^l-1}+1)^{2^l+1} = (y_0+1)^{2^l}x_0(x_0^{2^l-1}+1)^{2^l+1}. \tag{3.23}$$

□

Lemma 15. *Let everything be defined as in Lemma 13. If $p = (x_0, y_0)$ is a singular point of f_+ off of the lines $y = x$, $y = x + 1$ which satisfies equation (3.23) from Lemma 14, then the intersection number is bounded above by 2^l, i.e. $I_p(u, v) \leq 2^l$.*

Proof. Note $m_p = 2^l$, the multiplicity of p on h_+ and f_+. Let r and s be the degree of the lowest degree terms of $U = u(x + x_0, y + y_0)$ and $V = v(x + x_0, y + y_0)$ respectively. Recall H_i is the polynomial composed of the terms of $h(x+x_0, y+y_0)$ of degree i. Define F_i, U_i and V_i similarly.

From previous work we can summarize the following:

$$H_{m_p} + H_{m_p+1} + H_{m_p+2} + ... = (U_r + U_{r+1} + U_{r+2} + ...)(V_s + V_{s+1} + V_{s+2} + ...)$$

If r or s is 0, then U or V does not contain p and $I_p(u, v) = 0$. As p satisfies equation (3.23) from Lemma 14, F_{m_p} and F_{m_p+1} have a line in common; call that line t.

$$F_{m_p} = \alpha_1(H_{m_p}) = d_1x^{2^l} + d_2y^{2^l}$$

$$F_{m_p+1} = \alpha_1(H_{m_p+1}) + (x + y)H_{m_p} = c_1x^{2^l+1} + c_2y^{2^l+1}$$

where α_1 is a constant.

Thus, $H_{m_p} = U_r V_s = t^{2^l}$ and $H_{m_p+1} = U_r V_{s+1} + U_{r+1} V_s$.

Note that $\gcd(F_{m_p}, F_{m_p+1}) = t$ implying that $\gcd(H_{m_p}, H_{m_p+1}) = t$ by the proof of Corollary 6. As the degrees of U_r and V_s are both positive and $U_r V_s = t^{2^l}$, then $t|U_r$ and $t|V_s$. Therefore, $\gcd(U_r, V_s) \geq t$. However, $\gcd(U_r, V_s) > t$ would imply that $\gcd(H_{m_p}, H_{m_p+1}) > t$, a contradiction, and thus $\gcd(U_r, V_s) = t$. Without loss of generality, we may thus assume that $V_s = t$ (and so $s = 1$) and that $U_r = t^{2^l-1}$ (so that $r = 2^l - 1$).

Since $t^2 \nmid H_{m_p+1}$ then $t \nmid U_{r+1}$ implying as well that $U_{r+1} \neq 0$.

As $s = 1$, p is a simple point on V, hence by Fulton [11] (page 81), $I_p(U, V) = \mathrm{ord}_p^V(U)$ in the discrete valuation ring $O_p(V)$. Any line not tangent to H at p can be taken as a uniformizing parameter, let us pick x. Note that if $\mathrm{ord}(\alpha) < \mathrm{ord}(\beta)$ then $\mathrm{ord}(\alpha + \beta) = \mathrm{ord}(\alpha)$.

First, $\mathrm{ord}(U_r) = \mathrm{ord}(U_{2^l-1}) = \mathrm{ord}(t^{2^l-1}) > 2^l$ as $\mathrm{ord}(t) \geq 2$. Second, let us write U_{2^l} as $\prod_{j=1}^{2^l}(\alpha_j x + \beta_j t) = \alpha x^{2^l} + O(x^{2^l+1})$ where $\alpha = \prod \alpha_j \neq 0$. We can do this as $t \nmid U_{2^l}$. Clearly, the order of $U_{2^l} = 2^l$. Any higher degree terms of U will have larger order and thus $I_p(U, V) = \mathrm{ord}(U) = 2^l$ as desired. □

Lemma 16. *The tangent lines of h_+ at a singular point at infinity, $p = (w : 1 : 0)$ for $w \neq 1$ are the factors of the lowest degree terms of f_+, i.e. $F_{m_p} = (w+1)^2 H_{m_p}$. Also, $F_{m_p+1} = H_{m_p+1}(w+1)^2 + H_{m_p} z(w+1)$. In the case $w = 1$, the tangent lines are the factors of the lowest degree terms of f_+ divided by $(x)(x+z)$, i.e. $H_{m_p} = \frac{F_{m_p+2}}{x(x+z)}$, where m_p is the multiplicity of p on $\tilde{h}_+$.*

Proof. Recall w is a root of $x^{\frac{m'-1}{2}} = 1$. The tangent lines of h_+ at p are the factors of H_{m_p}. Write $\tilde{H}_+ = \tilde{h}_+(x + w, z) = R + \tilde{H}_{m_p+1} + \tilde{H}_{m_p}$ where R is the polynomial composed of all of the terms of degree greater than $m_p + 1$. Then,

$$\begin{aligned}
\tilde{F}_+ &= \tilde{H}_+[(x + w + 1)(x + z + w + 1)] \\
&= [R + \tilde{H}_{m_p+1} + \tilde{H}_{m_p}][x(x + z) + z(w + 1) + (w + 1)^2] \\
&= \{R[x(x + z) + z(w + 1) + (w + 1)^2] + \tilde{H}_{m_p+1}[x(x + z) + z(w + 1)] + \\
&\quad + \tilde{H}_{m_p}[x(x + z)]\} + \{\tilde{H}_{m_p+1}[(w + 1)^2] + \tilde{H}_{m_p}[z(w + 1)]\} + \tilde{H}_{m_p}[(w + 1)^2]
\end{aligned}$$

If $w \neq 1$, then note that the terms in the second set of braces of the last equation compose $\tilde{F}_{m_p+1}$ so $\tilde{F}_{m_p+1} = \tilde{H}_{m_p+1}(w+1)^2 + \tilde{H}_{m_p} z(w+1)$. Also, $\tilde{F}_{m_p} = (w+1)^2 \tilde{H}_{m_p}$.

In the case $w = 1$ then

$$\tilde{F}_+ = \tilde{H}_+[(x+w+1)(x+z+w+1)] = \tilde{H}_+[x(x+z)]$$

and so the terms of lowest degree in h_+ are the terms of lowest degree (m_p+2) in f_+ divided by $(x)(x+z)$, i.e. $H_{m_p} = \frac{F_{m_p+2}}{x(x+z)}$. □

Recall that if $m \equiv 3 \pmod 4$ then there are no singular points at infinity.

Corollary 7. *For Type III a singularities,* $I_p(u,v) \leq \left(\frac{2^l-2}{2}\right)^2$.

Proof. Here $p = (1:1:0)$ which has multiplicity of 2^l on $\tilde{f}_+$ and $2^l - 2$ on $\tilde{h}_+$. The terms of degree $m_p = 2^l - 2$ in $\tilde{h}_+$ are $\frac{x^{2^l} + xz^{2^l-1}}{x(x+z)} = \frac{x^{2^l-1} + z^{2^l-1}}{(x+z)}$ by Lemma 16. The factors of this are all distinct and so $I_p(u,v) \leq \left(\frac{2^l-2}{2}\right)^2$. □

Corollary 8. *For Type III b singularities,* $I_p(u,v) \leq (2^{l-1})^2$.

Proof. For singular points $p = (w:1:0)$ where w is a root of $x^{\frac{m'-1}{2}} = 1$ such that $w^d = 1, w \neq 1$. p has multiplicity 2^l on $\tilde{f}_+$ and $\tilde{h}_+$. The tangent lines to $\tilde{f}_+$ are the factors of

$$x^{2^l} w^{m-2^l-1} + xz^{2^l-1} w^{m-2^l-1} + z^{2^l}(1 + w^{m-2^l-1}).$$

It is easy to check that all the roots of this polynomial are distinct hence the tangent lines are all distinct. From Lemma 16, the tangents lines to $\tilde{f}_+$ and $\tilde{h}_+$ are the same. Therefore, $I_p \leq (2^{l-1})^2$. □

Corollary 9. *For Type III c singularities,* $I_p(u,v) = 0$.

Proof. Here $p = (w:1:0)$ where w is a root of $x^{\frac{m'-1}{2}} = 1$ such that $w^d \neq 1$. They have multiplicity $m_p = 2^l - 1$ and $\tilde{F}_{2^l-1} = z^{2^l-1}(1 + w^{m-2^l})$ by the proof of Lemma 10. Thus, the tangent lines are all z.

$\gcd(\tilde{H}_{2^l}, \tilde{H}_{2^l-1}) = \gcd(\tilde{H}_{2^l}(w+1)^2 + \tilde{H}_{2^l-1}(z)(w+1), \tilde{H}_{2^l-1}) = \gcd(\tilde{F}_{2^l}, \tilde{F}_{2^l-1})$ by Lemma 16. As $\tilde{F}_{2^l-1} = cz^{2^l-1}$ for some constant c, so $\gcd(\tilde{F}_{2^l}, \tilde{F}_{2^l-1}) = 1$ if and only if $z \nmid \tilde{F}_{2^l}$. From the proof of Lemma 10 as

$$\tilde{F}_{2^l} = x^{2^l} w^{m-2^l-1} + xz^{2^l-1} w^{m-2^l-1} + z^{2^l+1}(1 + w^{m-2^l-1})$$

clearly $z \nmid \tilde{F}_{2^l}$. Thus, Lemma 1 implies that $I_p(u, v) = 0$. □

3.4 Proof of Theorem 1

The following two theorems, Theorem 8 and Theorem 9, when combined give the main result, Theorem 1.

Theorem 8. *If $d = 1$, then h_+ has an absolutely irreducible factor defined over $\mathbb{F}_2$.*

Proof. First, assume for contradiction that h_+ has no absolutely irreducible factors over $\mathbb{F}_2$. As $\deg(h_+) = m - 3$, Lemma 5 implies that $e = \frac{I_{tot}}{\frac{(m-3)^2}{4}} \geq \frac{8}{9}$ where I_{tot} is any upper bound on the global intersection number of u and v for all factorizations $h = u \cdot v$ over the algebraic closure of $\mathbb{F}_2$. We need to calculate an estimate to use for I_{tot}.

If $m \equiv 3 \pmod 4$, then $l = 1$ and the only singularities are those of Type I b and Type II c. Thus $\sum_p I_p(u, v) = 0$ where the sum runs over all projective points. Clearly, as $I_{tot} = 0$, we get a contradiction. Thus, in the case that $m \equiv 3 \pmod 4$, h is absolutely irreducible. Therefore we just consider the case $m \equiv 1 \pmod 4$ and so $l > 1$.

As $d = 1$ by assumption, Theorem 7 and Corollary 2 shows that there are only 4 types of singularities possible, Types I b, II c, III a and III c.

Therefore, Theorem 7 gives us the bound $\sum_p I_p(u, v) \leq (2^{l-1}-1)^2 + 2^l(\frac{m'-3}{2})(m' - a - 3)$ where the sum runs over all projective points.

Now assume for simplicity that $m > 20$ (we can check by hand all m less than this). We shall work towards a contradiction using the fact that $e \geq \frac{8}{9}$. Recall that $e = \frac{I_{tot}}{\frac{(m-3)^2}{4}}$ where I_{tot} is now the bound $(2^{l-1} - 1)^2 + 2^l(\frac{m'-3}{2})(m' - a - 3)$.

We know that $\frac{m-1}{2^l} \geq 3$ since $m \neq 2^j + 1$ for any j and 2^l is precisely the power of 2 that divides $m - 1$. Thus $\frac{m-1}{6} \geq 2^{l-1} > 2^{l-1} - 1$ implying $(2^{l-1} - 1)^2 < \frac{(m-1)^2}{36}$.

$$\begin{aligned} e &= \frac{(2^{l-1}-1)^2 + 2^l(\frac{m'-3}{2})(m'-a-3)}{\frac{(m-3)^2}{4}} < \frac{\frac{(m-1)^2}{36} + (m-3)(m'-a-3)}{\frac{(m-3)^2}{4}} \\ &< \frac{\frac{(m-1)^2}{9} + 4(m-3)(\frac{(m'-1)}{2}-1)}{(m-3)^2} \leq \frac{1}{7} + 2\frac{(m'-3)}{(m-3)} \end{aligned}$$

with the $\frac{1}{7}$ coming from the fact that for $m > 20$, $\frac{(m-1)^2}{9(m-3)^2} \leq \frac{1}{7}$. Note that we also used that $m' - a - 3 \leq \frac{m'-1}{2} - 1$ where a is the largest power of 2 less than m', i.e. $a = 2^{\lfloor \log_2(m') \rfloor}$.

Now as $m \geq m'$, $e < \frac{1}{7} + 2\frac{(m'-1)}{(m-1)}$ yielding our final estimate of

$$e < \frac{1}{7} + \frac{1}{2^{l-2}}$$

For $l \geq 3$, then $e < .65 < \frac{8}{9}$, a contradiction! Therefore, we are left with the case $l = 2$.

To show that $l = 2$ also leads to a contradiction, we need to change the way we are counting the number of singular points. From Lemma 13, we can bound the number of points of Type II c by $\left(\frac{m'-3}{2}\right)(2^l-2)(2^l+1)$ instead of $\left(\frac{m'-3}{2}\right)(m'-a-3)$. This version of counting gives us a bound on the global intersection number of $\sum I \leq (2^{l-1}-1)^2 + 2^l(\frac{m'-3}{2})(2^l-2)(2^l+1)$.

Thus,

$$e = \frac{(2^{l-1}-1)^2 + 2^l(\frac{m'-3}{2})(2^l-2)(2^l+1)}{\frac{(m-3)^2}{4}} < \frac{(2^{l-1}-1)^2 + (m-3)(2^l-2)(2^l+1)}{\frac{(m-3)^2}{4}}.$$

Substitute in $l = 2$ and simplify.

$$e < \frac{4 + 40(m-3)}{(m-3)^2} < \frac{8}{9}$$

with the last inequality holding when $m > 48$. This gives us our contradiction in the case $l = 2$ and $m > 48$. We can easily check by hand or computer that for all $m \leq 48$ where $l = 2$ and $d = 1$ (i.e. $m = 21, 29, 45$) h_+ is absolutely irreducible. Thus h_+ must have an absolutely irreducible factor over $\mathbb{F}_2$ in the case that $d = 1$. $\square$

Theorem 9. *h_+ has an absolutely irreducible factor defined over $\mathbb{F}_2$ provided $1 < d < \frac{m'-1}{2}$.*

Proof. First, assume for contradiction that h_+ has no absolutely irreducible factors over $\mathbb{F}_2$. As $\deg(h_+) = m-3$, Lemma 5 implies that $e = \frac{I_{tot}}{\frac{(m-3)^2}{4}} \geq \frac{8}{9}$ where I_{tot} is any upper bound on the global intersection number of u and v for all factorizations $h = u \cdot v$ over the algebraic closure of $\mathbb{F}_2$. We need to calculate an estimate for I_{tot}.

From Theorem 7, we have five types of affine singularities. All five may occur on h_+ and thus the sum of the intersection numbers at all affine singularities is bounded above by $2(d-1)(2^{l-1})^2 + (d-1)(d-3)(2^{l-1})(2^{l-1}+1) + 2^l((\frac{m'-3}{2})(m'-a-3) - (d-1)(d-3))$.

Again using the chart in Theorem 7, the sum of the intersection numbers at infinity is bounded above by $(2^{l-1}-1)^2 + (d-1)(2^{l-1})^2$.

Thus we get a bound on the global intersection number.

$$\sum_p I_p(u,v) \leq 2(d-1)(2^{l-1})^2 + (d-1)(d-3)(2^{l-1})(2^{l-1}+1) +$$

$$+2^l\left(\left(\frac{m'-3}{2}\right)(m'-a-3) - (d-1)(d-3)\right) + (2^{l-1}-1)^2 + (d-1)(2^{l-1})^2$$

Since we are assuming $1 < d < \frac{m'-1}{2}$ and $d = \gcd(\frac{m'-1}{2}, 2^l - 1)$ is a divisor of $\frac{m'-1}{2}$, then $m' \geq 19$. Also, as $d > 1$, $l \geq 2$. Note that this implies that $m \geq 37$. Now, we shall work towards a contradiction using the fact that $e \geq \frac{8}{9}$. Recall that $e = \frac{I_{tot}}{\frac{(m-3)^2}{4}}$ where I_{tot} is now the global intersection bound listed above.

Simplifying e we get that

$$e = \frac{2^{l-1}[(m'-3)(m'-a-3) - 2(d-1)(d-3)] + 3(d-1)(2^{l-1})^2}{\frac{(2^{l-1}(m'-1)-2)^2}{4}} +$$

$$+\frac{(d-1)(d-3)(2^{l-1})(2^{l-1}+1) + (2^{l-1}-1)^2}{\frac{(2^{l-1}(m'-1)-2)^2}{4}}$$

Now define $\hat{e}$ as

$$\hat{e} = \frac{2^{l-1}[(m'-3)(m'-a-3)-2(d-1)(d-3)]+3(d-1)(2^{l-1})^2}{\frac{(2^{l-1}(m'-1)-2)^2}{4}}+$$

$$+\frac{(d-1)(d-3)(2^{l-1})(2^{l-1}+1)+(2^{l-1})^2}{\frac{(2^{l-1}(m'-1)-2)^2}{4}}$$

Note that $e < \hat{e}$. Ignore the limitation that l gives to d and think of d as solely limited by m'. This may give us too large of an upper bound, but it will still be a valid upper bound. Now, using calculus one can easily show that $\hat{e}$ is a decreasing function of l for positive l. Therefore, for $l \geq 3$,

$$\begin{aligned}
\hat{e} &\leq \frac{4(m'-3)(m'-a-3)+48(d-1)+12(d-1)(d-3)+16}{\frac{(4(m'-1)-2)^2}{4}} \\
&\leq \frac{(m'-3)(m'-a-3)+12(d-1)+3(d-1)(d-3)+4}{(m'-\frac{3}{2})^2} \\
&\leq \frac{(m'-3)(\frac{m'-1}{2}-3)+12(d-1)+3(d-1)(d-3)+4}{(m'-\frac{3}{2})^2} \\
&\leq \frac{\frac{1}{2}(m'-3)(m'-7)+12(d-1)+3(d-1)(d-3)+4}{(m'-\frac{3}{2})^2}
\end{aligned}$$

Recall that $d|\frac{m'-1}{2}$ and as we are assuming $d \neq \frac{m'-1}{2}$ we know that $d \leq \frac{m'-1}{6}$. Substitute this in.

$$\hat{e} \leq \frac{\frac{1}{2}(m'-3)(m'-7)+2(m'-7)+\frac{1}{12}(m'-7)(m'-19)+4}{(m'-\frac{3}{2})^2}$$

As m' approaches infinity, $\hat{e}$ approaches $\frac{7}{12}$. One can verify that the right-hand side is a strictly increasing function for $m' > 15$ and we noticed earlier that $m' \geq 19$ by our assumptions. Thus, $e < \hat{e} < \frac{7}{12}$ contradicting that $e \geq \frac{8}{9}$.

Now consider the case $l = 2$. Using the strict alternative bound on the number of Type II c singularities from Lemma 13,

$$I_{tot} = (2^l)\left(\left(\frac{m'-3}{2}\right)(2^l-2)(2^l+1) - (d-1)(d-3)\right) + 3(d-1)(2^{l-1})^2$$

$$+(d-1)(d-3)(2^{l-1})(2^{l-1}+1) + (2^{l-1}-1)^2$$

For $l = 2$, it becomes

$$I_{tot} = 4\left(10\left(\frac{m'-3}{2}\right) - (d-1)(d-3)\right) + 12(d-1) + 6(d-1)(d-3) + 1$$

Again let $e = \frac{I_{tot}}{\frac{(m-3)^2}{4}} = \frac{I_{tot}}{\frac{(2^{l-1}(m'-1)-2)^2}{4}}$ and so

$$e = \frac{20(m'-3) - 4(d-1)(d-3) + 12(d-1) + 6(d-1)(d-3) + 1}{\frac{(2(m'-1)-2)^2}{4}}$$

$$= \frac{20(m'-3) + 2(d-1)(d+3) + 1}{(m'-2)^2}$$

Again, as $d \neq \frac{m'-1}{2}$, we know that $d \leq \frac{m'-1}{6}$. This implies

$$e < \frac{20(m'-3) + \frac{1}{18}(m'-7)(m'+19) + 1}{(m'-2)^2}$$

which is a decreasing function of m' for $m' \geq 5$ and our assumptions imply $m' \geq 19$. Calculations show that for $m' \geq 27$, $e < .86 < \frac{8}{9}$, a contradiction. We can check by hand the remaining numbers, $m' = 19$ and 23 for $l = 2$ (recall that $m' \equiv 3 \pmod 4$), and h_+ is absolutely irreducible in these cases. Thus for all l and m', provided $1 < d < \frac{m'-1}{2}$, h_+ has an absolutely irreducible factor defined over $\mathbb{F}_2$. □

Chapter 4

Negative Exponents

4.1 Singularities of h_-

Theorem 10. *Assume $m \equiv 1$ (mod 4). The singular points of h_- are described by Table 4.1.*

Singularities of h_-				
Type	Description	m_p	I_p Bound	Number of Points
1	(0,0), (0,1), (1,0), and (1,1)	$m-1$	$\left(\frac{m-1}{2}\right)^2$	4
2	Other affine singularities	2	0	Not important
3	(0:1:0) and (1:0:0)	$m-1$	$\left(\frac{m-1}{2}\right)^2$	2

Table 4.1: All singularities of h_-

The proof will follow from Lemmas 17-24 and their corollaries. Type 2 singularities are all points of the form (x_0, y_0) where $x_0^{m+1} = (x_0+1)^{m+1} = (y_0+1)^{m+1} = y_0^{m+1}$ and $x_0 \neq y_0, y_0+1$. Note that when $m \equiv 3$ (mod 4), then h_- has many more singularities, but we will not address that case here.

Lemma 17. *The four points $(0,0), (1,0), (0,1),$ and $(1,1)$ are singular on f_-. Additionally, all points of the form (x_0, y_0) where $x_0^{m+1} = (x_0+1)^{m+1} = (y_0+1)^{m+1} = y_0^{m+1}$ are also singular on f_-. There are no other affine singular points.*

Proof. First, let $p = (x_0, y_0)$ be a singular point of f_-. As p is singular,

$$f_-(x_0, y_0) = x_0^m(x_0+1)^m(y_0^m + (y_0+1)^m) + y_0^m(y_0+1)^m(x_0^m + (x_0+1)^m) = 0 \quad (4.1)$$

We also need $\frac{\partial f_-}{\partial x}(x_0, y_0) = 0$ which means

$$(y_0^m+(y_0+1)^m)(x_0^{m-1}(x_0+1)^m+x_0^m(x_0+1)^{m-1})+y_0^m(y_0+1)^m(x_0^{m-1}+(x_0+1)^{m-1}) = 0$$

Clearly, the four points $(0,0), (1,0), (0,1),$ and $(1,1)$ are all singular. Likewise, if $x_0 = 0$ or 1 then $y_0 = 0$ or 1, and the converse holds true as well. Thus, we may assume that $x_0 \neq 0, 1$ and $y_0 \neq 0, 1$ for the remainder of the proof having already addressed that case. Simplifying $\frac{\partial f_-}{\partial x}(x_0, y_0) = 0$ yields

$$(y_0^m+(y_0+1)^m)x_0^{m-1}(x_0+1)^{m-1}((x_0+1)+x_0)+y_0^m(y_0+1)^m(x_0^{m-1}+(x_0+1)^{m-1}) = 0$$

By multiplying both sides by $x_0(x_0 + 1)$ we get

$$(y_0^m + (y_0 + 1)^m)x_0^m(x_0 + 1)^m + x_0y_0^m(y_0 + 1)^m(x_0^{m-1} + x_0^m + (x_0 + 1)^m) = 0$$

Using equation 4.1,

$$y_0^m(y_0 + 1)^m(x_0^m + (x_0 + 1)^m) + x_0y_0^m(y_0 + 1)^m(x_0^{m-1} + x_0^m + (x_0 + 1)^m) = 0$$

As $y_0 \neq 0, 1$ we may divide both sides by $y_0^m(y_0 + 1)^m$.

$$x_0^m + (x_0 + 1)^m + x_0(x_0^{m-1} + x_0^m + (x_0 + 1)^m) = 0$$

$$(x_0 + 1)^m + x_0(x_0 + 1)^m + x_0^{m+1} = 0$$

$$(x_0+1)^{m+1} = x_0^{m+1}$$

Due to symmetry, from $\frac{\partial f_-}{\partial y}$ we get that $(y_0+1)^{m+1} = y_0^{m+1}$.

Every singular point must satisfy these two equations. Substituting these into equation (4.1) after multiplying it by $(x_0+1)(y_0+1)$ and simplifying yields that $(x_0+1)^{m+1} = (y_0+1)^{m+1}$.

One can also verify that every point satisfying the equation $x_0^{m+1} = (x_0+1)^{m+1} = (y_0+1)^{m+1} = y_0^{m+1}$ is singular. This fully describes the singular points of f_-. □

Note that h_- has approximately the same singular points as f_- up to multiplicity. Any points on either of the lines $y = x$ or $y = x+1$ will have multiplicity one less on h_- than on f_-. However, this may mean that some singular points on f_- are nonsingular on h_-.

Lemma 18. *If $l > 1$, i.e. $m \equiv 1$ (mod 4), then the only singular points at infinity of $\hat{f}_-$ are $(1:0:0), (0:1:0)$, and $(1:1:0)$. If $l = 1$, i.e. $m \equiv 3$ (mod 4), then the singular points include the previous three plus points of the form $(x_0:1:0)$ where $x_0^{m+1} = 1, x_0 \neq 1$.*

Proof. Recall that $\hat{f}_-$ is the homogenized form of f_-, and $\hat{h}_-$ is the homogenized form of h_-. Thus,

$$\begin{aligned}
\hat{f_-} &= x^m(x+z)^m\left(\frac{y^m+(y+z)^m}{z}\right) + y^m(y+z)^m\left(\frac{x^m+(x+z)^m}{z}\right) \\
\frac{\partial \hat{f}_-}{\partial x} &= x^{m-1}(x+z)^m\left(\frac{y^m+(y+z)^m}{z}\right) + x^m(x+z)^{m-1}\left(\frac{y^m+(y+z)^m}{z}\right) + \\
&\quad + y^m(y+z)^m\left(\frac{x^{m-1}+(x+z)^{m-1}}{z}\right)
\end{aligned}$$

As we want singular points at infinity, substitute in $z = 0$. Note that as $m-1$ is even, $\binom{m-1}{1} = 0$.

$$\frac{\partial \hat{f}_-}{\partial x}|_{z=0} = x^{m-1}x^m(y^{m-1}) + x^m x^{m-1}(y^{m-1}) + y^m y^m\left(\binom{m-1}{1}x^{m-2}\right) = 0.$$

By symmetry, $\frac{\partial \hat{f}_-}{\partial y}|_{z=0} = 0$.

$$\hat{f}_- = x^{2m}y^{m-1} + y^{2m}x^{m-1} + z\left(\binom{m}{2}x^{2m}y^{m-2} + x^{2m-1}y^{m-1} + \right.$$

$$\left. + \binom{m}{2}x^{m-2}y^{2m} + x^{m-1}y^{2m-1}\right) + z^2(i(x,y,z)) \text{ for some polynomial } i(x,y,z)$$

As $\binom{m}{2} = 1$ if only if $l = 1$ and is 0 otherwise, then

$$\frac{\partial \hat{f}_-}{\partial z}|_{z=0} = \begin{cases} x^{2m-1}y^{m-1} + x^{m-1}y^{2m-1} & \text{if } l > 1 \\ x^{2m}y^{m-2} + x^{2m-1}y^{m-1} + x^{m-1}y^{2m-1} + x^{m-2}y^{2m} & \text{if } l = 1 \end{cases}$$

Lastly,

$$\hat{f}_-|_{z=0} = x^{2m}y^{m-1} + x^{m-1}y^{2m}.$$

If $y = 0$, then $\frac{\partial \hat{f}_-}{\partial z}|_{z=0} = \hat{f}_-|_{z=0} = 0$. Then we can assume $x = 1$ by scaling if necessary and we have that $(1:0:0)$ is a singular point. Otherwise, we may assume $y = 1$ by scaling if necessary. Let $(x_0 : 1 : 0)$ be a singular point and then $\hat{f}_-(x_0 : 1 : 0) = 0$ if and only if $x_0^{m+2} = x_0$. This is equivalent to $x_0 = 0$ or $x_0^{m+1} = 1$. Also, from $\frac{\partial \hat{f}_-}{\partial z}$, we get that

$$\frac{\partial \hat{f}_-}{\partial z}(x_0 : 1 : 0) = \begin{cases} x_0^{m-2}(1 + x_0) & \text{if } l > 1 \\ 0 & \text{if } l = 1 \end{cases}.$$

Therefore, if $l = 1$, the singular points are $(1:0:0)$, $(1:1:0)$, $(0:1:0)$, and $(x_0 : 1 : 0)$ where $x_0^{m+1} = 1$. If $l > 1$, then the only singular points are $(1:0:0)$, $(1:1:0)$, and $(0:1:0)$. □

4.2 Multiplicity and I_p Bounds of Singularities of h_-

Lemma 19. *Let $p = (x_0, y_0)$ be a singular point of h_- with multiplicity m_p. If $x_0 = y_0$ or $x_0 = y_0 + 1$, then $F_{m_p+1} = (x+y)H_{m_p}$ and $(x+y)gcd(H_{m_p}, H_{m_p+1}) = gcd(F_{m_p+1}, F_{m_p+2})$.*

If $x_0 \neq y_0$ and $x_0 \neq y_0 + 1$, then the tangent lines of f_- are the same as the tangent lines of h_- at p, i.e. $F_{m_p} = cH_{m_p}$ for some constant c. Also $gcd(H_{m_p}, H_{m_p+1}) = gcd(F_{m_p}, F_{m_p+1})$.

Proof. Write $h_-(x + x_0, y + y_0)$ as $H_{m_p} + H_{m_p+1} + H_{m_p+2} + H_R$ where H_R is the polynomial composed of all the terms of degree greater than $m_p + 2$. Let $c = (x_0 + y_0)(x_0 + y_0 + 1)$. Thus,

$$\begin{aligned} f_-(x + x_0, y + y_0) &= [h_-(x + x_0, y + y_0)][(x + x_0 + y + y_0)(x + x_0 + 1 + y + y_0)] \\ &= (H_{m_p} + H_{m_p+1} + H_{m_p+2} + H_R)((x+y)^2 + (x+y) + c) \\ &= \{((x+y)^2 + (x+y) + c)H_R + ((x+y)^2 + (x+y))H_{m_p+2} \\ &\quad + (x+y)^2 H_{m_p+1}\} + \{cH_{m_p+2} + (x+y)H_{m_p+1} + \\ &\quad + (x+y)^2 H_{m_p}\} + \{cH_{m_p+1} + (x+y)H_{m_p}\} + \{cH_{m_p}\} \end{aligned}$$

First, assume that $x_0 \neq y_0$ and $x_0 \neq y_0 + 1$. Then, $c \neq 0$ and so p will have the same multiplicity on both f_- and h_-. Also, $F_{m_p} = cH_{m_p}$ and $F_{m_p+1} = cH_{m_p+1} + (x+y)H_{m_p}$.

Now, clearly F_{m_p} and H_{m_p} have the same factors, and so the tangent lines of f_- are the same as the tangent lines of h_- at p. Also,

$$\begin{aligned} \gcd(H_{m_p}, H_{m_p+1}) &= \gcd(H_{m_p}, cH_{m_p+1}) \\ &= \gcd(H_{m_p}, cH_{m_p+1} + (x+y)H_{m_p}) \\ &= \gcd(F_{m_p}, F_{m_p+1}). \end{aligned}$$

Now assume that $x_0 = y_0$ or $x_0 = y_0 + 1$ so that $c = 0$. Then p has multiplicity one less on h_- than on f_-. Also, $F_{m_p+1} = (x+y)H_{m_p}$ and $F_{m_p+2} = (x+y)H_{m_p+1} + (x+y)^2 H_{m_p}$. Therefore, if the tangent lines of f_- at p are distinct, then so are the tangent lines to h_- at p. Also,

$$\begin{aligned}(x+y)\gcd(H_{m_p}, H_{m_p+1}) &= \gcd((x+y)H_{m_p}, (x+y)H_{m_p+1}) \\ &= \gcd((x+y)H_{m_p}, (x+y)H_{m_p+1} + (x+y)^2 H_{m_p}) \\ &= \gcd(F_{m_p+1}, F_{m_p+2}).\end{aligned}$$

□

Lemma 20. *The Type 1 singular points, (0,0), (0,1), (1,0), and (1,1), have multiplicity $m-1$ on h_- and $I_p \leq \left(\frac{m-1}{2}\right)^2$.*

Proof.

$$f_-(x+x_0, y+y_0) = (x+x_0)^m(x+x_0+1)^m((y+y_0)^m + (y+y_0+1)^m) +$$

$$+ (y+y_0)^m(y+y_0+1)^m((x+x_0)^m + (x+x_0+1)^m)$$

Note that by symmetry $f_-(x+x_0, y+y_0)$ is identical for $(x_0, y_0) = (0,0)$, $(1,0)$, $(0,1)$, or $(1,1)$. Therefore, we may assume $p = (x_0, y_0) = (0,0)$. The minimal terms of $f_-(x+0, y+0)$ are $x^m + y^m$. Thus, p has multiplicity m on f_-. As p is on $y = x$ or $y = x+1$, it has multiplicity $m-1$ on h_-. Also, as m is odd, the factors of $x^m + y^m$ are all distinct. By Lemma 19, the tangent lines of h_- at these points are also all distinct. Recall from the background material section that when the tangent lines are all distinct then the intersection multiplicity of that point is the product of the singularity multiplicities, $m_p(u)$ and $m_p(v)$, of the two factors. Since the sum of their singularity multiplicities is $m-1$, their product is bounded above by $\left(\frac{m-1}{2}\right)^2$. Thus $I_p \leq \left(\frac{m-1}{2}\right)^2$. □

Lemma 21. *Let $p = (x_0, y_0)$ be a singular point of h_- that satisfies $x_0^{m+1} = (x_0+1)^{m+1} = (y_0+1)^{m+1} = y_0^{m+1}$ and $x_0, y_0 \neq 0, 1$. Assume $m \equiv 1$ (mod 4). Then $x_0 \neq y_0$ and $x_0 \neq y_0 + 1$, and p has multiplicity 2 on h_-. Also, $I_p = 0$.*

Proof. Recall F_a is the polynomial composed of the terms of $f_-(x+x_0, y+y_0)$ of degree a. As p is a singular point of f_-, clearly $F_0 = 0$ and $F_1 = 0$. Let F_{2,x^2} be the coefficient of x^2 in F_2. Then as $\binom{m}{2} = 0$,

$$F = f_-(x+x_0, y+y_0) = (x+x_0)^m(x+x_0+1)^m((y+y_0)^m + (y+y_0+1)^m) +$$

$$+ (y+y_0)^m(y+y_0+1)^m((x+x_0)^m + (x+x_0+1)^m)$$

$$\begin{aligned} F_{2,x^2} &= x_0^{m-1}(x_0+1)^{m-1}(y_0^m + (y_0+1)^m) + 0 = \frac{x_0^{m-1}(x_0+1)^{m-1}y_0^m}{(y_0+1)} \\ &= \frac{x_0^{3m+2}}{(x_0+1)^2(y_0+1)x_0y_0} = \left(\frac{x_0^{3m+2}}{(x_0+1)(y_0+1)y_0}\right)\left(\frac{1}{x_0(x_0+1)}\right) \end{aligned}$$

By symmetry,

$$F_{2,y^2} = \frac{y_0^{m-1}(y_0+1)^{m-1}x_0^m}{(x_0+1)} = \left(\frac{x_0^{3m+2}}{(x_0+1)(y_0+1)y_0}\right)\left(\frac{1}{y_0(y_0+1)}\right)$$

Note that as $x_0, y_0 \neq 0, 1$, these are nonzero.

$$\begin{aligned} F_{2,xy} &= (x_0^{m-1}(x_0+1)^m + x_0^m(x_0+1)^{m-1})(y_0^{m-1} + (y_0+1)^{m-1}) + \\ &\quad + (y_0^{m-1}(y_0+1)^m + y_0^m(y_0+1)^{m-1})(x_0^{m-1} + (x_0+1)^{m-1}) \\ &= x_0^{m-1}(x_0+1)^{m-1}(x_0+1+x_0)(y_0^{m-1} + (y_0+1)^{m-1}) + \\ &\quad + y_0^{m-1}(y_0+1)^{m-1}(y_0+1+y_0)(x_0^{m-1} + (x_0+1)^{m-1}) \end{aligned}$$

$$\begin{aligned} F_{2,xy}(x_0+1)^2(y_0+1)^2 &= x_0^{m-1}(x_0+1)^{m+1}(y_0^{m-1}) + y_0^{m-1}(y_0+1)^{m+1}(x_0^{m-1}) \\ &= 0 \end{aligned}$$

Thus as $x_0 \neq 1$ and $y_0 \neq 1$, we have that $F_{2,xy} = 0$. For simplicity let $\alpha_2 = \left(\frac{x_0^{3m+2}}{(x_0+1)(y_0+1)y_0}\right)$, $\beta_1 = \left(\frac{1}{x_0(x_0+1)}\right)$ and $\beta_2 = \left(\frac{1}{y_0(y_0+1)}\right)$, then $F_2 = \alpha_2\beta_1\beta_2(y_0(y_0+1)x^2 + x_0(x_0+1)y^2)$. Note that p has multiplicity 2 on f_-, and the two tangent lines of f_- are identical.

Now, $F_{3,x^3} = 0 = F_{3,y^3}$ as $\binom{m}{3} = \binom{m}{2} = 0$. Also,

$$\begin{aligned} F_{3,x^2y} &= x_0^{m-1}(x_0+1)^{m-1}(y_0^{m-1} + (y_0+1)^{m-1}) + 0 \\ F_{3,x^2y}(x_0+1)^2(y_0+1)^2 &= x_0^{m-1}(x_0+1)^{m+1}(y_0^{m-1}) \\ F_{3,x^2y}(x_0+1)^2(y_0+1)^2x_0^2y_0^2 &= x_0^{m+1}(x_0+1)^{m+1}y_0^{m+1} \\ &= x_0^{3m+3} \end{aligned}$$

Thus, $F_{3,x^2y} = \frac{x_0^{3m+3}}{(x_0+1)^2(y_0+1)^2x_0^2y_0^2}$ and by symmetry F_{3,xy^2} is the same. Call $\alpha_3 = F_{3,x^2y}$. Then, $F_3 = \alpha_3(x^2y + xy^2) = \alpha_3xy(x+y)$.

Now, assume $x_0 = y_0$ or $y_0 + 1$ for contradiction. Then p, which has multiplicity 2 on f_-, has multiplicity 1 on h_-. Thus, p is nonsingular on h, a contradiction. Thus, $x_0 \neq y_0, y_0 + 1$ and thus p has multiplicity 2 on both f_- and h_-.

Also, as $x_0(x_0+1) \neq y_0(y_0+1)$, then $(x+y) \nmid F_2$. Hence $\gcd(F_2, F_3) = 1$. By Lemma 19, $\gcd(H_2, H_3) = 1$, and so by Lemma 1, $I_p = 0$. □

Lemma 22. *Let $p = (x_0 : y_0 : 0)$ be a singular point of $\hat{f}_-$. If $x_0 \neq y_0$, then the tangent lines at p of $\tilde{f}_-$ are the same as those of $\tilde{h}_-$ at p. Also, $gcd(\tilde{H}_{m_p}, \tilde{H}_{m_p+1}) = gcd(\tilde{F}_{m_p}, \tilde{F}_{m_p+1})$, where m_p is the multiplicity of p on h_-. If $x_0 = y_0$, then the tangent lines of $\tilde{f}_-$ at p are the tangent lines to $\tilde{h}_-$ plus the lines x and $x+z$, i.e. $\tilde{F}_{m_p} = \tilde{H}_{m_p}[x(x+z)]$.*

Proof. If $y_0 = 0$, then $p = (1:0:0)$, which by symmetry behaves identically to (0:1:0). Therefore, we may assume $y_0 \neq 0$. Define $x_0' = \frac{x_0}{y_0}$. Write $\tilde{h}_-(x + x_0', z + 0)$ as $\tilde{H}_{m_p} + \tilde{H}_{m_p+1} + \tilde{H}_R$ where $\tilde{H}_R$ is the polynomial composed of all of the terms of degree greater than $m_p + 1$. Let $c = (x_0' + 1)$. Thus,

$$\begin{aligned}\tilde{f}_-(x+x_0',z+0) &= [\tilde{h}_-(x+x_0',z)][(x+x_0'+1)(x+x_0'+1+z)]\\ &= (\tilde{H}_{m_p}+\tilde{H}_{m_p+1}+\tilde{H}_R)(x(x+z)+cz+c^2)\\ &= \{\tilde{H}_R[x(x+z)+cz+c^2]+\tilde{H}_{m_p+1}[x(x+z)+cz]+\\ &\quad +\tilde{H}_{m_p}[x(x+z)]\}+\{c^2\tilde{H}_{m_p+1}+cz\tilde{H}_{m_p}\}+\{c^2\tilde{H}_{m_p}\}\end{aligned}$$

If $x_0 \neq y_0$, then, $x_0' \neq 1$ and $c \neq 0$. Also, p will have the same multiplicity on both $\hat{f}_-$ and $\hat{h}_-$, and $\tilde{F}_{m_p} = \{c\tilde{H}_{m_p}\}$ and $\tilde{F}_{m_p+1} = \tilde{H}_{m_p+1} + cz\tilde{H}_{m_p}$. Now, clearly $\tilde{F}_{m_p}$ and $\tilde{H}_{m_p}$ have the same factors, and so the tangent lines of $\hat{f}_-$ are the same as the tangent lines of $\hat{h}_-$ at p. Also,

$$\begin{aligned}\gcd(\tilde{H}_{m_p},\tilde{H}_{m_p+1}) &= \gcd(c\tilde{H}_{m_p},c^2\tilde{H}_{m_p+1})\\ &= \gcd(c\tilde{H}_{m_p},c^2\tilde{H}_{m_p+1}+z(c\tilde{H}_{m_p}))\\ &= \gcd(\tilde{F}_{m_p},\tilde{F}_{m_p+1}).\end{aligned}$$

Now assume that $x_0 = y_0$ so that $x_0' = 1$ and $c = 0$. Then, $\tilde{F}_{m_p+2} = \tilde{H}_{m_p}[x(x+z)]$ and thus the tangent lines of $\tilde{f}_-$ at p are the tangent lines to $\tilde{h}_-$ plus the lines x and $x+z$, i.e. $\tilde{F}_{m_p+2} = x(x+z)\tilde{H}_{m_p}$. □

Lemma 23. *Let p be either of the singular points $(0:1:0)$ or $(1:0:0)$ of $\hat{h}_-$, then p has multiplicity $m-1$ on $\hat{h}_-$, and the tangent lines of $\tilde{h}_-$ at p are all distinct. Thus $I_p \leq \left(\frac{m-1}{2}\right)^2$.*

Proof. By symmetry, we may assume without loss of generality that $p = (0:1:0)$. Dehomogenize $\hat{f}_-$ relative to y to get

$$\tilde{f}_- = x^m(x+z)^m\left(\frac{1+(1+z)^m}{z}\right)+(z+1)^m\left(\frac{x^m+(x+z)^m}{z}\right)$$

In this new system, $p = (0,0)$ and the multiplicity of p is the degree of the lowest nonzero terms in the above function. The terms of lowest degree are $\frac{x^m+(x+z)^m}{z}$ and are of degree $m-1$. Since p was originally not on $x+y$ nor $x+y+z$, it has the same multiplicity on both $\hat{h}_-$ and $\hat{f}_-$. The tangent lines at p are the factors of $\frac{x^m+(x+z)^m}{z}$.

Note that this is a homogeneous polynomial. Let $x = \frac{x}{z}$ and we want the factors of $x^m + (x+1)^m$. This has all distinct factors, so by Lemma 22, the tangent lines of $\tilde{h}_-$ are all distinct. Therefore, $I_p \leq \left(\frac{m-1}{2}\right)^2$. □

Lemma 24. *Let $p = (1:1:0)$. Then if $m \equiv 1$ (mod 4), p is nonsingular on $\hat{h}_-$. If $m \equiv 3$ (mod 4), then p is singular with multiplicity of $2^k - 2$ on $\hat{h}_-$ with all distinct tangent lines.*

Proof. Dehomogenize $\hat{f}_-$ relative to y to get

$$\tilde{f}_- = x^m(x+z)^m\left(\frac{1+(1+z)^m}{z}\right) + (z+1)^m\left(\frac{x^m+(x+z)^m}{z}\right)$$

In this new system, $p = (1,0)$ and the multiplicity of p is the degree of the lowest nonzero terms in the function

$$\begin{aligned}\tilde{f}_-(x+1,z+0) &= (x+1)^m(x+z+1)^m\left(\frac{1+(1+z)^m}{z}\right) + \\ &\quad + (z+1)^m\left(\frac{(x+1)^m+(x+z+1)^m}{z}\right).\end{aligned}$$

Consider the terms of degree $b < 2^k - 1$. I claim these terms are congruent to 0 in $\mathbb{F}_2[x,z]$. Note $\binom{m}{b} = \binom{m}{b+1} = 1$ by the definition of k in Definition 3 and Lucas's Theorem. The terms of degree b are:

$$\sum_{i=0}^{b}(x+z)^i\sum_{j=0}^{b-i}x^j z^{b-i-j} + \sum_{i=0}^{b}\left(\frac{x^{i+1}+(x+z)^{i+1}}{z}\right)z^{b-i}.$$

As this is homogeneous, we can divide by z^b and set $x = \frac{x}{z}$ to get

$$\sum_{i=0}^{b}(x+1)^i\sum_{j=0}^{b-i}x^j + \sum_{i=0}^{b}(x^{i+1}+(x+1)^{i+1})$$

$$= \sum_{i=1}^{b}(x+1)^i\sum_{j=0}^{b-i}x^j + \sum_{j=0}^{b}x^j + \sum_{i=1}^{b+1}(x^i+(x+1)^i)$$

$$= \sum_{i=1}^{b} (x+1)^{i-1}(1+x^{b-i+1}) + \sum_{i=0}^{b} x^i + \sum_{i=1}^{b+1} x^i + \sum_{i=1}^{b+1} (x+1)^i$$

$$= \sum_{i=0}^{b-1} (x+1)^i(1+x^{b-i}) + 1 + x^{b+1} + \sum_{i=1}^{b-1} (x+1)^i + (x+1)^b + (x+1)^{b+1}$$

$$= \sum_{i=1}^{b-1} (x+1)^i(1+x^{b-i}) + 1 + x^b + 1 + x^{b+1} + \sum_{i=1}^{b-1} (x+1)^i + (x+1)^b + (x+1)^{b+1}$$

$$= \sum_{i=1}^{b-1} (x+1)^i x^{b-i} + x^b + x^{b+1} + (x+1)^b + (x+1)^{b+1}$$

$$= \sum_{i=1}^{b} (x+1)^i x^{b-i} + x^b + x^{b+1} + (x+1)^{b+1}$$

The terms of degree 0 in this expression are clearly 0 as are those of degree $b+1$. The terms of degree b in this expression are $(b+1)x^b + \binom{b+1}{b}x^b = 0$. Now consider the terms of degree c where $1 \leq c \leq b-1$ in the above expression. Their coefficient is given by

$$\sum_{i=1}^{b} \binom{i}{c+i-b} + \binom{b+1}{c} = \sum_{i=1}^{b} \binom{i}{b-c} + \binom{b+1}{c}$$

$$= \sum_{i=b-c}^{b} \binom{i}{b-c} + \binom{b+1}{c} = \binom{b+1}{b-c+1} + \binom{b+1}{c} = 2\binom{b+1}{c} = 0.$$

Thus the terms of degree $b < 2^k - 1$ in $\tilde{f}_-(x+1, z+0)$ are 0. Now consider the terms of degree $b = 2^k - 1$ in $\tilde{f}_-(x+1, z+0)$. These are

$$\sum_{i=0}^{b}(x+z)^i\sum_{j=0}^{b-i}x^jz^{b-i-j}+\sum_{i=0}^{b}\left(\frac{x^{i+1}+(x+z)^{i+1}}{z}\right)z^{b-i}-\left(\frac{x^{b+1}+(x+z)^{b+1}}{z}\right)-z^b$$

as $\binom{m}{b}=1$ but $\binom{m}{b+1}=0$.

Again, this is homogeneous, so we can divide by z^b and redefine $x=\frac{x}{z}$ to get the expression

$$\sum_{i=0}^{b}(x+1)^i\sum_{j=0}^{b-i}x^j+\sum_{i=0}^{b}(x+1)^{i+1}+\sum_{i=0}^{b}x^{i+1}+x^{b+1}+(x+1)^{b+1}+1$$

As $b+1=2^k$, $(x+1)^{b+1}=x^{b+1}+1$ and the expression above simplifies to

$$\sum_{i=0}^{b}(x+1)^i\sum_{j=0}^{b-i}x^j+\sum_{i=0}^{b}(x+1)^{i+1}+\sum_{i=0}^{b}x^{i+1}.$$

But by the work above for the case $b<2^k-1$, this expression is 0 in $\mathbb{F}_2[x]$.

Lastly, consider the terms of degree $b=2^k$ in $\tilde{f}_-(x+1,z+0)$. Note that $\binom{m}{b}=\binom{m}{b+1}=0$. Thus, the terms of degree b are

$$\left\{\sum_{i=0}^{b}(x+z)^i\sum_{j=0}^{b-i}x^jz^{b-i-j}+\sum_{i=0}^{b}\left(\frac{x^{i+1}+(x+z)^{i+1}}{z}\right)z^{b-i}\right\}$$

$$-\left\{\left(\frac{x^b+(x+z)^b}{z}\right)-z^{b-1}\right\}-\left\{x^b+(x+z)^b+z^b+z^b+\left(\frac{x^{b+1}+(x+z)^{b+1}}{z}\right)\right\}$$

The terms in the first and second set of braces are zero from previous work. In the remaining set of terms, substitute in that $b=2^k$ to get

$$x^{2^k}+x^{2^k}+z^{2^k}+z^{2^k}+z^{2^k}+\left(\frac{x^{2^k+1}+x^{2^k+1}+x^{2^k}z+xz^{2^k}+z^{2^k+1}}{z}\right)$$

$$= z^{2^k} + x^{2^k} + xz^{2^k-1} + z^{2^k} = x(x^{2^k-1} + z^{2^k-1})$$

These are all distinct factors and thus by Lemma 22, all the tangent lines to $\hat{h}_-$ at p are distinct. Also as p was originally on both $x+y$ and $x+y+z$, the multiplicity on $\hat{h}_-$ is $2^k - 2$. Now, if $m \equiv 1 \pmod 4$ then $k = 1$ hence the multiplicity is 0 on $\hat{h}_-$ indicating that p is not a singular point. □

4.3 Proof of Theorem 2

Theorem 2. *Assume $m \equiv 1$ (mod 4) and $m > 1$. Then, h_- has an absolutely irreducible factor defined over $\mathbb{F}_2$.*

Proof. First, assume for contradiction that h_- has no absolutely irreducible factors over $\mathbb{F}_2$. Lemma 5 implies that $e = \frac{I_{tot}}{\frac{(\deg(h_-))^2}{4}} \geq \frac{8}{9}$ where I_{tot} is any upper bound on the global intersection number of u and v for all factorizations $h_- = u \cdot v$ over the algebraic closure of $\mathbb{F}_2$. Note $\deg(h_-) = 3m - 1$.

We need to calculate an estimate for I_{tot}. According to Theorem 10, there are three types of singularities. Adding their I_p bounds gives the estimate $I_{tot} = 6(\frac{m-1}{2})^2$. Thus,

$$e \leq \frac{6(\frac{m-1}{2})^2}{\left(\frac{(3m-1)}{2}\right)^2} = \frac{6(m-1)^2}{(3m-1)^2} \leq \frac{2}{3}\frac{(m-\frac{1}{3})^2}{(m-\frac{1}{3})^2} = \frac{2}{3} < \frac{8}{9}.$$

This contradicts that $e \geq \frac{8}{9}$. Thus h_- must have an absolutely irreducible factor over $\mathbb{F}_2$. □

Chapter 5

Future Research

5.1 The Last Positive Case

All power functions with positive exponents have been classified as either APN over infinitely many finite fields of characteristic 2 or over only a finite number, except for the case $d = \frac{m'-1}{2}$. This last case is clearly not addressed satisfactorily. When l is the smallest it can be, i.e. when $2^l - 1 = \frac{m'-1}{2}$, then the monomial is already known to be APN over infinitely many fields; these are the Kasami power functions, $x^{4^j-2^j+1}$. All other monomials in this case appear to be APN over only finitely many fields.

This case actually gives us no problems except when h_+ has affine singular points off of the lines $y = x$ and $y = x + 1$, something that is statistically rare; see Conjecture 1. If all affine singular points fall on these two lines then the following corollary to Theorem 9 shows that h_+ has an absolutely irreducible factor defined over $\mathbb{F}_2$.

Corollary 10. *Assume $d = \frac{m'-1}{2} > 1$. If all of the affine singular points of h_+ fall on the lines $y = x$, $y = x + 1$ then h_+ has an absolutely irreducible factor over $\mathbb{F}_2$ provided $m \neq 13$.*

Proof. Follow the proof of Theorem 9 but remove the intersection number estimates for all affine singular points off the lines $y = x$, $y = x + 1$ from I_{tot}. Note that $l > 1$ and $m' \geq 7$ as $d > 1$.

Thus, we can bound the global intersection number by

$$\begin{aligned}\sum_p I_p(u,v) &\leq 2(d-1)(2^{l-1})^2 + (d-1)(2^{l-1})^2 + (2^{l-1}-1)^2 \\ &< 3(d-1)(2^{l-1})^2 + (2^{l-1})^2\end{aligned}$$

Call this last bound I_{tot}.

$$e = \frac{I_{tot}}{\frac{(m-3)^2}{4}} = \frac{3(d-1)(2^{l-1})^2 + (2^{l-1})^2}{\frac{(2^{l-1}(m'-1)-2)^2}{4}}$$

It is easy to show that if we consider m' and d fixed, then e is a decreasing function of l. Ignore the relationship between l and d. Therefore, the largest value occurs when $l = 2$ and

$$e \leq \frac{3(d-1)(4)+4}{\frac{(2(m'-1)-2)^2}{4}} = \frac{12d-8}{(m'-2)^2} = \frac{6m'-14}{(m'-2)^2}.$$

The bound above is a decreasing function of m' for $m' \geq 3$, and so for $m' \geq 11$, $e \leq \frac{52}{81} < \frac{8}{9}$, a contradiction! Clearly as $d = \frac{m'-1}{2} > 1$, $m' > 3$. In the only remaining case $m' = 7$ so $d = 3$. Substituting those into e yields

$$e = \frac{7(2^{l-1})^2 - 2(2^{l-1}) + 1}{(3(2^{l-1})-1)^2}$$

which is a decreasing function of l for $l > 1$. For $l \geq 3$ then $e < .87 < \frac{8}{9}$, a contradiction!

Therefore, provided we are not in the case $d = 3, m' = 7, l = 2$ (which is when $m = 13$) then h_+ has an absolutely irreducible factor defined over $\mathbb{F}_2$. □

The method used in this paper fails to give a general solution in this last case as the estimate of the global intersection number that we can calculate from singularities is very close to what Bezout's Theorem says the global intersection number should be. Applying this method to this last case only gives a bound on the number of factors, c, that h_+ can have: $c < .89\sqrt{m'}$ (under the reasonable assumption that

h_+ is irreducible over $\mathbb{F}_2$). Perhaps this bound can lead to a contradiction if one could show that as m grows, h_+ must have more factors, but I have been unable to prove this. The number of factors that h_+ has when $2^l - 1 = \frac{m'-1}{2}$ suggests that this method may work though.

Theorem 11. *Assume $d = \frac{m'-1}{2} \neq 2^l - 1$ and that h_+ is not absolutely irreducible. If h_+ is irreducible over $\mathbb{F}_2$, then when h_+ factors over the algebraic closure, it has fewer than $.89\sqrt{m'}$ factors for $m' \geq 15$. If $m' < 15$, then h_+ irreducible over $\mathbb{F}_2$ implies that h_+ is absolutely irreducible.*

Proof. First, as $d = \gcd(\frac{m'-1}{2}, 2^l - 1) = \frac{m'-1}{2} \neq 2^l - 1$, clearly $\frac{m'-1}{2} | 2^l - 1$ and $\frac{m'-1}{2} < 2^l - 1$. This implies that $\frac{m'-1}{2} \leq \frac{2^l-1}{3}$ which is equivalent to $\frac{3m'-1}{4} \leq 2^{l-1}$. Let $w = 2^{l-1}$ for simplicity.

Since h_+ is irreducible over $\mathbb{F}_2$, when it factors it will have c factors which are conjugates. Group these conjugates as evenly as possible into two polynomials u and v such that $h_+ = u \cdot v$ and $\deg(u) = \deg(v) + \frac{m-3}{c}$. From Lemma 5, $e = \frac{I_{tot}}{\frac{(m-3)^2}{4}} \geq \frac{8}{9}$ where I_{tot} is a bound on the global intersection number of u and v. From the work at the end of Theorem 9, we have a bound on the global intersection number,

$$w(m'-3)(\frac{m'-1}{2} - 3) - w(d-1)(d-3) + 3w^2(d-1) + w^2(d-1)(d-3) + (w-1)^2.$$

Substitute this and that $d = \frac{m'-1}{2}$ into the definition of e. Combine similar terms to get

$$\begin{aligned} e &= \frac{(\frac{w}{2} - \frac{w}{4})(m'-3)(m'-7) + \frac{3w^2}{2}(m'-3) + \frac{w^2}{4}(m'-3)(m'-7) + (w-1)^2}{\frac{(w(m'-1)-2)^2}{4}} \\ &= \frac{w(m'-3)(m'-7) + 6w^2(m'-3) + w^2(m'-3)(m'-7) + 4(w-1)^2}{(w(m'-1)-2)^2} \\ &= \frac{w(m'-3)(m'-7) + w^2(m'-3)(m'-1) + 4(w-1)^2}{(w(m'-1)-2)^2}. \end{aligned}$$

A fair bit of calculus shows that this is a decreasing function of w for $w > 0$ and fixed $m' \geq 7$. Thus, as $w \geq \frac{3m'-1}{4}$,

$$
\begin{aligned}
e &\leq \frac{\frac{3}{4}(m'-\frac{1}{3})(m'-3)(m'-7)+\frac{9}{16}(m'-\frac{1}{3})^2(m'-3)(m'-1)+\frac{9}{4}(m'-\frac{5}{3})^2}{\frac{9}{16}((m'-\frac{1}{3})(m'-1)-\frac{8}{3})^2} \\
&\leq \frac{(m')^4-\frac{10}{3}(m')^3-4(m')^2+\frac{50}{3}m'+\frac{19}{9}}{(m')^4-\frac{8}{3}(m')^3-\frac{26}{9}(m')^2+\frac{56}{9}m'+\frac{49}{9}} \\
&\leq \frac{9(m')^4-30(m')^3-36(m')^2+150m'+19}{9(m')^4-24(m')^3-26(m')^2+56m'+49} \\
&\leq 1+\frac{-6(m')^3-10(m')^2+94m'-30}{9(m')^4-24(m')^3-26(m')^2+56m'+49} \\
&< 1-\frac{2}{3m'} \text{ for } m' \geq 7
\end{aligned}
$$

Recall from the proof of Lemma 5 that $\sqrt{1-\frac{1}{c^2}} \leq e$. Therefore combining this with the bound on e, we get that $c < \frac{3m'}{2\sqrt{3m'-1}}$. For $m' = 7$, we get the bound that $c < 2.4$ implying that there are at most two conjugates. However, from the proof of Lemma 5 if c is even then $e \geq 1$, and we can see that $e < 1$. Hence, in this case, if h_+ is irreducible over $\mathbb{F}_2$ then it is absolutely irreducible.

For $m' \geq 11$, $c < 2.97$ implying again that there are at most two conjugates. Hence again if h_+ is irreducible over $\mathbb{F}_2$ then it is absolutely irreducible in this case.

Lastly, for $m' \geq 15$, we can loosen the bound and simplify it to $c < .89\sqrt{m'}$. □

Corollary 10 shows that if h_+ has no singularities that are off of the lines two lines $y + x$ and $x + y + 1$, then h_+ has an absolutely irreducible factors over $\mathbb{F}_2$, provided $m \neq 13$. I claimed that this is statistically rare and the justification is below.

For m and m', the function f_+ has the same singular points (although the multiplicity will vary), so we may assume for the next theorem that we are working with m' (i.e. that $m \equiv 3 \pmod 4$).

Theorem 12. *The Equivalence Theorem: Assume $m \equiv 3$ (mod 4). Let $b = \frac{m-1}{2}$, and μ_b be the multiplicative group of the bth roots of unity.*

Then there exists $w_0, z_0 \in \mu_b - \{1\}$ with $w_0 \neq z_0^{\pm 1}$ such that $\frac{1+w_0}{1+z_0} \in \mu_b$ if and only if there exist singular points p of f_+ off the lines $y = x$, $y = x + 1$.

Proof. A point (x_0, y_0) is singular if and only if it satisfies the following three equations.

$$(x_0+1)^{\frac{m-1}{2}} = (x_0)^{\frac{m-1}{2}} \quad (5.1)$$

$$(x_0)^{\frac{m-1}{2}} = (y_0)^{\frac{m-1}{2}} \quad (5.2)$$

$$(y_0+1)^{\frac{m-1}{2}} = (y_0)^{\frac{m-1}{2}} \quad (5.3)$$

Clearly $x_0 \neq 0, 1$. As $b = \frac{m-1}{2}$, divide equation (5.1) above by x_0^b to get $(1+\frac{1}{x_0})^b = 1$. Let $z_0 = x_0^{-1} + 1$ so that $z_0^b = 1$ implying $z_0 \in \mu_b$. Do the same for equation (5.3) by letting $w_0 = y_0^{-1} + 1$ implying $w_0 \in \mu_b$. Then equation (5.2) is equivalent to $(\frac{x_0}{y_0})^b = 1$ which is equivalent to $\left(\frac{1+w_0}{1+z_0}\right)^b = 1$, i.e. $\left(\frac{1+w_0}{1+z_0}\right) \in \mu_b$. Therefore, (x_0, y_0) is singular if and only if $\left(\frac{1+w_0}{1+z_0}\right) \in \mu_b$.

Now the point is off the lines $y = x$, $y = x + 1$ if and only if $y_0 \neq x_0, x_0 + 1$. This is equivalent to requiring $w_0 \neq z_0, z_0^{-1}$ □

Theorem 13. *Pigeonhole Criterion: Set $b = \frac{m'-1}{2}$. Let n be the smallest integer such that $b|2^n - 1$, i.e. $\mu_a \subset \mathbb{F}_{2^n}$. If $\frac{b(b-1)}{2} > 2^n - 1$ then there exists singular points p of f_+ off the lines $y = x$ and $y = x + 1$.*

Proof. First, note that n is also the order of 2 mod b. Let $c = \frac{2^n-1}{a}$. The elements of μ_b are the elements of the form w^{ci} for $i = 0, 1, 2, ...b - 1$ where w is a generator for $\mathbb{F}_{2^n}^*$. Consider the set $I = \{1 + w^{ci}\}_{i=1}^{b-1}$. Rewrite the members of this set as $I = \{w^{j_i}\}_{i=1}^{b-1}$ where $1 + w^{ci} = w^{j_i} \in \mathbb{F}_{2^n}$. If any two of the j_i's are the same mod c, say $j_{d_1} \equiv j_{d_2}$, then $\frac{1+w^{cd_1}}{1+w^{cd_2}} = \frac{w^{j_{d_1}}}{w^{j_{d_2}}} = w^{ce} \in \mu_b$ for some integer e. By Theorem 12 this would imply that there exists singular points p off the two lines $y = x$,$y = x+1$ provided w^{cd_1} and w^{cd_2} were distinct and not inverses of each other.

I has $b-1$ distinct elements. If $\frac{b-1}{2} > c$, then by the Pigeonhole Principle, there are more than 3 distinct j_i's that are the same mod c. Thus, there are at least two that do not correspond to elements of μ_b that are inverses of each other, and so there would be singular points off the two lines! Substitute that $c = \frac{2^n-1}{b}$ and we get $\frac{b(b-1)}{2} > 2^n - 1$. □

Conjecture 1. *For almost all integers $m \equiv 3$ (mod 4), h_+ has no singular points off the lines $y = x$ and $y = x + 1$.*

Evidence: Using the computer software package Magma, one can quickly show that up to $m' = 307$, there are no h_+ that have singular points off those two lines except for the few cases where the Pigeonhole Criterion applies. Statistical evidence shows that as m' grows, the "probability" of having points off the two lines $y = x$ and $y = x + 1$ drops quickly.

Let $b = \frac{m'-1}{2}$. Let n, c be defined as in Theorem 13: The Pigeonhole Criterion. We will assume that Theorem 13 does not apply, i.e. $c \geq \frac{b-1}{2}$. Remember that there are singular points off the two lines when the set I as defined in Theorem 13 has more than two j_i's that are the same mod c. There are $\frac{b-1}{2}$ "independent" j_i's (since an element of μ_b and its inverse both map to the same mod c and we discount inverses). Assume that these j_i's really are approximately independent. While this is not completely true (the elements of I have definite structure), as m' grows the j_i's appear to distribute evenly mod c.

With our assumption, we can calculate the probability that two or more of our j_i's are the same mod c. It is $\frac{c!}{\left(c-(\frac{b-1}{2})\right)!c^{\left(\frac{b-1}{2}\right)}}$. Since $c \geq \frac{b-1}{2}$, this is bounded above by $\frac{c!}{(c-c)!c^c} = \frac{c!}{c^c}$. This bounds our birthday probability above and converges to 0 relatively quickly as c increases. For $c = 10$ this probability is already less than .0004. Now $c \geq \frac{b-1}{2} = \frac{\frac{m'-1}{2}-1}{2} = \frac{m'-3}{4}$, so as m' grows, c grows at approximately the same rate, and the "probability" of h_+ having points off the lines $y = x$ and $y = x + 1$ decreases quickly. Note that on average c actually increases faster than m' making our estimate very conservative.

5.2 Other Questions

1. Are there any other power functions that are APN over $\mathbb{F}_{2^n}$ for infinitely many positive integers n?

   Conjecture 2. *The three known cases listed in section 1.4 are the only families of power functions with constant exponents which are APN over $\mathbb{F}_{2^n}$ for infinitely many positive integers n.*

The conjecture has been proved for all but one case of positive exponents and one case of negative exponents; see section 5.1 for the positive case. The Kasami power functions fall in this class and are APN for infinitely many n, but all other monomials in this class appear to be APN over $\mathbb{F}_{2^n}$ for only finitely many positive integers n.

For negative exponents, I am still working on the case $m \equiv 3 \pmod 4$. There are many more types of singularities and bounding the intersection number is more complicated. However, only the already known case of x^{-1} appears to be APN for infinitely many n.

2. As most power functions are APN over only a finite number of fields, what is the largest n for which x^m (or x^{-m}) is APN?

   Weil's Bound [20] contains an estimate as to when x^m can no longer be APN. This bound depends on the genus of the absolutely irreducible factor of h. It appears that most of the time h itself is absolutely irreducible. On this assumption, one could attempt to calculate the bound.

3. What polynomials are APN over $\mathbb{F}_{2^n}$ for infinitely many positive integers n?

   One can extend the investigation from monomials into polynomials. The assumption that $\alpha = 1$ in the definition of APN no longer holds, but rather the restriction must hold in fact for all α. This suggests that perhaps few polynomials will prove to be APN. Recently, a quadratic polynomial was shown to be APN over $\mathbb{F}_{2^{10}}$ in [10]. Byrne and McGuire [4] demonstrated that it was APN over only finitely many extensions of the field of definition. An infinite class of quadratic APN functions has recently been found [3]. Byrne and McGuire [5] are working on the general case of quadratic polynomials.

4. Are there any families of functions that are known to be APN over specific fields?

   Other classes of power functions are known to be APN over $\mathbb{F}_{2^n}$ for specific n (cataloged in [9]). For example, x^{2^m+3} is APN over $\mathbb{F}_{2^{2m+1}}$. Note that here the exponent depends on the field. Data from computer tests gathered in my research indicates that there may be other such classes of mappings.

References

1. R. D. Baker, J. H. van Lint, and R. M. Wilson, On the Preparata and Goethals codes, *IEEE Transactions on Information Theory,* vol. IT-29, 1983, pp. 342-345.

2. T. Beth and C. Ding, On almost perfect nonlinear permutations, Advances in Cryptology - EUROCRYPT '93, T. Helleseth Ed., *Lecture Notes in Computer Science*, vol. 765, Springer-Verlag, Berlin, Germany, 1994, pp 65-76.

3. L. Budaghyan, C. Carlet, P. Felke, G. Leander, An infinite class of quadratic APN functions which are not equivalent to power functions, preprint, http://eprint.iacr.org/2005/359.pdf, 2005.

4. E. Byrne and G. McGuire, Certain new quadratic APN functions are not APN infinitely often, submitted to Proc WCC2005, 2005.

5. E. Byrne and G. McGuire, On the non-existence of quadratic APN and crooked functions on finite fields, submitted to Journal of Algebraic Combinatorics, 2005.

6. C. Carlet, P. Charpin, and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Designs, Codes and Cryptography*, vol. 15, 1998, pp. 125-156.

7. F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, Advances in Cryptology-EUROCRYPT '94, A. De Santis, Ed., *Lecture Notes in Computer Science,* vol. 950, Springer-Verlag, New York, 1995, pp. 356-365.

8. J. Daemen and V. Rijmen, *The Design of Rijndael*, Springer-Verlag, New York, 2002.

9. H. Dobbertin, Almost perfect nonlinear power functions on GF (2^n): The Welch case, *IEEE Transactions on Information Theory,* vol. 45, 1999, pp. 1271-1275.

10. Y. Edel, G. Kyureghyan, and A. Pott, A new APN function which is not equivalent to a power mapping, preprint, http://arxiv.org/abs/math.CO/0506420, 2005.

11. W. Fulton, *Algebraic Curves*, Benjamin, New York, 1969.

12. R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, *IEEE Transactions on Information Theory,* vol. 14, 1968, pp. 154-165.

13. H. Janwa, G. McGuire and R. M. Wilson, Double-error-correcting cyclic codes and absolutely irreducible polynomials over GF(2), *Journal of Algebra*, vol. 178, 1995, pp. 665-676.

14. H. Janwa and R. M. Wilson, Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes, Proceedings of AAEEC-10, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, G. Cohen, T. Mora, and O. Moreno, Eds., *Lecture Notes in Computer Science,* vol. 673, Springer-Verlag, New York, 1993, pp 180-194.

15. T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes, *Information and Control,* vol. 18, 1971, pp. 369-394.

16. R. Lidl and H. Niederreiter, Finite Fields, *Encyclopedia of Math and its Applications*, vol. 20, Cambridge University Press, 2000.

17. J. H. van Lint and R. M. Wilson, On the minimum distance of cyclic codes, *IEEE Transactions on Information Theory,* vol. TI-32, 1986, pp. 23-40.

18. K. Nyberg, Differentially uniform mappings for cryptography. Advances in Cryptology - EUROCRYPT '93, T. Helleseth, Ed., *Lecture Notes in Computer Science*, vol. 765, Springer-Verlag, New York, 1994, pp. 55-64.

19. K. Nyberg and L. R. Knudsen, Provable security against a differential attack," *Journal of Cryptology*, vol. 8, no. 1, 1995, pp. 27-38.

20. A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, *Actualités Sci. Ind.*, no. 1041, Hermann, Paris, 1948.

VITA

David Charles Jedlicka was born in Victoria, Texas on August 11, 1978, the son of Fred and Jane Jedlicka. Growing up in Point Comfort, Texas, he attended high school at nearby Calhoun High School. In 1996, he graduated and entered Rice University in Houston, Texas. He received a Bachelor of Arts degree in mathematics from Rice in May 2000. Then in September 2000, he began work on a Doctorate of Philosophy in the mathematics department of the University of Texas.

Permanent Address: 210 Willowbend Drive, Port Lavaca, Texas 77979

This dissertation was typed by the author.