Monomial Hyperovals in Desarguesian Planes

Timothy Vis

University of Colorado Denver

February 22, 2008
Basic Definitions

**Definition**

In a projective plane of order $n$, where $n$ is even, a **hyperoval** is a set of $n + 2$ points, no three collinear.

In a Desarguesian plane of order $q$, we may assume the hyperoval consists of the points $\{(1, x, f(x)) : x \in GF(q)\} \cup \{(0, 1, 0), (0, 0, 1)\}$.

**Definition**

A polynomial $f(x)$ describing a hyperoval in the above manner is called an **o-polynomial**.
A hyperoval with a monomial $o$-polynomial is called a **monomial hyperoval**.

**Definition**

We examine the following set of points for a given value of $k$.

$$D(k) = \{(1, x, x^k) : x \in GF(q)\} \cup \{(0, 1, 0), (0, 0, 1)\}$$

The following are all known monomial hyperovals in $PG(2, 2^h)$:

- **Regular**: $D(2)$ for all $h$.
- **Translation**: $D(2^i)$, $(i, h) = 1$, for all $h$ (Segre, 1957).
- **Segre**: $D(6)$ for $h$ odd (Segre and Bartocci, 1971).
- **Glynn I**: $D(\sigma + \gamma)$, $\sigma^2 \equiv \gamma^4 \equiv 2 \mod q - 1$ for $h$ odd (Glynn, 1983).
- **Glynn II**: $D(3\sigma + 4)$ for $h$ odd (Glynn, 1983).
Glynn’s Criterion

Definition

We define the following partial ordering on integers $a$ and $b$. Express $a = \sum a_i2^i$ and $b = \sum b_i2^i$, where $a_i, b_i \in \{0, 1\}$. Then $a \preceq b$ if and only if $a_i \leq b_i$ for all $i$.

The following theorem of Glynn (1983) provides a powerful tool for the classification of monomial hyperovals.

Theorem

$D(k)$ is a hyperoval in $PG(2, 2^h)$ if and only if $d \not\preceq kd$ for all $1 \leq d \leq q - 2$, where $kd$ is reduced mod $q - 1$ to lie in $\{0, \ldots, q - 1\}$ with the convention that 0 is reduced to zero and any nonzero multiple of $q - 1$ to $q - 1$. 
Some Classifications

Theorem ((Segre, 1957))

If $D(2^{i_0})$ is a hyperoval in $PG(2, 2^h)$, then $(i_0, h) = 1$ and $D(2^{i_0})$ is a translation hyperoval.

Theorem ((Cherowitzo and Storme, 1998))

If $D(2^{i_0} + 2^{i_1})$ is a hyperoval in $PG(2, 2^h)$, then $D(2^{i_0} + 2^{i_1})$ is either a translation hyperoval, a Segre hyperoval, or a Glynn I hyperoval.
Two-Bit Classification

The two-bit classification \( \mathcal{D} (2^i_0 + 2^i_1) \) involves several steps:

1. Assume \( \alpha = 2^i_0 \), where \( (i_0, h) = 1 \) and classify \( i \), where \( k = \alpha + \alpha^i \).
2. Show that any hyperoval is of the form \( \mathcal{D} (\alpha + \alpha^i) \).
3. Classify \( \alpha \).

We attempt to classify three-bit monomial hyperovals \( \mathcal{D} (2^i_0 + 2^i_1 + 2^i_2) \) in the same manner.
Common Divisor Conditions

Lemma

If for some $m > 1$, $m | i_0$, $m | i_1$, $m | i_2$, and $m | h$, $D(2^{i_0} + 2^{i_1} + 2^{i_2})$ is not a hyperoval in $PG(2, 2^h)$.

Proof.

Set $d = \sum_{a=0}^{h-1} 2^{am}$. Then $kd = 3d = \sum_{a=0}^{h-1} (2^{am} + 2^{am+1})$ and $d \leq kd$.

Lemma

If each of $(i_0, h)$, $(i_1, h)$, and $(i_2, h)$ is greater than one and $(i_0, i_1, i_2, h) = 1$, then WLOG there exists an $m$ dividing $i_0$ and $h$ but neither $i_1$ nor $i_2$. 
Divisor Conditions

Lemma

If $i_1$ and $i_2$ are not both congruent to $-1 \mod m$, then $D \left( 2^{i_0} + 2^{i_1} + 2^{i_2} \right)$ is not a hyperoval in $PG(2,2^h)$.

Lemma

If $D \left( 2^{i_0} + 2^{i_1} + 2^{i_2} \right)$ is a hyperoval in $PG(2,2^h)$ then one of the following three conditions holds.

1. $(i_a, h) = (i_b, h) \equiv -1 \mod (i_c, h)$ for some choice of $a$, $b$, and $c$.
2. $i_a \equiv i_b \equiv -1 \mod (i_c, h)$ for all choices of $a$, $b$, and $c$.
3. $(i_a, h) = 1$ for some choice of $i_a$. 
\[(i_a, h) = (i_b, h) \equiv -1 \mod (i_c, h)\]

**Lemma**

Let \( k = 2^{i_0} + 2^{i_1} + 2^{i_2} \) and let \( c \mid (i_1, h), c \mid (i_2, h) \) for \( c > 1 \), with \( i_0 \not\equiv 0 \mod c \). Let \( x' = \frac{x}{c} \) for \( x \in \{i_1, i_2, h\} \) and let \( k' = 2^{i'_1} + 2^{i'_2} \). If there exists a \( d' \) such that \( d' \preceq k'd' \) and the product \( k'd' \) involves no carries, \( D(k) \) is not a hyperoval in \( PG(2, 2^h) \).

This lemma, together with work from Cherowitzo and Storme in the two-bit classification, eliminates the first case.
Reduction

Definition

If $c|h$ and $i_0$, $i_1$, and $i_2$ are pairwise incongruent mod $c$, then the reduction of $D \left(2^{i_0} + 2^{i_1} + 2^{i_2}\right)$ in $PG(2, 2^h)$ with respect to $c$ is $D \left(2^{i'_0} + 2^{i'_1} + 2^{i'_2}\right)$ in $PG(2, 2^c)$, where $i'_0$, $i'_1$, and $i'_2$ are the residues of $i_0$, $i_1$, and $i_2$ mod $c$.

Theorem

If $D(k)$ is a hyperoval in $PG(2, 2^h)$, any reduction of $D$ is also a hyperoval.
Implications of Reduction

Definition
If $k$ has no reduction, $k$ is called irreducible; otherwise $k$ is called reducible.

Theorem
If $\mathcal{D}(k)$ is irreducible in $\text{PG}(2, 2^h)$, then $h$ has at most two prime divisors.

Proof.
Suppose $h = p^\alpha q^\beta r$, where $(pq, r) = 1$. Then each of $p^\alpha r$, $q^\beta r$, and $p^\alpha q^\beta$ must divide one of the differences $i_0 - i_2$, $i_1 - i_0$, or $i_2 - i_1$. With the relationships among these differences, this is only possible if at least one of the differences is $h$, a contradiction.

Theorem
If $\mathcal{D}(2^{i_0} + 2^{i_1} + 2^{i_2})$ is irreducible in $\text{PG}(2, 2^h)$, then at least one of $(i_0, h)$, $(i_1, h)$, or $(i_2, h)$ must be one.
With one bit relatively prime to $h$, we may express $k$ as $\alpha + \alpha^i + \alpha^j$. In an $\alpha$-ary expansion, which merely permutes the bits of $k$, we may apply Glynn’s criterion, so long as no bits in the products coincide. Using five choices of $d$, motivated by the values used in the two-bit classification, along with some inspection and analysis, we are able to restrict the form of such a monomial hyperoval. In general, we use the division algorithm to express $h$ as $mj + ni + l$, where $ni + l < j$ and $l < i$. 
The Remaining Cases

Recall $h = mj + ni + l$

1. $i - 1 = l$, $n = 0$, and $m = 1$
2. $i = 2$ and $l = 1$
3. $i - 1 = l$, $m = 1$, and $j = ni + 2i - 1$ or $j = ni + 2i - 2$
4. $n = 0$ and $j \leq i + l$
5. $n = 1$, $m = 1$, and $2i + 1 \leq j \leq 2i + l$
6. $n = 1$, $j = 2i$, and $l \neq 0$
7. $m = 1$, $j = i + l - 1$, and $n = 0$
8. $m = 1$ and $j = ni + i + l$
9. $n = 1$, $j = i + l$, and $l = 0$
10. $j = ni + l + 1$ and $m = 1$. 
Using the first value of $d$ and analyzing the carries, we are able to (mostly) eliminate this case. In fact, one of the following two conditions must hold, where $\alpha' = 2$.

1. $r = h - 1$
2. $i \leq 3$

In the $r = h - 1$ case, the only hyperoval is $\mathcal{D}\left(\frac{7}{8}\right)$, a translation hyperoval. If $i = 3$, the only hyperoval is $\mathcal{D}\left(3\sigma + 4\right)$, a Glynn hyperoval. Finally, if $i = 2$, the only hyperovals are $\mathcal{D}\left(\frac{1}{1-2^{2m+1}}\right)$ and $\mathcal{D}\left(\frac{7}{8}\right)$, both translation hyperovals.
Going back to the three divisor cases, only one case remains (when the ongoing work to complete the $\alpha + \alpha^i + \alpha^j$ is completed).

**Theorem**

If $D(2^{i_0} + 2^{i_1} + 2^{i_2})$ is a hyperoval in $PG(2, 2^h)$ that is reducible with each of $(i_0, h), (i_1, h), (i_2, h)$ greater than one and with $i_1 \equiv i_2 \equiv -1 \mod (i_0, h)$ then there exists a monomial hyperoval of the form $D(2^i + 2^j + 2^{h-1})$, where neither $i$ nor $j$ is relatively prime to $h$. Such a hyperoval would be new.

Completion of the $\alpha + \alpha^i + \alpha^j$ case would (if the result is that all such monomial hyperovals are known) therefore complete the classification.
Immediate Work

The most immediate concern is to complete the classification of the remaining $\alpha + \alpha^i + \alpha^j$ cases. It appears that examining the carries that occur will be crucial in such an effort, bringing in the further parameter $r$. Due to the greater variety of known examples and $\alpha$-ary representations of these examples, this is a non-trivial task.
The Big Goal

Clearly the result desired is a complete classification of monomial hyperovals. There are several ideas for this classification.

- Show that any monomial hyperoval is equivalent to one with at most three bits.
- Find some set of families of values for $d$ that eliminates everything except the known hyperovals.
- Explore extensions of results for two and three bits to obtain partial results.