Classifying toric surface codes of dimension 7

Emily Cairncross[1], Stephanie Ford[2], & Eli Garcia[3]

Mentor: Kelly Jabbusch

University of Michigan - Dearborn REU 2019

[1]Oberlin College [2]Texas A&M University [3]MIT

February 1, 2020

Overview

Creating a code

- **k-dimensional linear code:** k-dimensional subspace of $\mathbb{F}_q^n$ (where $\mathbb{F}_q$ is a finite field of order q)

Creating a code

- **k-dimensional linear code:** k-dimensional subspace of $\mathbb{F}_q^n$ (where $\mathbb{F}_q$ is a finite field of order q)

- **Toric surface code:** a linear code given by a generator matrix constructed from a lattice polygon P in $\mathbb{R}^2$

Creating a code

- **k-dimensional linear code:** k-dimensional subspace of $\mathbb{F}_q^n$ (where $\mathbb{F}_q$ is a finite field of order q)

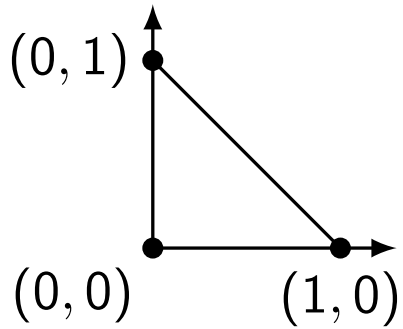
- **Toric surface code:** a linear code given by a generator matrix constructed from a lattice polygon P in $\mathbb{R}^2$

Simple example

We construct a toric surface code using the following parameters:

- Finite field: $\mathbb{F}_5$
- Lattice polygon in $\mathbb{R}^2$: unit triangle

Example cont.

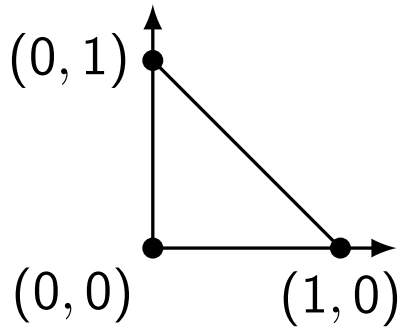


Generator matrix (G):

Lattice points $(\vec{e_i})$ Elements of $(\mathbb{F}_5^*)^2$ $(\vec{a_j})$

$$\begin{matrix}(0,0)\\(1,0)\\(0,1)\end{matrix}\begin{bmatrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\1&1&1&1&2&2&2&2&3&3&3&3&4&4&4&4\\1&2&3&4&1&2&3&4&1&2&3&4&1&2&3&4\end{bmatrix}$$

Example cont.



Generator matrix (G):

Lattice points $(\vec{e_i})$ Elements of $(\mathbb{F}_5^*)^2$ $(\vec{a_j})$

$$\begin{matrix}(0,0)\\(1,0)\\(0,1)\end{matrix}\begin{bmatrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\1&1&1&1&2&2&2&2&3&3&3&3&4&4&4&4\\1&2&3&4&1&2&3&4&1&2&3&4&1&2&3&4\end{bmatrix}$$

For $\vec{e_i} = (e_1, e_2)$ and $\vec{a_j} = (a_1, a_2)$:

$$G_{ij} = (\vec{a_j})^{\vec{e_i}} = a_1^{e_1} a_2^{e_2}$$

Example cont.

Generator matrix (generated by unit triangle and $\mathbb{F}_5$):

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 \\ 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \end{bmatrix}$$

Codewords:

Linear combinations of rows of G:

$$Code = \{\vec{u}G : \vec{u}\epsilon(\mathbb{F}_5)^3\}$$

Example cont.

Generator matrix (generated by unit triangle and $\mathbb{F}_5$):

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 \\ 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \end{bmatrix}$$

Codewords:

Linear combinations of rows of G:

$$Code = \{\vec{u}G : \vec{u}\epsilon(\mathbb{F}_5)^3\}$$

Examples:

$$(1,1,0) \cdot G = (2,2,2,2,3,3,3,3,4,4,4,4,0,0,0,0)$$

$$(0,1,2) \cdot G = (3,0,2,4,4,1,3,0,0,2,4,1,1,3,0,2)$$

Analyzing a code

- **Hamming distance:** number of indices at which two codewords are different
  - Hamming distance between example codewords: 12

Analyzing a code

- **Hamming distance:** number of indices at which two codewords are different
  - Hamming distance between example codewords: 12
- **Three important invariants:**
  - length of codewords $n = (q-1)^2$
    - $n = (5-1)^2 = 16$

Analyzing a code

- **Hamming distance:** number of indices at which two codewords are different
  - Hamming distance between example codewords: 12
- **Three important invariants:**
  - length of codewords $n = (q-1)^2$
    - $n = (5-1)^2 = 16$
  - dimension of code $k = \#(P)$, the number of lattice points in P
    - $k = \#(P) = 3$

Analyzing a code

- **Hamming distance:** number of indices at which two codewords are different
  - Hamming distance between example codewords: 12
- **Three important invariants:**
  - length of codewords $n = (q-1)^2$
    - $n = (5-1)^2 = 16$
  - dimension of code $k = \#(P)$, the number of lattice points in P
    - $k = \#(P) = 3$
  - minimum distance d varies (minimum Hamming distance between any two codewords)
    - $d = (q-1)(q-2) = (5-1)(5-2) = 12$

Motivation

- Previous work done by Little and Schwartz, Soprunov and Soprunova, and Yau et. al
  - Classification of toric surface codes up to dimension $k = 6$
- We continue this classification for dimension $k = 7$

Monomial Equivalence

Definition

Let G_1 and G_2 be the generator matrices for linear codes C_1 and C_2 with dimension k and length n. We call C_1 and C_2 monomially equivalent if there exists an invertible $n \times n$ diagonal matrix Δ and an $n \times n$ permutation matrix Π such that

$$G_1 = G_2 \Delta \Pi.$$

Lattice equivalence

Definition

Let P_1 and P_2 be lattice convex polytopes in $\mathbb{R}^m$. We call P_1 and P_2 *lattice equivalent* if there exists a unimodular affine transformation

$$T : \mathbb{R}^m \to \mathbb{R}^m$$

defined by

$$T(\vec{x}) = M\vec{x} + \lambda$$

where $M \in \mathrm{SL}(m, \mathbb{Z})$ and $\lambda \in \mathbb{Z}^m$ such that

$$T(P_1) = P_2.$$

Lattice equivalence

Definition

Let P_1 and P_2 be lattice convex polytopes in $\mathbb{R}^m$. We call P_1 and P_2 *lattice equivalent* if there exists a unimodular affine transformation

$$T : \mathbb{R}^m \to \mathbb{R}^m$$

defined by

$$T(\vec{x}) = M\vec{x} + \lambda$$

where $M \in \mathrm{SL}(m, \mathbb{Z})$ and $\lambda \in \mathbb{Z}^m$ such that

$$T(P_1) = P_2.$$

- Valid transformations: shear, translation, rotation by a multiple of 90°
  - Scaling is *not* an affine transformation

Lattice equivalence

Definition

Let P_1 and P_2 be lattice convex polytopes in $\mathbb{R}^m$. We call P_1 and P_2 *lattice equivalent* if there exists a unimodular affine transformation

$$T : \mathbb{R}^m \to \mathbb{R}^m$$

defined by

$$T(\vec{x}) = M\vec{x} + \lambda$$

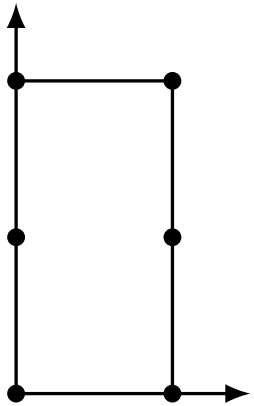
where $M \in \mathrm{SL}(m, \mathbb{Z})$ and $\lambda \in \mathbb{Z}^m$ such that

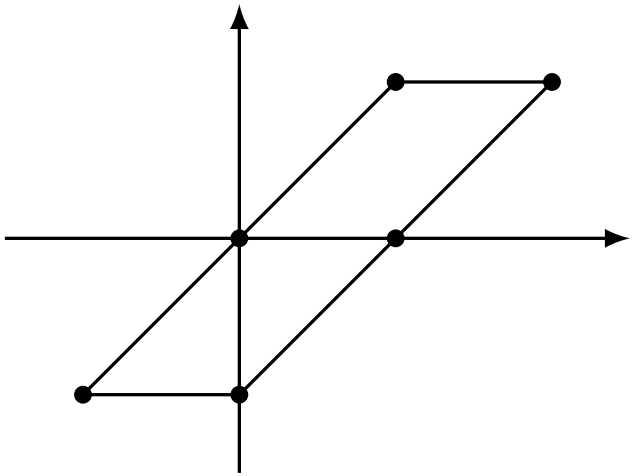
$$T(P_1) = P_2.$$

- Valid transformations: shear, translation, rotation by a multiple of 90°
  - Scaling is *not* an affine transformation
- Lattice equivalence $\Rightarrow$ monomial equivalence

Lattice equivalence

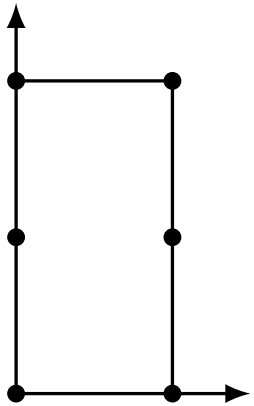
Lattice equivalent:

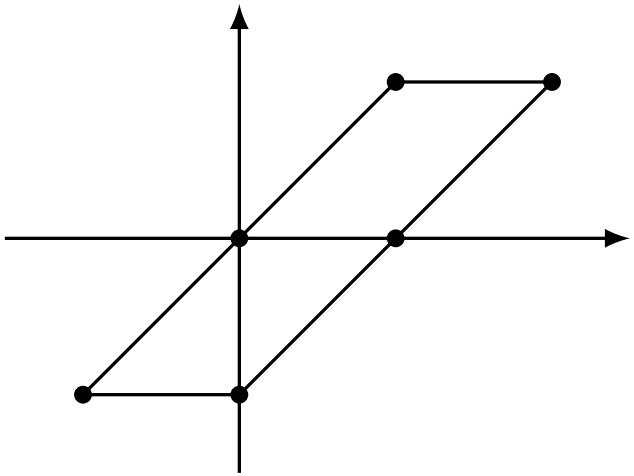




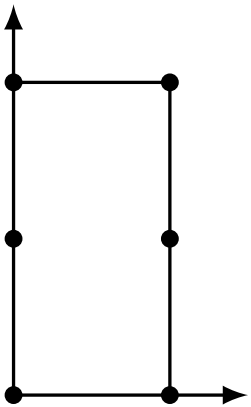
Lattice equivalence

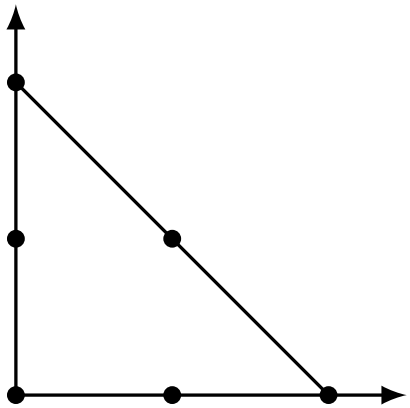
Lattice equivalent:





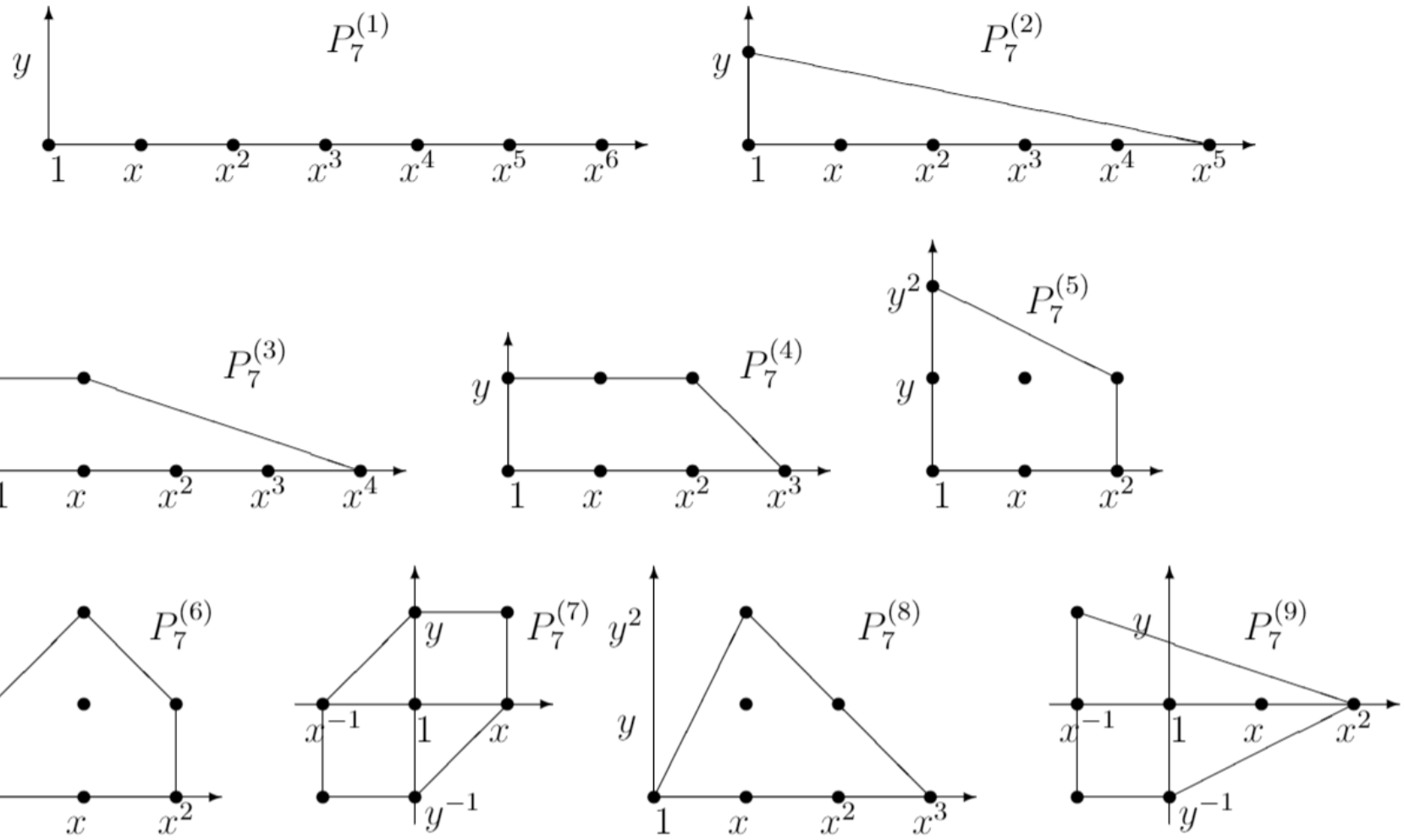
Lattice inequivalent:



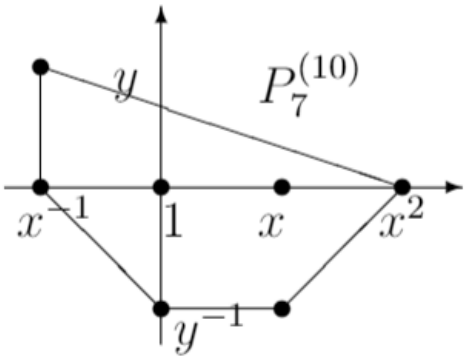


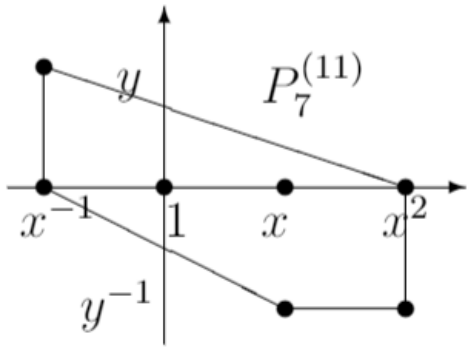
Lattice equivalence classes for $k = 7$

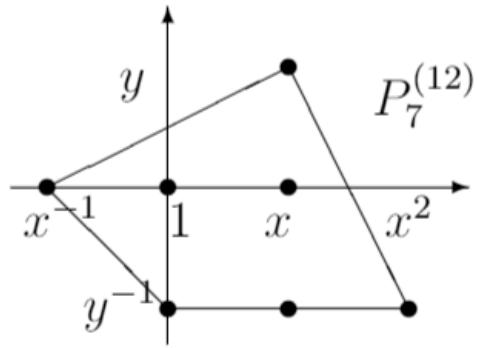
For $P_k^{(i)}$, k refers to the number of lattice points while i is the number assigned to the equivalence class.

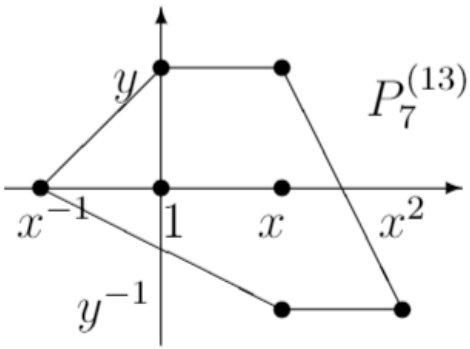


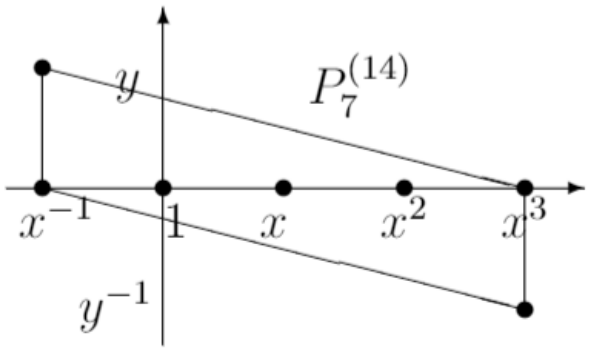
Lattice equivalence classes for $k = 7$

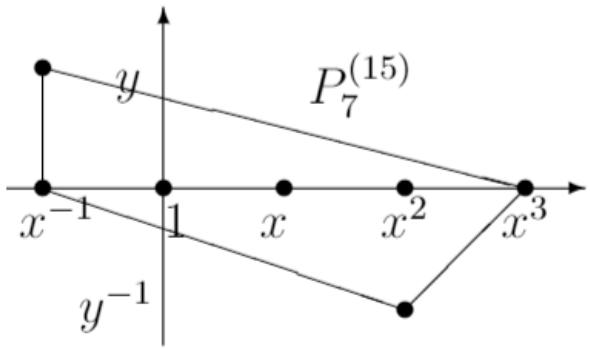




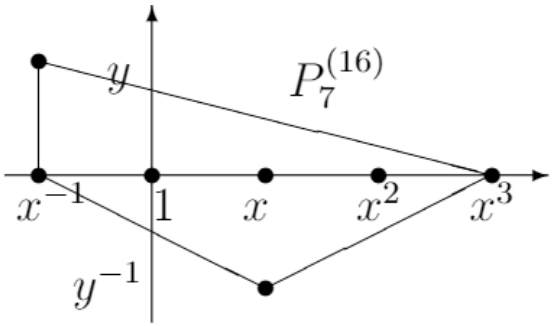


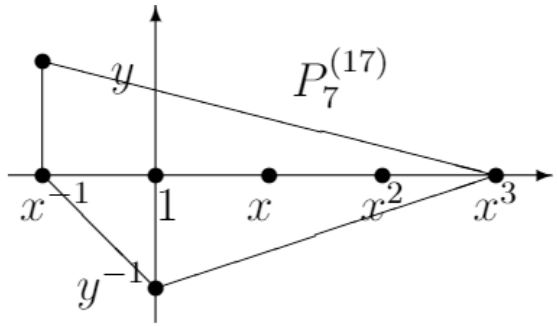


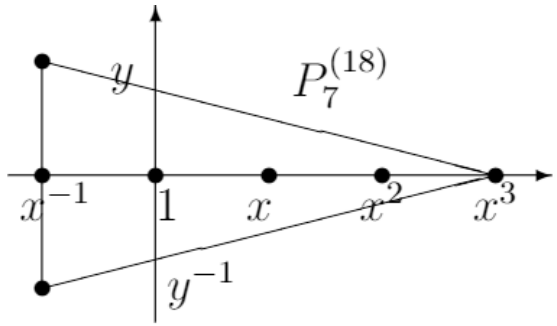


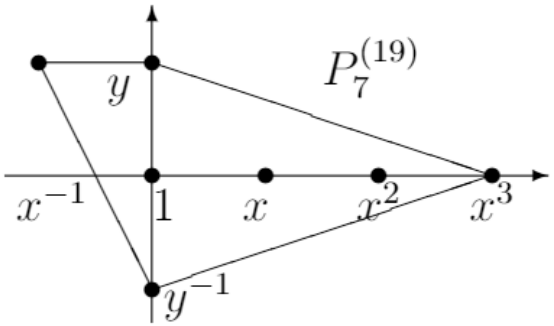


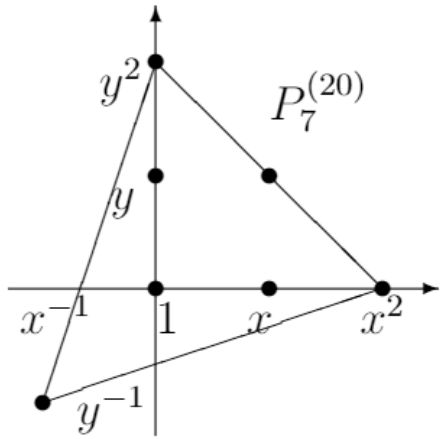
Lattice equivalence classes for $k = 7$

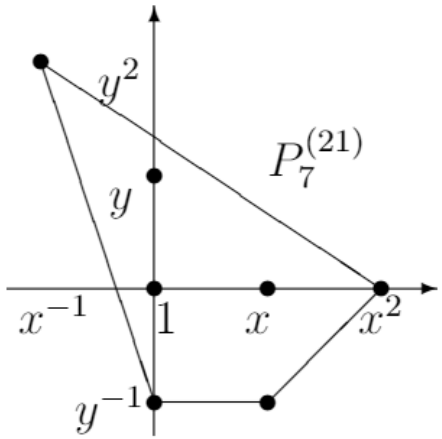


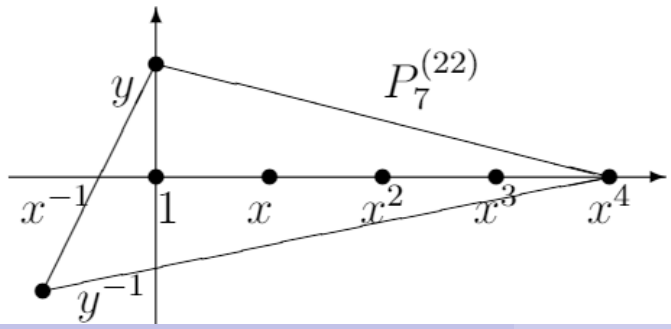












Classification of $k = 7$ polygons

Theorem: C.F.G. 2019

Every toric surface code generated by a polygon with $k = 7$ lattice points is monomially equivalent to a code given by one of the polygons in the preceding slides.

Classification of $k = 7$ polygons

Theorem: C.F.G. 2019

Every toric surface code generated by a polygon with $k = 7$ lattice points is monomially equivalent to a code given by one of the polygons in the preceding slides.

Sketch of the proof

Classification of $k = 7$ polygons

Theorem: C.F.G. 2019

Every toric surface code generated by a polygon with $k = 7$ lattice points is monomially equivalent to a code given by one of the polygons in the preceding slides.

Sketch of the proof

- **Goal:** prove that we have all polygons with 7 lattice points
- Each P_7 polygon has at least one P_6 polygon as a subset

Classification of $k = 7$ polygons

Theorem: C.F.G. 2019

Every toric surface code generated by a polygon with $k = 7$ lattice points is monomially equivalent to a code given by one of the polygons in the preceding slides.

Sketch of the proof

- **Goal:** prove that we have all polygons with 7 lattice points
- Each P_7 polygon has at least one P_6 polygon as a subset
- Take each P_6 and find all possible P_7 by adding lattice points

Illustration of the proof

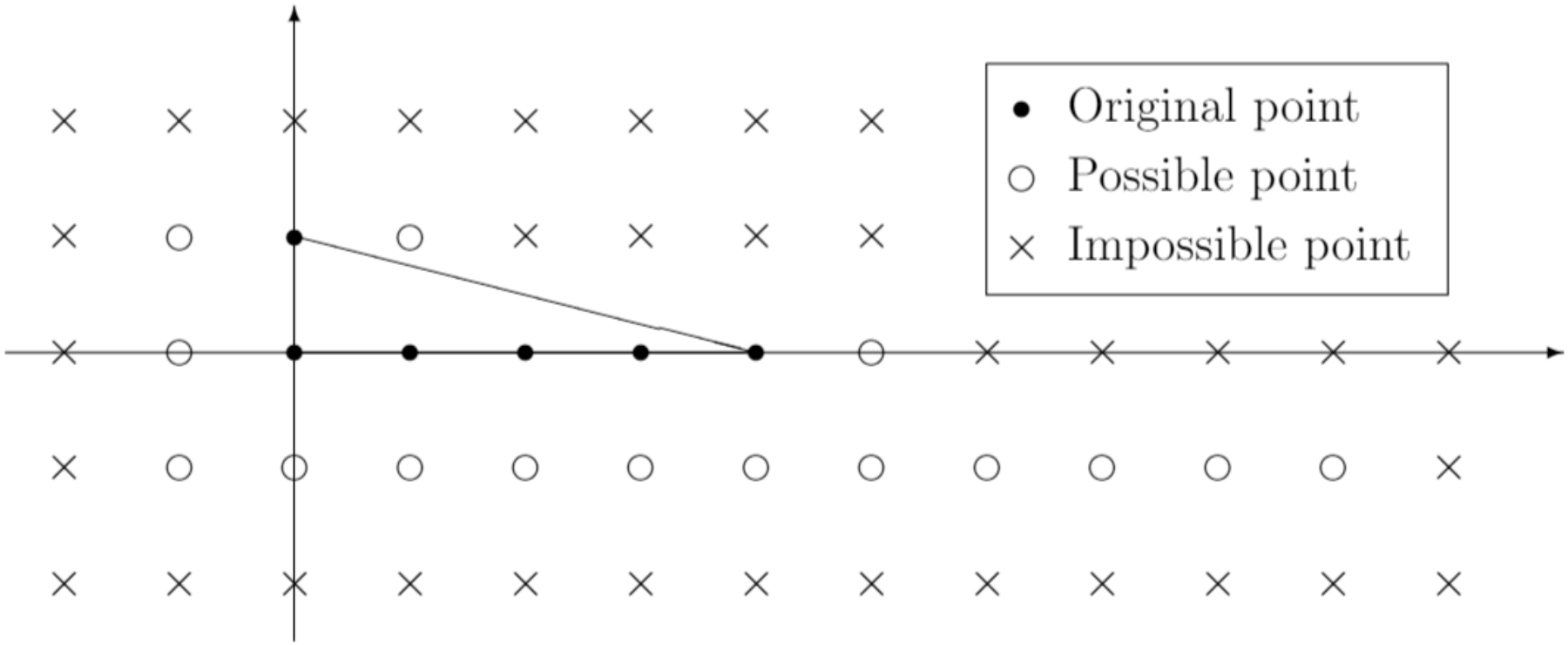


Figure: Illustration for $P_6^{(2)}$.

Classification of $k = 7$ codes

Theorem: C.F.G. 2019

The toric surface codes $C_{P_7^{(i)}}, 1 \leq i \leq 22$, are pairwise monomially inequivalent over $\mathbb{F}_q$ for sufficiently large q.

Classification of $k = 7$ codes

Theorem: C.F.G. 2019

The toric surface codes $C_{P_7^{(i)}}, 1 \leq i \leq 22$, are pairwise monomially inequivalent over $\mathbb{F}_q$ for sufficiently large q.

Sketch of the proof

Classification of $k = 7$ codes

Theorem: C.F.G. 2019

The toric surface codes $C_{P_7^{(i)}}, 1 \leq i \leq 22$, are pairwise monomially inequivalent over $\mathbb{F}_q$ for sufficiently large q.

Sketch of the proof

- **Goal:** prove that no pair of the 22 codes are monomially equivalent

Classification of $k = 7$ codes

Theorem: C.F.G. 2019

The toric surface codes $C_{P_7^{(i)}}, 1 \leq i \leq 22$, are pairwise monomially inequivalent over $\mathbb{F}_q$ for sufficiently large q.

Sketch of the proof

- **Goal:** prove that no pair of the 22 codes are monomially equivalent
- We know that codes with different minimum distances are inequivalent

Classification of $k = 7$ codes

Theorem: C.F.G. 2019

The toric surface codes $C_{P_7^{(i)}}, 1 \leq i \leq 22$, are pairwise monomially inequivalent over $\mathbb{F}_q$ for sufficiently large q.

Sketch of the proof

- **Goal:** prove that no pair of the 22 codes are monomially equivalent
- We know that codes with different minimum distances are inequivalent
- To further distinguish codes, we need finer invariants
- We consider the number of codewords of particular weights (distance from $\vec{0} \in \mathbb{F}_q^n$)

Minimum distances

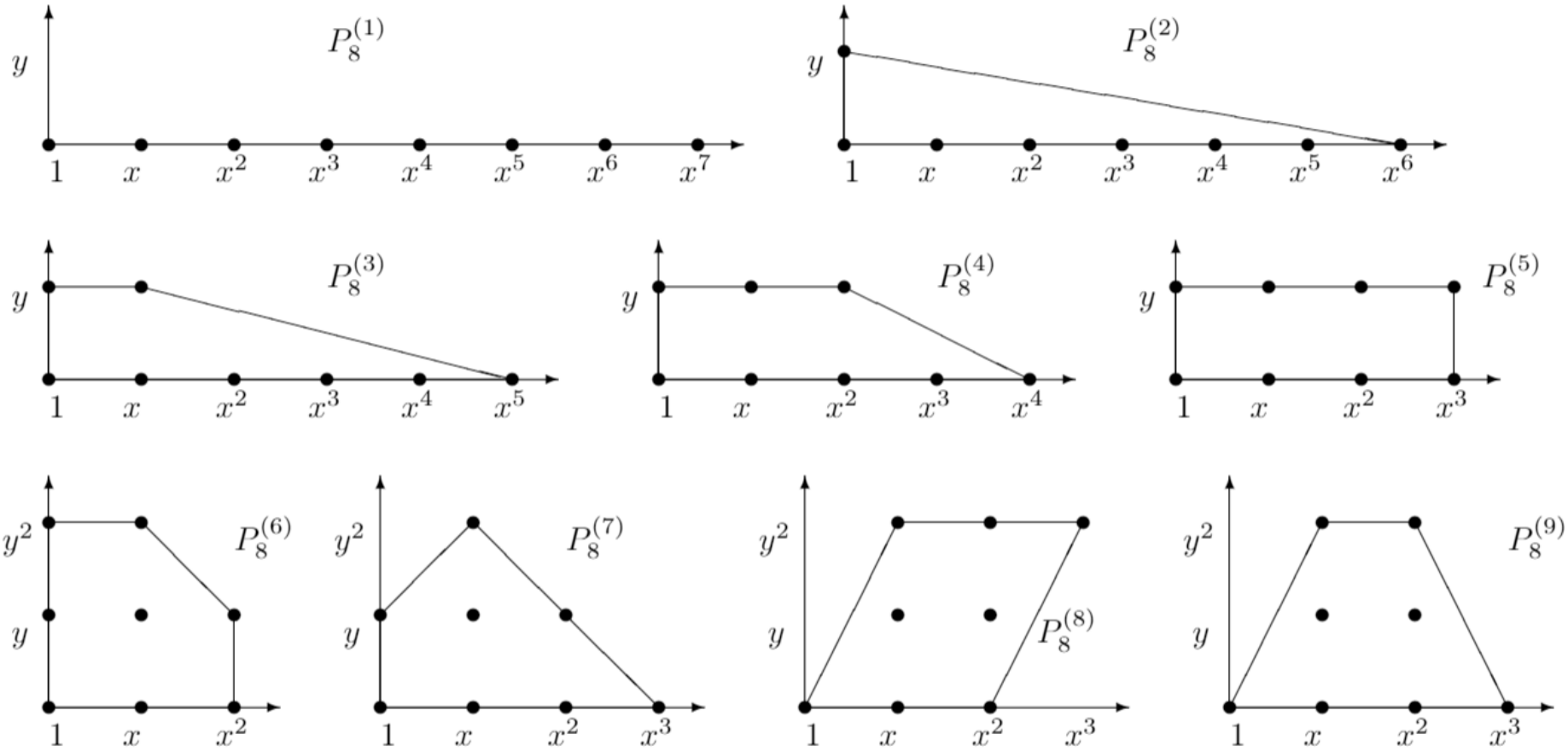
Lattice Equivalence Class	Minimum Distance Formula
$P_7^{(1)}$	$(q-1)(q-7)$
$P_7^{(2)}$	$(q-1)(q-6)$
$P_7^{(3,14-18,22)}$	$(q-1)(q-5)$
$P_7^{(4,8-11,19)}$	$(q-1)(q-4)$
$P_7^{(5-7,12)}$	$(q-2)(q-3)$
$P_7^{(13)}$	$(q-1)(q-3) \geq d > (q-2)(q-3)$
$P_7^{(20-21)}$	$(q-1)(q-3)$

Classification of $k = 8$ polygons

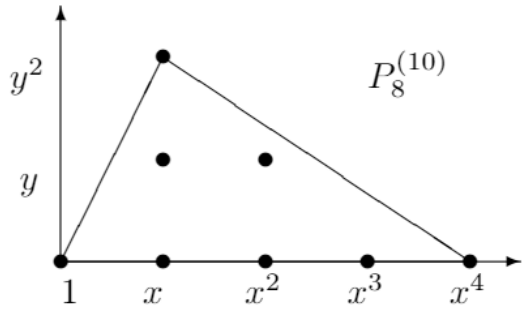
Theorem: C.F.G. 2019

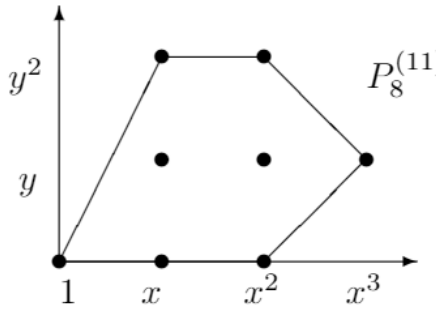
Every toric surface code generated by a polygon with $k = 8$ lattice points is monomially equivalent to a code given by one of the 42 polygons in the following slides.

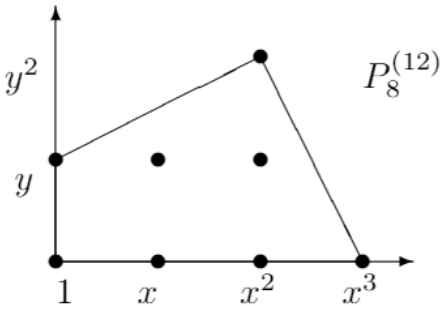
Lattice equivalence classes for $k = 8$

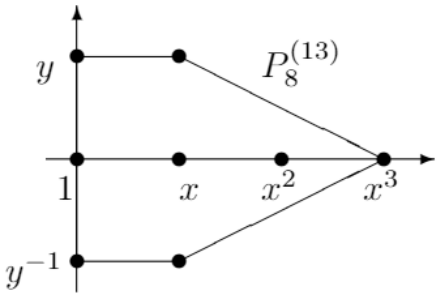


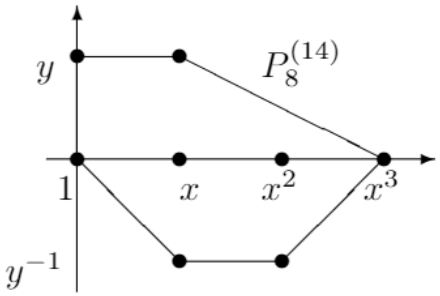
Lattice equivalence classes for $k = 8$

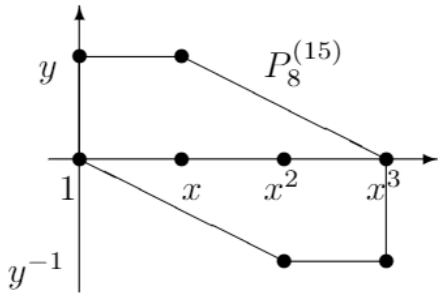


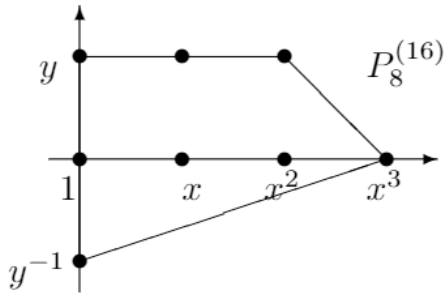


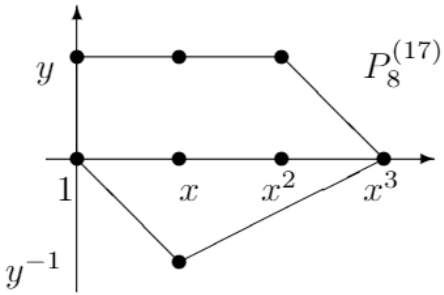


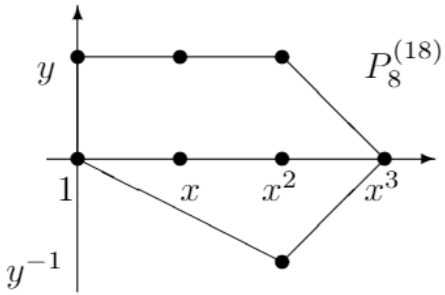


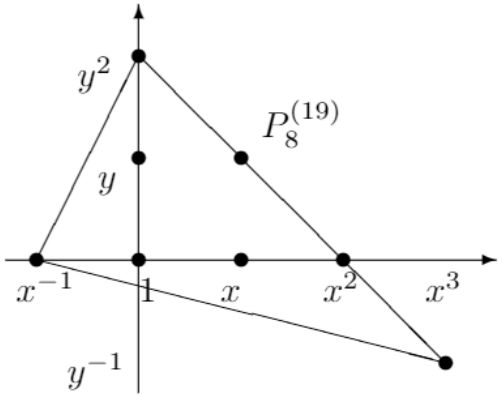




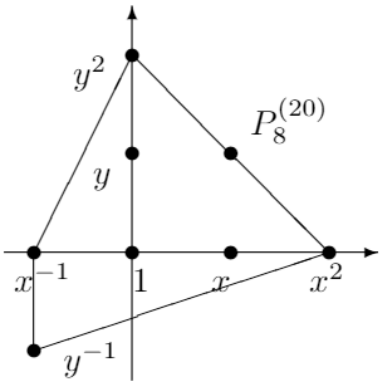


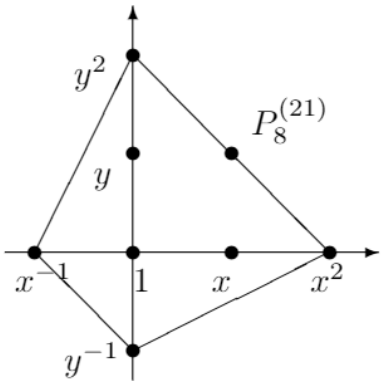


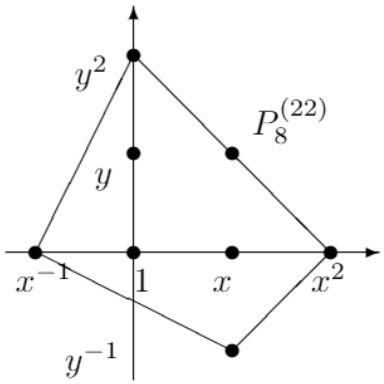


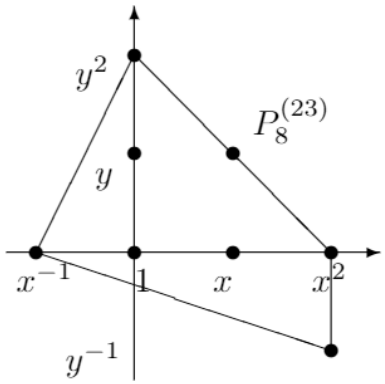


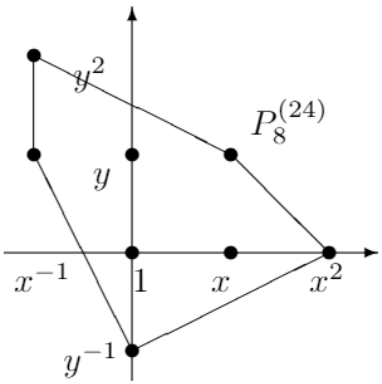
Lattice equivalence classes for $k = 8$

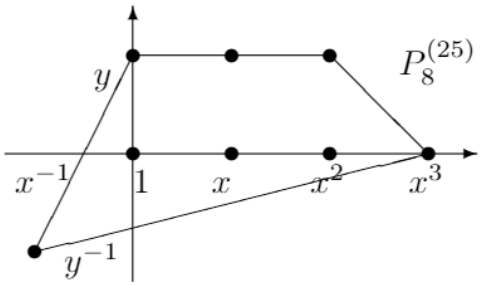


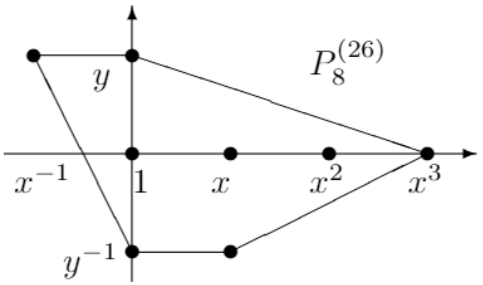


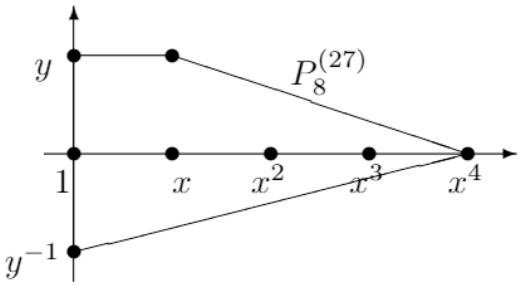


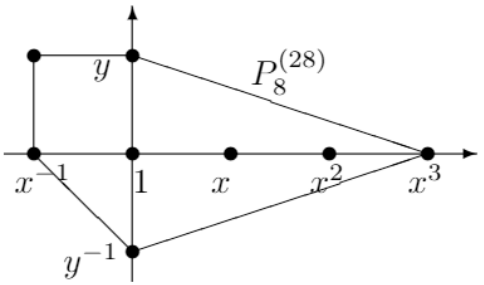


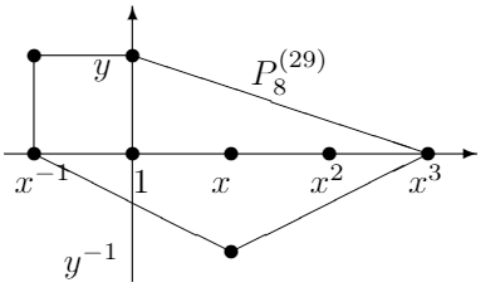




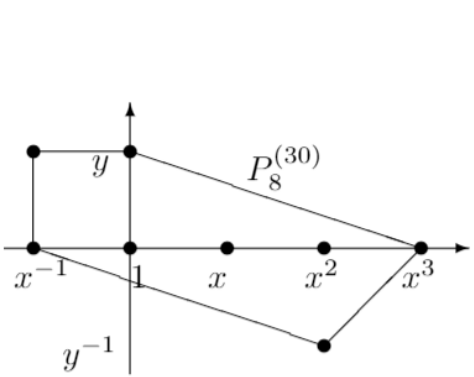


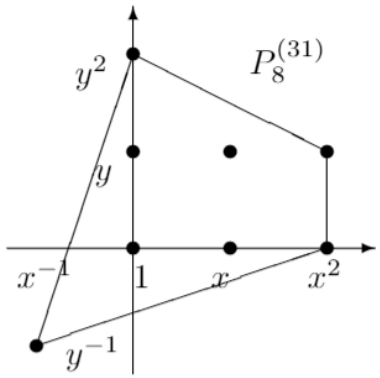


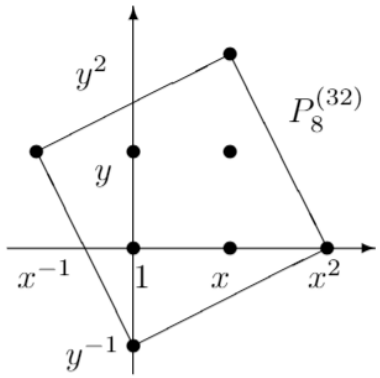


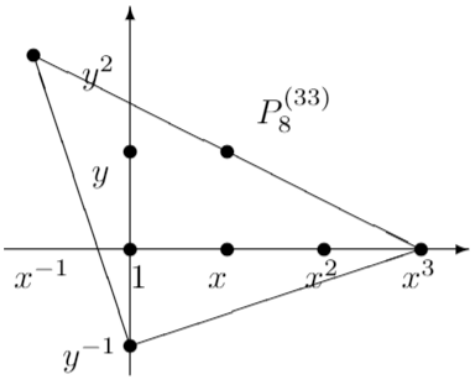


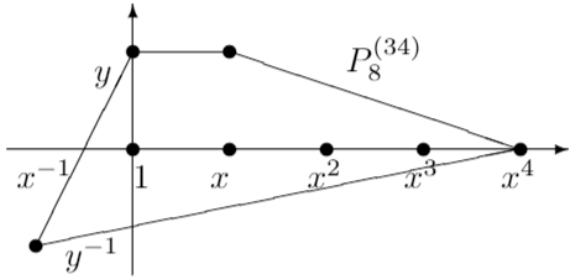
Lattice equivalence classes for $k = 8$

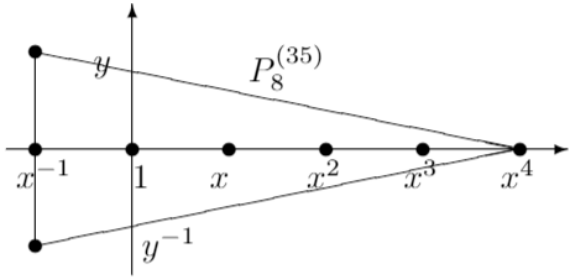


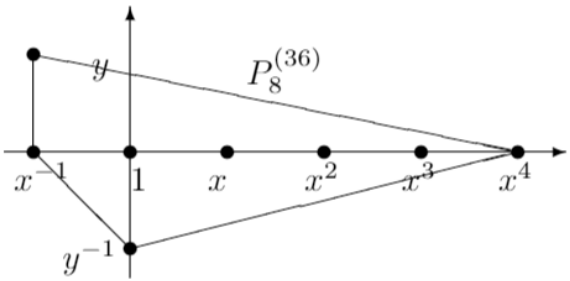


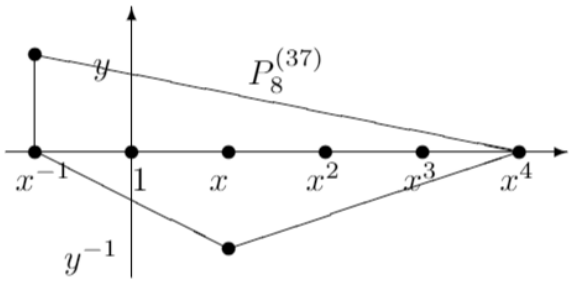


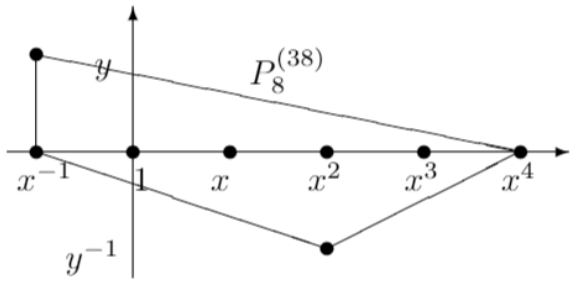




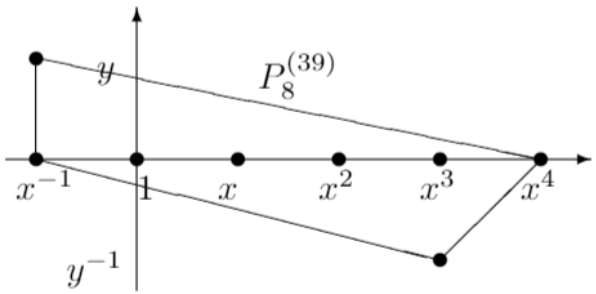


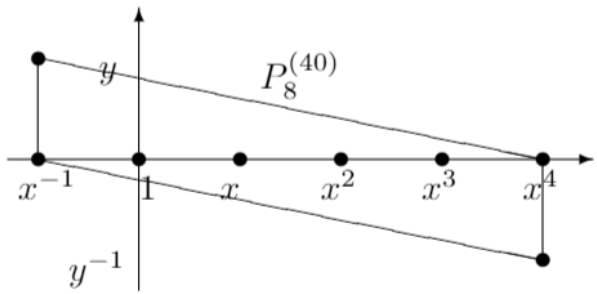


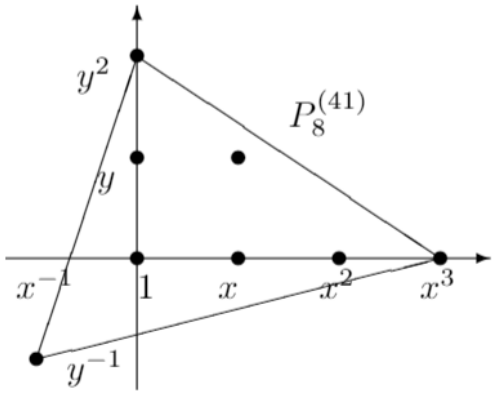


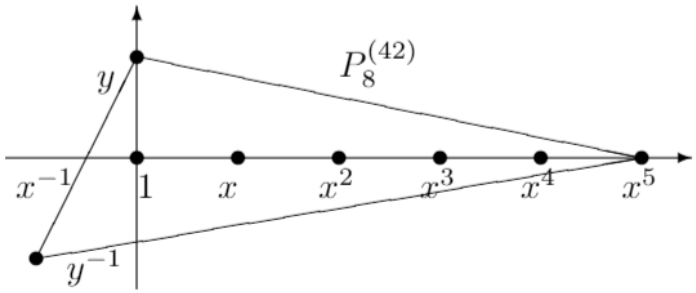


Lattice equivalence classes for $k = 8$









Acknowledgements

This research was conducted at the NSF REU Site (DMS-1659203) in Mathematical Analysis and Applications at the University of Michigan-Dearborn. We would like to thank the National Science Foundation, National Security Agency, University of Michigan-Dearborn (SURE 2019), and the University of Michigan-Ann Arbor for their support.