Classifying Hyperovals: Bit by Bit by Bit

Timothy Vis

University of Colorado Denver

April 25, 2008
Projective Planes

Definition

A projective plane consists of a set of points, a set of lines, and an incidence relation between the points and lines with the following three axioms:

1. Any pair of distinct points is incident with exactly one line.
2. Any pair of distinct lines is incident with exactly one point.
3. There exist four points with no three collinear (incident with a common line).

Definition

If any line is incident with exactly \( n + 1 \) points, the plane is said to have order \( n \).
The Plane $PG(2, q)$

We consider the plane $PG(2, q)$ built over $GF(q)$ in the following manner:

- The 1-dimensional subspaces of $GF(q)^3$ are points.
- The 2-dimensional subspaces of $GF(q)^3$ are lines.
- A point is incident with a line precisely when the point is a subspace of the line.

Such a plane has order $q$. 
Definition

In a projective plane of order $n$, a set of $n + 1$ points, no three collinear is called an **oval** and a set of $n + 2$ points, no three collinear is called an **hyperoval**.

Theorem

*In a projective plane of odd order, hyperovals do not exist. In a projective plane of even order, every oval is contained in exactly one hyperoval.*

In the planes $PG(2, 2^h)$, hyperovals have yet to be classified and many infinite families are known.
The Fundamental Quadrangle

In $PG(2, q)$, we use the notation $(x_0, x_1, x_2)$ to represent the point (1-dimensional subspace) generated by $(x_0, x_1, x_2)$.

**Definition**

The fundamental quadrangle consists of the points $(0, 0, 1)$, $(0, 1, 0)$, $(1, 0, 0)$, and $(1, 1, 1)$.

**Theorem**

*Any hyperoval can be mapped (essentially by a change of basis) to one containing the fundamental quadrangle.*
If a hyperoval of $PG(2, 2^h)$ contains the fundamental quadrangle, it can be shown that the hyperoval consists precisely of the points $(0, 0, 1), (0, 1, 0)$ and $(1, x, f(x))$, where $f(x)$ is a permutation satisfying the following conditions:

- $f(0) = 0$,
- $f(1) = 1$,
- $f_s(x)$ permutes the elements of $GF(2^h)$ for all $s \in GF(2^h)$, where

$$f_s(x) = \begin{cases} 0 & x = 0 \\ \frac{f(x+s)+f(s)}{x} & x \neq 0 \end{cases}$$

Definition

Such a permutation is called an $o$-polynomial.
Monomials

With the classification of hyperovals being a difficult open problem it is interesting to attempt to classify some class of hyperovals: those given by monomials.

To do this, we require some conventions.

- We always work in $PG(2,2^h)$.
- We always assume the monomial is $x^k$.
- We denote by $D(k)$ the set of points

$$D(k) = \left\{ \left( 1, x, x^k \right) : x \in GF(2^h) \right\} \cup \{(0, 0, 1), (0, 1, 0)\}.$$
In order to use a powerful classification criterion, we place the following partial order on the integers.

**Definition**

For integers $a$ and $b$, we say $a \preceq b$ if the binary expansion of $b$ dominates the binary expansion of $a$; that is, if every term in the binary expansion of $a$ is also in the binary expansion of $b$.

**Example**

$5 \preceq 13$, since $5 = 2^0 + 2^2$ and $13 = 2^0 + 2^2 + 2^3$. 
The following theorem, due to Glynn, is a powerful tool for classifying monomial hyperovals.

**Theorem (Glynn, 1983)**

\[ D(k) \text{ is a hyperoval in } PG(2,2^h) \text{ if and only if for all } 1 \leq d \leq 2^h - 2, \ d \not\preceq kd, \text{ where } kd \text{ is reduced modulo } q - 1. \]

So, to prove that \( D(k) \) is not a hyperoval, it suffices to find some \( d \) such that \( d \preceq kd \).
Every known monomial hyperoval is equivalent to either \( D(2^{i_0}) \), \( D(2^{i_0} + 2^{i_1}) \) or \( D(2^{i_0} + 2^{i_1} + 2^{i_2}) \).

**Theorem (Segre, 1957)**

*If \( D(2^{i_0}) \) is a hyperoval, then \( D(2^{i_0}) \) is either a regular hyperoval or a translation hyperoval.*

**Theorem (Cherowitzo, Storme, 1998)**

*If \( D(2^{i_0} + 2^{i_1}) \) is a hyperoval, then \( D(2^{i_0} + 2^{i_1}) \) is either a translation hyperoval, a Segre hyperoval, or a Glynn hyperoval.*
Divisibility Relations

Theorem (V.)

If $D(2^{i_0} + 2^{i_1} + 2^{i_2})$ is a hyperoval in $PG(2, 2^h)$, then either at least one of $i_0$, $i_1$, and $i_2$ is relatively prime to $h$, or $(i_0, h)$, $(i_1, h)$, and $(i_2, h)$ are all distinct with the property that $i_x \equiv -1 \mod (i_y, h)$ for every pair of distinct $x$ and $y$.

Theorem (V.)

The second case can only produce new hyperovals if the first case produces new hyperovals.
If $\alpha = 2^{i_0}$ and $(i_0, h) = 1$, then any $k$ can be expressed in an $\alpha$-ary expansion that is simply a permutation of the digits of the binary expansion.

Since we reduced to the case in which one of $i_0$, $i_1$, or $i_2$ is relatively prime to $h$, we can use this and consider only those sets $D(\alpha + \alpha^i + \alpha^j)$, thereby eliminating a parameter from the classification.
The Strategy

To aid the classification, we break down $h$ using the division algorithm as follows, where we assume $j > i$.

$$h = mj + ni + l$$

with $ni + l < j$ and $l < i$. This allows us to construct values of $d$ that rule out many values for $k$. In fact, without much difficulty...
The Cases

...we can restrict these parameters to one of the following ten cases.

1. \( i - 1 = l, \ n = 0, \) and \( m = 1, \)
2. \( i = 2 \) and \( l = 1, \)
3. \( i - 1 = l, \ m = 1, \) and \( j = 2n + 2i - 2, \)
4. \( n = 0 \) and \( j \leq i + l, \)
5. \( n = m = 1 \) and \( 2i + 1 \leq j \leq 2i + l, \)
6. \( n = 1, \ j = 2i, \) and \( l \neq 0, \)
7. \( m = 1, \ n = 0, \) and \( j = i + l - 1, \)
8. \( m = 1, \) and \( j = ni + i + l, \)
9. \( n = 1, \ j = i + 1, \) and \( l = 0, \)
10. \( m = 1, \) and \( j = ni + l + 1. \)
The Classified Cases

As yet, only two of these cases have been completely classified: Cases 5 and 9.

Theorem (V.)

*If* $n = m = 1$ and $2i + 1 \leq j \leq 2i + l$, then $D(\alpha + \alpha^i + \alpha^j)$ is not a hyperoval.

Theorem (V.)

*If* $n = 1$, $j = i + 1$, and $l = 0$, then $D(\alpha + \alpha^i + \alpha^j)$ is a hyperoval if and only if it is a Glynn hyperoval or a translation hyperoval.

Currently, work is underway on Case 2 ($i = 2$, and $l = 1$).
Further Work

- Classify the remaining cases.
- Consolidate results to clean up this classification.
The main goal is the classification of all monomial hyperovals. That would be accomplished if the following conjecture were true:

**Conjecture (Cherowitzo)**

*Every monomial hyperoval is equivalent to one in which $k$ is the sum of either one, two, or three distinct powers of two.*

Proving this conjecture and completing the classification for three distinct powers of two would complete the full classification.
Other Ideas

- Some of the ideas being used for the classification with three powers of two may generalize easily to restrict the scope of what remains.
- It may be feasible to determine some sort of minimal set of values for $d$ that will rule out all values of $k$ which do not correspond to known monomial hyperovals.