

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY



NEROVNOSTI PRE GOWERSOVE NORMY

DIPLOMOVÁ PRÁCA

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

NEROVNOSTI PRE GOWERSOVE NORMY

DIPLOMOVÁ PRÁCA

Študijný program: Ekonomicko-finančná matematika a modelovanie
Študijný odbor: Matematika
Školiace pracovisko: Katedra aplikovanej matematiky a štatistiky
Vedúci práce: Mgr. Martin Niepel, PhD.



Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bc. Marek Rakús
Študijný program: ekonomicko-finančná matematika a modelovanie
(Jednoodborové štúdium, magisterský II. st., denná forma)
Študijný odbor: matematika
Typ záverečnej práce: diplomová
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Nerovnosti pre Gowersove normy
Inequalities for Gowers norms

Anotácia: 1. Nerovnosti medzi p - a q -normami na C^n vedú v limitnom prípade k inklúziám medzi l_p priestormi. Pre Gowersove normy $U_{\{d,l\}}$ platia niektoré podobné nerovnosti triviálne, ale nezdá sa, že by nerovnosti a prípadné vzťahy inklúzií boli dostatočne preskúmané/známe.
2. Youngova nerovnosť dáva ohraničenie r -normy pre konvolúciu: $\|f * g\|_r \leq \|f\|_p \|g\|_q$. Platnosť podobného typu nerovnosti sa dá očakávať aj pre Gowersove normy (normy uniformity) a zovšeobecnenia konvolúcií.

Cieľ: 1. Nájsť vzťahy medzi p -normami a rôznymi Gowersovými $U_{\{d,l\}}$ -normami. Identifikovať možné inklúzie medzi priestormi l_p a $u_{\{d,l\}}$ pre nekonečné postupnosti, resp. vhodné funkcie na S^1 .
2. Pomocou Fourierovej duality a techník odvodiť nerovnosti Youngovho typu pre Gowersove normy.

Vedúci: Mgr. Martin Niepel, PhD.
Katedra: FMFI.KAMŠ - Katedra aplikovanej matematiky a štatistiky
Vedúci katedry: doc. Mgr. Igor Melicherčík, PhD.
Dátum zadania: 11.01.2022

Dátum schválenia: 14.01.2022

prof. RNDr. Daniel Ševčovič, DrSc.
garant študijného programu

.....
študent

.....
vedúci práce

Ďakujem vedúcemu práce Mgr. Martinovi Niepelovi, PhD. za odovzdané vedomosti, venovaný čas, užitočné rady a trpezlivosť. A v neposlednom rade, že som mohol objavovať zaujímavú časť matematiky.

Abstrakt v štátnom jazyku

RAKÚS, Marek: Nerovnosti pre Gowersove normy [Diplomová práca], Univerzita Komenského v Bratislave, Fakulta matematiky, fyziky a informatiky, Katedra aplikovanej matematiky a štatistiky; školiteľ: Mgr. Martin Niepel, PhD., Bratislava, 2023, 74 s.

V našej práci sa zaoberáme uniformnými normami rádu d a stupňa l definovanými v článku M. Niepela [7]. V práci najskôr uvádzame prehľad diskkrétnej Fourierovej transformácie na grupe zvyškových tried po delení číslom N . Odvodíme identity na základe Poissonovej sumačnej formuly vyššieho rádu. Definujeme Gowersove uniformné normy a následne aj ich zovšeobecnenia - uniformné normy rádu d a stupňa l . Tieto zovšeobecnenia definujeme novým spôsobom, pomocou maticových podmienok. Prehľad vlastností uniformných noriem rádu d a stupňa l využívame na odvodenie nerovností medzi uniformnými normami vzhľadom na rád d a stupeň l . Na základe dokázaných nerovností naznačíme, aké inklúzie priestorov funkcií môžu existovať v prípade nekonečných Abelovských grúp. Na záver dokážeme jednu analógiu Youngovej konvolučnej nerovnosti, v ktorej bude vystupovať ohraňenie pomocou novej normy.

Kľúčové slová: diskrétna Fourierova transformácia, Gowersove uniformné normy, autokorelácia, ekvivalencia noriem, normované priestory, Youngova konvolučná nerovnosť

Abstract

RAKÚS, Marek: Inequalities for Gowers norms [Master Thesis], Comenius University in Bratislava, Faculty of Mathematics, Physics and Informatics, Department of Applied Mathematics and Statistics; Supervisor: Mgr. Martin Niepel, PhD., Bratislava, 2023, 74 p.

Our thesis focuses on uniformity norms of order d and degree l , which are defined in working paper by M. Niepel [7]. Firstly, we present overview of discrete Fourier transform on group of integers modulo N . We derive identities based on higher order Poisson summation formula. Next, we define Gowers uniformity norms and follow up with their generalizations - uniformity norms of order d and degree l . These generalizations are defined in a new way using matrix equations as a condition. Overview of properties of uniformity norms of order d and degree l is then used to derive inequalities between uniformity norms with different order d or degree l . We use derived inequalities to indicate, what sort of inclusions of function spaces may exist for infinite Abelian groups. Lastly, we prove one analogy of Young's convolution inequality, where boundary by newly defined norm appears.

Keywords: discrete Fourier transform, Gowers uniformity norms, autocorrelation, equivalence of norms, normed spaces, Young's convolution inequality

Obsah

Zoznam použitých symbolov	9
Úvod	10
1 Diskrétna Fourierova analýza vyšších rádov	11
1.1 Poissonova sumačná formula vyšších rádov	15
1.2 Gowersove uniformné normy	23
2 $U(d,l)$ normy	31
2.1 Uniformné usporiadanie podmnožín	32
2.2 $U(d,l)$ (polo)normy	38
3 Nerovnosti pre $U(d,l)$ normy	48
3.1 Autokorelácie vyšších rádov	56
3.2 Youngova konvolučná nerovnosť	66
Záver	73
Zoznam použitej literatúry	74

Zoznam použitých symbolov

$\mathbb{Z}_N$	grupa zvyškových tried po delení číslom N
$\widehat{\mathbb{Z}}_N$	duálna grupa charakterov na $\mathbb{Z}_N$
$\mathbb{Z}_N^d$	d -násobný priamy súčin $\mathbb{Z}_N$
$\widehat{\mathbb{Z}}_N^d$	d -násobný priamy súčin $\widehat{\mathbb{Z}}_N$
$\mathbb{C}(\mathbb{Z}_N)$	priestor funkcií $f : \mathbb{Z}_N \rightarrow \mathbb{C}$, vektorový priestor s N -zložkovými vektormi so zložkami v $\mathbb{C}$
$\mathbb{C}(\widehat{\mathbb{Z}}_N)$	priestor funkcií $F : \widehat{\mathbb{Z}}_N \rightarrow \mathbb{C}$
$\mathbb{S}^1$	jednotková kružnica (unit circle)
$\mathbb{C}(\mathbb{S}^1)$	priestor funkcií definovaných na jednotkovej kružnici $f : \mathbb{S}^1 \rightarrow \mathbb{C}$
$\mathbb{C}(\mathbb{Z})$	priestor obojstranných nekonečných postupností, resp. priestor funkcií definovaných na celých číslach $F : \mathbb{Z} \rightarrow \mathbb{C}$
x	premenná v $\mathbb{Z}_N$
χ	premenná v $\widehat{\mathbb{Z}}_N$
$\mathbf{x}$	vektor v $\mathbb{Z}_N^d$, $\mathbf{x} = \begin{bmatrix} x_1 & x_2 & \cdots & x_d \end{bmatrix}^T$
x_i	i -ta zložka vektora $\mathbf{x}$
$\boldsymbol{\chi}$	vektor v $\widehat{\mathbb{Z}}_N^d$, $\boldsymbol{\chi} = \begin{bmatrix} \chi_1 & \chi_2 & \cdots & \chi_d \end{bmatrix}^T$
χ_i	i -ta zložka vektora $\boldsymbol{\chi}$
$\mathbf{A}_{r \times s}$	matica $\mathbf{A}$ s r riadkami a s stĺpcami
A_{ij}	zložka matice $\mathbf{A}$ v i -tom riadku a j -tom stĺpci
$\text{rank}(\mathbf{A})$	hodnota matice $\mathbf{A}$
$\text{Diag}(\mathbf{x})$	diagonálna matica, ktorej diagonálu tvoria zložky vektora $\mathbf{x}$
$\mathbf{A}$	množina
$\emptyset$	prázdna množina
$ \mathbf{A} $	počet prvkov množiny $\mathbf{A}$
f	funkcia definovaná na $\mathbb{Z}_N$, $f : \mathbb{Z}_N \rightarrow \mathbb{C}$
F	funkcia definovaná na $\widehat{\mathbb{Z}}_N$, $F : \widehat{\mathbb{Z}}_N \rightarrow \mathbb{C}$

$\mathcal{F}f$	diskrétna Fourierova transformácia funkcie f
$\mathcal{F}^{(-1)}F$	inverzná diskrétna Fourierova transformácia funkcie F
z	znamienko, $z \in \{\pm 1\}$
$\mathbf{z}$	vektor znamienok, $\mathbf{z} \in \{\pm 1\}^d$
i	imaginárna jednotka, $i = \sqrt{-1}$
$\bar{c}$	komplexne združené číslo $c = a + i b$, $a, b \in \mathbb{R}$, $\bar{c} = a - i b$
${}^z\bar{c}$	znamienkovo združené číslo $c = a + i b$, $a, b \in \mathbb{R}$, ${}^z\bar{c} = a + z i b$
ω	N -tá odmocnina z 1, $\omega = \exp\left(\frac{2\pi i}{N}\right)$
$\mathcal{H}$	podgrupa $\mathbb{Z}_N^d$
$ \mathcal{H} $	počet prvkov podgrupy $\mathcal{H}$
$\widehat{\mathcal{H}}$	podgrupa $\widehat{\mathbb{Z}}_N^d$, duálna podgrupa
$\mathcal{H}^\perp$	podgrupa $\widehat{\mathbb{Z}}_N^d$, ortogonálny doplnok $\mathcal{H}$, obsahuje vektory kolmé na vektory z $\mathcal{H}$ (resp. anihilujúce vektory z $\mathcal{H}$), $\mathcal{H}^\perp = \left\{ \boldsymbol{\chi} \in \widehat{\mathbb{Z}}_N^d \mid \boldsymbol{x}^\top \boldsymbol{\chi} = 0, \boldsymbol{x} \in \mathcal{H} \right\}$
$\mathcal{H}^{\perp \mathbf{z}}$	podgrupa $\widehat{\mathbb{Z}}_N^d$, obsahuje vektory kolmé na súčin matice $\mathbf{Diag}(\mathbf{z})$ a vektorov z $\mathcal{H}$ (resp. anihilujúce súčin matice $\mathbf{Diag}(\mathbf{z})$ a vektorov z $\mathcal{H}$), $\mathcal{H}^{\perp \mathbf{z}} = \left\{ \boldsymbol{\chi} \in \widehat{\mathbb{Z}}_N^d \mid \boldsymbol{x}^\top \mathbf{Diag}(\mathbf{z}) \boldsymbol{\chi} = 0, \boldsymbol{x} \in \mathcal{H} \right\}$

Úvod

Nové pohľady na použitie diskkrétnej Fourierovej transformácie v aditívnej kombinatorike priniesol T. Gowers článkom [4], v ktorom novým spôsobom dokázal Szemerédiho vetu. Navyše sa týmto postupom dokázali nové kvantitatívne ohraničenia v Szemerédiho vete, ktoré nebolo možné dosiahnuť kombinatorickým prístupom, resp. použitím ergodickej teórie. Zavedenie Gowersových uniformných noriem viedlo k objavu nových prepojení medzi funkcionálnou analýzou a aditívnou kombinatorikou s dôsledkami pre rôzne oblasti matematiky, v ktorých je skúmaná náhodnosť, napríklad rozloženie prvočísel. Tieto prepojenia približuje T. Tao v [11]. Využitie Fourierovej analýzy vyšších rádov v aditívnej kombinatorike je popísané v prehľadovom článku T. Gowersa [5], z ktorého sme čerpali.

Užitočným sa vďaka práci T. Gowersa stal pojem Gowersových uniformných noriem rádu d . M. Niepel v pracovnom článku [7] definuje uniformné normy rádu d a stupňa l na konečných Abelovských grupách ako zovšeobecnenie Gowersových uniformných noriem. Toto zovšeobecnenie navyše zahŕňa aj 2^d -normy funkcií na konečných Abelovských grupách a 2^d -normy ich diskrétnych Fourierových transformácií. Ako dôležité prepojenie sa v článku [7] ukazuje zovšeobecnenie Parsevalovej identity, ktoré prepája uniformné normy rádu d a stupňa l funkcií na konečných Abelovských grupách s uniformnými normami rádu d a stupňa $d - l - 1$ ich diskrétnych Fourierových transformácií.

Uniformné normy rádu d a stupňa l definujeme na konečnorozmerných priestoroch, preto platí, že sú ekvivalentné. Vďaka ekvivalentnosti noriem existujú nerovnosti medzi uniformnými normami vzhľadom na rád d a stupeň l . Takéto nerovnosti pre štandardné Gowersove uniformné normy sú známe, pre ich zovšeobecnenia to tak nie je, keďže predstavujú nový pojem v pracovnom článku M. Niepela [7]. Niektoré nerovnosti sú pomerne ľahko overiteľné pomocou zovšeobecnenia Cauchy-Schwarzovej nerovnosti, avšak iné budú vyžadovať ďalšie tvrdenia. Na overenie nerovností medzi uniformnými normami definujeme zovšeobecnenie autokorelácie funkcie f . Nerovnosti medzi normami majú ako dôsledok inklúzie priestorov funkcií s konečnou normou.

Youngova konvolučná nerovnosť z článku W. Younga [12] predstavuje klasický výsledok štandardnej funkcionálnej analýzy. Táto nerovnosť opäť porovnáva normy, konkrétne p -normy. Ako vyzerá analógia Youngovej konvolučnej nerovnosti pre uniformné normy rádu d a stupňa l nie je okamžite zrejmé.

Obsah našej práce tvorí prehľad nástrojov diskkrétnej Fourierovej analýzy vyšších rádo, uniformných noriem rádu d a stupňa l a následné nerovnosti medzi normami. Uniformné normy rádu d a stupňa l definujeme novým spôsobom, pomocou matíc podmienok. Odvádzame nové zovšeobecnenia autokorelácie, ktoré využívame na nový prístup k známym identitám a dôkaz nerovností medzi uniformnými normami. Nerovnosti medzi uniformnými normami využívame, aby sme ukázali, aké sa dajú očakávať inklúzie medzi priestormi funkcií s konečnou uniformnou normou rádu d a stupňa l (za predpokladu existencie limitného prechodu). Na záver sa venujeme zovšeobecneniam Youngovej konvolučnej nerovnosti, ktoré nás privedú k definícii novej normy. V práci poukazujeme na miesta, kde je možné vo výskume pokračovať.

1 Diskrétna Fourierova analýza vyšších rádo

Táto kapitola sa zaoberá diskrétnou Fourierovou transformáciou na komutatívnej grupe zvyškových tried po delení číslom N , ktorú budeme označovať $\mathbb{Z}_N$. Predpokladáme, že tvrdenia uvádzané v tejto kapitole by bolo možné zovšeobecniť pre ľubovoľné konečné abelovské grupy, pre ľahšiu čitateľnosť textu ale budeme pracovať so $\mathbb{Z}_N$. Okrem $\mathbb{Z}_N$ budeme pracovať aj s k nej duálnou grupou charakterov, ktorú budeme označovať $\hat{\mathbb{Z}}_N$.

Definícia 1.1 (DFT a IDFT). *Diskrétna Fourierova transformácia (ďalej DFT) funkcie $f : \mathbb{Z}_N \rightarrow \mathbb{C}$ je funkcia $\mathcal{F}f : \hat{\mathbb{Z}}_N \rightarrow \mathbb{C}$ s predpisom*

$$\mathcal{F}f(\chi) = \mathcal{F}[f(x)](\chi) = N^{-1} \sum_{x \in \mathbb{Z}_N} f(x) \exp\left(-\frac{2\pi i x \chi}{N}\right),$$

kde i je imaginárna jednotka, $i^2 = -1$.

Inverzná diskrétna Fourierova transformácia (ďalej IDFT) funkcie $F : \hat{\mathbb{Z}}_N \rightarrow \mathbb{C}$ je funkcia $\mathcal{F}^{(-1)}F : \mathbb{Z}_N \rightarrow \mathbb{C}$ s predpisom

$$\mathcal{F}^{(-1)}F(x) = \mathcal{F}^{(-1)}[F(\chi)](x) = \sum_{\chi \in \hat{\mathbb{Z}}_N} F(\chi) \exp\left(\frac{2\pi i x \chi}{N}\right).$$

Označme $\omega = \exp\left(\frac{2\pi i}{N}\right)$.

Ako sme uviedli vyššie, $\hat{\mathbb{Z}}_N$ je grupa charakterov, duálna k $\mathbb{Z}_N$. Dá sa ukázať, že $\hat{\mathbb{Z}}_N$ je izomorfná s grupou zvyškových tried po delení číslom N , tento izomorfizmus však nie je kanonický.

Presnejšie, $\widehat{\mathbb{Z}}_N$ definujeme ako grupu homomorfizmov z aditívnej grupy zvyškových tried po delení číslom N ($\mathbb{Z}_N, +$) do grupy nenulových komplexných čísel s operáciou súčinu $(\mathbb{C} \setminus \{0\}, \cdot)$. Pre $\chi \in \mathbb{Z}$, $\chi \geq 0$ definujeme zobrazenie $\chi : (\mathbb{Z}_N, +) \rightarrow (\mathbb{C} \setminus \{0\}, \cdot)$ predpisom

$$\chi : x \mapsto \omega^{x\chi}. \quad (1)$$

Pri značení zobrazení pomocou χ sa ukáže aditívna štruktúra

$$\chi + \chi' : x \mapsto \underbrace{\omega^{x\chi} \omega^{x\chi'}}_{\text{bodový súčin zobrazení v } (\mathbb{C}, \cdot)} = \omega^{x(\chi + \chi')},$$

teda súčin zobrazení χ a χ' zodpovedá súčtu čísel χ a χ' v $\mathbb{Z}$.

Lahko sa nahliadne, že ide o homomorfizmus a tiež, že zobrazenia χ a χ' sú zhodné ak $\chi \equiv \chi' \pmod{N}$

$$\chi' : x \mapsto \omega^{x\chi'} = \omega^{x(\chi + kN)} = \omega^{x\chi} \underbrace{\omega^{xkN}}_{\exp(2\pi i xk)=1} = \omega^{x\chi},$$

pre nejaké $k \in \mathbb{Z}$.

Grupu homomorfizmov môžeme reprezentovať N zobrazeniami $\chi \in \{0, 1, \dots, N-1\}$. Množina $\{0, 1, \dots, N-1\}$ s operáciou sčítania, zodpovedajúca $\widehat{\mathbb{Z}}_N$, je izomorfná s $\mathbb{Z}_N$.

Keďže homomorfizmus $(\mathbb{Z}_N, +) \rightarrow (\mathbb{C} \setminus \{0\}, \cdot)$ je jednoznačne určený obrazom generátora $\bar{1} \in \mathbb{Z}_N$, ktorý má rád N , každý homomorfizmus musí mať tvar (1).

Rozlíšenie medzi $\mathbb{Z}_N$ a $\widehat{\mathbb{Z}}_N$ je dôležité, keďže izomorfizmus nie je kanonický a v limitnom prípade $N \rightarrow \infty$ neplatí. Priestoru $\mathbb{C}(\mathbb{Z}_N)$ zodpovedá v limite pre $N \rightarrow \infty$ priestor funkcií definovaných na jednotkovej kružnici $\mathbb{C}(\mathbb{S}^1)$ (vzhľadom na použitú mieru na $\mathbb{Z}_N$). V prípade priestoru $\mathbb{C}(\widehat{\mathbb{Z}}_N)$ povedie limitný proces pre $N \rightarrow \infty$ k (obojsmerným) nekonečným postupnostiam Fourierových koeficientov, ktoré zodpovedajú funkciám definovaným na $\mathbb{Z}$ - priestoru $\mathbb{C}(\mathbb{Z})$.

Lema 1.2. *Nech $a \in \mathbb{Z}$. Platí*

$$\sum_{x=0}^{N-1} \omega^{ax} = \begin{cases} N, & \text{ak } a = CN, C \in \mathbb{Z}, \\ 0 & \text{inak.} \end{cases}.$$

Dôkaz. Pre $a = CN$, $C \in \mathbb{Z}$ platí

$$\omega^a = \omega^{CN} = \exp(2\pi i C) = 1.$$

Odtiaľ vyplýva

$$\sum_{x=0}^{N-1} \omega^a = \sum_{x=0}^{N-1} 1 = N.$$

Nech $a \neq CN$, $C \in \mathbb{Z}$. Platí $\omega^a \neq 1$. Upravujme výraz prenášobený nenulovou konštantou $\omega^a - 1$

$$(\omega^a - 1) \sum_{x=0}^{N-1} \omega^{ax} = \sum_{x=0}^{N-1} \omega^{a(x+1)} - \sum_{x=0}^{N-1} \omega^{ax} = \omega^{aN} - \omega^0 = 0,$$

kde sme využili, že $\omega^{aN} = \exp(2\pi ia) = 1$. □

Označme operátor komplexného združenia komplexného čísla $c \in \mathbb{C}$, $c = a + bi$, $a, b \in \mathbb{R}$ podľa znamienka $z \in \{\pm 1\}$ ako ${}^z\bar{c} = a + zbi$. V prípade, že $z = -1$, budeme písať iba $(-1)\bar{c} = \bar{c}$, čo je štandardné označenie pre komplexné združenie. Platí ${}^z\overline{\omega^x} = \omega^{zx}$, podľa vzťahu $e^{i\theta} = \cos(\theta) + i\sin(\theta)$.

Veta 1.3. *Inverzné zobrazenie k DFT je IDFT.*

Dôkaz. DFT môžeme charakterizovať ako lineárne zobrazenie $\mathbb{C}(\mathbb{Z}_N) \rightarrow \mathbb{C}(\widehat{\mathbb{Z}}_N)$ dané maticou $\mathbf{A}$, so zložkami $A_{ij} = N^{-1}\omega^{-ij}$, $i, j \in \{0, 1, \dots, N-1\}$ s predpisom

$$\mathbf{F} = \mathbf{A}\mathbf{f},$$

kde $f_i = f(i)$ a $F_i = \mathcal{F}f(i)$, $i \in \{0, 1, \dots, N-1\}$. Podobne IDFT je lineárne zobrazenie $\widehat{\mathbb{Z}}_N \rightarrow \mathbb{Z}_N$ dané maticou $\mathbf{B}$, so zložkami $B_{ij} = \omega^{ij}$, $i, j \in \{0, 1, \dots, N-1\}$.

Pre zložky súčinu týchto matíc podľa lemy 1.2 platí

$$AB_{ij} = N^{-1} \sum_{k=0}^{N-1} \omega^{-ik+kj} = N^{-1} \sum_{k=0}^{N-1} \omega^{k(i-j)} = \begin{cases} 1, & \text{ak } i = j, \\ 0 & \text{inak,} \end{cases}$$

teda matica $\mathbf{AB}$ je identická matica.

Zároveň z lemy 1.2 vyplýva

$$\begin{aligned} [A^\top \bar{A}]_{ij} &= N^{-2} \sum_{k=0}^{N-1} \omega^{-ik+kj} = \begin{cases} N^{-1}, & \text{ak } i = j, \\ 0 & \text{inak,} \end{cases} \\ [B^\top \bar{B}]_{ij} &= \sum_{k=0}^{N-1} \omega^{ik-kj} = \begin{cases} N, & \text{ak } i = j, \\ 0 & \text{inak,} \end{cases} \end{aligned}$$

čo znamená, že stĺpce matice $\mathbf{A}$ sú navzájom ortogonálne, taktiež stĺpce matice $\mathbf{B}$ sú navzájom ortogonálne.

Keďže stĺpce v maticiach A a B sú ortogonálne, DFT a IDFT sú regulárne zobrazenia. Zloženie regulárnych zobrazení DFT a IDFT dané maticou $\mathbf{AB}$ je identita, preto sú tieto zobrazenia navzájom inverzné. $\square$

Podgrupu $\mathbb{Z}_N^d$ budeme označovať $\mathcal{H}$, podgrupu $\widehat{\mathbb{Z}}_N^d$ budeme označovať $\widehat{\mathcal{H}}$ a $|\mathcal{H}|$ bude označovať počet prvkov podgrupy $\mathcal{H}$.

Definícia 1.4 (diskrétny integrály). *Nech $d \in \mathbb{N}$, $f : \mathbb{Z}_N^d \rightarrow \mathbb{C}$ a $\mathcal{H}$ je nejaká podgrupa $\mathbb{Z}_N^d$. Diskrétny integrál funkcie f na podgrupe $\mathcal{H}$ definujeme ako očakávanú funkčnú hodnotu funkcie f na $\mathcal{H}$*

$$\mathbb{E}_{\mathbf{x} \in \mathcal{H}} f(\mathbf{x}) = |\mathcal{H}|^{-1} \sum_{\mathbf{x} \in \mathcal{H}} f(\mathbf{x}).$$

Nech $F : \widehat{\mathbb{Z}}_N^d \rightarrow \mathbb{C}$ a $\widehat{\mathcal{H}}$ je nejaká podgrupa $\widehat{\mathbb{Z}}_N^d$. Na duálnej podgrupe $\widehat{\mathcal{H}}$ definujeme diskrétny integrál funkcie F ako súčet funkčných hodnôt funkcie F na $\widehat{\mathcal{H}}$, $\sum_{\boldsymbol{\chi} \in \widehat{\mathcal{H}}} F(\boldsymbol{\chi})$.

V prípade, že, $\mathcal{H} = \mathbb{Z}_N^d$, alebo $\widehat{\mathcal{H}} = \widehat{\mathbb{Z}}_N^d$, budeme väčšinou písať iba $\mathbb{E}_{\mathbf{x}}$ a $\sum_{\boldsymbol{\chi}}$.

Poznámka: Očakávaná hodnota $\mathbb{E}$ je iné označenie pre strednú hodnotu $\mathbf{E}(X)$ náhodnej premennej X . Keďže všetky prvky podgrupy $\mathcal{H}$ sú v nej zastúpené rovnakou váhou, X má rovnomerné rozdelenie. Diskrétny integrál $\mathbb{E}_{\mathbf{x} \in \mathcal{H}} f(\mathbf{x})$ zodpovedá strednej hodnote náhodnej premennej $Y = f(X)$. Očakávaná funkčná hodnota v tomto prípade zodpovedá priemeru funkčných hodnôt. Voľba miery v diskretnom integráli $\sum_{\boldsymbol{\chi} \in \widehat{\mathcal{H}}} F(\boldsymbol{\chi})$ zodpovedá počítacej miere (counting) na duálnom priestore.

Pomocou diskretných integrálov a označenia $\omega = \exp\left(\frac{2\pi i}{N}\right)$ môžeme zapísať DFT a IDFT ako

$$\mathcal{F}f(\boldsymbol{\chi}) = \mathbb{E}_{\mathbf{x}} f(\mathbf{x}) \omega^{-\mathbf{x}\boldsymbol{\chi}}, \quad \mathcal{F}^{(-1)}F(\mathbf{x}) = \sum_{\boldsymbol{\chi}} F(\boldsymbol{\chi}) \omega^{\mathbf{x}\boldsymbol{\chi}}.$$

Ďalej zavedieme značenie pre DFT a IDFT podľa d premenných pre funkcie d premenných $f : \mathbb{Z}_N^d \rightarrow \mathbb{C}$, $F : \widehat{\mathbb{Z}}_N^d \rightarrow \mathbb{C}$

$$\mathcal{F}^{(d)}f(\boldsymbol{\chi}) = \mathbb{E}_{\mathbf{x}} f(\mathbf{x}) \omega^{-\mathbf{x}^\top \boldsymbol{\chi}}, \quad \mathcal{F}^{(-d)}F(\mathbf{x}) = \mathbb{E}_{\boldsymbol{\chi}} F(\boldsymbol{\chi}) \omega^{\mathbf{x}^\top \boldsymbol{\chi}}.$$

Platí obdoba Fubiniho vety pre diskrétné integrály

$$\begin{aligned}
\mathcal{F}^{(d)} f(\chi) &= \mathbb{E}_x \underbrace{f(x)}_{\text{označíme } f_{x_2, \dots, x_d}(x_1)} \omega^{-x^\top \chi} \\
&= \mathbb{E}_{x_2, \dots, x_d} \left(\mathbb{E}_{x_1} f_{x_2, \dots, x_d}(x_1) \omega^{-x_1 \chi_1} \right) \omega^{-(x_2 \chi_2 + \dots + x_d \chi_d)} \\
&= \mathbb{E}_{x_2, \dots, x_d} \underbrace{\mathcal{F} f_{x_2, \dots, x_d}(\chi_1)}_{\text{označíme } \mathcal{F} f_{\chi_1}(x_2, \dots, x_d)} \omega^{-(x_2 \chi_2 + \dots + x_d \chi_d)} \\
&= \mathcal{F}^{(d-1)} [\mathcal{F} f_{\chi_1}](\chi_2, \dots, \chi_d) \\
&\vdots \\
&= \mathcal{F} \left[\dots \mathcal{F} [\mathcal{F} f_{\chi_1}]_{\chi_2} \dots \right]_{\chi_d},
\end{aligned} \tag{2}$$

teda DFT podľa viacerých premenných je len viackrát použitá DFT podľa jednotlivých premenných.

Príklad 1.1 (vlastnosti DFT). Označme $f_-(x) = f(-x)$, $\bar{f}(x) = \overline{f(x)}$ a $f_t(x) = f(x+t)$. Vyjadriť DFT týchto funkcií pomocou $\mathcal{F}f$.

Riešenie. Upravujeme DFT funkcií f_- , $\bar{f}$, f_t

$$\mathcal{F}[f_-](\chi) = \mathbb{E}_x f_-(x) \omega^{-x\chi} = \mathbb{E}_x \underbrace{f(-x)}_{\text{označíme } y} \omega^{-x\chi} = \mathbb{E}_y f(y) \omega^{-y(-\chi)} = \mathcal{F}f(-\chi),$$

$$\mathcal{F}[\bar{f}](\chi) = \mathbb{E}_x \bar{f}(x) \omega^{-x\chi} = \mathbb{E}_x \overline{f(x)} \omega^{-x\chi} = \overline{\mathbb{E}_x f(x) \omega^{-x(-\chi)}} = \overline{\mathcal{F}f(-\chi)},$$

$$\mathcal{F}[f_t](\chi) = \mathbb{E}_x f_t(x) \omega^{-x\chi} = \mathbb{E}_x \underbrace{f(x+t)}_{\text{označíme } y} \omega^{-x\chi} = \mathbb{E}_y f(y) \omega^{-y\chi + t\chi} = \mathcal{F}f(\chi) \omega^{t\chi}. \quad \square$$

1.1 Poissonova sumačná formula vyšších rádov

V tejto podkapitole formulujeme Poissonovu sumačnú formulu vyšších rádov (ďalej Poissonova formula), ako sa nachádza v článku M. Niepela [7], avšak s iným dôkazom. Pre prehľadnosť toto tvrdenie uvádzame bez komplexných združení, ktoré doplníme až v dôsledku 1.10.

V bakalárskej práci [8] sme pomocou Poissonovej formuly odvodili zovšeobecnenú konvolučnú identitu pre funkcie $f : \mathbb{Z}_P \rightarrow \mathbb{C}$ (P je prvočíslo), ktorú v tejto práci využijeme na dôkaz tvrdení v kapitole 2. Zovšeobecnenú konvolučnú identitu uvádzame aj s dôkazom v tvrdení 1.8, a to vo všeobecnejšej formulácii pre funkcie $f : \mathbb{Z}_N \rightarrow \mathbb{C}$, ako bola formulácia v bakalárskej práci [8]. Ďalej odvodíme duálnu zovšeobecnenú konvolučnú identitu.

Situáciu skomplikuje fakt, že nepracujeme nutne s konečným poľom $\mathbb{Z}_P$, ale s okruhom $\mathbb{Z}_N$ - preto množiny dané maticovými rovnosťami nemusia mať štruktúru vektorového podpriestoru, ale pôjde o moduly nad $\mathbb{Z}_N$.

Zavedieme značenie pre funkcie

$$\begin{aligned}\delta(x) &= \begin{cases} N, & \text{ak } x = 0, \\ 0 & \text{inak,} \end{cases} & \Delta(\chi) &= \begin{cases} 1, & \text{ak } \chi = 0, \\ 0 & \text{inak,} \end{cases} \\ \mathbf{1}(x) &= 1, & \mathbf{1}(\chi) &= 1. \end{aligned}$$

Funkcie δ a Δ sú diskkrétne Diracove delta funkcie, funkcie s jednobodovým nosičom, ktorých diskrétne integrál na príslušnej grupe je 1.

Označme $\mathcal{H}^\perp$ ortogonálny doplnok podgrupy $\mathcal{H}$. Podgrupa $\mathcal{H}^\perp$ je daná

$$\mathcal{H}^\perp = \left\{ \chi \in \widehat{\mathbb{Z}}_N^d \mid \mathbf{x}^\top \chi = 0, \mathbf{x} \in \mathcal{H} \right\}.$$

Vektory $\mathbf{x}$ a χ sú na seba kolmé práve vtedy, keď $\mathbf{x}^\top \chi = 0$, resp. (ko)vektor $\chi \in \widehat{\mathbb{Z}}_N^d$ anihiluje vektor $\mathbf{x} \in \mathbb{Z}_N^d$.

Lema 1.5. *Nech $\chi \in \widehat{\mathbb{Z}}_N$. Platia identity:*

$$\text{i) } \mathcal{F}\delta(\chi) = \mathbf{1}(\chi),$$

$$\text{ii) } \mathcal{F}\mathbf{1}(\chi) = \Delta(\chi).$$

Nech $d \in \mathbb{N}$, $\mathcal{H}$ je podgrupa $\mathbb{Z}_N^d$, $\chi \in \widehat{\mathbb{Z}}_N^d$. Platí identita

$$\text{iii) } \mathbb{E}_{\mathbf{x} \in \mathcal{H}} \omega^{\mathbf{x}^\top \chi} = \begin{cases} 1, & \text{ak } \chi \in \mathcal{H}^\perp, \\ 0 & \text{inak.} \end{cases}$$

Dôkaz. Prvé dve identity získame priamym výpočtom

$$\begin{aligned}\mathcal{F}\delta(\chi) &= \mathbb{E}_x \delta(x) \omega^{-x\chi} = N^{-1} \delta(0) \omega^0 = 1 = \mathbf{1}(\chi), \\ \mathcal{F}\mathbf{1}(\chi) &= \mathbb{E}_x \omega^{-x\chi} = N^{-1} \underbrace{\sum_{x=0}^{N-1} \omega^{-x\chi}}_{\text{lema 1.2}} = \begin{cases} 1, & \text{ak } \chi = 0, \\ 0 & \text{inak.} \end{cases} \end{aligned}$$

Nech χ je kolmé na každé $\mathbf{x} \in \mathcal{H}$. Zrejme platí

$$\mathbb{E}_{\mathbf{x} \in \mathcal{H}} \omega^{\mathbf{x}^\top \chi} = \mathbb{E}_{\mathbf{x} \in \mathcal{H}} \omega^0 = 1.$$

Nech χ nie je kolmé na všetky vektory z podgrupy $\mathcal{H}$. Upravujme ľavú stranu identity iii)

$$\mathbb{E}_{x \in \mathcal{H}} \omega^{x^\top \chi} = \mathbb{E}_{x \in \mathcal{H}} \exp \left(2\pi i \frac{x^\top \chi}{N} \right).$$

Podgrupu $\mathcal{H}$ môžeme reprezentovať ako k -násobný priamy súčin grúp zvyškových tried $\mathbb{Z}_{N_1}, \mathbb{Z}_{N_2}, \dots, \mathbb{Z}_{N_k}$, $k \leq d$, pričom $N_1, N_2, \dots, N_k$ sú nejaké delitele N . Potom existuje vyjadrenie

$$x_i = A_{i1} \frac{N}{N_1} y_1 + A_{i2} \frac{N}{N_2} y_2 + \dots + A_{ik} \frac{N}{N_k} y_k,$$

pre $i \in \{1, 2, \dots, d\}$, kde $y_j \in \mathbb{Z}_{N_j}$, pre $j \in \{1, 2, \dots, k\}$ a vhodnú maticu $\mathbf{A} \in \mathbb{Z}_N^{d \times k}$. Voľne povedané, násobenie $\frac{N}{N_1} y_1$ mení zvyšok v $\mathbb{Z}_{N_1}$ na zvyšok v $\mathbb{Z}_N$.

Vyjadrenie v maticovom zápise zodpovedá

$$\mathbf{x} = \mathbf{A} \begin{bmatrix} \frac{N}{N_1} & & & \\ & \frac{N}{N_2} & & \\ & & \ddots & \\ & & & \frac{N}{N_k} \end{bmatrix} \mathbf{y}.$$

Hodnotu $\mathbf{x}^\top \chi$ môžeme vyjadriť pomocou $\mathbf{y} \in \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \dots \times \mathbb{Z}_{N_k}$ ako

$$\mathbf{x}^\top \chi = \mathbf{y}^\top \begin{bmatrix} \frac{N}{N_1} & & & \\ & \frac{N}{N_2} & & \\ & & \ddots & \\ & & & \frac{N}{N_k} \end{bmatrix} \underbrace{\mathbf{A}^\top \chi}_{\text{označíme } \varphi} = \mathbf{y}^\top \begin{bmatrix} \frac{N}{N_1} & & & \\ & \frac{N}{N_2} & & \\ & & \ddots & \\ & & & \frac{N}{N_k} \end{bmatrix} \varphi$$

kde $\varphi \in \mathbb{Z}_N^k$.

Ďalej máme

$$\begin{aligned} \mathbb{E}_{x \in \mathcal{H}} \exp \left(2\pi i \frac{x^\top \chi}{N} \right) &= \mathbb{E}_{\mathbf{y} \in \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \dots \times \mathbb{Z}_{N_k}} \exp \left(2\pi i \left(\frac{y_1 \varphi_1}{N_1} + \frac{y_2 \varphi_2}{N_2} + \dots + \frac{y_k \varphi_k}{N_k} \right) \right) \\ &= \prod_{j=1}^k \underbrace{\mathbb{E}_{y_j \in \mathbb{Z}_{N_j}} \exp \left(\frac{2\pi i y_j \varphi_j}{N_j} \right)}_{\omega \text{ na zvyškovej triede } \mathbb{Z}_{N_j}}. \end{aligned}$$

Z lemy 1.2 vyplýva

$$\mathbb{E}_{y_j \in \mathbb{Z}_{N_j}} \exp \left(\frac{2\pi i y_j \varphi_j}{N_j} \right) = \begin{cases} 1, & \text{ak } \varphi_j = C_j N_j, C_j \in \mathbb{Z}, \\ 0 & \text{inak,} \end{cases}$$

pre všetky $j \in \{1, 2, \dots, k\}$. Preto platí

$$\mathbb{E}_{\mathbf{x} \in \mathcal{H}} \omega^{\mathbf{x}^\top \boldsymbol{\chi}} = \begin{cases} 1, & \text{ak pre všetky } j \in \{1, 2, \dots, k\} \text{ platí } \varphi_j = C_j N_j, C_j \in \mathbb{Z}, \\ 0 & \text{inak,} \end{cases}$$

Nech $\boldsymbol{\chi} \notin \mathcal{H}^\perp$, teda pre $\boldsymbol{\chi}$ existuje vektor $\mathbf{x} \in \mathcal{H}$ taký, že platí $\mathbf{x}^\top \boldsymbol{\chi} \neq 0$. Ak platí $\varphi_j = C_j N_j$ pre všetky $j \in \{1, 2, \dots, k\}$, máme $\frac{N}{N_j} \varphi_j = C_j N \equiv 0 \pmod{N}$. Potom pre všetky $\mathbf{x} \in \mathcal{H}$ platí

$$\mathbf{x}^\top \boldsymbol{\chi} = \mathbf{y}^\top \begin{bmatrix} \frac{N}{N_1} & & & \\ & \frac{N}{N_2} & & \\ & & \ddots & \\ & & & \frac{N}{N_k} \end{bmatrix} \boldsymbol{\varphi} \equiv 0 \pmod{N},$$

čo je spor s predpokladom, že $\boldsymbol{\chi} \notin \mathcal{H}^\perp$. □

V leme 1.5 je identita iii) zovšeobecnením identity ii) pre DFT podľa viacerých premenných.

Fakt, že podgrupu $\mathcal{H}$ môžeme reprezentovať ako k -násobný priamy súčin jednorozmerných grúp zvyškových tried $\mathbb{Z}_{N_1}, \mathbb{Z}_{N_2}, \dots, \mathbb{Z}_{N_k}$, $k \leq d$, pričom $N_1, N_2, \dots, N_k$ sú delitele N , je dôsledkom štruktúrálnej vety pre Abelovské grupy, ktorá sa nachádza napríklad v knihe [1, str. 472] a tento dôsledok je známy.

Poissonovu formulu uvádza M. Niepel v článku [7] ako známe tvrdenie. Dôkaz Poissonovej formuly pre podgrupu $\mathbb{Z}_P^d$, kde P je prvočíslo, sme odvodili v bakalárskej práci [8, str. 32]. V tejto práci ďalej uvádzame všeobecnejší dôkaz pre podgrupu $\mathbb{Z}_N^d$, $N \in \mathbb{N}$, ktorý sme odvodili pomocou lemy 1.5.

Veta 1.6 (Poissonova sumačná formula vyššieho rádu). *Nech $d \in \mathbb{N}$, $f_1, f_2, \dots, f_d : \mathbb{Z}_N \rightarrow \mathbb{C}$ a $\mathcal{H}$ je podgrupa $\mathbb{Z}_N^d$. Platí Poissonova sumačná formula vyššieho rádu*

$$\mathbb{E}_{\mathbf{x} \in \mathcal{H}} \prod_{i=1}^d f_i(x_i) = \sum_{\boldsymbol{\chi} \in \mathcal{H}^\perp} \prod_{i=1}^d \mathcal{F} f_i(\chi_i).$$

Dôkaz. Funkcie f_i sú IDFT funkcií $\mathcal{F}f_i$. Upravujme výraz na ľavej strane

$$\begin{aligned}
\mathbb{E}_{\mathbf{x} \in \mathcal{H}} \prod_{i=1}^d f_i(x_i) &= \mathbb{E}_{\mathbf{x} \in \mathcal{H}} \prod_{i=1}^d \sum_{\chi_i} \mathcal{F}f_i(\chi_i) \omega^{x_i \chi_i} \\
&= \mathbb{E}_{\mathbf{x} \in \mathcal{H}} \sum_{\boldsymbol{\chi}} \prod_{i=1}^d \mathcal{F}f_i(\chi_i) \prod_{j=1}^d \omega^{x_j \chi_j} \\
&= \underbrace{\sum_{\boldsymbol{\chi}} \prod_{i=1}^d \mathcal{F}f_i(\chi_i) \mathbb{E}_{\mathbf{x} \in \mathcal{H}} \omega^{\mathbf{x}^\top \boldsymbol{\chi}}}_{\text{lema 1.5}} \\
&= 1 \left(\sum_{\boldsymbol{\chi} \in \mathcal{H}^\perp} \prod_{i=1}^d \mathcal{F}f_i(\chi_i) \right) + 0 \left(\sum_{\boldsymbol{\chi} \notin \mathcal{H}^\perp} \prod_{i=1}^d \mathcal{F}f_i(\chi_i) \right). \quad \square
\end{aligned}$$

Ďalej uvádzame definíciu konvolúcie, krížovej korelácie a autokorelácie. Tieto operácie patria medzi základné nástroje v teórii spracovania diskretných signálov, avšak majú široké použitie v rôznych oblastiach matematiky. Jedným z prepojení týchto pojmov a Fourierovej transformácie je konvolučná identita a jej analógie, ktoré uvádzame v príkladoch 1.2 a 1.3.

Definícia 1.7. *Nech $f, g : \mathbb{Z}_N \rightarrow \mathbb{C}$, $t \in \mathbb{Z}_N$. Definujeme*

- i) *konvolúciu funkcií f a g ako $(f * g)(t) = \mathbb{E}_x f(t - x)g(x)$,*
- ii) *krížovú koreláciu (cross correlation) funkcií f a g ako $(f \star g)(t) = \mathbb{E}_x f(t + x) \overline{g(x)}$,*
- iii) *autokoreláciu funkcie f ako $(f)_K(t) = (f \star f)(t)$.*

Poznámka: Vo všeobecnosti budeme v texte uvádzať definície výrazov obsahujúcich diskretné integrály iba na $\mathbb{Z}_N$. Všetky výrazy definované na $\mathbb{Z}_N$ pomocou diskretného integrálu $\mathbb{E}$, definujeme aj na $\widehat{\mathbb{Z}}_N$ pomocou diskretného integrálu Σ . Napríklad konvolúciu funkcií F a G na $\widehat{\mathbb{Z}}_N$ definujeme $(F * G)(\tau) = \Sigma_{\chi} F(\tau - \chi)G(\chi)$.

Keďže jediné, čo sa zmení v definičnom výraze je použitá miera v diskretnom integráli, teda suma nahradí očakávanú hodnotu (priemer), definície na $\widehat{\mathbb{Z}}_N$ sú plne analogické a nebudeme ich uvádzať.

Príklad 1.2. *Odvodíme konvolučnú identitu $\mathcal{F}[f * g](\tau) = \mathcal{F}f(\tau)\mathcal{F}g(\tau)$.*

Riešenie. Upravujme DFT konvolúcie

$$\begin{aligned}
\mathcal{F}[f * g](\tau) &= \mathbb{E}_t(f * g)(t) \omega^{-t\tau} \\
&= \mathbb{E}_{t,x} f(\underbrace{t-x}_{\text{označíme } y}) g(x) \omega^{-(t-x)\tau - x\tau} \\
&= \mathbb{E}_y f(y) \omega^{-y\tau} \mathbb{E}_x g(x) \omega^{-x\tau} \\
&= \mathcal{F}f(\tau) \mathcal{F}g(\tau). \quad \square
\end{aligned}$$

Ekvivalentný zápis konvolúcie je $(f * g)(t) = \mathbb{E}_{x_1+x_2=t} f(x_1)g(x_2)$. Vďaka vete 1.3 platí, že IDFT je inverzné zobrazenie k DFT. Konvolučná identita je ďalej ekvivalentná $(f * g)(t) = \mathcal{F}^{(-1)}[\mathcal{F}f\mathcal{F}g](t)$. Identita v tvrdení 1.8 je zovšeobecnením konvolučnej identity v tvare

$$\mathbb{E}_{x_1+x_2=t} f(x_1)g(x_2) = \mathcal{F}^{(-1)}[\mathcal{F}f\mathcal{F}g](t).$$

Zovšeobecnenie, ktoré uvádzame, sme odvodili v bakalárskej práci [8, str.47].

Tvrdenie 1.8 (zovšeobecnená konvolučná identita). *Nech $d \in \mathbb{N}$, $f_1, f_2, \dots, f_d : \mathbb{Z}_N \rightarrow \mathbb{C}$, $\mathbf{A} \in \mathbb{Z}_N^{k \times d}$, $\text{rank}(\mathbf{A}) = k$, pričom nulový priestor $\mathbf{A}$ tvorí podgrupu $\mathbb{Z}_N^d$ izomorfnú $\mathbb{Z}_N^{d-k}$, a pre vektor $\mathbf{t} \in \mathbb{Z}_N^k$ existuje riešenie systému $\mathbf{A}\mathbf{x} = \mathbf{t}$. Označme $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_d$ stĺpce matice $\mathbf{A}$. Platí identita*

$$\mathbb{E}_{\mathbf{A}\mathbf{x}=\mathbf{t}} \prod_{i=1}^d f_i(x_i) = \mathcal{F}^{(-k)} \left[\prod_{i=1}^d \mathcal{F}f_i(\mathbf{a}_i^\top \boldsymbol{\tau}) \right] (\mathbf{t}).$$

Dôkaz. Nech podgrupa $\mathcal{H}$ je daná predpisom

$$\mathcal{H} = \left\{ \mathbf{y} \in \mathbb{Z}_N^d \mid \mathbf{A}\mathbf{y} = \mathbf{0} \right\} = \ker(\mathbf{A}),$$

kde $\ker(\mathbf{A})$ je nulový priestor matice $\mathbf{A}$ s predpokladanými vlastnosťami.

Nech vektor $\mathbf{s}$ je nejaké riešenie systému $\mathbf{A}\mathbf{s} = \mathbf{t}$. Upravujme výraz

$$\mathbb{E}_{\mathbf{A}\mathbf{x}=\mathbf{t}} \prod_{i=1}^d f_i(\underbrace{x_i}_{\text{označíme } y_i + s_i}) = \mathbb{E}_{\mathbf{A}\mathbf{y}+\mathbf{A}\mathbf{s}=\mathbf{t}} \prod_{i=1}^d f_i(y_i + s_i) = \mathbb{E}_{\mathbf{A}\mathbf{y}=\mathbf{0}} \prod_{i=1}^d f_i(y_i + s_i) = \mathbb{E}_{\mathbf{y} \in \mathcal{H}} \prod_{i=1}^d \underbrace{f_i(y_i + s_i)}_{\text{označíme } f_i^{s_i}(y_i)}.$$

Použijeme vetu 1.6

$$\mathbb{E}_{\mathbf{y} \in \mathcal{H}} \prod_{i=1}^d f_i^{s_i}(y_i) = \underbrace{\sum_{\chi \in \mathcal{H}^\perp} \prod_{i=1}^d \mathcal{F}f_i^{s_i}(\chi_i)}_{\text{príklad 1.1}} = \sum_{\chi \in \mathcal{H}^\perp} \prod_{i=1}^d \mathcal{F}f_i(\chi_i) \omega^{s_i \chi_i}.$$

Podľa predpokladu je podgrupa $\mathcal{H}$, daná rovnicou $\mathbf{A}\mathbf{y} = \mathbf{0}$, izomorfná z $\mathbb{Z}_N^{d-k}$, teda je $(d-k)$ -rozmerná. V termínoch voľných modulov: podgrupa $\mathcal{H}$ je voľný modul ranku $(d-k)$ nad $\mathbb{Z}_N$ a dá sa vygenerovať pomocou $(d-k)$ riešení rovnice $\mathbf{A}\mathbf{y} = \mathbf{0}$. Podgrupa $\mathcal{H}^\perp$ je potom tiež voľná a má rank k (je k -rozmerná).

Keďže podgrupa $\mathcal{H}$ obsahuje vektory, ktoré sú kolmé na riadky matice $\mathbf{A}$, pre podgrupu $\mathcal{H}^\perp$ preto platí, že je daná práve lineárnymi kombináciami riadkov matice $\mathbf{A}$, čo môžeme zapísať ako

$$\mathcal{H}^\perp = \left\{ \chi \in \widehat{\mathbb{Z}}_N^d \mid \chi = \mathbf{A}^\top \tau, \tau \in \widehat{\mathbb{Z}}_N^k \right\}.$$

Využívame fakt, že pokiaľ nulový priestor matice $\mathbf{A}$ je izomorfný $\mathbb{Z}_N^{d-k}$, riadkový priestor matice $\mathbf{A}$ je izomorfný $\mathbb{Z}_N^k$.

Môžeme preto spraviť substitúciu $\chi = \mathbf{A}^\top \tau$, $\tau \in \widehat{\mathbb{Z}}_N^k$. Táto substitúcia pre $i \in \{1, 2, \dots, d\}$ zodpovedá $\chi_i = \mathbf{a}_i^\top \tau$. Ďalej platí

$$\begin{aligned} \sum_{\chi \in \mathcal{H}^\perp} \prod_{i=1}^d \mathcal{F}f_i(\chi_i) \omega^{s_i \chi_i} &= \sum_{\tau} \prod_{i=1}^d \mathcal{F}f_i(\mathbf{a}_i^\top \tau) \omega^{s_i \mathbf{a}_i^\top \tau} \\ &= \sum_{\tau} \prod_{i=1}^d \mathcal{F}f_i(\mathbf{a}_i^\top \tau) \prod_{j=1}^k \omega^{s_j \mathbf{a}_j^\top \tau} \\ &= \sum_{\tau} \prod_{i=1}^d \mathcal{F}f_i(\mathbf{a}_i^\top \tau) \underbrace{\omega^{\sum_{j=1}^k s_j \mathbf{a}_j^\top \tau}}_{\omega^{(\mathbf{A}\mathbf{s})^\top \tau} = \omega^{\mathbf{t}^\top \tau}} \\ &= \mathcal{F}^{(-k)} \left[\prod_{i=1}^d \mathcal{F}f_i(\mathbf{a}_i^\top \tau) \right] (\mathbf{t}). \end{aligned} \quad \square$$

Podrobnejšie sa problematikou zovšeobecnenia konvolučnej identity zaoberáme v práci [8]. Okrem konvolučnej identity platí aj iná ľahko overiteľná identita, ktorá je v istom zmysle duálna konvolučná identita

$$\sum_{\chi_1 + \chi_2 = \tau} \mathcal{F}f(\chi_1) \mathcal{F}g(\chi_2) = \mathcal{F}[fg](\tau).$$

Nasledujúci dôsledok je zovšeobením duálnej konvolučnej identity.

Dôsledok 1.9 (duálna zovšeobená konvolučná identita). *Nech $d \in \mathbb{N}$, $f_1, f_2, \dots, f_d : \mathbb{Z}_N \rightarrow \mathbb{C}$, $\mathbf{A} \in \widehat{\mathbb{Z}}_N^{k \times d}$ a $\text{rank}(\mathbf{A}) = k$, pričom nulový priestor $\mathbf{A}$ tvorí podgrupu $\widehat{\mathbb{Z}}_N^d$ izomorfnú $\widehat{\mathbb{Z}}_N^{d-k}$, a pre vektor $\tau \in \widehat{\mathbb{Z}}_N^k$ existuje riešenie systému $\mathbf{A}\chi = \tau$. Označme $\alpha_1, \alpha_2, \dots, \alpha_d$ stĺpce matice $\mathbf{A}$. Platí identita*

$$\mathbb{E}_{\mathbf{A}\chi=\tau} \prod_{i=1}^d \mathcal{F}f_i(\chi_i) = \mathcal{F}^{(k)} \left[\prod_{i=1}^d f_i(\alpha_i^\top \mathbf{t}) \right] (\tau).$$

Dôkaz. Postupom analogickým k dôkazu tvrdenia 1.8 by sme overili identitu

$$\mathbb{E}_{\mathbf{A}\chi=\tau} \prod_{i=1}^d F_i(\chi_i) = \mathcal{F}^{(k)} \left[\prod_{i=1}^d \mathcal{F}^{(-1)} F_i(\boldsymbol{\alpha}_i^\top \mathbf{t}) \right] (\boldsymbol{\tau}),$$

ktorá platí pre $F_1, F_2, \dots, F_d : \widehat{\mathbb{Z}}_N \rightarrow \mathbb{C}$.

Ak zvolíme $F_i = \mathcal{F} f_i$ pre $i \in \{1, 2, \dots, d\}$, dostaneme dokazovanú identitu. $\square$

Podobne ako pre konvolúciu platí konvolučná identita, platia analogické identity pre krížovú koreláciu a autokoreláciu.

Príklad 1.3. *Vyjadríme, aké identity platia pre DFT krížovej korelácie a autokorelácie.*

Riešenie. Postupom analogickým k odvodeniu konvolučnej identity máme

$$\begin{aligned} \mathcal{F}[f \star g](\tau) &= \mathbb{E}_t(f * g)(t) \omega^{-t\tau} \\ &= \mathbb{E}_{t,x} f(\underbrace{t+x}_{\text{označíme } y}) \overline{g(x)} \omega^{-(t+x)\tau+x\tau} \\ &= \mathbb{E}_y f(y) \omega^{-y\tau} \overline{\mathbb{E}_x g(x) \omega^{-x\tau}} \\ &= \mathcal{F}f(\tau) \overline{\mathcal{F}g(\tau)}. \end{aligned}$$

Identita pre autokoreláciu je priamym dôsledkom

$$\mathcal{F}(f)_K(\tau) = \mathcal{F}[f \star f](\tau) = |\mathcal{F}f(\tau)|^2. \quad \square$$

Na zovšeobecnenie týchto identít potrebujeme identity dokázané v tvrdení 1.8 a dôsledku 1.9 doplniť o komplexné združenia.

Označme $\mathbf{z}$ ortogonálny doplnok $\mathcal{H}$

$$\mathcal{H}^{\perp \mathbf{z}} = \left\{ \chi \in \widehat{\mathbb{Z}}_N^d \mid \mathbf{x}^\top \mathbf{Diag}(\mathbf{z}) \chi = 0, \mathbf{x} \in \mathcal{H} \right\},$$

kde $\mathbf{z} \in \{\pm 1\}^d$ je vektor znamienok a $\mathbf{Diag}(\mathbf{z})$ je diagonálna matica, ktorá má na diagonále zložky vektora $\mathbf{z}$.

Dôsledok 1.10. *Nech $d \in \mathbb{N}$, $f_1, f_2, \dots, f_d : \mathbb{Z}_N \rightarrow \mathbb{C}$, $\mathcal{H}$ je podgrupa $\mathbb{Z}_N^d$, $\mathbf{z} \in \{\pm 1\}^d$.*

Potom pre komplexne združené funkcie podľa vektora $\mathbf{z}$ platia identity:

i) *Poissonova formula*

$$\mathbb{E}_{\mathbf{x} \in \mathcal{H}} \prod_{i=1}^d \overline{f_i(x_i)} = \sum_{\chi \in \mathcal{H}^{\perp \mathbf{z}}} \prod_{i=1}^d \overline{\mathcal{F}f_i(\chi_i)},$$

ii) *zovšeobecnená konvolučná identita*

$$\mathbb{E}_{\mathbf{A}\mathbf{x}=\mathbf{t}} \prod_{i=1}^d \overline{z_i f_i(x_i)} = \mathcal{F}^{(-k)} \left[\prod_{i=1}^d \overline{z_i \mathcal{F} f_i(z_i \mathbf{a}_i^T \boldsymbol{\tau})} \right] (\mathbf{t}),$$

pre $\mathbf{A} \in \mathbb{Z}_N^{k \times d}$, $\text{rank}(\mathbf{A}) = k$, pričom nulový priestor $\mathbf{A}$ tvorí podgrupu $\mathbb{Z}_N^d$ izomorfnú $\mathbb{Z}_N^{d-k}$, pre vektor $\mathbf{t} \in \mathbb{Z}_N^k$ existuje riešenie systému $\mathbf{A}\mathbf{x} = \mathbf{t}$ a vektory $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_d$ sú stĺpce matice $\mathbf{A}$,

iii) *duálna zovšeobecnená konvolučná identita*

$$\mathbb{E}_{\mathbf{A}\boldsymbol{\chi}=\boldsymbol{\tau}} \prod_{i=1}^d \overline{z_i \mathcal{F} f_i(\chi_i)} = \mathcal{F}^{(k)} \left[\prod_{i=1}^d \overline{z_i f_i(z_i \mathbf{a}_i^T \mathbf{t})} \right] (\boldsymbol{\tau}),$$

pre $\mathbf{A} \in \widehat{\mathbb{Z}}_N^{k \times d}$, $\text{rank}(\mathbf{A}) = k$, pričom nulový priestor $\mathbf{A}$ tvorí podgrupu $\widehat{\mathbb{Z}}_N^d$ izomorfnú $\widehat{\mathbb{Z}}_N^{d-k}$, pre vektor $\boldsymbol{\tau} \in \widehat{\mathbb{Z}}_N^k$ existuje riešenie systému $\mathbf{A}\boldsymbol{\chi} = \boldsymbol{\tau}$ a vektory $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_d$ sú stĺpce matice $\mathbf{A}$.

Dôkaz. Označme $g_i = \overline{z_i f_i}$ pre $i \in \{1, 2, \dots, d\}$. Z príkladu 1.1 vyplýva

$$\mathcal{F} g_i(\chi_i) = \mathcal{F} \left[\overline{z_i f_i} \right] (\chi_i) = \overline{z_i \mathcal{F} f_i(z_i \chi_i)}.$$

Identity vyplývajú z aplikovania vety 1.6 (Poissonova formula), tvrdenia 1.8 (zovšeobecnená konvolučná identita) a dôsledku 1.9 (duálna zovšeobecnená konvolučná identita) na funkcie g_i , pre $i \in \{1, 2, \dots, d\}$. $\square$

V dôsledku 1.10 uvádzame Poissonovu formulu v rovnakom tvare, ako sa nachádza v článku [7]. Identity v dôsledku 1.10 budeme využívať v kapitole 2. Zároveň predpokladáme, že dokázané identity v dôsledku platia aj pre všeobecnú konečnú Abelovskú grupu $\mathcal{G}$, nielen grupu zvyškových tried $\mathbb{Z}_N$. Poissonova formula uvedená v článku [7] je formulovaná pre všeobecnú $\mathcal{G}$ a predpokladáme, že argument v dôkaze zovšeobecenej konvolyčnej identity a duálnej zovšeobecenej konvolyčnej identity bude priamočiaro analogický aj pre $\mathcal{G}$.

1.2 Gowersove uniformné normy

V tejto podkapitole zavedieme Gowersove uniformné normy rádu d a ukážeme ich niektoré základné vlastnosti. V článku [7] definícia Gowersových uniformných noriem predchádza

Poissonovej formule, keďže identity pre Gowersove normy slúžia ako motivácia pre Poissonovu formulu. My sme poradie týchto formulácií vymenili, keďže dôsledky Poissonovej formuly využijeme na odvodenie identity pre Gowersovu uniformnú normu rádu 3 v príklade 1.6.

Na tomto mieste uvádzame najmä motiváciu ku kapitole 2 a podkapitole 3.1, podrobnejšie sa budeme venovať zovšeobecneniam Gowersových uniformných noriem v kapitole 2. O Gowersových uniformných normách píše podrobne T. Tao v knihe [11], taktiež sme sa im venovali v bakalárskej práci [8].

Definícia 1.11 (*p*-norma). *Nech $f : \mathbb{Z}_N \rightarrow \mathbb{C}$, $p \in \mathbb{R}$, $p \geq 1$. Definujeme p -normu funkcie f*

$$\|f\|_p = \left(\mathbb{E}_x |f(x)|^p \right)^{1/p}.$$

Definícia 1.12 (skalárny súčin). *Nech $d \in \mathbb{N}$, $f, g : \mathbb{Z}_N^d \rightarrow \mathbb{C}$ a $\mathcal{H}$ je podgrupa $\mathbb{Z}_N^d$. Skalárny súčin funkcie f s funkciou g na $\mathcal{H}$ definujeme ako*

$$\langle f, g \rangle_{\mathcal{H}} = \mathbb{E}_{\mathbf{x} \in \mathcal{H}} f(\mathbf{x}) \overline{g(\mathbf{x})}.$$

V prípade, že $\mathcal{H} = \mathbb{Z}_N^d$ budeme väčšinou písať len $\langle f, g \rangle$.

Tvrdenie 1.13 (vlastnosti skalárneho súčinu). *Nech $d \in \mathbb{N}$, $f, g : \mathbb{Z}_N^d \rightarrow \mathbb{C}$, $C \in \mathbb{C}$ a $\mathcal{H}$ je podgrupa $\mathbb{Z}_N^d$. Pre skalárny súčin platia identity:*

- i) *komplexná antisymetria $\langle f, g \rangle_{\mathcal{H}} = \overline{\langle g, f \rangle_{\mathcal{H}}}$,*
- ii) *kladná definitnosť $\langle f, f \rangle_{\mathcal{H}} \geq 0$,
pričom rovnosť nastáva pre $f(\mathbf{x}) = 0$, $\forall \mathbf{x} \in \mathcal{H}$,*
- iii) *Cauchy-Schwarzova nerovnosť $|\langle f, g \rangle_{\mathcal{H}}|^2 \leq \langle f, f \rangle_{\mathcal{H}} \langle g, g \rangle_{\mathcal{H}}$,
pričom rovnosť nastáva pre $f(\mathbf{x}) = Cg(\mathbf{x})$ alebo $g(\mathbf{x}) = Cf(\mathbf{x})$, $\forall \mathbf{x} \in \mathcal{H}$.*

Dôkaz. Prvé dve vlastnosti vyplývajú priamo z definície 1.12. Máme

$$\langle f, g \rangle_{\mathcal{H}} = \mathbb{E}_{\mathbf{x} \in \mathcal{H}} f(\mathbf{x}) \overline{g(\mathbf{x})} = \overline{\mathbb{E}_{\mathbf{x} \in \mathcal{H}} g(\mathbf{x}) \overline{f(\mathbf{x})}} = \overline{\langle g, f \rangle_{\mathcal{H}}},$$

$$\langle f, f \rangle_{\mathcal{H}} = \mathbb{E}_{\mathbf{x} \in \mathcal{H}} f(\mathbf{x}) \overline{f(\mathbf{x})} = \mathbb{E}_{\mathbf{x} \in \mathcal{H}} |f(\mathbf{x})|^2 \geq 0,$$

a rovnosť v uvedenej nerovnosti nastane len pre f identicky rovné 0 na $\mathcal{H}$.

Pre $g = Cf$ na $\mathcal{H}$ máme

$$|\langle f, Cf \rangle_{\mathcal{H}}|^2 = |C|^2 |\langle f, f \rangle_{\mathcal{H}}|^2 = \underbrace{\langle f, f \rangle_{\mathcal{H}}}_{\in \mathbb{R}} \langle Cf, Cf \rangle_{\mathcal{H}},$$

teda rovnosť v Cauchy-Schwarzovej nerovnosti.

Prípád, keď f alebo g je identicky rovné 0, zodpovedá $f = 0$ alebo $g = 0$ a nastáva rovnosť v Cauchy-Schwarzovej nerovnosti.

Z kladnej definitnosti a definície 1.12 pre $a \in \mathbb{C}$ vyplýva

$$0 \leq \langle f - ag, f - ag \rangle_{\mathcal{H}} = \langle f, f \rangle_{\mathcal{H}} - a \langle g, f \rangle_{\mathcal{H}} - \bar{a} \langle f, g \rangle_{\mathcal{H}} + |a|^2 \langle g, g \rangle_{\mathcal{H}}.$$

Nech existuje $\mathbf{x} \in \mathcal{H}$, pre ktoré je $g(\mathbf{x}) \neq 0$. Zvoľme $a = \frac{\langle f, g \rangle_{\mathcal{H}}}{\langle g, g \rangle_{\mathcal{H}}}$. Máme

$$\begin{aligned} 0 &\leq \langle f, f \rangle_{\mathcal{H}} - \frac{|\langle f, g \rangle_{\mathcal{H}}|^2}{\langle g, g \rangle_{\mathcal{H}}} - \frac{|\langle f, g \rangle_{\mathcal{H}}|^2}{\langle g, g \rangle_{\mathcal{H}}} + \frac{|\langle f, g \rangle_{\mathcal{H}}|^2}{\langle g, g \rangle_{\mathcal{H}}} \\ &= \langle f, f \rangle_{\mathcal{H}} - \frac{|\langle f, g \rangle_{\mathcal{H}}|^2}{\langle g, g \rangle_{\mathcal{H}}}, \end{aligned}$$

čo po úprave zodpovedá Cauchy-Schwarzovej nerovnosti. □

Dôkaz týchto vlastností je štandardný a známy, napriek tomu sme ho uviedli, aby bolo zrejmé, že Cauchy-Schwarzova nerovnosť platí aj pre funkcie viacerých premenných a skalárne súčiny na ľubovoľnej podgrupe $\mathcal{H}$ priestoru $\mathbb{Z}_N^d$.

Tvrdenie 1.14 (Parsevalova identita). *Nech $d \in \mathbb{N}$, $f, g : \mathbb{Z}_N^d \rightarrow \mathbb{C}$. Platí Parsevalova identita*

$$\langle f, g \rangle_{\mathbf{x}} = \langle \mathcal{F}^{(d)} f, \mathcal{F}^{(d)} g \rangle_{\chi}.$$

Dôkaz. Funkciu f prepíšeme ako IDFT funkcie $\mathcal{F}f$, čo vedie k výsledku

$$\begin{aligned} \langle f, g \rangle_{\mathbf{x}} &= \mathbb{E}_{\mathbf{x}} f(\mathbf{x}) \overline{g(\mathbf{x})} \\ &= \mathbb{E}_{\mathbf{x}} \left(\sum_{\chi} \mathcal{F}^{(d)} f(\chi) \omega^{\mathbf{x}^T \chi} \right) \overline{g(\mathbf{x})} \\ &= \sum_{\chi} \mathcal{F}^{(d)} f(\chi) \overline{\mathbb{E}_{\mathbf{x}} g(\mathbf{x}) \omega^{-\mathbf{x}^T \chi}} \\ &= \sum_{\chi} \mathcal{F}^{(d)} f(\chi) \overline{\mathcal{F}^{(d)} g(\chi)} \\ &= \langle \mathcal{F}^{(d)} f, \mathcal{F}^{(d)} g \rangle_{\chi}. \end{aligned} \quad \square$$

Štandardne sa pod pojmom Parsevalova identita uvádza identita

$$\mathbb{E}_x f(x) \overline{g(x)} = \sum_{\chi} \mathcal{F}f(\chi) \overline{\mathcal{F}g(\chi)},$$

pre funkcie $f, g : \mathbb{Z}_N \rightarrow \mathbb{C}$, ktorej špeciálnym prípadom je identita $\|f\|_2 = \|\mathcal{F}f\|_2$.

Ďalej zavedieme definíciu Gowersovej uniformnej normy, ako ju uvádza napríklad T. Tao v [11, str. 57] alebo B. Szegedy v [10, str. 3].

Definícia 1.15 (Gowersova $U(d)$ (polo)norma). *Nech $f : \mathbb{Z}_N \rightarrow \mathbb{C}$ a $t \in \mathbb{Z}_N$. Multiplikatívnu deriváciu funkcie f v bode x podľa t definujeme*

$$\Delta_t f(x) = f(x+t) \overline{f(x)}.$$

Nech $d \in \mathbb{N}$. Gowersovu uniformnú (polo)normu rádu d funkcie f definujeme ako

$$\|f\|_{U(d)} = \left(\mathbb{E}_{x,a} \Delta_{a_1} \Delta_{a_2} \dots \Delta_{a_d} f(x) \right)^{1/2^d}.$$

Pomocou multiplikatívnej derivácie môžeme prepísať autokoreláciu z definície 1.7 ako

$$(f)_K(t) = \mathbb{E}_x \Delta_t f(x).$$

Pre $d > 1$ je $\|f\|_{U(d)}$ norma funkcie f a $\|f\|_{U(1)}$ je polonorma funkcie f . Polonorma $U(1)$ je polonorma, keďže $\|f\|_{U(1)}$ nie je kladne definitná, teda $\|f\|_{U(1)}$ môže byť 0 pre funkciu f , ktorá nie je identicky rovná nule. Gowersove $U(d)$ normy zaviedol T. Gowers v článku [4, str. 19], kde uvádza aj dôkaz, že $U(d)$ je norma pre $d > 1$.

Jeden z dôvodov, prečo sú $U(d)$ normy zaujímavé je fakt, že sú citlivé na znamienka funkčných hodnôt funkcie f (na rozdiel od p -normiem). Pre p -normy platí, že funkcie f a $|f|$ majú rovnakú p -normu. Ako ukážeme v nasledujúcom príklade, pre $U(d)$ normy to neplatí.

Príklad 1.4. *Pre funkciu $f : \mathbb{Z}_3 \rightarrow \{\pm 1\}$, $f(x) = (-1)^x$ overíme, že platí nerovnosť $\|f\|_{U(2)} < \| |f| \|_{U(2)}$.*

Riešenie. Z definície 1.15 vyplýva

$$\begin{aligned} \|f\|_{U(2)}^4 &= \mathbb{E}_{x,a,b} \Delta_a \Delta_b f(x) \\ &= \mathbb{E}_{x,a,b} \Delta_b f(x+a) \overline{\Delta_b f(x)} \\ &= \mathbb{E}_{x,a,b} f(x+a+b) \overline{f(x+a)} \overline{f(x+b)} \overline{f(x)} \\ &= \mathbb{E}_{x,a,b} f(x+a+b) \overline{f(x+b)f(x+a)} f(x). \end{aligned}$$

Zvyšková trieda $\mathbb{Z}_3$ obsahuje 3 prvky: 0, 1, 2. Spočítajme hodnoty funkcie f v týchto bodoch

$$f(0) = 1, \quad f(1) = -1, \quad f(2) = 1.$$

Určime najskôr $U(2)$ normu funkcie $|f|$

$$\| |f| \|_{U(2)}^4 = \mathbb{E}_{x,a,b} |f(x+a+b)| \overline{|f(x+b)| |f(x+a)|} |f(x)| = \mathbb{E}_{x,a,b} 1 = 1.$$

Súčin $f(x+a+b) \overline{f(x+b)f(x+a)} f(x)$ môže nadobúdať len hodnoty 1 a -1 . Aby platilo $\|f\|_{U(2)} < \| |f| \|_{U(2)}$, musí existovať aspoň jedna trojica $x, a, b \in \{0, 1, 2\}$, pre ktorú platí $f(x+a+b) \overline{f(x+b)f(x+a)} f(x) = -1$. Takých trojíc ale existuje hneď niekoľko, napríklad

$$f(0+1+2) \overline{f(0+2)f(0+1)} f(0) = \underbrace{f(0)}_1 \underbrace{\overline{f(2)}}_1 \underbrace{\overline{f(1)}}_{-1} \underbrace{f(0)}_1 = -1.$$

Nerovnosť $\|f\|_{U(2)} < \| |f| \|_{U(2)}$ teda platí. Konkrétne hodnoty $U(2)$ normy funkcií f a $|f|$ sú

$$\|f\|_{U(2)} = \left(\frac{11}{27}\right)^{1/4} < 1 = \| |f| \|_{U(2)}. \quad \square$$

Nasledujúci príklad vychádza z prehľadového článku T. Gowersa [5, str. 10].

Príklad 1.5. *Odvodíme vzťah medzi $U(2)$ normou funkcie f a 4-normou funkcie $\mathcal{F}f$.*

Riešenie. Upravujme štvrtú mocninu $U(2)$ normy. Podľa príkladu 1.4 platí

$$\|f\|_{U(2)}^4 = \mathbb{E}_{x,a,b} f(x+a+b) \underbrace{\overline{f(x+b)f(x+a)}}_{\text{označíme } y} f(x) = \mathbb{E}_a \underbrace{\mathbb{E}_y f(y+a) \overline{f(y)}}_{(f)_K(a)} \underbrace{\mathbb{E}_x \overline{f(x+a)} f(x)}_{\overline{(f)_K(a)}}.$$

Ďalej môžeme výraz prepísať pomocou skalárneho súčinu a použiť Parsevalovu identitu v tvrdení 1.14

$$\|f\|_{U(2)}^4 = \mathbb{E}_a (f)_K(a) \overline{(f)_K(a)} = \langle (f)_K, (f)_K \rangle = \langle \mathcal{F}[(f)_K], \mathcal{F}[(f)_K] \rangle.$$

Pre autokoreláciu sme už odvodili identitu $\mathcal{F}(f)_K(\tau) = |\mathcal{F}f(\tau)|^2$. Máme

$$\|f\|_{U(2)}^4 = \left\langle |\mathcal{F}f(\tau)|^2, |\mathcal{F}f(\tau)|^2 \right\rangle = \sum_{\chi} |\mathcal{F}f(\chi)|^4 = \|\mathcal{F}f\|_4^4. \quad \square$$

V štandardnom odvodení vzťahu $\|f\|_{U(2)} = \|\mathcal{F}f\|_4$, ako ho uvádza T. Gowers v článku [5, str. 10], sa namiesto autokorelácie využíva konvolúcia $(f * f)$. Pre nás bude vhodnejšiou autokorelácia, ktorej súčasťou je komplexné združenie (na rozdiel od konvolúcie) a vieme nájsť jej zovšeobecnenie, ktoré bude vystupovať v $U(3)$ norme.

V príklade 1.6 uvádzame naše odvodenie identity pre $U(3)$ normu pomocou autokorelácie rádu 2.

Príklad 1.6. Pre $U(3)$ normu pomocou analogickej série argumentov, ako sme použili v príklade 1.5, nájdeme analogickú identitu k identite $\|f\|_{U(2)} = \|\mathcal{F}f\|_4$.

Riešenie. Definujeme autokoreláciu funkcie f rádu 2 predpisom

$$(f)_{K(2)}(a, b) = \mathbb{E}_x f(x + a + b) \overline{f(x + b)f(x + a)} f(x).$$

Označme maticu $\mathbf{P}$ a vektor $\mathbf{z}$

$$\mathbf{P} = \begin{bmatrix} 1 & -1 & & \\ 1 & & -1 & \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad \mathbf{z} = \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix}.$$

Platí ekvivalentné vyjadrenie

$$(f)_{K(2)}(a, b) = \mathbb{E}_{\mathbf{P}\mathbf{x} = \begin{bmatrix} a \\ b \\ 0 \end{bmatrix}} \prod_{i=1}^4 z_i \overline{f_i(x_i)}.$$

Keďže toto vyjadrenie je ekvivalentné, máme splnené predpoklady dôsledku 1.10. Nulový priestor matice $\mathbf{P}$ je izomorfný $\mathbb{Z}_N$, keďže vo vyjadrení autokorelácie diskkrétne integrujeme cez $x \in \mathbb{Z}_N$. Tiež platí rovnosť

$$\begin{bmatrix} 1 & -1 & & \\ 1 & & -1 & \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} a + b \\ b \\ a \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ b \\ 0 \end{bmatrix},$$

teda existuje riešenie systému $\mathbf{P}\mathbf{x} = \begin{bmatrix} a \\ b \\ 0 \end{bmatrix}$.

Podľa dôsledku 1.10 môžeme spočítať diskretnú Fourierovu transformáciu autokorelácie rádu 2. Máme

$$\begin{aligned} (f)_{\mathbf{K}(2)}(a, b) &= \underbrace{\mathbb{E}_{\mathbf{P}x = \begin{bmatrix} a \\ b \\ 0 \end{bmatrix}} \prod_{i=1}^4 z_i \overline{f_i(x_i)}}_{\text{dôsledok 1.10}} \\ &= \mathcal{F}^{(-3)} \left[\mathcal{F}f(\alpha + \beta + \gamma) \overline{\mathcal{F}f(\beta + \gamma) \mathcal{F}f(\alpha + \gamma) \mathcal{F}f(\gamma)} \right] (a, b, 0). \end{aligned}$$

Môžeme použiť vyjadrenie DFT podľa viacerých premenných (2)

$$\begin{aligned} (f)_{\mathbf{K}(2)}(a, b) &= \mathcal{F}^{(-2)} \left[\mathcal{F}^{(-1)} \left[\mathcal{F}f(\alpha + \beta + \gamma) \overline{\mathcal{F}f(\beta + \gamma) \mathcal{F}f(\alpha + \gamma) \mathcal{F}f(\gamma)} \right] (0) \right] (a, b) \\ &= \mathcal{F}^{(-2)} \left[\sum_{\gamma} \mathcal{F}f(\alpha + \beta + \gamma) \overline{\mathcal{F}f(\beta + \gamma) \mathcal{F}f(\alpha + \gamma) \mathcal{F}f(\gamma)} \omega^0 \right] (a, b) \\ &= \mathcal{F}^{(-2)} \left[(\mathcal{F}f)_{\mathbf{K}(2)}(\alpha, \beta) \right] (a, b), \end{aligned}$$

čo vedie k identite

$$\mathcal{F}^{(2)}(f)_{\mathbf{K}(2)}(\alpha, \beta) = (\mathcal{F}f)_{\mathbf{K}(2)}(\alpha, \beta).$$

S identitou pre autokoreláciu rádu 2 môžeme zopakovať kroky argumentu pre $\|f\|_{\mathbf{U}(2)} = \|\mathcal{F}f\|_4$ aj pre $\mathbf{U}(3)$ normu. Upravujme $\mathbf{U}(3)$ normu

$$\begin{aligned} \|f\|_{\mathbf{U}(3)}^8 &= \mathbb{E}_{x, a, b, c} \Delta_a \Delta_b \Delta_c f(x) \\ &= \mathbb{E}_{x, a, b, c} \Delta_a \Delta_b \left(\underbrace{f(x+c) \overline{f(x)}}_{\text{označíme } y} \right) \\ &= \mathbb{E}_{a, b} \mathbb{E}_y \Delta_a \Delta_b f(y) \overline{\mathbb{E}_x \Delta_a \Delta_b f(x)}. \end{aligned}$$

Ďalej platí

$$\begin{aligned} \mathbb{E}_x \Delta_a \Delta_b f(x) &= \mathbb{E}_x \Delta_a f(x+b) \overline{f(x)} \\ &= \mathbb{E}_x f(x+a+b) \overline{f(x+b) f(x+a) f(x)} \\ &= (f)_{\mathbf{K}(2)}(a, b). \end{aligned}$$

Máme vyjadrenie

$$\|f\|_{\mathbf{U}(3)}^8 = \mathbb{E}_{a, b} (f)_{\mathbf{K}(2)}(a, b) \overline{(f)_{\mathbf{K}(2)}(a, b)}.$$

Opäť môžeme výraz prepísať pomocou skalárneho súčinu a použiť Parsevalovu identitu

1.14

$$\|f\|_{U(3)}^8 = \langle (f)_{K(2)}, (f)_{K(2)} \rangle = \langle \mathcal{F}^{(2)}(f)_{K(2)}, \mathcal{F}^{(2)}(f)_{K(2)} \rangle.$$

Z identity pre autokoreláciu rádu 2 vyplýva

$$\|f\|_{U(3)}^8 = \langle (\mathcal{F}f)_{K(2)}, (\mathcal{F}f)_{K(2)} \rangle = \|\mathcal{F}f\|_{U(3)}^8,$$

kde odvodenie rovnosti $\|\mathcal{F}f\|_{U(3)}^8 = \langle (\mathcal{F}f)_{K(2)}, (\mathcal{F}f)_{K(2)} \rangle$ je analogické. $\square$

Príklady 1.5 a 1.6 využívajú analogický postup. Napriek tomu vedú k odlišnému typu výsledkov, v príklade 1.5 k vyjadreniu $U(2)$ normy funkcie f pomocou 4-normy jej DFT, v príklade 1.6 k vyjadreniu $U(3)$ normy funkcie f pomocou $U(3)$ normy jej DFT. Pre vyjadrenie $U(4)$ normy funkcie f by sme dokonca nedosiahli vyjadrenie pomocou žiadnych doposiaľ (v tomto texte) definovaných noriem funkcie $\mathcal{F}f$.

Prirodzenou otázkou je, či je možné definovať normu funkcie $\mathcal{F}f$ (označíme $\|\mathcal{F}f\|_X$), pre ktorú platí $\|f\|_{U(4)} = \|\mathcal{F}f\|_X$. Podobne nás môže zaujímať, či vieme definovať normu funkcie f (označíme $\|f\|_Y$), pre ktorú platí $\|f\|_Y = \|\mathcal{F}f\|_8$. Aj keď by sme mohli priamym výpočtom nájsť predpis noriem X a Y , vhodné by bolo zaviesť všeobecnú definíciu pre ľubovoľný rád d . Potrebujeme teda zaviesť definíciu, ktorá nám dá vyjadrenia

$$\|f\|_{U(d)} = \|\mathcal{F}f\|_{X(d)}, \quad \|f\|_{Y(d)} = \|\mathcal{F}f\|_{2^d},$$

pre ľubovoľný rád d a normy $X(d)$, $Y(d)$ závislé od rádu d . Z príkladov 1.5, 1.6 a Parsevalovej identity vieme, že platí:

- $X(2)$ zodpovedá 4-norme,
- $X(3)$ zodpovedá $U(3)$ norme,
- $Y(2)$ zodpovedá $U(2)$ norme,
- $Y(1)$ zodpovedá 2-norme.

M. Niepel v článku [7] zaviedol pojem uniformných noriem rádu d a stupňa l (ďalej $U(d, l)$ normy), ktoré sú odpoveďou na vyššie uvedené otázky. Ako sa ukáže, identity v príkladoch 1.5 a 1.6 sú zovšeobecnením Parsevalovej identity $\|f\|_2 = \|\mathcal{F}f\|_2$, M. Niepel ich preto označuje ako „*identity Parsevalovho typu*“ [7].

2 $U(d, l)$ normy

V tejto kapitole uvádzame vlastný prístup k definícii uniformných (polo)normiem rádu d a stupňa l (ďalej $U(d, l)$ (polo)normy). Využívame vlastné pojmy uniformného usporiadania podmnožín, podmienok rádu d zodpovedajúcich množine $\mathbb{N}$ a matice podmienok rádu d a stupňa l . Naše definície nepokrývajú všeobecné definície v článku M. Niepela [7] pre ľubovoľnú konečnú Abelovskú grupu $\mathcal{G}$, iba prípad keď $\mathcal{G} = \mathbb{Z}_N$.

Zavedením vlastných definícií sme sa snažili dosiahnuť prehľadnejší a pre čitateľa prístupnejší text, využívajúci matice so zložkami v $\{-1, 0, 1\}$. Taktiež pre nás bolo užitočné mať vlastné definície pri hľadaní nových tvrdení, prepojení so zovšeobecnenou konvolučnou identitou a neskôr v dôkaze nerovností v kapitole 3. Nakoľko využívame iné definície, ako sa nachádzajú v článku M. Niepela [7], uvádzané dôkazy tvrdení sme odvodili nanovo.

Pri definícii $U(d, l)$ (polo)normiem sa často stretujeme s binomickým koeficientom (budeme označovať $\binom{d}{n} = \frac{d!}{(d-n)!n!}$). Súčet prvých n binomických koeficientov označíme

$$\sum_{i=0}^n \binom{d}{i}.$$

Binomický koeficient a súčet binomických koeficientov budú súvisieť s rozmerom priestoru, resp. rankom voľného modulu nad $\mathbb{Z}_N$ v prípade podgrúp $\mathbb{Z}_N^d$, cez ktorý integrujeme v definícii $U(d, l)$ (polo)normy. Bez dôkazu uvádzame nasledujúce známe vlastnosti binomického koeficientu.

Lema 2.1 (vlastnosti binomického koeficientu). *Nech $d \in \mathbb{N}$, $n \in \mathbb{N}$, $1 \leq n \leq d$, $a, b \in \mathbb{R}$. Pre binomické koeficienty platia identity*

$$\text{i) } \binom{d}{n} = \binom{d}{d-n},$$

$$\text{ii) } \binom{d+1}{n} = \binom{d}{n} + \binom{d}{n-1},$$

$$\text{iii) } \sum_{i=d-n}^d \binom{d}{i},$$

$$\text{iv) } \sum_{i=0}^n \binom{d+1}{i} = \sum_{i=0}^n \binom{d}{i} + \sum_{i=0}^{n-1} \binom{d}{i},$$

$$\text{v) binomická veta } (a+b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}.$$

2.1 Uniformné usporiadanie podmnožín

M. Niepel v článku [7] definuje $U(d, l)$ (polo)normy na konečnej abelovskej grupe $\mathcal{G}$ pomocou „ A -značených d -rozmerných l -stupňových kociek v $\mathcal{G}$ “. V našom prístupe zdefinujeme maticové podmienky rádu d a stupňa l $\mathbf{P}(d, l)$. Podgrupa daná riešeniami systému $\mathbf{P}(d, l)\mathbf{x} = \mathbf{0}$ potom bude ekvivalentná priestoru „ A -značených d -rozmerných l -stupňových kociek v $\mathbb{Z}_N$ “. Výhodou nášho prístupu bude, že maticová rovnica je prístupnejšia ako ťažšie predstaviteľný pojem d -rozmerných l -stupňových kociek. Taktiež budeme môcť využiť nástroje lineárnej algebry na operácie s maticami, a teda aj so skúmanými podgrupami.

Definícia 2.2 (uniformné usporiadanie podmnožín). *Nech $d \in \mathbb{N}$. Uniformné usporiadanie podmnožín $\mathbf{N}_1, \mathbf{N}_2, \dots, \mathbf{N}_{2^d} \subseteq \{1, 2, \dots, d\}$ je lineárne usporiadanie všetkých podmnožín $\{1, 2, \dots, d\}$, dané rekurzívnym pravidlom*

$$\forall n \in \{0, 1, \dots, d-1\} \quad \forall i \in \{2^n + 1, 2^n + 2, \dots, 2^{n+1}\} : \quad \mathbf{N}_i = \mathbf{N}_{i-2^n} \cup \{n+1\},$$

s počiatočnou podmienkou $\mathbf{N}_1 = \emptyset$.

Uniformný vektor znamienok $\mathbf{z} \in \{\pm 1\}^{2^d}$ je vektor so zložkami $z_j = (-1)^{|\mathbf{N}_j|}$, pre $j \in \{1, 2, \dots, 2^d\}$.

Pre všetky $j \in \{1, 2, \dots, 2^d\}$ priradíme j -ty riadok identickej matice $\mathbf{I}_{2^d \times 2^d}$ podmnožine $\mathbf{N}_j$, označíme $\mathbf{e}(\mathbf{N}_j)$.

Príklad 2.1. Pre $d = 3$ uvedieme

- i) uniformné usporiadanie podmnožín,
- ii) uniformný vektor znamienok,
- iii) priradenie riadkov matice $\mathbf{I}$ uniformne usporiadaným podmnožinám.

Riešenie. Máme

i) podmnožiny $N_1, N_2, \dots, N_8$

$$\begin{aligned}
N_1 &= \emptyset &= \emptyset &= \emptyset, \\
N_2 &= N_1 \cup \{1\} &= \emptyset \cup \{1\} &= \{1\}, \\
N_3 &= N_1 \cup \{2\} &= \emptyset \cup \{2\} &= \{2\}, \\
N_4 &= N_2 \cup \{2\} &= \{1\} \cup \{2\} &= \{1, 2\}, \\
N_5 &= N_1 \cup \{3\} &= \emptyset \cup \{3\} &= \{3\}, \\
N_6 &= N_2 \cup \{3\} &= \{1\} \cup \{3\} &= \{1, 3\}, \\
N_7 &= N_3 \cup \{3\} &= \{2\} \cup \{3\} &= \{2, 3\}, \\
N_8 &= N_4 \cup \{3\} &= \{1, 2\} \cup \{3\} &= \{1, 2, 3\},
\end{aligned}$$

ii) vektor $\mathbf{z}$

$$\mathbf{z} = \begin{bmatrix} (-1)^{|\emptyset|} \\ (-1)^{|\{1\}|} \\ (-1)^{|\{2\}|} \\ (-1)^{|\{1,2\}|} \\ (-1)^{|\{3\}|} \\ (-1)^{|\{1,3\}|} \\ (-1)^{|\{2,3\}|} \\ (-1)^{|\{1,2,3\}|} \end{bmatrix} = \begin{bmatrix} (-1)^0 \\ (-1)^1 \\ (-1)^1 \\ (-1)^2 \\ (-1)^1 \\ (-1)^2 \\ (-1)^2 \\ (-1)^3 \end{bmatrix} = \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \\ -1 \\ 1 \\ 1 \\ -1 \end{bmatrix},$$

iii) riadky matice $\mathbf{I}_{8 \times 8}$

$$\begin{bmatrix} \mathbf{e}(\emptyset) \\ \mathbf{e}(1) \\ \mathbf{e}(2) \\ \mathbf{e}(1, 2) \\ \mathbf{e}(3) \\ \mathbf{e}(1, 3) \\ \mathbf{e}(2, 3) \\ \mathbf{e}(1, 2, 3) \end{bmatrix} = \begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{bmatrix}.$$

□

Všimnime si, že uvedený uniformný vektor znamienok zodpovedá komplexným združeniam v $U(3)$ norme z definície 1.15. Podobne, ako v príklade 1.4, môžeme $U(3)$ normu

vyjadriť ako

$$\begin{aligned}
\|f\|_{U(3)}^8 &= \mathbb{E}_{x,a,b,c} f(x+a+b+c) \overline{f(x+b+c)f(x+a+c)f(x+c)} \\
&\quad \overline{f(x+a+b)} f(x+b) f(x+a) \overline{f(x)} \\
&= \mathbb{E}_{x,a,b,c} {}^{z_1} \overline{f(x+a+b+c)} {}^{z_2} \overline{f(x+b+c)} {}^{z_3} \overline{f(x+a+c)} {}^{z_4} \overline{f(x+c)} \\
&\quad {}^{z_5} \overline{f(x+a+b)} {}^{z_6} \overline{f(x+b)} {}^{z_7} \overline{f(x+a)} {}^{z_8} \overline{f(x)}.
\end{aligned}$$

Definícia 2.3 (podmienky stupňa n). *Nech $d \in \mathbb{Z}$, $d \geq 0$, $n \in \mathbb{Z}$, $0 \leq n \leq d$ a $\mathbf{N} \subseteq \{1, 2, \dots, d\}$, $|\mathbf{N}| = n$. Podmienka rádu d , zodpovedajúca množine $\mathbf{N}$ je 2^d -rozmerný riadkový vektor definovaný ako*

$$\mathbf{p}_d(\mathbf{N}) = \sum_{a=0}^{|\mathbf{N}|} \sum_{\substack{\mathbf{A} \subseteq \mathbf{N}, \\ |\mathbf{A}|=a}} (-1)^a \mathbf{e}(\mathbf{A}).$$

Nech $\mathbf{N}_1, \mathbf{N}_2, \dots, \mathbf{N}_{2^d}$ je uniformné usporiadanie podmnožín, $l \in \mathbb{Z}$. Maticu podmienok rádu d a stupňa l $\mathbf{P}(d, l)_{2^d \times 2^d}$ definujeme ako

$$\mathbf{P}(d, l) = \begin{bmatrix} \mathbf{p}_d(\mathbf{N}_1), & \text{ak } |\mathbf{N}_1| > l, & \mathbf{0}_{1 \times 2^d} & \text{inak} \\ \mathbf{p}_d(\mathbf{N}_2), & \text{ak } |\mathbf{N}_2| > l, & \mathbf{0}_{1 \times 2^d} & \text{inak} \\ \vdots & & \vdots & \\ \mathbf{p}_d(\mathbf{N}_{2^d}), & \text{ak } |\mathbf{N}_{2^d}| > l, & \mathbf{0}_{1 \times 2^d} & \text{inak} \end{bmatrix}.$$

Poznámka: V texte budeme väčšinou pracovať iba s maticami podmienok rádu d a stupňa $l \in \{-1, 0, \dots, d\}$. V niektorých prípadoch je ale výhodné mať zadefinovanú aj maticu pre stupeň mimo tejto množiny, najmä pokiaľ ide o rekurzívne vyjadrenia.

Vo všeobecnosti bude pre každé n existovať $\binom{d}{n}$ rôznych podmienok $\mathbf{p}_d(\mathbf{N})$ pre $|\mathbf{N}| = n$, keďže používame všetky n -prvkové podmnožiny $\{1, 2, \dots, d\}$.

Podmienka rádu d zodpovedajúca podmnožine $\mathbf{N}_{2^d} = \{1, 2, \dots, d\}$ bude identická s transpozíciou uniformného vektora znamienok

$$\mathbf{p}_d(1, 2, \dots, d) = \mathbf{z}^\top.$$

Príklad 2.2. *Pre $d = 3$ nájdeme podmienky rádu 3 a maticu podmienok rádu 3 a stupňa -1 .*

Riešenie. Pre každú z podmnožín množiny $\{1, 2, 3\}$ máme jednu podmienku rádu 3

$$\begin{bmatrix} \mathbf{p}_3(\emptyset) \\ \mathbf{p}_3(1) \\ \mathbf{p}_3(2) \\ \mathbf{p}_3(1, 2) \\ \mathbf{p}_3(3) \\ \mathbf{p}_3(1, 3) \\ \mathbf{p}_3(2, 3) \\ \mathbf{p}_3(1, 2, 3) \end{bmatrix} = \begin{bmatrix} \mathbf{e}(\emptyset) \\ \mathbf{e}(\emptyset) - \mathbf{e}(1) \\ \mathbf{e}(\emptyset) - \mathbf{e}(2) \\ \mathbf{e}(\emptyset) - \mathbf{e}(1) - \mathbf{e}(2) + \mathbf{e}(1, 2) \\ \mathbf{e}(\emptyset) - \mathbf{e}(3) \\ \mathbf{e}(\emptyset) - \mathbf{e}(1) - \mathbf{e}(3) + \mathbf{e}(1, 3) \\ \mathbf{e}(\emptyset) - \mathbf{e}(2) - \mathbf{e}(3) + \mathbf{e}(2, 3) \\ \mathbf{e}(\emptyset) - \mathbf{e}(1) - \dots - \mathbf{e}(1, 2, 3) \end{bmatrix} = \begin{bmatrix} 1 & & & & & & & \\ 1 & -1 & & & & & & \\ 1 & & -1 & & & & & \\ 1 & -1 & -1 & 1 & & & & \\ 1 & & & & -1 & & & \\ 1 & -1 & & & & -1 & 1 & \\ 1 & & -1 & & -1 & & 1 & \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}.$$

Uvedená matica je zároveň $\mathbf{P}(3, -1)$. □

V príklade 1.6 vystupovala matica $\mathbf{P}$. Táto matica zodpovedá matici podmienok rádu 2 a stupňa 0 $\mathbf{P}(2, 0)$ (okrem nulového riadku)

$$\mathbf{P}(2, 0) = \begin{bmatrix} \mathbf{0}_{1 \times 4} \\ \mathbf{P} \end{bmatrix}.$$

Z príkladu 2.2 môžeme nahliadnuť, ako by sme rekurzívne definovali maticu podmienok rádu $d + 1$ a stupňa -1 . Platí vyjadrenie

$$\mathbf{P}(d + 1, -1) = \left[\begin{array}{c|c} \mathbf{P}(d, -1) & \\ \hline \mathbf{P}(d, -1) & -\mathbf{P}(d, -1) \end{array} \right] = \left[\begin{array}{c|c} \mathbf{P}(d, -1) & \\ \hline \mathbf{P}(d, -2) & -\mathbf{P}(d, -2) \end{array} \right],$$

s počiatočnou podmienkou $\mathbf{P}(0, -1) = [1]$. Pripomenieme, že z definície 2.3 vyplýva $\mathbf{P}(d, -k) = \mathbf{P}(d, -1)$ pre $k \in \mathbb{N}$. Rekurzívne vyjadrenie bude existovať aj pre všeobecný stupeň l .

Tvrdenie 2.4 (rekurzívne vyjadrenie). *Nech $d \in \mathbb{Z}$, $d \geq 0$, $l \in \mathbb{Z}$, $-1 \leq l \leq d + 1$. Matica $\mathbf{P}(d + 1, l)$ má rekurzívne vyjadrenie*

$$\mathbf{P}(d + 1, l) = \left[\begin{array}{c|c} \mathbf{P}(d, l) & \\ \hline \mathbf{P}(d, l - 1) & -\mathbf{P}(d, l - 1) \end{array} \right].$$

Dôkaz. Nech $\mathbf{N}_1, \mathbf{N}_2, \dots, \mathbf{N}_{2^{d+1}} \subseteq \{1, 2, \dots, d + 1\}$ sú uniformne usporiadané podmnožiny. Riadkový vektor $\mathbf{e}(\mathbf{N}_i)$ je i -ty riadok identickej matice $\mathbf{I}_{2^d \times 2^d}$ priradený k podmnožine $\mathbf{N}_i$, $i \in \{1, 2, \dots, 2^d\}$. Označme $\mathbf{e}_{d+1}(\mathbf{N}_i)$ i -ty riadok identickej matice $\mathbf{I}_{2^{d+1} \times 2^{d+1}}$ priradený k podmnožine $\mathbf{N}_i$, $i \in \{1, 2, \dots, 2^{d+1}\}$.

Nech $i \in \{1, 2, \dots, 2^d\}$. Z definície 2.2 vyplýva

$$\begin{aligned} \mathbf{e}_{d+1}(\mathbf{N}_i) &= \left[\mathbf{e}(\mathbf{N}_i) \mid \mathbf{0}_{1 \times 2^d} \right], \\ \mathbf{e}_{d+1}(\mathbf{N}_{i+2^d}) &= \left[\mathbf{0}_{1 \times 2^d} \mid \mathbf{e}(\mathbf{N}_i) \right] = \mathbf{e}_{d+1}(\mathbf{N}_i \cup \{d+1\}). \end{aligned}$$

Pre podmienku rádu $d+1$, zodpovedajúcu podmnožine $\mathbf{N}_i$ platí z definície 2.3

$$\mathbf{p}_{d+1}(\mathbf{N}_i) = \sum_{a=0}^{|\mathbf{N}_i|} \sum_{\substack{\mathbf{A} \subseteq \mathbf{N}_i, \\ |\mathbf{A}|=a}} (-1)^a \mathbf{e}_{d+1}(\mathbf{A}) = \sum_{a=0}^{|\mathbf{N}_i|} \sum_{\substack{\mathbf{A} \subseteq \mathbf{N}_i, \\ |\mathbf{A}|=a}} (-1)^a \left[\mathbf{e}(\mathbf{A}) \mid \mathbf{0}_{1 \times 2^d} \right] = \left[\mathbf{p}_d(\mathbf{N}_i) \mid \mathbf{0}_{1 \times 2^d} \right].$$

Podobne máme vyjadrenie

$$\mathbf{p}_{d+1}(\mathbf{N}_{i+2^d}) = \sum_{a=0}^{|\mathbf{N}_{i+2^d}|} \sum_{\substack{\mathbf{A} \subseteq \mathbf{N}_{i+2^d}, \\ |\mathbf{A}|=a}} (-1)^a \mathbf{e}_{d+1}(\mathbf{A}) = \sum_{a=0}^{|\mathbf{N}_i \cup \{d+1\}|} \sum_{\substack{\mathbf{A} \subseteq (\mathbf{N}_i \cup \{d+1\}), \\ |\mathbf{A}|=a}} (-1)^a \mathbf{e}_{d+1}(\mathbf{A}).$$

Ďalej môžeme sumu cez podmnožiny $\mathbf{A}$ rozdeliť, podľa toho, či $d+1$ patrí do $\mathbf{A}$

$$\begin{aligned} \mathbf{p}_{d+1}(\mathbf{N}_{i+2^d}) &= \sum_{a=0}^{|\mathbf{N}_i \cup \{d+1\}|} \left(\sum_{\substack{\mathbf{A} \subseteq (\mathbf{N}_i), \\ |\mathbf{A}|=a}} (-1)^a \mathbf{e}_{d+1}(\mathbf{A}) + \sum_{\substack{\mathbf{A} \subseteq (\mathbf{N}_i \cup \{d+1\}), \\ d+1 \in \mathbf{A}, \\ |\mathbf{A}|=a}} (-1)^a \mathbf{e}_{d+1}(\mathbf{A}) \right) \\ &= \sum_{a=0}^{|\mathbf{N}_i \cup \{d+1\}|} \left(\sum_{\substack{\mathbf{A} \subseteq (\mathbf{N}_i), \\ |\mathbf{A}|=a}} (-1)^a \mathbf{e}_{d+1}(\mathbf{A}) + \sum_{\substack{\mathbf{A} \subseteq (\mathbf{N}_i), \\ |\mathbf{A} \cup \{d+1\}|=a}} (-1)^a \mathbf{e}_{d+1}(\mathbf{A} \cup \{d+1\}) \right) \\ &= \sum_{a=0}^{|\mathbf{N}_i|} \left(\sum_{\substack{\mathbf{A} \subseteq (\mathbf{N}_i), \\ |\mathbf{A}|=a}} (-1)^a \mathbf{e}_{d+1}(\mathbf{A}) + \sum_{\substack{\mathbf{A} \subseteq (\mathbf{N}_i), \\ |\mathbf{A}|=a}} (-1)^{a+1} \mathbf{e}_{d+1}(\mathbf{A} \cup \{d+1\}) \right). \end{aligned}$$

Prepíšeme výraz pomocou riadkov $\mathbf{e}(\mathbf{A})$ a máme

$$\begin{aligned} \mathbf{p}_{d+1}(\mathbf{N}_{i+2^d}) &= \sum_{a=0}^{|\mathbf{N}_i|} \sum_{\substack{\mathbf{A} \subseteq (\mathbf{N}_i), \\ |\mathbf{A}|=a}} (-1)^a \left[\mathbf{e}(\mathbf{A}) \mid \mathbf{0}_{1 \times 2^d} \right] - \sum_{a=0}^{|\mathbf{N}_i|} \sum_{\substack{\mathbf{A} \subseteq (\mathbf{N}_i), \\ |\mathbf{A}|=a}} (-1)^a \left[\mathbf{0}_{1 \times 2^d} \mid \mathbf{e}(\mathbf{A}) \right] \\ &= \left[\mathbf{p}_d(\mathbf{N}_i) \mid \mathbf{0}_{1 \times 2^d} \right] - \left[\mathbf{0}_{1 \times 2^d} \mid \mathbf{p}_d(\mathbf{N}_i) \right] \\ &= \left[\mathbf{p}_d(\mathbf{N}_i) \mid -\mathbf{p}_d(\mathbf{N}_i) \right]. \end{aligned}$$

Matica $\mathbf{P}(d+1, l)$ je definovaná

$$\mathbf{P}(d+1, l) = \left[\begin{array}{ccc|ccc} \mathbf{p}_{d+1}(\mathbf{N}_1), & \text{ak } |\mathbf{N}_1| > l, & \mathbf{0}_{1 \times 2^d} & \text{inak} & & \\ \vdots & & \vdots & & & \\ \mathbf{p}_{d+1}(\mathbf{N}_{2^d}), & \text{ak } |\mathbf{N}_{2^d}| > l, & \mathbf{0}_{1 \times 2^d} & \text{inak} & & \\ \mathbf{p}_{d+1}(\mathbf{N}_{1+2^d}), & \text{ak } |\mathbf{N}_{1+2^d}| > l, & \mathbf{0}_{1 \times 2^d} & \text{inak} & & \\ \vdots & & \vdots & & & \\ \mathbf{p}_{d+1}(\mathbf{N}_{2^d+2^d}), & \text{ak } |\mathbf{N}_{2^d+2^d}| > l, & \mathbf{0}_{1 \times 2^d} & \text{inak} & & \end{array} \right].$$

Podmienka $|\mathbf{N}_{i+2^d}| > l$ zodpovedá $|\mathbf{N}_i \cup \{d+1\}| > l$, teda $|\mathbf{N}_i| > l-1$, pre $i \in \{1, 2, \dots, 2^d\}$.

Z vyjadrení podmienok rádu $d+1$ pomocou podmienok rádu d vyplýva

$$\begin{aligned} \mathbf{P}(d+1, l) &= \left[\begin{array}{c|ccc} \mathbf{p}_d(\mathbf{N}_1) & \mathbf{0}_{1 \times 2^d}, & \text{ak } |\mathbf{N}_1| > l, & \mathbf{0}_{1 \times 2^d} & \text{inak} \\ \vdots & \vdots & & \vdots & \\ \mathbf{p}_d(\mathbf{N}_{2^d}) & \mathbf{0}_{1 \times 2^d}, & \text{ak } |\mathbf{N}_{2^d}| > l, & \mathbf{0}_{1 \times 2^d} & \text{inak} \\ \hline \mathbf{p}_d(\mathbf{N}_1) & -\mathbf{p}_d(\mathbf{N}_1), & \text{ak } |\mathbf{N}_1| > l-1, & \mathbf{0}_{1 \times 2^d} & \text{inak} \\ \vdots & \vdots & & \vdots & \\ \mathbf{p}_d(\mathbf{N}_{2^d}) & -\mathbf{p}_d(\mathbf{N}_{2^d}), & \text{ak } |\mathbf{N}_{2^d}| > l-1, & \mathbf{0}_{1 \times 2^d} & \text{inak} \end{array} \right] \\ &= \left[\begin{array}{c|c} \mathbf{P}(d, l) & \\ \hline \mathbf{P}(d, l-1) & -\mathbf{P}(d, l-1) \end{array} \right]. \end{aligned}$$

□

Tvrdenie 2.5 (ortogonalita). *Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $-1 \leq l \leq d$. Platí*

$$\mathbf{P}(d, l) \mathbf{Diag}(\mathbf{z}) \mathbf{P}(d, d-l-1)^\top = \mathbf{0}.$$

Dôkaz. Pre $l = -1$ a $l = d$ rovnosť platí

$$\mathbf{P}(d, -1) \mathbf{Diag}(\mathbf{z}) \mathbf{P}(d, d)^\top = \mathbf{P}(d, -1) \mathbf{Diag}(\mathbf{z}) \mathbf{0}^\top = \mathbf{0}.$$

Ďalej uvažujme $0 \leq l \leq d-1$. Nech $\mathbf{N}$ a $\mathbf{M}$ sú dve podmnožiny $\{1, 2, \dots, d\}$. Aby sme dokázali tvrdenie, musíme pre príslušné podmienky ukázať

$$\underbrace{\mathbf{p}_d(\mathbf{N}) \mathbf{Diag}(\mathbf{z}) \mathbf{p}_d(\mathbf{M})^\top}_{\text{označíme } S(\mathbf{N}, \mathbf{M})} = 0,$$

pre všetky $\mathbf{N}, \mathbf{M}$, pričom $l+1 \leq |\mathbf{N}| \leq d$, $d-l \leq |\mathbf{M}| \leq d$.

Keď výraz $S(\mathbf{N}, \mathbf{M})$ rozpíšeme podľa definície 2.3, máme

$$\begin{aligned} S(\mathbf{N}, \mathbf{M}) &= \left(\sum_{a=0}^{|\mathbf{N}|} \sum_{\substack{\mathbf{A} \subseteq \mathbf{N}, \\ |\mathbf{A}|=a}} (-1)^a \mathbf{e}(\mathbf{A}) \right) \mathbf{Diag}(\mathbf{z}) \left(\sum_{b=0}^{|\mathbf{M}|} \sum_{\substack{\mathbf{B} \subseteq \mathbf{M}, \\ |\mathbf{B}|=b}} (-1)^b \mathbf{e}(\mathbf{B}) \right)^{\mathsf{T}} \\ &= \sum_{a=0}^{|\mathbf{N}|} \sum_{b=0}^{|\mathbf{M}|} \sum_{\substack{\mathbf{A} \subseteq \mathbf{N}, \\ |\mathbf{A}|=a}} \sum_{\substack{\mathbf{B} \subseteq \mathbf{M}, \\ |\mathbf{B}|=b}} (-1)^{a+b} \mathbf{e}(\mathbf{A}) \mathbf{Diag}(\mathbf{z}) \mathbf{e}(\mathbf{B})^{\mathsf{T}}. \end{aligned}$$

Súčin vektorov $\mathbf{e}(\mathbf{A})$ a $\mathbf{e}(\mathbf{B})^{\mathsf{T}}$ je nenulový iba pre $\mathbf{A} = \mathbf{B}$ a z definície 2.2 uniformného vektora znamienok máme

$$\underbrace{(-1)^{a+b} \mathbf{e}(\mathbf{A}) \mathbf{Diag}(\mathbf{z}) \mathbf{e}(\mathbf{B})^{\mathsf{T}}}_{(-1)^{|\mathbf{A}|} \mathbf{e}(\mathbf{A}) = (-1)^a \mathbf{e}(\mathbf{A})} = \begin{cases} (-1)^{a+a+a} = (-1)^a, & \text{ak } \mathbf{A} = \mathbf{B}, \\ 0 & \text{inak.} \end{cases}$$

Keďže $\mathbf{A} \subseteq \mathbf{N}$ a $\mathbf{B} \subseteq \mathbf{M}$, z podmienky $\mathbf{A} = \mathbf{B}$ vyplýva $\mathbf{A} = \mathbf{B} \subseteq \mathbf{N} \cap \mathbf{M}$. Vďaka nerovnostiam $|\mathbf{N}| \geq l+1$, $|\mathbf{M}| \geq d-l$ máme $|\mathbf{N}| + |\mathbf{M}| \geq d+1$ a z Dirichletovho princípu vyplýva, že množiny $\mathbf{N}$ a $\mathbf{M}$ musia mať aspoň jeden prvok spoločný, preto $|\mathbf{N} \cap \mathbf{M}| > 0$.

Prepíšeme výraz $S(\mathbf{N}, \mathbf{M})$ pomocou kombinačných čísel a máme

$$S(\mathbf{N}, \mathbf{M}) = \sum_{a=0}^{|\mathbf{N} \cap \mathbf{M}|} \sum_{\substack{\mathbf{A} \subseteq \mathbf{N} \cap \mathbf{M}, \\ |\mathbf{A}|=a}} (-1)^a = \underbrace{\sum_{a=0}^{|\mathbf{N} \cap \mathbf{M}|} \binom{|\mathbf{N} \cap \mathbf{M}|}{a} (-1)^a}_{\text{binomická veta}} = (1-1)^{|\mathbf{N} \cap \mathbf{M}|} = 0. \quad \square$$

2.2 $\mathbf{U}(d, l)$ (polo)normy

$\mathbf{U}(d, l)$ (polo)normy sú v článku M. Niepela [7] dané diskretným integrálom cez podgrupu „ A -značených d -rozmerných l -stupňových kociek v $\mathbb{Z}_N$ “. Vďaka definícii 2.6 môžeme tieto priestory charakterizovať pomocou rovnice $\mathbf{P}(d, l) \mathbf{x} = \mathbf{0}$.

Dôkazy tvrdení v tejto podkapitole využívajú značne odlišné definície ako sa nachádzajú v článku [7], uvádzané dôkazy sú preto nové. Okrem identít, ktorých analógie sa nachádzajú v článku [7], prinášame aj vlastné tvrdenie 2.9, ktoré využíva nami dokázanú zovšeobecnenú konvolučnú identitu.

Definícia 2.6 ($\mathbf{U}(d, l)$ (polo)norma). *Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$ $-1 \leq l \leq d$, $f : \mathbb{Z}_N \rightarrow \mathbb{C}$ a $\mathbf{z} \in \{\pm 1\}^{2^d}$ je uniformný vektor znamienok. Uniformnú (polo)normu rádu d a stupňa l funkcie f definujeme ako*

$$\|f\|_{\mathbf{U}(d, l)} = \left(\mathbb{E}_{\mathbf{P}(d, l) \mathbf{x} = \mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f(x_i)} \right)^{1/2^d}.$$

Nech $f_1, f_2, \dots, f_{2^d} : \mathbb{Z}_N \rightarrow \mathbb{C}$. Zovšeobecnený skalárny súčin rádu d a stupňa l (ďalej $G(d, l)$ skalárny súčin) definujeme ako

$$\langle f_1, f_2, \dots, f_{2^d} \rangle_{G(d, l)} = \mathbb{E}_{\mathbf{P}(d, l) \mathbf{x} = \mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f_i(x_i)}.$$

Nasledujúcu vetu dokázal M. Niepel v článku [7]. V tomto texte jej dôkaz neuvádzame, iba neskôr naznačíme ako postupovať.

Veta 2.7 ($U(d, l)$ je (polo)norma). Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $0 \leq l \leq d - 1$. Platí

- i) $\|f\|_{U(d, l)}$ je norma funkcie f ,
- ii) $\|f\|_{U(d, -1)}$ a $\|f\|_{U(d, d)}$ sú polonormy funkcie f .

Veta 2.8 (dualita $G(d, l)$ skalárnych súčinov). Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $-1 \leq l \leq d$ a $f : \mathbb{Z}_N \rightarrow \mathbb{C}$. Platí dualita

$$\langle f_1, f_2, \dots, f_{2^d} \rangle_{G(d, l)} = \langle \mathcal{F} f_1, \mathcal{F} f_2, \dots, \mathcal{F} f_{2^d} \rangle_{G(d, d-l-1)}.$$

Dôkaz. Označme

$$\mathcal{H} = \left\{ \mathbf{x} \in \mathbb{Z}_N^{2^d} \mid \mathbf{P}(d, l) \mathbf{x} = \mathbf{0} \right\}.$$

Podľa tvrdenia 2.5, stĺpce matice $\mathbf{Diag}(\mathbf{z}) \mathbf{P}(d, d-l-1)^\top$ patria do podgrupy $\mathcal{H}$. Dolná trojuholníková matica $\mathbf{P}(d, l)$ má $\sum_{i=0}^{d-l-1} \binom{d}{i}$ nenulových riadkov, teda podgrupa $\mathcal{H}$ má rozmer $2^d - \sum_{i=0}^{d-l-1} \binom{d}{i} = \sum_{i=l}^d \binom{d}{i} - \sum_{i=0}^{d-l-1} \binom{d}{i} = \sum_{i=l}^d \binom{d}{i}$. Zároveň matica $\mathbf{Diag}(\mathbf{z}) \mathbf{P}(d, d-l-1)^\top$ má $\sum_{i=l}^d \binom{d}{i}$ nenulových stĺpcov, ktoré sú lineárne nezávislé. Počet prvkov priestoru daný lineárnymi kombináciami stĺpcov matice $\mathbf{Diag}(\mathbf{z}) \mathbf{P}(d, d-l-1)^\top$ je rovnaký ako počet prvkov podgrupy $\mathcal{H}$, preto pre každý vektor $\mathbf{x} \in \mathcal{H}$ existuje vyjadrenie pomocou lineárnej kombinácie stĺpcov matice $\mathbf{Diag}(\mathbf{z}) \mathbf{P}(d, d-l-1)^\top$.

Podľa definície 2.6 máme

$$\langle f_1, f_2, \dots, f_{2^d} \rangle_{G(d, l)} = \mathbb{E}_{\mathbf{P}(d, l) \mathbf{x} = \mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f_i(x_i)} = \mathbb{E}_{\mathbf{x} \in \mathcal{H}} \prod_{i=1}^{2^d} z_i \overline{f_i(x_i)}.$$

Z Poissonovej formuly v dôsledku 1.10 vyplýva

$$\mathbb{E}_{\mathbf{x} \in \mathcal{H}} \prod_{i=1}^{2^d} z_i \overline{f_i(x_i)} = \sum_{\chi \in \mathbf{z} \mathcal{H}^\perp} \prod_{i=1}^{2^d} z_i \overline{\mathcal{F} f_i(\chi_i)}.$$

Podgrupa $\mathcal{H}^{\perp \mathbf{z}}$ je daná

$$\mathcal{H}^{\perp \mathbf{z}} = \left\{ \boldsymbol{\chi} \in \widehat{\mathbb{Z}}_N^{2^d} \mid \mathbf{x}^\top \mathbf{Diag}(\mathbf{z}) \boldsymbol{\chi} = 0, \mathbf{x} \in \mathcal{H} \right\}.$$

Podľa tvrdenia 2.5 platí

$$\mathbf{P}(d, l) \underbrace{\mathbf{Diag}(\mathbf{z}) \mathbf{Diag}(\mathbf{z}) \mathbf{Diag}(\mathbf{z})}_{\mathbf{I}} \mathbf{P}(d, d-l-1)^\top = \mathbf{0}.$$

Vektor $\mathbf{x} \in \mathcal{H}$ je daný lineárnou kombináciou stĺpcov matice $\mathbf{Diag}(\mathbf{z}) \mathbf{P}(d, d-l-1)^\top$, pre vektor $\boldsymbol{\chi}$ daný lineárnou kombináciou stĺpcov matice $\mathbf{Diag}(\mathbf{z}) \mathbf{P}(d, l)^\top$, bude splnená podmienka $\mathbf{x}^\top \mathbf{Diag}(\mathbf{z}) \boldsymbol{\chi} = 0$. Podľa tvrdenia 2.5 bude zároveň pre vektor $\boldsymbol{\chi}$ platiť podmienka $\mathbf{P}(d, d-l-1) \boldsymbol{\chi} = \mathbf{0}$.

Máme vyjadrenie

$$\mathcal{H}^{\perp \mathbf{z}} = \left\{ \boldsymbol{\chi} \in \widehat{\mathbb{Z}}_N^{2^d} \mid \mathbf{P}(d, d-l-1) \boldsymbol{\chi} = \mathbf{0} \right\},$$

z ktorého vyplýva

$$\sum_{\boldsymbol{\chi} \in \mathcal{H}^\perp} \prod_{i=1}^{2^d} z_i \overline{\mathcal{F}f_i(\chi_i)} = \sum_{\mathbf{P}(d, d-l-1) \boldsymbol{\chi} = \mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{\mathcal{F}f_i(\chi_i)} = \left\langle \mathcal{F}f_1, \mathcal{F}f_2, \dots, \mathcal{F}f_{2^d} \right\rangle_{\mathbf{G}(d, d-l-1)}. \quad \square$$

Zároveň nám duálna zovšeobecnená konvolučná idenita v dôsledku 1.10 ponúkne iný prístup k vyjadreniu $\mathbf{G}(d, l)$ skalárnych súčinov, ktorý uvádzame ako vlastný výsledok.

Tvrdenie 2.9 (priame vyjadrenie $\mathbf{G}(d, l)$ skalárnych súčinov). *Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $-1 \leq l \leq d$, $f_1, f_2, \dots, f_{2^d} : \mathbb{Z}_N \rightarrow \mathbb{C}$ a $\mathbf{z} \in \{\pm 1\}^{2^d}$ je uniformný vektor znamienok. Označme $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_{2^d}$ stĺpce matice $\mathbf{P}(d, d-l-1) \mathbf{Diag}(\mathbf{z})$. Platí identita*

$$\left\langle f_1, f_2, \dots, f_{2^d} \right\rangle_{\mathbf{G}(d, l)} = \mathbb{E}_{\mathbf{t}} \prod_{i=1}^{2^d} z_i \overline{f_i(\mathbf{s}_i^\top \mathbf{t})},$$

kde $\mathbf{t} \in \mathbb{Z}_N^{2^d}$, pričom $t_i = 0$, ak i -ty riadok matice $\mathbf{P}(d, d-l-1)$ je $\mathbf{0}^\top$.

Dôkaz. Z duality vo vete 2.8 vyplýva

$$\left\langle f_1, f_2, \dots, f_{2^d} \right\rangle_{\mathbf{G}(d, l)} = \underbrace{\left\langle \mathcal{F}f_1, \mathcal{F}f_2, \dots, \mathcal{F}f_{2^d} \right\rangle_{\mathbf{G}(d, d-l-1)}}_{\text{definícia 2.6}} = \sum_{\mathbf{P}(d, d-l-1) \boldsymbol{\chi} = \mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{\mathcal{F}f_i(\chi_i)}.$$

Overíme, že sú splnené podmienky dôsledku 1.10. Pre pravú stranu $\mathbf{0}$ vždy existuje riešenie systému $\mathbf{P}(d, d-l-1) \boldsymbol{\chi} = \mathbf{0}$.

Pre dané l má matica $\mathbf{P}(d, d-l-1)$ presne $\sum_{i=d-l}^d \binom{d}{i} = \sum \binom{d}{i}$ nenulových riadkov. Potrebujeme, aby nulový priestor matice $\mathbf{P}(d, d-l-1)$ bol izomorfný $\hat{\mathbb{Z}}_N^{2^d - \sum \binom{d}{i}}$. Ako sme už využili v dôkaze tvrdenia 1.8, nulový priestor matice $\mathbf{P}(d, d-l-1)$ je izomorfný $\hat{\mathbb{Z}}_N^{2^d - \sum \binom{d}{i}}$ práve vtedy, keď riadkový priestor matice $\mathbf{P}(d, d-l-1)$ je izomorfný $\hat{\mathbb{Z}}_N^{\sum \binom{d}{i}}$. Keďže matica $\mathbf{P}(d, d-l-1)$ je dolná trojuholníková matica, rank voľného modulu, ktorý zodpovedá riadkovému priestoru je $\sum \binom{d}{i}$.

Matica $\mathbf{P}(d, d-l-1)^\top$ tvorí hornú trojuholníkovú maticu, v ktorej pivoty sú ± 1 . Z tvrdenia 2.4 pre $d > 1$ vyplýva

$$\mathbf{P}(d, d-l-1)^\top = \left[\begin{array}{c|c} \mathbf{P}(d, l)^\top & \mathbf{P}(d, l-1)^\top \\ \hline & -\mathbf{P}(d, l-1)^\top \end{array} \right].$$

Ekvivalentnými úpravami nad $\mathbb{Z}_N$ (násobenie -1 a sčítovanie ± 1 -násobkov riadkov) sa vieme dostať k matici

$$\left[\begin{array}{c|c} \mathbf{P}(d, l)^\top & \\ \hline & \mathbf{P}(d, l-1)^\top \end{array} \right].$$

Postup môžeme zopakovať $(d-1)$ -krát, čím sa dostaneme k matici

$$\mathbf{A} = \left[\begin{array}{cccc} \mathbf{P}(1, a_1) & & & \\ & \mathbf{P}(1, a_2) & & \\ & & \ddots & \\ & & & \mathbf{P}(1, a_{2^d}) \end{array} \right],$$

kde $\mathbf{a} \in \{-1, 0\}^{2^d}$. Platí $\mathbf{P}(1, -1) = 1$ a $\mathbf{P}(1, 0) = 0$, teda matica $\mathbf{A}$ je diagonálna matica, ktorej zložky na diagonále sú 0 a 1. Keďže dimenzia riadkového priestoru matice $\mathbf{P}(d, d-l-1)$ je $\sum \binom{d}{i}$, na diagonále $\mathbf{A}$ sa nachádza presne $\sum \binom{d}{i}$ -krát 1.

Stĺpcový priestor matice $\mathbf{A}$ je nutne izomorfný $\hat{\mathbb{Z}}_N^{2^d - \sum \binom{d}{i}}$. Keďže úpravy, ktorými sme sa dostali k matici $\mathbf{A}$, boli ekvivalentné nad $\mathbb{Z}_N$, aj riadkový priestor matice $\mathbf{P}(d, d-l-1)$ je izomorfný $\hat{\mathbb{Z}}_N^{\sum \binom{d}{i}}$, teda nulový priestor matice $\mathbf{P}(d, d-l-1)$ je izomorfný $\hat{\mathbb{Z}}_N^{2^d - \sum \binom{d}{i}}$.

Vďaka duálnej zovšeobecnenej konvolučnej identite v dôsledku 1.10 máme

$$\begin{aligned} \langle f_1, f_2, \dots, f_{2^d} \rangle_{\mathcal{G}(d,l)} &= \mathcal{F}^{\left(\sum \binom{d}{i}\right)} \left[\prod_{i=1}^{2^d} \overline{f_i \left(z_i \underbrace{\mathbf{a}_i^\top \mathbf{t}}_{\substack{i\text{-ty stĺpec} \\ \text{matice } \mathbf{P}(d,d-l-1)}} \right)} \right] (\mathbf{0}) \\ &= \mathcal{F}^{\left(\sum \binom{d}{i}\right)} \left[\prod_{i=1}^{2^d} \overline{f_i \left(z_i \mathbf{a}_i^\top \mathbf{t} \right)} \right] (\mathbf{0}) \end{aligned}$$

$$= \mathbb{E}_{\mathbf{t}} \prod_{i=1}^{2^d} \overline{f_i(\mathbf{s}_i^T \mathbf{t})} \omega^0,$$

keďže i -ty stĺpec matice $\mathbf{P}(d, d-l-1)$ má všetky zložky 0 alebo z_i . $\square$

Pre zložky i -teho stĺpca matice $\mathbf{P}(d, d-l-1)$ platí, že sú 0 alebo z_i . Násobenie matice $\mathbf{P}(d, d-l-1)$ a matice $\mathbf{Diag}(\mathbf{z})$ je ekvivalentné absolútnej hodnote zložiek matice $\mathbf{P}(d, d-l-1)$. Zložky vektora $\mathbf{s}_i$ sú preto iba 0 a 1.

Dokázané identity vo vete 2.8 a v tvrdení 2.9 budú platiť aj pre $\mathbf{U}(d, l)$ (polo)normu.

Dôsledok 2.10. *Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $-1 \leq l \leq d$, $f : \mathbb{Z}_N \rightarrow \mathbb{C}$ a $\mathbf{z} \in \{\pm 1\}^{2^d}$ je uniformný vektor znamienok. Označme $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_{2^d}$ stĺpce matice $\mathbf{P}(d, d-l-1) \mathbf{Diag}(\mathbf{z})$. Platia identity*

$$\text{i) dualita } \|f\|_{\mathbf{U}(d, l)} = \|\mathcal{F}f\|_{\mathbf{U}(d, d-l-1)},$$

$$\text{ii) priame vyjadrenie } \|f\|_{\mathbf{U}(d, l)} = \left(\mathbb{E}_{\mathbf{t}} \prod_{i=1}^{2^d} \overline{f(\mathbf{s}_i^T \mathbf{t})} \right)^{1/2^d}, \text{ kde } \mathbf{t} \in \mathbb{Z}_N^{2^d}, \text{ pričom } t_i = 0, \\ \text{ak } i\text{-ty riadok matice } \mathbf{P}(d, d-l-1) \text{ je } \mathbf{0}^T.$$

Dôkaz. Dôsledky vyplývajú z definície 2.6. $\mathbf{U}(d, l)$ normu môžeme vyjadriť ako $\|f\|_{\mathbf{U}(d, l)} = (\langle f, f, \dots, f \rangle_{\mathbf{G}(d, l)})^{1/2^d}$. $\square$

Príklad 2.3. *Pre $d = 2$ napíšeme priame vyjadrenie $\mathbf{U}(2, l)$ (polo)normou pre $-1 \leq l \leq 2$.*

Riešenie. Určíme matice $\mathbf{P}(2, 2-l-1) \mathbf{Diag}(\mathbf{z})$.

$$\begin{aligned} \mathbf{P}(2, 2) \mathbf{Diag}(\mathbf{z}) &= \begin{bmatrix} & & & \\ & & & \\ & & & \\ & & & \end{bmatrix}, & \mathbf{P}(2, 1) \mathbf{Diag}(\mathbf{z}) &= \begin{bmatrix} & & & \\ & & & \\ 1 & 1 & 1 & 1 \\ & & & \end{bmatrix}, \\ \mathbf{P}(2, 0) \mathbf{Diag}(\mathbf{z}) &= \begin{bmatrix} 1 & 1 & & \\ 1 & & 1 & \\ 1 & 1 & 1 & 1 \\ & & & \end{bmatrix}, & \mathbf{P}(2, -1) \mathbf{Diag}(\mathbf{z}) &= \begin{bmatrix} 1 & & & \\ 1 & 1 & & \\ 1 & & 1 & \\ 1 & 1 & 1 & 1 \end{bmatrix}. \end{aligned}$$

Pre jednoduchosť zápisu umocníme $U(2, l)$ (polo)normy na 4. Máme

$$\begin{aligned}
\|f\|_{U(2,-1)}^4 &= f(0) \overline{f(0)} f(0) f(0) \\
&= |f(0)|^4, \\
\|f\|_{U(2,0)}^4 &= \mathbb{E}_x f(x) \overline{f(x)} f(x) f(x) \\
&= \|f\|_4^4, \\
\|f\|_{U(2,1)}^4 &= \mathbb{E}_{x,a,b} f(x+a+b) \overline{f(x+a)} \overline{f(x+b)} f(x) \\
&= \|f\|_{U(2)}^4, \\
\|f\|_{U(2,2)}^4 &= \mathbb{E}_{x,a,b,c} f(x+a+b+c) \overline{f(x+a)} \overline{f(x+b)} f(x) \\
&= \left| \mathbb{E}_x f(x) \right|^4.
\end{aligned}$$

□

Môžeme si všimnúť niekoľko vlastností, ktoré budú platiť všeobecne.

$U(d, -1)$ a $U(d, d)$ nie sú normy, ale iba polonormy, nakoľko nie sú kladne definitné, iba kladne semidefinitné. Zároveň sú pre všetky rády d rovnaké

$$\|f\|_{U(d,-1)} = |f(0)|, \quad \|f\|_{U(d,d)} = \left| \mathbb{E}_x f(x) \right| = \left| \mathbb{E}_x f(x) \omega^0 \right| = |\mathcal{F}f(0)|.$$

$U(d, 0)$ normy budú vždy zodpovedať príslušnej p -norme pre $p = 2^d$

$$\|f\|_{U(d,0)} = \|f\|_{2^d}.$$

$U(d, 1)$ normy sú identické s $U(d)$ normami z definície 1.15

$$\|f\|_{U(d,1)} = \|f\|_{U(d)}.$$

Dôkaz týchto identít pre ľubovoľné d bude vyžadovať ďalšie tvrdenie, ktoré je dôsledkom rekurzívneho vyjadrenia matice $\mathbf{P}(d+1, l)$ v tvrdení 2.4. V spomínanom tvrdení ukážeme, že $U(d, l)$ (polo)normu môžeme vyjadriť pomocou skalárneho súčinu a $G(d-1, l)$ skalárneho súčinu.

Tvrdenie 2.11. *Nech $d \in \mathbb{Z}$, $d \geq 0$, $l \in \mathbb{Z}$, $-1 \leq l \leq d$, $f : \mathbb{Z}_N \rightarrow \mathbb{C}$ a $\mathbf{z} \in \{\pm 1\}^{2^{d+1}}$ je uniformný vektor znamienok. Pre 2^{d+1} mocninu $U(d+1, l)$ (polo)normy funkcie f existujú vyjadrenia:*

- i) $\|f\|_{\mathbf{U}(d+1,l+1)}^{2^{d+1}} = \mathbb{E}_{\mathbf{P}(d,l)\mathbf{x}=\mathbf{0}} \left\langle \Delta_{x_1} f, \Delta_{x_2} f, \dots, \Delta_{x_{2^d}} f \right\rangle_{\mathbf{G}(d,l+1)},$
- ii) *existuje $\mathcal{H}$ podgrupa $\mathbb{Z}_N^{2^d}$, existuje $g : \mathcal{H} \rightarrow \mathbb{C}$ také, že platí*
 $\|f\|_{\mathbf{U}(d+1,l+1)}^{2^{d+1}} = \langle g, g \rangle_{\mathcal{H}}.$

Dôkaz. Z definície $\mathbf{U}(d, l)$ (polo)normy a tvrdenia 2.4 vyplýva

$$\begin{aligned} \|f\|_{\mathbf{U}(d+1,l+1)}^{2^{d+1}} &= \mathbb{E}_{\mathbf{P}(d,l+1)\mathbf{y}=\mathbf{0}} \prod_{i=1}^{2^d} \overline{f(y_i)}^{z_i} \overline{f(\underbrace{y_{2^d+i}}_{\text{označíme } v_i})} \\ &= \mathbb{E}_{\begin{bmatrix} \mathbf{P}(d,l+1) & \\ & -\mathbf{P}(d,l) \end{bmatrix} \begin{bmatrix} \mathbf{u} \\ \mathbf{v} \end{bmatrix} = \mathbf{0}} \prod_{i=1}^{2^d} \overline{f(u_i)}^{z_i} \overline{f(v_i)} \\ &= \mathbb{E}_{\substack{\mathbf{P}(d,l+1)\mathbf{u}=\mathbf{0} \\ \mathbf{P}(d,l)\mathbf{u}=\mathbf{P}(d,l)\mathbf{v}}} \prod_{i=1}^{2^d} \overline{f(\underbrace{u_i}_{\text{označíme } v_i + x_i})}^{z_i}. \end{aligned}$$

Podmienka $\mathbf{P}(d, l+1)\mathbf{u} = \mathbf{0}$ je ekvivalentná podmienke $\mathbf{P}(d, l+1)\mathbf{v} = \mathbf{0}$, keďže máme aj podmienku $\mathbf{P}(d, l)\mathbf{u} = \mathbf{P}(d, l)\mathbf{v}$ a matica $\mathbf{P}(d, l)$ obsahuje všetky nenulové riadky matice $\mathbf{P}(d, l+1)$. Ďalej máme

$$\begin{aligned} \|f\|_{\mathbf{U}(d+1,l+1)}^{2^{d+1}} &= \mathbb{E}_{\mathbf{P}(d,l)\mathbf{x}=\mathbf{0}} \mathbb{E}_{\mathbf{P}(d,l+1)\mathbf{v}=\mathbf{0}} \prod_{i=1}^{2^d} \overline{f(v_i + x_i)}^{z_i} \overline{f(v_i)} \\ &= \mathbb{E}_{\mathbf{P}(d,l)\mathbf{x}=\mathbf{0}} \mathbb{E}_{\mathbf{P}(d,l+1)\mathbf{v}=\mathbf{0}} \prod_{i=1}^{2^d} \overline{\Delta_{x_i} f(v_i)}^{z_i} \\ &= \mathbb{E}_{\mathbf{P}(d,l)\mathbf{x}=\mathbf{0}} \left\langle \Delta_{x_1} f, \Delta_{x_2} f, \dots, \Delta_{x_{2^d}} f \right\rangle_{\mathbf{G}(d,l+1)}. \end{aligned}$$

Alternatívne nech $\mathcal{H}$ je daná

$$\mathcal{H} = \left\{ \mathbf{t} \in \mathbb{Z}_N^{2^d} \mid \forall i \in \{1, 2, \dots, 2^d\} : |\mathbf{N}_i| \neq l+1 \implies t_i = 0 \right\},$$

kde $\mathbf{N}_1, \mathbf{N}_2, \dots, \mathbf{N}_{2^d}$ sú uniformne usporiadané podmnožiny.

Podmienka $\mathbf{P}(d, l)\mathbf{u} = \mathbf{t} \in \mathcal{H}$ zodpovedá podmienkam:

- 1) $\mathbf{p}_d(\mathbf{N}_i)\mathbf{u} = t_i \in \mathbb{Z}_N$, pre $|\mathbf{N}| = l+1$
- 2) $\mathbf{p}_d(\mathbf{N}_i)\mathbf{u} = 0$, pre $|\mathbf{N}| \neq l+1$,

pre $i \in \{1, 2, \dots, 2^d\}$. Podmienky z kategórie 2) zodpovedajú rovnosti $\mathbf{P}(d, l+1)\mathbf{u} = \mathbf{0}$. Súbor podmienok $\mathbf{P}(d, l+1)\mathbf{u} = \mathbf{0}$, $\mathbf{P}(d, l+1)\mathbf{v} = \mathbf{0}$ a $\mathbf{P}(d, l)\mathbf{u} = \mathbf{P}(d, l)\mathbf{v}$ zodpovedá podmienkám $\mathbf{P}(d, l)\mathbf{u} = \mathbf{P}(d, l)\mathbf{v} = \mathbf{t} \in \mathcal{H}$.

Máme vyjadrenie

$$\begin{aligned}
\|f\|_{\mathbf{U}(d+1, l+1)}^{2^{d+1}} &= \mathbb{E}_{\mathbf{P}(d, l) \mathbf{u} = \mathbf{P}(d, l) \mathbf{v} = \mathbf{t} \in \mathcal{H}} \prod_{i=1}^{2^d} \overline{f(u_i)} \overline{f(v_i)} \\
&= \underbrace{\mathbb{E}_{\mathbf{t} \in \mathcal{H}} \mathbb{E}_{\mathbf{P}(d, l) \mathbf{u} = \mathbf{t}} \prod_{i=1}^{2^d} \overline{f(u_i)}}_{\text{označíme } g(\mathbf{t})} \underbrace{\mathbb{E}_{\mathbf{P}(d, l) \mathbf{v} = \mathbf{t}} \prod_{i=1}^{2^d} \overline{f(v_i)}}_{\text{označíme } \overline{g(\mathbf{t})}} \\
&= \langle g, g \rangle_{\mathcal{H}}. \quad \square
\end{aligned}$$

Overíme, že vo vyjadrení ii) v tvrdení 2.11 sedí veľkosť dimenzie priestoru, v ktorom diskkrétne integrujeme.

V definičnom predpise $\mathbf{U}(d+1, l+1)$ (polo)normy integrujeme cez premennú zo $\mathbb{Z}_N^{2^{d+1}}$, na ktorú máme $\binom{d-l}{i} \binom{d+1}{i}$ podmienok. Tento priestor má dimenziu $2^{d+1} - \binom{d-l}{i} \binom{d+1}{i} = \binom{d+1}{i} - \binom{d-l}{i} \binom{d+1}{i} = \binom{l+1}{i} \binom{d+1}{i}$.

Vo vyjadrení cez $\mathbf{t} \in \mathcal{H}$ integrujeme cez $\mathcal{H}$, s dimenziou $\binom{d}{l+1}$ a premenné $\mathbf{u}, \mathbf{v}$, na ktoré máme podmienky $\mathbf{P}(d, l) \mathbf{u} = \mathbf{t}, \mathbf{P}(d, l) \mathbf{v} = \mathbf{t}$. Pre $\mathbf{u}, \mathbf{v}$ platí, že sú z priestoru s dimenziou $2^d - \binom{d-l}{i} \binom{d}{i} = \binom{d}{i} - \binom{d-l}{i} \binom{d}{i} = \binom{l}{i} \binom{d}{i}$. Keď integrujeme cez $\mathbf{u}, \mathbf{v}$ a $\mathbf{t}$, integrujeme cez podpriestor s dimenziou $\binom{l}{i} \binom{d}{i} + \binom{l}{i} \binom{d}{i} + \binom{d}{l+1} = \binom{l}{i} \binom{d}{i} + \binom{l+1}{i} \binom{d}{i} = \binom{l+1}{i} \binom{d+1}{i}$ podľa lemy 2.1. Veľkosti dimenzie sa zhodujú.

Dôsledok 2.12 (ekvivalencia definícií). *Nech $d \in \mathbb{N}$, $f : \mathbb{Z}_N \rightarrow \mathbb{C}$. Platia identity:*

$$\begin{aligned}
\text{i) } \underbrace{\|f\|_{\mathbf{U}(d, 1)}}_{\text{definícia 2.6}} &= \underbrace{\|f\|_{\mathbf{U}(d)}}_{\text{definícia 1.15}}, \\
\text{ii) } \underbrace{\|f\|_{\mathbf{U}(d, 0)}}_{\text{definícia 2.6}} &= \underbrace{\|f\|_{2^d}}_{\text{definícia 1.11}}.
\end{aligned}$$

Dôkaz. Podľa tvrdenia 2.11 platí

$$\|f\|_{\mathbf{U}(d, 1)}^{2^d} = \mathbb{E}_{\mathbf{P}(d-1, l-1) \mathbf{x} = \mathbf{0}} \left\langle \Delta_{x_1} f, \Delta_{x_2} f, \dots, \Delta_{x_{2^d}} f \right\rangle_{\mathbf{G}(d-1, 1)}.$$

Matica $\mathbf{P}(d-1, 0)$ obsahuje $2^{d-1} - 1$ nenulových riadkov, pričom v každom z nich je rovnaký počet zložiek 1 a -1 . Zrejme vektor $\mathbf{x}$ musí spĺňať $\underbrace{x_1 = x_2 = \dots = x_{2^{d-1}}}_{\text{označíme } a_1}$.

Ďalej platí

$$\|f\|_{\mathbf{U}(d, 1)}^{2^d} = \mathbb{E}_{a_1} \left\langle \Delta_{a_1} f, \Delta_{a_1} f, \dots, \Delta_{a_1} f \right\rangle_{\mathbf{G}(d-1, 1)} = \mathbb{E}_{a_1} \left\| \Delta_{a_1} f \right\|_{\mathbf{U}(d-1, 1)}^{2^{d-1}}.$$

Ak tento postup zopakujeme $(d-1)$ -krát, máme

$$\begin{aligned}
\|f\|_{U(d,1)}^{2^d} &= \mathbb{E}_{a_1, a_2, \dots, a_{d-1}} \left\| \Delta_{a_1} \Delta_{a_2} \dots \Delta_{a_{d-1}} f \right\|_{U(1,1)}^2 \\
&= \mathbb{E}_{a_1, a_2, \dots, a_{d-1}} \underbrace{\mathbb{E}_{x, a_d} \Delta_{a_1} \Delta_{a_2} \dots \Delta_{a_{d-1}} f(x + a_d) \overline{\Delta_{a_1} \Delta_{a_2} \dots \Delta_{a_{d-1}} f(x)}}_{\text{priame vyjadrenie v dôsledku 2.10 pre } U(1,1)} \\
&= \underbrace{\mathbb{E}_{x, a} \Delta_{a_1} \Delta_{a_2} \dots \Delta_{a_d} f(x)}_{\text{definícia 1.15}} \\
&= \|f\|_{U(d)}^{2^d}.
\end{aligned}$$

Podobne z definície $U(d, 0)$ normy máme predpis

$$\|f\|_{U(d,0)}^{2^d} = \underbrace{\mathbb{E}_{\mathbf{P}(d,0) \mathbf{x}=\mathbf{0}}}_{x_1=x_2=\dots=x_{2d}} \prod_{i=1}^{2^d} z_i \overline{f(x_i)} = \mathbb{E}_a \prod_{i=1}^{2^d} z_i \overline{f(a)} = \underbrace{\mathbb{E}_a |f(a)|^2}_{\text{definícia 1.11}} = \|f\|_{2^d}^{2^d}. \quad \square$$

Rekurzívne vyjadrenie $\|f\|_{U(d+1)}^{2^{d+1}} = \mathbb{E}_a \|\Delta_a f\|_{U(d)}^{2^d}$, ktoré sa nachádza v dôkaze dôsledku 2.12, sa v niektorých textoch využíva na definíciu Gowersovej uniformnej normy rádu d . Napríklad B. Host a B. Kra takto definujú $U(d)$ normu v článku [6, str. 4]. Podobná definícia sa využíva aj v limitnom prípade na definíciu Gowers-Host-Kra uniformnej polonormy v článku [2, str. 3].

Príklad 2.4 (vlastnosti $U(d, l)$ (polo)normy). Označme $f_-(x) = f(-x)$, $\bar{f}(x) = \overline{f(x)}$ a $f_t(x) = f(x+t)$. Overíme, že pre všetky d, l platí $\|f_-\|_{U(d,l)} = \|\bar{f}\|_{U(d,l)} = \|f\|_{U(d,l)}$ a pre $0 \leq l \leq d$ platí $\|f_t\|_{U(d,l)} = \|f\|_{U(d,l)}$.

Riešenie. Z definície $U(d, l)$ (polo)normy máme

$$\|h\|_{U(d,l)}^{2^d} = \mathbb{E}_{\mathbf{P}(d,l) \mathbf{x}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{h(x_i)}.$$

V tomto vyjadrení za h postupne dosadíme f_- , $\bar{f}$, f_t .

Pre f_- získame riešenie priamym výpočtom

$$\mathbb{E}_{\mathbf{P}(d,l) \mathbf{x}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f_-(x_i)} = \mathbb{E}_{\mathbf{P}(d,l) \mathbf{x}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f(-x_i)} = \underbrace{\mathbb{E}_{\mathbf{P}(d,l) \mathbf{y}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f(y_i)}}_{\text{označíme } y_i} = \|f\|_{U(d,l)}^{2^d}.$$

Rovnosť pre $\bar{f}$ vyplýva z tvrdenia 2.11

$$\mathbb{E}_{\mathbf{P}(d,l) \mathbf{x}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{\bar{f}(x_i)} = \overline{\mathbb{E}_{\mathbf{P}(d,l) \mathbf{x}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f(x_i)}} = \overline{\langle g, g \rangle} = \langle g, g \rangle = \|f\|_{U(d,l)}^{2^d}.$$

Ďalej označme $\mathbf{t} = \begin{bmatrix} t & t & \dots & t \end{bmatrix}^\top$ a upravujme výraz pre f_t

$$\begin{aligned} \mathbb{E}_{\mathbf{P}(d,l)\mathbf{x}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f_t(x_i)} &= \mathbb{E}_{\mathbf{P}(d,l)\mathbf{x}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f(x_i + t)} \\ &= \mathbb{E}_{\mathbf{P}(d,l)\mathbf{x}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{\underbrace{f(x_i + t)}_{\text{označíme } y_i}} \\ &= \mathbb{E}_{\mathbf{P}(d,l)\mathbf{y}-\mathbf{P}(d,l)\mathbf{t}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f(y_i)}. \end{aligned}$$

Podľa tvrdenia 2.5 platí $\mathbf{P}(d,l) \mathbf{Diag}(\mathbf{z}) \mathbf{P}(d,d-l-1)^\top = \mathbf{0}$. Pre $0 \leq l \leq d$ tvorí posledný riadok matice $\mathbf{P}(d,d-l-1)$ podmienka $\mathbf{p}_d(1,2,\dots,d) = \mathbf{z}^\top$. Ďalej platí, že posledný stĺpec súčinu $\mathbf{Diag}(\mathbf{z}) \mathbf{P}(d,d-l-1)^\top$ je identický s vektorom $\mathbf{Diag}(\mathbf{z}) \mathbf{z} = \begin{bmatrix} 1 & 1 & \dots & 1 \end{bmatrix}^\top$.

Pre vektor $\mathbf{t}$ máme

$$\begin{aligned} \mathbf{P}(d,l) \mathbf{t} &= t \mathbf{P}(d,l) \begin{bmatrix} 1 & 1 & \dots & 1 \end{bmatrix}^\top \\ &= t \mathbf{P}(d,l) \mathbf{Diag}(\mathbf{z}) \mathbf{z} \\ &= t \underbrace{\mathbf{P}(d,l) \mathbf{Diag}(\mathbf{z}) \mathbf{p}_d(1,2,\dots,d)^\top}_{\text{tvrdenie 2.5}} \\ &= 0, \end{aligned}$$

odtiaľ dostávame výsledok

$$\mathbb{E}_{\mathbf{P}(d,l)\mathbf{y}-\mathbf{P}(d,l)\mathbf{t}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f(y_i)} = \mathbb{E}_{\mathbf{P}(d,l)\mathbf{y}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f(y_i)} = \|f\|_{\mathbf{U}(d,l)}^{2^d}. \quad \square$$

V tejto kapitole sme uviedli niektoré dôležité vlastnosti $\mathbf{U}(d,l)$ (polo)noriem a zovšeobecnených skalárnych súčinov, najmä dualitu vo vete 2.8 a vyjadrenie pomocou skalárneho súčinu v tvrdení 2.11. Dôkazom, že $\mathbf{U}(d,l)$ je norma pre $0 \leq l \leq d-1$ (uvedené vo vete 2.7) sme sa nezaoberali, môžeme ale aspoň naznačiť, ako by sme postupovali.

Trojuholníková nerovnosť sa dokazuje pomocou Gowers-Cauchy-Schwarzovej nerovnosti

$$\left| \langle f_1, f_2, \dots, f_{2^d} \rangle_{\mathbf{G}(d,l)} \right| \leq \|f_1\|_{\mathbf{U}(d,l)} \|f_2\|_{\mathbf{U}(d,l)} \cdots \|f_{2^d}\|_{\mathbf{U}(d,l)},$$

ktorú neskôr formulujeme v tvrdení 3.1.

Z Gowers-Cauchy-Schwarzovej nerovnosti vyplýva Minkowského nerovnosť, ktorá zodpovedá trojuholníkovej nerovnosti

$$\|f + g\|_{\mathbf{U}(d,l)} \leq \|f\|_{\mathbf{U}(d,l)} + \|g\|_{\mathbf{U}(d,l)},$$

argumentom, ktorý uviedol už T. Gowers v [4, str. 20].

Absolútna homogenita vyplýva z definície $U(d, l)$ normy v definícii 2.6 a uniformného vektora znamienok v definícii 2.2. Pre zložky uniformného vektora znamienok máme

$$z_{2^{d-1}+i} = (-1)^{|N_{2^{d-1}+i}|} = (-1)^{|N_i \cup \{d\}|} = -(-1)^{|N_i|} = -z_i,$$

pre $i \in \{1, 2, \dots, 2^{d-1}\}$.

Ďalej pre konštantu $C \in \mathbb{C}$ platí

$$\|Cf\|_{U(d,l)} = \left(\mathbb{E}_{\mathbf{P}(d,l)} \prod_{i=1}^{2^{d-1}} z_i \overline{Cf(x_i)}^{-z_i} \overline{Cf(x_{2^{d-1}+i})} \right)^{1/2^d} = |C| \|f\|_{U(d,l)}.$$

Z tvrdenia 2.11 vieme, že $U(d, l)$ norma je kladne semidefinitná, keďže existuje vyjadrenie $\|f\|_{U(d,l)}^{2^d} = \langle g, g \rangle_{\mathcal{H}}$. Ďalej by sme potrebovali dokázať, že $\|f\|_{U(d,l)}$ je kladne definitná, teda funkcia g vo vyjadrení z tvrdenia 2.11 je identicky rovná 0 iba vtedy, keď funkcia f je identicky rovná 0. Iný prístup k dôkazu semidefinitnosti uvádzame vďaka dôsledku 3.2 v kapitole 3.

Z týchto vlastností potom vyplýva, že $\|f\|_{U(d,l)}$ je norma funkcie f . Ako sme už vyššie spomenuli, presný dôkaz sa nachádza v článku M. Niepela [7].

3 Nerovnosti pre $U(d, l)$ normy

V tretej kapitole využijeme dokázané vlastnosti $U(d, l)$ (polo)normiem na odvodenie nerovností, v ktorých vystupujú $U(d, l)$ (polo)normy. Nerovnosti pre $U(d, l)$ (polo)normy doposiaľ neboli preskúvané, nakoľko pracovný článok M. Niepela [7] sa im nevenuje.

Keďže vektorové priestory $\mathbb{C}(\mathbb{Z}_N)$, resp. $\mathbb{C}(\widehat{\mathbb{Z}}_N)$ sú konečnorozmerné, všetky normy na nich definované sú ekvivalentné. V tejto kapitole nájdeme najlepšie konštanty $C, c \in \mathbb{R}$, ktoré spĺňajú

$$C \|f\|_{U(d,l)} \leq \|f\|_{U(d',l')} \leq c \|f\|_{U(d,l)}.$$

Podobne budeme skúmať, či existujú funkcie f , pre ktoré sa v týchto ohraničeníach nadobúda rovnosť.

Naša definícia $U(d, l)$ (polo)normiem v definícii 2.6 sa ukáže ako výhodná práve v podkapitole 3.1, kde vďaka nej odvodíme nový pojem autokorelácií vyšších rádov a dokážeme kľúčovú vetu 3.5.

V podkapitole 3.2 sériou príkladov odvodíme jednu analógiu Youngovej konvolučnej nerovnosti pre $U(d, l)$ (polo)normy. Podkapitola 3.2 slúži aj ako prehľadná podkapitola počítania s $U(d, l)$ (polo)normami, keďže sme sa v nej viac zamerali na príklady.

Príklad 3.1. *Nájdeme $U(d, l)$ normu funkcií $\mathbf{1}, \delta, \mathbf{1}, \Delta$ a určíme aké nerovnosti platia pre $U(d, l)$ normy δ funkcie vzhľadom na rád d a stupeň l .*

Riešenie. Máme

$$\begin{aligned}\|\mathbf{1}\|_{U(d, l)}^{2^d} &= \mathbb{E}_{\mathbf{P}(d, l)\mathbf{x}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{\mathbf{1}(x_i)} = \mathbb{E}_{\mathbf{P}(d, l)\mathbf{x}=\mathbf{0}} \mathbf{1} = 1, \\ \|\delta\|_{U(d, l)}^{2^d} &= \mathbb{E}_{\mathbf{P}(d, l)\mathbf{x}=\mathbf{0}} \underbrace{\prod_{i=1}^{2^d} z_i \overline{\delta(x_i)}}_{\substack{0 \text{ pre } \mathbf{x} \neq \mathbf{0} \\ N^{2^d} \text{ pre } \mathbf{x} = \mathbf{0}}} = N^{2^d - \sum \binom{d}{i}},\end{aligned}$$

keďže z podmienky $\mathbf{P}(d, l)\mathbf{x} = \mathbf{0}$ vyplýva, že robíme priemer cez $\sum \binom{d}{i}$ -rozmernú podgrupu.

Podobne platí

$$\begin{aligned}\|\mathbf{1}\|_{U(d, l)}^{2^d} &= \sum_{\mathbf{P}(d, l)\chi=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{\mathbf{1}(\chi_i)} = \sum_{\mathbf{P}(d, l)\chi=\mathbf{0}} \mathbf{1} = N^{\sum \binom{d}{i}}, \\ \|\Delta\|_{U(d, l)}^{2^d} &= \sum_{\mathbf{P}(d, l)\chi=\mathbf{0}} \underbrace{\prod_{i=1}^{2^d} z_i \overline{\Delta(\chi_i)}}_{\substack{0 \text{ pre } \chi \neq \mathbf{0} \\ 1 \text{ pre } \chi = \mathbf{0}}} = 1.\end{aligned}$$

Pre δ funkciu máme nerovnosti

$$\begin{aligned}\|\delta\|_{U(d+1, l)} &= N^{1 - \sum \binom{d+1}{i}} / 2^{d+1} \geq N^{1 - \sum \binom{d}{i} / 2^d} = \|\delta\|_{U(d, l)}, \\ \|\delta\|_{U(d+1, l+1)} &= N^{1 - \sum \binom{d+1}{i}} / 2^{d+1} \leq N^{1 - \sum \binom{d}{i} / 2^d} = \|\delta\|_{U(d, l)},\end{aligned}$$

keďže podľa lemy 2.1, identita iv) platí

$$\begin{aligned}\sum \binom{d+1}{i} &= \sum \binom{d}{i} + \sum^{l-1} \binom{d}{i} \leq 2 \left(\sum \binom{d}{i} \right), \\ \sum^{l+1} \binom{d+1}{i} &= \sum^{l+1} \binom{d}{i} + \sum \binom{d}{i} \geq 2 \left(\sum \binom{d}{i} \right),\end{aligned}$$

(v prípade, že $l = 0$ definujeme $\sum^{l-1} \binom{d}{i} = 0$).

Spojením týchto nerovností máme nerovnosť

$$\|\delta\|_{U(d, l)} \geq \|\delta\|_{U(d, l+1)}.$$

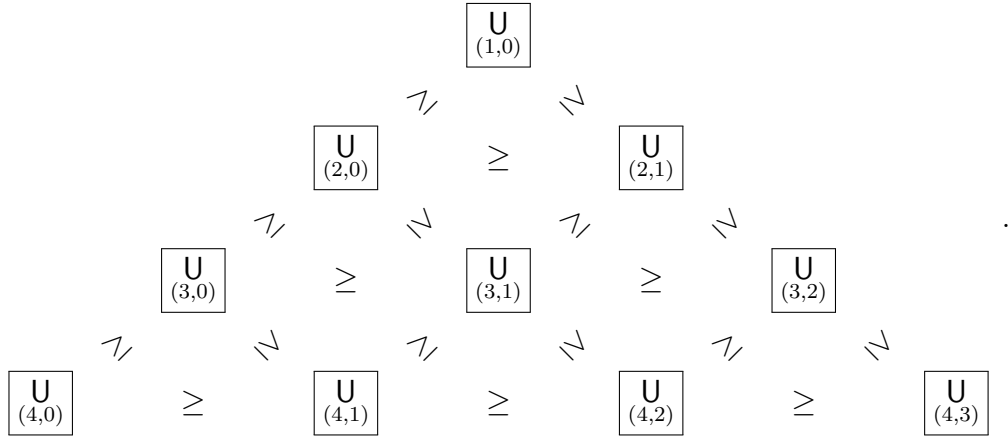
□

Budeme skúmať nerovnosti medzi $U(d, l)$ normami vzhľadom na rád d a stupeň l . Použijeme značenie

$$\boxed{U}_{(d,l)} = \|f\|_{U(d,l)},$$

pre nejakú funkciu $f : \mathbb{Z}_N \rightarrow \mathbb{C}$.

Z príkladu 3.1 predpokladáme, že nerovnosti sa vyskytujú podľa nasledujúcej schémy



Zároveň z príkladu 3.1 vieme, že existuje funkcia, v ktorej nastávajú v celej schéme rovnosti, je ňou funkcia 1.

Niektoré z uvedených nerovností sú známe, napríklad B. Szegedy uvádza v [10, str. 27] nerovnosť $\|f\|_{U(d)} \leq \|f\|_{2^{d-1}}$, ktorá vďaka dôsledku 2.12 zodpovedá nerovnosti $\|f\|_{U(d,1)} \leq \|f\|_{U(d-1,0)}$.

V predpokladanej schéme nerovností si môžeme všimnúť opakujúcu sa štruktúru

$$\begin{array}{ccc} & \boxed{U}_{(d,l)} & \\ \nearrow & & \searrow \\ \boxed{U}_{(d+1,l)} & \geq & \boxed{U}_{(d+1,l+1)} \\ \searrow & & \nearrow \\ & \boxed{U}_{(d+2,l+1)} & \end{array} \quad (3)$$

Aby sme dokázali, že nerovnosti platia podľa tejto schémy pre všetky $d \in \mathbb{N}$ a $l \in \mathbb{Z}$, $0 \leq l \leq d-1$, potrebujeme dokázať nerovnosti

$$\|f\|_{U(d,l)} \leq \|f\|_{U(d+1,l)}, \quad \|f\|_{U(d,l)} \geq \|f\|_{U(d+1,l+1)}.$$

Poznámka: Doplnením predpokladanej schémy nerovností o polonormy $U(d, d)$ máme

$$\begin{array}{ccccccc}
 & & \boxed{U_{(1,0)}} & \geq & \boxed{U_{(1,1)}} & & \\
 & \nearrow & & \searrow & \nearrow & \searrow & \\
 & & \boxed{U_{(2,0)}} & \geq & \boxed{U_{(2,1)}} & \geq & \boxed{U_{(2,2)}} \\
 & \nearrow & & \searrow & \nearrow & \searrow & \\
 \boxed{U_{(3,0)}} & \geq & \boxed{U_{(3,1)}} & \geq & \boxed{U_{(3,2)}} & \geq & \boxed{U_{(3,3)}}
 \end{array} ,$$

keďže pre všetky $d, p \in \mathbb{N}$ platí

$$\|f\|_{U(d,d-1)} = \|\mathcal{F}f\|_{2^d} = \left(\sum_{\chi} |\mathcal{F}f(\chi)|^{2^d} \right)^{1/2^d} \geq \left(|\mathcal{F}f(0)|^{2^d} \right)^{1/2^d} = \|f\|_{U(p,p)} .$$

Pre polonormy $U(d, -1)$ nerovnosti nemáme. Stále platí, že $\|f\|_{U(d,-1)} = \|f\|_{U(p,-1)}$ pre ľubovoľné d a p , ale nerovnosť medzi $\|f\|_{U(d,-1)}$ a $\|f\|_{U(p,0)}$ môže ísť oboma smermi.

Príklad 3.2 (nerovnosti medzi 2^d -normami). *Overíme, že medzi 2^d -normami $\|f\|_{2^d}$ a $\|\mathcal{F}f\|_{2^d}$, zodpovedajúcimi $\|f\|_{U(d,0)}$ a $\|f\|_{U(d,d-1)}$ platia nerovnosti:*

- i) $\|f\|_{U(d,d-1)} \geq \|f\|_{U(d+1,d)},$
- ii) $\|f\|_{U(d,0)} \geq N^{-1/2^{d+1}} \|f\|_{U(d+1,0)},$

a uvidíme príklad funkcií, v ktorých nastáva v daných nerovnostiach rovnosť.

Riešenie. Vďaka dualite v dôsledku 2.10 a ekvivalencii v dôsledku 2.12 platí

$$\|f\|_{U(d,d-1)} = \|\mathcal{F}f\|_{U(d,0)} = \|\mathcal{F}f\|_{2^d}, \quad \|f\|_{U(d,0)} = \|f\|_{2^d}.$$

Prvá nerovnosť vyplýva zo štandardného vzorca pre druhú mocninu súčtu. Umocníme ľavú stranu nerovnosti na 2^{d+1} a máme

$$\begin{aligned}
 \|\mathcal{F}f\|_{2^d}^{2^{d+1}} &= \left(\sum_{\chi} |\mathcal{F}f(\chi)|^{2^d} \right)^2 \\
 &= \sum_{\chi} |\mathcal{F}f(\chi)|^{2^{d+1}} + 2 \sum_{\chi \neq \varphi} |\mathcal{F}f(\chi) \mathcal{F}f(\varphi)|^{2^d} \\
 &\geq \sum_{\chi} |\mathcal{F}f(\chi)|^{2^{d+1}} \\
 &= \|\mathcal{F}f\|_{2^{d+1}}^{2^{d+1}} .
 \end{aligned}$$

Podobné úpravy môžeme vykonať aj pre druhú nerovnosť, pričom konštanta $N^{-1/2^{d+1}}$ vyplýva z inej miery v diskretnom integráli. Upravujme 2^{d+1} mocninu 2^d -normy funkcie f

$$\begin{aligned}
\|f\|_{2^d}^{2^{d+1}} &= \left(\mathbb{E}_x |f(x)|^{2^d} \right)^2 \\
&= \frac{1}{N^2} \left(\sum_{x=0}^{N-1} |f(x)|^{2^d} \right)^2 \\
&= \frac{1}{N^2} \sum_{x=0}^{N-1} |f(x)|^{2^{d+1}} + 2 \frac{1}{N^2} \sum_{x=0}^{N-1} \sum_{\substack{y=0 \\ x \neq y}}^{N-1} |f(x)f(y)|^{2^d} \\
&\geq \frac{1}{N} \mathbb{E}_x |f(x)|^{2^{d+1}} \\
&= \frac{1}{N} \|f\|_{2^{d+1}}^{2^{d+1}}.
\end{aligned}$$

Z postupu, ktorým sme odvodili nerovnosti vidíme, že v oboch prípadoch nastane rovnosť práve vtedy, keď platí $\mathcal{F}f(\chi)\mathcal{F}f(\varphi) = 0$ pre $\chi \neq \varphi$ a $f(x)f(y) = 0$ pre $x \neq y$. Príklad funkcie, v ktorej nastane rovnosť v druhej nerovnosti, je $f = \delta$. Analogicky v prvej nerovnosti nastane rovnosť, keď $\mathcal{F}f = \Delta$, čo vďaka leme 1.5 zodpovedá funkcii $f = 1$. Fakt, že vo funkcii 1 sa všetky $U(d, l)$ normy rovnajú, sme už ukázali v príklade 3.1. $\square$

Na dôkaz ďalších nerovností zo schémy (3) využijeme Gowers-Cauchy-Schwarzovu nerovnosť. Táto nerovnosť je analógiou Cauchy-Schwarzovej nerovnosti v tvrdení 1.13 a je potrebná na dôkaz vety 2.7, kde z nej vyplýva trojuholníková nerovnosť pre $U(d, l)$ (polo)normy.

Tvrdenie 3.1 (Gowers-Cauchy-Schwarzova nerovnosť). *Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $0 \leq l \leq d-1$, $f_1, f_2, \dots, f_{2^d} : \mathbb{Z}_N \rightarrow \mathbb{C}$. Platí nerovnosť*

$$\left| \langle f_1, f_2, \dots, f_{2^d} \rangle_{G(d, l)} \right| \leq \|f_1\|_{U(d, l)} \|f_2\|_{U(d, l)} \cdots \|f_{2^d}\|_{U(d, l)}.$$

Dôkaz. Pre prípad $d = 1$, je jediné prípustné $l = 0$, tento prípad je priamo Cauchy-Schwarzova nerovnosť v tvrdení 1.13.

Nech $d > 1$. Postupom analogickým k dôkazu tvrdenia 2.11 môžeme odvodiť vyjadrenie

$$\langle f_1, f_2, \dots, f_{2^d} \rangle_{G(d, l)} = \langle g, h \rangle_{\mathcal{H}},$$

kde $\mathcal{H}$ je daná

$$\mathcal{H} = \left\{ \mathbf{t} \in \mathbb{Z}_N^{2^{d-1}} \mid \forall i \in \{1, 2, \dots, 2^{d-1}\} : |\mathbf{N}_i| \neq l+1 \implies t_i = 0 \right\},$$

a funkcie g a h majú vyjadrenie

$$g(\mathbf{t}) = \mathbb{E}_{\mathbf{P}(d-1, l-1)\mathbf{x}=\mathbf{t}} \prod_{i=1}^{2^{d-1}} \overline{z_i f_i(x_i)}, \quad h(\mathbf{t}) = \mathbb{E}_{\mathbf{P}(d-1, l-1)\mathbf{x}=\mathbf{t}} \prod_{i=1}^{2^{d-1}} \overline{z_i f_{2^{d-1}+i}(x_i)}.$$

Ďalej je dôkaz analogický k prípadu $d = 2$, $l = 1$, ako ho uvádza T. Gowers v prehľadovom článku [5, str.11]. Z Cauchy-Schwarzovej nerovnosti vyplýva

$$\left| \langle f_1, f_2, \dots, f_{2^d} \rangle_{\mathbf{G}(d, l)} \right| = \left| \langle g, h \rangle_{\mathcal{H}} \right| \leq \langle g, g \rangle_{\mathcal{H}}^{1/2} \langle h, h \rangle_{\mathcal{H}}^{1/2}.$$

Z vyjadrenia $\mathbf{G}(d, l)$ skalárneho súčinu ako skalárneho súčinu funkcií g, h vyplýva

$$\langle g, g \rangle_{\mathcal{H}} = \langle f_1, \dots, f_{2^{d-1}}, f_1, \dots, f_{2^{d-1}} \rangle_{\mathbf{G}(d, l)}.$$

Platí nasledujúca symetria

$$\langle f_1, \dots, f_{2^{d-1}}, f_1, \dots, f_{2^{d-1}} \rangle_{\mathbf{G}(d, l)} = \langle f_1, f_1, \dots, f_{2^{d-1}}, f_{2^{d-1}} \rangle_{\mathbf{G}(d, l)},$$

ktorú v tomto texte nebudeme dokazovať. Myšlienka dôkazu spočíva v zámene úlohy prvkov 1 a d z množiny $\{1, 2, \dots, d\}$ v definícii uniformne usporiadaných podmnožín z definície 2.2. Presný dôkaz sa nachádza v článku M. Niepela [7].

Máme nerovnosť

$$\left| \langle f_1, f_2, \dots, f_{2^d} \rangle_{\mathbf{G}(d, l)} \right| \leq \langle f_1, f_1, \dots, f_{2^{d-1}}, f_{2^{d-1}} \rangle_{\mathbf{G}(d, l)}^{1/2} \langle f_{2^{d-1}+1}, f_{2^{d-1}+1}, \dots, f_{2^d}, f_{2^d} \rangle_{\mathbf{G}(d, l)}^{1/2}.$$

Postup môžeme zopakovať $(d-1)$ -krát, čo vedie k nerovnosti

$$\left| \langle f_1, f_2, \dots, f_{2^d} \rangle_{\mathbf{G}(d, l)} \right| \leq \underbrace{\langle f_1, \dots, f_1 \rangle_{\mathbf{G}(d, l)}^{1/2^d}}_{\|f_1\|_{\mathbf{U}(d, l)}} \underbrace{\langle f_2, \dots, f_2 \rangle_{\mathbf{G}(d, l)}^{1/2^d}}_{\|f_2\|_{\mathbf{U}(d, l)}} \dots \underbrace{\langle f_{2^d}, \dots, f_{2^d} \rangle_{\mathbf{G}(d, l)}^{1/2^d}}_{\|f_{2^d}\|_{\mathbf{U}(d, l)}}. \quad \square$$

Nerovnosť $\|f\|_{\mathbf{U}(d, l)} \leq \|f\|_{\mathbf{U}(d+1, l)}$ zo schémy (3) je dôsledkom Gowers-Cauchy-Schwarzovej nerovnosti.

Dôsledok 3.2. *Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $0 \leq l \leq d-1$, $f : \mathbb{Z}_N \rightarrow \mathbb{C}$. Platia nerovnosti:*

- i) $\|f\|_{\mathbf{U}(d, l)} \leq \|f\|_{\mathbf{U}(d+1, l)},$
- ii) $\|f\|_{\mathbf{U}(d, l)} \leq N^{\binom{d}{l+1}/2^{d+1}} \|f\|_{\mathbf{U}(d+1, l+1)}.$

Dôkaz. V dôkaze využijeme Gowers-Cauchy-Schwarzovu nerovnosť z tvrdenia 3.1 a funkcie $\mathbf{1}$ a $\mathbf{1}$.

Vezmime $G(d+1, l)$ skalárny súčin z 2^d -krát funkcie f a 2^d -krát funkcie $\mathbf{1}$. Vďaka rekurzívnemu vyjadreniu v tvrdení 2.4 platí

$$\begin{aligned} \langle f, f, \dots, f, \mathbf{1}, \mathbf{1}, \dots, \mathbf{1} \rangle_{G(d+1, l)} &= \mathbb{E}_{\mathbf{P}(d+1, l) \mathbf{x}=\mathbf{0}} \prod_{i=1}^{2^d} \overline{f(x_i)}^{z_i} \underbrace{\overline{\mathbf{1}(x_{2^d+i})}}_{\text{označíme } y_i} \\ &= \mathbb{E}_{\mathbf{P}(d, l) \mathbf{y}=\mathbf{0}} \prod_{i=1}^{2^d} \overline{f(y_i)}^{z_i} \\ &= \|f\|_{U(d, l)}^{2^d}. \end{aligned}$$

Ďalej z Gowers-Cauchy-Schwarzovej nerovnosti vyplýva

$$\|f\|_{U(d, l)}^{2^d} = \langle f, f, \dots, f, \mathbf{1}, \mathbf{1}, \dots, \mathbf{1} \rangle_{G(d+1, l)} \leq \|f\|_{U(d+1, l)}^{2^d} \underbrace{\|\mathbf{1}\|_{U(d+1, l)}^{2^d}}_1 = \|f\|_{U(d+1, l)}^{2^d}.$$

Na overenie druhej nerovnosti budeme postupovať analogicky, avšak rozdiel bude v tom, že funkcia $\mathbf{1} : \widehat{\mathbb{Z}}_N \rightarrow \mathbb{C}$ nemá $U(d, l)$ normu 1. Nech $r \in \mathbb{Z}$, $0 \leq r \leq d-1$. Využijeme dualitu vo vete 2.8 a máme

$$\begin{aligned} \langle \mathcal{F}f, \mathcal{F}f, \dots, \mathcal{F}f, \mathbf{1}, \mathbf{1}, \dots, \mathbf{1} \rangle_{G(d+1, r)} &= \sum_{\mathbf{P}(d+1, r) \chi=\mathbf{0}} \prod_{i=1}^{2^d} \overline{\mathcal{F}f(\chi_i)}^{z_i} \underbrace{\overline{\mathbf{1}(\chi_{2^d+i})}}_{\text{označíme } \zeta_i} \\ &= \sum_{\left[\begin{smallmatrix} \mathbf{P}(d, r) \\ \mathbf{P}(d, r-1) \end{smallmatrix} \right] \left[\begin{smallmatrix} \varphi \\ \zeta \end{smallmatrix} \right] = \mathbf{0}} \prod_{i=1}^{2^d} \overline{\mathcal{F}f(\varphi_i)}^{z_i} \underbrace{\overline{\mathbf{1}(\zeta_i)}}_1 \\ &= \sum_{\mathbf{P}(d, r) \varphi=\mathbf{0}} \prod_{i=1}^{2^d} \overline{\mathcal{F}f(\varphi_i)}^{z_i} \underbrace{\sum_{\mathbf{P}(d, r-1) \zeta=\mathbf{P}(d, r-1) \varphi} 1}_{\text{suma cez } \sum_{\Sigma}^{r-1} \binom{d}{i} \text{-rozmernú podgrupu}} \\ &= N^{\sum_{\Sigma}^{r-1} \binom{d}{i}} \|\mathcal{F}f\|_{U(d, r)}^{2^d} \\ &= N^{\sum_{\Sigma}^{r-1} \binom{d}{i}} \|f\|_{U(d, d-r-1)}^{2^d}. \end{aligned}$$

Opäť môžeme použiť Gowers-Cauchy-Schwarzovu nerovnosť

$$\begin{aligned} \langle \mathcal{F}f, \mathcal{F}f, \dots, \mathcal{F}f, \mathbf{1}, \mathbf{1}, \dots, \mathbf{1} \rangle_{G(d+1, r)} &\leq \|\mathcal{F}f\|_{U(d+1, r)}^{2^d} \underbrace{\|\mathbf{1}\|_{U(d+1, r)}^{2^d}}_{\text{príklad 3.1}} \\ &= N^{\sum_{\Sigma}^r \binom{d+1}{i}} / 2 \cdot \|f\|_{U(d+1, d-r)}^{2^d}. \end{aligned}$$

Spojením vyššie uvedených výrazov máme

$$\|f\|_{\mathcal{U}(d,d-r-1)}^{2^d} \leq N^{\frac{r}{\Sigma} \binom{d+1}{i} / 2 - r_{\Sigma}^{-1} \binom{d}{i}} \|f\|_{\mathcal{U}(d+1,d-r)}^{2^d}.$$

Z lemy 2.1 vyplýva

$$\frac{\frac{r}{\Sigma} \binom{d+1}{i}}{2} - r_{\Sigma}^{-1} \binom{d}{i} = \underbrace{\frac{\frac{r}{\Sigma} \binom{d+1}{i} - r_{\Sigma}^{-1} \binom{d}{i}}{2}}_{\text{lema 2.1, identita iv}} - \frac{r_{\Sigma}^{-1} \binom{d}{i}}{2} = \frac{\frac{r}{\Sigma} \binom{d}{i}}{2} - \frac{r_{\Sigma}^{-1} \binom{d}{i}}{2} = \frac{\binom{d}{r}}{2} = \frac{\binom{d}{d-r}}{2},$$

čo vedie na nerovnosť

$$\|f\|_{\mathcal{U}(d,d-r-1)}^{2^d} \leq N^{\binom{d}{d-r}/2} \|f\|_{\mathcal{U}(d+1,d-r)}^{2^d}.$$

Po označení $r = d - l - 1$ a sa výraz upraví na nerovnosť ii). □

Nerovnosť $\|f\|_{\mathcal{U}(d)} \leq \|f\|_{\mathcal{U}(d+1)}$ nie je nový výsledok, uvádza ho už T. Gowers napríklad v [5, str.18], rovnako argument pomocou Gowers-Cauchy-Schwarzovej nerovnosti už v tomto prípade bol použitý. Dôsledkom 3.2 sme najmä overili, že tento argument zostáva rovnaký aj pre $\mathcal{U}(d, l)$ normy, kde $l \neq 1$ a našli sme konštanty v opačných nerovnostiach, ktoré sú najlepšie, ako neskôr ukážeme v príklade 3.7.

Z príkladu 3.2 a dôsledku 3.2 môžeme nahliadnuť nasledujúcu schému nerovností

$$\dots \geq \boxed{\mathcal{U}_{(4,0)}} \geq \boxed{\mathcal{U}_{(3,0)}} \geq \boxed{\mathcal{U}_{(2,0)}} \geq \boxed{\mathcal{U}_{(1,0)}} \geq \boxed{\mathcal{U}_{(2,1)}} \geq \boxed{\mathcal{U}_{(3,2)}} \geq \boxed{\mathcal{U}_{(4,3)}} \geq \dots$$

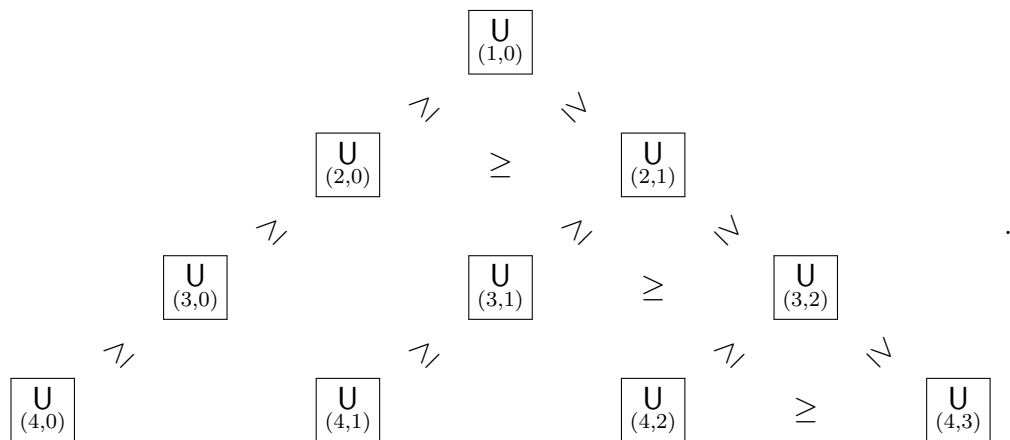
Táto schéma je konzistentná s predpokladanou schémou pre nerovnosti $\mathcal{U}(d, l)$ noriem. V príklade 3.2 a dôsledku 3.2 sme našli aj opačné nerovnosti, preto máme aj druhú schému nerovností

$$\dots \leq N^{-1/4-1/8} \boxed{\mathcal{U}_{(2,0)}} \leq N^{-1/4} \boxed{\mathcal{U}_{(2,0)}} \leq \boxed{\mathcal{U}_{(1,0)}} \leq N^{1/4} \boxed{\mathcal{U}_{(2,1)}} \leq N^{1/4+1/8} \boxed{\mathcal{U}_{(3,2)}} \leq \dots$$

Uvedené schémy pre $\mathcal{U}(d, 0)$ normy a $\mathcal{U}(d, d-1)$ normy zodpovedajú ekvivalencii 2^d -noriem v N -rozmernom komplexnom vektorovom priestore $\mathbb{C}(\mathbb{Z}_N)$.

Dôsledkom 3.2 a príkladom 3.2 sme v schéme nerovností pre $d \leq 4$ zatiaľ dokázali

nasledujúce nerovnosti



Tieto nerovnosti sú zároveň postačujúci argument pre kladnú definitnosť $U(d, l)$ normiem. Zo schémy vyplýva, že každá $U(d, l)$ norma je väčšia ako $U(l+1, l)$ norma. $U(l+1, l)$ norma funkcie f je ale vďaka dualite v dôsledku 2.10 identická s $U(l+1, 0)$ normou jej DFT, ktorá je podľa dôsledku 2.12 ekvivalentná 2^l -norme. Kladná definitnosť $U(d, l)$ normy potom vyplýva z kladnej definitnosti 2^l -normy DFT funkcie f .

Na dokázanie ďalších nerovností zo schémy (3) budeme potrebovať definovať nový pojem - autokorelácia vyšších rádo.

3.1 Autokorelácie vyšších rádo

Motiváciou zovšeobecnenia autokorelácie funkcie f $(f)_K$ nám bude vyjadrenie v tvrdení 2.11. V príklade 1.6 sme definovali autokoreláciu rádu 2 funkcie f , ktorú sme označili $(f)_{K(2)}$. Okrem zovšeobecnenia autokorelácie $(f)_K$ z definície 1.7 by bolo žiadúce, aby pojem autokorelácie vyšších rádo bol zároveň aj zovšeobecnením autokorelácie $(f)_{K(2)}$.

Pripomenieme si tvrdenie 2.11. Máme vyjadrenie

$$\|f\|_{U(d+1, l+1)}^{2^{d+1}} = \langle g, g \rangle_{\mathcal{H}},$$

kde funkcia g má predpis

$$g(\mathbf{t}) = \mathbb{E}_{\mathbf{P}(d, l) \mathbf{x} = \mathbf{t}} \prod_{i=1}^{2^d} z_i \overline{f(x_i)},$$

a $\mathbf{t} \in \mathcal{H}$. $\mathcal{H}$ je daná

$$\mathcal{H} = \left\{ \mathbf{t} \in \mathbb{Z}_N^{2^d} \mid \forall i \in \{1, 2, \dots, 2^d\} : |\mathbf{N}_i| \neq l+1 \implies t_i = 0 \right\}.$$

Príklad 3.3. Nájdeť vyjadrenie funkcie g pre $d = 1, 2$ a $l = 0$.

Riešenie. Pre $d = 1, l = 0$ máme

$$\begin{aligned}
g(\mathbf{t}) &= \mathbb{E}_{\mathbf{P}(1,0)\mathbf{x}=\mathbf{t}} f(x_1) \overline{f(x_2)} \\
&= \mathbb{E}_{\begin{bmatrix} 1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ t_2 \end{bmatrix}} f(x_1) \overline{f(x_2)} \\
&= \mathbb{E}_{x_1 - x_2 = t_2} f(x_1) \overline{f(x_2)} \\
&= \mathbb{E}_{x_2} f(x_2 + t_2) \overline{f(x_2)} \\
&= (f)_K(t_2),
\end{aligned}$$

teda autokorelácia $(f)_K$ je špeciálnym prípadom funkcie g .

Podobne upravujeme funkciu g pre $d = 2$ a $l = 0$

$$g(\mathbf{t}) = \mathbb{E}_{\mathbf{P}(2,0)\mathbf{x}=\mathbf{t}} f(x_1) \overline{f(x_2)f(x_3)} f(x_4) = \mathbb{E}_{\begin{bmatrix} 1 & -1 & & \\ 1 & & -1 & \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0 \\ t_2 \\ t_3 \\ 0 \end{bmatrix}} f(x_1) \overline{f(x_2)f(x_3)} f(x_4).$$

Podmienka $\mathbf{P}(2,0)\mathbf{x}=\mathbf{t}$ je ekvivalentná

$$x_2 = x_1 - t_2,$$

$$x_3 = x_1 - t_3,$$

$$x_4 = -x_1 + x_2 + x_3 = -x_1 + (x_1 - t_2) + (x_1 - t_3) = x_1 - t_2 - t_3.$$

Dosadíme vyjadrenie premenných x_2, x_3, x_4 podľa x_1 do funkcie g

$$\begin{aligned}
g(\mathbf{t}) &= \mathbb{E}_{x_1} f(x_1) \overline{f(x_1 - t_2)f(x_1 - t_3)} \underbrace{f(x_1 - t_2 - t_3)}_{\text{označíme } y} \\
&= \mathbb{E}_y f(y + t_2 + t_3) \overline{f(y + t_3)f(y + t_2)} f(y),
\end{aligned}$$

čo zodpovedá autokorelácií rádu 2 funkcie f z príkladu 1.6, $(f)_{K(2)}(t_2, t_3)$. □

Funkcia g je teda istým zovšeobecnením autokorelácie a využijeme ju na definíciu autokorelácie rádu d a stupňa l .

Definícia 3.3 (autokorelácie vyšších rádov). *Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $-1 \leq l \leq d$, a $\mathbf{N}_1, \mathbf{N}_2, \dots, \mathbf{N}_{2^d}$ sú uniformne usporiadané podmnožiny. $\mathcal{H}$ je podgrupa $\mathbb{Z}_N^{2^d}$ daná*

$$\mathcal{H} = \left\{ \mathbf{t} \in \mathbb{Z}_N^{2^d} \mid \forall i \in \{1, 2, \dots, 2^d\} : |\mathbf{N}_i| \neq l + 1 \implies t_i = 0 \right\}.$$

Nech $f : \mathbb{Z}_N \rightarrow \mathbb{C}$, $\mathbf{z} \in \{\pm 1\}^{2^d}$ je uniformný vektor znamienok a $\mathbf{t} \in \mathcal{H}$. Autokoreláciu rádu d a stupňa l funkcie f definujeme predpisom

$$(f)_{\mathbf{K}(d,l)}(\mathbf{t}) = \mathbb{E}_{\mathbf{P}(d,l)\mathbf{x}=\mathbf{t}} \prod_{i=1}^{2^d} z_i \overline{f(x_i)}.$$

Z príkladu 3.3 vyplýva

$$(f)_{\mathbf{K}(1,0)}(0, t_2) = \underbrace{(f)_{\mathbf{K}}(t_2)}_{\text{definícia 1.7}}, \quad (f)_{\mathbf{K}(2,0)}(0, t_2, t_3, 0) = \underbrace{(f)_{\mathbf{K}(2)}(t_2, t_3)}_{\text{príklad 1.6}}.$$

Poznámka: Vďaka vzťahu

$$\|f\|_{\mathbf{U}(d+1,l+1)}^{2^{d+1}} = \left\langle (f)_{\mathbf{K}(d,l)}, (f)_{\mathbf{K}(d,l)} \right\rangle_{\mathcal{H}},$$

by sme mohli postupovať analogicky k príkladu 1.6. Pomocou dôsledku 1.10 by sme našli DFT autokorelácie $(f)_{\mathbf{K}(d,l)}$. Ďalej by sme využili Parsevalovu identitu na odvodenie analogickej identity k identite $\|f\|_{\mathbf{U}(3)} = \|\mathcal{F}f\|_{\mathbf{U}(3)}$ z príkladu 1.6. Tento postup je už ale redundantný, keďže hľadanú identitu poznáme vďaka vete 2.8.

Zároveň ale platí

$$\|f\|_{\mathbf{U}(d+1,d-l-1)}^{2^{d+1}} = \left\langle (\mathcal{F}f)_{\mathbf{K}(d,d-l-2)}, (\mathcal{F}f)_{\mathbf{K}(d,d-l-2)} \right\rangle_{\widehat{\mathcal{H}}},$$

kde $\widehat{\mathcal{H}}$ je daná

$$\widehat{\mathcal{H}} = \left\{ \boldsymbol{\tau} \in \widehat{\mathbb{Z}}_N^{2^d} \mid \forall i \in \{1, 2, \dots, 2^d\} : |\mathbf{N}_i| \neq d - l - 1 \implies \tau_i = 0 \right\}.$$

Postup z príkladu 1.6 naznačuje, že platí identita

$$\mathcal{F}_{(l+1)}^{(d)} \left[(f)_{\mathbf{K}(d,l)} \right] (\boldsymbol{\tau}) = (\mathcal{F}f)_{\mathbf{K}(d,d-l-2)} (\boldsymbol{\tau}).$$

Dokázať uvedenú identitu môže byť zaujímavou úlohou, ktorou sa v tejto práci ale ďalej nezaobráame.

Príklad 3.4. Vyjadríme $\mathbf{U}(2,0)$ normu a $\mathbf{U}(2,1)$ normu funkcie f pomocou autokorelácie $(f)_{\mathbf{K}(2,0)}$.

Riešenie. Napíšeme predpis štvrtých mocnín $\mathbf{U}(2,0)$ normy a $\mathbf{U}(2,1)$ normy z príkladu 2.3

$$\begin{aligned} \|f\|_{\mathbf{U}(2,0)}^4 &= \mathbb{E}_x f(x) \overline{f(x)} \overline{f(x)} f(x), \\ \|f\|_{\mathbf{U}(2,1)}^4 &= \mathbb{E}_{x,a,b} f(x+a+b) \overline{f(x+b)} \overline{f(x+a)} f(x). \end{aligned}$$

Ďalej z príkladu 3.3 máme

$$(f)_{\mathbf{K}(2,0)}(0, t_2, t_3, 0) = \mathbb{E}_x f(x + t_2 + t_3) \overline{f(x + t_3)} \overline{f(x + t_2)} f(x).$$

Zrejme platí

$$\|f\|_{\mathbf{U}(2,0)}^4 = (f)_{\mathbf{K}(2,0)}(0, 0, 0, 0), \quad \|f\|_{\mathbf{U}(2,1)}^4 = \mathbb{E}_{a,b} (f)_{\mathbf{K}(2,0)}(0, a, b, 0). \quad \square$$

Analogické vzťahy platia aj pre ľubovoľný rád d a stupeň l .

Lema 3.4. *Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $-1 \leq l \leq d$. Pre autokorelácie vyšších rádov platí*

- i) $(f)_{\mathbf{K}(d,l)}(\mathbf{0}) = \|f\|_{\mathbf{U}(d,l)}^{2^d},$
- ii) $\mathbb{E}_{\mathbf{t} \in \mathcal{H}} (f)_{\mathbf{K}(d,l-1)}(\mathbf{t}) = \|f\|_{\mathbf{U}(d,l)}^{2^d}.$

Dôkaz. Prvá identita vyplýva priamo z definícií 2.6 a 3.3.

Ďalej upravujeme

$$\mathbb{E}_{\mathbf{t} \in \mathcal{H}} (f)_{\mathbf{K}(d,l-1)}(\mathbf{t}) = \mathbb{E}_{\mathbf{t} \in \mathcal{H}} \mathbb{E}_{\mathbf{P}(d,l-1)\mathbf{x}=\mathbf{t}} \prod_{i=1}^{2^d} z_i \overline{f(x_i)} = \mathbb{E}_{\left[\begin{smallmatrix} \mathbf{x} \\ \mathbf{t} \end{smallmatrix}\right] \in \mathcal{G}} \prod_{i=1}^{2^d} z_i \overline{f(x_i)},$$

kde podgrupa $\mathcal{G}$ je daná

$$\mathcal{G} = \left\{ \left[\begin{smallmatrix} \mathbf{x} \\ \mathbf{t} \end{smallmatrix}\right] \in \mathbb{Z}_N^{2^{d+1}} \mid \mathbf{P}(d, l-1)\mathbf{x} = \mathbf{t}, \forall i \in \{1, 2, \dots, 2^d\} : |\mathbf{N}_i| \neq l \implies t_i = 0 \right\}.$$

Nech $\mathbf{N}_1, \mathbf{N}_2, \dots, \mathbf{N}_{2^d}$ sú uniformne usporiadané podmnožiny. Matica $\mathbf{P}(d, l-1)$ obsahuje všetky nenulové riadky matice $\mathbf{P}(d, l)$. Z definície 2.3 vyplýva, že i -ty riadok matice $\mathbf{P}(d, l)$ je nenulový práve vtedy, keď $|\mathbf{N}_i| > l$ pre $i \in \{1, 2, \dots, 2^d\}$. Z ohraničenia $|\mathbf{N}_i| > l$ vyplýva $t_i = 0$. Podgrupu $\mathcal{G}$ môžeme vyjadriť ako

$$\mathcal{G} = \left\{ \left[\begin{smallmatrix} \mathbf{x} \\ \mathbf{t} \end{smallmatrix}\right] \in \mathbb{Z}_N^{2^{d+1}} \mid \mathbf{P}(d, l)\mathbf{x} = \mathbf{0}, \mathbf{P}(d, l-1)\mathbf{x} = \mathbf{t} \right\}.$$

Ďalej platí

$$\mathbb{E}_{\mathbf{t} \in \mathcal{H}} (f)_{\mathbf{K}(d,l-1)}(\mathbf{t}) = \mathbb{E}_{\left[\begin{smallmatrix} \mathbf{x} \\ \mathbf{t} \end{smallmatrix}\right] \in \mathcal{G}} \prod_{i=1}^{2^d} z_i \overline{f(x_i)} = \mathbb{E}_{\mathbf{P}(d,l)\mathbf{x}=\mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f(x_i)} \underbrace{\mathbb{E}_{\mathbf{t}=\mathbf{P}(d,l-1)\mathbf{x}} 1}_{\text{diskrétne integrál podľa } \mathbf{t}} = \|f\|_{\mathbf{U}(d,l)}^{2^d}. \quad \square$$

Príklad 3.5. *Určíme, v akom bode sa nadobúda maximum absolútnej hodnoty autokorelácie $(f)_{\mathbf{K}}$ funkcie f .*

Riešenie. Upravujeme pre $t \in \mathbb{Z}_N$

$$\left| (f)_K(t) \right| = \left| \mathbb{E}_x \underbrace{f(x+t) \overline{f(x)}}_{\text{označíme } f_t(x)} \right| = \left| \langle f_t, f \rangle \right|.$$

Z Cauchy-Schwarzovej nerovnosti vyplýva

$$\left| (f)_K(t) \right| \leq \underbrace{\|f_t\|_2}_{\text{príklad 2.4}} \|f\|_2 = \|f\|_2^2 = \mathbb{E}_x f(x) \overline{f(x)} = (f)_K(0).$$

Z nerovnosti $\left| (f)_K(t) \right| \leq (f)_K(0)$ vyplýva

$$\max_t \left| (f)_K(t) \right| = (f)_K(0). \quad \square$$

Nasledujúca veta o maxime autokorelácie vyšších rádov je jedným z hlavných výsledkov našej práce.

Veta 3.5 (maximum autokorelácie vyšších rádov). *Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $0 \leq l \leq d-1$, $f : \mathbb{Z}_N \rightarrow \mathbb{C}$. Pre maximum autokorelácie rádu d a stupňa l funkcie f platí*

$$\max_{\mathbf{t} \in \mathcal{H}} \left| (f)_{K(d,l)}(\mathbf{t}) \right| = (f)_{K(d,l)}(\mathbf{0}).$$

Dôkaz. Postup bude analogický k príkladu 3.5, úlohu Cauchy-Schwarzovej nerovnosti nahradí Gowers-Cauchy-Schwarzova nerovnosť. Aby sme ju mohli využiť, potrebujeme autokoreláciu rádu d a stupňa l vyjadriť ako $G(d,l)$ skalárny súčin 2^d funkcií f posunutých v argumente.

Z definície 3.3 máme

$$(f)_{K(d,l)}(\mathbf{t}) = \mathbb{E}_{\mathbf{P}(d,l)\mathbf{x}=\mathbf{t}} \prod_{i=1}^{2^d} z_i \overline{f(x_i)}.$$

Nech $\mathbf{N}_1, \mathbf{N}_2, \dots, \mathbf{N}_{2^d}$ sú uniformne usporiadané podmnožiny. Nech $i \in \{1, 2, \dots, 2^d\}$, pričom $|\mathbf{N}_i| = l+1$. Použijeme substitúciu

$$y_j = \begin{cases} x_j - (-1)^{l+1} t_i, & \text{ak } \mathbf{N}_i \subseteq \mathbf{N}_j, \\ x_j & \text{inak.} \end{cases}$$

pre $j \in \{1, 2, \dots, 2^d\}$.

Nech $\mathbf{M} \subseteq \{1, 2, \dots, d\}$, $|\mathbf{M}| \geq l+1$. Podmienka $\mathbf{p}_d(\mathbf{M})$ je jedným z riadkov matice $\mathbf{P}(d,l)$. Upravujeme podľa definície 2.3 súčin $\mathbf{p}_d(\mathbf{M})\mathbf{y}$

$$\mathbf{p}_d(\mathbf{M})\mathbf{y} = \sum_{a=0}^{|\mathbf{M}|} \sum_{\substack{\mathbf{A} \subseteq \mathbf{M}, \\ |\mathbf{A}|=a}} (-1)^a e(\mathbf{A})\mathbf{y}.$$

Sumu môžeme rozdeliť podľa toho, či A obsahuje podmnožinu N_i . Ďalej máme

$$\begin{aligned}
\mathbf{p}_d(\mathbf{M})\mathbf{y} &= \sum_{a=0}^{|\mathbf{M}|} \sum_{\substack{A \subseteq \mathbf{M}, \\ N_i \not\subseteq A, |A|=a}} (-1)^a \mathbf{e}(A)\mathbf{y} + \sum_{a=0}^{|\mathbf{M}|} \sum_{\substack{A \subseteq \mathbf{M}, \\ N_i \subseteq A, \\ |A|=a}} (-1)^a \mathbf{e}(A)\mathbf{y} \\
&= \sum_{a=0}^{|\mathbf{M}|} \sum_{\substack{A \subseteq \mathbf{M}, \\ N_i \not\subseteq A, |A|=a}} (-1)^a \mathbf{e}(A)\mathbf{x} + \sum_{a=0}^{|\mathbf{M}|} \sum_{\substack{A \subseteq \mathbf{M}, \\ N_i \subseteq A, \\ |A|=a}} (-1)^a (\mathbf{e}(A)\mathbf{x} - (-1)^{l+1}t_i) \\
&= \sum_{a=0}^{|\mathbf{M}|} \sum_{\substack{A \subseteq \mathbf{M}, \\ |A|=a}} (-1)^a \mathbf{e}(A)\mathbf{x} - t_i \sum_{a=0}^{|\mathbf{M}|} \sum_{\substack{A \subseteq \mathbf{M}, \\ N_i \subseteq A, \\ |A|=a}} (-1)^{a+l+1} \\
&= \mathbf{p}_d(\mathbf{M})\mathbf{x} - t_i \sum_{a=0}^{|\mathbf{M}|} \sum_{\substack{A \subseteq \mathbf{M}, \\ N_i \subseteq A, \\ |A|=a}} (-1)^{a+l+1}.
\end{aligned}$$

V prípade, že $\mathbf{M}$ neobsahuje podmnožinu N_i , platí $\mathbf{p}_d(\mathbf{M})\mathbf{y} = \mathbf{p}_d(\mathbf{M})\mathbf{x}$. Nech $N_i \subseteq \mathbf{M}$.

V prípade, že A obsahuje podmnožinu N_i , musí platiť $|A| \geq l+1$. Ďalej platí

$$-t_i \sum_{a=l+1}^{|\mathbf{M}|} \sum_{\substack{A \subseteq \mathbf{M}, \\ N_i \subseteq A, \\ |A|=a}} (-1)^{a+l+1} = -t_i \sum_{a=l+1}^{|\mathbf{M}|} \sum_{\substack{A \subseteq (\mathbf{M} \setminus N_i), \\ |A|=a-l-1}} (-1)^{a+l+1} = -t_i \sum_{a=0}^{|\mathbf{M} \setminus N_i|} \sum_{\substack{A \subseteq (\mathbf{M} \setminus N_i), \\ |A|=a}} \underbrace{(-1)^{a+2l+2}}_{(-1)^a}.$$

Vďaka binomickej vete máme

$$\sum_{a=0}^{|\mathbf{M} \setminus N_i|} \sum_{\substack{A \subseteq (\mathbf{M} \setminus N_i), \\ |A|=a}} (-1)^a = \sum_{a=0}^{|\mathbf{M} \setminus N_i|} \underbrace{\binom{|\mathbf{M} \setminus N_i|}{a}}_{\text{počet } a\text{-prvkových podmnožín množiny } \mathbf{M} \setminus N_i} (-1)^a = (1-1)^{|\mathbf{M} \setminus N_i|} = \begin{cases} 1, & \text{ak } \mathbf{M} = N_i, \\ 0 & \text{inak,} \end{cases}$$

čo vedie k výsledku

$$\mathbf{p}_d(\mathbf{M})\mathbf{y} = \begin{cases} \mathbf{p}_d(\mathbf{M})\mathbf{x} - t_i = 0, & \text{ak } \mathbf{M} = N_i, \\ \mathbf{p}_d(\mathbf{M})\mathbf{x} & \text{inak,} \end{cases}$$

pre všetky $\mathbf{M} \subseteq \{1, 2, \dots, d\}$. V maticovom zápise máme

$$\mathbf{P}(d, l)\mathbf{y} = \underbrace{\mathbf{P}(d, l)\mathbf{x}}_{\mathbf{t}} - t_i \mathbf{e}(N_i)^\top = \mathbf{t} - t_i \mathbf{e}(N_i)^\top.$$

Postup môžeme zopakovať pre všetky N_j , $|N_j| = l+1$, $j \in \{1, 2, \dots, 2^d\}$, teda spolu $\binom{d}{l+1}$ -krát.

Výsledná substitúcia bude

$$u_j = x_j - \underbrace{(-1)^{l+1} \sum_{\substack{\mathbf{N}_k \subseteq \mathbf{N}_j, \\ |\mathbf{N}_k|=l+1}} t_k}_{\text{označíme } T_j} = x_j - T_j,$$

pre všetky $j \in \{1, 2, \dots, 2^d\}$, čo nám zabezpečí

$$\mathbf{P}(d, l) \mathbf{u} = \underbrace{\mathbf{P}(d, l) \mathbf{x}}_{\mathbf{t}} - \underbrace{\sum_{|\mathbf{N}_j|=l+1} t_j \mathbf{e}(\mathbf{N}_j)^\top}_{\mathbf{t}} = \mathbf{0}.$$

Upravujeme autokoreláciu

$$\begin{aligned} (f)_{\mathbf{K}(d, l)}(\mathbf{t}) &= \mathbb{E}_{\mathbf{P}(d, l) \mathbf{x} = \mathbf{t}} \prod_{i=1}^{2^d} z_i \overline{f(x_i)} \\ &= \mathbb{E}_{\mathbf{P}(d, l) \mathbf{u} = \mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{\underbrace{f(u_i + T_i)}_{\text{označíme } f_{T_i}(u_i)}} \\ &= \mathbb{E}_{\mathbf{P}(d, l) \mathbf{u} = \mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{f_{T_i}(u_i)}. \end{aligned}$$

Podľa definície 2.6 teda platí

$$(f)_{\mathbf{K}(d, l)}(\mathbf{t}) = \langle f_{T_1}, f_{T_2}, \dots, f_{T_{2^d}} \rangle_{\mathbf{G}(d, l)}.$$

Z Gowers-Cauchy-Schwarzovej nerovnosti vyplýva

$$\begin{aligned} |(f)_{\mathbf{K}(d, l)}(\mathbf{t})| &= \left| \langle f_{T_1}, f_{T_2}, \dots, f_{T_{2^d}} \rangle_{\mathbf{G}(d, l)} \right| \\ &\leq \underbrace{\|f_{T_1}\|_{\mathbf{U}(d, l)} \|f_{T_2}\|_{\mathbf{U}(d, l)} \cdots \|f_{T_{2^d}}\|_{\mathbf{U}(d, l)}}_{\text{príklad 2.4}} \\ &= \underbrace{\|f\|_{\mathbf{U}(d, l)}^{2^d}}_{\text{lema 3.4}} \\ &= (f)_{\mathbf{K}(d, l)}(\mathbf{0}). \end{aligned} \quad \square$$

Príklad 3.6. Dokážeme nerovnosť $\|f\|_{\mathbf{U}(d, l)} \geq \|f\|_{\mathbf{U}(d, l+1)}$ medzi $\mathbf{U}(d, l)$ normami s rovnakým rádom d .

Riešenie. Vďaka vete 3.5 máme

$$\underbrace{\|f\|_{\mathbf{U}(d, l+1)}^{2^d}}_{\text{lema 3.4}} = \underbrace{\mathbb{E}_{\mathbf{t}} (f)_{\mathbf{K}(d, l)}(\mathbf{t})}_{\text{priemer } (f)_{\mathbf{K}(d, l)}} \leq \max_{\mathbf{t}} |(f)_{\mathbf{K}(d, l)}(\mathbf{t})| = \underbrace{(f)_{\mathbf{K}(d, l)}(\mathbf{0})}_{\text{lema 3.4}} = \|f\|_{\mathbf{U}(d, l)}^{2^d}. \quad \square$$

Okrem nerovností medzi normami s rovnakým rádom d máme, ako dôsledok vety 3.5 a tvrdenia 2.11, aj zvyšné doposiaľ nedokázané nerovnosti v schéme (3). Nerovnosti v dôsledku 3.6 doposiaľ neboli pre $U(d, l)$ normy overené.

Dôsledok 3.6. *Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $0 \leq l \leq d - 1$, $f : \mathbb{Z}_N \rightarrow \mathbb{C}$. Platia nerovnosti:*

$$\begin{aligned} \text{i)} \quad & \|f\|_{U(d, l)} \geq \|f\|_{U(d+1, l+1)}, \\ \text{ii)} \quad & \|f\|_{U(d, l)} \geq N^{-\binom{d}{l}/2^{d+1}} \|f\|_{U(d+1, l)}. \end{aligned}$$

Dôkaz. Nech $\mathcal{H}$ je daná

$$\mathcal{H} = \left\{ \mathbf{t} \in \mathbb{Z}_N^{2^d} \mid \forall i \in \{1, 2, \dots, 2^d\} : |\mathbf{N}_i| \neq l + 1 \implies t_i = 0 \right\}.$$

Z tvrdenia 2.11 vyplýva

$$\begin{aligned} \|f\|_{U(d+1, l+1)}^{2^{d+1}} &= \left\langle (f)_{\mathbf{K}(d, l)}, (f)_{\mathbf{K}(d, l)} \right\rangle_{\mathcal{H}} \\ &= \mathbb{E}_{\mathbf{t} \in \mathcal{H}} \left| (f)_{\mathbf{K}(d, l)}(\mathbf{t}) \right|^2 \\ &\leq \underbrace{\left(\max_{\mathbf{t} \in \mathcal{H}} \left| (f)_{\mathbf{K}(d, l)}(\mathbf{t}) \right| \right)^2}_{\text{veta 3.5}} \\ &= \left| (f)_{\mathbf{K}(d, l)}(\mathbf{0}) \right|^2 \\ &= \|f\|_{U(d, l)}^{2^{d+1}}. \end{aligned}$$

Postup pre nerovnosť ii) je analogický. Nech $r \in \mathbb{Z}$, $0 \leq r \leq d - 1$ a $\widehat{\mathcal{H}}$ je daná

$$\widehat{\mathcal{H}} = \left\{ \boldsymbol{\tau} \in \widehat{\mathbb{Z}}_N^{2^d} \mid \forall i \in \{1, 2, \dots, 2^d\} : |\mathbf{N}_i| \neq r + 1 \implies \tau_i = 0 \right\}.$$

Vďaka tvrdeniu 2.11 máme

$$\begin{aligned} \|\mathcal{F}f\|_{U(d+1, r+1)}^{2^{d+1}} &= \left\langle (\mathcal{F}f)_{\mathbf{K}(d, r)}, (\mathcal{F}f)_{\mathbf{K}(d, r)} \right\rangle_{\widehat{\mathcal{H}}} \\ &= \sum_{\boldsymbol{\chi} \in \widehat{\mathcal{H}}} \left| (\mathcal{F}f)_{\mathbf{K}(d, r)}(\boldsymbol{\chi}) \right|^2 \\ &\leq \sum_{\boldsymbol{\chi} \in \widehat{\mathcal{H}}} \underbrace{\left(\max_{\boldsymbol{\tau} \in \widehat{\mathcal{H}}} \left| (\mathcal{F}f)_{\mathbf{K}(d, r)}(\boldsymbol{\tau}) \right| \right)^2}_{\text{veta 3.5}} \\ &= \left| (\mathcal{F}f)_{\mathbf{K}(d, r)}(\mathbf{0}) \right|^2 \sum_{\boldsymbol{\chi} \in \widehat{\mathcal{H}}} 1 \\ &= N^{\binom{d}{r+1}} \|\mathcal{F}f\|_{U(d, r)}^{2^{d+1}}, \end{aligned}$$

keďže vektory $\chi \in \widehat{\mathcal{H}}$ majú $\binom{d}{r+1}$ zložiek, ktoré nie sú identické s 0, $\widehat{\mathcal{H}}$ má rozmer $\binom{d}{r+1}$.

Z duality v dôsledku 2.10 vyplýva

$$\|f\|_{\mathcal{U}(d,l)} = \|\mathcal{F}f\|_{\mathcal{U}(d,d-l-1)} \geq N^{-\binom{d}{d-l}/2^{d+1}} \|\mathcal{F}f\|_{\mathcal{U}(d+1,d-l)} = N^{-\binom{d}{l}/2^{d+1}} \|f\|_{\mathcal{U}(d+1,l)}. \quad \square$$

Poznámka: Nerovnosť ii) v dôsledku 3.6 je konzistentná s nerovnosťou ii) v príklade 3.2 pre $\mathcal{U}(d,0)$ normy, keďže $\binom{d}{0} = 1$.

Dôsledkami 3.2 a 3.6 sme dokázali, že platí schéma nerovností (3). Navyše sme našli aj schému opačných nerovností

$$\begin{array}{ccc} & N^{\binom{d}{l}/2^{d+1}} \boxed{\mathcal{U}_{(d,l)}} & \\ \swarrow & & \searrow \\ \boxed{\mathcal{U}_{(d+1,l)}} & \leq & N^{\binom{d+1}{l+1}/2^{d+1}} \boxed{\mathcal{U}_{(d+1,l+1)}} \\ \searrow & & \swarrow \\ & N^{\binom{d+1}{l+1}/2^{d+2}} \boxed{\mathcal{U}_{(d+2,l+1)}} & \end{array} \quad (4)$$

V schéme (3) zrejme existujú funkcie, pre ktoré sa v nerovnostiach nadobúda rovnosť. Z príkladu 3.1 vieme, že pre schému (3) je takou funkciou 1. V nasledujúcom príklade ukážeme, že aj pre schému (4) existujú funkcie, v ktorých sa v nerovnostiach nadobúda rovnosť.

Príklad 3.7. *Určíme funkciu f pre ktorú platí*

$$\|f\|_{\mathcal{U}(d,l)} = \underbrace{N^{\binom{d}{l+1}/2^{d+1}} \|f\|_{\mathcal{U}(d+1,l+1)}}_{\text{z dôsledku 3.2}} = \underbrace{N^{-\binom{d}{l}/2^{d+1}} \|f\|_{\mathcal{U}(d+1,l)}}_{\text{z dôsledku 3.6}}.$$

Riešenie. Ekvivalentne hľadáme funkciu, pre ktorú platí

$$\begin{aligned} \text{i)} \quad & \|f\|_{\mathcal{U}(d,l)}^{2^{d+1}} = N^{\binom{d}{l+1}} \|f\|_{\mathcal{U}(d+1,l+1)}^{2^{d+1}}, \\ \text{ii)} \quad & \|f\|_{\mathcal{U}(d,l)}^{2^{d+1}} = N^{-\binom{d}{l}} \|f\|_{\mathcal{U}(d+1,l)}^{2^{d+1}}. \end{aligned}$$

Ukážeme, že funkciou, pre ktorú platia tieto rovnosti, je $f = \delta$.

Z príkladu 3.1 vyplýva

$$\|\delta\|_{\mathcal{U}(d,l)}^{2^{d+1}} = N^{2^{d+1}-2^l \binom{d}{l}}.$$

Podobne pre $U(d+1, l+1)$ a $U(d+1, l)$ normy funkcie δ platí

$$\|\delta\|_{U(d+1, l+1)}^{2^{d+1}} = N^{2^{d+1} - \binom{d+1}{l+1}}, \quad \|\delta\|_{U(d+1, l)}^{2^{d+1}} = N^{2^{d+1} - \binom{d+1}{l}}.$$

Rovnosť i) platí práve vtedy, keď $-2 \binom{d}{l}_{\Sigma} = \binom{d}{l+1} - \binom{d+1}{l}_{\Sigma}$. Z lemy 2.1 vyplýva

$$-2 \binom{d}{l}_{\Sigma} = \binom{d}{l+1} - \binom{d}{l+1} - 2 \binom{d}{l}_{\Sigma} = \binom{d}{l+1} - \underbrace{\binom{d+1}{l}_{\Sigma} - \binom{d}{l}_{\Sigma}}_{\text{lema 2.1, identita iv}} = \binom{d}{l+1} - \binom{d+1}{l}_{\Sigma}.$$

Rovnosť ii) platí práve vtedy, keď $-2 \binom{d}{l}_{\Sigma} = -\binom{d}{l} - \binom{d+1}{l}_{\Sigma}$. Podobne platí

$$-2 \binom{d}{l}_{\Sigma} = -\binom{d}{l} - \underbrace{\binom{d+1}{l}_{\Sigma} - \binom{d}{l}_{\Sigma}}_{\text{lema 2.1, identita iv}} = -\binom{d}{l} - \binom{d+1}{l}_{\Sigma}. \quad \square$$

Keďže v schéme (3) aj v schéme (4) sme našli funkcie, v ktorých platí rovnosť, neexistujú konštanty $c, C, c', C' \in \mathbb{R}^+$ také, že

$$\begin{aligned} C \|f\|_{U(d+1, l)} &\leq \|f\|_{U(d, l)} \leq c \|f\|_{U(d+1, l)}, \\ C' \|f\|_{U(d+1, l+1)} &\leq \|f\|_{U(d, l)} \leq c' \|f\|_{U(d+1, l+1)}, \end{aligned}$$

kde pre konštanty c, C, c', C' platí

$$C > N^{-\binom{d}{l}/2^{d+1}}, \quad c < 1, \quad C' > 1, \quad c' < N^{\binom{d}{l+1}/2^{d+1}}.$$

Pre takéto konštanty c, C, c', C' by sa v prípade δ funkcie nadobudli opačné nerovnosti ako dokázané nerovnosti v dôsledkoch 3.2 a 3.6.

Inými slovami, ohraňovania, ktoré sme našli v dôsledkoch 3.2 a 3.6, a ktoré sa nachádzajú v schémach (3) a (4), sú najlepšie možné.

Jedným z dôvodov, prečo má zmysel skúmať nerovnosti medzi normami je, že charakterizujú inklúzie priestorov funkcií s konečnou normou.

Priestory funkcií $f : \mathbb{S}^1 \rightarrow \mathbb{C}$, prípadne priestory nekonečných postupností $F : \mathbb{Z} \rightarrow \mathbb{C}$, v ktorých je daná p -norma konečná, budeme označovať $L_p(\mathbb{S}^1)$, resp. $\ell_p(\mathbb{Z})$. Potom, ak platí nerovnosť $\|f\|_p \leq \|f\|_q$, funkcia f s konečnou q -normou, $\|f\|_q < \infty$, bude mať nutne konečnú p -normu, $\|f\|_p < \infty$. Teda pre $f : \mathbb{S}^1 \rightarrow \mathbb{C}$ zo všeobecného vzťahu $\|f\|_p \leq \|f\|_q$ vyplýva: ak $f \in L_q(\mathbb{S}^1)$ tak $f \in L_p(\mathbb{S}^1)$, inými slovami $L_p(\mathbb{S}^1) \subseteq L_q(\mathbb{S}^1)$. Analogicky dáva vzťah $\|F\|_p \leq \|F\|_q$ pre všetky funkcie $F : \mathbb{Z} \rightarrow \mathbb{C}$ inklúziu $\ell_p(\mathbb{Z}) \subseteq \ell_q(\mathbb{Z})$.

S opomenutím netriviálnych detailov súvisiacich s teóriou miery, by sme mohli definovať $G(d, l)$ skalárny súčin a $U(d, l)$ normu aj na nekonečných abelovských grupách. Predpokladajme, že nerovnosti pre funkcie $f : \mathbb{Z}_N \rightarrow \mathbb{C}$ a $F : \widehat{\mathbb{Z}}_N \rightarrow \mathbb{C}$ platia aj v limitnom prípade $N \rightarrow \infty$. Ako sme uviedli v kapitole 1, limitným prípadom $\mathbb{Z}_N$ je $\mathbb{S}^1$ a limitným prípadom $\widehat{\mathbb{Z}}_N$ je $\mathbb{Z}$. Predpokladajme, že daný limitný prechod $N \rightarrow \infty$ vieme spraviť a nerovnosti medzi $U(d, l)$ normami sa limitným prechodom zachovávajú. Priestory funkcií $f : \mathbb{S}^1 \rightarrow \mathbb{C}$, prípadne priestory nekonečných postupností $F : \mathbb{Z} \rightarrow \mathbb{C}$, v ktorých je daná $U(d, l)$ norma konečná, by sme označili $U_{d,l}(\mathbb{S}^1)$ a $u_{d,l}(\mathbb{Z})$.

Ak sa limitným prechodom nerovnosti medzi $U(d, l)$ normami naozaj zachovávajú, máme inklúzie priestorov funkcií $f : \mathbb{S}^1 \rightarrow \mathbb{C}$

$$U_{d+1,l+1}(\mathbb{S}^1) \subseteq U_{d,l}(\mathbb{S}^1) \subseteq U_{d+1,l}(\mathbb{S}^1).$$

Ak sa limitným prechodom zachová aj dualita vo vete 2.8, máme pre priestory postupností $F : \mathbb{Z} \rightarrow \mathbb{C}$ inklúzie

$$u_{d+1,d-l-1}(\mathbb{Z}) \subseteq u_{d,d-l-1}(\mathbb{Z}) \subseteq u_{d+1,d-l}(\mathbb{Z}),$$

ktoré po označení $r = d - l - 1$ zodpovedajú

$$u_{d+1,r+1}(\mathbb{Z}) \supseteq u_{d,r}(\mathbb{Z}) \supseteq u_{d+1,r}(\mathbb{Z}).$$

Inklúzie v prípade priestoru nekonečných postupností $F : \mathbb{Z} \rightarrow \mathbb{C}$ by teda boli (za predpokladu, že limitný prechod sa naozaj dá spraviť) opačné ako v prípade funkcií $f : \mathbb{S}^1 \rightarrow \mathbb{C}$. Opačné inklúzie zodpovedajú známemu faktu, že nerovnosti medzi p -normami a q -normami, $p < q$, na priestoroch $\mathbb{C}(\mathbb{S}^1)$ a $\mathbb{C}(\mathbb{Z})$ sú opačným smerom.

3.2 Youngova konvolučná nerovnosť

V tejto podkapitole využívame dokázané tvrdenia a identity na hľadanie analógií Youngovej konvolučnej nerovnosti. Youngovu konvolučnú nerovnosť dokázal W. Young v článku [12].

Formuláciu Youngovej konvolučnej nerovnosti pre funkcie definované na obore reálnych čísel, teda v priestoroch $L_p(\mathbb{R})$, $L_q(\mathbb{R})$ a $L_r(\mathbb{R})$, uvádzame v nasledujúcom tvrdení.

Tvrdenie 3.7 (Youngova konvolučná nerovnosť). *Nech $f, g : \mathbb{R} \rightarrow \mathbb{C}$, $p, q, r \in \mathbb{R}$, $1 \leq p, q, r \leq \infty$, pričom $\frac{1}{p} + \frac{1}{q} = \frac{1}{r} + 1$. Platí Youngova konvolučná nerovnosť (ďalej Youngova nerovnosť)*

$$\|f * g\|_r \leq \|f\|_p \|g\|_q.$$

Youngovu nerovnosť na tomto mieste nedokazujeme, nakoľko by jej muselo predchádzať niekoľko ďalších tvrdení z oblasti teórie miery a Lebesgueovho integrálu. Štandardný postup je ukázať ekvivalentnú nerovnosť pre konvolúciu troch funkcií, a ďalej použiť Hölderovu nerovnosť. Youngovou nerovnosťou sa zaoberajú napríklad E. Stein a R. Shakarchi v [9, str. 39,40,60].

Poznámka: Označme $f_-(x) = f(-x)$, $\bar{f}(x) = \overline{f(x)}$ a $f_t(x) = f(x+t)$. Pre $U(d, l)$ normu $0 \leq l \leq d$ podľa príkladu 2.4 platí

$$\|f_-\|_{U(d,l)} = \|\bar{f}\|_{U(d,l)} = \|f_t\|_{U(d,l)} = \|f\|_{U(d,l)}.$$

Zároveň platí

$$(f * g)(t) = \mathbb{E}_x f(t-x)g(x) = \mathbb{E}_x f_-(-t+x) \overline{\bar{g}(x)} = (f_- \star \bar{g})(-t).$$

Máme ekvivalenciu

$$\|f * g\|_A \leq \|f\|_B \|g\|_C \iff \|f \star g\|_A \leq \|f\|_B \|g\|_C.$$

Inými slovami, nerovnosti typu Youngovej nerovnosti môžeme formulovať aj pomocou krížovej korelácie.

Jedno z riešení rovnice $\frac{1}{p} + \frac{1}{q} = \frac{1}{r} + 1$ je $p = q = 2$ a $r = \infty$, ktorého dôsledkom je, že konvolúcia dvoch funkcií z $L_2(\mathbb{R})$ je rovnomerne ohraničená súčinom $\|f\|_2 \|g\|_2$. Iné zaujímavé riešenia vyžadujú aby $p < 2$ alebo $q < 2$. Do štruktúry $U(d, l)$ noriem patria spomedzi p -noriem iba 2^d -normy, pre ktoré nutne platí $2^d \geq 2$. Priamu analógiu Youngovej nerovnosti teda nemôžeme očakávať.

Napriek spomínaným komplikáciám sa môžeme pokúsiť hľadať analógie Youngovej nerovnosti (formulovanej pomocou krížovej korelácie) pre uniformné normy s tým, že v Youngovej nerovnosti sa pokúsime nahradiť p -normy vhodnými $U(d, l)$ normami. Vďaka dokázaným nerovnostiam $\|f\|_{2^d} \geq \|f\|_{U(d,l)}$ môže ísť o netriviálne výsledky.

Príklad 3.8 (Youngova rovnosť pre polonormy $U(d, d)$). *Overíme pomerne triviálnu identitu $\|f \star g\|_{U(r,r)} = \|f\|_{U(p,p)} \|g\|_{U(q,q)}$, pre ľubovoľné p, q a r .*

Riešenie. Pre polonormy $U(d, d)$ platí $\|f\|_{U(d,d)} = |\mathcal{F}f(0)|$. Ďalej platí

$$\|f \star g\|_{U(r,r)} = \underbrace{\left| \mathcal{F}[f \star g](0) \right|}_{\text{príklad 1.3}} = \left| \mathcal{F}f(0) \overline{\mathcal{F}g(0)} \right| = \left| \mathcal{F}f(0) \right| \left| \mathcal{F}g(0) \right| = \|f\|_{U(p,p)} \|g\|_{U(q,q)}. \quad \square$$

Príklad 3.9 (Ohraničenie 2-normou). *Ukážeme, že pre ľubovoľné $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $-1 \leq l \leq d$ platí nerovnosť $\|f \star g\|_{U(d,l)} \leq \|f\|_2 \|g\|_2$.*

Riešenie. V príklade 3.5 sme ukázali nerovnosť $|(f \star g)(t)| \leq \|f\|_2^2$ pre autokoreláciu funkcie f . Pre krížovú koreláciu platí analogická nerovnosť

$$|(f \star g)(t)| = \left| \mathbb{E}_x \underbrace{f(x+t) \overline{g(x)}}_{\text{označíme } f_t(x)} \right| = \underbrace{\left| \langle f_t, g \rangle \right|}_{\text{Cauchy-Schwarzova nerovnosť}} \leq \|f\|_2 \|g\|_2.$$

Nerovnosť $\|f \star g\|_{U(d,l)} \leq \|f\|_2 \|g\|_2$ je dôsledkom absolútnej homogenity $U(d, l)$ normy.

Máme

$$\|f \star g\|_{U(d,l)} \leq \| |f \star g| \|_{U(d,l)} \leq \|f\|_2 \|g\|_2. \quad \square$$

Príklad 3.10. *Overíme nerovnosť $\|f \star g\|_{U(2,1)} \leq \|f\|_{U(3,2)} \|g\|_{U(3,2)}$.*

Riešenie. Pre $\|f \star g\|_{U(2,1)}$ podľa príkladu 1.5 platí

$$\begin{aligned} \|f \star g\|_{U(2,1)} &= \underbrace{\left\| \mathcal{F}[f \star g] \right\|_4}_{\text{príklad 1.3}} \\ &= \left\| \mathcal{F}f \overline{\mathcal{F}g} \right\|_4 \\ &= \underbrace{\left\langle |\mathcal{F}f|^4, |\mathcal{F}g|^4 \right\rangle^{1/4}}_{\text{Cauchy-Schwarzova nerovnosť}} \\ &\leq \left\| |\mathcal{F}f|^4 \right\|_2^{\frac{1}{4}} \left\| |\mathcal{F}g|^4 \right\|_2^{1/4} \\ &= \left\| \mathcal{F}f \right\|_8 \left\| \mathcal{F}g \right\|_8 \\ &= \|f\|_{U(3,2)} \|g\|_{U(3,2)}. \quad \square \end{aligned}$$

Aj vo všeobecnosti platí

$$\|f \star g\|_{U(d,d-1)} \leq \|f\|_{U(d+1,d)} \|g\|_{U(d+1,d)},$$

vďaka dualite $\|f\|_{U(d,d-1)} = \|\mathcal{F}f\|_{U(d,0)} = \|\mathcal{F}f\|_{2^d}$, pričom zvyšok argumentu zostáva nezmenený.

Pre $U(2, 0)$ normu, teda 4-normu, už taký priamočiary výsledok nedostaneme.

Príklad 3.11. Analogickým postupom ako v predchádzajúcom príklade budeme hľadať nerovnosť pre $\|f \star g\|_4 = \|f \star g\|_{\mathcal{U}(2,0)}$.

Riešenie. Vďaka dualite v dôsledku 2.10 môžeme vykonať sériu úprav

$$\begin{aligned}
\|f \star g\|_4^4 &= \underbrace{\|\mathcal{F}[f \star g]\|_{\mathcal{U}(2,1)}^4}_{\text{príklad 1.3}} \\
&= \|\mathcal{F}f \overline{\mathcal{F}g}\|_{\mathcal{U}(2,1)}^4 \\
&= \sum_{\xi, \alpha, \beta} \Delta_\alpha \Delta_\beta \mathcal{F}f(\xi) \overline{\mathcal{F}g(\xi)} \\
&= \underbrace{\left\langle \Delta_\alpha \Delta_\beta \mathcal{F}f(\xi), \Delta_\alpha \Delta_\beta \mathcal{F}g(\xi) \right\rangle}_{\text{Cauchy-Schwarzova nerovnosť}} \\
&\leq \left(\sum_{\xi, \alpha, \beta} \Delta_\alpha \Delta_\beta \mathcal{F}f(\xi) \overline{\mathcal{F}f(\xi)} \right)^{1/2} \left(\sum_{\xi, \alpha, \beta} \Delta_\alpha \Delta_\beta \mathcal{F}g(\xi) \overline{\mathcal{F}g(\xi)} \right)^{1/2} \\
&= \|\mathcal{F}f \overline{\mathcal{F}f}\|_{\mathcal{U}(2,1)}^2 \|\mathcal{F}g \overline{\mathcal{F}g}\|_{\mathcal{U}(2,1)}^2 \\
&= \|\mathcal{F}(f)_\mathbb{K}\|_{\mathcal{U}(2,1)}^2 \|\mathcal{F}(g)_\mathbb{K}\|_{\mathcal{U}(2,1)}^2 \\
&= \|(f)_\mathbb{K}\|_4^2 \|(g)_\mathbb{K}\|_4^2.
\end{aligned}$$

Výraz $\|(f)_\mathbb{K}\|_4^{1/2}$ nezodpovedá žiadnej $\mathcal{U}(d, l)$ norme, nakoľko po rozpísaní autokorelácie sa jedná o výraz s 5 diskretnými integrálmi a súčinom 8 funkcií. $\square$

Nerovnosť v príklade 3.11 sa dá zovšeobecniť na všeobecný výsledok pre ľubovoľnú $\mathcal{U}(d, l)$ normu, keďže v postupe nevyužívame konkrétny tvar $\mathcal{U}(2, 1)$ -normy a pre každú $\mathcal{U}(d, l)$ normu platí dualita v dôsledku 2.10.

Veta 3.8. *Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $0 \leq l \leq d - 1$ a $f, g : \mathbb{Z}_N \rightarrow \mathbb{C}$. Potom platí nerovnosť*

$$\|f \star g\|_{\mathcal{U}(d, l)} \leq \|(f)_\mathbb{K}\|_{\mathcal{U}(d, l)}^{1/2} \|(g)_\mathbb{K}\|_{\mathcal{U}(d, l)}^{1/2}.$$

Dôkaz. Z definície 2.6, duality v dôsledku 2.10 a príkladu 1.3 vyplýva

$$\begin{aligned}
\|f \star g\|_{\mathcal{U}(d, l)}^{2^d} &= \|\mathcal{F}[f \star g]\|_{\mathcal{U}(d, d-l-1)}^{2^d} \\
&= \|\mathcal{F}f \overline{\mathcal{F}g}\|_{\mathcal{U}(d, d-l-1)}^{2^d} \\
&= \sum_{\mathbf{P}(d, l) \chi = \mathbf{0}} \prod_{i=1}^{2^d} z_i \overline{\mathcal{F}f(\chi_i)} \overline{\mathcal{F}g(\chi_i)}
\end{aligned}$$

$$\begin{aligned}
&= \sum_{\mathbf{P}(d,l)\chi=\mathbf{0}} \underbrace{\prod_{i=1}^{2^d} z_i \overline{\mathcal{F}f(\chi_i)}}_{\text{označíme } \Phi[f](\chi)} \prod_{i=1}^{2^d} {}^{-z_i} \overline{\mathcal{F}g(\chi_i)} \\
&= \sum_{\mathbf{P}(d,l)\chi=\mathbf{0}} \Phi[f](\chi) \overline{\Phi[g](\chi)}.
\end{aligned}$$

Nech $\widehat{\mathcal{H}}$ je daná

$$\widehat{\mathcal{H}} = \left\{ \chi \in \widehat{\mathbb{Z}}_N^{2^d} \mid \mathbf{P}(d, l) \chi = \mathbf{0} \right\}.$$

Výraz $\|f \star g\|_{\mathbf{U}(d,l)}^{2^d}$ môžeme vyjadriť pomocou skalárneho súčinu a ďalej platí

$$\|f \star g\|_{\mathbf{U}(d,l)}^{2^d} = \underbrace{\langle \Phi[f], \Phi[g] \rangle_{\widehat{\mathcal{H}}}}_{\mathbf{U}(d,l) \text{ je norma}} = \underbrace{\left| \langle \Phi[f], \Phi[g] \rangle_{\widehat{\mathcal{H}}} \right|}_{\text{Cauchy-Schwarzova nerovnosť}} \leq \langle \Phi[f], \Phi[f] \rangle_{\widehat{\mathcal{H}}}^{1/2} \langle \Phi[g], \Phi[g] \rangle_{\widehat{\mathcal{H}}}^{1/2}.$$

Postup, ktorým sem odvodili vyjadrenie $\|f \star g\|_{\mathbf{U}(d,l)}^{2^d} = \langle \Phi[f], \Phi[g] \rangle_{\widehat{\mathcal{H}}}$, môžeme obrátiť a dostávame nerovnosť

$$\|f \star g\|_{\mathbf{U}(d,l)}^{2^d} \leq \langle \Phi[f], \Phi[f] \rangle_{\widehat{\mathcal{H}}}^{1/2} \langle \Phi[g], \Phi[g] \rangle_{\widehat{\mathcal{H}}}^{1/2} = \|(f)_{\mathbf{K}}\|_{\mathbf{U}(d,l)}^{2^{d-1}} \|(g)_{\mathbf{K}}\|_{\mathbf{U}(d,l)}^{2^{d-1}}. \quad \square$$

Norma $\|(f)_{\mathbf{K}}\|_{\mathbf{U}(d,l)}^{1/2}$ sa zjednoduší na štandardnú $\mathbf{U}(d, l)$ normu iba v niektorých prípadoch, napríklad, keď platí $l = d - 1$ alebo $l = d$.

Keďže všetky odvodenia nerovností pre $\mathbf{U}(d, l)$ normy využívali Cauchy-Schwarzovu nerovnosť, platí, že pre funkciu $g = Cf$ sa v nich nadobudne rovnosť.

Nerovnosť vo vete 3.8 je silnejšia ako štandardné ohraňenie 2-normou funkcií f a g . Pre autokoreláciu podľa príkladu 3.5 platí

$$\left| (f)_{\mathbf{K}}(t) \right| \leq (f)_{\mathbf{K}}(0) = \underbrace{\|f\|_{\mathbf{U}(1,0)}}_{\text{dôsledok 2.12}} = \|f\|_2,$$

čo vedie na nerovnosť

$$\|(f)_{\mathbf{K}}\|_{\mathbf{U}(d,l)}^{1/2} \leq \|f\|_2.$$

Tvrdenie 3.9. *Nech $d \in \mathbb{N}$, $l \in \mathbb{Z}$, $-1 \leq l \leq d - 1$ a $f : \mathbb{Z}_N \rightarrow \mathbb{C}$. Potom výraz $\|(f)_{\mathbf{K}}\|_{\mathbf{U}(d,l)}^{1/2}$ je norma funkcie f .*

Dôkaz. Nech $l \geq 0$. Trojuholníková nerovnosť pre $\|(f)_{\mathbf{K}}\|_{\mathbf{U}(d,l)}^{1/2}$ vyplýva z trojuholníkovej

nerovnosti pre $U(d, l)$ normu

$$\begin{aligned}
\| (f + g)_K \|_{U(d, l)}^{1/2} &= \underbrace{\| (f)_K + (f \star g) + (g \star f) + (g)_K \|_{U(d, l)}^{1/2}}_{\text{trojuholníková nerovnosť pre } U(d, l)} \\
&\leq \left(\| (f)_K \|_{U(d, l)} + 2 \underbrace{\| f \star g \|_{U(d, l)}}_{\text{veta 3.8}} + \| (g)_K \|_{U(d, l)} \right)^{1/2} \\
&\leq \left(\| (f)_K \|_{U(d, l)} + 2 \| (f)_K \|_{U(d, l)}^{1/2} \| (g)_K \|_{U(d, l)}^{1/2} + \| (g)_K \|_{U(d, l)} \right)^{1/2} \\
&= \| (f)_K \|_{U(d, l)}^{1/2} + \| (g)_K \|_{U(d, l)}^{1/2}.
\end{aligned}$$

Ďalej bude platiť absolútna homogenita

$$\| (Cf)_K \|_{U(d, l)}^{1/2} = \| |C| (f)_K \|_{U(d, l)}^{1/2} = |C| \| (f)_K \|_{U(d, l)}^{1/2},$$

pre konštantu $C \in \mathbb{C}$.

Kladnú definitnosť môžeme overiť využitím duality v dôsledku 2.10 a príkladu 1.3. Máme

$$\| (f)_K \|_{U(d, l)}^{1/2} = \| \mathcal{F}f \overline{\mathcal{F}f} \|_{U(d, d-l-1)}^{1/2}.$$

Norma $U(d, d-l-1)$ je kladne definitná pre $0 \leq l \leq d-1$. Navyše DFT je regulárne zobrazenie, preto platí, že $\mathcal{F}f$ je identicky rovné nule práve vtedy, keď f je identicky rovné nule.

Pre $l = -1$ máme

$$\| (f)_K \|_{U(d, -1)}^{1/2} = \| (f)_K(0) \|^{1/2} = \left\| \mathbb{E}_x f(x) \overline{f(x)} \right\|^{1/2} = \| f \|_2. \quad \square$$

Keďže výraz $\| (f)_K \|_{U(d, l)}^{1/2}$ je norma funkcie f , nerovnosť vo vete 3.8 je naozaj nerovnosť medzi normami a predstavuje analógiu Youngovej nerovnosti.

Ako ukážeme v nasledujúcom príklade, norma $\| (f)_K \|_{U(2, 1)}^{1/2}$ má vlastnosť $U(d, l)$ (polo)-normiem, ktorú sme overili v príklade 1.4, teda citlivosť na absolútnu hodnotu.

Príklad 3.12. Overíme, že pre normu $\| (f)_K \|_{U(2, 1)}^{1/2}$ existujú funkcie $f : \mathbb{Z}_3 \rightarrow \mathbb{C}$, pre ktoré platí nerovnosť $\| (f)_K \|_{U(2, 1)}^{1/2} < \| (|f|)_K \|_{U(2, 1)}^{1/2}$.

Riešenie. Spočítajme autokoreláciu funkcie $f(x) = (-1)^x$ v $\mathbb{Z}_3$

$$(f)_K(t) = \mathbb{E}_x f(x+t) \overline{f(x)} = \mathbb{E}_x (-1)^{2x+t} = \mathbb{E}_x (-1)^t = (-1)^t = f(t).$$

Podľa príkladu 1.4 platí

$$\| (f)_\mathbf{K} \|_{\mathbf{U}(2,1)}^{1/2} = \underbrace{\| f \|_{\mathbf{U}(2,1)}^{1/2}}_{\text{dôsledok 2.12}} = \underbrace{\| f \|_{\mathbf{U}(2)}^{1/2}}_{\text{príklad 1.4}} < \| |f| \|_{\mathbf{U}(2)}^{1/2} = \| (|f|)_\mathbf{K} \|_{\mathbf{U}(2,1)}^{1/2}. \quad \square$$

V nasledujúcom príklade nájdeme, akú hodnotu má norma $\| (f)_\mathbf{K} \|_{\mathbf{U}(d,l)}^{1/2}$ funkcie δ , ktorá pre nás bola kľúčová pri hľadaní schémy nerovnosti 3.

Príklad 3.13. *Spočítame normu δ funkcie $\| (\delta)_\mathbf{K} \|_{\mathbf{U}(d,l)}^{1/2}$.*

Riešenie. Pre autokoreláciu δ funkcie platí

$$(\delta)_\mathbf{K} = \mathbb{E}_x \delta(x+t) \underbrace{\overline{\delta(x)}}_{\substack{0 \text{ pre } x \neq 0 \\ N \text{ pre } x=0}} = \frac{1}{N} \delta(0+t) \underbrace{\overline{\delta(0)}}_N = \delta(t).$$

Z príkladu 3.1 potom vyplýva

$$\| (\delta)_\mathbf{K} \|_{\mathbf{U}(d,l)}^{1/2} = \| \delta \|_{\mathbf{U}(d,l)}^{1/2} = N^{1/2 - \frac{l}{\Sigma} \binom{d}{i} / 2^{d+1}}. \quad \square$$

Vieme, že výraz $\| (f)_\mathbf{K} \|_{\mathbf{U}(d,-1)}^{1/2}$ je norma funkcie f , ktorá pre väčšinu stupňov l nadobúda iné hodnoty ako $\mathbf{U}(d,l)$ (polo)normy, avšak zachováva niektoré vlastnosti $\mathbf{U}(d,l)$ noriem. Z týchto dôvodov a z toho, že vystupuje v analógii Youngovej nerovnosti vo vete 3.8, môže byť zaujímavou úlohou ďalej skúmať normu $\| (f)_\mathbf{K} \|_{\mathbf{U}(d,-1)}^{1/2}$.

V článku [3] uvádzajú H. Brascamp a E. Lieb zovšeobecnenie Youngovej nerovnosti pre viac ako tri funkcie. Predmetom ďalšieho výskumu by mohlo byť skúmanie, aký súvis majú naše zovšeobecnenia autokorelácie v definícii 3.3 a zovšeobecnenia konvolúcie v článku [3].

Záver

V našej diplomovej práci patrilo medzi ciele nájsť vzťahy medzi p -normami (špeciálne 2^d -normami) a zovšeobecneniami Gowersových uniformných noriem - $U(d, l)$ normami. Z dôsledku 2.12 vyplýva, že spomínané 2^d normy sú len špeciálnym prípadom $U(d, l)$ noriem pre $l = 0$. Dokázané nerovnosti v dôsledkoch 3.2 a 3.6 charakterizujú nerovnosti medzi $U(d, l)$ normami vzhľadom na rád d a stupeň l , ktoré charakterizujú hľadané vzťahy. Ukázali sme nielen že $U(d, l)$ normy sú ekvivalentné (čo nutne platí pre normy na konečnorozmerných priestoroch), ale našli sme aj najlepšie konštanty, ktoré vystupujú v nerovnostiach medzi $U(d, l)$ normami.

Zároveň sme vďaka získaným nerovnostiam v podkapitole 3.1 popísali, aké by mohli platiť inklúzie priestorov funkcií na jednotkovej kružnici, resp. obojstranných nekonečných postupností. Identifikácia možných inklúzií priestorov funkcií na $\mathbb{S}^1$, resp. nekonečných postupností na $\mathbb{Z}$, patrila medzi ďalšie ciele našej diplomovej práce.

V podkapitole 3.2 sme uviedli jeden prístup k hľadaniu analógie Youngovej konvolučnej identity pre $U(d, l)$ normy. Spomíname ale aj potenciálne problémy hľadania týchto zovšeobecnení - $U(d, l)$ normy nemáme definované tak, aby p -normy pre $p < 2$ zodpovedali niektorej $U(d, l)$ norme. Naš prístup viedol k definícii novej normy, ktorá má niektoré vlastnosti $U(d, l)$ noriem.

Okrem spomínaných výsledkov v kapitole 3 sa v našej práci v kapitole 1 nachádza prehľad niektorých zaujímavých nástrojov diskkrétnej Fourierovej analýzy vyšších rádov a Gowersových uniformných noriem. Medzi nové výsledky v týchto oblastiach patrí všeobecnejšia formulácia zovšeobecnenej konvolučnej identity v tvrdení 1.8 a duálnej zovšeobecnenej konvolučnej identity v dôsledku 1.9 a ich aplikácia v prípade priameho vyjadrenia $G(d, l)$ skalárnych súčinov v tvrdení 2.9. V kapitole 2 ďalej uvádzame zovšeobecnenia Gowersových uniformných noriem z pracovného článku M. Niepela [7]. Definície, ktoré využívame v kapitole 2 sú originálne, a poskytujú iný pohľad na $U(d, l)$ normy.

V práci často uvádzame príklady, ktoré slúžia ako motivácia ďalších tvrdení a definícií, alebo poukazujú na zaujímavé vlastnosti skúmanej témy. Mnohé z uvádzaných tvrdení dokazujeme spôsobom, ktorý je iný ako v článku [7], a tým ilustruje nové prepojenia. Tiež v práci zavádzame nové pojmy, ktoré slúžia ako užitočný nástroj pre $U(d, l)$ normy. Na záver práce spomíname niekoľko oblastí, v ktorých je priestor na ďalší výskum.

Zoznam použitej literatúry

- [1] Artin, M.: *Algebra*, Prentice Hall, New Jersey, 1991
- [2] Bergelson, V., Tao, T., Ziegler, T.: *An Inverse Theorem for the Uniformity Seminorms Associated with the Action of $\mathbb{F}_p^\infty$* , Geometric and Functional Analysis 19 (2010), 1539-1596
- [3] Brascamp, H. J., Lieb, E. H.: *Best Constants in Young's Inequality, Its Converse, and Its Generalization to More than Three Functions*, Advances in Mathematics 20 (1976), 151-173
- [4] Gowers, W. T.: *A new proof of Szemerédi's theorem*, Geometric and Functional Analysis 11 (2001), 465-588
- [5] Gowers, W. T.: *Generalizations of Fourier analysis, and how to apply them*, Bulletin of the American Mathematical Society 54 (2017), 1-44
- [6] Host, B., Kra, B.: *A point of view on Gowers uniformity norms*, The New York Journal of Mathematics 18 (2012), 213-248
- [7] Niepel, M.: *Parseval type identities for Gowers uniformity norms in finite Abelian groups*, preprint, Comenius University, Bratislava, 2020
- [8] Rakús, M.: *Identity vo Fourierovej analýze vyšších rádov*, bakalárska práca, FMFI UK, Bratislava, 2021
- [9] Shakarchi, R., Stein E. M.: *Functional Analysis: Introduction to Further Topics in Analysis*, Princeton University Press, Princeton and Oxford, 2011
- [10] Szegedy, B.: *On higher order Fourier analysis*, preprint, University of Toronto, Toronto, 2012, dostupné na internete (15.1.2023) <https://arxiv.org/pdf/1203.2260.pdf>
- [11] Tao, T.: *Higher order Fourier analysis*, American Mathematical Society, Providence, Rhode Island, 2012
- [12] Young, W. H.: *On the multiplication of successions of Fourier constants*, Proceedings of the Royal Society A 87 (1912), 331-339