1. Einführung

Zentrale Fragestellung:

Wieviele Gruppen der Ordnung $n \in \mathbb{N}$ gibt es (bis auf Isomorphie)?

DEF | $f(n) := \#$ Iso-Klassen v. Gruppen d. Ord. n |

Z.T. kann man diese Frage leicht beantworten:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
f(n)	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14

Ist p eine Primzahl, so ist $f(p) = 1$.

(Alle Gruppen von Primzahlordnung sind zyklisch.)

Genaues:
$f(n) = 1$ gdw.
$ggT(n, \varphi(n)) = 1$
Eulers φ-Funktion:
$\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$

Für große Zahlen wird es aber teilweise sehr schwer, $f(n)$ zu bestimmen. Ein „Rekord":

$$f(2^{10}) = 49\ 487\ 365\ 422 \quad \text{[Besche, Eick, O'Brien]}$$

($2^{10} = 1024$)

Beobachtungen: a) $f(n)$ ist erratisch: $f(2^{10}) \approx 50$ Milliarden, $f(2^{10}-3) = 1$

b) Primzahlpotenzen haben „hohe" Werte

Wg. a) scheint eine exakte Formel für f unwahrscheinlich.
Wir suchen also nach Abschätzungen für f.

Wie mißt man Größe?

DEF Sei $f : \mathbb{N} \to \mathbb{R}$ eine Funktion. Wir schreiben

$$f(n) \leq \mathcal{O}(g(n))$$

(„Landau-$\mathcal{O}$") Analog „$\geq$".

für eine Funktion $g : \mathbb{N} \to \mathbb{R}$ falls ein $M \in \mathbb{R}_+$ existiert s.d. für alle $n > n_0 \in \mathbb{N}$

$$f(n) \leq M(g(n))$$

gilt.

Bsp.

- Beschränkte Funktionen f sind genau jene, die $f(n) \leq \mathcal{O}(1)$ erfüllen.
- P ein Polynom, dann $P(n) \leq \mathcal{O}(e^n)$.

Zurück zu den Beobachtungen. b) weckt die Hoffung, daß das Problem leichter wird, wenn man zunächst Primzahlpotenzen betrachtet. Im Verlauf des Seminares werden wir folgendes beweisen:

$$f(p^m) \geqslant p^{2/27\, m^3 - \mathcal{O}(m^2)} \quad [\text{Higman}]$$

Präzise nach obiger Def: $-\log_p f(p^m) + \frac{2}{27} m^3 \geq \mathcal{O}(m^2)$

$$f(p^m) \leq p^{2/27\, m^3 + \mathcal{O}(m^{8/3})} \quad [\text{Sims}]$$

Um von Primzahlpotenzen zu allg. $n \in \mathbb{N}$ zurückzukehren benötigen wir ein Maß der „arithmetischen Größe":

DEF Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung

$$n = \prod_{i=1}^{\ell(n)} p_i^{\alpha_i}.$$

Dann definiere

$$\mu(n) := \max_{i=1}^{\ell(n)} \alpha_i \quad \text{und} \quad \lambda(n) := \sum_{i=1}^{\ell(n)} \alpha_i$$

$\mu(n)$ ist NICHT die Möbius-Funktion

Damit ist $\mu(p^m) = m$. Wir kommen zum Satz von Pyber

$$f(n) \leq n^{2/27 \, \mu(n)^2 + O(\mu(n)^{5/3})}$$

Vergleiche mit Sims oberer Schranke

den wir in einem Spezialfall beweisen wollen.

---

2. Einfache / Elementare Schranken

DEF Eine Menge $M \neq \emptyset$ mit einer Operation $\cdot : M \times M \to M$ heißt Magma.

Ein Magma mit einem neutralen Element $1_M \in M$ heißt unitäres Magma. d.h. $1_M \cdot m = m = m \cdot 1_M \; \forall m \in M$

Ein Magma, indem das Assoziativitätsgesetz gilt, heißt Halbgruppe.

Ein Magma M mit der Eigenschaft, daß für alle $m, n \in M$ Elemente $x, y \in M$ existieren, so daß $m \cdot x = n$ und $y \cdot m = n$ („Links- / Rechtsinverse" oder -Teiler) gilt, heißt Quasi-Gruppe.

(Ein unitäres Magma, das zugleich auch Halb- und Quasi-Gruppe ist, ist eine Gruppe.)

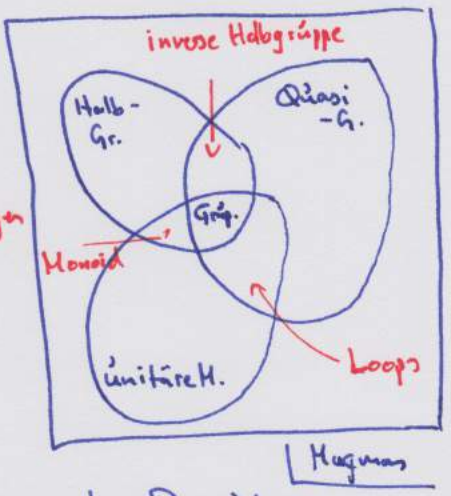
Jedes Magma wird durch seine Cayley-Tafel beschrieben, d.h. durch seine Multiplikationstafel.

D.h.

$$f_{\text{Magma}}(n) \leq n^{n^2}$$

n = # Magmen der Ordnung n

n^2 = # aller möglichen $n \times n$ Tafeln mit n verschiedenen Einträgen



Ein Isomorphismus von Magmas ist eine Bijektion der unterliegenden Mengen. Legen wir uns auf eine feste Trägermenge $\{0, \ldots, n-1\}$ fest, müssen wir nur die $n!$ Permutationen beachten. Es ergibt sich:

$$\frac{n^{n^2}}{n!} \leq f_{\text{Magma}}(n) \leq n^{n^2}$$

Übergang zu unitären Magmas schränkt uns kaum weiter ein. Es ist lediglich die Spalte und die Zeile des neutralen Elements festgelegt, d.h.

$$\frac{n^{(n-1)^2}}{(n-1)!} \leq f_{\text{unit. Mag.}}(n) \leq n^{(n-1)^2}$$

Das reflektiert den Fakt, daß man durch Hinzufügen eines einzigen Elementes ein Magma zu einem unitären Magma machen kann.

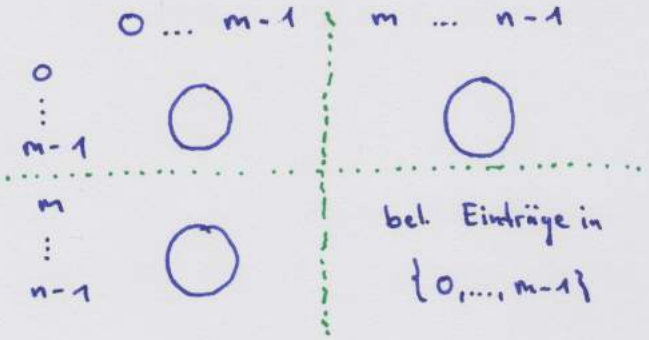
Wir sind also noch weit von den Schranken für Gruppen entfernt!

Halbgruppen: Wir beweisen eine untere Schranke durch die Konstruktion vieler nicht-isomorpher Halbgruppen.

Benenne die Elemente von M mit $\{0, \dots, n-1\}$ und setze

$$i \cdot j = \begin{cases} 0 & \text{wenn } i \text{ oder } j < m \\ \text{bel.} < m & \text{sonst} \end{cases},$$

d.h. die Multiplikationstafel ist von der Gestalt



M ist assoziativ: $\forall\, i,j,k \in M \quad i \cdot (\underbrace{j \cdot k}_{\in \{0,\dots,m-1\}}) = 0 = (\underbrace{i \cdot j}_{\in \{0,\dots,m-1\}}) \cdot k$.

Es gilt also für jedes $m \in M$: Setze $m := n^{1-\frac{1}{2}\varepsilon}$

$$f_{\text{Halbgruppe}}(n) \geq \frac{m^{(n-m)^2}}{n!} = n^{(1-\frac{1}{2}\varepsilon)\cdot(n-n^{1-\frac{1}{2}\varepsilon})^2} \geq n^{(1-\varepsilon)n^2}$$

$n!$: Kümmert sich um die Isomorphie

für alle $\varepsilon > 0$ und ab genügend großen $n \in \mathbb{N}_0$. (genügend groß für obiges Einsetzen)

Trotz Assoziativität verbleiben wir sehr dicht an n^{n^2}!

Die nächste Hoffnung ist Invertierbarkeit, also Quasi-Gruppen.

Genaueres Resultat:

$$f_{\text{Halbgr.}}(n) = \left(\sum_{t=1}^{n} g_n(t)\right)(1+O(1))$$

$$g_n(t) = \binom{n}{t} t^{1+(n-t)^2}$$

mit derselben Idee.

LEMMA Ein Magma M ist genau dann eine Quasi-Gruppe, wenn seine Multiplikationstafel ein Lateinisches Quadrat ist.

d.h. ein „boxenfreies Sudoku", jede Zahl kommt in jeder Zeile und Spalte genau einmal vor.

$*$ Ang.: M ist eine Quasi-Gruppe. In der Spalte von $i \in M$ taucht $j \in M$ auf, da es ein $x \in M$ gibt, s.d. $x \cdot i = j$ gilt. (Analog für Zeilen mit $i \cdot y = j$). Umkehrung klar. □

Leider ist die Zahl der Lateinischen Quadrate der Größe n ein Mysterium; es ist keine Asymptotik bekannt. Aber:

$$n^{\frac{1}{2}n^2 - \mathcal{O}(n)} \leq f_{\text{Quasi-Gruppen}}(n) \leq n^{n^2} \quad [\text{M. Hall}]$$

Also reicht auch Invertierbarkeit nicht für eine signifikante Senkung der Anzahl aus. Man muß alle drei besprochenen Eigenschaften gemeinsam betrachten, d.h. Gruppen.

SATZ (Elementare obere Schranke)

$$f(n) \leq n^{n\lambda(n)}$$

← Viel kleines als n^{n^2}!

Wir verwenden den Satz von Lagrange & den Satz von Cayley.

$H \leq G \Rightarrow |G| = |G:H| \cdot |H|$ (Satz von Lagrange)

$|G| = n \Rightarrow G \cong \bar{G} \leq \mathrm{Sym}(n)$. (Satz von Cayley)

Definiere $d(G) :=$ minimale Größe eines Erzeugendensystems von G, den Rang von G.

LEMMA Es gilt $d(G) \leq \lambda(n)$, $n = |G|$.

Sei $G = G_r \wedge G_{r-1} \wedge \dots \wedge G_1 \wedge \{1\} = G_0$ eine maximale Kette ineinander enthaltener Untergruppen von G. Wähle für jedes $i \in \{1, \dots, r\}$ $g_i \in G_i \setminus G_{i-1}$.

Dann gilt $\langle g_1, \dots, g_i \rangle = G_i$; wäre $\langle g_1, \dots, g_i \rangle < G_i$ könnte man die Kette verfeinern.

Ins. ist $r \geq d(G)$. Nach Lagrange gilt

$$|G| = \prod_{i=1}^{r} \underbrace{|G_i : G_{i-1}|}_{\geq 2} \quad \left(\geq 2^r \right)$$

Weiterhin muß $r \leq \lambda(n)$ gelten, denn $\lambda(n)$ ist die maximale Länge eines nicht trivialen Produktes von n.

□

* Beweis d. Satzes

Nach dem Satz v. Cayley ist $G \leq \mathrm{Sym}(|G|)$. (Bis auf Isomorphie.)

Also:

$f(n) \leq$ # Untergruppen der Ordnung n von $\mathrm{Sym}(n)$ (UGn könnten isomorph sein.)

$\leq$ # Untergruppen von $\mathrm{Sym}(n)$, die von $\lambda(n)$ Elementen erzeugt werden (nach Lemma umfaßt das alle Ordn. n UGn)

$\leq$ # Teilmengen von $\mathrm{Sym}(n)$ mit $\lambda(n)$ Elementen

$= (n!)^{\lambda(n)} \leq n^{n\lambda(n)}$

□