Westfälische Wilhelms-Universität Münster
Mathematisches Institut

PD Dr. Karin Halupczok

Der Satz von Green-Tao

2-std. Vorlesung im Wintersemester 2010/11

Inhaltsverzeichnis

1 Einführung

Wir betrachten endliche arithmetische Progressionen wie z.B. $5, 8, 11, 14, 17$.

Definition 1. *Eine arithmetische Progression (AP) der Länge $k \in \mathbb{N}$ ist eine Menge $Q \subseteq \mathbb{Z}$ der Form*

$$Q = \{a, a+q, a+2q, a+3q, \ldots, a+(k-1)q\}$$

mit Startwert $a \in \mathbb{Z}$ und Differenz $q \in \mathbb{N}$.

Sei $\mathbb{P} \subseteq \mathbb{Z}$ die Menge der (positiven) Primzahlen.

Beispiele für APs aus Primzahlen:

(1) $5, 11, 17, 23, 29$

(2) $\{199 + 210n;\ 0 \leq n \leq 9\} = \{199, 409, \ldots, 2089\}$

(3) ein Rekord von M. Frind 2003: $\{376859931192959+18549279769020k;\ k = 0, 1, \ldots, 21\}$ (mittlerweile kennt man auch APs der Länge 23)

Problem: Gibt es für jedes $k \in \mathbb{N}$ eine AP der Länge k aus Primzahlen?

Sei $\pi(N) := |\{p \in \mathbb{P};\ p \leq N\}|$ die Primzahlzählfunktion.

Wegen dem Primzahlsatz $\pi(N) \sim \frac{N}{\log N}$ nahm man an, daß ca. $\frac{N^2}{\log^k N}$ viele APs der Länge k in $\{p \in \mathbb{P};\ p \leq N\}$ existieren müßten. (Aus der k-Tupel-Vermutung von Hardy und Littlewood 1923)

Gelöst wurde das Problem erst 2004 von Ben Green und Terence Tao:

Satz 1. *(Satz von Green-Tao) $\mathbb{P}$ enthält APs der Länge k für jedes $k \in \mathbb{N}$, noch schärfer: Sei $A \subseteq \mathbb{P}$ gegeben mit $\limsup_{N\to\infty} \frac{|A\cap[1,N]|}{\pi(N)} > 0$. Dann enthält A (unendlich viele!) APs der Länge k für jedes $k \in \mathbb{N}$.*

Für $k = 1$ gilt die Aussage von Satz 1 mit $A = \mathbb{P}$ trivialerweise, da $|\mathbb{P}| = \infty$, ebenso für $k = 2$, da es unendlich viele Primzahlpaare gibt, die eine AP der Länge 2 definieren.

Für $k = 3$ wurde die Aussage 1939 von van der Corput bewiesen: es existieren unendlich viele Tripel aus Primzahlen, die eine AP bilden.

Für $k = 4$ war die Aussage vor 2004 unbekannt, die beste Annäherung war die von Heath-Brown aus dem Jahr 1981, der zeigte: Es existieren unendlich viele Quadrupel aus 3 Primzahlen und einer P_2-Zahl (eine sogenannte Fast-Primzahl, das ist eine natürliche Zahl, die aus maximal 2 Primfaktoren besteht), die eine AP bilden.

Bemerkung 1. Der Beweis des Satzes von Green-Tao ist nicht konstruktiv. Aber er zeigt: Es gibt eine AP der Länge k mit Einträgen unterhalb von

$$2^{2^{2^{2^{2^{2^{2^{(100k)}}}}}}}$$

Diese Schranke ist längst nicht optimal; man vermutet, daß diese eher die Größenordnung $k! + 1$ haben müßte.

Bemerkung 2. Der Beweis ist ein Mix aus Zahlentheorie, Ergodentheorie (einem Teilgebiet der Stochastik), harmonische Analysis, diskrete Geometrie, Kombinatorik.

2 Beweisübersicht

Ausgangspunkt ist der Satz von Szemerédi: Satz 1 gilt mit $\mathbb{Z}$ statt $\mathbb{P}$, d. h.:

Satz 2. *(Szemerédi) Sei $N \in \mathbb{N}$, $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$. Sei $\delta > 0$ reell, und sei $k \geq 3$ ganzzahlig. Dann existiert ein (minimales) $N_0(\delta, k)$ mit folgender Eigenschaft: Ist $N \geq N_0(\delta, k)$, $A \subseteq \mathbb{Z}_N$, $|A| > \delta N$, so enthält A eine AP der Länge k.*

Die limsup-Bedingung von oben wurde hier ausformuliert.

Verschiedene Beweise von Satz 2 sind bekannt:

- Szemerédi 1969/75: kombinatorisch
- Furstenberg 1977: ergodentheoretisch
- Gowers 1998/2001: mit harmonischer Analysis

Bemerkung 1. Satz 2 kann nicht für $A = \mathbb{P}$ angewendet werden, da

$$\frac{|\mathbb{P} \cap [1, N]|}{N} = \frac{\pi(N)}{N} \ll \frac{1}{\log N} \longrightarrow_{N \to \infty} 0.$$

Die Strategie von Green-Tao ist nun: finde eine Version von Satz 2, mit der dieses Problem umgangen werden kann. Ausgangspunkt dafür war eine ergodische Umformulierung, dafür zunächst noch die folgende Notation.

Notation. Sei $A \subseteq \mathbb{Z}$ endlich, $f : A \to \mathbb{C}$ eine Funktion. Dann ist

$$\mathbb{E}(f) = \mathbb{E}(f(x) \mid x \in A) := \frac{1}{|A|} \sum_{x \in A} f(x)$$

der Mittelwert bzw. der Erwartungswert von f. Wir schreiben

$$\mathbb{E}(f(x) \mid P(x)) := \frac{\sum_{x \in A, P(x)} f(x)}{|\{x \in A, P(x)\}|}$$

für den Mittelwert der $f(x)$ für die $x \in A$, die eine Eigenschaft $P(x)$ erfüllen.

Damit läßt sich Satz 2 nun umformulieren:

Satz 2'. *(Szemerédi, ergodische Version) Sei $\nu_{\text{const}} : \mathbb{Z}_N \to \mathbb{R}^+$ die konstante Funktion $\nu_{\text{const}} \equiv 1$. Sei $0 < \delta \leq 1$, $k \geq 3$ fest. Sei $N \in \mathbb{N}$ groß, sei $f : \mathbb{Z}_N \to \mathbb{R}^+$ mit $0 \leq f(x) \leq \nu_{\text{const}}(x)$ für alle $x \in \mathbb{Z}_N$, und $\mathbb{E}(f(x) \mid x \in \mathbb{Z}_N) \geq \delta$. Dann gilt:*

$$\mathbb{E}(f(x)f(x+r)f(x+2r)\cdots f(x+(k-1)r) \mid x, r \in \mathbb{Z}_N) \geq c(k, \delta) - \underbrace{o_{k,\delta}(1)}_{\text{Nullfolge für } N \to \infty}$$

für eine reelle Konstante $c(k, \delta) > 0$, unabhängig von f oder N.

Bemerkungen

- Für $f(x) := \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$, der charakteristischen Funktion von A, erhalten wir mit Satz 2' wieder Satz 2 zurück.
- Die Behauptung von Satz 2' liefert sogar eine Abschätzung der Anzahl von APs in A, nämlich $\gg N^2$ (d. h. $\geq CN^2$ für eine Konstante $C > 0$) viele.

Die Strategie ist nun:

- ersetze $\nu_{\text{const}} \equiv 1$ durch ein pseudozufälliges Maß $\nu(x)$ (kurz "Maß" ν) auf $\mathbb{Z}_N$, nämlich durch eine geeignete Funktion $\nu : \mathbb{Z}_N \to \mathbb{R}^+$ mit $\mathbb{E}(\nu) = 1 + o(1)$, wobei $o(1)$ wieder eine Nullfolge für $N \to \infty$ bezeichne.
- untersuche, für welche ν Satz 2' immernoch gilt, dies wird dann der "Satz von Szemerédi-Green-Tao"
- wähle für ν eine Funktion, die eng mit Primzahlen zusammenhängt und deren charakteristische Funktion geeignet majorisiert, zeige dann: dieses ν ist pseudozufällig (dieser Beweisteil enthält einen siebtheoretischen Ansatz nach Goldston/Yıldırım), mittlerweile geht dieser Beweisteil rein siebtheoretisch

Zum Beweis des Szemerédi-Green-Tao-Satzes werden Gowers-Normen benötigt:

die Gowers-Norm von $f : \mathbb{Z}_N \to \mathbb{R}$ ist dabei

$$\|f\|_{U^2} := (\mathbb{E}(f(x)f(x+s)f(x+t)f(x+s+t) \mid x, s, t \in \mathbb{Z}_N)^{1/4},$$

und $\|f\|_{U^m}$ wird für $m \geq 3$ entsprechend definiert.

Gezeigt wird folgendes:

Proposition 1. $0 \leq |f_i| \leq 1, 0 \leq i \leq k \Rightarrow |\mathbb{E}(f_0(x)f_1(x+y)\cdots f_k(x+ky) \mid x, y \in \mathbb{Z}_N)| \leq \min_{i=1,\ldots,k} \|f_i\|$ *Diese Abschätzung zeigt: hat ein Faktor f_i kleine Gowers-Norm, so ist auch dieser Erwartungswert klein.*

Gleiches gilt bis auf Faktor, falls $|f_i(x)| \leq \nu(x)$. ("verallgemeinerter von Neumann-Satz")

Damit wird dann folgendes "Transfer-Prinzip" verfolgt:

Transfer-Prinzip Sei ν ein Maß, $0 \leq |f| \leq \nu$. Dann existiert eine Funktion g, $|g| \leq 1$, mit $\mathbb{E}(g(x) \mid x \in \mathbb{Z}_N) = \mathbb{E}(f(x) \mid x \in \mathbb{Z}_N)$, d. h. g verhält sich wie f bzgl. $\mathbb{E}$.

Genauer zeigen wir folgende Aussage, dies wird dann der schwierige Teil:

Proposition 2. $\forall \varepsilon > 0 \exists f_1, f_2, f_3 : \quad f = f_1 + f_2 + f_3, f_1 \in [0,1], f_2 \in [0, \nu], \|f_2\|_{U^k} < \varepsilon, \mathbb{E}(f_3(x) \mid x \in \mathbb{Z}_N) < \varepsilon.$

Idee nun: f_1 ist hier die einzige wichtige Funktion zur Abschätzung von $\mathbb{E}(f(x)\cdots f(x+ky) \mid x, y \in \mathbb{Z}_N)$ wegen dem verallgemeinerten von Neumann-Satz, der für f_2 greift. Der Fehler bei Übergang von f zu f_1 wird also klein sein, und f_3 ist ohnehin als Fehler anzusehen. Damit führen wir die Aussage auf den bisher bekannten Szemerédi-Satz 2 zurück, der als "black box" für f_1 benutzt wird.

In den nächsten Abschnitten werden wir also Satz 2/2' verallgemeinern zum Satz von Szemerédi-Green-Tao.

3 Pseudozufällige Maße

Sei ab jetzt $k \geq 3$ fest, $N = |\mathbb{Z}_N|$ prim und groß. (Dann sind alle $1, \ldots, k \in \mathbb{Z}_N$ invertierbar), und wir schreiben $o(1)$ für eine Nullfolge, wenn $N \to \infty$, und $O(1)$ für eine beschränkte Funktion, wenn $N \to \infty$.

Wir behandeln Maße, darunter verstehen wir hier Funktionen $\nu : \mathbb{Z}_N \to \mathbb{R}^+$ für die $\mathbb{E}(\nu) = 1 + o(1)$ gilt.

Wir werden zwei Bedingungen an Maße stellen: die Linearformbedingung und die Korrelationsbedingung. Diese definieren wir wie folgt.

Definition 3.1. *(Linearformbedingung)*

Seien $m_0, t_0, L_0 \in \mathbb{N}$ klein. Ein Maß ν erfüllt die (m_0, t_0, L_0)-Linearformbedingung, falls gilt:

Sind für $m \leq m_0$, $t \leq t_0$, rationale Zahlen $(L_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq t}} \subseteq \mathbb{Q}$ derart, daß deren Zähler und Nenner (der gekürzten Darstellung) $\leq L_0$ im Absolutbetrag sind, und sind weiter $b_i \in \mathbb{Z}_N$, $i = 1, \ldots, m$, $\psi_i : \mathbb{Z}_N^t \to \mathbb{Z}_N$, $\psi_i(\underline{x}) = \sum_{j=1}^t L_{ij} x_j + b_i$ für $\underline{x} = (x_1, \ldots, x_t) \in \mathbb{Z}_N^t$, wobei $L_{ij} \in \mathbb{Z}_N$ interpretiert wird (da N prim, $N > L_0$), sind die $(L_{ij})_{1 \leq j \leq t} \in \mathbb{Q}^t$ nicht $\underline{0}$ und ist keines dieser t-Tupel rationales Vielfaches eines anderen, so gilt:

$$\mathbb{E}(\nu(\psi_1(\underline{x})) \cdots \nu(\psi_m(\underline{x})) \mid \underline{x} \in \mathbb{Z}_N^t) = 1 + \underbrace{o_{L_0, m_0, t_0}(1)}_{\text{glm. in } b_1, \ldots, b_m} .$$

Bemerkung: Für $m = 1, t = 1, L_{11} = 1$ erhalten wir die Maßbedingung $\mathbb{E}(\nu) = 1 + o(1)$ zurück.

Definition 3.2. *(Korrelationsbedingung) Sei $m_0 \in \mathbb{N}$. Ein Maß ν erfüllt die m_0-Korrelationsbedingung, falls für alle $1 < m \leq m_0$ eine Funktion $\tau = \tau_m : \mathbb{Z}_N \to \mathbb{R}^+$ existiert mit $\mathbb{E}(\tau^q) = O_{m,q}(1)$ für alle $1 \leq q < \infty$ gilt (d. h. man hat "beschränkte Momente"), und so daß*

$$\mathbb{E}(\nu(x + h_1)\nu(x + h_2) \cdots \nu(x + h_m) \mid x \in \mathbb{Z}_N) \leq \sum_{1 \leq i, j \leq m} \tau(h_i - h_j)$$

für alle $h_1, \ldots, h_m \in \mathbb{Z}_N$ gilt (die h_i nicht notwendig paarweise verschieden).

Definition 3.3. *(pseudozufälliges Maß)*

Ein Maß ν heißt k-pseudozufällig, falls ν die $(k \cdot 2^{k-1}, 3k - 4, k)$-Linearformbedingung und die 2^{k-1}-Korrelationsbedingung erfüllt.

Klar: $\nu_{\text{const}} \equiv 1$ ist pseudozufälliges Maß.

Lemma 3.4. *Sei ν ein k-pseudozufälliges Maß. Dann ist auch $\nu_{1/2} := \frac{\nu + \nu_{\text{const}}}{2} = \frac{\nu + 1}{2}$ ein k-pseudozufälliges Maß.*

Beweis: Klar ist $\nu_{1/2} \geq 0$, $\mathbb{E}(\nu_{1/2}) = 1 + o(1)$. Für die Linearformbedingung ersetze ν durch $\frac{\nu+1}{2}$ in der Definition, dies ergibt eine Summe aus 2^m Summanden, geteilt durch 2^m, jeder dieser Terme ist $1 + o(1)$. Für die Korrelationsbedingung geht man ebenso vor. □

Auch kann dies für $(1 - \theta)\nu + \theta\nu_{\text{const}}$ mit beliebigen $0 \leq \theta \leq 1$ gezeigt werden.

Unser erstes Ziel ist es nun, die folgende Verallgemeinerung von Satz 2/2' zu beweisen:

Satz 3. *(Satz von Szemerédi-Green-Tao, Szemerédi-Satz für pseudozufällige Maße)*

Sei $k \geq 3$, $0 < \delta \leq 1$ fest, ν sei k-pseudozufälliges Maß, sei $f : \mathbb{Z}_N \to \mathbb{R}^+$ eine Funktion mit $0 \leq f(x) \leq \nu(x)$ für alle $x \in \mathbb{Z}_N$, und $\mathbb{E}(f) \geq \delta$. Dann gilt:

$$\mathbb{E}(f(x)f(x+r)\cdots f(x+(k-1)r) \mid x, r \in \mathbb{Z}_N) \geq c(k,\delta) - o_{k,\delta}(1)$$

mit derselben Konstanten $c(k,\delta)$ wie in Satz 2'.

Bevor wir den Beweis angehen, vereinbaren wir einige

Notationen:

Für reelles $1 \leq q < \infty$ und eine Funktion $f : \mathbb{Z}_N \to \mathbb{C}$ definieren wir die L^q-Norm von f als

$$\|f\|_{L^q} := \mathbb{E}(|f|^q)^{1/q}, \text{ sowie } \|f\|_{L^\infty} := \sup_{x \in \mathbb{Z}_N} |f(x)|.$$

Sei $L^q(\mathbb{Z}_N)$ der Banachraum aller Funktionen $\mathbb{Z}_N \to \mathbb{C}$ mit der L^q-Norm.

$L^2(\mathbb{Z}_N)$ ist komplexer Hilbertraum mit Skalarprodukt $\langle f, g\rangle := \mathbb{E}(f\overline{g})$.

Für $\Omega \subseteq \mathbb{Z}_N$ sei $1_\Omega : \mathbb{Z}_N \to \mathbb{C}$, $1_\Omega(x) = \begin{cases} 1, & x \in \Omega \\ 0, & \text{sonst} \end{cases}$ die Indikatorfunktion von Ω.

Schreiben auch: $1_{P(x)}$ für $1_{\{x \in \mathbb{Z}_N; P(x)\}}$.

4 Uniformitätsnormen (Gowersnormen) und ein verallgemeinerter von Neumann-Satz

Definition 4.1. *Sei $d \geq 1$ eine Dimension (eine natürliche Zahl, typischerweise $= k-1$), sei $\{0,1\}^d$ der diskrete d-dimensionale Standardwürfel, die Elemente seien $\omega = (\omega_1, \ldots, \omega_d)$ mit $\omega_j \in \{0,1\}$ für $j = 1, \ldots d$. Wir schreiben $|\omega| := \omega_1 + \cdots + \omega_d$, und für $h = (h_1, \ldots, h_d) \in \mathbb{Z}_N^d$ definieren wir $\omega \cdot h := \omega_1 h_1 + \cdots + \omega_d h_d$.*

Für ein $\{0,1\}^d$-Tupel von Funktionen $(f_\omega)_{\omega \in \{0,1\}^d}$ in $L^\infty(\mathbb{Z}_N)$ definieren wir das <u>*innere Gowers-Produkt*</u>

$$\langle (f_\omega)_{\omega \in \{0,1\}^d} \rangle_{U^d} = \mathbb{E}\Big(\prod_{\omega \in \{0,1\}^d} \mathcal{C}^{|\omega|} f_\omega(x + \omega \cdot h) | x \in \mathbb{Z}_N, h \in \mathbb{Z}_N^d \Big),$$

wobei $\mathcal{C}f(x) := \overline{f(x)}$ die komplexe Konjugation bezeichne.

Kurz schreiben wir: $\langle f_\omega \rangle_{U^d} = \mathbb{E}(\prod_\omega \mathcal{C}^{|\omega|} f_\omega(x + \omega \cdot h) | x, h)$.

Beispiel: Für $d = 1$ haben wir die Formel $\langle f_\omega \rangle_{U^1} = \mathbb{E}(f_0(x)\overline{f_1(x+h)} | x, h)$,

für $d = 2$ haben wir $\langle f_\omega \rangle_{U^2} = \mathbb{E}(f_{00}(x)\overline{f_{01}(x+h_2)f_{10}(x+h_1)}f_{11}(x+h_1+h_2) | x, h_1, h_2)$.

Eigenschaften von $\langle \cdot \rangle_{U^d}$:

- Hängt f_ω nicht von der letzten Variablen ω_d von ω ab, so gilt:

$$\langle f_\omega \rangle_{U^d} = \mathbb{E}\Big(\prod_{\omega' \in \{0,1\}^{d-1}} \mathcal{C}^{|\omega'|}(f_{\omega'}(x + \omega' h')\overline{f_{\omega'}(x + h_d + \omega' h')}) | x, h', h_d \Big)$$

$$=\mathbb{E}\Big(|\mathbb{E}\Big(\prod_{\omega'}\mathcal{C}^{|\omega'|}f_{\omega'}(x+\omega' h')|y\in\mathbb{Z}_N\Big)|^2|h'\in\mathbb{Z}_N^{d-1}\Big)\geq 0.$$

Damit definieren wir Gowers Gleichmäßigkeitsnorm von $f:\mathbb{Z}_N\to\mathbb{C}$ als

$$\|f\|_{U^d}:=\langle(f)_\omega\rangle_{U^d}^{1/2^d}=\mathbb{E}\Big(\prod_{\omega}\mathcal{C}^{|\omega|}f(x+\omega h)|x\in\mathbb{Z}_N,h\in\mathbb{Z}_N^d\Big)^{1/2^d}.$$

- Es gilt die Gowers Cauchy-Schwarz Ungleichung:
$$|\langle f_\omega\rangle_{U^d}|\leq\prod_\omega\|f_\omega\|_{U^d}$$
- Es gilt die Gowers Δ-Ungleichung:
$$\|f+g\|_{U^d}\leq\|f\|_{U^d}+\|g\|_{U^d}$$
- Es gilt $\|cf\|_{U^d}=|c|\|f\|_{U^d}$, also sind die U^d-Normen Seminormen.
- Es gilt $\|f\|_{U^1}\leq\|f\|_{U^2}\leq\|f\|_{U^3}\leq\dots$.
- Die U^1-Norm ist keine Norm: $\|f\|_{U^1}=|\mathbb{E}(f)|$, dies kann $=0$ sein mit $f\not\equiv 0$
- Die U^2-Norm ist eine Norm: Es gilt die Formel
$$\|f\|_{U^2}=\Big(\sum_\xi|\hat{f}(\xi)|^4\Big)^{1/4}$$
für die Fouriertransformierte $\hat{f}(\xi):=\mathbb{E}(f(x)e(-x\xi/N)|x\in\mathbb{Z}_N)$, wo $e(t):=\exp(2\pi it)$. Demnach ist $\|f\|_{U^2}=0\Leftrightarrow f\equiv 0$. Da die Normen von f monoton steigend in d sind, sind dann auch die U^d-Normen für $d\geq 2$ echte Normen.

Lemma 4.2. *ν sei k-pseudozufällig. Dann gilt: $\|\nu-\nu_{const}\|_{U^d}=\|\nu-1\|_{U^d}=o(1)$.*

Beweis: Da die U^d-Normen nichtfallend in d sind, sei ohne Einschränkung $d=k-1$.

Damit genügt es, zu zeigen: $\mathbb{E}(\prod_\omega(\nu(x+\omega h)-1)|x,h)\stackrel{!}{=}o(1)$.
Die linke Seite ist ausmultipliziert

$$=\sum_{A\subseteq\{0,1\}^{k-1}}(-1)^{|A|}\mathbb{E}\Big(\prod_{\omega\in A}\nu(x+\omega h)|x,h\Big).$$

Der $\mathbb{E}$-Ausdruck darin ist von der Form $\mathbb{E}(\nu(\psi_1(\underline{x}))\cdots\nu(\psi_{|A|}(\underline{x}))|\underline{x}\in\mathbb{Z}_N^k)=1+o(1)$, denn ν ist k-pseudozufällig, daher kann die $(2^{k-1},k,1)$-Linearformbedingung angewendet werden auf die $|A|\leq 2^{k-1}$ vielen Linearformen $\psi_1,\dots,\psi_{|A|}$, die nur eine Anordnung der Linearformen $x+\omega h$ sind; diese haben k viele Variablen (nämlich $x,h_1,\dots,h_{k-1}$), und die Koeffizienten sind maximal durch 1 beschränkt.

Somit erhalten wir für die linke Seite $=\sum_{A\subseteq\{0,1\}^{k-1}}(-1)^{|A|}+o(1)=(1-1)^{k-1}+o(1)=o(1)$. □

Wir zeigen nun folgenden Satz, der die Kernidee für den Satz von Szemerédi-Green-Tao ist:

Proposition 4.3. *(Verallgemeinerter von Neumann-Satz): Sei ν ein k-pseudozufälliges Maß, seien $f_0, \dots, f_{k-1} \in L^1(\mathbb{Z}_N)$ mit $|f_j(x)| \le \nu(x) + 1$ für alle $x \in \mathbb{Z}_N$, $0 \le j \le k-1$. Dann ist*

$$\mathbb{E}\Big(\prod_{j=0}^{k-1} f_j(x + jr) | x, r \in \mathbb{Z}_N\Big) = O\Big(\min_{0 \le j \le k-1} \|f_j\|_{U^{k-1}}\Big) + o(1).$$

Bemerkungen:

- Ersetze die Voraussetzung $|f_j(x)| \le \nu(x) + 1$ durch $|f_j(x)| \le \nu(x)$, es genügt, den Satz in dieser Version zu zeigen! (Denn ist $\nu(x) < f_j(x) \le \nu(x) + 1$ für ein x, betrachte das Maß $(\nu(x)+1)/2 \ge |f_j|/2$ (ebenso k-pseudozufällig nach Lemma 3.1), die Behauptung für $f_j/2$ liefert dann die Behauptung für f_j.)
- Mit demselben Trick können wir annehmen, daß $\nu(x) > 0$ ist für alle x.
- Weiter sei $\min_{0 \le j \le k-1} \|f_j\|_{U^{k-1}} = \|f_0\|_{U^{k-1}}$, denn der folgende Beweis geht auch dann durch, wenn das Minimum bei irgendeinem j_0 statt 0 angenommen wird.
- Damit bleibt zu zeigen:

$$\mathbb{E}\Big(\prod_{j=0}^{k-1} f_j(x + jr) | x, r\Big) \stackrel{!}{=} O(\|f_0\|_{U^{k-1}}) + o(1).$$

Für den Beweis benötigen wir ein Hilfslemma, das eine Anwendung der Cauchy-Schwarz-Ungleichung ist, und dafür die folgende **Notation**:

Für $0 \le d \le k-q$, $y = (y_1, \dots, y_{k-1}) \in \mathbb{Z}_N^{k-1}$, $y' = (y'_{k-d}, \dots, y'_{k-1}) \in \mathbb{Z}_N^d$, für $S \subseteq \{k-d, \dots, k-1\}$ definieren wir $y^{(S)} = (y_1^{(S)}, \dots, y_{k-1}^{(S)}) \in \mathbb{Z}_N^{k-1}$ als

$$y_i^{(S)} := \begin{cases} y_i, & i \notin S, \\ y'_i, & i \in S \end{cases}$$

Das bedeutet, S gibt an, welche der letzten d Komponenten von $y^{(S)}$ von y_i auf y'_i "umgeschaltet" werden. Damit formulieren wir eine Cauchy-Schwarz-Ungleichung wie folgt.

Lemma 4.4. *(Cauchy-Schwarz) Sei $\nu : \mathbb{Z}_N \to \mathbb{R}^+$ Maß, seien $\phi_0, \dots, \phi_{k-1} : \mathbb{Z}_N^{k-1} \to \mathbb{Z}_N$ Funktionen in $k-1$ Variablen y_i, wobei ϕ_i nicht von y_i abhängt, $1 \le i \le k-1$. Seien $f_0, \dots, f_{k-1} \in L^1(\mathbb{Z}_N)$ Funktionen mit $|f_i(x)| \le \nu(x)$ für alle x und i.*

Für $0 \le d \le k-1$ definieren wir

$$J_d := \mathbb{E}\Big(\prod_{S \subseteq \{k-d, \dots, k-1\}} \prod_{i=0}^{k-d-1} \mathcal{C}^{|S|} f_i(\phi_i(y^{(S)})) \cdot \prod_{i=k-d}^{k-1} \nu^{1/2}(\phi_i(y^{(S)})) | y, y'\Big),$$

und

$$P_d := \mathbb{E}\Big(\prod_{S \subseteq \{k-d, \dots, k-1\}} \nu(\phi_{k-d-1}(y^{(S)})) | y, y'\Big).$$

Dann gilt für $0 \le d \le k-2$: $|J_d|^2 \le P_d J_{d+1}$.

Beweis: Da ϕ_{k-d-1} unabhängig von y_{k-d-1} ist, schreiben wir

$$J_d = \mathbb{E}(G(y,y')H(y,y')|y,y' \text{ ohne } y_{k-d-1})$$

mit

$$G(y,y') := \prod_{S\subseteq\{k-d,\dots,k-1\}} \mathcal{C}^{|S|} f_{k-d-1}(\phi_{k-d-1}(y^{(S)}))\nu^{-1/2}(\phi_{k-d-1}(y^{(S)}))$$

und

$$H(y,y') := \mathbb{E}\Big(\prod_{S\subseteq\{k-d,\dots,k-1\}} \prod_{i=0}^{k-d-2} \mathcal{C}^{|S|} f_i(\phi_i(y^{(S)})) \prod_{i=k-d-1}^{k-1} \nu^{1/2}(\phi_i(y^{(S)})) \mid y_{k-d-1}\in\mathbb{Z}_N\Big).$$

Dann zeigt die Cauchy-Schwarz-Ungleichung, daß

$$|J_d|^2 \le \mathbb{E}(|G|^2|\dots)\cdot\mathbb{E}(|H|^2|\dots)$$

gilt, wobei der erste Faktor $\le P_d$ ist wegen $|f_{k-d-1}(\phi_{k-d-1}(y^{(S)}))| \le \nu(\phi_{k-d-1}(y^{(S)}))$, und der zweite läßt sich durch Variablensubstitution auf J_{d+1} bringen. □

Wendet man dieses Lemma $(k-1)$-mal an, so folgt:

$$|J_0|^{2^{k-1}} \le J_{k-1}\prod_{d=0}^{k-2} P_d^{2^{k-2-d}},$$

wobei $J_0 = \mathbb{E}(\prod_i f_i(\phi_i(y))|y\in\mathbb{Z}_N^{k-1})$ bezeichnet.

Nun zum **Beweis** von Proposition 4.3: Wir wählen die ϕ_i geschickt nun so, daß diese eine AP der Länge k durchlaufen. Dafür setzen wir

$$\phi_i(y) := \sum_{j=1}^{k-1}\left(1-\frac{i}{j}\right)y_j \text{ für } i=0,\dots,k-1.$$

Dann ist $\phi_0(y) = y_1+\dots+y_{k-1}$, $\phi_i(y)$ unabhängig von y_i, die $\phi_i(y)$ bilden eine AP der Länge k und Differenz $\sum_{j=1}^{k-1}\frac{y_j}{j}$.

Betrachte nun die Funktion $\Phi : \mathbb{Z}_N^{k-1}\to\mathbb{Z}_N^2$,

$$\Phi(y) := (y_1+\dots+y_{k-1}, \frac{y_1}{1}+\frac{y_2}{2}+\dots+\frac{y_{k-1}}{k-1}),$$

diese ist eine "gleichmäßige Überdeckung", das bedeutet, daß $\Phi : A\to B$ surjektiv ist und alle Fasern $\{\Phi^{-1}(b); b\in B\}$ die gleiche Kardinalität haben. Bei einer gleichmäßigen Überdeckung gilt für alle $f : B\to\mathbb{C}$ die Gleichung $\mathbb{E}(f(\Phi(a))|a) = \mathbb{E}(f(b)|b)$, somit folgt für die linke Seite der Behauptung in Proposition 4.3, daß diese

$$= \mathbb{E}(\prod_{i=0}^{k-1} f_i(x+ir)|x,r) = \mathbb{E}(\prod_{i=0}^{k-1} f_i(\phi_i(y))|y\in\mathbb{Z}_N^{k-1}) = J_0$$

ist.

Wir haben $P_d = 1 + o(1)$ für alle $0 \le d \le k-2$, da ν k-pseudozufällig ist und daher die $(2^d, k-1+d, k)$-Linearformbedingung gilt. Somit ist

$$J_0^{2^{k-1}} \le (1+o(1))J_{k-1}$$

Für $y \in \mathbb{Z}_N^{k-1}$ fest durchläuft $\phi_0(y^{(S)})$ mit $S \subseteq \{1,\dots,k-1\}$ die Menge $\{x+\omega\cdot h : \omega \in \{0,1\}^{k-1}\}$, wobei $x = y_1 + \cdots + y_{k-1}$ und $h_i = y_i' - y_i$, $i = 1,\dots,k-1$ ist. (Die Addition mit h_i ersetzt in x den Summanden y_i durch y_i'.)

Somit ist (wobei y_{k-1} durch $x - y_1 - \cdots - y_{k-2}$ ersetzt ist):

$$J_{k-1} = \mathbb{E}\Big(W(x,h) \prod_{\omega\in\{0,1\}^{k-1}} \mathcal{C}^{|\omega|} f_0(x+\omega\cdot h) \mid x,h\Big)$$

mit

$$\begin{aligned} W(x,h) &= \mathbb{E}\Big(\prod_{\omega\in\{0,1\}^{k-1}} \prod_{i=1}^{k-1} \nu^{1/2}(\phi_i(y+\omega h)) \mid y_1,\dots,y_{k-2}\Big) \\ &= \mathbb{E}\Big(\prod_{i=1}^{k-1} \prod_{\substack{\omega\in\{0,1\}^{k-1}\\ \omega_i=0}} \nu(\phi_i(y+\omega h)) \mid y_1,\dots,y_{k-2}\Big). \end{aligned}$$

Nun ist

$$\mathbb{E}\Big(\prod_{\omega\in\{0,1\}^{k-1}} \mathcal{C}^{|\omega|} f_0(x+\omega\cdot h) \mid x,h\Big) = \|f_0\|_{U^{k-1}}^{2^{k-1}}.$$

Daher genügt es, zu zeigen:

$$\mathbb{E}((W(x,h)-1)\prod_{\omega} \mathcal{C}^{|\omega|} f_0(x+\omega h)|x,h) \stackrel{!}{=} o(1).$$

Dafür wiederum genügt es, zu zeigen (da $|f_0| \le \nu$):

$$\mathbb{E}(|W(x,h)-1|\prod_{\omega} \nu(x+\omega h)|x,h) \stackrel{!}{=} o(1).$$

Wegen Lemma 4.2 ($\|\nu - 1\|_{U^d} = o(1)$) ist $\mathbb{E}(\prod_\omega \nu(x+\omega h)|x,h) = O(1)$, also genügt es mit CS, zu zeigen:

Lemma 4.5.

$$\mathbb{E}(|W(x,h)-1|^2\prod_{\omega} \nu(x+\omega h)|x,h) \stackrel{!}{=} o(1).$$

Durch Ausmutliplizieren des Quadrats reicht es dann, zu zeigen:

$$\mathbb{E}(W(x,h)^q\prod_{\omega} \nu(x+\omega h)|x,h) \stackrel{!}{=} 1+o(1),\ q=0,1,2.$$

Für $q=0$ benutze die $(2^{k-1},k,1)$-Linearformbedingung für die Formen $x+\omega h$ in den Variablen $x, h_1,\dots,h_{k-1}$.

Für $q = 1$ benutze die $(2^{k-2}(k+1), 2k-2, k)$-Linearformbedingung für die Formen $\phi_i(y + \omega h)$, $\omega_i = 0$, $1 \le i \le k-2$, sowie $\phi_{k-1}(x - y_1 - \cdots - y_{k-2} + \omega h)$, $\omega_{k-1} = 0$, $x + \omega h$ in den Variablen $x, h_1, \ldots, h_{k-1}, y_1, \ldots, y_{k-2}$.

Für $q = 2$ benutze die $(2^{k-1}k, 3k-4, k)$-Linearformbedingung für die Formen $x+\omega h$, $\phi_i(y+\omega h)$, $\omega_i = 0$, $1 \le i \le k-1$, $\phi_i(y'+\omega h)$, $\omega_i = 0$, $1 \le i \le k-1$ (beachte $y_{k-1} = x - y_1 - \cdots - y_{k-2}$, $y'_{k-1} = x - y'_1 - \cdots - y'_{k-2}$) in den Variablen $x, h_1, \ldots, h_{k-1}, y_1, \ldots, y_{k-2}, y'_1, \ldots, y'_{k-2}$. □

5 Anti-Uniformität

Für $k \ge 3$, wenn die Gowers-Norm $\|\cdot\|_{U^{k-1}}$ eine echte Norm ist, definieren wir die duale $(U^{k-1})^*$-Norm von $g : \mathbb{Z}_N \to \mathbb{C}$ als

$$\|g\|_{U^{k-1^*}} := \sup\{|\langle f, g\rangle| \; ; \; f \in U^{k-1}(\mathbb{Z}_N), \|f\|_{U^{k-1}} \le 1\}$$

Zur Erinnerung: $\langle f, g\rangle := \mathbb{E}(f\overline{g}) = \frac{1}{N}\sum_{x\in\mathbb{Z}_N} f(x)\overline{g}(x)$

Definition. *g heißt Gowers-antiuniform, falls $\|g\|_{U^{k-1^*}} = O(1)$ und $\|g\|_{L^\infty} = O(1)$.*

Es gilt: $|\langle f, g\rangle| \le \|f\|_{U^{k-1}}\|g\|_{U^{k-1^*}}$

Definition. *Für $F \in L^1(\mathbb{Z}_N)$ definieren wir die duale Funktion von F als*

$$\mathcal{D}F(x) := \mathbb{E}\Big(\prod_{\omega\in\{0,1\}^{k-1},\, \omega\neq\underline{0}} \mathcal{C}^{|\omega|-1}F(x+\omega h) | h \in \mathbb{Z}_N^{k-1}\Big)$$

Lemma 5.1. *Sei $F \in L^1(\mathbb{Z}_N)$. Dann gilt:*

(i) $|\langle F, \mathcal{D}F\rangle| = \|F\|_{U^{k-1}}^{2^{k-1}}$

(ii) $\|\mathcal{D}F\|_{U^{k-1^*}} = \|F\|_{U^{k-1}}^{2^{k-1}-1}$

(iii) Ist ν k-pseudozufällig und $|F(x)| \le \nu(x) + 1$ für alle $x \in \mathbb{Z}_N$, so gilt $\|\mathcal{D}F\|_{L^\infty} \le 2^{2^{k-1}-1} + o(1)$.

Beweis: (i): Definition einsetzen und ausschreiben.

(ii): Sei ohne Einschränkung $F \not\equiv 0$, es genügt dann mit (i), für beliebige Funktionen $f \in L^1(Z_N)$ zu zeigen:

$$|\langle f, \mathcal{D}F\rangle| \le \|f\|_{U^{k-1}}\|F\|_{U^{k-1}}^{2^{k-1}-1}$$

Die linke Seite ist hier der Betrag des inneren Gowers-Produkts $\langle f_\omega\rangle_{U^{k-1}}$, wo $f_{\underline{0}} = f$ und $f_\omega = F$ für $\omega \neq \underline{0}$ ist. Die Gowers-Cauchy-Schwarz-Ungleichung liefert dann die Abschätzung.

(iii): Es ist $F \le 2 \cdot \frac{\nu+1}{2} = 2\nu_{1/2}$ und daher $\mathcal{D}F \le 2^{2^{k-1}-1}\mathcal{D}\nu_{1/2}$. Weiter ist

$$\mathcal{D}\nu_{1/2}(x) = \mathbb{E}\Big(\prod_{\omega\neq 0} \nu_{1/2}(x+\omega h) | h \in \mathbb{Z}_N^{k-1}\Big) = 1 + o(1)$$

aufgrund der Linearformbedingung für das k-pseudozufällige Maß $\nu_{1/2}$. Dies zeigt die Abschätzung. □

Definition. *Ist F punktweise beschränkt durch $\nu+1$, ν k-pseudozufällig, so heißt $\mathcal{D}F$ antiuniforme Basisfunktion.*

Bemerkung: Diese ist antiuniform falls $\|F\|_{U^{k-1}} = O(1)$, nach (ii) und (iii) des Lemmas.

Proposition 5.2 (Uniforme Verteilung bzgl. anti-uniformer Basisfunktionen)**.** *Sei ν k-pseudozufällig, $K \geq 1$, $\Phi : \mathbb{C}^K \to \mathbb{C}$ stetige Funktion, seien $\mathcal{D}F_1, \dots, \mathcal{D}F_K$ antiuniforme Basisfunktionen, und sei $\psi : \mathbb{Z}_N \to \mathbb{C}$ definiert durch*

$$\psi(x) := \Phi(\mathcal{D}F_1(x), \dots, \mathcal{D}F_K(x)).$$

Dann gilt

$$\langle \nu - 1, \psi \rangle = o_{K,\Phi}(1).$$

Zusatz: Durchläuft Φ eine kompakte Menge von stetiger Funktionen in der L_∞-Topologie, dann sind die Schranken gleichmäßig in Φ (d. h. man kann dann $o_{K,\Phi}(1)$ durch $o_{K,E}(1)$ ersetzen).

Wir führen den Beweis in zwei Schritten: Erst behandeln wir Polynome Φ, dann folgt ein Approximationsargument. Weiter ersetzen wir die Voraussetzung $|F_j(x)| \leq \nu(x)+1$ ohne Einschränkung durch $|F_j(x)| \leq \nu(x)$ (wieder durch Ersetzen von ν durch $\frac{\nu+1}{2}$).

Zum ersten Schritt:

Lemma 5.3. *Sei $d \geq 1$, P ein Polynom in K Variablen vom Grad d und mit komplexen, von N unabhängigen Koeffizienten. Dann gilt:*

$$\|P(\mathcal{D}F_1, \dots, \mathcal{D}F_K)\|_{U^{k-1^*}} = O_{K,d,P}(1).$$

Beweis: Ohne Einschränkung sei P ein Monom, und zwar $P(z_1, \dots, z_K) = z_1 \cdots z_K$ (erweitere K auf dK, wiederhole F_j, wenn nötig).

Dann genügt es, zu zeigen:

$$\Big\langle f, \prod_{j=1}^{K} \mathcal{D}F_j \Big\rangle \stackrel{!}{=} O_K(1)$$

für alle $f : \mathbb{Z}_N \to \mathbb{C}$ mit $\|f\|_{U^{k-1}} \leq 1$.

Die linke Seite ist

$$\mathbb{E}\Bigg(f(x) \prod_{j=1}^{K} \mathbb{E}\Big(\prod_{\omega \in \{0,1\}^{k-1},\ \omega \neq \underline{0}} F_j(x + \omega \cdot h^{(j)}) \;\Big|\; h^{(j)} \in \mathbb{Z}_N^{k-1} \Big) \;\Bigg|\; x \in \mathbb{Z}_N \Bigg).$$

Die Substituion $h^{(j)} = h + H^{(j)}$ gibt denselben Wert für jedes $h \in \mathbb{Z}_N^{k-1}$, daher bilden wir noch den Erwartungswert über h und formen den Ausdruck um in

$$\mathbb{E}\Bigg(f(x) \prod_{j=1}^{K} \mathbb{E}\Big(\prod_{\omega \in \{0,1\}^{k-1},\ \omega \neq \underline{0}} F_j(x + \omega \cdot H^{(j)} + \omega \cdot h) \;\Big|\; H^{(j)} \in \mathbb{Z}_N^{k-1} \Big) \;\Bigg|\; x \in \mathbb{Z}_N, h \in \mathbb{Z}_N^{k-1} \Bigg).$$

Durch Vertauschen der Erwartungswerte nach x, h und H schreiben wir den inneren Ausdruck als inneres Gowers-Produkt, nämlich wir erhalten

$$\mathbb{E}\big(\langle (f_{\omega,H})_{\omega \in \{0,1\}^{k-1}} \rangle_{U^{k-1}} \;\big|\; H \in (\mathbb{Z}_N^{k-1})^K \big),$$

wobei $H := (H^{(1)}, \dots, H^{(K)})$, $f_{0,H} := f$, und $f_{\omega,H} := g_{\omega\cdot H}$ für $\omega \neq \underline{0}$, wobei $\omega \cdot H := (\omega \cdot H^{(1)}, \dots, \omega \cdot H^{(K)})$ und

$$g_{u^{(1)},\dots,u^{(K)}}(x) := \prod_{j=1}^{K} F_j(x + u^{(j)}) \text{ für alle } u^{(1)}, \dots, u^{(K)} \in \mathbb{Z}_N.$$

Nach der Gowers-Cauchy-Schwarz-Ungleichung ist dies

$$\leq \mathbb{E}\Big(\|f\|_{U^{k-1}} \prod_{\omega\in\{0,1\}^{k-1},\ \omega\neq\underline{0}} \|g_{\omega\cdot H}\|_{U^{k-1}} \ \Big|\ H \in (\mathbb{Z}_N^{k-1})^K \Big),$$

daher genügt es, zu zeigen, daß

$$\mathbb{E}\Big(\prod_{\omega\in\{0,1\}^{k-1},\ \omega\neq\underline{0}} \|g_{\omega\cdot H}\|_{U^{k-1}} \ \Big|\ H \in (\mathbb{Z}_N^{k-1})^K \Big) = O_K(1).$$

Nach der Hölderschen Ungleichung genügt es wiederum,

$$\mathbb{E}\big(\|g_{\omega\cdot H}\|_{U^{k-1}}^{2^{k-1}-1} \ \big|\ H \in (\mathbb{Z}_N^{k-1})^K \big) = O_K(1)$$

für jedes $\omega \neq \underline{0}$ zu zeigen, und da $2^{k-1} - 1 \leq 2^{k-1}$, reicht nach Höldern auch der Nachweis von

$$\mathbb{E}\big(\|g_{\omega\cdot H}\|_{U^{k-1}}^{2^{k-1}} \ \big|\ H \in (\mathbb{Z}_N^{k-1})^K \big) \stackrel{!}{=} O_K(1).$$

Die Abbildung $\Phi : \mathbb{Z}_N^K \to (\mathbb{Z}_N^{k-1})^K$, $H \to \omega H$ ist eine gleichmäßige Überdeckung für $\omega \neq \underline{0}$ (d. h. $\Phi : A \to B$ ist surjektiv und alle Fasern $\Phi^{-1}(b)$ haben die gleiche Kardinalität. Dafür gilt dann für alle $f : B \to \mathbb{C}$: $\mathbb{E}(f(\Phi(a))|a) = \mathbb{E}(f(b)|b)$).

Somit ist die linke Seite gleich

$$\begin{aligned}
&\mathbb{E}\big(\|g_{u^{(1)},\dots,u^{(K)}}\|_{U^{k-1}}^{2^{k-1}} \ \big|\ u^{(1)}, \dots, u^{(K)} \in \mathbb{Z}_N \big) \\
=&\mathbb{E}\Big(\prod_{\tilde{\omega}\in\{0,1\}^{k-1}} \prod_{j=1}^{K} F_j(x + u^{(j)} + h\cdot\tilde{\omega}) \ \Big|\ x \in \mathbb{Z}_N, h \in \mathbb{Z}_N^{k-1}, u^{(1)}, \dots, u^{(K)} \in \mathbb{Z}_N \Big) \\
=&\mathbb{E}\Big(\prod_{j=1}^{K} \mathbb{E}\big(\prod_{\tilde{\omega}\in\{0,1\}^{k-1}} F_j(x + u^{(j)} + h\cdot\tilde{\omega}) \ \big|\ u^{(j)} \in \mathbb{Z}_N \big) \ \Big|\ x \in \mathbb{Z}_N, h \in \mathbb{Z}_N^{k-1} \Big) \\
\leq&\mathbb{E}\Big(\mathbb{E}\big(\prod_{\tilde{\omega}\in\{0,1\}^{k-1}} \nu(\underbrace{x+u}_{=:y} + h\cdot\tilde{\omega}) \ \big|\ u \in \mathbb{Z}_N \big)^K \ \Big|\ x \in \mathbb{Z}_N, h \in \mathbb{Z}_N^{k-1} \Big) \\
=&\mathbb{E}\Big(\mathbb{E}\big(\prod_{\tilde{\omega}\in\{0,1\}^{k-1}} \nu(y + h\cdot\tilde{\omega}) \ \big|\ y \in \mathbb{Z}_N \big)^K \ \Big|\ h \in \mathbb{Z}_N^{k-1} \Big),
\end{aligned}$$

zu zeigen ist nun die Beschränktheit dieses Ausdrucks. Aufgrund der Korrelationsbedingung für ν (das einzige Mal, wo diese benutzt wird!), gilt

$$\mathbb{E}\Big(\prod_{\tilde{\omega}\in\{0,1\}^{k-1}} \nu(y + h\cdot\tilde{\omega}) \ \Big|\ y \in \mathbb{Z}_N \Big) \leq \sum_{\tilde{\omega},\tilde{\omega}'\in\{0,1\}^{k-1},\ \tilde{\omega}\neq\tilde{\omega}'} \tau(h\cdot(\tilde{\omega} - \tilde{\omega}')),$$

wobei τ derart ist, daß alle $\mathbb{E}(\tau^q) = O_{m,q}(1)$ sind (hier ist $m = 2^{k-1} - 1$).

Somit genügt es nach Anwenden der Dreiecksungleichung in $L^K(\mathbb{Z}_N^{k-1})$, zu zeigen daß

$$\mathbb{E}\big(\tau(h \cdot (\tilde{\omega} - \tilde{\omega}'))^K \;\big|\; h \in \mathbb{Z}_N^{k-1}\big) \stackrel{!}{=} O_K(1)$$

für alle verschiedenen $\tilde{\omega}, \tilde{\omega}' \in \{0,1\}^{k-1}$ gilt.

Die Abbildung $h \mapsto h \cdot (\tilde{\omega} - \tilde{\omega}')$ ist wieder eine gleichmäßige Überdeckung $(\mathbb{Z}_N)^{k-1} \to \mathbb{Z}_N$, also ist die linke Seite gleich $\mathbb{E}(\tau^K) = O_K(1)$. □

Nun der eigentliche **Beweis von Proposition 5.2**: Sei Φ, ψ gegeben, $\varepsilon > 0$. Die Werte von $\mathcal{D}F_j$ liegen wegen $\|\mathcal{D}F_j\|_{L^\infty} \leq 2^{2^{k-1}-1} + o(1)$ für großes N im (kompakten) Ball $\{z \in \mathbb{C} \;;\; |z| \leq 2^{2^{k-1}}\}$. Nach dem Weierstraßschen Approximationssatz läßt sich Φ dort approximieren durch ein Polynom P, d. h. so daß

$$\|\Phi(\mathcal{D}F_1, \ldots, \mathcal{D}F_K) - P(\mathcal{D}F_1, \ldots, \mathcal{D}F_K)\|_{L^\infty} \leq \varepsilon.$$

Es folgt:

$$|\langle \nu - 1, (\Phi - P)(\mathcal{D}F_1, \ldots, \mathcal{D}F_K)\rangle| \leq \mathbb{E}(|\nu - 1|)\varepsilon \leq (2 + o(1))\varepsilon$$

wegen $\mathbb{E}(\nu) = 1 + o(1)$. Andererseits ist

$$\langle \nu - 1, \Phi(\mathcal{D}F_1, \ldots, \mathcal{D}F_K)\rangle \leq \|\nu - 1\|_{U^{k-1}} \|P(\mathcal{D}F_1, \ldots, \mathcal{D}F_K)\|_{U^{k-1^*}} = o_{K,\varepsilon}(1)$$

wegen $\|\nu - 1\|_{U^{k-1}} = o(1)$ (Lemma 4.2) und Lemma 5.3.

Somit ist dann

$$|\langle \nu - 1, \Phi(\mathcal{D}F_1, \ldots \mathcal{D}F_K)\rangle| \leq 4\varepsilon,$$

wenn N groß genug ist (abhängig von K, ε).

Der Zusatz ist klar: Man überdecke die kompakte Menge mit endlich vielen Bällen. □

6 Verallgemeinerte Bohr-Mengen und σ-Algebren

Seien ab jetzt alle Funktionen auf $\mathbb{Z}_N$ reellwertig.

Definition 6.1.

- *σ-Algebra $\mathcal{B}$ in $\mathbb{Z}_N$: System von Teilmengen von $\mathbb{Z}_N$, inkl. $\emptyset$ und $\mathbb{Z}_N$, abgeschl. unter Komplementbildung, Vereinigungen, Schnitten*
- *Atome einer σ-Algebra $\mathcal{B}$: minimale, nichtleere Elemente von $\mathcal{B}$ (bzgl. Inklusion), die Atome von $\mathcal{B}$ entsprechen bilden eine Partition von $\mathbb{Z}_N$ und umgekehrt*
- *$f \in L^q(\mathbb{Z}_N)$ heißt meßbar bzgl. $\mathcal{B}$, falls alle $\{f^{-1}(\{x\});\; x \in \mathbb{R}\}$ in $\mathcal{B}$ liegen, d. h. f ist konstant auf jedem Atom von $\mathcal{B}$*
- *$L^q(\mathcal{B}) \subseteq L^q(\mathbb{Z}_N)$ sind die $\mathcal{B}$-meßbaren Funktionen mit L^q-Norm*
- *Konditioneller Erwartungsoperator: $\mathbb{E}(f|\mathcal{B})(x) := \mathbb{E}(f(y)|y \in \mathcal{B}(x))$, wobei $\mathcal{B}(x)$ das Atom bezeichnet, das x enthält. Ist $\mathcal{B}'$ eine Subalgebra von $\mathcal{B}$, so folgt $\mathbb{E}(\mathbb{E}(f|\mathcal{B})|\mathcal{B}') = \ldots$*

- *Sind $\mathcal{B}_1, \dots, \mathcal{B}_K$ σ-Algebren, so ist $\mathcal{B}_1 \vee \dots \vee \mathcal{B}_K$ die davon erzeugte σ-Algebra, d. h. die Atome davon sind die Schnitte der Atome in $\mathcal{B}_1, \dots, \mathcal{B}_K$. (Für $K = 0$ ist diese $= \{\emptyset, \mathbb{Z}_N\}$.)*

Proposition 6.2. *(Jede Funktion erzeugt eine σ-Algebra) Sei ν k-pseudozufällig, $0 < \varepsilon < 1$, $0 < \eta < 1/2$, $G \in L^\infty(\mathbb{Z}_N)$ Funktion mit Werten in $I := [-2^{2^{k-1}}, 2^{2^{k-1}}] \subseteq \mathbb{R}$. Dann gibt es eine σ-Algebra $\mathcal{B}_{\varepsilon,\eta}(G)$ mit:*

- *Für jede σ-Algebra $\mathcal{B}$ gilt*

$$\|G - \mathbb{E}(G|\mathcal{B} \vee \mathcal{B}_{\varepsilon,\eta}(G))\|_{L^\infty(\mathbb{Z}_N)} \leq \varepsilon.$$

- *$\mathcal{B}_{\varepsilon,\eta}(G)$ wird von höchstens $O(1/\varepsilon)$ vielen Atomen erzeugt.*
- *Ist A ein Atom in $\mathcal{B}_{\varepsilon,\eta}(G)$, so gibt es eine stetige Funktion $\Psi_A : I \to [0,1]$ so daß*

$$\|(\mathbf{1}_A - \Psi_A(G)) \cdot (\nu + 1)\|_{L^1(\mathbb{Z}_N)} = O(\eta).$$

  Weiter: Ψ_A liegt in fester, kompakter Menge $E = E_{\varepsilon,\eta}$ von $C^0(I)$ (unabhängig von F, ν, N, oder A).

Beweis:

Es gilt

$$\int_0^1 \sum_{n\in\mathbb{Z}} \mathbb{E}\big(\mathbf{1}_{G(x)\in[\varepsilon(n-\eta+\alpha),\varepsilon(n+\eta+\alpha)]}(\nu(x)+1) \;\big|\; x \in \mathbb{Z}_N\big)\, d\alpha = 2\eta\mathbb{E}(\nu(x)+1|x \in \mathbb{Z}_N) = O(\eta),$$

also gibt es nach dem Schubfachprinzip ein $0 \leq \alpha \leq 1$ mit

$$\sum_{n\in\mathbb{Z}} \mathbb{E}\big(\mathbf{1}_{G(x)\in[\varepsilon(n-\eta+\alpha),\varepsilon(n+\eta+\alpha)]}(\nu(x)+1) \;\big|\; x \in \mathbb{Z}_N\big) = O(\eta). \qquad (*)$$

Nun sei $\mathcal{B}_{\varepsilon,\eta}(G)$ die σ-Algebra, dessen Atome die Mengen $G^{-1}([\varepsilon(n+\alpha), \varepsilon(n+1+\alpha)))$ für $n \in \mathbb{Z}$ sind. Da die Intervalle $[\varepsilon(n+\alpha), \varepsilon(n+1+\alpha))$ die reelle Achse aufteilen, ist diese wohldefiniert. Auf einem Atom von $\mathcal{B} \vee \mathcal{B}_{\varepsilon,\eta}(G)$ hat also G Werte in einem Intervall der Länge ε, so daß (i) folgt.

Zu (iii): Sei $A := G^{-1}([\varepsilon(n+\alpha), \varepsilon(n+1+\alpha)))$ ein nichtleeres Atom. Da G Werte in I annimmt, gilt $n = O(1/\varepsilon)$, da A sonst leer wäre; damit folgt bereits (ii).

Sei nun $\psi_\eta : \mathbb{R} \to [0,1]$ eine feste stetige Ausschneidefunktion mit

$$\psi_\eta(x) = \begin{cases} 1, & x \in [\eta, 1-\eta], \\ 0, & x \notin [-\eta, 1+\eta] \end{cases},$$

und setze $\Psi_A(x) := \psi_\eta(\frac{x}{\varepsilon} - n - \alpha)$. Dann folgt mit (*) die Abschätzung in (iii). Werden außerdem alle Atome A durchlaufen, liegen die Ψ_A in einer kompakten Teilmenge $E_{\varepsilon,\eta}$ von $C^0(I)$, da n und α beschränkt. □

Nun betrachten wir für G Gowers-antiuniforme Basisfunktionen (die Atome der zugehörigen σ-Algebra werden als „verallgemeinerte Bohrmengen“ betrachtet.

Proposition 6.3. *Sei ν k-pseudozufällig, $K \geq 1$, $\mathcal{D}F_1, \ldots, \mathcal{D}F_K \in L^\infty(\mathbb{Z}_N)$ seien Gowers antiuniforme Basisfunktionen, $0 < \varepsilon < 1$, $0 < \eta < 1/2$, $\mathcal{B}_{\varepsilon,\eta}(\mathcal{D}F_j)$, $j = 1, \ldots, K$, wie in Proposition 6.2. Sei $\mathcal{B} := \mathcal{B}_{\varepsilon,\eta}(\mathcal{D}F_1) \vee \ldots \vee \mathcal{B}_{\varepsilon,\eta}(\mathcal{D}F_K)$. Ist $\eta < \eta_0(\epsilon, K)$ hinreichend klein und $N > N_0(\epsilon, K, \eta)$ hinreichend groß, so gilt*

$$\|\mathcal{D}F_j - \mathbb{E}(\mathcal{D}F_j|\mathcal{B})\|_{L^\infty(\mathbb{Z}_N)} \leq \varepsilon \text{ für alle } 1 \leq j \leq K.$$

Weiter existiert eine Menge Ω in $\mathcal{B}$ so daß

$$\mathbb{E}((\nu+1)\mathbf{1}_\Omega) = O_{K,\varepsilon}(\eta^{1/2})$$

und

$$\|(1-\mathbf{1}_\Omega)\cdot\mathbb{E}(\nu-1|\mathcal{B})\|_{L^\infty(\mathbb{Z}_N)} = O_{K,\varepsilon}(\eta^{1/2})$$

gilt.

Beweis: Die erste Abschätzung folgt direkt aus Prop. 6.2(i). Zum Beweis der Existenz von Ω: $\mathcal{B}$ wird von $O_{K,\varepsilon}(1)$ vielen Atomen erzeugt, da jedes $\mathcal{B}_{\varepsilon,\eta}(\mathcal{D}F_j)$ von $O(1/\varepsilon)$ vielen Atomen erzeugt wird nach Prop. 6.2(ii).

Def.: Ein Atom A von $\mathcal{B}$ heißt klein, falls $\mathbb{E}((\nu+1)\mathbf{1}_A) \leq \eta^{1/2}$, und sei Ω die Vereinigung aller kleinen Atome. Also gilt $\mathbb{E}(\nu+1)1_\Omega = O_{K,\varepsilon}(1)\eta^{1/2}$.

Nun zur letzten Abschätzung der Proposition. Dafür genügt es, zu zeigen:

$$\frac{\mathbb{E}((\nu-1)\mathbf{1}_A)}{\mathbb{E}(\mathbf{1}_A)} = \mathbb{E}(\nu-1|A) \stackrel{!}{=} o_{K,\varepsilon,\eta}(1) + O_{K,\varepsilon}(\eta^{1/2})$$

für alle A, die nicht klein sind. Ist A nicht klein, so gilt

$$\mathbb{E}((\nu-1)\mathbf{1}_A) + 2\mathbb{E}(\mathbf{1}_A) = \mathbb{E}((\nu+1)\mathbf{1}_A) \geq \eta^{1/2}.$$

Daher genügt es wiederum, zu zeigen, daß

$$\mathbb{E}((\nu-1)\mathbf{1}_A) = o_{K,\varepsilon,\eta}(1) + O_{K,\varepsilon}(\eta).$$

Andererseits gilt $A = A_1 \cap \ldots \cap A_K$, wobei A_j ein Atom von $\mathcal{B}_{\varepsilon,\eta}(\mathcal{D}F_j)$ ist. Mit Prop. 6.2(iii) und Induktion folgt dann die Existenz einer stetigen Funktion $\Psi_A : I^K \to [0,1]$ mit

$$\|(\nu+1)(\mathbf{1}_A - \Psi_A(\mathcal{D}F_1, \ldots, \mathcal{D}F_K))\|_{L^1(\mathbb{Z}_N)} = O_K(\eta),$$

insb.

$$\|(\nu-1)(\mathbf{1}_A - \Psi_A(\mathcal{D}F_1, \ldots, \mathcal{D}F_K))\|_{L^1(\mathbb{Z}_N)} = O_K(\eta). \qquad (+)$$

Dabei gilt: Ψ_A liegt in einer kompakten Menge $E_{\varepsilon,\eta,K}$ von $\mathcal{C}^0(I^K)$ nach Prop. 6.2 (iii, Zusatz), so daß wegen Prop. 5.2 gilt:

$$\mathbb{E}((\nu-1)\Psi_A(\mathcal{D}F_1, \ldots, \mathcal{D}F_K))) = o_{K,\varepsilon,\eta}(1)$$

für $N \geq N_0(K, \varepsilon, \eta)$. Also folgt mit der Dreiecksungleichung daraus und aus $(+)$ die Behauptung. □

7 Ein Furstenberg-Turm und der Beweis des Satzes von Szemerédi-Green-Tao

Wir gehen aus von folgendem Zerlegungssatz:

Proposition 7.1. *(Verallgemeinerter Koopman-von Neumann Struktursatz)*

Sei ν k-pseudozufällig, $f \in L^1(\mathbb{Z}_N)$ nichtnegativ mit $0 \leq f(x) \leq \nu(x)$ für alle $x \in \mathbb{Z}_N$, $0 < \varepsilon \ll 1$ klein, $N > N_0(\varepsilon)$ hinreichend groß. Dann existiert eine σ-Algebra $\mathcal{B}$ und eine Ausnahmemenge $\Omega \in \mathcal{B}$ mit:

(i) $\mathbb{E}(\nu 1_\Omega) = o_\varepsilon(1)$ *„Kleinheitsbedingung“*

(ii) $\|(1-1_\Omega)\mathbb{E}(\nu - 1|\mathcal{B})\|_{L^\infty} = o_\varepsilon(1)$ *„ν ist außerhalb Ω gleichmäßig verteilt“*

(iii) $\|(1-1_\Omega)(f - \mathbb{E}(f|\mathcal{B}))\|_{U^{k-1}} \leq \varepsilon^{1/2^k}$ *„f ist uniform“*

Bemerkung: Nach dieser Proposition zerlegt sich f additiv zu $f = f_U + f_{U^\perp} + 1_\Omega f$, bestehend aus einer uniformen Funktion

$$f_U := (1-1_\Omega)(f - \mathbb{E}(f|\mathcal{B})),$$

einer antiuniformen Funktion

$$f_{U^\perp} = (1-1_\Omega)\mathbb{E}(f|\mathcal{B})$$

und einer Fehlerfunktion $1_\Omega f$.

Beweis von Satz 3 (Szemerédi-Green-Tao) mit Proposition 7.1:

Seien f und δ wie in Satz 3 gegeben, sei $0 < \varepsilon \ll \delta$ fest (wird später gewählt). Sei $\mathcal{B}$ und $\Omega \in \mathcal{B}$ wie in der Zerlegung von Proposition 7.1 gegeben, weiter f_U und $f_{U^\perp}$ zu f wie oben definiert.

Dann gilt wegen der Meßbarkeit von Ω, $f \leq \nu$ und der Voraussetzung $\mathbb{E}(f) \geq \delta$ und 7.1.(i):

$$\mathbb{E}(f_{U^\perp}) = \mathbb{E}((1-1_\Omega)f) \geq \mathbb{E}(f) - \mathbb{E}(\nu 1_\Omega) \geq \delta - o_\varepsilon(1).$$

Wegen 7.1(ii) ist $f_{U^\perp}$ beschränkt durch $1+o_\varepsilon(1)$, da $f_{U^\perp} \leq (1-1_\Omega)\mathbb{E}(f-1|\mathcal{B})+1 \leq o_\varepsilon(1)+1$. Da f nichtnegativ, ist auch $f_{U^\perp}$ nichtnegativ. Daher läßt sich Satz 2' auf $f_{U^\perp} - o_\varepsilon(1)$ anwenden, und es folgt:

$$\mathbb{E}(f_{U^\perp}(x)f_{U^\perp}(x+r)\cdots f_{U^\perp}(x+(k-1)r)|x,r) \geq c(k,\delta) - o_{k,\delta,\varepsilon}(1) \qquad (+)$$

Wegen 7.1(iii) ist $\|f_U\|_{U^{k-1}} \leq \varepsilon^{1/2^k}$.

Nun ist $(1-1_\Omega)f$ punktweise beschränkt durch ν, und $f_{U^\perp}$ ebenso durch $1+o_\varepsilon(1)$, also ist f_U punktweise beschränkt durch $\nu + 1 + o_\varepsilon(1)$ (denn $f_U = (1-1_\Omega)f - f_{U^\perp}$). Damit kann der verallgemeinerte von Neumann-Satz, Proposition 4.3, eingesetzt werden, nach diesem folgt, daß gilt:

$$\mathbb{E}(f_0(x)f_1(x+r)\cdots f_{k-1}(x+(k-1)r)|x,r) = O(\varepsilon^{1/2^k}), \qquad (*)$$

wobei jedes f_j gleich f_U oder $f_{U^\perp}$ ist, aber mindestens eines der f_j gleich f_U ist. Damit besteht (*) also aus $2^k - 1$ vielen Abschätzungen, für jede mögliche Kombination der f_j (außer der in (+)) also eine.

Alle diese Abschätzungen werden nun aufaddiert; mit $\tilde{f} := f_U + f_{U^\perp}$ erhält man also

$$\mathbb{E}(\tilde{f}(x)\tilde{f}(x+r)\cdots\tilde{f}(x+(k-1)r)|x,r) \geq c(k,\delta) - O(\varepsilon^{1/2^k}) - o_{k,\delta,\varepsilon}(1)$$

Da $0 \leq \tilde{f} = (1-1_\Omega)f \leq f$ ist, folgt

$$\mathbb{E}(f(x)f(x+r)\cdots f(x+(k-1)r|x,r) \geq c(k,\delta) - O(\varepsilon^{1/2^k}) - o_{k,\delta,\varepsilon}(1).$$

Da ε beliebig klein gewählt werden kann, folgt die Behauptung. □

Bleibt nun der **Beweis des Struktursatzes, Prop. 7.1.** Hierfür wird die σ-Algebra $\mathcal{B}$ und die Ausnahmemenge Ω iterativ konstruiert. Man startet mit $\mathcal{B} = \{\emptyset, \mathbb{Z}_N\}$. Ist $f - \mathbb{E}(f|\mathcal{B})$ schon uniform (d.h. gilt 7.1.(iii)), so ist man fertig, und ansonsten findet man eine geeignete antiuniforme Basisfunktion $\mathcal{D}F$ und nimmt dann $\mathcal{B}_{\varepsilon,\eta}(\mathcal{D}F)$ zu $\mathcal{B}$ hinzu, wobei aber die Ausnahmemenge nach Prop. 7.2 vergrößert wird. Dies wird solange durchgeführt bis $f - \mathbb{E}(f|\mathcal{B})$ genügend uniform ist. Dabei zeigt Prop. 7.2, daß die L^2-Norm von $\mathbb{E}(f|\mathcal{B})$ (außerhalb Ω) schrittweise wächst, aber $\mathbb{E}(f|\mathcal{B})$ außerhalb Ω gleichmäßig beschränkt bleibt, so daß der Algorithmus – rechtzeitig – abbrechen muß. Wir präzisieren die Idee im folgenden. Dafür werden die Abschätzungen (i) und (ii) in Proposition 7.1. in jedem Schritt ersetzt durch

$$(i)_K \qquad \mathbb{E}((\nu+1)1_{\Omega_K}) = O_{K,\varepsilon}(\eta^{1/2})$$
$$(ii)_K \qquad \|(1-1_{\Omega_K})\mathbb{E}(\nu-1|\mathcal{B}_K)\|_{L^\infty} = O_{K,\varepsilon}(\eta^{1/2})$$

Diese Eigenschaften bleiben in jedem Iterationsschritt erhalten laut Proposition 7.2.

Konstruktion von $\mathcal{B}$ und Ω:

Sei $0 < \eta \ll \varepsilon$, K_0 die kleinste natürliche Zahl $> 2^{2^k}/\varepsilon + 1$, und sei $0 \leq K \leq K_0$. Konstruiert wird eine Folge von antiuniformen Hilfsfunktionen $\mathcal{D}F_1, \ldots, \mathcal{D}F_K$ auf $\mathbb{Z}_N$, Ausnahmemengen $\Omega_0 \subseteq \Omega_1 \subseteq \cdots \subseteq \Omega_K \subseteq \mathbb{Z}_N$, und eine aufsteigende Folge von σ-Algebren $\mathcal{B}_0 \subseteq \cdots \subseteq \mathcal{B}_K$ wie folgt:

Schritt 0: Initialisiere $K := 0$, $\Omega_0 := \emptyset$.

Schritt 1: Definiere $\mathcal{B}_K := \mathcal{B}_{\varepsilon,\eta}(\mathcal{D}F_1) \vee \cdots \vee \mathcal{B}_{\varepsilon,\eta}(\mathcal{D}F_K)$ (mit den σ-Algebren zu den $\mathcal{D}F_j$ gemäß Proposition 6.2). Setze $F_{K+1} := (1-1_{\Omega_K})(f - \mathbb{E}(f|\mathcal{B}_K))$. (Dabei wird $\mathcal{B}_0 = \{\emptyset, \mathbb{Z}_N\}$ und $F_1 := f - \mathbb{E}(f)$ gesetzt, so daß $(i)_0$ und $(ii)_0$ schon gelten.)

Schritt 2: Falls $\|F_{K+1}\|_{U^k-1} \leq \varepsilon^{1/2^k}$, d.h. (iii) gilt, setze $\Omega := \Omega_K$, $\mathcal{B} := \mathcal{B}_K$ und breche den Algorithmus erfolgreich ab.

Schritt 3: Falls $\|F_{K+1}\|_{U^{k-1}} > \varepsilon^{1/2^k}$, definiere $\mathcal{B}_{K+1} := \mathcal{B}_K \vee \mathcal{B}_{\varepsilon,\eta}(\mathcal{D}F_{K+1})$. Nach Proposition 7.2 existiert eine Ausnahmemenge $\Omega_{K+1} \supseteq \Omega_K$, mit der $(i)_{K+1}$ und $(ii)_{K+1}$, sowie die „Energiezunahmeeigenschaft“ gilt.

Schritt 4: Erhöhe K auf $K+1$. Falls $K > K_0$, breche den Algorithmus mit Fehler ab, ansonsten gehe zu Schritt 1.

Mit dieser Konstruktion und der Verwendung von Proposition 7.2, die wir gleich im Anschluß zeigen, beweisen wir nun Proposition 7.1:

Endet der Algorithmus erfolgreich in Schritt 2, so ist $K \leq K_0$. Dann wählen wir η klein so, daß aus $(i)_K$ und $(ii)_K$ die ursprünglich zu zeigenden Abschätzungen (i) und (ii) folgen. Die Abschätzung (iii) gilt wegen Eintretens von Schritt 2.

Es bleibt zu zeigen, daß ein Abbruch in Schritt 4 nicht eintreten kann: Falls doch, so betrachte man die K_0-te Iteration davor.

Wir untersuchen nun die „Energien“

$$E_K := \|(1 - 1_{\Omega_K})\mathbb{E}(f|\mathcal{B}_K)\|^2_{L^2(\mathbb{Z}_N)}, \qquad 0 \leq K \leq K_0 + 1.$$

Die Energiezunahmeeigenschaft von Prop. 7.2 besagt, daß $E_{K+1} \geq E_K + 2^{-2^k+1}\varepsilon$ für $0 \leq K \leq K_0$ gilt. Andererseits ist wegen Prop. 7.2 (iii) aber $0 \leq E_K \leq 1 + O_{K,\varepsilon}(\eta^{1/2})$ für alle $0 \leq K \leq K_0$.

Ist $\eta < \eta_0(K, \varepsilon)$ hinreichend klein, widersprechen sich beide Abschätzungen aber gerade für $K = K_0$. Dieser Widerspruch zeigt, daß ein Abbruch in Schritt 4 doch nicht erfolgen kann. □

Damit bleibt zum Beweis noch die Proposition 7.2 übrig, die wir jetzt angehen.

Proposition 7.2. *(Iterativer Schritt)*

Sei ν k-pseudozufällig, $f \in L^1(\mathbb{Z}_N)$, $0 \leq f(x) \leq \nu(x)$ für alle $x \in \mathbb{Z}_N$, $0 < \eta \ll \varepsilon \ll 1$ klein, $K \geq 0$ ganz, sei $\eta < \eta_0(\varepsilon, K)$, $N > N_0(\varepsilon, K, \eta)$, seien $F_1, \ldots, F_K \in L^1(\mathbb{Z}_N)$ Funktionen mit

$$|F_j(x)| \leq (1 + O_{K,\varepsilon}(\eta^{1/2}))(\nu(x) + 1)$$

für alle j und x. Sei $\mathcal{B}_K := \mathcal{B}_{\varepsilon,\eta}(\mathcal{D}F_1) \vee \cdots \vee \mathcal{B}_{\varepsilon,\eta}(\mathcal{D}F_K)$ mit σ-Algebren wie in Prop. 6.2. Weiter gebe es eine Menge $\Omega_K \subseteq \mathbb{Z}_N$ mit $(i)_K$ und $(ii)_K$.

Sei $F_{K+1} := (1 - 1_{\Omega_K})(f - \mathbb{E}(f|\mathcal{B}_K))$, und gelte $\|F_{K+1}\|_{U^{k-1}} > \varepsilon^{1/2^k}$. Dann gilt:

$$(iv) \quad \|(1 - 1_{\Omega_K})\mathbb{E}(f|\mathcal{B}_K)\|_{L^\infty(\mathbb{Z}_N)} \leq 1 + O_{K,\varepsilon}(\eta^{1/2})$$
$$(v) \quad |F_{K+1}(x)| \leq (1 + O_{K,\varepsilon}(\eta^{1/2}))(\nu(x) + 1).$$

Ist $\mathcal{B}_{K+1} := \mathcal{B}_K \vee \mathcal{B}_{\varepsilon,\eta}(\mathcal{D}F_{K+1})$, so gibt es weiter eine Menge $\Omega_{K+1} \supseteq \Omega_K$ mit $(i)_{K+1}$, $(ii)_{K+1}$, und der Energiezunahmeeigenschaft $E_{K+1} \geq E_K + 2^{-2^k+1}\varepsilon$.

Beweis von Proposition 7.2:

Da $f \leq \nu$, folgt aus $(ii)_K$ bereits (iv).

Aus (iv) und der Definition von F_{K+1} folgt bereits (v).

Daher sind $\mathcal{D}F_1, \ldots, \mathcal{D}F_{K+1}$ Gowers antiuniforme Basisfunktionen (bis auf den multiplikativen Faktor $(1 + O_{K,\varepsilon}(\eta^{1/2}))$.

Aus Lemma 5.1 folgt dann, daß $\|\mathcal{D}F_j\|_{L^\infty} \leq 2^{2^{k-1}-1} + O_{K,\varepsilon}(\eta^{1/2})$ für alle j gilt, wenn N groß ist (nach Ausskalieren des Faktors $(1 + O_{K,\varepsilon}(\eta^{1/2}))$.

Nach Proposition 6.3 existiert somit eine Menge $\tilde{\Omega} \in \mathcal{B}_{K+1}$ mit $\mathbb{E}((\nu+1)1_{\tilde{\Omega}}) = O_{K,\varepsilon}(\eta^{1/2})$ und $\|(1-1_{\tilde{\Omega}})\mathbb{E}(\nu-1|B_{K+1})\|_{L^\infty} = O_{K,\varepsilon}(\eta^{1/2})$.

Wir setzen dann $\Omega_{K+1} := \Omega_K \cup \tilde{\Omega}$, so daß damit also $(i)_{K+1}$ und $(ii)_{K+1}$ gilt.

Zu zeigen bleibt damit die Energiezunahmeeigenschaft: Zur einfacheren Notation schreiben wir hier Ω für Ω_K, Ω' für Ω_{K+1}, $\mathcal{B}$ für $\mathcal{B}_K$, $\mathcal{B}'$ für $\mathcal{B}'_{K+1}$, F für F_K und F' für F_{K+1}.

Aus der Voraussetzung $\|F'\|_{U^{k-1}} > \varepsilon^{1/2^k}$ folgern wir, daß

$$|\langle (1-1_\Omega)(f-\mathbb{E}(f|\mathcal{B})), \mathcal{D}F'\rangle| = |\langle F', \mathcal{D}F'\rangle| = \|F'\|_{U^{k-1}}^{2^{k-1}} > \varepsilon^{1/2}.$$

Andererseits gilt

$$\begin{aligned}&|\langle (1_{\Omega'}-1_\Omega)(f-\mathbb{E}(f|\mathcal{B})), \mathcal{D}F'\rangle| \leq \|\mathcal{D}F'\|_{L^\infty}\mathbb{E}((1_{\Omega'}-1_\Omega)|f-\mathbb{E}(f|\mathcal{B})|)\\ &= O_{K,\varepsilon}(\eta^{1/2})\mathbb{E}((1_{\Omega'}-1_\Omega)(\nu+1)) = O_{K,\varepsilon}(\eta^{1/2})\end{aligned}$$

wegen obiger Abschätzung für $\|\mathcal{D}F_j\|_{L^\infty}$, sowie

$$\begin{aligned}&|\langle (1-1_{\Omega'})(f-\mathbb{E}(f|\mathcal{B})), \mathcal{D}F' - \mathbb{E}(\mathcal{D}F'|\mathcal{B}')\rangle|\\ &\leq \|\mathcal{D}F' - \mathbb{E}(\mathcal{D}F'|\mathcal{B}')\|_{L^\infty}\cdot\mathbb{E}((1-1_{\Omega'})|f-\mathbb{E}(f|\mathcal{B})|)\\ &\leq O(\varepsilon)\mathbb{E}((1-1_{\Omega'})(\nu+1)) = O(\varepsilon)\end{aligned}$$

wegen der entsprechenden Abschätzung in Proposition 6.2.

Mit der Dreiecksungleichung lassen sich alle drei vorigen Ergebnisse zusammensetzen zu der Abschätzung

$$|\langle (1-1_{\Omega'})(f-\mathbb{E}(f|\mathcal{B})), \mathbb{E}(\mathcal{D}F'|\mathcal{B}')\rangle| \geq \varepsilon^{1/2} - O_{K,\varepsilon}(\eta^{1/2}) - O(\varepsilon).$$

In dieser läßt sich nun wegen der Meßbarkeit der Funktionen $1-1_{\Omega'}$ und $\mathbb{E}(\mathcal{D}F'|\mathcal{B}')$ bzgl. $\mathcal{B}'$ die Funktion f durch $\mathbb{E}(f|\mathcal{B}')$ ersetzen, und wir erhalten

$$|\langle (1-1_{\Omega'})(\mathbb{E}(f|\mathcal{B}')-\mathbb{E}(f|\mathcal{B})), \mathbb{E}(\mathcal{D}F'|\mathcal{B}')\rangle| \geq \varepsilon^{1/2} - O_{K,\varepsilon}(\eta^{1/2}) - O(\varepsilon).$$

Mit der Cauchy-Schwarz-Ungleichung, die wir auf die linke Seite anwenden können, erhalten wir wieder mit der bekannten Abschätzung von $\|\mathcal{D}F'\|_{L^\infty}$, daß

$$\|(1-1_{\Omega'})(\mathbb{E}(f|\mathcal{B}')-\mathbb{E}(f|\mathcal{B}))\|_{L^2} \geq 2^{-2^{k-1}+1}\varepsilon^{1/2} - O_{K,\varepsilon}(\eta^{1/2}) - O(\varepsilon).$$

Außerhalb von Ω ist $\mathbb{E}(f|\mathcal{B}) \leq 1 + O_{K,\varepsilon}(\eta^{1/2})$ wegen (iv), also ist für kleines η:

$$\|(1_{\Omega'}-1_\Omega)\mathbb{E}(f|\mathcal{B})\|_{L^2}^2 \leq 2\|1_{\Omega'}-1_\Omega\|_{L^2}^2 \leq 2\|1_{\Omega'}-1_\Omega\|_{L^1} \leq \mathbb{E}(1_{\Omega'}) = O_{K,\varepsilon}(\eta^{1/2})$$

nach $(i)_K$, welches für $\nu+1$ formuliert war, so daß deshalb auch $\mathbb{E}(1_{\Omega'})$ abgeschätzt werden kann.

Damit genügt es nun, die Behauptung

$$\|(1-1_{\Omega'})\mathbb{E}(f|\mathcal{B}')\|_{L^2}^2 \overset{!}{\geq} \|(1-1_{\Omega'})\mathbb{E}(f|\mathcal{B})\|_{L^2}^2 + 2^{-2^k+2}\varepsilon - O_{K,\varepsilon}(\eta^{1/2}) - O(\varepsilon)$$

zu zeigen, wobei wir dann die O-Terme mit dem Summanden $2^{-2^k+2}\varepsilon$ zusammen abschätzen, um die behauptete Energiezunahme zu erhalten.

Wir schreiben hier die linke Seite als

$$\begin{aligned}&= \|(1-1_{\Omega'})\mathbb{E}(f|\mathcal{B}) + (1-1_{\Omega'})(\mathbb{E}(f|\mathcal{B}') - \mathbb{E}(f|\mathcal{B}))\|_{L^2}^2\\ &= \|(1-1_{\Omega'})\mathbb{E}(f|\mathcal{B})\|_{L^2}^2 + \|(1-1_{\Omega'})(\mathbb{E}(f|\mathcal{B}') - \mathbb{E}(f|\mathcal{B}))\|_{L^2}^2\\ &+ 2\langle(1-1_{\Omega'})\mathbb{E}(f|\mathcal{B}), (1-1_{\Omega'})(\mathbb{E}(f|\mathcal{B}') - \mathbb{E}(f|\mathcal{B}))\rangle\end{aligned}$$

unter Verwendung des Kosinussatzes $\|x+y\|_2^2 = \|x\|_2^2 + \|y\|_2^2 + 2\langle x, y\rangle$.

Daher genügt zu zeigen, daß der Skalarproduktausdruck $\stackrel{!}{=} O_{K,\varepsilon}(\eta^{1/2})$ ist, welcher sich auch als $\langle(1-1_{\Omega'})\mathbb{E}(f|\mathcal{B}), \mathbb{E}(f|\mathcal{B}') - \mathbb{E}(f|\mathcal{B})\rangle$ schreiben läßt.

Es gilt nun: $\langle(1-1_{\Omega})\mathbb{E}(f|\mathcal{B})$ ist meßbar bzgl. $\mathcal{B}$ und ist deswegen orthogonal zu $\mathbb{E}(f|\mathcal{B}') - \mathbb{E}(f|\mathcal{B})$, da $\mathcal{B}$ eine Unter-σ-Algebra von $\mathcal{B}'$ ist.

Also ist der Skalarproduktausdruck

$$\begin{aligned}&= \langle(1_{\Omega'} - 1_{\Omega})\mathbb{E}(f|\mathcal{B}), \mathbb{E}(f|\mathcal{B}') - \mathbb{E}(f|\mathcal{B})\rangle\\ &= \langle(1_{\Omega'} - 1_{\Omega})\mathbb{E}(f|\mathcal{B}), f - \mathbb{E}(f|\mathcal{B})\rangle,\end{aligned}$$

wobei verwendet wurde, daß $(1_{\Omega'} - 1_{\Omega})\mathbb{E}(f|\mathcal{B})$ meßbar bzgl. $\mathcal{B}'$ ist. Da nun $\mathbb{E}(f|B) \leq 2$ ist für kleines η und $x \notin \Omega$ wegen (iv), ist dies

$$\begin{aligned}&\leq 2\mathbb{E}((1_{\Omega'} - 1_{\Omega})|f - \mathbb{E}(f|\mathcal{B})|)\\ &\leq 2\mathbb{E}((1_{\Omega'} - 1_{\Omega})(\nu + \mathbb{E}(\nu|\mathcal{B})|)\\ &\leq 4\mathbb{E}((1_{\Omega'} - 1_{\Omega})(\nu+1)) = O_{K,\varepsilon}(\eta^{1/2})\end{aligned}$$

wegen Eigenschaft $(i)_{K+1}$. Damit ist der Beweis beendet. □

---

8 Ein pseudozufälliges Maß, das $\mathbb{P}$ majorisiert

Für den zweiten Teil, dem Beweis von Satz 1 unter Verwendung des Satzes 3 (von Szemerédi-Green-Tao), benötigen wir erst ein paar zahlentheoretische Vorbereitungen:

Definition 8.1. *Zahlentheoretische Funktion:* $f : \mathbb{N} \to \mathbb{C}$, *Menge:* $\mathcal{F} := \{f : \mathbb{N} \to \mathbb{C}\}$,

$f \in \mathcal{F}$ *multiplikativ:* $\forall n, m \in \mathbb{N}, (n,m) = 1 : f(nm) = f(n)f(m)$

$f \in \mathcal{F}$ *additiv:* $\forall n, m \in \mathbb{N}, (n,m) = 1 : f(nm) = f(n) + f(m)$ *(z. B.* $f = \log$*).*

(Zahlentheoretische) Faltung $*$*: Für* $f, g \in \mathcal{F}$ *ist* $f * g \in \mathcal{F}$ *definiert durch*

$$f * g(n) := \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big)$$

Es gilt: Sind f, g multiplikativ, dann auch $f * g$.

Satz 8.2. *(1)* $(\mathcal{F}, *)$ *ist eine abelsche Halbgruppe mit neutralem Element* ε*, wo* $\varepsilon(n) := \lfloor \frac{1}{n} \rfloor = \begin{cases} 1, & n = 1, \\ 0 & n > 1 \end{cases}$

(2) $\mathcal{Z} := \{f \in \mathcal{F}; f(1) \neq 0\}$ *ist mit* $*$ *eine abelsche Gruppe mit neutralem Element* ε

(3) $\mathcal{M} := \{f \in \mathcal{Z}; f\,multiplikativ\}$ *ist eine Untergruppe von* $(\mathcal{Z}, *)$.

(4) Das Faltungsinverse von $\mathbf{1}$, $\mathbf{1}(n) := 1$, *ist die Möbiusfunktion*

$$\mu(n) := \begin{cases} 1, & n = 1, \\ 0, & n \text{ durch Quadratzahl teilbar}, \\ (-1)^r, & n = p_1 \cdots p_r \text{ sonst} \end{cases}$$

Es gilt also $\mu * \mathbf{1} = \varepsilon$ *bzw.*

$$\sum_{d|n} \mu(d) = \varepsilon(n).$$

Um die letztere Formel zu zeigen, genügt es wegen der Multiplikativität der beiden Formelseiten, die Gleichheit auf Primpotenzen zu checken, und das geht ganz leicht. Die Invertierbarkeit bekommt man durch rekursives Auflösen nach den $g(n)$, wenn g die Inverse von f bezeichnet; diese ist dann auch multiplikativ, wenn f es war.

Möbiussche Umkehrformel: $F = f * \mathbf{1} \Leftrightarrow f = F * \mu$

Diese Formel erlaubt es, nach f „aufzulösen".

Beispiele für wichtige zahlentheoretische Funktionen:

(1) **Eulersche φ-Funktion:** $\varphi(n) := \#\{a \in \mathbb{N}; 1 \leq a \leq n, (a, n) = 1\}$

(2) **von Mangoldt-Funktion** $\Lambda : \mathbb{N} \to \mathbb{R}^+$, $\Lambda(n) := \begin{cases} \log p, & n = p^m, m \geq 1, \\ 0, & \text{sonst} \end{cases}$

Es gilt: Λ ist weder multiplikativ noch additiv, aber es ist $\Lambda * \mathbf{1} = \log$, d. h. $\sum_{d|n} \Lambda(n) = \log n$. Die Möbius-Umkehrformel zeigt dann, daß $\Lambda(n) = \mu * \log$ gilt, ausgeschrieben:

$$\Lambda(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) = -\sum_{d|n} \mu(d) \log(d).$$

Die letzte Gleichheit erhält man wegen $\log(n/d) = \log(n) - \log(d)$.

Im folgenden bezeichne p immer eine Primzahl $p \in \mathbb{P}$.

Definition 8.3. *Primzahlzählfunktion:* $\pi(x) := \#\{p \leq x; p \in \mathbb{P}\}$

1. Tschebytschev-Fkt.: $\vartheta(x) := \sum_{p \leq x} \log p$

2. Tschebytschev-Fkt.: $\psi(x) := \sum_{p^m \leq x, m \geq 1} \log p$

Der Satz von Tschebytschev (auch Tschebytschev-Ungleichungen genannt) besagt, daß es positive Konstanten $c_1, c_2, c_1', c_2', c_1'', c_2''$ gibt mit

$$\frac{c_1 x}{\log x} < \pi(x) < \frac{c_2 x}{\log x},$$

wofür es auch die äquivalenten Umformulierungen

$$\Leftrightarrow c_1' x < \vartheta(x) < c_2' x \Leftrightarrow c_1'' x < \psi(x) < c_2'' x$$

gibt.

Dabei unterscheiden sich die beiden Tschebytschev-Funktionen kaum voneinander:

Bemerkung: $\psi(x) = \vartheta(x) + O(\sqrt{x})$

Denn:

$$\psi(x) = \sum_{p^m \leq x} \log p = \vartheta(x) + \sum_{\substack{p^m \leq x \\ m \geq 2}} \log p = \vartheta(x) + \sum_{p \leq \sqrt{x}} \log p \, O\Big(\frac{\log x}{\log p}\Big) = \vartheta(x) + O(\sqrt{x})$$

wegen der Tschebytschev-Ungleichungen.

Noch schärfer als diese Ungleichungen ist der **Primzahlsatz** (Beweis geht analytisch). Nach diesem gilt:

$$\pi(x) = \frac{x}{\log x}(1 + o(1)),$$

was auch äquivalent umformuliert werden kann zu

$$\Leftrightarrow \psi(x) = x + o(x) \Leftrightarrow \vartheta(x) = x + o(x),$$

bzw.

$$\frac{1}{x} \sum_{m \leq x} \Lambda(m) = 1 + o(1).$$

Analog zum Primzahlsatz kann man auch den folgenden **Primzahlsatz in Progressionen** beweisen: Ist

$$\pi(x; q, a) := \#\{p \leq x; p \equiv a \ (q)\}$$

für $(a, q) = 1$ die Anzahl der Primzahlen, die in der Restklasse von a mod q liegen, so gilt

$$\pi(x; q, a) = \frac{x}{\varphi(q) \log x}(1 + o_q(1)).$$

Dieses Ergebnis läßt sich äquivalent umformulieren zu der ϑ- bzw. ψ-Version

$$\vartheta(x; q, a) = \frac{x}{\varphi(x)}(1 + o_q(1)) \Leftrightarrow \psi(x; q, a) = \frac{x}{\varphi(x)}(1 + o_q(1)).$$

Zur Anwendung des Satzes von Szemerédi-Green-Tao-Satzes auf $\mathbb{P}$ brauchen wir ein pseudozufälliges Maß ν mit $0 \leq \Lambda(n)c(k) \leq \nu(n)$ für alle $n \in \mathbb{N}$. Wir bemerken, daß Λ nach dem PZS den asymptotischen Mittelwert 1 hat. Die Funktion Λ kann aber nicht als pseudozufälliges Maß genommen werden, da ihre Werte nicht gleichverteilt auf *allen* Restklassen mod q sind; man kann zeigen, daß pseudozufällige Maße diese Eigenschaft haben. Statt dessen beheben Green und Tao das Problem mit dem sogenannten "W-Trick". Dabei ist die Idee, anstelle der primen n einfach die primen $Wn + 1$ zu untersuchen, so daß die Gleichverteilung auf Restklassen damit gewährleistet ist. Dabei muß W geeignet gewählt sein.

Dafür sei $w = w(N)$ eine Funktion, die mit $N \to \infty$ langsam gegen ∞ geht, etwa $w(N) = \log\log N$ ist eine geeignete Wahl; man benötigt, daß $\frac{1}{w(N)} = o(1)$ gilt. Dann setzt man

$$W := \prod_{p \leq w(N)} p,$$

und definiert

$$\tilde{\Lambda}(n) := \begin{cases} \frac{\varphi(W)}{W} \log(Wn+1), & Wn+1 \text{ prim}, \\ 0, & \text{sonst}. \end{cases}$$

Der PZS in Progressionen liefert nun, daß

$$\frac{1}{N} \sum_{n \leq N} \tilde{\Lambda}(n) = \frac{1}{N} \frac{\varphi(W)}{W} \sum_{\substack{p \leq NW+1 \\ p \equiv 1 \ (W)}} \log p = 1 + o(1).$$

Wir werden $\tilde{\Lambda}$ durch ein pseudozufälliges Maß majorisieren:

Proposition 8.1. *Sei $\varepsilon_k := \frac{1}{2^k(k+4)!}$, N hinreichend groß und prim. Dann existiert ein k-pseudozufälliges Maß $\nu : \mathbb{Z}_N \to \mathbb{R}_{\geq 0}$ mit $\nu(n) \geq k^{-1}2^{-k-5}\tilde{\Lambda}(n)$ für alle n mit $\varepsilon_k N \leq n \leq 2\varepsilon_k N$.*

Wir beweisen nun den Satz 1 von Green-Tao unter Annahme von Proposition 8.1 unter Verwendung des Satzes von Szemerédi-Green-Tao:

Sei N groß und prim, und $f \in L^1(\mathbb{Z}_N)$ definiert durch $f(n) := k^{-1}2^{-k-5}\tilde{\Lambda}(n)$ für alle n, $\varepsilon_k N \leq n \leq 2\varepsilon_k N$, und $= 0$ sonst. Es gilt, wieder mit dem PZS in Progressionen:

$$\mathbb{E}(f) = \frac{k^{-1}2^{-k-5}}{N} \sum_{\varepsilon_k N \leq n \leq 2\varepsilon_k N} \tilde{\Lambda} = k^{-1}2^{-k-5}\varepsilon_k(1+o(1)),$$

so daß unter Verwendung von Proposition 8.1 und der Verwendung des Satzes von Szemerédi-Green-Tao nun folgt:

$$\mathbb{E}(f(x)f(x+r)\cdots f(x+(k-1)r) | x, r \in \mathbb{Z}_N) \geq c(k, k^{-1}2^{-k-5}\varepsilon_k) - o(1).$$

Der Fall $r = 0$ liefert nur $O(\frac{1}{N}\log^k N) = o(1)$ zur linken Seite und daher einen vernachlässigbaren Summanden. Weiter ist jede Progression, die links gezählt wird, nicht nur eine in $\mathbb{Z}_N$, sondern auch eine echte AP in $\mathbb{Z}$, da $\varepsilon < 1/k$ und die Elemente der Progression ja in $[\varepsilon_k N, 2\varepsilon_k N]$ liegen. Da die rechte Seite der Abschätzung positiv ist für großes N, folgt die Behauptung aus der Definition von f bzw. $\tilde{\Lambda}$. □

Damit bleibt Proposition 8.1 zu zeigen. Dafür definieren wir das Maß ν jetzt wie folgt:

Definition 8.2: Sei $R \in \mathbb{R}$, dann sei

$$\Lambda_R(n) := \sum_{\substack{d|n, \\ d \leq R}} \mu(d) \log\left(\frac{R}{d}\right) = \sum_{d|n} \mu(d) \log_+\left(\frac{R}{d}\right),$$

wobei $\log_+(x) := \max\{0, \log x\}$ die abgeschnittene log-Funktion ist.

Definition 8.2: Sei $R := N^{k^{-1}2^{-k-4}}$, $\varepsilon_k := 1/(2^k(k+4)!)$, und $\nu : \mathbb{Z}_N \to \mathbb{R}_{\geq 0}$,

$$\nu(n) := \begin{cases} \frac{\varphi(W)}{W}\frac{\Lambda_R(Wn+1)^2}{\log R}, & \varepsilon_k N \leq n \leq 2\varepsilon_k N, \\ 1 & \text{sonst für } 0 \leq n < N. \end{cases}$$

Im folgenden betrachten wir immer dieses Maß ν und zeigen, daß es den erforderlichen Ansprüchen in Proposition 8.1 genügt.

Lemma 8.4: Wir haben $\nu(n) \geq 0$ für alle $n \in \mathbb{Z}_N$ (klar!), sowie $\nu(n) \geq k^{-1}2^{-k-5}\tilde{\Lambda}(n)$ für alle n mit $\varepsilon_k N \leq n \leq 2\varepsilon_k N$ (für großes N in Abhängigkeit von k).

Beweis: Ist $Wn+1$ zusammengesetzt, ist die Abschätzung trivial wegen $\tilde{\Lambda}(Wn+1) = 0$. Sei daher $Wn+1$ prim. Dann ist $Wn+1 > R$ für großes N laut Definition von R. Somit gilt: In

$$\Lambda_R = \sum_{\substack{d \mid Wn+1 \\ d \leq R}} \mu(d)\log(R/d)$$

ist nur der Summand mit $d = 1$ enthalten, also ist $\Lambda_R(Wn+1) = \log R$, d. h. $\nu(n) = \varphi(W)W^{-1}\log R \overset{!}{\geq} k^{-1}2^{-k-5}\tilde{\Lambda}(n)$, Letzteres gilt nach Konstruktion von R und N. □

Einschub (Weihnachtsvorlesung): Der Beweis des Primzahlsatzes

Wir zeigen erst die Äquivalenz der verschiedenen Versionen des PZS, nämlich $\pi(x) = \frac{x}{\log x}(1+o(1)) \Leftrightarrow \vartheta(x) = x + o(x) \Leftrightarrow \psi(x) = x + o(x)$.

Die zweite Äquivalenz ist klar wegen $\psi(x) = \vartheta(x) + O(\sqrt(x)\log x)$, und dies gilt wegen

$$\psi(x) = \vartheta(x) + \sum_{p \leq x^{1/2}} \sum_{k \leq \log x/\log p} \log p = \vartheta(x) + O(\sqrt{x}\log x).$$

Die erste Äquivalenz bekommt man mit partieller Summation: Ist etwa die Asymptotik für ϑ bekannt, folgt die für π wegen

$$\pi(x) = \sum_{p \leq x} \log p \frac{1}{\log p} = \vartheta(x)\frac{1}{\log x} + \int_2^x \vartheta(t)\frac{dt}{t\log^2 t},$$

und dies ist

$$= \frac{x}{\log x} + o(\frac{x}{\log x}) + O(\int_2^x \frac{dt}{\log^2 t}),$$

und der letzte Fehlerterm mit dem Integral ist

$$\int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t} = o(\frac{x}{\log x}).$$

Dabei haben wir partielle Summation benutzt, das ist die Formel

$$\sum_{n\le x} a_n g(n) = (\sum_{n\le x} a_n) g(x) - \int_1^x (\sum_{n\le t} a_n) g'(t) dt,$$

sofern g eine differenzierbare Funktion ist.

Ebenso läßt sich mit partieller Summation auch die Umkehrung zeigen, d. h. aus der π-Asymptotik folgt auch die ψ-Asymptotik.

Die hier vorgestellte Rechnung zeigt auch, daß es für den Beweis der oberen Tschebytschev-Abschätzungen $\vartheta(x) \ll x$, $\psi(x) \ll x$, $\pi(x) \ll x/\log x$ genügt, nur eine davon zu zeigen.

Die für ϑ geht mit einem eleganten Trick nach Erdős:

Es ist

$$\prod_{n<p\le 2n} p \mid \binom{2n}{n} = \frac{(2n)!}{(n!)^2} < (1+1)^{2n} = 4^n,$$

und die linke Seite ist $= \exp(\sum_{n<p\le 2n} \log p) = \exp(\vartheta(2n) - \vartheta(n))$, so daß schon mal $\vartheta(2n) - \vartheta(n) < n \log 4$ folgt. Ist nun $x < 2^k \le 2x$, so folgt

$$\vartheta(x) \le \vartheta(2^k) = \sum_{j=0}^{k-1} (\vartheta(2^{j+1}) - \vartheta(2^j)) < \log 4 \sum_{j=0}^{k-1} 2^j \ll x.$$

Die Brücke zwischen Analysis und Zahlentheorie bilden die L-Reihen bzw. L-Funktionen. Eine Dirichlet-Reihe ist eine Funktion der Form $F(s) := \sum_{n=1}^{\infty} a_n n^{-s}$ für $s \in \mathbb{C}$ und $a_n \in \mathbb{C}$ für alle n. Traditionell schreibt man $s = \sigma + i\tau$.

Eine Dirichlet-Reihe konvergiert entweder nirgends oder überall oder für $\sigma > \sigma_0$ mit einem $\sigma_0 \in \mathbb{R}$, σ_0 heißt Konvergenzabszisse.

Ebenso gilt für die absolute Konvergenz: Eine Dirichlet-Reihe konvergiert entweder nirgends oder überall absolut, oder für $\sigma > \sigma_1$ mit einem $\sigma_1 \in \mathbb{R}$, σ_1 heißt absolute Konvergenzabszisse.

Anders als bei Potenzreihen können sich die Konvergenzbereiche unterscheiden, und es gilt $\sigma_0 \le \sigma_1 \le \sigma_0 + 1$.

Weiter gilt für zwei Dirichlet-Reihen F und G mit den Koeffizienten $a(n)$ und $b(n)$, daß auf dem gemeinsamen Konvergenzbereich gilt: $F(s)G(s) = \sum_{n=1}^{\infty} (a * b)(n) n^{-s}$, wobei hier die zahlentheoretische Faltung $(a * b)(n) = \sum_{d|n} a(d) b(n/d)$ zu nehmen ist. Bei Potenzreihen hat man hingegen die gewöhnliche Cauchy-Faltung.

Die einfachste Dirichlet-Reihe ist die Zeta-Funktion

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s},$$

für diese gilt $\sigma_0 = \sigma_1 = 1$. Sie ist nicht holomorph fortsetzbar in $s = 1$ (dies besagt der Satz von Landau), und offenbar ist $\sum_n 1/n$ die harmonische Reihe, die bekanntermaßen divergiert.

Die für $\sigma > 1$ über die Dirichlet-Reihe definierte ζ-Funktion läßt sich durch eine auf $\{\mathrm{Re}\ s > 0; s \ne 1\}$ definierte Funktion aber holomorph fortsetzen. Dort gilt nämlich

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} - s \int_1^{\infty} B_1(t) t^{-s-1} dt$$

mit dem Bernoulli-Polynom $B_1(t) = t - \lfloor t \rfloor - \frac{1}{2}$.

Der Beweis kann wieder mit der partiellen Summation geführt werden.

Weiter gilt für $\sigma > 1$, daß

$$-\frac{\zeta'}{\zeta}(s) = \sum_n \Lambda(n) n^{-s},$$

denn es gilt

$$-\zeta'(s) = \sum_n \frac{d}{ds} n^{-s} = \sum_n (\log n) n^{-s} = \sum_n (\Lambda * \mathbf{1})(n) n^{-s} = (\sum_n \Lambda(n) n^{-s}) \zeta(s).$$

Mit dieser Formel wird klar, daß Nullstellen von ζ auf $\sigma = 1$ zu Singularitäten der Dirichlet-Reihe mit den Λ als Koeffizienten führen. Divergiert die Reihe, dann hat das Konsequenzen für das Wachstumsverhalten der Koeffizientensumme. Und je besser man die Nullstellenabstinenz von ζ kontrollieren kann, desto bessere Abschätzungen kann man daraus für die Koeffizientensummenfunktion ψ ableiten. Den Primzahlsatz bekommt man dann also mit analytischen Hilfsmitteln, und am einfachsten geht dies mit dem Newmanschen Taubersatz, der genau den PZS in der genannten Form für ψ liefert. Mit der Perronschen Formel bekommt man auch eine genauere quantitative Abschätzung des Fehlerterms im PZS, wenn man über das nullstellenfreie Gebiet von ζ besser bescheid weiß.

Wir begnügen uns hier mit dem Zitieren dieser analytischen Hilfsmittel und zeigen hier lediglich (nach Hadamard und de la Vallée-Poussin):

Fakt: Für $\tau \in \mathbb{R} \setminus \{0\}$ ist $\zeta(1 + i\tau) \neq 0$.

Beweis: Zunächst gilt für beliebiges $\varphi \in \mathbb{R}$, daß

$$3 + 4\cos\varphi + \cos(2\varphi) = 2(1 - \cos\varphi)^2 \geq 0$$

ist. Für $\sigma > 1$, $\tau \neq 0$ folgt, daß

$$V(\sigma, \tau) := \text{Re } (3\frac{\zeta'}{\zeta}(\sigma) + 4\frac{\zeta'}{\zeta}(\sigma + i\tau) + \frac{\zeta'}{\zeta}(\sigma + 2i\tau)) = -\sum_n \frac{\Lambda(n)}{n^\sigma} \text{Re } (3 + 4n^{i\tau} + n^{-2i\tau}) \leq 0.$$

Wir nehmen nun an, daß ζ eine m-fache Nullstelle bei $1 + i\tau$ habe, $\tau \neq 0$ fest, $m \geq 1$.

Mit dem Ansatz $\zeta(\sigma + i\tau) = (\sigma - 1)^m \tilde{h}_1(\sigma - 1)$, $\tilde{h}_1$ nahe 0 ungleich 0, kann man dann

$$-\frac{\zeta'}{\zeta}(\sigma + i\tau) = \frac{m}{\sigma - 1} + h_1(\sigma - 1), \quad h_1 \text{ nahe 0 beschränkt},$$

zeigen, und ebenso ist

$$-\frac{\zeta'}{\zeta}(\sigma + 2i\tau) = \frac{\mu}{\sigma - 1} + h_2(\sigma - 1), \quad h_2 \text{ nahe 0 beschränkt},$$

mit $\mu \geq 0$, da ζ wegen der holomorphen Fortsetzungseigenschaft von oben keinen Pol auf $\{1 + i\tau; \tau \neq 0\}$ hat, sowie

$$-\frac{\zeta'}{\zeta}(\sigma) = \frac{-1}{\sigma - 1} + h_3(\sigma - 1), \quad h_3 \text{ nahe 0 beschränkt},$$

wegen dem einfachen Pol von ζ bei $s = 1$.

Nach obigem hat V immer negatives Vorzeichen, so daß folgt, daß

$$\frac{-3 + 4m + \mu}{\sigma - 1} + \text{Beschränktes} \leq 0$$

ist für alle σ nahe 1. Läßt man σ aber gegen 1 gehen, divergiert die linke Seite nach $+\infty$, was den gewünschten Widerspruch liefert. □

Zu zeigen ist noch, daß oben konstruiertes ν tatsächlich k-pseudozufällig ist, also daß die Linearform- und Korrelationsbedingungen für ν gelten. Dafür brauchen wir die Propositionen 8.5. und 8.6., deren Beweisidee in einer vereinfachten Form wir im nächsten Kapitel untersuchen möchten.

Beginnen wir mit Proposition 8.5 und dem Nachweis, daß ν die Linearformbedingung erfüllt:

Proposition 8.5 (Goldston-Yıldırım)**.** *$m, t \in \mathbb{N}$, $1 \leq i \leq m$, sei $\psi_i(\mathbf{x}) := \sum_{j=1}^{t} L_{ij} x_j + b_i$ eine Linearform mit Koeffizienten $L_{ij} \in \mathbb{Z}$ mit $|L_{ij}| \leq \sqrt{w(N)}/2$ für alle $i = 1, \ldots m$ und $j = 1, \ldots, t$. Weiter seien die t-Tupel $(L_{ij})_{j=1}^{t}$ nie identisch 0, keine zwei t-Tupel seien rationale Vielfache voneinander. Schreibe $\theta_i := W\psi_i + 1$, sei $B = \prod_{i=1}^{t} I_i \subset \mathbb{R}^t$, wo I_i ein Intervall der Länge $\geq R^{10m}$ sei. Dann gilt (falls $w(N)$ langsam in N wächst):*

$$\mathbb{E}(\Lambda_R(\theta_1(\mathbf{x}))^2 \ldots \Lambda_R(\theta_m(\mathbf{x}))^2 | \underline{x} \in B) = (1 + o_{m,t}(1)) \left(\frac{W \log R}{\phi(W)} \right)^m .$$

Damit zeigen wir schon mal:

Lemma 8.7. *Das Maß ν aus Definition 8.3 erfüllt $\mathbb{E}(\nu) = 1 + o(1)$.*

Beweis: Setze $m := t := 1$, $\psi_1(x_1) := x_1$ und $B := [\varepsilon_k N, 2\varepsilon_k N]$, und wende Prop. 8.5 an. Es folgt

$$\mathbb{E}(\nu(x) \mid x \in [\varepsilon_k N, 2\varepsilon_k N]) = 1 + o(1),$$

und außerdem ist

$$\mathbb{E}(\nu(x) \mid x \in \mathbb{Z}_N \backslash [\varepsilon_k N, 2\varepsilon_k N]) = 1;$$

jetzt sind diese Mittelwerte zusammenzusetzen. □

Proposition 8.8. *Die Funktion ν erfüllt die $(k \cdot 2^{k-1}, 3k - 4, k)$-Linearformbedingung.*

Proof. Sei $\psi_i(\underline{x}) = \sum_{j=1}^{t} L_{ij} x_j + b_i$ eine Linearform wie in Definition 3.1, d. h. $m \leq k \cdot 2^{k-1}$, $t \leq 3k - 4$, die L_{ij} sind aus $\mathbb{Q}$, und wobei Zähler und Nenner im Betrag höchstens so groß wie k sind, und kein t-Tupel $(L_{ij})_{j=1}^{t}$ ist $= \underline{0}$ oder gleich einem rationalen Vielfachen voneinander. Zu zeigen ist:

$$\mathbb{E}(\nu(\psi_1(\underline{x})) \ldots \nu(\psi_m(\underline{x})) \mid \underline{x} \in \mathbb{Z}_N^t) = 1 + o(1). \tag{1}$$

Ohne Einschränkung seien die L_{ij} ganz, wobei dann die Schranke für L_{ij} zu $|L_{ij}| \leq (k+1)!$ erhöht werden muß. Da $w(N)$ langsam in N nach ∞ geht, ist $(k+1)! < \sqrt{w(N)}/2$ für große N; damit ist Proposition 8 anwendbar.

Wir zerlegen den Summationsbereich für (1) in Q^t viele Quader, wobei $Q = Q(N)$ eine langsam in N wachsende Funktion ist, die wir später wählen:

$$B_{u_1,\dots,u_t} = \{\underline{x} \in \mathbb{Z}_N^t : x_j \in [\lfloor u_j N/Q \rfloor, \lfloor (u_j+1)N/Q \rfloor), j = 1,\dots,t\},$$

und die u_j betrachten wir mod Q, d. h. $\underline{u} \in \mathbb{Z}_Q^t$. Bis auf den vernachlässigbaren multiplikativen Fehler $1 + o(1)$ (da die Quader nicht ganz gleich groß sind) kann die linke Seite von (1) geschrieben werden als

$$\mathbb{E}(\mathbb{E}(\nu(\psi_1(\underline{x}))\dots\nu(\psi_m(\underline{x}))|\underline{x} \in B_{u_1,\dots,u_t})|u_1,\dots,u_t \in \mathbb{Z}_Q).$$

Wir nennen ein t-Tupel $(u_1,\dots,u_t) \in \mathbb{Z}_Q^t$ *nett*, falls für alle $1 \le i \le m$ die Mengen $\psi_i(B_{u_1,\dots,u_t})$ entweder ganz im Intervall $[\varepsilon_k N, 2\varepsilon_k N]$ enthalten sind oder damit disjunkt sind. Nach Prop. 8.5 und der Definition für ν haben wir

$$\mathbb{E}(\nu(\psi_1(\underline{x}))\dots\nu(\psi_m(\underline{x}))|\underline{x} \in B_{u_1,\dots,u_t}) = 1 + o_{m,t}(1)$$

sobald $(u_1,\dots,u_t)$ nett ist, da dann gilt, daß jedes $\nu(\psi_i(\underline{x}))$ entweder den Faktor $\frac{\phi(W)}{W\log R}\Lambda_R^2(\theta_i(\underline{x}))$ oder 1 liefert, und N/Q ist größer als R^{10m} für Q langsam genug wachsend in N, wegen der Definition von R und der oberen Schranke für m. Ist $(u_1,\dots,u_t)$ nicht nett, schätzen wir ν grob ab durch $1 + \frac{\phi(W)}{W\log R}\Lambda_R^2(\theta_i(\underline{x}))$, multiplizieren aus, und wieder mit Proposition 8.5 erhalten wir

$$\mathbb{E}(\nu(\psi_1(\underline{x}))\dots\nu(\psi_m(\underline{x}))|\underline{x} \in B_{u_1,\dots,u_t}) = O_{m,t}(1).$$

Es genügt nun, zu zeigen, daß der Anteil der nicht-netten $(u_1,\dots,u_t)$ in $\mathbb{Z}_Q^t$ höchstens $O_{m,t}(1/Q)$ ist, denn damit ist die linke Seite von (1) gleich $1 + o_{m,t}(1) + O_{m,t}(1/Q)$, und die Behauptung folgt, falls Q als hinreichend langsam wachsende Funktion in N gewählt wird.

Sei dafür $(u_1,\dots,u_t)$ nicht nett. Dann gibt es $1 \le i \le m$ und $\underline{x}, \underline{x}' \in B_{u_1,\dots,u_t}$ mit $\psi_i(\underline{x}) \in [\varepsilon_k N, 2\varepsilon_k N]$, aber $\psi_i(\underline{x}') \notin [\varepsilon_k N, 2\varepsilon_k N]$. Laut Definition für $B_{u_1,\dots,u_t}$ (und der Schranken für L_{ij}) gilt

$$\psi_i(\underline{x}), \psi_i(\underline{x}') = \sum_{j=1}^t L_{ij}\lfloor Nu_j/Q \rfloor + b_i + O_{m,t}(N/Q).$$

Diese Formel gilt also auch für einen der Randpunkte des Intervalls $[\varepsilon_k N, 2\varepsilon_k N]$, also gilt

$$a\varepsilon_k N = \sum_{j=1}^t L_{ij}\lfloor Nu_j/Q \rfloor + b_i + O_{m,t}(N/Q)$$

für $a = 1$ oder $a = 2$. Teilen wir dies durch N/Q und erhalten

$$\sum_{j=1}^t L_{ij}u_j = a\varepsilon_k Q + b_i Q/N + O_{m,t}(1) \mod Q.$$

Da $(L_{ij})_{j=1}^t$ nicht $\underline{0}$ ist, ist die Anzahl solcher t-Tupel $(u_1,\dots,u_t)$, die dieses LGS erfüllen, höchstens $O_{m,t}(Q^{t-1})$. Mit den Werten für a und i sehen wir, daß der Anteil nicht-netter t-Tupel höchstens $O_{m,t}(1/Q)$ ist (die Abhängigkeit von m und t ist irrelevant, da beides Funktionen von k sind). □

Für die Korrelationsbedingung brauchen wir das folgende Goldston-Yıldırım-Ergebnis:

Proposition 8.6 (Goldston-Yıldırım). *Sei $m \geq 1$, B ein Interval der Länge $\geq R^{10m}$, $h_1, \ldots, h_m \in \mathbb{Z}$ verschieden, $|h_i| \leq N^2$ für alle $1 \leq i \leq m$, und sei*

$$\Delta := \prod_{1 \leq i < j \leq m} |h_i - h_j|.$$

Dann gilt (für N groß in Abhängigkeit von m, und $w(N)$ langsam wachsend in N):

$$\begin{aligned} &\mathbb{E}(\Lambda_R(W(x+h_1)+1)^2 \ldots \Lambda_R(W(x+h_m)+1)^2 | x \in B) \\ &\leq (1+o_m(1)) \left(\frac{W \log R}{\phi(W)}\right)^m \prod_{p|\Delta} (1 + O_m(p^{-1/2})). \end{aligned} \tag{2}$$

Hier und im folgenden bezeichnet p stets eine Primzahl.

Zunächst behandeln wir das Produkt in dieser Abschätzung:

Lemma 8.9. *Sei $m \geq 1$. Dann existiert eine Funktion $\tau = \tau_m : \mathbb{Z} \to \mathbb{R}^+$ mit $\tau(n) \geq 1$ für alle $n \neq 0$, und so daß wir für alle verschiedenen $h_1, \ldots, h_j \in [\varepsilon_k N, 2\varepsilon_k N]$ haben:*

$$\prod_{p|\Delta} (1 + O_m(p^{-1/2})) \leq \sum_{1 \leq i < j \leq m} \tau(h_i - h_j),$$

wobei Δ wie in Proposition 8.6. gegeben ist, und so daß $\mathbb{E}(\tau^q(n) | 0 < |n| \leq N) = O_{m,q}(1)$ für alle reellen $0 < q < \infty$.

Beweis: Wir haben

$$\prod_{p|\Delta} (1 + O_m(p^{-1/2})) \leq \prod_{1 \leq i < j \leq m} \left(\prod_{p | h_i - h_j} (1 + p^{-1/2}) \right)^{O_m(1)}.$$

Nach der Ungleichung vom arithmetischen und geometrischen Mittel (indem wir alle Konstanten in den $O_m(1)$ Faktor absorbieren) nehmen wir $\tau_m(n) := O_m(1) \prod_{p|n} (1+p^{-1/2})^{O_m(1)}$ für alle $n \neq 0$. Somit reicht es, zu zeigen:

$$\mathbb{E}\left(\prod_{p|n} (1 + p^{-1/2})^{O_m(q)} \;\middle|\; 0 < |n| \leq N \right) = O_{m,q}(1) \text{ für alle } 0 < q < \infty.$$

Da $(1+p^{-1/2})^{O_m(q)}$ beschränkt durch $1+p^{-1/4}$ ist für alle bis auf $O_{m,q}(1)$ viele Primzahlen p, haben wir

$$\mathbb{E}\left(\prod_{p|n} (1 + p^{-1/2})^{O_m(q)} \;\middle|\; 0 < |n| \leq N \right) \leq O_{m,q}(1) \mathbb{E}\left(\prod_{p|n} (1 + p^{-1/4}) \;\middle|\; 0 < n \leq N \right).$$

Aber $\prod_{p|n}(1 + p^{-1/4}) \leq \sum_{d|n} d^{-1/4}$, und somit ist

$$\begin{aligned} \mathbb{E}\left(\prod_{p|n} (1 + p^{-1/2})^{O_m(q)} \;\middle|\; 0 < |n| \leq N \right) &\leq O_{m,q}(1) \frac{1}{2N} \sum_{1 \leq |n| \leq N} \sum_{d|n} d^{-1/4} \\ &\leq O_{m,q}(1) \frac{1}{2N} \sum_{d=1}^{N} \frac{N}{d} d^{-1/4}, \end{aligned}$$

was $O_{m,q}(1)$ ist wie gewünscht. □

Proposition 8.10. *Das Maß ν erfüllt die 2^{k-1}-Korrelationsbedingung.*

Beweis: Für $1 \le m \le 2^{k-1}$ und $h_1, \dots, h_m \in \mathbb{Z}_N$ müssen wir die Schranke

$$\mathbb{E}\big(\nu(x+h_1)\nu(x+h_2)\dots\nu(x+h_m) \;\big|\; x \in \mathbb{Z}_N\big) \le \sum_{1\le i<j\le m} \tau(h_i - h_j), \tag{3}$$

zeigen, wobei die Funktion $\tau = \tau_m$ beschränkt in L^q ist für alle q.

Nimm τ aus Lemma 8, und setze

$$\tau(0) := \exp(Cm \log N / \log\log N)$$

für eine Konstante $C > 0$. Nach dem vorigen Lemma ist $\mathbb{E}(\tau^q) = O_{m,q}(1)$ für alle q, da $\tau(0)$ nur höchstens $o_{m,q}(1)$ zur Summe in $\mathbb{E}$ beiträgt.

1. Fall: mindestens zwei der h_i sind gleich. Dann ist die linke Seite von (1) grob $\le \|\nu\|_{L^\infty}^m$, aber laut der Definition für ν, wegen $\Lambda_R(n) \le d(n)\log R$ und der bekannten Abschätzung $d(n) \ll \exp(C \log N/\log\log N)$ für die Teilerfunktion haben wir die grobe Schranke $\|\nu\|_{L^\infty} \ll \exp(C\log N/\log\log N)$, und die Behauptung folgt wegen unserer Wahl von $\tau(0)$.

2. Fall: alle h_i verschieden. Sei

$$g(n) := \frac{\phi(W)}{W}\frac{\Lambda_R^2(Wn+1)}{\log R}\mathbf{1}_{[\varepsilon_k N, 2\varepsilon_k N]}(n).$$

Nach Konstruktion von ν ist

$$\begin{aligned}\mathbb{E}\big(\nu(x+h_1)\dots\nu(x+h_m) \;\big|\; x\in\mathbb{Z}_N\big) &\\ \le \mathbb{E}\big((1+g(x+h_1))\dots(1+g(x+h_m)) \;\big|\; x\in\mathbb{Z}_N\big) &\\ = \sum_{A\subseteq\{1,\dots,m\}} \mathbb{E}\Big(\prod_{i\in A} g(x+h_i) \;\Big|\; x\in\mathbb{Z}_N\Big)&\end{aligned}$$

Für $i, j \in A$ sei ohne Einschränkung $|h_i - h_j| \le \varepsilon_k N$, da sonst der Erwartungswert verschwindet. Nach Proposition 8.6 and Lemma 8.9 haben wir also

$$\mathbb{E}\Big(\prod_{i\in A} g(x+h_i) \;\Big|\; x\in\mathbb{Z}_N\Big) \le \sum_{1\le i<j\le m} \tau(h_i-h_j) + o_m(1).$$

Wir summieren über A und passen τ mit einem beschränkten Faktor an (der nur von m, also nur von k abhängt), und erhalten das Ergebnis. □

Es folgt Proposition 8.1., d. h. ν ist k-pseudozufälliges Maß. □

9 Bemerkungen zum Beweis der Goldston-Yıldırım-Ergebnisse Proposition 8.5 und 8.6

Gesucht sind asymptotische Formeln für die Mittelwerte von Produkten der Funktion Λ_R bzw. Λ_R^2. Letzteres läßt sich auf ersteres zurückführen, das heißt auf Ausdrücke der Gestalt

$$\sum_{n\le N} \Lambda(n+j_1)\cdots\Lambda(n+j_k)$$

bringen. Ziel ist eine explizite asymptotische Formel für solche Ausdrücke.

In der Arbeit von Tao und Green werden dafür Ideen von Goldston-Yıldırım benutzt. Deren Methode benötigt das nichttriviale klassische nullstellenfreie Gebiet $\Re s > 1 - \frac{c}{\Im s}$.

Mit einer Idee, die in T. Tao's Preprint "A Remark on Goldston-Yıldırım Correlation Estimates"

`http://www.math.ucla.edu/~tao/preprints/Expository/gy-corr.dvi`

dargestellt wird, läßt sich dies derart vermeiden, daß lediglich die Kenntnis über das Divergenzverhalten der ζ-Funktion nahe $s = 1$ ausreicht. Außerdem wird dabei die Methode wesentlich einfacher.

Ein Haken dieser Vereinfachung ist noch der, daß dabei eine Glättung der Λ_R-Funktion vorgenommen werden muß.