Zeta Functions of a Class of Artin-Schreier Curves With Many Automorphisms

Renate Scheidler

UNIVERSITY OF CALGARY

Joint work with **Irene Bouw**, **Wei Ho**, **Beth Malmskog**, **Padmavathi Srinivasan** and **Christelle Vincent**

Thanks to *WIN3* — 3^{rd} *Women in Numbers* BIRS Workshop
Banff International Research Station, Banff (Alberta, Canada), April 20-24, 2014

Université de Bordeaux I, 3 March 2015

Our Main Protagonist

Let p be a prime and $\overline{\mathbb{F}}_p$ the algebraic closure of the finite field $\mathbb{F}_p$.

An **Artin-Schreier curve** is a projective curve with an affine equation

$$y^p - y = F(x) \quad \text{with } F(x) \in \overline{\mathbb{F}}_p(x) \text{ non-constant .}$$

Standard examples: elliptic and hyperelliptic curves for $p = 2$.

We focus on the special case of p odd and the curve

$$C_R : y^p - y = xR(x)$$

where $R(x)$ is an **additive** polynomial, i.e. $R(x+z) = R(x) + R(z)$.

These were investigated by van der Geer & van der Vlugt for $p = 2$.

(Compositio Math. **84**, 1992)

Why are these curves of interest?

- Connection to weight enumerators of subcodes of Reed-Muller codes
- Connection to certain lattice constructions
- Potentially good source for algebraic geometry codes
- Lots of interesting properties (especially the automorphisms of C_R)

C_R and Reed-Muller Codes

For $n \in \mathbb{N}$, consider the field $\mathbb{F}_{p^n}$ as an n-dimensional vector space over $\mathbb{F}_p$.

$$\text{Let} \quad \beta : \begin{array}{rcl} \{\text{Polynomials of degree} \leq 2 \text{ in } n \text{ variables}\} & \longrightarrow & \mathbb{F}_{p^n} \cong \mathbb{F}_p^n \\ f & \mapsto & (f(x))_{x \in \mathbb{F}_{p^n}} \end{array}$$

$\mathcal{R}(p, n) = \mathrm{im}(\beta)$ is the **(order 2) Reed-Muller code** over $\mathbb{F}_p$ of length p^n.

Restricting to polynomials f of the form $f(x) = \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x))$ where $R(x)$ runs through all additive polynomials over $\mathbb{F}_{p^n}$ of some fixed degree p^h yields a subcode $\mathcal{C}_h$ of $\mathcal{R}(p, n)$ with good properties.

The weight of a code word $w_R = (\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)))_{x \in \mathbb{F}_{p^n}}$ is

$$\begin{aligned} \mathrm{wt}(w_R) &= \#\{x \in \mathbb{F}_{p^n} \mid \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) \neq 0\} \\ &= p^n - \#\{x \in \mathbb{F}_{p^n} \mid \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0\} \\ &= p^n - \frac{1}{p} \cdot (\text{number of } \mathbb{F}_{p^n}\text{-rational points on } C_R) \end{aligned}$$

because $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0$ if and only if $xR(x) = y^p - y$ for some $y \in \mathbb{F}_{p^n}$, and then exactly all $y + i$ with $i \in \mathbb{F}_p$ satisfy this identity.

So the $\mathbb{F}_{p^n}$-point count for all curves C_R yields the weight enumerator of $\mathcal{C}_h$.

Algebraic Geometry Codes

Let $C : F(x, y) = 0$ be an affine curve over some finite field $\mathbb{F}_{p^n}$ with a unique point at infinity P_∞.

Let S be a set of $\mathbb{F}_{p^n}$-rational points on C, $r \in \mathbb{N}$, and $L(rP_\infty)$ the **Riemann-Roch space** of rP_∞, i.e. the set of functions on C with poles only at P_∞ and each pole of order $\leq r$.

For each $f \in L(rP_\infty)$, the tuple $(f(P))_{P \in S}$ forms a code word, and the collection of all these code words forms an **algebraic geometry code** $\mathcal{C}$.

The length of $\mathcal{C}$ is $\#S$. So curves with lots of $\mathbb{F}_{p^n}$-rational points yield good codes.

Our curves C_R are **maximal** (or **minimal**) for appropriate choices of n, i.e. the $\mathbb{F}_{p^n}$-point count for C_R attains the theoretical maximum (or minimum).

A Symmetric Bilinear Form Associated to C_R

Let $C_R : y^p - y = xR(x)$ with $R(x) \in \overline{\mathbb{F}}_p[x]$ additive.

$R(x)$ is of the form $R(x) = \sum_{i=0}^{h} a_i x^{p^i}$ for some $h \geq 0$, so $\deg(R) = p^h$.

Associated to the quadratic form $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x))$ on $\mathbb{F}_{p^n}$ is the symmetric bilinear form $\frac{1}{2}\left(\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(z) + zR(x))\right)$ with kernel

$$W_n = \{x \in \mathbb{F}_{p^n} \mid \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(z) + zR(x)) = 0 \text{ for all } z \in \mathbb{F}_{p^n}\} .$$

Proposition

W_n is the set of zeros in F_{p^n} of the additive polynomial

$$E(x) = R(x)^{p^h} + \sum_{i=0}^{h} (a_i x)^{p^{h-i}} \text{ of degree } p^{2h}.$$

Define $\mathbb{F}_q$ to be the splitting field of $E(x)$.

Set $W = W_n \cap \mathbb{F}_q$, so $\dim_{\mathbb{F}_p}(W) = 2h$.

Point Count

Recall $C_R : y^p - y = xR(x)$ with $R(x) \in \mathbb{F}_q[x]$ additive.

Theorem

The number of $\mathbb{F}_{p^n}$-rational points on C_R is $p^n + 1$ for $n - w_n$ odd and $p^n + 1 \pm (p-1)p^{(w_n+n)/2}$ for $n - w_n$ even, where $w_n = \dim_{\mathbb{F}_p}(W_n)$.

Proof ingredients: Counting and classical results on the size of the zero locus of a non-degenerate diagonalizable quadratic form over a finite field, applied to the quadric $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x))$ on the quotient space $\mathbb{F}_{p^n}/W_n$ of $\mathbb{F}_p$-dimension $n - w_n$.

Theorem (Hasse-Weil)

Let N be the number of $\mathbb{F}_{p^n}$-rational points of a curve C of genus $g = g(C)$. Then $(p^n+1) - 2gp^{n/2} \leq N \leq (p^n+1) + 2gp^{n/2}$.

Note that $g(C_R) = \dfrac{p^h(p-1)}{2}$, so for $\mathbb{F}_q \subseteq \mathbb{F}_{p^n}$ and n even, C_R is always either maximal or minimal.

Some Points and Automorphisms on AS-Curves

Let $C : y^p - y = F(x) \in \overline{\mathbb{F}}_p(x)$ be an Artin-Schreier curve.

Examples of points on C:

- P_∞
- (a, i) for all $i \in \mathbb{F}_p$, where $F(a) = 0$
- In fact, if (x, y) is a point on C_R, then so is $(x, y + i)$ for all $i \in \mathbb{F}_p$.

Examples of automorphisms on C:

- The identity
- The **Artin-Schreier operator** ρ of order p via $\rho(x, y) = (x, y + 1)$

Note that both these automorphisms fix P_∞.

The points described above are orbits of the Artin-Schreier operator.

Notation

$\mathrm{Aut}(C)$ denotes the group of automorphisms on C defined over $\overline{\mathbb{F}}_p$.
$\mathrm{Aut}^\infty(C)$ denotes the group of automorphisms on C that fix P_∞, i.e. the stabilizer of P_∞ under $\mathrm{Aut}(C)$.

The Group $\mathrm{Aut}(C_R)$

Proposition

- *If $R(x) = x$, then $\mathrm{Aut}(C_R) \cong SL_2(\mathbb{F}_p)$.*
- *If $R(x) = x^p$, then $\mathrm{Aut}(C_R) \cong PGU_3(\mathbb{F}_p)$ (Hermitian case).*
- *If $R(x) \notin \{x, x^p\}$ and $R(x)$ is monic, then $\mathrm{Aut}(C_R) \cong \mathrm{Aut}^{\infty}(C_R)$.*

The map $(x, y) \mapsto (ux, y)$ with $u^{p^h} = a_h^{-1}$ is an isomorphism from C_R to $C_{\tilde{R}}$ where $\tilde{R}(x) = R(ux)$ is monic.

Since we consider automorphisms of C_R over $\overline{\mathbb{F}}_p$, there is thus no restriction to assume that $R(x)$ is monic; structurally, $\mathrm{Aut}(C_R)$ and $\mathrm{Aut}(C_{\tilde{R}})$ are the same.

Moreover, for $R(x) \notin \{x, x^p\}$, if suffices to investigate $\mathrm{Aut}^{\infty}(C_R)$. We now do this for any additive polynomial $R(x)$, including x, x^p, and non-monic ones.

Explicit Description of $\mathrm{Aut}^\infty(C_R)$

Theorem

The automorphisms on C_R that fix P_∞ are precisely of the form

$$\sigma_{a,b,c,d}(x,y) = (ax + c; dy + B_c(ax) + b)$$

where

- $B_c(x) \in x\mathbb{F}_q[x]$ *is the unique polynomial such that*
$$B_c(x)^p - B_c(x) = cR(x) - R(c)x$$
- $d \in \mathbb{F}_p^* \subseteq \mathbb{F}_q$
- $c \in W \subset \mathbb{F}_q$
- $b = B_c(c)/2 + i$ *with* $i \in \mathbb{F}_p$, *so* $b \in \mathbb{F}_q$
- $a^{p^i+1} = d$ *whenever* $a_i \neq 0$, *for* $0 \leq i \leq h$.

Remarks:

- $B_c(x)$ is additive and depends only on c
- $B_c(x) = 0$ if and only if $c = 0$; $\deg(B) = p^{h-1}$ otherwise
- $\sigma_{1,1,0,1} = \rho$ is the Artin-Schreier operator $(x,y) \mapsto (x, y+1)$

Extraspecial Groups

Definition

A non-commutative p-group G is **extraspecial** if its center $Z(G)$ has order p and the quotient group $G/Z(G)$ is elementary abelian.

Theorem

For p odd, the only extraspecial group of order p^3 and exponent p is the group

$$E(p^3) = \langle A, B \mid A^p = B^p = [A, B]^p = 1, \ [A, B] \in Z(E(p^3)) \rangle$$

It is realizable as the **discrete Heisenberg group** *over $\mathbb{F}_p$, i.e. the group of upper triangular 3×3 matrices with entries in $\mathbb{F}_p$ and ones on the diagonal.*

Every extraspecial group of exponent p and odd order p^{2n+1} is the central product of n copies of $E(p^3)$.

The Structure of $\mathrm{Aut}^\infty(C_R)$

Let $H \subset \mathrm{Aut}^\infty(C_R)$ consist of all automorphisms $\sigma_{a,0,0,d}$,
$P \subset \mathrm{Aut}^\infty(C_R)$ consist of all automorphisms $\sigma_{1,b,c,1}$.

Note that all the automorphisms in P are defined over $\mathbb{F}_q$.

Theorem

- *H is a cyclic subgroup of $\mathrm{Aut}^\infty(C_R)$ of order $e\,\dfrac{p-1}{2} \cdot \gcd\limits_{\substack{i \geq 0 \\ a_i \neq 0}}(p^i + 1)$, where $e = 2$ if all of the indices i with $a_i \neq 0$ have the same parity, and $e = 1$ otherwise.*
- *P is the unique Sylow p-subgroup of $\mathrm{Aut}^\infty(C_R)$. It has order p^{2h+1}. and center $Z(P) = \langle \rho \rangle$.*
- *P is normal in $\mathrm{Aut}^\infty(C_R)$, and $\mathrm{Aut}^\infty(C_R) = P \rtimes H$.*
- *If $h = 0$, then $P = Z(P)$. If $h > 0$, then P is an extraspecial group of exponent p and thus a central product of h copies of $E(p^3)$.*

Note: for $p = 2$, P has exponent 4 which yields a factorization of $E(x)$.

Maximal Abelian Subgroups of P

Proposition

Suppose $h \geq 1$ and let M be any maximal abelian subgroup of P. Then the following hold:

- $M \cong (\mathbb{Z}/p\mathbb{Z})^{h+1}$ *and M is normal in P.*
- *Any subgroup $A_p \cong (\mathbb{Z}/p\mathbb{Z})^h$ of M with $\rho \notin A_p$ yields a decomposition $M = \langle\rho\rangle \cup A_1 \cup \cdots \cup A_{p-1} \cup A_p$ where $A_1, \ldots A_{p-1}$ are subgroups of M with $A_i \cong (\mathbb{Z}/p\mathbb{Z})^h$, $\rho \notin A_i$, and $A_i \cap A_j = \{1\}$ for $i \neq j$ $(1 \leq i, j \leq p-1)$.*
- *Any two such subgroups A_p, A'_p of M are P-conjugate.*

Key to these results is the fact that the map $P \to W$ via $\sigma_{1,b,c,1} \to c$ is a surjective group homomorphism whose kernel is $Z(P) = \langle\rho\rangle$.

Any maximal abelian subgroup M of P maps to a maximal isotropic subspace W_M of W, and this correspondence can be made explicit via appropriate basis choices.

Quotient Curves of C_R

Definition

Let C be a curve and G a subgroup of $\mathrm{Aut}(C)$. On the points on C, define the equivalence relation $P \sim Q$ if and only if P and Q belong to the same G-orbit. Then the image of the natural map $C \to C/\sim$ is the **quotient curve** of C by G, denoted C/G.

Proposition

- *Let G be any subgroup of $\mathrm{Aut}^\infty(C_R)$ that contains the Artin-Schreier operator ρ. Then C_R/G has genus zero.*
- *Let $M \cong (Z/p\mathbb{Z})^{h+1}$ be a maximal abelian subgroup of P and $A \cong (\mathbb{Z}/p\mathbb{Z})^h$ a subgroup of M not containing ρ. Then C/A is an Artin-Schreier curve with an affine model of the form $y^p - y = f(x)$ with $f(x) \in \mathbb{F}_q[x]$ of degree 2.*
- *Different choices of A yield $\mathbb{F}_q$-isomorphic curves C/A, so up to isomorphism, $f(x) = f_M(x)$ only depends on M.*

Explicit Affine Models of the Curves C/A

Proposition

Suppose $h \geq 1$. Then for any automorphism $\sigma = \sigma_{1,b,c,1} \in P$ with $c \neq 0$, the quotient curve $C/\langle\sigma\rangle$ is $\mathbb{F}_q$-isomorphic to an Artin-Schreier curve with affine model $y^p - y = x\tilde{R}(x)$ where $\tilde{R}(x) \in \mathbb{F}_q[x]$ is an additive polynomial of degree p^{h-1}.

Proof ingredients: a suitable change of coordinates and messy calculations.

Theorem

Suppose $h \geq 1$ and let $M \cong (Z/p\mathbb{Z})^{h+1}$ be a maximal abelian subgroup of P. For any subgroup $A \cong (\mathbb{Z}/p\mathbb{Z})^h$ of M not containing ρ, the quotient curve C/A is $\mathbb{F}_q$-isomorphic to an an Artin-Schreier curve with affine model $y^p - y = m_M x^2$ where $m_M = \frac{a_h}{2} \prod_{c \in W_M \setminus \{0\}} c \ \in \mathbb{F}_q^*$.

Proof ingredients: decomposition of M from before, the previous proposition, and induction on h.

The Jacobian of C_R

Definition

For a curve C, the free group on the points on C_R is the group of **divisors** on C, denoted $\mathrm{Div}(C_R)$. It contains the subgroup $\mathrm{Div}^0(C)$ of degree zero divisors $D = \sum n_P P$ with $\sum n_P = 0$.

Two divisors are **equivalent** if they differ by a **principal** divisor, i.e. a divisor of the form $\mathrm{div}(\alpha) = \sum n_P P$ where α is a function on C and n_P is the order of vanishing of α at P.

The set of linear equivalence classes of degree zero divisors forms a finite abelian algebraic group which is the **Jacobian** of C, denoted $\mathrm{Jac}(C)$.

Theorem

- $\mathrm{Jac}(C_R)$ *is* $\mathbb{F}_q$*-isogenous to a product of* p^h *copies of Jacobians* $\mathrm{Jac}(C/A)$ *with* A *as in the previous proposition.*
- $\mathrm{Jac}(C_R)$ *is* $\overline{\mathbb{F}}_p$*-isogenous to a product of supersingular elliptic curves (because all the slopes of the Newton polygon of the L-polynomial of* C_R *are equal to* $1/2$ *— stay tuned for L-polynomials).*

The L-Polynomial of a Curve

Definition

Let C be a curve C over a field $\mathbb{F}_q$. For $n \in \mathbb{N}$, the L-**polynomial** of C over $\mathbb{F}_{q^n}$ is the polynomial $L_{C,q^n}(t) = (1-t)(1-q^n t)Z_C(t)$ where $Z_C(t) = \exp(\sum_{k \geq 1} N_k t^k / k)$ is the **zeta function** of C and N_k is the number of $\mathbb{F}_{q^k}$-rational points on C.

Properties:

- $L_{C,q}(t) = \displaystyle\prod_{i=1}^{2g}(1-\alpha_i t) \in \mathbb{Z}[t]$ where $\alpha_i \alpha_{2g-i} = q$ and $|\alpha_i| = \sqrt{q} \;\; \forall i$.
- $L_{C,q^n}(t) = \displaystyle\prod_{i=1}^{2g}(1-\alpha_i^n t)$ and $N_n = 1 + q^n - \displaystyle\sum_{i=1}^{2g} \alpha_i^n$.

So C is $\left\{ \begin{array}{c} \text{maximal} \\ \text{minimal} \end{array} \right\}$ over $\mathbb{F}_{q^n}$ if and only if $\alpha_i^n = \left\{ \begin{array}{c} -q^{n/2} \\ +q^{n/2} \end{array} \right\} \;\forall i$.

L-polynomial of C_R, First Try

Proposition

Let $\mathbb{F}_{p^n}$ be an extension field of $\mathbb{F}_q$.

If n is even, then $L_{C_R,p^n} = (1 \pm p^{n/2}t)^{2g}$.

If n is odd, then $L_{C_R,p^n} = (1 \pm p^n t^2)^g$.

Proof: Write $L_{C_R,p^n} = \prod(1 - \beta_i t)^{2g}$.
Case n even: Then $N_n = p^n + 1 \pm 2gp^{n/2}$, so $\beta_i = \pm p^{n/2}$ for $1 \leq i \leq 2g$.

Case n odd: Then $N_{2n} = p^{2n} + 1 \pm 2gp^n$, so $\beta_i^2 = \pm p^n$ for $1 \leq i \leq 2g$.

Subcase 1: $\beta_i^2 = -p^n \ \ \forall i$. Then $\beta_{2g-i} = p^n/\beta_i = -\beta_i$. This yields g factors $(1 - \beta_i t)(1 - \beta_{2g-i}t) = (1 - \beta_i t)(1 + \beta_i t) = (1 - \beta_i^2 t^2) = 1 + p^n t^2$.

Subcase 2: $\beta_i^2 = p^n \ \ \forall i$. Then $\beta_{2g-i} = p^n/\beta_i = \beta_i$. Since $N_n = p^n + 1$, it is easy to deduce that $\beta_i = p^{n/2}$ for half (i.e. $g/2$) of the indices $i \in \{1, \ldots, g\}$, and $\beta_i = -p^{n/2}$ for the other half. This yields g factors $(1 - p^{n/2}t)(1 + p^{n/2}t) = 1 - p^n t^2$. $\square$

Resolving $+$ and $-$ in $L_{C_R,p^n}(t)$

The decomposition result for maximal abelian subgroups of P yields

$$L_{C_R,q}(t) = L_{C/A,q}(t)^{p^h}$$

where A is as in the previous theorem.

So for $\mathbb{F}_q \subseteq \mathbb{F}_{p^n}$, it suffices to determine $L_{C_R,p^n}(t)$ for $h = 0$, i.e. $R(x) = mx$ with $m \in \mathbb{F}_q$:

- For m a square in $\mathbb{F}_{p^n}^*$, C_{mx} is $\mathbb{F}_q$-isomorphic to the curve C_x defined over $\mathbb{F}_p$, and the problem reduces to simple point-counting on C_x over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$.
- For m a nonsquare in $\mathbb{F}_{p^n}^*$ and n odd, the $\mathbb{F}_q$-automorphism $(x, y) \mapsto (m^{(p^n-p)/2(p-1)}x, y)$ sends C_{mx} to a curve C_{ux} with $u \in \mathbb{F}_p^*$. Then the $\mathbb{F}_p$-automorphism $(x, y) \mapsto (u^i x, y)$ with $2i \equiv -1 \pmod{p}$ sends C_{ux} to C_x, reducing this case to the previous case.
- For m a nonsquare in $\mathbb{F}_{p^n}^*$ and n even, one can count points on C_{mx} and C_x over $\mathbb{F}_{p^n}$ using techniques from the previous two cases.

Note: in the literature, one can find result on zeta functions of curves similar to C_R that resort to Gauss sums.

L-polynomial of C_R

Theorem

Suppose that $\mathbb{F}_q \subseteq \mathbb{F}_{p^n}$. Then

$L_{C_R,p^n}(t) = (1 - p^n t^2)^g$ *if* $p \equiv 1 \pmod 4$ *and* n *is odd.*

$L_{C_R,p^n}(t) = (1 + p^n t^2)^g$ *if* $p \equiv 3 \pmod 4$ *and* n *is odd.*

$L_{C_R,p^n}(t) = (1 - p^{n/2} t)^{2g}$, *with* C_R *a minimal curve over* $\mathbb{F}_{p^n}$, *if*

- $p \equiv 1 \pmod 4$, n *is even and* m *is a square in* $\mathbb{F}_{p^n}^*$ *or*
- $p \equiv 3 \pmod 4$, $n \equiv 0 \pmod 4$ *and* m *is a square in* $\mathbb{F}_{p^n}^*$ *or*
- $p \equiv 3 \pmod 4$, $n \equiv 2 \pmod 4$ *and* m *is a nonsquare in* $\mathbb{F}_{p^n}^*$

$L_{C_R,p^n}(t) = (1 + p^{n/2} t)^{2g}$, *with* C_R *a maximal curve over* $\mathbb{F}_{p^n}$, *if*

- $p \equiv 1 \pmod 4$, n *is even and* m *is a nonsquare in* $\mathbb{F}_{p^n}^*$ *or*
- $p \equiv 3 \pmod 4$, $n \equiv 0 \pmod 4$ *and* m *is a nonsquare in* $\mathbb{F}_{p^n}^*$ *or*
- $p \equiv 3 \pmod 4$, $n \equiv 2 \pmod 4$ *and* m *is a square in* $\mathbb{F}_{p^n}^*$

Here, m is the leading coefficient of $R(x)$ if $h = 0$, and m is any element as given in our earlier construction when $h > 0$.

Some Examples

Examples for $h = 0$, i.e. $R(x) = mx$

The following two maximal curves are additions to the database `www.manYPoints.org`:

- The curve $y^{11} - y = mx^2$, with m a nonsquare in $\mathbb{F}_{11^4}$, is maximal over $\mathbb{F}_{11^4}$.
- The curve $y^{19} - y = mx^2$, with m a nonsquare in $\mathbb{F}_{19^4}$, is maximal over $\mathbb{F}_{19^4}$.

The main difficulty of finding examples of minimal or maximal curves for $h > 0$ is to construct suitable elements m.

Families of examples for $h > 0$ and $R(x) = mx^{p^h}$

- The curve $y^p - y = x^{p^h+1}$ is minimal over $\mathbb{F}_q = \mathbb{F}_{p^{4h}}$.
- The curve $y^p - y = mx^{p^h+1}$, with $m^{p^h-1} = -1$, is maximal over $\mathbb{F}_q = \mathbb{F}_{p^{2h}}$.


Thank You!
Questions?