Profinite Zahlen, Gleichverteilung, Diskrepanz

Peter Zinterhof

Universität Salzburg

24.03.2025

Keywords: Uniform distribution of sequences, profinite numbers, discrepancy, monothetic groups, numerical integration of functions

Summary: Let Γ be the group of all roots of the unity. The dual group G of the discrete group Γ is a compact group.
Uniform distribution of sequences in G and a notion of discrepancy will be considered, error estimations for numerical integration and estimations of discrepancy are in the scope.
Zusammenfassung: Sei Γ die Gruppe aller Einheitswurzeln. Die Dualgruppe G der diskreten Gruppe Γ ist eine kompakte Gruppe. Es werden die Gleichverteilung von Folgen in G und ein Diskrepanzbegriff eingeführt; dabei stehen Fehlerabschätzungen für die numerische Integration von Funktionen und Abschätzungen der Diskrepanz im Mittelpunkt.

Sei also Γ die Menge aller $z = \exp(2\pi i r),\ r \in \mathbb{Q}$ als diskrete multiplikative Gruppe behandelt. Die duale Gruppe $G = \hat{\Gamma}$ ist somit eine kompakte Gruppe, wobei $\hat{G} = \Gamma$ keine Basis besitzt und nicht endlich erzeugt ist. Wir benötigen das folgende Ergebnis über die Dualität zwischen Untergruppen und Quotientengruppen aus [3]:
Struktursatz:

Satz 1. *Sei H eine abgeschlossene Untergruppe der LCA-Gruppe G und sei Λ die Menge aller $\gamma \in \Gamma$ mit $\langle x, \gamma\rangle = 1 \quad \forall x \in H$, also der Annihilator von H. Λ ist offensichtlich eine abgeschlossene Untergruppe von Γ. Darum gilt der Struktursatz:*
Λ und Γ/Λ sind die dualen Gruppen von G/H bzw. H, wobei diese Gleichheit die homöomorphe Isomorphie bedeutet.

Wir betrachten nun die diskrete Gruppe $\Gamma = \{\exp(2\pi ir),\ r \in \mathbb{Q}\}$ näher: $z = \exp(2\pi ir),\ r \in \mathbb{Q}$, lässt sich darstellen als $z = \exp(2\pi i p/q)$, wobei $q \in \mathbb{N}$, $\mathrm{ggT}(q,p) = 1, 1 \leq p < q$, ist. Wir betrachten Γ als multiplikative Untergruppe von

$$\begin{aligned} D &= \{|z| = 1\} : \\ z_1 \cdot z_2 &= \exp(2\pi i p_1/q_1) \cdot \exp(2\pi i p_2/q_2) \\ &= \exp(2\pi i p_3/q_3) \\ &= z_3, \end{aligned}$$

wobei $\mathrm{ggT}(q_3, p_3) = 1,\ q \leq p_3 < q_3$. Sei nun

$$B = \{G = (q,p),\ q \in \mathbb{N},\ \mathrm{ggT}(q,p) = 1,\ 1 \leq p < q\} \tag{1}$$

Es gibt also eine bijektive Entsprechung zwischen Γ und B vermöge

$$z = \exp(2\pi i p/q) \iff B = (q,p),$$

wobei sich die multiplikative Struktur von Γ als Operation auf B überträgt, was B ebenfalls zu einer diskreten abelschen Gruppe macht.
Sei nun $\mathbb{Z}^{(B)}$ die frei-abelsche Gruppe mit der Basis $B \cong \Gamma$, also ist $\mathbb{Z}^{(B)}$ die Menge aller Familien, $\alpha = (\alpha(b))_b$, mit $\alpha(b) \in \mathbb{Z}$, jedoch $\alpha(b) \neq 0 \in \mathbb{Z}$ für höchstens endlich viele $b \in B$. Die Elemente $\varepsilon_b, b \in B$, mit $\varepsilon_b = (\varepsilon_b(b'))_{b' \in B}$ und $\varepsilon_b(b') = \delta_{bb'}$, bilden eine Basis von $\mathbb{Z}^{(B)}$.
Sei nun $D = \{z \in \mathbb{C},\ |z| = 1\}$ und D^B das vollständige direkte Produkt

$$D^B = \{(z(b))_{b \in B},\ z(b) \in \mathbb{Z}\} \cong D^\Gamma.$$

Also ist D^B die Menge aller Funktionen von B nach D.
Wir betrachten D^B als multiplikative Gruppe mit der komponentenweisen Multiplikation, ausgestattet mit der Produkttopologie. Die duale Gruppe von D^B ist offenbar $\mathbb{Z}^{(B)}$

$$\hat{D}^B = \mathbb{Z}^{(B)}. \tag{2}$$

Wir betrachten nun die Abbildung $\phi : \mathbb{Z}^{(B)} \to \Gamma$, die definiert ist durch

$$\phi(\alpha) = \prod_{b \in B} z(b)^{\alpha(b)}, \tag{3}$$

wobei nur endlich viele $\alpha(b) \neq 0,\ \alpha(b) \in \mathbb{Z}$. Sei nun

$$\ker = \ker(\phi) = \{\alpha : \phi(\alpha) = 1\} \tag{4}$$

der Kern der Abbildung ϕ. Dann gilt offensichtlich der Satz 1: $\Gamma \cong {}^{\mathbb{Z}^{(B)}}/_{\ker}$, Γ ist Quotient der frei-abelschen Gruppe $\mathbb{Z}^{(B)}$.
Aus dem anfangs angesprochenen Struktursatz Satz 1 ergibt sich die Folgerung:

Korollar 2. *Für die duale Gruppe G von Γ, $\hat{\Gamma} = G$, gilt*

$$G = \mathrm{Ann}(\ker) \tag{5}$$

und

$$\hat{\ker} \cong {}^{D^B}\!/_G \tag{6}$$

Gleichung (5), nämlich $G = Ann(\ker)$, bedeutet

$$G = \left\{ (z(b))_b \in D^B : \prod_{b\in B} z(b)^{\alpha(b)} = 1 \quad \forall \alpha \in \ker \right\}.$$

Die frei-abelsche Gruppe $\mathbb{Z}^{(\Gamma)} \cong \mathbb{Z}^{(B)}$ wird von $\Gamma \cong B$ erzeugt, wobei Γ bzw. B selbst homöomorphe (diskrete) abelsche Gruppen mit der Multiplikation in $\mathbb{C}$ mit: $z_1, z_2 \in D$, $z_3 = z_1 \cdot z_2 \in D$. Wir führen in üblicher Weise die Faltung von Basiselementen $\varepsilon_z = (\delta_{z,z'})_{z'\in\Gamma}$ ein: $\varepsilon_Z, \circledast\varepsilon_{z_2} := \varepsilon_{z_1\cdot z_2}$ und setzen die Operation $\circledast$ auf $\mathbb{Z}^{(\Gamma)} \cong \mathbb{Z}^{(B)}$ fort:

Definition 3. Für $\alpha, \beta \in \mathbb{Z}^{(\Gamma)}$ und $z \in \Gamma$ sei additiv geschrieben

$$(\alpha \circledast \beta)(z) = \sum_{z'\in\Gamma} \alpha(z')\beta(z - z') = \sum_{z'\in\Gamma} \alpha(z - z')\beta(z'). \tag{7}$$

Damit wird $\mathbb{Z}^{(\Gamma)}$ zur Gruppenalgebra $\mathbb{Z}[\Gamma]$.
Wir erläutern nun die Definition von ϕ in Gleichung (3) auf

$$\phi : D^\Gamma \times Z[\Gamma] \to D$$

durch

$$\phi(x, \alpha) = \prod_{z\in\Gamma} x(z)^{\alpha(z)} \tag{8}$$

für $x \in (x(z))_{z\in\Gamma}$, $\alpha = (\alpha(z))_{z\in\Gamma}$.
Hier ist wieder

$$z(b) = \exp(2\pi i {}^p\!/_q),\ q = 1, 2, \ldots,\ \mathrm{ggT}(q, p) = 1,\ b = (q, p).$$

Wir identifizieren zwanglos die $z(b)$, $b = (q, p)$ und die ε_z. Die Funktion $\phi(x, \alpha)$ ist auf $\mathbb{Z}^{(\Gamma)} \times \mathbb{Z}[\Gamma]$ stetig und beschreibt die Charaktere von $D^\Gamma \cong D^B$, $\hat{D^\Gamma} = \mathbb{Z}[\Gamma]$. Die Charaktere der Gruppe $G = \mathrm{Ann}(\ker) = \hat{\Gamma}$ sind die Elemente $\alpha \in \mathbb{Z}[\Gamma]$ modulo der Gruppe $\ker \subseteq \mathbb{Z}^{(\Gamma)}$. Die Charaktere von G werden also durch die Basiselemente $\varepsilon_z, z \in \Gamma$, der Gruppenalgebra $\mathbb{Z}[\Gamma]$ repräsentiert. Es gilt daher der

Satz 4. *Für* $x = (\alpha(z))_{z\in\Gamma} \in G$ *und* $\varepsilon_{z_0} \in \Gamma = \hat{G}$ *gilt*

$$\phi(x, \varepsilon_{z_0}) = x(z_0), \tag{9}$$

wobei die Verknüpfung der $\varepsilon_z, z \in \Gamma$, *gemäß* $\varepsilon_{z_1} \circledast \varepsilon_{z_2} = \varepsilon_{z_3} = \varepsilon_{z_1 \cdot z_2}$ *erfolgt.*

Wir schreiben für $x \in D^\Gamma$ und $\alpha \in \mathbb{Z}[\Gamma] = \hat{D}^\Gamma$

$$\langle x, \alpha\rangle = \phi(x, \alpha) \tag{10}$$

und auf (G, Γ), $\Gamma = \hat{G}$, $x \in G$, $\varepsilon_z \in \Gamma$:

$$\langle x, \varepsilon_z\rangle = \phi(x, \varepsilon_z) = x(z). \tag{11}$$

Die Charaktere γ_z der Gruppe $G \subseteq D^\Gamma$ entsprechen also den „Projektionen“ der Elemente $x = (x(z))_{z\in\Gamma} \in G$ auf D, wobei $\gamma_z \cong \varepsilon_z$, und die ε_z eine Basis von $\mathbb{Z}[\Gamma]$ bilden.
Wir beschreiben nun die Gruppe $G = \hat{\Gamma}$ etwas näher:
Nach Gleichung (3) und Gleichung (4) ist mit $z(b) = \exp(2\pi i p/q)$, $q \in \mathbb{N}$, $\mathrm{ggT}(q, p) = 1$

$$\ker = \ker(\phi) = \left\{\alpha \in \mathbb{Z}^{(B)} : \prod_b \left(\exp(2\pi i p/q)\right)^{\alpha(b)} = 1\right\}. \tag{12}$$

Also ist für $\alpha_z = q \cdot \varepsilon_z$ das Element α_z im Kern von ϕ, da $\phi(\alpha_z)$ trivial gleich 1 ist. Da weiters nach Gleichung (5) gilt $G = \mathrm{Ann}(\ker)$, folgt für $x = (x(b))_{b\in B} \in G$ sofort, dass $x \in B$ für $b \in B$ eine q-te Einheitswurzel ist: $x(b)^q = 1$. Es gilt also die

Bemerkung 1. Notwendig für die Zugehörigkeit der Elemente $x \in D^B$ zur Gruppe G ist $x(b)^q = 1$ für alle $b = (q, p) \in B$. Diese Bedingung ist jedoch nicht hinreichend.

Wir beschreiben nun die Topologie von $G = \hat{\Gamma}$:
Wir bezeichnen das neutrale Element der Gruppe $D^B \cong D^\Gamma$ mit 1, also $1 = (1)_z = (\exp(0))_z$.
Eine (G, Γ) Umgebungsbasis von 1 wird gebildet von

$$U_\varepsilon(1) = \{x \in G : |\langle x, \gamma_1\rangle - 1| < \varepsilon, \ldots, |\langle x, \gamma_n\rangle - 1| < \varepsilon\},$$

$\gamma_1, \ldots, \gamma_n \in \Gamma$, $\varepsilon > 0$. Also mit $\gamma_1 = z_1, \ldots, \gamma_n = z_n \in \Gamma$:

$$U_\varepsilon(n) = \{x \in G \quad |x(z_1) - 1| < \varepsilon, \ldots, |x(z_n) - 1| < \varepsilon\},$$

wobei $z_1 = \exp(2\pi i p_1/q_1), \ldots, z_n = \exp(2\pi i p_n/q_n)$.
Da nach Bemerkung 1 die Komponenten $x(b) = x((q, p)) = x(\exp(2\pi i p/q))$, also $x(b) = x(z)$, $x = \exp(2\pi i p/q)$, jeweils q-te Einheitswurzel und diskret sind, bildet für hinreichend kleine $\varepsilon > 0$ die Familie

$$U_{z_1,\ldots,z_n}(1) = \{x \in G : x(z_1) = 1, \ldots, x(z_n) = 1\}, \tag{13}$$

$z_1, \ldots, z_n \in \Gamma$ eine Umgebungsbasis von $1 = (1)_\Gamma$ in G. Wir definieren nun für die Einfachheit der Bezeichnung die Höhe $h(z)$ des Charakters $z = \gamma_z = \exp(2\pi i p/q) \cong z = (q,p)$:

Definition 5. $h(z) := q$, also $h(b) = h\left((q,p)\right) = q$

Damit wird die Mengenfamilie

$$U_{q'}(1) = \left\{x \in G : \, x\left((q,p)\right) = 1, h(b) = q'\right\}, \, q' = 1, 2, \ldots \tag{14}$$

zu einer Umgebungsbasis von $1 = (\exp(0))_\Gamma \in G \subseteq \mathbb{Z}[\Gamma]$. Durch Translation in G ergibt sich die Umgebungsbasis von $y \in G$ durch

$$U_{q'}(y) = \left\{x \in G : \, x\left((q,p)\right) = y\left((q,p)\right), \text{ für } h(b \mid\leq q')\right\}, \tag{15}$$

$q' = 1, 2, \ldots, \; b = (q,p), h(b) = q.$

Da

$$\Gamma = \{z = \exp(2\pi i p/q), \; \mathrm{ggT}(q,p) = 1, q \in \mathbb{N}\}$$

eine (multiplikative) Untergruppe von $D = \{z : |z| = 1\}$ ist, ist nach einem bekannten Satz von Halmos, Kakutani die duale kompakte Gruppe $G = \hat{\Gamma}$ monothetisch, enthält also eine zu $\mathbb{Z}$ isomorphe und in G dichte Untergruppe [3].

Wir geben nun einen Generator der Gruppe G an:
Die Dualgruppe Γ von G besteht ja aus allen $z = \exp(2\pi i p/q)$, $\mathrm{ggT}(q,p) = 1$, $q = 1, 2, \ldots,$ $q \leq p \leq q$. Mit $b = (q,p)$ haben wir wieder $\Gamma = \{z = z(b), b \in B\}$. Wir definieren nun das Element $w_1 \in G$ durch

$$w_1 = (z(b))_{b \in B} = (\exp(2\pi i p/q))_{(q,p) \in B}. \tag{16}$$

Ist $z(b')$, b' fest aus B, ein Charakter $\gamma_b \in \Gamma$, so ist

$$\langle w_1, \gamma_{b'} \rangle = z(b') \neq 1, \tag{17}$$

falls $\gamma_{b'}$ nicht trivial ist, und es ist

$$\langle w_1, \gamma_{b'} \rangle = 1, \tag{18}$$

falls $\gamma_{b'} = 1 \in \Gamma$ der triviale Charakter in Γ ist. Also ist für jeden nicht trivialen Charakter $\gamma_{b'}$

$$\langle w_1, \gamma_{b'} \rangle = z(b') = \exp(w\pi i p'/q') \neq 1. \tag{19}$$

Wir wenden nun die Standard Überlegung an:

$$\begin{aligned}\left|\frac{1}{N}\sum_{n=1}^{N-1}\langle w_1^n,\gamma_{b'}\rangle\right| &= \left|\frac{1}{N}\sum_{n=0}^{N-1}\left(\exp\left(2\pi i p'/q'\right)\right)^n\right| \\ &\leq \frac{2}{|1-\exp(2\pi i p'/q')|}\cdot\frac{1}{N} \\ &\overset{N\to\infty}{\longrightarrow} 0,\end{aligned} \tag{20}$$

falls $\gamma_{b'}$ nicht trivial ist. Also ist die Folge $w_k := w_k^n, k = 0, 1, \ldots,$ in G gleich verteilt, also in G dicht. Das Element w_1 ist offensichtlich in $G = \mathrm{Ann}(\Gamma)$ und somit Generator von G. Es gilt also der

Satz 6. *Das Element $w_1 = (z(b))_{b\in B} \in G$ ist Generator der Gruppe G und $w_n = w_1^n, n \in \mathbb{Z}$ bzw. $n \in \mathbb{N}$ ist in G gleichverteilt.*

Korollar 7. *G besteht aus den Elementen $x \in D^\Gamma \cong D^B$, die durch Glieder der Folge $w_n, n \in \mathbb{Z}$ beliebig approximierbar sind. G ist also der Abschluss von $\{w_n, n \in \mathbb{Z}\}$.*

Das bedeutet generell:
Ist $y \in G$, $y = (y(b))_{b\in B}$ und $U_{q'}(y)$ eine Umgebung von y gemäß Gleichung (14), dann gibt es ein $n = n\,(y, q') \in \mathbb{Z}$ sodass $w_n \in U_{q'}(y)$, also

$$y\,((q,p)) = w_n\,((q,p)) = w_1^n\,((q,p)) \text{ für } h(q) \leq q'. \tag{21}$$

Wegen Bemerkung 1 ist

$$y\,((q,p)) = \exp(2\pi i^{a(q,p)}/_q), \tag{22}$$

mit $a(q,p) \in \mathbb{Z}$ mal q. Weiters ist

$$w_1^n\,((q,p)) = \exp(2\pi i n p/_q). \tag{23}$$

Also sind die simultanen Kongruenzen

$$\alpha(q,p) \equiv n \cdot p(q) \mod q,\ h(q) \leq q' \tag{24}$$

genau für die Elemente $y \in G$ lösbar.

Der Chinesische Restsatz lehrt weiter: Ist $n = n(y, q')$ eine Lösung von Gleichung (24), so erhält man alle Lösungen n_k von Gleichung (24) durch

$$n_k = n_k(y, q') = n(y, q') + k \cdot \mathrm{kgV}(1, 2, \ldots, q'), k \in \mathbb{Z}. \tag{25}$$

Da $w_n = w_1^n \in G$, $n \in \mathbb{Z}$ dicht in G ist, gibt es beim Übergang von q' auf $q' + 1$ eine Lösung $n = n(y, q' + 1)$ der Kongruenzen

$$\alpha(q,p) \equiv n \cdot p(q) \text{ und } q \text{ für } h(q) \leq q' + 1, \tag{26}$$

die sich unter den $n_k, k \in \mathbb{Z}$ von Gleichung (25) befindet. Alle Lösungen für $q'+1$ werden wieder durch

$$n_k = n_k(y, q'+1) = n(y, q'+1) + k \cdot \mathrm{kgV}(1, 2, \ldots, q', q'+1) \tag{27}$$

erhalten.
Wir halten weiters fest: Sei $q \in \mathbb{N}$, dann bezeichnen wir die Menge

$$B = \{(q,p), \mathrm{ggT}(q,p) = 1, 1 \leq p < q\}$$

als q-te Zelle von B. Es ist also

$$B = \bigcup_{q=1}^{\infty} \{b = (q,p),\ \mathrm{ggT}(q,p) = 1,\ 1 \leq p < 1\}.$$

Betrachten wir nun das beliebige Element $y \in G$ auf der q-ten Zelle:

$$y(b) = y\left((q,p)\right) = \exp(2\pi i^{a(q,p)/q}),$$

wobei die $a(q,p)$ modulo q bestimmt sind.
Da die Folge $w_k = w_1^k$, $k \in \mathbb{Z}$ dicht in G ist, ist für ein $n = n(y,q)$ auf der gesamten q-ten Zelle

$$y = y\left((q,p)\right) = \exp(2\pi i n^{p/q}). \tag{28}$$

Also genügt wegen $\mathrm{ggT}(q,p) = 1$ die Kenntnis eines einzigen $\alpha(q,p_0)$ und q für die Kenntnis aller $\alpha(q,p)$ und auch für die Kenntnis von $n \mod q$. Die Komponenten von y in der q-ten Zelle sind also in diesem Sinn verschränkt. So genügt etwa $\alpha(q,1)$ und q für die Kenntnis aller $\alpha(q,p),\ \mathrm{ggT}(q,p) = 1$ und von $n = n(y,q)$ und q. Dies gibt Anlass für die

Definition 8. Ist $x, y \in G$, dann sei $x \sim y$ und q, wenn auf der q-ten Zelle gilt $x(b) = y(b)$. Weiters sei $x \sim y \mod r, r \in \mathbb{N}$, wenn $x(b) = y(b)$ für alle q mit $h(q) \leq r$.

Sei nun für $y \in G$ und $r \in \mathbb{N}$ die Menge $U_r(y)$ gegeben als Äquivalenzklasse modulo r:

$$U_r(y) = \{x \in G : x \sim y \mod r\}. \tag{29}$$

Wir bestimmen nun die $U_r(y)$ näher: Die Folge $w_n = w_1^n$ liegt dicht in G und erzeugt G. Es gibt $\mod V(r)$ genauer $V(r)$ inkongruente w_n etwa $w_0 = w_1^0, \ldots, w_{V(r)-1}$, wobei $V(r) = \mathrm{kgV}(1, \ldots, r)$ ist. Also gilt für jedes $r = 1, 2, \ldots$

$$G = \bigcup_{k=0}^{V(r)-1} V_r(w_n), \tag{30}$$

wobei diese Vereinigung disjunkt ist. Jedes $y \in G$ findet sich also in genau einem $U_r(w_k)$ und die $U_r(y), r = 1, 2, \ldots$ bilden eine offene Umgebungsbasis von $y \in U_r(w_k)$. Wir betrachten

nun den Übergang $r \to r+1$:
Sei $b(r+1) = \mathrm{ggT}(V(r), r+1)$. Dann ist

$$V(r) = b(r_1)s(r+1),\ r+1 = b(r+1) \cdot t(r+1),$$

wobei $\mathrm{ggT}\,(s(r+1), t(r+1)) = 1$.

Es ergibt sich das einfache

Lemma 9. $V(r+1) = V(r) \cdot t(r+1) = s(r+1) \cdot (r+1)$*;*

wenn wir mit r die Höhe der Umgebung $U_r(y)$ bezeichnen ergibt sich das

Korollar 10. *Jedes*

$$U_r(w_{n(r)}),\ n(r) = 0, \ldots,\ V(r) - 1$$

zerfällt in $z(r+1)$ *Äquivalenzklassen und* $(r+1)$*:* $U_{r+1}\left(w_{n(r+1)}\right)$ *mit* $n(r+1) = n(r) + l(r+1)$, $l(r+1) = 0, \ldots, t(r+1) - 1$.

Wir sagen naheliegend:

Definition 11. Das System

$$U_r\left(w_{n(r)}\right),\ r = 1, 2, \ldots,\ n(r) = 0, \ldots, V(r) - 1$$

heißt Umgebungsbaum der Gruppe G.

Es ergibt sich sofort die

Feststellung 1. Die Folge $(X_m)_m$ aus G ist genau dann eine Cauchy-Folge in der uniformen Strukturen von G, wenn es zu jedem $r = 1, 2, \ldots$ ein $M(r)$ gibt, wobei für alle $m \geq M(r)$ und $k = 0, 1, 2, \ldots$ gilt $x_m \sim x_{m+k} \mod r$.

Wir machen zum Haarmaß μ auf G die

Feststellung 2. Da nach Gleichung (29) G in $V(r)$ Translata von $U_r(w_n)$ zerfällt, die als offen-abgeschlossene Mengen messbar sind, gilt für $n = 0, \ldots, V(r) - 1$:

$$\mu\left(U_r(w_n)\right) = {}^1\!/_{V(r)}. \tag{31}$$

Wir machen weiters die

Feststellung 3. Ist $f(x) \in C(G)$, so folgt aus dem Weyl'schen Kriterium

$$\int_G f(x)d\mu(x) = \lim_{M\to\infty} \frac{1}{M} \sum_{m=0}^{M-1} f(w_m), \tag{32}$$

wobei $w_m = w_1^m$ die erzeugende Folge mit dem Erzeuger

$$w_1 \left(\exp(2\pi i p/q)\right)_{b\in B}, \; b = (q,p), \; \mathrm{ggT}(q,p) = 1$$

ist.

Wir beschreiben den Indikator der Menge $U \subseteq G$ mit $I(U;x)$:

$$I(U;x) = \begin{cases} 1 & \text{für } x \in U \\ 0 & \text{für } x \notin U \end{cases}$$

und treffen die

Feststellung 4. Der Indikator der Umgebung $U_r(y) = \{x : x \sim y \mod r\}$ ist stetig.

Dies ist leicht einzusehen, da $U_r(y) = U_r(w_{k_0})$ für ein $1 \leq k_0 \leq V(r) - 1$ und U_r offen ist. Der Indikator I ist gleich 1 auf der offenen Menge $U_r(w_{k_0})$ und gleich 0 auf der gemäß Gleichung (29) ebenfalls offenen Menge $G \setminus U_r(w_{k_0})$.

Wir sehen nun in nahe liegender Weise die $U_r(y)$ nicht nur als zur Umgebungsbasis gehörige Mengen oder als Äquivalenzklassen modulo r an, sondern bezeichnen die $U_r(y)$ auch als Intervalle der Höhe r in der Gruppe G. Da die Treppenfunktionen über diesen Intervallen in $C(G)$ dicht liegen ergibt sich sofort der

Satz 12. *Die Folge $(x_m)_m$ aus G ist genau dann in G gleichverteilt, wenn für jedes Intervall $U_r(y)$, $r \in \mathbb{N}$, $y \in G$ gilt:*

$$\lim_{M\to\infty} \frac{1}{M} \#\{x_m \in U_r(y)\} = \mu\left(U_r(y)\right). \tag{33}$$

Wir zeigen nun, dass die Kongruenz in Gleichung (33) gleichmäßig ist, genau wenn $(x_m)_m$ gleichverteilt in G ist:
Sei $r \geq 1$ und sei $U_r(w_j)$, $j = 0, \ldots, V(r) - 1$ eine Partition von G durch die Intervalle $U_r(w_j)$ der Höhe r. Sei weiters $U_q(y)$, $u \in G$ ein beliebiges Intervall der Höhe q. Es gilt:

$$U_q(y) = U_q(y) \cap G = \bigcup_{j=0}^{V(r)-1} \left(U_q(y) \cap U_r(w_j)\right).$$

Wenn $U_q(y) \cap U_r(w_{j_0}) \neq \emptyset$ für ein $j_0 = 0, \ldots, V(r) - 1$, dann ist

$$\text{a) für } r \geq q : U_q(y) \supseteq U_r(w_{j_0}), \tag{34a}$$

$$\text{b) für } r \leq q : U_r(w_{j_0}) \supseteq U_q(y). \tag{34b}$$

Sei $I(q,p) = \{j,\, 0 \le j \le V(r)-1 : U_q(y) \cap U_r(w_j) \neq \emptyset\}$. Für $r \le q$ ist $I(q,p)$ einelementig, $I(q,p) = \{j_0\}$. Es gilt

$$\text{im Fall a) } U_q(y) = \bigcup_{j \in I(q,p)} U_r(w_j), \tag{35a}$$

$$\text{im Fall b) } U_r(w_{j_0}) \supseteq U_q(y). \tag{35b}$$

Angenommen die Folge $(x_m)_m$ ist gleichverteilt in G. Dann gibt es ein $M_0 = M_0(r)$, sodass für alle $M \ge M_0(r)$ gilt

$$\frac{1}{V(r)}\left(1 - \frac{1}{V(r)}\right) \le \frac{\#\left(U_r(w_j); M\right)}{M} \le \frac{1}{V(r)}\left(1 + \frac{1}{V(r)}\right) \tag{36}$$

für $j = 0, \ldots, V(r)-1$.

Dann gilt bei Gleichung (35a):

$$\mu\left(U_q(y)\right) = {}^1\!/_{V(q)} = \sum_{j \in I(q,p)} \frac{1}{V(r)} = \frac{\#I(q,p)}{V(r)} \tag{37}$$

und weiters

$$\frac{\#\left(U_q(y); M\right)}{M} = \left(\sum_{j \in I(q,p)} \#\left(U_r(w_j); M\right)\right) \cdot \frac{1}{M}. \tag{38}$$

Daraus folgt

$$\mu\left(U_q(y)\right)\left(1 - \frac{1}{V(r)}\right) \le \frac{\#\left(U_q(y); M\right)}{M} \le \mu\left(U_q(y)\right)\left(1 + \frac{1}{V(r)}\right) \tag{39}$$

und weiters nach Gleichung (37):

$$\frac{\#\left(I(q,p)\right)}{V(r)}\left(1 - \frac{1}{V(r)}\right) \le \frac{\#\left(U_q(y); M\right)}{M} \le \frac{\#\left(I(q,p)\right)}{V(r)}\left(1 + \frac{1}{V(r)}\right). \tag{40}$$

Aus Gleichung (39) folgt

$$-\frac{\mu\left(U_q(y)\right)}{V(r)} \le \frac{\#\left(U_q(y); M\right)}{M} - \mu\left(U_q(y)\right) \le \frac{\mu\left(U_q(y)\right)}{V(r)}, \tag{41}$$

und auch

$$-\frac{\#I(q,p)}{V(r)^2} \le \frac{\#\left(U_1(y); M\right)}{M} - \mu\left(U_q(y)\right) \le \frac{\#I(q,p)}{V(r)^2}. \tag{42}$$

Da $\mu\left(U_1(y)\right) \le 1$, folgt aus Gleichung (41):

$$-\frac{1}{V(r)} \le \frac{\#\left(U_q(y); M\right)}{M} - \mu\left(U_q(y)\right) \le \frac{1}{V(r)}. \tag{43}$$

Also erhalten wir bei Gleichung (35a) für alle $M \geq M_0(r)$:

$$\left| \frac{\#\left(U_q(y); M\right)}{M} - \mu\left(U_q(y)\right) \right| \leq \frac{1}{V(r)} < \varepsilon. \tag{44}$$

Wir kommen nun zu Gleichung (35b):
Hier ist für ein j_0, $0 \leq j_0 \leq V(r)-1$, $U_r(w_{j_0}) \supseteq U_q(y)$. Nach Gleichung (36) haben wir wieder für $M \geq M_0(r)$

$$\frac{1}{V(r)}\left(1 - \frac{1}{V(r)}\right) \leq \frac{\#\left(U_r(w_{j_0}), M\right)}{M} \leq \frac{1}{V(r)}\left(1 + \frac{1}{V(r)}\right). \tag{45}$$

Es ist $\mu\left(U_r(y_{j_0})\right) = 1/V(r) \geq \mu\left(U_q(y)\right) = 1/V(r)$. Weiters ist

$$\frac{\#\left(U_q(y); M\right)}{M} \leq \frac{\#\left(U_r(y_{j+0}); M\right)}{M}. \tag{46}$$

Es gilt trivial in Gleichung (35b)

$$\left(\mu\left(U_q(y)\right) - \frac{1}{V(r)}\right)\left(1 - \frac{1}{V(r)}\right) \leq \frac{\#\left(U_q(y); M\right)}{M}. \tag{47}$$

Also gilt mit Gleichung (45) und Gleichung (46):

$$\begin{aligned} (\mu(U_q(y)) - \tfrac{1}{V(r)})(1 - \tfrac{1}{V(r)}) &\leq \frac{\#(U_q(y); M)}{M} \\ &\leq \tfrac{1}{V(r)}(1 + \tfrac{1}{V(r)}) \\ &\leq (\mu(U_q(y)) + \tfrac{1}{V(r)})(1 + \tfrac{1}{V(r)}). \end{aligned} \tag{48}$$

Also ausmultipliziert:

$$\begin{aligned} \mu(U_q(y)) - \frac{1}{V(r)} - \frac{\mu(U_q(y))}{V(r)} + \frac{1}{V(r)^2} \leq \frac{\#(U_q(y); M)}{M}, \\ \frac{\#(U_q(y); M)}{M} \leq \mu(U_q(y)) + \frac{1}{V(r)} + \frac{\mu(U_q(y))}{V(r)} + \frac{1}{V(r)^2}. \end{aligned} \tag{49}$$

Also gilt wegen $\mu\left(U_q(y)\right) \leq 1$:

$$-\frac{2}{V(r)} + \frac{1}{V(r)^2} \leq \frac{\#\left(U_q(y); M\right)}{M} - \mu\left(U_q(y); M\right) \leq \frac{2}{V(r)} + \frac{1}{V(r)^2}. \tag{50}$$

Also gilt auch bei Gleichung (35b) für $M \geq M_0(r)$

$$\left| \frac{\#\left(U_q(y); M\right)}{M} - \mu\left(U_q(y)\right) \right| \leq \frac{2}{V(r)} + \frac{1}{V(r)^2} < \varepsilon. \tag{51}$$

Wenn wir die Diskrepanz der Folge $(x_m)_m$ durch

$$D_M = \sup\left\{ \left| \frac{\#\left(U_q(y); M\right)}{M} - \mu\left(U_q(y)\right) \right|,\ y \in G,\ q = 1, 2, \ldots \right\} \tag{52}$$

definieren, gilt der

Satz 13. *Die Folge* $(x_m)_m$ *ist gleichverteilt in* G *genau dann wenn* $\lim_{M\to\infty} D_M = 0$.

Dass die Bedingung hinreichend ist, ist offensichtlich.
Wie schätzen nun die Diskrepanz der Folge $x_m = w_m = w_1^m,\ m = 0, 1, 2, \ldots$ ab:
Betrachte ein beliebiges Intervall $U_r(w_n)$, mit $r \in \mathbb{N},\ n \in \mathbb{Z}$ fest, sowie $x_0, \ldots, x_m, \ldots x_{M-1}$ $M = 1, 2, \ldots$. Dann ist $M = K \cdot V(r) + L$ mit $0 \leq L \leq V(r)$. sei $A(M; r, n)$ die Anzahl der Folgenglieder in $U_r(w_n)$:

$$A(M) = A(M; r, n) = \#\left\{x_m \in U_r(w_n), 0 \leq m \leq M-1\right\}. \tag{53}$$

Dabei gilt: $x_m \in U_r(w_n) \iff n_0 \equiv m \mod V(r)$.
Für $V(r) = 1$ gibt es nichts abzuschätzen, also sei $V(r) > 1$. Wir sehen unmittelbar die beiden Fälle:

$$\text{a) } A(M) = K, \qquad \text{falls } 0 \leq L < n < V(r) - 1, \tag{54a}$$

$$\text{b) } A(M) = K + 1, \qquad \text{falls } 0 \leq n \leq L < V(r) - 1. \tag{54b}$$

Im Falle von Gleichung (54a) erhalten wir:

$$\frac{A(M)}{M} - \frac{1}{V(r)} = \frac{K}{K \cdot V(r) + L} - \frac{1}{V(r)} = -\frac{1}{M} \cdot \frac{L}{V(r)}, \tag{55}$$

also

$$\left|\frac{A(M)}{M} - \frac{1}{V(r)}\right| \leq \frac{1}{M} \cdot \frac{L}{V(r)} \leq \frac{1}{M}. \tag{56}$$

Im Fall von Gleichung (54b) ergibt sich:

$$\begin{aligned} \frac{A(M)}{M} - \frac{1}{V(r)} &= \frac{K}{M} + \frac{1}{M} - \frac{1}{V(r)} \\ &= -\frac{L}{V(r)} \cdot \frac{1}{M} + \frac{1}{M} \\ &= \frac{1}{M}\left(\frac{V(r) - L}{V(r)}\right) \\ &\leq \frac{1}{M}, \end{aligned} \tag{57}$$

also insgesamt

$$\frac{1}{M} \cdot \frac{1}{V(r)} \leq \frac{A(M)}{M} - \frac{1}{V(r)} \leq \frac{1}{M}. \tag{58}$$

Für $V(r) = 1$ oder $M = 1$ ist trivial $0 = {}^{A(M)}/_{M} - {}^{1}/_{V(r)}$.
Wegen $\mu\left(U_r(w_n)\right) = {}^{1}/_{V(r)}$ gilt also der Sachverhalt:

Für die Folge $x_m = w_1^m,\ m = 0, 1, \ldots$ gilt

$$D_M = \sup_{n,r} \left| \frac{A\left(M; r, n\right)}{M} - \mu\left(U_r(w_n)\right) \right| \leq \frac{1}{M}. \tag{59}$$

Wir geben nun eine Abschätzung von D_M nach unten und beweisen den folgenden

Satz 14. *Ist* $x_1, \ldots, x_m, \ldots x_M \in G$ *und* $r(M)$ *bestimmt durch*

$$V\left(r(M) - 1\right) \leq M < V\left(r(M)\right),$$

so gilt $D_M \geq 1/V(r(M))$.

Diese Abschätzung ist nicht verbesserbar.

Beweis. G zerfällt in

$$G = \bigcup_{n=0}^{V(r(M))-1} U_{r(M)}(w_n).$$

Da $M < V\left(r(M)\right)$, gibt es ein $n_0,\ 0 \leq n_0 \leq V\left(r(M)\right) - 1$, sodass das Intervall $U_{r(M)}(W_{n_0})$ keines der $x_m,\ m = 1, \ldots, M$, enthält. Folglich gilt:

$$\begin{aligned} D_M &= \sup_{r,y} \left| \frac{A\left(M; U_r(y)\right)}{M} - \mu\left(U_r(y)\right) \right| \\ &\geq \left| \frac{A\left(M; U_{r(M)}(w_{n_0})\right)}{M} - \frac{1}{V\left(r(M)\right)} \right| \\ &= \frac{1}{V\left(r(M)\right)}, \end{aligned} \tag{60}$$

was zu zeigen war.

□

Wir verwenden nun die Knoten $x_m = w_m = w_1^m$ mit dem Generator w_1 zur numerischen Integration von Funktionen mit absolut konvergenter Fourierreihe.

Definition 15. Eine Funktion

$$P_r(X) = \sum_{b \in B} C(b) \gamma_b(x) \tag{61}$$

heißt trigonometrisches Polynom der Ordnung r, wenn $C(b) = 0$ für $h(b) \leq r$.

Feststellung 5. Die Integrationsmethode

$$I_M(l) = \frac{1}{M} \sum_{m=1}^{M-1} f(x_m) \tag{62}$$

ist für die Stützstellen $x_m = w_1^m,\ m = 0, \ldots, V(r) - 1$ exakt, falls f ein trigonometrisches Polynom der Maximalordnung r ist.

Beweis. Für $\gamma_2(x_m) = \exp(2\pi i p^m/q)$ und $1 \leq h(b) \leq r)$ gilt

$$\frac{1}{V(r)} \sum_{m=0}^{V(r)-1} \exp(2\pi i p \cdot {}^m/_q) = 0, \tag{63}$$

und für $q = 1 = p$ ist

$$\frac{1}{V(r)} \sum_{m=0}^{V(r)-1} 1 = 1. \tag{64}$$

□

Daraus ergibst sich sofort der

Satz 16. *Hat $f(x)$ die absolut konvergente Fourierreihe*

$$f(x) = \sum_{b \in B} \hat{f}(b)\gamma_b(x), \tag{65}$$

so ergibt sich mit $M = V(r)$

$$|R_M(f)| = \left| \frac{1}{M} \sum_{m=0}^{V(r)-1} f(w_m) - \int_b f \mathrm{d}\mu \right| = \sum_{|h(b)|>r} \left| \hat{f}(b) \right|. \tag{66}$$

Diese langsame Konvergenz hat eine Entsprechung auf dem s-dimensionalen Torus T^s, wo für kartesische Produkte von eindimensionalen Regeln der „curse of dimensionality“wirkt. Wir wählen daher wie in [4] eine andere Funktionenklasse: Für das erzeugende Element $w_1 = (\exp(2\pi i p/q))_{b \in B}$, $b = (q, p)$ ist für jeden nicht trivialen Charakter γ_0 der Wert $\langle w_1, p \rangle = \exp(2\pi i p/q) \neq 1$. Sei nun A_1 die Klasse aller Funktionen $f(x)$ mit

$$N(f) = \sum_{\gamma}{}' \left| \hat{f}(\gamma) \right| (|1 - \gamma(w_1)|)^{-1} < \infty, \tag{67}$$

dann gilt für den Quadraturfehler mit den Knoten $x_m = w_1^m = w_m,\ m = 0, \ldots, M-1$

$$|R_M(f)| = \left| \frac{1}{M} \sum_{m=0}^{M-1} f(w_1^m) - \int_G f(x) \mathrm{d}\mu \right| \leq \sum_{\gamma'} |\hat{f}(\gamma)| \cdot (|1 - \gamma(w_1)|)^{-1} \cdot 2M, \tag{68}$$

da ja für nicht triviale Charaktere γ gilt:

$$\left| \frac{1}{M} \sum_{m=0}^{M-1} \langle w_1^k, \gamma \rangle \right| = \frac{1}{M} \left| \frac{1 - \langle w_1, \gamma \rangle^M}{1 - \langle w_1, \gamma \rangle} \right| \leq \frac{2}{M} \frac{1}{|1 - \langle w_1, \gamma \rangle|}. \tag{69}$$

Also gilt der

Satz 17. *Für $f \in A_1$ und die Knoten w_m, $m = 0, 1, 2, \ldots$ gilt*

$$|R_M(f)| = \left| \frac{1}{M} \sum_{m=0}^{M-1} f(w_m) - \int_G f(x) \mathrm{d}\mu \right| \leq \frac{2}{M} N(f). \tag{70}$$

Dieser Ansatz Gleichung (67) wird in [4, 5] auf kompakten Gruppen ausführlich diskutiert, wobei auch Quadraturmethoden höherer Ordnung behandelt werden. Der Spezialfall unserer Gruppe G legt eine spezielle Funktionenklasse A_2 nahe: Offensichtlich haben wir

$$\begin{aligned} \exp\left(2\pi i p/q\right) - q &= \exp\left(\pi i p/q\right) \left(\exp\left(\pi i p/q\right) - \exp\left(-\pi i p/q\right)\right) \\ &= \exp\left(\pi i p/q\right) \cdot \sin\left(\pi p/q\right) \cdot 2i. \end{aligned}$$

Also ist für $q > 1$

$$2 \geq \left|\exp\left(p/q\right) - 1\right| \geq \frac{2}{q},$$

woraus sich mit $\gamma \iff (q, p) \in B$

$$\sum_{\gamma}{}' \left|\hat{f}(b)\right| \left(|1 - \langle w_1, \gamma\rangle|\right)^{-1} \leq \sum_{\gamma}{}' |\hat{f}(\gamma)| \cdot q \tag{71}$$

ergibt. Das führt zur

Definition 18. Die Funktionenklasse A_2 sei die Klasse der Funktionen mit

$$\sum_{p}{}' |\hat{f}(\gamma)| \cdot q < \infty. \tag{72}$$

Offensichtlich ist $A_2 \subseteq A_1$ und für $f \in A_2$ gilt $R_M = O(1/M)$. Diese Ordnung $R_M = O(1/M)$ ist im folgenden Sinn bestmöglich:

Satz 19. *Ist x_1 Generator der kompakten Gruppe H und B eine Funktionenklasse von $f : H \to \mathbb{C}$, die einen nicht trivialen Charakter enthält, so ist eine Fehlerabschätzung $R_M = o(1/M)$ nicht möglich.*

Beweis. Angenommen, es gibt ein x_1, sodass auf B gilt

$$R_M = o\left(\frac{1}{M}\right). \tag{73}$$

Sei γ ein nicht trivialer Charakter in B. Es gilt $\int \gamma d\mu = 0$ und folglich wäre nach Annahme:

$$\sum_{m=0}^{M-1} \langle x_1^m, \gamma\rangle = o(1), \tag{74a}$$

$$\sum_{m=0}^{M} \langle x_1^m, \gamma\rangle = o(1), \tag{74b}$$

$$\sum_{m=0}^{M} - \sum_{m=0}^{M-1} = \langle x_1, \gamma\rangle^M = o(1). \tag{74c}$$

Der Widerspruch $|\langle x_1, \gamma\rangle| = 1 = o(1)$ beweist den Satz.

□

Es zeigt sich nun eine weitere Besonderheit der Gruppe G: Ist $\mathcal{G}G$ die Menge aller Generatoren der Gruppe G, so haben alle $x \in \mathcal{G}G$ die gleichen „diophantischen“ Eigenschaften, nämlich $|1 - \gamma_z(x)| \geq {}^2/_{q(b)}$ für alle nicht trivialen Charaktere $\gamma_b,\ b = (q,p),\ q \neq 1$.
Wir schließen so: Jedes $x = (x(b))_{b\in B} \in \mathcal{G}G$, also x ist Generator von G, hat die Komponenten $x(b) = \exp\left(2\pi i {}^{p(b)}/_{q(b)}\right),\ b \in B,\ b = (q,p)$, wobei $p(b) \not\equiv 0 \mod q(b)$ ist, da ja $x \in \mathcal{G}G$ ein Generator von G ist. Es folgt sofort mit $<< t >> := \min\{g \in \mathbb{Z} : |t - g|\}$ die Abschätzung

$$|1 - \exp\left(2\pi i {}^{a}/_{q}\right)| \geq \frac{2}{q}. \tag{75}$$

Diese Abschätzung gilt also nicht nur für den speziellen Generator $w_1 = \left(\exp\left(w\pi i {}^{p}/_{q}\right)\right)_{b\in B}$, der $\Gamma = \{z = \exp(2\pi i p q)\}$ erzeugt, sondern für alle Generatoren $x \in \mathcal{G}G$ der Gruppe G. Bekanntlich hat die Menge der Generatoren einer unendlichen Gruppe das volle Maß, wobei $\mathcal{G}G$ offensichtlich nicht abzählbar ist.
Wir fassen zusammen:

Satz 20. *Die Funktionenklassen A_1 und A_2 fallen für alle Generatoren $x \in \mathcal{G}G$ der Gruppe G zusammen und für Funktionen $f(x)$ aus A_2 gilt für jeden Generator $x \in \mathcal{G}G$*

$$|R_\Gamma(f,x)| = \left|\frac{1}{M}\sum_{m=0}^{M-1} f(x^m) - I(1)\right| \leq \frac{1}{M}{\sum_{\gamma}}' |\hat{f}(\gamma)|. \tag{76}$$

Diese Abschätzung ist der Ordnung nach nicht verbesserbar.

Literatur

[1] M. Drmota and R. F. Tichy. *Sequences, Discrepancies and Applications*, volume 1651 of *Lecture Notes in Mathematics*. Springer, 1997.

[2] L. Kuipers and H. Niederreiter. *Uniform Distribution of Sequences*. John Wiley, 1974.

[3] W. Rudin. *Fourier Analysis on Groups*. John Wiley, 1962.

[4] P. Zinterhof. Diaphonien auf kompakten Gruppen. https://preprints.zinterhof.com. Preprint.

[5] P. Zinterhof. Fastperiodische Funktionen, Quadratur, Interpolation und Gleichverteilung auf LCA-Groups. https://preprints.zinterhof.com. Preprint.

[6] P. Zinterhof. Über Punktfolgen, Hilberträume mit reproduzierendem Kern, Integration und Interpolation. https://preprints.zinterhof.com. Preprint.