Equivalence of Functions over Finite Spaces via Group Theory

Ulrich Dempwolff

We consider:

Functions $f : X \to Y$, X, Y finite dimensional spaces over a prime field $\mathbb{F}_p$.

Affine transformations $\alpha = \Phi \circ \tau_v \in \mathsf{AGL}(V)$, $V = X \times Y$, where $\Phi \in \mathsf{GL}(V)$ and for $v = (x_0, y_0)$ one has $(x, y)\tau_v = (x + x_0, y + y_0)$.

Write $\Phi = \begin{pmatrix} \Phi_{XX} & \Phi_{XY} \\ \Phi_{YX} & \Phi_{YY} \end{pmatrix}$ when

$$(x, y)\Phi = (x\Phi_{XX} + y\Phi_{YX}, x\Phi_{XY} + y\Phi_{YY}).$$

$\Gamma(f) = \{(x, f(x)) \mid x \in X\} \subset V = X \times Y$ graph of f.

DEFINITION. Two functions $f, g : X \to Y$ are CCZ equivalent, if there exists $\alpha \in \mathrm{AGL}(V)$ with

$$\Gamma(g) = \Gamma(f)\alpha.$$

If $\alpha = \Phi \circ \tau_v$ ($\Phi = \begin{pmatrix} \Phi_{XX} & \Phi_{XY} \\ \Phi_{YX} & \Phi_{YY} \end{pmatrix}$, $v = (x_0, y_0)$ as above) this means:

$$g(x\Phi_{XX} + f(x)\Phi_{YX} + x_0) = f(x)\Phi_{YY} + x\Phi_{XY} + y_0$$

Requiring $\Phi_{YX} = 0$ leads to:

DEFINITION. Two functions $f, g : X \to Y$ are EA equivalent (extended affine), if there exists $\alpha = \Phi \circ \tau_v \in \mathrm{AGL}(V)$ with $(0 \times Y)\Phi = 0 \times Y$ and

$$\Gamma(g) = \Gamma(f)\alpha.$$

Equivalent to

$$g(x\Phi_{XX} + x_0) = f(x)\Phi_{YY} + x\Phi_{XY} + y_0.$$

Even more special is affine equivalent where we require in addition $(X \times 0)\Phi = X \times 0$ i.e. $\Phi_{XY} = 0$, leading to

$$g(x\Phi_{XX} + x_0) = f(x)\Phi_{YY} + y_0.$$

INVARIANTS

Common Approach: Use invariants to solve equivalence problems.

EXAMPLE: If $g(x) = f(x\Phi_X + x_0)\Phi_Y + x\Phi_{XY} + y_0$ then f and g have the same degree (viewed as polynomial functions).

So two functions with different degrees are not EA equivalent.

EXAMPLE: Let $\mathcal{D}(f)$ be the multiset of $|\Gamma(f) \cap \Gamma(f)\tau_v|$, $v \in V$. Then $\mathcal{D}(f) = \mathcal{D}(g)$ if f and g are CCZ equivalent.

$$\mathbf{G}(f) = \{\alpha \in \mathsf{AGL}(V) \mid \Gamma(f) = \Gamma(f)\alpha\}$$

is the group of CCZ automorphisms.

One has

$$\mathbf{A}(f) \leq \mathbf{EA}(f) \leq \mathbf{G}(f),$$

where $\mathbf{A}(f)$ ($\mathbf{EA}(f)$) is the group of group of affine automorphisms (group of EA automorphisms).

GOAL: Use (partial) knowledge about these groups to solve equivalence problems.

OBSERVATION:

If $\alpha : \Gamma(f) \to \Gamma(g)$ CCZ-isomorphism then

$$\mathbf{G}(g) = \alpha^{-1}\mathbf{G}(f)\alpha.$$

Similarly, for α EA-isomorphism or affine isomorphism

$$\mathbf{EA}(g) = \alpha^{-1}\mathbf{EA}(f)\alpha \quad \text{or} \quad \mathbf{A}(g) = \alpha^{-1}\mathbf{A}(f)\alpha.$$

Lemma. Let $p > 2$ and $f, g : X \to Y$ EA equivalent functions. Assume $f(0) = g(0) = 0$ and $f(-x) = f(x)$, $g(-x) = g(x)$ for all $x \in X$. Then there exist $\Phi_X \in \mathsf{GL}(X)$, $\Phi_Y \in \mathsf{GL}(Y)$, such that

$$f(x\Phi_X) = g(x)\Phi_Y \quad \text{all} \quad x \in X.$$

We have $\iota = diag(-1_X, 1_Y) \in \mathbf{EA}(f) \cap \mathbf{EA}(g)$. Let $\alpha \in \mathrm{AGL}(V)$ be an EA isomorphism from f to g. Then

$$\iota, \alpha^{-1}\iota\alpha \in \mathbf{EA}(g) = \alpha^{-1}\mathbf{EA}(f)\alpha.$$

By Sylow's Theorem there exists $\psi \in \mathbf{EA}(g)$ with

$$\iota = \psi^{-1}(\alpha^{-1}\iota\alpha)\psi.$$

$\beta = \alpha \circ \psi$ is also an EA-automorphism from f to g with

$$\beta\iota = \iota\beta.$$

Forces (if $\beta = \Phi \circ \tau_v$)

$$\Phi = diag(\Phi_X, \Phi_Y) \quad \text{and} \quad v = 0.$$

STRATEGY

Let $\alpha : \Gamma(f) \to \Gamma(g)$ be an EA isomorphism (CCZ isomorphism).

1. Locate groups $A \leq \mathbf{EA}(f)$ (or $\mathbf{G}(f)$) and $B \leq \mathbf{EA}(g)$ (or $\mathbf{G}(g)$).

2. Try to modify α such that $B = \alpha^{-1} A \alpha$ (group theory!).

3. Draw conclusions from 2.

In our case: 1. $A = B = \langle \iota \rangle$, 2. modification $\alpha \to \beta$ by Sylow's Thm. and 3. conclusion $\beta = \Phi$ is an affine isomorphism in $\mathrm{GL}(V)$.

POWER FUNCTIONS:

Let $X = Y = \mathbb{F}_{p^n}$ and define $p_k : X \to Y$ by $p_k(x) = x^k$.

Theorem 1. (Yoshiara 2016, D. 2018) p_k is CCZ equivalent to p_ℓ iff there exists a $0 \leq a < n$, such that $k \equiv p^a \ell \pmod{p^n - 1}$ or $k\ell \equiv p^a \pmod{p^n - 1}$.

SOME MAIORANA BENT FUNCTIONS:

Let $F = \mathbb{F}_{p^n}$, $X = F \times F$, $Y = \mathbb{F}_p$, assume $(k, p^n - 1) = 1$ and define $\mu_k : X \to Y$ by $\mu_k(x_1, x_2) = \mathrm{Tr}(x_1 x_2^k)$ where $\mathrm{Tr} : F \to \mathbb{F}_p$ is the absolute trace. Then μ_k is a bent function (of Maiorana type):

Theorem 2. (D. 2019) μ_k is EA equivalent to μ_ℓ iff there exists a $0 \leq a < n$, such that $k \equiv p^a \ell \pmod{p^n - 1}$.

Note:

Theorem. (Budaghyan, Carlet 2011) Two bent functions are CCZ equivalent iff they are EA equivalent.

ON THEOREM 2:

Observation. Let $(k, p^n - 1) = 1$ and $0 < \bar{k} < p^n - 1$ the unique number with

$$k\bar{k} \equiv -1 \pmod{p^n - 1}.$$

Define $z_a \in \mathrm{GL}(V)$, $a \in F^*$ by

$$z_a = diag(T(a), T(a^{\bar{k}}), 1)$$

where $T(a) : F \ni x \mapsto ax \in F$ i.e.

$$(x_1, x_2, y)z_a = (ax_1, a^{\bar{k}}x_2, y).$$

Then

$$\mathcal{Z}(k) = \{z_a \mid a \in F^*\} \leq \mathbf{A}(\mu_k).$$

Assume $p > 2$ (easier than $p = 2$) and that μ_k and μ_ℓ are EA equivalent.

By the Lemma there exists $\Phi \in \mathrm{GL}(V)$ which fixes $X = F \times F \times 0$ and $Y = 0 \times 0 \times \mathbb{F}_p$ such that

$$\mu_\ell(x_1, x_2)\Phi_Y = \mu_k((x_1, x_2)\Phi_X),$$

in particular:

$$\mathcal{Z}(\ell), \Phi^{-1}\mathcal{Z}(k)\Phi \leq \mathbf{A}(\mu_\ell) = \Phi^{-1}\mathbf{A}(\mu_k)\Phi$$

Goal: Show, that we can choose Φ such that

$$\mathcal{Z}(\ell) = \Phi^{-1}\mathcal{Z}(k)\Phi.$$

Simplification for Φ:

Definition. For a function $f : X \to Y$ and $v \in X$ the function $D_v f : X \to Y$ defined by $D_v f(x) = f(x+v) - f(x)$ is the derivative of f in direction v.

Result: If k is not a p-power, then $D_v D_v \mu_k = 0$ iff $v \in X_1 = F \times 0$.

Consequence: The group $\mathbf{A}(\mu_k)$ (k not a p-power) and Φ_X both fix the subspace X_1.

Byproduct: $\mu_k \not\sim \mu_{p^a}$, k not a p-power.

Let $W = X_1$ or X/X_1. Then the restrictions $(\Phi^{-1}\mathcal{Z}(k)\Phi)_W$ and $\mathcal{Z}(\ell)_W$ are Singer groups in GL(W) but also of $\mathbf{A}(\mu_\ell)_W$. One knows from group theory, that Singer groups of $\mathbf{A}(\mu_\ell)_W$ are conjugate. By adjusting Φ with an element from $\mathbf{A}(\mu_\ell)$ we may assume

$$(\Phi^{-1}\mathcal{Z}(k)\Phi)_W = \mathcal{Z}(\ell)_W.$$

A basic theorem of group theory (Schur-Zassenhaus Theoren) allows a further adjustment, so that we may even assume

$$\Phi^{-1}\mathcal{Z}(k)\Phi = \mathcal{Z}(\ell).$$

A generator of $\mathcal{Z}(k)$ has the form

$$z_\omega = diag(T(\omega), T(\omega^{\bar{k}}), 1) = \begin{pmatrix} T(\omega) & 0 & 0 \\ 0 & T(\omega^{\bar{k}}) & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

ω primitive in F^*. Note $\Phi = diag(\Phi_{X_1}, \Phi_{X_2}, c)$ ($X_2 = 0 \times F$), so

$$\Phi^{-1} z_\omega \Phi = diag(\Phi_{X_1}^{-1} T(\omega) \Phi_{X_1}, \Phi_{X_2}^{-1} T(\omega^{\bar{k}}) \Phi_{X_2}, 1)$$

is a generator of $\mathcal{Z}(\ell)$. Typical element of $\mathcal{Z}(\ell)$

$$z'_\zeta = diag(T(\zeta), T(\zeta^{\bar{\ell}}), 1).$$

For a suitable ζ:

$$\Phi_{X_1}^{-1} T(\omega) \Phi_{X_1} = T(\zeta), \quad \Phi_{X_2}^{-1} T(\omega^{\bar{k}}) \Phi_{X_2} = T(\zeta^{\bar{\ell}})$$

The characteristic polynomial of the $\mathbb{F}_p$-linear operator $T(a)$ is

$$f_a(X) = (X - a)(X - a^p) \cdots (X - a^{p^{n-1}}).$$

Hence

$$f_\omega(X) = f_\zeta(X) \quad and \quad f_{\omega^{\bar{k}}}(X) = f_{\zeta^{\bar{\ell}}}(X).$$

Conclude

$$\ell \equiv p^x k \pmod{p^n - 1}.$$

ON THEOREM 1:

Set $X = Y = F = \mathbb{F}_{p^n}$, $V = X \times Y$ and recall $p_k(x) = x^k$. Set

$$z_a = diag(T(a), T(a^k)).$$

Then

$$\mathcal{Z}(k) = \{z_a \mid a \in F^*\} \leq \mathbf{A}(p_k).$$

GOAL: Show, that there exists $\Phi \in \mathrm{GL}(V)$ such that

$$\Phi^{-1}\mathcal{Z}(k)\Phi = \mathcal{Z}(\ell)$$

and that either Φ fixes X and Y; i.e.

$$\Phi = diag(\Phi_X, \Phi_Y) \quad \Rightarrow \quad \ell \equiv p^a k \pmod{p^n - 1}$$

or Φ interchanges X and Y; i.e.

$$\Phi = \begin{pmatrix} 0 & \Phi_{XY} \\ \Phi_{YX} & 0 \end{pmatrix} \quad \Rightarrow \quad k\ell \equiv p^a \pmod{p^n - 1}.$$

Easy:

If $\alpha \in \mathrm{AGL}(V)$ with $\Gamma(p_\ell) = \Gamma(p_k)\alpha$ then there exists even $\Phi \in \mathrm{GL}(V)$ with $\Gamma(p_\ell) = \Gamma(p_k)\Phi$. In particular:

$$\mathbf{G}(p_\ell) = \Phi^{-1}\mathbf{G}(p_k)\Phi$$

From number theory:

Theorem. (Zsigmondy 1899) Let p be a prime, $n > 1$.
(1) Either there exists a prime r which divides $p^n - 1$ but not $p^k - 1$ for $1 \leq k < n$.
(2) Or $n = 2$, $p + 1$ is a 2-power or $p = 2$, $n = 6$.

Assume, that we can use Zsigmondy's Theorem and let $r \mid p^n - 1$ a "Zsigmondy prime".

For $m = k, \ell$ let $\mathcal{Z}(m)_r$ be the Sylow r-subgroup of $\mathcal{Z}(m)$.

Easy: $\mathcal{Z}(m)_r$ is a Sylow r-subgroup of $\mathbf{G}(p_m)$. By Sylow's Theorem we may assume.

$$\mathcal{Z}(\ell)_r = \Phi^{-1}\mathcal{Z}(k)_r\Phi.$$

Let

$$z = diag(T(\omega), T(\omega^k))$$

be a generator of $\mathcal{Z}(k)_r$. The restriction of z to X and Y have characteristic polynomials $f_\omega(X)$ and $f_{\omega^k}(X)$. Distinguish:

Case A. $f_\omega(X) \neq f_{\omega^k}(X)$

Case B. $f_\omega(X) = f_{\omega^k}(X)$

To Case A:

X and Y are the **only spaces** invariant under $\mathcal{Z}(\ell)_r = \Phi^{-1}\mathcal{Z}(k)_r\Phi$

$\Rightarrow X$ and Y are the **only spaces** invariant under $\mathcal{Z}(\ell)$ and $\Phi^{-1}\mathcal{Z}(k)\Phi$ since these groups commute with $\mathcal{Z}(\ell)_r$

$$\Rightarrow \mathcal{Z}(\ell) = \Phi^{-1}\mathcal{Z}(k)\Phi \quad \text{done!}$$

To Case B: More difficult.

Here $T(\omega) \sim T(\omega^k)$ where $z = diag(T(\omega), T(\omega^k))$. With $\phi = T(\omega)$:

$$z \sim \begin{pmatrix} \phi & 0 \\ 0 & \phi \end{pmatrix}.$$

By Schur's Lemma (consider as ϕ as irreducible $n \times n$-matrix)

$$\{\psi \in \mathbb{F}_p^{n \times n} \mid \psi\phi = \phi\psi\} \simeq F \simeq \mathbb{F}_{p^n}$$

and

$$H = \{\Psi \in \mathsf{GL}(V) \mid \Psi z = z\Psi\} \simeq \mathsf{GL}(2, p^n).$$

This group is very well studied!

Have

$$\mathcal{Z}(\ell),\ \Phi^{-1}\mathcal{Z}(k)\Phi \leq H.$$

WARNING: Two cyclic subgroups of order $p^n - 1$ in H need not to be conjugate!

HOWEVER: $\mathcal{Z}(\ell)$ and $\Phi^{-1}\mathcal{Z}(k)\Phi$ leave the set $\Gamma(p_\ell) \subset V$ invariant.

Then group theoretic arguments show, that there exists a

$$\Psi \in \langle \mathcal{Z}(\ell), \Phi^{-1}\mathcal{Z}(k)\Phi \rangle$$

with

$$\mathcal{Z}(\ell) = \Psi^{-1}(\Phi^{-1}\mathcal{Z}(k)\Phi)\Psi = (\Phi\Psi)^{-1}\mathcal{Z}(k)\Phi\Psi \quad \text{done!}$$