

Being Discrete: Hiding Behind Bits

Timothy Vis

August 3, 2007

Definition 1 *An oval in a finite projective plane of order q is a set of $q + 1$ points, such that no three of the points lie on a common line.*

Theorem 2 *If q is even, any oval can be uniquely extended to a hyperoval, a set of $q + 2$ points, no three collinear.*

Lemma 3 *Any hyperoval in a finite Desarguesian plane of even order is projectively equivalent to a hyperoval containing the points $(0, 0, 1)$, $(0, 1, 0)$, $(1, 0, 0)$, and $(1, 1, 1)$, known collectively as the fundamental quadrangle.*

The points of the hyperoval other than $(0, 0, 1)$ and $(0, 1, 0)$ must have a non-zero first entry. If we normalize for this first entry, the second and third entries must be permutations on the elements of $GF(2^h)$.

We may, then, express the remaining points as $(1, x, f(x))$, where x runs through the elements of $GF(q)$, and where $f(x)$ is a permutation such that

- $f(0) = 0$
- $f(1) = 1$
- $f_s(x)$ defines a permutation for all $s \in GF(q)$, where

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

- $f(x)$ has degree less than $q - 1$.

Definition 4 *Such a permutation is called an α -polynomial.*

The classification of hyperovals in finite Desarguesian planes of even order remains an open problem.

It is interesting, then, to place restrictions on the σ -polynomial and to attempt to classify the hyperovals with σ -polynomials satisfying that restriction.

In particular, we ask the following: For what values of k is $f(x) = x^k$ an σ -polynomial over $GF(2^h)$?

Such an σ -polynomial defines a *monomial* hyperoval.

Some conventions before we proceed:

- We will always consider planes of order $q = 2^h$.
- We will always consider the monomial $f(x) = x^k$.
- We focus on the set of points $\mathcal{D}(k) = \{(1, x, x^k) \mid x \in GF(q)\} \cup \{(0, 1, 0), (0, 0, 1)\}$.

Thus, the question becomes: For what k is $\mathcal{D}(k)$ a hyperoval?

Known monomial hyperovals:

Name h	k Reference
Hyperconics All h	$k = 2$
Translation All h	$k = 2^i, (i, h) = 1$ Segre, 1957
Segre Odd h	$k = 6$ Segre and Bartocci, 1971
Glynn I Odd h	$k = 3\sigma + 4, \sigma^2 \equiv 2 \pmod{q-1}$ Glynn, 1983
Glynn II Odd h	$k = \sigma + \gamma, \sigma^2 \equiv \gamma^4 \equiv 2 \pmod{q-1}$ Glynn, 1983

It is known (Glynn, 1983) that if $\mathcal{D}(k)$ defines a hyperoval, then $\mathcal{D}(1 - k)$ and $\mathcal{D}\left(\frac{1}{k}\right)$ define projectively equivalent hyperovals. This leads to six equivalent exponents for any monomial hyperoval:

$$\begin{array}{cc}
 k & 1 - k \\
 \\
 \frac{1}{k} & 1 - \frac{1}{k} \\
 \\
 \frac{1}{1 - k} & \frac{k}{1 - k}
 \end{array}$$

Definition 5 Let $a = \sum_{i=0}^{\infty} a_i 2^i$, and $b = \sum_{i=0}^{\infty} b_i 2^i$, where a_i and b_i lie in $\{0, 1\}$. We define the following partial ordering (due to Glynn) on the nonnegative integers:

$$a \preceq b \iff a_i \leq b_i \quad \forall i$$

That is, $a \preceq b$ if and only if the binary expansion of b dominates the binary expansion of a .

The most significant tool in the classification effort is the following theorem due to Glynn (1983).

Theorem 6 *$f(x) = x^k$ is an σ -polynomial over $PG(2, q)$ if and only if $d \not\leq kd$ for all d satisfying $1 \leq d \leq q - 2$, where kd is reduced modulo $q - 1$ with the convention that zero is reduced to zero and any nonzero multiple of $q - 1$ is reduced to $q - 1$.*

This theorem is especially useful in ruling out a value of k as the exponent in a monomial σ -polynomial, as all that is necessary is to find some d such that $d \leq kd$.

Example 7 *Let k be odd. Then $\mathcal{D}(k)$ is not a hyperoval.*

Proof: Consider $d = 1$. Then $kd = k$. Since k is odd, it must dominate d .

One potential means of classification is to classify $\mathcal{D}(k)$ based on the number of bits in the binary expansion of k .

If $\mathcal{D}(2^i)$ is a hyperoval, then $\mathcal{D}(k)$ is either a hyperconic or a translation hyperoval (Segre, 1957).

If $\mathcal{D}(2^i + 2^j)$ is a hyperoval, then $\mathcal{D}(k)$ is either a translation hyperoval, a Segre hyperoval, or a Glynn hyperoval with $k = \sigma + \gamma$ (Cherowitzo and Storme, 1998).

If $\mathcal{D}(2^{i_0} + 2^{i_1} + 2^{i_2})$ is a hyperoval, then...the problem remains open, although work is underway.

Of course, doing this for all numbers of bits is impossible, so something more is needed.

Notice however, that every known monomial hyperoval is projectively equivalent to some $\mathcal{D}(k)$, where k has at most three bits in its binary expansion.

Conjecture 8 *If $\mathcal{D}(k)$ is a hyperoval, then $\mathcal{D}(k)$ is projectively equivalent to $\mathcal{D}(\hat{k})$, where \hat{k} has at most three bits in its binary expansion.*

If we could prove this conjecture and classify the three-bit monomial hyperovals, monomial hyperovals would be completely classified.

A useful extension of Glynn's criterion uses the following tool. If $\alpha = 2^i$, for $(i, h) = 1$, we can express k in an α -ary expansion having the same number of bits as the binary expansion. Such an expansion merely permutes the bits of the binary expansion, so that Glynn's criterion holds equally with this α -ary expansion.

The two-bit classification consists of two distinct steps:

- Show that if $k = 2^i + 2^j$ and $\mathcal{D}(k)$ is a hyperoval, one of i and j must be relatively prime to h . Without loss of generality, $(i, h) = 1$.
- Classify monomial hyperovals of the form $\mathcal{D}(\alpha + \alpha^i)$, where $\alpha = 2^i$.

These steps suggest some possibilities for a three-bit classification:

- Determine necessary relationships among i_0 , i_1 , and i_2 for $\mathcal{D}(2^{i_0} + 2^{i_1} + 2^{i_2})$ to be a hyperoval.
- Use these relationships to simplify the problem and solve the simplified problem.

Some three-bit divisibility relationships:

Proposition 9 *If $m > 1$ is a common divisor of i_0, i_1, i_2 , and h , then $\mathcal{D}(2^{i_0} + 2^{i_1} + 2^{i_2})$ is not a hyperoval in $PG(2, 2^h)$.*

Proof Let $d = \sum_{j=0}^{\frac{h}{m}-1} 2^j$. Then $kd = \sum_{j=0}^{\frac{h}{m}-1} 2^j + 2^{j+1}$. Since $m > 1$, $d \preceq kd$.

$$d = 00 \dots 01 \ 00 \dots 01 \ \dots \ 00 \dots 01 \quad (1)$$

$$2^{i_0}d = 00 \dots 01 \ 00 \dots 01 \ \dots \ 00 \dots 01 \quad (2)$$

$$2^{i_1}d = 00 \dots 01 \ 00 \dots 01 \ \dots \ 00 \dots 01 \quad (3)$$

$$2^{i_2}d = 00 \dots 01 \ 00 \dots 01 \ \dots \ 00 \dots 01 \quad (4)$$

$$kd = 00 \dots 11 \ 00 \dots 11 \ \dots \ 00 \dots 11 \quad (5)$$

A straightforward argument shows that if (i_0, h) , (i_1, h) , and (i_2, h) are all greater than one, then, without loss of generality, i_0 and h share a common factor m dividing neither i_1 nor i_2 .

Proposition 10 *If m is a common factor of i_0 and h dividing neither i_1 nor i_2 , and if i_1, i_2 are not both congruent to $-1 \pmod{m}$, $\mathcal{D}(k)$ is not a hyperoval.*

Proof Let $d = \sum_{j=0}^{\frac{h}{m}-1} 2^j$ and let d_1 and d_2 be the reductions of i_1 and $i_2 \pmod{m}$. Then $kd = \sum_{j=0}^{\frac{h}{m}-1} 2^j + 2^{j+d_1} + 2^{j+d_2}$. Since d_1 and d_2 are not both $m-1$ no carry can be made resulting in an extra 2^j term, so that $d \leq kd$.

Assuming we have $(i_0, h) = 1$ (which we cannot yet show to always be the case), we set $\alpha = 2^{i_0}$ and create an α -ary expansion $k = \alpha + \alpha^i + \alpha^j$, with $j > i > 1$.

Proposition 11 *If $h = mj + ni + l$, with $ni + l < j$, $l < i - 1$, $j \neq 3$, $\mathcal{D}(k)$ is not a hyperoval in $PG(2, 2^h)$.*

Sketch of Proof Let $d = \sum_{t=0}^{l-1} \alpha^t + \sum_{t=0}^{n-1} \alpha^{it+l} + \sum_{t=0}^{m-1} \alpha^{jt+ni+l}$.

Then under these conditions, $d \preceq kd$.

This proposition leaves two possibilities for hyperovals:

- $j = 3$
- $h = mj + ni + i - 1$

The case $j = 3$ indicates that $k = 2^{i_0} + 2^{2i_0} + 2^{3i_0}$. If $i_0 = -1$, a valid choice for i_0 in a number of fields, $k = \frac{7}{8}$. But then $k = 1 - \frac{1}{8}$. But $\frac{1}{8} = 2^{h-3}$ and if $(h-3, h) = 1$, $\mathcal{D}(k)$ defines a translation hyperoval. We can conclude that $j = 3$ will require deeper analysis.

On the other hand, we can further restrict the other case.

Proposition 12 *If $h = mj + ni + i - 1$, with $ni + 1 < j$, $i > 2$, $n > 1$, $\mathcal{D}(k)$ is not a hyperoval in $PG(2, 2^h)$.*

Sketch of Proof Let $d = \sum_{t=0}^{i-2} \alpha^t + \alpha^{2i-2} + \sum_{t=2}^n \alpha^{ti-1} + \sum_{t=0}^{m-1} \alpha^{j+ni+i-1}$.

Then under these conditions, $d \preceq kd$.

Future directions:

- Further restrict the relationships between i_0 , i_1 , i_2 , and h .
- Complete the classification for $k = \alpha + \alpha^i + \alpha^j$.
- Classify any other cases that remain.
- Determine relationships among numbers of bits in k and $\frac{1}{k}$.