Vinogradov's method and some applications

Aimo Tietäväinen

Turku Centre for Computer Science
TUCS Technical Report No 28
June 1996
ISBN 951-650-784-0
ISSN 1239-1891

Abstract

In this talk we consider in an elementary way some simple problems which relate to incomplete sums and can be studied by appealing to a classical method of Vinogradov and its modifications. Vinogradov's idea was to use finite Fourier transforms in order to estimate an incomplete sum by means of complete but in some respects more complicated sums. A natural application was to estimate an incomplete sum of multiplicative characters by means of Gaussian sums. This application can be generalized in many natural ways; e.g., we may find bounds for the least nonnegative residue or nonresidue of a polynomial modulo a prime. Mordell and some others modified Vinogradov's method in order to find small solutions of congruences or small boxes containing solutions of a system of equations over finite fields. We survey these results briefly and in a very elementary way. Thereafter we consider a new interesting application. Code division multiple access systems require large families of sequences with good correlation properties. For many famous sets of sequences the full-period correlation can be easily calculated or estimated. On the other hand, though in applications the partial-period correlations may be as important as the full-period ones, they are difficult to estimate even in most well-known cases. Vinogradov's method is a device for estimating.

TUCS Research Group
Coding Theory Group

1 Vinogradov's method

Let n be a positive integer and let F be $\mathbf{Z}_n$, the set of residues modulo n. Let φ be a mapping from F to $\mathbf{C}$, the field of complex numbers. We shall consider so-called incomplete sums of the form

$$\sum_{x\in B}\varphi(x)$$

where B is a proper subset of F. Throughout this paper we shall abbreviate the complete sum $\sum_{x\in F}$ by just $\sum_x$. If $|B|$, the cardinality of B, is equal to b and if the values of φ are in a sense well distributed then

$$\sum_{x\in B}\varphi(x)=\frac{b}{n}\sum_x\varphi(x)+\quad\text{something}$$

where this something, say $A(\varphi,B)$, depends on φ and B and is small.

In order to estimate $A(\varphi,b)$ we use finite Fourier transforms. If we define, for $z\in F$,

$$\psi(z)=\sum_x\varphi(x)e_n(xz), \tag{1.1}$$

where $e_n(\alpha)=e^{2\pi i\alpha/n}$, and use the well known result

$$\sum_z e_n((x-t)z)=\begin{cases} n & \text{if} \qquad x=t \ \text{ in } \ F,\\ 0 & \text{otherwise,}\end{cases} \tag{1.2}$$

we obtain

$$\sum_z\psi(z)e_n(-tz)=\sum\varphi(x)\sum_z e_n((x-t)z)=n\varphi(t).$$

Therefore

$$\begin{aligned}\sum_{t\in B}\varphi(t) &= \tfrac{1}{n}\sum_z\psi(z)\sum_{t\in B}e_n(-tz)\\ &= \tfrac{b}{n}\psi(0)+\tfrac{1}{n}\sum_{z\neq 0}\sum_x\varphi(x)e_n(xz)\sum_{t\in B}e_n(-tz)\\ &= \tfrac{b}{n}\sum_x\varphi(x)+\tfrac{\theta}{n}\Delta(\varphi)E(B),\end{aligned} \tag{1.3}$$

where θ is a complex number whose absolute value is at most 1,

$$\Delta(\varphi)=\max_{z\neq 0}|\sum_x\varphi(x)e_n(xz)|, \tag{1.4}$$

and

$$E(B)=\sum_{z\neq 0}|\sum_{t\in B}e_n(tz)|. \tag{1.5}$$

Often we use the result (1.3) in the following form.

Theorem 1.1 (Vinogradov's inequality) We have

$$|\sum_{t\in B}\varphi(t)-\frac{b}{n}\sum_{n}\varphi(x)|\leq\frac{1}{n}\Delta(\varphi)E(B)$$

where Δ and E are defined by (1.4) and (1.5).

Vinogradov (see[41, Chapter V, Problem 12 a]) proved this result for the set of residues modulo n but we could prove Vinogradov's inequality (or, in fact, the appropriate modification of Vinogradov's inequality) for finite Abelian groups and so especially in the cases where F is $\mathbf{F}_q$, the finite field of q elements, or the linear space $\mathbf{F}_q^s$, or $\mathbf{Z}_n^m$, the set of m-tuples over $\mathbf{Z}_n$. Of course, in the latter cases the product xz must be replaced by the corresponding dot product.

Though Vinogradov's inequality is easy to understand and easy to prove, it has several interesting applications which will be considered in the sequel. Then in order to use Theorem 1.1 we should be able to calculate or to estimate the functions Δ and E.

2 Upper bounds for the function E

In general it is difficult to find good estimates of the sum

$$\sum_{t\in B}e_n(tz) \tag{2.1}$$

where z is non-zero. However, if B is a set of consecutive integers, say

$$B=\{h+1,h+2,\ldots,h+b\} \tag{2.2}$$

for some integer h, then the estimating is very easy because the sum (2.1) is geometric and therefore

$$|\sum_{t\in B}e_n(tz)|=\left|\frac{1-e_n(bz)}{1-e_n(z)}\right|\leq\frac{1}{\sin(\pi z/n)}=\quad\mathrm{cosec}(\pi z/n)$$

when $1\leq z\leq n-1$. Because the cosecant is a convex function on $(0,\pi)$, we have

$$\mathrm{cosec}(\pi z/n)\leq\int_{z-1/2}^{z+1/2}\mathrm{cosec}(\pi x/n)dx.$$

Hence we obtain the following result due to Sarwate [29]:

$$\begin{aligned}\sum_{z\neq 0}|\sum_{t\in B}e_n(tz)| &\leq 2\int_{1/2}^{n/2}\mathrm{cosec}(\pi x/n)dx\\ &= -(2n/\pi)\ln\tan(\pi/4n)\\ &< (2n/\pi)\ln(4n/\pi)\end{aligned}$$

if n is odd. If n is even, the problem can be treated on the same lines. Thus we have the following result.

Theorem 2.1 If B is defined by (2.2) and

$$L(n) = (2/\pi)\ln(4n/\pi) \tag{2.3}$$

then

$$E(B) < nL(n). \tag{2.4}$$

Vinogradov [41, Chapter III, Problem 11c] proved Theorem 2.1 with $L(n)$ replaced by $\ln(n) - \kappa$ where κ is a constant which is equal to 1 if $n \geq 60$. Of course, more careful calculations would yield slightly better results than (2.3) (see [14, p. 447] and [21, p. 686]).

Chalk considered the case where $F = Z_n^m$ and

$$B = \{\underline{x} = (x_1, \ldots, x_m) | \forall i : h_i + 1 \leq x_i \leq h_i + b\}$$

and showed [7, p. 294] that then

$$E(B) < (nln(n))^m \quad \text{if} \quad n \geq 60. \tag{2.5}$$

3 Multiplicative characters

Let F be a prime field $\mathbf{F}_p$ and let φ be χ, a nontrivial multiplicative character of F. It is convenient to extend the definition of χ by putting $\chi(0) = 0$. Then the Fourier transform of χ is the simplest hybrid sum, the Gaussian sum $\tau_z(\chi)$, defined by

$$\tau_z(\chi) = \sum_x \chi(x) e_p(xz).$$

Clearly

$$\tau_0(\chi) = \sum_x \chi(x) = 0. \tag{3.1}$$

For non-zero elements z we have the following well known result.

Lemma If $z \neq 0$ then $|\tau_z(\chi)| = p^{1/2}$.

Proof. Consider the square

$$|\tau_z(\chi)|^2 = \sum_x \sum_y \chi(x) e_p(xz) \overline{\chi(y) e_p(yz)}.$$

Since $\chi(0) = 0$, we may sum only over nonzero values of y. Furthermore, $\overline{\chi(y)} = (\chi(y))^{-1} = \chi(y^{-1})$ and $\overline{e_p(yz)} = (e_p(yz))^{-1} = e_p(-yz)$. By substituting $\chi = ty$ we thus obtain

$$\begin{aligned} |\tau_z(\chi)|^2 &= \sum_{y\neq 0}\sum_t \chi(ty)e_p(tyz)\chi(y^{-1})e_p(-yz) \\ &= \sum_t \chi(t)\sum_{y\neq 0} e_p((t-1)yz) \\ &= \sum_t \chi(t)\sum_y e_p((t-1)yz) - \sum_t \chi(t) \\ &= \sum_t \chi(t)\sum_y e_p((t-1)yz). \end{aligned}$$

Hence, by (1.2),

$$|\tau_z(\chi)|^2 = p\chi(1) = p.$$

□

The lemma above shows that $\Delta(\chi) = p^{1/2}$. By Theorem 1.1 and the results (3.1) and (2.4), we thus have the following result which is essentially due to Vinogradov [40] and Polya [28].

Theorem 3.1 If B is defined by (2.2) and L by (2.3), we have

$$|\sum_{t\in B}\chi(t)| < p^{1/2}L(p). \tag{3.2}$$

Bateman, Chowla and Erdös [1] showed that the left-hand side of (3.2) can be of order $p^{1/2}\ln\ln(p)$. On the other hand, an upper bound of this order was proved by Montgomery and Vaughan [23] under the assumption of the Riemann Hypothesis for Dirichlet functions. Further, Burgess [4] showed that there are nontrivial upper bounds for $b > p^{1/4+\varepsilon}$ by proving the following result: For $\varepsilon > 0$ there exists a positive number δ such that if χ is a nontrivial character to a sufficiently large p and if b is an integer satisfying $b > p^{1/4+\varepsilon}$ then the left-hand side of (3.2) is less than $bp^{-\delta}$.

Let d be a factor of $p-1$ and greater than 1. Denote the least positive d^{th} power non-residue (mod p) by κ. Theorem 3.1 implies that κ is less than $p^{1/2}L(p)$. There are several better results. For example, using his result above and an argument due to Vinogradov, Burgess proved in [3] that in the case $d = 2$ we have $\kappa = 0(p^{\alpha})$, for any fixed α greater than $1/(4e^{1/2})$.

There are several natural generalizations (see [35]). For example, we may replace the prime field $\mathbf{F}_p$ by a general finite field $\mathbf{F}_q$ and the argument x of χ by a polynomial $f(x)$.

4 On residues and non-residues of a polynomial

Above we considered non-residues of a d^{th} power (mod p). In this section we try to estimate residues and non-residues of a general polynomial and extend some results to general finite fields. For this purpose we need some estimates of certain character sums. Many of these estimates depend on a classical result of Weil [42] for which Stepanov later (see, e.g., [33], [34] and [30]) gave a new proof which does not depend on algebraic geometry.

Let $q = p^m$ where p is the characteristic of $\mathbf{F}_p$. Then the trace function tr defined by

$$tr(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{m-1}}$$

satisfies the equation $tr(\alpha + \beta) = tr(\alpha) + tr(\beta)$ for all α and β in $\mathbf{F}_q$, and therefore the function e defined by $e(\alpha) = e_p(tr(\alpha))$ is an additive character of $\mathbf{F}_q$.

The following theorem is due to Weil [42], see also [19, p. 223] and [30, p. 44].

Theorem 4.1 If $f \in \mathbf{F}_q[x]$ is a polynomial of degree d and $gcd(d, q) = 1$ then $|\sum_{x \in \mathbf{F}_q} e(f(x))| \le (d-1)q^{1/2}$.

Carlitz and Uchiyama [5] showed that in Theorem 4.1 it suffices to assume that f is not of the form $g^p - g + \beta$ with $g \in \mathbf{F}_q[x]$ and $\beta \in \mathbf{F}_q$. Therefore this form of Theorem 4.1 is often called the Carlitz-Uchiyama theorem. Deligne [11, Theorem 8.4] generalized Theorem 4.1 for polynomials of several variables in the following way.

Theorem 4.2 If $f \in \mathbf{F}_q[x_1, \ldots, x_s]$ is a polynomial of degree d and $gcd(d, q) = 1$ and if the maximal degree homogeneous part of f is nonsingular as a form over the algebraic closure of $\mathbf{F}_q$, then

$$|\sum_{(x_1,\ldots,x_s) \in \mathbf{F}_q^s} e(f(x_1, \ldots, x_s))| \le (d-1)^s q^{s/2}.$$

In an important application we shall need hybrid sums combining a multiplicative character χ and the additive character e. Theorem 4.3 is a special case of a theorem due to Weil [42], see also [30, p. 45]. It is easy to see that the lemma of Section 3 is a special case of Theorem 4.3.

Theorem 4.3 If χ is a nontrivial multiplicative character of $\mathbf{F}_q$, $f \in \mathbf{F}_q[x]$ is a polynomial of degree d and $gcd(d, q) = 1$ then

$$|\sum_{x \in \mathbf{F}_q} e(f(x))\chi(x)| \le dq^{1/2}.$$

Consider now the least non-negative residue of a polynomial $f \in \mathbf{F}_p[x]$ of degree d where $2 \leq d < p$. Let $\varphi(a)$ be the number of solutions of the congruence $f(x) \equiv a \pmod{p}$ and let F be $\mathbf{F}_p$ again. Then

$$\sum_a \varphi(a) e_p(az) = \sum_x e_p(zf(x)).$$

Since $\sum_a \varphi(a) = p$, Theorems 1.1 and 4.1 and the inequality (2.4) imply

$$\sum_{a=0}^{b-1} \varphi(a) = b + \theta(d-1)p^{1/2}L(p) \tag{4.1}$$

where the absolute value of θ is less than 1. An immediate consequence of this equation is the following theorem of Mordell [25] (here and many times hereafter we replace $\ln(p)$ by $L(p)$).

Theorem 4.4 κ, the least non-negative residue of $f \pmod{p}$, satisfies the inequality

$$\kappa < (d-1)p^{1/2}L(p). \tag{4.2}$$

Theorem 4.4 extends for the traces in general finite fields without any significant difficulties. Let q be equal to p^m, let $f(x)$ be a polynomial which satisfies the assumptions of the Carlitz-Uchiyama theorem and let $\varphi(a)$ be the number of solutions $x \in \mathbf{F}_q$ of the congruence $tr(f(x)) \equiv a \ (\mathrm{mod} p)$. Thus Theorem 1.1, the equation $\sum_a \varphi(a) = q$, the Carlitz-Uchiyama theorem and the inequality (2.4) imply the following result of Cavior [6].

Theorem 4.5 If $q = p^m$, $f \in \mathbf{F}_q[x]$ and f is not of the form $g^p - g + \beta$ with $g \in \mathbf{F}_q[x]$, $\beta \in \mathbf{F}_q$, then μ, the least non-negative trace of f, satisfies the inequality

$$\mu < (d-1)p^{1-m/2}L(p). \tag{4.3}$$

Using deeper and more complicated arguments Bombieri and Davenport [2] proved the following.

Theorem 4.6 Let f be a polynomial of degree d (≥ 2), and suppose that at least one of the irreducible factors of $(f(x) - f(y))/(x - y)$ over $\mathbf{F}_p$ is absolutely irreducible. Then there exists a number $C(d)$ depending only on d such that, for every large p, there is some λ with

$$0 < \lambda < C(d)p^{1/2}L(p) \tag{4.4}$$

for which the congruence $f(x) \equiv \lambda \pmod{p}$ is insoluble.

5 The distribution of solutions of congruences

For $s \geq 3$ and $d \geq 2$, let $f(\underline{x}) = f(x_1, \ldots, x_s)$ be a polynomial in the s variables $x_1, \ldots, x_s$ of degree d and with coefficients in $\mathbf{F}_p$. We define a box B as the set of points $\underline{x} = (x_1, \ldots, x_s) \in \mathbf{F}_p^s$ for which

$$h_i + 1 \leq x_i \leq h_i + b \quad (i = 1, 2, \ldots, s).$$

Let $N(B)$ denote the number of $\underline{x} \in B$ for which $f(\underline{x}) = 0$. Then it is natural to denote $\mathbf{F}_p^s$ by F and to write

$$\varphi(\underline{x}) = \left\{ \begin{array}{ll} 1 & \text{if } \ f(\underline{x}) = 0 \\ 0 & \text{otherwise} \end{array} \right\} = \frac{1}{p} \sum_{k \in \mathbf{F}_p} e_p(kf(\underline{x})).$$

Hence

$$N(B) = \sum_{\underline{x} \in B} \varphi(x), \ N(F) = \sum_{\underline{x}} \varphi(x),$$

and, by (1.3) and (2.5),

$$N(B) = \frac{|B|}{p^s} N(F) + \frac{\theta}{p^s} \Delta(\varphi)(p \ \ln(p))^s \tag{5.1}$$

if p is large. In this application

$$\begin{aligned} \Delta(\varphi) &= \max_{\underline{z} \neq \underline{0}} |\sum_{\underline{x}} \varphi(\underline{x}) e_p(\underline{x} \cdot \underline{z})| \\ &= \max_{\underline{z} \neq \underline{0}} |\frac{1}{p} \sum_{k \in \mathbf{F}_p} \sum_{\underline{x}} e_p(kf(\underline{x}) + \underline{x} \cdot \underline{z})|. \end{aligned}$$

In the special case where the variables can be separated, e.g. in the case

$$f(\underline{x}) = x_1^d + \ldots + x_s^d, \quad d|(p-1),$$

we can estimate $\Delta(\varphi)$ by the result of Weil in the following way:

$$\begin{aligned} \Delta(\varphi) &\leq \max_{\substack{\underline{z} \neq \underline{0} \\ k \neq 0}} |\prod_{j=1}^{s} \sum_{x_j \in \mathbf{F}_p} e_p(kx_j^d + z_j x_j)| \\ &\leq (d-1)^s p^{s/2}. \end{aligned}$$

Further,

$$\begin{aligned} N(F) &= \frac{1}{p} \sum_{\underline{x}} \sum_{k \in \mathbf{F}_p} e_p(kf(\underline{x})) \\ &= p^{s-1} + \frac{\theta_1}{p} \sum_{k \neq 0} \prod_{j=1}^{s} |\sum_{x_j \in \mathbf{F}_p} e_p(kx_j^d)| \\ &= p^{s-1} + \theta_2 (d-1)^s p^{s/2}, \end{aligned}$$

and hence, by (5.1), for any $\varepsilon > 0$ and any $p > p_0(\varepsilon)$,

$$N(B) = \frac{|B|}{p} + \theta_3(1+\varepsilon)(d-1)^s p^{s/2}(ln(p))^s$$

where $|\theta_i| \leq 1$ $(i = 1, 2, 3)$. Thus the polynomial $x_1^d + \ldots + x_s^d$ has a zero in B if p is large and

$$|B| > (1+\varepsilon)(d-1)^s p^{(s+2)/2}(\ln(p))^s,$$

i.e., if

$$b > (1+\varepsilon)^{1/s}(d-1)p^{(s+2)/(2s)}\ln(p). \tag{5.2}$$

These investigations are due to Mordell ([24],[26]) and to Chalk and Williams ([7] and [9]). There are, of course, a lot of more recent results (see, e.g., [14] for quadratic congruences).

6 An improvement

Often Theorem 1 and its modifications are used in order to answer a question of the following form:

(a) What is the number of important elements in a certain box B?

On the other hand, in some other applications it is natural to ask the following question:

(b) How large must a box be to ensure that each box of this size contains at least one important element?

In the applications above the "important elements" were residues, non-residues or zeros of a polynomial but there are of course other applications, too.

In order to calculate the number of important elements in a box B it is natural to define

$$\varphi(x) = \begin{cases} 1 & \text{if } x \text{ is an important element} \\ 0 & \text{otherwise} \end{cases}$$

and to estimate the incomplete sum $\sum_{x \in B} \varphi(x)$ by means of Theorem 1.1. Then we have to calculate or to estimate the functions $\Delta(\varphi)$ and $E(B)$. The former of these functions was estimated by using results of Weil and others, and it is certainly difficult to give general improvements for these results. $E(B)$ was estimated by using the inequality (2.4) and its modifications, and in this inequality also the logarithm factor is unavoidable in the absence of any further restriction on the box B.

However, in the applications of the form (b) the situation is different. Let $\alpha(t)$ be a function on F such that $\alpha(t) \leq 0$ if t is not important. Then in order to show that a set A contains an important element it suffices to show that $\sum_{t\in A}\alpha(t)>0$. For instance, if we can write the set A in the form $B+B=\{x+y|x\in B,\ y\in B\}$, we may define $\alpha(t)$ to be the number of ways of expressing t as the sum of two (not necessarily different) elements of B. Then we have, by the argument given in Section 1,

$$\begin{aligned}\sum_{t\in A}\alpha(t) &= \sum_{x\in B}\sum_{y\in B}\varphi(x+y)\\ &= \tfrac{1}{n}\sum_{z}\psi(z)\sum_{x\in B}\sum_{y\in B}e_n(-(x+y)z)\\ &= \tfrac{b^2}{n}\sum_{x}\varphi(x)+\tfrac{\theta}{n}\Delta(\varphi)E_2(B)\end{aligned}\tag{6.1}$$

where

$$E_2(B)=\sum_{z\neq 0}|\sum_{t\in B}e_n(tz)|^2.$$

Further, $E_2(B)$ can be calculated very easily:

$$\begin{aligned}E_2(B) &= \sum_{z}\sum_{t\in B}e_n(tz)\sum_{u\in B}e_n(-uz)-b^2\\ &= \sum_{t\in B}\sum_{u\in B}\sum_{z}e_n((t-u)z)-b^2\end{aligned}$$

and so, by (1.2),

$$E_2(B)=bn-b^2<bn.$$

Thus

$$|\sum_{t\in A}\alpha(t)-\frac{b^2}{n}\sum_{x}\varphi(x)|<b\Delta(\varphi).$$

Using this modification of the Vinogradov inequality we observe that in the solution of the problem (b) the logarithm factor of $E(B)$ can be avoided.

For example, the equation (4.1) can be replaced by

$$\left|\sum_{t=0}^{2b-2}\alpha(t)-b^2\right|<b(d-1)p^{1/2}.$$

Thus in the set $\{0,1,2,\ldots,2b-2\}$ there is a t such that $\alpha(t)>0$ provided $b\geq(d-1)\sqrt{p}$, and we may replace the inequality (4.2) by

$$\kappa<2(d-1)p^{1/2}.$$

In the same way ([36], [37], and [38]) in the inequalities (4.3) and (4.4) $L(p)$ and in the inequality (5.2) $(1+\varepsilon)^{1/s}\ln(p)$ can be replaced by 2.

This method was extended by Chalk [8] and Cochrane [10].

7 The distribution of solutions of a system of equations

Of course, there are a lot of generalizations (see, e.g., [27] and [32]). Consider now briefly an easily understandable problem. Let $\mathbf{F}_q$ be the finite field of $q = p^m$ elements and let V be set of solutions of

$$\begin{cases} f_1(x_1, \ldots, x_s) = 0 \\ f_2(x_1, \ldots, x_s) = 0 \\ \cdots \\ f_t(x_1, \ldots, x_s) = 0; \end{cases} \tag{7.1}$$

in other words,

$$V = \{\underline{x} \in \mathbf{F}_q^s | \underline{f}(\underline{x}) = \underline{0}\}$$

where $\underline{x} = (x_1, \ldots, x_s)$ and $\underline{f}(\underline{x}) = (f_1(\underline{x}), \ldots, f_t(\underline{x}))$. The problem is whether we can assert the existence of some b, relatively small compared with q^s, for which $|B| \geq b$ necessarily implies $(B + B) \cap V \neq \emptyset$.

We extend the method of Section 5 in two respects: The original Vinogradov method will be replaced by its modification and the character sum estimate of Weil (Theorem 4.1) by a result of Deligne (Theorem 4.2).

A polynomial $g(\underline{x}) = g(x_1, \ldots, x_s)$ is said to be nonsingular at infinity over $\mathbf{F}_q$ if its maximal degree homogeneous part is nonsingular as a form over the algebraic closure of $\mathbf{F}_q$.

Let

$$\varphi(\underline{x}) = \left\{ \begin{array}{ll} 1 & \text{if } \ \underline{f}(\underline{x}) = \underline{0} \\ 0 & \text{otherwise} \end{array} \right\} = \frac{1}{q^t} \sum_{\underline{k} \in \mathbf{F}_q^t} e(\underline{k} \cdot \underline{f}(\underline{x})),$$

$$S(\underline{z}) = \sum_{\underline{x} \in B} e(-\underline{x} \cdot \underline{z}),$$

and

$$\psi(\underline{z}) = \sum_{\underline{x} \in \mathbf{F}_q^s} \varphi(\underline{x}) e(\underline{x} \cdot \underline{z}).$$

Then it follows from the equation (6.1) and from the observation

$$\sum_{\underline{z} \in \mathbf{F}_q^s} |S(\underline{z})|^2 = |B| q^s$$

that

$$\begin{aligned} \sum_{\underline{x} \in B} \sum_{\underline{y} \in B} \varphi(\underline{x} + \underline{y}) &= \frac{1}{q^s} \sum_{\underline{z} \in \mathbf{F}_q^s} \psi(\underline{z}) S(\underline{z}))^2 \\ &= \frac{1}{q^{s+t}} \sum_{\underline{k} \in \mathbf{F}_q^t} \sum_{\underline{z} \in \mathbf{F}_q^s} (S(\underline{z}))^2 \sum_{\underline{x} \in \mathbf{F}_q^s} e(\underline{k} \cdot \underline{f}(\underline{x}) + \underline{x} \cdot \underline{z}) \\ &= \frac{|B|^2}{q^t} + \theta |B| \max_{\underline{z} \in \mathbf{F}_q^s} \max_{\substack{\underline{k} \in \mathbf{F}_q^t \\ \underline{k} \neq \underline{0}}} | \sum_{\underline{x} \in \mathbf{F}_q^s} e(\underline{k} \cdot \underline{f}(\underline{x}) + \underline{x} \cdot \underline{z})|. \end{aligned}$$

If every polynomial in the set

$$\{\underline{k} \cdot \underline{f}(\underline{x}) = \sum_{i=1}^{t} k_i f_i(\underline{x}) | \underline{k} \in \mathbf{F}_q^t, \quad \underline{k} \neq \underline{0}\}$$

is of degree greater than 1 and not divisible by p and is nonsingular at infinity then the theorem of Deligne implies the inequality

$$\max_{\underline{z} \in \mathbf{F}_q^s} \max_{\substack{\underline{k} \in \mathbf{F}_q^t \\ \underline{k} \neq \underline{0}}} |\sum_{\underline{x} \in \mathbf{F}_q^s} e(\underline{k} \cdot \underline{f}(\underline{x}) + \underline{x} \cdot \underline{z}| \leq (d-1)^s q^{s/2}$$

where d is the maximum of degrees of polynomials $f_1(\underline{x}), \ldots, f_t(\underline{x})$. Thus in this case

$$\left| \sum_{\underline{x} \in B} \sum_{\underline{y} \in B} \varphi(\underline{x} + \underline{y}) - \frac{|B|^2}{q^t} \right| \leq |B|(d-1)^s q^{s/2}$$

and we have the following theorem [10].

Theorem 7.1 Assume that every polynomial in the set $\{\underline{k} \cdot \underline{f}(\underline{x}) | \underline{k} \in \mathbf{F}_q^t, \quad \underline{k} \neq \underline{0}\}$ is of degree less than or equal to d, greater than 1 and not divisible by p, and is nonsingular at infinity. Then the system (7.1) has a solution in the set $B + B$ provided that

$$|B| > (d-1)^s q^{(s+2t)/2}$$

Many results of this section and earlier sections were surveyd also in [39].

8 Partial-period correlations

Assume that $q = 2^m$ and γ is a primitive element of $\mathbf{F}_q$. Let P be an additive subgroup of $\mathbf{F}_q[x]$ and $n = 2^m - 1$. Define the binary linear code $C(P)$ by the equation

$$C(P) = \{\underline{c}(f) | f \in P\}$$

where

$$\underline{c}(f) = (tr(f(1)), tr(f(\gamma)), tr(f(\gamma^2)), \ldots, tr(f(\gamma^{n-1}))).$$

For any binary word $\underline{x} = (x_0, x_1, \ldots, x_{n-1})$ let $S\underline{x} = (x_{n-1}, x_0, \ldots, x_{n-2})$. A code C is called cyclic if it is linear and if for each $\underline{c} \in C$ also $S\underline{c} \in C$. It is known (see, e.g., [12, Chapter 1, Theorem 5.8] and [15, Theorem 4.2]) that for each binary cyclic code C of length n there are integers $s_1, \ldots, s_u$ such that $C = C(P)$ where $P = \{\sum_{i=1}^{u} a_i x^{s_i} | a_i \in \mathbf{F}_q\}$.

Binary cyclic codes are used to derive certain sets of binary sequences with good correlation properties [22]. Let $\underline{x} = (x_0, \ldots, x_{n-1})$ and $\underline{y} =$

$(y_0, \ldots, y_{n-1})$ be two binary sequences. The correlation $\vartheta(\underline{x}, \underline{y})$ is the number of components where $\underline{x}$ and $\underline{y}$ are equal minus the number of components where they differ. If $\underline{x} = \underline{c}(f)$, $\underline{y} = \underline{c}(g)$ and we denote $f - g$ by h, we have

$$\begin{aligned} \vartheta(\underline{x}, \underline{y}) &= |\{i | tr(h(\gamma^i)) = 0\}| - |\{i | tr(h(\gamma^i)) = 1\}| \\ &= |\{i | e(h(\gamma^i)) = 1\}| - |\{i | e(h(\gamma^i)) = -1\}| \\ &= \sum_{i=0}^{n-1} e(h(\gamma^i)) \end{aligned} \tag{8.1}$$

If $X = \{\underline{x}_1, \ldots, \underline{x}_K\}$ is a set of binary sequences of length n, the numbers $\vartheta(\underline{x}_i, S^k \underline{x}_j)$ are called the full-period correlations in X. The case $i = j$, $k = 0$ is trivial. Therefore the maximal full-period correlation of X is defined to be

$$\vartheta(X) = \max |\vartheta(\underline{x}_i, S^k \underline{x}_j)|$$

where the maximum is taken over all values i, j and k such that $1 \leq i \leq K$, $1 \leq j \leq K$, $0 \leq k \leq n-1$, $k \neq 0$ if $i = j$.

Let $C = C(P)$. We say that two elements of C are conjugate if one is a cyclic shift of the other. Assume that $X = \{\underline{x}_1, \ldots, \underline{x}_K\}$ is a set of representatives of all the conjugacy classes that have n codewords. If $k \neq 0$ or $i \neq j$, then $\underline{x}_i + S^k \underline{x}_j$ is a nonzero element $\underline{c} = \underline{c}(f)$ in C. If we denote $\mathbf{Z}_n$ by F, we thus have

$$\vartheta(\underline{x}_i, S^k \underline{x}_j) = \sum_{i \in F} e(f(\gamma^i)) = \sum_{x \in \mathbf{F}_q^*} e(f(x)), \tag{8.2}$$

where $\mathbf{F}_q^* = \mathbf{F}_q \setminus \{0\}$, and so

$$\vartheta(X) \leq 1 + \max_{f \in P, f \neq 0} |\sum_{x \in \mathbf{F}_q} e(f(x))|. \tag{8.3}$$

Thus $\vartheta(X)$ can be estimated by means of complete character sums.

Let B be the proper subset of F defined by (2.2). Then the corresponding partial-period correlation

$$\vartheta_B(\underline{x}_i, S^k \underline{x}_j) = \sum_{i \in B} e(f(\gamma^i)),$$

$$\vartheta_B(X) = \max |\theta_B(\underline{x}_i, S^k \underline{x}_j)|,$$

where the maximum is taken just like for $\vartheta(X)$, and so it is natural to define the maximal partial-period correlation of X by the equation

$$\hat{\vartheta}(X) = \max_B \vartheta_B(X)$$

where the maximum is taken over all proper subsets B of F. Thus $\hat{\vartheta}(X)$ can be estimated by estimating the maximum absolute value of the incomplete character sum

$$S_B(f) = \sum_{i \in B} e(f(\gamma^i))$$

when $B \subset F$ and $f \in P$, $f \neq 0$. If we want to use the Vinogradov method, we should be able to estimate the hybrid sum

$$\sum_{i \in F} e(f(\gamma^i)) e_n(i) = \sum_{x \in \mathbf{F}_q} e(f(x)) \chi(x) \tag{8.4}$$

where χ is thus a nontrivial multiplicative character of $\mathbf{F}_q$. Using the lemma of Section 3, Theorem 4.3 and [18], we may mention here the following three cases.

1) **m-sequences.** Let $P = \{ax | a \in \mathbf{F}_q\}$. Then X contains only one word $\underline{x}$ and by (8.2), (8.3) and (1.2) we have $\vartheta(X) = 1$. Further, by Theorem 1.1, the lemma of Section 3 and (2.4) we obtain ([22],[29])

$$\hat{\vartheta}(X) < q^{1/2} L(q-1) + 1.$$

2) **Dual BCH sequences.** Let $r < 2^{m/2-1} + 1$ and

$$P = \{a_1 x + a_2 x^3 + \ldots + a_r x^{2r-1} | a_1, \ldots, a_r \in \mathbf{F}_q\}.$$

Then $C(P)$ is in fact (see, e.g., [21, Chapter 9]) the dual of the binary BCH code of length n with designed distance $2r+1$. Define X, the corresponding set of sequences, as in the discussion above. By (8.3) and Theorem 4.1,

$$\vartheta(X) \leq 1 + (2r-2) q^{1/2}.$$

$\hat{\vartheta}(x)$ can be estimated by using Vinogradov's method. By Theorem 4.3, the sum (8.4) can be upper bounded by $(2r-1)q^{1/2}$. Thus ([20], [15])

$$\hat{\vartheta}(X) < (2r-1) q^{1/2} (L(q-1) + 1).$$

3) **Small Kasami sets of sequences.** Let $q = 2^{2r}$ and $\varepsilon \in \mathbf{F}_q \setminus \mathbf{F}_{2^r}$ and choose $P = \{bx + ax^{2^r+1} | b \in \mathbf{F}_q,\ a \in \varepsilon \mathbf{F}_{2^r}\}$. The code $C(P)$ is cyclic because $f(\gamma x) \in P$ for all $f(x) \in P$. Denote $f(x) = bx + ax^{2^r+1}$. The case $a = 0$ is trivial. If $a \neq 0$ then

$$\begin{aligned}
\Big(\sum_{x \in \mathbf{F}_q} e(f(x))\Big)^2 &= \sum_{x \in \mathbf{F}_q} \sum_{z \in \mathbf{F}_q} e(f(x) + f(x+z)) \\
&= \sum_{x \in \mathbf{F}_q} \sum_{z \in \mathbf{F}_q} e(f(z)) e(ax^{2^r} z) e(axz^{2^r}),
\end{aligned}$$

and because $e(ax^{2^r} z) = e(a^{2^r} x z^{2^r})$ we further obtain

$$\begin{aligned}
\Big(\sum_{x \in \mathbf{F}_q} e(f(x))\Big)^2 &= \sum_{x \in \mathbf{F}_q} \sum_{z \in \mathbf{F}_q} e(f(z)) e(a^{2^r} x z^{2^r} + axz^{2^r}) \\
&= \sum_{z \in \mathbf{F}_q} e(f(z)) \sum_{x \in \mathbf{F}_q} e(x(a^{2^r} + a) z^{2^r}) = q
\end{aligned}$$

because the fact that a is not in $\mathbf{F}_{2^r}$ implies that $a^{2^r} + a \neq 0$. When we denote the set of sequences corresponding to P by X, we thus have

$$\vartheta(X) \leq q^{1/2} + 1.$$

To estimate $\hat{\vartheta}(X)$ we use the result [18]

$$|\sum_{x \in \mathbf{F}_q} e(bx + ax^{2^r+1})\chi(x)| \leq 2q^{1/2}.$$

Thus in this case

$$\hat{\vartheta}(X) < 2q^{1/2}(L(q-1)+1).$$

Of course, it would be desirable to know if more or less similar results for $\hat{\vartheta}(X)$ can be found in the case of large and very large Kasami sets and Gold sets, etc. For sets of sequences over Galois rings (see, e.g., [13]) there are some corresponding results ([31], [17]). A natural research problem is to try to find methods which yield better results than the Vinogradov approach.

References

[1] P. T. Bateman, S. Chowla, and P. Erdös: Remarks on the size of $L(1, \chi)$. – Publ. Math. Debrecen 1 (1950), 165–182.

[2] E. Bombieri and H. Davenport: On two problems of Mordell. – Amer. J. Math. 88 (1966), 61–70.

[3] D. A. Burgess: The distribution of quadratic residues and non-residues. – Mathematika 4 (1957), 106–112.

[4] D. A. Burgess: On character sums and primitive roots. – Proc. London Math. Soc. 12 (1962), 179–192.

[5] L. Carlitz and S. Uchiyama: Bounds for exponential sums. – Duke Math. J. 24 (1957), 37–41.

[6] S. R. Cavior: On the least non-negative trace of a polynomial over a finite field. – Boll. Un. Mat. Ital. (3)20 (1965), 120–121.

[7] J. H. H. Chalk: The number of solutions of congruences in incomplete residue systems. – Canad. J. Math. 15 (1963), 291–296.

[8] J. H. H. Chalk: The Vinogradov–Mordell–Tietäväinen inequalities. – Indag. Math. 42 (1980), 367–374.

[9] J. H. H. Chalk and K. S. Williams: The distribution of solutions of congruences. – Mathematika 12 (1965), 176–192.

[10] T. Cochrane: The distribution of solutions to equations over finite fields. – Trans. Amer. Math. Soc. 293 (1986), 819–825.

[11] P. Deligne: La conjecture de Weil. I. – Inst. Hautes Etudes Sci. Publ. Math. 42 (1974), 273–307.

[12] P. Delsarte: An algebraic approach to the association schemes of coding theory. – Philips Research Reports Supplements, No 10 (1973).

[13] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé: The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. – IEEE Trans. Information Theory 40 (1994), 301-319.

[14] D. R. Heath-Brown: Small solutions of quadratic congruences. – Glasgow Math. J. 27 (1985), 87-93.

[15] I. Honkala and A. Tietäväinen: Codes and number theory. In Handbook of Coding Theory (Eds. R. A. Brualdi, W. C. Huffman and V. S. Pless), to appear.

[16] T. Kasami: Weight distributions of Bose-Chaudhury-Hocquenghem codes. In: R. C. Bose and T. A. Dowling (eds.): Combinatorial Math. and its Applications, Univ. of North Carolina Press, Chapel Hill, NC (1969).

[17] S. Koponen and J. Lahtonen: On maximal aperiodic and odd correlations of binary Shanbhag-Kumar-Helleseth sequences. Preprint.

[18] J.Lahtonen: Examples of small hybrid sums. – Proc. of the third international conference on finite fields and applications (to appear).

[19] R. Lidl and H. Niederreiter: Finite Fields. – Addison-Wesley (1983)

[20] S. Litsyn and A. Tietäväinen: Character sum constructions of constrained error-correcting codes. – Appl. Algebra in Engineering, Communication and Computing 5 (1994), 45–51.

[21] F. J. MacWilliams and N. J. A. Sloane: The Theory of Error-Correcting Codes. – Amsterdam: North-Holland, 1977.

[22] R. J. McEliece: Correlation properties of sets of sequences derived from irreducible cyclic codes. – Information and Control 45 (1980), 18–25.

[23] H. L. Montgomery and R. C. Vaughan: Exponential sums with multiplicative coefficients. – Invent. Math. 43 (1977), 69–82.

[24] L. J. Mordell: On the number of solutions in incomplete residue sets of quadratic congruences. – Arch. Math. 8 (1957), 153–157.

[25] L. J. Mordell: On the least residue and non-residue of a polynomial. – J. London Math. Soc. 38 (1963), 451–453.

[26] L. J. Mordell: Incomplete exponential sums and incomplete residue systems for congruences. – Czechoslovak Math. J. 14 (1964), 235–242.

[27] G. Myerson: The distribution of rational points on varieties defined over a finite field. – Mathematika 28 (1981), 153–159.

[28] G. Pólya: Über die Verteilung der quadratischen Reste und Nichtreste. – Göttinger Nachr. 1918, 21–29.

[29] D. V. Sarwate: An upper bound on the aperiodic autocorrelation function for a maximal-length sequence. – IEEE Trans. Inform. Theory 30 (1984), 685–687.

[30] W. M. Schmidt: Equations over Finite Fields. An Elementary Approach. – Lecture Notes in Mathematics 536, Berlin: Springer (1976).

[31] A. G. Shanbhag, P. V. Kumar and T. Helleseth: An upper bound for the aperiodic correlation of weighted-degree CDMA sequences. – Proc. of the 1995 IEEE International Symposium on Information Theory (1995) 92.

[32] I. E. Shparlinski and A. N. Skorobogatov: Exponential sums and rational points on complete intersections. – Mathematika 37 (1990), 201–208.

[33] S. A. Stepanov: Elementary method in the theory of congruences for a prime modulus. – Acta Arith. 17 (1970), 231–247.

[34] S. A. Stepanov: An elementary proof of the Hasse-Weil theorem for hyperelliptic curves. – J. Number Theory 4 (1972), 118–143.

[35] S. A. Stepanov: Character sums and coding theory. Preprint.

[36] A. Tietäväinen: On the trace of a polynomial over a finite field. – Ann. Univ. Turku Ser. AI 87 (1966), 7 pp.

[37] A. Tietäväinen: On non-residues of a polynomial. – Ann. Univ. Turku Ser. AI 94 (1966), 6 pp.

[38] A. Tietäväinen: On the solvability of equations in incomplete finite fields. – Ann. Univ. Turku Ser. AI 102 (1967), 13 pp.

[39] A. Tietäväinen: Incomplete sums and two applications of Deligne's result. – Lecture Notes in Mathematics 1352, Berlin, Springer (1988), 190–205.

[40] I. M. Vinogradov: Sur la distribution des résidus et des non-résidus des puissances. – Ẑ. Fiz.-Mat. Obŝ ĉ. Permsk. Gos. Univ. 1918, no 1, 94–98.

[41] I. M. Vinogradov: Elements of number theory. – Dover, 1954.

[42] A. Well: Sur les courbes algébriques et les veriétés qui s'en déduisent. – Actualités Sci. Ind., no. 1041, Hermann, Paris, 1948.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.abo.fi

University of Turku
- **Department of Mathematical Sciences**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**