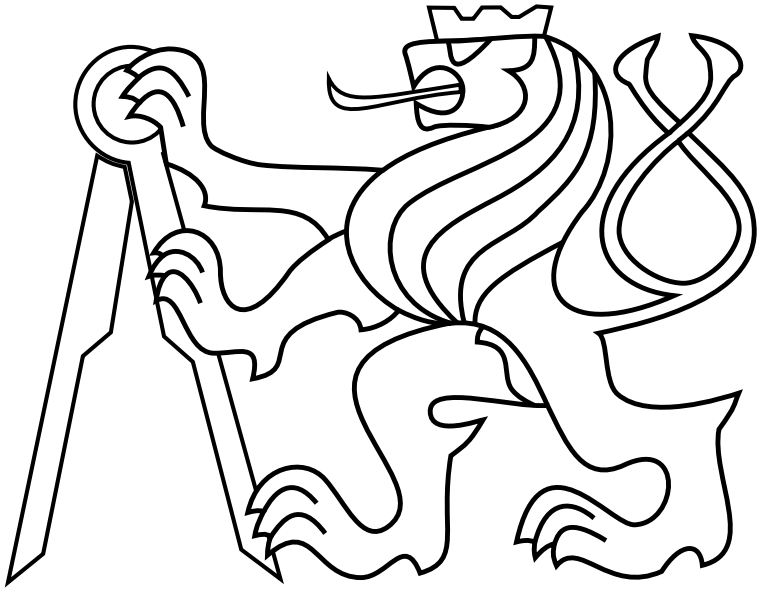
České vysoké učení technické v Praze

Fakulta elektrotechnická

Diplomová práce



Michal Gabriel

Metody sít v moderní teorii prvočísel

Katedra počítačů

Vedoucí práce: **doc. RNDr. Martin Klazar, Dr.**

Prohlášení autora práce

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.[11]

V Praze dne..... .....

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Gabriel** Jméno: **Michal** Osobní číslo: **434673**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra počítačů**

Studijní program: **Otevřená informatika**

Specializace: **Kybernetická bezpečnost**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Metody sít v moderní teorii prvočísel

Název diplomové práce anglicky:

Sieves Methods in Modern Number Theory

Pokyny pro vypracování:

Student zpracuje přehledově Maynardův článek, v němž se dokazuje, že vzdálenosti dvou sousedních prvočísel mají konečný liminf, a vyloží i teorii nutnou pro tento důkaz. Pokusí se také v teorii prvočísel využít svou ideu odhadu chyby v lineární aproximaci c.fi(m)/m pro počet čísel velkých nejvýše c a nesoudělných s m (případně splňujících jisté kongruence).

Seznam doporučené literatury:

[1] Maynard, James: Small gaps between primes. Ann. of Math. (2) 181 (2015), no. 1, 383–413.
[2] Friedlander, John; Iwaniec, Henryk: Opera de cribro. American Mathematical Society Colloquium Publications, 57. American Mathematical Society, Providence, RI, 2010. xx+527 pp.
[3] Letendre, Patrick: The larger sieve and polynomial congruences, arXiv:1810.11436

Jméno a pracoviště vedoucí(ho) diplomové práce:

doc. RNDr. Martin Klazar, Dr., Katedra aplikované matematiky, Matematicko-fyzikální fakulta, Univerzita Karlova

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **05.02.2020** Termín odevzdání diplomové práce: **22.05.2020**

Platnost zadání diplomové práce: **30.09.2021**

doc. RNDr. Martin Klazar, Dr. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Mgr. Petr Páta, Ph.D. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

. Datum převzetí zadání

Podpis studenta

Poděkování

Chtěl bych poděkovat vedoucímu práce panu Martinu Klazarovi za spolupráci a možnost zpracovat práci na téma z teorie čísel. Oponentovi práce panu Petru Habalovi děkuji za ochotu a čas věnovaný při zvažování nápadů. Dále bych rád poděkoval příteli Richardu Štecovi za četné a přínosné konzultace.

Abstract

Sieve methods are used to evaluate count of prime numbers in the number theory. The arrangement of prime numbers in direction to infinity is a mystery even these days. Existence of infinitly repetitious prime gap was proven less than fifteen years ago. Yitang Zhang gave particular bound of such prime gap in 2013. James Maynard proved significantly better boundary in his article *Small gaps between primes* which is subject of this work. We will pass through all steps of proof of several results about prime number differency limit inferior in detail. Concepts needed for this method will be given also.

Abstrakt

V teorii čísel umožňují metody sít vyhodnotit počty prvočísel, jejichž rozmístění směrem k nekonečnu je stále záhadou. Až v posledních patnácti letech bylo dokázáno, že existuje mezera mezi dvěma následujícími prvočísly, která se opakuje nekonečně často. Konkrétní mez pro velikost takové mezery podal v roce 2013 Yitang Zhang a nedlouho potom dokázal výrazně nižší mez i James Maynard ve svém článku *Small gaps between primes*, kterému se věnuje tato práce. Projdeme si dopodrobna všechny kroky vedoucí k důkazu několika závěrů ohledně limes inferior rozdílu prvočísel. Vyloženy budou i koncepty potřebné pro tuto metodu.

Obsah

Značení

$\mathbb{N}$	množina přirozených čísel $\{1, 2, 3, \dots\}$
$\mathbb{R}$	množina reálných čísel
$\mathbb{P}$	množina prvočísel $\{2, 3, 5, \dots\}$
$\lvert A\rvert$	počet prvků množiny A
$\chi_A(x)=1$	prvek x patří do množiny A
$\chi_A(x)=0$	prvek x nepatří do množiny A
$\chi_A(B)$	počet prvků B patřících do množiny A
p_n	n-té prvočíslo
$d\mid n$	číslo d dělí číslo n
$d_1, d_2\mid n$	čísla d_1 a d_2 dělí číslo n
$d\mid n, m$	číslo d dělí čísla n a m
$d_1, d_2\mid n, m$	čísla d_1 a d_2 dělí čísla n a m
$\pi(n)$	počet prvočísel menších nebo rovných n
$\gcd(a, b)$	nejvyšší společný dělitel čísel a a b
$\operatorname{lcm}(a, b)$	nejmenší společný násobek čísel a a b
$\log(x)$	přirozený logaritmus čísla x
$\lfloor x\rfloor$	spodní celá část čísla x (největší celé číslo menší než x)
$\lceil x\rceil$	horní celá část čísla x (nejmenší celé číslo větší než x)
$\tau_k(n)$	počet možností zapsání čísla n jako součinu k přirozených čísel
$\varphi(n)$	Eulerova funkce z čísla n
$\mu(n)$	Möbiova funkce z čísla n
$f(n) \ll g(n)$	$f(n) \in O(g(n))$ (neboli $\exists c > 0\ \exists n_0 :\ \forall n > n_0\ \lvert f(n)\rvert \le c\,\lvert g(n)\rvert$)
$f(n) \ll_m g(n)$	$\exists c(m) > 0\ \exists n_0 :\ \forall n > n_0\ \lvert f(n)\rvert \le c(m)\,\lvert g(n)\rvert$
$f(n) \sim g(n)$	$\lim_{n\to\infty} \frac{f(n)}{g(n)}=1$
$\liminf_{n\to\infty} a_n$	$\lim_{n\to\infty} (\inf_{m\ge n} a_m)$

1 Úvod

Vlastnosti rozmístění prvočísel ve velkých číslech limitně jdoucích do nekonečna je stále do značné míry neprobádaná oblast. Není známa ani odpoveď na zdánlivě jednoduchou otázku, zda se každá možná velikost prvočíselné mezery opakuje nekonečněkrát. Ač známým speciálním případem je domněnka o nekonečném počtu prvočíselných dvojic, předpokládá se, že nekonečněkrát se vyskytuje každá možná prvočíselná mezera.

Podobně důležité otázky se snaží řada matematiků řešit pomocí metod takzvaných sít. Ty mají za cíl určit obecně v nějaké podmnožině přirozených čísel počet prvočísel, popřípadě čísel nedělitelných určitou sadou prvočísel.

Velikost nejmenší nekonečně časté prvočíselné mezery vyjadřuje limes inferior rozdílu dvou po sobě jdoucích prvočísel. Limes inferior obecně vyjadřuje limitní hodnotu minima z prvků následujících prvku jdoucího do nekonečna. Snaha je tak omezit zeshora hodnotu $\liminf_{n\to\infty}(p_{n+1}-p_n)$, a to ideálně až k hodnotě 2. Přitom teprve patnáct let zpět bylo dokázáno, že taková konečná hranice vůbec existuje.

Náš zájem budí i limes inferior z rozdílů prvočísel, která spolu přímo nesousedí. Například $\liminf_{n\to\infty}(p_{n+2}-p_n)$, ale i obecně $\liminf_{n\to\infty}(p_{n+m}-p_n)$.

V této práci se budeme věnovat průlomovému článku Jamese Maynarda *Small gaps between primes*, v kterém autor dokázal několik nerovností týkajících se limes inferior rozdílu prvočísel. Nejvýraznějším výsledkem je tvrzení $\liminf_{n\to\infty}(p_{n+1}-p_n) \leq 600$, nicméně obsaženy jsou další závěry, některé podmíněné dosud nerozhodnutou domněnkou.

Nejdříve si v první části popíšeme některé základní myšlenky a koncepty, které jsou potřebné pro samotný důkaz. Druhá část již pečlivě prochází Maynardův článek a snaží se objasnit každý krok jeho inovativního postupu.

1.1 Multiplikativní a zcela multiplikativní funkce

V teorii čísel hrají významnou roli multiplikativní funkce, které splňují identitu dávající do souvislosti součin funkčních hodnot nesoudělných argumentů a funkční hodnotu součinu těchto argumentů.

Definice 1 (Multiplikativní funkce): *Aritmetickou funkcí f nazýváme multiplikativní právě tehdy, když pro všechna nesoudělná a a b ($\gcd(a, b) = 1$) platí*

$$f(ab) = f(a) \cdot f(b).$$

Podstatným důsledkem je, že hodnota funkce pro neutrální prvek na násobení musí být rovna neutralnímu prvku na násobení, tedy platí $f(1) = 1$, neboť číslo 1 je nesoudělné se všemi ostatními přirozenými čísly.

Jako zcela multiplikativní funkci pak označujeme takovou funkci, pro kterou rovnost platí bez ohledu na soudělnost a a b.

Definice 2 (Zcela multiplikativní funkce): *Aritmetickou funkci f nazýváme zcela multiplikativní právě tehdy, když pro všechna a a b platí*

$$f(ab) = f(a) \cdot f(b).$$

Jednou z nejvýznamnějších multiplikativních funkcí je Eulerova funkce φ vyjadřující počet (přirozených) čísel menších nebo rovno[1] argumentu s nim nesoudělných.

Definice 3 (Eulerova funkce): *Multiplikativní funkce Eulerova funkce je definována pro mocninu prvočísla*

$$\varphi(p^k) = p^{k-1}(p-1).$$

Diky multiplikativnosti muzeme psat

$$\varphi(n) = \prod_{p|n} \varphi(p^{k_p}) = \prod_{p|n} p^{k_p} \left(1 - \frac{1}{p}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

[1] Rovnost se uplatní pouze pro $\varphi(1)$.

Alternativně bychom mohli funkci definovat ve smyslu původní intuice

$$\varphi(n) = \sum_{\substack{1 \leq i \leq n \\ \gcd(i,n)=1}} 1.$$

Za význačné hodnoty můžeme považovat hlavně $\varphi(1) = 1$ a $\varphi(p) = p - 1$.

Vzhledem k definici a multiplikativnosti je snadné hodnotu spočítat při znalosti prvočíselného rozkladu argumentu, avšak absence algoritmu s polynomialní složitostí pro výpočet hodnoty Eulerovy funkce bez znalosti rozkladu je duležitou vlastností této funkce.

Další funkcí, kterou v následujícím textu budeme často využívat, je Möbiova funkce umoznujici rozlisit mezi čísly obsahujici sudy nebo lichy pocet prvočísel a čísly obsahujici nějaké prvočíslo násobně.

Definice 4 (Möbiova funkce): *Möbiovu funkcí definujeme pro přirozené číslo n podle*

$$\mu(n) = \begin{cases} 1 & \textit{pro bezčtvercové číslo se sudým počtem prvočinitelů,} \\ -1 & \textit{pro bezctvercove číslo s lichým počtem prvočinitelů,} \\ 0 & \textit{pro číslo obsahující mocninu prvočinitele.} \end{cases}$$

Jiná používaná definice vyzaduje funkce ω a Ω vyjadřující počet unikátních prvočinitelů, respektive pocet prvočinitelů včetně násobností. Pomocí Ω je definována i Liouvilleova funkce, která se často v definici Möbiovy funkce používá pro jejich shodu v bezčtvercovych argumentech.

Časté použití Möbiovy funkce spociva v nasobeni jejím kvadrátem, obvzláště v součtech, což zajistí nulový příspěvek pro členy nesplňující bezčtvercovost. Bezčtvercová čísla mají v teorii čísel značnou důležitost a ve spoustě vět či tvrzení se pracuje pouze s nimi, neboť čísla obsahující čtverec buď danou zajímavou vlastnost postrádaji, nebo se dají nahradit svým takzvaným radikálem, tedy číslem obsahující stejná prvočísla, ale bez umocnění.

Zajímavou vlastností Eulerovy funkce je hodnota součtu přes dělitele

$$\sum_{d|n} \varphi(d) = n,$$

a z toho Möbiovou inverzí vyvstávající vztah

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n\sum_{d|n}\frac{\mu(d)}{d},$$

pro Möbiovu funkci potom suma přes dělitele odpovídá

$$\sum_{d|n}\mu(d) = \begin{cases} 1 & \text{pro } n = 1 \\ 0 & \text{pro } n > 1. \end{cases} \tag{1}$$

Zadefinujme si na chvíli multiplikativní funkci g vztahem pro prvočísla $g(p) = p - 2$. Potom analogicky k (1.1) máme pro bezčtvercové n (důkaz bychom vedli indukcí)

$$\sum_{d|n} g(d) = \varphi(n). \tag{2}$$

1.2 Symetrické polynomy

Polynom více proměnných, který je shodný z pohledu všech proměnných, nazýváme symetrickým polynomem.

Definice 5 (Symetrický polynom): *Nechť $P(x_1, \ldots, x_k)$ je polynom k proměnných a $\sigma : \{1, \ldots, k\} \mapsto \{1, \ldots, k\}$ permutace na indexech x, potom polynom je symetrický, pokud pro všechna σ platí*

$$P(x_1, \ldots, x_k) = P(x_{\sigma(1)}, \ldots, x_{\sigma(k)}).$$

1.3 Kvadratické formy

V symetrické dvojité sumaci součinu, jehož prvky můžeme rozdělit na členy závislé na jednom indexu, symetrickým výrazem pro oba indexy, a členy závislé na obou indexech, můžeme spatřovat nasobení matic vektorem. Proto zavedeme následující pojem, který nám pomůže přejít k maticovému počtu, což využijeme při hledání extrémů výrazu nabízejícího na první pohled příliš kombinatorických možnosti.

Definice 6 (Kvadratická forma): *Zobrazení $Q : \mathbb{R}^n \mapsto \mathbb{R}$ nazýváme kvadratická forma, pokud existuje symetrická čtvercová matice $A \in \mathbb{R}^{n,n}$ taková, že*

$$\forall x \in \mathbb{R}^n : \quad Q(x) = x^T A x.$$

Pokud hodnotu Q vyjádříme namísto maticového násobení pomocí sum, získáme

$$Q(x) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j,$$

kde a_{ij} odkazuje na jednotlivé prvky matice, stejně jako x_i na jednotlivé prvky vektoru proměnných x.

1.4 Erastothenovo síto

Erastothenovo síto je základní a velmi jednoduchý algoritmus pro vygenerování všech prvočísel do dané meze. Postup je znám již od dob starověkého Řecka, jeho zformulování je připisováno Erastothenovi z Kyrény.

Algoritmus prochází množinu začínající jako interval přirozených čísel od 2 do horní meze. Každé číslo, které se ocitne na začátku seznamu je označeno za prvočíslo a poté jsou vyloučeny ("vysítovány") i jeho násobky. Seznam tak začíná dalším prvočíslem, s kterým se provede stejná operace. Po nalezení prvočísla většího než druhá odmocnina horní meze je jasné, že zbylá nevyloučená čísla jsou prvočísly.

Na následujícím příkladu vidíme průběh algoritmu pro mez 25.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	**3**	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	3	4	**5**	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

V prvním kroku jsme označili číslo dva jako prvočíslo a vyškrtli všechny jeho násobky. V následujících dvou krocích jsme totéž zopakovali pro čísla tři a pět, neboť číslo čtyři jsme již vyškrtli. Další na řadě by bylo číslo sedm, jenže to už je vyšší než odmocnina z nejvyššího čísla v množině, a proto v posledním kroku označíme všechna zbylá čísla za prvočísla.

1.5 Legendreovo síto

V případě Erastothenova síta bylo cílem získat množinu prvočísel, nicméně pouhá znalost počtu prvočísel na určitém rozsahu přirozených čísel, či v rámci nějaké jejich podmnožiny, je dostačující pro spoustu přínosných závěrů. Pokusme se vyčíslit počet prvočísel současně s během Erastothenova postupu.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

V prvním kroku jsme, při počítání od jedničky, vyloučili každé druhé číslo, neboli každé číslo dělitelné dvěma. Počtem tedy volně řečeno polovinu. V druhém kroku vyškrtáváme každé třetí číslo, tedy (pro tuto chvili) třetinu čísel. Jenže vidíme, že některá čísla jsme vyloučili dvakrát, konkrétně čísla dělitelná dvěma i třemi, tedy dělitelné šesti. I ve vyčíslování počtu vyškrtávaných čísel jsme tato čísla odečetli od původního počtu dvakrát. Pro vyrovnáni stačí jednoduše přičíst jedenkrát počet právě takových čísel - šestinu všech.

Při pokračování vyloučením násobku pěti, budeme potřebovat vyrovnat společné násobky s již vylučovanými čísly, konkrétně násobky deseti a patnácti. Tím však společné násobky (násobky třiceti) přičtem v rámci vyrovnání násobku dvou čísel dvakrát, proto opět odečtem počet čísel dělitelných třiceti.

Počet přirozených čísel menších než X dělitelných d můžeme vyjádřit za pomoci funkce spodní celá část, udávající nejvyšší celé číslo menší nebo rovno argumentu, jako $\lfloor \frac{X}{d} \rfloor$. Potom počet čísel, která nevyloučíme po sítování čísly $\{2, 3, 5\}$ odpovídá

$$\lfloor X \rfloor - \left\lfloor \frac{X}{2} \right\rfloor - \left\lfloor \frac{X}{3} \right\rfloor - \left\lfloor \frac{X}{5} \right\rfloor + \left\lfloor \frac{X}{6} \right\rfloor + \left\lfloor \frac{X}{10} \right\rfloor + \left\lfloor \frac{X}{15} \right\rfloor - \left\lfloor \frac{X}{30} \right\rfloor .$$

Princip, kdy pro vyčíslení velikosti sloučení množin sečtem velikost sčítaných množin a odečtem velikost jejich průniku, a to rekurzivně, se nazývá *princip inkluze a exkluze*. Přitom můžeme vidět, že odečítání nebo přičítání závisí pouze na paritě počtu nejvyšších množin, z jejichž průniku příspěvek počítáme. V našem případě je příslušnost k dané množině určena dělitelností a pro rozhodnutí mezi přičítáním a odečítáním je stěžejní počet prvočinitelů dělitele. Takovou vlastnost vyjadřuje Liouvillova funkce, pro bezčtvercová čísla shodná s Möbiovo funkcí.

Zavedmě si několik základních pojmů potřebných pro síta. V první řadě si označme množinu přirozených čísel, v kterém chceme vyčíslit počet (nebo častěji odhad počtu) jako A a pomocí A_d značme podmožinu A, jejichž prvky jsou dělitelné d ($A_d = \{a \in A | a \pmod d \equiv 0\}$). Dále označme P součin prvočísel, kterými chceme sítovat, alternativně budeme využívat součin všech prvočísel do meze $P(z) = \prod_{p \in \mathbb{P} | p \leq z} p$. Konečně označme velikost výsledné vysítované množiny $S(A, P) = |\{n \in A | \gcd(n, P) = 1\}|$.

Pokud zůstaneme u obecného vyjádření množin A_d, dostáváme základní síto vycházející

přímo z principu inkluze a exkluze, pojmenované po Adrien-Marie Legendreovi.

Věta 1 (Legendreovo síto): *Nechť A je sítovací množina, P součin prvočísel a A_d podmnožina A obsahující pouze prvky dělitelné d, potom*

$$S(A,P) = \sum_{d|P} \mu(d)\,|A_d|\,,$$

kde μ značí Möbiovu funkci.

Ujasněme si, že 1 dělí jakékoliv číslo, proto $d = 1$ je také jeden z dělitelů, přes které je prováděn součet s tím, že A_1 reprezentuje celou množinu, od které jsme při naší intuici odečítali.

Připomeňme, že Legendreovo síto v této formulaci nevyžaduje A jakožto souvislý interval, ale může ji být libovolná podmnožina přirozených čísel. Pro různé problémy můžeme začínat s různými množinami, například pouze čísla zapsatelná ve tvaru $n^2 + 1$ pro $n \in \mathbb{N}$ nebo spadající do konkrétní zbytkové třídy pro daný modul.

Pokud nás však zajímají pouze souvislé intervaly, můžeme se omezit dokonce pouze na čísla od jedné po horní mez, neboť pro hodnotu síta na intervalu nezačínajícího nulou můžeme od hodnoty pro horní mez odečíst hodnotu síta pro spodní mez. Pouze v případě odhadu zvolíme pro hodnotu pro spodní mez opačně maximální nebo minimální hodnotu.

Jak jsme již řekli výše, pro takovou situaci využijeme funkci spodní celá část. Hodnota Legendreova síta, při značení $S(X,P) = S(\{1,2,\ldots,X\},P)$, potom je

$$S(X,P) = \sum_{d|P} \mu(d) \left\lfloor \frac{X}{d} \right\rfloor .$$

Kdybychom chtěli znát počet prvočísel do hranice X, zvolili bychom $P = P(z)$ pro $z = \left\lfloor \sqrt{X} \right\rfloor$. Nutno podotknout, že z celkového počtu čísel by byla vysítována i prvočísla, kterými jsme sítovali. Proto

$$S\left(X, P\left(\left\lfloor \sqrt{X} \right\rfloor\right)\right) = \pi(X) - \pi\left(\left\lfloor \sqrt{X} \right\rfloor\right).$$

Nespojitá funkce spodní celá část je velkou komplikací při použití síta v této podobě, proto se pokusíme spodní celou část rozdělit podle vztahu

$$\forall a, d \in \mathbb{N} : \left\lfloor \frac{a}{d} \right\rfloor = \frac{a}{d} - \frac{a \pmod d}{d},$$

přičemž při označení zlomkové části, tedy jakéhosi zbytku po dělení jednou, jako $\{a\}$, kdy z definice $0 \leq \{a\} < 1$, píšeme

$$\forall a, d \in \mathbb{N} : \left\lfloor \frac{a}{d} \right\rfloor = \frac{a}{d} - \left\{ \frac{a}{d} \right\}.$$

Pro hodnotu síta pro přirozená čísla do meze dostáváme

$$\begin{aligned} S(X,P) &= \sum_{d|P} \mu(d) \left\lfloor \frac{X}{d} \right\rfloor = \sum_{d|P} \mu(d) \left(\frac{X}{d} - \left\{ \frac{X}{d} \right\} \right) \\ &= \sum_{d|P} \mu(d) \frac{X}{d} - \sum_{d|P} \mu(d) \left\{ \frac{X}{d} \right\} = X \sum_{d|P} \mu(d) \frac{1}{d} - \sum_{d|P} \mu(d) \left\{ \frac{X}{d} \right\}. \end{aligned}$$

Suma přes dělitele z převrácené hodnoty násobené Möbiovou funkcí by nám měla být povědomá ze vztahu pro Eulerovu funkci, díky kterému máme

$$\sum_{d|P} \frac{\mu(d)}{d} = \frac{\varphi(P)}{P}.$$

Síto se nám tak zjednodušuje na vůči X lineární člen a jakýsi chybový člen podle

$$S(X,P) = X \frac{\varphi(P)}{P} - \sum_{d|P} \mu(d) \left\{ \frac{X}{d} \right\} = \frac{\varphi(P)}{P} X - E(X,P),$$

přičemž onen chybový člen se skládá pouze ze součtu konečného počtu relativně malých hodnot, konkrétně nezáporných realných čísel menších než jedna. Avšak počet takových hodnot odpovídá počtu dělitelů P, rovného $2^{\omega(P)}$, kde $\omega(P)$ značí počet prvočinitelů P. Jelikož polovina z nich je odečítána a polovina přičítána, máme s použitím základního omezení $0 \leq \{a\} < 1$ dosti neuspokojivý odhad

$$-2^{\omega(P)-1} < E(X,P) < 2^{\omega(P)-1}.$$

Nutno podotknout, že $E(X,P)$ je vůči X periodické s periodou P, neboť pro všechna čísla ze stejné zbytkové třídy modulo P mají shodné zbytky i pro všechny dělitele P. Pro každý dělitel d máme obecně d možností, jakých může sčítanec nabývat (0 až $\frac{d-1}{d}$), avšak mezi různými děliteli je vazba, neboť konkrétní zbytkové třídy modulo jednotlivá prvočísla z P jednoznačně určují i zbytky modulo složené dělitele, což podle Čínské věty o zbytcích odpovídá právě oněm P možnostem. Jak i numerické výpočty naznačují, existuje mnohem použitelnější $E_{max}(P)$ vyhovující

$$\max_{X\in\{0,1,\ldots,P-1\}} |E(X,P)| \leq E_{max}(P) < 2^{\omega(P)-1},$$

bohužel se zatím žádné takové vhodné $E_{max}(P)$ nepodařilo dokázat.

1.6 Selbergovo síto

Hodnotou síta $S(A,P)$ chceme obecně vyjádřit počet prvků A nesoudělných s P, což lze zapsat

$$S(A,P) = |\{n \in A | \gcd(n,P) = 1\}| = \sum_{n\in A} \delta_1^{\gcd(n,P)},$$

kde δ_b^a je Kroneckerovo delta rovnající se jedné právě tehdy, když $a = b$, jinak je rovna nule.

Pro posouzení rovnosti s jednou využijeme sumu přes dělitele, kdy

$$\delta_1^{\gcd(a,b)} = \sum_{d|\gcd(a,b)} \mu(d) = \sum_{d|a,b} \mu(d),$$

proto

$$S(A,P) = \sum_{n\in A} \sum_{d|n,P} \mu(d).$$

Základní trik v Selbergově sítu spočívá v nahrazení Möbiovy funkce obecně libovolnými čísly λ tak, aby platila nerovnost

$$\sum_{d|n,P} \mu(d) \leq \left(\sum_{d|n,P} \lambda_d \right)^2.$$

Pro případ $\gcd(n, P) > 1$ nabývá levá strana nulové hodnoty a díky kvadrátu pravé strany je jasné, že nerovnost je splněna. V případě $\gcd(n, P) = 1$ je levá strana rovna jedné, proto i pravá strana musí být větší nebo rovna jedné. Jelikož však jediným dělitelem $\gcd(n, P) = 1$ je 1, musí být příspěvek tvořen pouze λ_1^2, z čehož vyplývá skutečnost $\lambda_1 = 1$. To je jediná podmínka pro hodnoty λ_d, ostatní hodnoty můžeme prozatím považovat za libovolná reálná čísla.

V důsledku Selbergův postup vede k hornímu odhadu

$$S(A, P) = \sum_{n \in A} \sum_{d|n,P} \mu(d) \leq \sum_{n \in A} \left(\sum_{d|n,P} \lambda_d \right)^2 ,$$

kde čtverec sumy rozepíšeme po jednotlivých členech rozvoje, což můžeme chápat jako sumu součinu dvou λ přes všechny kombinace dělitelů d_1 a d_2 (včetně $d_1 = d_2$), proto

$$S(A, P) \leq \sum_{n \in A} \left(\sum_{d_1, d_2 | n, P} \lambda_{d_1} \lambda_{d_2} \right) ,$$

což ale můžeme psát také jako

$$S(A, P) \leq \sum_{d_1, d_2 | P} \lambda_{d_1} \lambda_{d_2} \sum_{\substack{n \in A \\ d_1, d_2 | n}} 1.$$

Vyjádřit hodnotu $S(X, P)$ součtem hlavního a zbytkového členu můžeme při použití $\left\lfloor \frac{X}{d} \right\rfloor = \frac{X}{d} + \left\{ \frac{X}{d} \right\} = \frac{X}{d} + O(1)$ pro počet čísel menších než X dělitelných d jako

$$S(X, P) = X \sum_{d_1, d_2 | P} \frac{\lambda_{d_1} \lambda_{d_2}}{\operatorname{lcm}(d_1, d_2)} + O\left(\sum_{d_1, d_2 | P} |\lambda_{d_1}| \, |\lambda_{d_2}| \right) .$$

Koeficienty λ_d jsou následně zpravidla odhadovány vhodně zvolenou multiplikativní funkcí a pro jejich součty je použita Möbiova iverze. Nicméně hlavní myšlenka Selbergova síta spočívá právě v součtu všech kombinací součinu koeficientů λ_d pro dva dělitele d (včetně stejných).

1.7 Distribuce prvočísel

Rozmístění prvočísel, a tím i průběh prvočíselné funkce $\pi(x)$, značící počet prvočísel menších nebo rovno x, je významnou otázkou již od dob Euklida, který ukázal, že jejich počet je nekonečný. První použitelnou aproximací byl vztah

$$\pi(x) \sim \frac{x}{\log x},$$

neboli

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1,$$

jak roku 1896 dokázali nezávisle na sobě Jacques Hadamard a Charles Jean de la Vallée Poussin.[6, p. 2]

De la Vallée Poussin v roce 1899 dokázal i domněnku vyslovenou Drichletem lépe přibližující počet prvočísel integrálem převrácené hodnoty logaritmu (li) podle vzorce

$$\pi(x) = \mathrm{Li}(x) + O\left(xe^{-a\sqrt{\log x}}\right),$$

kde

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t} dt = \mathrm{li}(x) - \mathrm{li}(2).$$

Nicméně pod pojmem *prvočíselná věta* se zpravidla rozumí první vztah, který je vzhledem ke své jednoduchosti hojné používán pro aproximaci počtu prvočísel na intervalu a stejně tomu tak je i v našem textu.

1.8 Distribuce prvočísel v aritmetické posloupnosti

Drichletova věta praví, že pro každou nesoudělnou dvojici (přirozených čísel) a a q existuje nekonečně mnoho prvočísel tvaru $a + nq$ ($n \in \mathbb{N}$), tedy každá aritmetická posloupnost nesoudělného základu a diference generuje nekonečně mnoho prvočísel. Jinak řečeno je nekonečně prvočísel kongruentních s a modulo q, pokud a a q jsou nesoudělné.

A dokonce pozdější výsledky ukázaly, že rozdělení mezi těmito zbytkovými třídami je v určitém slova smyslu rovnoměrné, neboli, označíme-li počet prvočísel menších nebo rovno x kongruentních s a modulo q jako $\pi(x; q, a)$, pak budeme uvažovat

$$\pi(x; q, a) \approx \frac{\pi(x)}{\varphi(q)}$$

pro a nesoudělné s q.

Kumulací maximální chyby přes prvočísla do dané hranice se dostáváme k důležitému pojmu *úroveň distribuce prvočísel*.

Definice 7 (Úroveň distribuce prvočísel v aritmetické posloupnosti): *Úrovní distribuce prvočísel θ nazýváme reálné kladné číslo splňující pro všechna $A > 0$:*

$$\sum_{q \leq x^{\theta}} \max_{\gcd(a,q)=1} \left| \pi(x;q,a) - \frac{\pi(x)}{\varphi(q)} \right| \ll_A \frac{x}{\log^A x}.$$[2]

Neboli zvažujeme mez pro prvočísla vztažené k hranici, do které počítáme počet prvočísel tak, aby součet přes tato prvočísla maximálních chyb nerostl rychleji než poměr x a logaritmu x umocněného na libovolné kladné A (pro $A = 1$ poměr aproximuje počet prvočísel, tedy obecně součet chyb neroste rychleji než počet prvočísel), zatímco konstanta potřebná pro zachování nerovnosti je zavislá pouze na A.

Přičemž Enrico Bombieri a Askold Ivanovich Vinogradov nezávisle na sobě ukázali[6, p. 6], že podmínce vyhovují všechna $\theta < \frac{1}{2}$.

Věta 2 (Bombieri–Vinogradova věta):

$$\forall A > 0 \quad \exists B > 0 : \quad \sum_{q \leq \frac{\sqrt{x}}{\log^B x}} \max_{\gcd(a,q)=1} \left| \pi(x;q,a) - \frac{\pi(x)}{\varphi(q)} \right| \ll_A \frac{x}{\log^A x}$$

Peter D. T. A. Elliott a Heini Halberstam vyslovili v roce 1968[6, p. 6] domněnku, že vlastnost úrovně distribuce splňují všechna $\theta < 1$. Tento předpoklad je poměrně silný, ale stále nedokázaný, v Maynardově případě pak získáváme slabší, nicméně bezpodmínečný výsledek a dva silnější závěry vyžadující platnost Elliott–Halberstamovi domněnky.

Domněnka 1 (Elliott–Halberstamova domněnka):

$$\forall \theta \in (0;1) \quad \forall A > 0 : \quad \sum_{q \leq x^{\theta}} \max_{\gcd(a,q)=1} \left| \pi(x;q,a) - \frac{\pi(x)}{\varphi(q)} \right| \ll_A \frac{x}{\log^A x}$$

[2] Nekdy se take misto $\pi(x;q,a) = \sum_{\substack{p \in \mathbb{P}, p \leq x \\ p \equiv a \pmod q}} 1$ pouziva $\Theta(x;q,a) = \sum_{\substack{p \in \mathbb{P}, p \leq x \\ p \equiv a \pmod q}} \log p$, pricemz chyba se v takovem pripade pocita od $\frac{x}{\varphi(x)}$, coz vychazi z prvočíselne vety.

1.9 Prvočíselné k-tice

Termínem prvočíselná k-tice označujeme (zpravidla opakující se) vzor v rozdílech prvočísel. Pokud připočteme jednotlivé prvky množiny k vhodnému n, získáváme pouze prvočísla. Je přirozeným zvykem zapisovat výčet v pořadí od nejnižšího čísla po nejvyšší, přičemž bez újmy na obecnosti (zvolili bychom jiné n) nejnižším prvkem je nula.

Definice 8 (Splnitelná množina): *Množinu nezáporných celých čísel* $\mathcal{H} = \{h_1, h_2, \ldots, h_k\}$ *nazýváme splnitelnou množinou, pokud*

$$\forall p \in \mathbb{P} \quad \exists a_p \in \mathbb{N} : \quad \forall h \in \mathcal{H} \quad a_p \not\equiv h \pmod{p}.$$

Volně řečeno pro žádné prvočíslo p nepokrývají prvky množiny všechny zbytkové třídy modulo p. V opačném případě by totiž alespoň jedno z čísel $n + h$ muselo být dělitelné prvočíslem a takový vzor by pak tvořil prvočísla maximálně pro jedno n, kdy dotčené $n+h$ je rovno právě onomu prvočíslu, pro které jsou pokryty všechny zbytkové třídy.

Je zřejmé, že pro prvočísla větší než je počet prvků v množině (tedy větší než k) nemůžeme pokrýt všechny zbytky a proto pro dané k získáváme konečný počet prvočísel, vůči kterým je potřeba dotyčnou vlastnost testovat.

Při zachování nulového prvního (nejmenšího) prvku je zřejmé, že všechna čísla v $\mathcal{H}$ musí být sudá, protože lichým číslem bychom vyčerpali obě zbytkové třídy po dělení dvěma.

Počet prvočísel vzniklých přičtením $\mathcal{H}$ k danému n označme $\chi_{\mathbb{P}}(n + \mathcal{H})$. [3]

Domněnka 2 (Domněnka o prvočíselných k-ticích): *Nechť* $\mathcal{H} = \{h_1, \ldots, h_k\}$ *je splnitelná množina velikosti* k*. Potom existuje nekonečně mnoho* n*, pro která platí* $\chi_{\mathbb{P}}(n + \mathcal{H}) = k$*.*

Domněnka nebyla dokázána obecně, ani pro žádné konkrétní k. [4] Známým specialním případem je splnitelná množina $\mathcal{H} = \{0, 2\}$ - hypotéza o prvočíselných dvojicích.

[3] Většinou se χ_A používá jako zobrazení na množinu $\{0, 1\}$, tedy ve smyslu argument patří nebo nepatří do množiny A, nikoliv ve smyslu kolik prvků z argumentu je prvkem A. Avšak toto naše stručné označení považuji za přehlednější než $\sum_{i=1}^{k} \chi_{\mathbb{P}}(n + h_i)$ a méně matoucí než některými autory užívané $\pi(n + \mathcal{H})$, protože $\pi(x)$ zpravidla značí celkový počet prvočísel od nuly (tedy $\sum_{i=1}^{x} \chi_{\mathbb{P}}(i)$).

[4] Výjimkou je samozřejmě triviální případ $k = 1$, tedy tvrzení, že prvočísel je nekonečně mnoho. (Euklidova věta)

Nicméně dále uvidíme, že převratným poznatkem je i zjištění, že pro nějaké $\mathcal{H}$ existuje nekonečně n takových, že $\chi_{\mathbb{P}}(n+\mathcal{H}) \geq 2$.

1.10 Metoda GPY

S metodou využívající splnitelné množiny přišli ve svém článku *Primes in tuples I.* Daniel Goldston, Janos Pintz, Cem Yıldırım.

Nechť $\mathcal{H}$ je splnitelná množina o k prvcích, $\rho > 0$, váhy $w_n \geq 0$ a $n \in \mathbb{N}$. Potom metoda GPY spočívá ve zkoumání sumy

$$S(N,\rho) = \sum_{N \leq n < 2N} (\chi_{\mathbb{P}}(n+\mathcal{H}) - \rho) w_n. \tag{3}$$

Pokud je hodnota $S(N,\rho)$ kladná, potom alespoň jeden člen musí mít kladný příspěvek, což vzhledem k nezápornosti vah znamená, že pro dané n počet prvočísel vzniklých přičtením $\mathcal{H}$ převyšuje ρ. V součtu tak na intervalu $[N;2N)$ musí být alespoň jedno n, pro které platí, že počet prvočísel z $n+\mathcal{H}$ je minimálně $\lfloor \rho + 1 \rfloor$. V důsledku, pokud je $S(N,\rho)$ kladné pro všechna velká N, je nekonečně mnoho přirozených čísel n takových, že po přičtení prvku $\mathcal{H}$ přinejmenším $\lfloor \rho + 1 \rfloor$ z nich jsou prvočísla.

Jelikož není požadována prvočíselnost pro všechny prvky $n+\mathcal{H}$ (ρ vybereme menší než k - počet prvků v množině $\mathcal{H}$), neumožní nám suma dokázat domněnku o prvočíselnych k-ticich ani pro konkrétní splnitelnou množinu, ale analýza sumy podá zajímavé závěry o počtu prvočísel na intervalech konečné délky.

Pomocí této metody trojice Goldston, Pintz a Yıldırım dokázala nulovou hodnotu limes inferior poměru prvočíselné mezery a logaritmu prvočísla, neboli

$$\liminf_n \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Tento výsledek částečně ztrácí na významu s důkazy existence konečné limes inferior samotné prvočíselné mezery, přesto byl v době svého předložení značným průlomem.

V metodě byly dělitelé omezeny podle $R = N^{\frac{\theta}{2}}$ a váhy byly založeny na Selbergově

sítu, konkretně podle

$$w_n = \left(\sum_{\substack{d \mid \prod_{i=1}^{k}(n+h_i) \\ d<R}} \lambda_d \right)^2,$$

kde

$$\lambda_d = \mu(d) F\left(\log\left(\frac{R}{d} \right) \right).$$

Jako vhodnou hladkou funkci skupina zvolila polynom

$$F(x) = x^{k+l}, \quad l \in \mathbb{N}.$$

Dále při předpokladu úrovně distribuce prvočísel $\theta > \frac{1}{2}$ ukázali existenci konečné limes inferior rozdílu dvou po sobě jdoucích prvočísel s tím, že konstanta je závislá na úrovni distribuce θ.

$$\liminf_n (p_{n+1} - p_n) \leq c(\theta)$$

S předpokladem platnosti Elliott–Halberstamovy domněnky, tedy že za úroveň distribuce můžeme vzít jakékoliv $\theta < 1$ (potřebná úroveň je $\theta > \frac{20}{21}$[10, p. 7]), dokázali také tvrzení

$$\liminf_n (p_{n+1} - p_n) \leq 16.$$

Jinými slovy existuje nekonečně mnoho dvojic prvočísel, která se liší maximalně o 16.

Pozdější průlom přišel od Yitanga Zhanga, když bez předpokladu Elliott–Halberstamovy domněnky dokázal

$$\liminf_n (p_{n+1} - p_n) \leq 7 \cdot 10^7,$$

čímž podal první nepodmíněný důkaz existence maxima nekonečněkrát se vyskytující prvočíselné mezery.

2 Maynardův pokrok

Hlavní část této práce tvoří analýza postupu Jamese Maynarda, který použil ve svém článku *Small gaps between primes* k důkazu nových poznatků, jež si probereme v první podkapitole. V druhé podkapitole projdeme důkazy jednotlivých závěrů za pomoci vyjádření síta odvozeného v podkapitole třetí a čtvrté. V posledních dvou podkapitolách se budeme věnovat vhodným funkcím pro váhy.

2.1 Výsledky Maynardovi práce

James Maynard ve svém článku z roku 2014 Small gaps between primes dochází k pěti významným závěrům:

Věta 3: *Nechť $m \in \mathbb{N}$, potom*

$$\liminf_n (p_{n+m} - p_n) \ll m^3 e^{4m}.$$

Věta 4: *Nechť $m \in \mathbb{N}$, dále $\mathcal{A} = \{a_1, \ldots, a_r\}$, kde $a_i \in \mathbb{N}$ a $r \in \mathbb{N}$ je dostatečně velké v závislosti na m, potom*

$$\frac{|\mathcal{H} = \{h_1, \ldots, h_m\} \subseteq \mathcal{A} : \text{ pro nekonečně mnoho } n\ \chi_{\mathcal{P}}(n + \mathcal{H}) = m|}{|\{h_1, \ldots, h_m\} \subseteq \mathcal{A}|} \gg_m 1.$$

Věta 5: *Nepodmíněně platí*

$$\liminf_n (p_{n+1} - p_n) \leq 600.$$

Tento výsledek omezující limis inferior dvou po sobě jdoucích prvočísel je nejsilnějším z posledních tří a na rozdíl od následujících nepředpokládá žádné nedokázané skutečnosti.

Konečnost limes inferior dvou po sobě jdoucích prvočísel dokázal ve své práci již Yitang Zhang, nicméně posun od hranice 70 000 000 k hodnotě 600 nelze neoznačit za signifikantní. Závěr lze vyložit ve smyslu, že existuje nekonečně mnoho prvočíselných mezer (rozdílu dvou po sobě jdoucích prvočísel) velikosti menší nebo rovno 600.

Věta 6: *Předpokládejme, že prvočísla mají úroveň distribuce θ pro všechna $\theta < 1$ (Elliott–Halberstamova domněnka), potom*

$$\liminf_n (p_{n+2} - p_n) \leq 600.$$

$$\liminf_n (p_{n+1} - p_n) \leq 12,$$

S předpokladem platnosti Elliott–Halberstamovy domněnky tak získáváme výrazné zlepšení krajní hodnoty liminf dvou po sobě jdoucích prvočísel a původní hodnotu ze závěru bez platnosti podmínky získaváme jako maximum liminf rozdílu obnásledujících prvočísel.

2.2 Důkazy výsledku

Inovace výše uvedené metody GPY spočívá v použití obecně specifických koeficientu λ pro každou kombinaci dělitelů jednotlivých prvků $n + \mathcal{H}$. V názvosloví Selbergova síta bychom mohli psát

$$w_n = \left(\sum_{\forall i \ d_i | n+h_i} \lambda_{d_1,\ldots,d_k} \right)^2 .$$

Umocněním sumy na druhou získáváme jistotu nezápornosti celkové váhy w_n. Samotné koeficienty $\lambda_{d_1,\ldots,d_k}$ pak zvolíme tak, abychom je s přijatelnou chybou mohli nahradit pomocí hladké funkce podle

$$\lambda_{d_1,\ldots,d_k} \approx \left(\prod_{i=1}^{k} \mu(d_i) \right) f(d_1, \ldots, d_k).$$

Abychom později v hledání optimální hladké funkce mohli uvažovat $n \approx \varphi(n) \approx g(n)$[5], potřebovali bychom vyloučit čísla obsahující v nějaké míře malá prvočísla, proto sítovací množinu omezíme na jedinou zbytkovou třídu (v_0) modulo součin relativně malých prvočísel (W), a to všech až po určitou mez (D_0). Přesná hranice není vzhledem k řádu W a N podstatná, použitá je řádově hodnota

$$D_0 = \log\log\log N,$$
$$W = \prod_{p \leq D_0} p,$$
$$W \ll (\log\log N)^2 .$$

[5]Zcela multiplikativní funkce $g(p) = p - 2$ bude definována později.

Ze splnitelnosti množiny $\mathcal{H}$ vyplýva, že pro všechna prvočísla, a tím pádem i pro prvočísla zahrnutá ve W, existuje zbytková třída modulo W, v které žadný z prvku $\mathcal{H}$ neleží. Čínská věta o zbytcích nám tak umožňuje vybrat v_0 jako zbytkovou třídu modulo W tak, aby pro všechna $h \in \mathcal{H}$ platilo $\gcd(v_0 + h, W) = 1$. Sumu pak omezujeme podmínkou $n \equiv v_0 \pmod W$.

Základní hodnotu GPY síta (3) rozdělme na dvě sumy:

$$S = S_2 - \rho S_1,$$

$$S_1 = \sum_{\substack{N \le n < 2N \\ n \equiv v_0 \pmod W}} \left(\sum_{\forall i \; d_i \mid n + h_i} \lambda_{d_1,\ldots,d_k} \right)^2, \tag{4}$$

$$S_2 = \sum_{\substack{N \le n < 2N \\ n \equiv v_0 \pmod W}} \chi_{\mathbb{P}}(n + \mathcal{H}) \left(\sum_{\forall i \; d_i \mid n + h_i} \lambda_{d_1,\ldots,d_k} \right)^2. \tag{5}$$

Nahrazení koeficientu $\lambda_{d_1,\ldots,d_k}$ integrovatelnou hladkou funkci je kritickým trikem ve vyhodnocení síta. Sumy vyjádříme pomocí následujícího tvrzení, jehož odvození si, jakožto nejkomplikovanější část práce, vyčleníme do dvou samostatných kapitol.

Tvrzení 1: *Nechť $\theta > 0$ je úroveň distribuce prvočísel a $R = N^{\frac{\theta}{2} - \delta}$ pro určité malé $\delta > 0$. Dále nechť $F : \mathbb{R}^k \mapsto \mathbb{R}$ je vhodná hladká funkce nulová mimo $\mathcal{R}_k = \{(x_1, \ldots, x_k) \in [0,1]^k : \sum_{i=1}^k x_i \le 1\}$. Definujme koeficienty $\lambda_{d_1,\ldots,d_k}$ jako nulové, pokud $\gcd(\prod_{i=1}^k d_i; W) \ne 1$ a v opačném případě*

$$\lambda_{d_1,\ldots,d_k} = \left(\prod_{i=1}^k \mu(d_i) d_i \right) \sum_{\substack{r_1,\ldots,r_k \\ \forall i \; d_i \mid r_i \\ \forall i \; gcd(r_i, W) = 1}} \frac{\mu(\prod_{i=1}^k r_i)^2}{\prod_{i=1}^k \varphi(r_i)} F\left(\frac{\log r_1}{\log R}, \ldots, \frac{\log r_k}{\log R} \right).$$

Potom získaváme

$$S_1 = \frac{(1 + o(1)) \; \varphi(W)^k \; N \; (\log R)^k}{W^{k+1}} \; I_k(F),$$

$$S_2 = \frac{(1 + o(1)) \; \varphi(W)^k \; N \; (\log R)^{k+1}}{W^{k+1} \log N} \; \sum_{m=1}^k J_k^{(m)}(F),$$

kde

$$I_k(F) = \int_0^1 \cdots \int_0^1 F(t_1, \ldots, t_k)^2 \, dt_1 \cdots dt_k \neq 0,$$
$$J_k^{(m)}(F) = \int_0^1 \cdots \int_0^1 \left(\int_0^1 F(t_1, \ldots, t_k) \right)^2 \, dt_1 \cdots dt_{m-1} dt_{m+1} \cdots dt_k \neq 0.$$

Dostatečné velký poměr S_2 a S_1 vede k žádaným výsledkům ohledně počtu prvočísel v množině $n + \mathcal{H}$.

Tvrzení 2: *Mějme stejné předpoklady a vyjádření jako v předchozím tvrzení. Dále označme $\mathcal{S}_k$ množinu všech Riemannovsky integrovatelných funkcí $F : [0,1]^k \mapsto \mathbb{R}$ [6] nulových mimo $\mathcal{R}_k = \{(x_1, \ldots, x_k) \in [0,1]^k : \sum_{i=1}^k x_i \leq 1\}$. Nechť*

$$M_k = \sup_{F \in \mathcal{S}_k} \frac{\sum_{m=1}^k J_k^{(m)}(F)}{I_k(F)},$$
$$r_k = \left\lceil \frac{\theta M_k}{2} \right\rceil.$$

Potom existuje nekonečně mnoho přirozených čísel n takových, že z $n + \mathcal{H}$ je alespoň r_k prvočísel.

Důkaz: Položíme $R = N^{\frac{\theta}{2} - \delta}$ pro dostatečně malé $\delta > 0$. Vybereme $F_0 \in \mathcal{S}_k$ tak, že $\sum_{m=1}^k J_k^{(m)}(F_0) > (M_k - \delta) I_k(F_0) > 0$ (přičemž jistě taková F_0 existuje z definice M_k). Jelikož F_0 je Riemannovsky integrovatelná, potom bude existovat hladká funkce F_1, jejichž integrály $J_k^{(m)}$ a I_k se budou od původních lišit jen o libovolné málo, a tím i rozdíl $J_k^{(m)}(F_1)$ a $I_k(F_1)$, proto zvolíme F_1 tak, že můžeme psát $\sum_{m=1}^k J_k^{(m)}(F_1) > (M_k - 2\delta) I_k(F_1) > 0$. Potom

$$\begin{aligned} S = S_2 - \rho S_1 &= \frac{(1 + o(1))\, \varphi(W)^k \; N \; \log^k R}{W^{k+1}} \left(\frac{\log R}{\log N} \sum_{m=1}^k J_k^{(m)}(F_1) \; - \; \rho I_k(F_1) \right) \\ &= \frac{\varphi(W)^k \; N \; \log^k R}{W^{k+1}} \left(\frac{\log R}{\log N} \sum_{m=1}^k J_k^{(m)}(F_1) \; - \; \rho I_k(F_1) + o(1) \right) \\ &\geq \frac{\varphi(W)^k \; N \; \log^k R}{W^{k+1}} I_k(F_1) \left(\left(\frac{\theta}{2} - \delta \right) (M_k - 2\delta) + o(1) \right). \end{aligned}$$

[6] V předchozím tvrzení jsme definovali F jako funkci z $\mathbb{R}^k$, nicméně jelikož hledáme maximum z určitého integrálu přes omezenou oblast (zahrnující celý rozsah, kde je původní funkce nenulová), můžeme množinu funkcí omezit doménou zahrnující pouze oblast integrace.

Přičemž jistě $W > 0$, $\varphi(W) > 0$, $N > 0$, $\log(R) > 0$ ($R > 1$) a $I_k(F_1) > 0$ (určitý integrál). Tudíž

$$\frac{\varphi(W)^k \; N \; \log^k R}{W^{k+1}} I_k(F_1) > 0,$$
$$\left(\frac{\theta}{2} - \delta\right)(M_k - 2\delta) - \rho = \frac{\theta M_k}{2} - \delta\theta - \delta M_k + 2\delta^2 - \rho > 0 \implies S > 0.$$

Položme $\rho = \frac{\theta M_k}{2} - \epsilon$ s nějakým vhodným $\epsilon > 0$.

$$\frac{\theta M_k}{2} - \delta\theta - \delta M_k + 2\delta^2 - \frac{\theta M_k}{2} + \epsilon > 0 \implies S > 0$$
$$\epsilon > \delta(\theta + M_k - 2\delta) \implies S > 0$$

Ve výsledku nám postačuje zvolit δ v závislosti na ϵ.

Z principu GPY síta získáváme závěr, že z množiny $n + \mathcal{H}$ je alespoň $\lfloor \rho + 1 \rfloor$ prvočísel. Přitom z definice ρ při malém ϵ máme $= \lfloor \rho + 1 \rfloor = \left\lceil \frac{\theta M_k}{2} \right\rceil = r_k$ a tím docházíme k výsledku Tvrzení 2.

Důsledek 1:

$$\liminf_n (p_{n+r_k-1} - p_n) \leq \max_{1 \leq i,j \leq k} (h_i - h_j)$$

Pro využití předchozího k vyvození konkrétních hranic limes inferior při dané úrovni distribuce prvočísel bychom potřebovali spodní odhady M_k. Pro dokončení důkazu předpokladejme následující odhady, které si dokážeme později.

Tvrzení 3: *Předpokládejme vše jako v Tvrzení 2. Potom máme*

1. $M_5 > 2$,
2. $M_{105} > 4$,
3. *a* $M_k > \log k - 2\log(\log k) - 2$, *pokud je* k *dostatečně velké.*

Začneme nejzásadnějším výsledkem, tedy že liminf dvou po sobě jdoucích prvočísel je menší než 600 s dokázanou úrovní distribuce (Věta 5).

Důkaz Věty 5

Vezměme splnitelnou množinu o 105 prvcích. Díky Bombieri–Vinogradovove větě víme, že $\forall \epsilon > 0 : \ \theta = \frac{1}{2} - \epsilon$ (jinak řečeno $\theta \leq 0$) a z posledního tvrzení máme $M_{105} = 4 + \alpha$ pro nějaké $\alpha > 0$. Vyjádříme hodnotu r_k z Tvrzení 2 a dosadíme do Důsledku 1:

$$r_k = \left\lceil \frac{\theta M_k}{2} \right\rceil = \left\lceil \frac{(\frac{1}{2} - \epsilon)(4 + \alpha)}{2} \right\rceil = 1 + \left\lceil \frac{\alpha}{4} - \frac{\epsilon\alpha}{2} - 2\epsilon \right\rceil,$$

$$\epsilon < \frac{\alpha}{2\alpha - 8} \implies r_k \geq 2,$$

$$\liminf_n (p_{n+1} - p_n) \leq \max_{1 \leq i,j \leq 105} (h_i - h_j).$$

Thomas Engelsma nalezl [1] splnitelnou množinu [7] o 105 prvcích, kde největším prvkem je číslo 600 (a nejnižším samozřejmě 0). Tím získáváme Větu 5.

Dukaz Věty 6

Nyní předpokládejme platnost Elliott–Halberstamovy domněnky, neboli $\forall \epsilon > 0 : \ \theta = 1 - \epsilon$. Potom pro stejnou splnitelnou množinu $\mathcal{H}$ dostáváme první část Věty 6:

$$r_k = \left\lceil \frac{\theta M_k}{2} \right\rceil = \left\lceil \frac{(1 - \epsilon)(4 + \alpha)}{2} \right\rceil = 2 + \left\lceil \frac{\alpha}{2} - \frac{\epsilon\alpha}{2} - 2\epsilon \right\rceil,$$

$$\epsilon < \frac{\alpha}{\alpha - 4} \implies r_k \geq 3,$$

$$\liminf_n (p_{n+2} - p_n) \leq \max_{1 \leq i,j \leq 105} (h_i - h_j) = 600.$$

Pro druhou část Věty 6 vezmeme pětiprvkovou množinu $\mathcal{H} = \{0, 2, 6, 8, 12\}$ a nadále předpokládejme Elliott–Halberstamovu domněnku. Pro $k = 5$ máme z tvrzení 3 $M_5 = 2 + \alpha$,

[7] $\mathcal{H} = \{0,\ 10,\ 12,\ 24,\ 28,\ 30,\ 34,\ 42,\ 48,\ 52,\ 54,\ 64,\ 70,\ 72,\ 78,\ 82,\ 90,\ 94,\ 100,\ 112,\ 114,\ 118,\ 120,\ 124,\ 132,\ 138,\ 148,\ 154,\ 168,\ 174,\ 178,\ 180,\ 184,\ 190,\ 192,\ 202,\ 204,\ 208,\ 220,\ 222,\ 232,\ 234,\ 250,\ 252,\ 258,\ 262,\ 264,\ 268,\ 280,\ 288,\ 294,\ 300,\ 310,\ 322,\ 324,\ 328,\ 330,\ 334,\ 342,\ 352,\ 358,\ 360,\ 364,\ 372,\ 378,\ 384,\ 390,\ 394,\ 400,\ 402,\ 408,\ 412,\ 418,\ 420,\ 430,\ 432,\ 442,\ 444,\ 450,\ 454,\ 462,\ 468,\ 472,\ 478,\ 484,\ 490,\ 492,\ 498,\ 504,\ 510,\ 528,\ 532,\ 534,\ 538,\ 544,\ 558,\ 562,\ 570,\ 574,\ 580,\ 582,\ 588,\ 594,\ 598,\ 600\}$[8]

kde $\alpha > 0$. Když opět vyjádříme nerovnici z Důsledku 1 získáváme požadovaný závěr:

$$r_k = \left\lceil \frac{\theta M_k}{2} \right\rceil = \left\lceil \frac{(1-\epsilon)(2+\alpha)}{2} \right\rceil = 1 + \left\lceil \frac{\alpha}{2} - \frac{\epsilon\alpha}{2} - \epsilon \right\rceil,$$
$$\epsilon < \frac{\alpha}{\alpha - 2} \implies r_k \geq 2,$$
$$\liminf_n (p_{n+1} - p_n) \leq \max_{1 \leq i,j \leq 5} (h_i - h_j) = 12.$$

Dukaz Věty 3

Zbývají nám první dva Maynardovy závěry s libovolně velkými k a bez předpokladu Elliott–Halberstamovy domněnky, máme proto $\forall \epsilon > 0 : \ \theta = \frac{1}{2} - \epsilon$ z Bombier-Vinogradovovy věty, ve výrazu r_k tak získáme

$$r_k = \left\lceil \frac{\theta M_k}{2} \right\rceil = \left\lceil \frac{(\frac{1}{2} - \epsilon) M_k}{2} \right\rceil \geq \left(\frac{1}{4} - \frac{\epsilon}{2} \right) (\log k - 2 \log\log k - 2).$$

A hledáme, kdy je větší než dané m. Položme $\epsilon = \frac{1}{k}$, díky čemuž můžeme zcela zanedbat člen způsobený $-\frac{\epsilon}{2}$, neboť $\frac{\log k}{k}$ konverguje k nule (stejně jako $\frac{\log\log k}{k}$). Získáme

$$\log k > 4m + 2 \log\log k + 2,$$
$$e^{\log k} > e^{4m + 2\log\log k + 2},$$
$$k > e^2 e^{4m} e^{2 \log\log k},$$

z čehož je jasné, že hledané k bude obsahovat $e^2 e^{4m}$, označme si proto k' zbytek k podle

$$k' := \frac{k}{e^{4m} e^2},$$
$$k = k' e^{4m+2}.$$

Potom dostáváme

$$k' > e^{2 \log\log(k' e^{4m+2})},$$
$$k' > e^{2 \log\left(\log(k') + \log(e^{4m+2})\right)},$$
$$k' > e^{2 \log(\log(k') + 4m + 2)},$$
$$k' > e^{\log((\log(k') + 4m + 2)^2)},$$
$$k' > (\log(k') + 4m + 2)^2.$$

Protože jsou obě strany kladné

$$\sqrt{k'} > \log(k') + 4m + 2,$$

v čemž můžeme z asymptotického růstu odhadnout tvar k' na $C'm^2$ pro nějakou konstantu C'. Ověříme dosazením, kdy

$$\sqrt{C'}m > \log C' + 2\log m + 4m + 2,$$
$$\frac{\sqrt{C'}-4}{2}m > \log m + \log\sqrt{C'} + 1,$$

což očividně platí pro dostatečně velké k a vhodnou konstatnu C'. Proto můžeme řici, že nerovnost platí pro

$$k = k'e^{4m+2} > C'm^2e^{4m}e^2 = Cm^2e^{4m}.$$

V důsledku to znamená, že pro libovolnou splnitelnou množinu $\mathcal{H} = \{h_1, \ldots, h_k\}$ o $k \geq Cm^2e^{4m}$ prvcích (s předpokladem dostatečně velkého k), alespoň $m+1$ z $n + h_i$ musí být prvočísly pro nekonečně mnoho n.

Zvolme množinu prvních k prvočísel větších než k $\mathcal{H} = \{p_{\pi(k)+1}, \ldots, p_{\pi(k)+k}\}$ (nebo normovanou na $\mathcal{H} = \{0, p_{\pi(k)+2} - p_{\pi(k)+1}, \ldots, p_{\pi(k)+k} - p_{\pi(k)+1}\}$). Ta je bezpochyby splnitelná, neboť žádný prvek není násobkem prvočísla menšího než k a zároveň k prvku nemůže pokrýt všechny zbytkové třídy modulo prvočíslo větší než k.

Podle Prvočíselné věty je rozdíl mezi nejmenším a největším prvkem množiny $p_{\pi(k)+k} - p_{\pi(k)+1} \ll k\log k$. Tudíž po dosazení do Důsledku 1 dostáváme při zvolení nejmenšího možného $k = \lceil Cm^2e^{4m} \rceil$ asymptoticky odhad

$$\liminf_n (p_{n+m} - p_n) \ll k\log k \ll m^3e^4m.$$

Důkaz Věty 4

Na základě daného m zvolíme nejmenší k, pro které bude platit $\frac{\theta M_k}{2} > m$, tedy podle předchozího $k = \lceil Cm^2e^{4m} \rceil$.

Zadaná množina $\mathcal{A}$ nemusí být splnitelná, proto označme $\mathcal{A}_2$ množinu vycházející z $\mathcal{A}$, kdy pro každé prvočíslo $p \leq k$, odstraníme všechny členy, které odpovídají jedné konkretní zbytkové třídě modulo p. Abychom odstranili co nejméně členů $\mathcal{A}$, vybereme takovou zbytkovou třídu, do které spadá nejméně prvků $\mathcal{A}$. Jakákoliv podmnožina $\mathcal{A}_2$ velikosti k je potom nutně splnitelná, neboť pro žádné $p \leq k$ nepokrývá všechny zbytkové třídy a pro prvočísla větší než k také určitě nemůže vzhledem k své velikosti. Pro velikost množiny $\mathcal{A}_2$, kterou označíme s, známe

$$s = |\mathcal{A}_2| \geq r \prod_{p \leq k} \left(1 - \frac{1}{p}\right) \gg_m r.$$

Předpokládejme $s > k$, neboť r je zvoleno dostatečně velké vůči r. Počet množin $\mathcal{H} \subseteq \mathcal{A}_2$ velikosti k je $\binom{s}{k}$. Podle Věty 3 pro takovou splnitelnou množinu o $k = \lceil Cm^2 e^{4m} \rceil$ prvcích platí, že pro nekonečně mnoho n je alespoň m z $n + \mathcal{H}$ prvočísel. Proto musí existovat alespoň jedna podmnožina $\{h'_1, \ldots, h'_m\} \subseteq \mathcal{H}$ velikosti m, pro kterou pro všechny prvky existuje nekonečně mnoho n, pro které $n + h'$ tvoří prvočíslo, neboť nekonečný příspěvek nemůže být zaručen součtem z konečného počtu konečných příspěvků.

Stejná splnitelná množina $\{h'_1, \ldots, h'_m\} \subseteq \mathcal{H}$ velikosti m je obsazena v počtu $\binom{s-m}{k-m}$ ze všech množin $\mathcal{H}$ velikosti k. Proto hledaný počet množin, kde všechny prvky tvoří prvočísla pro nekonečné mnoho n, je

$$\frac{\binom{s}{k}}{\binom{s-m}{k-m}} \gg_m s^m \gg_m r^m.$$

Celkový počet podmnožin $\mathcal{A}$ velikosti m odpovídá $\binom{r}{m} \leq r^m$, čímž získáváme závěr o poměru počtu množin.

2.3 Odvození síta

Prozatím jsme využili vyjádření síta z Tvrzení 1, které jsme ponechali bez odůvodnění. Nyní si hodnoty S_1 a S_2 odvodíme.

Omezme nenulové hodnoty $\lambda_{d_1,\ldots,d_k}$ podmínkou součinu dělitelů pro všechna i menším než hranice daná úrovní distribuce prvočísel ($d = \prod_{i=1}^{k} d_i < R = N^{\frac{\theta}{2}-\delta}$), dale na nesoudělnost součinu s malými prvočísly ($\gcd(d, W) = 1$) a na jeho bezčtvercovost ($\mu(d)^2 =$

1), z které vyplývá, že dělitelé pro různé i nezahrnují stejná prvočísla ($\forall i \neq j :\ \gcd(d_i, d_j) = 1$).

Lemma 1: *Nechť*

$$y_{r_1,\dots,r_k} = \left(\prod_{i=1}^{k} \mu(r_i)\varphi(r_i)\right) \sum_{\substack{d_1,\dots,d_k \\ \forall i\ r_i|d_i}} \frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k} d_i}$$

a $y_{max} = \sup_{r_1,\dots,r_k} |y_{r_1,\dots,r_k}|$. *Potom*

$$S_1 = \frac{N}{W} \sum_{r_1,\dots,r_k} \frac{y_{r_1,\dots,r_k}^2}{\prod_{i=1}^{k} \varphi(r_i)} + O\left(\frac{y_{max}^2\, \varphi(W)^k\, N\, \log^k(R)}{W^{k+1} D_0}\right)$$

Důkaz: Stejně jako v klasickém Selbergově postupu rozepíšeme v (4) umocnění celé sumy na sumu součinu a prohodíme pořadí sumace (viz 1.6).

$$S_1 = \sum_{\substack{N\le n<2N \\ n\equiv v_0 \pmod W}} \left(\sum_{\forall i\ d_i|n+h_i} \lambda_{d_1,\dots,d_k}\right)^2 = \sum_{\substack{N\le n<2N \\ n\equiv v_0 \pmod W}} \left(\sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}\right)$$

$$= \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \left(\sum_{\substack{N\le n<2N \\ n\equiv v_0 \pmod W \\ \forall i\ \operatorname{lcm}(d_i,e_i)|n+h_i}} 1\right)$$

Pro vnitřní sumu mohou nastat dva případy.

Buď jsou čísla W a $\operatorname{lcm}(d_i, e_i)$ pro všechna i po dvou nesoudělná, v tom případě můžeme vnitřní sumu vidět jako počet čísel mezi N a $2N$, která nabývají jedné zbytkové třídy modulo součin $W\prod_{i=1}^{k} \operatorname{lcm}(d_i, e_i)$. Jak již víme z dřívějška, takový počet se od podílu délky intervalu a modulu může lišit o -1 az $+1$, tedy o $O(1)$.

V opačném případě vyžadujeme nulový příspěvek. V případě soudělnosti s W je zajištěna nulová hodnota koeficientu λ ($\gcd(d, W) = 1$), stejně tak v případě soudělnosti dělitelů pro různá i v rámci jedné proměnné λ ($\mu(d)^2 = 1$). Zbývá nám pouze soudělnost dělitelů pro různé i mezi proměnnými λ ($\gcd(d_i, e_j) = 1\ i \neq j$). Stojí za připomenutí, že podmínka nesoudělnosti $\operatorname{lcm}(d_i, e_j)$ neimplikuje nesoudělnost mezi děliteli pro stejné i ($\gcd(d_i, e_i) \geq 1$).

Označme na chvíli $\sum'$ součet pouze přes takové $d_1, \ldots, d_k$ a $e_1, \ldots, e_k$, pro které platí $\operatorname{lcm}(d_i, e_j) = 1$ $i \neq j$. Potom

$$\begin{aligned} S_1 &= \sum_{\substack{d_1,\ldots,d_k \\ e_1,\ldots,e_k}}{}' \lambda_{d_1,\ldots,d_k}\lambda_{e_1,\ldots,e_k} \left(\frac{2N - N}{W \prod_{i=1}^{k} \operatorname{lcm}(d_i, e_i)} + O(1) \right) \\ &= \frac{N}{W} \sum_{\substack{d_1,\ldots,d_k \\ e_1,\ldots,e_k}}{}' \frac{\lambda_{d_1,\ldots,d_k}\lambda_{e_1,\ldots,e_k}}{\prod_{i=1}^{k} \operatorname{lcm}(d_i, e_i)} + O\left(\sum_{\substack{d_1,\ldots,d_k \\ e_1,\ldots,e_k}}{}' |\lambda_{d_1,\ldots,d_k}\lambda_{e_1,\ldots,e_k}| \right). \end{aligned} \tag{6}$$

Rádi bychom uvolnili vazbu mezi d a e, nacož využijeme vzorec pro součet hodnot Eulerovy funkce dělitelů, kdy

$$\begin{aligned} n &= \sum_{u|n} \varphi(u), \\ gcd(a, b) &= \sum_{d|a,b} \varphi(d), \\ \operatorname{lcm}(a, b) &= \frac{ab}{\gcd(a, b)}, \\ \frac{1}{\operatorname{lcm}(d_i, e_i)} &= \frac{1}{d_i e_i} \sum_{u_i|d_i,e_i} \varphi(u_i). \end{aligned}$$

Jako hlavní člen pak získáváme

$$\frac{N}{W} \sum_{\substack{d_1,\ldots,d_k \\ e_1,\ldots,e_k}}{}' \prod_{i=1}^{k} \left(\sum_{u_i|d_i,e_i} \varphi(u_i) \right) \frac{\lambda_{d_1,\ldots,d_k}\lambda_{e_1,\ldots,e_k}}{\prod_{i=1}^{k} d_i e_i}.$$

Kde můžeme konkrétní u vytknout a prohodit tak pořadí sumace (ve výsledku sčítáme všechny původní kombinace $d_1, \ldots, d_k$ a $e_1, \ldots, e_k$, jen seskupené po dělitelnosti u).

$$\frac{N}{W} \sum_{u_1,\ldots,u_k} \left(\prod_{i=1}^{k} \varphi(u_i) \right) \sum_{\substack{d_1,\ldots,d_k \\ e_1,\ldots,e_k \\ \forall i\ u_i|d_i,e_i}}{}' \frac{\lambda_{d_1,\ldots,d_k}\lambda_{e_1,\ldots,e_k}}{\left(\prod_{i=1}^{k} d_i \right) \left(\prod_{i=1}^{k} e_i \right)}$$

V této formě vyřešíme podmínku pro nesoudělnost d_i a e_j vynásobením součtu hodnot Möbiovy funkce dělitelů, který je roven jedné právě tehdy, když dělenec je 1, a nule v ostatních případech (viz (1)) a použijeme obdobný trik pro přehození pořadí sumy:

$$\frac{N}{W}\sum_{u_1,\dots,u_k}\left(\prod_{i=1}^{k}\varphi(u_i)\right)\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ \forall i\ u_i|d_i,e_i}}\left(\sum_{\forall i\neq j\ s_{i,j}|d_i,e_j}\mu(s_{i,j})\right)\frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\left(\prod_{i=1}^{k}d_i\right)\left(\prod_{i=1}^{k}e_i\right)}$$

$$=\frac{N}{W}\sum_{u_1,\dots,u_k}\left(\prod_{i=1}^{k}\varphi(u_i)\right)\sum_{s_{1,2}\,,\dots,\,s_{k,k-1}}\left(\prod_{\substack{1\le i,j\le k\\ i\neq j}}\mu(s_{i,j})\right)\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ \forall i\ u_i|d_i,e_i\\ \forall i\neq j\ s_{i,j}|d_i,e_j}}\frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\left(\prod_{i=1}^{k}d_i\right)\left(\prod_{i=1}^{k}e_i\right)}$$

$$=\frac{N}{W}\sum_{u_1,\dots,u_k}\left(\prod_{i=1}^{k}\varphi(u_i)\right)\sum_{s_{1,2}\,,\dots,\,s_{k,k-1}}\left(\prod_{\substack{1\le i,j\le k\\ i\neq j}}\mu(s_{i,j})\right)\sum_{\substack{d_1,\dots,d_k\\ \forall i\ u_i|d_i\\ \forall i\neq j\ s_{i,j}|d_i?}}\frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k}d_i}\sum_{\substack{e_1,\dots,e_k\\ \forall i\ u_i|e_i\\ \forall i\neq j\ s_{i,j}|e_j}}\frac{\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^{k}e_i}.$$

Nyní zavedeme nové proměnné pro součet přes kombinace $d_1,\dots,d_k$:

$$y_{r_1,\dots,r_k}=\left(\prod_{i=1}^{k}\mu(r_i)\varphi(r_i)\right)\sum_{\substack{d_1,\dots,d_k\\ \forall i\ r_i|d_i}}\frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k}d_i}.$$

S vyloučením r obsahující čtverec můžeme vyjádřit ($\mu(r)\neq 0$) jako

$$\left(\prod_{i=1}^{k}\frac{1}{\mu(r_i)\varphi(r_i)}\right)y_{r_1,\dots,r_k}=\sum_{\substack{d_1,\dots,d_k\\ \forall i\ r_i|d_i}}\frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k}d_i}.$$

A protože pro $\mu(r)\neq 0$ se $\frac{1}{\mu(r)}$ rovná $\mu(r)$, máme rovnost

$$\left(\prod_{i=1}^{k}\frac{\mu(r)}{\varphi(r_i)}\right)y_{r_1,\dots,r_k}=\sum_{\substack{d_1,\dots,d_k\\ \forall i\ r_i|d_i}}\frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k}d_i}.$$

Jelikož hodnota $\lambda_{d_1,\dots,d_k}$ je nulová, pokud jsou dělitelé pro danou lambdu soudělné, můžeme stejně tak omezit $s_{i,j}$ na nesoudělné s u_i a u_j. Stejně tak uvažujeme pouze $s_{i,j}$ nesoudělné s $s_{i,l}$ pro všechna l (kromě j) a nesoudělné s $s_{l,j}$ pro všechna l (kromě i). Sumu přes $s_{i,j}$ s těmito omezeními značíme $\sum\!{}^{*}_{s_{1,2}\,,\dots,\,s_{k,k-1}}$.

Po dosazení předchozího vyjádření do hlavního členu s tím, že $a_i = u_i \prod_{j\neq i} s_{i,j}$ a $b_i = u_i \prod_{j\neq i} s_{j,i}$, dostáváme

$$\frac{N}{W}\sum_{u_1,\dots,u_k}\left(\prod_{i=1}^{k}\varphi(u_i)\right)\sum_{s_{1,2}\,,\dots,\,s_{k,k-1}}^{*}\left(\prod_{\substack{1\le i,j\le k\\ i\neq j}}\mu(s_{i,j})\right)\left(\prod_{i=1}^{k}\frac{\mu(a_i)\mu(b_i)}{\varphi(a_i)\varphi(b_i)}\right)y_{a_1,\dots,a_k}y_{b_1,\dots,b_k}.$$

Díky nesoudělnosti všech činitelů v a_i a b_i (u_i a odpovídajících $s_{i,j}$) a protože Möbiova i Eulerova funkce jsou multiplikativní, můžeme rozepsat $\mu(a_i)$ a $\varphi(a_i)$ podle $\mu(a_i) = \mu(u_i)\prod_{i\neq j}\mu(s_{i,j})$, $\varphi(a_i) = \varphi(u_i)\prod_{i\neq j}\varphi(s_{i,j})$, pro b_i potom obdobně. Získáváme

$$\begin{aligned}&\frac{N}{W}\sum_{u_1,\dots,u_k}\left(\prod_{i=1}^{k}\varphi(u_i)\right)\left(\prod_{i=1}^{k}\frac{\mu(u_i)^2}{\varphi(u_i)^2}\right)\sum_{s_{1,2}\,,\dots,\,s_{k,k-1}}^{*}\left(\prod_{\substack{1\le i,j\le k\\ i\neq j}}\frac{\mu(s_{i,j})^3}{\varphi(s_{i,j})^2}\right)y_{a_1,\dots,a_k}y_{b_1,\dots,b_k}\\ =&\frac{N}{W}\sum_{u_1,\dots,u_k}\left(\prod_{i=1}^{k}\frac{\mu(u_i)^2}{\varphi(u_i)}\right)\sum_{s_{1,2}\,,\dots,\,s_{k,k-1}}^{*}\left(\prod_{\substack{1\le i,j\le k\\ i\neq j}}\frac{\mu(s_{i,j})}{\varphi(s_{i,j})^2}\right)y_{a_1,\dots,a_k}y_{b_1,\dots,b_k}.\end{aligned}$$

Z podmínky pro y víme, že členy $s_{i,j}$ soudělné s W nemají žádný vliv, proto potřebujeme zvážit ty rovné jedné ($s_{i,j} = 1$) a takové, které obsahují prvočíslo větší než největší prvočíslo v W (a tudíž i $s_{i,j} > D_0$).

Pro prvky $s_{i,j} = 1$ získáváme vyjádření

$$\begin{aligned}&\frac{N}{W}\sum_{u_1,\dots,u_k}\left(\prod_{i=1}^{k}\frac{1}{\varphi(u_i)}\right)\sum_{\substack{s_{1,2}\,,\dots,\,s_{k,k-1}\\ s_{i,j}=1}}^{*}\left(\prod_{\substack{1\le i,j\le k\\ i\neq j}}\frac{\mu(1)}{\varphi(1)^2}\right)y_{a_1,\dots,a_k}y_{b_1,\dots,b_k}\\ =&\frac{N}{W}\sum_{u_1,\dots,u_k}\frac{y^2_{u_1,\dots,u_k}}{\prod_{i=1}^{k}\varphi(u_i)}.\end{aligned}$$

Pro prvky $s_{i,j} > D_0$ odhadneme asymptoticky růst vyjádřený pomocí maximální hodnoty proměnné y ($y_{max} = \sup_{r_1,\dots,r_k} |y_{r_1,\dots,r_k}|$) podle

$$\begin{aligned}
&\frac{N}{W} \sum_{u_1,\dots,u_k} \left(\prod_{i=1}^{k} \frac{\mu(u_i)^2}{\varphi(u_i)} \right) \sum_{\substack{s_{1,2}\,,\,\dots\,,\,s_{k,k-1} \\ s_{i,j}>D_0}}^{*} \left(\prod_{\substack{1\le i,j\le k \\ i\neq j}} \frac{\mu(s_{i,j})}{\varphi(s_{i,j})^2} \right) y_{a_1,\dots,a_k} y_{b_1,\dots,b_k} \\
&\qquad \ll \frac{N\, y_{max}^2}{W} \sum_{u_1,\dots,u_k} \left(\prod_{i=1}^{k} \frac{\mu(u_i)^2}{\varphi(u_i)} \right) \sum_{\substack{s_{1,2}\,,\,\dots\,,\,s_{k,k-1} \\ s_{i,j}>D_0}}^{*} \left(\prod_{\substack{1\le i,j\le k \\ i\neq j}} \frac{\mu(s_{i,j})}{\varphi(s_{i,j})^2} \right) \\
&\ll \frac{N\, y_{max}^2}{W} \left(\sum_{\substack{u<R \\ \gcd(u,W)=1}} \frac{\mu(u)^2}{\varphi(u)} \right)^{k} \left(\sum_{s\ge 1} \frac{\mu(s)^2}{\varphi(s)^2} \right)^{k^2-k+1} \sum_{s_{i,j}>D_0} \frac{\mu(s_{i,j})^2}{\varphi(s_{i,j})^2} \\
&\qquad \ll \frac{y_{max}^2\, \varphi(W)^k\, N\, (\log R)^k}{W^{k+1}\, D_0}.
\end{aligned}$$

Zbývá nám objasnit chybový člen z (6). Označme $\lambda_{max} = \sup_{d_1,\dots,d_k} |\lambda d|$ a $\tau_k(d)$ počet způsobů zapsání d jako součinu k přirozených čísel. Nenulové hodnoty $\lambda_{d_1,\dots,d_k}$ jsou omezeny na $d = \prod_{i=1}^{k} d_i < R$ a proto

$$\sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k}}{}' |\lambda_{d_1,\dots,d_k} \lambda_{e_1,\dots,e_k}| \ll \lambda_{max}^2 \left(\sum_{d<R} \tau_k(d) \right)^2 \ll \lambda_{max}^2 \left(\sum_{d<R} \log R^k \right)^2 \ll \lambda_{max}^2 R^2 (\log R)^{2k}.$$

Pro vyjádření λ_{max} užijeme součet zavedené proměnné y podle

$$\begin{aligned}
\sum_{\substack{r_1,\dots,r_k \\ \forall i\ d_i|r_i}} \frac{y_{r_1,\dots,r_k}}{\prod_{i=1}^{k} \varphi(r_i)} &= \sum_{\substack{r_1,\dots,r_k \\ \forall i\ d_i|r_i}} \left(\prod_{i=1}^{k} \frac{\mu(r_i)\varphi(r_i)}{\varphi(r)} \right) \sum_{\substack{e_1,\dots,e_k \\ \forall i\ r_i|e_i}} \frac{\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^{k} e_i} \\
&= \sum_{e_1,\dots,e_k} \frac{\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^{k} e_i} \sum_{\substack{r_1,\dots,r_k \\ \forall i\ d_i|r_i \\ \forall i\ r_i|e_i}} \prod_{i=1}^{k} \mu(r_i) = \frac{\lambda_{d_1,\dots,d_k} \prod_{i=1}^{k} \mu(d_i)}{\prod_{i=1}^{k} d_i} = \frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k} \mu(d_i) d_i},
\end{aligned} \tag{7}$$

tudíž

$$\lambda_{d_1,\dots,d_k} = \left(\prod_{i=1}^{k} \mu(d_i) d_i\right) \sum_{\substack{r_1,\dots,r_k \\ \forall i\ d_i | r_i}} \frac{y_{r_1,\dots,r_k}}{\prod_{i=1}^{k} \varphi(r_i)}.$$

Při vytknutí maximalní hodnoty $y_{max} = \sup_{r_1,\dots,r_k} |y_{r_1,\dots,r_k}|$ nesmíme zapomenout, že $y_{r_1,\dots,r_k}$ nabývá nulové hodnoty pro $\prod_{i=1}^{k} r_i$ větší nebo rovno R a obsahujíc čtverec, proto do sumy přes $r_1, \dots, r_k$ tyto podmínky přidáme, neboli

$$\lambda_{max} \leq \sup_{\substack{d_1,\dots,d_k \\ \prod_{i=1}^{k} d_i \text{ bezčtvercové}}} y_{max} \left(\prod_{i=1}^{k} d_i\right) \sum_{\substack{r_1,\dots,r_k \\ \forall i\ d_i | r_i \\ \prod_{i=1}^{k} r_i < R, \text{ beztvercove}}} \frac{1}{\prod_{i=1}^{k} \varphi(r_i)}.$$

Zavedmě substituci $r' = \prod_{i=1}^{k} \frac{r_i}{d_i}$. Abychom vyrovnali, že nové r' nahrazuje několik kombinací původních $r_1, \dots, r_k$, vynásobíme výraz počtem možností rozepsání r' jakožto součinu k přirozených čísel ($\tau_k(r')$). Náhradu $\prod_{i=1}^{k} r_i = r' \prod_{i=1}^{k} d_i$ jsme použili ve jmenovateli, proto $\varphi(d_i)$ umístíme do jmenovatele členu společného pro všechna r'. Bezčtvercovost r' nám potom zaručí $\mu(r')^2$. Celkově

$$\lambda_{max} \leq y_{max} \sup_{\substack{d_1,\dots,d_k \\ \prod_{i=1}^{k} d_i \text{ bezčtvercové}}} \left(\prod_{i=1}^{k} \frac{d_i}{\varphi(d_i)}\right) \sum_{\substack{r' < R \prod_{i=1}^{k} d_i^{-1} \\ \gcd(r', \prod_{i=1}^{k} d_i) = 1}} \frac{\mu(r')^2 \tau_k(r')}{\prod_{i=1}^{k} \varphi(r')}.$$

Nyní využijeme identitu $\frac{d}{\varphi(d)} = \sum_{e|d} \frac{1}{\varphi(e)}$ (viz 1.1)spolu se zapsaním bezčtvercovosti pomocí Möbiovi funkce pro vyjádření

$$\lambda_{max} \leq y_{max} \sup_{d_1,\dots,d_k} \sum_{d | \prod_{i=1}^{k} d_i} \frac{\mu(d)^2}{\varphi(d)} \sum_{\substack{r' < R \prod_{i=1}^{k} d_i^{-1} \\ \gcd(r', \prod_{i=1}^{k} d_i) = 1}} \frac{\mu(r')^2 \tau_k(r')}{\prod_{i=1}^{k} \varphi(r')}.$$

Pro poslední zjednodušení položíme $u = dr'$, kde pro spodní odhad použijeme zřejmou skutečnost $\tau_k(dr') \leq \tau(r')$, a dostáváme

$$\lambda_{max} \leq y_{max} \sum_{u < R} \frac{\mu(u)^2 \tau_k(u)}{\varphi(u)} \ll y_{max} (\log R)^k. \tag{8}$$

Ve výsledku získáváme chybový člen $O(y_{max}^2 R^2 (\log R)^{4k})$.

Celkovou hodnotu sumy S_1 vyjádříme jako

$$S_1 = \frac{N}{W} \sum_{u_1,\ldots,u_k} \frac{y^2_{u_1,\ldots,u_k}}{\prod_{i=1}^k \varphi(u_i)} + O\left(\frac{y^2_{max}\,\varphi(W)^k\,N\,(\log R)^k}{W^{k+1}\,D_0} + y^2_{max}R^2(\log R)^{4k}\right).$$

Přičemž v chýbovém členu můžeme vidět, že

$$\begin{aligned} &O\left(y^2_{max}\,(\log R)^k\left(\frac{\varphi(W)^k\,N}{W^{k+1}\,D_0} + R^2(\log R)^{3k}\right)\right) \\ =&O\left(y^2_{max}\,(\log R)^k\left(\frac{N}{(\log\log N)^2\,\log\log\log N} + R^{2+\epsilon}\right)\right). \end{aligned}$$

Proto první chybový člen dominuje a získáváme Lemma 1.

□

Nyní se podíváme na vyjádření sumy S_2, které rozdělíme pro jednotlivé prvky splnitelné množiny $\mathcal{H}$ indexem $m \in \{1,\ldots,k\}$. Potom

$$S_2 = \sum_{m=1}^{k} S_2^{(m)},$$

kde

$$S_2^{(m)} = \sum_{\substack{N\le n\le 2N \\ n\equiv v_0 \pmod W}} \chi_{\mathbb{P}}(n+h_m)\left(\sum_{\substack{d_1,\ldots,d_k \\ \forall i\ d_i \mid n+h_i}} \lambda_{d_1,\ldots,d_k}\right)^2.$$

Lemma 2: *Nechť*

$$y^{(m)}_{r_1,\ldots,r_k} = \left(\prod_{i=1}^k \mu(r_i)g(r_i)\right) \sum_{\substack{d_1,\ldots,d_k \\ \forall i\ r_i\mid d_i \\ d_m=1}} \frac{\lambda_{d_1,\ldots,d_k}}{\prod_{i=1}^k \varphi(d_i)},$$

kde g je zcela multiplikativní funkce na prvočíslech definovaná vztahem $g(p) = p-2$, a $y^{(m)}_{max} = \sup_{r_1,\ldots,r_k}\left|y^{(m)}_{r_1,\ldots,r_k}\right|$. Potom pro všechna $A > 0$ máme

$$S_2^{(m)} = \frac{N}{\varphi(W)\,\log N}\sum_{r_1,\ldots,r_k} \frac{(y^{(m)}_{r_1,\ldots,r_k})^2}{\prod_{i=1}^k g(r_i)} + O\left(\frac{(y^{(m)}_{max})^2\,\varphi(W)^{k-2}\,N\,(\log N)^{k-2}}{W^{k-1}D_0}\right) + O\left(\frac{y^2_{max}N}{(\log N)^A}\right).$$

Důkaz: Již tradičně začneme roznásobením kvadrátu a přehozením pořadí sumace.

$$S_2^{(m)} = \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \sum_{\substack{N\le n\le 2N \\ n\equiv v_0 \pmod W \\ \forall i\ \mathrm{lcm}(d_i,e_i)\mid n+h_i}} \chi_{\mathbb{P}}(n+h_m)$$

Pro vyhodnocení vnitřní sumy opět užijeme periodicitu přes $q = W\prod_{i=1}^{k}\mathrm{lcm}(d_i,e_i)$ za podmínky nesoudělnosti W a $\mathrm{lcm}(d_i,e_i)$ pro všechna i. Nyní však nestačí vyčíslit jen počet čísel v dané zbytkové třídě, neboť vyžadujeme prvočíselnost $n+h_m$. Z podmínky sumy $\forall i\ \mathrm{lcm}(d_i,e_i)\mid n+h_i$ nám vyvstává poznatek, že d_m i e_m jsou rovny jedné (jinak by $n+h_m$ nebylo prvočíslo). Počet prvočísel spadajících do určité zbytkové třídy nesoudělné s modulem odpovída počtu onich prvočísel vyděleného hodnotou Eulerovy funkce z modulu (viz 1.8).

Označme X_N počet prvočísel na sítovací množině a $E(N,q)$ maximální chybu této aproximace zvětšenou o jedna (kvůli běžné odchylce v počtu čísel příslušících na obecném intervalu dané zbytkové třídě):

$$X_N = \sum_{N\le n<2N} \chi_{\mathbb{P}}(n).$$

Potom počet prvočísel kongruentních s a modulo q takové, že $\gcd(a,q)=1$, lze vyjádřit jako $\frac{X_N}{\varphi(q)} + O(E(N,q))$, kde

$$E(N,q) = 1 + \sup_{\gcd(a,q)=1} \left| \sum_{\substack{N\le n<2N \\ n\equiv a \pmod q}} \chi_{\mathbb{P}}(n) \;-\; \frac{1}{\varphi(q)} \sum_{N\le n<2N} \chi_{\mathbb{P}}(n) \right|.$$

V případě soudělnosti v rámci W a $\mathrm{lcm}(d_i,e_i)$ (tuto podmínku opět označíme užitím $\sum'$) nebo pokud $d_m > 1$ či $e_m > 1$ požadujeme nulovou hodnotu vnitřní sumy. Tím získáváme rovnost

$$S_2^{(m)} = \frac{X_N}{\varphi(W)} \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k \\ e_m=d_m=1}}{}' \frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^{k}\varphi(\mathrm{lcm}(d_i,e_i)} + O\left(\sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k}} |\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}|\, E(N,q) \right)$$

Závislosti na $\operatorname{lcm}(d,e)$ se tentokrát zbavíme s využitím tvrzení $\varphi(n) = \sum_{d|n} g(d)$ pro bezčtvercové n (podle (2)). Vezmeme

$$\frac{1}{\varphi(\operatorname{lcm}(d_i,e_i))} = \frac{1}{\varphi(d_i)\varphi(e_i)} \sum_{u_i|d_i,e_i} g(u_i)$$

a pro hlavní člen získáváme

$$\frac{X_N}{\varphi(W)} \sum_{u_1,\dots,u_k} \left(\prod_{i=1}^{k} g(u_i)\right) \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k \\ e_m=d_m=1}}{}' \frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^{k}\varphi(d_i)\varphi(e_i)}.$$

S podmínkou sumy na nesoudělnost $d_i a e_j$ pro $i \neq j$ (jakožto jedinou nepokrytou možností z podmínky na nesoudělnost W a $\operatorname{lcm}(d_i,e_i)$) se vyrovnáme jako v případě S_1 pomocí nové proměnné $s_{i,j}$:

$$\frac{X_N}{\varphi(W)} \sum_{u_1,\dots,u_k} \left(\prod_{i=1}^{k} g(u_i)\right) \sum_{s_{1,2},\dots,s_{k,k-1}}{}^{*} \left(\prod_{\substack{1\le i,j\le k \\ i\neq j}} \mu(s_{i,j})\right) \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k \\ e_m=d_m=1}} \frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^{k}\varphi(d_i)\varphi(e_i)}.$$

proměnnou y zavedeme tentokrát jako

$$y^{(m)}_{r_1,\dots,r_k} = \left(\prod_{i=1}^{k} \mu(r_i)g(r_i)\right) \sum_{\substack{d_1,\dots,d_k \\ \forall i\ r_i|d_i \\ d_m=1}} \frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k}\varphi(d_i)}. \tag{9}$$

Tím získaváme hlavní člen

$$\frac{X_N}{\varphi(W)} \sum_{u_1,\dots,u_k} \left(\prod_{i=1}^{k} g(u_i)\right) \sum_{s_{1,2}\,,\dots,\,s_{k,k-1}}{}^{*} \left(\prod_{\substack{1\le i,j\le k \\ i\neq j}} \mu(s_{i,j})\right) \left(\prod_{i=1}^{k} \frac{\mu(a_i)\mu(b_i)}{g(a_i)g(b_i)}\right) y^{(m)}_{a_1,\dots,a_k} y^{(m)}_{b_1,\dots,b_k},$$

kde $a_i = u_i \prod_{i\neq j} s_{i,j}$ a $b_i = u_i \prod_{i\neq j} s_{j,i}$. Neboli po obdobných úpravách jako pro S_1, protože

g je také multiplikativní funkce, máme

$$\frac{X_N}{\varphi(W)} \sum_{u_1,\dots,u_k} \left(\prod_{i=1}^{k} \frac{\mu(u_i)^2}{g(u_i)} \right) \sum_{s_{1,2}\,,\,\dots\,,\,s_{k,k-1}}{}^{*} \left(\prod_{\substack{1\le i,j\le k \\ i\neq j}} \frac{\mu(s_{i,j})}{g(s_{i,j})^2} \right) y^{(m)}_{a_1,\dots,a_k} y^{(m)}_{b_1,\dots,b_k}.$$

Pro $s_{i,j} = 1$ se výraz zjednoduší na

$$\frac{X_N}{\varphi(W)} \sum_{u_1,\dots,u_k} \frac{(y^{(m)}_{u_1,\dots,u_k})^2}{\prod_{i=1}^{k} g(u_i)}.$$

Pro $s_{i,j} > 1$ potom máme asymptotický odhad

$$\begin{aligned} &\ll \frac{X_N}{\varphi(W)} \sum_{u_1,\dots,u_k} \left(\prod_{i=1}^{k} \frac{\mu(u_i)^2}{g(u_i)} \right) \sum_{\substack{s_{1,2}\,,\,\dots\,,\,s_{k,k-1} \\ s_{i,j}>1}}{}^{*} \left(\prod_{\substack{1\le i,j\le k \\ i\neq j}} \frac{\mu(s_{i,j})}{g(s_{i,j})^2} \right) \left(y^{(m)}_{max}\right)^2 \\ &\ll \frac{(y^{(m)}_{max})^2\, N}{\varphi(W)\, \log N} \left(\sum_{\substack{u<R \\ \gcd(u,W)=1}} \frac{\mu(u)^2}{g(u)} \right)^{k-1} \left(\sum_{s} \frac{\mu(s)^2}{g(s)^2} \right)^{k^2-k-1} \sum_{s_{i,j}>D_0} \frac{\mu(s_{i,j})^2}{g(s_{i,j})^2} \\ &\ll \frac{(y^{(m)}_{max})^2\, \varphi(W)^{k-2}\, N (\log R)^{k-1}}{W^{k-1} D_0\, \log N}. \end{aligned}$$

Podle Prvočíselné věty $X_N = \frac{N}{\log N} + O\left(\frac{N}{(\log N)^2}\right)$ a po roznásobení získáváme nový chybový člen

$$\ll \frac{(y^{(m)}_{max})^2\, N}{\varphi(W)\, (\log N)^2} \left(\sum_{\substack{u<R \\ \gcd(u,W)=1 \\ u \text{ bezčtvercové}}} \frac{1}{g(u)} \right)^{k-1} \ll \frac{(y^{(m)}_{max})^2\, N\, \varphi(W)^{k-2} (\log R)^{k-3}}{W^{k-1}},$$

který se ztratí ve výše předcházejícím chybovém členu (vzniklém při $s_{i,j} > 1$).

Zbývá chybový člen pocházející z počtu prvočísel ve zbytkové třídě. Z (8) vime, ze $\lambda_{max} \ll y_{max} (\log R)^k$. Pro rozdělení bezčtvercového r mezi $d_1, \dots, d_k$, $e_1, \dots, e_k$ a W máme

při podmínce nesoudělnosti W a jednotlivých $\operatorname{lcm}(d_i, e_i)$ maximálně $\tau_{3k}(r)$ možností. Proto tento chybový člen je

$$\ll y_{max}^2 (\log R)^{2k} \sum_{r<R^2W} \mu(r)^2 \tau_{3k}(r) E(N,r).$$

Asymptotický odhad chyby pro počet prvočísel v dané zbytkové třídě nám dává předpoklad distribuce prvočísel (viz Definice 7). Argument sumy rozdělíme na dvě části, na které využijeme Cauchy–Schwarzovu nerovnost, kdy části čtverce $E(N,r)$ rozdělíme mezi obě části a v jednom případě nahradíme nejhorším odhadem $E(N,r) \ll \frac{N}{\varphi(r)}$.

$$\begin{aligned} &\ll y_{max}^2 (\log R)^{2k} \left(\sum_{r<R^2W} \mu(r)^2 \tau_{3k}^2(r) \frac{N}{\varphi(r)} \right)^{\frac{1}{2}} \left(\sum_{r<R^2W} \mu(r)^2 E(N,r) \right)^{\frac{1}{2}} \\ &\ll y_{max}^2 (\log N)^k \left(\sum_{r<R^2W} N \right)^{\frac{1}{2}} \left(\frac{N}{(\log N)^A} \right)^{\frac{1}{2}} \ll \frac{y_{max}^2 N}{(\log N)^A} \end{aligned}$$

□

Ve vyjádření S_2 jsme zavedli proměnnou $y^{(m)}_{r_1,\dots,r_k}$, kterou bychom potřebovali vztahnout k $y_{r_1,\dots,r_k}$ z vyjádření S_1.

Lemma 3: *Nechť $r_m = 1$, potom*

$$y^{(m)}_{r_1,\dots,r_k} = \sum_{a_m} \frac{y_{r_1,\dots,r_{m-1},a_m,r_{m+1},\dots,r_k}}{\varphi(a_m)} + O\left(\frac{y_{max}\, \varphi(W)\, \log R}{W D_0} \right).$$

Důkaz: Do definičního vztahu $y^{(m)}_{r_1,\dots,r_k}$ (9) dosadíme $\lambda_{d_1,\dots,d_k}$ podle inverzního vztahu pro $y_{r_1,\dots,r_k}$ (7), čímž získáme rovnost

$$y^{(m)}_{r_1,\dots,r_k} = \left(\prod_{i=1}^k \mu(r_i) g(r_i) \right) \sum_{\substack{d_1,\dots,d_k \\ \forall i\ r_i \mid d_i \\ d_m = 1}} \left(\prod_{i=1}^k \frac{\mu(d_i) d_i}{\varphi(d_i)} \right) \sum_{\substack{a_1,\dots,a_k \\ \forall i\ d_i \mid a_i}} \frac{y_{a_1,\dots,a_k}}{\prod_{i=1}^k \varphi(a_i)}.$$

Prohodíme pořadí sumy, sumu přes $d_1, \ldots, d_k$ zahrneme do hlavní a máme

$$y^{(m)}_{r_1,\ldots,r_k} = \left(\prod_{i=1}^{k} \mu(r_i) g(r_i)\right) \sum_{\substack{a_1,\ldots,a_k \\ \forall i\ d_i \mid a_i}} \frac{y_{a_1,\ldots,a_k}}{\prod_{i=1}^{k} \varphi(a_i)} \prod_{i \neq m} \frac{\mu(a_i) r_i}{\varphi(a_i)}.$$

Z omezení hodnot $y_{a_1,\ldots,a_k}$ víme, že stačí uvažovat a_i nesoudělné s W. Jelikož r_i dělí a_i víme, že potom buď $a_i = r_i$ nebo $a_i > D_0 r_i$. S předpokladem $i \neq m$ pro druhý případ hodnotu $y^{(m)}_{r_1,\ldots,r_k}$ pouze asymptoticky odhadneme jako

$$\begin{aligned} &\ll y_{max} \left(\prod_{j=1}^{k} g(r_j) r_j\right) \left(\sum_{\substack{r_i \mid a_i \\ a_i > D_0 r_i}} \frac{\mu(a_i)^2}{\varphi(a_i)^2}\right) \left(\sum_{\substack{a_m < R \\ \gcd(a_m, W) = 1}} \frac{\mu(a_m)^2}{\varphi(a_m)}\right) \prod_{\substack{1 \leq j \leq k \\ j \neq i, m}} \left(\sum_{r_j \mid a_j} \frac{\mu(a_j)^2}{\varphi(a_j)^2}\right) \\ &\ll \left(\prod_{j=1}^{k} \frac{g(r_j) r_j}{\varphi(r_j)^2}\right) \frac{y_{max}\, \varphi(W)\, \log R}{W\, D_0} \ll \frac{y_{max}\, \varphi(W)\, \log R}{W\, D_0}, \end{aligned}$$

což nám dává chybový člen. Hlavní člen tvoří případy, kdy pro všechna i kromě m platí $a_i = r_i$, jež vyjádříme ve tvaru

$$y^{(m)}_{r_1,\ldots,r_k} = \left(\prod_{i=1}^{k} \frac{g(r_i) r_i}{\varphi(r_i)^2}\right) \sum_{a_m} \frac{y_{r_1,\ldots,r_{m-1},a_m,r_{m+1},\ldots,r_k}}{\varphi(a_m)} + O\left(\frac{y_{max}\, \varphi(W)\, \log R}{W D_0}\right).$$

Pro prvočísla se nám nabízí zjednodušení

$$\frac{g(p) p}{\varphi(p)^2} = \frac{p^2 - 2p}{p^2 - 2p + 1} = 1 + O(p^{-2}),$$

což platí i obecně pro bezčtvercová čísla, neboť g i φ jsou multiplikativní funkce. Proto

$$\prod_{i=1}^{k} \frac{g(r_i) r_i}{\varphi(r_i)^2} = 1 + O(D_0^{-1}),$$

pričemž chybový člen můžeme zahrnout do stávajícího.

□

2.4 Hladké y

Nyní potřebujeme za proměnnou $y_{r_1,\dots,r_k}$ zvolit vhodně hladkou funkci, kterou dokážeme dobře integrovat. Využitím metody Lagrangeových multiplikátorů na poměr sum S_1 a S_2, pro který se snažíme najít extrémní hodnotu, dostáváme podmínku

$$\lambda\, y_{r_1,\dots,r_k} = \left(\prod_{i=1}^{k} \frac{\varphi(r_i)}{g(r_i)}\right) \sum_{m=1}^{k} \frac{g(r_m)}{\varphi(r_m)} y^{(m)}_{r_1,\dots,r_{m-1},1,r_{m+1},\dots,r_k}$$

Jelikož požadujeme nesoudělnost r s W, víme, že r_i je prosté malých prvočísel, a pro takové r_i (s předpokladem bezčtvercovosti) můžeme psát

$$g(r_i) = \prod_{p|r_i}(p-2) \approx \varphi(r_i) = \prod_{p|r_i}(p-1) \approx r_i = \prod_{p|r_i} p,$$
$$\frac{\varphi(r_i)}{g(r_i)} \approx 1 \approx \frac{g(r_i)}{\varphi(r_i)}.$$

Tím se nám podmínka zjednodušuje na

$$\lambda\, y_{r_1,\dots,r_k} \approx \sum_{m=1}^{k} \frac{g(r_m)}{\varphi(r_m)} y^{(m)}_{r_1,\dots,r_{m-1},1,r_{m+1},\dots,r_k},$$

což nám vyhovuje vzhledem k nezávislosti na prvočíselném rozkladu čísla r nebo jiných potenciálních nespojitostech výrazu.

Definujme $y_{r_1,\dots,r_k}$ pomocí hladké funkce $F : \mathbb{R}^k \mapsto \mathbb{R}$ nulové mimo $\mathcal{R}_k = \{(x_1,\dots,x_k) \in [0,1]^k : \sum_{i=1}^{k} x_k \le 1\}$. Pro r soudělné s W nebo obsahující čtverec požadujeme $y_{r_1,\dots,r_k} = 0$, v opačném případě položíme

$$y_{r_1,\dots,r_k} = F\left(\frac{\log r_1}{\log R},\dots,\frac{\log r_k}{\log R}\right).$$

Následující lemma, které použili ve své práci již Goldston, Pintz a Yıldırım, nám umožní přesun od problematického součtu přes dělitele k integraci spojité funkce a ve spojení s volbou y tím i získat finální hladké odhady síta.

Lemma 4: *Nechť A_1, A_2, $L > 0$ a $\gamma : \mathbb{N} \mapsto \mathbb{R}$ je multiplikativní funkce, jež pro všechna $2 \leq w \leq z$ splňuje*

$$0 \leq \frac{\gamma(p)}{p} \leq 1 - A_1,$$
$$-L \leq \sum_{w \leq p \leq z} \frac{\gamma(p) \log p}{p} - \log \frac{z}{w} \leq A_2.$$

Dále nechť h je zcela multiplikativní funkce na prvočíslech definovaná podle $h(p) = \frac{\gamma(p)}{p - \gamma(p)}$ a $G : [0,1] \mapsto \mathbb{R}$ je hladká funkce. Označme $G_{max} = sup_{t \in [0,1]} (|G(t)| + |G'(t)|)$. Potom

$$\sum_{\substack{d<z \\ d \text{ bezčtvercové}}} h(d) G\left(\frac{\log d}{\log z}\right) = \mathfrak{S} \log z \int_0^1 G(x) dx + O_{A_1,A_2}(\mathfrak{S} L G_{max}),$$

kde

$$\mathfrak{S} = \prod_p \left(\frac{p-1}{p - \gamma(p)}\right).$$

Důkaz: Sumu lze psát jako

$$\sum_{d<z} \mu(d)^2 h(d) G\left(\frac{\log d}{\log z}\right) = \int_1^z G\left(\frac{\log u}{\log z}\right) dD(u),$$

kde

$$D(u) = \sum_{d<z} \mu(d)^2 h(d),$$

pričemž podle [4, Lemma 3] platí

$$\sum_{d<z} \mu(d)^2 h(d) = \mathfrak{S} \log u + E(u)$$

pro určitý chybový člen $E(u) \ll \mathfrak{S} L$.

Hlavní integrál vypočteme díky substituci $u = z^x$ jako

$$\begin{aligned} \int_1^z G\left(\frac{\log u}{\log z}\right) d(\mathfrak{S} \log u) &= \int_1^z G\left(\frac{x \log z}{\log z}\right) d(\mathfrak{S} x \log z) \\ &= \int_0^1 G(x)\, d(x \mathfrak{S} \log z) = \int_0^1 \mathfrak{S} \log z G(x)\, dx. \end{aligned}$$

chybový integrál potom integrací per partes vypočteme jako

$$\int_1^z G\left(\frac{\log u}{\log z}\right) dE(u) = \left[G\left(\frac{\log u}{\log z}\right) E(u)\right]_1^z - \int_1^z \frac{1}{\log z} G'\left(\frac{\log u}{\log z}\right) E(u)du$$
$$\ll sup_{t\in[0,1]} \left(|G(t)| + |G'(t)|\right) E(u) \ll G_{max}\mathfrak{S}L.$$

□

Následující dvě lemma dokazují Tvrzení 1. První se vztahuje k sumě S_1 pro všechna čísla (pri zohlednění daných vah), druhé pak k sumě $S_2^{(m)}$ pro prvočísla odpovídající posunu podle m-tého prvku $\mathcal{H}$.

Lemma 5: *Nechť* $y_{r_1,\dots,r_k} = F\left(\frac{\log r_1}{\log R}, \dots, \frac{\log r_k}{\log R}\right)$, *kde* F *je hladká funkce, která je nulová mimo* $\mathcal{R}_k = \{(x_1, \dots, x_k) \in [0,1]^k : \sum_{i=1}^k x_k \leq 1\}$. *Dale označíme*

$$F_{max} = \sup_{(t_1,\dots,t_k)\in[0,1]^k} |F(t_1, \dots, t_k)| + \sum_{i=1}^k \left|\frac{\partial F(t_1, \dots, t_k)}{\partial t_i}\right|.$$

Potom

$$S_1 = \frac{\varphi(W)^k N (\log R)^k}{W^{k+1}} I_k(F) + O\left(\frac{F_{max}^2 \varphi(W)^k N (\log R)^k}{W^{k+1} D_0}\right),$$

kde

$$I_k(F) = \int_0^1 \cdots \int_0^1 F(t_1, \dots, t_k)^2 dt_1 \dots dt_k.$$

Důkaz: Dosazením volby $y_{r_1,\dots,r_k}$ do předchozího vyjádření sumy S_1 (z Lemmatu 1) získáme

$$S_1 = \frac{N}{W} \sum_{\substack{u_1,\dots,u_k \\ \forall i\neq j\ \gcd(u_i,u_j)=1 \\ \forall i\ \gcd(u_i,W)=1}} \left(\prod_{i=1}^k \frac{\mu(u_i)^2}{\varphi(u_i)}\right) F\left(\frac{\log u_1}{\log R}, \dots, \frac{\log u_k}{\log R}\right)^2 + O\left(\frac{F_{max}^2 \varphi(W)^k N (\log R)^k}{W^{k+1} D_0}\right).$$

Rádi bychom upustili od podmínky na nesoudělnost mezi u_i a u_j (pro $i \neq j$). Víme, že pokud mají společný faktor, ale přitom jsou nesoudělné s W, musí být onen faktor větší než největší prvočíslo v W (D_0). Jejich příspěvek vyjádříme stejnou sumou, ale s omezením na velikost prvočísel. Tu odhadneme jako

$$\ll \frac{F_{max}^2\, N}{W} \sum_{p>D_0} \sum_{\substack{u_1,\ldots,u_k<R \\ p\mid u_i,u_j \\ \forall i:\, \gcd(u_i,W)=1}} \prod_{i=1}^{k} \frac{\mu(u_i)^2}{\varphi(u_i)} \ll \frac{F_{max}^2\, N}{W} \sum_{p>D_0} \frac{1}{(p-1)^2} \left(\sum_{\substack{u<R \\ \gcd(u,W)=1}} \frac{\mu(u_i)^2}{\varphi(u_i)} \right)^k$$
$$\ll \frac{F_{max}^2\, \varphi(W)^k\, N\, (\log R)^k}{W^{k+1}\, D_0}.$$

Získaný chybový člen tak začleníme do puvodního z Lemmatu 1.

Pro hlavní člen využijeme opakovaně Lemma 4. Funkci $\gamma(p)$ zvolíme tak, aby funkce h zajistila podmínku nulovosti při soudělnosti u s W a v opačném případě dala převrácenou hodnotu Eulerovy funkce. Proto položíme

$$\gamma(p) = \begin{cases} 0, & p \mid W, \\ 1, & p \nmid W. \end{cases}$$

Pak totiž pro u_i, jehož bezčtvercovost nám zajišťuje kvadrát Möbiovy funkce, máme vztahy

$$h(p) = \frac{\gamma(p)}{p-\gamma(p)} \begin{cases} \frac{0}{p-0}, & p \mid W, \\ \frac{1}{p-1}, & p \nmid W, \end{cases}$$
$$h(u_i) = \prod_{p\mid u_i} h(p) = \begin{cases} 0, & \exists p \mid W, \\ \prod_{i=1}^{k} \frac{1}{p-1} = \frac{1}{\varphi(u_i)}, & \forall p \nmid W. \end{cases}$$

Připomeňme jen, že v terminologii Lemmatu 4 platí

$$z = R,$$
$$G_i(x) = F(t_1, \dots, x, \dots, t_k)^2 \quad 1 \le i \le k,$$
$$L \ll \sum_{p|W} \frac{\log(p)}{p} - \sum_{p} \frac{\log(p)}{p} - \log\left(\frac{R}{R}\right) \ll 1 + \sum_{p|W} \frac{\log p}{p} \ll \log D_0,$$
$$\mathfrak{S} = \prod_{p} \frac{p-1}{p-\gamma(p)} = \left(\prod_{p|W} \frac{p-1}{p}\right)\left(\prod_{p\not|W} \frac{p-1}{p-1}\right) = \frac{\varphi(W)}{W}.$$

Po k aplikacích Lemmatu 4 získáváme na místo hlavního členu

$$\frac{N}{W}\left(\frac{\varphi(W)^k\,(\log R)^k}{W^k} I_k(F) + O\left(\frac{F_{max}^2\,\varphi(W)^k\,(\log R)^{k-1}\,\log(D_0)}{W^k}\right)\right),$$

čehož chybovou část můžeme začlenit do celkového chybového členu.

□

Lemma 6: *Nechť $y_{r_1,\dots,r_k}$, F i F_{max} jsou stejně jako v Lemmatu 5. Potom*

$$S_2^{(m)} = \frac{\varphi(W)^k\,N\,(\log R)^{k+1}}{W^{k+1}\,\log N} J_k^{(m)}(F) + O\left(\frac{F_{max}^2\,\varphi(W)^k\,N\,(\log R)^k}{W^{k+1} D_0}\right),$$

kde

$$J_k^{(m)}(F) = \int_0^1 \cdots \int_0^1 \left(\int_0^1 F(t_1, \dots, t_k) dt_m\right)^2 dt_1 \dots dt_{m-1} dt_{m+1} \dots dt_k.$$

Důkaz: Pro dosazení do Lemmatu 2 pro sumu $S_2^{(m)}$ potřebujeme nejprve vyjádřit $y_{r_1,\dots,r_k}^{(m)}$. Pro $r_m = 1$ a součin přes všechny složky bezčtvercové a nesoudělné s W vezmeme hodnotu podle Lemma 3, v opačném případě požadujeme hodnotu nulovou.

$$y_{r_1,\dots,r_k}^{(m)} = \sum_{\gcd(u, W\prod_{i=1}^k r_i)=1} \frac{\mu(u)^2}{\varphi(u)} F\left(\frac{\log r_1}{\log R}, \dots, \frac{\log r_{m-1}}{\log R}, \frac{\log u}{\log R}, \frac{\log r_{m+1}}{\log R}, \dots, \frac{\log r_k}{\log R}\right) + \left(\frac{F_{max}\,\varphi(W)\,\log R}{W D_0}\right).$$

Vidíme, že situaci nemáme stejnou pro všech k rozměrů, proto nejdřív užijeme Lemma 4 v jedné podobě pro index m a následně v jiné podobě pro $k-1$ zbylých případů.

Stejně jako v situaci pro S_1 potřebujeme takovou funkci h, aby za spravných podmínek složila převrácenou hodnotu Eulerovy funkce, ale tentokrát je podmínkou nesoudělnost s $W\prod_{i=1}^{k} r_i$. Proto zvolíme

$$\gamma(p) = \begin{cases} 0, & p \mid W\prod_{i=1}^{k} r_i, \\ 1, & p \nmid W\prod_{i=1}^{k} r_i. \end{cases}$$

Pro L potom máme odhad

$$L \ll 1 + \sum_{p\mid W\sum_{i=1}^{k} r_i} \frac{\log p}{p} \ll \sum_{p>\log R} \frac{\log p}{p} + \sum_{\substack{p\mid W\sum_{i=1}^{k} r_i \\ p>\log R}} \frac{\log\log R}{\log R} \ll \log\log N.$$

Označíme

$$F^{(m)}_{r_1,\dots,r_k} = \int_0^1 F\left(\frac{\log r_1}{\log R},\dots,\frac{\log r_{m-1}}{\log R}, t_m, \frac{\log r_{m+1}}{\log R},\dots,\frac{\log r_k}{\log R}\right) dt_m.$$

Potom dostáváme

$$y^{(m)}_{r_1,\dots,r_k} = (\log R)\frac{\varphi(W)}{W}\left(\prod_{i=1}^{k}\frac{\varphi(r_i)}{r_i}\right) F^{(m)}_{r_1,\dots,r_k} + O\left(\frac{F_{max}\,\varphi(W)\,\log R}{W D_0}\right).$$

vyjádření $y^{(m)}_{r_1,\dots,r_k}$ dosadíme do vzorce pro $S_2^{(m)}$ z Lemmatu 2, přičemž členy, kdy má být hodnota nulová, ze sumy jenoduše vynecháme, čímž získáme

$$S_2^{(m)} = \frac{N}{\varphi(W)\,\log N}\left(\frac{\varphi(W)\,\log(R)}{W}\right)^2 \sum_{\substack{r_1,\dots,r_k \\ \forall i\ \gcd(r_i,W)=1 \\ \forall i\neq j\ \gcd(r_i,r_j)=1 \\ r_m=1}} \left(\prod_{i=1}^{k}\frac{\mu(r_i)^2\,\varphi(r_i)^2}{g(r_i)\,r_i^2}\right)\left(F^{(m)}_{r_1,\dots,r_k}\right)^2$$
$$+ O\left(\left(\frac{\varphi(W)F_{max}(\log R)}{W}\right)^2 \frac{\varphi(W)^{k-2}\,N\,(\log N)^{k-2}}{W^{k-1}\,D_0}\right) + O\left(\frac{N}{(\log N)^A}\right).$$

Tedy

$$S_2^{(m)} = \frac{\varphi(W)\,N\,(\log R)^2}{W^2\,\log N} \sum_{\substack{r_1,\dots,r_k \\ \forall i\ \gcd(r_i,W)=1 \\ \forall i\neq j\ \gcd(r_i,r_j)=1 \\ r_m=1}} \left(\prod_{i=1}^{k} \frac{\mu(r_i)^2\,\varphi(r_i)^2}{g(r_i)\,r_i^2}\right) \left(F^{(m)}_{r_1,\dots,r_k}\right)^2 + O\left(\frac{F_{max}^2\,\varphi(W)^k\,N\,(\log R)^k}{W^{k+1}\,D_0}\right).$$

Opět zkusíme upustit od podmínky nesoudělnosti r_i a r_j pro $i \neq j$. Proto si vyhodnotíme příspěvek r_i s faktorem větším než D_0, tentokrát jako

$$\begin{aligned}
&\ll \frac{N}{W} \sum_{p>D_0} \sum_{\substack{u_1,\dots,u_k<R \\ p\mid u_i,u_j \\ \forall i:\,\gcd(u_i,W)=1}} \left(\prod_{i=1}^{k} \frac{\mu(u_i)^2}{\varphi(u_i)}\right) F_{max}^2 \\
&\ll \frac{F_{max}^2\,N}{W} \sum_{p>D_0} \frac{1}{(p-2)^2} \left(\sum_{\substack{u<R \\ \gcd(u,W)=1}} \frac{\mu(u)^2}{\varphi(u)}\right)^k \\
&\ll \frac{F_{max}^2\,\varphi(W)^k\,N\,(\log N)^k}{W^{k+1}\,D_0}.
\end{aligned}$$

Opět ho tak můžeme začlenit do předchozího chybového členu.

Zbývá nám vyhodnotit samotnou sumu bez předchozí podmínky a přes $k-1$ dimenzí, neboť $r_m = 1$. Vezmeme proto

$$\sum_{\substack{r_1,\dots,r_{m-1},r_{m+1},\dots,r_k \\ \forall i\ \gcd(r_i,W)=1}} \left(\prod_{\substack{1\leq i\leq k \\ i\neq m}} \frac{\mu(r_i)^2\,\varphi(r_i)^2}{g(r_i)\,r_i^2}\right) \left(F^{(m)}_{R_1,\dots,R_k}\right)^2.$$

Abychom na situaci mohli užít Lemma 4, potřebujeme z funkce h složit $\frac{\varphi(r_i)^2}{g(r_i)r_i^2}$. Proto položíme

$$\gamma(p) = \begin{cases} 0, & p \mid W, \\ \frac{p^3-2p^2+p}{p^3-p^2-2p+1}, & p \nmid W, \end{cases}$$

Pro $p \nmid W$ totiž máme

$$h(p) = \frac{\gamma(p)}{p - \gamma(p)} = \frac{p^3 - 2p^2 + p}{(p^4 - p^3 - 2p^2 + p) - (p^3 - 2p^2 + p)} = \frac{p(p-1)^2}{p^4 - 2p^3} = \frac{(p-1)^2}{(p-2)p^2} = \frac{\varphi(p)^2}{g(p)p^2}.$$

Připomeňme, že funkce h je zcela multiplikativní, proto

$$h(r_i) = \prod_{p|r_i} h(p) = \begin{cases} 0, & \exists p | W, \\ \prod_{i=1}^{k} \frac{\varphi(r_i)^2}{g(r_i) r_i^2} = \frac{\varphi(r_i)^2}{g(r_i) r_i^2}, & \forall p \nmid W. \end{cases}$$

L vezmeme v tomto případě stejně jako při aplikaci lemmatu v obdobné situaci pro integral I_k.

Závěrem použijeme $(k-1)$-krát Lemma 4, což nám dá vyjádření

$$S_2^{(m)} = \frac{\varphi(W)^k N (\log R)^{k+1}}{W^{k+1} \log N} J_k^{(m)}(F) + O\left(\frac{F_{max}^2 \varphi(W)^k N (\log R)^k}{W^{k+1} D_0} \right),$$

kde

$$J_k^{(m)}(F) = \int_0^1 \cdots \int_0^1 \left(\int_0^1 F(t_1, \ldots, t_k) dt_m \right)^2 dt_1 \ldots dt_{m-1} dt_{m+1} \ldots dt_k.$$

□

2.5 Funkce vhodná pro velké k

Naší snahou je najít největší poměr mezi sumami S_2 a S_1, které máme vyjádřené pomocí integrálu funkce F. Jelikož je jasné, že konkrétní maximum nenajdeme, snažíme se omezit náš odhad zdola.

Jak jiz bylo zavedeno v Tvrzení 2, $\mathcal{S}$ značíme množinu všech Riemannovsky integrovatelných funkcí $F : [0,1]^k \mapsto \mathbb{R}$, které nabývají nulové hodnoty mimo množinu $\mathcal{R}_k =$

$\{(x_1, \ldots, x_k) \in [0,1]^k : \sum_{i=1}^k x_i \leq 1\}$ a s podmínkou nenulovosti $I_k(F)$ a $J_k^{(m)}(F)$ pro všechna m, kde

$$I_k(F) = \int_0^1 \cdots \int_0^1 F(t_1, \ldots, t_k)^2 \, dt_1 \cdots dt_k,$$
$$J_k^{(m)}(F) = \int_0^1 \cdots \int_0^1 \left(\int_0^1 F(t_1, \ldots, t_k) \right)^2 \, dt_1 \cdots dt_{m-1} dt_{m+1} \cdots dt_k.$$

Potom se snažíme najít spodní odhad

$$M_k = \sup_{F \in \mathcal{S}_k} \frac{\sum_{m=1}^k J_k^{(m)}(F)}{I_k(F)}.$$

Zvolíme F jako

$$F(t_1, \ldots, t_k) = \begin{cases} \prod_{i=1}^k g(kt_i) & pro \sum_{i=1}^k t_i \leq 1, \\ 0 & jinak. \end{cases}$$

Zde $g : [0, \infty] \mapsto \mathbb{R}$ je nějaká hladká funkce s nulovými hodnotami mimo úsek $[0, T]$. To nám výrazně zjednoduší situaci, neboť funkce je symetrická ve všech směrech, a proto můžeme hledat

$$M_k = \sup_{F \in \mathcal{S}_k} \frac{k J_k^{(1)}(F)}{I_k(F)}.$$

Očividnou komplikací při nahrazení F jako funkce k proměnných funkcí jedné proměnné $(g(u))$ je omezení nenulových hodnot funkce $F(t_1, \ldots, t_k)$ podmínkou $\sum_{i=1}^k t_i \leq 1$. Rádi bychom I_k a J_k vyjádřili pomocí obecného integrálu nějaké podoby funkce g přes celý předmětný interval $[0, T]$ ($[0, \frac{T}{k}]$ pro $g(kt)$), který můžeme vzhledem k nulovým hodnotam mimo tento interval ztotožnit s intervalem přes celý definiční obor $[0, \infty]$ (a neřešit tak vnitřní funkci mezi t a argumentem g, je-li v určitém smyslu rozumná).

Označíme si

$$\zeta = \int_{u \geq 0} g(u) \, du,$$
$$\gamma = \int_{u \geq 0} g(u)^2 \, du,$$
$$\xi = \int_{u \geq 0} u g(u)^2 \, du.$$

Jelikož I_k figuruje v jmenovateli M_k, potřebujeme horní odhad tohoto členu, což vzhledem k čtverci v integrandu splňuje integrace přes větší oblast. Proto

$$\begin{aligned} I_k &= \int_{\mathcal{R}_k} \cdots \int F(t_1,\ldots,t_k)^2 dt_1,\ldots,dt_k = \int_{\substack{0 \\ \sum_{i=1}^k t_i \le 1}}^{\frac{T}{k}} \cdots \int_0^{\frac{T}{k}} \prod_{i=1}^k g(kt_i)^2 dt_1,\ldots,dt_k \\ &\le \int_0^{\frac{T}{k}} \cdots \int_0^{\frac{T}{k}} \prod_{i=1}^k g(kt_i)^2 dt_1,\ldots,dt_k = \int_0^{\infty} \cdots \int_0^{\infty} \prod_{i=1}^k g(kt_i)^2 dt_1,\ldots,dt_k \\ &= \left(\int_0^{\infty} g(kt)^2 dt\right)^k = \left(\frac{1}{k}\int_0^{\infty} g(u)^2 du\right)^k = \left(\frac{\gamma}{k}\right)^k. \end{aligned}$$

Funkce g má nulové hodnoty mimo interval $[0,T]$, tudíž funkce $g(kt)$ je nulová pro argument t mimo interval $[0,\frac{T}{k}]$. Protože hledáme spodní odhad, pro integraci podle první proměnné zvolíme maximalní úsek ($[0,\frac{T}{k}]$), neboť další integrály mohou vzhledem ke kvadrátu nabývat již pouze kladných příspěvků. Pro zbylé integrace nám tak zbývá podmínka $\sum_{i=2}^k t_i \le 1-\frac{T}{k}$. Díky tomu nám podmínka omezeného součtu zbývá pouze pro integrační proměnné v symetrické situaci:

$$\begin{aligned} J_k &\ge \int_{\substack{0 \\ \sum_{i=2}^k t_i \le 1-\frac{T}{k}}}^{\frac{T}{k}} \cdots \int_0^{\frac{T}{k}} \left(\int_0^{\frac{T}{k}} \prod_{i=1}^k g(kt_i) dt_1\right)^2 dt_2,\ldots,dt_k \\ &= \int_{\substack{0 \\ \sum_{i=2}^k t_i \le 1-\frac{T}{k}}}^{\infty} \cdots \int_0^{\infty} \left(\int_0^{\infty} \prod_{i=1}^k g(kt_i) dt_1\right)^2 dt_2,\ldots,dt_k. \end{aligned}$$

Předpokládáme, že příbytek způsobený oblastí integrace nesplňující podmínku by byl malý, proto odhad rozdělíme na integrál bez podmínky a chybový člen E_k zahrnující pouze oblast porušující podmínku. Odhad rozepíšeme jako

$$\int_0^\infty \cdots \int_0^\infty \left(\int_0^\infty \prod_{i=1}^k g(kt_i) dt_1 \right)^2 dt_2, \ldots, dt_k$$
$$\sum_{i=2}^k t_i \leq 1 - \frac{T}{k}$$

$$= \int_0^\infty \cdots \int_0^\infty \left(\int_0^\infty \prod_{i=1}^k g(kt_i) dt_1 \right)^2 dt_2, \ldots, dt_k - \int_0^\infty \cdots \int_0^\infty \left(\int_0^\infty \prod_{i=1}^k g(kt_i) dt_1 \right)^2 dt_2, \ldots, dt_k$$
$$\sum_{i=2}^k t_i > 1 - \frac{T}{k}$$

$$= \left(\int_0^\infty g(kt_1)\, dt_1 \right)^2 \left(\int_0^\infty g(kt)^2\, dt \right)^{k-1} - \left(\int_0^\infty g(kt_1)\, dt_1 \right)^2 \int_0^\infty \cdots \int_0^\infty \prod_{i=2}^k g(kt_i)^2 dt_2, \ldots, dt_k$$
$$\sum_{i=2}^k t_i > 1 - \frac{T}{k}$$

$$= \left(\frac{1}{k} \int_0^\infty g(u)\, du \right)^2 \left(\frac{1}{k} \int_0^\infty g(u)^2\, du \right)^{k-1} - \left(\frac{1}{k} \int_0^\infty g(u)\, du \right)^2 \int_0^\infty \cdots \int_0^\infty \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k$$
$$\sum_{i=2}^k u_i > k - T$$

$$= \left(\frac{\zeta}{k} \right)^2 \left(\frac{\gamma}{k} \right)^{k-1} - \left(\frac{\zeta}{k} \right)^2 \left(\frac{1}{k} \right)^{k-1} \int_0^\infty \cdots \int_0^\infty \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k.$$
$$\sum_{i=2}^k u_i > k - T$$

To můžeme shrnout jako

$$J_k \geq \left(\frac{\zeta}{k} \right)^2 \left(\frac{\gamma}{k} \right)^{k-1} - E_k,$$

$$E_k = \left(\frac{\zeta}{k} \right)^2 \left(\frac{1}{k} \right)^{k-1} \int_0^\infty \cdots \int_0^\infty \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k, \tag{10}$$
$$\sum_{i=2}^k u_i > k - T$$

kde se dále snažíme ukázat, že E_k je dostatečně malé.

Protože hledáme spodní hranici maxima, muzeme zůžit množinu funkcí, pro něž extrém hledáme. Přidáme si požadavek pro g zahrnující poměr integrálu $ug(u)^2$ a $g(u)^2$, který označíme μ, ve tvaru

$$\mu = \frac{\xi}{\gamma} = \frac{\int_{u \geq 0} ug(u)^2\, du}{\int_{u \geq 0} g(u)^2\, du} < 1 - \frac{T}{k}. \tag{11}$$

Nyní označme $\eta = \frac{k-T}{k-1} - \mu$, přičemž

$$\eta = \frac{k-T}{k-1} - \mu > \frac{k-T}{k-1} - \left(1 - \frac{T}{k}\right) = \frac{k-T}{k(k-1)} > 0,$$
$$k - T = (\mu + \eta)(k-1).$$

Dále bychom potřebovali výraz $(k-1)\eta^2$ odhadnout zespoda (nachází se ve jmenovateli). Z nerovnosti $\mu < 1 - \frac{T}{k}$ vyjádříme $\mu = 1 - \frac{T}{k} - \epsilon$ pro $0 \leq \epsilon \leq 1$. Potom

$$(k-1)\eta^2 = \frac{(k-T)^2}{k^2(k-1)} + \epsilon^2(k-1) + 2\epsilon\frac{k-T}{k} = \frac{k-T}{k}\left(\frac{k-T}{k(k-1)} + 2\epsilon\right) + \epsilon^2 k - \epsilon^2.$$

Máme odhad

$$(k-1)\eta^2 \geq k\left(1 - \frac{T}{k} - \mu\right)^2, \tag{12}$$

neboť

$$\frac{(k-T)^2}{k^2(k-1)} \geq 0,$$
$$\frac{2(k-T)}{k} > \epsilon,$$
$$\frac{k-T}{k}\left(\frac{k-T}{k(k-1)} + 2\epsilon\right) \geq \epsilon^2.$$

Podmínku omezující oblast integrace přeformulujeme:

$$\sum_{i=2}^{k} u_i > (k-T),$$
$$\sum_{i=2}^{k} u_i > (k-1)(\mu+\eta),$$
$$\frac{\sum_{i=2}^{k} u_i}{k-1} > \mu + \eta,$$
$$\frac{1}{\eta}\left(\frac{\sum_{i=2}^{k} u_i}{k-1} - \mu\right) > 1,$$
$$1 < \eta^{-2}\left(\frac{\sum_{i=2}^{k} u_i}{k-1} - \mu\right)^2.$$

Pokud touto podmínkou vynásobíme integrand chybového integrálu, můžeme upustit od podmínky omezující oblast integrace, neboť ta je již zahrnuta ve výchozí nerovnosti. Takže

$$E_k < \left(\frac{\zeta}{k}\right)^2 \left(\frac{1}{k}\right)^{k-1} \int_0^\infty \cdots \int_0^\infty \eta^{-2} \left(\frac{\sum_{i=2}^k u_i}{k-1} - \mu\right)^2 \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k,$$

$$E_k < \zeta^2 k^{-k-1} \eta^{-2} \int_0^\infty \cdots \int_0^\infty \left(\frac{\sum_{i=2}^k u_i}{k-1} - \mu\right)^2 \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k.$$

Integrál bez omezení teď dokážeme lépe vyjádřit. Začneme roznásobením čtverce podle

$$\begin{aligned} &\int_0^\infty \cdots \int_0^\infty \left(\frac{\sum_{i=2}^k u_i}{k-1} - \mu\right)^2 \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k \\ &= \int_0^\infty \cdots \int_0^\infty \left(\frac{\sum_{2\le i,j\le k} u_i u_j}{(k-1)^2} - \frac{2\mu \sum_{i=2}^k u_i}{k-1} + \mu^2\right) \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k \end{aligned} \tag{13}$$

a vidíme, že až na členy s u_i^2 $(i = j)$ dokážeme vše vyjádřit pomocí hodnoty integrálu kvadrátu funkce g (integrálu znaceneho γ).

Pro začátek člen pouze s konstantou z vyjádření (13) vyhodnotíme jako

$$\int_0^\infty \cdots \int_0^\infty \mu^2 \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k = \mu^2 \int_0^\infty \cdots \int_0^\infty \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k = \mu^2 \gamma^{k-1}.$$

Připomeňme, že podle definice μ v rovnici (11) můžeme vyjádřit integrál ξ integrálem γ podle

$$\int_{u\ge 0} u g(u)^2 \, du = \mu \int_{u\ge 0} g(u)^2 \, du = \mu\gamma.$$

V prostředním členu z vyjádření (13) vidíme, že situace je symetrická pro všechna u_i a my tak můžeme na integrál nahlížet jako na $(k-1)$ případů integrálu pro jednu dimenzi

ve tvaru $ug(u)^2$ (integrál typu ξ) a pro ostatní ve tvaru $g(u)^2$ (integrál typu γ), proto

$$\begin{aligned}
&\int_0^\infty \cdots \int_0^\infty - \frac{2\mu \sum_{i=2}^k u_i}{k-1} \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k \\
&= \frac{-2\mu}{k-1} \int_0^\infty \cdots \int_0^\infty \sum_{i=2}^k u_i \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k \\
&= \frac{-2\mu}{k-1} \sum_{i=2}^k \left(\int_0^\infty \cdots \int_0^\infty u_i \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k \right) \\
&= \frac{-2\mu}{k-1}(k-1) \int_0^\infty \cdots \int_0^\infty u_2 \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k \\
&= \frac{-2\mu}{k-1}(k-1) \left(\mu\gamma\, \gamma^{k-2} \right) = -2\mu^2 \gamma^{k-1}.
\end{aligned}$$

Poslední a nejsložitější člen rozdělíme na případy $i \neq j$, kdy je závislost stále linearní, pouze na dvou dimenzích (ve dvou směrech integrál typu ξ a ve zbylých typu γ), a na případy kvadratické závislosti v situaci $i = j$, ve smyslu

$$\begin{aligned}
&\int_0^\infty \cdots \int_0^\infty \frac{\sum_{2 \leq i,j \leq k} u_i u_j}{(k-1)^2} \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k \\
&= (k-1)^{-2} \int_0^\infty \cdots \int_0^\infty \sum_{\substack{2 \leq i,j \leq k \\ i \neq j}} u_i u_j \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k \\
&+ (k-1)^{-2} \int_0^\infty \cdots \int_0^\infty \sum_{i=2}^k u_i^2 \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k.
\end{aligned}$$

případ pro různé i a j vyřešíme ve stejném gardu jako předchozí člen. Uvědomíme si,

že takových dvojic i a j (mezi 2 a k) je právě $(k-1)(k-2)$, proto

$$\begin{aligned}
&(k-1)^{-2}\int_0^\infty \cdots \int_0^\infty \sum_{\substack{2\le i,j\le k\\ i\neq j}} u_i u_j \prod_{i=2}^{k} g(u_i)^2 du_2, \ldots, du_k \\
&= (k-1)^{-2} \sum_{\substack{2\le i,j\le k\\ i\neq j}} \left(\int_0^\infty \cdots \int_0^\infty u_i u_j \prod_{i=2}^{k} g(u_i)^2 du_2, \ldots, du_k \right) \\
&= (k-1)^{-2}(k-1)(k-2)\int_0^\infty \cdots \int_0^\infty u_2 u_3 \prod_{i=2}^{k} g(u_i)^2 du_2, \ldots, du_k \\
&= (k-1)^{-2}(k-1)(k-2)\left((\mu\gamma)^2 (\gamma)^{k-3} \right) = \frac{(k-2)\mu^2\gamma^{k-1}}{k-1}.
\end{aligned}$$

Pro situaci s kvadratickou závislostí si vystačíme s horním odhadem, kdy využijeme vlastnosti funkce g, která je pro argument větší než T nulová. Proto odhadneme jeden činitel u nejhorším případem T (v případě většího u bude nulový činitel ve formě produktu funkce $g(u_i)$), čímž získáváme

$$u_i^2 g(u_i)^2 \le T u_i g(u_i)^2.$$

integrál tak odhadneme podle

$$\begin{aligned}
&(k-1)^{-2}\int_0^\infty \cdots \int_0^\infty \sum_{i=2}^{k} u_i^2 \prod_{i=2}^{k} g(u_i)^2 du_2, \ldots, du_k \\
&= (k-1)^{-2} \sum_{i=2}^{k} \left(\int_0^\infty \cdots \int_0^\infty u_i^2 \prod_{i=2}^{k} g(u_i)^2 du_2, \ldots, du_k \right) \\
&= (k-1)^{-2}(k-1) \left(\int_0^\infty \cdots \int_0^\infty u_2^2 \prod_{i=2}^{k} g(u_i)^2 du_2, \ldots, du_k \right) \\
&\le (k-1)^{-2}(k-1) \left(\int_0^\infty \cdots \int_0^\infty T u_2 \prod_{i=2}^{k} g(u_i)^2 du_2, \ldots, du_k \right) \\
&= \frac{T}{k-1}\left(\mu\gamma\gamma^{k-2}\right) = \frac{\mu T \gamma^{k-1}}{k-1}.
\end{aligned}$$

Složením všech přesně vyjádřených členů získáváme

$$\mu^2\gamma^{k-1} - 2\mu^2\gamma^{k-1} + \frac{(k-2)\mu^2\gamma^{k-1}}{k-1} = \frac{\mu^2\gamma^{k-1}\left((k-1) - 2(k-1) + (k-2)\right)}{k-1} = \frac{-\mu^2\gamma^{k-1}}{k-1}.$$

Celý chybový integrál E_k (z rovnice (10)) pak odhadneme jako

$$\begin{aligned} E_k &< \zeta^2 k^{-k-1}\eta^{-2}\int_0^\infty \cdots \int_0^\infty \left(\frac{\sum_{i=2}^k u_i}{k-1} - \mu\right)^2 \prod_{i=2}^k g(u_i)^2 du_2, \ldots, du_k \\ &= \zeta^2 k^{-k-1}\eta^{-2}\left(\frac{-\mu^2\gamma^{k-1}}{k-1} + \frac{\mu T\gamma^{k-1}}{k-1}\right) = \frac{\zeta^2\mu\gamma^{k-1}\left(T-\mu\right)}{\eta^2(k-1)k^{k+1}} \\ &\leq \frac{\zeta^2\mu\gamma^{k-1}T}{\eta^2(k-1)k^{k+1}}. \end{aligned}$$

Celý integrál J_k potom jako

$$J_k \geq \frac{\zeta^2\gamma^{k-1}}{k^{k+1}} - \frac{\zeta^2\mu\gamma^{k-1}T}{\eta^2(k-1)k^{k+1}} = \frac{\zeta^2\gamma^{k-1}}{k^{k+1}}\left(1 - \frac{\mu T}{\eta^2(k-1)}\right).$$

Výsledkem naší maximalizace je tak odhad

$$\frac{kJ_k}{I_k} \geq \frac{\zeta^2\gamma^{k-1}k^{-k}}{\gamma^k k^{-k}}\left(1 - \frac{\mu T}{\eta^2(k-1)}\right) = \frac{\zeta^2}{\gamma}\left(1 - \frac{\mu T}{\eta^2(k-1)}\right).$$

Ten si za cenu snížení maxima zjednodušíme pro následné užití díky nerovnostem $\mu < 1$ (podle našeho požadavku z (11)) a $(k-1)\eta^2 \geq k\left(1 - \frac{T}{k} - \mu\right)^2$ (12) do tvaru

$$\frac{kJ_k}{I_k} \geq \frac{\zeta^2}{\gamma}\left(1 - \frac{\mu T}{\eta^2(k-1)}\right) \geq \frac{\zeta^2}{\gamma}\left(1 - \frac{T}{k\left(1 - \frac{T}{k} - \mu\right)^2}\right),$$

tedy

$$\frac{kJ_k}{I_k} \geq \frac{\left(\int_0^\infty g(u)du\right)^2}{\int_0^\infty g(u)^2 du}\left(1 - \frac{T}{k\left(1 - \frac{T}{k} - \mu\right)^2}\right).$$

potřebovali bychom proto najít maximální $\int_0^T g(u)du$ při zachování $\int_0^T g(u)^2du = \gamma$ a $\int_0^T ug(u)^2du = \mu\gamma$. Tuto extremální úlohu můžeme vyjádřit funkcí

$$\begin{aligned} L(u, g(u), g'(u)) &= \int_0^T g(u)du - \alpha\left(\int_0^T g(u)^2du - \gamma\right) - \beta\left(\int_0^T ug(u)^2du - \mu\gamma\right) \\ &= \int_0^T \left(g(u) - \alpha g(u)^2 - \beta ug(u)^2 + \alpha\gamma + \beta\mu\gamma\right) du. \end{aligned}$$

Podle Euler–Lagrangeovy rovnice $\frac{\partial L}{\partial g(u)} - \frac{d}{du}\frac{\partial L}{\partial g'(u)} = 0$ a podle $\frac{\partial L}{\partial g'(u)} = 0$ získáváme pro $u \in [0, T]$ vztahy

$$\begin{aligned} \frac{\partial}{\partial g(u)}\left(g(u) - \alpha g(u)^2 - \beta ug(u)^2 + \alpha\gamma + \beta\mu\gamma\right) &= 0, \\ 1 - 2\alpha g(u) - 2\beta ug(u) &= 0, \\ g(u) &= \frac{1}{2\alpha + 2\beta u}. \end{aligned}$$

Z předchozího je zřejmé, že vynásobení funkce kladnou konstantou nezmění maximalizovaný poměr. Tudíž

$$g(u) = \frac{C}{2\alpha + 2\beta u} = \frac{C}{2\alpha\left(1 + \frac{\beta}{\alpha}u\right)}$$

a při volbě $C := 2\alpha$ a $A := \frac{\beta}{\alpha}$ získáváme jednodušší formu hledané funkce

$$g(u) = \frac{1}{1 + Au} \qquad (\forall u \in [0, T]).$$

Pro tento tvar nám vychází integrály

$$\begin{aligned}
\int_0^T g(u)du &= \int_0^T \frac{1}{1+Au}du = \left[\frac{\log(1+Au)}{A}\right]_0^T = \frac{\log(1+AT)}{A},\\
\int_0^T g(u)^2du &= \int_0^T (1+Au)^{-2}\,du = \left[\frac{1}{A}\frac{-1}{1+Au}\right]_0^T = \frac{1}{A}\left(1-\frac{1}{1+AT}\right),\\
\int_0^T ug(u)^2du &= \int_0^T u\,(1+Au)^{-2}\,du = \left[\frac{1}{A^2}\left(\log(1+Au)+\frac{1}{1+Au}\right)\right]_0^T\\
&= \frac{1}{A^2}\left(\log(1+AT)+\frac{1}{1+AT}-1\right).
\end{aligned}$$

Stále nám zbyvají dva parametry, proto zvolíme $T := \frac{e^A-1}{A}$, což nám usnadní situaci vzhledem k rovnostem $1+AT = e^A$ a $\log(1+AT) = \log(e^A) = A$. Výše spočtené integrály a jejich poměr μ vyjádříme s touto volbou T jako

$$\begin{aligned}
\zeta &= \int_0^T g(u)\,du = 1,\\
\gamma &= \int_0^T g(u)^2\,du = \frac{1}{A}\left(1-e^{-A}\right),\\
\xi &= \int_0^T ug(u)^2\,du = \frac{1}{A^2}\left(A+e^{-A}-1\right),\\
\mu &= \frac{\int_0^T ug(u)^2\,du}{\int_0^T g(u)^2\,du} = \frac{A+e^{-A}-1}{A\left(1-e^{-A}\right)} = \frac{1}{1-e^A}-\frac{1}{A}.
\end{aligned}$$

Pro samotný hlavní odhad pak máme nerovnost

$$\frac{kJ_k}{I_k} \geq \frac{A}{1-e^{-A}}\left(1-\frac{T}{k\left(1-\frac{T}{k}-\mu\right)^2}\right),$$

který si dále upravíme s využitím vztahu

$$\begin{aligned}
\frac{A}{1-e^{-A}} &\geq A,\\
T = \frac{e^A-1}{A} &\leq \frac{e^A}{A},\\
\mu = \frac{1}{1-e^{-A}}-\frac{1}{A},&\\
1-\frac{T}{k}-\mu \geq 1-\frac{e^A}{Ak}-\frac{e^A}{e^A-1}+\frac{1}{A} = \frac{1}{A}-\frac{e^A}{Ak}-\frac{e^A-1-e^A}{e^A-1}+ &\geq \frac{1}{A}\left(1-\frac{e^A}{k}-\frac{A}{e^A-1}\right)
\end{aligned}$$

do podoby

$$\frac{kJ_k}{I_k} \geq A\left(1 - \frac{Ae^A}{k\left(1 - \frac{A}{e^A-1} - \frac{e^A}{k}\right)^2}\right).$$

Zvolíme $A := \log k - 2\log\log k$, potom

$$e^A = \frac{k}{\log^2 k},$$
$$e^A - 1 = \frac{k - \log^2 k}{\log^2 k},$$
$$\frac{1}{e^A - 1} = \frac{\log^2 k}{k - \log^2 k},$$
$$\frac{A}{e^A - 1} = \frac{\log^2 k\,(\log k - 2\log\log k)}{k - \log^2 k} = \frac{\log^3 k - 2\log k \log\log k}{k - \log^2 k} \leq \frac{\log^3 k}{k},$$
$$1 - \frac{T}{k} - \mu \geq \frac{1}{A}\left(1 - \frac{\log^3 k}{k} - \frac{1}{\log^2 k}\right),$$

takže požadavek $\mu < 1 - \frac{T}{k}$ (11) evidentně platí.

Po dosazení dostáváme

$$\frac{kJ_k}{I_k} \geq (\log k - 2\log\log k)\left(1 - \frac{\log k - 2\log\log k}{\log^2 k\left(1 - \frac{A}{e^A-1} - \frac{e^A}{k}\right)^2}\right)$$
$$\geq \log k - 2\log\log k - \log k\left(\frac{\log k}{\log^2 k\left(1 - \frac{A}{e^A-1} - \frac{e^A}{k}\right)^2}\right).$$

Jmenovatel ve zlomku vypadá blízký $\log^2 k$, proto si vyjádřeme rozdíl od jedné v koeficientu pro $\log^2 k$ jako

$$\left(1 - \frac{A\log^2 k}{k - \log^2 k} - \frac{1}{\log^2 k}\right)^2 - 1 = \frac{A^2\log^4 k}{(k - \log^2 k)^2} + \frac{1}{\log^4 k} - \frac{2A\log^2 k}{k - \log^2 k} - \frac{2}{\log^2 k} + \frac{A}{k - \log^2 k}$$
$$= \frac{A^2\log^4 k}{(k - \log^2 k)^2} + \frac{1}{\log^2 k}\left(\frac{1}{\log^2 k} - 2\right) + \frac{A}{k - \log^2 k}\left(1 - 2\log^2 k\right) \leq \frac{A^2\log^4 k}{(k - \log^2 k)^2}$$
$$\leq \frac{\log^6 k}{(k - \log^2 k)^2} \ll 1.$$

A protože

$$\begin{aligned} \log^2 k &\leq O(1), \\ -\log^2 k &\leq -2\log^2 k + O(1), \\ -\log^2 k &\leq -2(\log^2 k + O(1)), \\ -\frac{\log^2 k}{\log^2 k + O(1)} &\leq -2, \end{aligned}$$

máme pro dostatečně velké k

$$M_k \geq \frac{kJ_k}{I_k} \geq \log k - 2\log\log k - 2.$$

2.6 Funkce vhodná pro malé k

Symetričnost vůči jednotlivým prvkům splnitelné množiny $\mathcal{H}$ je stěžejní pro uchopitelnost celé metody, proto pro malá k, pro která je postup z předchozí kapitoly nepoužitelný, si zvolíme funkci F ve tvaru symetrického polynomu. Omezením na polynomy samozřejmě zmenšujeme množinu možných funkcí a tím i velmi pravděpodobně zhoršíme odhad našeho extrému, nicméně polynomy splňují hladkost a snadno se pracuje s jejich obecnými tvary. Funkci F definujeme jako

$$F(t_1, \ldots, t_k) = \begin{cases} P(t_1, \ldots, t_k) & \text{pro } (t_1, \ldots, t_k) \in \mathcal{R}_k \\ 0 & \text{jinak,} \end{cases}$$

kde

$$P = \sum_{i=1}^{d} a_i (1 - P_1)^{b_i} P_2^{c_i} = \sum_{i=1}^{d} a_i Q_i,$$

přičemž P_j jsou čistě mocninné polynomy podle

$$P_j = \sum_{i=1}^{k} t_i^j.$$

Pro $Q_i = (1-P_1)^{b_i} P_2^{c_i}$ dokážeme hodnotu integrálu podle následujícího lemma.

Lemma 7: *Nechť* $P_j = \sum_{i=1}^{k} t_i^j$ *je symetrický polynom a* $\mathcal{R}_k = \{(x_1, \ldots, x_k) \in [0,1]^k : \sum_{i=1}^{k} x_i \leq 1\}$, *potom*

$$\int_{\mathcal{R}_k} \cdots \int (1-P_1)^a P_j^b dt_1, \ldots, dt_k = \frac{a!}{(a+jb+k)!} G_{b,j}(k),$$

kde

$$G_{b,j}(x) = b! \sum_{r=1}^{b} \binom{x}{r} \sum_{\substack{b_1,\ldots,b_k \geq 1 \\ \sum_{i=1}^{r} b_i = b}} \prod_{i=1}^{r} \frac{(jb_i)!}{b_i!}$$

je polynom stupně b.

Důkaz: Přímo mocněný polynom P_j rozepíšeme podle multinomické věty

$$P_j^b = \left(\sum_{i=1}^{k} t_i^j\right)^b = \sum_{\substack{b_1,\ldots,b_k \in \mathbb{N}_0 \\ \sum_{i=1}^{k} b_i = b}} \binom{b}{b_1, \ldots, b_k} \prod_{i=1}^{k} (t_i^j)^{b_i} = \sum_{\substack{b_1,\ldots,b_k \\ \sum_{i=1}^{k} b_i = b}} \frac{b!}{\prod_{i=1}^{k} b_i!} \prod_{i=1}^{k} t_i^{jb_i}.$$

Po dosažení P_j^b i P_1 do vychozího výrazu získáme

$$\int_{\mathcal{R}_k} \cdots \int \left(1 - \sum_{i=1}^{k} t_i\right)^a \sum_{\substack{b_1,\ldots,b_k \\ \sum_{i=1}^{k} b_i = b}} \frac{b!}{\prod_{i=1}^{k} b_i!} \prod_{i=1}^{k} t_i^{jb_i}\ dt_1, \ldots, dt_k$$

$$= \sum_{\substack{b_1,\ldots,b_k \\ \sum_{i=1}^{k} b_i = b}} \frac{b!}{\prod_{i=1}^{k} b_i!} \int_{\mathcal{R}_k} \cdots \int \left(1 - \sum_{i=1}^{k} t_i\right)^a \prod_{i=1}^{k} t_i^{jb_i} dt_1, \ldots, dt_k.$$

Podiváme-li se na integrál z pohledu jedné proměnné (bez újmy na obecnosti t_1) a zvolíme-li substituci $v = \frac{t_1}{1-\sum_{i=2}^{k} t_i}$, dostáváme

$$\begin{aligned}
&\int_0^{1-\sum_{i=2}^{k} t_i} \left(1-\sum_{i=1}^{k} t_i\right)^a \prod_{i=1}^{k} t_i^{jb_i} dt_1 \\
&= \left(1-\sum_{i=2}^{k} t_i\right)^a \left(\prod_{i=2}^{k} t_i^{jb_i}\right) \int_0^{1-\sum_{i=2}^{k} t_i} \left(\frac{1-\sum_{i=1}^{k} t_i}{1-\sum_{i=2}^{k} t_i}\right)^a t_1^{jb_1} dt_1 \\
&= \left(1-\sum_{i=2}^{k} t_i\right)^a \left(\prod_{i=2}^{k} t_i^{jb_i}\right) \int_0^{1-\sum_{i=2}^{k} t_i} \left(1-\frac{t_1}{1-\sum_{i=2}^{k} t_i}\right)^a t_1^{jb_1} dt_1 \\
&= \left(1-\sum_{i=2}^{k} t_i\right)^a \left(\prod_{i=2}^{k} t_i^{jb_i}\right) \int_0^{1} (1-v)^a \left(v\left(1-\sum_{i=2}^{k} t_i\right)\right)^{jb_1} \left(1-\sum_{i=2}^{k} t_i\right) dv \\
&= \left(1-\sum_{i=2}^{k} t_i\right)^{a+jb_1+1} \left(\prod_{i=2}^{k} t_i^{jb_i}\right) \int_0^{1} (1-v)^a v^{jb_1} dv.
\end{aligned}$$

V integrálu vidíme podobu s Eulerovým integrálem prvního druhu (Beta funkci), který má obecně tvar $\int_0^1 x^n(1-x)^m dx = \frac{n!m!}{(n+m+1)!} = B(n+1, m+1)$ a proto

$$\left(1-\sum_{i=2}^{k} t_i\right)^{a+jb_1+1} \left(\prod_{i=2}^{k} t_i^{jb_i}\right) \int_0^{1} (1-v)^a v^{jb_1} dv = \left(1-\sum_{i=2}^{k} t_i\right)^{a+jb_1+1} \left(\prod_{i=2}^{k} t_i^{jb_i}\right) \frac{a!(jb_1)!}{(a+jb_1+1)!}$$

Po k-násobném použití předchozího principu získáváme celkově

$$\sum_{\substack{b_1,\ldots,b_k \\ \sum_{i=1}^{k} b_i = b}} \frac{b!}{\prod_{i=1}^{k} b_i!} \frac{a! \prod_{i=1}^{k} (jb_i)!}{\prod_{i=1}^{k} (a+jb_i+1)!} = \frac{a!b!}{(a+jb+k)!} \sum_{\substack{b_1,\ldots,b_k \\ \sum_{i=1}^{k} b_i = b}} \prod_{i=1}^{k} \frac{(jb_i)!}{b_i!}.$$

Tímto postupem maximalizace celkové funkce F s využitím současných znalosti se nevyhneme numerickým výpočtům, takže nám přijde vhod rozdělit sumu přes $b_1, \ldots, b_k$ podle počtu nenulových b_i. Počet možností, jak vybrat r nenulových prvků $b_1, \ldots, b_k$, můžeme vyjádřit kombinačním číslem $\binom{k}{r}$, proto

$$\sum_{\substack{b_1,\ldots,b_k \\ \sum_{i=1}^{k} b_i = b}} \prod_{i=1}^{k} \frac{(jb_i)!}{b_i!} = \sum_{r=1}^{b} \binom{k}{r} \sum_{\substack{b_1,\ldots,b_r \geq 1 \\ \sum_{i=1}^{k} b_i = b}} \prod_{i=1}^{k} \frac{(jb_i)!}{b_i!}.$$

□

Zbývá nám vyhodnotit integrály I_k a $J_k^{(m)}$ z celkového polynomu P.

Lemma 8: *Nechť* $F(t_1,\dots,t_k) = P(t_1,\dots,t_k)$ *pro argument z* $\mathcal{R}_k = \{(x_1,\dots,x_k) \in [0,1]^k : \sum_{i=1}^k x_i \le 1\}$ *a* $F(t_1,\dots,t_k) = 0$ *jinak. Dále* $P = \sum_{i=1}^d a_i Q_i$, *přičemž* $Q_i = (1-P_1)^{b_i} P_2^{c_i}$ *s* $a_i \in \mathbb{R}$ *a* $b_i, c_i \in \mathbb{N}_0$, *kde* $P_1 = \sum_{i=1}^k t_i$ *a* $P_2 = \sum_{i=1}^k t_i^2$. *Potom pro* $1 \le m \le k$ *platí*

$$I_k(F) = \sum_{1\le i,j\le d} a_i a_j \frac{(b_i+b_j)!\, G_{c_i+c_j,2(k)}}{(b_i+b_j+2c_i+2c_j+k)!},$$

$$J_k^{(m)}(F) = \sum_{1\le i,j\le d} a_i a_j \sum_{c_1'=0}^{c_i}\sum_{c_2'=0}^{c_j} \binom{c_i}{c_1'}\binom{c_j}{c_2'} \frac{\gamma_{b_i,b_j,c_i,c_j,c_1',c_j'}\, G_{c_i'+c_j',2(k-1)}}{(b_i+b_j+2c_i+2c_j+k)!},$$

kde

$$\gamma_{b_i,b_j,c_i,c_j,c_1',c_j'} = \frac{b_i!b_j!(2c_i-2c_1')!(2c_j-2c_2')!(b_i+b_j+2c_i+2c_j-2c_1'-2c_2'+2)!}{(b_i+2c_i-2c_1'+1)!\,(b_j+2c_j-2c_2'+1)!},$$

$$G_{b,j}(x) = b! \sum_{r=1}^{b} \binom{x}{r} \sum_{\substack{b_1,\dots,b_k\ge 1\\ \sum_{i=1}^r b_i = b}} \prod_{i=1}^{r} \frac{(jb_i)!}{b_i!}.$$

Důkaz: Podle Lemmatu 7

$$\begin{aligned}
I_k(F) &= \int_{\mathcal{R}_k}\cdots\int P^2 dt_1,\dots,dt_k = \int_{\mathcal{R}_k}\cdots\int \left(\sum_{i=1}^d a_i Q_i\right)^2 dt_1,\dots,dt_k \\
&= \int_{\mathcal{R}_k}\cdots\int \sum_{1\le i,j\le d} a_i Q_i a_j Q_j dt_1,\dots,dt_k \\
&= \int_{\mathcal{R}_k}\cdots\int \sum_{1\le i,j\le d} a_i (1-P_1)^{b_i} P_2^{c_i} a_j (1-P)^{b_j} P_2^{c_j} dt_1,\dots,dt_k \\
&= \sum_{1\le i,j\le d} \int_{\mathcal{R}_k}\cdots\int a_i a_j (1-P)^{b_i+b_j} P_2^{c_i+c_j} dt_1,\dots,dt_k \\
&= \sum_{1\le i,j\le d} a_i a_j \frac{(b_i+b_j)!}{(b_i+b_j+2c_i+2c_j+k)!\,()!} G_{c_i+c_j,2}(k).
\end{aligned}$$

Vzhledem k symetričnosti vůči t_i si opět můžeme dovolit ztotožnit $J_k^{(m)}(F)$ s $J_k^{(1)}(F)$. Proto vyjádřeme vnitřní integrál zapomoci binomické věty

$$\begin{aligned}
\int_0^{1-\sum_{j=2}^k t_j} a_i Q_i dt_1 &= a_1 \int_0^{1-\sum_{i=2}^k t_i} (1-P_1)^{b_1} P_2^{c_1} dt_1 \\
&= a_1 \int_0^{1-\sum_{i=2}^k t_i} \left(1-\sum_{j=1}^k t_j\right)^{b_1} \left(\sum_{j=1}^k t_j^2\right)^{c_1} dt_1 \\
&= a_1 \int_0^{1-\sum_{i=2}^k t_i} \left(1-\sum_{j=1}^k t_j\right)^{b_1} \left(t_1^2+\sum_{j=2}^k t_j^2\right)^{c_1} dt_1 \\
&= a_1 \int_0^{1-\sum_{i=2}^k t_i} \left(1-\sum_{j=1}^k t_j\right)^{b_1} \sum_{c'=0}^{c} \binom{c}{c'} \left(t_1^2\right)^{c-c'} \left(\sum_{j=2}^k t_j^2\right)^{c'} dt_1 \\
= a_1 \sum_{c'=0}^{c} \binom{c}{c'} \left(\sum_{j=2}^k t_j^2\right)^{c'} &\left(1-\sum_{j=2}^k t_j\right)^{b_1} \int_0^{1-\sum_{i=2}^k t_i} \left(1-\frac{t_1}{1-\sum_{j=2}^k t_j}\right)^{b_1} (t_1)^{2c-2c'} dt_1,
\end{aligned}$$

kde stejně jako v Lemmatu 7 zvolíme substituci $v = \frac{t_1}{1-\sum_{j=2}^k t_j}$. S použitím Beta funkce dostáváme

$$\begin{aligned}
&a_1 \sum_{c'=0}^{c} \binom{c}{c'} \left(\sum_{j=2}^k t_j^2\right)^{c'} \left(1-\sum_{j=2}^k t_j\right)^{b_1} \int_0^1 (1-v)^{b_1} \left(v\left(1-\sum_{j=2}^k t_j\right)\right)^{2c-2c'} \left(1-\sum_{j=2}^k t_j\right) dv \\
=&a_1 \sum_{c'=0}^{c} \binom{c}{c'} \left(\sum_{j=2}^k t_j^2\right)^{c'} \left(1-\sum_{j=2}^k t_j\right)^{b_i+2c-2c'+1} \int_0^1 (1-v)^{b_i} v^{2c-2c'} dv \\
=&a_1 \sum_{c'=0}^{c} \binom{c}{c'} \left(\sum_{j=2}^k t_j^2\right)^{c'} \left(1-\sum_{j=2}^k t_j\right)^{b_i+2c-2c'+1} \frac{b_i!(2c-2c')!}{(b_i+2c-2c'+1)!}.
\end{aligned}$$

Umocněním součtu $P = \sum_{i=1}^d a_i Q_i$ na druhou získáváme celý integrand pro zbylých

$(k-1)$ vnějších integrací v $J_k^{(1)}$, neboli

$$\left(\int_0^1 F(t_1,\dots,t_k)dt_1\right)^2 = \left(\sum_{i=1}^d a_1 \int_0^{1-\sum_{i=2}^k t_i} (1-P_1)^{b_1} P_2^{c_1} dt_1\right)^2$$

$$= \sum_{1\le i,j\le d} a_i a_j \sum_{c_1'=0}^{c_i}\sum_{c_2'=0}^{c_j} \binom{c_i}{c_1'}\binom{c_j}{c_2'} \left(\sum_{j=2}^k t_j^2\right)^{c_1'+c_2'} \left(1-\sum_{j=2}^k t_j\right)^{b_i+b_j+2c_i+2c_j-2c_1'-2c_2'+2}$$
$$\cdot \frac{b_i!b_j!(2c_i-2c_1')!(2c_j-2c_2')!}{(b_i+2c_i-2c_1'+1)!(b_j+2c_j-2c_2'+1)!}.$$

Na sumy $\sum_{i=2}^k t_i$ a $\sum_{i=2}^k t_i^2$ můžeme nahlížet jako na P_j z Lemmatu 7 s počtem dimenzí o jedna menší (tedy $k-1$). A tak použijeme toto lemma násobně na poslední výsledek. Celkové vyjádření $J_k^{(m)}(F)$ tak můžeme psát jako

$$J_k^{(m)}(F) = \int_0^1 \cdots \int_0^1 \left(\int_0^1 F(t_1,\dots,t_k)dt_1\right)^2 dt_2\dots dt_k$$

$$= \sum_{1\le i,j\le d} a_i a_j \sum_{c_1'=0}^{c_i}\sum_{c_2'=0}^{c_j} \binom{c_i}{c_1'}\binom{c_j}{c_2'} \frac{b_i!b_j!(2c_i-2c_1')!(2c_j-2c_2')!}{(b_i+2c_i-2c_1'+1)!(b_j+2c_j-2c_2'+1)!}$$
$$\cdot \int\limits_{\sum_{l=2}^k t_l\le 1} \cdots \int \left(\sum_{l=2}^k t_l^2\right)^{c_1'+c_2'} \left(1-\sum_{l=2}^k t_l\right)^{b_i+b_j+2c_i+2c_j-2c_1'-2c_2'+2} dt_2\dots dt_k$$

$$= \sum_{1\le i,j\le d} a_i a_j \sum_{c_1'=0}^{c_i}\sum_{c_2'=0}^{c_j} \binom{c_i}{c_1'}\binom{c_j}{c_2'} \frac{b_i!b_j!(2c_i-2c_1')!(2c_j-2c_2')!}{(b_i+2c_i-2c_1'+1)!(b_j+2c_j-2c_2'+1)!}$$
$$\cdot \frac{b_i+b_j+2c_i+2c_j-2c_1'-2c_2'+2}{b_i+b_j+2c_i+2c_j+k+1} G_{c_1'+c_2',2}(k-1).$$

□

Na vyjádření z Lemmatu 8 se můžeme dívat jako na kvadratické formy (viz 1.3) s vektorem $\mathbf{a} = (a_1,\dots,a_d)$ a s maticemi rozměrů $d\times d$, konkrétně matici A_1 pro $I_k(F)$ definovanou po prvcích podle

$$A_1(i,j) = \frac{(b_i+b_j)!\, G_{c_i+c_j,2(k)}}{(b_i+b_j+2c_i+2c_j+k)!}$$

a A_2 pro $J_k^{(m)}(F)$ podle vzorce

$$A_2(i,j) = \sum_{c_1'=0}^{c_i}\sum_{c_2'=0}^{c_j} \binom{c_i}{c_1'}\binom{c_j}{c_2'} \frac{\gamma_{b_i,b_j,c_i,c_j,c_1',c_j'}\, G_{c_i'+c_j',2(k-1)}}{(b_i+b_j+2c_i+2c_j+k)!,}.$$

Proto můžeme numericky spočítat matice pro vybranou sadu $Q = (1 - P_1)^b P_2^c$ a poté najít extrém v rámci jejich lineárních kombinací (s koeficienty $\mathbf{a} = (a_1, \ldots, a_d)$).

Lemma 9: *Nechť A_1 a A_2 jsou symetrické a pozitivně definitní matice realných čísel. Potom hodnota maxima poměrů*

$$\frac{\mathbf{a}^T A_2 \mathbf{a}}{\mathbf{a}^T A_1 \mathbf{a}}$$

odpovídá největšímu vlastnímu číslu $(A^{-1}A_2)$, a to právě tehdy, když $\mathbf{a}$ je vlastní vektor odpovídající tomuto vlastnímu číslu.

Důkaz: Nechť $l = \sqrt{\mathbf{a}^T A_1 \mathbf{a}}$ a vektor $\mathbf{a}' = \frac{\mathbf{a}}{l}$. Potom

$$\mathbf{a}'^T A_1 \mathbf{a}' = \frac{\mathbf{a}^T A_1 \mathbf{a}}{l^2} = 1,$$

přičemž poměr

$$\frac{\mathbf{a}'^T A_2 \mathbf{a}'}{\mathbf{a}'^T A_1 \mathbf{a}'} = \frac{l^2 \mathbf{a}^T A_2 \mathbf{a}}{l^2 \mathbf{a}^T A_1 \mathbf{a}} = \frac{\mathbf{a}^T A_2 \mathbf{a}}{\mathbf{a}^T A_1 \mathbf{a}}$$

se nezmění. Proto můžeme bez újmy na obecnosti uvažovat vektor $\mathbf{a}$ takový, že $\mathbf{a}^T A_1 \mathbf{a} = 1$.

V důsledku se snažíme maximalizovat výraz $\mathbf{a}^T A_2 \mathbf{a}$ s vazbou $\mathbf{a}^T A_1 \mathbf{a} - 1 = 0$. Metodou Lagrangeových multiplikátorů získáváme Lagrangeovu funkci

$$\mathcal{L}(\mathbf{a}, \lambda) = \mathbf{a}^T A_2 \mathbf{a} - \lambda \left(\mathbf{a}^T A_1 \mathbf{a} - 1 \right) = \mathbf{a}^T \left(A_2 - \lambda A_1 \right) \mathbf{a} + \lambda.$$

S využitím symetrie matice $(A_2 - \lambda A_1)$ dojdeme při rozepsání matice $\left(\mathbf{a}^T \left(A_2 - \lambda A_1 \right) \mathbf{a} \right)$ a derivaci podle jednotlivých prvků $\mathbf{a}$ k rovnosti

$$\frac{\partial L}{\partial \mathbf{a}} = \left(2A_2 - 2\lambda A_1 \right) \mathbf{a} = \mathbf{o}.$$

Díky faktu, že matice A_1 je pozitivně definitní, získáme po upravách

$$\begin{aligned} 2A_2\mathbf{a} - 2\lambda A_1\mathbf{a} &= \mathbf{o}, \\ A_2\mathbf{a} &= \lambda A_1\mathbf{a}, \\ A_1^{-1}A_2\mathbf{a} &= \lambda\mathbf{a}. \end{aligned}$$

Tudíž λ musí být vlastní číslo $\left(A_1^{-1}A_2\right)$ a zároveň

$$\begin{aligned} \mathbf{a}^T A_2\mathbf{a} &= \lambda\mathbf{a}^T A_1\mathbf{a}, \\ \lambda &= \frac{\mathbf{a}^T A_2\mathbf{a}}{\mathbf{a}^T A_1\mathbf{a}}. \end{aligned}$$

Proto maxima nabývá předmětný poměr pro největší vlastní číslo a jeho hodnota je rovna tomuto číslu.

□

Pro druhý bod Tvrzení 3 s $k = 105$ omezil Maynard zkoumané polynomy stupněm 11, tedy na lineární kombinace členů $Q = (1 - P_1)^b P_2^c$ takových, pro které $b + 2c \leq 11$. Jelikož takových členů je 42 možných, stačí najít největší vlastní číslo odpovídající matice $A^{-1}A_2$ velikosti 42×42, které činí přibližně 4.0020697. A proto

$$M_{105} > 4.$$

Pro první bod Tvrzení 3 s $k = 5$ autor vybral hodnoty

i	1	2	3	4
a_i	1	$\frac{7}{10}$	$\frac{1}{14}$	$-\frac{3}{14}$
b_i	1	2	0	1
c_i	1	0	1	0

neboli polynom

$$P = (1 - P_1)P_2 + \frac{7}{10}(1 - P_1)^2 + \frac{1}{14}P^2 - \frac{3}{14}(1 - P_1),$$

který ukazuje, že

$$M_5 \geq \frac{1417255}{708216} > 2.$$

3 Závěr

Uvedli jsme si jasný příklad ukazující, že v teorii čísel je neustále prostor pro nové objevy. O prvočíslech máme i nadále nedostatek znalostí. Ač nabývá objem poznatků, týkajících se například prvočísel specifického tvaru, jedná se často o nedokázané hypotézy, popřípadě maji výsledky jen omezený dopad. Metody sít se věnují i základním vlastnostem prvočísel jako celku.

Významným poznatkem ohledně obecného rozložení prvočísel ve velkých číslech je znalost limes inferior rozdílu dvou po sobě jdoucích prvočísel, přičemž nejsilnějším možným závěrem je v tomto ohledu $\liminf_{n\to\infty}(p_{n+1} - p_n) = 2$, což odpovídá slavné domněnce o nekonečném počtu prvočíselnych dvojic.

S předpokladem Elliott–Halberstamovy domněnky předložili nerovnost $\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 16$ již Goldston, Pintz a Yıldırım, ale první nepodmíněný závěr co do konečné hodnoty pro limes inferior dvou po sobě jdoucích prvočísel uvedl v roce 2013 Yitang Zhang, kdy dokázal tvrzení $\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 7 \times 10^7$. Spoluprací v ramci projektu *Polymath8a* byl Zhanguv závěr značně vylepšen na $\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 4680$.

Článek Jamese Maynarda *Small gaps between primes*, jak jsme si ukázali v této práci, posouvá hranici ještě níže, a to konkrétně jako $\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 600$ nepodmíněně a $\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 12$ podmíněné platností Elliott–Halberstamovy domněnky.

Nicméně ani to není aktuální nejsilnější mez, neboť na *Polymath8a* navázal projekt *Polymath8b*, který, s užitím metod popsaných na stránkách výše a rozsáhlejších numerických výpočtů, než jaké původně provedl Maynard, podal nerovnost $\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 246$ a pod takzvanou zobecněnou formou Elliott–Halberstamovou domněnkou (viz [3, Tvrzeni 2.6]) dokonce $\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 6$.

Projekt *Polymath8b* vylepšil i další Maynardův výsledek ($\liminf_{n\to\infty}(p_{n+m} - p_n) \ll m^3 e^{4m}$) na $\liminf_{n\to\infty}(p_{n+m} - p_n) \ll me^{\left(4-\frac{24}{181}\right)m}$. Přitom před Maynardovým článkem byl pro limes inferior rozdílu m následujících prvočísel znám asymptotický odhad jen s předpokladem Elliott–Halberstamovy domněnky, konkrétně $\liminf_{n\to\infty}(p_{n+m} - p_n) \ll m^3 e^{2m}$ podané trojicí Goldston, Pintz a Yıldırım. Pod touto podmínkou posunul *Polymath8b* mez na me^{2m}.

Reference

[1] James Maynard. Small gaps between primes. *Annals of Mathematics*, 2014. arXiv:1311.4600.

[2] Henryk Iwaniec John Friedlander. *Opera de Cribro*. American Mathematical Society, 2010.

[3] D. H. J. Polymath. Variants of the selberg sieve, and bounded intervals containing many primes. 2014. arXiv:1407.4897.

[4] D. A. Goldston, S.W. Graham, J. Pintz, and C.Y. Yildirim. Small gaps between products of two primes. 2006. arXiv:math/0609615.

[5] Jack Dalton. An exposition of Selberg's sieve. *Graduate College Dissertations and Theses*, 720, 2017. https://scholarworks.uvm.edu/graddis/720.

[6] Alex Kontorovich. Levels of distribution and the affine sieve. 2014. arXiv:1406.1375.

[7] Andrew Sutherland. Sieve theory and small gaps between primes: Introduction, 2015. Explicit Methods in Number Theory.

[8] Andrew Sutherland. Narrow admissible tuples. http://math.mit.edu/ primegaps/.

[9] Yitang Zhang. Bounded gaps between primes. *Annals of Mathematics*, 2014. http://dx.doi.org/10.4007/annals.2014.179.3.7.

[10] Elchin Hasanalizade. The Goldston-Pintz-Yıldırım sieve and some applications. Master's thesis, KTH Royal Institute of Technology, 2012.

[11] ČVUT v Praze. Metodický pokyn č. 1/2009 O dodržování etických principů při přípravě vysokoškolských závěrečných prací.