A representation of the p-sylow subgroup of $\mathrm{Perm}(\mathbb{F}_p^n)$ and a cryptographic application

Stefan Maubach
Jacobs University Bremen
Bremen, Germany
s.maubach@jacobs-university.de

July 14, 2011

Abstract

This article concerns itself with the triangular permutation group, induced by triangular polynomial maps over $\mathbb{F}_p$, which is a p-sylow subgroup of $\mathrm{Perm}(\mathbb{F}_p^n)$. The aim of this article is twofold: on the one hand, we give an alternative to $\mathbb{F}_p$-actions on $\mathbb{F}_p^n$, namely $\mathbb{Z}$-actions on $\mathbb{F}_p^n$ and how to describe them as what we call "$\mathbb{Z}$-flows". On the other hand, we describe how the triangular permutation group can be used in applications, in particular we give a cryptographic application for session-key generation. The described system has a certain degree of information theoretic security. We compute its efficiency and storage size.

To make this work, we give explicit criteria for a triangular permutation map to have only one orbit, which we call "maximal orbit maps". We describe the conjugacy classes of maximal orbit maps, and show how one can conjugate them even further to the map $z \longrightarrow z+1$ on $\mathbb{Z}/p^n\mathbb{Z}$.

AMS classification: 14R20, 20B25, 94A60

1 Introduction

When generalizing the concept of algebraic additive group actions on k^n where k is of characteristic zero, to fields of characteristic p, one tends to (obviously) go to $(k,+)$ actions on k^n. These then automatically have order p. This makes the generalization, though seemingly natural in some way, restrictive. For example, a common class of additive group actions is those induced by strictly triangular polynomial maps: maps of the form $(X_1+g_1,\ldots,X_n+g_n)$ where $g_i \in k[X_1,\ldots,X_{i-1}]$. In characteristic zero all these maps can be embedded into a unique algebraic additive group action $\varphi : (k,+)\times k^n \longrightarrow k^n$ such that $\varphi(1,X_1,\ldots,X_n)$ is exactly this map: analytically speaking, they are the "time one-maps of a $(k,+)$ flow on k^n". However, in characteristic p they do not always have order p, so they cannot be part of a $(k+)$-action.

To give an example, if $F = (x + y + z, y + z, z)$ in characteristic zero, then the additive group action becomes

$$(t, (x, y, z)) \longrightarrow (x + ty + \frac{1}{2}(t^2 + t)z, y + tz, z).$$

In particular, one can find a triangular polynomial map F_T having coefficients in $k[t]$ such that F_m, being the evaluation of F_T at $T = m$, equals F^m for each $m \in \mathbb{Z}$. One of the nice things of strictly triangular polynomial maps in characteristic zero is indeed this property that it is easy to compute powers of the map, i.e if F is a strictly triangular map, then it is easy to compute $F^m(v)$ for any given $n \in \mathbb{N}, v \in k^n$: such a formula F_T explains this. If one would like to consider $(x + y + z, y + z, z)$ as a map $\mathbb{F}_p^3 \longrightarrow \mathbb{F}_p^3$, however, it is not directly possible to give such an explicit formula, as one cannot divide by 2! This article shows how to solve this problem for the case $k = \mathbb{F}_p$, by studying $(\mathbb{Z}, +)$-actions in stead of $(k, +)$ actions. Regardless of these actions, we explain how to quickly compute $F^m(v)$ for this case.

Being able to compute $F^m(v)$ quickly can be useful: in applications it can be useful to have a set of maps φ_m which commute: an example is Diffie-Hellmann key exchange (see section 6). One takes $\varphi_m = F^m$. We explain how to do this, compute its storage size and computational difficulty, and explain why it has a certain degree of security.

All of the theorems in section 2 are motivated by the application in section 5 and 6, while those of section 4 are inspired by it. Section 3 is a preparation for section 4.

Contents

2 Triangular polynomial maps

2.1 The triangular permutation group $\mathcal{B}_n(\mathbb{F}_p)$

Below, write $A_n := \mathbb{F}_p[X_1, \ldots, X_n]$, and write $\mathfrak{i}_n$ for the ideal in A_n generated by the $X_i^p - X_i$. (Writing $\mathfrak{i}, A$ if n is clear.) Write $x_i := X_i + \mathfrak{i}$, and write $R_n := \mathbb{F}_p[x_1, \ldots, x_n] = A_n/\mathfrak{i}_n$. In this article, a polynomial map is an element $F \in (A_n)^n$. Each F induces a map $\mathbb{F}_p^n \longrightarrow \mathbb{F}_p^n$, i.e. we have a map $\pi : (A_n)^n \longrightarrow \mathrm{Hom}(\mathbb{F}_p^n, \mathbb{F}_p^n)$. Then $\mathfrak{i}^n$ (please read as subset of A^n, not $\mathfrak{i}^n \subset A$!) is the kernel of π. Hence, we may see $\pi(F)$ as an element of $(R_n)^n$, and since π is surjective, these elements coincide one to one with the elements of $\mathrm{Hom}(\mathbb{F}_p^n, \mathbb{F}_p^n)$. So it means that we can write maps like $(x_1^2 + x_2, x_2 + 1 + x_1) \in \mathrm{Hom}(\mathbb{F}_p^n, \mathbb{F}_p^n)$. The set of elements in $\mathrm{Hom}(\mathbb{F}_p^n, \mathbb{F}_p^n)$ which are isomorphisms we denote, as usual, by $\mathrm{Perm}(\mathbb{F}_p^n)$.

We define a polynomial map to be *triangular* if $F = (F_1, \ldots, F_n)$ where $F_i \in A_i = \mathbb{F}_p[X_1, X_2, \ldots, X_i]$.[1] Similarly, F is called *strictly triangular* if $F_i - X_i \in A_{i-1} = \mathbb{F}_p[X_1, \ldots, X_{i-1}]$. We state that an element in $\mathrm{Hom}(\mathbb{F}_p^n, \mathbb{F}_p^n)$ is strictly triangular if it is the image of a strictly triangular element in A_n^n.

Polynomial maps can be composed, yielding another polynomial map, and hence we have an associative operation $\circ$ on $(A_n)^n$. The polynomial map $I := (X_1, \ldots, X_n)$ is an identity with respect to this operation, and a polynomial map is said to be invertible if it has a polynomial inverse. The polynomial maps which are invertible form a group, denoted $\mathrm{GA}_n(\mathbb{F}_p)$. Thus, $\pi(\mathrm{GA}_n(\mathbb{F}_p)) \subseteq \mathrm{Perm}(\mathbb{F}_p^n)$ (see [10, 11, 12] on the image of this group). The set of strictly triangular polynomial maps forms a subgroup (see [6] section 3.6) denoted by $\mathrm{B}_n^0(\mathbb{F}_p)$ (see [2] for the reasoning behind

[1] Note that often the definition is to let $F_i \in \mathbb{F}_p[X_i, \ldots, X_n]$ (and in fact we are used to it ourselves) but for this article it turned out to be more convenient to choose the definition in the text; some induction proofs then have easier indexes).

the naming of these groups). One can also define the groups $\mathrm{B}_{n-m}(A_m) \subset \mathrm{B}_n(\mathbb{F}_p)$ and $\mathrm{B}^0_{n-m}(A_m) \subset \mathrm{B}^0_n(\mathbb{F}_p)$.

In this article we will focus on the group $\pi(\mathrm{B}^0_n(\mathbb{F}_p))$, for which we introduce the shorthand notation $\mathcal{B}_n(\mathbb{F}_p)$. We also have the groups[2]

$$\mathcal{B}_{n-m}(R_m) < \mathcal{B}_n(\mathbb{F}_p).$$

Elements $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ thus have a unique representation of the form

$$\sigma = (x_1 + g_1, x_2 + g_2(x_1), \dots, x_n + g_n(x_1, \dots, x_n))$$

where we assume that $\deg_{x_i}(g_j) \le p-1$ for each $1 \le i, j \le n$. If $\sigma \in \mathcal{B}_{n-m}(R_m)$, then it is like above, only $g_i = 0$ if $i \le m$. We will write $e = \pi(I) \in \mathrm{Perm}(\mathbb{F}_p^n)$. We start with a few generalities on elements of $\mathcal{B}_n$:

Lemma 2.1. *Let $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ where $q = p^m$. Then*

i $\mathcal{B}_{n-m}(R_m) \lhd \mathcal{B}_n(\mathbb{F}_p)$.

ii $\mathcal{B}_{n-m}(R_m)/\mathcal{B}_{n-m-k}(R_{m+k}) \cong \mathcal{B}_k(R_m)$. *In particular,* $\mathcal{B}_{n-m}(R_m)/\mathcal{B}_{n-m-1}(R_{m+1}) \cong \mathcal{B}_1(R_m)$*, which is isomorphic with the group* $< R_m, + >$.

iii If $\sigma \in \mathcal{B}_{n-m}(R_m)$*, then* $\sigma^p \in \mathcal{B}_{n-m-1}(R_{m+1})$.

iv If $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$*, then* $\sigma^{p^n} = e$.

v Any cycle in $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ *has length* p^i *for some* i.

vi $\#\mathcal{B}_{n-m}(R_m) = p^{\left(\frac{p^n - p^m}{p-1}\right)}$. *In particular,* $\mathcal{B}_n(\mathbb{F}_p)$ *is a p-sylow subgroup of* $\mathrm{Perm}(\mathbb{F}_p^n)$.

vii If $\gcd(m, p) = 1$*, then for* $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ *there exists* $\tau \in \mathcal{B}_n(\mathbb{F}_p)$ *such that* $\tau^m = \sigma$.

Proof. (i) If $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$, write $\sigma_m \in \mathcal{B}_m(\mathbb{F}_p)$ for the first m coordinates. If one composes elements $\sigma, \tau \in \mathcal{B}_n(\mathbb{F}_p)$, then one can easily check that $(\sigma\tau)_m = \sigma_m\tau_m$. Now $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ satisfies $\sigma \in \mathcal{B}_{n-m}(R_m)$ if and only if $\sigma_m = e \in \mathcal{B}_{n-m}(R_m)$. Thus, if $\sigma \in \mathcal{B}_{n-m}(R_m)$ and $\tau \in \mathcal{B}_n(\mathbb{F}_p)$, then $(\tau^{-1}\sigma\tau)_m = \tau_m^{-1} e \tau_m = e \in \mathcal{B}_{n-m}(R_m)$, hence $\mathcal{B}_{n-m}(R_m)$ is closed under conjugation by elements of $\mathcal{B}_n(\mathbb{F}_p)$ and hence normal.
(ii) A proof sketch to save space: modding out $\mathcal{B}_{n-m-k}(R_{m+k})$ removes the last $n-m-k$ coordinates and leaves the first $m+k$ coordinates intact. To understand

[2] There's a small formal issue here: if $\sigma \in \mathcal{B}_k(R)$ then $\sigma = (x_1 + g_1, \dots, x_n + g_n)$ where $g_i \in R[x_1, \dots, x_{i-1}]$, but we actually mean $\sigma \in \mathcal{B}_{n-m}(R_m)$ then $\sigma = (x_{1+m} + g_{1+m}, \dots, x_n + g_n)$ where $g_{i+m} \in R_m[x_{1+m}, \dots, x_{i+m-1}]$, and not even that: we identify $(x_{1+m} + g_{1+m}, \dots, x_n + g_n)$ with $(x_1, x_2, \dots, x_m, x_{1+m} + g_{1+m}, \dots, x_n + g_n)$. However, these formal things are easily fixed, and we do not want to interrupt the flow of the article with these formalities: all elements are from the group $\mathcal{B}_n(\mathbb{F}_p)$ and the groups mentioned are all subgroups of this group.

$\mathcal{B}_1(R)$ for a ring R, note that elements are of the form (x_1+r) and that $(x_1+r)(x_1+s) = (x_1+r+s)$.
(iii) Any element in $< R_m, + >$ has order p, hence if $\sigma \in \mathcal{B}_{n-m}(R_m)$ then $\sigma + \mathcal{B}_{n-m-1}(R_{m+1}) \in \mathcal{B}_{n-m}(R_m)/\mathcal{B}_{n-m-1}(R_{m+1})$ has order p; hence $\sigma^p \in \mathcal{B}_{n-m-1}(R_{m+1})$.
(iv) Applying (iii) n times, yields that if $\sigma \in \mathcal{B}_n(\mathbb{F}_p) = \mathcal{B}_n(R_0)$, then $\sigma^{p^n} \in \mathcal{B}_0(R_n)$ which is the trivial group.
(v) follows easily from (iv).
(vi): The number of coefficients of g_i is p^{i-1}. Hence, an element in $\mathcal{B}_{n-m}(R_m)$ is determined by $p^m + p^{m+1} + \ldots + p^n = p^m \frac{p^{n-m}-1}{p-1}$ coefficients. The stated formula follows since each coefficient can take p values.
(vii) Since $(m, p^n) = 1$ there exist $a, b \in \mathbb{Z}$ such that $am + bp^n = 1$. Pick $\tau := \sigma^a$, then $\tau^m = \sigma^{am} = \sigma$. □

Remark 2.2. In respect to lemma 2.1 part (vi) we mention the papers of Kaluznin from 1945 and 1947 [7, 8] which were motivated by finding the p-sylow subgroups of $\mathrm{Perm}(N)$ where $N \in \mathbb{N}^*$. His description of the p-sylow groups of $\mathrm{Perm}(p^n)$ is exactly the triangular permutation group. This example of a p-sylow group resembles the following well-known example: let $B := \{I + N \mid N \in Mat_n(F_p)$ strictly upper triangular$\}$ be the set of unipotent upper triangular matrices in $\mathrm{GL}_n(\mathbb{F}_p)$. Then B is a p-sylow subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$. In fact, $B = \mathrm{GA}_n(\mathbb{F}_p) \cap \mathrm{B}_n(\mathbb{F}_p)$.

2.2 Maximal orbit maps

Definition 2.3. We define $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ being *of maximal orbit* if σ consists of one permutation cycle of length p^n.

Next to the theoretical interest, our motivation for studying maximal orbit maps is for the application in the last section. The reason that we do not generalize the results of this article to other finite fields (i.e. finite extensions of $\mathbb{F}_p$) is that there exist no elements of maximal orbit in $\mathcal{B}_n(\mathbb{F}_{p^m})$ if $m \geq 2$. (One can prove lemma 2.1 part (i) for $\mathbb{F}_{p^m}$ for all m, so the longest possible orbit is p^n in stead of p^{nm}.)

Theorem 2.4. *$\sigma = (x_1 + g_1, \ldots, x_n + g_n)$ is of maximal orbit if and only if the coefficient c_i of $x_1^{p-1} \cdots x_{i-1}^{p-1}$ in g_i is nonzero for each $1 \leq i \leq n$. Furthermore, if σ is of maximal orbit, then*

$$\sigma^{p^{n-1}}(\tilde{\alpha}, a) = (\tilde{\alpha}, a + (-1)^{n-1}c_n)$$

for each $a \in \mathbb{F}_p, \tilde{\alpha} \in \mathbb{F}_p^{n-1}$.

Proof. We will prove the result by induction to n. If $n = 1$ then $\sigma = (x_1 + g_1)$, and this is a cycle of length p if and only if $g_1 \neq 0$. Suppose the theorem is proven for $n-1$. Write $\sigma = (\tilde{\sigma}, \sigma_n)$ where $\tilde{\sigma}$ can be seen as an element of $\mathcal{B}_{n-1}(\mathbb{F}_p)$. Let $\alpha = (\tilde{\alpha}, \alpha_n) \in \mathbb{F}_p^n$ where $\alpha_n \in \mathbb{F}_p, \tilde{\alpha} \in \mathbb{F}_p^{n-1}$. By the induction assumption, $\tilde{\sigma}$ permutes $\mathbb{F}_p^{n-1}$ with a p^{n-1} cycle if and only if the coefficients are as described in the theorem. In particular, if $\tilde{\sigma}$ does not permute $\mathbb{F}_p^{n-1}$ then let $\beta \in \mathbb{F}_p^{n-1}$ such that iterating $\tilde{\sigma}$ on $\tilde{\alpha}$ never reaches some $\tilde{\beta}$. Then iterating σ on α will never reach $(\tilde{\beta}, \alpha_n)$ and σ is not of maximal order. So let us assume that $\tilde{\sigma}$ is of maximal order, and let us try to determine whether the coefficient of $(x_2 x_3 \cdots x_n)^{p-1}$ in σ_n determines if σ is of maximal order.

Iterating $\tilde{\sigma}$ to $\tilde{\alpha}$ cycles through all elements

$$\tilde{\alpha}_0, \tilde{\alpha}_1, \ldots, \tilde{\alpha}_{p^{n-1}-1}$$

(where $\tilde{\alpha}_0 := \tilde{\alpha}$) of $\mathbb{F}_p^{n-1}$, and $\tilde{\sigma}^{p^{n-1}}(\tilde{\alpha}) = \tilde{\alpha}$. Hence, $\sigma^i(\alpha) = (\tilde{\alpha}_i, c_i)$ for some $c_i \in \mathbb{F}_p$. One sees that $\sigma(\tilde{\alpha}_i, c_i) = (\tilde{\alpha}, c_i + g_n(\tilde{\alpha}_i))$ and thus we have that $c_{i+1} = c_i + g_n(\tilde{\alpha}_i)$, yielding the formula

$$c_i := \alpha_0 + \sum_{j=0}^{i-1} g_n(\tilde{\alpha}_j).$$

We apply the above formula for $i = p^{n-1}$, where we need to compute

$$\sum_{j=0}^{p^{n-1}-1} g_n(\tilde{\alpha}_i) = \sum_{\beta \in \mathbb{F}_p^{n-1}} g_n(\beta).$$

We can split the sum for each monomial appearing in g_n. By the below lemma 2.5 we see that only the term $(x_1 x_3 \cdots x_{n-1})^{p-1}$ is of importance. Hence, if the coefficient of this term in g_n is zero, then $\sigma^{p^{n-1}}(\alpha) = \alpha$ and σ is not of maximal order, and if the coefficent is $a \in \mathbb{F}_p^*$, then

$$\sigma^{p^{n-1}}(\tilde{\alpha}, \alpha_n) = (\tilde{\alpha}, \alpha_n + (-1)^{n-1} a)$$

and hence σ is of maximal order. □

Lemma 2.5. *Let $M(x_1, \ldots, x_n) = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ where $0 \le a_i \le p-1$ for each $1 \le i \le n$. Then $\sum_{\alpha \in \mathbb{F}_p^n} M(\alpha) = 0$ unless $a_1 = a_2 = \ldots = a_n = p-1$, when it is $(-1)^n$.*

Proof. We proceed by induction to n. For $n = 1$ we have a standard exercise on finite fields: we get sums of d-th powers of the elements in $\mathbb{F}_p$, which we call S. Let a be a generator of $\mathbb{F}_p^*$. Then $S = \sum_{i=1}^{p-1} (a^i)^d$. Let $b = a^d$. Then $S = \sum_{i=1}^{p-1} b^i$. If $d = p-1$, then $b = 1$ and $S = p - 1 = -1$. If $d < p-1$, then $b \neq 1$. Then $S(b-1) = b^p - 1 = 0$. Since $b - 1 \neq 0$, $S = 0$.

Now assume the lemma has been proven for $n-1$. Define $\tilde{M} = x_2^{a_2} \cdots x_n^{a_n}$. Then

$$\begin{aligned} \textstyle\sum_{\alpha \in \mathbb{F}_p^n} M(\alpha) &= \textstyle\sum_{b \in \mathbb{F}_p} \sum_{\tilde{\alpha} \in \mathbb{F}_p^{n-1}} b^{a_1} \tilde{M}(\tilde{\alpha}) \\ &= \textstyle\sum_{b \in \mathbb{F}_p} b^{a_1} \big(\sum_{\tilde{\alpha} \in \mathbb{F}_p^{n-1}} \tilde{M}(\tilde{\alpha}) \big) \\ \text{(induction)} &= \delta \cdot \textstyle\sum_{b \in \mathbb{F}_p} b^{a_1} \end{aligned}$$

where $\delta = 0$ unless $a_2 = \ldots = a_n = p-1$, when it is $(-1)^{n-1}$, by induction. Now $\sum_{b \in \mathbb{F}_p} b^{a_1} = 0$ unless when $a_1 = p-1$, when it is -1. Thus the lemma is proven. □

So, the above theorem 2.4 gives a clear citerion in the coefficients appearing in σ for when an element in $\mathcal{B}_n(\mathbb{F}_p)$ is of maximal order. Now, note that lemma 2.1 part (vi) actually tells one that it is possible to find an "m-th root" of any $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ when $(m, p) = 1$. For $m = p$, however, it will not be always possible. (In particular, if σ is of maximal orbit, it is not possible.) This induces a few questions we were unable to solve satisfactory like theorem 2.4 does:

Question 2.6.
(1) Can one recognise of the coefficients in $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ if σ is a p-th power of another map in $\mathcal{B}_n(\mathbb{F}_p)$? In particular, what is $\mathcal{B}_{n-1}(R_1)/G$ where $G :=< \sigma^p \mid \sigma \in \mathcal{B}_n(\mathbb{F}_p) >$.
(2) Can one recognise of the coefficients in $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ if σ is a p^i-th power of a map of maximal orbit?

(Note that G in (1) is a fully invariant subgroup of $\mathcal{B}_n(\mathbb{F}_p)$, and in particular normal, see [14] page 28.)

There are some necessary requirements, like in (1) σ must be in $\mathcal{B}_{n-1}(R_1)$ and (consequently) in (2) $\sigma \in \mathcal{B}_{n-i}(R_i)$, but these are by no means sufficient: (x_1, x_2+x_1) is not a p-th power while $(x_1, x_2 + 1)$ is.

2.3 Classification of maximal order maps

The following few lemmas are meant to be tools to reduce the number of coefficients necessary to describe σ. First, we will consider the issue that if two maps are powers of each other, then they are interchangeable in some semse (in particular in the application). After that we will find the conjugacy classes of maximal order maps.

Definition 2.7. We say that two permutations $c, c' \in \mathrm{Perm}(N)$ where $N \in \mathbb{N}^*$ are equivalent if $< c >=< c' >$, i.e. there exist $a, b \in \mathbb{N}^*$ such that $c^a = c', (c')^b = c$.

Definition 2.8. $\sigma = (x_1 + g_1, \ldots, x_n + g_n) \in \mathcal{B}_n(\mathbb{F}_p)$ is said to be on *standard form* if $\sigma(0, 0, \ldots, 0) = (0, 0, \ldots, 0, 1)$, i.e. the constant terms of $g_2, \ldots, g_n$ are zero and $g_1 = 1$.

Lemma 2.9. *If $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ of maximal order, then there is exactly one $\sigma' \in \mathcal{B}_n(\mathbb{F}_p)$ on standard form, such that σ, σ' are equivalent. In other words, standard form maximal order maps form a representant system of the maximal order maps modulo equivalence.*

Proof. Write $\sigma = (x_1 + g_1, \tilde{\sigma})$. Since σ is of maximal order, $g_1 \neq 0$. Now let $a \in \mathbb{N}$ be an inverse of g_1 modulo p. Then $\sigma^a = (x_1 + ag_1, \ldots) = (x_1 + 1, \ldots)$ and by lemma 2.1 part (vii), σ^a is equivalent to σ. So we can assume that $g_1 = 1$ by replacing σ by σ^a.

Now, starting with $O := (0, 0, \ldots, 0)$ and iterating σ, then we see that $\sigma^m(O) = (m \mod p, \ldots)$. So, this first coordinate equals 1 if and only if $m \mod p = 1$

which means that $m = ap + 1$ for some $a \in \mathbb{N}$. Since σ is of maximal order, the sequence $O, \sigma(O), \sigma^2(O), \ldots, \sigma^{p^n-1}(O)$ lists all elements of $\mathbb{F}_p^n$. The sublist of vectors starting with 1 is $\sigma(O), \sigma^{p+1}(O), \sigma^{2p+1}(O), \ldots, \sigma^{p^n-p+1}(O)$. One of these elements equals $(0, 0, \ldots, 0, 1)$, i.e. there exists exactly one $a \in \mathbb{N}$ such that $\sigma^{ap+1}(O) = (0, 0, \ldots, 0, 1)$. By lemma 2.1 (vii) , σ^{ap+1} is equivalent to σ, and satisfies the above requirement. (Uniqueness is automatic, as for a cycle of length p^n in $\mathrm{Perm}(\mathbb{F}_p^n)$ there is only one power of that cycle sending O to $(0, 0, \ldots, 0, 1)$.) $\square$

We will now focus on finding representants for the conjugacy classes of maximal order maps.

Definition 2.10. Write $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for $\alpha \in \mathbb{F}_p^n$. Define

$$R_n^- := \sum_{\alpha \in \mathbb{F}_p^n, \alpha \neq (p-1,\ldots,p-1)} \mathbb{F}_p x^\alpha$$

the subvector space of R_n without the monomial $(x_1 \cdots x_n)^{p-1}$.
If $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$, define $\sigma^* : R_n \longrightarrow R_n$ by $\sigma^*(f) = f(\sigma)$. We denote by e^* the identity map on R_n.

Lemma 2.11. *If $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ is of maximal orbit, then* $\ker(\sigma^* - e^*) = \mathbb{F}_p$. *(The converse is also true: if the kernel is $\mathbb{F}_p$, then σ is of maximal orbit.)*

Proof. Let $f \in \ker(\sigma^* - e^*)$. Then $0 = \sigma^*(f) - e^*(f) = f(\sigma) - f$ so $f = f(\sigma)$, and thus $f = f(\sigma^i)$ for all i. Let $\alpha \in \mathbb{F}_p^n$, then $f(\alpha) = f(\sigma^i(\alpha))$ for each i. Since σ is of maximal orbit, we thus get that $f(\alpha) = f(\beta)$ for each $\beta \in \mathbb{F}_p^n$, in other words, f is a constant function. Notice that since $f \in R_n$ this indeed means $f = 0$.
The converse goes similarly: if σ is not of maximal orbit, then f only needs to be constant on the orbits of σ. $\square$

Corollary 2.12. *If $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$, then* $\mathrm{Im}(\sigma^* - e^*) \subseteq R_n^-$. *If σ is of maximal orbit, then we even have equality* $\mathrm{Im}(\sigma^* - e^*) = R_n^-$.

Proof. Note that $\sigma^*(R_n^-) \subset R_n^-$. A computation shows that $(\sigma^* - e^*)((x_1 \cdots x_n)^{p-1}) \in \mathbb{R}_n^-$. Because of linearity of $\sigma^* - e^*$ we thus have that $(\sigma^* - e^*)R_n = (\sigma^* - e^*)(\mathbb{F}_p(x_1 \cdots x_n)^{p-1} + R_n^-) \subseteq \mathbb{F}_p(\sigma^* - e^*)((x_1 \cdots x_n)^{p-1}) + (\sigma^* - e^*)(R_n^-) \subseteq R_n^-$.

The second part follows from lemma 2.11: the kernel has dimension 1, so the image must have codimension 1. $\square$

Proposition 2.13. *Let $\sigma, \tau \in \mathcal{B}_n(\mathbb{F}_p)$ of maximal orbit, i.e.*

$$\sigma = (x_1 + \lambda_1,\ x_2 + \lambda_2 x_1^{p-1} + g_2,\ x_3 + \lambda_3(x_1 x_2)^{p-1} + g_3, \ldots,\ x_n + \lambda_n(x_1 \cdots x_n)^{p-1} + g_n),$$

$$\tau = (x_1 + \mu_1, x_2 + \mu_2 x_1^{p-1} + h_2, x_3 + \mu_3(x_1 x_2)^{p-1} + h_3, \ldots, x_n + \mu_n(x_1 \cdots x_n)^{p-1} + h_n),$$

where $\lambda_i, \mu_i \in \mathbb{F}_p^*$, and $g_i, h_i \in R_{i-1}$. Then there exists $\varphi \in \mathcal{B}_n(\mathbb{F}_p)$ such that $\varphi^{-1}\sigma\varphi = \tau$ if and only if $\lambda_i = \mu_i$ for all $1 \leq i \leq n$. If φ exists, then one may additionally assume φ to be on standard form (see definition 2.8), and then φ is unique.

The above proposition hence shows that $\lambda_1, \ldots, \lambda_n$ is a defining invariant for σ.

Proof. By induction to n. The case $n = 1$ is obvious (one picks $\varphi = (x_1 + 1)$, which is on standard form). Write $\sigma = (\tilde{\sigma}, x_n + g_n), \tau = (\tilde{\tau}, x_n + h_n)$. The induction assumption means we can find a unique standard form map $\tilde{\varphi}$ in $n-1$ variables such that $\tilde{\varphi}^{-1}\sigma\tilde{\varphi} = \tilde{\tau}$ if and only if $\lambda_1 = \mu_1, \ldots, \lambda_{n-1} = \mu_{n-1}$. We will extend $\varphi := (\tilde{\varphi}, x_n)\phi$ where $\phi := (x_1, \ldots, x_{n-1}, x_n + f_n)$. Write $(\tilde{\varphi}, x_n)^{-1}\sigma(\tilde{\varphi}, x_n) = (\tilde{\tau}, x_n + \lambda_n(x_1 \cdots x_n)^{p-1} + k_n)$ where $k_n \in R^-_{n-1}$. Now a computation reveals $\phi^{-1}(\tilde{\tau}, x_n + \lambda_n(x_1 \cdots x_n)^{p-1} + k_n)\phi = (\tilde{\tau}, x_n + \lambda_n(x_1 \cdots x_n)^{p-1} + k_n + (e^* - \tilde{\tau}^*)(f_n))$. We thus are (only) able to change $\lambda_n(x_1 \cdots x_n)^{p-1} + k_n$ by elements of R^-_{n-1} as corollary 2.12 shows, meaning that τ and σ are only conjugate if $\lambda_n = \mu_n$. Let us assume the latter, and pick f_n so that $(e^* - \tilde{\tau}^*)(f_n) = k_n$. If we assume f_n to have constant part zero then f_n is unique. φ is now on normal form by construction, and the above shows that it is unique. $\square$

Definition 2.14. Define $\delta_i \in R_i$ as the polynomial such that $\delta_i(p-1, \ldots, p-1) = 1$ and $\delta(\alpha) = 0$ for all other $\alpha \in \mathbb{F}_p^i$. (And $\delta_0 = 1$.) Then define

$$\Delta := (x_1 + \delta_0, x_2 + \delta_1, \ldots, x_n + \delta_{n-1}).$$

Theorem 2.15. *Let $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ of maximal orbit. Then there exist a unique $\varphi \in \mathcal{B}_n(\mathbb{F}_p)$ on standard form, and a diagonal linear map D, such that $D^{-1}\varphi^{-1}\sigma\varphi D = \Delta$.*

Proof. Write μ_i for the coefficient of $(x_1 \cdots x_{i-1})^{p-1}$ in δ_{i-1} ($\mu_1 = 1$). By proposition 2.13 we see that σ is equivalent to $(x_1 + \lambda_1, x_2 + \lambda_2\delta_1, \ldots, x_n + \lambda_n\delta_{n-1})$ for some $\lambda_i \in \mathbb{F}_p^*$. Write $D := (\lambda_1 x_1, \ldots, \lambda_n x_n)$. By proposition 2.13 there exists a unique $\varphi \in \mathcal{B}_n(\mathbb{F}_p)$ on standard form such that $\varphi^{-1}\sigma\varphi = (x_1 + \lambda_1, x_2 + \lambda_2\delta_1(D^{-1}), x_3 + \lambda_3\delta_2(D^{-1}), \ldots, x_n + \lambda_n\delta_{n-1}(D^{-1}))$. Now a computation reveals that $D^{-1}\varphi^{-1}\sigma\varphi D = \Delta$. $\square$

The above theorem thus enables us to see *all* maximal orbit maps as a unique conjugate of one map, namely Δ. This map is, in some sense, very simple, as the following remark shows:

Remark 2.16. Define the bijection $\zeta : \mathbb{Z}/p^n\mathbb{Z} \longrightarrow (\mathbb{F}_p)^n$ by $\zeta(a_0 + a_1 p + \ldots + a_{n-1}p^{n-1}) = (a_0, \ldots, a_{n-1}) \mod p$ where $0 \leq a_i \leq p-1$. Then $\zeta\Delta\zeta^{-1}$ is the map $m \longrightarrow m + 1$.

The following lemma is specifically necessary for the application in section 5, in order to prove a certain degree of security.

Lemma 2.17. *Let $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ be of maximal orbit, and let $\alpha_i \in \mathbb{F}_p^n$ for $1 \leq i \leq m+1$ and $\beta_i := \sigma(\alpha_i)$. Let*

$$\Omega := \{\tau \in \mathcal{B}_n(\mathbb{F}_p) \mid \tau(\alpha_i) = \beta_i,\ 1 \leq i \leq m,\ \tau \text{ of maximal orbit}\}.$$

Then for any $j \in \mathbb{N}$, $j \leq \log_p(m)$, $\tau \in \Omega$, $\tau_j(\alpha_m)$ is fixed, while for any $j > \log_p(m)$, the values $\tau_j(\alpha)$ where τ runs over Ω are uniformly distributed on $\mathbb{F}_p$.
Hence, when knowing m pairs $(\alpha_i, \sigma(\alpha_i))$ of a specific σ as above, then given another value α_{m+1}, one can predict the first $[\log_p(m)]$ coordinates of $\sigma(\alpha_{m+1})$ with 100% certainty, while the other coordinates are fully unknown.

Proof. Let $\sigma = (f_1, \ldots, f_n)$ like stated. Note that $f_j = x_j + g_j(x_1, \ldots, x_{j-1})$ and that g_j has p^{j-1} coefficients (of which one, the coefficient of $(x_1x_2\cdots x_{j-1})^{p-1}$, is nonzero, a fact we will ignore). What in fact is given, is for each $0 \leq j \leq n-1$ a list of m pairs $(\alpha_i, g_{n-j}(\alpha_i))$. Each such pair gives one linear equation on the coefficients of g_{n-j}. If $j \leq \log_p(m)$, then $p^j \leq m$, and we have an overdetermined set of linear equations, so g_{n-j} is fixed. If $j > \log_p(m)$, then $p^j > m$, and we have an underdetermined set of linear equations on the coefficients of g_{n-j}. It is now standard to see that g_{n-j} can still be any value, and the possible outcomes of g_{n-j} can appear with equal chance. (The set of degree p polynomials in one variable where $p-1$ values are fixed, is exactly of size p: for each value of $\mathbb{F}_p$ there's one polynomial.) $\square$

3 Generalities on polynomial maps $\mathbb{Z} \longrightarrow \mathbb{F}_p$

The below definitions we took from [4]. These concepts first appeared in [13].

Definition 3.1. Let $A, B \subseteq \mathbb{Q}$. Then define

$$\mathrm{Int}(A, B) := \{f \in \mathbb{Q}[T] \mid f(A) \subseteq B\}.$$

In this article, A will be $\mathbb{Z}_{(p)}$ or $\mathbb{Z}$, and $B = \mathbb{Z}$. In particular, we abbreviate $\mathrm{Int}(\mathbb{Z}) = \mathrm{Int}(\mathbb{Z}, \mathbb{Z})$. Note that $\mathrm{Int}(A, B)$ is a subring of $\mathbb{Q}[T]$.

The following is a well-known lemma:

Lemma 3.2.

$$\mathrm{Int}(\mathbb{Z}) = \bigoplus_{i\in\mathbb{N}} \mathbb{Z}\binom{T}{i} = \mathbb{Z}\left[\binom{T}{i} \,\middle|\, i \in \mathbb{N}\right].$$

Proof. (sketch) Let V be the set of polynomials of degree d and less having coefficients in $\mathbb{Q}$. The polynomials $\binom{T}{0}, \binom{T}{1}, \ldots, \binom{T}{d}$ form a $\mathbb{Q}$-basis for V. This means that $f = \sum_{i=0}^{d} a_i\binom{T}{i}$ for some $a_i \in \mathbb{Q}$. Let $v = (f(0), f(1), \ldots, f(d)) \in \mathbb{Z}^{d+1}$, $\vec{a} = (a_0, a_1, \ldots, a_d)$. Define $A := (\binom{i}{j})$ of size $(d+1)\times(d+1)$. Then $v = A\vec{a}$ where A has coefficients in $\mathbb{Z}$, is of upper triangular form, and has only 1's on the diagonal. Hence, A is invertible with an inverse having coefficients in $\mathbb{Z}$. Thus, $\vec{a} = A^{-1}v$ is a vector in $\mathbb{Z}^{d+1}$ proving the lemma. $\square$

Corollary 3.3.

$$\mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(p)}) = \bigoplus_{i\in\mathbb{N}} \mathbb{Z}_{(p)}\binom{T}{i} = \mathbb{Z}_{(p)}\left[\binom{T}{i} \,\middle|\, i \in \mathbb{N}\right].$$

If $f \in \mathbb{Z}[\binom{T}{m} \mid m \in \mathbb{N}]$ then it makes sense to consider the map $\mathbb{Z} \longrightarrow \mathbb{F}_p$ given by $n \longrightarrow f(n) \mod p$. Also, if $r \in \mathbb{Z}_{(p)}$, then it makes sense to write down $r \mod p$ in the following way: if $r = \frac{a}{b}$ where $a \in \mathbb{Z}, b \in \mathbb{Z}\backslash p\mathbb{Z}$ then $r \mod p = (a \mod p)(b \mod p)^{-1}$.

Definition 3.4. Define $\tau : \mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(p)}) \longrightarrow \mathrm{Hom}(\mathbb{Z}, \mathbb{F}_p)$ by $\tau(f)(n) = f(n) \mod p$ for any $f \in \mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(p)})$.
We say that $f, g \in \mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(p)})$ are *equivalent under* τ if $\tau(f) = \tau(g)$.

Remark 3.5. If $f \in \mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(p)})$ then there is some $g \in \mathrm{Int}(\mathbb{Z})$ which is equivalent under τ.

Definition 3.6. Define $Q_i := \binom{T}{p^i}$.

Proposition 3.7. *Let $f \in \mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(p)})$ be of degree d. Then f is equivalent to some $g \in \mathbb{Z}[Q_0, Q_1, \ldots, Q_r]$ where $r = [\log_p(d)]$. Furthermore, g is at most of degree $p-1$ in each Q_i.*

The above proposition is based on Lucas' Theorem [9]:

Lucas' Theorem: Let $0 \le \alpha_i < p, 0 \le \beta_i < p$ where $\alpha_i, \beta_i \in \mathbb{N}$. Then

$$\binom{\alpha_0 + \alpha_1 p + \alpha_2 p^2 + \ldots + \alpha_n p^n}{\beta_0 + \beta_1 p + \beta_2 p^2 + \ldots + \beta_n p^n} \equiv_p \binom{\alpha_0}{\beta_0}\binom{\alpha_1}{\beta_1}\binom{\alpha_2}{\beta_2}\cdots\binom{\alpha_n}{\beta_n}.$$

Proof. (of proposition 3.7.) First, note that the polynomial $Q_i(T) = \binom{T}{p^i}$ assigns to $\alpha_0 + \alpha_1 p + \ldots + \alpha_i p^i + \ldots + \alpha_n p^n$ the value α_i, using Lucas' Theorem. Let f be as in the proposition. By corollary 3.3 f is a $\mathbb{Z}_{(p)}$-linear combination of $\binom{T}{0}, \binom{T}{1}, \ldots, \binom{T}{d}$, which means by remark 3.5 that f is equivalent to a $\mathbb{Z}$-linear combination of $\binom{T}{0}, \binom{T}{1}, \ldots, \binom{T}{d}$. Now if $d = \alpha_0 + \alpha_1 p + \ldots + \alpha_n p^n$ we use Lucas' Theorem again to derive the following:

$$\begin{aligned}\binom{T}{d} &= \binom{\binom{T}{1}}{\alpha_0}\binom{\binom{T}{p}}{\alpha_1}\binom{\binom{T}{p^2}}{\alpha_1}\cdot\cdots\cdot\binom{\binom{T}{p^n}}{\alpha_n} \\ &= \binom{Q_0}{\alpha_0}\binom{Q_1}{\alpha_1}\binom{Q_2}{\alpha_1}\cdot\cdots\cdot\binom{Q_n}{\alpha_n}.\end{aligned}$$

Note that $\binom{T}{d}$ is a polynomial in $Q_0, \ldots, Q_n$ where the highest coefficient in the Q_i is $Q_0^{\alpha_0} Q_1^{\alpha_1} \cdots Q_n^{\alpha_n}$. Hence, since f is equivalent to a $\mathbb{Z}$-linear combination of $\binom{T}{0}, \binom{T}{1}, \ldots, \binom{T}{d}$, the highest coefficient of $Q_0, \ldots, Q_{n-1}$ is possibly $p-1$, and the highest coefficient of Q_n is α_n. □

4 Exponents of triangular maps over $\mathbb{F}_p$

4.1 Some more generalities

Definition 4.1. Define $B_n := \mathbb{Z}[Q_0, Q_1, \ldots, Q_{n-1}]$ where the Q_i are independent variables, and $B := \cup B_n$. We also define $S_n := B_n/\mathfrak{j}_n$ where $\mathfrak{j}_n := (Q_i^p - Q_i \mid 1 \le$

$i \leq n$), and $\mathfrak{j} := \cup \mathfrak{j}_n$ and $S := \cup S_n = B/\mathfrak{j}$. We will abuse notation, and write "Q_i" when we might mean "$Q_i + \mathfrak{j}$". At some point we will denote Q_0 by t.

In section 3 we already introduced the map $\tau : B \longrightarrow \mathrm{Hom}(\mathbb{Z}, \mathbb{F}_p)$ defined by $\tau(Q_i)(a) = \binom{a}{p^i} \mod p$ if $a \in \mathbb{Z}$. (In fact, we can extend the definition to $\tau : \mathbb{Z}_{(p)}[Q_0, Q_1, \ldots, Q_{n-1}] \longrightarrow \mathrm{Hom}(\mathbb{Z}, \mathbb{F}_p)$, but proposition 3.7 allows us to avoid this extension for now.) However, we will extend τ naturally to

$$\tau : B[X_1, \ldots, X_n] \longrightarrow \mathrm{Hom}(\mathbb{Z} \times \mathbb{F}_p^n, \mathbb{F}_p).$$

Now the kernel of this map includes the ideal $\mathfrak{i} \subseteq \mathbb{Z}[X_1, \ldots, X_n]$ as defined in section 2, hence this map factors

$$\tau : B[X_1, \ldots, X_n] \longrightarrow B[x_1, \ldots, x_n] \longrightarrow \mathrm{Hom}(\mathbb{Z} \times \mathbb{F}_p^n, \mathbb{F}_p)$$

where $B[x_1, \ldots, x_n] = B \otimes \mathbb{Z}[X_1, \ldots, X_n]/\mathfrak{i}$. Notice that the ideal $\mathfrak{j}$ is also in the kernel (as $\tau(Q_i^p)(a) = \binom{a}{p^i}^p \mod p = \binom{a}{p^i} \mod p = \tau(Q_i)(a)$) hence the map factors again

$$\tau : B[X_1, \ldots, X_n] \longrightarrow B[x_1, \ldots, x_n] \longrightarrow S[x_1, \ldots, x_n] \longrightarrow \mathrm{Hom}(\mathbb{Z} \times \mathbb{F}_p^n, \mathbb{F}_p).$$

Now it is not hard to check that this last map is injective (not surjective!), so $S[x_1, \ldots, x_n]$ represents the part of $\mathrm{Hom}(\mathbb{Z} \times \mathbb{F}_p^n, \mathbb{F}_p)$ that we're interested in.

Then, finally, we extend the map τ to n variables:

$$\tau : B[X_1, \ldots, X_n]^n \longrightarrow S[x_1, \ldots, x_n]^n \subset \mathrm{Hom}(\mathbb{Z} \times \mathbb{F}_p^n, \mathbb{F}_p^n).$$

Note that in all equations above one can replace B by B_m and S by S_m.

4.2 More general triangular groups

If one has a ring K, then one can make the group $\mathrm{B}_n(K)$ and $\mathrm{B}_n^0(K)$ as described in section 2. But, it is possible to make slightly less intuitive groups: suppose that $K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n$ is a chain of rings. Then one can make the set

$$\{(X_1 + g_1, X_2 + g_2, \ldots, X_n + g_n) \mid g_i \in K_i[X_1, \ldots, X_{i-1}]\}$$

which becomes a subgroup of $\mathrm{B}_n^0(K)$. However, one can even make this work for more general subsets of K which are not necessarily subrings.

Definition 4.2. Let K be a ring and let W_i a subgroup of $(K[X_1, \ldots, X_{i-1}], +)$ such that

$$W_i \circ (X_1 + W_1, X_2 + W_2, \ldots, X_i + W_i) \subseteq W_i.$$

Then define

$$\mathrm{B}(W_1, W_2, \ldots, W_n) := \{(X_1 + g_1, \ldots, X_n + g_n) \mid g_i \in W_i\}$$

which is a subset of $\mathrm{B}_n(K)$.

Lemma 4.3. $\mathrm{B}(W_1, W_2, \ldots, W_n)$ *is a subgroup of* $\mathrm{B}_n(K)$.

Proof. (sketch) The fact that the identity is in $\mathrm{B}(W_1, \ldots, W_n)$ follows from the fact that W_i is a subgroup and hence contains 0. A sketchy proof of the fact that it contains the inverse of an element $(X_1 + g_1, \ldots, X_n + g_n)$: then $(X_1 - g_1, X_2, \ldots, X_n)$ is also in the set, and composing it with this element yields the first coordinate is X_1; iterating this process one ends up at $(X_1, \ldots, X_n)$. The requirement "$W_i \circ (X_1 + W_1, X_2 + W_2, \ldots, X_i + W_i) \subseteq W_i$" is exactly what is needed to have the set closed under composition: here one needs to check that $g_i(X_1 + h_1, \ldots, X_{i-1} + h_{i-1}) \in W_i$ for each $g_i \in W_i, h_j \in W_j$. $\square$

Since one has a group homomorphism $\mathrm{B}_n^0(K) \longrightarrow \mathrm{Perm}(K^n)$, there exists also a group homomorphism $\mathrm{B}(W_1, \ldots, W_n) \longrightarrow \mathrm{Perm}(K^n)$. We study the special case that K is an $\mathbb{F}_p$-algebra such that $r = r^p$ for each $r \in K$. (Given an $\mathbb{F}_p$-algebra, one can get such an algebra by modding out the kernel of the frobenius endomorphism $r \longrightarrow r^p$; one could also say that such an algebra is an $\mathbb{F}_p$ algebra with Frobenius automorphism being the identity.) We will consider the case of subsection 4.1. Then the map $\mathrm{B}^0(S) \longrightarrow \mathrm{Perm}(S^n)$ is a restriction of the map $\tau : S[X_1, \ldots, X_n]^n \longrightarrow S[x_1, \ldots, x_n]^n \longrightarrow \mathrm{Hom}(S^n, S^n)$ and thus it makes sense to write down $\mathcal{B}_n(S)$, and we denote elements in this group like $\sigma := (x_1 + g_1, \ldots, x_n + g_n)$ where $g_i \in S[x_1, \ldots, x_n]$. Thus, we can also define the subgroup

$$\mathcal{B}(W_1, \ldots, W_n) \subset \mathcal{B}_n(S)$$

where $W_i \subset S[x_1, \ldots, x_{i-1}]$. (Normally we should define this as $W_i \subseteq S[X_1, \ldots, X_{i-1}]$, but the groups coincide modulo $(X_1^p - X_1, \ldots, X_n^p - X_n)$ so this notation makes sense.)

In this article there are two such groups that we consider: remember that we defined $R_m := \mathbb{F}_p[x_1, x_2, \ldots, x_m]$, $S_i := \mathbb{F}_p[Q_0, \ldots, Q_{i-1}]/\jmath$ where $\jmath$ is generated by the $Q_i^p - Q_i$, and note that $S_i R_j = S_i \otimes R_j = S_i[x_1, \ldots, x_j]$. We will consider $\mathcal{B}(S_1 R_0, S_2 R_1, \ldots, S_n R_{n-1})$ and the one mentioned in the next lemma. Both of them occur naturally in the next subsection.

Lemma 4.4. *If* $W_i := S_{i-1} R_{i-1} + \mathbb{F}_p Q_{i-1}$, *then* $W_i \circ (x_1 + W_1, \ldots, x_{i-1} + W_{i-1}) \subseteq W_i$. *Hence,* $\mathcal{B}(W_1, \ldots, W_n)$ *is a subgroup of* $\mathcal{B}(S_1 R_0, \ldots, S_n R_{n-1})$ *and of* $\mathcal{B}_n(S_n)$.

Proof. Let $g_i \in W_i$, i.e. $g_i = P(x_1, \ldots, x_{i-1}) + \lambda Q_{i-1}$ where $P \in S_{i-1} R_{i-1}$. Let $h_j \in W_j$, then we need to prove that $P(x_1 + h_1, \ldots, x_{i-1} + h_{i-1}) + \lambda Q_i = g_i(x_1 + h_1, \ldots, x_{i-1} + h_{i-1}) \in W_i$. Now $x_j + h_j \in S_j R_{j-1} \subseteq S_{i-1} R_{i-1}$, and since $P \in S_{i-1} R_{i-1}$ we get $P(x_1 + h_1, \ldots, x_{i-1} + h_{i-1}) \in S_{i-1} R_{i-1}$ and we are done. $\square$

4.3 Exponents of triangular maps: $\mathbb{Z}$-flows

Over a field K of characteristic zero, given a strictly triangular polynomial map F, then it is always possible to give a formula for exponents F^m of F, to be more precise: there is a strictly triangular polynomial map $F_T \in \mathrm{GA}_n(K[T])$ such that $F_m = F^m$ for each $m \in \mathbb{N}$.[3] To give a simple (even linear) example:

Example 4.5. Let $F = (x+y+z, y+z, z)$, if $F_T := (x+Ty+\frac{1}{2}(T^2+T)z, y+Tz, z)$, then $F_m = F^m$ for each $n \in \mathbb{N}$.

However, if one picks K a field of characteristic two, and considers the same map $F := (x+y+z, y+z, z)$, then one runs into trouble defining F_T, as it includes the polynomial $\frac{1}{2}(T^2+T)$. However, we can now use the previous subsection to solve this problem. Note that if $\sigma_T \in \mathcal{B}_n(S_n)$, then one can substitute a value $m \in \mathbb{Z}$ for T (thus mapping $Q_i(T)$ to $Q_i(m)$ etc.) and one gets an element $\sigma_m \in \mathcal{B}_n(\mathbb{F}_p)$.

Definition 4.6. Let $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$. Suppose $\sigma_T \in \mathcal{B}_n(S_n)$ is such that $\sigma_m = \sigma^m$ for each $m \in \mathbb{Z}$. Then we define $\boldsymbol{\sigma_T}$ as the **$\mathbb{Z}$-flow of $\boldsymbol{\sigma}$**.

The wording $\mathbb{Z}$-flow come from the analytic case: If F is a holomorphic map $\mathbb{C}^n \longrightarrow \mathbb{C}^n$, then under some circumstances one can define a holomorphic map $F_T : \mathbb{C} \times \mathbb{C}^n \longrightarrow \mathbb{C}^n$ such that $F_a F_b = F_{a+b}$ for each $a, b \in \mathbb{C}$, $F_1 = F$ and $F_0 = I$. Then F_T is called a flow of F.

Theorem 4.7. *Let $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$. Then*
(1) there exists a $\mathbb{Z}$-flow $\sigma_T \in \mathcal{B}(S_1R_0, S_2R_1, \dots, S_nR_{n-1})$ of σ,
(2) and even $\sigma_T \in \mathcal{B}(W_1, \dots, W_n)$ where W_i as in lemma 4.4.

Proof. We use induction to n. For $n = 1$, $\sigma = (x_1 + a)$ where $a \in \mathbb{F}_p$, , and we can take $\sigma_T := (x_1 + Ta) \in x_1 + R_0S_0 + \mathbb{F}_pQ_0$.
Let $\sigma = (\tilde{\sigma}, x_n + g_n) \in \mathcal{B}_n(\mathbb{F}_p)$. We know that we can find $\tilde{\sigma}_T \in \mathcal{B}(W_1, \dots, W_{n-1})$ such that $\sigma^m = (\tilde{\sigma}_m, x_n + h_m)$ where $h_m \in R_{n-1}$. Now pick $H_m \in \mathbb{Z}[x_2, \dots, x_n]$ such that $H_m \mod p = h_m$. Define

$$M_i(T) := \prod_{j=0, j\neq i}^{p^n-1} \frac{(T-j)}{i-j}$$

and define $G(T) := M_0H_0 + M_1H_1 + \ldots + M_{p^n-1}H_{p^n-1}$. Note that $G(T)$ is of degree $p^n - 1$ in T. Note that $G(i) = H_i$, and $G(T) \in \mathbb{Q}[T][x_1, \dots, x_n]$. Thus, if $c(T)$ is one of the coefficients in $\mathbb{Q}[T]$, then $c(\{0, 1, \dots, p^n - 1\}) \subset \mathbb{Z}$. Using lemma 3.2 we get that $c(\mathbb{Z}) \subset \mathbb{Z}$. Using proposition 3.7 we can replace each coefficient $c(T) \in \mathbb{Q}[T]$ by an equivalent element in $\mathbb{Z}[Q_0, Q_1, \dots, Q_{n-1}]$ (as $[\log_p(p^n - 1)] = n - 1$), so we can assume that $G_T \in \mathbb{Z}[Q_0, \dots, Q_{n-1}][x_1, \dots, x_n]$. Thus define $g_T \in \mathbb{F}_p[Q_0, \dots, Q_{n-1}][x_1, \dots, x_{n-1}] = S_nR_{n-1}$ as the image of G_T, and now we can define

$$\sigma_T := (\tilde{\sigma}_T, x_n + g_T)$$

[3] More precisely, without details, it is possible to give a locally nilpotent derivation D such that $F^m = \exp(mD)$, and then one can define $F_T := \exp(TD)$. In this article, we take this as a fact, for details we refer to [5] chapter 2.

and thus $\sigma_m = (\tilde{\sigma}_m, x_n + g_m) = (\tilde{\sigma}_m, x_n + h_m) = \sigma^m$, which is what is required.

Left to prove is that $g_T \in \mathbb{F}_p Q_{n-1} + S_{n-1}R_{n-1}$ (where we only have $g_T \in S_n R_{n-1}$ so far). Note that $\sigma^{p^{n-1}}(\tilde{\alpha}, \alpha_n) = (\tilde{\alpha}, \alpha_n + (-1)^{n-1}a)$ where a is the coefficient of $(x_1 \cdots x_{n-1})^{p-1}$ in $x_n + g_n$ (see theorem 2.4). This means that $\sigma^m = (x_1 + (-1)^{n-1}a, x_2, \ldots, x_n)$ if p^{n-1} divides m. Write $\lambda = a(-1)^{n-1} \in \mathbb{F}_p$, then $g_{mp^{n-1}} = m\lambda$. Now define $h_T := g_T - Q_{n-1}(T)\lambda$. Then $h_{p^{n-1}} = 0$, and thus h_T does not depend on Q_{n-1} (which has order p^n). Thus, $h_T \in S_{n-1}R_{n-1}$ and $g_T \in S_{n-1}R_{n-1} + \mathbb{F}_p Q_{n-1} = W_n$. □

It might be that this theorem can be improved, in the sense that the W_i can be chosen smaller. This comes down to the following question:

Question 4.8. Find $W_1, \ldots, W_n$ such that

$$\mathcal{B}(W_1, W_2, \ldots, W_n) = \langle \sigma_T \mid \sigma \in \mathcal{B}_n(\mathbb{F}_p) \rangle .$$

However, the below version is what is needed in the next section (as it is more efficient). We denote $t := Q_0$, thus $\mathbb{F}_p[t] := \mathbb{F}_p[T]/(T^p - T)$.

Theorem 4.9. *Let $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$. Then there exist*

$$\sigma_{i,T} \in \mathcal{B}(\mathbb{F}_p t, R_{i+1}[t], R_{i+2}[t], \ldots, R_{n-1}[t]) \subset \mathcal{B}_n(\mathbb{F}_p[t])$$

for $0 \le i \le n-1$ such that $\sigma^{p^i m} = \sigma_{i,m}$ for each $0 \le m \le p-1$.

Proof. Lemma 4.10 gives the case $i = 0$. Defining $\tau := \sigma^{p^i}$, then $\tau \in \mathrm{B}_{n-i}(\mathbb{F}_p)$, so we can apply lemma 4.10 to τ to find $\tau_{0,T}$; now define $\sigma_{i,T} := \tau_{0,T}$, and $\sigma^{p^i m} = \tau^m = \tau_{0,m} = \tau_{i,m}$ for each $0 \le m \le p-1$. □

Lemma 4.10. *Let $\sigma \in \mathcal{B}_{n-i}(R_i)$. Then there exists*

$$\sigma_{i,T} \in \mathcal{B}(\mathbb{F}_p t, R_{i+1}[t], R_{i+2}[t], \ldots, R_{n-1}[t])$$

such that $\sigma^m = \sigma_{i,m}$ for each $0 \le m \le p-1$.

Proof. Let $M_i(t) := \prod_{j=0, j\neq i}^{p-1} \frac{t-j}{i-j}$. Then define $\sigma_{0,T} = \sum_{i=0}^{p-1} M_i f^i$. It is now clear that $\sigma_{0,T} \in \mathcal{B}_n(\mathbb{F}_p[t])$, one only needs to see that the first component is of the form $x_1 + t\lambda$ for some $\lambda \in \mathbb{F}_p$. But since the first component of σ is $x_1 + \lambda$ for some λ, and thus σ^m has $x_1 + m\lambda$ as first component, this is exactly the case. □

5 Efficiently exponentiating maximal orbit triangular maps

5.1 Basic idea

In some applications (the next secion is an example) it might be necessary to evaluate $\sigma^a(v)$ for a given $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ of maximal orbit, and $a \in \mathbb{Z}$, $v \in \mathbb{F}_p^n$. Here we explain how to do this most efficiently, with respect to computation and storage space.

First, we find φ and D as given in theorem 2.15: thus $\sigma = D\varphi\Delta\varphi^{-1}D^{-1}$. First, note that because of remark 2.16 it is trivial to compute $\Delta^a(v)$ for any given $v \in \mathbb{F}_p^n, a \in Z$: this part of the computation is negligible. We will consider any addition to be negligible anyway, and simply count the number of multiplications in $\mathbb{F}_p$ are needed. Hence, the evaluation $\sigma^a(v)$ needs

- evaluations $D(v), D^{-1}(v)$,
- evaluations $\varphi(v), \varphi^{-1}(v)$.

The storage of φ does not immediately mean that φ^{-1} is stored (or efficiently computable). However, the following representation solves this:

Definition 5.1. Write $(x_i + g_i)$ for the map $(x_1, \ldots, x_{i-1}, x_i + g_i, x_{i+1}, \ldots, x_n)$. Its inverse is (as can be easily checked) $(x_i - g_i)$.

Note that if $\varphi = (x_1 + g_1, \ldots, x_n + g_n)$ then $\varphi = (x_1 + g_1)(x_2 + g_2) \cdots (x_n + g_n)$. Hence, $\varphi^{-1} = (x_n - g_n)(x_{n-1} - g_{n-1}) \cdots (x_1 - g_1)$. Thus, evaluation of $\varphi^{-1}(v)$ is of the same complexity as $\varphi(v)$, and it is not necessary to store anything extra.

5.2 Storage size

Storage size of a map σ is bounded by the number of different elements in $\mathrm{B}_n(\mathbb{F}_p)$ of maximal orbit. Approximately, this means (see lemma 2.1 part (vi)) that there are $\frac{p^n-1}{p-1}$ coefficients necessary.

If we want to store the useful description above, then one stores D, φ and Δ, which is approximately double of that, i.e. we have to store approximately $2\frac{p^n-1}{p-1}$ coefficients in $\mathbb{F}_p$.

5.3 Efficiency

We need to determine how many multiplications are necessary. Note that the below basic lemma can probably be improved (see for example [1]).

Lemma 5.2. *Let $f \in \mathbb{F}_p[x_1, \ldots, x_k]$ where $k \geq 1$ and $\deg_{x_i}(f) \leq (p-1)$ arbitrary. Then the expected amount of multiplications to evaluate f is $\mathcal{E}[k] := p^{k-1}$.*

Proof. We ignore the one-time computations necessary to evaluate x_i^m for each $m \leq \log_2(p)$. A polynomial $f = \sum_{i=0}^{p-1} f_i x_k^i$ where $f_i \in \mathbb{F}_p[x_1, \ldots, x_{k-1}]$ so we need to evaluate the f_i and for all but f_0 we need to multiply them by x_k^i. This means that $\mathcal{E}[k] = p\mathcal{E}[k-1] - 1$. Since $\mathcal{E}[1] = 0$, this recursive formula comes down to $\mathcal{E}[k] = p^{k-1} - 1$. We ignore the "-1" as we're rounding off some values anyway. □

Lemma 5.3. *If $\varphi \in \mathcal{B}_n(\mathbb{F}_p)$, then evaluation $\varphi(\lambda)$ for some $\lambda \in \mathbb{F}_p^n$ takes approximately $\frac{p^{n-1}-1}{p-1}$ multiplications.*

Proof. If $\sigma = (x_1 + g_1, \ldots, x_n + g_n)$ where $g_i \in R_{i-1}$, then evaluation of σ means evaluationg the g_i. By lemma 5.2, evaluation of g_i $(i \geq 2)$ costs p^{i-2} multiplications. Thus, we have possibly $1 + p + p^2 + \ldots + p^{n-2} = \frac{p^{n-1}-1}{p-1}$ multiplications that have to be done. $\square$

Remark: If $p = 2$, then multiplication is of the same complexity as addition, so the author suspects that the above focus on "amount of multiplications" may be misleading. Nevertheless, we expect that especially the $p = 2$ case is very efficient and can be very useful in applications.

6 A symmetric key cryptographic application: Diffie-Hellmann session-key exchange.

6.1 Introduction

In cryptography, it is often desireable to not use a secret key continuously, but only use the secret key to make session keys. If one session key is broken, then the system is not completely (or completely not) broken, except for that session. The generic protocol (Diffie-Hellmann session key exchange, see [15] p. 513 or [3] p. 145 protocol 5.2) has the following form:

- Alice and Bob share a secret key S, and have a set of parametrized maps ϕ_a which commute, $\phi_a \phi_b = \phi_{ab}$.
- Alice chooses a random value a, and Bob chooses a random value b.
- Alice publicly sends $M_a := \phi_a(S)$, Bob publicly sends $M_b := \phi_b(S)$.
- Alce computes $K := \phi_a(M_b)$, Bob computes $K := \phi_b(M_a)$ and the session key K is established.

In almost all settings the ϕ_a is iteration of a map, i.e. there is a map ϕ and $\phi_a = \phi^a$; commutativity of all ϕ_a, ϕ_b is then automatic. (An exception would be Chebyshev polynomials, for example. Then ϕ_a is the a-th Chebyshev polynomial.) The most common example is in a discrete log session: then ϕ_a is simply exponentiation (and ϕ is multiplication by the base value), i.e. $\phi_a(h) = h^a$. In this case, there is only one map ϕ which is publicly available. In case there are more maps ϕ available, then the choice of map is part of the secret key. The most extreme case is when ϕ can be any permutation (a not very efficient system, as the secret key will be huge).

Any such system needs to satisfy some basic requirements:

- Preferrably, the orbit $\{\phi_a(S) \mid a \in \text{(set of allowed values for } a)\}$ should be the complete set of possible session keys (or in the very least the orbits of ϕ should be large). For if not, then an eavesdropper hearing M_a, M_b might learn in which orbit of ϕ S is, which can be undesireable.

- If one or more session keys are broken, then an attacker knows some triples $(\phi_a(S), \phi_b(S), \phi_{ab}(S))$. It should be not possible to reconstruct S from such triples (or only give away very little) - this can be under the condition of a certain threshold of amount of broken keys.

- It should be feasible to compute $\phi_a(S)$ (and it should take approximately equally long for each a).

In the discrete log setting, the security is based on infeasiblility of the discrete log problem: It is then assumed that if s is the secret key, then sending s^a, s^b gives no information on s, and if a session key $k = s^{ab}$ is broken, then it is assumed that it is an infeasible problem to find s given $M_a = s$, $M_b = s^b$, and $K = s^{ab}$. Note that if one session key is broken, then an attacker does have all *information* on the secret key s (as there is only one solution (s, a, b) of $s^a = M_a, s^b = M_b, s^{ab} = K$). This makes this system not desireable for certain applications, like low-power applications where the discrete log setting has to be small (and hence breakable) in order to be computable for the low-power device. Another case is when the communication involves data that can be sensitive for many years (like medical or governmental data), where one should assume that in the future infeasible computations become feasible.

It is possible to provide alternatives to the discrete log setting, but it is not so easy: the most difficult thing is that one needs commuting maps ϕ_a for which it is easy to compute $\phi_a(s)$, and where $\phi_a(s)$ gives away no information. The work done in the previous sections provides the tools for exactly such a method: here, ϕ_a will be a conjugation of σ^a for some $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$.

6.2 System description

Setup phase: Alice and Bob (or a TTP) choose $n \in \mathbb{N}^*$, p a prime, choose some $v \in \mathbb{F}_p^n$, pick a random $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ of maximal orbit and of standard form, and compute φ, D as in theorem 2.15 so that $\sigma = D^{-1}\varphi^{-1}\Delta\varphi D$.

Additionally, a bijection $\omega : \mathbb{F}_p^n \longrightarrow \mathbb{F}_p^n$ will be chosen.[4] Alice and Bob store $(\omega, \varphi, \Delta, w := \varphi D\omega(v))$ and additionally ω^{-1}, if necessary. (Alice and Bob store $\varphi D\omega(v)$ in stead of v, as v itself is not needed in computations).

The map $\phi = \omega^{-1}\sigma\omega$, and $\phi^a = \omega^{-1}\sigma^a\omega$.

Communication phase: Alice and Bob will now establish a session key.

- Alice chooses a random integer value $a \in [0, p^n - 1]$ and Bob chooses a random integer value $b \in [0, p^n - 1]$.

[4]We don't elaborate on what bijections ω may be chosen - a suggestion is to take a triangular polynomial maps, but conjugated with $(x_n, \ldots, x_1)$, i.e. having variables reversed. Also, depending on the possible choices for ω, one could take $v = 0$ in stead of random.

- Alice publicly sends $M_a := \omega^{-1}D^{-1}\varphi^{-1}\Delta^a(w)$, Bob publicly sends $M_b := \omega^{-1}D^{-1}\varphi^{-1}\Delta^b(w)$.
- Alice computes $K := \omega^{-1}D^{-1}\varphi^{-1}\Delta^a\varphi D\omega M_b$, Bob computes $K := \omega^{-1}D^{-1}\varphi^{-1}\Delta^b\varphi D\omega M_a$. K is the established session key $\omega^{-1}D^{-1}\varphi^{-1}\Delta^{a+b}(w)$.

6.3 Security

In order to make computations on security, we will assume that ω is the identity map - hence the below security computations are only a worst-case bound.

Disclosed information to an eavesdropper: such a person will only hear $\sigma^a(v), \sigma^b(v)$ while not knowing a, b, v and σ. Since σ is of maximal orbit, $\sigma^a(v)$ can be any value in $\mathbb{F}_p^n$, and the same for $\sigma^b(v)$. This hence gives zero information on v, nor on σ, and there is no information even on $\sigma^{a+b}(v)$.

Breaking a session key: If an attacker breaks a session key $K = \sigma^{a+b}(v)$, how much does this reveal from σ and v? So now an attacker hears a triple $(\sigma^a(v), \sigma^b(v), \sigma^{a+b}(v))$. For the attacker, $\sigma^a(v)$ is indistinguishable from a random value w since a is random (and unknown). Hence, such a triple can be seen as a triple $(w, \sigma^b(v), \sigma^b(w))$.

Claim: The information learned by a triple $(u, \sigma^b(v), \sigma^b(u))$ is comparable (or less) to the information learned by a pair $(u, \sigma(u))$.
We will not rigidly prove the claim (as we're unable to!), but indicate why it is reasonable to assume the claim: first, notice that the triple $(u, \sigma^b(v), \sigma^b(u))$ has an additional unknown, namely b. So, intuitively speaking, having three values is equivalent to having two values with one free variable less. Also, notice that $\sigma^b(v)$ itself sounds to the eavesdropper as a random variable (as b is unknown), and that the pair $(u, \sigma^b(u))$ gives less information than a pair $(u, \sigma(u))$.

Lemma 2.17 discusses exactly the information revealed by $(u, \sigma(u))$: for $m \geq 1$ such values, the last $[\log_p(m)] + 1$ coordinates of σ (and hence of $\sigma_{i,T}$ and v) are disclosed while the others are completely unknown. (Notice that if ω is not the identity, this disclosure is spread out over all the coordinate values in a sort of unclear way, depending on the complicatedness of ω.) If one wants to be absolutely sure that the system has a degree of forward security, then one could decide to use only the first so-many coordinate values of $\sigma^{a+b}(v)$. For example, ignoring the last coordinate value gives the system $p-1$-forward security.

6.4 Storage size

Stored is $(\omega, \varphi, \Delta, w)$. Of these, φ and Δ are described in section 5.2, which means $\frac{p^n-1}{p-1}$ coefficients in $\mathbb{F}_p$ for each. Storage size for ω depends on which maps are allowed, our suggestion of using "lower-triangular" permutations amounts to another share of that size.

6.5 Efficiency

The computational tasks Alice has to do, are to do evaluations $\omega(u)$, $\varphi(u)$, $D(u)$, and $\Delta(u)$ for $u \in \mathbb{F}_p^n$. Evaluations $\Delta(u)$ are trivial by remark 2.16, as are evaluations $D(u)$. If we assume ω is a "lower triangular permutation" this amounts to evaluations of order as described in lemma 5.3, i.e. $\frac{p^{n-1}-1}{p-1}$ multiplications. In each session-key establishment each party has to do these evaluations something like 6 times (a fixed finite number of times).

7 Future research

A topic that requires further research is the role of the conjugation map ω in the last section: how should it be chosen such that it hussles up σ^a well enough? We proposed triangular maps in the other order of variables, but is this enough? Or is it enough to simply use a linear or affine map?

Acknowledgements: The author would like to thank some people for discussing the manuscript at some stage in the production: Berry Schoenmakers, David Finston, and Arno van den Essen.

References

[1] Ballico, Edoardo; Elia, Michele; Sala, Massimiliano; *Complexity of multivariate polynomial evaluation* preprint (2011) arXiv:1106.2720v1

[2] Bass, Hyman; Maubach, Stefan; Van Chau, Nguyen; Lecture notes from the International School and Workshop (ICPA2006) held in Hanoi, October 9–20, 2006. Publishing House for Science and Technology, Hanoi, 2007. xii+160 pp.14-06

[3] Boyd, Colin; Mathuria, Anish; Protocols for Authentication and Key Establishment. Springer Verlag, (2003). xxiv, 321 p.

[4] Elliott, Jesse; *Integer-valued polynomials, t-closure, and associated primes.* preprint (2011) arXiv:1105.0142v1

[5] van den Essen, Arno; Polynomial Automorphisms and the Jacobian Conjecture, volume 190 of *Progress in Mathematics*, Birkhäuser (2000)

[6] Freudenburg, Gene; Algebraic theory of locally nilpotent derivations. Encyclopaedia of Mathematical Sciences, 136. Springer-Verlag, Berlin, 2006.

[7] Kaloujnine, Léo; *Sur les p-groupes de Sylow du groupe symtrique du degré* p^m. (French) C. R. Acad. Sci. Paris 221, (1945). 222–224.

[8] Kaloujnine, Léo; *La structure des p-groupes de Sylow des groupes symétriques finis.* (French) Ann. Sci. cole Norm. Sup. (3) 65, (1948). 239–276.

[9] Lucas, Edouard; *Théorie des Fonctions Numériques Simplement Périodiques*, American Journal of Mathematics 1 (1878)

[10] Maubach, Stefan; *Polynomial automorphisms over finite fields.* Serdica Math. J. 27 (2001), no. 4, 343–350.

[11] Maubach, Stefan; Willems, Roel; *Polynomial automorphisms over finite fields: Mimicking non-tame and tame maps by the Derksen group.* preprint (2009), arXiv:0912.3387v1

[12] Maubach, Stefan; Willems, Roel; *Polynomial endomorphisms over finite fields: experimental results.* preprint (2011), arXiv:1103.3363v1

[13] Ostrowski, Alexandre; Pólya, George; *Über ganzwertige Polynome in algebraischen Zahlkörpren*, J. Reine Angew. Math. 149 (1919), 97-1244.

[14] Robinson, Derek J.S.; A Course in the Theory of Groups, Graduate text in mathematics 80 (second edition), Springer verlag

[15] Schneier, Bruce; Applied Cryptography (Second Edition). John Wiley & Sons, 1996