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

We are interested in studying sets known as Finite Fields.

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

An important property of finite fields is the existence of a primitive root, a generator of the nonzero elements of $\mathbb{F}_q$.

Definition 3. *A **primitive root** $\alpha \in \mathbb{F}_q$ is a generator for the multiplicative group $\mathbb{F}_q^\times$*

Example 1. *Consider the finite field $\mathbb{F}_7$. We have that: $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$, so 3 is a primitive root of $\mathbb{F}_7$.*

We are interested in studying polynomials defined over finite fields. Specifically, our interest lies in the value set of these polynomials.

Definition 4. *Let $f(x)$ be a polynomial defined over a finite field $\mathbb{F}_q$. Then the **value set** of f is defined as $V_f = \{f(a) \mid a \in \mathbb{F}_q\}$*

In our work we characterize V_f for a specific class of polynomials defined over finite fields. From this characterization we can provide information on the amount of permutation polynomials of our class.

Definition 5. *Consider a finite field $\mathbb{F}_q$. A polynomial $f(x)$ defined over $\mathbb{F}_q$ is said to be a permutation polynomial if $V_f = \mathbb{F}_q$.*

Example 2. *Consider the polynomial $f(x) = x + 3$ defined over $\mathbb{F}_7$. We have that $f(0) = 3, f(1) = 4, f(2) = 5, f(3) = 6, f(4) = 0, f(5) = 1, f(6) = 2$, so $f(x)$ is a permutation polynomial over $\mathbb{F}_7$*

VALUE SET OF A CLASS OF POLYNOMIALS

Our interest is studying the value set of a specific class of permutation polynomials. The class of polynomials we consider is defined as follows:

$$F_{a,b}(x) = x^{\frac{q+1}{2}} + a \cdot x^{\frac{q+1}{d}} + b \cdot x$$

Where $a, b \in \mathbb{F}_q$ and $d \mid q - 1$. More formally, we would like to characterize the value set V_F of $F_{a,b}(x)$ based on the parameters a and b. It is easy to see that $F_{a,b}(0) = 0 \ \forall a, b \in \mathbb{F}_q$, it follows that 0 is always in V_F. For a fixed pair a, b we separate $V_F \setminus \{0\}$ into smaller subsets in the following way:

Definition 1. *Let $F_{a,b}(x) = x^{\frac{q+1}{2}} + a \cdot x^{\frac{q+1}{d}} + b \cdot x$ be a polynomial defined over $\mathbb{F}_q$ where $d \mid q - 1$. We define the sets $A_i = \{F_{a,b}(\alpha^{d \cdot k + i}) \mid k = 0, ..., \frac{q-1}{d}\}$ for $i = 0, ..., d - 1$, where α is a primitive root of $\mathbb{F}_q$.*

Using properties of these sets we will characterize V_F. First we would like to note that for $i \neq j$ the sets A_i and A_j are either equal, or distinct.

Lemma 1. *Let $F_{a,b}(x)$ be defined over $\mathbb{F}_q$. For two sets A_i and A_j we must have that either $A_i \cap A_j = \emptyset$ or $A_i = A_j$.*

Lemma 1 provides an immediate characterization of the value set and insight on conditions to make $F_{a,b}(x)$ a permutation polynomial. In our studies we also determine the size of the sets A_i.

Lemma 2. *Let $F_{a,b}(x)$ be defined over $\mathbb{F}_q$ and A_i be defined as above. We have that $|A_i| = \frac{q-1}{d}$ or $A_i = \{0\}$*

Now we are also interested in correlations between the pairs a, b and the value sets of distinct polynomials of the for $F_{a,b}(x)$. We proved a lemma that gives us a correspondence among some of these polynomials. In other words, these polynomials have the same value set.

Lemma 3. *Let $F_{a,b}(x)$ defined over $\mathbb{F}_q$ and let α denote a primitive root of $\mathbb{F}_q$. If we write $a = \alpha^i$ and $b = \alpha^j$ then we have that*

$$F_{\alpha^i,\alpha^j}(\alpha^k) = -\alpha \cdot F_{\alpha^{i+(d+2)\cdot\frac{q-1}{2d}},\,\alpha^{j+\frac{q-1}{2}}}(\alpha^{k-1})$$

From lemma 1 we know that for a fixed polynomial the sets A_i are either distinct or equal. Finally from lemma 3 we have that up to $2d$ distinct polynomials of the form $F_{a,b}(x)$ have the same value set. This information gives us the following theorem:

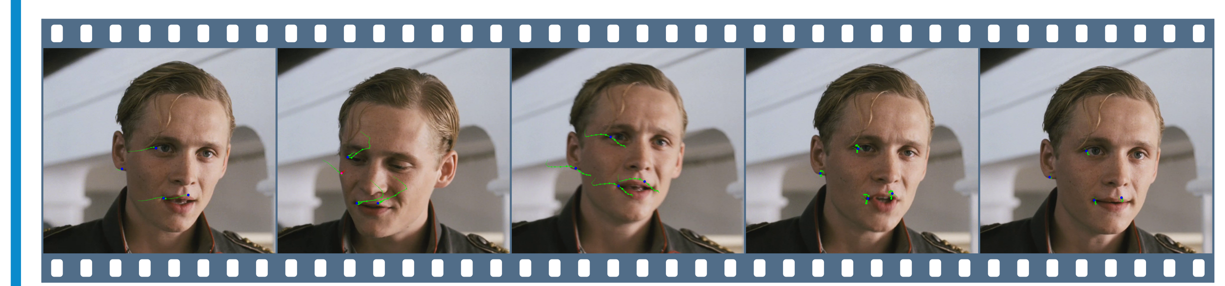
Proposition 1. *Let $F_{a,b}(x)$ be defined over $\mathbb{F}_q$. Then we have that the amount of polynomials of the form $F_{a,b}(x)$ such that $|V_F| = r \cdot \frac{q-1}{d} + 1, r \leq d$ is divisible by d when d is even and by $2d$ when dis odd.*

CONDITIONS FOR PERMUTATIONS OF THE FROM $F_{a,b}(x)$

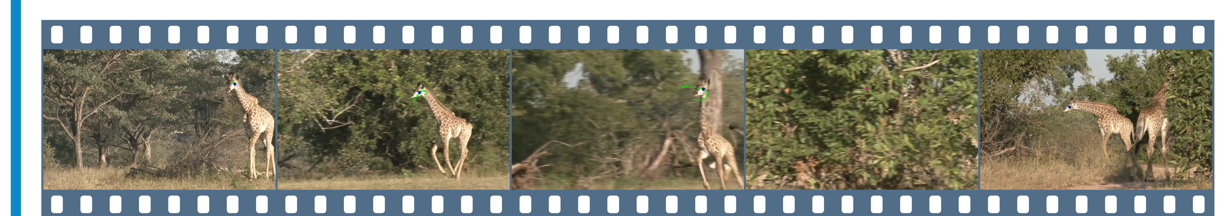
We incorporated a background model, where a click informs us not only that 'this is how the patch looks like', but also for the rest of the frame, 'this is how the patch does not look like'.

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

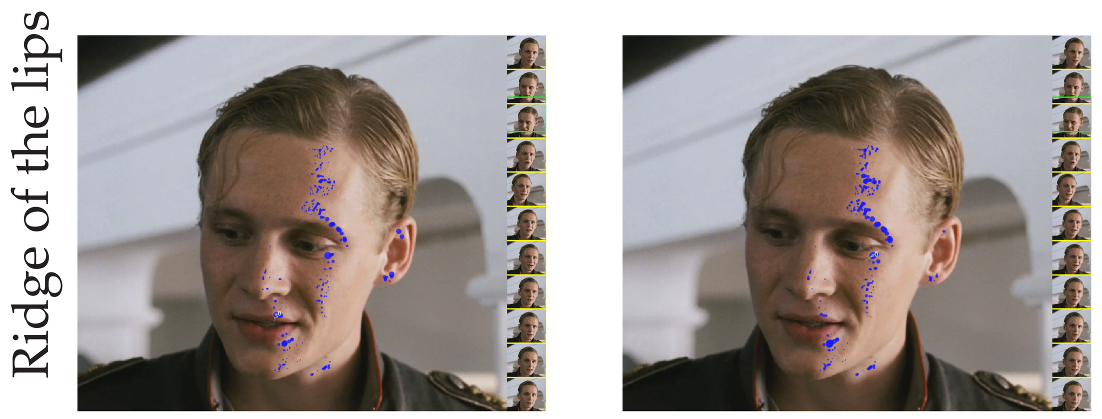
Between one and three user clicks were needed to achieve accurate tracking for the head sequence. Note the correct handling of the occluded ear, which required only a single click.

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`