Abstract

I present some results towards a complete classification of monomials 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 [A. Weil, Sur les courbes algébriques et les variétés qui s’en déduisent, in: Actualités Sci. Ind., vol. 1041, Hermann, Paris, 1948] 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 specific, narrowly defined cases, all monomials have such a factor over a finite field of characteristic 2. Two of these cases, those with exponents of the form $2^k + 1$ or $4^k - 2^k + 1$ for any integer $k$, are already known to be APN for infinitely many fields. The last, relatively rare case when a certain gcd is maximal is still unproven; my method fails. Some specific, special cases of power functions have already been known to be APN over only finitely many fields, but they also follow from the results below.

© 2007 Elsevier Inc. All rights reserved.

Keywords: Almost Perfect Nonlinear (APN); Monomial; AES S-box; Irreducible

1. Introduction and results

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

$$\#\{x \in \mathbb{F}_{2^n} \mid \phi(x + \alpha) - \phi(x) = \beta\} \leq 2. \quad (*)$$
For a function $\phi$ to be APN over $\mathbb{F}_{2^n}$, there cannot be an $\alpha$, $x$, 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 $y = x + \alpha$. Let $\phi(x) = x^m$ for the rest of the paper. We will assume that $m$ is odd, $m > 5$, and that $m \neq 2^k + 1$ for any integer $k$ as these monomials are already well studied. We may also assume without loss of generality that $\alpha = 1$. If there is an $\alpha, \beta$ pairing for which $\phi(x)$ fails to be differentially uniform, then $\phi(x)$ will fail to be differentially uniform for $1, \frac{\beta}{\alpha^{\deg(\phi)}}$ as well. This motivates the following definition.

**Definition 2.** Define $f(x, y) = (x + 1)^m + x^m + (y + 1)^m + y^m$ and $h(x, y) = \frac{f(x, y)}{(x+y)(x+y+1)}$.

Thus, $\phi$ 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 $y = x + 1$. While $f$ and $h$ explicitly depend on the parameter $m$ for simplicity I shall suppress the $m$ in the notation. 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 $f(x, y)$ and $h(x, y)$. The following definition will be used throughout the paper.

**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 $d = \gcd(m - 1, 2^l - 1) = \gcd(m - 1, 2^l - 1)$.

Note that $l = 1$ implies $m \equiv 3 \pmod{4}$.

The previously known results as well as a summary of my results are summarized in Table 1.

Two classes of monomials are already known to be APN over $\mathbb{F}_{2^n}$ for infinitely many $n$. $\phi(x) = x^{2^k + 1}$ 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, Kasami power functions, $\phi(x) = x^{4^k - 2^k + 1}$, is known to be APN over $\mathbb{F}_{2^n}$ also provided $(n, k) = 1$. They were shown to be APN by Welch (unpublished, see Dillon [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 et al. [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 $x^{(2^n)(2^k + 1)}$ or $x^{(2^n)(4^k - 2^k + 1)}$) also produces APN monomials. I conjecture that these are the only

<table>
<thead>
<tr>
<th>Function</th>
<th>APN for large $n$?</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^{2^j+1}$ for $\gcd(n, j) = 1$</td>
<td>Yes</td>
<td>Gold [6], Janwa and Wilson [8]</td>
</tr>
<tr>
<td>$x^{4^j-2^j+1}$ for $\gcd(n, j) = 1$</td>
<td>Yes</td>
<td>Welch [unpublished]</td>
</tr>
<tr>
<td>$x^m$ for $m \equiv 3 \pmod{4}$ and $m &gt; 3$</td>
<td>No</td>
<td>Janwa et al. [7]</td>
</tr>
<tr>
<td>$x^m$ for $d = 1$, $h$ has no singularities off the lines $y = x$ and $y = x + 1$</td>
<td>No</td>
<td>Janwa et al. [7]</td>
</tr>
<tr>
<td>$x^m$ for $d &lt; \frac{m-1}{2^l}$, $m &gt; 5$</td>
<td>No</td>
<td>Jedlicka</td>
</tr>
<tr>
<td>$x^{-m}$ for $m \equiv 1 \pmod{4}$, $m &gt; 5$</td>
<td>No</td>
<td>Jedlicka</td>
</tr>
</tbody>
</table>

Table 1
All known results including this paper
two classes because for all other monomials, \( f(x, y) \) appears to have an absolutely irreducible factor over \( \mathbb{F}_2 \).

**Conjecture 1.** The two cases, \( 2^k + 1 \) and \( 4^k - 2^k + 1 \), listed above are the only families of monomials with constant exponents which are APN over \( \mathbb{F}_{2^n} \) for infinitely many \( n \).

The conjecture has been proved for all but one special case of monomials; see Section 6. A version of this conjecture is mentioned in Janwa et al. [7].

Two large special classes 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 et al. [7] and also follow from Theorem 1.

In the last open case, when \( d = \frac{m-1}{2} \), there are some results in Section 6, but the general case is still unproved. 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 \( n \).

My main result is the following theorem and its importance is explained in the results of the corollary.

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

**Corollary 1.** If \( h \) has an absolutely irreducible factor over \( \mathbb{F}_2 \), then \( \phi(x) = x^m \) is not APN over \( \mathbb{F}_{2^n} \) for large enough \( n \).

**Proof.** Following Lidl and Niederreiter [9, p. 365], let \( p(x, y) \) be the absolutely irreducible factor of \( h \), and let \( d \) be its degree. Then there are at most \( 2d \) rational points on \( p \) with either \( y = x \) or \( y = x + 1 \). Let \( P \) be the number of total rational points on \( p \) over \( \mathbb{F}_{2^n} \). The Weil bound shows that \( |P - (2^n + 1)| \leq 2g\sqrt{2^n} \) where \( g \) denotes the genus of \( p \). For sufficiently large \( n \), the total number of points will exceed \( 2d \) and thus \( f \) will have a zero off the lines \( y = x \) and \( y = x + 1 \). Therefore, \( \phi(x) = x^m \) will not be APN over \( \mathbb{F}_{2^n} \) for large enough \( n \). □

2. Definitions and general technique

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 nonzero 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 \( F_{m_p} \).
Lemma 1. Let $I_p(u,v)$ be an affine curve defined over $\mathbb{F}_2$ 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 $\text{dim}_K(O_p(\mathbb{A}^2)/(u,v))$, where $K$ is the field $\mathbb{F}_2$ 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 [5, 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 et al. [7] is the following.

Lemma 1. Let $J(x, y) = 0$ be an affine curve defined over $\mathbb{F}_q$ for positive integer $q$, and let $J(x, y) = u(x, y) \cdot v(x, y)$. Write $J(x + a, y + b) = J_m + J_{m+1} + \cdots$ 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 transversally 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 [12] states that the number of rational points, $N$, over $\mathbb{F}_q$ 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 $\gamma$ 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 $y = x + \alpha$.

Definition 5. Let $\tilde{f}$ be the usual homogenized, projective form of $f$. Define $\tilde{f}$ to be the dehomogenized form of $\tilde{f}$ relative to $y$, redefining $x = \frac{x}{y}$ and $z = \frac{z}{y}$. As in the affine case, for any nonnegative integer $T$, define $F_T$ 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, the global intersection number equals the product of the degrees of the curves, i.e. $\sum_p I_p(u,v) = d_u \cdot d_v$ where the sum runs over all points of intersection. For a proof, see Fulton [5, pp. 112–115]. This theorem shows that the intersection number is the proper way to count the multiplicity of an intersection point. 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 $\mathbb{F}_2^n$.

Lucas’s theorem gives a useful formula for computing $\binom{a}{b} \mod 2$. Writing $a = a_j 2^j + a_{j-1} 2^{j-1} + \cdots + a_1 2 + a_0$ and $b = b_j 2^j + b_{j-1} 2^{j-1} + \cdots + b_1 2 + b_0$, 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 $\binom{a}{b} = 0$ for $1 < q < 2^l$.

The method I will use of proving that $h$ has 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. Lemma 11 will show that we can find factorization whose global intersection number, the sum of the intersection number at all intersection points, is at least a certain size.
### Table 2
All singularities of \( h \)

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>( mp(h) )</th>
<th>( I_p ) bound</th>
<th>Max number of points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ia</td>
<td>Affine, on a line, ( x_0, y_0 \in F_{2}^{*} )</td>
<td>( 2^l )</td>
<td>( (2^l-1)^2 )</td>
<td>( 2(d-1) )</td>
</tr>
<tr>
<td>Ib</td>
<td>Affine, on a line, ( x_0, y_0 \notin F_{2}^{*} )</td>
<td>( 2^l - 1 )</td>
<td>0</td>
<td>( m' - 3 )</td>
</tr>
<tr>
<td>IIA</td>
<td>Affine, off both lines, ( x_0, y_0 \in F_{2}^{*} )</td>
<td>( 2^l + 1 )</td>
<td>( 2^l-1(2^l-1+1) )</td>
<td>( (d-1)(d-3) )</td>
</tr>
<tr>
<td>IIB</td>
<td>Affine, off both lines, exactly one of ( x_0, y_0 \in F_{2}^{*} )</td>
<td>( 2^l )</td>
<td>0</td>
<td>Not important</td>
</tr>
<tr>
<td>IIC</td>
<td>Affine, off both lines, ( x_0, y_0 \notin F_{2}^{*} )</td>
<td>( 2^l )</td>
<td>( 2^l ) if ( l &gt; 1 )</td>
<td>( (\frac{m'-3}{2})(m'-a-3) - (d-1)(d-3) ) and ( (\frac{m'-3}{2})(2^l-2)(2^l+1) )</td>
</tr>
<tr>
<td>IIIA</td>
<td>( (1 : 1 : 0) )</td>
<td>( 2^l - 2 )</td>
<td>( (\frac{2^l-2}{2})^2 )</td>
<td>1</td>
</tr>
<tr>
<td>IIIB</td>
<td>( (w : 1 : 0), w^d = 1, w \neq 1 )</td>
<td>( 2^l )</td>
<td>( (2^l-1)^2 )</td>
<td>( d-1 )</td>
</tr>
<tr>
<td>IIIC</td>
<td>( (w : 1 : 0), w^d \neq 1 )</td>
<td>( 2^l - 1 )</td>
<td>0</td>
<td>Not important</td>
</tr>
</tbody>
</table>

These two bounds will often lead to a contradiction. The basic idea behind this method first appears in the literature in Janwa et al. [7].

### 3. Singularities

**Theorem 2.** The singular points of \( h \) are described in Table 2. If \( m \equiv 3 \pmod{4} \), then \( h \) has no singularities at infinity (Type III).

The proof will follow from Lemmas 2–10 and their corollaries. Note that if \( m \equiv 3 \pmod{4} \), then \( d = l = 1 \) and so according to the chart, there will be no points with multiplicity greater than 1, i.e. no singular points. 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. Let \( a \) denote the largest power of 2 less than \( m' \), i.e. \( a = 2^{\lfloor \log_2(m') \rfloor} \). Also, \( w \) is a root of \( x^{m'-1} = 1 \).

**Lemma 2.** The affine 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,

\[
(x_0 + 1)^{m-1} = x_0^{m-1},
\]

\[
(y_0 + 1)^{m-1} = y_0^{m-1}.
\]

Now, take Eqs. (1) and (2) and multiply them by \( x_0 + 1 \) and \( y_0 + 1 \), respectively, to get

\[
(x_0 + 1)^{m} = x_0^{m} + x_0^{m-1},
\]

\[
(y_0 + 1)^{m} = y_0^{m} + y_0^{m-1}.
\]
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 3.** The total number of affine singularities of \( f \) (Types I and II) is at most \( \left( \frac{m'-3}{2} \right)(m' - 1 - a) \) where \( a \) is the largest power of 2 less than \( m' \), i.e. \( a = 2^{\left\lfloor \log_2(m') \right\rfloor} \). 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 \( x_0, y_0 \in \mathbb{F}_2^* \). 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 2, the singular points \( (x_0, y_0) \) of \( f \) are precisely the solutions to the following three equations:

\[ \begin{align*}
  x_0^{m-1} &= y_0^{m-1}, \\
  (x_0 + 1)^{m-1} &= x_0^{m-1}, \\
  (y_0 + 1)^{m-1} &= y_0^{m-1}.
\end{align*} \]

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

\[ \begin{align*}
  \frac{m'-1}{2} x_0 &= \frac{m'-1}{2} y_0, \\
  \frac{m'-1}{2} (x_0 + 1) &= \frac{m'-1}{2} x_0, \\
  \frac{m'-1}{2} (y_0 + 1) &= \frac{m'-1}{2} y_0.
\end{align*} \]

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

Equation (9) has at most \( \frac{m'-3}{2} \) roots. Now for any root, \( x_0 \), of (9) 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 \( \alpha = x_0^{m'-1} \) and substitute this into Eq. (8) to get \( y_0^{m'-1} = \alpha \). 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 Eq. (10) as \((\sum_v y_0^v + \frac{m'-1}{2}) = 0\), 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
\[
\sum_v y_0^v = 0
\]
(11)
where the asterisk indicates that this sum runs over all possible partial sums except \(v \neq \frac{m'-1}{2}\).

Now multiply Eq. (11) by \(\frac{m'-1}{2} - 2ib-l\) substituting in \(\frac{m'-1}{2} = \alpha\) 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 \(m' - 1 - 2ib-l\) and \(m' < 2ib-l\) in \(E\). Thus, its degree in \(E\) is at most \(\frac{m'-1}{2} - 1 - 2ib-l\). By Lucas’s theorem, the next largest degree in (11) below \(2ib-l\) is \(\frac{m'-1}{2} - 2ib-l\). To be more specific, since \(2ib-l\) 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 Eq. (11) would be the sum of all other powers of 2 that occur, i.e. \(\frac{m'-1}{2} - 2ib-l\). That next largest exponent then becomes a term of degree \(m' - 1 - 2ib-l+1\) in \(E\). Since \(\frac{m'-1}{2} - 1 - 2ib-l < m' - 1 - 2ib-l+1\), this is the largest degree term in \(E\) as the claim stated.

Thus, we have at most \(m' - 1 - \alpha\) choices for \(y_0\) and the maximum number of affine singularities for \(f\) and \(h\) is \((\frac{m'-3}{2})(m' - 1 - \alpha)\).

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 \(\mathbb{F}_2\), \((\frac{m}{q}) = 0\) 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,
\[
0 = ((x_0+1)^{m-2^l-1} + x_0^{m-2^l-1})(x_0+1)^{2l} = x_0^{m-2^l-1}.
\]
This implies \(x_0 = 0\), a contradiction. Thus, the coefficient of \(x^{2^l+1}\) is nonzero, and so the multiplicity of \((x_0, y_0)\) is at most \(2^l + 1\).

The polynomial \(h = \frac{f}{(x+y)(x+y+1)}\) 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,
implies \( x_0^{2j-1} = 1 \) which is equivalent to \( x_0 \in \mathbb{F}_{2^j}^* \). The same must apply to \( y_0 \). Every step is reversible, so the implication is if and only if. \( \square \)

**Corollary 2.** The affine singular points of \( f \) all have multiplicity \( 2^j \) if and only if \( d = \gcd(2^j - 1, m' - 1) = 1 \). There are \( 2(d - 1) \) singularities of Type Ia and \( (d - 1)(d - 3) \) singularities of Type IIa. Therefore, there are at most \( \left( \frac{m' - 2}{2} \right)(m' - a - 3) - (d - 1)(d - 3) \) singularities of Type IIc.

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

\[
\frac{m'-1}{x} = x_0^{m'-1}, \quad \frac{m'-1}{x} = y_0^{m'-1}, \quad \text{and} \quad \frac{m'-1}{y} = y_0^{m'-1}.
\]

Assume first that there exists a singular point \((x_0, y_0)\) with multiplicity of \( 2^j + 1 \). I shall show the \( \gcd(2^j - 1, m' - 1) > 1 \). Lemma 3 shows that a singular point having multiplicity of exactly \( 2^j + 1 \) implies that \( x_0, y_0 \in \mathbb{F}_{2^j}^* \). Thus \( x_0 \) also satisfies \( x_0^{2j-1} = 1 \) and \( (x_0 + 1)^{2j-1} = 1 \). Note that \( x_0 \neq 0, 1 \).

Let \( j \equiv \frac{m'-1}{2} \mod (2^j - 1) \). 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 \( z_0, z_0 + 1 \in \mathbb{F}_{2^j}^* \) and so \( (z_0 + 1)^{2^j-1} = 1 \). Thus the order of \( z_0 + 1 \), \( \text{ord}(z_0 + 1) \), divides \( 2^j - 1 \) and \( j \). This implies that \( \text{ord}(z_0 + 1) \mid \frac{m'-1}{2} \). Since the order divides both \( 2^j - 1 \) and \( \frac{m'-1}{2} \), it divides their \( \gcd \). However, \( \text{ord}(z_0 + 1) > 1 \) and so \( \gcd(2^j - 1, \frac{m'-1}{2}) > 1 \).

Now assume that \( \gcd(2^j - 1, \frac{m'-1}{2}) = d > 1 \). Again, let \( j \equiv \frac{m'-1}{2} \mod (2^j - 1) \). Then, \( d \mid j \).

Let \( w_0 \neq 1 \) be an element in the subgroup of order \( d \) in \( \mathbb{F}_{2^j}^* \). 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 \((1 + \frac{1}{z_0})^j = 1 \) 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 \( x_0, y_0 \in \mathbb{F}_{2^j}^* \), this singular point has multiplicity \( 2^j + 1 \).

We have thus proven the contrapositive of the if and only if statement. Clearly there are only \( 2(d - 1) \) singularities of Type Ia as the subgroup of order \( d \) in \( \mathbb{F}_{2^j}^* \), 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 \( y_0 \) that does not satisfy \( y = x \) nor \( y = x + 1 \), there are \( (d - 1)(d - 3) \) singularities of Type IIa. Given the bound in the total number of affine singularities in Lemma 3, there are at most \( \left( \frac{m'-2}{2} \right)(m' - a - 3) - (d - 1)(d - 3) \) singularities of Type IIc. This bound may be able to be improved, but it is sufficient for our purposes. \( \square \)
Lemma 4. 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 \( p = (w : 1 : 0) \) has multiplicity
\[
m_p = \begin{cases} 
2^l - 2 & \text{if } w = 1 \text{ (Type IIIa)}, \\
2^l & \text{if } w \neq 1, w^d = 1 \text{ (Type IIIb)}, \\
2^l - 1 & \text{else (Type IIIc).}
\end{cases}
\]

Proof. First, we will use an unusual projective form of \( w \) singular points at infinity. Let \( \text{Lemma 4}. \) If
\[
m \equiv 1014 \mod 4.
\]
These, \( x \) equation so it becomes \( x \) simplifications,
\[
\frac{\partial h}{\partial x} = (x + z)^{m-1} + x^{m-1},
\]
\[
\frac{\partial h}{\partial y} = (y + z)^{m-1} + y^{m-1},
\]
\[
\frac{\partial h}{\partial z} = (x + z)^{m-1} + (y + z)^{m-1}.
\]

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, \( \frac{\partial h}{\partial x} = 0, \frac{\partial h}{\partial y} = 0 \) and \( \frac{\partial h}{\partial z} = x_0^{m-1} + 1 \). We may take the \( 2^l \) th 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 nonzero 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)
\[
\binom{m}{2^l}(x + z)^{2^l}x_0^{m-2^l} + \binom{m}{2^l}x_0^m - 2^l + \binom{m}{2^l}z^{2^l} = z^{2^l-1}(x_0^{m-2^l} + 1).
\]

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 \( \tilde{f} \).
\[
\frac{(x + z)^{2^l+1}(1) + x^{2^l+1} + z^{2^l+1}}{z} = x^{2^l} + xz^{2^l-1} \neq 0.
\]
Lemma 5. Let $H_{mp}(h)$ be the factors of $y$ tangent lines to $h$ in $\tilde{h}(x + x_0, z):$

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

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

This describes the singular points of $f$ at infinity, $\hat{f} = \frac{f}{(x+y)(x+y+z)}$, 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 $\hat{f}$ 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.

4. $I_p$ bounds

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

Lemma 5. 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 $F_{mp+2} = H_{mp+1}(x + y) + H_{mp}(x + y)^2$ and $F_{mp+1} = H_{mp}(x + y)$. Also, the tangent lines to $h$ at $p$ are the factors of $f(x_0, y_0) = (x_0 + y_0)^{-1}$, 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, $H_{mp}$, composed of the lowest degree terms of $h(x + x_0, y + y_0)$.

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

$$f(x + x_0, y + y_0) = h(x + x_0, y + y_0)\left[\left((x + x_0 + y + y_0)(x + x_0 + y + y_0 + 1)\right]\right]$$

$$= [R + H_{mp+1} + H_{mp}]\left[(x + y)^2 + (x + y)\right]$$

$$= R\left[(x + y)^2 + (x + y)\right] + H_{mp+1}(x + y)^2 + H_{mp} (x + y)^2 + \left[H_{mp+1}(x + y) + H_{mp}(x + y)^2\right] + H_{mp}(x + y)^2].$$

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, $F_{mp+2} = H_{mp+1}(x + y) + H_{mp}(x + y)^2$. The terms of degree $m_p + 1$ are those in the last set of brackets, and thus $F_{mp+1} = H_{mp}(x + y)$. The lowest degree terms of $f(x + x_0, y + y_0)$ must be of the form $b_1x^{m_{p+1} + y} + b_2y^{m_{p+1}}$ for constants $b_1, b_2$. However, since the terms must be divisible by $(x + y)$, clearly $b_1 = b_2 = 0$. Thus, $H_{mp} = b_1(x^{m_{p+1} + y} + y^{m_{p+1}})$ and so the tangent lines to $h$ at $p$ are the factors of $f(x_0, y_0)$.
Corollary 3. For Type Ia singularities, \( I_p(u, v) \leq (2^l - 1)^2 \).

**Proof.** These singular points have multiplicity \( 2^l \) on \( h \) and \( x_0, y_0 \in \mathbb{F}^*_2 \). Lemma 5 shows that the tangent lines to \( h \) at \( p \) are the factors of \( \frac{(x^2 + y^2 + 1)}{(x+y)} \) 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 \( (2^l)^2 \). Therefore, \( I_p(u, v) \leq (2^l - 1)^2 \). \( \square \)

Corollary 4. For Type Ib singularities, \( I_p(u, v) = 0 \).

**Proof.** By Lemma 3 and Corollary 2, Type Ib singularities have multiplicity \( 2^l - 1 \) on \( h \). By Lemma 5, 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 3, \( H_{2^l - 1} \neq 0 \) as \( x_0, y_0 \notin \mathbb{F}^*_2 \). We already know \( H_{2^l - 1} = b_1(x+y)^{2^l-1} \) for some constant \( b_1 \). By Lemma 5, \( F_{2^l-1} = H_{2^l-1}(x+y) \). Thus, \( \gcd(H_{m_p+1}, H_{m_p}) = \gcd(H_{2^l-1}, H_{2^l-1}) = \gcd(F_{2^l+1}, H_{2^l-1}) = \gcd((x+y)^{2^l-1}, H_{2^l-1}) \). From \( F(x + x_0, y + y_0) \), we can easily calculate \( F_{2^l+1} \):

\[
F_{2^l+1} = x^{2^l+1}(x + x_0)^{m-2^l-1} + (x_0 + y_0)^m + (y + y_0)^m,
\]

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 \( \gcd(F_{2^l+1}, H_{2^l-1}) = 1 \). 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 Ib. \( \square \)

Lemma 6. Let \( p \) be a singular point of 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,

\[
f(x + x_0, y + y_0) = h(x + x_0, y + y_0)[(x + x_0 + y + y_0)(x + x_0 + y + y_0 + 1)]
\]

\[
= [R + H_{m_p+1} + H_{m_p}][(x + y)^2 + (x + y) + c]
\]

\[
= \{ R[(x + y)^2 + (x + y) + c] + H_{m_p+1}[(x + y)^2 + (x + y)]
\]

\[
+ H_{m_p}[(x + y)^2] \} + \{ cH_{m_p+1} + H_{m_p}[x + y] \} + cH_{m_p}.
\]

Note that the terms in the last set of braces compose the polynomial \( F_{m_p+1} \), and \( F_{m_p} = cH_{m_p} \). \( \square \)
Corollary 5. For Type IIa 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 6, \( cH_{mp} = F_{mp} \) 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 \( c_1x^{mp} + c_2y^{mp} \) for some constants \( c_1, c_2 \neq 0 \). As \( m_p = 2^l + 1 \) is odd, the tangent lines are all distinct. Therefore, \( I_p(u, v) \leq (2^l-1)(2^l-1+1). \) □

Corollary 6. For Type IIb 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 6, \( cH_{mp} = F_{mp} \) 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 \( c_1x^{mp} + c_2y^{mp} \) for some constants \( c_1, c_2 \). As \( y_0 \in \mathbb{F}_{2^l}^* \) then \( c_2 = 0 \) from the proof of Lemma 3; 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 3, \( F_{2^l+1} = c_1x^{2^l+1} + c_2y^{2^l+1} \) for some \( c_1, c_2 \neq 0. \) Thus
\[
1 = \gcd(F_{2^l+1}, F_{2^l}) = \gcd(c_{H_{2^l+1}} + H_{2^l}(x+y), c_{H_{2^l}}) = \gcd(H_{2^l+1}, H_{2^l}).
\]
Therefore Lemma 1 implies \( I_p = 0. \) □

Lemma 7. For Type IIc singularities, \( I_p(u, v) \leq 2^l. \) If \( l = 1, \) then \( I_p(u, v) = 0. \) Also, there are at most \( \frac{(m-3)(2^l-2)(2^l+1) - (d-1)(d-3)}{2} \) 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 \( 2^l \) on both \( f \) and on \( h. \) The lowest degree terms of \( f \) must be of the form \( c_1x^{mp} + c_2y^{mp} \) for some constants \( c_1, c_2 \) and \( m_p = 2^l. \) As the multiplicity is \( 2^l, \) Lemma 3 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 6 and the proof of Corollary 6, \( \gcd(H_{2^l}, H_{2^l+1}) = \gcd(F_{2^l}, F_{2^l+1}). \) Now,
\[
F_{2^l+1} = (x_0 + 1)^{m-2^l-1} x_0^{m-2^l-1} + (x_0 + 1)^{m-2^l-1} y_0^{m-2^l-1} y^{2^l+1} + c_1x^{2^l+1} + c_2y^{2^l+1},
\]
\[
F_{2^l} = (x_0 + 1)^{m-2^l-1} x_0^{m-2^l-1} + (y_0 + 1)^{m-2^l-1} y^{2^l+1} = d_1x^{2^l} + d_2y^{2^l}.
\]
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 \( c_3 = \frac{2^l \sqrt{c_1}}{c_2}. \)
The factors of \( F_{2^l} \) are equivalent to the factors of \( (d_3z)^{2^l} + 1 \) where \( d_3 = \frac{2^l \sqrt{d_1}}{d_2}. \)
The only factor they could have in common then is \( d_3z + 1 \) (equivalently, \( d_3x + y). \) By Lemma 8 below, they have this factor in common precisely when the singular point \( p = (x_0, y_0) \) satisfies
\[
(x_0 + 1)^{2^l} y_0^{2^l+1} = (y_0 + 1)^{2^l} x_0^{2^l+1} (x_0^{2^l-1} + 1)^{2^l+1}. \quad (12)
\]
If \( l = 1 \), then \( p \) cannot satisfy Eq. (12) as \( y_0 \neq x_0 \) and \( y_0 \neq x_0 + 1 \). Therefore \( \gcd(F_{2l+1}, F_{2l'}) = 1 \) which implies \( \gcd(H_{2l+1}, H_{2l'}) = 1 \). 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 Eq. (12). However, if \( x_0, y_0 \in \mathbb{F}_2^3 \), we get a solution to Eq. (12), and there are \( (d - 1)(d - 3) \) such solutions. As \( x_0, y_0 \notin \mathbb{F}_2^3 \), we can actually bound the number of these singularities with nonzero intersection number by \( \frac{m - 3}{2}(2^l - 2)(2^l + 1) - (d - 1)(d - 3) \). \( \square \)

**Lemma 8.** The polynomials \( S = c_1 x^{2l+1} + c_2 y^{2l+1} \) and \( T = d_1 x^{2l} + d_2 y^{2l} \) as defined in Lemma 7 have a common factor precisely when there exists a singular point \( (x_0, y_0) \) of \( f \) that satisfies \( (x_0 + 1)^2 y_0(y_0^{2l-1} + 1)^{2l+1} = (y_0 + 1)^2 x_0(x_0^{2l-1} + 1)^{2l+1} \).

**Proof.** Singular points satisfy the equations

\[
\begin{align*}
x_0^{m-1} &= y_0^{m-1}, \\
(x_0 + 1)^{m-1} &= x_0^{m-1}, \\
(y_0 + 1)^{m-1} &= y_0^{m-1}.
\end{align*}
\]

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

\[
\left( \frac{c_1}{c_2} \right)^{2l} = \left( \frac{d_1}{d_2} \right)^{2l+1}.
\]

From the proof of Lemma 7, we have that

\[
c_1 = (x_0 + 1)^{m-2l-1} + x_0^{m-2l-1} \quad \text{and} \quad c_2 = (y_0 + 1)^{m-2l-1} + y_0^{m-2l-1}.
\]

Using Eqs. (14) and (15), we can easily write them as \( c_1 = \frac{x_0^{m-2l-1}}{(x_0+1)^{2l}} \) and \( c_2 = \frac{y_0^{m-2l-1}}{(y_0+1)^{2l}} \). Thus,

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

Next, from the proof of Lemma 7, \( d_1 = (x_0 + 1)^{m-2l} + x_0^{m-2l} \). We can rewrite it as
\[ d_1 = \frac{(x_0 + 1)^{m-2^l} + x_0^{m-2^l}(x_0 + 1)^{2^l}}{(x_0 + 1)^{2^l}} = \frac{(x_0 + 1)(x_0 + 1)^{m-1} + x_0^{m-2^l}(x_0 + 1)^{2^l}}{(x_0 + 1)^{2^l}}. \]

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

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

Substituting what we know into Eq. (16) gives the equivalent

\[ \frac{y_0^{2^l}}{x_0^{2^l}} \frac{(y_0 + 1)^{2^l}}{(y_0^{2^l-1}+1)} \frac{y_0^{2^l-1}}{x_0^{2^l-1}} \frac{(y_0 + 1)^{2^l}y_0^{2^l-1}}{x_0^{2^l-1}(y_0 + 1)^{2^l}(y_0^{2^l-1}+1)(2^l+1)} \]

which, as desired, simplifies to

\[ (x_0 + 1)^{2^l}y_0(y_0^{2^l-1}+1)^{2^l+1} = (y_0 + 1)^{2^l}x_0(y_0^{2^l-1}+1)^{2^l+1}. \]

**Lemma 9.** Let everything be defined as in Lemma 7. If \( p = (x_0, y_0) \) is a singular point of \( f \) off of the lines \( y = x, y = x + 1 \) which satisfies Eq. (17) from Lemma 8, 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:

\[ H_{m_p} + H_{m_p+1} + H_{m_p+2} + \cdots = (U_r + U_{r+1} + U_{r+2} + \cdots)(V_s + V_{s+1} + V_{s+2} + \cdots). \]

If \( r \) or \( s \) is 0, then \( U \) or \( V \) does not contain \( p \) and \( I_p(u, v) = 0 \); thus, assume \( r, s > 0 \). As \( p \) satisfies Eq. (17) from Lemma 8, \( F_{m_p} \) 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 \( \alpha_1 \) is a constant.

Thus, \( H_{m_p} = U_rV_r = t^{2^l} \) and \( H_{m_p+1} = U_rV_{s+1} + U_{r+1}V_s \).

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 \( U_rV_s = t^{2^l} \), then \( t \mid U_r \) and \( t \mid V_s \). Therefore, \( t \mid \gcd(U_r, V_s) \). However, if \( \gcd(U_r, V_s) \) was more than just \( t \) then \( \gcd(H_{m_p}, H_{m_p+1}) \)
would also be more than just \( t \), 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 \( t^2 \nmid H_{mp+1} \), 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 [5, p. 81], \( I_0(U, V) = \text{ord}_V(U) \) in the discrete valuation ring \( O_0(V) \). Any line not tangent to \( H \) at \( p \) can be taken as a uniformizing parameter, let us pick \( x \). Note that if \( \text{ord}(\alpha) < \text{ord}(\beta) \) then \( \text{ord}(\alpha + \beta) = \text{ord}(\alpha) \).

First, \( \text{ord}(U_r) = \text{ord}(U_{r-1}) = \text{ord}(t^{2^l - 1}) > 2^l \) as \( \text{ord}(t) \geq 2 \). Note that \( l > 1 \). Second, let us write \( U_{2l} = \prod_{j=1}^{2l}(\alpha_j x + \beta_j t) = \alpha x^{2l} + O(x^{2l+1}) \) where \( \alpha = \prod \alpha_j \neq 0 \). We can do this as \( t \nmid U_{2l} \). Clearly, the order of \( U_{2l} = 2^l \). Any higher degree terms of \( U \) will have larger order and thus \( I_0(U, V) = \text{ord}(U) = 2^l \) as desired. \( \square \)

**Lemma 10.** 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. \( F_{mp} = (w + 1)^2 H_{mp} \). Also, \( F_{mp+1} = H_{mp+1}(w + 1)^2 + H_{mp}z(w + 1) \). 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. \( H_{mp} = \frac{F_{mp+2}}{x(x+z)} \), where \( m_p \) is the multiplicity of \( p \) on \( \tilde{h} \).

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

\[
\tilde{F} = \tilde{H}[(x + w + 1)(x + z + w + 1)]
= [R + \tilde{H}_{mp+1} + \tilde{H}_{mp}][x(x + z) + z(w + 1) + (w + 1)^2]
= \{R[x(x + z) + z(w + 1) + (w + 1)^2] + \tilde{H}_{mp+1}[x(x + z) + z(w + 1)]
+ \tilde{H}_{mp}[x(x + z)]\} + \{\tilde{H}_{mp+1}[(w + 1)^2] + \tilde{H}_{mp}[z(w + 1)]\} + \tilde{H}_{mp}[(w + 1)^2].
\]

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

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. \( H_{mp} = \frac{F_{mp+2}}{x(x+z)} \). \( \square \)

Recall that if \( m \equiv 3 \pmod{4} \) then there are no singular points at infinity.

**Corollary 7.** For the Type IIIa singularity, \( I_p(u, v) \leq \left(\frac{2^l-2}{2}\right)^2 \).

**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, up to a constant multiple, \( \frac{x^{d-1} + x^{d-2}z^{-1}}{x(x+z)} = \frac{x^{d-1} - z^{-1}}{(x+z)} \) by Lemma 10. The factors of this are all distinct and so \( I_p(u, v) \leq \left(\frac{2^l-2}{2}\right)^2 \). \( \square \)
Corollary 8. For Type IIIb singularities, $I_p(u, v) \leq (2^{l-1})^2$.

Proof. For singular points $p = (w : 1 : 0)$ where $w$ is a root of $x^{m-1}/z = 1$ 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 10, the tangents lines to $\tilde{f}$ and $\tilde{h}$ are the same. Therefore, $I_p \leq (2^{l-1})^2$. \qed

Corollary 9. For Type IIIc singularities, $I_p(u, v) = 0$.

Proof. Here $p = (w : 1 : 0)$ where $w$ is a root of $x^{m-1}/z = 1$ such that $w^d \neq 1$. They have multiplicity $m_p = 2^l - 1$ and, up to a constant multiple, $\tilde{F}_{2l-1} = z^{2^l-1}(1 + w^{m-2^l})$ by the proof of Lemma 4. Thus, the tangent lines are all $z$.

We have $\gcd(\tilde{H}_{2l}, \tilde{H}_{2l-1}) = \gcd(\tilde{H}_{2l}(w + 1)^2 + \tilde{H}_{2l-1}(w + 1), \tilde{H}_{2l-1}) = \gcd(\tilde{F}_{2l}, \tilde{F}_{2l-1})$ by Lemma 10. As $\tilde{F}_{2l-1} = cz^{2^l-1}$ for some constant $c$, so $\gcd(\tilde{F}_{2l}, \tilde{F}_{2l-1}) = 1$ if and only if $z \nmid \tilde{F}_{2l}$. From the proof of Lemma 4 as

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

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

5. Proof of main results

First a lemma to set up our method.

Lemma 11. If $h$ has no absolutely irreducible factors over $\mathbb{F}_2$, then $e = \frac{l_{tot}}{(\deg(h))^2} \geq \frac{8}{9}$ where $l_{tot}$ is any upper bound on the global intersection number of $u$ and $v$ for all factorizations of $h$ into two factors $u$ and $v$ over the algebraic closure of $\mathbb{F}_2$. Equivalently, if $h$ has no absolutely irreducible factors over $\mathbb{F}_2$, then there exists a factoring of $h$ into $u$ and $v$ such that $\sum_p I_p(u, v) \geq \frac{2(\deg(h))^2}{9}$.

Proof. Assume that $h$ factors over $\mathbb{F}_2$ as $h = e_1e_2\ldots e_r$ 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 $\deg(u) - \deg(v) \leq \frac{\deg(h)}{2}$. Given that $\deg(u) + \deg(v) = \deg(h)$, we have that $\deg(u) \deg(v) \geq \frac{\deg(h)^2}{8}$. Since $l_{tot} \geq \deg(u) \deg(v)$ by Bezout’s theorem and $e = \frac{l_{tot}}{(\deg(h))^2}$, we get that $e \geq \frac{8}{9}$. \qed

The following two theorems, Theorems 3 and 4, when combined give the main result, Theorem 1.
Theorem 3. 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 11 implies that \( e = \frac{I_{\text{tot}}}{(m-3)^2} \geq \frac{8}{9} \) where \( I_{\text{tot}} \) 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 \( I_{\text{tot}} \).

If \( m \equiv 3 \pmod{4} \), then \( l = 1 \) and the only singularities are those of Type Ib and Type Iic. Thus \( \sum p I_{p}(u, v) = 0 \) where the sum runs over all projective points. Clearly, as \( I_{\text{tot}} = 0 \), 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 2 and Corollary 2 shows that there are only 4 types of singularities possible, Types Ib, Iic, IIIa and IIIc.

Therefore, Theorem 2 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 \( e = \frac{I_{\text{tot}}}{(m-3)^2} \) where \( I_{\text{tot}} \) 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 \( m \neq 2^l + 1 \) for any \( j \) and \( 2^j \) is precisely the power of 2 that divides \( m - 1 \). Thus \( \frac{m-1}{6} \geq 2^{l-1} > 2^{l-1} - 1 \) implying \( (2^{l-1} - 1)^2 < \frac{(m-1)^2}{36} \).

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

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 \( l > 3 \), 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 7, we can bound the number of points of Type Iic by \( (\frac{m'-3}{2})(2^l - 2)(2^l + 1) \) instead of \( (\frac{m'-3}{2})(m'-a-3) \). This version of counting gives us a bound on the global intersection number of \( \sum l \leq (2^{l-1} - 1)^2 + 2^l (\frac{m'-3}{2})(2^l - 2)(2^l + 1) \).

Thus,

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

$h$ has an absolutely irreducible factor defined over $\mathbb{F}_2$ when $1 < d < \frac{m'-1}{2}$.

**Proof.** First, assume for contradiction that $h$ has no absolutely irreducible factors over $\mathbb{F}_2$. As $\deg(h) = m - 3$, Lemma 11 implies that $e = \frac{I_{\text{tot}}}{(m-3)^2} \geq \frac{8}{9}$ where $I_{\text{tot}}$ 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 $I_{\text{tot}}$.

From Theorem 2, 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

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

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

Again using the chart in Theorem 2, 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 $e = \frac{I_{\text{tot}}}{(m-3)^2}$ where $I_{\text{tot}}$ is now the global intersection bound listed above.

Simplifying $e$ we get that

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

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

Now define $\hat{e}$ as
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 \( l \geq 3 \),

\[
\hat{e} \leq \frac{4(m' - 3)(m' - a - 3) + 48(d - 1) + 12(d - 1)(d - 3) + 16}{(4(m' - 1) - 2)^2} \\
\leq \frac{(m' - 3)(m' - a - 3) + 12(d - 1) + 3(d - 1)(d - 3) + 4}{(m' - \frac{3}{2})^2} \\
\leq \frac{(m' - 3)(\frac{m' - 1}{2} - 3) + 12(d - 1) + 3(d - 1)(d - 3) + 4}{(m' - \frac{3}{2})^2} \\
\leq \frac{\frac{1}{2}(m' - 3)(m' - 7) + 12(d - 1) + 3(d - 1)(d - 3) + 4}{(m' - \frac{3}{2})^2}.
\]

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 \( e \geq \frac{8}{5} \).

Now consider the case \( l = 2 \). Using the strict alternative bound on the number of Type IIc singularities from Lemma 7, we can redefine \( I_{\text{tot}} \) as

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

For \( l = 2 \), our new definition becomes

\[
I_{\text{tot}} = 4\left(10\left(\frac{m' - 3}{2}\right) - (d - 1)(d - 3)\right) + 12(d - 1) + 6(d - 1)(d - 3) + 1.
\]
Again let

\[ e = \frac{I_{\text{tot}}}{(m-3)^2} = \frac{I_{\text{tot}}}{(2^{l-1}(m-1)-2)^2} \]

and so

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

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

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 \( m' \geq 27 \), \( e < 0.86 < \frac{8}{9} \), 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 \( \mathbb{F}_2 \).

6. The last case, \( d = \frac{m'-1}{2} \)

All monomials have been classified as either APN over infinitely many fields \( \mathbb{F}_{2^n} \) or over only a finite number, except for the singular case when \( d = \frac{m'-1}{2} \). 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.

To get an idea of how rare this case is, consider how many of them there are below 100. First, recall that \( m = 2^l \left( \frac{m'-1}{2} \right) + 1 \) and that \( d = \gcd \left( \frac{m'-1}{2}, 2^l - 1 \right) \). If \( d = \frac{m'-1}{2} \), then \( \frac{m'-1}{2} \) divides \( 2^l - 1 \). The smallest nontrivial \( m' \) is 7, which limits \( l \), i.e. \( 3 \mid 2^l - 1 \). Clearly, \( l \) must be even. Notice that \( m \) grows exponentially with \( l \). Thus for \( m' = 3 \), there are only two possible \( l \) values that satisfy the gcd limitation and correspond to \( m \) values below 100. For \( m' = 5 \), there is one \( l \) and thus one \( m \) value in our range and likewise for \( m' = 7 \). There are no other \( m' \) values that yield an \( m < 100 \) satisfying our restriction. Thus, there are four \( m \) values below 100 that fall into this last case. There are only eight \( m \) values below 1000. (Note that to satisfy the gcd restriction, essentially \( l \) must be a multiple of the multiplicative order of 2 mod \( \frac{m'-1}{2} \), and \( m \) is approximately \( m' \cdot 2^l \) which explains the rarity.)

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. If all affine singular points fall on these two lines then the following corollary to Theorem 4 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 4 but remove the intersection number estimates for all affine singular points off the lines \( y = x, y = x + 1 \) from \( I_{\text{tot}} \). Note that \( l > 1 \) and \( m' \geq 7 \) as \( d > 1 \).

Thus, we can bound the global intersection number by

\[
\sum_p I_p(u, v) \leq 2(d - 1)(2^{l-1})^2 + (d - 1)(2^{l-1})^2 + (2^{l-1} - 1)^2 < 3(d - 1)(2^{l-1})^2 + (2^{l-1})^2.
\]

Call this last bound \( I_{\text{tot}} \):

\[
eq \frac{I_{\text{tot}}}{(m-3)^2} = \frac{3(d - 1)(2^{l-1})^2 + (2^{l-1})^2}{(2^{l-1}(m-1)-2)^2}.\]

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 \( d \) fixed. Therefore, the largest value occurs when \( l = 2 \) and

\[
eq \frac{3(d - 1)(4) + 4}{(2(m'-1)-2)^2} = \frac{12d - 8}{(m'-2)^2} = \frac{6m' - 14}{(m'-2)^2}.\]

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

\[
eq \frac{7(2^{l-1})^2 - 2(2^{l-1}) + 1}{(3(2^{l-1}) - 1)^2}
\]

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 \( \mathbb{F}_2 \). \( \square \)

Alternatively, if one can show that \( h \) is irreducible over \( \mathbb{F}_2 \), something that appears to be true for all \( m \geq 5 \), then one can show that for \( m \equiv 1, 2 \) (mod 3), \( h \) is absolutely irreducible in the following way. If \( h \) is irreducible but not absolutely irreducible, then it splits into say \( c \) conjugates over some extension. Using the global intersection number estimates in Theorem 4, one can easily show 2 things. First, \( c \) must be odd (since \( e < 1 \)). Second, \( c < .89\sqrt{m'} \). The first is helpful since for \( m \equiv 1, 2 \) (mod 3), \( h \) has the smooth point \( (\omega, 0) \) in \( \mathbb{F}_2^2 \), where \( \omega^2 + \omega + 1 = 0 \). This implies that if \( h \) 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 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: \( c < \frac{.89\sqrt{m'}}{m'} \) (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 5.** 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 \( \frac{m'-1}{2} \mid 2^l - 1 \) 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 11, \( e = \frac{I_{\text{tot}}}{(m-3)c} \geq \frac{8}{9} \) where \( I_{\text{tot}} \) is a bound on the global intersection number of \( u \) and \( v \). Using the strict alternative bound on the number of Type IIc singularities from Lemma 7, we have a bound on the global intersection number,

\[
w(m' - 3) \left( \frac{m' - 1}{2} - 3 \right) - w(d - 1)(d - 3) + 3w^2(d - 1) + w^2(d - 1)(d - 3) + (w - 1)^2.
\]

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

\[
e = \frac{(\frac{w}{4} - \frac{w}{4})(m' - 3)(m' - 7) + \frac{3w^2}{4}(m' - 3) + \frac{w^2}{4}(m' - 3)(m' - 7) + (w - 1)^2}{(w(m' - 1) - 2)^2}
\]

\[
= \frac{w(m' - 3)(m' - 7) + 6w^2(m' - 3) + w^2(m' - 3)(m' - 7) + 4(w - 1)^2}{(w(m' - 1) - 2)^2}
\]

\[
= \frac{w(m' - 3)(m' - 7) + w^2(m' - 3)(m' - 1) + 4(w - 1)^2}{(w(m' - 1) - 2)^2}.
\]

A fair bit of calculus shows that this is a decreasing function of \( w \) for \( w > \frac{2}{m'-1} \) and fixed \( m' \geq 7 \). Thus, as \( w \geq \frac{3m'-1}{4} \),

\[
e \leq \frac{\frac{3}{4}(m' - 1)(m' - 3)(m' - 7) + \frac{9}{16}(m' - 1)^2(m' - 3)(m' - 1) + \frac{9}{4}(m' - \frac{5}{3})^2}{\frac{9}{16}((m' - 1)^2)(m' - 1) - \frac{8}{3})^2}
\]

\[
\leq \frac{\frac{10}{3}(m')^2 - 4(m')^2 + \frac{50}{3}m' + \frac{19}{3}}{(m')^2 - \frac{8}{3}(m')^2 + \frac{26}{3}m' + \frac{49}{9}}
\]

\[
\leq \frac{9(m')^4 - 30(m')^3 - 36(m')^2 + 150m' + 19}{9(m')^4 - 24(m')^3 - 26(m')^2 + 56m' + 49}
\]

\[
\leq 1 + \frac{6(m')^3 - 10(m')^2 + 94m' - 30}{9(m')^4 - 24(m')^3 - 26(m')^2 + 56m' + 49}
\]

\[
< 1 - \frac{2}{3m'} \quad \text{for } m' \geq 7.
\]
Recall from the proof of Lemma 11 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 11 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 $c < .89\sqrt{m'}$. □

References