Properties of sets with digital restrictions

Manfred G. Madritsch

Department for Analysis and Computational Number Theory
Graz University of Technology
madritsch@tugraz.at

Journées Numération
27 May 2008

joint work with **Jörg M. Thuswaldner**, University of Leoben.

Supported by the Austrian Research Fund (FWF), Projects S9603, S9610 and S9611.

Outline

Digital restrictions

Number systems over $\mathbb{F}_q[X]$

Number systems over $\mathbb{F}_q[X, Y]/p(X, Y)\mathbb{F}_q[X, Y]$

Summary

Number systems over $\mathbb{Z}$

- Let $q \geq 2$ be an integer. Then every positive integer n can be represented in the form

$$n = \sum_{\ell \geq 0} d_\ell q^\ell.$$

- We call a function f strictly q-additive if it acts on the q-ary digits of a number. E.g. the sum of digits function

$$s_q(n) = \sum_{\ell \geq 0} d_\ell.$$

Number systems over $\mathbb{Z}$

- Let $q \geq 2$ be an integer. Then every positive integer n can be represented in the form

$$n = \sum_{\ell \geq 0} d_\ell q^\ell.$$

- We call a function f strictly q-additive if it acts on the q-ary digits of a number. E.g. the sum of digits function

$$s_q(n) = \sum_{\ell \geq 0} d_\ell.$$

The digitally restricted set

Let $q_1, \ldots, q_r$ be coprime positive integers, $j_1, \ldots, j_r$ and $m_1, \ldots, m_r$ be positive integers. Then we define the set

$$\mathcal{S} := \{n \in \mathbb{N} : f_1(n) \equiv j_1 \pmod{m_1}, \ldots, f_r(n) \equiv j_r \pmod{m_r}\},$$

where f_i is a q_i-additive function.

The distribution within the set $\mathcal{S}$

Let H the subgroup generated by the digital restrictions, *i.e.*

$$H := \{(s_{q_1}(n) \equiv j_1\,(m_1), \ldots, s_{q_r}(n) \equiv j_r\,(m_r)) : n \geq 1\}\,.$$

Then Kim could show the distribution into these classes.

Theorem Kim (1999)

$$\frac{1}{N}(\mathcal{S} \cap [1, N]) = \frac{1}{\#H} + \mathcal{O}\left(N^{-\delta}\right)$$

where $\delta > 0$.

The distribution within the set $\mathcal{S}$

Let H the subgroup generated by the digital restrictions, *i.e.*

$$H := \{(s_{q_1}(n) \equiv j_1\,(m_1), \ldots, s_{q_r}(n) \equiv j_r\,(m_r)) : n \geq 1\}\,.$$

Then Kim could show the distribution into these classes.

Theorem Kim (1999)

$$\frac{1}{N}(\mathcal{S} \cap [1, N]) = \frac{1}{\#H} + \mathcal{O}\left(N^{-\delta}\right)$$

where $\delta > 0$.

Waring's problem and uniform distribution

- We look for an asymptotic formula for the number of solutions of

$$n = x_1^k + \cdots + x_s^k, \quad x_1, \ldots, x_s \in \mathcal{S}.$$

- We order the elements of $\mathcal{S}$ by the sequence $(s_i)_{i\geq 0}$. Is the sequence

$$(h(s_i))_{i\geq 0}$$

uniformly distributed modulo 1 for h a polynomial with at least one irrational coefficient?

Waring's problem and uniform distribution

- We look for an asymptotic formula for the number of solutions of

$$n = x_1^k + \cdots + x_s^k, \quad x_1, \ldots, x_s \in \mathcal{S}.$$

- We order the elements of $\mathcal{S}$ by the sequence $(s_i)_{i \geq 0}$. Is the sequence

$$(h(s_i))_{i \geq 0}$$

uniformly distributed modulo 1 for h a polynomial with at least one irrational coefficient?

An idea of Gelfond

The main rôle in the proof is played by the following exponential sum, which can be rewriten in the following way.

$$\sum_{\substack{n\leq N\\ n\in\mathcal{S}}} e\left(h(n)\right) = \frac{1}{m_1\cdots m_r}\sum_{r_i=0}^{m_1-1}\cdots\sum_{r_i=0}^{m_1-1} e\left(-\sum_{i=1}^{r}\frac{r_i j_i}{m_i}\right)$$

$$\times \sum_{n\leq N} e\left(h(n)+\sum_{i=1}^{r}\frac{r_i}{m_i}f_i(n)\right)$$

where $e(x) := \exp(2\pi i\, x)$.

Higher correlation

In order to estimate the exponential sum one has to apply the method of Weyl differences and thus consider correlations of the form

$$\sum_{h_1 \leq H_1} \cdots \sum_{h_k \leq H_k} \left| \sum_{n \leq N} e\left(\frac{r_i}{m_i} \Delta_k(s_{q_i}(n); h_1, \ldots, h_k) \right) \right|^2 .$$

The main problem here is the carry propagation within the higher correlation sums.

Waring's Problem with digital restrictions

Theorem Thuswaldner, Tichy (2005)

The equation

$$n = x_1^k + \cdots + x_s^k, \quad s_q(x_1) \equiv j_1\,(m_r), \ldots, s_q(x_s) \equiv j_s\,(m_s),$$

has always a solution for sufficiently large n provided that s is large in terms of k.

Theorem Wagner (2007)

The same holds for the equation

$$n = x_1^k + \cdots + x_s^k, \quad x_1, \ldots, x_s \in \mathcal{S}.$$

Waring's Problem with digital restrictions

Theorem Thuswaldner, Tichy (2005)

The equation

$$n = x_1^k + \cdots + x_s^k, \quad s_q(x_1) \equiv j_1\,(m_r), \ldots, s_q(x_s) \equiv j_s\,(m_s),$$

has always a solution for sufficiently large n provided that s is large in terms of k.

Theorem Wagner (2007)

The same holds for the equation

$$n = x_1^k + \cdots + x_s^k, \quad x_1, \ldots, x_s \in \mathcal{S}.$$

Overview

	$\mathbb{Z}$	$\mathbb{F}_q[X]$	$\mathbb{F}_q[X,Y]$
q-additive functions	Kim		
Uniform Distribution			
Waring's Problem	Thuswaldner Tichy Wagner		

Outline

Digital restrictions

Number systems over $\mathbb{F}_q[X]$

Number systems over $\mathbb{F}_q[X,Y]/p(X,Y)\mathbb{F}_q[X,Y]$

Summary

Definitions of the "integers" and the "reals"

- Finite field: $\mathbb{F}_q$ with $q = p^n$ elements.
- Valuation at infinity: For $A = P/Q \in \mathbb{F}_q(X)$

$$\nu_\infty(A) := \deg Q - \deg P, \quad |A|_\infty = q^{-\nu_\infty(A)}.$$

- Completition of $\mathbb{F}_q$: $\mathbb{F}_q((X^{-1}))$ the set of formal Laurent series.
- Elements: For $\alpha \in \mathbb{F}_q((X^{-1}))$ we get that

$$\alpha = \sum_{k=\nu_\infty(\alpha)}^{\infty} a_k X^{-k} \quad (a_k \in \mathbb{F}_q).$$

Definitions of the "integers" and the "reals"

- Finite field: $\mathbb{F}_q$ with $q = p^n$ elements.
- Valuation at infinity: For $A = P/Q \in \mathbb{F}_q(X)$

$$\nu_\infty(A) := \deg Q - \deg P, \quad |A|_\infty = q^{-\nu_\infty(A)}.$$

- Completition of $\mathbb{F}_q$: $\mathbb{F}_q((X^{-1}))$ the set of formal Laurent series.
- Elements: For $\alpha \in \mathbb{F}_q((X^{-1}))$ we get that

$$\alpha = \sum_{k=\nu_\infty(\alpha)}^{\infty} a_k X^{-k} \quad (a_k \in \mathbb{F}_q).$$

Definitions of the "integers" and the "reals"

- Finite field: $\mathbb{F}_q$ with $q = p^n$ elements.
- Valuation at infinity: For $A = P/Q \in \mathbb{F}_q(X)$

$$\nu_\infty(A) := \deg Q - \deg P, \quad |A|_\infty = q^{-\nu_\infty(A)}.$$

- Completition of $\mathbb{F}_q$: $\mathbb{F}_q((X^{-1}))$ the set of formal Laurent series.
- Elements: For $\alpha \in \mathbb{F}_q((X^{-1}))$ we get that

$$\alpha = \sum_{k=\nu_\infty(\alpha)}^{\infty} a_k X^{-k} \quad (a_k \in \mathbb{F}_q).$$

Haar measure and character E

- Haar measure: For all $\beta \in \mathbb{F}_q((X^{-1}))$

$$\int_{\nu_\infty(\alpha-\beta)<-n} 1 \cdot \mathrm{d}\alpha = q^{-n}.$$

- Character: $\operatorname{Res}(\alpha)$ is the coefficient of X^{-1} of α.

$$E(\alpha) := \exp\left(2\pi i \operatorname{tr}(\operatorname{Res}\alpha)/p\right),$$

where $\operatorname{tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the usual trace of an element of $\mathbb{F}_q$ in $\mathbb{F}_p$.

Haar measure and character E

- Haar measure: For all $\beta \in \mathbb{F}_q((X^{-1}))$

$$\int_{\nu_\infty(\alpha-\beta)<-n} 1 \cdot \mathrm{d}\alpha = q^{-n}.$$

- Character: $\mathrm{Res}(\alpha)$ is the coefficient of X^{-1} of α.

$$E(\alpha) := \exp\left(2\pi i \,\mathrm{tr}(\mathrm{Res}\,\alpha)/p\right),$$

where $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the usual trace of an element of $\mathbb{F}_q$ in $\mathbb{F}_p$.

Q-ary digital expansion

- Q-ary digital expansion: Fix $Q \in \mathbb{F}_q[X]$, then for $A \in \mathbb{F}_q[X]$

$$A = \sum_{i \geq 0} D_i Q^i \qquad (\deg D_i < \deg Q).$$

- Strongly Q-additive:
  A function $f : \mathbb{F}_q[X] \to \mathbb{F}_q[X]$ is called strongly Q-additive if

$$f(A) := \sum_{i \geq 0} f(D_i).$$

Q-ary digital expansion

- Q-ary digital expansion: Fix $Q \in \mathbb{F}_q[X]$, then for $A \in \mathbb{F}_q[X]$

$$A = \sum_{i \geq 0} D_i Q^i \qquad (\deg D_i < \deg Q).$$

- Strongly Q-additive:
  A function $f : \mathbb{F}_q[X] \to \mathbb{F}_q[X]$ is called strongly Q-additive if

$$f(A) := \sum_{i \geq 0} f(D_i).$$

The general setting

- Fix Q_i-additive functions f_i $(1 \leq i \leq r)$ and consider the set

$$\mathcal{S} := \{A \in \mathbb{F}_q[X] : f_1(A) \equiv J_1\,(M_1), \ldots, f_r(A) \equiv J_r\,(M_r)\}.$$

- By $(S_\ell)_{\ell \geq 0}$ we denote a sequence through all elements of $\mathcal{S}$ such that $m \leq n \Rightarrow \deg S_m \leq \deg S_n$.

The general setting

- Fix Q_i-additive functions f_i $(1 \leq i \leq r)$ and consider the set

$$\mathcal{S} := \{A \in \mathbb{F}_q[X] : f_1(A) \equiv J_1 \,(M_1), \ldots, f_r(A) \equiv J_r \,(M_r)\}.$$

- By $(S_\ell)_{\ell \geq 0}$ we denote a sequence through all elements of $\mathcal{S}$ such that $m \leq n \Rightarrow \deg S_m \leq \deg S_n$.

The distribution into the different residue classes

As in the case of number systems over $\mathbb{Z}$ we could consider the distribution into residue classes. Therefore let H denote the subgroup generated by the set $\mathcal{S}$, *i.e.*,

$$H := \{(f_1(A) \equiv J_1\,(M_1), \ldots, f_r(A) \equiv J_r\,(M_r)) : A \in \mathbb{F}_q[X]\}.$$

Then M and Thuswaldner (2008) could show by the methods of Drmota and Gutenbrunner (2005) that

$$\frac{1}{N}\#\{Z_\ell \in \mathcal{S} : 0 \le \ell < N\} = \frac{1}{\#H} + \mathcal{O}\left(N^{-\delta}\right)$$

with $\delta > 0$.

The distribution into the different residue classes

As in the case of number systems over $\mathbb{Z}$ we could consider the distribution into residue classes. Therefore let H denote the subgroup generated by the set $\mathcal{S}$, *i.e.*,

$$H := \{(f_1(A) \equiv J_1\,(M_1), \ldots, f_r(A) \equiv J_r\,(M_r)) : A \in \mathbb{F}_q[X]\}.$$

Then M and Thuswaldner (2008) could show by the methods of Drmota and Gutenbrunner (2005) that

$$\frac{1}{N}\#\{Z_\ell \in \mathcal{S} : 0 \leq \ell < N\} = \frac{1}{\#H} + \mathcal{O}\left(N^{-\delta}\right)$$

with $\delta > 0$.

The exponential sum

In this number field the exponential sum looks similar to that in $\mathbb{Z}$. Thus we have to consider

$$\sum_{\ell=0}^{N-1} E\left(h(Z_\ell) + \sum_{i=1}^{r} \frac{R_i}{M_i} f_i(Z_\ell)\right)$$

where $(Z_\ell)_{\ell\geq 0}$ is a sequence of all elements of $\mathbb{F}_q[X]$ such that

$$m \leq n \Rightarrow \deg Z_m \leq \deg Z_n$$

for all $m, n \in \mathbb{N}$.

Higher correlation

In order to estimate the exponential sum on the slide before we have again to consider higher correlation of the following form

$$\sum_{\deg H_1 < h_1} \cdots \sum_{\deg H_k < h_k} \left| \sum_{\ell=0}^{N-1} E\left(\sum_{i=1}^{r} \frac{R_i}{M_i} \Delta_k(f_i(Z_\ell); H_1, \ldots, H_k) \right) \right| .$$

Here we do not have to cope with carry propagation therefore we could get the effect of cancelation.

Uniform distribution

Theorem M,Thuswaldner (2008)

Let h be a polynomial of degree $0 < k < p = \operatorname{char}\mathbb{F}_q$. Then

the sequence $h(S_i)$ is uniformly distributed in $\mathbb{F}_q((X^{-1}))$
if and only if
at least one coefficient of $h(Y) - h(0)$ is irrational.

Corresponding problem of Waring

Theorem M (200?)

For $N \in \mathbb{F}_q[X]$ the equation

$$N = P_1^k + \cdots + P_s^k, \quad \left(P_i \in \mathcal{S}, \deg P_i < \left\lceil \frac{\deg N}{k} \right\rceil\right)$$

always has a solution provided N has sufficiently large degree and $s > k2^k$.

Overview

	$\mathbb{Z}$	$\mathbb{F}_q[X]$	$\mathbb{F}_q[X, Y]$
q-additive functions	Kim	Drmota Gutenbrunner	
Uniform Distribution		M Thuswaldner	
Waring's Problem	Thuswaldner Tichy Wagner	M	

Outline

Digital restrictions

Number systems over $\mathbb{F}_q[X]$

Number systems over $\mathbb{F}_q[X,Y]/p(X,Y)\mathbb{F}_q[X,Y]$

Summary

Number systems over function fields

Number systems in these fields have been investigated by Scheicher and Thuswaldner. In a more recent paper these considerations were extended to arbitrary fields by Beck, Brunotte, Scheicher and Thuswaldner.
We get the following characterization.

Theorem Scheicher, Thuswaldner
If $p(X, Y)$ is monic in X and Y then every $A \in \mathbb{F}_q[X, Y]$ has an unique and finite expansion by

$$A = \sum_{i \geq 0} D_i Y^i \qquad (D_i \in \mathbb{F}_q[X], \deg D_i < \deg_X p).$$

Y-additive functions

Strongly Q-additive: A function $f : \mathbb{F}_q[X,Y] \to \mathbb{F}_q[X,Y]$ is called strongly Y-additive if it acts on the D_i only. *E.g.* the sum of digits function, which is defined by

$$s_Y(A) := \sum_{i \geq 0} D_i.$$

The general setting

- We fix only one Y-additive f and consider the set

$$\mathcal{S} := \{A \in \mathbb{F}_q[X, Y] : f(A) \equiv J\,(M)\}$$

The function field

- In order to apply Hardy and Littlewood's circle method we need to consider extensions of the valuation ν defined above to ω for the function field.
- We can represent Y as a Laurent-series with rational exponents and thus deduce the value of Y according to the valuation ω.
- Finally we can look at the function field as an algebraic curve and apply Riemann-Roch. Thus we restrict ourselves to sufficiently large spaces according to the valuation.

The function field

- In order to apply Hardy and Littlewood's circle method we need to consider extensions of the valuation ν defined above to ω for the function field.
- We can represent Y as a Laurent-series with rational exponents and thus deduce the value of Y according to the valuation ω.
- Finally we can look at the function field as an algebraic curve and apply Riemann-Roch. Thus we restrict ourselves to sufficiently large spaces according to the valuation.

The function field

- In order to apply Hardy and Littlewood's circle method we need to consider extensions of the valuation ν defined above to ω for the function field.
- We can represent Y as a Laurent-series with rational exponents and thus deduce the value of Y according to the valuation ω.
- Finally we can look at the function field as an algebraic curve and apply Riemann-Roch. Thus we restrict ourselves to sufficiently large spaces according to the valuation.

The exponential sum

The exponential sum in this area looks like the following

$$\sum_{A\in\mathbb{B}(n)} E\left(h(A)+\frac{R}{M}f(A)\right),$$

where $\mathbb{B}$ is the set of integers in $\mathbb{F}_q(X,Y)/p(X,Y)\mathbb{F}_q(X,Y)$ over $\mathbb{F}_q[X]$.

Waring's Problem

Theorem M,Thuswaldner (200?)

If $s > k2^k$ then there always exists a solution for

$$N = P_1^k + \cdots + P_s^k \quad (P_i \in (\mathbb{B}(m) \cap \mathcal{S}))$$

provided that N is sufficiently large, where $\mathbb{B}(m)$ denotes the set of all integers with valuation ω less than m.

Outline

Digital restrictions

Number systems over $\mathbb{F}_q[X]$

Number systems over $\mathbb{F}_q[X,Y]/p(X,Y)\mathbb{F}_q[X,Y]$

Summary

Overview

	$\mathbb{Z}$	$\mathbb{F}_q[X]$	$\mathbb{F}_q[X, Y]$
q-additive functions	Kim	Drmota Gutenbrunner	
Uniform Distribution		M Thuswaldner	(M)
Waring's Problem	Thuswaldner Tichy	M	M Thuswaldner

Extensions

- For Goldbach's Problem one has to consider sums of the form
$$\sum_{p\leq P} e\left(h(p)+\sum_{i=1}^{r}\frac{r_i}{m_i}f_i(p)\right)$$
where the sum is extended over the primes.
- A possible extension of these considerations of exponential sums could be to estimate the following
$$\sum_{n\leq N} e\left(\theta n^k+\alpha s_q(n)\right)$$
for $\theta,\alpha\in[0,1)$.

Extensions

- For Goldbach's Problem one has to consider sums of the form
$$\sum_{p\leq P} e\left(h(p)+\sum_{i=1}^{r}\frac{r_i}{m_i}f_i(p)\right)$$
where the sum is extended over the primes.
- A possible extension of these considerations of exponential sums could be to estimate the following
$$\sum_{n\leq N} e\left(\theta n^k+\alpha s_q(n)\right)$$
for $\theta,\alpha\in[0,1)$.

- T. Beck, H. Brunotte, K. Scheicher, and Jörg M. Thuswaldner, *Number systems and tilings over Laurent series*, submitted (2007).
- Mireille Car, *Le problème de Waring pour l'anneau des polynômes sur un corps fini*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A141–A144.
- ______, *Waring's problem in function fields*, Proc. London Math. Soc. (3) **68** (1994), no. 1, 1–30.
- L. Carlitz, *Diophantine approximation in fields of characteristic p*, Trans. Amer. Math. Soc. **72** (1952), 187–208.
- A. Dijksma, *Uniform distribution of polynomials over* $\mathrm{GF}\{q, x\}$ *in* $\mathrm{GF}[q, x]$*. I*, Nederl. Akad. Wetensch. Proc. Ser. A 72 = Indag. Math. **31** (1969), 376–383.

- ———, *Uniform distribution of polynomials over* $\mathrm{GF}\{q,x\}$ *in* $\mathrm{GF}[q,x]$*. II*, Nederl. Akad. Wetensch. Proc. Ser. A 73=Indag. Math. **32** (1970), 187–195.
- M. Drmota and G. Gutenbrunner, *The joint distribution of Q-additive functions on polynomials over finite fields*, J. Théor. Nombres Bordeaux **17** (2005), no. 1, 125–150.
- Dong-Hyun Kim, *On the joint distribution of q-additive functions in residue classes*, J. Number Theory **74** (1999), no. 2, 307–336.
- R. M. Kubota, *Waring's problem for* $\mathbf{F}_q[x]$, Dissertationes Math. (Rozprawy Mat.) **117** (1974), 60.
- M. G. Madritsch and J. M. Thuswaldner, *Waring's Problem in Function Fields with digital restrictions*, manuscript.

- ———, *Weyl Sums in $\mathbb{F}_q[x]$ with digital restrictions*, submitted.
- K. Scheicher and J. M. Thuswaldner, *Digit systems in polynomial rings over finite fields*, Finite Fields Appl. **9** (2003), no. 3, 322–333.
- J. M. Thuswaldner and R. F. Tichy, *Waring's problem with digital restrictions*, Israel J. Math. **149** (2005), 317–344, Probability in mathematics.
- W. A. Webb, *Waring's problem in $\mathrm{GF}[q, x]$*, Acta Arith. **22** (1973), 207–220.