On a Class of Permutation Polynomials

Christian A. Rodríguez & Alex D. Santos
University of Puerto Rico, Rio Piedras
Department of Computer Science

Abstract

A polynomial $f(x)$ defined over a set A is called a **permutation polynomial** if $f(x)$ acts as a permutation over the elements of A. This is, if $f : A \to A$ is 1-1 and onto. We are studying the coefficients a and b that make polynomials of the form $F_{a,b}(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$ a permutation polynomial where $a, b \in \mathbb{F}_q^{\times}$. More specifically we study the family of polynomials: $F_{a,b}(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$. Our approach in studying $F(x)$ is to use the division algorithm to consider $x = \alpha^n$ where $n = 6k + r, r = 0, ..., 5$. If $F_{a,b}(x)$ is a permutation, this partitions $\mathbb{F}_q^{\times}$ into 6 classes: $F_{a,b}(\alpha^{6k+r})$ for $r = 0, ..., 5$.

Preliminaries

Definition 1. *A polynomial $f(x)$ defined over a set A is called a **permutation polynomial** if $f(x)$ acts as a permutation over the elements of A. This is, if $f : A \to A$ is 1-1 and onto.*

We study permutation polynomials defined over finite fields $\mathbb{F}_q$. This is, polynomials that permute the elements of $\mathbb{F}_q$

Definition 2. *A **finite field** $\mathbb{F}_q$, $q = p^r$, p prime is a field with q elements.*

Definition 3. *A polynomial $f(x)$ defined over a set A is called a **permutation polynomial** if $f(x)$ acts as a permutation over the elements of A. This is, if $f : A \to A$ is 1-1 and onto.*

We study permutation polynomials defined over finite fields $\mathbb{F}_q$. This is, polynomials that permute the elements of $\mathbb{F}_q$

Definition 4. *A **finite field** $\mathbb{F}_q$, $q = p^r$, p prime is a field with q elements.*

Definition 5. *A polynomial $f(x)$ defined over a set A is called a **permutation polynomial** if $f(x)$ acts as a permutation over the elements of A. This is, if $f : A \to A$ is 1-1 and onto.*

We study permutation polynomials defined over finite fields $\mathbb{F}_q$. This is, polynomials that permute the elements of $\mathbb{F}_q$

Definition 6. *A **finite field** $\mathbb{F}_q$, $q = p^r$, p prime is a field with q elements.*

Value set of a class of polynomials

We formulated tracking as path search in a large graph, and solve it efficiently with a modificiation of Dijkstra's algorithm.

The preliminaries is based on [**?**]. Our main contributions are

1. Efficient incorporation of a background appearance model
2. Formulation as a shortest path abstract
3. (Correct) handling of occlusions
4. High-Efficiency implementation with up to 150 fps for a high resolution video

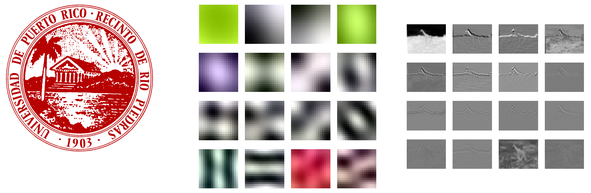

Image Filter Bank Response

Speed is achieved by preprocessing the video with an adaptive filter bank as in [**?**]. Preprocessing was sped up significantly, but is still slower than realtime.

This encodes the video into 16 byte per pixel feature vectors. We implemented an efficient search for similar patches using the SIMD hardware of modern processors, and only evaluate the cost on these candidate patches. (Typically 200 patches per frame). Candidate search and reasoning are highly efficient resulting in an interactive system.

Note that the preprocessing is not specific to the interestpoints tracked later. A single preprocessed video can therefore be used in many annotation sessions.

Conditions for permutations of the from $F_{a,b}(x)$

We incorporated a background model, where a click informs us not only that 'this is how the patch looks like', but also for the rest of the frame, 'this is how the patch does not look like'.

Can we also *efficiently* use a background tracks model, allowing us to reason, 'this would be a good track, but part of it can be better explained by tracking another point'.

Applications

Frame 0 24 48 72 95

Frame 0 100 200 300 458

Between one and three user clicks were needed to achieve accurate tracking for the head sequence. Note the correct handling of the occluded ear, which required only a single click.

The eye of the running giraffe required eight user interactions, of which three marked occlusions.

Future Work

With background model | Without background model

Ridge of the lips

References

The source code and compiled executables with an interactive interface are available at
`http://www.cs.unibas.ch/personen/amberg_brian/graphtrack`