Several generalizations of Weil sums

Fan R. K. Chung
Bellcore
Morristown, NJ 07960

Abstract

We consider several generalizations and variations of the character sum inequalities of Weil and Burgess. A number of incomplete character sum inequalities are proved while further conjectures are formulated. These inequalities are motivated by extremal graph theory with applications to problems in computer science.

1. Introduction

One of the classical problems in number theory concerns the distribution of residues and non-residues in the finite field $\mathcal{F}_p$ for a prime p. Roughly speaking, it is widely believed that the quadratic character or, more generally, a nontrivial multiplicative character, is almost "evenly distributed", as evidenced by many well-known character sum inequalities, some of which we mention in the following:

1. The Gauss sum: Let ζ denote $exp(2\pi i/p)$. For each nonzero j in $\mathcal{F}_p$, we have

$$\left|\sum_{x\in\mathcal{F}_p} \chi(x)\zeta^{jx}\right| = \sqrt{p}.$$

2. The Weil sum: Let χ be a multiplicative character of order $m > 1$ in $\mathcal{F}_q$ for a prime power q and let $f \in \mathcal{F}_q[x]$ be a polynomial of positive degree that is not an mth power of a polynomial. Let d be the number of distinct roots of f in its splitting field over $\mathcal{F}_q$. Then

$$\left|\sum_{x\in\mathcal{F}_q} \chi(f(x))\right| \leq (d-1)\sqrt{q}.$$

3. In 1918, Polya [26] and Vinogradov [30] independently proved the following inequality:

$$|\sum_{m=n}^{n+h} \chi(m)| < p^{1/2}\log p. \tag{1}$$

where χ is a nontrivial multiplicative character of $\mathcal{F}_p$.

4. Montgomery and Vaughan [24] have shown that assuming the Generalized Riemann Hypothesis the following holds:

$$\left|\sum_{m=n}^{n+h} \chi(m)\right| < \sqrt{p}\log\log p \tag{2}$$

In the other direction, a lower bound for $\sum_{m=1}^{h}\chi(m)$ for some choice of h is of the same order $\sqrt{p}\log\log p$. This is due to Bateman, Chowla and Erdös [5] and improves upon earlier lower bound of $\sqrt{p}$, given by Paley [25] and Chowla [9].

5. Estimates for character sums over an interval in terms of the length of the interval were considered by Burgess [2, 3, 4] and also by Wang [31, 32]. The best known result, due to Burgess [3] in 1962, is the following:

For $\epsilon > 0$, there exists a positive δ such that if χ is a nontrivial multiplicative character in $\mathcal{F}_p$, then

$$\left| \sum_{m=n+1}^{n+h} \chi(m) \right| \leq hp^{-\delta} \tag{3}$$

where n is an arbitrary integer and $h > p^{\frac{1}{4}+\epsilon}$.

In this paper, we consider several generalizations and variations of the above character sum inequalities. A number of incomplete character sum inequalities are given and further conjectures are formulated. Many of these inequalities have a combinatorial flavor since they are motivated by problems in graph theory [10, 13, 14] with applications to a number of areas in computer science [7, 8, 15, 29, 33, 34].

Instead of summing over intervals, we consider double sums ranging over given subsets which will be described in Section 2. In Section 3, we consider triple sums and more generally k-tuple sums. The coset inequalities considered in Section 4 concern generalizations of Weil's inequality where the sum is taken over a coset. In Section 5 we discuss the connections with graph theory and various applications to extremal graphs, communication complexity and circuit complexity.

2. Double sum inequalities

The following theorem can be viewed as a "2-dimensional" generalization of the Burgess inequality in (3).

Theorem 2.1. *Let χ denote a non-trivial multiplicative character in $\mathcal{F}_p$. Let S and T denote subsets of elements in $\mathcal{F}_p$. Then*

$$\left| \sum_{a \in S} \sum_{b \in T} \chi(a+b) \right| \leq \sqrt{p|S||T|} \left(1 - \frac{|S|}{p}\right)^{1/2} \left(1 - \frac{|T|}{p}\right)^{1/2}$$

Proof: For a in $\mathcal{F}_p$, we define $\tau_a = \sum_x \chi^{-1}(x)\zeta^{ax} = \chi(a)\tau_1$ and $|\tau_1| = \sqrt{p}$. Therefore

$$\left| \sum_{a \in S} \sum_{b \in T} \chi(a+b) \right|$$

$$
\begin{aligned}
&= \frac{1}{\sqrt{p}}\left|\sum_{a\in S}\sum_{b\in T}\tau_{a+b}\right| \\
&= \frac{1}{\sqrt{p}}\left|\sum_{a\in S}\sum_{b\in T}\sum_{x}\chi^{-1}(x)\zeta^{(a+b)x}\right| \\
&= \frac{1}{\sqrt{p}}\left|\sum_{x}\chi^{-1}(x)\sum_{a\in S}\sum_{b\in T}\zeta^{(a+b)x}\right| \\
&\leq \frac{1}{\sqrt{p}}\sum_{x\neq 0}\left|\sum_{a\in S}\zeta^{ax}\right|\left|\sum_{b\in T}\zeta^{bx}\right| \\
&\leq \frac{1}{\sqrt{p}}\left(\sum_{x\neq 0}\left|\sum_{a\in S}\zeta^{ax}\right|^2\right)^{1/2}\left(\sum_{x\neq 0}\left|\sum_{b\in T}\zeta^{bx}\right|^2\right)^{1/2} \\
&\leq \frac{1}{\sqrt{p}}(p|S|-|S|^2)^{1/2}(p|T|-|T|^2)^{1/2} \\
&\leq \sqrt{p|S||T|}\left(1-\frac{|S|}{p}\right)^{1/2}\left(1-\frac{|T|}{p}\right)^{1/2}.
\end{aligned}
$$

It is easy to see that Theorem 2.1 implies that

$$\left|\sum_{a,b\in S}\chi(a-b)\right| \leq \sqrt{p}|S|(1-|S|/p) \leq p^{3/2}/4$$

How good is the upper bound in Theorems 2.1 ? When $|S|$ is large, say about $p/2$, it is not difficult to see the upper bounds are within an absolute constant factor of the optimum [17]. In other words, there exists S with about $p/2$ elements so that $\left|\sum_{a,b\in S}\chi(a-b)\right| > c\,p^{3/2}$. When $|S| < c\sqrt{p}$, the inequalities in Theorem 2.1 does not yield nontrivial bounds. Not much is known for the case when $|S|$ is smaller than $\sqrt{p}$ and the following (folklore) conjecture remains open (for $\epsilon < 1/2$).

Conjecture 2.2: For any fixed $\epsilon > 0$, let S be a subset of $\mathcal{F}_p$ with at least p^{ϵ} elements. Then there is a positive δ, such that

$$\left|\sum_{a,b\in S}\chi(a-b)\right| < |S|^{2-\delta} \tag{4}$$

where the prime p is sufficiently large.

It would be of particular interest to verify the conjecture for the quadratic character η. We remark that Theorem 2.1 and 2.2 confirm the above conjecture for $|S| > p^{\frac{1}{2}+\epsilon}$. Also, when S and T are large subsets of intervals $\mathcal{S}, \mathcal{T}$, such as for any given positve ϵ and $\epsilon_i < \epsilon/3$ for $i = 1, ..., 3, |\mathcal{S}|\ |\mathcal{T}| > p^{\frac{1}{2}+\epsilon_1}$, $|S| > |\mathcal{S}|p^{\epsilon_2}$, and $|T| > |\mathcal{T}|p^{\epsilon_3}$, E. Bombieri [1] observed the above conjecture holds by using techniques similar to those in proving the Burgess inequality in (3), and a number of estimates was given b J. Friedlander and H. Iwaniec in [18]. We note that when $|S|$ is very small, say approximately some power of $\log p$, (4) no longer holds since Montgomery [23] showed that assuming the Generalized Riemann Hypothesis, the least quadratic non-residue is as large as $c \log p \log \log p$ for infinitely many primes p. A recent result of S. Graham and C. Ringrose [19] proved that the least quadratic non-residue is of order at least $c \log p \log \log \log p$ infinitely often. If we choose S to be an interval consisting of $\{1, 2, \cdots, \lfloor \frac{c}{2} \log p \log \log p \rfloor\}$, then we get $\sum\limits_{a,b \in S} \eta(a-b) = |S|^2$.

A more general but slightly weaker inequality can be described as follows:

Theorem 2.3. *Let χ be a multiplicative character of order $m > 1$ in $\mathcal{F}_q$ for a prime power q and let $f \in \mathcal{F}_q[x]$ be a polynomial of positive degree that is not an mth power of a polynomial. Let d be the number of distinct roots of f in its splitting field over $\mathcal{F}_q$. Then for $S, T \subset \mathcal{F}_q$,*

$$\left| \sum_{a \in S} \sum_{b \in T} \chi(f(a+b)) \right| \leq d\sqrt{q|S||T|}$$

.

Proof: We consider a $q \times q$ matrix M with entries $M_{uv} = \chi(f(u-v))$. The eigenvalues of M are the Gaussian sums

$$g(j) = \sum_{x \in \mathcal{F}_q} \chi(f(x))\zeta^{jx}$$

for $j = 0, 1, ..., q-1$. We note that $g(j)$ is just a "hybrid" Gaussian sum (see e.g., p. 45 of [27]) and therefore

$$|g(j)| \leq d\sqrt{q} \tag{5}$$

For $S \subseteq \mathcal{F}_q$, let h_S denote the vector with entries $h_S(v)$ being 1 if v is in S and 0 otherwise. Let $-T$ denote $\{v : -v \in T\}$.

$$\sum_{a \in S} \sum_{b \in T} \chi(f(a+b)) \quad = \quad | < h_S, Mh_{-T} > |$$

$$\begin{aligned} &\leq d\sqrt{q}||h_S||\ ||h_{-T}|| \\ &= d\sqrt{q|S||T|}. \end{aligned}$$

Theorem 2.2 is proved.

Corollary 2.4.

$$|\sum_{a\in S}\sum_{b\in T}\chi(f(a+b))| \leq dq^{3/2}$$

where χ, f, d, S, T are as defined in Theorem 2.3.

We remark that the analogous version of Conjecture 2.2 for characters in $\mathcal{F}_q$ instead of in $\mathcal{F}_p$ is not true in general.

3. More incomplete sums

In Section 2 we investigated double sums which can be viewed as "2-dimensional" sums. Here we consider "higher-dimensional" analogues.

Theorem 3.1. Let χ denote a non-trivial multiplicative character in $\mathcal{F}_p$ for a prime p. Let X, Y, Z denote three subsets of $\mathcal{F}_p \times \mathcal{F}_p$. Then we have

$$\left|\sum_{(a,b,c)\in W}\chi(a+b+c)\right| \leq \sqrt{2}p^{3/4}|X|^{1/2}|Y|^{1/4}|Z|^{1/4} \tag{6}$$

where $W = W(X,Y,Z) = \{(a,b,c) : (a,b) \in X, (b,c) \in Y \text{ and } (c,a) \in Z\}$.

Proof: Let us assume without the loss of generality that $|X| \leq |Y| \leq |Z|$. For $T \subseteq \mathcal{F}_p \times \mathcal{F}_p$ and $s \in \mathcal{F}_p$, we denote $T^s = \{s' : (s,s') \in T\}$ and $T_s = \{s' : (s',s) \in T\}$.

By repeatedly using the Cauchy-Schwarz inequality and Theorem 2.2, we have

$$\begin{aligned} &\frac{1}{|X|}\left|\sum_{(a,b,c)\in W}\chi(a+b+c)\right|^2 \\ \leq\ & \sum_{(a,b)\in X}\left|\sum_{c\in Y^b\cap Z_a}\chi(a+b+c)\right|^2 \\ \leq\ & \sum_{(a,b)\in \mathcal{F}_p\times\mathcal{F}_p}\left|\sum_{c\in Y^b\cap Z_a}\chi(a+b+c)\right|^2 \end{aligned}$$

$$\begin{aligned}
&= \sum_{(a,b)\in\mathcal{F}_p\times\mathcal{F}_p}\ \sum_{c,c'\in Y^b\cap Z_a} \overline{\chi(a+b+c)}\chi(a+b+c') \\
&\leq \sum_{c,c'\in\mathcal{F}_p}\ \sum_{a\in Z^c\cap Z^{c'}}\ \sum_{b\in Y_c\cap Y_{c'}} \overline{\chi(a+b+c)}\chi(a+b+c') \\
&= \sum_{c\in\mathcal{F}_p} |Z^c||Y_c| + \sum_{c\neq c'}\ \sum_{a\in Z^c\cap Z^{c'}}\ \sum_{b\in Y_c\cap Y_{c'}} \overline{\chi(a+b+c)}\chi(a+b+c') \\
&\leq \sum_{c\in\mathcal{F}_p} |Z^c||Y_c| + 2\sum_{c\neq c'} \sqrt{p|Z^c||Y_{c'}|} \\
&\leq 2\sqrt{p}(\sum_c \sqrt{|Z^c|})\cdot(\sum_{c'} \sqrt{|Y_{c'}|}) \\
&\leq 2p^{3/2}(\sum_c |Z^c|)^{1/2}(\sum_{c'} |Y_{c'}|)^{1/2} \\
&\leq 2p^{3/2}|Z|^{1/2}|Y|^{1/2}
\end{aligned}$$

Therefore

$$\left|\sum_{(a,b,c)\in W} \chi(a+b+c)\right| \leq \sqrt{2}\, p^{3/4}|X|^{1/2}|Y|^{1/4}|Z|^{1/4}$$

As an immediate consequence of Theorem 3.1, we have

Corollary 3.2

$$|\sum_{(a,b,c)\in W} \chi(a+b+c)| \leq \sqrt{2}p^{11/4}$$

We remark that for the special case of $f = S_1 \times S_2$, $g = S_2 \times S_3$ and $h = S_3 \times S_1$ for subsets $S_1, S_2, S_3 \subseteq \mathcal{F}_q$, with $|S_1| \leq |S_2| \leq |S_3|$ we have

$$\begin{aligned}
&\left|\sum_{a\in S_1, b\in S_2, c\in S_3} \chi(a+b+c)\right| \\
&\leq \sum_{a\in S_1}\left|\sum_{b\in S_2, c\in S_3} \chi(a+b+c)\right| \\
&\leq \sqrt{p}|S_1|\sqrt{|S_2||S_3|} \\
&\leq \sqrt{p}(|f||g||h|)^{1/3}
\end{aligned}$$

It seems reasonable to make the following conjecture which, if true, has significant consequence on the discrepancy of graphs which will be described later in Section 5.

Conjecture 3.3 Let X denote a non-trivial multiplicative character in $\mathcal{F}_p$ for a prime p. For any three subsets X, Y, Z of $\mathcal{F}_p \times \mathcal{F}_p$, we have

$$\left| \sum_{(a,b,c) \in W} \chi(a+b+c) \right| \leq cp^{5/2}$$

where $W = W(X, Y, Z) = \{(a,b,c) : (a,b) \in X, (b,c) \in Y, (c,a) \in Z\}$ for some absolute constant c.

Theorem 3.4. Let χ denote a non-trivial character of order $m > 1$ in $\mathcal{F}_q$ for a prime power q and let $f \in \mathcal{F}_q(x)$ be a polynomial of positive degree that is not an m-th power of a polynomial. Let d be the number of distinct roots of f in its splitting field over $\mathcal{F}_q$. Then for every $c \in \mathcal{F}_q$ and subsets $R_1, ..., R_k$ of $(\mathcal{F}_q)^{k-1} = \overbrace{\mathcal{F}_q \times ... \times \mathcal{F}_q}^{k-1}$, we have

$$\left| \sum_{(a_1,...,a_k) \in W} \chi(f(a_1 + ... + a_k)) \right| \leq (d2^{k-2})^{2^{-k+2}} q^{1-2^{-k+1}} (|R_1|...|R_k|)^{1/k}$$

where $W(R_1, ..., R_k) = \{(a_1, ..., a_k) : (a_1, ..., a_{t-1}, a_{t+1} ..., a_k) \in R_t \text{ for } t = 1, ..., k\}$. The proof of Theorem 3.4 is a straightforward generalization of the proof of Theorem 3.1 and will be omitted. In fact it can be shown that

$$\left| \sum_{(a_1,...,a_k) \in W} \chi(f(a_1 + ... + a_k) \right| \leq (d2^{k-2})^{2^{-k+2}} q^{1-2^{-k+1}} |R_1^{1/2}||R_2|^{1/4} ... |R_{k-2}|^{2^{-k+2}} (|R_{k-1}||R_k|)^{1/2^{k-1}}$$

Conjecture 3.5.

$$\left| \sum_{(a_1,...,a_k) \in W} \chi(a_1 + ... + a_k) \right| \leq c \; q^{k-1/2}$$

and c is some absolute constant.

where χ, W and q are as defined in Theorem 3.4.

Theorem 3.4 can be further generalized as follows which is based on the motivation from the r-discrepancy of hypergraphs (cf. Section 5):

Theorem 3.6 Let χ denote a non-trivial character of order $m > 1$ in $\mathcal{F}_q$ for a prime power q and let $f \in \mathcal{F}_q[x]$ be a polynomial of positive degree that is not an m-th power of a polynomial. Let d be the number of distinct roots of f in its splitting field over $\mathcal{F}_q$. Let R_I denote subsets of $(\mathcal{F}_q)^r$ for a fixed integer $r < k$ and the indices of R_I range over all r-subsets of $\{1, ..., k\}$ denoted by $I \in C_r^k$. For a k-tuple $\bar{a} = (a_1, ..., a_k), a_i \in \mathcal{F}_q$, we denote $(\bar{a})_I = (a_{i_1}, ..., a_{i_r})$ where $i_1 < ... < i_r$ are in I.

For $R_I, I \in C_r^k$, we define

$$W_r(R_I)_{I \in C_r^k} = \{\bar{a} = (a_i, ..., a_k) : (\bar{a})_I \in R_I \text{ for all } I \in C_r^k\}$$

We have

$$\left| \sum_{(a_1, ..., a_k) \in W} \chi(f(a_1 + ... + a_k)) \right| \leq (d2^{r-1})^{2^{-r+1}} q^{1-2^{-r}} (\prod_I |R_I|)^{(k-r)/(k\binom{k-2}{r-1})}$$

4. Coset inequalities

The following inequality of incomplete character sums over cosets was conjectured in [10] and proved in [22].

Let χ denote a nontrivial complex-value multiplicative character defined on an extension field E over a finite field K of dimension t. Then for any $x \in E$ such that $E = K(x)$ we have

$$\left| \sum_{a \in K} \chi(x + a) \right| \leq (t-1)\sqrt{|K|}. \tag{7}$$

We can use the above coset inequality to derive another generalization of Theorem 2.1.

Theorem 4.1. Let χ denote a nontrivial complex-valued multiplicative character defined on an extension field E over a finite field K with dimension $t > 1$. Then for any $x \in E$ such that $E = K(x)$, and for any $S, T \subseteq E^*$ we have

$$\alpha \left| \sum_{\chi \in \Phi} \sum_{\substack{u \in S \\ v \in T}} \chi(uv + x) \right| \leq (t-1)\sqrt{|K|}\sqrt{|S||T|}$$

where Φ consists of all nontrivial characters χ such that $\chi/K = 1$, $\chi(0) = 0$ and $\alpha = |K^*|/|E^*|$.

Proof: We consider a matrix M with rows and columns indexed by elements in E^*. We define $A_{u,v}$ to be 1 if $u/v \in x + K$. Let J denote the matrix with all entries being 1 and we consider $M = A - \alpha J$. M has eigenvalues 1 and $\sum\limits_{a \in K} \chi(x+a)$, where χ ranges over all non-trivial multiplicative characters. Therefore using (7) and $t > 1$, we have

$$|< v_S, M v_{T^{-1}} >| \leq (t-1)\sqrt{|K|}\sqrt{|S||T|}$$

where T^{-1} consists of all t so that $t^{-1} \in T$, v_S is the vector with v-th entry being 1 if v is in S and 0 otherwise.

We note that

$$\begin{aligned} < v_S, M v_{T^{-1}} > &= \sum_{\substack{u \in S \\ v \in T}} M_{uv} \\ &= \sum_{u \in S, v \in T} \phi(uv + x) \\ \text{where } \phi(y) &= \{ \begin{array}{ll} 1-\alpha & \text{if } y \in K \\ -\alpha & \text{otherwise} \end{array} \end{aligned}$$

since $|\Phi| = \alpha^{-1} - 1$.

It is not difficult to see that

$$\phi = \alpha \sum_{\chi \in \Phi} \chi$$

Therefore we have

$$\alpha \left| \sum_{\chi \in \Phi} \sum_{\substack{u \in S \\ v \in T}} \chi(uv + x) \right| \leq (t-1)\sqrt{|K|}\sqrt{|S||T|}$$

Theorem 4.1 is proved.

5. Character sums and graph theory

Many character sum inequalities mentioned in previous sections are intimately related to problems in extremal graph theory. Here we will discuss the connections with graph theory and, in particular, point out the implications and applications of various conjectures if they can be proved to be true.

Graph theory is a study of discrete structures and their fundamental properties. A graph consists of a node set N together with an edge set which is a prescribed set of unordered pairs of N. More generally, a hypergraph has a node set N together with an edge set consisting of subsets of N. If all the edges in the edge set of a hypergraph are of size k, the hypergraph is called a k-graph. Among all graphs or hypergraphs, of particular interest are those satisfying certain desired properties. Some of these properties are not only interesting of their own right but also are closely related to many problems and applications in broad range of areas. For example, one of the key graph invariants is the discrepancy of a graph G, which is defined to be the maximum difference of the number of edges contained in a node subset S from the expected value, where S ranges over all subsets of t nodes of G. The discrepancy of G is the maximum discrepancy over all subsets on t nodes for some given t. The reader is referred to [11, 12] for the definitions and further discussions on the discrepancy of graphs and its relationship to other graph invariants.

To find graphs with a desired property, there are basically two different approaches: the probabilistic method and explicit constructions. The probabilistic method consists of two steps: first an appropriate (probability) measure is defined on a class of graphs; second, the subclass of desired graphs is shown to have positive measure. Suppose we assign equal probability to all graphs on n nodes. It can be easily shown that a graph on n nodes has discrepancy no more than $cn^{3/2}$ with probability approaching 1 as n approaches infinity. In other words, a random graph has discrepancy at most $cn^{3/2}$ for some absolute constant c. In fact, for $s = n^\epsilon$ for fixed $\epsilon > 0$, the discrepancy for a random graph on s nodes is at most $cn^{\epsilon/2}$ for an absolute constant c depending only on ϵ. As we will see, for $\epsilon < \frac{1}{2}$, the best known constructions yield results much weaker than by the probabilistic methods. So, while we can conclude that almost all graphs on n nodes have the desired property (such as discrepancy on s nodes no more than $cn^{3\epsilon/2}$, for $s = n^\epsilon, \epsilon < 1/2$) we are unable to construct such graphs for infinitely many n.

Perhaps the most obvious candidate for simulating a random graph is the so-called Paley graph Q_p. The Paley graph consists of p nodes for a prime p congruent to 1 modulo 4. Two nodes i and j are adjacent if and only if $i - j$ is a quadratic residue modulo p. A Paley sum graph $\tilde{Q}_p$ has node set Z_p for a prime p, and two nodes are adjacent if and only if $i + j$ is a quadratic residue modulo p. Theorem 2.1 gives an upper bound for the discrepancy for the Paley graphs and Paley sum graphs. When s is large, say $s = \alpha p$ for $0 < \alpha < 1$, the bound is best possible within a constant depending on α. When s is small, say $s < n^{1/2}$, the bound is not useful. Conjecture 2.2 is partly based on the belief that the Paley graph behaves like a random graph and thus might have small discrepancy on $s = n^\epsilon$ nodes , where $\epsilon < 1/2$. We note that if Conjecture 2.2 is true, there are many applications in extracting almost unbiased bits from weak random sources [8, 34] and deterministic simulation of randomized algorithms [6].

The character sum inequalities in Section 3 relate to the discrepancies of a k-graph. We can define a Paley k-graph with node set Z_p for a prime p and $a_1, ..., a_k$ form an edge if $a_1 + ... + a_k$ is a quadratic residue modulo p. Let G denote a k-graph G on n nodes N. Let H be an r-graph with node set N for $r < k$. The subgraph of G induced by H denoted by $G[H]$ has node set N and edges $\{a_1, ..., a_k\}$ where all r-subsets of $\{a_1, ..., a_k\}$ are all edges of H. An 1-graph has edge-set being a subset of the node set.

The r-discrepancy of a k-graph is defined to be the maximum difference of the number of edges in $G[H]$ and the expected value (which is $\frac{e(G)}{e(K)}\ e(K[H])$) over all r-graphs H where K denotes the complete k-graph which contains all k-sets of N as edges and $e(G)$ denotes the number of edges in G.

Theorem 3.1, 3.4 and 3.6 give upper bounds for the r-discrepancies of a k-graph. There are a number of related applications such as amplifying random bits [15, 29], communication complexity [7] and circuit complexity [20, 21]. Conjecture 3.5, if true, would have significant consequence to k-party communication complexity.

The character sum inequalities in Section 4 concern constructions of graphs with edge density small, say graphs with p^t nodes and p^{t+1} edges for a fixed integer t. The coset graph which has adjacency matrix A_{uv} is described in the proof of Theorem 4.1 and the discrepancy for the coset graph is upper bounded in Theorem 4.1.

Acknowledgement:

The author is extremely grateful to Enrico Bombieri for illuminating discussions. The author also wishes to thank Hendrik Lenstra, Winnie Li and Andrew Odlyzko for many helpful comments.

References

[1] E. Bombieri, personal communication.

[2] D.A. Burgess, The distribution of quadratic residues and and non-residues, *Mathematica* **4** (1957) 106-112.

[3] D.A. Burgess, On character sums and primitive roots, *Proc. London Math. Soc.* **12** (1962) 179-192.

[4] D.A. Burgess, A note on the distribution of residues and non-residues, *J. London Math. Soc.* **38** (1963) 253-256.

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

[6] M. Blum and S. Micali, How to generate cryptographically strong sequences of pseudo-random bit, *SIAM J. Compt.* **13** (1984), 850-863.

[7] L. Babai, N. Nisan and M. Szegedy, Multiparty protocols and logspace-hard pseudo-random sequences, *Proceedings of 21st Annual ACM Symp. on Theory of Computing* (1989) 1-11.

[8] B. Chor and O. Goldreich, Unbiased bits from sources of weak randomness and probabilistic communication complexity, *26th Annual Symp. on Foundations of Computer Science* (1985) 429-442.

[9] S. Chowla, A theorem on characters II, *J. Indian Math Soc.* **19** (1932) 279-284.

[10] F.R.K. Chung, Diameters and eigenvalues, *Journal of the Amer. Math. Soc.* **2** (1989) 187-196.

[11] F.R.K. Chung, Constructing random-like graphs, AMS Short Course Lecture Notes (1991).

[12] F.R. K. Chung and R. L. Graham, Quasi-random set systems, *Journal of the Amer. Math. Soc.* bf 4 (1991) 151-196.

[13] F.R.K. Chung, R.L. Graham and R.M. Wilson, Quasi-random graphs, *Combinatoric* 9 (1989) 345-362.

[14] F.R.K. Chung and P. Tetali, Communication complexity and quasi-randomness, *SIAM J. Discrete Math.* 6 (1993), 110-123

[15] A. Cohen and A. Wigderson, Dispersers, deterministic amplification and weak random sources, *FOCS*, 30(1989) 14-19.

[16] H. Davenport and P. Erdös, The distribution of quadratic and higher residues, *Publ. Math. Debrecen* **2** (1952) 252-265.

[17] E. Erdös and J. Spencer, Imbalanced in k-colorations, *Networks* **1** (1971) 379-385.

[18] J. Friedlander and H. Iwaniec, Estimates for character sums. *Proc. Amer. Math. Soc.* 119 (1993) 365-372

[19] S. Graham and C. Ringrose, Lower bounds for least quadratic non-residues, in *Analytic Number Theory* (Allerton park, Il. 1989) *Progr. Math.* 85, Birkhauser, Boston, (1990) 269-309

[20] Johan Hastad and Michael Goldmann, On the power of small-depth threshold circuits, *31st Annual Symp. on Foundations of Computer Science* (1990) 610-618.

[21] A. Hajnal, W. Mass, P. Pudlak, M. Szegedy and G. Turan, Threshold circuits of bounded depth, *Proceedings of 28th Annual Symposium on Foundations Computer Science* (1987) 99-110.

[22] N.M. Katz, An estimate for character sums, *J. of Amer. Math. Soc.* **2** (1989) 197-200.

[23] H.L. Montgomery, Topics in multiplicative number theory, Lecture Notes in Math. 227, Springer-Verlag, New York (1971).

[24] H.L. Montgomery and R.C. Vaughn, Exponential sums with multiplicative coefficients, *Invent. Math* **43** (1977) 69-82.

[25] R.E.A.C Paley, A theorem on characters, *J. London Math. Soc.* **7** (1932) 28-32.

[26] G. Pólya, Uber die verteilung der quadratischen Reste und Nichtreste, *Göttinger Nachrichten* (1918) 21-29.

[27] Wolfgang M. Schmidt, Equations over Finite Fields, An Elementary Approach, Springer-Verlag, Berlin-New York (1975)

[28] Michael Sipser, Expanders, randomness or time versus space, *J. of Computer and System Sciences* **36** (1988) 379-383.

[29] A. V. Sokolovskü, Lower bounds in the "Large Sieve", (Russian), *Zap. Nucn. Sem. Lenigrad. Otdel. Mat. Inst. Steklov.* **91** (1979) 125-133, *J. Soviet Math.* **17** (1981) 2166-2173.

[30] I.M. Vinogradov, Sur la distribution des résidus et des non-résidus des puissances *J. Phys.-Math. Soc. Perm.* **1** (1918) 94-96.

[31] Y. Wang, A note on the least primitive root of a prime, *Sci. Record (N.S.)* **3** (1959) 174-179.

[32] Y. Wang, A note on the least primitive root of a prime (Chinese), *Acta Math. Sinica* **9** (1959) 432-441; *Sci. Sinica* **10** (1961) 1-14.

[33] Andrew C.-C. Yao, On ACC and threshold circuits, *31st Annual Symposium on Foundations of Computer Science* (1990) 619-627.

[34] D. Zuckerman, General weak random sources, *Symposium on Foundations of Computer Science* (1990) 534-543.