APN Power Functions Over GF(2^n) for Infinitely Many n

David Jedlicka
University of Texas at Austin
Department of Mathematics
Austin, TX 78712
USA
jedlicka@math.utexas.edu

July 11, 2005

Abstract

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 n. APN functions are useful in constructing S-boxes in AES-like cryptosystems. An application of Weil's theorem 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 three cases, all power functions have such a factor. Two of these cases are already known to be APN for infinitely many fields. The third case is still unproven. Some specific cases of power functions have already been known to be APN over only finitely many fields, but they will mostly follow from the main result below.

Key Words: Almost Perfect Nonlinear (APN), power function, AES S-box, algebraic curve, singularities

1 Introduction

A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is said to be APN (Almost Perfect Nonlinear) or differentially 2-uniform if it has the following property: For all $\alpha \in \mathbb{F}_{2^n} - 0$, $\beta \in \mathbb{F}_{2^n}$,

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

Equivalently, we can look at the polynomial $h(x,y) = f(x+\alpha) - f(x) - f(y+\alpha) + f(y)$ and ask that this has no solutions outside of $x = y$ and $x = y + \alpha$. A theorem by Weil estimates the number of solutions an absolutely irreducible polynomial can have over $\mathbb{F}_q$ as $q + O(\sqrt{q})$. Thus if $h(x,y)$ has an absolutely irreducible factor defined over $\mathbb{F}_2$, then for sufficiently large enough n, $f(x)$ will not be APN over $\mathbb{F}_{2^n}$. Note that when $f(x)$ is a monomial, we may assume $\alpha = 1$ without loss of generality. If there is an α, β pairing for which $f(x)$ fails to be differentially uniform, then $f(x)$ will fail to be differentially uniform for 1, $\frac{\beta}{(\alpha)^{\deg(f)}}$ as well.

Two classes of monomials are already known to be APN over $\mathbb{F}_2$ for infinitely many n. $f(x) = x^{2^k+1}$ is APN over $\mathbb{F}_{2^n}$ provided $(n, k) = 1$. This class was shown to be maximally nonlinear by Gold [6] for odd n which implies APN according to Chabaud and Vaudenay [3, Theorem 4]. This class was shown to be APN for all n provided $(n, k) = 1$ by Janwa and Wilson [8] as well as Nyberg [11].

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

The equivalence of this problem to finding double-error-correcting cyclic codes with minimum distance 5 is discussed in Carlet et al. [2]. Thus, the first class of monomials was also shown to be APN in Baker, Lint, and Wilson [1]. The Kasami power functions were shown to be APN by van Lint and Wilson [10] in the case of odd n and by Janwa and Wilson [8] in the case of even n.

Composing these functions with the Frobenius automorphism (giving functions of the form $x^{(2^a)(2^k+1)}$ or $x^{(2^a)(4^k-2^k+1)}$) also produces APN monomials. I conjecture that these are the only two classes as for all other monomials $h(x, y)$ appears to have an absolutely irreducible factor over $\mathbb{F}_2$.

Conjecture 1. *The two cases listed above are the only families of monomials which are APN over $\mathbb{F}_{2^n}$ for infinitely many n.*

The conjecture has been proved for all but one case of monomials; see section 7.

2 Main Results

Define $h_m(x, y) = (x + 1)^m + x^m + (y + 1)^m + y^m$ and $g_m(x, y) = \frac{h_m(x,y)}{(x+y)(x+y+1)}$. We shall assume for the rest of the paper that we are working over the field $\mathbb{F}_{2^n}$, a large enough field to contain all the singularities of $h_m(x, y)$ and $g_m(x, y)$. We will also assume that m is odd.

Definition 1. *A positive integer m is called* **reduced** *if $m \equiv 3 \pmod 4$. Every m can be reduced in the following way: Let l be the largest integer such that 2^l divides $m - 1$, then the* **reduction** *of m is $m' = \frac{m-1}{2^{l-1}} + 1$.*

Theorem 1. *Let m be an odd integer, $m > 5$ and $m \neq 2^k+1$ for any integer k. Let m' be the reduction of m with l defined as in Definition 1. Let $d = gcd(m-1, 2^l-1) = gcd(\frac{m'-1}{2}, 2^l-1)$. Then, g_m has an absolutely irreducible factor defined over $\mathbb{F}_2$ provided $d < \frac{m'-1}{2}$.*

Two large cases of monomials have already been known to not be APN over $\mathbb{F}_{2^n}$ for infinitely many n. When $m \equiv 3 \pmod 4$, $m > 5$ then g_m is absolutely irreducible. In the case that $d = 1$ and g_m has no singular points off the lines $y = x$ and $y = x + 1$, then g_m is again absolutely irreducible or has an absolutely irreducible factor. These results are proven in Janwa et al. [7] and now follow as special cases of Theorem 1.

In the last open case, when $d = \frac{m'-1}{2}$, there are some results in Section 7, but the general case is still unsolved.

3 General Technique

Let $i(x, y)$ be an affine curve defined over the field $\mathbb{F}_{2^n}$. Let $p = (x_0, y_0)$ be a point on the curve $i(x, y)$, then the multiplicity of p on i, $m_p(i)$, is the degree of the smallest degree term with non-zero coefficients in $i(x + x_0, y + y_0)$. Thus $m_p(i) \geq 1$, and p is a singular point by definition when $m_p(i) \geq 2$. Let I_{m_p} be the homogeneous polynomial composed of the smallest degree terms of $i(x + x_0, y + y_0)$. Then, the linear factors of I_{m_p} are the tangent lines to $i(x, y)$ at p.

Now, two plane curves, u and v, that intersect at p are said to intersect transversally if they have no tangent lines in common at p. The intersection number $I_p(u, v)$ is the unique nonnegative integer satisfying the seven properties listed on pages 74-75 of Fulton [5]. Note that 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 more property I will need which is proven in Janwa et al. [7] is:

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

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. Note that as $I_p(u, v) = 0$ for non-intersection points, the sum can be taken to be over all points in the algebraic closure of $\mathbb{F}_{2^n}$.

The method I will use of proving that $h_m(x, y)$ has an absolutely irreducible factor defined over $\mathbb{F}_2$ will be to compute the intersection number over all possible intersection points and compare this sum to the intersection number that Bezout's Theorem gives for certain factorizations of h_m. I will show that these expressions cannot be equal and thus h_m has an absolutely irreducible factor defined over $\mathbb{F}_2$. This method first appears in the literature in Janwa et al. [7].

4 Singularities

Theorem 2. *Let m be an odd integer with $m > 5$, $m \neq 2^k + 1$ for any $k > 0$. Let m' be the reduction of m with l defined as in Definition 1. The number of affine singularities of g_m 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 h_m, each singularity has multiplicity at 2^l or $2^l + 1$. A singularity has multiplicity exactly $2^l + 1$ on h_m if and only if both $x_0, y_0 \in \mathbb{F}^*_{2^l}$. On g_m, singularities on either of the lines $y = x$*

or $y = x+1$ will have multiplicity one less than they have on h_m; all other singularities will have the same multiplicity on both curves.

Proof. First let us calculate the singularities of

$$(1) \qquad h_m(x,y) = (x+1)^m + x^m + (y+1)^m + y^m.$$

$$(2) \qquad \frac{\partial h}{\partial x} = (x+1)^{m-1} + x^{m-1}$$

$$(3) \qquad \frac{\partial h}{\partial y} = (y+1)^{m-1} + y^{m-1}$$

Singular points (x_0, y_0) must be zeroes of all three of these. Since $2^l|(m-1)$, then over $\mathbb{F}_{2^n}$, equation (2) reduces to $(x_0+1)^{\frac{m-1}{2^{l-1}}} + x_0^{\frac{m-1}{2^{l-1}}} = 0$. But $m'-1 = \frac{m-1}{2^{l-1}}$ so this is equivalent to

$$(4) \qquad (x_0+1)^{m'-1} + x_0^{m'-1} = 0.$$

Equation (3) reduces similarly to

$$(5) \qquad (y_0+1)^{m'-1} + y_0^{m'-1} = 0.$$

If a singular point satisfies equations (1) and (2) then

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

Again, we can take the square root of both sides $l-1$ times to get (6) $x_0^{m'-1} = y_0^{m'-1}$. This proves that the singular points of h_m are the same as $h_{m'}$, although the multiplicity may vary.

Now for any root, x_0, of (4), if we let $y_0 = x_0$ or $y_0 = x_0+1$ then (x_0, y_0) is a singular point of h_m, but there may be more choices for y_0. We can take the square root of equations (4) and (5) one more time. For example, (4) becomes $(x_0+1)^{\frac{m'-1}{2}} + x_0^{\frac{m'-1}{2}} = 0$ which is an equation of degree $\frac{m'-3}{2}$. There are $\frac{m'-3}{2}$ (distinct) choices for x_0.

Now fix an x_0 and let us count the number of possible y_0's. Take the square root of equation (6) and substitute $b = x_0^{\frac{m'-1}{2}}$ to get $y_0^{\frac{m'-1}{2}} = b$. Write m in the form $(\sum_{j=1}^k 2^{i_j}) + 2^l + 1$ for some k where $i_j > i_{j-1}$ and $i_j > l$ for all j. Thus $m' = (\sum_{j=1}^k 2^{i_j-l+1}) + 2 + 1$ and $(\frac{m'-1}{2}) = ((\sum_{j=1}^k 2^{i_j-l}) + 1$.

In this context we can write equation (5) $(y_0+1)^{\frac{m'-1}{2}} + y_0^{\frac{m'-1}{2}} = 0$ as $(\sum_e y_0^e) + y_0^{\frac{m'-1}{2}}$, where the sum runs over all possible partial sums of the terms in the binary expansion of $\frac{m'-1}{2}$. We can cancel out the two top degree terms to get equation (7) $\sum_e y_0^e = 0$ where this sum runs over all possible partial sums except the entire sum.

Now multiply equation (7) by $y_0^{\frac{m'-1}{2} - 2^{i_1-l}}$ substituting in $y_0^{\frac{m'-1}{2}} = b$ for any terms of degree greater than or equal to $\frac{m'-1}{2}$ and call the resulting equation (8). I claim equation

(8) has degree $m' - 1 - 2^{i_1 - l + 1} = m' - 1 - a$ 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 (7) with degree greater than or equal to $2^{i_1 - l}$ is, after the multiplication and substitution, dropped to a term of degree $c - 2^{i_1 - l}$ where c is the original degree. Thus, its degree in (8) is at most $\frac{m'-1}{2} - 1 - 2^{i_1 - l}$. The next largest degree in (7) below $2^{i_1 - l}$ is $\frac{m'-1}{2} - 2^{i_1 - l}$ which becomes a term of degree $m' - 1 - 2^{i_1 - l + 1}$ in (8). Since $\frac{m'-1}{2} - 1 - 2^{i_1 - l} < m' - 1 - 2^{i_1 - l + 1}$, this is the largest degree term in (8) as the claim stated.

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

Lastly, we must calculate the maximum multiplicity of the singular points. Shift h_m by (x_0, y_0).

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

Over any extension of $\mathbb{F}_2$, it is known that $\binom{m}{q} = 0$ for $1 < q < 2^l$. As p is a singular point, it will have multiplicity at least 2. Therefore, the multiplicity is at least 2^l. 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 this is zero. Then,

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

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

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 $2^l + 1$.

Now $g_m = \frac{h_m}{(x+y)(x+y+1)}$ will have at most the same number of singularities with at most the same multiplicity as h_m. This gives us our bound.

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

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

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

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

$$0 = x_0^{m-1} + \frac{x_0^m + x_0^{m - 2^l}}{x_0 + 1}$$

as all singular points obey $(x_0 + 1)^{m-1} = x_0^{m-1}$. Next,

$$0 = \frac{x_0^m + x_0^{m-1} + x_0^m + x_0^{m - 2^l}}{x_0 + 1}$$

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

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

Corollary 1. *Let $m > 5$ be an odd integer. Let m' be the reduction of m with l defined as in Definition 1. The singular points of h_m all have multiplicity 2^l if and only if gcd$(2^l - 1, m' - 1) = 1$.*

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

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

Assume first that there exists a singular point (x_0, y_0) with multiplicity of $2^l + 1$. I shall show the gcd$(2^l-1, m'-1) > 1$. Theorem 2 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 $k \equiv \frac{m'-1}{2}$ mod $(2^l - 1)$. Then x_0 must satisfy $(x_0+1)^k = x^k$. Divide this by x_0^k to get $(1 + \frac{1}{x_0})^k = 1$. Now let $z_0 = \frac{1}{x_0}$ and we can rewrite the equation as $(z_0 + 1)^k = 1$. 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 $z_0 + 1$, ord$(z_0 + 1)$, divides $2^l - 1$ and k. This implies that 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, 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 $k \equiv \frac{m'-1}{2}$ mod $(2^l - 1)$. Then, $d|k$. Let $w_0 \neq 0, 1$ be an element in the subgroup of order d in $\mathbb{F}_{2^l}^*$. Thus $w_0^k = 1$. Let $z_0 = w_0 + 1$ to get $(1 + z_0)^k = 1$. Now let $x_0 = \frac{1}{z_0}$ to get the equation $(1 + \frac{1}{x_0})^k = 1$ which is equivalent to $(x_0 + 1)^k = (x_0)^k$. 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 h_m. As $x_0 \in \mathbb{F}_{2^l}^*$, this singular point has multiplicity $2^l + 1$.

We have thus proven the contrapositive of the bijective statement. □

Theorem 3. *Let $m > 5$ be an odd integer with m' being m's reduction and l defined as in Definition 1. Then provided $m \neq m'$ (i.e. that $m \equiv 1$ (mod 4), g_m has $\frac{m'-1}{2}$ points at infinity. If $m = m'$, then g_m has no singularities at infinity. Let w be a root of $x^{\frac{m'-1}{2}} = 1$.*

If gcd$(m-1, 2^l-1) = d = 1$, then on g_m the singular point $p = (w : 1 : 0)$ has multiplicity

$$m_p = \begin{cases} 2^l - 2, \textit{if } w = 1 \\ 2^l - 1, \textit{else} \end{cases}$$

If gcd$(m - 1, 2^l - 1) = d > 1$, then on g_m the singular point $(w : 1 : 0)$ has multiplicity

$$m_p = \begin{cases} 2^l - 2, \textit{if } w = 1 \\ 2^l, \textit{if } w \neq 1, w^d = 1 \\ 2^l - 1, \textit{else} \end{cases}$$

Proof. First, we will use an unusual projective form of h_m. Let $J_m = (x+z)^m + x^m + (y+z)^m + y^m$. This is the usual projective form of h_m, call it H_m, multiplied by z.

$$\frac{\partial J_m}{\partial x} = (x+z)^{m-1} + x^{m-1}$$

$$\frac{\partial J_m}{\partial y} = (y+z)^{m-1} + y^{m-1}$$

$$\frac{\partial J_m}{\partial z} = (x+z)^{m-1} + (y+z)^{m-1}$$

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

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, $x = 1$, as this is the only root on the lines $y = x$ and $y = x + z$ and it is on both.

For multiplicity, dehomogenize J_m relative to y. Let $x' = \frac{x}{y}$ and $z' = \frac{z}{y}$. Thus, the singular point $(x_0 : 1 : 0)$ becomes $({x'}_0, 0)$. Now look at $H_m = \frac{J_m}{z}$. Note the dehomogenized form of H_m is ${H'}_m = \frac{(x'+z')^m + (x')^m + (z'+1)^m + 1}{z'}$. Now shift by $({x'}_0, 0)$ to get

$${H'}_m(x' + {x'}_0, z' + 0) = \frac{(x' + {x'}_0 + z')^m + (x' + {x'}_0)^m + (z'+1)^m + 1}{z'}.$$

There are no non-zero terms of degree q in the numerator where $1 < q < 2^l$ as $\binom{m}{q} = 0$. One can check that there are no terms of degree less than 2 in the numerator. Consider the terms of degree $2^l - 1$ (of degree 2^l in the numerator). They are:

$$\frac{\binom{m}{2^l}(x'+z')^{2^l}({x'}_0)^{m-2^l} + \binom{m}{2^l}(x')^{2^l}({x'}_0)^{m-2^l} + \binom{m}{2^l}(z')^{2^l}}{z'} = \frac{(z')^{2^l}({x'}_0)^{m-2^l} + (z')^{2^l}}{z'}$$

$$= (z')^{2^l - 1}({x'}_0^{m-2^l} + 1).$$

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 $({x'}_0)^{(gcd(\frac{m'-1}{2}, 2^l - 1)} = 1$.

If $\gcd(\frac{m'-1}{2}, 2^l - 1) = 1$, 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 ${H'}_m(x' + 1, z')$, we can see it has multiplicity 2^l.

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

If $\gcd(\frac{m'-1}{2}, 2^l - 1) = d > 1$ 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 ${H'}_m(x' + {x'}_0, z')$.

$$\frac{(x'+z')^{2^l+1}(x'_0)^{m-2^l-1}+(x')^{2^l+1}(x'_0)^{m-2^l-1}+(z')^{2^l+1}}{z'}$$

$$=\frac{(x')^{2^l}z'(x'_0)^{m-2^l-1}+x'(z')^{2^l}(x'_0)^{m-2^l-1}+(z')^{2^l+1}(1+(x'_0)^{m-2^l-1})}{z'}$$

$$=(x')^{2^l}(x'_0)^{m-2^l-1}+x'(z')^{2^l-1}(x'_0)^{m-2^l-1}+(z')^{2^l}(1+(x'_0)^{m-2^l-1})\neq 0$$

as $x'_0 \neq 0$.

Thus, the multiplicity of these points is exactly 2^l.

This describes the singular points of h_m at infinity. $g_m = \frac{h_m}{(x+y)(x+y+1)}$, 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 g_m but $(1:1:0)$ has multiplicity 2 less.

The last item to discuss is the case when $m = m'$, i.e. $l = 1$. Here, $d = 1$ and the work above shows that all the singular points of h_m except $(1:1:0)$ have multiplicity $2^l - 1$ on g_m which is 1 (i.e. nonsingular) when $l = 1$. Likewise, $(1:1:0)$ has multiplicity $2^l - 2$ on g_m which is 0 when $l = 1$. Thus there are no singular points at infinity in this case. □

5 Tangent Lines

To calculate the intersection number of a singularity we need to calculate the tangent lines.

Theorem 4. *Let $m > 5$ be an odd integer, $m \neq 2^k + 1$ for any integer k. Let m' be the reduction of m. Again, $h_m = (x+1)^m + x^m + (y+1)^m + y^m$ and $g_m = \frac{h_m}{(x+y)(x+y+1)}$. Let $p = (x_0, y_0)$ be a singular point of g_m and let m_p be its multiplicity. Then the tangent lines to g_m at p are the factors of $\frac{(x^{m_p+1}+y^{m_p+1})}{(x+y)}$ if p is on either of the lines $y = x$ or $y = x+1$. If p is not on either of the lines, then the tangent lines of g_m at p are the tangent lines of h_m at p.*

Proof. The tangent lines to g_m at p are the factors of the homogeneous polynomial $P(x,y)$ composed of the lowest degree terms of $g_m(x+x_0, y+y_0)$. Let m_p be the multiplicity of p which is also the degree of P.

First assume that p is on the line $y = x$ or the line $y = x+1$. I claim that the lowest degree terms of h_m centered at p are $P \cdot (x+y)$. By definition $g_m(x+x_0, y+y_0)[(x+x_0+y+y_0)(x+x_0+y+y_0+1)] = h_m(x+x_0, y+y_0)$. Let $g_m(x+x_0, y+y_0) = Q(x,y) + P(x,y)$ where Q are all the terms of degree greater than m_p. Then,

$$h_m(x+x_0,y+y_0) = g_m(x+x_0,y+y_0)[((x+x_0+y+y_0)(x+x_0+y+y_0+1))]$$

$$= g_m(x+x_0,y+y_0)[(x+y)^2+(x+y)(x_0+y_0)+(x+y)(x_0+y_0+1)+(x_0+y_0)(x_0+y_0+1)].$$

As p is on $y = x$ or $y = x + 1$,

$$= g_m(x + x_0, y + y_0)[(x + y)^2 + (x + y)(1) + 0]$$

$$= g_m(x + x_0, y + y_0)[(x + y)^2 + (x + y)]$$

$$= [Q\{(x + y)^2 + (x + y)\} + P\{(x + y)^2\}] + P\{x + y\}.$$

The terms in brackets all have degree greater than $m_p + 1$ while $P\{x + y\}$ has degree $m_p + 1$. Thus, the lowest degree terms of $h_m(x + x_0, y + y_0)$ are exactly the lowest degree terms of $g_m(x + x_0, y + y_0)$ times $(x + y)$.

The lowest degree terms of

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

must be of the form $b_1x^{m_p+1} + b_2y^{m_p+1}$ with $b_1, b_2 \in \mathbb{F}_{2^n}$. However, since the terms must be divisible by $(x + y)$, clearly $b_1 = b_2 \neq 0$. Thus, $P = \frac{b_1(x^{m_p+1}+y^{m_p+1})}{(x+y)}$ and we may ignore the constant b_1.

Second, assume that p is on neither $y = x$ nor $y = x + 1$. Now,

$$h_m(x + x_0, y + y_0) = g_m(x + x_0, y + y_0)[(x + x_0 + y + y_0)(x + x_0 + y + y_0 + 1)]$$

$$= g_m(x + x_0, y + y_0)[(x + y)^2 + (x + y) + (x_0 + y_0)(x_0 + y_0 + 1)]$$

$$= [Q + P][(x + y)^2 + (x + y) + (x_0 + y_0)(x_0 + y_0 + 1)]$$

Let k be the non-zero constant $(x_0 + y_0)(x_0 + y_0 + 1)$.

$$= [Q\{(x + y)^2 + (x + y) + k\} + P\{(x + y)^2 + (x + y)\}] + kP$$

Every term in brackets has degree greater than m_p while the term outside brackets has degree m_p. kP is the polynomial composed of the lowest degree terms of $h_m(x+x_0, y+y_0)$. The lowest degree terms of h_m must be of the form $c_1x^{m_p} + c_2y^{m_p}$ for some $c_1, c_2 \in \mathbb{F}_{2^n}$. Clearly, at least one of c_1, c_2 is nonzero by the definition of m_p and P.

In the case that $\gcd(m - 1, 2^l - 1) = 1$ (the most common case), then Corollary 1 shows that both are nonzero. In fact, c_1 is precisely zero when $x_0 \in \mathbb{F}_{2^l}$ and similarly for c_2.

In the case that both are nonzero, then if $m_p = 2^l$ we get 2^l copies of the same line $c_3x + c_4y$ (where c_3, c_4 are the 2^lth roots of c_1, c_2 respectively). If $m_p = 2^l + 1$ then we get distinct tangent lines.

In the case that exactly one of them is zero, then we get m_p copies of either x or y for the tangent lines. □

Corollary 2. *Consider the singular points p of g_m that are on the lines $y = x$ and $y = x+1$. They have multiplicity $m_p = 2^l$ or $2^l - 1$. The tangent lines to g_m at p in the case $m_p = 2^l$ are the factors of $\frac{(x^{2^l+1}+y^{2^l+1})}{(x+y)}$ which are unique. The tangent lines to g_m at p in the case $m_p = 2^l - 1$ are $2^l - 1$ copies of $x + y$.*

Proof. Just apply Theorem 4 and Theorem 2. □

Lemma 2. *Consider the singular points $p = (x_0, y_0)$ with multiplicity m_p on g_m that are on the lines $y = x$ and $y = x + 1$. Then the terms of degree $m_p + 1$ in $g_m(x + x_0, y + y_0)$ are the terms of degree $m_p + 2$ in $h_m(x + x_0, y + y_0)$ after dividing by $x + y$ and then subtracting the terms of degree $m_p + 1$ in $h_m(x + x_0, y + y_0)$.*

Proof. Start as in the proof of Theorem 4, but let $g_m(x + x_0, y + y_0) = R + Q + P$ where P is the polynomial composed of the terms of degree m_p, Q is the polynomial composed of the terms of degree $m_p + 1$ and R is the polynomial composed of the terms of degree greater than $m_p + 1$. Then, we get that

$$h_m(x+x_0, y+y_0) = [R\{(x+y)^2+(x+y)\}+Q(x+y)^2]+[Q(x+y)+P(x+y)^2]+[P(x+y)].$$

The terms of degree $m_p + 2$ in $h_m(x + x_0, y + y_0)$ are the terms in the second set of brackets. □

Theorem 5. *The tangent lines of g_m at a singular point at infinity, $p = (w : 1 : 0)$ for $w \neq 1$ are the factors of the lowest degree terms of h_m. In the case $w = 1$, the tangent lines are the factors of the lowest degree terms of h_m divided by $(x')(x' + z')$.*

Proof. Recall w is a root of $x^{\frac{m'-1}{2}} = 1$. The tangent lines of g_m at p are the factors of the polynomial composed of the lowest degree terms of $g_m(x' + w, z')$ when we dehomogenize relative to y and recenter at p. Call this polynomial $P(x', z')$. Let m_p be the multiplicity of p on g_m which is also the degree of $P(x', z')$.

Now $g_m(x' + w, z') = Q(x', z') + P(x', z')$ where Q is the polynomial composed of the terms of degree greater than m_p.

$$h_m(x' + w, z') = g_m(x' + w, z')[(x' + w + 1)(x' + z' + w + 1)]$$

$$= (Q + P)[(x')(x' + z') + (w + 1)(z') + (w + 1)^2]$$

$$= \{Q[(x')(x' + z') + (w + 1)(z') + (w + 1)^2] + P[(x')(x' + z') + (w + 1)(z')\} + P[(w + 1)^2]$$

Every term in braces has degree greater than m_p while the term outside has degree exactly m_p. In fact, the terms of lowest degree in $h_m(x' + w, z')$ are exactly the lowest degree terms in $g_m(x' + w, z')$ times a constant.

In the case $w = 1$ then

$$h_m(x' + w, z') = g_m(x' + w, z')[(x' + w + 1)(x' + z' + w + 1)]$$

$$= g_m(x' + w, z')[(x')(x' + z')]$$

and so the terms of lowest degree in g_m are the terms of lowest degree (degree $m_p + 2$) in h_m divided by $(x')(x' + z')$. □

Corollary 3. *The tangent lines to the singular points at infinity of g_m are described below. Let $gcd(m - 1, 2^l - 1) = d$. Recall that if $l = 1$ (i.e. m is reduced) then there are no singular points at infinity. Let $p = (w : 1 : 0)$ where w is a root of $x^{\frac{m'-1}{2}} = 1$.*

If $d = 1$, then the tangent lines are $\begin{cases} \textit{the distinct factors of } \frac{(x')^{2^l-1}+(z')^{2^l-1}}{(x'+z')}, \textit{if } w = 1 \\ 2^l - 1 \textit{ copies of the line } z', \textit{if } w \neq 1 \end{cases}$

If $d \neq 1$, then the tangent lines are $\begin{cases} \textit{the distinct factors of } \frac{(x')^{2^l-1}+(z')^{2^l-1}}{(x'+z')}, \textit{if } w = 1 \\ 2^l - 1 \textit{ copies of the line } z', \textit{if } w \neq 1, w^d \neq 1 \\ \textit{the distinct factors of } r(x', z'), \textit{if } w \neq 1, w^d = 1 \end{cases}$
where $r(x', z') = (x')^{2^l} w^{m-2^l-1} + x'(z')^{2^l-1} w^{m-2^l-1} + (z')^{2^l}(1 + w^{m-2^l-1})$.

Proof. For $d = 1, w \neq 1$, then the terms of degree $m_p = 2^l - 1$ where $p = (w : 1 : 0)$ in $h_m(x' + w, z')$ are equal to $(z')^{2^l-1}(1 + w^{m-2^l})$ by Theorem 3. Thus, the tangent lines are all z'.

For $d = 1, w = 1$, then the terms of degree $m_p = 2^l$ in $h_m(x' + w, z')$ are $\frac{(x')^{2^l}+x'(z')^{2^l-1}}{x'(x'+z')} = \frac{(x')^{2^l-1}+(z')^{2^l-1}}{(x'+z')}$.

For $d > 1, w = 1$, then the tangent lines are the same factors as in the case $d = 1, w = 1$.

For $d > 1, w^d \neq 1$ then we get the same tangent lines as in the case $d = 1, w \neq 1$, all copies of z'.

For the last case where $d > 1, w^d = 1, w \neq 1$, then the tangent lines are the factors of

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

It is easy to check that all the roots of this polynomial are distinct. □

6 Proof of Main Results

First a lemma which will show that it is unimportant whether or not g_m factors over the ground field.

Lemma 3. *If g_m has no absolutely irreducible factors over $\mathbb{F}_2$, then $e = \frac{I_{tot}}{\frac{(m-3)^2}{4}} \geq \frac{8}{9}$ where I_{tot} is any upper bound on the global intersection number of u and v for all factorizations $g_m = u \cdot v$ over the algebraic closure of $\mathbb{F}_2$.*

Proof. First, assume that g_m is irreducible over $\mathbb{F}_2$ but not absolutely irreducible. Let c be the number of factors of g_m when it splits over the algebraic closure of $\mathbb{F}_2$. The degree of each factor is $\frac{m-3}{c}$. Let I_{tot} be any upper bound on the global intersection number of u and v for all factorizations of $g_m = u \cdot v$ over the algebraic closure of $\mathbb{F}_2$. Let $e = \frac{I_{tot}}{\frac{(m-3)^2}{4}}$.

If c is even, then we can find a factorization $g_m = u \cdot v$ so that $\deg(u) = \deg(v)$ and so $(\deg(u))(\deg(v)) = \frac{(m-3)^2}{4}$. By Bezout's Theorem, $\sum_p I_P(u,v) = (\deg(u))(\deg(v))$. This implies that $\frac{(m-3)^2}{4} \leq I_{tot}$ and thus that $e \geq 1$.

If c is odd, $c \geq 3$, then we find a factorization so that $\deg(u) = \deg(v) + \frac{m-3}{c}$ implying that $\deg(v) = \frac{m-3}{2}(1 - \frac{1}{c})$. Therefore, $(\deg(u))(\deg(v)) = \frac{(m-3)^2}{4}(1 - \frac{1}{c^2})$. Bezout's Theorem implies $\frac{(m-3)^2}{4}(1 - \frac{1}{c^2}) \leq I_{tot}$ and thus that $(1 - \frac{1}{c^2}) \leq e$. Since $c \geq 3$ we clearly must have $e \geq \frac{8}{9}$.

Thus, regardless of the parity of c, $e \geq \frac{8}{9}$.

Now consider the case where g_m factors over $\mathbb{F}_2$. Let $g_m = e_1 e_2 ... e_r$ where each e_i is irreducible over $\mathbb{F}_2$ and $r \geq 2$. Assume that every e_i factors over some extension. Then over the algebraic closure of $\mathbb{F}_2$ each e_i factors into c_i conjugates each of degree $\frac{(\deg(e_i))}{c_i}$.

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 g_m such that $\deg(u) - \deg(v) \leq \frac{m-3}{3}$. Given that $\deg(u) + \deg(v) = m - 3$, we have that $(\deg(u))(\deg(v)) \geq \frac{(m-3)^2}{4}(\frac{8}{9})$. Since $I_{tot} \geq (\deg(u))(\deg(v))$ by Bezout's Theorem and $e = \frac{I_{tot}}{\frac{(m-3)^2}{4}}$, we get again that $e \geq \frac{8}{9}$.

Therefore regardless of whether g_m is irreducible over $\mathbb{F}_2$, $e \geq \frac{8}{9}$. □

The following two theorems, Theorem 6 and Theorem 7, when combined give the main result. First, let $d = \gcd(m-1, 2^l - 1) = \gcd(\frac{m'-1}{2}, 2^l - 1)$.

Theorem 6. *Let m be an odd integer, $m > 5$ and $m \neq 2^k + 1$ for any integer k. Let m' be the reduction of m with l defined as in Definition 1. Assume $d = 1$. Then, g_m has an absolutely irreducible factor defined over $\mathbb{F}_2$.*

Proof. First, assume for contradiction that g_m has no absolutely irreducible factors over $\mathbb{F}_2$. Lemma 3 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 $g_m = u \cdot v$ over the algebraic closure of $\mathbb{F}_2$. We need to calculate an estimate of I_{tot}, the global intersection number.

Claim 1: $I_p(u,v) = 0$ for all affine singular points on the lines $y = x$, $y = x + 1$.

Proof of claim: By Corollary 1, all the affine singular points of h_m that occur on the lines $y = x$ or $y = x + 1$ have multiplicity 2^l and thus on g_m they have multiplicity $2^l - 1$. By Theorem 4, the tangent lines of g_m at an affine singular point $p = (x_0, y_0)$ are the factors of $(x+y)^{2^l - 1}$. Define G_i to be the polynomial composed of the terms of $g_m(x + x_0, y + y_0)$ of degree i and H_i to be the polynomial composed of the terms of $h_m(x + x_0, y + y_0)$ of degree i. From Theorem 2, $G_{2^l} \neq 0$. We already know $G_{2^l - 1} = (x+y)^{2^l - 1}$. By Lemma 2, $H_{2^l + 1} = G_{2^l}(x+y) + G_{2^l - 1}(x+y)^2$. Thus, the $\gcd(G_{m_p+1}, G_{m_p}) = \gcd(G_{2^l}, G_{2^l - 1}) = \gcd(G_{2^l} + G_{2^l - 1}(x+y), G_{2^l - 1}) = \gcd(\frac{H_{2^l+1}}{(x+y)}, G_{2^l - 1})$.

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

$$H_{2^l+1} = x^{2^l+1}(x_0+1)^{m-2^l-1} + x^{2^l+1}x_0^{m-2^l-1} + y^{2^l+1}(y_0+1)^{m-2^l-1} + y^{2^l+1}y_0^{m-2^l-1}$$

$$H_{2^l+1} = x^{2^l+1}[(x_0+1)^{m-2^l-1} + x_0^{m-2^l-1}] + y^{2^l+1}[(y_0+1)^{m-2^l-1} + y_0^{m-2^l-1}]$$

$$H_{2^l+1} = [(x_0+1)^{m-2^l-1} + x_0^{m-2^l-1}](x^{2^l+1} + y^{2^l+1}) \text{ as } y_0 = x_0 \text{ or } y_0 = x_0+1.$$

Let $k = [(x_0+1)^{m-2^l-1} + x_0^{m-2^l-1}]$ and $k \neq 0$ as $H_{2^l+1} \neq 0$. Thus,

$$H_{2^l+1} = k[x^{2^l+1} + y^{2^l+1}].$$

$$\frac{H_{2^l+1}}{(x+y)} = k[x^{2^l} + x^{2^l-1}y + x^{2^l-2}y^2 + ... + xy^{2^l-1} + y^{2^l}]$$

Note that as $G_{2^l-1} = (x+y)^{2^l-1}$, we have that $\gcd(\frac{H_{2^l+1}}{(x+y)}, G_{2^l-1}) \neq 1$ if and only if $(x+y)|\frac{H_{2^l+1}}{(x+y)}$. However, if we let $y = x$, then $\frac{H_{2^l+1}}{(x+y)} = kx^{2^l} \neq 0$, so $(x+y) \nmid \frac{H_{2^l+1}}{(x+y)}$, and thus $\gcd(\frac{H_{2^l+1}}{(x+y)}, G_{2^l-1}) = 1$.

Therefore, by Lemma 1 as $\gcd(G_{m_p}, G_{m_p+1}) = 1$ and there is only one tangent line at p, $I_p(u,v) = 0$ for all affine singular points p, as the claim stated.

Claim 2: We can bound the sum of the intersection numbers at all affine points by $\sum_p I(u,v) \leq 2^l(\frac{m'-3}{2})(m'-a-3)$ if $l > 1$. When $l = 1$, $\sum_p I(u,v) = 0$.

Proof of claim: Let $p = (x_0, y_0)$ be a singular point not on the lines $y = x$, $y = x+1$. By Corollary 1, p has multiplicity of 2^l on both h_m and on g_m. From Theorem 4 and its proof, as $m_p = 2^l$ and $d = 1$, the tangent lines are 2^l identical copies of the line $x + by$ for some constant b. From Theorem 2 we know that $G_{2^l} \neq 0$ and $G_{2^l+1} \neq 0$. Next we will show that $\gcd(G_{2^l}, G_{2^l+1}) = 1$.

Using work similar to Theorem 4, let $g_m(x+x_0, y+y_0) = R + G_{2^l+1} + G_{2^l}$ where R is the polynomial composed of all the terms of degree greater than 2^l+1. Then,

$$h_m(x+x_0,y+y_0) = g_m(x+x_0,y+y_0)[(x+x_0+y+y_0)(x+x_0+y+y_0+1)]$$

$$= [R + G_{2^l+1} + G_{2^l}][(x+y)^2 + (x+y) + (x_0+y_0)(x_0+y_0+1)]$$

If we let $b = (x_0+y_0)(x_0+y_0+1)$, then

$$h_m(x+x_0,y+y_0) = \{R[(x+y)^2 + (x+y) + b] + G_{2^l+1}[(x+y)^2 + (x+y)] + G_{2^l}[(x+y)^2]\} +$$

$$+\{bG_{2^l+1} + G_{2^l}[x+y]\} + bG_{2^l}$$

Note that the terms in the second set of braces compose the polynomial H_{2^l+1}, and $H_{2^l} = bG_{2^l}$. Then,

$$\gcd(G_{2^l}, G_{2^l+1}) = \gcd(G_{2^l}, bG_{2^l+1}) = \gcd(G_{2^l}, bG_{2^l+1} + G_{2^l}[x+y]) =$$
$$= \gcd(bG_{2^l}, H_{2^l+1}) = \gcd(H_{2^l}, H_{2^l+1})$$

Now, from $h_m(x+x_0, y+y_0) = (x+x_0+1)^m + (x+x_0)^m + (y+y_0+1)^m + (y+y_0)^m$, we can calculate

$$H_{2^l+1} = [(x_0+1)^{m-2^l-1} + x_0^{m-2^l-1}]x^{2^l+1} + [(y_0+1)^{m-2^l-1} + y_0^{m-2^l-1}]y^{2^l+1} = c_1 x^{2^l+1} + c_2 y^{2^l+1}$$

$$H_{2^l} = [(x_0+1)^{m-2^l} + x_0^{m-2^l}]x^{2^l} + [(y_0+1)^{m-2^l} + y_0^{m-2^l}]y^{2^l} = d_1 x^{2^l} + d_2 y^{2^l}$$

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

The only factor they could have in common then is $d_3 z + 1$ (equivalently, $d_3 x + y$). They have this factor in common precisely when the singular point (x_0, y_0) satisfies $\frac{y_0(y_0^{2^l-1}+1)^{2^l+1}}{(y_0+1)^{2^l}} = \frac{x_0(x_0^{2^l-1}+1)^{2^l+1}}{(x_0+1)^{2^l}}$ by Lemma 4. Call this equation C.

If $l = 1$, then p cannot satisfy equation C and we have $\gcd(H_{2^l+1}, H_{2^l}) = 1$. As $\gcd(G_{2^l}, G_{2^l+1}) = 1$ and there is only one tangent line at p, by Lemma 1 $I_p(u,v) = 0$. Thus the sum over all affine singularities is zero, i.e. $\sum_p I_p(u,v) = 0$.

If $l > 1$, then there may exist singular points off of the lines $y = x, y = x+1$ that satisfy equation C above. From lemma 5, we can bound the intersection number of these singular points by 2^l and by Theorem 2 we have at most $(\frac{m'-3}{2})(m'-a-3)$ of these points (where $a = 2^{\lfloor \log_2(m') \rfloor}$). Thus, we can bound the sum of the intersection numbers at all affine intersection points, i.e. $\sum_p I(u,v) \leq 2^l(\frac{m'-3}{2})(m'-a-3)$, as Claim 2 stated.

Claim 3: The sum of the intersection numbers at infinity is bounded above by $(2^{l-1}-1)^2$ if $l > 1$. When $l = 1$, there are no singular points at infinity, so $\sum I_p(u,v) = 0$.

Proof of claim: In the case that m is reduced (i.e. $l = 1$), then there are no singular points at infinity by Theorem 3.

In the case that m is not reduced, consider now the singular point $p = (1:1:0)$ at infinity. By Theorem 3, this has multiplicity $m_p = 2^l - 2$ and the tangent lines are all distinct. Therefore $I_p(u,v) = m_p(u) \cdot m_p(v)$. Also $m_p(u) + m_p(v) = 2^l - 2$. This gives us the bound $I_p(u,v) \leq \frac{(2^l-2)^2}{4}$.

Lastly, let $p = (w:1:0)$ be one of the other singular points at infinity where w is a root of $x^{\frac{m'-1}{2}} = 1$. By Theorem 3, they all have multiplicity $m_p = 2^l - 1$ and the tangent lines are identical copies of $z' = z/y$.

Take the projective form of h_m and dehomogenize it relative to y. Call this $h'_m = \frac{(x'+z')^m + (x')^m + (z'+1)^m + (z')^m}{z'}$. Thus $g'_m = \frac{h'_m}{(x'+1)(x'+z'+1)}$. Let G'_i be the polynomial composed of the terms of $g'_m(x'+w,z')$ of degree i, and let H'_i be the polynomial composed of the terms of $h'_m(x'+w,z')$ of degree i

As in Theorem 5, let $g'_m(x'+w,z') = R + G'_{2^l} + G'_{2^l-1}$ where R is the polynomial composed of all the terms of degree greater than 2^l. Then,

$$h'_m(x'+w,z') = g'_m(x'+w,z')[(x'+w+1)(x'+z'+w+1)]$$

$$= g'_m(x'+w,z')[x'(x'+z') + z'(w+1) + (w+1)^2]$$

$$= \{R[x'(x'+z') + z'(w+1) + (w+1)^2] + G'_{2^l}[x'(x'+z') + z'(w+1)] + G'_{2^l-1}[x'(x'+z')]\} +$$

$$+\{G'_{2^l}[(w+1)^2] + G'_{2^l-1}[z'(w+1)]\} + \{G'_{2^l-1}[(w+1)^2]\}$$

Note that the terms in the second set of braces compose H'_{2^l}. Now $\gcd(G_{m_p+1}, G_{m_p}) = \gcd(G'_{2^l}, G'_{2^l-1}) = \gcd(G'_{2^l}(w+1)^2 + G'_{2^l-1}(z')(w+1), G'_{2^l-1}) = \gcd(H'_{2^l}, G'_{2^l-1})$. Recall $G'_{2^l-1} = (z')^{2^l-1}$, so $\gcd(H'_{2^l}, G'_{2^l-1}) \neq 1$ if and only if $z'|H'_{2^l}$. As

$$S(x',z') = \frac{(x'+z')^{2^l+1}w^{m-2^l-1} + (x')^{2^l+1}w^{m-2^l-1} + (z')^{2^l+1}}{z'}$$

clearly $z' \nmid H'_{2^l}$. Also, because there is only one tangent line at p, Lemma 1 implies that $I_p(u,v) = 0$.

Thus the sum over all the singularities at infinity is $\sum_p I_p(u,v) \leq \frac{(2^l-2)^2}{4} = (2^{l-1}-1)^2$ as Claim 3 stated.

In the case that $l = 1$, all together the claims imply that $\sum_p I_p(u,v) = 0$ where the sum runs over all projective points. Combined with Bezout's Theorem this implies that g_m is absolutely irreducible.

In the case $l > 1$, the claims imply that $\sum_p I_p(u,v) \leq (2^{l-1}-1)^2 + 2^l(\frac{m'-3}{2})(m'-a-3)$ 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), and we may assume $l > 1$ as the case $l = 1$ has already led to a contradiction. 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 $(2^{l-1}-1)^2 + 2^l(\frac{m'-3}{2})(m'-a-3)$.

$\frac{m-1}{2^l} \geq 3$ since $m \neq 2^k+1$ for any k 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 $(2^{l-1}-1)^2 < \frac{(m-1)^2}{36}$.

$$e = \frac{(2^{l-1}-1)^2 + 2^l(\frac{m'-3}{2})(m'-a-3)}{\frac{(m-3)^2}{4}} < \frac{\frac{(m-1)^2}{36} + (m-3)(m'-a-3)}{\frac{(m-3)^2}{4}}$$

$$< \frac{\frac{(m-1)^2}{9} + 4(m-3)(\frac{(m'-1)}{2} - 1)}{(m-3)^2} \leq \frac{1}{7} + 2\frac{(m'-3)}{(m-3)}$$

with the $\frac{1}{7}$ coming from the fact that for $m > 20$, $\frac{(m-1)^2}{9(m-3)^2} \leq \frac{1}{7}$.

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 $e < .65$ which is less than $\frac{8}{9}$ yielding 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. Since any affine singular points that have nonzero intersection number must also satisfy equation C, we can bound the number of such points by $(\frac{m'-3}{2})(1 + (2^l - 1)(2^l + 1) - 2^l - 2) = (\frac{m'-3}{2})(2^l - 2)(2^l + 1)$ instead of $(\frac{m'-3}{2})(m' - a - 3)$. 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 $l = 2$.

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

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

Lemma 4. *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 Theorem 6 have a common factor precisely when there exists a singular point* (x_0, y_0) *of* h_m *that satisfies* $\frac{y_0(y_0^{2^l-1}+1)^{2^l+1}}{(y_0+1)^{2^l}} = \frac{x_0(x_0^{2^l-1}+1)^{2^l+1}}{(x_0+1)^{2^l}}$.

Proof. Singular points satisfy the equations

$$(1) \quad x_0^{m-1} = y_0^{m-1} \qquad (2) \quad (x_0 + 1)^{m-1} = x_0^{m-1} \qquad (3) \quad (y_0 + 1)^{m-1} = y_0^{m-1}$$

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

$$(4) \quad (\frac{c_1}{c_2})^{2^l} = (\frac{d_1}{d_2})^{2^l+1}.$$

From the proof of Theorem 6, $c_1 = (x_0 + 1)^{m-2^l-1} + x_0^{m-2^l-1}$ and $c_2 = (y_0 + 1)^{m-2^l-1} + y_0^{m-2^l-1}$. Using equations (2) and (3), 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,

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

Next, from the proof of Theorem 6 $d_1 = (x_0+1)^{m-2^l} + x_0^{m-2^l}$. 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,

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

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

Substituting what we know into equation (4) 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 is equivalent to

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

as desired. □

Lemma 5. *Let everything be defined as in Theorem 6. If $p = (x_0, y_0)$ is a singular point off the lines $y = x$, $y = x+1$ which satisfies the equation C given in Lemma 4, then the intersection number is bounded above by 2^l, i.e. $I_p(u,v) \leq 2^l$.*

Proof. Let $m_p = 2^l$, the multiplicity of p on g_m and h_m. 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. Let G_i be the polynomial composed of the terms of $g(x+x_0, y+y_0)$ of degree i. Similarly for H_i, U_i and V_i.

From previous work we can summarize the following:

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

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

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

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

where α_1 is a constant.

Thus, $G_{m_p} = U_rV_s = t^{2^l}$ and $G_{m_p+1} = U_rV_{s+1} + U_{r+1}V_s$.

Note that $\gcd(H_{m_p}, H_{m_p+1}) = t$ implying that $\gcd(G_{m_p}, G_{m_p+1}) = t$ by the proof of Theorem 6. As the degrees of U_r and V_s are both positive and $U_rV_s = t^{2^l}$, 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 $\gcd(G_{m_p}, G_{m_p+1}) > t$, 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 $r = 2^l - 1$).

Now, since $t^2 \nmid G_{m_p+1}$, $t \nmid U_{r+1}$ implying as well that $U_{r+1} \neq 0$.

As $s = 1$, p is a simple point on V, hence by Fulton [5] (page 81), $I_p(U, V) = \text{ord}_p^V(U)$ in the discrete valuation ring $O_p(V)$. Any line not tangent to G at p can be taken as a uniformizing parameter, let us pick x. Note that if $\text{ord}(\alpha) < \text{ord}(\beta)$ then the $\text{ord}(\alpha + \beta) = \text{ord}(\alpha)$.

First, $\text{ord}(U_r) = \text{ord}(U_{2^l-1}) = \text{ord}(t^{2^l-1}) > 2^l$ as $\text{ord}(t) \geq 2$. Second, let us write U_{2^l} as $\prod_{j=1}^{2^l}(\alpha_jx + \beta_jt) = \alpha x^{2^l} + O(x^{2^l+1})$ 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 $I_p(U, V) = \text{ord}(U) = 2^l$ as desired. □

Theorem 7. *Let m be an odd integer, $m > 5$ and $m \neq 2^k + 1$ for any integer k. Let m' be the reduction of m with l defined as in Definition 1. Assume $d > 1$. Then g_m has an absolutely irreducible factor defined over $\mathbb{F}_2$ provided $d < \frac{m'-1}{2}$.*

Proof. First, assume for contradiction that g_m has no absolutely irreducible factors over $\mathbb{F}_2$. Lemma 3 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 $g_m = u \cdot v$ over the algebraic closure of $\mathbb{F}_2$. We need to calculate an estimate for I_{tot}.

Claim 1: The sum of the intersection number at all affine singularities is bounded above by $2(d-1)(2^{l-1})^2 + (d-1)(d-3)(2^{l-1})(2^{l-1}+1) + (2^l)((\frac{m'-3}{2})(m'-a-3) - (d-1)(d-3))$.

Proof of claim: Let $p = (x_0, y_0)$ be an affine singularity of g_m. From Theorem 2 and Corollary 1, we have five types of affine singularities.

For singularities with multiplicity 2^l on h_m that satisfy either $y = x$ or $y = x + 1$ Claim 1 of the proof of Theorem 6 shows $I_p(u, v) = 0$.

Singularities with multiplicity $2^l + 1$ on h_m that are on either of the two lines above have multiplicity of 2^l on g_m and $x_0, y_0 \in \mathbb{F}_{2^l}^*$. Corollary 1 shows there are at most $2(d-1)$ of these as there are $d - 1$ choices for x_0 and then 2 choices for y_0. Theorem 4 shows that the tangent lines to g_m at p are all distinct. Therefore, $I_p(u, v) \leq (2^{l-1})^2$.

For singular points with multiplicity $2^l + 1$ on h_m that are not on either of the two lines $y = x$, $y = x + 1$, Theorem 4 shows that the tangent lines of g_m are all distinct and thus the intersection number is bounded above by $(2^{l-1})(2^{l-1} + 1)$. There are at most $(d-1)(d-3)$ of these by Corollary 1.

For singular points with multiplicity 2^l on h_m that are on neither of the two lines, there are two possibilities: either one of x_0, y_0 is in $\mathbb{F}_{2^l}^*$ or neither are. In the case that neither are, then Claim 2 of Theorem 6 bounds the intersection number by 2^l. There are at most $(\frac{m'-3}{2})(m' - a - 3) - (d-1)(d-3)$ of them, where $a = 2^{\lfloor \log_2(m') \rfloor}$.

In the last case, assume for simplicity that $y_0 \in \mathbb{F}_{2^l}^*$ but x_0 is not. From Theorem 4, the tangent lines to g_m at p would be 2^l copies of x. However, by Theorem 2 and Corollary 1, $H_{2^l+1} = c_1 x^{2^l+1} + c_2 y^{2^l+1}$ for some $c_1, c_2 \neq 0$. Clearly, $x \nmid H_{2^l+1}$. Note that $H_{2^l} = bG_{2^l}$ for some constant b, and so $\gcd(H_{2^l}, H_{2^l+1}) = 1$. As in Theorem 6, this implies $\gcd(G_{2^l}, G_{2^l+1}) = 1$. Therefore, Lemma 1 implies $I_p = 0$.

Thus, the sum of the intersection numbers over all affine points is less than or equal to $2(d-1)(2^{l-1})^2 + (d-1)(d-3)(2^{l-1})(2^{l-1}+1) + (2^l)((\frac{m'-3}{2})(m'-a-3) - (d-1)(d-3))$, as Claim 1 stated.

Claim 2: The sum of the intersection numbers at infinity is bounded above by $(2^{l-1}-1)^2 + (d-1)(2^{l-1})^2$.

Proof of claim: Recall Theorems 3 and 5 and Corollary 3. At infinity, we still have the singular point $(1:1:0)$ with $I_p \leq (2^{l-1}-1)^2$. We also have the singular points $(w:1:0)$ where w is a root of $x^{\frac{m'-1}{2}} = 1$ and $w^d \neq 1$ which have $I_p = 0$. For singular points $(w:1:0)$ where $w^d = 1, w \neq 1$ then we have 2^l distinct tangents and so $I_p \leq (2^{l-1})^2$. There are $d-1$ of these. Then as Claim 2 stated, 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.

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

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

Since we are assuming $1 < d < \frac{m'-1}{2}$ and d 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'. Now, using calculus one can easily show that $\hat{e}$ is a decreasing function of l for positive l. Therefore, for $l \geq 3$,

$$\begin{aligned}\hat{e} &\le \frac{4(m'-3)(m'-a-3)-8(d-1)(d-3)+48(d-1)+20(d-1)(d-3)+16}{\frac{(4(m'-1)-2)^2}{4}} \\ &= \frac{(m'-3)(m'-a-3)+12(d-1)+3(d-1)(d-3)+4}{(m'-\frac{3}{2})^2} \\ &\le \frac{(m'-3)(\frac{m'-1}{2}-3)+12(d-1)+3(d-1)(d-3)+4}{(m'-\frac{3}{2})^2} \\ &\le \frac{\frac{1}{2}(m'-3)(m'-7)+12(d-1)+3(d-1)(d-3)+4}{(m'-\frac{3}{2})^2}\end{aligned}$$

Note that for a fixed d, as m' grows $\hat{e}$ approaches $\frac{1}{2}$. Now recall that $d|\frac{m'-1}{2}$ and as we are assuming $d \neq \frac{m'-1}{2}$ we know that $d \le \frac{m'-1}{6}$. Substitute this in.

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

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 so $e < \hat{e} < \frac{7}{12}$ contradicting that $e \ge \frac{8}{9}$.

Now consider the case $l = 2$. As in the proof of Theorem 6 we will use the other method of counting singular points off the lines $y = x$, $y = x + 1$. Then

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

For $l = 2$, it becomes

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

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

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

Again, as $d \neq \frac{m'-1}{2}$, we know that $d \le \frac{m'-1}{6}$. 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 $m' \ge 5$ and our assumptions imply $m' \ge 19$. Calculations show that for $m' \ge 27$, $e < .86 < \frac{8}{9}$, a contradiction. We can check by hand the remaining numbers, $m' = 19$ and 23 for $l = 2$, and g_m is absolutely irreducible in these cases. Thus for all l and m', provided $d \neq \frac{m'-1}{2}$, g_m has an absolutely irreducible factor defined over $\mathbb{F}_2$. □

7 The Last Case, $d = \frac{m'-1}{2}$

All monomials have been classified as either APN over infinitely fields $\mathbb{F}_{2^n}$ 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. All other monomials in this case appear to not be.

This case actually gives us no problems except when g_m has affine singular points off the lines $y = x, y = x + 1$ something that is statistically rare. If all affine singular points fall on these two lines then the following corollary to Theorem 7 shows that g_m has an absolutely irreducible factor defined over $\mathbb{F}_2$.

Corollary 4. *Let m be an odd integer, $m > 5$ and $m \neq 2^k + 1$ for any integer k. Let m' be the reduction of m with l defined as in Definition 1. Assume $d = \frac{m'-1}{2}$. If all affine singular points fall on the lines $y = x$, $y = x + 1$ then g_m has an absolutely irreducible factors over $\mathbb{F}_2$, provided $m \neq 13$.*

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

Thus, we can bound the global intersection number by

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

Recall $e = \frac{I_{tot}}{\frac{(m-3)^2}{4}}$. Loosen the bound by letting $\hat{e} = \frac{3(d-1)(2^{l-1})^2 + (2^{l-1})^2}{\frac{(m-3)^2}{4}}$. We can rewrite this as

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

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

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

The bound above is a decreasing function of m' for $m' \geq 3$, and for $m' \geq 11$, $e < \hat{e} \leq \frac{52}{81} < \frac{8}{9}$, a contradiction!

For the last case $m' = 7$, we know that $d = 3$. 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 g_m has an absolutely irreducible factor defined over $\mathbb{F}_2$. □

Alternatively, if one can show that g_m is irreducible over $\mathbb{F}_2$, something that appears to be true for all $m \geq 5$, then one can show that for $m \equiv 1, 2 \pmod 3$, g_m is absolutely irreducible in the following way. If g_m is irreducible but not absolutely irreducible, then it splits into say c conjugates over some extension. Using the global intersection number estimates in Theorem 7, one can easily show 2 things. First, c must be odd (since $\hat{e} < 1$). Second, $c < .87\sqrt{m'}$. The first is helpful since for $m \equiv 1, 2 \pmod 3$, g_m has the smooth point $(\omega, 0)$ in $\mathbb{F}_{2^2}$, where $\omega^2 + \omega + 1 = 0$. This implies that if g_m factors, it does so in $\mathbb{F}_{2^2}$ and thus c is even, a contradiction.

The method used in this paper fails to give a general solution in this last case as the estimate of the global intersection number 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 g_m can have (under the reasonable assumption that g_m is irreducible over $\mathbb{F}_2$); see the last paragraph of Section 7. Perhaps this bound can lead to a contradiction if one could show that g_m should have more factors, but I have been unable to prove this. The number of factors that g_m has when $2^l - 1 = \frac{m'-1}{2}$ suggest that this method may work though.

8 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. C. Carlet, P. Charpin, and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.*, vol. 15, no. 2, 1998, pp. 125-156.

3. 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, Berlin, Germany, 1995, pp. 356-365.

4. 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.

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

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

7. 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.

8. H. Janwa and R. M. Wilson, Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings AAEEC-10, G. Cohen, T. Mora, and O. Moreno,

Eds., *Lecture Notes in Computer Science,* vol. 673, Springer-Verlag, New York/Berlin, 1993.

9. T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes, *IEEE Transactions on Information Theory,* vol. 18, 1971, pp. 369-394.

10. J. J. 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.

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