Resemblance

Robert Coulter

Department of Mathematical Sciences
University of Delaware
Newark, DE 19716 USA
coulter@udel.edu

September 2023

Joint work

This is joint work with

Dr. Li-An Chen
Department of Mathematical Sciences
Boise State University
Boise, ID 83725 USA

The work presented here comes from her Ph.D dissertation, which she completed recently with me at the University of Delaware.

Disclaimers

Disclaimers

It is not once, nor twice, but times without number that the same ideas make their appearance in the world – Aristotle

Disclaimers

> *It is not once, nor twice, but times without number that the same ideas make their appearance in the world* – Aristotle

To the best of my knowledge, the central idea to be discussed in this talk has not been studied before

Disclaimers

> *It is not once, nor twice, but times without number that the same ideas make their appearance in the world* – Aristotle

To the best of my knowledge, the central idea to be discussed in this talk has not been studied before. . . but that doesn't mean it has not.

Disclaimers

> *It is not once, nor twice, but times without number that the same ideas make their appearance in the world* – Aristotle

To the best of my knowledge, the central idea to be discussed in this talk has not been studied before. . . but that doesn't mean it has not.

The utility of the basic idea is up for debate

Disclaimers

> *It is not once, nor twice, but times without number that the same ideas make their appearance in the world* – Aristotle

To the best of my knowledge, the central idea to be discussed in this talk has not been studied before. . . but that doesn't mean it has not.

The utility of the basic idea is up for debate – I think it could be important, but we haven't yet got something astounding from it.

Some notation

Throughout $\mathcal{G}$ denotes a finite group of order q, written additively but not necessarily abelian, and $\mathcal{G}^\star = \mathcal{G} \setminus \{0\}$.

For a finite set $\mathcal{S}$, $\#\mathcal{S}$ denotes the cardinality of $\mathcal{S}$.

Some notation

Throughout $\mathcal{G}$ denotes a finite group of order q, written additively but not necessarily abelian, and $\mathcal{G}^\star = \mathcal{G} \setminus \{0\}$.

For a finite set $\mathcal{S}$, $\#\mathcal{S}$ denotes the cardinality of $\mathcal{S}$.

Now let $f : \mathcal{G} \to \mathcal{G}$.

Then $\mathrm{Im}(f) = \{f(x) : x \in \mathcal{G}\}$ denotes the image set of f,

and $V(f) = \#\,\mathrm{Im}(f)$ denotes the cardinality of the image set.

Let $f : \mathcal{G} \to \mathcal{G}$.

Question: How do we measure how close f is to being a permutation?

Let $f : \mathcal{G} \to \mathcal{G}$.

Question: How do we measure how close f is to being a permutation?

The standard answer is $V(f)$, the size of the image set of f.
(Or $\#\mathcal{G} + 1 - V(f)$, if you're that way inclined.)

The motivating example

The motivating example

Let $\mathcal{G}$ be any group of order $2n$ with n odd, and let $\mathcal{H}$ be the normal subgroup of $\mathcal{G}$ of index 2.

Choose any $a \in \mathcal{G} \setminus \mathcal{H}$, so that $\mathcal{H}$ and $a + \mathcal{H}$ are the two cosets of $\mathcal{H}$ that partition $\mathcal{G}$.

The motivating example

Let $\mathcal{G}$ be any group of order $2n$ with n odd, and let $\mathcal{H}$ be the normal subgroup of $\mathcal{G}$ of index 2.

Choose any $a \in \mathcal{G} \setminus \mathcal{H}$, so that $\mathcal{H}$ and $a + \mathcal{H}$ are the two cosets of $\mathcal{H}$ that partition $\mathcal{G}$.

Define a function $f : \mathcal{G} \to \mathcal{G}$ so that it is bijective on $\mathcal{H}$ and where $f(a + h) = f(h)$ for all $h \in \mathcal{H}$.

The motivating example

Let $\mathcal{G}$ be any group of order $2n$ with n odd, and let $\mathcal{H}$ be the normal subgroup of $\mathcal{G}$ of index 2.

Choose any $a \in \mathcal{G} \setminus \mathcal{H}$, so that $\mathcal{H}$ and $a + \mathcal{H}$ are the two cosets of $\mathcal{H}$ that partition $\mathcal{G}$.

Define a function $f : \mathcal{G} \to \mathcal{G}$ so that it is bijective on $\mathcal{H}$ and where $f(a + h) = f(h)$ for all $h \in \mathcal{H}$.

Then $V(f) = n$, half the size of the group on which it is defined.

The motivating example

Let $\mathcal{G}$ be any group of order $2n$ with n odd, and let $\mathcal{H}$ be the normal subgroup of $\mathcal{G}$ of index 2.

Choose any $a \in \mathcal{G} \setminus \mathcal{H}$, so that $\mathcal{H}$ and $a + \mathcal{H}$ are the two cosets of $\mathcal{H}$ that partition $\mathcal{G}$.

Define a function $f : \mathcal{G} \to \mathcal{G}$ so that it is bijective on $\mathcal{H}$ and where $f(a + h) = f(h)$ for all $h \in \mathcal{H}$.

Then $V(f) = n$, half the size of the group on which it is defined.

Question: Do you think f is nearly a permutation?

The motivating example

Let $\mathcal{G}$ be any group of order $2n$ with n odd, and let $\mathcal{H}$ be the normal subgroup of $\mathcal{G}$ of index 2.

Choose any $a \in \mathcal{G} \setminus \mathcal{H}$, so that $\mathcal{H}$ and $a + \mathcal{H}$ are the two cosets of $\mathcal{H}$ that partition $\mathcal{G}$.

Define a function $f : \mathcal{G} \to \mathcal{G}$ so that it is bijective on $\mathcal{H}$ and where $f(a + h) = f(h)$ for all $h \in \mathcal{H}$.

Then $V(f) = n$, half the size of the group on which it is defined.

Now define $g : \mathcal{G} \to \mathcal{G}$ by $g(h) = 0$ and $g(a + h) = a$ for all $h \in \mathcal{H}$.

The motivating example

Let $\mathcal{G}$ be any group of order $2n$ with n odd, and let $\mathcal{H}$ be the normal subgroup of $\mathcal{G}$ of index 2.

Choose any $a \in \mathcal{G} \setminus \mathcal{H}$, so that $\mathcal{H}$ and $a + \mathcal{H}$ are the two cosets of $\mathcal{H}$ that partition $\mathcal{G}$.

Define a function $f : \mathcal{G} \to \mathcal{G}$ so that it is bijective on $\mathcal{H}$ and where $f(a + h) = f(h)$ for all $h \in \mathcal{H}$.

Then $V(f) = n$, half the size of the group on which it is defined.

Now define $g : \mathcal{G} \to \mathcal{G}$ by $g(h) = 0$ and $g(a + h) = a$ for all $h \in \mathcal{H}$.

Then it is easy to see that $g + f$ is a permutation.

The motivating example

Let $\mathcal{G}$ be any group of order $2n$ with n odd, and let $\mathcal{H}$ be the normal subgroup of $\mathcal{G}$ of index 2.

Choose any $a \in \mathcal{G} \setminus \mathcal{H}$, so that $\mathcal{H}$ and $a + \mathcal{H}$ are the two cosets of $\mathcal{H}$ that partition $\mathcal{G}$.

Define a function $f : \mathcal{G} \to \mathcal{G}$ so that it is bijective on $\mathcal{H}$ and where $f(a + h) = f(h)$ for all $h \in \mathcal{H}$.

Then $V(f) = n$, half the size of the group on which it is defined.

Now define $g : \mathcal{G} \to \mathcal{G}$ by $g(h) = 0$ and $g(a + h) = a$ for all $h \in \mathcal{H}$.

Then it is easy to see that $g + f$ is a permutation.

Question: Do you think f is nearly a permutation now?

The basic idea

Definition

Let $f, h : \mathcal{G} \to \mathcal{G}$.

The *resemblance* $\mathrm{Res}(f, h)$ of f to h is defined by

$$\mathrm{Res}(f, h) = V(f - h).$$

The basic idea

Definition

Let $f, h : \mathcal{G} \to \mathcal{G}$.

The *resemblance* $\mathrm{Res}(f, h)$ of f to h is defined by

$$\mathrm{Res}(f, h) = V(f - h).$$

The following facts are easily observed.

The basic idea

Definition

Let $f, h : \mathcal{G} \to \mathcal{G}$.

The *resemblance* $\mathrm{Res}(f, h)$ of f to h is defined by

$$\mathrm{Res}(f, h) = V(f - h).$$

The following facts are easily observed.

- $\mathrm{Res}(f, h) = \mathrm{Res}(h, f)$.

The basic idea

Definition

Let $f, h : \mathcal{G} \to \mathcal{G}$.

The *resemblance* $\mathrm{Res}(f, h)$ of f to h is defined by

$$\mathrm{Res}(f, h) = V(f - h).$$

The following facts are easily observed.

- $\mathrm{Res}(f, h) = \mathrm{Res}(h, f)$.
- $\mathrm{Res}(f, c + h) = \mathrm{Res}(f, h)$ for any constant $c \in \mathcal{G}$.

The basic idea

Definition

Let $f, h : \mathcal{G} \to \mathcal{G}$.

The *resemblance* $\mathrm{Res}(f, h)$ of f to h is defined by

$$\mathrm{Res}(f, h) = V(f - h).$$

The following facts are easily observed.

- $\mathrm{Res}(f, h) = \mathrm{Res}(h, f)$.
- $\mathrm{Res}(f, c + h) = \mathrm{Res}(f, h)$ for any constant $c \in \mathcal{G}$.
- $1 \leq \mathrm{Res}(f, h) \leq \#\mathcal{G}$.
  The minimum is achieved when $f = h$, while the maximum can be achieved when one of f or h is a constant and the other a bijection.

The basic idea

Definition

Let $f, h : \mathcal{G} \to \mathcal{G}$.

The *resemblance* $\mathrm{Res}(f, h)$ *of* f *to* h is defined by

$$\mathrm{Res}(f, h) = V(f - h).$$

The utility of this idea is in its application in certain directions.

The basic idea

Definition

Let $f, h : \mathcal{G} \to \mathcal{G}$.

The *resemblance* $\mathrm{Res}(f, h)$ *of* f *to* h is defined by

$$\mathrm{Res}(f, h) = V(f - h).$$

The utility of this idea is in its application in certain directions.

For a given function $f : \mathcal{G} \to \mathcal{G}$, consider

$$\min\{\mathrm{Res}(f, h) : h \text{ has property P}\}.$$

This is a way to measure how far f is from having property P.

Two examples

Let $\Omega_{\mathcal{G}}$ denote the set of all permutation functions on $\mathcal{G}$, and let $\mathrm{Hom}(\mathcal{G})$ be the set of all homomorphisms on $\mathcal{G}$.

Two examples

Let $\Omega_{\mathcal{G}}$ denote the set of all permutation functions on $\mathcal{G}$, and let $\mathrm{Hom}(\mathcal{G})$ be the set of all homomorphisms on $\mathcal{G}$.

Definition

For $f : \mathcal{G} \to \mathcal{G}$, we define

- the *permutation resemblance* of f by

$$\text{P-Res}(f) = \min\{\text{Res}(f, h) : h \in \Omega_{\mathcal{G}}\},$$

Two examples

Let $\Omega_{\mathcal{G}}$ denote the set of all permutation functions on $\mathcal{G}$, and let $\mathrm{Hom}(\mathcal{G})$ be the set of all homomorphisms on $\mathcal{G}$.

Definition

For $f : \mathcal{G} \to \mathcal{G}$, we define

- the *permutation resemblance* of f by

$$\text{P-Res}(f) = \min\{\text{Res}(f, h) : h \in \Omega_{\mathcal{G}}\},$$

- the *linear resemblance* of f by

$$\text{L-Res}(f) = \min\{\text{Res}(f, h) : h \in \mathrm{Hom}(\mathcal{G})\},$$

The central idea

Definition

For $f : \mathcal{G} \to \mathcal{G}$, we define the *permutation resemblance of* f by

$$\text{P-Res}(f) = \min\{\text{Res}(f, h) \ : \ h \in \Omega_{\mathcal{G}}\},$$

The central idea

Definition

For $f : \mathcal{G} \to \mathcal{G}$, we define the *permutation resemblance of* f by

$$\text{P-Res}(f) = \min\{\text{Res}(f, h) \ : \ h \in \Omega_{\mathcal{G}}\},$$

or equivalently,

$$\text{P-Res}(f) = \min\{\text{Res}(f, h) \ : \ h \in \Omega_{\mathcal{G}}\}$$

The central idea

Definition

For $f : \mathcal{G} \to \mathcal{G}$, we define the *permutation resemblance of* f by

$$\text{P-Res}(f) = \min\{\text{Res}(f, h) \ : \ h \in \Omega_{\mathcal{G}}\},$$

or equivalently,

$$\text{P-Res}(f) = \min\{V(f - h) \ : \ h \in \Omega_{\mathcal{G}}\}$$

The central idea

Definition

For $f : \mathcal{G} \to \mathcal{G}$, we define the *permutation resemblance of* f by

$$\text{P-Res}(f) = \min\{\text{Res}(f, h) \ : \ h \in \Omega_{\mathcal{G}}\},$$

or equivalently, by writing $f - h = -g$,

$$\text{P-Res}(f) = \min\{V(f - h) \ : \ h \in \Omega_{\mathcal{G}}\}$$

The central idea

Definition

For $f : \mathcal{G} \to \mathcal{G}$, we define the *permutation resemblance of* f by

$$\text{P-Res}(f) = \min\{\text{Res}(f, h) \, : \, h \in \Omega_{\mathcal{G}}\},$$

or equivalently, by writing $f - h = -g$,

$$\text{P-Res}(f) = \min\{V(g) \, : \, g + f \in \Omega_{\mathcal{G}}\}.$$

First things first

$$\text{P-Res}(f) = \min\{V(g) \,:\, g + f \in \Omega_{\mathcal{G}}\}.$$

We're hoping to use permutation resemblance as a reasonable measure of how far a function f over $\mathcal{G}$ is from being a permutation.

First things first

$$\text{P-Res}(f) = \min\{V(g) \,:\, g + f \in \Omega_{\mathcal{G}}\}.$$

We're hoping to use permutation resemblance as a reasonable measure of how far a function f over $\mathcal{G}$ is from being a permutation.

We do at least have the extremes doing what we would want, for we have:

- $\text{P-Res}(f) = 1$ if and only if f is a permutation, and
- $\text{P-Res}(f) = \#\mathcal{G}$ if and only if f is a constant.

First things first

$$\text{P-Res}(f) = \min\{V(g) \,:\, g + f \in \Omega_{\mathcal{G}}\}.$$

We're hoping to use permutation resemblance as a reasonable measure of how far a function f over $\mathcal{G}$ is from being a permutation.

We do at least have the extremes doing what we would want, for we have:

- $\text{P-Res}(f) = 1$ if and only if f is a permutation, and
- $\text{P-Res}(f) = \#\mathcal{G}$ if and only if f is a constant.

And no, $\text{P-Res}(f) \neq \#\mathcal{G} + 1 - V(f)$.

First things first

$$\text{P-Res}(f) = \min\{V(g) \,:\, g + f \in \Omega_{\mathcal{G}}\}.$$

We're hoping to use permutation resemblance as a reasonable measure of how far a function f over $\mathcal{G}$ is from being a permutation.

We do at least have the extremes doing what we would want, for we have:

- $\text{P-Res}(f) = 1$ if and only if f is a permutation, and
- $\text{P-Res}(f) = \#\mathcal{G}$ if and only if f is a constant.

And no, $\text{P-Res}(f) \neq \#\mathcal{G} + 1 - V(f)$. (At least not always!)

Intuition behind the idea

$$\text{P-Res}(f) = \min\{V(g) \,:\, g + f \in \Omega_{\mathcal{G}}\}.$$

Permutation resemblance is equal to the minimum value $V(g)$ (the smallest image size) as g runs through all functions on $\mathcal{G}$ for which $g + f$ is a permutation.

So P-Res measures the smallest number of different shifts required to alter a function so that it becomes a permutation.

Intuition behind the idea

$$\text{P-Res}(f) = \min\{V(g) \,:\, g + f \in \Omega_{\mathcal{G}}\}.$$

Permutation resemblance is equal to the minimum value $V(g)$ (the smallest image size) as g runs through all functions on $\mathcal{G}$ for which $g + f$ is a permutation.

So P-Res measures the smallest number of different shifts required to alter a function so that it becomes a permutation.

It isn't hard to see that this is very different from $V(f)$; just think back to that example.

That easy example

That easy example

Let $\mathcal{G}$ be any group of order $2n$ with n odd, and let $\mathcal{H}$ be the normal subgroup of $\mathcal{G}$ of index 2.

Choose any $a \in \mathcal{G} \setminus \mathcal{H}$, so that $\mathcal{H}$ and $a + \mathcal{H}$ are the two cosets of $\mathcal{H}$ that partition $\mathcal{G}$.

Define a function $f : \mathcal{G} \to \mathcal{G}$ so that it is bijective on $\mathcal{H}$ and where $f(a + h) = f(h)$ for all $h \in \mathcal{H}$.

Then $V(f) = n$, half the size of the group on which it is defined.

Now define the function $g : \mathcal{G} \to \mathcal{G}$ given by $g(h) = 0$ and $g(a + h) = a$ for all $h \in \mathcal{H}$.

So $g + f \in \Omega_{\mathcal{G}}$, but

That easy example

Let $\mathcal{G}$ be any group of order $2n$ with n odd, and let $\mathcal{H}$ be the normal subgroup of $\mathcal{G}$ of index 2.

Choose any $a \in \mathcal{G} \setminus \mathcal{H}$, so that $\mathcal{H}$ and $a + \mathcal{H}$ are the two cosets of $\mathcal{H}$ that partition $\mathcal{G}$.

Define a function $f : \mathcal{G} \to \mathcal{G}$ so that it is bijective on $\mathcal{H}$ and where $f(a + h) = f(h)$ for all $h \in \mathcal{H}$.

Then $V(f) = n$, half the size of the group on which it is defined.

Now define the function $g : \mathcal{G} \to \mathcal{G}$ given by $g(h) = 0$ and $g(a + h) = a$ for all $h \in \mathcal{H}$.

So $g + f \in \Omega_{\mathcal{G}}$, but we can make n, and hence $V(f)$, arbitrarily large in this example, while the permutation resemblance will always be 2.

Better bounds

Let $f : \mathcal{G} \to \mathcal{G}$. We define two terms.

- For $b \in \mathcal{G}$, the set of preimages of b under f is denoted by

$$\mathsf{PreIm}(f, b) = \{x \in \mathcal{G} : f(x) = b\}.$$

Better bounds

Let $f : \mathcal{G} \to \mathcal{G}$. We define two terms.

- For $b \in \mathcal{G}$, the set of preimages of b under f is denoted by

$$\mathrm{PreIm}(f, b) = \{x \in \mathcal{G} : f(x) = b\}.$$

- The *uniformity* of f is given by

$$u(f) = \max_{b \in \mathcal{G}} \# \mathrm{PreIm}(f, b).$$

Better bounds

Let $f : \mathcal{G} \to \mathcal{G}$. We define two terms.

- For $b \in \mathcal{G}$, the set of preimages of b under f is denoted by

$$\mathrm{PreIm}(f, b) = \{x \in \mathcal{G} : f(x) = b\}.$$

- The *uniformity* of f is given by

$$u(f) = \max_{b \in \mathcal{G}} \# \mathrm{PreIm}(f, b).$$

Theorem

For $f : \mathcal{G} \to \mathcal{G}$,

$$\text{P-Res}(f) \qquad .$$

Better bounds

Let $f : \mathcal{G} \to \mathcal{G}$. We define two terms.

- For $b \in \mathcal{G}$, the set of preimages of b under f is denoted by

$$\mathrm{PreIm}(f, b) = \{x \in \mathcal{G} : f(x) = b\}.$$

- The *uniformity* of f is given by

$$u(f) = \max_{b \in \mathcal{G}} \# \mathrm{PreIm}(f, b).$$

Theorem

For $f : \mathcal{G} \to \mathcal{G}$,

$$\text{P-Res}(f) \leq \qquad\qquad .$$

Better bounds

Let $f : \mathcal{G} \to \mathcal{G}$. We define two terms.

- For $b \in \mathcal{G}$, the set of preimages of b under f is denoted by

$$\mathrm{PreIm}(f, b) = \{x \in \mathcal{G} : f(x) = b\}.$$

- The *uniformity* of f is given by

$$u(f) = \max_{b \in \mathcal{G}} \# \mathrm{PreIm}(f, b).$$

Theorem

For $f : \mathcal{G} \to \mathcal{G}$,

$$\text{P-Res}(f) \leq \#\mathcal{G} + 1 - V(f).$$

Better bounds

Let $f : \mathcal{G} \to \mathcal{G}$. We define two terms.

- For $b \in \mathcal{G}$, the set of preimages of b under f is denoted by

$$\mathrm{PreIm}(f, b) = \{x \in \mathcal{G} : f(x) = b\}.$$

- The *uniformity* of f is given by

$$u(f) = \max_{b \in \mathcal{G}} \# \mathrm{PreIm}(f, b).$$

Theorem

For $f : \mathcal{G} \to \mathcal{G}$,

$$\leq \text{P-Res}(f) \leq \#\mathcal{G} + 1 - V(f).$$

Better bounds

Let $f : \mathcal{G} \to \mathcal{G}$. We define two terms.

- For $b \in \mathcal{G}$, the set of preimages of b under f is denoted by

$$\mathrm{PreIm}(f, b) = \{x \in \mathcal{G} : f(x) = b\}.$$

- The *uniformity* of f is given by

$$u(f) = \max_{b \in \mathcal{G}} \# \mathrm{PreIm}(f, b).$$

Theorem

For $f : \mathcal{G} \to \mathcal{G}$,

$$u(f) \leq \text{P-Res}(f) \leq \#\mathcal{G} + 1 - V(f).$$

Proving the lower bound

Theorem For $f : \mathcal{G} \to \mathcal{G}$,

$$u(f) \leq \text{P-Res}(f).$$

Proving the lower bound

Theorem For $f : \mathcal{G} \to \mathcal{G}$,

$$u(f) \leq \text{P-Res}(f).$$

For any $\text{PreIm}(f, b)$ of cardinality at least 2, choose distinct $x, y \in \text{PreIm}(f, b)$.

When $g + f$ is a permutation, we have

$$\begin{aligned}(g+f)(x) \neq (g+f)(y) &\Rightarrow g(x) + b \neq g(y) + b \\ &\Rightarrow g(x) \neq g(y),\end{aligned}$$

so that g must be injective on every preimage set of f, implying $u(f) \leq V(g)$ whenever $g + f$ is a permutation.

Proving the upper bound

Theorem For $f : \mathcal{G} \to \mathcal{G}$,

$$\text{P-Res}(f) \leq \#\mathcal{G} + 1 - V(f).$$

Proving the upper bound

Theorem For $f : \mathcal{G} \to \mathcal{G}$,

$$\text{P-Res}(f) \leq \#\mathcal{G} + 1 - V(f).$$

The proof is by construction (of g).

Let g map exactly one element from each non-empty set $\text{PreIm}(f, b)$ to 0.

Then $0 \in \text{Im}(g)$ and $\text{Im}(f) \subseteq \text{Im}(g + f)$.

Proving the upper bound

Theorem For $f : \mathcal{G} \to \mathcal{G}$,

$$\text{P-Res}(f) \leq \#\mathcal{G} + 1 - V(f).$$

The proof is by construction (of g).

Let g map exactly one element from each non-empty set $\text{PreIm}(f, b)$ to 0.

Then $0 \in \text{Im}(g)$ and $\text{Im}(f) \subseteq \text{Im}(g + f)$.

At this point, both the domain and codomain of g have $\#\mathcal{G} - V(f)$ elements left unassigned.

Proving the upper bound

Theorem For $f : \mathcal{G} \to \mathcal{G}$,

$$\text{P-Res}(f) \leq \#\mathcal{G} + 1 - V(f).$$

The proof is by construction (of g).

Let g map exactly one element from each non-empty set $\text{PreIm}(f, b)$ to 0.

Then $0 \in \text{Im}(g)$ and $\text{Im}(f) \subseteq \text{Im}(g + f)$.

At this point, both the domain and codomain of g have $\#\mathcal{G} - V(f)$ elements left unassigned.

Now pair off the unassigned domain/codomain elements (x, y) and set $g(x) = y - f(x)$.

This ensures $g + f \in \Omega_{\mathcal{G}}$ and $V(g) \leq \#\mathcal{G} + 1 - V(f)$ at worst.

The bounds can be the same

$$u(f) \leq \text{P-Res}(f) \leq \#\mathcal{G} + 1 - V(f).$$

The bounds can be the same

$$u(f) = \text{P-Res}(f) = \#\mathcal{G} + 1 - V(f).$$

The bounds can be the same

$$u(f) = \text{P-Res}(f) = \#\mathcal{G} + 1 - V(f).$$

Theorem

Let $f : \mathcal{G} \to \mathcal{G}$.

Then $u(f) = \#\mathcal{G} + 1 - V(f)$ if and only if f is a permutation or there exists a unique element $b \in \mathcal{G}$ for which $\#\,\text{PreIm}(f, b) > 1$.

The bounds can be the same

$$u(f) = \text{P-Res}(f) = \#\mathcal{G} + 1 - V(f).$$

Theorem
Let $f : \mathcal{G} \to \mathcal{G}$.
Then $u(f) = \#\mathcal{G} + 1 - V(f)$ if and only if f is a permutation or there exists a unique element $b \in \mathcal{G}$ for which $\#\,\text{PreIm}(f, b) > 1$.

The immediate implication is that P-Res can meet either bound.

But the real question is how does P-Res really behave?

For starters, perhaps we should determine if it can be equal to either bound when they are not the same?

The bounds can be the same

$$u(f) = \text{P-Res}(f) = \#\mathcal{G} + 1 - V(f).$$

Theorem
Let $f : \mathcal{G} \to \mathcal{G}$.
Then $u(f) = \#\mathcal{G} + 1 - V(f)$ if and only if f is a permutation or there exists a unique element $b \in \mathcal{G}$ for which $\#\,\text{PreIm}(f, b) > 1$.

The immediate implication is that P-Res can meet either bound.

But the real question is how does P-Res really behave?

For starters, perhaps we should determine if it can be equal to either bound when they are not the same?

The proof of that upper bound is on a worst-case scenario, so we don't expect that most functions will be at or near it, so we concentrated on the lower bound.

Two classes of functions that achieve the lower bound, I

Let p be prime and $\mathbb{F}_p$ denote the finite field of p elements.

Two classes of functions that achieve the lower bound, I

Let p be prime and $\mathbb{F}_p$ denote the finite field of p elements.

Theorem

Let $\eta(X) = X^{(p-1)/2} \in \mathbb{F}_p[X]$ with p an odd prime. Then

$$\text{P-Res}(\eta) = \begin{cases} u(\eta) + 1 = \frac{p+1}{2}, & \text{if } p \equiv 1 \pmod 4; \\ u(\eta) = \frac{p-1}{2}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Two classes of functions that achieve the lower bound, I

Let p be prime and $\mathbb{F}_p$ denote the finite field of p elements.

Theorem
Let $\eta(X) = X^{(p-1)/2} \in \mathbb{F}_p[X]$ with p an odd prime. Then

$$\text{P-Res}(\eta) = \begin{cases} u(\eta) + 1 = \frac{p+1}{2}, & \text{if } p \equiv 1 \pmod 4; \\ u(\eta) = \frac{p-1}{2}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Note that $\eta(X)$ is the quadratic character over $\mathbb{F}_p$, so that $V(\eta) = 3$.
Thus we see

$$\frac{p \pm 1}{2} = \text{P-Res}(\eta) < p - 2$$

provided $p \geq 7$.

Indeed, we see P-Res is roughly half of the possible upper bound for this class of functions.

Two classes of functions that achieve the lower bound, II

Now let $q = p^e$ for some natural number e.

Recall that the set of p-polynomials over $\mathbb{F}_q$, that is those of the form

$$\sum_i a_i X^{p^i},$$

represents the set of all linear operators of $(\mathbb{F}_q, +)$ when viewed as a vector space over $\mathbb{F}_p$.

Two classes of functions that achieve the lower bound, II

Now let $q = p^e$ for some natural number e.

Recall that the set of p-polynomials over $\mathbb{F}_q$, that is those of the form

$$\sum_i a_i X^{p^i},$$

represents the set of all linear operators of $(\mathbb{F}_q, +)$ when viewed as a vector space over $\mathbb{F}_p$.

Theorem

Any p-polynomial $L \in \mathbb{F}_q[X]$ satisfies P-Res$(L) = u(L)$.

Proof that linear operators meet the lower bound

Let $L \in \mathbb{F}_{p^e}[X]$ be a linear operator.

Proof that linear operators meet the lower bound

Let $L \in \mathbb{F}_{p^e}[X]$ be a linear operator.

Its image set is a k-dimensional subspace of $\mathbb{F}_q$.

Thus $V(L) = p^k$.

Further, we can partition $\mathbb{F}_q$ into p^{e-k} additive cosets of $\mathrm{Im}(L)$ with coset representatives $\{c_i\}$.

Proof that linear operators meet the lower bound

Let $L \in \mathbb{F}_{p^e}[X]$ be a linear operator.

Its image set is a k-dimensional subspace of $\mathbb{F}_q$.

Thus $V(L) = p^k$.

Further, we can partition $\mathbb{F}_q$ into p^{e-k} additive cosets of $\mathrm{Im}(L)$ with coset representatives $\{c_i\}$.

Its null set $\mathcal{N}$ is an $(e-k)$-dimensional subspace.

Further, for any $b \in \mathrm{Im}(L)$, $\mathrm{PreIm}(L, b) = \mathcal{N} + z$ where $L(z) = b$.

Thus $u(L) = p^{e-k}$.

Further, we can partition $\mathbb{F}_q$ into p^{e-k} subsets $\mathcal{A}_i$ of size p^k in such a way that each $\mathcal{A}_i$ contains exactly one preimage for every element of $\mathrm{Im}(L)$.

Proof that linear operators meet the lower bound

Let $L \in \mathbb{F}_{p^e}[X]$ be a linear operator.

Its image set is a k-dimensional subspace of $\mathbb{F}_q$.

Thus $V(L) = p^k$.

Further, we can partition $\mathbb{F}_q$ into p^{e-k} additive cosets of $\mathrm{Im}(L)$ with coset representatives $\{c_i\}$.

Its null set $\mathcal{N}$ is an $(e-k)$-dimensional subspace.

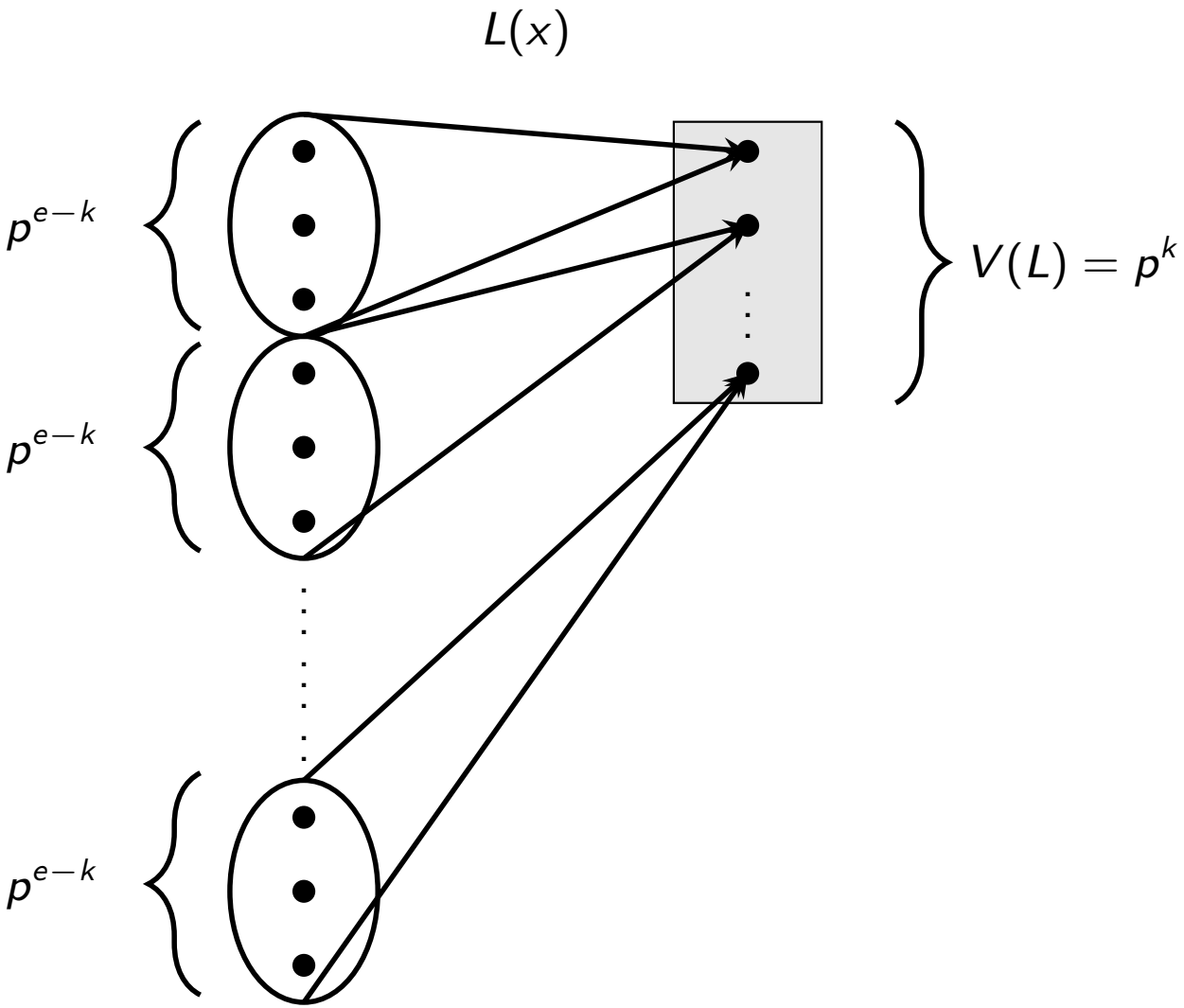
Further, for any $b \in \mathrm{Im}(L)$, $\mathrm{PreIm}(L, b) = \mathcal{N} + z$ where $L(z) = b$.

Thus $u(L) = p^{e-k}$.

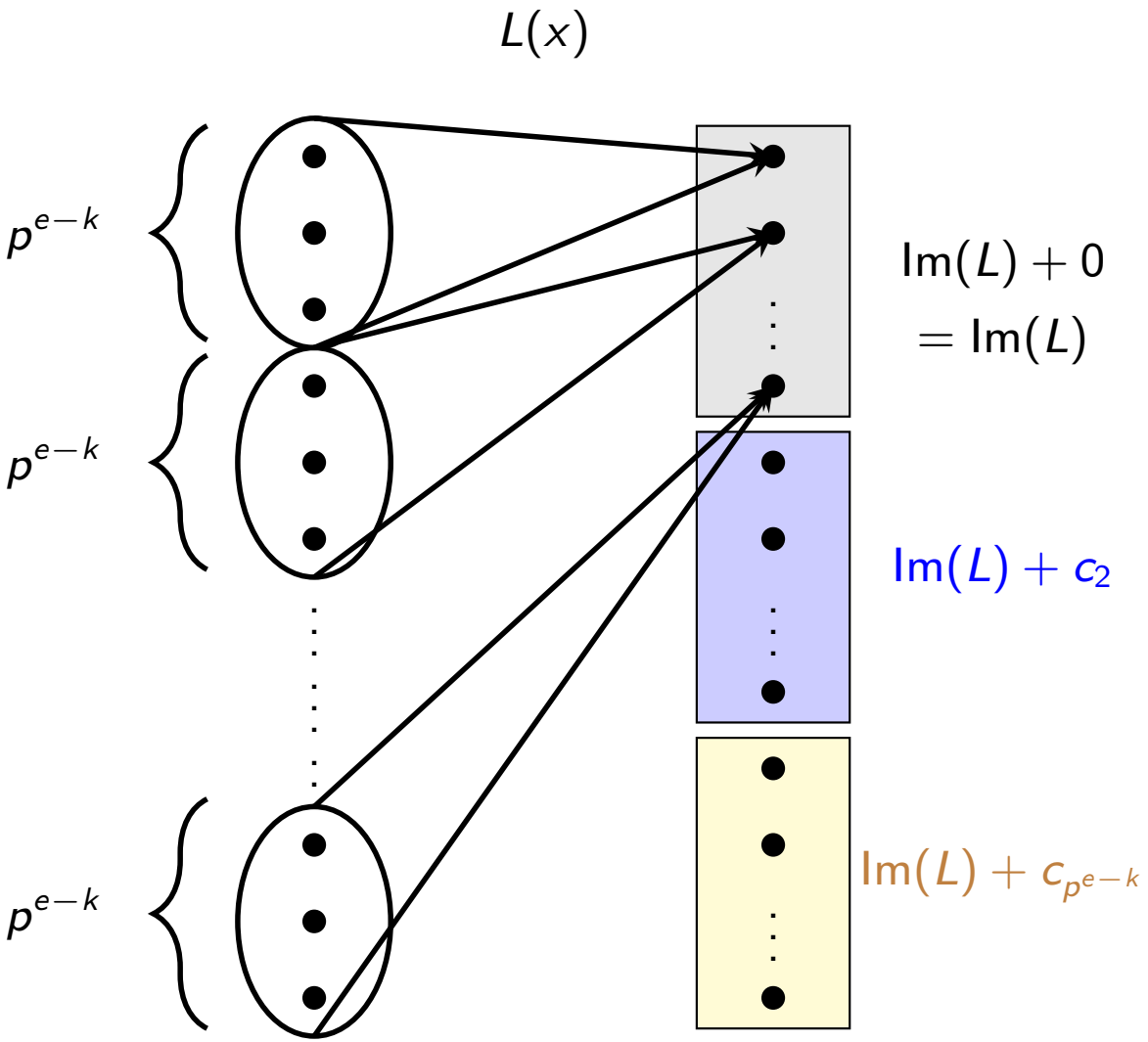
Further, we can partition $\mathbb{F}_q$ into p^{e-k} subsets $\mathcal{A}_i$ of size p^k in such a way that each $\mathcal{A}_i$ contains exactly one preimage for every element of $\mathrm{Im}(L)$.

All of this allows for a nice little argument.

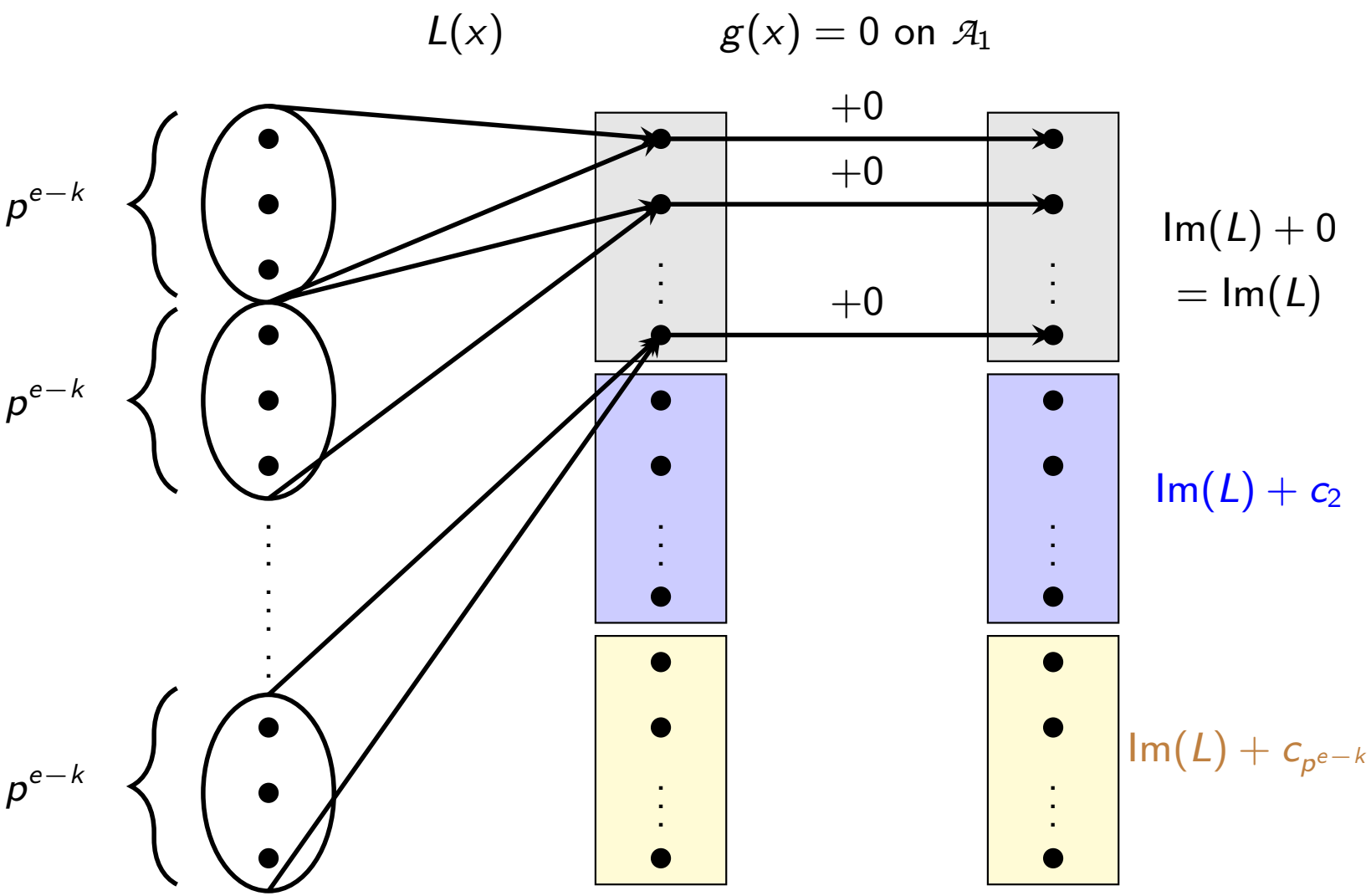
Proof that linear operators meet the lower bound



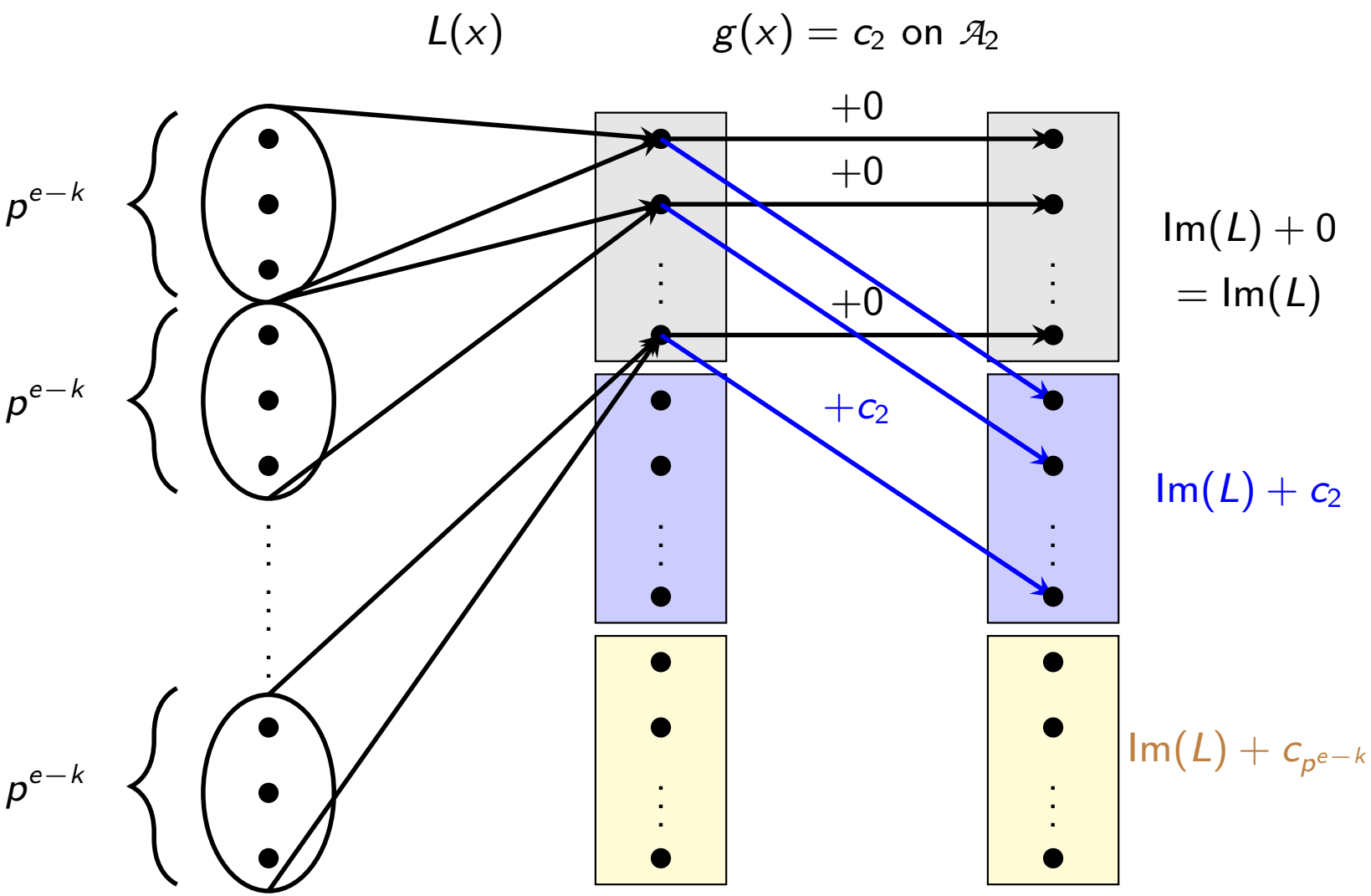
Proof that linear operators meet the lower bound



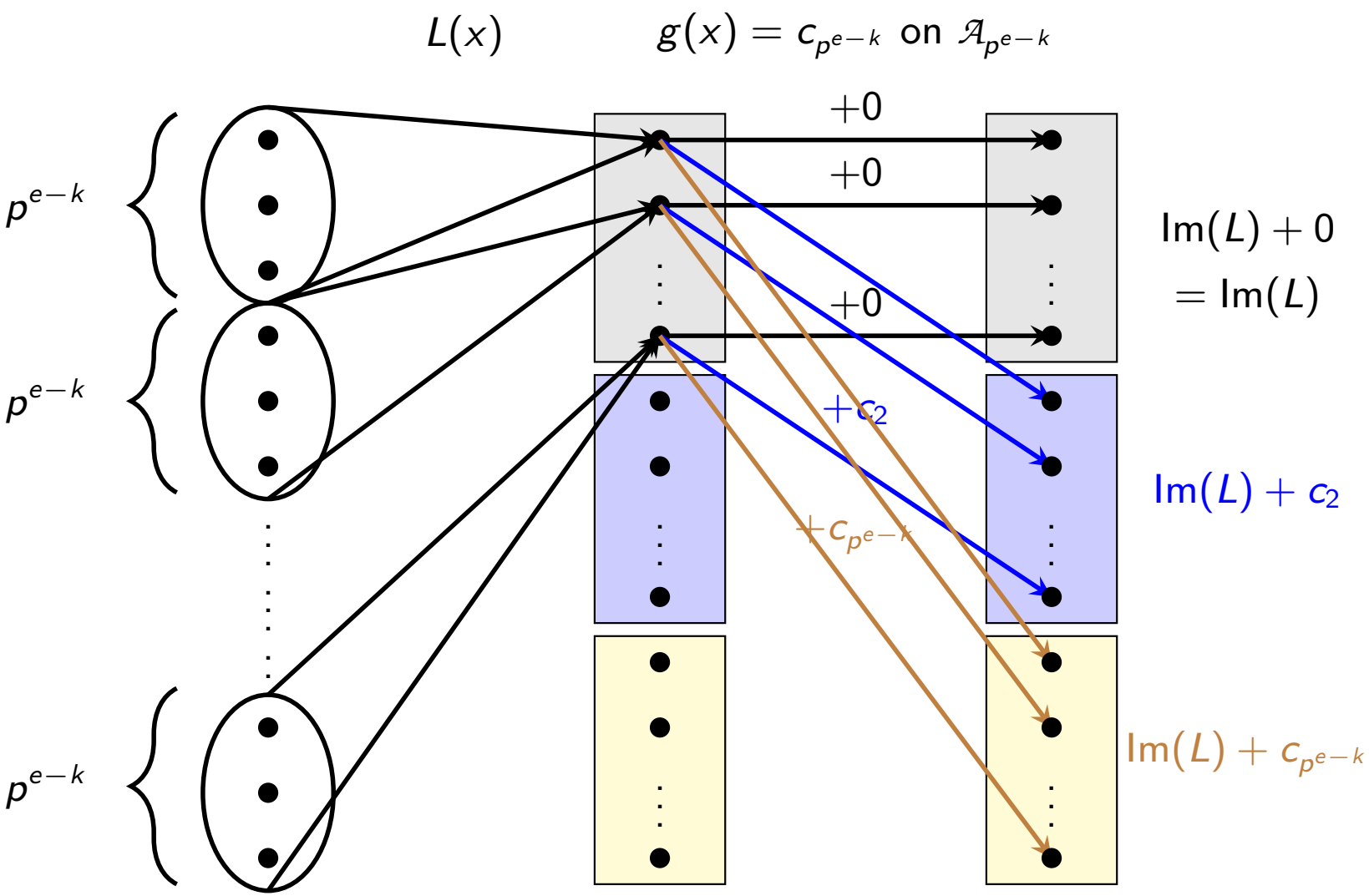
Proof that linear operators meet the lower bound



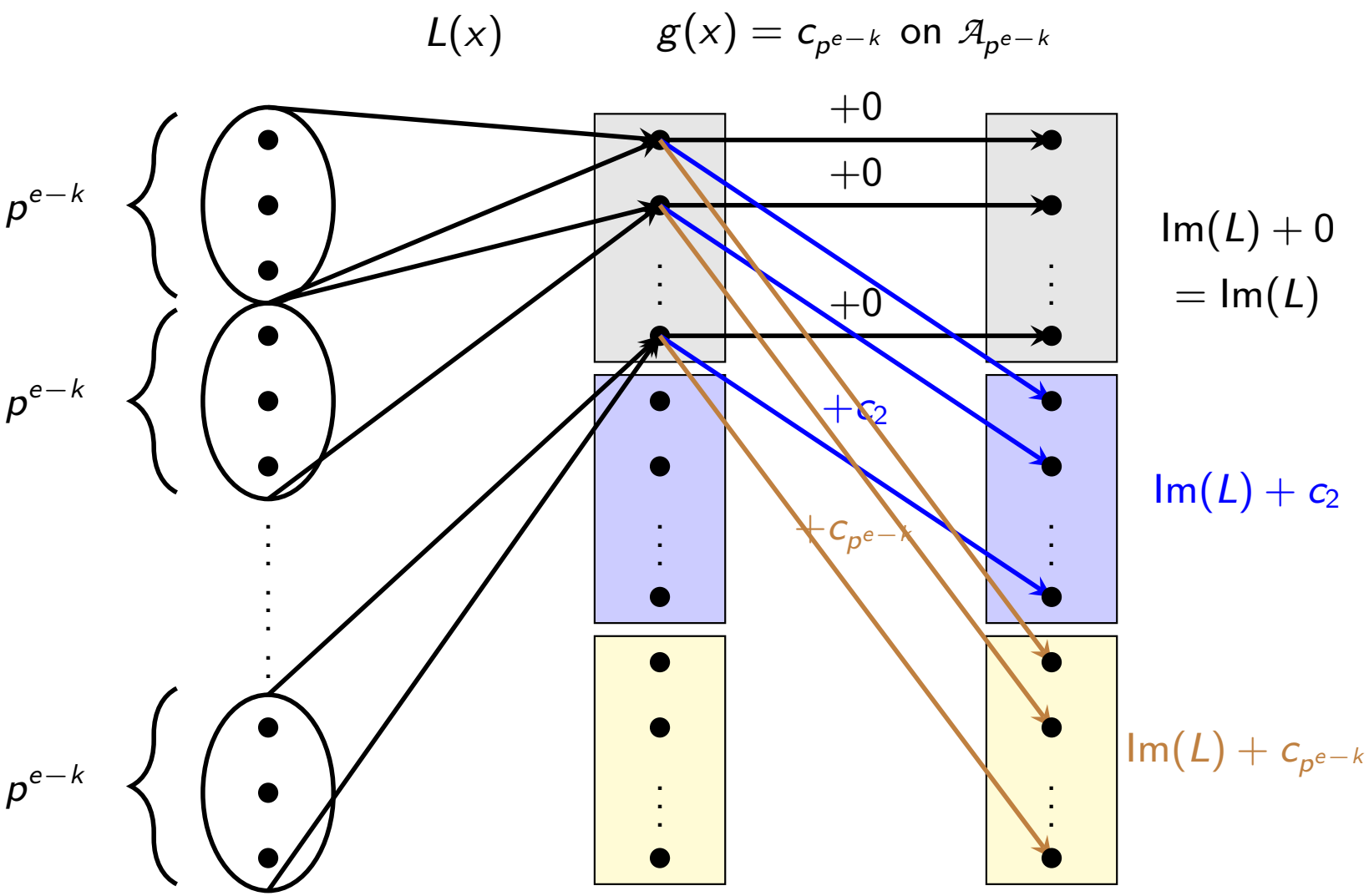
Proof that linear operators meet the lower bound



Proof that linear operators meet the lower bound



Proof that linear operators meet the lower bound



So $u(L) \leq \text{P-Res}(L) \leq p^{e-k} = u(L)$.

An application of permutation resemblance

Differential uniformity

Let $\mathcal{G}$ be an abelian group and $f : \mathcal{G} \to \mathcal{G}$.

Define the *differential operator* of f with respect to $a \in \mathcal{G}$ by

$$\Delta_{f,a}(x) = f(x+a) - f(x).$$

For $(a, b) \in \mathcal{G}^\star \times \mathcal{G}$, define

$$\delta_f(a, b) = \#\,\mathrm{PreIm}(\Delta_{f,a}, b).$$

The *differential uniformity of f (DU)* is given by

$$\delta_f = \max_{a \in \mathcal{G}^*, b \in \mathcal{G}} \delta_f(a, b).$$

Differential uniformity

The applications of DU are famous.

Differential uniformity

The applications of DU are famous to those present.

Differential uniformity

Low DU permutations are, of course, highly desirable.

For finite fields $\mathbb{F}_q$, our best possible differential uniformities are:

- When q is even, we have APN functions, which are 2-DU.

Differential uniformity

Low DU permutations are, of course, highly desirable.

For finite fields $\mathbb{F}_q$, our best possible differential uniformities are:

- When q is even, we have APN functions, which are 2-DU.
  As we all know, constructing APN permutations in square ordered fields of characteristic 2 is a big problem.

Differential uniformity

Low DU permutations are, of course, highly desirable.

For finite fields $\mathbb{F}_q$, our best possible differential uniformities are:

- When q is even, we have APN functions, which are 2-DU.
  As we all know, constructing APN permutations in square ordered fields of characteristic 2 is a big problem.
  And we're not doing very well.
- When q is odd, we have planar functions, which are 1-DU.

Differential uniformity

Low DU permutations are, of course, highly desirable.

For finite fields $\mathbb{F}_q$, our best possible differential uniformities are:

- When q is even, we have APN functions, which are 2-DU.
  As we all know, constructing APN permutations in square ordered fields of characteristic 2 is a big problem.
  And we're not doing very well.
- When q is odd, we have planar functions, which are 1-DU.
  Here, we've got a bigger issue, as we know planar functions cannot be permutations, meaning the best we can hope for is near-optimal DU permutations.

P-Res and DU

Theorem

Let $\mathcal{G}$ be a finite abelian group and $f, g : \mathcal{G} \to \mathcal{G}$. Then

$$\delta_{g+f} \leq \delta_f \cdot \left(V(g)^2 - V(g) + 1\right).$$

P-Res and DU

Theorem

Let $\mathcal{G}$ be a finite abelian group and $f, g : \mathcal{G} \to \mathcal{G}$. Then

$$\delta_{g+f} \leq \delta_f \cdot \left(V(g)^2 - V(g) + 1\right).$$

Again, the bound comes from a worst-case scenario we don't expect to happen in most cases.

The whole point

$$\delta_{g+f} \leq \delta_f \cdot \left(V(g)^2 - V(g) + 1\right).$$

The whole point

$$\delta_{g+f} \leq \delta_f \cdot \left(V(g)^2 - V(g) + 1\right).$$

Now apply the bound in the case where g is one of those functions for which $g + f$ is a permutation that most resembles f.

This means $V(g) = \text{P-Res}(f)$, and $g + f \in \Omega_{\mathcal{G}}$. So

$$\delta_{g+f} \leq \delta_f \cdot \left(\text{P-Res}(f)^2 - \text{P-Res}(f) + 1\right)$$

The whole point

$$\delta_{g+f} \leq \delta_f \cdot \left(V(g)^2 - V(g) + 1\right).$$

Now apply the bound in the case where g is one of those functions for which $g + f$ is a permutation that most resembles f.

This means $V(g) = \text{P-Res}(f)$, and $g + f \in \Omega_{\mathcal{G}}$. So

$$\delta_{g+f} \leq \delta_f \cdot \left(\text{P-Res}(f)^2 - \text{P-Res}(f) + 1\right)$$

We are therefore constructing permutations from f whose differential uniformity is bounded above by only δ_f and P-Res(f).

In the case where we start with a planar function, we find we are guaranteed to construct permutations $h = g + f$ for which

$$\delta_h \leq \text{P-Res}(f)^2 - \text{P-Res}(f) + 1.$$

And what of P-Res for planar functions?

And what of P-Res for planar functions?

Theorem

Let $f \in \mathbb{F}_q[X]$ be planar. Then

$$2 < \text{P-Res}(f) \leq \frac{q+1}{2}.$$

And what of P-Res for planar functions?

Theorem

Let $f \in \mathbb{F}_q[X]$ be planar. Then

$$2 < \text{P-Res}(f) \leq \frac{q+1}{2}.$$

This is quite disappointing

And what of P-Res for planar functions?

Theorem

Let $f \in \mathbb{F}_q[X]$ be planar. Then

$$2 < \text{P-Res}(f) \leq \frac{q+1}{2}.$$

This is quite disappointing, and it doesn't get much better if we weaken the hypothesis to...

And what of P-Res for planar functions?

Theorem

Let $f \in \mathbb{F}_q[X]$ be planar. Then

$$2 < \text{P-Res}(f) \leq \frac{q+1}{2}.$$

This is quite disappointing, and it doesn't get much better if we weaken the hypothesis to...

Theorem

Let $f \in \mathbb{F}_q[X]$, q odd, and suppose $f(0) = 0$ and f is two-to-one on $\mathbb{F}_q^\star$. Then

$$\text{P-Res}(f) \leq \left\lceil 2\sqrt{q-1} \right\rceil - 1.$$

When $q-1$ is a perfect square, the bound can be improved to

$$\text{P-Res}(f) \leq 2\sqrt{q-1} - 2.$$

Computational aspects

You really can!

$$\text{P-Res}(f) = \min\{V(g) \,:\, g + f \in \Omega_{\mathcal{G}}\}.$$

You really can!

$$\text{P-Res}(f) = \min\{V(g) \,:\, g + f \in \Omega_{\mathcal{G}}\}.$$

At first glance, finding a decent algorithm for determining permutation resemblance would appear to be hard.

You really can!

$$\text{P-Res}(f) = \min\{V(g) \,:\, g + f \in \Omega_{\mathcal{G}}\}.$$

At first glance, finding a decent algorithm for determining permutation resemblance would appear to be hard.

However, to my great surprise, Li-An found a nice way of turning this into an optimization problem which could be solved using linear integer programming techniques.

With her IP techniques, we can determine:

You really can!

$$\text{P-Res}(f) = \min\{V(g) \,:\, g + f \in \Omega_{\mathcal{G}}\}.$$

At first glance, finding a decent algorithm for determining permutation resemblance would appear to be hard.

However, to my great surprise, Li-An found a nice way of turning this into an optimization problem which could be solved using linear integer programming techniques.

With her IP techniques, we can determine:

- P-Res(f) for any function f defined on a group, and

You really can!

$$\text{P-Res}(f) = \min\{V(g) \,:\, g + f \in \Omega_{\mathcal{G}}\}.$$

At first glance, finding a decent algorithm for determining permutation resemblance would appear to be hard.

However, to my great surprise, Li-An found a nice way of turning this into an optimization problem which could be solved using linear integer programming techniques.

With her IP techniques, we can determine:

- P-Res(f) for any function f defined on a group, and
- permutations with the best possible DU over a given field (or even specifying a desired maximum DU).

You really can!

$$\text{P-Res}(f) = \min\{V(g) \,:\, g + f \in \Omega_{\mathcal{G}}\}.$$

At first glance, finding a decent algorithm for determining permutation resemblance would appear to be hard.

However, to my great surprise, Li-An found a nice way of turning this into an optimization problem which could be solved using linear integer programming techniques.

With her IP techniques, we can determine:

- P-Res(f) for any function f defined on a group, and
- permutations with the best possible DU over a given field (or even specifying a desired maximum DU).

The two algorithms can also be combined in such a way as to significantly reduce the number of variables of the combined IP while finding low DU functions among those permutations that most resemble a given f. The cost is that you can no longer insist upon optimal low DU.

Using the P-Res algorithm on x^2

All of the computational results I give here were generated on a simple laptop.

Our initial concerns with resemblance have been to prove some theoretical results and establish the feasiblility of computational results.

Using the P-Res algorithm on x^2

Using the P-Res algorithm on x^2

Prime p	P-Res(x^2)	$\lceil 2\sqrt{q-1} \rceil - 1$
13 to 37	4	6 to 11
41	5	12
43,47,103	4	12,13,20
53 to 101	5	14 to 19
107 to 251	5	20 to 31
257	6	31
263,269,271	5	32
277,281	6	33
293,307,311	5	34,34,35
313	6	35
317	5	35
331,337	6	36

Note the very slow growth of P-Res.

We obtained similar results for prime powers $q \leq 343$, and for x^d with $d \mid (q-1)$.

Using the optimal DU algorithm

Using the optimal DU algorithm

Using the optimal DU strategy:

Using the optimal DU algorithm

Using the optimal DU strategy:

- We first tested the full algorithm in some small fields.
  For $\mathbb{F}_{17}$ and $\mathbb{F}_{19}$ the algorithm found optimal solutions in under half an hour. In both cases, we found 2-DU permutation polynomials with many terms.

Using the optimal DU algorithm

Using the optimal DU strategy:

- We first tested the full algorithm in some small fields.
  For $\mathbb{F}_{17}$ and $\mathbb{F}_{19}$ the algorithm found optimal solutions in under half an hour. In both cases, we found 2-DU permutation polynomials with many terms.
- On the otherhand, over $\mathbb{F}_9$ we only find 3-DU permutations, showing there is no 2-DU permutation over $\mathbb{F}_9$.

Using the optimal DU algorithm

Using the optimal DU strategy:

- We first tested the full algorithm in some small fields.
  For $\mathbb{F}_{17}$ and $\mathbb{F}_{19}$ the algorithm found optimal solutions in under half an hour. In both cases, we found 2-DU permutation polynomials with many terms.
- On the otherhand, over $\mathbb{F}_9$ we only find 3-DU permutations, showing there is no 2-DU permutation over $\mathbb{F}_9$.
- Not surprisingly, for larger q, we start to run into memory and time issues.

Using the optimal DU algorithm

Using the optimal DU strategy:

- We first tested the full algorithm in some small fields.
  For $\mathbb{F}_{17}$ and $\mathbb{F}_{19}$ the algorithm found optimal solutions in under half an hour. In both cases, we found 2-DU permutation polynomials with many terms.
- On the otherhand, over $\mathbb{F}_9$ we only find 3-DU permutations, showing there is no 2-DU permutation over $\mathbb{F}_9$.
- Not surprisingly, for larger q, we start to run into memory and time issues.

The optimal DU IP algorithm is sufficiently adaptable that we can weaken the optimality condition, insisting only that the algorithm find a permutation with DU≥ 3.

When we do so, the algorithm finds 3-DU permutations over $\mathbb{F}_q$ for all $q \leq 37$ in decent time frames.

Using the 2-step P-Res/DU algorithm

When we use the 2-step algorithm, the reduction in variables drastically improves the efficiency of the algorithm.

Using the 2-step P-Res/DU algorithm

When we use the 2-step algorithm, the reduction in variables drastically improves the efficiency of the algorithm.

In odd characteristic, we tested the algorithm against x^2.

- We find optimal 3-DU permutations over $\mathbb{F}_q$ for all odd q in the range $17 \leq q \leq 37$. The algorithm takes under 4 seconds (on a laptop) to complete in each of these cases.

Using the 2-step P-Res/DU algorithm

When we use the 2-step algorithm, the reduction in variables drastically improves the efficiency of the algorithm.

In odd characteristic, we tested the algorithm against x^2.

- We find optimal 3-DU permutations over $\mathbb{F}_q$ for all odd q in the range $17 \leq q \leq 37$. The algorithm takes under 4 seconds (on a laptop) to complete in each of these cases.
- For $q \in \{41, 43, 47, 49\}$, we find 4-DU permutations, all in under 3 minutes. These are again optimal.

Using the 2-step P-Res/DU algorithm

When we use the 2-step algorithm, the reduction in variables drastically improves the efficiency of the algorithm.

In odd characteristic, we tested the algorithm against x^2.

- We find optimal 3-DU permutations over $\mathbb{F}_q$ for all odd q in the range $17 \leq q \leq 37$. The algorithm takes under 4 seconds (on a laptop) to complete in each of these cases.
- For $q \in \{41, 43, 47, 49\}$, we find 4-DU permutations, all in under 3 minutes. These are again optimal.

We also did some initial testing against APN functions.

Using the 2-step P-Res/DU algorithm

When we use the 2-step algorithm, the reduction in variables drastically improves the efficiency of the algorithm.

In odd characteristic, we tested the algorithm against x^2.

- We find optimal 3-DU permutations over $\mathbb{F}_q$ for all odd q in the range $17 \leq q \leq 37$. The algorithm takes under 4 seconds (on a laptop) to complete in each of these cases.
- For $q \in \{41, 43, 47, 49\}$, we find 4-DU permutations, all in under 3 minutes. These are again optimal.

We also did some initial testing against APN functions.

- Over $\mathbb{F}_{64}$, the APN function x^3 has P-Res $= 7$. It took under 2 seconds to find a 6-DU permutation among those that resemble x^3 the closest. (This may or may not be optimal.)
  For the APN function $f(x) = x^{24} + \alpha^{59}x^{17} + \alpha^{60}x^3$, which has P-Res $= 5$, we find an optimal 6-DU permutation in under 3 minutes.

Using the 2-step P-Res/DU algorithm

When we use the 2-step algorithm, the reduction in variables drastically improves the efficiency of the algorithm.

In odd characteristic, we tested the algorithm against x^2.

- We find optimal 3-DU permutations over $\mathbb{F}_q$ for all odd q in the range $17 \leq q \leq 37$. The algorithm takes under 4 seconds (on a laptop) to complete in each of these cases.
- For $q \in \{41, 43, 47, 49\}$, we find 4-DU permutations, all in under 3 minutes. These are again optimal.

We also did some initial testing against APN functions.

- Over $\mathbb{F}_{64}$, the APN function x^3 has P-Res $= 7$. It took under 2 seconds to find a 6-DU permutation among those that resemble x^3 the closest. (This may or may not be optimal.)
  For the APN function $f(x) = x^{24} + \alpha^{59}x^{17} + \alpha^{60}x^3$, which has P-Res $= 5$, we find an optimal 6-DU permutation in under 3 minutes.
- Over $\mathbb{F}_{256}$, again using the APN function x^3, with a non-optimal setting the algorithm finds an 8-DU permutation in under 4 minutes.

Open problems

Open problems

The most pressing ones might be:

- Expand the computational results for P-Res, especially with regard to finding new low-DU permutations in odd characteristic and in simply carrying out much more work on APN functions. (Also using some significant computing power might be an idea!)

Open problems

The most pressing ones might be:

- Expand the computational results for P-Res, especially with regard to finding new low-DU permutations in odd characteristic and in simply carrying out much more work on APN functions. (Also using some significant computing power might be an idea!)
- Understand the behavior of P-Res better, especially the computational results on P-Res(x^2), which suggests we should be able to prove much better bounds in such cases.

Open problems

The most pressing ones might be:

- Expand the computational results for P-Res, especially with regard to finding new low-DU permutations in odd characteristic and in simply carrying out much more work on APN functions. (Also using some significant computing power might be an idea!)
- Understand the behavior of P-Res better, especially the computational results on P-Res(x^2), which suggests we should be able to prove much better bounds in such cases.
- Linear resemblance seems an obvious direction. Li-An and I have done some work in this direction.

Open problems

The most pressing ones might be:

- Expand the computational results for P-Res, especially with regard to finding new low-DU permutations in odd characteristic and in simply carrying out much more work on APN functions. (Also using some significant computing power might be an idea!)
- Understand the behavior of P-Res better, especially the computational results on P-Res(x^2), which suggests we should be able to prove much better bounds in such cases.
- Linear resemblance seems an obvious direction. Li-An and I have done some work in this direction.
- Apply resemblance in other settings.

Open problems

The most pressing ones might be:

- Expand the computational results for P-Res, especially with regard to finding new low-DU permutations in odd characteristic and in simply carrying out much more work on APN functions. (Also using some significant computing power might be an idea!)
- Understand the behavior of P-Res better, especially the computational results on P-Res(x^2), which suggests we should be able to prove much better bounds in such cases.
- Linear resemblance seems an obvious direction. Li-An and I have done some work in this direction.
- Apply resemblance in other settings.

Conjecture

There exists a 2-DU permutation over all sufficiently large finite fields.

Many thanks for your time.