# Pointless curves of genus three and four

Everett W. Howe[1] Kristin E. Lauter[2] Jaap Top[3]

[1]Center for Communications Research, La Jolla

[2]Microsoft Research

[3]Department of Mathematics, University of Groningen

Joint Mathematics Meetings, San Antonio, 2006
(Slides revised in view of comments made at talk.)

# Curves over finite fields with many points.

**Question**

Why are there so many papers written about curves over finite fields with many points?

**Answer (van der Geer and van der Vlugt)**

The attention given to curves with many points is

> *motivated partly by possible applications in coding theory and cryptography, but just as well by the fact that the question represents an attractive mathematical challenge.*

# Pointless curves.

Curves with *few* points are just as interesting mathematically. (But with fewer applications in coding theory and cryptography!)

**Definition**

A curve over a field $k$ is pointless if it has no $k$-rational points.

**Question**

For a given genus $g$, over which finite fields do there exist pointless curves of genus $g$?

# Pointless curves of genus less than 3.

Previously known results:

**Wedderburn**

Every genus-0 curve over a finite field has points.

**Hasse**

Every genus-1 curve over a finite field has points.

**Stark**

If a genus-2 curve over $\mathbb{F}_q$ has no points, then $q \leq 11$.

**Maisner and Nart**

A complete list of pointless genus-2 curves over finite fields $\mathbb{F}_q$. They exist for every $q \leq 11$.

# Pointless curves of genus 3 and 4.

We show:

**Theorem**

*There exist pointless genus-3 hyperelliptic curves over $\mathbb{F}_q$ if and only if $q \leq 25$.*

**Theorem**

*There exist pointless smooth plane quartics over $\mathbb{F}_q$ if and only if either $q \leq 23$ or $q = 29$ or $q = 32$.*

**Theorem**

*There exist pointless genus-4 curves over $\mathbb{F}_q$ if and only if $q \leq 49$.*

# Being and nothingness.

There are two aspects to proving these results:

1. For the $q$ for which we claim no pointless curves exist, we must prove no such curves exist.
2. For the $q$ for which we claim there *are* pointless curves, we would like to provide examples of such curves.

Easy first step for item 1: Serre's refinement of Weil bound.

- If a genus-3 curve over $\mathbb{F}_q$ has no points, then $q \leq 32$.
- If a genus-4 curve over $\mathbb{F}_q$ has no points, then $q \leq 59$.

But in this talk, we focus on item 2.

# A criterion for pointlessness of covers.

Suppose $C \to D$ is a cover of curves over a finite field $k$.

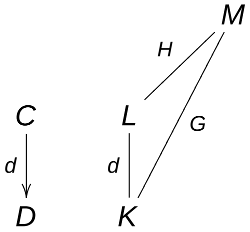
$$\begin{array}{ccc} C & & L \\ \downarrow & & | \\ D & & K \end{array}$$

Let $L/K$ be the corresponding extension of function fields.

$$S = \{\text{places P of K} \mid \exists Q \text{ of } L \text{ over } P \text{ with } k(Q) = k(P)\}$$

$C$ is pointless $\iff$ $S$ contains no places of degree 1.

# Enter Chebotarev.




Let $M$ be the Galois closure of $L/K$.
Let $G = \mathrm{Gal}(M/K)$, $H = \mathrm{Gal}(M/L)$.
Let $\delta = \#(\cup_{\tau \in G} H^\tau)/\#G$.

Note: We have $\delta \geq 1/d$, and
$\delta = 1/d \iff L/K$ is Galois.

$$S = \{\text{places P of K} \mid \exists Q \text{ of } L \text{ over } P \text{ with } k(Q) = k(P)\}$$

Chebotarev: The set $S$ has Dirichlet density $\delta$.
If $M$ has constant field $k$, then $S$ has natural density $\delta$.

**Heuristic**

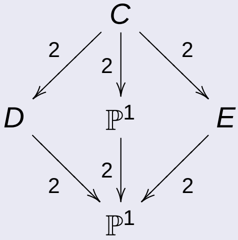
If $M$ has constant field $k$, then $C$ is pointless with probability $(1-\delta)^{\#D(k)}$.

# Example: Galois covers of $\mathbb{P}^1$.

## Generic hyperelliptic curves.


Expect a hyperelliptic curve to be pointless with probability $(1/2)^{q+1}$.

## Hyperelliptic $V_4$-covers of $\mathbb{P}^1$.




Expect a hyperelliptic $V_4$-cover of $\mathbb{P}^1$ to be pointless with probability $(3/4)^{q+1}$.

# Have some salt.

It is hard to justify using this heuristic for anything other than suggesting where to look for pointless curves.

Consider the case of genus-3 hyperelliptic curves over $\mathbb{F}_q$.

There are about $2q^5$ such curves, each with probability $(1/2)^{q+1}$ of being pointless.
Expected number: $q^5/2^q$.

But this figure assumes that a hyperelliptic curve has no other 'reason' to be pointless. (Or *not* to be pointless.)

For instance, there are about $4q^3$ hyperelliptic $V_4$-covers of $\mathbb{P}^1$, each with probability $(3/4)^{q+1}$ of being pointless.
Expected number: $3q^3(3/4)^q$.

Which is more accurate?

# Example: The heuristic in a borderline case.

Neither of these figures need be too accurate for the fields we are considering!

When $q = 25$, we have $q^5/2^q \approx 0.3$ and $3q^3(3/4)^q \approx 35.3$.

In fact, there's exactly one pointless genus-3 curve over $\mathbb{F}_{25}$. (Namely $y^2 = a(x^8 + 1)$ with $a \in \mathbb{F}_{25}$ nonsquare.)

It is a $V_4$-cover of $\mathbb{P}^1$ in five different ways.

# Searches guided by the heuristic.

Over these small fields, it is not hard to enumerate all pointless hyperelliptic genus-3 curves, so we did not need to limit our searches.

But for genus-4 curves over larger fields, it was very helpful to search over restricted classes of curves, each curve having a better-than-average chance of being pointless.

We looked at genus-4 $V_4$-covers of $\mathbb{P}^1$:

$$y^2 = f(x) \qquad z^2 = g(x)$$

where $f$ and $g$ are separable cubic polynomials with no common roots.

# Some genus-4 examples.

| $q$ | Pointless curve | |
|---|---|---|
| 29 | $y^2 = x^3 + x$ | $z^2 = 2x^3 + 12x + 14$ |
| 31 | $y^2 = x^3 - 10$ | $z^2 = 3x^3 + 9$ |
| 37 | $y^2 = x^3 + x + 4$ | $z^2 = 2x^3 - 17x^2 + 5x + 15$ |
| 41 | $y^2 = x^3 + x + 17$ | $z^2 = 3x^3 - x^2 - 12x - 16$ |
| 43 | $y^2 = x^3 - 9$ | $z^2 = 2x^3 + 18$ |
| 47 | $y^2 = x^3 + 5x - 12$ | $z^2 = 5x^3 + 2x^2 + 19x - 9$ |
| 49 | $y^2 = x^3 + 4$ where $a^2 - a + 3 = 0$ | $z^2 = a(x^3 + 2)$ |

Table: Examples, for several fields $\mathbb{F}_q$, of pointless genus-4 curves over $\mathbb{F}_q$ with automorphism group containing the Klein 4-group.

# Closing questions about the heuristic.

## Generic curves of genus $g$.

A generic curve of genus $g$ has a $(g-2)$-dimensional family of degree-$g$ maps to $\mathbb{P}^1$. Generically the Galois group is $S_g$, and $\delta \to 1 - 1/e$ as $g \to \infty$.

## Question

What is the probability that a *generic* curve of genus $g$ over $\mathbb{F}_q$ is pointless? Is it close to $d^{q+1}$, where $d$ is the probability that an element of $S_g$ is a derangement?

## Exercise

For plane quartics $C$, why shouldn't one estimate the probability of pointlessness by using the 1-dimensional family of degree-3 maps $C \to \mathbb{P}^1$?