Gowers norm and pseudorandom measures of the pseudorandom binary sequences

伪随机二进制数列的Gowers 范数与随机测度

Huaning LIU (刘华宁)

Department of Mathematics, Northwest University

Xi'an, Shaanxi, P. R. China

E-mail: hnliumath@hotmail.com

Introduction to . . .

Pseudorandom . . .

Examples of the . . .

Large families of . . .

Gowers norm of . . .

Abstract

Recently there has been much progress in the study of arithmetic progressions. An important tool in these developments is the Gowers uniformity norm. In the past decade in a series of papers C. Mauduit, J. Rivat and A. Sarkozy studied the pseudorandomness of the pseudo-random binary sequences. In this talk we introduce the developments of the pseudorandom binary sequences, and study the Gowers norm for the pseudorandom binary sequences. Some examples are given to show that the "good" pseudorandom sequences have small Gowers norm.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

Outline

1. Introduction to pseudorandom sequences
2. Pseudorandom measures of PR binary sequences
3. Examples of pseudorandom binary sequences
4. Large families of pseudorandom binary sequences
5. Gowers norm of pseudorandom binary sequences

1 Introduction to pseudorandom sequences

✠ The pseudorandom sequences play an important role in many fields, so numerous papers have been written on this subject in the last several decades. In the majority of the papers constructions of pseudorandom sequences are given and / or tested for pseudorandomness.

✠ In general, the concept of "pseudorandom sequences" can be interpreted in three different ways:

1) $[0, 1)$ sequences;

2) pseudorandom sequences of integers selected from $\{1, \cdots, N\}$,

3) pseudorandom binary, or more generally, b-ary sequences.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Knuth [The art of computer programming, 1981] gives an excellent survey of these concepts. These concepts are closely related, and there are simple transition algorithms are described in Knuth's book.

✠ However, in spite of the close connection between the three types of pseudorandom sequences, there are also certain differences, and, in particular, the study of the different pseudorandom concepts may inspire different approaches and construction principles.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ So far mostly pseudorandom sequences of types 1 and 2 have been studied; excellent surveys of the theory of uniform pseudorandom sequences are given by Niederreiter in the references:

♠ H. Niederreiter, Recent trends in random number and random vector generation, Ann. Oper. Res., 1991

♠ H. Niederreiter, Random number generation and quasi-Monte Carlo methods, 1992

♠ .....

✠ In these others papers and books Niederreiter gives a brief description and analysis of the methods of pseudorandom sequences generation, starting from the most classical and widely used linear congruential method, and ending with the most promising, recently introduced method, which is based on the concepts of the multiplicative inverse.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ A common feature of all these methods is that the construction of the pseudorandom sequences

$$\mathbf{X} = (x_1, x_2, \cdots, x_N)$$

is given by a recursion

$$x_n = f(x_{n-1}, x_{n-2}, \cdots, x_{n-k}).$$

✠ Niederreiter (later with coauthors) did a work of basic importance in justifying the use of these construction methods by carrying out the "serial test" in all these cases, i.e., he showed that the $[0, 1)$ pseudorandom sequences constructed by these methods are such that the discrepancy of the sequence

$$(x_1, x_2, \cdots, x_s), \cdots, (x_n, x_{n+1}, \cdots, x_{n+s-1}), \cdots, (x_{N-s+1}, x_{N-s+2}, \cdots, x_N)$$

of s-dimension vectors is "small" (for fixed s).

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ For the construction of the pseudorandom sequences

$$\mathbf{X} = (x_1, x_2, \cdots, x_N),$$

which is given by a recursion

$$x_n = f(x_{n-1}, x_{n-2}, \cdots, x_{n-k}),$$

an important advantage of this sort of constructions is that the elements of the pseudorandom sequences can be computed by a simple algorithm.

✠ On the other hand, there are disadvantages as well. In particular, as H. Niederreiter [Ann. Oper. Res., 1991] writes, a deficiency of the most used linear congruential method is :"Other known regularities in sequences of linear congruential pseudorandom numbers are certain long-range correlations. These regularities can be disruptive in simulations where random irregularities are desired".

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ In general, the analysis of the known constructions leads to the conclusion that, although the new constructions are superior to the previous ones from many points of view, there is a price paid for this so that there is no perfect construction. Thus the selection of the construction method to be applied must depend on the application in mind; the construction which is superior in a certain situation may fail in another one.

✠ This also means that the search for new approaches and new constructions should be continued.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ A number of pseudorandom sequences of type 1 and 2 have been studied. However, less attention has been paid to pseudorandom sequences of type 3.

✠ In a series of papers Mauduit, Rivat and Sárközy (partly with other coauthors) studied finite pseudorandom binary sequences

$$E_N = \{e_1, \cdots, e_N\} \in \{-1, +1\}^N,$$

which play an important role in cryptography.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

2 Pseudorandom measures of the pseudorandom binary sequences (该节内容请参阅Mauduit 和Sárközy 于1997 年在Acta Arith. 的论文)

✠ In order to study the pseudorandom binary sequences, we must introduce some pseudorandom measures.

✠ How to define the measures?

✠ One may pose more and more criteria for pseudorandomness (and in certain applications, one can be forced to do this), and correspondingly, one may introduce more and more pseudorandom measures. However, it would be more and more difficult to handle the measures; besides posing too many pseudorandom requirements, it may occur that there is no pseudorandom binary sequence of a given size at all.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Thus one has to draw the limit somewhere.

✠ What we should do?

♠ First, we expect that this measure should reflect the most important and intensively studied random properties such as

1. normality;
2. well-distribution relative to arithmetic progressions;
3. small multiple correlations.

♠ Second, the pseudorandomness of binary sequences should be characterized by a real-valued function defined on the set of all finite binary sequences, so that one should be able to compare two sequences of the same length.

♠ Third, this measure should have different levels.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Explanation for the third requirement:

Definition [Page 162 of Knuth's book] A finite sequence $E_N = (e_1, \cdots, e_N) \in \{-1, +1\}^N$ is said to be pseudorandom if for all $k \in \mathbb{N}$ with $k \leq \dfrac{\log N}{\log 2}$, and for all $\mathbf{X} \in \{-1, +1\}^k$ we have

$$\left| T(E_N, N+1-k, X) - \frac{N+1-k}{2^k} \right| \leq \frac{1}{\sqrt{N}}.$$

✠ This definition allows two possibilities only: pseudorandom or not.

✠ 如果一个数列在上式中满足$\leq \dfrac{2}{\sqrt{N}}$, 那么这个数列是伪随机的吗? 更进一步, 如果此数列在其它方面同时具有非常好的性质, 那么怎么衡量这个数列?

✠ 因此我们的测度(measure) 应该是灵活一点, 要有层次.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ First we consider the case of infinite sequence $E = (e_1, e_2, \cdots) \in \{-1, +1\}^\infty$.

✠ For $k \in \mathbb{N}$, $\mathbf{X} = (x_1, \cdots, x_k) \in \{-1, +1\}^k$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $D = (d_1, \cdots, d_k) \in \mathbb{N}^k$, $d_1 < \cdots < d_k$, write

$$T(E, M, \mathbf{X}) = |\{n : 0 \le n < M, (e_{n+1}, e_{n+2}, \cdots, e_{n+k}) = \mathbf{X}\}| , \tag{2.1}$$

$$U(E, M, a, b) = \sum_{j=1}^{M} e_{a+jb} \tag{2.2}$$

and

$$V(E, M, D) = \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_k}. \tag{2.3}$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ E is said to be normal if

$$\left| T(E, M, \mathbf{X}) - \frac{M}{2^k} \right| = o(M) \tag{2.4}$$

for all fixed k and $\mathbf{X}$, as $M \longrightarrow \infty$, while the second and third random property can be expressed as

$$U(E, M, a, b) = \sum_{j=1}^{M} e_{a+jb} = o(M) \tag{2.5}$$

$$V(E, M, D) = \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_k} = o(M) \tag{2.6}$$

for all fixed a, b and D, as $M \longrightarrow \infty$.

✠ It is said in Mauduit and Sárközy's paper that (2.4) and (2.6) are equivalent. By an important theorem of Niven and Zuckerman [Pacific J. Math., 1951] the normality of E implies the well-distribution relative to arithmetic progressions. That is to say, (2.4) $\Longrightarrow$ (2.5).

✠ Therefore in the case of infinite binary sequences it suffices to require normality.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Now we consider the finite case. For $E_N = (e_1, \cdots, e_N) \in \{-1, +1\}^N$, we define the following measure:

♠ 1. Normality measure of order k:

$$N_k(E_N) = \max_{\mathbf{X} \in \{-1,+1\}^k} \max_{0 < M \le N+1-k} \left| T(E_N, M, \mathbf{X}) - \frac{M}{2^k} \right|,$$

♠ 2. Well-distribution measure:

$$W(E_N) = \max_{a,b,t} |U(E_N, t, a, b| = \max_{a,b,t} \left| \sum_{j=1}^{t} e_{a+jb} \right|,$$

where the maximum is taken over all a, b, t such that $a \in \mathbb{Z}$, $b, t \in \mathbb{N}$ and $1 \le a + b \le a + tb \le N$.

♠ 3. Correlation measure of order k:

$$C_k(E_N) = \max_{M,D} |V(E_N, M, D| = \max_{M,D} \left| \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_k} \right|,$$

where the maximum is taken over all $D = (d_1, \cdots, d_k)$ and M such that $M + d_k \le N$.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ In the finite case, the connection between normality, well-distribution in arithmetic progressions and correlation is much more complicated than in the infinite case.

✠ The connection between normality and small correlation is only one way:

$$N_k(E_N) \leq \max_{1\leq t\leq k} |C_t(E_N)| \,.$$

✠ Problems 28-30 of Knuth's book shows that Even if $C_k(E_N)$ is small, $W(E_N)$ can be quite large.

✠ On the other hand, it may occur that both $N_k(E_N)$ and $W(E_N)$ are very small, but $C_k(E_N)$ is very large. There is an example in Mauduit and Sárközy's paper.

✠ Therefore, in order to show a finite binary sequence E_N can be considered as a pseudorandom sequence, it suffices to show that both $W(E_N)$ and $C_k(E_N)$ are small.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ These two measures can be combined as the following measure:

♠ 4. Combined (well-distribution-correlation) pseudorandom measure of order k:

$$Q_k(E_N) := \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \cdots e_{a+jb+d_k} \right|,$$
$$1 \le a + jb + d_i \le N (j = 0, 1, \cdots, t; i = 1, 2, \cdots, k).$$

✠ 衡量伪随机性的这几个测度当然不是完美的, 肯定会有一些数列, 它们在这种衡量标准下被当作伪随机数列, 但却不是真正的随机数列.

✠ 然而不管怎样, 这套标准还是能够反映出伪随机性的最重要的三个方面的性质: normality, well-distribution 和correlation. 为了能够继续进行, 让我们暂且只考虑这么多.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Recall the following measures of pseudorandomness:

♣ Well-distribution measure:

$$W(E_N) := \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|, \quad 1 \le a \le a + (t-1)b \le N;$$

♣ Correlation measure of order k:

$$C_k(E_N) := \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_k} \right|, \quad 0 \le d_1 < \cdots < d_k \le N-M;$$

♣ Combined PR- measure of order k:

$$Q_k(E_N) := \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \cdots e_{a+jb+d_k} \right|,$$

$$1 \le a + jb + d_i \le N (j = 0, 1, \cdots, t; i = 1, 2, \cdots, k).$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ The sequence is considered as a "good" pseudorandom sequence if both $W(E_N)$ and $C_k(E_N)$ (at least for small k) are "small" in terms of N.

✠ Later Cassaigne, Mauduit and Sárközy [Acta Arith., 2002] proved that this terminology is justified since for a truly random $E_N \in \{-1,+1\}^N$, both $W(E_N)$ and $C_k(E_N)$ are less than $N^{\frac{1}{2}}(\log N)^c$.

✠ For details, for choosing each $E_N \in \{-1,+1\}^N$ with probability $1/2^N$, they proved that

$$\delta(\epsilon)\sqrt{N} < W(E_N) < 6\sqrt{N\log N}$$

and

$$\delta(\epsilon,k)\sqrt{N} < C_k(E_N) < 5\sqrt{kN\log N}$$

hold with probability at least $1-\epsilon$ for $E_N \in \{-1,+1\}^N$.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Recently N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl continued the work in this direction and investigated the typical and minimal values of these measures (概率论中指数分布).

✠ For choosing each $E_N \in \{-1,+1\}^N$ with probability $1/2^N$, they showed that

$$\delta(\epsilon)\sqrt{N} < W(E_N) < \frac{1}{\delta(\epsilon)}\sqrt{N}$$

and

$$\frac{2}{5}\sqrt{N\log\binom{N}{k}} < C_k(E_N) < \frac{7}{4}\sqrt{N\log\binom{N}{k}}$$

hold for $2 \le k \le N/4$with probability at least $1-\epsilon$.

✠ Furthermore, they proved that

$$\min\left\{C_k(E_N) : E_N \in \{-1,+1\}^N\right\} = 1 \quad \text{if } k \text{ is odd}$$

$$\min\left\{C_k(E_N) : E_N \in \{-1,+1\}^N\right\} > \sqrt{\frac{1}{2}\lfloor\frac{N}{k+1}\rfloor} \quad \text{if } k \text{ is even.}$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

3 Examples of the pseudorandom binary sequences

3.1. Legendre symbol

✠ Let p be an odd prime. If congruence $x^2 \equiv n(\mathrm{mod} p)$ has a solution we say that n is a quadratic residue mod p. If congruence $x^2 \equiv n(\mathrm{mod} p)$ has no solution we say that n is a quadratic nonresidue mod p.

✠ The Legendre symbol $\left(\frac{n}{p}\right)$ is defined as following:

$$\left(\frac{n}{p}\right) = \begin{cases} +1, & \text{if } n \text{ is a quadratic residue mod } p; \\ -1, & \text{if } n \text{ is a quadratic nonresidue mod } p; \\ 0, & \text{if } n \equiv 0(\mathrm{mod} p) \end{cases}$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ We know that every reduced residue system mod p contains exactly $(p-1)/2$ quadratic residues and exactly $(p-1)/2$ quadratic non-residues mod p.

✠ For example, $p = 11$,

$$\begin{array}{rcccccccccc} n = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \left(\frac{n}{p}\right) = & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \end{array}$$

$p = 13$

$$\begin{array}{rcccccccccccc} n = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ \left(\frac{n}{p}\right) = & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \end{array}$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ It was shown in [Acta Arith., 1997] that the Legendre symbol forms a "good" pseudorandom sequence. More exactly, let p be an odd prime, and

$$N = p - 1, \quad e_n = \left(\frac{n}{p}\right), \quad E_N = \{e_1, \cdots, e_N\}.$$

We have

$$\begin{aligned} W(E_N) &< N^{1/2} \log N \\ C_k(E_N) &< kN^{1/2} \log N \\ Q_k(E_N) &< 9kN^{1/2} \log N. \end{aligned}$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

Outline of the proof

✠ We only prove $Q_k(E_N) < 9kN^{1/2}\log N$, from which we easily get the other two estimates.

✠ Recall the definition of $Q_k(E_N)$:

$$Q_k(E_N) := \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \cdots e_{a+jb+d_k} \right|,$$
$$1 \le a + jb + d_i \le N (j = 0, 1, \cdots, t; i = 1, 2, \cdots, k).$$

We have

$$\left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \cdots e_{a+jb+d_k} \right|$$
$$= \left| \sum_{n=0}^{t} \left(\frac{a+nb+d_1}{p}\right) \left(\frac{a+nb+d_2}{p}\right) \cdots \left(\frac{a+nb+d_k}{p}\right) \right|$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

$$
\begin{aligned}
&= \left| \sum_{n=0}^{t} \left(\frac{a\bar{b} + n + d_1\bar{b}}{p} \right) \left(\frac{a\bar{b} + n + d_2\bar{b}}{p} \right) \cdots \left(\frac{a\bar{b} + n + d_k\bar{b}}{p} \right) \right| \\
&= \left| \sum_{n=0}^{t} \left(\frac{n + h_1}{p} \right) \left(\frac{n + h_2}{p} \right) \cdots \left(\frac{n + h_k}{p} \right) \right| \\
&= \left| \sum_{n=0}^{t} \left(\frac{f(n)}{p} \right) \right| = \left| \sum_{n=0}^{t} x_p^*(f(n)) \right|,
\end{aligned}
$$

where $f(n) = (n+h_1)(n+h_2)\cdots(n+h_k)$, $h_j \equiv (a+d_j)\bar{b}$. It is obvious that $h_i \not\equiv h_j (\mod p)$ for $1 \le i < j \le k$.

✠ To give an upper bound for the incomplete character sum in the above, we need the following lemma.

Lemma 3.1.1 Suppose that p is a prime number, χ is a non-principal character modulo p of order d (so that $d \mid p-1$), $f(x) \in \mathbb{F}_p[x]$ has degree k and a factorization $f(x) = b(x-x_1)^{d_1} \cdots (x-x_s)^{d_s}$ (where $x_i \neq x_j$ for $i \neq j$) in $\overline{\mathbb{F}}_p$ with $(d, d_1, \cdots, d_s) = 1$. Let X, Y be real numbers with $0 < Y \leq p$. Then

$$\left| \sum_{X<n\leq X+Y} \chi(f(n)) \right| < 9kp^{1/2} \log p.$$

- This Lemma follows from Weil's theorem.
- For details, see Mauduit and Sárközy's paper [Acta Arith., 1997].
- Therefore

$$\left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \cdots e_{a+jb+d_k} \right| = \left| \sum_{n=0}^{t} x_p^*(f(n)) \right| < 9kp^{1/2} \log p.$$

and

$$Q_k(E_N) = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \cdots e_{a+jb+d_k} \right| < 9kN^{1/2} \log N.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

3.2. Liouville function

✠ The Liouville function $\lambda(n)$ is defined by

$$\lambda(n) = (-1)^{a_1+\cdots+a_k}, \qquad \text{for} \qquad n = p_1^{a_1} \cdots p_k^{a_k}.$$

✠ It is natural to expect that the sequence $\lambda(n)$ behaves like a random sequence of $\pm$ signs.

✠ In [Acta Arith., 1999] and [Acta Arith., 2000], J. Cassaigne and coauthors studied the pseudorandomness of the Liouville function.

✠ For details, let $L_N = \{\lambda(1), \lambda(2), \cdots, \lambda(N)\}$. They showed that the well-distribution measure of the sequence is small. On the other hand, only very weak estimates can be given for the correlation of the sequence.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ First, they proved that $W(L_N) < N(\log N)^{-A}$ and

$W(L_N) < N^{\frac{5}{6}+\epsilon}$ (under the generalized Riemann hypothesis).

Outline of the proof

✠ Write $F_x(\alpha) = \sum_{n \le x} \lambda(n) \mathrm{e}(n\alpha)$.

Lemma 3.2.1 (i) For any real number $H > 0$, for $x > x_0(H)$ we have

$$|F_x(\alpha)| < x(\log x)^{-H} \quad \text{for all} \quad 0 \le \alpha \le 1.$$

(ii) Under the generalized Riemann hypothesis, for $\epsilon > 0$, $x > x_1(\epsilon)$ we have

$$|F_x(\alpha)| < x^{5/6+\epsilon} \quad \text{for all} \quad 0 \le \alpha \le 1.$$

Proof This is Lemma 2 in Sárközy's paper [Studia Sci. Math. Hung., 1988].

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

$$\left|\sum_{j=1}^{t}\lambda(a+jb)\right| = \left|\sum_{\substack{a<n\le a+tb\\ n\equiv a(\bmod b)}}\lambda(n)\right| = \left|\sum_{a<n\le a+tb}\lambda(n)\cdot\frac{1}{b}\sum_{h=1}^{b}\mathbf{e}\left(\frac{(n-a)h}{b}\right)\right|$$

$$= \frac{1}{b}\left|\sum_{h=1}^{b}\mathbf{e}\left(\frac{-ah}{b}\right)\sum_{a<n\le a+tb}\lambda(n)\mathbf{e}\left(\frac{nh}{b}\right)\right|$$

$$= \frac{1}{b}\left|\sum_{h=1}^{b}\mathbf{e}\left(\frac{-ah}{b}\right)\left(F_{a+tb}\left(\frac{h}{b}\right)-F_a\left(\frac{h}{b}\right)\right)\right|$$

$$\le \frac{1}{b}\sum_{h=1}^{b}\left(\left|F_{a+tb}\left(\frac{h}{b}\right)\right|+\left|F_a\left(\frac{h}{b}\right)\right|\right).$$

By Lemma 3.2.1 we have $\left|\sum_{j=1}^{t}\lambda(a+jb)\right| < 2N(\log N)^{-2A}$ unconditionally and, under GRH, $\left|\sum_{j=1}^{t}\lambda(a+jb)\right| < 2N^{5/6+\epsilon/2}$.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ It follows, for N large enough,

$$W(L_N) = \max_{a,b,t} \left| \sum_{j=1}^{t} \lambda(a+jb) \right| < N(\log N)^{-A}$$

unconditionally and, under GRH,

$$W(L_N) = \max_{a,b,t} \left| \sum_{j=1}^{t} \lambda(a+jb) \right| < N^{5/6+\epsilon}.$$

✠ Noting that the RH is equivalent to

$$\sum_{1 \le n \le x} \lambda(n) = O(x^{1/2+\epsilon}).$$

Therefore, it is very hard to prove that $W(L_N) \ll N^{1/2+\epsilon}$.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

Another possible approach (under GRH)

✠ Recently we proved that

$$W(L_N) = \max_{a,b,t} \left| \sum_{j=0}^{t} \lambda(a+jb) \right| \ll N^{\frac{1}{2}+\epsilon}, \qquad \text{under GRH.}$$

The proof is omitted.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ The estimate of the correlation measure of L_N is a hopelessly difficult problem. Many papers have been published on the estimate

$$\sum_{n \le x} g_1(n) g_2(n+1),$$

where g_1 and g_2 are multiplicative functions. However, as Hildebrand writes in his review on Elliott's paper [Mem. Amer. Math. Soc., 1994]: "For example, in the case when the functions $g_i(n)$ are both equal to the Möbius function $\mu(n)$ or the Liouville function $\lambda(n)$, one would naturally expect that the above sum is of order $o(x)$ when $x \longrightarrow \infty$, but even the much weaker relation

$$\liminf_{x \longrightarrow \infty} \frac{1}{x} \sum_{n \le x} \lambda(n)\lambda(n+1) < 1$$

is not known and seems to beyond reach of the present methods".

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

Related results

✠ Harman, Pintz and Wolke [Studia Sci. Math. Hungar., 1985] proved that

$$(1+o(1))\frac{1}{3} < \frac{1}{x}\sum_{n\le x}\lambda(n)\lambda(n+1) < 1-\frac{1}{(\log x)^{7+\epsilon}}.$$

✠ Elliott [Notas Soc. Mat. Chile, 1992] showed that

$$\liminf_{x\longrightarrow\infty}\frac{1}{x}\sum_{n\le x}\lambda(n)\lambda(n+1)\lambda(n+2) \le \frac{20}{21}.$$

✠ J. Cassaigne and coauthors [Acta Arith., 1999] proved that

$$\left|\sum_{n\le x}\lambda(n)\lambda(n+d)\cdots\lambda(n+2kd)\right|$$
$$\le \begin{cases} \left(1-\dfrac{2}{3(2k+1)}\right)x+O(\log x), & \text{if } d \text{ is even;} \\ \left(1-\frac{2}{3(k+1)}\right)x+O(\log x), & \text{if } d \text{ is odd.} \end{cases}$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

3.3. The exponent of a number mod a primitive root

✠ Let p be an odd prime, g a primitive root modulo p. Define ind$n$, by $1 \leq \text{ind}n \leq p-1$ and $n \equiv g^{\text{ind}n} (\text{mod} p)$. Write $N = p-1$ and define the sequence $E_N = \{e_1, \cdots, e_N\}$ by

$$e_n = \begin{cases} +1, & \text{if } 1 \leq \text{ind}n \leq (p-1)/2, \\ -1, & \text{if } (p+1)/2 \leq \text{ind}n \leq p-1. \end{cases}$$

A. Sárközy [Studia Sci. Math. Hungar.,2001] showed that

$$W(E_N) < 20N^{1/2}(\log N)^2$$

and

$$C_k(E_N) < 27k8^k N^{1/2}(\log N)^{k+1}.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

3.4. The signs of the Kloosterman sum

✠ Let p be a prime, and $\mathrm{e}(x) = \mathrm{e}^{2\pi i x}$. Denote the Kloosterman sum by

$$S(l, m; p) = \sum_{k=1}^{p-1} \mathrm{e}\left(\frac{lk + m\overline{k}}{p}\right),$$

where $\overline{k}$ is the multiplicative inverse of k modulo p. It is easy to show that $S(1, n; p)$ is a real non-zero number.

Proof

$$S(1, n; p) = \sum_{k=1}^{p-1} \mathrm{e}\left(\frac{k + n\overline{k}}{p}\right) = \sum_{k=1}^{p-1} \mathrm{e}\left(\frac{p - k + n\overline{p - k}}{p}\right)$$

$$= \sum_{k=1}^{p-1} \mathrm{e}\left(\frac{-k - n\overline{k}}{p}\right) = \overline{S(1, n; p)}.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Define $E_{p-1} = \{e_1, \cdots, e_{p-1}\}$ by

$$e_n = \begin{cases} +1, & \text{if } S(1,n;p) > 0, \\ -1, & \text{if } S(1,n;p) < 0. \end{cases}$$

E. Fouvry (with coauthors) [J. Aust. Math. Soc. 2004] showed that

$$W(E_{p-1}) \ll p^{3/4}(\log p)^{1/2} \quad \text{and} \quad C_l(E_{p-1}) \ll p^{\frac{2l+1}{2l+2}} (\log p)^{\frac{1}{l+1}} .$$

This shows that the signs of $K(1,n;p)$ form a "good" pseudorandom binary sequence.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

3.5. $\left\{(-1)^{\overline{n}+\overline{n+x}}\right\}$

✠ Let p be an odd prime. For each integer a with $t < a \leq t+u$ and $(a,p) = 1$, there exists one and only one $\overline{a}$ such that $0 < \overline{a} < p$ and $a\overline{a} \equiv 1 (\mathrm{mod} p)$. Let $r(p,u,t)$ be the number of cases in which a and $\overline{a}$ are of opposite parity, that is

$$r(p,u,t) = \sum_{\substack{t<a\leq t+u \\ (a,p)=1 \\ 2\nmid a+\overline{a}}} 1.$$

Define

$$E(p,u,t) = r(p,u,t) - \frac{1}{2} \sum_{\substack{t<a\leq t+u \\ (a,p)=1}} 1 \quad \text{and} \quad S(p,u) = \sum_{t=1}^{p} |E(p,u,t)|^2 .$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ W. Zhang [Acta Math. Hungar., 1998] showed that

$$S(p,u) = \frac{1}{4}up + O\left(u^2\sqrt{p}\log^2 p\right)$$

by proving the estimate

$$\sum_{\substack{n=1\\ p\nmid n+x}}^{p-1} (-1)^{\overline{n}+\overline{n+x}} \ll \sqrt{p}\log^2 p.$$

Therefore it is natural to expect that the sequence $\left\{(-1)^{\overline{n}+\overline{n+x}}\right\}$ behaves like a random sequence of $\pm$ signs.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Let p be an odd prime, and let x be an integer with $1 \le x \le p-1$. Define

$$e_n = \begin{cases} (-1)^{\overline{n}+\overline{n+x}}, & \text{if } p \nmid n \text{ and } p \nmid n+x, \\ 1, & \text{otherwise.} \end{cases}$$

Huaning Liu [Acta Arith., 2006] proved that

$$W\left(E_{p-1}\right) \ll p^{\frac{1}{2}} \log^3 p; \quad C_2\left(E_{p-1}\right) \ll p^{\frac{1}{2}} \log^5 p; \quad Q_2\left(E_{p-1}\right) \ll p^{\frac{1}{2}} \log^5 p.$$

✠ Later, he [Acta Arith., accepted for publication] showed that

$$C_k\left(E_{p-1}\right) \ll k p^{1/2} \left(\log p\right)^{2k+1}, \quad Q_k\left(E_{p-1}\right) \ll k p^{1/2} \left(\log p\right)^{2k+1}.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

3.6. $\left\{(-1)^{n+\overline{n}}\right\}$

✠ Let p be an odd prime number. For $n \in \{1, \cdots, p-1\}$ we denote the inverse of n modulo p by $\overline{n}$ with $\overline{n} \in \{1, \cdots, p-1\}$. Fix $\overline{0} = 0$ by convention. Let $N(p)$ be the number of cases in which n and $\overline{n}$ are of opposite parity, that is

$$N(p) = \sum_{\substack{n=1 \\ 2 \nmid n+\overline{n}}}^{p-1} 1.$$

In the book "Unsolved problems in number theory", D. H. Lehmer asked us to say something nontrivial about $N(p)$.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ W. Zhang [Compositio Mathematica, 1993] showed that

$$N(p) = \frac{1}{2}p + O\left(p^{1/2}\log^2 p\right)$$

by proving the estimate

$$\left|\sum_{n=1}^{p-1}(-1)^{n+\overline{n}}\right| \ll p^{1/2}\log^2 p.$$

✠ Let $f(x) \in \mathbb{F}_p[x]$ of degree d with $1 \le d < p$, and let s be its number of distinct roots in $\overline{\mathbb{F}}_p[x]$. Define

$$e_n = \begin{cases} +1, & \text{if } \overline{f(n)} \equiv R_p(f(n)) (\mathrm{mod} 2), \\ -1, & \text{if } \overline{f(n)} \not\equiv R_p(f(n)) (\mathrm{mod} 2), \end{cases}$$

and $E_p = (e_1, \cdots, e_p)$, where $R_p(x)$ denotes the unique $r \in \{0, 1, \cdots, p-1\}$ with $x \equiv r (\mathrm{mod} p)$. S. R. Louboutin et al [Proc. Amer. Math. Soc., 2007] proved that

$$W(E_p) \ll (d+s)p^{1/2}\log^3 p, \qquad C_2(E_p) \ll (d+s)p^{1/2}\log^5 p.$$

This shows that $\{e_n\}$ is a "good" pseudorandom binary sequence.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Furthermore, let $E_{p-1} = \{e_1, \cdots, e_{p-1}\}$ be defined by

$$e_n = \begin{cases} (-1)^{n+\overline{n}}, & \text{if } n \text{ is a quadratic residue mod } p; \\ (-1)^{n+\overline{n}+1}, & \text{if } n \text{ is a quadratic nonresidue mod } p, \end{cases}$$
$$= (-1)^{n+\overline{n}} \left(\frac{n}{p}\right).$$

Huaning Liu [Proc. Amer. Math. Soc., 2007] proved that

$$W(E_{p-1}) \ll p^{\frac{1}{2}} \log^2 p;$$
$$C_2(E_{p-1}) \ll p^{\frac{1}{2}} \log^3 p;$$
$$Q_2(E_{p-1}) \ll p^{\frac{1}{2}} \log^3 p.$$

This showed the sequence $\{e_n\}$ is a "good" pseudorandom sequence.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

4 Large families of pseudorandom binary sequences

✠ However, the above constructions produce only a “few” good sequences while in certain applications (e.g., in cryptography) one needs “large” families of “good” pseudorandom binary sequence. Therefore some “large” families of pseudorandom binary sequences were introduced as following.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Let p be an odd prime, and define $E_p = \{e_1, \cdots, e_p\}$ by

$$e_n = \begin{cases} +1, & \text{if } 0 \le R_p(f(n)) < p/2, \\ -1, & \text{if } p/2 \le R_p(f(n)) < p, \end{cases}$$

where $R_p(n)$ denotes the unique $r \in \{0, \cdots, p-1\}$ with $n \equiv r \bmod p$. Then for $f \in \mathbb{F}_p[x]$ of degree d and $2 \le l \le d-1$, C. Mauduit, J. Rivat and A. Sárközy [Monatsh. Math., 2004] showed that

$$W(E_p) \ll dp^{1/2} (\log p)^2, \qquad C_l(E_p) \ll dp^{1/2} (\log p)^{l+1}.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ If p is a prime, $f(x) \in \mathbb{F}_p[x]$ has degree $k(>0)$ and no multiple zero in $\overline{\mathbb{F}}_p$, and the binary sequence $E_p = \{e_1, \cdots, e_p\}$ is defined by

$$e_n = \begin{cases} \left(\dfrac{f(n)}{p}\right), & \text{for } (f(n), p) = 1, \\ +1, & \text{for } p \mid f(n). \end{cases}$$

L. Goubin, C. Mauduit and A. Sárközy [J. Number Theory, 2004] proved that $W(E_p) < 10kp^{1/2} \log p$.

Moreover, assume that for $l \in \mathbb{N}$ one of the following assumptions holds:

(i) $l = 2$; (ii) $l < p$, and 2 is a primitive rood modulo p; (iii) $(4k)^l < p$.

Then we also have $C_l(E_p) < 10klp^{1/2} \log p$.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Let $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree k, and define $E_{p-1} = \{e_1, \cdots, e_{p-1}\}$ by

$$e_n = \begin{cases} +1, & \textit{if } 1 \leq \mathrm{ind} f(n) \leq (p-1)/2, \\ -1, & \textit{if } (p+1)/2 \leq \mathrm{ind} f(n) \leq p-1 \textit{ or } p \mid f(n). \end{cases}$$

K. Gyarmati [Period. Math. Hungar., 2004] proved that $W(E_{p-1}) < 38kp^{1/2}(\log p)^2$.

Moreover, suppose that at least one of the following assumptions holds: (i) f is irreducible; (ii) If f has the factorization $f = \varphi_1^{\alpha_1}\varphi_2^{\alpha_2}\cdots\varphi_u^{\alpha_u}$ where $\alpha_i \in \mathbb{N}$ and φ_i is irreducible over $\mathbb{F}_p$, then there exists one β such that exactly one or two $\varphi_i's$ have the degree β; (iii) $l = 2$; (iv) $(4l)^k < p$ or $(4k)^l < p$. Then $C_l(E_{p-1}) < 10kl4^l p^{1/2}(\log p)^{l+1}$.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Assume that p is a prime, $f(x) \in \mathbb{F}_p[x]$ has degree $(0 <)k(< p)$ and no multiple zero in $\overline{\mathbb{F}}_p$. Define the binary sequence $E_p = \{e_1, \cdots, e_p\}$ by

$$e_n = \begin{cases} +1, & \text{if } (f(n), p) = 1, \quad R_p(\overline{f(n)}) < p/2, \\ -1, & \text{if either } (f(n), p) = 1, \quad R_p(\overline{f(n)}) > p/2 \text{ or } p \mid f(n). \end{cases}$$

C. Mauduit and A. Sárközy [Acta Math. Hungar., 2005] showed that $W(E_p) \ll kp^{1/2}(\log p)^2$.

Moreover, assume also that $l \in \mathbb{N}$ with $2 \le l \le p$, and one of the following conditions holds: (i) $l = 2$; (ii) $(4k)^l < p$. Then we also have $C_l(E_p) \ll klp^{1/2}(\log p)^{l+1}$.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Furthermore, let p be an odd prime, $f(x) \in \mathbb{F}_p[x]$ has degree $(0 <)d(< p)$ and no multiple zero in $\overline{\mathbb{F}_p}$. Let $E_{p-1} = \{e_1, \cdots, e_{p-1}\}$ be defined by

$$e_n = \begin{cases} (-1)^{\overline{f(n)}+\overline{f(n+x)}}, & \text{if } p \nmid f(n) \text{ and } p \nmid f(n+x), \\ 1, & \text{otherwise}, \end{cases}$$

Assume that $k \in \mathbb{N}$ with $2 \le k \le p$, and one of the following conditions holds:

$$(i) \quad k = 2; \qquad (ii) \quad (4d)^k < p.$$

Huaning Liu [Acta Arith., accepted for publication] showed that

$$\begin{aligned} W(E_{p-1}) &\ll dp^{1/2}(\log p)^3, \\ C_k(E_{p-1}) &\ll kdp^{1/2}(\log p)^{2k+1}, \\ Q_k(E_{p-1}) &\ll kdp^{1/2}(\log p)^{2k+1}. \end{aligned}$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Assume that p is an odd prime, and $f(x) \in \mathbb{F}_p[x]$. Let $E'_{p-1} = \{e'_1, \cdots, e'_{p-1}\}$ be defined by $e'_n = (-1)^{R_p(f(n))+\overline{n}}$, and let $E''_{p-1} = \{e''_1, \cdots, e''_{p-1}\}$ be defined by

$$e''_n = \begin{cases} +1, & \text{if } 0 \le R_p(f(n)+\overline{n}) < p/2, \\ -1, & \text{if } p/2 \le R_p(f(n)+\overline{n}) < p. \end{cases}$$

Huaning Liu proved that [submitted]

$$\begin{aligned} W\left(E'_{p-1}\right) &\ll (\deg(f)+1)\, p^{1/2} (\log p)^3, \\ Q_l\left(E'_{p-1}\right) &\ll (\deg(f)+l)\, p^{1/2} (\log p)^{2l+1}, \\ C_l\left(E'_{p-1}\right) &\ll (\deg(f)+l)\, p^{1/2} (\log p)^{2l+1}. \end{aligned}$$

and

$$\begin{aligned} W\left(E''_{p-1}\right) &\ll (\deg(f)+1)\, p^{1/2} (\log p)^2, \\ Q_l\left(E''_{p-1}\right) &\ll (\deg(f)+l)\, p^{1/2} (\log p)^{l+1}, \\ C_l\left(E''_{p-1}\right) &\ll (\deg(f)+l)\, p^{1/2} (\log p)^{l+1}. \end{aligned}$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

5 Gowers norm of pseudorandom binary sequences

5.1. Introduction to the Gowers norm

✠ The famous Szemerédi's theorem asserts that any set of integers of positive upper density contains arbitrarily long arithmetic progressions.

✠ E. Szemerédi [Acta Math. Acad. Sci. Hungar., 1969; Acta Arith., 1975] used combinatorial methods to give the first full proof of this theorem.

✠ Later, H. Furstenberg [J. Analyse Math., 1977; Bull. Amer. Math. Soc. (N.S.), 1982] introduced an ergodic theoretic proof of this theorem.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ W. T. Gowers [Geom. Funct. Anal., 2001] gave a proof which was both combinatorial and Fourier-analytic in nature.

✠ Meanwhile, there were a few other proofs of this theorem by other methods.

✠ Recently, B. Green and T. Tao applied the infinitary version of Szemerédi's theorem to demonstrate that primes contain arbitrarily long arithmetic progressions.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ In [Geom. Funct. Anal., 2001] W. T. Gowers introduced the Gowers uniformity norms $||f||_{U^d}$ for any complex function $f : G \to \mathbb{C}$. Roughly speaking, if a function has small uniformity norm, we would like to deduce that it is "pseudorandom".

✠ W. T. Gowers [Geom. Funct. Anal., 2001] proved that if $A \subseteq \mathbb{Z}_N$ is a subset of density δ, $f : \mathbb{Z}_N \to [-1, 1]$ is a normalized version of the characteristic function, and $||f||_{U^d}$ is sufficiently small, then A must contain arithmetic progressions of length $d + 1$.

✠ Furthermore, B. Green and T. Tao studied functions $f : G \to \mathbb{C}$ with large $||f||_{U^3}$.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ In [Geom. Funct. Anal., 2001] W. T. Gowers remarked that "$\cdots$ I still feel that it would be interesting to investigate the norms further $\cdots$". B. Green and T. Tao also said that "$\cdots$ it thus seems of interest to study these norms more systematically $\cdots$".

✠ Now we shall study the Gowers uniformity norm for pseudorandom binary sequences, and obtain some results.

✠ Here we give the definition of the Gowers norm as following:

♣ Let $d \geq 1$ be a dimension, and let $f : \mathbb{Z}_N \to \{-1, +1\}$ be a function. Then the Gowers uniformity norm $||f||_{U^d}$ is defined by the formula

$$||f||_{U^d} := \left(\mathbb{E}_{x, x_1, \cdots, x_d} \left(\prod_{S \subseteq [d]} f \left(x + \sum_{i \in S} x_i \right) \right) \right)^{1/2^d}.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

5.2. Connection between Gowers norm and correlation measure

✠ Huaning Liu [submitted] established some connection between Gowers norm and correlation measure of pseudorandom binary sequences as following:

Theorem 5.2.1 Let $f : \mathbb{Z}_N \to \{-1, +1\}$, and define

$$V_d(f) := \max_D \left| \sum_{n=1}^{N} f(n+d_1) f(n+d_2) \cdots f(n+d_k) \right|,$$

where $D = (d_1, d_2, \cdots, d_k)$ with $0 \le d_1 < d_2 < \cdots < d_k < N$ and $1 \le k \le 2^d$. Then we have

$$||f||_{U^d} \le \left(\frac{V_d(f)}{N} + \frac{1}{N^d} \right)^{1/2^d}.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

♠ Remarks:

✠ Noting that the definition of $V_d(f)$ is similar to that of correlation measure of order k:

$$\clubsuit \quad V_d(f) := \max_D \left| \sum_{n=1}^{N} f(n+d_1) f(n+d_2) \cdots f(n+d_k) \right|,$$

$$\clubsuit \; C_k\left(E_N\right) := \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_k} \right|, \; 0 \le d_1 < \cdots < d_k \le N-M.$$

This suggests that the "good" pseudorandom binary sequences may have small Gowers norm.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

5.3. Examples [submitted]

Theorem 5.3.1 Assume that p is an odd prime, $f(x) \in \mathbb{F}_p[x]$ has degree $k(>0)$, $f(x)$ has no multiple zero in $\overline{\mathbb{F}}_p$. Let $f_1 : \mathbb{Z}_p \to \{-1, +1\}$ be defined by

$$f_1(n) = \begin{cases} \left(\dfrac{f(n)}{p}\right) & \text{for} \quad (f(n), p) = 1, \\ +1 & \text{for} \quad p \mid f(n). \end{cases}$$

Moreover, assume that one of the following assumptions holds:

(i) $d = 1$; (ii) $2^d < p$, and 2 is a primitive root modulo p; (iii) $(4k)^{2^d} < p$.

Then we have

$$||f_1||_{U^d} \leq \left(\frac{2^d k(p^{1/2}+1)}{p} + \frac{1}{p^d}\right)^{1/2^d}.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ L. Goubin, C. Mauduit and A. Sárközy [J. Number Theory, 2004]:

Lemma 5.3.1. Let p be an odd prime, and let $f(x) \in \mathbb{F}_p[x]$ has degree $k(>0)$, $f(x)$ has no multiple zero in $\overline{\mathbb{F}}_p$. Assume that one of the following assumptions holds:

(i) $l = 2$; (ii) $l < p$, and 2 is a primitive root modulo p; (iii) $(4k)^l < p$. Write $f(x) = bg(x)$ with $b \in \mathbb{Z}_p$ and $g(x)$ is a unitary polynomial. Then the polynomial $h(x) := g(x+d_1)g(x+d_2)\cdots g(x+d_l)$, where $d_1, d_2 \cdots, d_l$ are integers with $0 \le d_1 < d_2 < \cdots < d_l < p$, has at least one zero in $\overline{\mathbb{F}}_p$ whose multiplicity is odd.

✠ C. Mauduit and A. Sárközy [Acta Arith, 1997]:

Lemma 5.3.2. Suppose that p is a prime number, χ is a non-principal character modulo p of order d, $f(x) \in \mathbb{F}_p[x]$ has degree k and a factorization $f(x) = b(x-x_1)^{d_1}\cdots(x-x_s)^{d_s}$ (where $x_i \neq x_j$ for $i \neq j$) in $\overline{\mathbb{F}}_p$ with $(d, d_1, \cdots, d_s) = 1$. Then we have

$$\left|\sum_{x\in\mathbb{F}_p} \chi\left(f(x)\right)\right| \le kp^{1/2}.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

Proof of Theorem 5.3.1

Write $f(x) = bg(x)$ with $b \in \mathbb{Z}_p$ and $g(x)$ is a unitary polynomial. Writing $\left(\frac{0}{p}\right) = 0$. For $2 \le l \le 2^d$ and $0 \le d_1 < d_2 < \cdots < d_l < p$, by the definition

$$f_1(n) = \begin{cases} \left(\frac{f(n)}{p}\right) & \text{for} \quad (f(n), p) = 1, \\ +1 & \text{for} \quad p \mid f(n). \end{cases}$$

we have

$$\begin{aligned} &\sum_{n=1}^{p} f_1(n+d_1) \cdots f_1(n+d_l) \\ &\le \left| \sum_{n=1}^{p} \left(\frac{f(n+d_1)}{p}\right) \cdots \left(\frac{f(n+d_l)}{p}\right) \right| + kl \\ &= \left| \left(\frac{b^l}{p}\right) \sum_{n=1}^{p} \left(\frac{g(n+d_1) \cdots g(n+d_l)}{p}\right) \right| + kl. \end{aligned}$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ By Lemma 5.3.1 we know that $g(n+d_1)\cdots g(n+d_l)$ has at least one zero in $\overline{\mathbb{F}}_p$ whose multiplicity is odd. Then from Lemma 5.3.2 we have

$$\sum_{n=1}^{p} f_1(n+d_1)\cdots f_1(n+d_l) \leq klp^{1/2}+kl = kl(p^{1/2}+1).$$

Therefore $V_d(f_1) \leq 2^d k\left(p^{1/2}+1\right)$. Then from Theorem 5.2.1 we have

$$||f_1||_{U^d} \leq \left(\frac{V_d(f_1)}{N}+\frac{1}{N^d}\right)^{1/2^d} \leq \left(\frac{2^d k(p^{1/2}+1)}{p}+\frac{1}{p^d}\right)^{1/2^d}.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

Theorem 5.3.2 Assume that p is an odd prime, $f(x) \in \mathbb{F}_p[x]$ has degree $k(1 < k < p)$ and no multiple zero in $\overline{\mathbb{F}}_p$. Let $f_2 : \mathbb{Z}_p \to \{-1, +1\}$ be defined by

$$f_2(n) = \begin{cases} +1, & \text{if} \quad (f(n), p) = 1, R_p(\overline{f(n)}) < p/2, \\ -1, & \text{if either} \quad (f(n), p) = 1, R_p(\overline{f(n)}) \geq p/2 \quad \text{or} \quad p \mid f(n). \end{cases}$$

Moreover assume that one of the following assumptions holds:

$$\text{(i) } d = 1; \quad \text{(ii) } (4k)^{2^d} < p.$$

Then we have

$$||f_2||_{U^d} \ll \left(2^d k p^{-1/2}\right)^{1/2^d} \log p.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ C. Mauduit, J. Rivat and A. Sárközy [Monatsh. Math., 2004]:

Lemma 5.3.3. For $n \in \mathbb{Z}$ and p an odd prime, we have

$$\frac{1}{p}\sum_{|a|<p/2} v_p(a)\mathrm{e}\left(\frac{an}{p}\right) = \begin{cases} +1, & \text{if } R_p(n) < \frac{p}{2}, \\ -1, & \textit{otherwise}, \end{cases}$$

where $v_p(a)$ is a function of period p such that $v_p(0) = 1$, and

$$v_p(a) = \begin{cases} O(1), & \text{if } a \text{ is even}, \\ -\frac{2ip}{\pi a} + O(1), & \text{if } a \text{ is odd}. \end{cases}$$

✠ C. Mauduit and A. Sárközy [Acta Math. Hungar., 2005]

Lemma 5.3.4. Let p be an odd prime, and let $f(x) \in \mathbb{F}_p[x]$ has degree $k(1 < k < p)$ and no multiple zero in $\overline{\mathbb{F}}_p$. Assume that $l \in \mathbb{N}$, and one of the following conditions holds: (i) $l = 2$; (ii) $(4k)^l < p$.

For $r \le l$, $0 \le d_{i_1} < \cdots < d_{i_r} < p$ and $h_{i_j} \neq 0$, $j = 1, \cdots, r$, define

$$Q(x) := \sum_{t=1}^{r} h_{i_t} \prod_{\substack{1\le j\le r \\ j\neq t}} f(x + d_{i_j}).$$

Then $Q(x)$ is not the 0 polynomial on $\mathbb{F}_p$.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ C. J. Moreno and O. Moreno [Proc. Amer. Math. Soc., 1991]:

Lemma 5.3.5. For any polynomials $g(x)$, $h(x) \in \mathbb{F}_p[x]$ such that the rational function $f(x) = g(x)/h(x)$ is not constant on $\mathbb{F}_p$, let s be the number of distinct roots of the polynomial $h(x)$, then we have

$$\left| \sum_{\substack{n \in \mathbb{F}_p \\ h(n) \neq 0}} \mathrm{e}\left(\frac{g(n)}{h(n)p} \right) \right| \leq \left(\max\left(\deg(g), \deg(h) \right) + s - 1 \right) \sqrt{p}.$$

Proof of Theorem 5.3.2

For $2 \le l \le 2^d$ and $0 \le d_1 < d_2 < \cdots < d_l < p$, by Lemma 5.3.3 we have

$$\sum_{n=1}^{p} f_2(n+d_1)\cdots f_2(n+d_l)$$

$$= \frac{1}{p^l} \sum_{\substack{n=1 \\ p\nmid f(n+d_1)\cdots f(n+d_l)}}^{p} \sum_{|h_1|<p/2} v_p(h_1)\mathrm{e}\left(\frac{h_1\overline{f(n+d_1)}}{p}\right)\cdots$$

$$\times \sum_{|h_l|<p/2} v_p(h_l)\mathrm{e}\left(\frac{h_l\overline{f(n+d_l)}}{p}\right) + O(kl)$$

$$= \frac{1}{p^l} \sum_{\substack{|h_1|<p/2 \\ (h_1,\cdots,h_l)\neq(0,\cdots,0)}} \cdots \sum_{|h_l|<p/2} v_p(h_1)\cdots v_p(h_l)$$

$$\times \sum_{\substack{n=1 \\ p\nmid f(n+d_1)\cdots f(n+d_l)}}^{p} \mathrm{e}\left(\frac{h_1\overline{f(n+d_1)}+\cdots+h_l\overline{f(n+d_l)}}{p}\right) + O(kl).$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

Since $(h_1, \cdots, h_l) \neq (0, \cdots, 0)$, we have some $0 \leq d_{i_1} < \cdots < d_{i_r} < p$ with $h_{i_j} \neq 0, j = 1, \cdots, r$, satisfying

$$\sum_{\substack{n=1 \\ p \nmid f(n+d_1)\cdots f(n+d_l)}}^{p} \mathrm{e}\left(\frac{h_1\overline{f(n+d_1)} + \cdots + h_l\overline{f(n+d_l)}}{p}\right)$$

$$= \sum_{\substack{n=1 \\ p \nmid f(n+d_{i_1})\cdots f(n+d_{i_r})}}^{p} \mathrm{e}\left(\frac{h_{i_1}\overline{f(n+d_{i_1})} + \cdots + h_{i_r}\overline{f(n+d_{i_r})}}{p}\right) + O(kl)$$

$$:= \sum_{\substack{n=1 \\ R(n)\neq 0}}^{p} \mathrm{e}\left(\frac{Q(n)}{R(n)p}\right) + O(kl),$$

where

$$Q(n) = \sum_{t=1}^{r} h_{i_t} \prod_{\substack{1\leq j\leq r \\ j\neq t}} f(n+d_{i_j}) \qquad \text{and} \qquad R(n) = \prod_{j=1}^{r} f(n+d_{i_j}).$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

By Lemma 5.3.4 we know that $Q(n)$ is not the 0 polynomial on $\mathbb{F}_p$. Therefore $Q(n)/R(n)$ is not constant on $\mathbb{F}_p$. Then by Lemma 5.3.5 we have

$$\sum_{\substack{n=1 \\ p\nmid f(n+d_1)\cdots f(n+d_l)}}^{p} \mathrm{e}\left(\frac{h_1\overline{f(n+d_1)}+\cdots+h_l\overline{f(n+d_l)}}{p}\right) \ll klp^{1/2}.$$

So from Lemma 5.3.3 we get

$$\begin{aligned}\sum_{n=1}^{p} f_2(n+d_1)\cdots f_2(n+d_l) &\ll \frac{1}{p^l}\sum_{\substack{|h_1|<p/2 \\ (h_1,\cdots,h_l)\neq(0,\cdots,0)}}\cdots\sum_{|h_l|<p/2}|v_p(h_1)|\cdots|v_p(h_l)|\,klp^{1/2} \\ &\ll klp^{1/2}(\log p)^l.\end{aligned}$$

Therefore $V_d(f_2) \ll 2^d kp^{1/2}(\log p)^{2^d}$. Then from Theorem 5.2.1 we have

$$||f_2||_{U^d} \leq \left(\frac{V_d(f_2)}{N}+\frac{1}{N^d}\right)^{1/2^d} \ll \left(2^d kp^{-1/2}\right)^{1/2^d}\log p.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

Theorem 5.3.3 Let p be an odd prime number, $f(x) \in \mathbb{F}_p[x]$ of degree k. Let $f_3 : \mathbb{Z}_p \to \{-1, +1\}$ be defined by

$$f_3(n) = \begin{cases} +1, & \text{if} \quad 0 \leq R_p(f(n)) < p/2, \\ -1, & \text{if} \quad p/2 \leq R_p(f(n)) < p. \end{cases}$$

For $2 \leq 2^d \leq k - 1$, we have

$$||f_3||_{U^d} \ll \left(kp^{-1/2}\right)^{1/2^d} \log p.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Recall

Lemma 5.3.3. For $n \in \mathbb{Z}$ and p an odd prime, we have

$$\frac{1}{p}\sum_{|a|<p/2} v_p(a)\mathrm{e}\left(\frac{an}{p}\right) = \begin{cases} +1, & \text{if } R_p(n) < \frac{p}{2}, \\ -1, & \textit{otherwise}, \end{cases}$$

where $v_p(a)$ is a function of period p such that $v_p(0) = 1$, and

$$v_p(a) = \begin{cases} O(1), & \text{if } a \text{ is even}, \\ -\frac{2ip}{\pi a} + O(1), & \text{if } a \text{ is odd}. \end{cases}$$

Lemma 5.3.5. For any polynomials $g(x)$, $h(x) \in \mathbb{F}_p[x]$ such that the rational function $f(x) = g(x)/h(x)$ is not constant on $\mathbb{F}_p$, let s be the number of distinct roots of the polynomial $h(x)$, then we have

$$\left|\sum_{\substack{n\in\mathbb{F}_p \\ h(n)\neq 0}} \mathrm{e}\left(\frac{g(n)}{h(n)p}\right)\right| \leq (\max(\deg(g), \deg(h)) + s - 1)\sqrt{p}.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ C. Mauduit, J. Rivat and A. Sárközy [Monatsh. Math., 2004]:

Lemma 5.3.6. Let p be a prime, $1 \leq l < p$, $f(x) \in \mathbb{F}_p[x]$ of degree $k \geq l$, and let $x_1, \cdots, x_l$ be l different elements of $\mathbb{F}_p$. Then for all $(a_1, \cdots, a_l) \in \mathbb{F}_p^l \backslash (0, \cdots, 0)$, the polynomial

$$G(x) := a_1 f(x + x_1) + \cdots + a_l f(x + x_l)$$

is of degree $\geq k - l + 1$.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

Proof of Theorem 5.3.3

For $2 \le l \le 2^d$ and $0 \le d_1 < d_2 < \cdots < d_l < p$, by Lemma 5.3.3 we have

$$\begin{aligned}
&\sum_{n=1}^{p} f_3(n+d_1)\cdots f_3(n+d_l) \\
&= \frac{1}{p^l} \sum_{|h_1|<p/2} \cdots \sum_{|h_l|<p/2} v_p(h_1)\cdots v_p(h_l) \\
&\qquad \times \sum_{n=1}^{p} \mathrm{e}\left(\frac{h_1 f(n+d_1)+\cdots+h_l f(n+d_l)}{p}\right) \\
&= \frac{1}{p^l} \sum_{\substack{|h_1|<p/2 \\ (h_1,\cdots,h_l)\neq(0,\cdots,0)}} \cdots \sum_{|h_l|<p/2} v_p(h_1)\cdots v_p(h_l) \\
&\qquad \times \sum_{n=1}^{p} \mathrm{e}\left(\frac{h_1 f(n+d_1)+\cdots+h_l f(n+d_l)}{p}\right) + O(1).
\end{aligned}$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

From Lemma 5.3.6 we know that the polynomial

$$h_1 f(n+d_1) + \cdots + h_l f(n+d_l)$$

is of degree ≥ 1, provided that $l \leq k$ and $(h_1, \cdots, h_l) \neq (0, \cdots, 0)$. Then from Lemma 5.3.5 and Lemma 5.3.3 we have

$$\sum_{n=1}^{p} f_3(n+d_1) \cdots f_3(n+d_l) \ll \frac{1}{p^l} \left(\sum_{|h|<p/2} |v_p(h)| \right)^l kp^{1/2} \ll kp^{1/2} (\log p)^l.$$

Therefore $V_d(f_3) \ll kp^{1/2} (\log p)^{2^d}$. So from Theorem 5.2.1 we have

$$||f_3||_{U^d} \leq \left(\frac{V_d(f_3)}{N} + \frac{1}{N^d} \right)^{1/2^d} \ll \left(kp^{-1/2} \right)^{1/2^d} \log p.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

✠ Assume that p is an odd prime, and $f(x) \in \mathbb{F}_p[x]$. Let $f_4 : \mathbb{Z}_p \to \{-1, +1\}$ be defined by

$$f_4(n) = \begin{cases} (-1)^{R_p(f(n))+\overline{n}}, & \text{if} \quad p \nmid n, \\ +1, & \text{if} \quad p \mid n, \end{cases}$$

and let $f_5 : \mathbb{Z}_p \to \{-1, +1\}$ be defined by

$$f_5(n) = \begin{cases} +1, & \text{if either} \quad p \nmid n, 0 \leq R_p(f(n) + \overline{n}) < p/2, \quad \text{or} \quad p \mid n, \\ -1, & \text{if} \quad p \nmid n, p/2 \leq R_p(f(n) + \overline{n}) < p. \end{cases}$$

Then we have

$$||f_4||_{U^d} \ll \left((\deg(f) + 2^d)p^{-1/2}(\log p)^{2^d+1}\right)^{1/2^d}$$

and

$$||f_5||_{U^d} \ll \left((\deg(f) + 2^d)p^{-1/2}\right)^{1/2^d} \log p.$$

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

Final Remarks

✠ 研究真正的随机数列上的Gowers 范数的上下界估计应该是有意义的, 但是很困难.

✠ 此外, 根据伪随机数列的Gowers 范数, 研究其对于数论问题的应用和意义, 或许是有意思的.

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .

Thank you!

Huaning Liu (刘华宁)

Department of Mathematics, Northwest University

Xi'an, Shaanxi, P. R. China

E-mail: hnliumath@hotmail.com

Introduction to . . .
Pseudorandom . . .
Examples of the . . .
Large families of . . .
Gowers norm of . . .