Power Structures in Finite Fields and the Riemann Hypothesis

Alessandro Dallari
ITIS *Leonardo da Vinci*, Carpi (MO) - Italy
alessandro.dallari@istruzione.it

Abstract

Some tools are discussed, in order to build power structures of primitive roots in finite fields for any order q^k; relations between distinct roots are deduced from m- and shift-and-add- sequences. Some heuristic computational techniques, where information in a m- sequence is built from below, are proposed. Full settlement is finally viewed in a physical scenario, where a path leading to the Riemann Hypothesis can be enlighted.

Contents

1 Introduction

Finite fields arise as number-theoretical entities, from initial works by Gauss and Euler; recent applications are in cryptography and coding theory. The main reason for such an interest is due to a trivial additive structure and an almost trivial multiplicative structure, together with a strongly untrivial exponential and logarithmic structure. Characteristic 2 is preferred since it gives a straight binary information; but quasi-randomness is shown by powers in fields $\mathbb{F}_{2^k}$ as well as $\mathbb{F}_{p^k}$ for any prime p and actual complexity seems to grow for higher k's rather than for higher p's.

Such an uncertainty was controlled at first by means of linear recurring sequences (see [12] for a background) and, only at a mature stage (since e.g. Golomb's work [13]), it has been driven to a fully informational machinery, where ordinary tools about (quasi-)randomess have been used and a wide class of similar objects came out: shift-register-, shift-and-add-, pseudo-random-, pseudo-noise- sequences. In recent years (see e.g. [14]), wider extensions reach p-adic structures and abstract vector spaces.

Main attention has been paid insofar to deduce linear sequences from generic primitive elements; the opposite way seems to have been neglected, so a basic

fact is hidden: maximal linear recurring sequences are built together with power structures of primitive elements and the relation comes out to be so close that it seems meaningless to ask *what* builds *whatelse*.

In present article, organization of m-sequences in power tables of primitive elements is explained in complete generality and a "counting everything perspective" is kept throughout each section; as an intermediate goal, it is shown that usual specifications of irreducible polynomials and primitive elements are almost secondary, since they all can be determined top-down by m-sequences and, when fields $\mathbb{F}_{q^l}$ for $q = p^h$ and $h \neq 1$ are not involved, equivalence of m- and shift-and-add- definitions makes a full environment of its own.

Exposition is self-contained as much as possible and many collateral roads (towards e.g. normal bases, autocorrelations or similar subjects) are not taken into account. Section 2 gives basic preliminaries, recalling difficulties in exact computation of multiplicative periods; mail tool to compute complete power structures, Gauss' algorithm, is presented in a matricial form where some significant properties can be easily managed; a remarkable "ferromagnetic" property of ascending sequences is (without proof) led to attention.

In section 3, power structures for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ are built row by row; both m- and shift-and-add- requirements are deduced from two properties, with elementary tools. Full counting of these structures and distinction between q prime or prime power are left to section 5.

Section 4 presents main results: a fixed power structure is always viewed globally as a matrix; organization of m-sequences fo a general finite field $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$ is discussed and theoretical tools of pure linear algebra are required. Framework for x primitive gives a complete account of power tables and their relations, since any power table for a generic α primitive can be built from a table with x primitive using only two tools: (1) Euler-like transformations (usually known as *decimations*) and (2) base change over the whole structure (since complete power structures are stable under such a transformation); a combinatorial exhaustion of power tables for $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$ is given.

Section 5 takes into account subfield relations for $\mathbb{F}_{p^k}$ over any $\mathbb{F}_{p^h}$ with $h|k$. Subject needs some subtleties, since m- vs shift-and-add- properties separate, even if power structures are built only by m-sequences that satisfy shift-and-add-properties; an *interleaving structure* (as defined in [14]) comes out and special representations, where a subfield $\mathbb{F}_{p^h}$ is made stable by a double reduction, can be treated; this allows any chain of stable subfields $\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^{k_1}} \hookrightarrow \ldots \hookrightarrow \mathbb{F}_{\left(\left(p^{k_1}\right)^{\cdots}\right)^{k_l}}$ to be fully defined and enumerated.

Section 6 proposes some heuristic constructions of m-sequences, *ex nihilo* of from linear recurring sequences of lower order. The most interesting property that emergies is self-organizational: sequences in power structures have an upper stability checksum, usually a shift-and-add- condition, that can be evoked als oin any interleaving structure.

As an outcome of ideas collected from anywhere along the article, section 7 enlarges the settlement to physical considerations and proposes informal traces leading to the Riemann Hypothesis.

2 Arithmetic preliminaries about finite fields

2.1 Prime fields $\mathbb{F}_p$

Building blocks of finite Arithmetic are rings $\mathbb{Z}_n$ of integers $\mod n$. Additive structure is trivial: due to associativity law, table $t_{i,j} = i + j \mod n$) is a latin square with consecutively shifted rows and columns: $t_{i+1,j} = t_{i,j+1} \mod n$).

Table of multiplication requires no zero-divisors $a, b \neq 0$ such that $a \cdot b = 0$, in order to have inverses for each non-zero element; this leads to restriction $n = p$ a prime. Multiplication can be fully deduced from power tables, a well-known fact shortly recalled.

Proposition 2.1 *([20], [11]) - Ring $\mathbb{Z}_p$ for p prime is a field; multiplicative group $\mathbb{Z}_p^\times$ is cyclic, that is $\exists a \neq 0, 1$ such that $\left(a^h\right)_{h=1}^{p-1}$ fills all values $1, \ldots, p-1$; this field, unique up to isomorphisms, is denoted $\mathbb{F}_p$.*

The *period* of a non-null element a, defined as the least h such that $a^h = 1$, will be indicated by $\pi(a)$; when $\pi(a) = p - 1$, the element is called a *primitive root*. Much of regularity is given by Euler ϕ-function, defined as:

$$\phi(n) = card\,\{k < n | MCD(k; n) = 1\}$$

and satisfying known properties [20]:

- if $k \nmid n$ then $(n - k) \nmid n$, that is $\phi(n)$ values prime with n are located simmetrically around $\frac{n}{2}$;
- if p is a prime number then $\phi(p^m) = p^m - p^{m-1}$, in particular $\phi(p) = p - 1$;
- ϕ is multiplicative, that is $\phi(hk) = \phi(h)\phi(k)$ whenever $MCD(h; k) = 1$;
- $n = \sum_{d|n} \phi(d)$

Following statement collects various results ([20],[11]) and shows that power structure in $\mathbb{F}_p$ is fully explained by Euler ϕ-function:

Proposition 2.2

1. *let k and k^{-1} be multiplicative inverses; then $\pi(k) = \pi(k^{-1})$ and powers of k^{-1} form the same sequence of k, in the opposite verse;*
2. *multiplicative group $\mathbb{F}_p^\times$ has $\phi(p-1)$ generators; they exchange one eachother in $\phi(p-1)$ exponents relatively primes with $p - 1$;*
3. *periods of non-primitive elements are associated with divisors of $p-1$, for each $d|(p-1)$ there are $\phi(d)$ elements with period d which exchange one eachother in exponents relatively primes with d;*
4. *for $k \in \mathbb{F}_p^\times$ with period $\pi(k)$, powers $k^\alpha, \alpha < \pi(k)$ are occupied either by other elements with period $\pi(k)$ or by elements with lower periods $\rho|\pi(k)$;*

5. *equation* $n = \sum_{d|n} \phi(d)$ *fills all values from* 1 *to* $p-1$ *with periods determined by* ϕ.

So one can face the main obstacle: multiplicative elements in a prime field build up a closed power structure, ruled by characteristic p.

2.2 Location of periods in additive values

A good result would be to write down suddenly (at least) one primitive root; a better result would be to write down all primitive elements; best result would be to give a closed rule for the location of periods in additive values; since 1 is clearly the only element with period 1, such a rule could be reduced to a theorem like

"if k has period α, then $(k+1)$ has period β"

Unfortunately, perfect combinatorics of power tables hardly matches with additive rules and situation expressed e.g. in [18] is: "no useful formula for a primitive root exists" and it isn't really changed.

As soon as one tries to combine multiplicative periods and additive sequence $1, \ldots, p-1$, only a few rules can be summarized.

2.2.1 Computing $\pi(k+1)$ from $\pi(k)$

Proposition 2.3 *Let* $\mathbb{F}_p^\times (p \neq 2)$ *be a a prime field; let* $k \in \mathbb{F}_p^\times$ *be such that* $\pi(k) = 3$, *then* $\pi(k+1) = 6$.

Proof - Let $k^3 = 1\ (mod\ p)$ with $k^2 \neq 1$ so that $k \neq \pm 1$. One has (with all coefficients unreduced):

$$\begin{aligned}(k+1)^6 = k^6 + 6k^5 + 15k^4 + 20k^3 + 15k^2 + 6k^5 + 1 = \\ = 1 + 6k^2 + 15k + 20 + 15k^2 + 6k + 1 = \\ = 21k^2 + 21k + 21 + 1 = 21(k^2 + k + 1) + 1\end{aligned}$$

now, $k^3 - 1 = 0\ (\ mod\ p)$ implies $(k-1)(k^2+k+1) = 0\ (\ mod\ p)$ that is $(k^2+k+1) = 0\ (mod\ p)$ due to integrity property; thus

$$21(k^2 + k + 1) + 1 = 1 \mod p$$

that is, element $k+1$ has period $1, 2, 3$ or 6. But $1, 2$ are impossible and

$$(k+1)^3 = 1 + 3k^2 + 3k + 1 = 3k^2 + 3k + 3 - 1 = 3(k^2 + k + 1) - 1 = -1$$

is a contradiction; thus $\pi(k) = 6$. $\diamond$

Complexity in higher periods is due to crossed relations between binomial coefficients and characteristic p, so the study of these values might be a world apart. Global location rule for elements with fixed periods undergoes combinatoral rules but, on the surface, a substantial randomness appears.

2.2.2 Periods of opposite additive values

A more readable property ties periods of opposite additive values $\pm k$ and it is nothing but an easy case of periods for a primitive polynomial (see [20]).

Proposition 2.4 *1. If $2 \nmid \pi(k)$ then $\pi(-k) = 2\pi(k)$, so $\pi(-k)$ has factor 2 just once;*

2. if $2|\pi(k)$ and $4 \nmid \pi(k)$ then $\pi(k) = 2\pi(-k)$;

3. if $4|\pi(k)$ then $\pi(-k) = \pi(k)$.

Proof -

1. Let $\pi(k) = \alpha$ be odd; then $(-k)^\alpha = (-1)^\alpha k^\alpha = -1$ and, by squaring, $(-k)^{2\alpha} = 1$ so $(-k)$ has period 2α.

2. Let $\pi(k) = \alpha = 2\beta$ with β odd; then $(-k)^\alpha = (-1)^\alpha k^\alpha = k^\alpha = 1$ and $\left(k^\beta\right)^2 = 1$, so $k^\beta = -1$ and $(-k)^\beta = (-1)^\beta k^\beta = (-1)^2 = 1$.

3. let $\pi(k) = \alpha = 4\beta$; then $(-k)^{4\alpha} = (-1)^{4\alpha} k^{4\alpha} = 1$ so $\pi(-k) \leq 4\beta$; but $\pi(-k) = 2\beta$ implies $(-k)^{2\beta} = (-1)^{2\beta} k^{2\beta} = 1$, a contradiction, and $\pi(-k) = 4\gamma$ for any $\gamma|\beta$ implies $(-k)^{4\gamma} = k^{4\gamma} = 1$, a contradiction; thus, $\pi(-k) \not< 4\beta$ and $\pi(-k) = 4\beta$. $\diamond$

This property gives a partition of periods around $\frac{p-1}{2}$ and it is worth to note the difference between a symmetric (opposite elements with period divisible by 4) and an anti-symmetric case (periods divisible only by 2).

2.3 Gauss' algorithm through iterated global sums

Since no pre-defined way is known to access a primitive element, it can be reached from below, given an initial element $a \neq 0, 1$. Gauss' algorithm is the best possible way to target such an element, starting from a random entry.

Gauss' algorithm [24]: given a multiplicative element $a \neq 0, 1$ of a finite field $\mathbb{Z}_p$ such that $\pi(a) \neq p - 1$, choose an element $b \neq a^i$ whose period $\pi(b)$ is not a divisor of $\pi(a)$; choose a decomposition $mn = mcm(\pi(a); \pi(b))$ such that $MCD(\pi(a); \pi(b)) = 1, m|\pi(a), n|\pi(b)$; then element $a^{\pi(a)/m} b^{\pi(b)/n}$ has period $mcm(\pi(a); \pi(b))$, so an higher period has been found.

Gauss' algorithm may look a bit obscure, but it can be easily computed through an iterated application of global sums or differences, where decomposition mn (a strange request, at a first glance) is a direct outcome of the following algorithm.

Let a non-primitive element a be given, with period $\pi(a) \neq (p - 1)$; write

down all its powers in column:

$$\left[\begin{array}{l} 1 \\ a \\ a^2 \\ \vdots \\ a^{\pi(a)-1} \\ (a^{\pi(a)}=1) \end{array}\right]$$

since a is non-primitive, not all sums $a^i \pm 1$ give some a^j; in fact, primitivity is equivalent to

$$\forall i \forall j \exists h \exists l (a^i + a^j = a^h \wedge a^i - a^j = a^l)$$

Choose $b = a^i \pm 1 \neq a^j$ and build subsequent columns, each with iterated multiplication by a (in column) and b (in row), up to the first value $b^\mu = a^\lambda$, clearly satisfying $MCD(\lambda; \mu) = 1$:

$$\left[\begin{array}{llll} 1 & b = a^i \pm 1 & b^2 & \ldots \quad b^\mu = a^\lambda \\ a & b \cdot a & b^2 \cdot a & \\ a^2 & b \cdot a^2 & b^2 \cdot a^2 & \\ \vdots & \vdots & \vdots & \\ a^{\pi(a)-1} & & & \\ (a^{\pi(a)}=1) & & & \end{array}\right]$$

Value b extends $\pi(a)$ and an element with period $\pi(a)\mu$ can be found by a suitable visit of this $\pi(a) \times \mu$ matrix. In fact, last column is a copy of the first one, maybe with some vertical shift; candidate element with higher period belongs to second column and is of the form $b \cdot a^l$, for some l expressing vertical jump across consecutive columns. Actually, subsequent powers $1, (b \cdot a^l), (b \cdot a^l)^2$ reach last column in a value $(b \cdot a^l)^\mu = a^{\lambda + l\mu}$ and correct requirement is relative primality with $\pi(a)$, for otherwise some values in the matrix would be excluded. Thus, higher periods $\pi(a) \cdot \mu$ are associated to each value $b \cdot a^l$ such that $MCD(\pi(a); \lambda + l\mu) = 1$.

If such an element is not primitive, another extension can be performed, and so on.

This tabular algorithm makes clear that any sequence of powers of a non-primitive element has a weak inner stability and reaches a stronger (maybe maximum) stability when it is perturbed by a global sum/difference and mixed with such a perturbation. Thus, global property of primitive elements can also be viewed as a complete stability of their power sequence under global additive operations, a fact that gives some relevance to the following property, maybe elementary but proper of a primitive element:

$$\forall i \forall k \exists h, h' \left(a^{i+k} + a^i = a^{i+h}, a^{i+k} - a^i = a^{i+h'} \right)$$

Previous realization of Gauss' algorithm, together with considerations about stability under global sum oeprations, will be widely applied to higher fields in subsequent chapters.

2.4 Finite fields $\mathbb{F}_{p^k}$ for $k > 1$

If a finite field with cardinality not a prime is required, only cardinalities p^k, powers of a prime, can be accepted. Euler ϕ-function is yet important. General properties about orders p^k for $k > 1$ are collected in the following statement.

Proposition 2.5 *[20]*

- *A finite product $\mathbb{F}_p \times \ldots \times \mathbb{F}_p = \mathbb{F}_{p^k}$ (k times) is a field under multiplication modulo an irreducible polynomial $P_k(x) = x^k + a_{k-1}x^{k-1} + \ldots + a_0$ of degree k.*
- *both additive and multiplicative structures are unique up to isomorphisms, so this field can be referred to as $\mathbb{F}_{p^k}$*
- *multiplicative group $\mathbb{F}_{p^k}^{\times}$ has $\phi(p^k - 1)$ generators; they exchange one eachother in $\phi(p^k - 1)$ exponents relatively primes with $p^k - 1$;*
- *periods of non-primitive elements are associated with divisors of $p^k - 1$ and follow the same rules as for $\mathbb{F}_p$*
- *$\mathbb{F}_{p^h}$ is a subfield of $\mathbb{F}_{p^k}$ if and only if $h|k$.*

Following property, absolutely non-trivial (note that e.g. $k \nmid (p^k - 1)$ happens very often) holds:

Proposition 2.6 *One has $k|\phi(p^k - 1)$ $\forall p$ prime, $\forall k > 1$.*

Proof A, enumerative - Powers p^i, $0 \leq i \leq k-1$, are all relatively prime with $p^k - 1$ and values d counted by $\phi\left(p^k - 1\right)$ are partitioned in equivalence classes by relation $d \sim d' \leftrightarrow d' = dp^h$ for some h.

Proof B, combinatorial - Values counted by $\phi(p^k - 1)$ are equally distributed in intervals

$$I_h = \left[\frac{h-1}{k}(p^k - 1) \ldots \frac{h}{k}(p^k - 1) \right[$$

for $h = 1, \ldots, k$. Once one has some care of boundaries, this is a deep application of Inclusion-Exclusion Principle (see [28]). Given ordinary factorization $\left(p^k - 1\right) = p_1^{\alpha_1} \ldots p_l^{\alpha_l}$, build sets

$$A_{j,h} = \{ip_j | i \in N\} \cap I_h \quad , \quad j = 1..l$$

and follow standard notation

$$T \subseteq \{1..l\} \quad , \quad A_{T,h} = \cap_{i \in T} A_{i,h} \quad , \quad S_m = \sum_{|T|=m} |A_{T,h}| \quad ;$$

then, distinct countings

$$\sharp \left(\overline{A_{1,h}} \cap \ldots \cap \overline{A_{l,h}} \right) = S_0 - S_1 + \ldots + (-1^l) S_l$$

cancel the same number of naturals in each interval. $\diamond$

2.5 An extra-property: number of ascending sequences

A remarkable property, that seems yet unproved, comes from counting sequences of monotone values, a phœnonenon that shows an extreme regularity.

Definition 2.1 *An ascending sequence is a maximal sequence of monotone powers $\beta^i < \beta^{i+1} < \ldots < \beta^{i+j}$ (in usual ordering of $\mathbb{N}$) such that $\beta^{i-1} > \beta^i$ and $\beta^{i+j+1} < \beta^{i+j}$.*

Location of value 1 seems ambiguous but, without contradiction, it could be placed either at the beginning (then, initial 1 means power a^0) or at the end (then, final 1 has to be discarded). Following regularity appears:

Proposition 2.7 *Let any list of powers $(1); k; k^2; \ldots; (k^{\pi(k)} = 1)$ be segmented in ascending sequences; then, from known examples,*

- *powers of primitive elements in $\mathbb{F}_p$ tend to be organized in $\frac{p-1}{2}$ monotone sequences;*
- *if k is not primitive and $a(k)$ is the number of monotone sequences in its power structure, one has*

$$\pi(k) = a(k) + a(k^{-1}) = \pi(k^{-1})$$

as it is shown in table 1 for $\mathbb{F}_{13}$.

	1	2	3	4	5	6	7	8	9	10	11	12
1	(1)											
2	2	4	8 ‖	3	6	12 ‖	11 ‖	9 ‖	5	10 ‖	7 ‖	(1)
3	3	9 ‖	(1)									
4	4	3	12 ‖	9	10 ‖	(1)						
5	5	12 ‖	10 ‖	(1)								
6	6	10 ‖	8	9 ‖	2	12 ‖	7 ‖	3	5 ‖	4	11 ‖	(1)
7	7	10 ‖	5	9	11	12 ‖	6 ‖	3	8 ‖	4 ‖	2 ‖	(1)
8	8	12 ‖	5 ‖	1								
9	9 ‖	3 ‖	(1)									
10	10 ‖	9	12 ‖	3	4 ‖	(1)						
11	11 ‖	4	5 ‖	3	7	12 ‖	2	9 ‖	8	10 ‖	6 ‖	(1)
12	12 ‖	(1)										

Table 1: ascending sequences *mod* 13

Ascending sequences give an addictional regularity, since this counting could be afforded by means of strict combinatorial considerations: find a partition of values $1, \ldots, p-1$ satisfying above combinatorics, together with all subsequences derived from Euler ϕ-function.

3 Power structures for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$: row-by-row construction

In present section, full details for power structures in fields $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^3}$ are given, together with an effective generalization to $\mathbb{F}_{q^k}$ generic. As a remarkable feature, machinery of linear recurring sequences is not needed to prove two general properties, always satisfied by any complete power structure.

3.1 General properties: non-nullity and permanence

Given a non-null element $\alpha \in \mathbb{F}_{q^k}^{\times}$, multiplication by α can be performed in a matricial form $\alpha^{h+1} = \alpha^h B(\alpha)$ whose entries $\alpha_{i,j}$ satisfy a recursive rule where a given irreducible polynomial $x^k \equiv a_0 + a_1 x + \ldots + a_{k-1}x^{k-1}$, irreducible over $\mathbb{F}_{q^k}$, appears:

$$\begin{aligned} \alpha_{0,j} &= \alpha_j^1 \\ \alpha_{i,j} &= \alpha_{i-1,j-1} + \alpha_{i-1,k-1}a_i \end{aligned}$$

Any power structure satisfies properties focused in following lemmas, where cases $k = 2, 3$ and $k > 3$ are distinguished for practical reasons.

3.1.1 Fields $\mathbb{F}_{q^2}$

Lemma 3.1 ***(Non-nullity)*** *- With notation as above, let $\alpha^h = \alpha_0^h + \alpha_1^h x$ be h-th power of α and $\left(\alpha_j^h\right)_h$ be the sequence of values for a fixed component $j = 0, 1$; if $\alpha_j^{h+i} = 0$ for two consecutive values $i = 0, 1$ then initial assumptions fail (that is, choosen polynomial is reducible or α has a null power) or the sequence $\left(\alpha_j^h\right)_h$ is everywhere null.*

Proof - Assume $\alpha_0^{h+i} = 0$ for $i = 0, 1$; then $\alpha_0^{h+1} = \left(\alpha_0^h; \alpha_1^h\right) \cdot (\alpha_{0,0}; \alpha_{1,0}) = \alpha_1^h \alpha_1^1 a_0 = 0$ means either $\alpha_1^h = 0$ and $\alpha^h \equiv 0$, a contradiction, or $\alpha_1^1 = 0$ and $\alpha \in \mathbb{F}_q$, a contradiction, or $a_0 = 0$ and choosen polynomial is reducible, a contradiction.

Assume $\alpha_1^{h+i} = 0$ for $i = 0, 1$; then $\alpha_1^{h+1} = \left(\alpha_0^h; \alpha_1^h\right) \cdot (\alpha_{0,1}; \alpha_{1,1}) = \alpha_0^h \alpha_1^1$ means either $\alpha_0^h = 0$ and $\alpha^h \equiv 0$, a contradiction, or $\alpha_1^1 = 0$ and $\alpha \in \mathbb{F}_q$, a contradiction. $\diamond$

Nullity of whole sequence $\left(\alpha_j^h\right)_h$ for $k > 2$ seems to be the deepest property, even if for $k = 2$ it is obvious:

- for $j = 0$:

$$\alpha_0^{h+2} = \left(\alpha_0^{h+1}; \alpha_1^{h+1}\right) \cdot (\alpha_{0,0}; \alpha_{1,0}) = \left(\alpha_1^h \alpha_{0,1} a_0\right) \alpha_{0,1} a_0 = 0$$

since $\alpha_1^h \alpha_{0,1} a_0 = \alpha_0^{h+1} = 0$;

- for $j = 1$:

$$\alpha_1^{h+2} = \left(\alpha_0^{h+1}; \alpha_1^{h+1}\right) \cdot (\alpha_{0,1}; \alpha_{1,1}) = \left(\alpha_0^h \alpha_{0,0}\right) \alpha_{0,1} = 0$$

since $\alpha_0^h \alpha_{0,1} = \alpha_1^{h+1} = 0$.

A sequence everywhere null occurs in special conditions, namely it is impossible when both q is prime and no subfield representation is stabilized. This case will be examined in chapter 5

Lemma 3.2 ***Permanence*** *- With notation as above, let $\alpha^h, \alpha^{h'}$ be distinct powers such that $\alpha_0^{h+i} = \alpha_1^{h'+i}$ for $i = 0, 1$; then $\alpha_0^{h+2} = \alpha_1^{h'+2}$.*

Proof - Condition $\alpha_0^{h+1} = \alpha_1^{h'+1}$, rewritten with substitution $\alpha_0^h = \alpha_1^{h'}$, means

$$\left(\alpha_1^{h'}; \alpha_1^h\right) \cdot (\alpha_{0,0}; \alpha_{1,0}) = \left(\alpha_0^{h'}; \alpha_1^{h'}\right) \cdot (\alpha_{0,1}; \alpha_{1,1})$$

and term $\alpha_1^{h'} \alpha_{0,0}$ can be reduced:

$$\left(\alpha_1^{h'}; \alpha_1^h\right) \cdot (0; \alpha_{1,0}) = \left(\alpha_0^{h'}; \alpha_1^{h'}\right) \cdot (\alpha_{0,1}; \alpha_{0,1} a_1)\,;$$

value

$$\alpha_0^{h+2} = \left(\alpha_0^{h+1}; \alpha_1^{h+1}\right) \cdot (\alpha_{0,0}; \alpha_{1,0}) = \left(\alpha_1^{h'+1}; \alpha_1^{h+1}\right) \cdot (\alpha_{0,0}; \alpha_{1,0})$$

can be further developed as

$$\left(\alpha_0^h; \alpha_1^h\right) \cdot B(\alpha) \begin{pmatrix} \alpha_{0,0} \\ \alpha_{1,0} \end{pmatrix} = \left(\alpha_1^{h'}; \alpha_1^h\right) \cdot B(\alpha) \begin{pmatrix} \alpha_{0,0} \\ \alpha_{1,0} \end{pmatrix}$$

Now, comparison

$$\alpha_0^{h+2} = \left(\alpha_0^{h+1}; \alpha_1^{h+1}\right) \cdot (\alpha_{0,0}; \alpha_{1,0}) \overset{?}{\leftrightarrow} \left(\alpha_0^{h'+1}; \alpha_1^{h'+1}\right) \cdot (\alpha_{0,1}; \alpha_{1,1}) = \alpha_1^{h'+2}$$

can be reduced:

$$\left(\alpha_1^{h'+1}; \alpha_1^{h+1}\right) \cdot (0; \alpha_{1,0}) \overset{?}{\leftrightarrow} \left(\alpha_0^{h'+1}; \alpha_1^{h'+1}\right) \cdot (\alpha_{0,1}; \alpha_{0,1} a_1)$$

$$\left(\alpha_0^h; \alpha_1^h\right) \cdot (\alpha_{0,1}; \alpha_{1,1})\, \alpha_{1,0} \overset{?}{\leftrightarrow} \left(\alpha_0^{h'+1}; \alpha_1^{h'+1}\right) \cdot (\alpha_{0,1}; \alpha_{0,1} a_1)$$

$$\left(\alpha_1^{h'}; \alpha_1^h\right) \cdot (\alpha_{0,1}; \alpha_{1,1})\, \alpha_{1,0} \overset{?}{\leftrightarrow} \left(\alpha_0^{h'+1}; \alpha_1^{h'+1}\right) \cdot (\alpha_{0,1}; \alpha_{0,1} a_1)$$

and $\alpha_1^h \alpha_{1,0}$ can be translated:

$$\left(\alpha_1^{h'} \alpha_{1,0}; \left(\alpha_0^{h'}; \alpha_1^{h'}\right) \cdot (\alpha_{0,1}; \alpha_{0,1} a_1)\right) (\alpha_{0,1}; \alpha_{1,1})\, \alpha_{1,0} \overset{?}{\leftrightarrow} \left(\alpha_0^{h'}; \alpha_1^{h'}\right) \cdot B(\alpha) \cdot (\alpha_{0,1}; \alpha_{0,1} a_1)$$

where two members are the same, since

$$\alpha_0^{h'} \alpha_{0,1} \alpha_{1,1} = \alpha_0^{h'} \alpha_{0,1} (\alpha_{0,0} + \alpha_{0,1} a_1) \diamond$$

3.1.2 Fields $\mathbb{F}_{q^3}$

Computations for fields $\mathbb{F}_{q^3}$ make a wider structure to appear.

Lemma 3.3 ***(Non-nullity)*** *- With notation as above, let $\alpha^h = \alpha_0^h + \alpha_1^h x + \alpha_2^h x^2$ be h-th power of α and $\left(\alpha_0^h\right)_h$ be the sequence of values for fixed component $j = 0$; if $\alpha_j^{h+i} = 0$ for a fixed $j = 0, 1, 2$ and three consecutive values $i = 0, 1, 2$ then $\alpha_j^{h+3} = 0$ and the sequence $\left(\alpha_j^h\right)_h$ is everywhere null.*

Proof

- Fix $j = 0$; then $\alpha_0^{h+1} = 0$ means a reduction

$$\hat{\alpha}_0^{h+1} = \alpha_1^h \alpha_{1,0} + \alpha_2^h \alpha_{2,0} = 0$$

and analogous $\alpha_0^{h+2} = 0$ means

$$\hat{\alpha}_0^{h+2} = \alpha_1^h \left(\alpha_{1,1}\alpha_{1,0} + \alpha_{1,2}\alpha_{2,0}\right) + \alpha_2^h \left(\alpha_{2,1}\alpha_{1,0} + \alpha_{2,2}\alpha_{2,0}\right) = 0$$

that is, first index 0 can always be omitted. Each of these reductions can be used to rewrite α_0^{h+3} as a combination $\alpha_1^h \beta_{1,0} + \alpha_2^h \beta_{2,0}$ where

$$\beta_{l,0} = \sum_{m_1, m_2 \neq 0} \alpha_{l,m_1} \alpha_{m_1,m_2} \alpha_{m_2,0}$$

now, top-down from $\hat{\alpha}_0^{h+2}$, following combinations can be cancelled:

$$\begin{aligned}
\hat{\alpha}_0^{h+2}\alpha_{1,1} &= \alpha_1^h \left(\alpha_{1,1}\alpha_{1,0}\alpha_{1,1} + \alpha_{1,2}\alpha_{2,0}\alpha_{1,1}\right) + \\
&\quad + \alpha_2^h \left(\alpha_{2,1}\alpha_{1,0}\alpha_{1,1} + \alpha_{2,2}\alpha_{2,0}\alpha_{1,1}\right) \\
\hat{\alpha}_0^{h+2}\alpha_{2,2} &= \alpha_1^h \left(\alpha_{1,1}\alpha_{1,0}\alpha_{2,2} + \alpha_{1,2}\alpha_{2,0}\alpha_{2,2}\right) + \\
&\quad + \alpha_2^h \left(\alpha_{2,1}\alpha_{1,0}\alpha_{2,2} + \alpha_{2,2}\alpha_{2,0}\alpha_{2,2}\right) \\
\hat{\alpha}_0^{h+1}\left(\alpha_{1,2}\alpha_{2,1}\right) &= \alpha_1^h \left(\alpha_{1,0}\alpha_{1,2}\alpha_{2,1}\right) + \alpha_2^h \left(\alpha_{2,0}\alpha_{1,2}\alpha_{2,1}\right) \\
\hat{\alpha}_0^{h+1}\left(-\alpha_{1,1}\alpha_{2,2}\right) &= \alpha_1^h \left(-\alpha_{1,0}\alpha_{1,1}\alpha_{2,2}\right) + \alpha_2^h \left(-\alpha_{2,0}\alpha_{1,1}\alpha_{2,2}\right)
\end{aligned}$$

and all terms reduce one each other, giving

$$\alpha_0^{h+3} = \hat{\alpha}_0^{h+2}\left(\alpha_{1,1} + \alpha_{2,2}\right) + \hat{\alpha}_0^{h+1}\left(\alpha_{1,2}\alpha_{2,1} - \alpha_{1,1}\alpha_{2,2}\right) = 0$$

- Fix $j = 1$ to obtain analogous reduction

$$\alpha_1^{h+3} = \hat{\alpha}_1^{h+2}\left(\alpha_{0,0} + \alpha_{2,2}\right) + \hat{\alpha}_1^{h+1}\left(\alpha_{0,2}\alpha_{2,0} - \alpha_{0,0}\alpha_{2,2}\right)$$

- Fix $j = 2$ to obtain analogous reduction

$$\alpha_2^{h+3} = \hat{\alpha}_2^{h+2}\left(\alpha_{0,0} + \alpha_{1,1}\right) + \hat{\alpha}_0^{h+1}\left(\alpha_{0,1}\alpha_{1,0} - \alpha_{0,0}\alpha_{1,1}\right) = 0 \diamond$$

The same machinery can be applied to permanence property.

Lemma 3.4 ***Permanence*** *- With notation as above, let $\alpha^h, \alpha^{h'}$ be distinct powers such that $\alpha_j^{h+i} = \alpha_{j'}^{h'+i}$ for $i = 0, 1, 2$; then $\alpha_j^{h+3} = \alpha_{j'}^{h'+3}$.*

Proof - Fix e.g. $\alpha_0^{h+i} = \alpha_2^{h'+i}$. As for non-nullity, $\alpha_0^h = \alpha_2^{h'}$ can be directly used in $\alpha_0^{h+1} = \alpha_2^{h'+1}$, giving a translation of

$$\alpha_0^h \alpha_{0,0} + \alpha_2^h \alpha_{2,0} = \alpha_0^{h'} \alpha_{0,2} + \alpha_1^{h'} \alpha_{1,2} + \alpha_2^{h'} (\alpha_{2,2} - \alpha_{0,0})$$

where the main ratio of permanence appears: linear combinations, as for non-nullity, are used not to be put $= 0$, but to transfer combination of coefficients $\alpha_{l,m}$ from $i = 0$ to $i' = 2$; indeed, $\alpha_0^{h+2} = \alpha_2^{h'+2}$, after reduction of previously translated terms, gives a translation of $\alpha_1^h \beta_{1,0} + \alpha_2^h \beta_{2,0}$ above. Since $\hat{\alpha}_0^{h+1}$ and $\hat{\alpha}_0^{h+2}$ can be translated, one can write down *all* terms of α_0^{h+3} and look at a translation

$$\alpha_0^{h+3} = \hat{\alpha}_0^{h+2} (\alpha_{0,0} + \alpha_{1,1} + \alpha_{2,2}) + \hat{\alpha}_0^{h+1} \left(\alpha_{0,0}^2 + \alpha_{0,1}\alpha_{1,0} + \alpha_{0,2}\alpha_{2,0} + \alpha_{1,2}\alpha_{2,1} - \alpha_{1,1}\alpha_{2,2}\right)$$

where, by direct computation (details omitted), terms in index h' can be exactly ricomposed to have $\alpha_2^{h'+3}$. A purely combinatorial rule appears, to be discussed in next subsection; direct computations for all cases in $\mathbb{F}_{q^3}$ give a general rule for translation:

$$\alpha_j^{h+3} = \hat{\alpha}_j^{h+2} (\alpha_{0,0} + \alpha_{1,1} + \alpha_{2,2}) + \\ + \alpha_j^{h+1} \left(\alpha_{j,j}^2 + \alpha_{0,1}\alpha_{1,0} + \alpha_{0,2}\alpha_{2,0} + \alpha_{1,2}\alpha_{2,1} - \alpha_{l\neq j, l\neq j}\alpha_{m\notin\{j,l\}, m\notin\{j,l\}}\right)$$

so permanence holds. $\diamond$

One can note following properties:

- rule for translation $\alpha_j^{h+i} \to \alpha_{j'}^{h'+i}$ relies only upon initial index j, since nested translations adjust dependence upon j';
- no distiction between $j <> j'$ matters, since translation depends on middle indexes of terms $\alpha_{l,m}$;
- non-nullity rule uses the same operations amongst $\alpha_{l,m}$, but $l, m = j$ are canceled.

3.1.3 Extension to general $\mathbb{F}_{q^k}$

Non-nullity and permanence are low-level properties and can be treated by means of a pure combinatorics of indexes, often an application of inclusion-exclusion principle.

Theorem 3.1 *Let $\alpha \in \mathbb{F}_{q^k}^{\times}$ be a non-null element of period $\pi(\alpha) > k$; then, with notation as above, non-nullity and permanence hold:*

- *for any h, j fixed, $\alpha_j^{h+i} = 0$ for $0 \leq i \leq k-1$ implies $\alpha_j^{h+k} = 0$;*

- *for any* h, h', j, j' *fixed,* $\alpha_j^{h+i} = \alpha_{j'}^{h'+i}$ *for* $0 \leq i \leq k-1$ *implies* $\alpha_j^{h+k} = \alpha_{j'}^{h'+k}$

Proof, sketch - About non-nullity. Let $\alpha_j^{h+i} = 0$ for $0 \leq i \leq k-1$; then a linear decomposition $\alpha_j^{h+i} = \sum_{l \neq j} \alpha_l^h \beta_{l,j}^{(i)}$ holds, where

$$\beta_{l,j}^{(i)} = \sum_{l_1, \ldots l_{i-1} \neq j} \alpha_{l,l_1} \alpha_{l_1, l_2 \ldots \alpha_{l_{i-1},j}}.$$

Now, $\alpha_j^{h+k} = \sum_{l \neq j} \alpha_l^h \beta_{l,j}^{(k)}$ can be written as a linear combination

$$\alpha_j^{h+k} = \alpha_j^{h+k-1} \gamma_{k-1,j} + \ldots + \alpha_j^h \gamma_{0,j}$$

where coefficients $\gamma_{l,j}$ are top-down determined as follows:

step 1.1 **-** terms $\alpha_{l,l}^{k-1} \alpha_{l,j}$ can be canceled, as a first choice, with $\alpha_{l,l} \left(\alpha_{l,l}^{k-2} \alpha_{l,j} \right)$ belonging to α_j^{h+k-2}, so $\gamma_{k-1,j} = \sum_{l \neq j} \alpha_{l,l}$ is applied;

steps $1.2 \ldots 1.k-1$ **-** for decreasing i's, each α_j^{h+i} cancels a maximum term given by cyclic indexes

$$\gamma_{i,j} = \sum_{\substack{l_1, \ldots, l_{k-i} \neq j, \\ l_m \text{all distinct}}} \alpha_{l_1,l_2} \alpha_{l_2,l_3} \ldots \alpha_{l_{k-i},l_1}$$

up to α_j^{h+1}, when initial α_j^{h+k} is canceled; e.g. all terms in α_1^{h+4} are canceled by

$$-\alpha_1^{h+3} (\alpha_{0,0} + \alpha_{2,2} + \alpha_{3,3}) - \alpha_1^{h+2} (\alpha_{0,2}\alpha_{2,0} + \alpha_{0,3}\alpha_{3,0} + \alpha_{2,3}\alpha_{3,2}) + \\ -\alpha_1^{h+1} (\alpha_{0,2}\alpha_{2,3}\alpha_{3,0} + \alpha_{0,3}\alpha_{3,2}\alpha_{2,0})$$

steps $2.1 \ldots 2.k-2$ **-** terms with minus sign appear, from α_j^{h+k-1} downto α_j^{h+1}, and terms remaining in α_j^{h+k-1} can be canceled by terms with opposite sign, from α_j^{h+k-2} downto α_j^{h+1}; e.g. terms remaining in α_1^{h+3} can be canceled by

$$\alpha_1^{h+2} (\alpha_{0,0}\alpha_{2,2} + \alpha_{0,0}\alpha_{3,3} + \alpha_{2,2}\alpha_{3,3}) + \\ +\alpha_1^{h+1} (\alpha_{0,2}\alpha_{2,0}\alpha_{3,3} + \alpha_{0,3}\alpha_{3,0}\alpha_{2,2} + \alpha_{2,3}\alpha_{3,2}\alpha_{0,0})$$

where indexes are partitioned in two disjoint sets;

step $i.j$ at each step, a larger partition of indexes is applied; this is a purely combinatorial property and reduces each term to lower ones, with alternate signs;

step $k-1.1$ last cancelation involves $(-1)^{k-1}\,\alpha_j^{h+1}\left(\prod_{l\neq j}\alpha_{l,l}\right)$, e.g. in previous example $-\alpha_1^{h+1}\,(\alpha_{0,0}\alpha_{2,2}\alpha_{3,3})$

About permanence. Each condition $\alpha_j^{h+i}=\alpha_{j'}^{h'+i}$ for $0\leq i\leq k-1$ translates components from h to h'; translation actually gives the same effect as non-nullity and has a combinatorial nature, so its rule depends only upon initial index j.

3.2 Passing to m- and shift-and-add- sequences

Previous results show that main properties about power structures have to be red in sequences of components and in relations between them; this leads in a natural way to ordinary treatement of linear sequences, discussed in next section. It can be useful to remark that basic properties of m- and shift-and-add-sequences follow in a natural way from non-nullity and permanence.

Theorem 3.2 *Let $\alpha\in\mathbb{F}_{q^k}$ for be a generic non-null element and let $S=\left[\alpha_j^h\right]_{i,j}$ be the matrix of its power structure, where each column is viewed as a closed sequence; then*

1. *if α is not primitive, each column of S is made of $\pi(\alpha)$ concatenated non-null k-tuples that form either equal (but shifted) or disjoint sequences, according to the existence (or not) of a fixed k-tuple in different columns;*

2. *if α is primitive, columns of S are equal but shifted and are made of one and the same concatenation of all q^k-1 non-null k-tuples; in this case, the sequence s corresponding to one (thus all) of the columns is a shift-and-add- sequence.*

Proof

1. follows directly from previous results;

2. shift-and-add- or shift-and-subtract- properties

$$\forall i\forall k\exists h\exists h'\left(\alpha^{i+k}+\alpha^i=\alpha^{i+h},\alpha^{i+k}-\alpha^i=\alpha^{i+h'}\right)$$

are implied by primitivity: q^k-1 concatenated places must be occupied by all q^k-1 non-null k-tuples since, otherwise, two locations of the same k-tuple starting from $\alpha_j^h,\alpha_j^{h'}$ would give an element $\alpha^l=\alpha^h-\alpha^{h'}$ (which surely exists) where null k-tuple starts, a contradiction $\diamond$

Symmetries in power structures can be deduced by basic properties of irreducible polynomials.

3.3 Some enumerations

Complete power structures show four obvious symmetries, combined by inversion of components and inversion of recyprocal polynomials

$$(x_0; \ldots; x_{k-1}) \longleftrightarrow (t_{k-1}; \ldots; t_0)$$

$$\begin{aligned} x^k &\equiv a_0 + a_1 x + \ldots + a_{k-1} x^{k-1} \\ 1 &\equiv a_0 t^k + a_1 t^{k-1} + \ldots + a_{k-1} t \\ t^k &\equiv a_0^{-1} - a_1 a_0^{-1} t - \ldots - a_{k-1} a_0^{-1} t^{k-1} \end{aligned}$$

with substitutions

$$\begin{aligned} a'_0 &= a_0^{-1} \\ a'_l &= -a_{k-l} a_0^{-1} \text{ for } 1 \leq l \leq k-1 \end{aligned}$$

One may ask whether enumeration of relative shifts amongst maximal sequences equals counting of irreducible polynomials times number of primitive elements in a field representation, that is

$$N_q(k)\, \phi\left(q^k - 1\right) = \frac{\phi\left(q^k - 1\right)}{k} \sum_{d|q} \mu(d)\, q^{k/d}$$

Without deeper considerations, a trivial result can be stated for $q^k = p^2$, since all possible choices for 1 are p and possible choices for 0 are $p-1$; thus, power structures for $\mathbb{F}_{p^2}$ simply come out from each relative shift between two instances of the same shift-and-add-sequence, giving element "10" in some place:

$$\frac{1}{2}\left[\mu(1)p^2 + \mu(2)p\right] \phi(p^2 - 1) = \frac{p^2 - p}{2}(p^2 - 1)$$

Exact counting will be proved in section 4 to hold for a general $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$ and only in section 5 it will be sketched for a general subfield relation.

Note that, for a choosen relative shift amongst maximal sequences, a *squaring condition* can always be tested, since tuples $(1; 0; \ldots; 0), \ldots, (0; 0; \ldots 1)$ must be

equi-distant to coefficients of reciprocal irreducible polynomials:

$$\begin{array}{c} a'_{k-1} \dots a'_0 \\ \downarrow d \\ [1\,0 \dots 0] \\ \downarrow d \\ [0 \dots 0\,1] \\ \downarrow d \\ a_0 \dots a_{k-1} \end{array}$$

Now, direct approach by means of linear sequences can be undertaken.

4 Power structures in $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$ for $k > 2$

4.1 Background on linear sequences and general formalism

Two properties previously described (non-nullity and invariance under iterated global sums) are basic for objects widely known as specializations of linear recurring sequences. Three of them are relevant in power structures.

Definition 4.1 *[14] A linear feedback shift register (or LFSR) sequence is a closed sequence $s = (s_i)_{i=1}^{l}$ of length l, with $s_i \in \mathbb{F}_p$ is defined by an iterative rule*

$$s_{i+k} = a_{k-1}s_{i+k-1} + \ldots + a_0 s_i$$

where initial tuple $(s_0; \ldots; s_{k-1})$ is non-null and $x^k \equiv a_{k-1}x^{k-1} + \ldots + a_0$ is a fixed polynomial of degree k.

Definition 4.2 *[14] A m-sequence (where m- stands for maximal) is a LFSR sequence of length $p^k - 1$ where all nonnull $k-$tuples of $(\mathbb{F}_p)^k$ are concatenated.*

Definition 4.3 *[14] A shift-and-add (or shift-and-subtract) sequence is a closed sequence $s = (s_i)_{i=1}^{l}$ where operations $s_{i+1} + s_i$ (or $s_{i+1} - s_i$) give either the same sequence s, shifted with cyclic indexes, or the null sequence.*

Present chapter uses linear and combinatorial tools to give a complete overview of such sequences, as they come out in power structures of fields $\mathbb{F}_{p^k}$ for any k. Presented results are essentially known, but relation with power structures seems to be natural and shows a basic fact: any power structure in any finite field is a linear structure with some additional properties.

As soon as one tries to manage sequences listed above, definitions and properties often overlap, or have different levels of easiness or hardness, depending on

the point of view: e.g., shift-and-add definition is trivially an ultimate property of sequences of components of primitive elements and, for a given non-primitive element, Gauss' algorithm makes a proper mixing of these properties, up to a primitive element.

An example with low complexity can be examined: let $\mathbb{F}_{3^3}$ be represented by $x^3 \equiv 1 + x + x^2$ irreducible over $\mathbb{F}_3$; power structure for x is:

$$\begin{array}{lllllll} x^1 & \rightarrow & (0;1;0) & x^8 & \rightarrow & (1;2;0) \\ x^2 & \rightarrow & (0;0;1) & x^9 & \rightarrow & (0;1;2) \\ x^3 & \rightarrow & (1;1;1) & x^{10} & \rightarrow & (2;2;0) \\ x^4 & \rightarrow & (1;2;2) & x^{11} & \rightarrow & (0;2;2) \\ x^5 & \rightarrow & (2;0;1) & x^{12} & \rightarrow & (2;2;1) \\ x^6 & \rightarrow & (1;0;1) & x^{13} & \rightarrow & (1;0;0) \end{array}$$

sequences $\left(x_0^i\right)^i, \left(x_2^i\right)^i = \sigma$ are the same, $\left(x_1^i\right) = \tau$ is both their shift-and-add and shift-and-subtract counterpart; Gauss' algorithm applied to $x^i - x^{i-1}$ gives:

$$\begin{array}{llll} \mathbf{(0;1;0)} & \rightarrow x^2 - x^1 \equiv & (0;2;1) & \rightarrow \left(x^2 - x^1\right)^2 \equiv & (1;2;2) \\ (0;0;1) & \rightarrow x^3 - x^2 \equiv & (1;1;0) & \vdots & (2;0;1) \\ (1;1;1) & \vdots & (0;1;1) & \vdots & (1;0;1) \\ (1;2;2) & & (1;1;2) & \vdots & (1;2;1) \\ (2;0;1) & & (2;0;0) & & (1;2;0) \\ (1;0;1) & & (0;2;0) & & (0;1;2) \\ (1;2;1) & & (0;0;2) & & (2;2;0) \\ (1;2;0) & & (2;2;2) & & (0;2;2) \\ (0;1;2) & & (2;1;1) & & (2;2;1) \\ (2;2;0) & & (1;0;2) & & (1;0;0) \\ (0;2;2) & & (2;0;2) & & \mathbf{(0;1;0)} \\ (2;2;1) & & (2;1;2) & & (0;0;1) \\ (1;0;0) & & (2;1;0) & & (1;1;1) \end{array}$$

with notations as in chapter 2, choose $b^2 = a^3$ and $l = 0$ so a primitive element is built up with its power table and the same sequence comes out in all components:

Stability under global sums or differences is an inner property of the sequence, not strictly related to a fixed primitive element; so, the most important step is to change point of view inside a power table and to look at sequences along components. Defining the order of a polynomial $p(x)$ as lowest e such that $f(x)|x^e - 1$, following known results are extracted from [14] and [20]:

Theorem 4.1 *1. Any irreducible polynomial $p(x)$ of degree k and order e over $\mathbb{F}_p$ outcomes a LFSR sequence of length e;*

2. nonnull $k-$tuples over $\mathbb{F}_p$ are partitioned in classes, each with cardinality e;

$\downarrow_\alpha$	$\downarrow_\beta$	$\downarrow_\gamma$	$\downarrow_\delta$	$\downarrow_\epsilon$	$\downarrow_\zeta$
0	1	0	0	2	0
0	2	1	0	1	2
1	2	2	2	1	1
1	1	2	2	2	1
1	2	1	2	1	2
0	0	2	0	0	1
2	2	0	1	1	0
1	0	2	2	0	1
1	0	0	2	0	0
2	**1**	0	1	2	0
1	**1**	**1**	2	2	2
0	**1**	**1**	0	2	2
1	0	**1**	2	0	2
$\downarrow_\delta$	$\downarrow_\epsilon$	$\downarrow_\zeta$	$\downarrow_\alpha$	$\downarrow_\beta$	$\downarrow_\gamma$

3. *if $q(x)$ is primitive, resulting sequence is a m-sequence;*

4. *each m-sequence is a shift-and-add sequence.*

Remark 4.1 - *Counting irreducible polynomials of degree k can be performed by two different formulas, namely*

$$\sum_{d|k} \mu(d)\, p^{k/d} = \sum_{\substack{e|\left(p^k-1\right) \\ e\nmid\left(p^h-1\right),h|k}} \phi(e)$$

where $\phi(e)/k$ counts irreducible polynomials of degree k and order e. Relation above is a simple application of inclusion-exclusion principle for $k = k_1 \cdot \ldots \cdot k_n$ and elementary property $p^k - 1 = \sum_{e|(p^k-1)} \phi(d)$ and it is relevant since, for k fixed, orders e avoid values $e|\left(p^h-1\right)$ for $h|k$ and this happens if and only if a given power structure entirely falls in subfield $\mathbb{F}_{p^h}$, so a lower degree polynomial and a LFSR subsequence are involved. This situation is fully studied in chapter 5.

Results from previous chapter show that these properties can be as well deduced if initial requirements are restricted to non-nullity and permanence; any further completion using Gauss' algorithm gives a proper shift-and-add sequence. But non-nullity and permanence for α generic have shown to be awful properties, so a purely combinatorial generalization from x to any α primitive is available:

1. non-nullity and permanence for x primitive follow from linear recurrence;

2. sequences in components of power tables for x^{p^l} (these elements are usually called *Galois conjugates*) are the same as for x, $\forall 1 \leq h \leq k-1$;

3. whenever $\left\{x^{id}\right\}_{i=1}^{k-1}$ are linearly independent, base change $\left\{x^{i}\right\}_{i=1}^{k-1} \rightarrow \left\{x^{id}\right\}_{i=1}^{k-1}$ gives a power table with the same sequence;

4. previous steps fulfill enumeration of primitive roots for $\mathbb{F}_{p^h}$ over $\mathbb{F}_p$.

Matricial notation is as in chapter 3 and special case $\alpha = x$ allows easier tools.

- Matrix $B(x)$, performing product $a \cdot x = a \cdot B(x)$, is usual companion matrix for polinomial $p(x)$ (see [20]) with changed signs:

$$B(x) = \begin{bmatrix} 0 & 1 & 0 & \dots & & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & & & & & \vdots \\ & & & & \ddots & \\ 0 & 0 & & \dots & & 1 \\ a_0 & a_1 & & \dots & & a_{k-1} \end{bmatrix}$$

  where $(b_{i,j})_{j=0}^{k-1}$ contains coefficients of x^i as as vector and last row gives $x^k \equiv a_0 + \ldots + a_{k-1}x^{k-1}$;

- global matrix $M(x) = \left[x_j^i\right]_{(i;j)=(1;0)}^{(\pi(x);k-1)}$ of order $\pi(x) \times k$, containing all powers of x as rows, has $B(x)$ as first block.

Properties of $M(x)$ are:

1. *(Reduction to previous row)*

$$x_j^i = x_{j-1}^{i-1} + x_{j-1}^{k-1} a_j \tag{1}$$

$$\left(x_j^i\right)_{j=0}^{k-1} = \left(x_j^{i-1}\right)_{j=0}^{k-1} \cdot B(x) \tag{2}$$

$$\tag{3}$$

2. *(Reduction up to first row)* - Each element x_j^i or $\alpha_{i,j}^{(h)}$ can be written as a row-column product where row shifts from $\left(x_j^{i-1}\right)_{j=0}^{k-1}$ to lower powers $\left(x_j^{i-l}\right)_{j=0}^{k-1}$ while column shifts from $\left(x_j^{1+l}\right)_{l=0}^{k-1}$ to higher powers $\left(x_j^{i}\right)_{j=0}^{k-1}$, as far as row $\left(x_j^{k}\right)_{j=0}^{k-1}$ and element x_j^{i-1} in column are reached:

$$\begin{aligned} x_j^i &= \left(x_0^{i-1}; \ldots; x_{k-1}^{i-1}\right) \cdot \left(x_j^1; \ldots; x_j^k\right) = \\ &= \left(x_0^{i-2}; \ldots; x_{k-1}^{i-2}\right) \cdot \left(x_j^2; \ldots; x_j^{k+1}\right) = \\ &= \left(x_0^{k}; \ldots; x_{k-1}^{k}\right) \cdot \left(x_j^{i-k}; \ldots; x_j^{i-1}\right) \end{aligned}$$

last equality simply means a restatement of recurrence relation, shifted along rows and columns:

$$x_j^i = a_0 x_j^{i-k} + \ldots + a_{k-1} x_j^{i-1}$$

3. linear independence $\left|\left(x_j^{h+i}\right)\right| \neq 0$ for each continuous block with h fixed and $i, j = 0 \ldots k-1$ follows since

$$\left|\left(x_j^{h+i}\right)\right|_{i,j=0}^{k-1} = \left|\left(x_j^i\right)\right|_{i,j=0}^{k-1} \cdot \left|B^h(x)\right| = 1 \cdot |B(x)|^h = \left((-1)^k a_0\right)^h \neq 0$$

Matrix $B(\alpha)$ performing product by any α and higher powers $B^h(\alpha)$ can be viewed as layers of a $3D$-matrix where $B(x) = B^0(\alpha)$ is front layer $B^0(\alpha) \forall \alpha$; following usual notation $\alpha_{i,j}^h$ for a general entry of $B^h(\alpha)$, reductions and properties similar to $M(x)$ may be useful:

1. *(Reduction to previous row)*

$$\left[\alpha_{i,j}^h\right]_j = \left[\alpha_{i-1,j-1}^h\right]_j + \alpha_{i-1,k-1}^h \left[a_j\right]_j$$

2. *(Reduction up to first row)*

$$\begin{aligned} \alpha_{i,j}^h &= \left(\alpha_{i-1,0}^h; \ldots; \alpha_{i-1,k-1}^h\right) \cdot \left(x_j^1; \ldots; x_j^k\right) = \\ &= \left(\alpha_{i-2,0}^h; \ldots; \alpha_{i-2,k-1}^h\right) \cdot \left(x_j^2; \ldots; x_j^{k+1}\right) = \\ &\vdots \\ &= \left(\alpha_{0,0}^h; \ldots; \alpha_{0,k-1}^h\right) \cdot \left(x_j^i; \ldots; x_j^{i+k-1}\right) \end{aligned}$$

3. linear independence $\left|\left(\alpha_j^{h+i}\right)\right| \neq 0$ is a special quest, often superseded by enumerations to be explained.

According to this notation, power α^h is in 0-th row of $B^h(\alpha)$ and power table for α is upper face of the parallepiped.

4.2 Power structures for x

Information in power structure of element x can be easily deduced from non-nullity and permanence.

Lemma 4.1 *Let $B(x), M(x)$ be power structures for $x \in \mathbb{F}_{p^h}$; then:*

1. ***(Non-nullity)** - for any fixed component $0 \leq j \leq k-1$ and any $1 \leq h \leq \pi(x)$, system of conditions*

$$\left\{x_j^{h+l} = 0 \text{ for } 0 \leq l \leq k-1\right.$$

implies $x_j^{h+k} = 0$, impossible for given assumptions;

2. ***(Permanence)*** *- for any fixed components $0 \leq j, j' \leq k-1$, if h, h' exist such that*

$$\left\{ x_j^{h+l} = x_{j'}^{h'+l} \text{ for } 0 \leq l \leq k-1 \right.$$

then $x_j^{h+k} = x_{j'}^{h'+k}$.

Proof - About non-nullity, if $x_j^{h+l} = 0$ for $0 \leq l \leq k-1$, then

$$\begin{aligned} x_j^{h+k} &= \left(x_0^{h+k-1}; \ldots; x_{k-1}^{h+k-1}\right) \cdot \left(x_j^1; \ldots; x_j^k\right) = \ldots \\ &= \left(x_0^k; \ldots; x_{k-1}^k\right) \cdot \left(x_j^h; \ldots; x_j^{h+k-1}\right) = 0 \end{aligned}$$

and whole sequence $\left(x_j^h\right)_{h=1}^{p^k-1}$ would be null.

About permanence, if $x_j^{h+l} = x_{j'}^{h'+l}$ for $0 \leq l \leq k-1$ then

$$\begin{aligned} x_j^{h+k} &= \left(x_0^{h+k-1}; \ldots; x_{k-1}^{h+k-1}\right) \cdot \left(x_j^1; \ldots; x_j^k\right) = \ldots \\ &= \left(x_0^k; \ldots; x_{k-1}^k\right) \cdot \left(x_j^h; \ldots; x_j^{h+k-1}\right) = \\ &= \left(x_0^k; \ldots; x_{k-1}^k\right) \cdot \left(x_{j'}^{h'}; \ldots; x_{j'}^{h'+k-1}\right) = \ldots \\ &= \left(x_0^{h'+k-1}; \ldots; x_{k-1}^{h'+k-1}\right) \cdot \left(x_{j'}^1; \ldots; x_{j'}^k\right) = x_{j'}^{h'+k}. \diamond \end{aligned}$$

Relation between irreducible polynomials and full power structures can thus be stated.

Theorem 4.2 *Let $\mathbb{F}_{p^h}$ be represented by $p(x)$ of order e, so that x has period $\pi(x) = e$; then*

1. *columns $\left(x_j^i\right)_{i=1}^{\pi(x)}$ in power table for x are LFSR sequences generated by $p(x)$ and either are equal but shifted or have no common concatenated k-tuples;*

2. *if p is primitive (thus x is a primitive root), columns $\left(x_j^i\right)_{i=1}^{p^k-1}$ are equal but shifted and are built of the m-sequence generated by p.*

Proof - Follows directly from previous lemmas. $\diamond$

Enumeration of primitive polynomials is $\dfrac{\phi\left(p^k-1\right)}{k}$ and recyprocal polynomials can be put together, so a complete example with low complexity can be $\mathbb{F}_{3^4}$ over $\mathbb{F}_3$, to have $\dfrac{\phi(80)}{4} = 4$ distinct m-sequences listed in tables 2 to 5, each with its own couple of primitive polynomials.

4.3 Reduction of sequences for x^{p^l} and decimations

Any α primitive is often considered together with what are called its *Galois conjugates* $\alpha^{p^l}, 2 \leq l \leq k-1$, which are also primitive. It can be shown that

$\rightarrow_\varepsilon$	1	0	0	0	1	0	0	2	1	0	1	1	1	2	0	0	$\rightarrow_\alpha$
$\rightarrow_\alpha$	2	2	0	1	0	2	2	1	1	0	1	0	1	2	1	2	$\rightarrow_\beta$
$\rightarrow_\beta$	2	1	2	0	1	2	2	2	2	0	0	0	2	0	0	1	$\rightarrow_\gamma$
$\rightarrow_\gamma$	2	0	2	2	2	1	0	0	1	1	0	2	0	1	1	2	$\rightarrow_\delta$
$\rightarrow_\delta$	2	0	2	0	2	1	2	1	1	2	1	0	2	1	1	1	$\rightarrow_\varepsilon$

Table 2: sequence s_1, $x^4 \equiv 1 + 2x \Leftrightarrow x^4 \equiv 1 + x^3$

$\rightarrow_\varepsilon$	1	0	0	0	1	0	0	1	1	0	1	2	1	1	0	0	$\rightarrow_\alpha$
$\rightarrow_\alpha$	2	1	0	2	0	1	2	2	1	0	1	0	1	1	1	1	$\rightarrow_\beta$
$\rightarrow_\beta$	2	2	2	0	1	1	2	1	2	0	0	0	2	0	0	2	$\rightarrow_\gamma$
$\rightarrow_\gamma$	2	0	2	1	2	2	0	0	1	2	0	1	0	2	1	1	$\rightarrow_\delta$
$\rightarrow_\delta$	2	0	2	0	2	2	2	2	1	1	1	0	2	2	1	2	$\rightarrow_\varepsilon$

Table 3: sequence s_2, $x^4 \equiv 1 + x \Leftrightarrow x^4 \equiv 1 + 2x^3$

$\rightarrow_\varepsilon$	1	0	0	0	1	2	2	1	1	1	0	0	2	2	0	1	$\rightarrow_\alpha$
$\rightarrow_\alpha$	0	0	1	0	1	0	2	2	1	0	2	1	2	1	1	0	$\rightarrow_\beta$
$\rightarrow_\beta$	1	1	1	1	2	1	0	1	2	0	0	0	2	1	1	2	$\rightarrow_\gamma$
$\rightarrow_\gamma$	2	2	0	0	1	1	0	2	0	0	2	0	2	0	1	1	$\rightarrow_\delta$
$\rightarrow_\delta$	2	0	1	2	1	2	2	0	2	2	2	2	1	2	0	2	$\rightarrow_\varepsilon$

Table 4: sequence s_3, $x^4 \equiv 1 + x + x^2 + 2x^3 \Leftrightarrow x^4 \equiv 1 + x + 2x^2 + 2x^3$

$\rightarrow_\varepsilon$	1	0	0	0	1	1	2	2	1	2	0	0	2	1	0	2	$\rightarrow_\alpha$
$\rightarrow_\alpha$	0	0	1	0	1	0	2	1	1	0	2	2	2	2	1	0	$\rightarrow_\beta$
$\rightarrow_\beta$	1	2	1	2	2	2	0	2	2	0	0	0	2	2	1	1	$\rightarrow_\gamma$
$\rightarrow_\gamma$	2	1	0	0	1	2	0	1	0	0	2	0	2	0	1	2	$\rightarrow_\delta$
$\rightarrow_\delta$	2	0	1	1	1	1	2	0	2	1	2	1	1	1	0	1	$\rightarrow_\varepsilon$

Table 5: sequence s_4, $x^4 \equiv 1 + 2x + x^2 + x^3 \Leftrightarrow x^4 \equiv 1 + 2x + 2x^2 + x^3$

they share the same m-sequence as α. Due to a basic property of characteristic p:

$$(a+b)^p = a^p + b^p \text{ in any } F_{p^k}$$

This leads to a general reduction of p-powers as vectors:

$$x^{hp^l} = \left(x_0^h + x_1^h x + \ldots + x_{k-1}^h x^{k-1}\right)^{p^l} = x_0^h x^0 + x_1^h x^{p^l} + \ldots + x_{k-1}^h x^{(k-1)p^l}$$

where exponents cannot be further reduced since they refer to rows of matrix $M(x)$. So, for x primitive, defining properties of a primitive sequence may be proved for sequences of x^{p^l}:

Non-nullity: previous condition, written on compontents, means

$$x_j^{hp^l} = \left(x_0^h; \ldots; x_{k-1}^h\right) \cdot \left(x_j^0; x_j^{p^l}; \ldots; x_j^{(k-1)p^l}\right)$$

thus $\left\{x_j^{(h+i)p^l} = 0 \text{ for } 0 \le i \le (k-1)\right.$ becomes a system in $x_j^{ip^l}$'s:

$$\left\{\left(x_m^{h+i}\right)_m \cdot \left(x_j^{mp^l}\right)_m = 0 \;\; i = 0, \ldots, k-1\right.$$

whose determinant

$$\begin{vmatrix} x_0^h & \ldots & x_{k-1}^h \\ \vdots & \ddots & \vdots \\ x_0^{h+k-1} & \ldots & x_{k-1}^{h+k-1} \end{vmatrix} = \begin{vmatrix} \left(x_j^h\right)_j \\ \vdots \\ \left(x_j^{h+k-1}\right)_j \end{vmatrix}$$

is $\neq 0$ since rows are a continuous block of $M(x)$; then $x_j^{ip^l} = 0 \; \forall i$ is the only solution, a contradiction since above formula for $x_j^{hp^l}$ would imply $\left(x_j^{hp^l}\right)_j$ to be a null sequence.

Pulling down to x_j^i: since $\left(x_j^{hp^l}\right)_{h=1}^{p^k-1}$ satisfies non-nullity, any of its segments of length k has one and only one location in $\left(x_j^i\right)_{i=1}^{p^k-1}$; fixed initial segment $\left(x_j^0; x_j^{p^l}; \ldots; x_j^{(k-1)p^l}\right)$, $\exists!$ h_l such that

$$\left(x_j^{ip^l}\right)_{i=0}^{k-1} = \left(x_j^{h_l+i}\right)_{i=0}^{k-1}$$

Thus, for each subsequent $x_j^{hp^l}$ one can apply usual reduction rules for $M(x)$:

$$\begin{aligned} x_j^{hp^l} &= \left(x_0^h; \ldots; x_{k-1}^h\right) \cdot \left(x_j^0; \ldots; x_j^{(k-1)p^l}\right) = \\ &= \left(x_0^h; \ldots; x_{k-1}^h\right) \cdot \left(x_j^{h_l}; \ldots; x_j^{h_l+k-1}\right) = x_j^{h+h_l} \diamond \end{aligned}$$

Non-nullity holds in a more general situation, where the question about any power structure can be put and answered.

Corollary 4.1 *In power table $M(x)$ for x primitive, let α be a generic element such that $\alpha^{d(h+i)}$ for $i = 0, \ldots, k-1$ are linearly independent; then, for any $l = 1, \ldots, k-1$ and j fixed, system*

$$\left\{ {}_{0 \le i \le (k-1)} \alpha_j^{d(h+i)p^l} = 0 \right.$$

is incompatible with initial assumptions.

Proof - Explicitation of $\left(\alpha_0^{d(h+i)} + \alpha_1^{d(h+i} x + \ldots + \alpha_{k-1}^{d(h+i)} x^{k-1}\right)^{p^l}$ gives system

$$\left\{ {}_{0 \le i \le (k-1)} \left(\alpha_0^{d(h+i)}; \ldots; \alpha_{k-1}^{d(h+i)}\right) \cdot \left(x_j^0; x_j^{p^l} \ldots; x_j^{(k-1)p^l}\right) = 0 \right.$$

whose determinant

$$\begin{vmatrix} \alpha^{dh} \\ \vdots \\ \alpha^{d(h+k-1)} \end{vmatrix}$$

is $\neq 0$, implying impossibility. $\diamond$

Now, one can partition exponents $1 \le d \le p^k - 1$ in four classes:

1. $d = p^l$, thus counted by $\phi(p^k - 1)$;
2. remaining $d \neq p^l$ counted by $\phi(p^k - 1)$;
3. $d = l \sum_{i=0}^{k|h} p^{k-ih}$ for $1 \le l \le p^h - 1$ and $h|k$;
4. d out of previous cases.

Power structures show to be strongly sensible to previous classification of d's and each power structure can be defined in a suitable way, starting from structures for x primitive. As a basic fact of finite fields, rows of $M(x)$ can be permuted according to exponents d counted by $\phi(p^k - 1)$; a purely combinatorial operation on rows in $M(x)$ is frequently appled to sequences of components.

Definition 4.4 *Let s be a given m-sequence of length $p^k - 1$ and $d = 1 \ldots p^k - 2$ fixed; then, let $MCD(d; p^k - 1) = e$ so that $d = ef$, $p^k - 1 = eg$ for f, g relatively primes; then, a decimation ϕ_d is the map defined componentwise as*

$$\phi_d(s) = \left\{ (s_{i+hd})_{h=0}^{g-1} \text{ for } 0 \le i \le (e-1) \right\}$$

If a decimation ϕ_d is applied on a whole $k-$tuple, cyclic groups properties seem to have a role superimposed to algebraic structure, but applications to a m-sequence are interesting: they simply pick out of s values s_h whose indices lie at distance d and, for d and $p^k - 1$ relatively primes, ϕ_d gives a new power structure. Main properties of ϕ_d are collected in a result quite obvious, that enlights the ratio for such a definition:

Lemma 4.2 *Image of ϕ_d is made of*

- *one sequence of length p^k-1 if and only if $MCD(d;p^k-1)=1$ and index $\overline{i}$ is indifferent;*
- *d sequences of length $\dfrac{p^k-1}{d}$ otherwise;*

each ϕ_d can be extended in an obvious way to rows of a whole power table, say $\left[\alpha^h\right]_{h=1}^{p^k-1}$ with α primitive, application from initial value $\alpha^{p^k-1}=1$ and $d \nmid (p^k-1)$ gives all $\phi(p^k-1)$ primitive elements for the choosen representation.

Transformations ϕ_d when $d|(p^k-1)$ are of special interest, since they may collapse in a primitive sequence for a subfield; for a while only ϕ_d's that keep united a sequence are considered and this means first $d=p,p^2,\ldots,p^{k-1}$, then other values.

Theorem 4.3 *Let $M(x)$ be a power structure for x primitive; then decimations ϕ_d for d counted by $\phi(p^k-1)$ give power structures $M\left(x^d\right)$ which (i) satisfy non-nullity and permanence (ii) are partitioned in classes $\left[dp^l\right]$ and (iii) power structures in each class are built upon one and the same m-sequence.*

Proof - Permanence is valid due to application of the same ϕ_d in each component; if s is a m-sequence, then application of ϕ_d's that bring together the sequence clearly commute:

$$\phi_{dp^l}(s)=\phi_d(\phi_{p^l}(s))=\phi_d(s)\diamond$$

General results due to Zierler and Blackburn (see [14]), together with special results for characteristic 2 in [13], exactly count m-sequences and allow reduction of Galois conjugates to hold in complete generality.

Theorem 4.4 *[14] Sequences of length p^k-1 over a prime field $\mathbb{F}_p$ are equivalently m-sequences or shift-and-add sequences.*

Theorem 4.5 *[14] There exist exactly $\frac{\phi(p^k-1)}{k}$ shift-and-add sequences of length p^k-1 over $\mathbb{F}_p$.*

Corollary 4.2 *Let α be primitive, so that α^{p^l} for $l=1,\ldots,k-1$ are too; then any power structure for α^{p^l} holds the same m-sequence.*

As a general case, global linear transformations amongst primitive elements can be formulated as base changes; this exhaustes all possible power structures.

4.4 Base change over a whole power structure

Power structure in a finite field is always defined by means of a linear transformation, so ultimate representation is by means of base changes. Following result shows that primitive elements and irreducible polynomials are different views of one and the same structure built up by a fixed m-sequence.

Lemma 4.3 *Let x be primitive and $1 \leq d \leq p^k - 1$ be fixed; then:*

1. *any system of vectors $\left\{x^{id}\right\}_{i=0}^{k-1}$ is a base if and only if x^{id}'s don't belong to a subfield $\mathbb{F}_{p^h}$;*
2. *x^{id}'s belong to a subfield if and only if $d = l\sum_{i=0}^{k|h} p^{k-ih}$ for some l and $h|k$;*
3. *number of distinct linearly idndependent systems $\left\{x^{id}\right\}$ is exactly counted by*

$$kN_p(k) = \sum_{h|k} \mu(h) p^{k/h}$$

Proof

1. Let $\left(x^{id}\right)_{i=0}^{k-1}$ be a base; then linear indipendence implies $\sum_{i=0}^{k-1} c_i x^{id} = \overline{0}$ if and only if $c_i = 0\ \forall i$, but for $d = l\left(p^h - 1\right)$ one has cyclic vectors, since x^d is a root of a polynomial of degree $h|k$, $\exists \overline{c}_o, \ldots \overline{c}_{h-1}$ not all $= 0$ such that $x^{hd} = \sum_{i=0}^{h-1} \overline{c}_i x^{id}$ and $\overline{c}_h = \ldots \overline{c}_{k-1} = 0$ can be added, contradicting previous indipendence. Argument is clearly invertible, due to the same definition of subfield.
2. values $d = l\frac{p^k-1}{p^h-1}$ lie cyclically in exponents satisfying basic rule $h|k$ needed for subfield relation.
3. Let $k = k_1^{\alpha_1} \ldots k_l^{\alpha_l}$ be prime decomposition of exponent k non-prime; each $h|k$ gives values

$$d = l\left(p^{k-h} + p^{k-2h} + \ldots + p + 1\right), 1 \leq l \leq p^h - 1$$

that have to be treated according to inclusion exclusion rules, so their coefficient in global counting is $\mu\left(\frac{k}{h}\right)$ and

$$\sum_{h|k} \mu\left(\frac{k}{h}\right)\left(p^h - 1\right) = \sum_{h|k} \mu\left(\frac{k}{h}\right) p^h - \sum_{h|k} \mu\left(\frac{k}{h}\right) = \sum_{h|k} \mu(h) p^{k/h} \ \diamond$$

Recurrence relation and ordinary base change give biggest set of transformations that leave a m-sequence unchanged. Any power structure S for x primitive can be simply viewed as a $(p^k - 1) \times k$ matrix where a base change $\left(x^i\right)_{i=0}^{k-1} \mapsto \left(x^{id}\right)_{i=0}^{k-1}$ is applied; matrix $A = \left[\left(x_{o,j}\right); \left(x_{d,j}\right); \ldots; \left(x_{(k-1)d,j}\right)\right]$ has columns related to *inverse* base change, so one can compute A^{-1}, transpose it and look at $S \times \left(A^{-1}\right)^t$ as a new power structure, obtained by means of purely linear tools.

Theorem 4.6 *Let x be primitive, with S associated global power structure; let $T(x^i) = x^{id}, 0 \leq i \leq k-1$ be any base change amongst linearly independent, regularly located powers of x and $T^{-1}(x^i) = x^{t_i}$ be inverse base change; then*

1. *matrix products $S' = S \times T(x^i)$ and $S'' = S \times T^{-1}(x^i)$ give other power structures;*
2. *resulting power structures are different from those derived by cyclicity properties, except for base change $T(x^i) = x^{ip}$, which gives the same result as for transformation ϕ_d;*
3. *S' and S'' are built upon the same primitive sequence as S.*

Proof

1. Completeness of power structures S', S'' is given by two facts: T, T^{-1} are bijections over $\mathbb{F}_{p^k}^{\times}$ and they correspond to a reduction

$$x^{kd} \equiv a_0 + a_1 x^d + \ldots + a_{k-1} x^{(k-1)d}$$

always valid since $p(x)$ is irreducible.

2. Definition of T for $\left\{x^i\right\} \mapsto \left\{x^{ip}\right\}$ is the same as ϕ_p over $x^0, \ldots, x^{k-1}$:

$$T\left(x^i\right)_j = \left(x_0^i; \ldots; x_{k-1}^i\right) \cdot \left(x_j^0; \ldots; x_j^{(k-1)p}\right) = \phi_p\left(x^i\right)$$

and ϕ_p is linear since $(\lambda a + \mu b)^p = \lambda a^p + \mu b^p$.

3. Let $T(x^i) = x^{id}, 0 \leq i \leq k-1$ be a fixed base change as above; by linearity, one has

$$T\left(x^h\right) = x_0^h + x_1^h x^d + \ldots + x_{k-1}^h x^{(k-1)d}$$

or, in components,

$$T\left(x^h\right)_j = \left(x_0^h; \ldots x_{k-1}^h\right) \cdot \left(x_j^0; x_j^d; \ldots; x_j^{(k-1)d}\right).$$

First, non-nullity holds: condition $T\left(x^{\overline{h}+h}\right) = 0$ for $0 \leq h \leq (k-1)$, that is

$$\left(x_0^{\overline{h}+h}; \ldots x_{k-1}^{\overline{h}+h}\right) \cdot \left(x_j^0; x_j^d; \ldots; x_j^{(k-1)d}\right) = 0, 0 \leq h \leq (k-1)$$

this is a system in $x_j^0, x_j^d, \ldots, x_j^{(k-1)d}$ whose matrix, a sequence of h consecutive powers of x, cannot have null determinant; so $x_j^{id} = 0, 0 \leq h \leq (k-1)$ is the only solution, a contradiction since it is a column of matrix with x^{id}'s, that is a base.

Then $\exists! h_1$ such that $T(x^0)_j = x_j^{h_1}, T(x^1)_j = x_j^{h_1+1}, \ldots, T(x^{k-1})_j = x_j^{h_1+k-1}$ and subsequent power k is

$$T(x^k)_j = \left(x_0^k; \ldots x_{k-1}^k\right) \cdot \left(x_j^0; x_j^d; \ldots; x_j^{(k-1)d}\right) =$$
$$= \left(x_0^k; \ldots x_{k-1}^k\right) \cdot \left(T(x^0)_j; T(x^1)_j; \ldots; T(x^{k-1})_j\right) =$$
$$= \left(x_0^k; \ldots x_{k-1}^k\right) \cdot \left(x^{h_1})_j; x_j^{h_1+1}; \ldots; x_j^{h_1+k-1}\right) = x_j^{h_1+k}$$

and $T(x^h)_j = x_j^{h_1+h}$ can be extended to any higher h, so for the whole sequence one has $S = S'$. Inverse linear transformation can also be applied, so that $T^{-1}(1) = 1, T^{-1}(x) = \alpha_1 = x^{t_1}, T^{-1}(x^2) = \alpha_2 = x^{t_2}, \ldots, T^{-1}(x^{k-1}) = \alpha_{k-1} = x^{t_{k-1}}$ where exponents t_i have no known relation with i. General definition is, by linearity, $T^{-1}(x^h) = x_0^h + x_1^h x^{t_1} + \ldots + x_{k-1}^h x^{t_{k-1}}$ and non-nullity is

$$T^{-1}(x^{\overline{h}+h})_j = x_0^h x_j^0 + x_1^h x_j^{t_1} + \ldots + x_{k-1}^h x_j^{t_{k-1}} =$$
$$= \left(x_0^h; \ldots x_{k-1}^h\right) \cdot \left(x_j^0; x_j^{t_1}; \ldots; x_j^{t_{k-1}}\right) = 0, 0 \leq h \leq (k-1)$$

and $x_j^0 = x_j^{t_1} = \ldots = x_j^{t_{k-1}} = 0$ is a contradiction, since it is a column of a base change. Then $\exists! h_1$ such that $T^{-1}(x^h)_j = x_j^{h_1+h}$ and subsequent power k is

$$T^{-1}(x^k)_j = \left(x_0^k; \ldots x_{k-1}^k\right) \cdot \left(x_j^0; x_j^{t_1}; \ldots; x_j^{t_{k-1}}\right) =$$
$$= \left(x_0^k; \ldots x_{k-1}^k\right) \cdot \left(T^{-1}(x^0)_j; T^{-1}(x^1)_j; \ldots; T^{-1}(x^{k-1})_j\right) =$$
$$= \left(x_0^k; \ldots x_{k-1}^k\right) \cdot \left(x^{h_1})_j; x_j^{h_1+1}; \ldots; x_j^{h_1+k-1}\right) = x_j^{h_1+k} \diamond$$

One can iterate base changes $\alpha^i \mapsto \alpha^{id'}$ for $\alpha = x^d$ but enumeration gives fewer acceptable values d'; instead, linearity gives the same properties for a general α.

Corollary 4.3 *Let $\alpha \in \mathbb{F}_{p^k}^{\times}$ be primitive with $\left\{\alpha^i\right\}_{i=0}^{k-1}$ lineary independent; for any fixed $d \neq l(p^k-1)(p^h-1), h|k$ base change $\alpha^i \mapsto \alpha^{di}$ gives a power structure built upon the same m-sequence as α.*

Proof - Reduction rule

$$\alpha^k \equiv a_0 + a_1\alpha + \ldots + a_{k-1}\alpha^{k-1}$$

is effective and, together with base change $T\left(\alpha^i\right) = \alpha^{di}$, gives the same result as for x; coherence of power structure is again implied by surjectivity and linearity. $\diamond$

It can be thus proved that any complete power structure is definitely turned into a recurrence relation, applied to k components.

Corollary 4.4 *For a fixed m-sequence, relative shifts amongst k instances giving an effective power structure are determined by a location of elements $\alpha^i = x^{di}$ (from an initial configuration where x is primitive) and prosecuted componentwise by recurrence relation.*

Proof - Once k rows $\alpha^i = x^{di}$ are choosen, for each component an initial state $(s_{i,j})_j$ is fixed and recurrence relation $s_h = a_{k-1}s_{h-1} + \ldots + a_0 s_{h-k}$ can be started; linearity assumes, in each component, the same outcome as for a base change. $\diamond$

As a final step, a complete enumeration can be collected.

4.5 Concluding enumeration of power structures

Previous results can be collected in an enumeration to fullfill total number

$$\frac{\phi\left(p^k-1\right)}{k}\sum_{d|k}\mu\left(d\right)p^{k/d}$$

of power structures for $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$; enumeration can be made shortly upon decimations and, at least, partitioned in different m-sequences.

Theorem 4.7 *Each of $\dfrac{\phi(p^k-1)}{k}$ primitive sequences of length p^k-1 can build $N_p(k)\cdot k = \sum_{d|k}\mu(d)p^{k/d}$ correct power structures for F_{p^k} over F_p; thus, global counting $\phi(p^k-1)N_p(k)$ always holds.*

Proof - Enumeration $\sum_{d|k}\mu(d)p^{k/d}$ can be applied to transformations ϕ_d for any $1 \leq d \leq (p^k-1)$, since any fixed ϕ_d falls into one and only one of following cases:

1. if $d \neq p^h - 1$ for all $h|k$, image of ϕ_d has cardinality $MCD(d; p^k-1)$ and fragments form a partition of non-null k-tuples;
2. if $d = p^h - 1$ for some $h|k$, image of ϕ_d collapses in fragments made of either one (and the same) primitive sequence for a representation of subfield F_{p^h}, or the null sequence $(0_i)_i$.

Transformations of type (1) correctly count all acceptable ϕ_d's, but they are used only to localize squaring conditions and they are not really applied; instead, transformations of type (2) have to be discarded, since they cannot build a structure of order (p^k-1).

Now, factorization of $k = p_1^{\alpha_1}\ldots p_n^{\alpha_n}$ gives values of d that have to be discarded and product of $p_i^{\alpha_i}$'s exactly matches requests for μ-function:

factorization $(p^k-1) = (p^{p_i}-1)\cdot(p^{p_i^{\alpha_i-1}}+\ldots+1)$ gives $(p^{p_i}-1)$ transformations $\phi_{l(p^{p_i^{\alpha_i-1}}+\ldots+1)}$ that have to be discarded; further exponents of p_i are

indifferent, since they are included in previous counting; indifference of α_i's is the same condition as $\mu(n) = 0$ when n contains almost a square. So, only values $d|k$ that are products of distinct p_i's count, with usual sums or subtractions in order to balance multiple countings; a direct application of Inclusion-Exclusion Principle gives total counting of acceptable ϕ_d's:

$$(p^k-1)-\sum_{|T|=n-1}\left(p^{\prod_{i\in T}p_i}-1\right)+\sum_{|T|=n-2}\left(p^{\prod_{i\in T}p_i}-1\right)-\ldots+(-1)^n\sum_{i=1}^{n}(p^{p_i}-1)$$

where (-1)'s can be collected and cancelled, since their total number is

$$\sum_{l=0}^{n}\binom{n}{l}(-1)^l=0$$

for a basic property of bynomials. Thus, previous counting gives same terms as $\sum_{d|k}\mu(d)p^{k/d}$. $\diamond$

Corollary 4.5 *For any fixed m-sequence of length p^k-1, following complete power structures can be built:*

- *Build an m-sequence s_1 of length p^k-1 over $\mathbb{F}_p$; checksum of elements $\left(\delta_j^i\right)_{j=0}^{k-1}$ at distance 1 gives basic structure for x primitive and identifies primitive recyprocal polynomials $p(x), \overline{p}(x)$.*
- *Transformations ϕ_{p^l} for $1 \leq l \leq (k-1)$ hold the same sequence s_1; checksum of elements $\left(\delta_j^i\right)_{j=0}^{k-1}$ at distances p^l give power structures for x^{p^l}.*
- *Transformations ϕ_d for d counted by $\phi(p^k-1)$ give power structures partitioned in m-sequences $s_2, \ldots, s_{\phi(p^k-1)/k}$ according to classes $\left[dp^l\right]$; checksum of elements $\left(\delta_j^i\right)_{j=0}^{k-1}$ at distance d is locked since primitive polynomials $p(x), \overline{p}(x)$ don't change under these operations.*
- *Transformations in previous step can be cyclically applied (e.g. to images of $\phi_d(s)$ or by means of base changes $\left\{x^{di}\right\} \rightarrow \left\{x^i\right\}$); a set of power structures of cardinality $\left(\phi(p^k-1)\right)^2/k$ is defined; the same cardinality is given by checksums of elements $\left(\delta_j^i\right)_{j=0}^{k-1}$ at distances d along all m-sequences; irreducible polynomials involved are all primitive.*
- *For d not counted by $\phi(p^k-1)$ and $d \neq l\frac{p^k-1}{p^h-1}$ with $h|k$, base changes $\left\{x^{di}\right\} \rightarrow \left\{x^i\right\}$ hold the same initial m-sequence s_i and fulfill remaining*

$$\frac{\phi(p^k-1)}{k}\left(\sum_{d|k}\mu(d)p^{k/d}-\phi(p^k-1)\right)$$

power structures; the same cardinality is given by checksums of elements $\left(\delta_j^i\right)_{j=0}^{k-1}$ *at distances* d *along all m-sequences; all irreducible polynomials involved have order* $e < (p^k - 1)$.

5 Subfield relation $\mathbb{F}_{p^h} \hookrightarrow \mathbb{F}_{p^k}$ for $h|k$

Distinct representations of a subfield $\mathbb{F}_{p^h} \hookrightarrow \mathbb{F}_{p^k}$ are all isomorphic and, after a theorem of Blackburn (see [14]), quest for shift-and-add- or m- properties implies that m-sequences over ground field $\mathbb{F}_p$ have always to be considered. But any $\mathbb{F}_{p^k}$ can also be built upon a fixed $\mathbb{F}_{p^h}$, required to be stable; this may give chains of subfields, for a fixed decomposition $k = h_1 \dots k_l$. Stability of a subfield is proved to give specific relative shifts amongst blocks of m-sequences.

5.1 General construction of power sub-structures

Following result collects basic results.

Lemma 5.1 *Let* $\alpha \in \mathbb{F}_{p^k}$ *be a primitive element,* $M(\alpha)$ *be the matrix of its power structure, with m-sequence* s *and* $k = hl, e = \left(p^k - 1\right) / \left(p^h - 1\right)$*; then*

1. *matrix* $M\left(\alpha^{ei}\right)$ *for* $1 \leq i \leq p^h - 1$ *is a power structure for (a representation of) a subfield* $\mathbb{F}_{p^h}$*;*
2. *columns of* $M\left(\alpha^{ei}\right)$ *are made of either one and the same m-sequence* t *of length* $p^h - 1$ *or the null sequence;*
3. *equally shifted rows* $M\left(\alpha^{ei+r}\right)$ *are made of either the same sequence* t *or the null sequence, thus* s *is uniquely determined as an extension of* t*.*

Proof

1. Elements α^{ei} satisfy $\left(\alpha^{ei}\right)^{p^h-1} = 1$, that is a basic property defining $\mathbb{F}_{p^h}$, both for additive and multiplicative structure.
2. Property $\forall i_1 \forall i_2 \exists i_3 \left(\alpha^{ei_1} + \alpha^{ei_2} = \alpha^{ei_3}\right)$ implies that components of add-shift, placed e.g. in position $\alpha^e + 1 = \alpha^{ei}$, thus they are made of either one and the same recurrence relation
$$t_i = b_0 t_{i-h} + \ldots + b_{h-1} t_{i-1}$$
or everywhere null values. It is worth noting that this recurrence is defined in h values but holds in k components (apart from everywhere null ones).
3. Segmentation of s at distances e means that a decimation ϕ_e has been applied, so proof of this part can be given for $\alpha = x$, that is for a primitive polynomial. Fix $1 \leq r \leq e - 1$ and extract rows $\left(x^{ei+r}\right)_{i=1}^{p^h-1}$ from $M(x)$; recurrence relation holds for x_j^{ei}, that is
$$x_j^{ei} = b_{h-1} x_j^{e(i-1)} + \ldots + b_0 x_j^{e(i-h)};$$

let $\left(x_j^r;\ldots;x_j^{(h-1)e+r}\right)$ be an initial segment, assumed to be $\neq \overline{0}$; then $\exists!$ position $i_{r,j}$ such that $x_j^{(i_{r,j}+l)e)} = x_j^{le+r}$ for $0 \leq l \leq h-1$. Subsequent value x_j^{he+r} can be computed for $x^{he+r} = x^{hl} \cdot B^r(x)$, where

$$\begin{aligned} x_j^{he+r} &= \left(\sum_{i=0}^{h-1} b_i x_0^{ie};\ldots;\sum_{i=0}^{h-1} b_i x_{k-1}^{ie}\right) \cdot \left(x_j^r;\ldots;x_j^{r+k-1}\right) = \\ &= \sum_{i=0}^{h-1} b_i \left(x_0^{ie};\ldots;x_{k-1}^{ie}\right) \cdot \left(x_j^r;\ldots;x_j^{r+k-1}\right) = \\ &= b_0 x_j^r + \ldots + b_{h-1} x_j^{(h-1)e+r} = \\ &= b_0 x_j^{i_{r,j}e} + \ldots + b_{h-1} x_j^{(i_{r,j}+h-1)e} = x_j^{(i_{r,j}+h)e} \end{aligned}$$

and recurrence relation can be extended along the whole component. If initial segment is null, last equivalence means $x_j^{(i_{r,j}+h)e} = 0$. $\diamond$

Decimations ϕ_d for $d = l\left(p^k-1\right)\left(p^h-1\right)$ were left aside in previous chapters, so full information for any d is now explained.

5.2 Power structures for $\mathbb{F}_{p^k}$ with a stabilized subfield $\mathbb{F}_{p^h}$

Special structures for $\mathbb{F}_{p^k}$ can be built upon an exact representation of $\mathbb{F}_{p^h}$; this happens together with a precise phoenomenology: power structure of $\mathbb{F}_{p^h}$ is surrounded by everywhere null components; algebraic equivalent is a system of (almost) two reductions

$$\begin{cases} x^h \equiv a_0 + \ldots + a_{h-1}x^{h-1},\ a_i \in \mathbb{F}_p \\ y^l \equiv b_0 + \ldots + b_{l-1}y^{l-1},\ b_i \in \mathbb{F}_{p^h} \\ \vdots \end{cases}$$

that can be studied in detail.

5.2.1 Representations of $\mathbb{F}_{p^k}$ with a $\mathbb{F}_{p^h}$ stable

When a power structure for $\mathbb{F}_{p^k}$ is built upon a power structure for a standard $\mathbb{F}_{p^h}$, elements of the latter appear in l copies and are everywhere surrounded by null components. One may say that these structures *stabilize* subfield $\mathbb{F}_{p^h}$. Since shift-and-add properties and maximal linear recurring properties on h-tuples hold also in each component, stabilization of a subfield implies a stronger regularity between m-sequences.

When $\mathbb{F}_{p^k}$ is built upon $\mathbb{F}_p$, relative shifts between components have been previously related to alighment of block $\left(\delta_j^i\right)$ at equal distances; this makes relative shifts everywhere different and shift-and-add property does not hold between h-tuples. But if a subfield $\mathbb{F}_{p^h}$ has to be stabilized, one and the same

shift-and-add property must hold between h-tuples; this implies a specific simmetry in relative shifts inside h-tuples: they are obtained by a power structure for $\mathbb{F}_{p^k}$ blowing at distance $\left(p^k-1\right)/\left(p^h-1\right)$.

Relative shifts $\sigma_1,\ldots\sigma_{h-1}$ referred to e.g. first column are related to shifts $\tau_1,\ldots\tau_{h-1}$ by rule

$$\sigma_i=\tau_i\left(p^k-1\right)/\left(p^h-1\right)$$

and each m-sequence for $\mathbb{F}_{p^h}$ seems to blow in $\dfrac{\phi\left(p^k-1\right)h}{k\phi\left(p^h-1\right)}$ m-sequences for $\mathbb{F}_{p^k}$.

A phœnomenology of stabilized subfields takes into account partitioned periods $[mp^n]$ for $1\leq m\leq p^k-1$ and $n|k$, where n is least integer such that $mp^n\equiv m\ mod\ p^k-1$.

Number a_n of classes with period n is given by empirical rule

$$\left[\begin{array}{c} a_1=p^k-p \\ a_d=\frac{1}{d}\left(p^d-p-\sum_{n|d}na_n\right)\ \forall\ d|k \end{array}\right.$$

this enumeration is however superseded by a more complete one, where a power structure for $\mathbb{F}_{p^k}$ can be blowed from a power structure for some $\mathbb{F}_{p^h}$.

5.2.2 Enumeration of sub-structures for $\mathbb{F}_{p^k}$ with a $\mathbb{F}_{p^h}$ stable

If a complete enumeration of power structures for $\mathbb{F}_{p^k}$ with a stable $\mathbb{F}_{p^h}$ is required, exact number

$$\phi\left(p^k-1\right)N_p(h)N_{p^h}(l)$$

can be reached with following steps:

1. power structures for $\mathbb{F}_{p^h}$ are

$$\phi\left(p^h-1\right)N_p(h)=\frac{\phi\left(p^h-1\right)}{h}\left(hN_p(h)\right)$$

2. each m-sequence t of length p^h-1 blows in $\dfrac{\phi\left(p^k-1\right)}{l\phi\left(p^h-1\right)}$ m-sequences s of length p^k-1 and the same happens for a whole power structure;

3. relative shifts amongst l blocks of h instances of s follow the same rule as described in section 4, with $lN_{p^h}(l)$ acceptable relative shifts; this gives total number

$$\frac{\phi\left(p^k-1\right)}{l\phi\left(p^h-1\right)}\phi\left(p^h-1\right)N_p(h)lN_{p^h}(l)$$

same as above.

Corollary 5.1 *For each decomposition $k = k_1 \dots k_l$, total number of power structures with a stabilized subfield for each k_i is*

$$\phi\left(p^k - 1\right) \prod_{i=1}^{l} N_{p^{k_1 \dots k_{i-1}}}(k_i)$$

Proof - Repeat iteratively previous steps for each k_i. $\diamond$

It is worth noting that primitivity of polynomials holds in a weak sense, since it depends upon representation of lower fields, but suitable relative shifts amongst m-sequences can hold information for any chain of subfields.

6 Self-organization of m-sequences

Historical results by d'Ocagne and Perrin (see [12]) show that any $(2k-1)$-tuple of consecutive values in a m-sequence forms a set of indipendent k-tuples:

$$\begin{vmatrix} s_1 & \dots & s_k \\ s_2 & \dots & s_{k+1} \\ \vdots & \ddots & \vdots \\ s_k & \dots & s_{2k-1} \end{vmatrix} \neq 0$$

This fact can be easily proved if s_i's are initial segment of components 0 or $k-1$ in a power structure, but one may thus ask whether any $(2k-1)$-tuple satisfying this condition can be extended to a m-sequence by rule $s_n = a_{k-1}s_{n-1} + \dots + a_0 s_{n-k}$, where polynomial $x^k \equiv a_0 + \dots + a_{k-1}x^{k-1}$ is a solution of

$$\{a_0 s_i + \dots + a_{k-1}s_{i+k-1} = s_{i+k}, \quad 1 \leq i \leq k$$

for a fixed $s_{2k} \in \mathbb{F}_p$.

This method happens to be really weak. An exhaustive method to build m-sequences *ex nihilo*, by means of lateral classes, is presented in [13]; but maximality properties lead to ask whether pure self-organization rules are enough, with no previously available information about irreducible polynomials or primitive roots. A few heuristic rules can be pointed out; computational aspects are left aside, since main attention is paid to what could be "random" deep meaning. One can focus two goals:

1. build up a m-sequence from a random fragment of length d;
2. build up a m-sequence from a m-subsequence.

6.1 Starting from random fragments

6.1.1 Gauss' algorithm applied to random d-tuples

Let a random non-null d-tuple $(s_i)_{i=0}^{d}$, $s_i \in \mathbb{F}_p$ be given; one may ask whether it is the sequence of any component in any power structure and whether an application of Gauss' algorithm may give a full m-sequence. Following preliminary requests are necessary:

- $p \nmid d$;
- converge occurs at lowest e such that $d|\,(p^e - 1)$
- d-tuples too much regular (e.g. constant) are forbidden;
- cyclicity may be closed with second d-tuple, since any global sum is defined modulo $(a_1; \ldots; a_d) \approx (a_1 + c; \ldots; a_d + c)$;
- as soon as an iteration breaks requirements of cardinality for some value $0 \ldots p-1$, computation cannot give an acceptable result.

Indeed, Gauss' algorithm always works when full information is available, but in a random situation it simply computes power-like values

$$\sum_{n=0}^{l} (-1)^n \binom{l}{n} a_{i+nh}$$

at step l and for a fixed h, as far as a cyclicity is closed. The only interesting remark is as follows.

Proposition 6.1 *Let $(s_i)_{i=1}^{d}$ be a random d-tuple in $\mathbb{F}_p$ and let k be the least exponent (if any) such that $d|(p^k - 1)$; if a representation for $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$ exists such that $(s_i)_{i=1}^{d}$ is associated to a component in power table of an element with period d, then Gauss' algorithm gives a linear sequence of higher order or maybe a m-sequence; this surely happens when initial tuple itself is a LFSR sequence.*

Some examples with d prime can be given.

- Choose $d = 5$ and pick at random $(1; 2; 2; 0; 1)$ over $(\mathbb{F}_3)$, put it in column and apply $a_i - a_{i-1}$ in subsequent columns; after 16 iterations the original comes back, so $5 \cdot 16 = 80 = 3^4 - 1$ elements have been generated, that are a m-sequences for $\mathbb{F}_{3^4}$. This example works in an optimal way, due to factorization.
- In $\mathbb{F}_{3^3}$ one has $3^3 - 1 = 2 \cdot 13$, factor 2 isn't enough and factor 13 is too much, so random 13-tuples give an unpredictable result, if randomness does not give a 13-tuple linearly recurring.
- If $(s_i)_{i=1}^{d}$ is a random tuple, $d|(p^k - 1)$ and exactly $\left(p^k - 1\right)$ iterations are needed to give back (s_i) it's a bad new, since $(s_i \pm s_{i+l})^{p^k - 1} = s_i \pm s_{i+l}$ is a basic property of arithmetic mod$p$ and every iterated sum ends like that. This may happen e.g. in $\mathbb{F}_{3^5}$, with $3^5 - 1 = 2 \cdot 11^2$, if a 11-tuple is choosen.

6.1.2 Effective algorithm with backtracking

Shift-and-add condition on k-tuples makes any m-sequence constructible with a step-by-step algorithm, that roughly searches for the first stability point under any cyclic sum; such a point may be for a non maximal linear sequence.

Definition 6.1 *A $(k+l)$-tuple $(s_1;\ldots;s_{k+l}) \in (\mathbb{F}_p)^{k+l}$ is acceptable if it verifies no conditions contradicting global stability, that means:*

- *k-tuples $(s_1;\ldots;s_k), (s_2;\ldots;s_{k+1}), \ldots, (s_{1+l};\ldots;s_{k+l})$ are all non-null and distinct;*
- *any fixed arbitrary cyclic sum $(s_i \pm s_{i+j_1} \pm \ldots \pm s_{i+j_m})$ between values (not necessarily consecutive) gives k-tuples either everywhere null, or non-null and distinct.*

An algorithm may simply backtrack acceptable tuples:

1. fix a non-null k-tuple $(s_1;\ldots;s_k)$;
2. given an acceptable segment of length $(k+l-1)$, entail a new value s_{k+l} and verify segment $(s_i)_{i=1}^{k+l}$ be also acceptable;
3. as soon as a configuration is reached, where a segment $(s_i)_{i=1}^{k+l}$ or any of its cyclic sums share a common tuple, segment $(s_i)_{i=1}^{k+l}$ has one and only one completion to a candidate linear sequence, maximal or not; each further entailed value must give an acceptable segment;
4. as soon as a non acceptable segment is reached, change last value entailed or backtrack to change more than one;

At step $(s_1;\ldots;s_{k+l})$, possible global sums are:

$$(\pm s_i \pm \delta_1 s_{i+1} \pm \ldots \pm \delta_l s_{i+l})_{i=1}^{k}$$

where $\delta_j = 0, 1$ is a Kroneker-like symbol; so, there are 2^{l+1} possible signs and $\left(2^l - 1\right)$ acceptable δ_j (since $\delta_j = 0 \quad \forall j$ returns initial segment and is discarded), so there are $2^{l+1}\left(2^l - 1\right)$ possible iterated sums of length at least k: indeed too much, but this algorithm only needs to reach a stable configuration as near as possible. Factors of $p^k - 1$ have some relevance, so Mersenne primes $M_k = 2^k - 1$ for k prime are worst examples and no subsequence can be reached; this is perhaps the main reason why such structures are best used in criptography.

6.2 Starting from m-subsequences

Known results about decimation [14] take into account subfield relation $\mathbb{F}_{p^h} \hookrightarrow \mathbb{F}_{p^k}$ for $k = hl$, with a given primitive element $\alpha \in \mathbb{F}_{p^k}$ and any $\omega \in \mathbb{F}_{p^k}$, along trace considerations; a m-sequence s of length $p^k - 1$ is thus written as a $\left(p^{k-h} + \ldots + 1\right) \times \left(p^h - 1\right)$ matrix whose columns are either a m-sequence t of

length $p^h - 1$ or a null sequence ($p^{k-2h} + \ldots + 1$ total occurrences). But one may try to tuild s by a checksum involving t, using no upward knoledge. Shift-and-add/-subtract properties are yet the cornerstone and a special empirical structure comes out.

Definition 6.2 *For k, h, l as above, a l-skeleton is a configuration of $p^{k-2h} + \ldots + p^h + 1$ positions in a closed sequence of length $p^{k-h} + \ldots + 1$ such that:*

1. *there is one and only one largest block of $l - 1$ consecutive positions;*
2. *number of positions at distance d is the same $\forall 1 \leq d \leq \left(p^{k-h} + \ldots + p^h\right)$, where distances need not to be counted in the same block.*

A l-skeleton can be computed by an independent task and, as a relevant fact, m-subsequence t seems to occupy positions around a l-skeleton; moreover, let ψ_d be a trasformation that exchanges columns of s for $MCD(d; p^{k-h} + \ldots + 1) = 1$, that is nothing but a decimation on columns; obviously, property (2) of a l-skeleton is invariant under ψ_d and, for p, k low, property (1) is invariant too. As the most relevant fact, the shape of a l-skeleton is invariant under some ψ_d's and empirical counting gives unproved formula

$$\frac{\phi\left(p^k - 1\right)}{k} \approx \frac{\phi\left(p^h - 1\right)}{h} \frac{\phi\left(p^{k-h} + \ldots + 1\right)}{\phi\left(l\right)}$$

where $\left(p^{k-h} + \ldots + 1\right) / \phi\left(l\right)$ is candidate total number of l-skeletons.

Given a l-skeleton and a m-sequence t as above, following heuristic tool is effective for add/subtract checksum:

- fix a block of order $\left(p^h - 1\right) \times l$

$$\begin{bmatrix} 0 & \ldots & 0 & s_1 \\ \vdots & & \vdots & \vdots \\ 0 & \ddots & 0 & s_{p^h - 1} \end{bmatrix}$$

  with only one non-null column;

- choose a checksum block of order $\left(p^h - 1\right) \times (l + 1)$

$$B(i,j) = \begin{bmatrix} s_i & \ldots & s_i & s_j \\ s_{i+1} & \ldots & s_{i+1} & s_{j+1} \\ \vdots & & \vdots & \vdots \\ s_{i-1} & \ddots & s_{i-1} & s_{j-1} \end{bmatrix}$$

  where first row is aligned with $(0; \ldots; 0; s_1)$ in previous block;

- each admissible location for $B(i,j)$, where $1 \leq i \neq j \leq (l-1)$, gives one and only one completion in full matrix, as far as either s is completed or a wrong values occurs.

Exact control occurs at nearest boundary around empty colums where checksum block is placed inside l-skeleton; dimension of this computation has been no further investigated and it can be surely optimized.

6.3 Other combinatorial regularities

Remark 6.1 *Fix a m-sequence for F_{q^2} and a matricial representation*

$$\begin{array}{ccccc} \rightarrow & 1 & \cdots & 0 & \rightarrow \\ \rightarrow & \alpha & & 0 & \rightarrow \\ & \vdots & \ddots & \vdots & \\ \rightarrow & \alpha^{-1} & \cdots & 0 & \rightarrow \end{array}$$

with α primitive for $\mathbb{F}_q$, columns from 1 (second index) to $p-1$ are made of transversal shifts of the first column (considered as cyclic) satysfing the conditions:

- $t_k + t_{p-k} = q$
- $\tau_{\frac{q-1}{2}} = \frac{q+1}{2}$, $\tau_{\frac{q-1}{2}-k} - \tau_{\frac{q-1}{2}+k} = \pm k$ where the sign is uniform for all k.

Such a regularity property allows to break down the number of combinations for transversal shifts and, since a regular location of 1 values implies a regularity for all the others, an equivalent formulation for this property is: given two consecutive zeroes $0_i \overset{p+1}{-} 0_{i+1}$, for each value a one has:

$$0_i \overset{d}{\longleftrightarrow} a \overset{p+1-d}{\longleftrightarrow} 0_{i+1} \Leftrightarrow 0_{\left(i-\frac{p+1}{2}+d\right)} \overset{p+1-d}{\longleftrightarrow} a \overset{d}{\longleftrightarrow} 0_{\left(i-\frac{p-1}{2}+d\right)}$$

7 A path towards the Riemann Hypothesis

Since shift-and-add- properties are intrinsic in power structures modulo decimations, some concluding remarks open a glimpse on a physical scenario; basic elements for such a transition are:

- additive structure in $\mathbb{Z}_n$ is a low-level interaction ("thermodynamical") and allows to built an upper structure if and only if n is a prime;
- non-nullity and permanence are global self-organizational properties and allow iterative construction of m-sequences of order p^k for any k;
- structural relation of m-sequences is invariance under global cyclic sums, that tend to be dissipative, but cannot change any m-sequence, due to shift-and-add- properties.

Wherever considerations about self-organization and stability can be carried out, a way is open towards an operative definition where primes p, prime powers p^k and composite integers $n = \prod_i p_i^{\alpha_i}$ are distinguished by means of a physical

dictionary, and processes of interaction (thus dynamics) between primes can be considered.

Such an opportunity is already written in elementary number theory itself: where is a prime number located ? and what does "where" means ? It means something about additive location, but it is driven by multiplicative structure, so this property seems a bit frustrating: a prime is located in a position at the same time fixed but undetermined (up to present knoledge) and this property involves a clear relation amongst primes: a prime falls wherever no lower prime (or any of its multiples) falls; one can try to write down such a rule as an interaction (a dynamics) between primes that compute altogether theire relative (as an outcome of interaction) or absolute (because they are fixed) positions and Riemann's ζ-function may have its place in such a frame.

7.1 Hilbert-Polya conjecture and its environement

In never-too-much-famous 8-pages Riemann's paper [25] defined complex function $\zeta(s)$ and posed known hypothesis ($\mathcal{RH}$ from now on) about location of prime numbers; a great amount of theoretical work succeded, in order to attack that conjecture on many battlefields. A deep suggestion was born from informal communications between Hilbert and Polya (see Odlyzko home page [23]) and the outcome has been an idea fully immersed in Physics: $\mathcal{RH}$ would be true if non-trivial zeros are related to eigenvalues of some hermitian matrix.

Further research enlighted a strong similarity between statistics of zeroes and GUE eigenvalues (see [26]) and went on enough to give many expected properties (see [3]), together with a deep confirmation of GUE statistics for ζ-functions over finite fields (see [17]). As a very relevant fact, physical analogies have been correctly posed in many aspects of Number Theory and, since scientific research often makes large amounts of analogies to become reality, some areas have grown, that can just be listed: Unified Field Theory, linked to $\mathcal{RH}$ via Noncommutative Geometry; black hole analogies, used to describe arithmeticity in gravitation theory; string theory and tools from p-adic and adelic Analysis.

The most prominent adherence is however in p-adic analysis (an important overview is [5]; original Hilbert-Polya conjecture suggested a matrix to describe such a dynamics and a p-adic matrix, as reported by [26], was Paul Cohen's line to approach $\mathcal{RH}$. But p-adic Analysis has been focused also for purely physical suggestions by Volovic *et alii* in a monography [30] and by Volovic alone in a seminal paper [29]. Two deep insights are sketched in the latter:

1. suggestion to abandon the Archimedean axiom at Planck scale, since (cited) 'this is a physical axiom which concerns the process of measurement', leads the author to think about Physics over p-adic fields (a road eventually taken by the author itself and by many others, see [2]);

2. suggestion to think about fluctuations of ground field, since (cited) 'all physical parameters undergo quantum fluctuations', leads the author to invoke use of automorphic functions (apart from cited report, this road has many confluences, mainly following Langlands program, see [21]).

Physical propositions are shifted into the kernel of Number Theory, a neo-pythagorism calling from a new order of *phœnomena* (see e.g. Seminar [22]); but also mathematical propositions come out from some intial phœnomenology (regularities observed in mathematical objects), fully satisfied by proved theorems. An arrow opposite to ordinary Mathematical Physics leads to a framework of Physical Mathematics.

7.2 A Physics of Mathematics

Deepest question only hinted in [29] is: build a physical theory upon finite fields; even if some suggestions are listed, the author seems to omit farest boundaries of this new horizon: ground fields can be subjected, like any other "object", to physical considerations.

Recent developments by He [15] move along this road.

Arguments collected in present article suggest to study whether numerical objects can have some *evolution* in some *space-time* or, equivalently, what does *move*, or *happen*, and *where*. Available materials can be collected in a (random) path along Number Theory, in order to find some arguments for a Physics in finite fields.

7.2.1 Characteristic p, thermodynamics and information

Basic property of $\mathbb{F}_{p^k}$ as an additive structure, $a + \ldots + a = 0$ (p times) defines characteristic for $a = 1$ and $1 + \ldots + 1 = 0$ (p times) means that any incremental operation goes back to 0. It is a remarkable fact that characteristic is always a prime p, since this allows cyclicity of $\mathbb{F}^{\times}$ as a group and irreducibility of polynomial needed to build $\mathbb{F}^{\times}_{p^k}$. Now, $+1$ is an elementary increment in any algebraic structure and skill to hold information is a basic property of m-sequences, so one can push on the analogy and look at characteristic as a quantity related to *entropy*; this implies usual equivalences between time arrow, information and similar concepts; but this implies that thermodynamics in finite fields violates second principle of thermodynamics, that means: some structures in finite fields have non-dissipative properties.

Thermodynamical-like properties indeed already came out in previous sections: primitive roots are fully determined by their relative global location (rules given by Euler ϕ) but their additive location has no known rule, a hint of *maximum entropy* principle, since they tend to occupy additive positions as random as possible. Difficulties in proving properties about primitive roots are well known (see [24]) and show some analogies between additive/multiplicative properties and thermodynamics:

- study statistical location of primitive roots for $\mathbb{F}_p$ (where p is big enough) and for $\mathbb{F}_{p^k}$;
- study whether primitive roots satisfy any maximality condition, in order to occupy maximum space available;

- compare it with some statistics of prime numbers in $\mathbb{N}$, since primitive roots for $\mathbb{F}_p$ resemble primes in $\mathbb{N}$.

7.2.2 p-adic numbers, locality and globality

Attempts to put p-adic numbers as the main wall separating $\mathcal{RH}$ and Physics opened some advanced lines of attack by means of p-adic strings or by a dynamical system defined *ad hoc* by Bost and Connes ([4]). Little attention has yet been put to a strong analogy: a particle is localized, a wave is global; equivalently, a prime p is localized, its $p-$-adic space balls is everywhere dense in $\mathbb{N}$.

Uncertainty conditions hold in following sense: prime numbers show global regularity (the whole structure of a prime p) and local randomness (additive location of a prime); in fact, additive $+1$ scale is of the same size as additive location. This may seem just another formulation of Heisenberg principle.

7.2.3 Singularities, space and time

Hilbert-Polya conjecture evokes a quantum-dynamical system but it is relevant that some advanced physical lines of research come instead from a non-commutative geometric setting (see [10]) with a short-circuit between Unified Field Theory and $\mathcal{RH}$.

Objects more often recalled in such a frame are black holes)considered in an abstract setting as singular solutions of space-time-like equations) and strings.

Black holes are often requested to fill in arithmetical properties of string theory ([10]) or come out in compactification techniques (from celebrated [6]). Yet stronger words can be cited from [19] about $2+1$ gravitation theory: 'black holes make universe arithmetic'. Recent results ([16]) hint another bridge to type II strings.

It is indeed quite immediate to look at a finite field as a black hole: a singularity, a clear separation of an inner horizon (p-adic or in characteristic p) where some space-time collapses, but such a setting is only propedeutic.

Such an amount of analogies leads to an overall scenario, that one can try to sketch.

7.3 Dynamics of numbers and the Riemann ζ-function

Fix $\mathbb{Z}_n$ as a set of values where global random additive exchanges happen; for n composite, all of these processes either fall in 0 or are incomplete or don't go back to 1 and no stable line of universe can be started; but for $n = p$ prime, non-null values find a self-organization stable under iterated global sums and each prime defines a singular universe, held together by stability properties, with a great amount of indeterminism, due to purely combinatorial rules: generators of multiplicative structure are exactly enumerated but indistinct and exchange one eachother by Euler ϕ-function.

Concatenation of non-null values, as performed in m-sequences, makes effective proximity relation and stability effective; one can represent central singularity of a prime field $\mathbb{F}_p$ by means of a choosen m-sequence or, equivalently, a choosen sequence of $(a_i)_{i=1}^{p-1}$ of non-null p-digits where a is primitive, central 0 means collapse of information and values have an almost spatial closeness by means of consecutive powers; this structure satisfies many invariance properties to be used as a primordial space structure: first of all, it comes out as a relation amongst objects.

Thus m-sequences (or, more generally, linear and algebraic sequences) may have relevant links to random matrices and GUE statistics, since they both show randomness properties.

Construction of primordial space properties could take into account two landscapes: Grothendieck's topoi (see [7]), where functions necessary to define space come from truth tables, and Łukasiewicz's logics $Ł_n$, that are functionally pre-complete if and only if $n-1$ is a prime; these give, together, Grothendieck's topoi with basic truth values choosen in $Ł_n$. Another perspective is to look at prime fields $\mathbb{F}_p$ as quantum processors, where each higher $\mathbb{F}_{p^k}$ is needed as a computing device.

While more than one theoretical setting can be applied to give a primitive definition of space inside a finite field, possible definition of time seems to be just one: arrow time as a thermodynamical quantity, that is arrow of increasing information (entropy).

One can study some topology (maybe algebraic) relating consecutive values $+1$ as additive or exponential increment; one can also extend, by means of some product (maybe topological), sequence $(a_i)_i$ to any higher degree sequence for $\mathbb{F}_{p^k}$; properties defining a m-sequence of length p^k-1 have much in common with properties of a space texture: global relation amongst elements, stability under global additive exchanges and under base change, dimension k (since k copies are needed); the most relevant property is localization: each value $1 \leq n \leq p^k-1$ is uniquely located in each copy of s, a sort of cohordinate system.

Evolution of $\mathbb{F}_{p^k}$'s is thus an effective self-evolution and both structures (additive and multiplicative, where additive is sequential in k and multiplicative is by relation $\mathbb{F}_{p^h} \hookrightarrow \mathbb{F}_{p^k}$ when $h|k$) keep the same basic proximity properties.

Whole structure ruled by $\mathbb{F}_p$ is $\mathbf{F}_p = \bigcup_{k\geq 1} \mathbb{F}_{p^k}$: this is *world* or *universe* in characteristic p, with its closed inner (physical) rules. Its outer limit can be made of p-adic numbers, that are no more in characteristic p, but are built upon it according to sub-mersions $\mathbb{F}_{p^k} \hookrightarrow \mathbb{F}_{p^{k+1}}$, due to limit definition of $\mathbb{Q}_p$, or even by enormous completion Ω_p (see [1]); but one can speak about an *outer limit* if and only if any *out* can be focused, and possible interactions between structures in different characteristic have to be considered, since out of a world in characteristic p there are worlds in other characteristics.

7.4 Conflict between characteristics

It is reasonable to say that, if one passes from $\mathbb{F}_{p^k}$ to either $\mathbb{F}_{p^{k+1}}$ or $\mathbb{F}_{p^{kh}}$, information increases, between either linear spaces or super-fields; but this happens

only in a strict sense: due to characteristic p, information in $\bigcup_{k\geq 1}\mathbb{F}_{p^k}$ increases only in a multiplicative sense.

Attempts to describe formally any sort of interaction between different characteristics gives unstable situations, but it is arguable that any attempt to put side-by-side different characteristics leads to an effective superposition of states, and two research lines start here:

- distinct characteristics p and $p^{'}$ build a world outer to both (the first world really outer to both), with some tensorial properties;
- multiplications in different characteristics (and, in general, factorization of composite integers) cohexist in superposed (maybe entangled) states.

Quantum-mechanical considerations would exactly come out, as quantum information, from computational properties and additive values begin to find a relative location, when spaces homogenize.

As a relevant property, factorization can be polynomially computed by quantum registers, as Shor's algorithm ([27]) proves.

7.5 Commesuration of primes and Riemann's ζ

If any representation of merged characteristics is possible, then multiplicative structure built up together by different primes leads step-by-step to a higher entropy and to a greater exchange of information; apply some thermodynamic limit and last object appears: a dynamics (in a global sense of inner evolution) that makes all primes com-mensurable, that is equally measured each one by the other.

One can at least argue that any dynamical system formalizing previous scenario *implies* some relation with function ζ, since reciprocal location (that is, interaction) of all primes gives monoid $\mathbb{N}$.

Where could any confirmation or confutation of $\mathcal{RH}$ be looked for? According to path traced insofar, its truth seems to follow from some global regularization leading to $\sigma = \frac{1}{2}$ as a shared exponent where primes recognize, compute and put aligned one eachother.

Indeed, absolute primality of a given n, proved if relative primality of n with any prime $p \leq n^{1/2}$ holds, is a property not exactly marginal but intrinsic: as soon as $n = p_i p_j$, value $\frac{1}{2}$ is central exponent for any possible decomposition from below (note that relative primality with any prime between $n^{1/2}$ and $n-1$ is unuseful) and a correct, shared arrow from-below-to-above can be created by a complete exchange of information between prime fields.

References

[1] M.R.Alain, *A course in p-adic analysis*, Springer Verlag, 2000.

[2] M.V.Altaisky, B.G.Sidarth, *p-Adic physics below and above Planck scale*, `arxiv:gr-qc/9802034`.

[3] M.Berry, Keating, $H = xp$ *and the Riemann zeros*, in Supersymmetry and Trace Formulae: Chaos and Disorder, Kluwer Acad. Pub.

[4] J.-B.Bost, A.Connes, *Hecke Algebras, Type III factors and phase transitions with spontaneous symmetry breaking in number theory*, Selecta Mathematica, New Series 1, n.3 (1995).

[5] L.Brekkea and P.G.O.Freund, *p-adic numbers in Physics*, Physics Reports Vol. 233, Issue 1 (1993), pp. 1-66.

[6] M.Banados, C.Teitelboim, J.Zanelli, *The Black Hole in Three Dimensional Space Time*, preprint at `http://www.arxiv.org`.

[7] P.Cartier, *A mad day's work: from Grothendieck to Connes and Kontsevich. The evolution of concepts of space and symmetry*, Bull.Amer.Math.Soc. Volume 38, nr. 4.

[8] C.Castro, various preprints at `http://vixra.org/`.

[9] C.Castro, J.Mahecha, *Final steps towards a proof of the Riemann hypothesis*, at `www.arxiv.org`.

[10] A.Connes, M.Marcolli, *Noncommutative Geometry, Quantum Fields and Motives*, AMS Colloquium Publications, vol. 55.

[11] Richard Crandall, Carl Pomerance, *Prime Numbers. A computationa perspective*, Springer.

[12] L.E.Dickson, *History of the Theory of Numbers, vol. 1*, Chelsea.

[13] S.Golomb, *Shift Register Sequences*, Aegean Park Press, 1982.

[14] M.Goresky, A.Klapper, *Algebraic Shift Register Sequences*, draft available at `www.cs.uky.edu`.

[15] Y.-H. He, *On Fields over Fields*, `arxiv:1003.2986`.

[16] Y.-H. He, V.Jejjala, D.Minic, *On the Physics of Riemann zeros*, `arxiv:1004.1172v1`.

[17] N.M.Katz, P.Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, AMS Coll. Publ., vol. 45.

[18] H.Iwaniec, E.Kowalski, *Analitic Number Theory*, AMS Coll. Publ., vol. 53.

[19] A.L.Kholodenko, *Statistical Mechanics of* $2+1$ *Gravity From Riemann Zeta Function and Alexander Polynomial:Exact Results*, J.Geom.Phys. 38 (2001).

[20] R.Lidl, H.Niederreiter, *Introduction to finite fields and their applications*, Cambridge Univ. Press.

[21] Links to Langlands program at `http://mathworld.wolfram.com`.

[22] *Number Theory and Physics at the Crossroads*, 2006 Banff International Research Station for Mathematical Innovation and Discovery.

[23] Correspondence about the origins of the Hilbert-Polya Conjecture in A.Odlyzko site at `http://www.dtc.umn.edu/`.

[24] P.Ribenboim, *The New Book of Prime Number Records*, Springer.

[25] B.Riemann, *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse*, available at `http://www.maths.tcd.ie`.

[26] D.Rockmore, *Stalking the Riemann Hypothesis*, Pantheon Pub.

[27] P.W.Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J.Sci.Statist.Comput. 26 (1997).

[28] Richard P.Stanley, *Enumerative Combinatorics*, Cambridge University Press.

[29] I.V.Volovic, *Number theory as the ultimate physical theory*, CERN-TH.4781/87.

[30] V.S.Vladimirov, I.V.Volovic, E.I.Zelenov, *p-adic Analysis and Mathematical Physics*, World Scientific.