Kombinatorik

Vorlesung

Sommersemester 2000

Johannes Waldmann, Institut für Informatik
Universität Leipzig, joe@informatik.uni-leipzig.de

Kapitel 1

Überblick

1.1 (Un–)Ordnung

6. April

C eine Klasse von Objekten, $\leq$ eine "Teilobjekt"–Relation auf C, P eine Eigenschaft von Objekten.

Oft gilt: in jedem genügend großen $Y \in C$ gibt es ein großes $X \leq Y$ mit $P(X)$.

für alle $n \in \mathbb{N}$
existiert $m \in \mathbb{N}$
für alle $Y \in C$
wenn $|Y| \geq m \Rightarrow$
existiert $X \leq Y$
$|X| \geq n$ und $P(X)$.

Philosophisch gesagt: es gibt keine beliebig große Unordnung.

Ob das Prinzip gilt oder nicht, hängt natürlich von der Klasse C, der Relation $\leq$ und der Eigenschaft P ab. Wir untersuchen das an vielen Beispielen.

Eines gibts hier schon: der Dirichletsche Schubfachschluß:

Für jede Abbildung $f : \{1 \dots a\} \to \{1 \dots b\}$ existiert ein y mit $|f^{-1}(y)| \geq \lceil a/b \rceil$.

Das ist anschaulich klar, Beweis: wenn nicht, dann wäre für alle y: $|f^{-1}(y)| < \lceil a/b \rceil$, aber weil das eine ganze Zahl ist, heißt das sogar $|f^{-1}(y)| < a/b$. Es muß aber $a = |\bigcup f^{-1}(y)| = \sum |f^{-1}(y)| < b \cdot a/b$ sein, Widerspruch.

Bringen wir das auf die prinzipielle Form: Die Klasse C besteht aus partiellen Abbildungen $f : \mathbb{N} \to \{1 \dots b\}$, wir sagen $g \leq f$, wenn g eine Einschränkung von f ist, und nennen $|\operatorname{domain} f|$ (Anzahl der Elemente im Definitionsbereich) die Größe von f. Die interessante Eigenschaft $P(f)$ ist dann $|\operatorname{range}(f)| = 1$.

Den Schubfachschluß brauchen wir demnächst wieder in der Ramsey–Theorie.

1.2 Themen der Vorlesung

6. April

- Ramsey–Theorie
  - klassische Ramsey–Zahlen
  - Ramsey–Zahlen für Hypergraphen, für Nicht–Cliquen
  - Ramsey–Aussagen in der Geometrie
  - Ramsey–Aussagen in der Arithmetik (Satz von van der Waerden)
- Wohl–Quasi–Ordnungen
  - WQOs auf Bäumen (Satz von Kruskal)
  - Rekursive Pfad–Ordnungen
  - WQOs auf Graphen (Theorie von Robertson/Seymour)
- Muster in unendlichen Wörtern
  - Fixpunkte von Homomorphismen
  - Sturmsche Wörter
  - D0L–Sprachen
  - Vermeidbare Muster in Wörtern
  - Burnside–Probleme

(Wahrscheinlich die Kapitel WQOs und Muster vertauschen.)

Kulturelle Notizen:

Es geht um Wörter, Bäume, Graphen.

Um endliche und unendliche Strukturen.

Um diskrete Mathematik und theoretische Informatik.

Historisch gesehen, spielt das meiste zwischen Anfang und Mitte unseres Jahrhunderts. Das kann man schon “klassisch” nennen.

Die Betrachtung von Mustern in Wörtern ist tatsächlich ein Ursprung für die Theorie der Formalen Sprachen. Diese ist damit eines der ältesten Gebiete der Informatik.

1.3 Beispiele (zu einigen Themen)

6. April

- Ramsey–Theorie
  - klassische Ramsey–Zahlen

    Von 6 Leuten kennen sich entweder irgendwelche drei paarweise, oder irgendwelche drei paarweise nicht.

    Die Zahlen $1, \ldots, 65$ sind mit 4 Farben gefärbt. Dann gibt es gleichfarbige a, b, c mit $a + b = c$.
  - Ramsey–Aussagen in der Geometrie

    Für alle n: existiert m: Aus jeder Anordnung von m Punkte in der Ebene (in allgemeiner Lage) kann man n Punkte auswählen, die ein konvexes Polygon bilden. (Untersuche für $n = 4$ oder $n = 5$.)
  - Ramsey–Aussagen in der Arithmetik:

    van der Waerdens Beweis der Baudetschen Vermutung: Für alle c, l: existiert m: Jede c–Färbung von $\{1, \ldots, m\}$ enthält einfarbige arithmetische Folge der Länge l. (Untersuche für $c = 2, l = 3$.)
- Wohl–Quasi–Ordnungen
  - WQOs auf Wörtern und Bäumen (Satz von Kruskal)

    Welche Primzahlen haben diese Eigenschaft: Egal, welche Ziffern man aus ihrer Dezimaldarstellung streicht, man erhält nie eine Primzahl.

    Beispiel: 2, 3, 5, 7, 11, 19, 41, 61, 89, 409, ..., 6469, ..., 66600049, ...

    Das gleiche für Quadratzahlen: 1, 4, 9, 25, ..., 7888885568656, ...

    Beide Mengen sind endlich!

    (Kasten Bier für explizite Angabe der zweiten Menge!)
- Muster in unendlichen Wörtern
  - Sturmsche Wörter

    Wir zeichnen eine Gerade durch den Nullpunkt mit Anstieg $1/\phi = (\sqrt{5} - 1)/2$ und schreiben auf, wie sie jeweils das Gitter schneidet (horizontal oder vertikal). (Sie geht durch keinen weiteren Gitterpunkt, weil der Anstieg irrational ist.) Das ergibt ein unendliches Wort

    $$f = VHVVHVHVVHVVHVHVVHVH\ldots$$
  - Fixpunkte von Homomorphismen

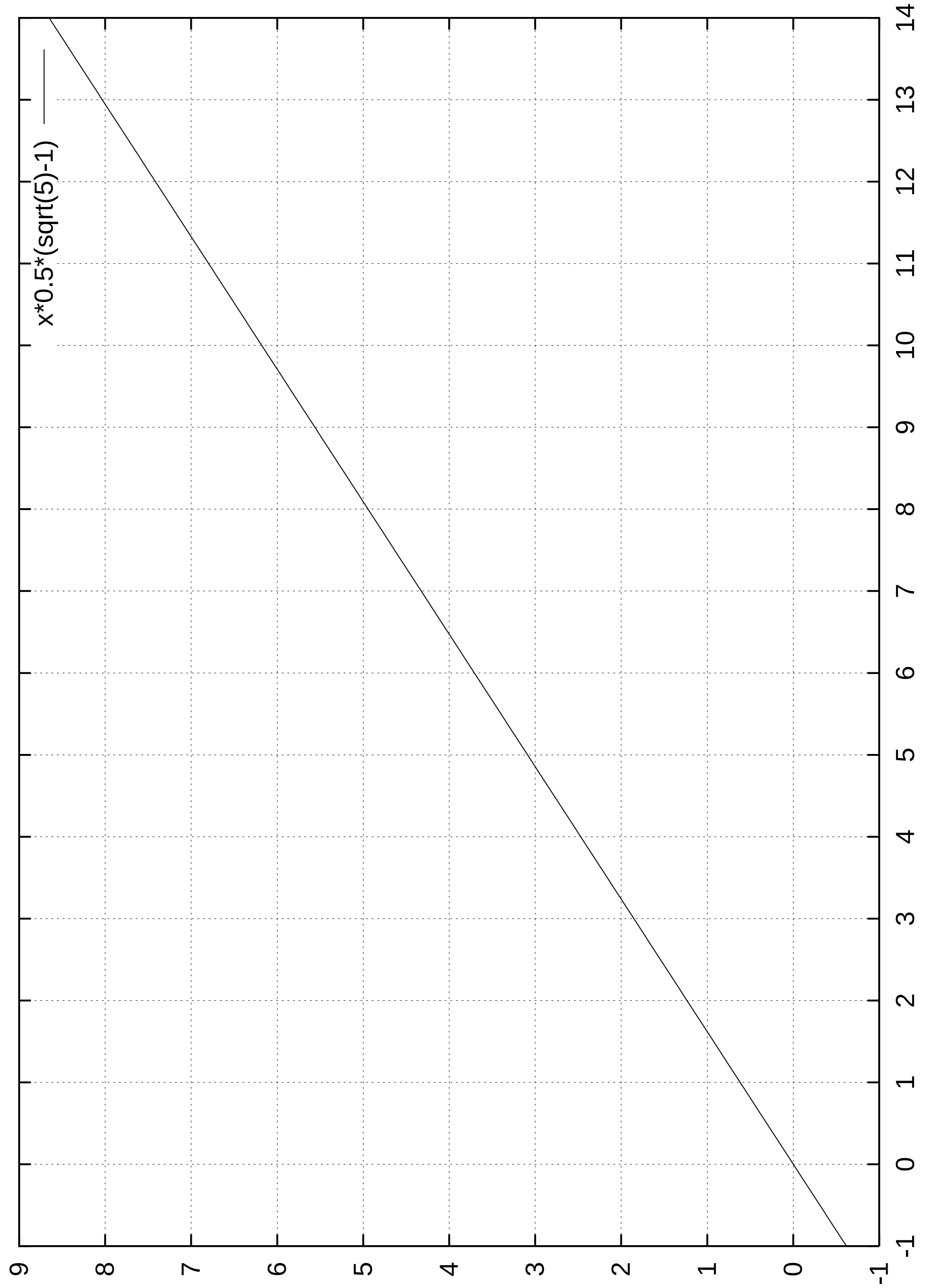
    In diesem Wort steht vor jedem H ein V. Wir können also Paare VH zusammenfassen und durch einen neuen Buchstaben A ersetzen. Ergibt

    $$g = AVAAVAVAAVAA\ldots$$

    Das ist wieder das Wort f, aber mit A statt V und V statt H. Das heißt: f ist der Grenzwert

    $$\lim h^n(V) \quad \text{mit} \quad h : V \mapsto VH, H \mapsto V$$

- Vermeidbare Muster in Wörtern
  Das Wort f enthält Quadrate und Kuben, aber keinen Faktor x^4.



Inhaltsverzeichnis

Literaturverzeichnis

[AZ98] Martin Aigner and Günter M. Ziegler. *Proofs from The Book*. Springer, 1998.

[BN98] Franz Baader and Tobias Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.

[Bol79] Belá Bollobás. *Graph Theory*. Springer, 1979.

[CK97] Christian Choffrut and Juhani Karhumäki. *Combinatorics of Words*, pages 329–428. Volume 1 of Rozenberg and Salomaa [RS97], 1997.

[Die96] Reinhard Diestel. *Graphentheorie*. Springer, 1996. http://www.math.uni-hamburg.de/home/diestel/books/graph.theory/.

[dLV99] Aldo de Luca and Stefano Varricchio. *Finiteness and Regularity in Semingroups and Formal Languages*. Springer, 1999.

[Fre98] Güther Frei. Zum gedenken an bartel leendert van der waerden. *Elemente der Mathematik*, 53:133–138, 1998. http://link.springer.de/link/service/journals/00017/.

[GO97] Jacob E. Goodman and Joseph O'Rourke, editors. *Handbook of Discrete and Computational Geometry*. CRC Press, Boca Raton, 1997.

[GR78] Ron L. Graham and B. L. Rothschild. *Ramsey Theory*, pages 80–99. Volume 17 of Rota [Rot78], 1978.

[Gra97] Ron L. Graham. *Euclidean Ramsey Theory*, pages 153–166. In Goodman and O'Rourke [GO97], 1997.

[Gro96] Jerry Grossman. The erdös number project. http://www.acs.oakland.edu/~grossman/erdoshp.html, 1996.

[GRS90] Graham, Rothschild, and Spencer. *Ramsey Theory*. John Wiley and Sons, 1990.

[Hal89] Rudolf Halin. *Graphentheorie*. Akademie–Verlag Berlin/Wissenschaftliche Buchgesellschaft Darmstadt, 1989.

[HK97] Tero Harju and Juhani Karhumäki. *Morphisms*, pages 439–510. Volume 1 of Rozenberg and Salomaa [RS97], 1997.

[Hof98] Paul Hoffman. *The Man Who Loved Only Numbers*. Fourth Estate, London, 1998.

[Klo94] Ton Kloks. *Treewidth—Computations and Approximations*, volume 842 of *Lecture Notes in Computer Science*. Springer, 1994.

[Knu98] Donald Erwin Knuth. *The Art of Computer Programming*, volume 3: Sorting and Searching. Addison-Wesley, 1998. http://www-cs-staff.stanford.edu/~uno/taocp.html.

[Lot97a] M. Lothaire. *Algebraic Combinatorics on Words*. http://www-igm.univ-mlv.fr/~berstel/Lothaire/, 1997.

[Lot97b] M. Lothaire. *Combinatorics on Words*. Cambridge Mathematical Library. Cambridge University Press, 1997.

[OR00] John J. O'Connor and Edmund F. Robertson. The MacTutor History of Mathematics Archive. http://www-groups.dcs.st-and.ac.uk:80/~history/, 2000.

[Rot78] Gian-Carlo Rota, editor. *Studies in Combinatorics*, volume 17 of *Studies in Mathematics*. The Mathematical Association of America, 1978.

[RS97] G. Rozenberg and A. Salomaa, editors. *Handbook of Formal Languages*. Springer, 1997.

[vdW98] Bartel L. van der Waerden. Wie der beweis der baudetschen vermmutung gefunden wurde. *Elemente der Mathematik*, 53:139–148, 1998. http://link.springer.de/link/service/journals/00017/.

[Win00] Martin Winkler. Happy end problem. http://www.crosswinds.net/~martinwinkler/happy_end.html, 2000.

1.4 Bezeichnungen

Zahlen

Die Menge der natürlichen Zahlen ist $\mathbb{N} = \{0, 1, \ldots\}$. Jede natürliche Zahl *ist* die Menge aller kleineren Zahlen: $0 = \emptyset, 1 = \{0\} = \{\emptyset\}, 2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$.

Mengen

Die Anzahl der Elemente einer endlichen Menge M ist $|M|$. Beispiel: $|\emptyset| = 0$.

Für eine Menge M und eine Zahl n: $\binom{M}{n} := \{T \mid T \subseteq M, |T| = n\}$.

Das sieht absichtlich so aus wie ein Binomialkoeffizient, denn $\left|\binom{M}{n}\right| = \binom{|M|}{n}$.

Beispiel: $\binom{\{a,b,c\}}{2} = \{\{a, b\}, \{a, c\}, \{b, c\}\}$

Graphen

Ein *Graph* G ist ein Paar (V, E). V ist eine endliche Menge, die Elemente von V heißen *Knoten* (englisch: *vertex*). E ist eine endliche Menge $\subseteq \binom{V}{2}$. Die Elemente von E heißen *Kanten* (englisch: *edge*).

P_n ist ein *Weg* (englisch: *path*) auf n Knoten.

C_n ist ein *Kreis* (englisch: *circle*) auf n Knoten.

K_n ist eine *Clique* auf n Knoten: jeder Knoten ist mit jedem verbunden.

bis hier am 13. April

Ein Graph ohne Kanten heißt *unabhängig*. Die Zahl n selbst bezeichnet einen unabhängigen Graph mit n Knoten.

Ein Graph heißt *zusammenhängend*, wenn je zwei Knoten durch einen Weg verbunden sind.

Ein Graph heißt *Baum*, wenn er zusammenhängend und kreisfrei ist.

Übung: Für Zahlen r und t mit $2r \leq t$: der *Kneser–Graph* $\mathsf{KG}(r, t)$ hat die Knotenmenge $V = \binom{t}{r}$ und die Kanten $E = \{xy \mid x, y \in V, x \cap y = \emptyset\}$. Der *Petersen–Graph* ist $\mathsf{KG}(2, 5)$.

Graph–Operationen

Das *Komplement* $\overline{G}$ eines Graphen $G = (V, E)$ ist der Graph $(V, \binom{V}{2} \setminus E)$.

Übung: $\overline{C_5}, \overline{P_4}, K_n = \overline{n}$.

Die *(disjunkte) Summe* $G_1 + G_2$ von Graphen $G_i = (V_i, E_i)$ mit $V_1 \cap V_2 = \emptyset$ ist der Graph (V, E) mit $V = V_1 \cup V_2$ und $E = E_1 \cup E_2$.

Beispiel: $C_3 + C_4$ ist ein Dreieck neben einem Quadrat.

Für eine Zahl n bedeutet $n \cdot G = \underbrace{G + \ldots + G}_{n\text{–mal}}$.

Das *Produkt* $G_1 * G_2$ von Graphen $G_i = (V_i, E_i)$ mit $V_1 \cap V_2 = \emptyset$ ist der Graph (V, E) mit $V = V_1 \cup V_2$ und $E = E_1 \cup E_2 \cup \{x_1 x_2 \mid x_1 \in V_1, x_2 \in V_2\}$

Übung: $C_n * 1$ ist ein Rad. $2 * 2 * 2$ ist ein Oktaeder. Was ist $1 * 2 * 1$?

Teil I

Ramsey–Theorie

Kapitel 2

Grundlagen

2.1 Einfarbige Teilstrukturen

Eine k–(Kanten–)Färbung eines Graphen $G = (V, E)$ ist eine Abbildung $c : E \to k$. 13. April

Satz: Jede 2-Färbung eines K_6 enthält einen einfarbigen K_3.

Beispiel: Finde eine 2–Färbung des K_5 ohne einfarbigen K_3.

Für welche Zahlen n gilt: Jede Rot–Blau–Färbung des K_n enthält einen roten K_3 oder einen blauen K_4?

Satz: Für alle Zahlen a, b: es existiert N: für alle $n \geq N$: für alle 2–Färbungen c des K_n: c enthält einen K_a der einen Farbe oder einen K_b der anderen Farbe.

Definition: das kleinste solche N heißt Ramsey–Zahl $R(a, b)$.

Satz: $R(a, b) = R(b, a)$; $R(2, a) = a$; $R(a + 1, b + 1) \leq R(a, b + 1) + R(a + 1, b)$.

Beweis (durch Induktion nach $a + b$):

Wir wollen die Behauptung für $(a + 1, b + 1)$ zeigen. Wir setzen $n = R(a, b + 1) + R(a+1, b)$ (nach Induktion existieren diese Zahlen.) Wir müssen zeigen, daß in einem beliebig gefärbten K_n ein roter K_{a+1} oder ein blauer K_{b+1} enthalten ist.

Wir wählen irgendeinen Knoten v aus K_n. Dieser hat $n - 1$ Nachbarn, also gehen von v genau $n - 1$ Kanten aus. Nach Schubfachschluß sind darunter

- entweder $R(a, b + 1)$ rote
- oder $R(a + 1, b)$ blaue

Erster Fall. Betrachte die Knoten, die mit v rot verbunden sind. Sie bilden einen $K_{R(a,b+1)}$. Nach Induktionsannahme enthält dieser

- einen roten K_a
- oder einen blauen K_{b+1}

Im ersten Unterfall nehmen wir v hinzu und erhalten einen blauen K_{a+1}, im zweiten Unterfall sind wir sofort fertig.

Der andere Fall symmetrisch.

2.2 Zahlenwerte

13. April

Folgerung: $R(a,b) \leq \binom{a+b-2}{a-1}$

Aufgabe: Ergänzen Sie $R(a,a) \leq 2^?$ Siehe auch die Aufgabe mit 512 Leuten.

Genaue Werte der R sind nur wenige bekannt.

2	3	4	5	6	7	8	9	10
3	6	9	14	18	23	28	36	40…43
4	9	18	25	35…41				
5	14	25	43…49					

Hier steht $R(3,4) = 9$. Unsere Abschätzung sagt $R(3,4) \leq 10$. Woher kommt der Unterschied?

Wir wiederholen unseren Beweis, aber für "eine Zahl weniger":

$9 = R(2,4) + R(3,3) - 1 = 4 + 6 - 1$

Was könnte schiefgehen? Es könnte kein v existieren, von dem ≥ 4 rote oder ≥ 6 blaue Kanten ausgehen. Dann müssen es aber $= 3$ rote und $= 5$ blaue sein. Das geht nicht (double counting). Deswegen:

Satz: Wenn $R(a,b+1) \leq A$ und $R(a+1,b) \leq B$ und A und B beide gerade Zahlen sind, dann $R(a+1,b+1) \leq A+B-1$.

Aufgaben:

$R(3,4) > 8$. Betrachte $G = (V,E)$ mit $V = 8$, $E = \{xy \mid x - y \equiv 3,4,5 \pmod 8\}$.

Verallgemeinere zu $R(3,t+1) \geq 3t$.

$R(4,4) > 17$. Betrachte $G = (V,E)$ mit $V = 17$, $E = \{xy \mid x-y \equiv \pm 2^k \pmod{17}\}$.

$R(3,5) > 13$. Welche Kanten muß man zu C_{13} hinzunehmen?

Um welche Ramsey–Zahl geht es hier? (Bundeswettbewerb Mathematik, 2. Runde, 1985)

Auf einer Party sind 512 Personen. Von je sechs kennen sich wenigstens zwei. Zeige, daß es sechs Leute gibt, von denen jeder jeden kennt.

Beweis: nimm irgendeinen. Der kennt entweder ≥ 256 Leute nicht, oder ≥ 256 Leute doch. Die anderen wegschicken, aus dem Rest irgendeinen auswählen, usw.

2.3 Explizite untere Schranken

13. April

Man schafft es hin und wieder, $n < R(a,b)$ dadurch direkt zu zeigen, daß man eine Färbung für den K_n angibt, die keinen roten K_a und keinen blauen K_b enthält. Das wird besonders einfach, wenn die Färbungen Symmetrieen besitzen. Sie könnten zum Beispiel zyklisch sein, d. h. die Farbe der Kante xy hängt nur von der Differenz $|x-y|$ ab. Wir zeigen auf diese Weise

Satz. Für $t \geq 1$ gilt $R(3, t+1) \geq 3t$.

Beweis. Wir geben eine zyklische Färbung des K_{3t-1} mit den Ecken $\{0, 1, \ldots, 3t-2\}$: die Kante xy erhält die erste Farbe (rot) (für die wir K_3 vermeiden wollen) genau dann, wenn $x - y \equiv 1 \pmod 3$.

Das enthält kein rotes Dreieck: falls doch, mit Ecken a, b, c, wäre $a - b \equiv 1 \equiv c - b$, also $a - c \not\equiv 1 \pmod 3$.

Es enthält kein blaues K_{t+1}: falls doch, mit Ecken $\{x_0, x_1, \ldots, x_t\}$, dann können wir oBdA $x_0 = 0$ setzen (die Färbung ist zyklisch).

Die mit 0 blau verbundenen Knoten sind $\{2, 3,\ 5, 6,\ 8, 9 \ldots\}$. Das sind genau die Ecken von $t-1$ roten Kanten. Für noch fehlenden t Ecken des gesuchten blauen K_{t+1} müssen wir aber aus wenigstens einer dieser Zweiergruppen beide Elemente auswählen (Schubfachschluß), diese sind aber rot verbunden.

Jason C. Stone behauptet in http://bmb-fs1.biochem.okstate.edu/OAS/OJAS/jstone.htm, $49 < R(5,5)$ durch die folgende zyklische Färbung:

BBB RRR BBB RRR BRBRBRBRBRB RR BRBRBRBRBRB RRR BBB RRR BBB

Überprüfe oder widerlege.

2.4 Nichtkonstruktive untere Schranken

13. April

Das folgende Abzählargument stammt von Paul Erdös.

Wir fixieren n und betrachten alle

$$A = 2^{\binom{n}{2}}$$

2–Färbungen.

Wieviele Färbungen enthalten (wenigstens) einen einfarbigen K_a? Er kann an $\binom{n}{a}$ Stellen vorkommen, in einer der beiden Farben. Die restlichen $\binom{n}{2} - \binom{a}{2}$ Kanten sind beliebig gefärbt. Die Anzahl aller solcher Färbungen ist

$$E \leq G = \binom{n}{a} \cdot 2 \cdot 2^{\binom{n}{2} - \binom{a}{2}}$$

(Das ist eine Abschätzung nach oben, weil wir Färbungen mit mehreren einfarbigen K_a mehrfach zählen.)

Wenn wir n so klein machen, daß $E \leq G < A$, dann wissen wir, daß es Färbungen des K_n ohne einfarbige K_a geben muß.

Wir können auf beiden Seiten $2^{\binom{n}{2}}$ kürzen, dann geht es um den Vergleich von

$$\binom{n}{a} \quad ? \quad 2^{\binom{a}{2}-1}$$

Wir setzen $n < 2^{a/2}$ in die nicht sehr großartige Abschätzung

$$\binom{n}{a} \leq \frac{n^a}{2^{a-1}} < 2^{a^2/2-a+1} < 2^{a^2/2-a/2}$$

Das liefert

$$2^{a/2} < R(a, a)$$

Als Beispiel fixieren wir $a = 5$, dann ist

$$\binom{11}{5} = 462 < 512 = 2^{10-1}$$

Also $11 < R(5, 5)$. Das ist korrekt, aber nicht berauschend.

Auch mit wesentlich höherem Aufwand läßt sich die Größenordnung solcher Abschätzungen nicht wesentlich verbessern. Die besten bekannten oberen und unteren Schranken für $R(a, b)$ klaffen derzeit immer noch weit auseinander.

Kapitel 3

Ramsey–Aussagen für Graphen

3.1 Mehr Farben

20. April

Satz: Für alle k: Für alle Tupel $(a_1, \ldots, a_k)$ von Zahlen $a_i \geq 2$: es existiert N: für alle $n \geq N$: für alle k–Färbungen c des K_n: c enthält einen K_{a_1} der Farbe 1 oder ... oder einen K_{a_k} der Farbe k.

Definition: das kleinste solche N heißt $R(a_1, \ldots, a_k)$, die Ramsey–Zahl von $(a_1, \ldots, a_k)$.

Wenn wir die Farben $2 \ldots k$ zu einer zusammenfassen, erhalten wir leicht

$$R(a_1, \ldots, a_k) \leq R(a_1, R(a_2, \ldots, a_k))$$

Beispiel $R(3,3,3) \leq R(3, R(3,3)) = R(3,6) = 18$. Wir können aber schärfer abschätzen:

Satz:

- $R(\ldots)$ ist symmetrisch
- $R(a_1) = a_1$
- $R(2, a_2, \ldots, a_k) = R(a_2, \ldots, a_k)$
- falls alle $a_i > 2$, dann $R(a_1 + 1, \ldots, a_k + 1) \leq$

  $$(2-k)+R(a_1, a_2+1, \ldots, a_k+1)+R(a_1+1, a_2, a_3+1, \ldots)+\ldots+R(a_1+1, \ldots, a_{n-1}+1, a_n)$$

Beweis: eins und zwei offensichtlich, drei wie mit Schubfachschluß wie für zweistellige Ramseyzahlen.

Beispiel: $R(3,3,3) \leq -1 + 3 \cdot R(2,3,3) = -1 + 3 \cdot 6 = 17$.

Übung: finde eine K_3–freie 3–Färbung für den K_{16}. Beachte dabei den Beweis (d. h. den Schubfachschluß über die Kantenzahl von einem Punkt aus): wieviel Kanten jeder Farbe können (müssen) von einem Punkt ausgehen? Wie muß der von den einfarbigen Endpunkten aufgespannte Untergraph aussehen?

Beispiel: $R(3,3,3,3) \leq -2 + 4 \cdot 17 = 66$

Satz: Jede 4–Färbung der Zahlen $\{1, \ldots, 65\}$ enthält gleichfarbige a, b, c mit $a+b = c$. (Dabei ist $a = b$ zugelassen.)

Beweis: Die gegebene Färbung heißt f. Konstruiere eine Färbung g des K_{66} mit Knoten $\{1, \ldots, 66\}$ so:

$$g(xy) = f(|x - y|)$$

Beachte, daß $f(0)$ und $f(66)$ hier nicht vorkommen (dürfen auch gar nicht).

Wegen $R(3, 3, 3, 3) \leq 66$ enthält g ein einfarbiges Dreieck. Die Ecken heißen x, y, z, wir können $x < y < z$ setzen. Dann sind also $g(xy) = g(yz) = g(xz)$. Für die ursprüngliche Färbung f heißt das $f(y - x) = f(z - y) = f(z - x)$. Es gilt aber $(y - x) + (z - y) = (z - x)$, also haben wir mit $a = y - x, b = z - y, c = z - x$ das gesuchte Dreieck.

3.2 Hyper–Graphen

20. April

Definition: Für eine Zahl k: ein k–(Hyper–)Graph G ist ein Paar (V, E), mit V endlich und $E \subseteq \binom{V}{k}$.

(Also Graphen sind 2-Graphen.)

Definition: K_n ist eine k–*Hyper–Clique* auf n Knoten: $G = (V, E)$ mit $V = n$ und $E = \binom{V}{k}$.

Satz: Für alle $k \geq 1$: Für alle $a, b \geq k$: existiert N: für alle $n \geq N$: jede 2–Färbung des vollständigen k–Graphen K_n enthält einen k–Hyper–K_a der Farbe 1 oder einen k–Hyper–K_a der Farbe 2.

Definition: Das kleinste solche N heißt $R_k(a, b)$.

Was ist eigentlich für $k = 1$?

Was ist ein 1–Graph? Die Kanten sind Einermengen, also: die Knoten selbst. Eine Kantenfärbung eines 1–Graphen ist tatsächlich eine Knotenfärbung. Wir haben

Satz: $R_1(a, b) = a + b - 1$

Beweis: das ist einfach der Schubfachschluß.

Satz:

- $R_k(a, b) = R_k(b, a)$
- $R_k(k, b) = b$
- $R_{k+1}(a + 1, b + 1) \leq 1 + R_k(R_{k+1}(a, b + 1), R_{k+1}(a + 1, b))$

Beweis durch Induktion nach k. Für $k = 2$ erwarten wie die einfachen Ramsey–Zahlen. In der Tat stimmt das. Setze die Definition von $R_1(,)$ ein!.

Für den Induktionsschritt. Betrachte eine 2-Färbung g eines vollständigen $(k + 1)$–Graphen G der Größe $m = 1 + R(A, B)$ mit $A = R_{k+1}(a, b + 1), B = R_{k+1}(a + 1, b)$.

Fixiere irgendeinen Knoten $v \in V(G)$. Betrachte die 2–Färbung h des k–Graphen

$$\begin{aligned} H &= \left(V(G) \setminus v, \binom{V(G) \setminus v}{k} \right) \\ h(e) &= g(e \cup v) \end{aligned}$$

Nun ist $|V(H)| = R_k(A, B)$, deswegen enthält H einen vollständigen k–Graphen K_A der ersten Farbe oder einen K_B der zweiten Farbe.

Für Fall eins: sei H' dieser Teilgraph. Wegen $A = R_{k+1}(a, b + 1)$ enthält H' einen $(k+1)$–K_a der ersten Farbe oder einen $(k+1)$–K_{b+1} der zweiten Farbe. Im Unterfall zwei sind wir fertig, im erste Unterfall erweitern wir den $(k + 1)$–K_a um den Knoten v. Die hinzukommenden Kanten haben die richtige Farbe.

Fall zwei: symmetrisch.

Beispiele für Ramsey–Zahlen für Hyper–Graphen

20. April

Für einen Flug zum Mars trainieren 6783 Kosmonauten. Zu einer Besatzung gehören drei Mann. Sie sollten bereits ein Team bilden, das heißt, wenigstens einmal miteinander trainiert haben.

Es ist bekannt, daß man unter beliebigen 4 der Kosmonauten stets ein Team findet. Zeige, daß es dann sogar 5 Mann gibt, von denen jede Dreiermenge ein Team bildet.

(Das ist offensichtlich eine Aufgabe aus der sowjetischen Schülerzeitschrift Quant.)

Nach Entfernen der Lyrik geht es darum, $R_3(4,5) \leq 6783$ zu zeigen. Warum? Wir haben dann entweder 5, von denen alle 3 ein Team bilden (das wollen wir) oder 4, von denen keine 3 ein Team bilden (das war explizit verboten).

$R_3(4,5) \leq 1 + R_2(R_3(3,5), R_3(4,4))$, $R_3(3,5) = 5$, $R_3(4,4) \leq 1 + R_2(R_3(3,4) + R_3(4,3))$, $R_3(3,4) = 4$, $R_2(4,4) = 18$, $R_3(4,4) \leq 19$, $R_3(4,5) \leq 1 + R_2(5,19)$

Es geht also um eine Abschätzung für $R_2(5,19)$. Allein mit den bereits bewiesenen Abschätzungen geht das nicht besser als die folgende Tabelle:

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
3	6	9	14	19	26	33	42	51	62	73	86	99	114	129	146	163	182	201	222
4	9	18	31	50	75	108	149	200	261	334	419	518	631	760	905	1068	1249	1450	1671
5	14	31	62	111	186	293	442	641	902	1235	1654	2171	2802	3561	4466	5533	$\boxed{6782}$	8231	9902

3.3 Einfarbige Teilgraphen

27. April

Satz: Für Graphen $G_1, \ldots, G_k$: es existiert N: für alle $n \geq N$: für jede k–Färbung f des K_n: existiert i: die Färbung f enthält einen G_i der Farbe i.

Definition: das kleinste solche N heißt $R(G_1, \ldots, G_k)$.

Bemerkung: das ist eine sinnvolle Verallgemeinerung früherer Bezeichnungen, denn

$$R_{\text{bisher}}(a_1, \ldots, a_k) = R_{\text{neu}}(K_{a_1}, \ldots, K_{a_k})$$

Beweis: Da es nur um Teilgraphen geht, können wir statt nach G_i auch nach $K_{|G_i|}$ suchen.

$$R(G_1, \ldots, G_k) \leq R(|G_1|, \ldots, |G_k|)$$

Das liefert natürlich im Allgemeinen eine höhere Schranke als nötig.

Beispiel: $R(C_4, C_4) = 6$.

Beweis: $R(C_4, C_4) > 5$ durch Betrachtung des C_5.

$R(C_4, C_4) \leq 6$: Wegen $6 = R(3, 3)$ gibt es ein einfarbiges K_3, o.B.d.A. ist es rot. Die Menge seiner Ecken heißt I (innen), die restlichen 3 Punkte heißen A (außen).

Von jedem $a \in A$ gibt es höchstens eine rote Kante nach I.

Von jedem $i \in I$ gibt es höchstens eine rote Kante nach A.

Falls es ein $a \in A$ ohne rote Kante nach I gibt, dann nimm $b \in A$. Von dort muß eine rote Kante zu einem $i \in I$ gehen. Die anderen I–Punkte sind j und k. Die Kanten jb und kb sind blau. Das gibt einen C_4 auf $ajbk$.

Also gibt es rote Kanten i_1a_1, i_2a_2, i_3a_3, und alle anderen i_*a_* sind blau.

Wenn a_xa_y rot, dann roter C_4 auf $i_xa_xa_yi_y$, also sind alle a_xa_y blau.

Dann aber blaue C_4 auf $a_1a_2a_3i_2$ (und andere).

Aufgabe (Bollobas):

$$R(\underbrace{C_4, \ldots, C_4}_{k\text{–mal}}) \leq k^2 + k + 2$$

Satz: T ist ein Baum auf $|T| = t$ Knoten. Dann

$$R(K_s, T) = (s-1)(t-1) + 1$$

Beispiel: T ist eine Pfad.

Beweis: Für $R(K_s, T) > (s-1)(t-1)$ betrachte $(s-1)K_{t-1}$.

Für $R(K_s, T) \leq (s-1)(t-1) + 1$: betrachte irgendeine rot/blau–Färbung eines K_n mit $n = (s-1)(t-1) + 1$. Wir nennen der Graphen aus den blauen Kanten G. (Farbwahl: wir wollen einen roten K_s oder einen blauen T.)

Wir suchen eine Einteilung der Knoten von G in Klassen, so daß die (blauen) Kanten alle zwischen verschiedenen Klassen laufen. Jede Klasse hat $< s$ Knoten (falls mehr, gäbe es einen roten K_s). Also brauchen wir dazu wenigstens $\lceil n/(s-1) \rceil = t$ Klassen.

Wir benutzen (alle Satznummern aus Diestel) Korollar 4.2.3: G enthält einen Teilgraphen H von Minimalgrad $\geq t-1$ und nach Korollar 0.5.4: Dann enthält H einen zu T isomorphen Teilgraphen. Beweise siehe unten.

Das erweckt den Anschein, die gewünschten einfarbigen Teilgraphen treten auf, weil wir einen K_n färbten, und dieser genügend Kanten hat.

Man könnte auch fragen: gibt es einen G ohne K_4, der bei beliebiger 2–Kanten–Färbung einen einfarbigen K_3 enthält?

Definition: Für Graphen $H, G_1, \ldots, G_k$ schreiben wir

$$H \to (G_1, \ldots, G_k)$$

, wenn für jede k–Färbung f der Kanten von H: existiert i: in H gibt es ein G_i der Farbe i.

Bemerkung:

$$R(G_1, G_2) = \min\{n \mid K_n \to (G_1, G_2)\} = 1 + \max\{n \mid K_n \not\to (G_1, G_2)\}$$

Definition: $\mathrm{cl}(G)$ ist die Größe einer maximalen Clique in G.

Satz (Nesetril, Rödl): Für alle $G_1, \ldots, G_k$: existiert H mit $\mathrm{cl}(H) = \max cl(G_i)$ und $H \to (G_1, \ldots, G_k)$.

Hier die nachgeholten Beweise zu Färbungen (aus Diestel):

Korollar 0.5.2: Jeder Baum hat eine Eckenaufzählung $v_1, \ldots, v_t$, so daß $\forall i > 1$ gilt: v_i hat genau einen Nachbarn in $\{v_1, \ldots, v_{i-1}\}$.

Beweis: wähle irgendeine Wurzel und durchlaufe T schichtweise (Breitensuche).

Korollar 0.5.4: Für jeden Baum T und jeden Graphen G mit Minimalgrad $\geq |T| - 1$ gilt $T \subseteq G$.

Beweis: Finde eine Kopie von T in G entlang der Eckenaufzählung aus Korollar 0.5.2.

Korollar 4.2.3: Jeder Graph G hat einen Untergraphen H vom Minimalgrad $\delta(H) \geq \chi(G) - 1$.

Beweis: Wir fixieren eine Eckenaufzählung $v_1, \ldots, v_n$ von G und färben die Ecken nach dem Greedy–Verfahren: v_i bekommt die kleinste Farbe, die unter seinen Nachbarn in $\{v_1, \ldots, v_{i-1}\}$ nicht vorkommt.

Insbesondere wählen wir die Aufzählung so, daß v_n minimalen Grad in G hat, und v_{n-1} minimalen Grad in $G - v_n$, und so weiter.

Für die Anzahl f der bei der Färbung von G benutzten Farben gilt: für alle $H \subseteq G$, die bei der Färbung betrachtet werden: $f \leq 1 + \delta(H)$. Nehmen wir alle anderen H noch dazu, folgt (Proposition 4.2.2): $\chi(G) \leq 1 + \max\{\delta(H) \mid H \subseteq G\}$

Durch Rumdrehen haben wir das Korollar.

3.4 Weitere konkrete Ramseyzahlen

LSGM, 13. Mai

Erinnerung: P_n ist ein Pfad, der n verschiedenen Knoten verbindet, also $n-1$ Kanten hat.

Vorsicht: oft bedeutet P_n einen Pfad mit n Kanten. Ich weiß nicht, welche Zählung besser oder häufiger stattfindent. Die hier benutzte Variante hat den Vorteil, konsistent mit der Benutzung in C_n (Kreis) und K_n zu sein, bei denen man ja auch Knoten (und nicht Kanten) zählt.

Erinnerung: $k \cdot G$ ist ein Graph, der aus k disjunkten Kopien von G besteht. Also $k \cdot P_2$ sind k isolierte Kanten.

Satz: Für $s \geq t \geq 1$ ist $R(sP_2, tP_2) = 2s + t - 1$.

Beweis (eine Richtung): Betrachte den Graphen $K_{2s-1}+(t-1)$, d. h. eine vollständige Menge der Größe $2s-1$ und eine unabhängige Menge der Größe $t-1$. Wir nennen die Kanten des Graphen rot und die des Komplements blau.

Der Graph enthält keinen roten sP_2: rote Kanten verlaufen nur innerhalb des K_{2s-1}, aber das ist ein Knoten zuwenig für s unabhängike Kanten.

Er enthält keinen blauen tP_2: Jede blaue Kanten hat wenigstens ein Ende im blauen K_{t-1}, aber von jedem dieser Punkte kann höchstens eine blaue Kante ausgehen, die zu einer unabhängigen Menge gehören will. Also fehlt wieder ein Knoten.

Beweis (andere Richtung): Wir zeigen die Lemmas

- für $t \geq 1$ gilt $R(tP_2, tP_2) \leq 3t - 1$
- für $s \geq t$ gilt $R((s+1)P_2, tP_2) \leq 2 + R(sP_2, tP_2)$.

Dann folgt durch Induktion $s \geq t \Rightarrow R(sP_2, tP_2) \leq 2(s-t) + R(tP_2, tP_2) = 2(s-t) + 3t - 1 = 2s + t - 1$.

Beweis der Lemmas: für $t \geq 1$ gilt $R(tP_2, tP_2) \leq 3t-1$. Induktionsanfang: Für $t = 1$ ist die Behauptung klar. Induktionsschritt: Nimm einen Graphen mit $3t+2$ Knoten. Dieser enthält ein Dreieck abc mit zwei verschiedenfarbigen Seiten. (Wenn nicht, ist er rot und vollständig oder blau und vollständig und enthält wegen $3t+2 > 2t+2$ in jedem Fall einfarbiges $2(t+1)P_2$.) Entferne a, b, c. Der Rest hat $3t-1$ Knoten und enthält nach Induktionsvoraussetzung roten sP_2 oder blauen tP_2. In beiden fällen können wir eine passende Kante des Dreicks disjunkt hinzufügen.

Das andere Lemma folgt aus dem nächsten Satz:

Satz: $R(G, H_1 + H_2) \leq \max(R(G, H_1) + |H_2|, R(G, H_2))$

Beweis: Nimm einen Graphen mit der gegebenen Knotenzahl n. Wegen $n \geq R(G, H_2)$ enthält er einen roten G, dann sind wir fertig, oder einen blauen H_2. Den löschen wir, übrig bleiben $R(G, H_1)$ Knoten. Dort gibt es einen roten G (fertig) oder einen blauen H_1. Zusammen mit dem gelöschten blauen H_2 haben wir einen blauen $H_1 + H_2$.

Folgerung: $R(G, sH) \leq R(G, H) + (s-1)|H|$

Beweis durch Induktion nach H.

Anfang: $R(G, 1H) = R(G, H)$.

Schritt: $R(G, sH + H) \leq \max(R(G, sH) + |H|, R(G, H)) = R(G, sH) + |H|$.

Ahnlichkeiten zu $R(sP_2, tP_2)$ hat $R(P_m, P_n)$:

Satz: Für $m \geq n$ ist $R(P_m, P_n) = m + \lfloor n/2 \rfloor - 1$.

Beweis (eine Richtung): mit dem gleichen extremalen Graphen wie eben folgt die untere Schranke.

Bemerkung: Wegen $sP_2 \subseteq P_{2s}$ gilt $R(sP_2, tP_2) \leq R(P_{2s}, P_{2t})$.

Beweis (andere Richtung): Wir zeigen

- für $m \geq 2$ gilt $R(P_m, P_2) = m$. (Klar. Der Graph ist dann vollständig rot.)
- für $m \geq 2$ gilt $R(P_m, P_3) = m$. (Wenn kein blauer P_3 da ist, müssen alle blauen Kanten disjunkt sein. Sie sind $x_1y_1, x_2y_2, \ldots x_ky_k$. Eventuell gibt es noch eine unabhäbgige (d. h. nur rot verbundene) Menge $z_1, , z_l$. Ein roter Pfad durch alle Knoten ist dann $x_1, x_1, \ldots, x_k, z_1, z_2, \ldots, x_l, y_1, y_2, \ldots, y_k$.)
- $R(P_{m+2}, P_{n+2}) \leq 3 + R(P_m, P_n)$. (Wie eben ist der Graph entweder vollständig rot, oder vollständig blau, oder es gibt ein Dreieck abc mit rotem ab und blauem ac. Wie weiter? Übung.

Satz: $R(2K_3, K_3) = 8$

Beweis: Wegen $K_5 + K_2$ gilt $R(2K_3, K_3) > 7$.

Bei einer Färbung des K_8: entferne zwei Punkte x, y. Im restlichen K_6 gibt es wegen $R(K_3, K, 3) = 6$ ein rotes K_3 oder ein blaues K_3. Falls blau, sind wir fertig, also rotes Dreieck abc.

Die fünf anderen Punkte 12345 (nicht auf dem roten Dreieck) sollten dann weder blauen noch roten K_3 enthalten, also wie ein Fünfeck (außern blau, innen rot) aussehen.

Von jedem $x \in abc$ gehen höchstens drei rote Kanten in das Fünfeck (sonst gibt es ein rotes Dreieck). Das heißt, von jedem abc gehen wenigstens zwei blaue Kanten in das Fünfeck. Diese beiden überspannen jeweils eine blaue Kante des Fünfecks. Das passiert von abc aus insgesamt dreimal, aus den drei überspannten blauen Kanten lassen sich aber zwei disjunkte auswählen. Zusammen mit ihren Dachpunkte in abc ergeben diese die gesuchten zwei diskunkten blauen Dreiecke.

Satz: $R(2K_3, 2K_3) = 10$

Beweis: Betrachte $K_5 + (1 * 3)$ für $R(2K_3, 2K_3) > 9$.

Andere Richtung: Übung. Wie eben.

Satz: Für $s \geq t \geq 1$ und $s \geq 2$ gilt $R(sK_3, tK_3) = 3s + 2t$.

Beweis: Übung. Analog zu $R(sP_2, tP_2)$.

3.5 Der Satz von Turan

4. Mai

Bemerkung: bei Ramsey–Aussagen suchen wir nach Dingen in der einen oder der anderen Farbe. Auch einseitige Fragen sind interessant, und führen in das wohl entwickelte Gebiet der extremalen Graphentheorie. Diese untersucht Fragen wie: wieviele Kanten darf ein Graph auf n Knoten haben, ohne daß er einen bestimmten Teilgraphen enthält. Ein klassisches Beispiel ist der Satz von Turan.

Definition: Ein Graph $G = (V, E)$ heißt r–partit, wenn es eine disjunkte Zerlegung $V = V_1 \cup \ldots V_r$ gibt, so daß für alle i gilt: $E \cap \binom{V_i}{2} = \emptyset$ (d. h. es gibt keine Kanten innerhalb einer Klasse).

Wir schreiben dann gleich $G = (V_1, \ldots, V_r, E)$.

Definition: Graphen der Form $n_1 * \ldots * n_r$ (also Produkte von unabhängigen Mengen) heißen *vollständig* r–partit.

Definition: Die Turan–Graphen $T_r(n)$ sind vollständige r–partite Graphen $(V_1, \ldots, V_r, E)$ auf n Knoten, wobei für die Größen der Zerlegung gilt

$$|V_1| \leq |V_2| \leq \ldots \leq |V_r| \leq |V_1| + 1$$

Beispiel: $T_3(10) = 3 * 3 * 4$.

Turan–Graphen sind (bis auf Isomorphie) eindeutig bestimmt.

Definition: Die Kantenzahl der Turan–Graphen $t_r(n) = |E(T_r(n))|$.

Satz (Turan, 1941): Für alle r, n: Bezeichne $e = t_{r-1}(n)$.

- Jeder Graph H mit mehr als e Kanten *enthält* einen K_r.
- Jeder Graph H mit genau e Kanten und ohne K_r *ist* ein $T_{r-1}(n)$.

Zur Vorbereitung des Beweises einige Lemmata:

Lemma: G ist ein Turan–Graph, wenn G vollständig r–partit ist, also $G = (V_1, \ldots, V_r, E)$ mit

$$\forall i < j : ||V_i| - |V_j|| \leq 1$$

(anschaulich klar.)

Lemma: Wenn $K_r \not\subseteq G$, dann existiert ein $(r-1)$–partiter Graph H auf der gleichen Knotenmenge mit $\forall x \in V(G) = V(H) : \deg_G(x) \leq \deg_H(x)$.

(Beweis folgt)

Lemma: Unter allen r–partiten Graphen auf n Knoten haben die Turan–Graphen die maximale Kantenzahl.

Beweis: Wir können die Graphen o.B.d.A. als r–partit und vollstädig annehmen (durch Auffüllen von Kanten zwischen den Klassen).

Ein Nicht–Turan–Graph hat dann zwei Klassen mit $|V_1| - |V_2| > 1$. Wenn wir einen Knoten von V_1 nach V_2 bewegen, und dann wieder alle Kanten zeichnen, erhalten wir einen Graphen mit mehr Kanten.

Beweis des Lemmas: durch Induktion nach r. Sei G ein Graph mit n Knoten ohne K_r.

Induktionsanfang: $r = 2$. Dann hat G gar keine Kanten, ist also unabhängig, alle Grade sind 0, und im entstprechenden Turan–Graphen $T_1(n) = n$ (eine unabhängige Menge) auch.

Induktionsschritt: Betrachte einen Knoten x maximalen Grades in G. Der von seinen Nachbarn aufgespannte Teilgraph ist G'. In G' gibt es kein K_{r-1}. (Sonst in G ein K_r mit x.)

Nach Voraussetzung gibt es einen $(r-2)$–partiten $H' = (V_1, \dots, V_{r-2}, E')$ auf $V(G')$ mit $\forall y \in V(H') : \deg_{G'}(y) \leq \deg_{H'}(y)$.

Wir nehmen x und alle seine Nicht–Nachbarn in die Menge V_{r-1}, und verbinden alle V_{r-1} mit allen $V_1 \cup \dots \cup V_{r-2}$, um $H = (V_1, \dots, V_{r-2}, V_{r-1}, E)$ zu erhalten

Wir müssen nachrechnen, daß dadurch kein K_r entsteht (klar), und daß die Knotengrade in H nicht kleiner als die in G sind: Dazu bemerken wir, daß nach Konstruktion $\deg_H(x) = \deg_G(x)$, aber auch für alle $z \in V_{r-1} \setminus x$ gilt $\deg_H(z) = \deg_H(x) = \deg_G(x) \geq \deg_G(z)$.

Wir können auch eine Turan–Frage für das Auftauchen von Bäumen stellen (Vergleiche $R(K_s, T) = (s-1)(t-1)+1$):

Vermutung (Erdös, Sos, 1963): Wenn G ein Graph auf n Knoten ist, und T ein Baum mit t Kanten, und G wenigstens $n(t-1)/2$ Kanten hat, dann enthält G einen T als Teilgraph.

Das ist bis heute (?) offen. Bewiesen ist die Richtigkeit, wenn T ein Pfad ist, und andererseits, wenn G keinen C_4 enthält.

3.6 Unendlichkeit und Kompaktheit

4. Mai

Zunächst eine weitere Abschätzung für endliche Ramsey–Zahlen:

(Bundeswettbewerb Mathematik, 2. Runde, 1985)

Auf einer Party sind 512 Personen. Von je sechs kennen sich wenigstens zwei. Zeige, daß es sechs Leute gibt, von denen jeder jeden kennt.

Beweis: nimm irgendeinen. Der kennt entweder ≥ 256 Leute nicht, oder ≥ 256 Leute doch. Die anderen wegschicken, aus dem Rest irgendeinen auswählen, usw.

Das ist tatsächlich ein Beweis für $R(a, a) \leq 2^{2a-3}$.

Nun eine Aussage über unendliche Graphen. (Was ist das? Die Knotenmenge V ist abzählbar unendlich, aber alle anderen Begriffe werden von endlichen Graphen übernommen: Kantenfärbung, einfarbig, vollständig usw. K_ω bezeichnet den vollständigen Graphen auf der Knotenmenge $\mathbb{N}$.)

Satz: Jede 2–Kanten–Färbung des K_ω enthält einen einfarbigen K_ω.

Beweis: Die Kantenfärbung heißt c. Der folgende Algorithmus erzeugt eine unendliche Folge $(x_0, x_1, \ldots) \subseteq \mathbb{N}$. Wir starten ihn mit $M_0 = \mathbb{N}$. Die Schleifen–Invariante ist, daß die Mengen M_k alle unendlich sind, und $x_k \in M_k$.

Wähle irgendeinen (z. B. den kleinsten) Knoten $x_k \in M_k$. Unter den Farben der (unendlich vielen) Kanten $\{x_k y \mid y \in M_k \setminus x_k\}$ kommt eine der beiden Farben $\{0, 1\}$ unendlich oft vor. Diese Farbe heißt f. Setze

$$M_{k+1} = \{y \mid y \in M_k \setminus x_k, c(x_k y) = f\}$$

Nach Konstruktion gilt

$$\forall k : \forall i, j < k : c(x_i x_k) = c(x_j x_k)$$

Deswegen können wir die Knoten $(x_1, x_2, \ldots)$ so färben: $d(x_k) := c(x_0 x_k) = c(x_1 x_k) = \ldots$. Unter den unendlich vielen x_k befinden sich unendlich viele der gleichen Farbe. Diese bilden den gesuchten einfarbigen Teilgraphen.

Aus (U) folgt (E)

- (U) jede 2–Färbung des K_ω enthält einfarbigen K_ω
- (E) für alle m: existiert N: für alle $n \geq N$: jede 2–Färbung des K_n enthält einfarbigen K_m

$(U) \to (E)$: eigentlich $\neg E \to \neg U$. Dann gibt es ein m, so daß $\forall N \exists n \geq n$: $\exists$ 2–Färbung des K_n ohne einfarbigen K_m. Wir nennen solche Färbungen "schlecht". Da jede schlechte Färbung eines K_n auf $\{1, \ldots, n\}$ wegen $n \geq N$ zu einer schlechten Färbung des K_N eingeschränkt werden kann, gilt sogar $\exists m : \forall n : \exists$ schlechte Färbung des K_n. Aus diesen Färbungen der K_n konstruieren wir eine 2–Färbung des K_ω ohne einfarbigen K_ω:

Betrachte dazu diesen Baum: in der Schicht n befinden sich alle schlechten 2-Färbungen des K_n (mit den Knoten $\{1 \ldots n\}$). Eine Färbung f aus der Schicht n ist verbunden mit einer Färbung f' aus der Schicht $n+1$, wenn f eine Einschränkung von f' ist. (D. h. wir erhalten f, wenn wir in f' alle Kanten zu $n+1$ ignorieren.)

Offenbar ist das ein Baum. Jeder Schicht ist endlich, jeder Knoten hat genau einen Vorgänger, jeder Knoten hat endlich viele (direkte) Nachbarn (weil die alle in der nächsten Schicht liegen und diese endlich ist). Nach Voraussetzung ist aber der ganze Baum unendlich tief (denn jede Schicht enthält wenigstens ein Element.) Nach dem Lemma von König gibt es in solch einem Baum einen unendlichen Pfad. Dieser beschreibt eine Färbung des K_ω (weil entlang des Pfades die Färbungen nur erweitert, aber nicht geändert werden).

Diese Färbung enthält keine einfarbigen K_ω: Falls doch, müßte es einen einfarbigen K_m bereits in irgendeiner Färbung eines K_n auf dem Pfad geben.

Die Aufgabe 7.4 in (Diestel) zeigt, daß wir das Resultat nicht so einfach auf größere Mächtigkeiten übertragen können:

Es gibt eine 2–Färbung des vollständigen Graphen auf $\mathbb{R}$ ohne einen vollständigen einfarbigen Untergraphen, der zu $\mathbb{R}$ gleichmächtig ist.

Hinweis: Wähle eine Wohlordnung auf $\mathbb{R}$, und vergleiche sie mit der natürlichen Ordnung. Benutze, daß jede abzählbare Vereinigung abzählbarer Mengen selbst abzählbar ist.

3.7 Ramsey–Aussagen für gerichtete Graphen

4. Mai

Jede 2–gefärbte (4×7)–Matrix enthält eine einfarbige (2×2)–Untermatrix, in Zeichen:

$$(4 \times 7) \to (2 \times 2)_2$$

Beispiel:

$$\begin{array}{ccccccc} 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & \boxed{1} & 1 & 0 & 0 & \boxed{1} & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & \boxed{1} & 0 & 1 & 0 & \boxed{1} & 0 \end{array}$$

Beweis: Betrachte die erste Zeile. Nach Schubfachschluß enthält sie wenigstens vier gleiche Elemente, oBdA 0. Betrachte deren zugeordnete Spalten. Dort kann in der zweiten Zeile höchstens eine 0 stehen, also wenigstens drei 1. Unter diesen steht in der dritten Zeile wieder höchstens eine 0, andererseits aber auch höchstens eine 1. (Beachte, daß wir die vierte Zeile nicht brauchen.)

Beachte auch in diesem Beispiel: durch Weglassen der vorletzten Spalte erhalten wir eine (4×6)–Matrix ohne einfarbiges (2×2), weil dann in den Spalten alle verschiedenen Möglichkeiten der Auswahlen von 2 Elementen aus 4 stehen.

Tatsächlich gilt:

$$(3 \times 7) \to (2 \times 2)_2, \ (5 \times 5) \to (2 \times 2)_2, \ (4 \times 6) \not\to (2 \times 2)_2,$$

Untersuche andere Zahlen! Wann gilt

$$(a \times b) \to (c \times d)_k$$

Was hat das mit Ramsey zu tun? Wenn die Matrix symmetrisch ist (weil unsere Graphen ungerichtet waren) und die Untermatrix auch noch symmetrisch drinliegt (d. h. wir wählen einige Zeilen und müssen dann die Spalten mit den gleichen Nummern nehmen) dann haben wir die üblichen Ramsey–Zahlen $R(x, x)$.

Bemerkung: der Schluß auf unendliche Objekte geht hier fehl. Wir haben zwar

$$(\omega \times \omega) \to (c \times d)_k$$

für beliebige c, d, k (behaupte ich mal einfach so, d. h. ist Übungsaufgabe für Zweifler), aber

$$(\omega \times \omega) \not\to (\omega \times \omega)_2$$

Beweis: Betrachte die unendliche 2–Färbung $\mathbb{N}^2 \to 2$: wir färben alle Punkte unterhalb (und auf) der Diagonalen rot, den Rest blau. Darin gibt es zwar (in beide Richtungen) beliebig große, aber keine (in beide Richtungen) unendliche einfarbige Untermatrix.

Die Moral der Geschichte (dieses und des vorigen Abschnitts mit K_ω: von Unendlich auf Endlich geht meistens (bei Kompaktheit), von Endlich auf Unendlich geht nicht immer.

Kapitel 4

Ramsey–Aussagen in der Geometrie

4.1 Geometrie im Wald

Zur Abwechslung mal eine Aufgabe (auch aus “Quant”) zur kombinatorischen Geometrie, die aber nichts mit Ramsey zu tun hat.

Im Wald stehen Birken und Lärchen. Um jede Birke stehen in genau zehn Meter Abstand zehn Lärchen. Trotzdem enthält der Wald mehr Birken als Lärchen. Kann das sein? Wie sieht das aus?

Antwort: Ja. Konstruktion:

Wir pflanzen eine Birke und darum zehn Lärchen. Das ist der Wald W_1.

Aus W_k erhalten wir W_{k+1} durch diese Vorschrift:

Zeichne einen Kreis mit Radius 10, auf dessen Mittelpunkt M kein Baum steht, und auf dessen Umfang bereits genau eine Lärche X_0 steht. Lege 9 weitere Punkte (beliebig, siehe unten) $X_1, \ldots, X_9$ auf dem Umfang fest.

Bilde V als die Vereinigung der Bilder von W_k unter den 10 Verschiebungen

$$\{\vec{X_0X_i} \mid 0 \leq i \leq 10\}$$

(eine davon ist die Identität).

Es gibt eine Birke im Abstand 10 von der Lärche X_0. W_{k+1} ist V und *zusätzliche Birken* in den Bildern von M unter den Verschiebungen

$$\{\vec{X_0L} \mid L \in \text{alle Lärchen in } W_k\}$$

Die Konstruktion ist korrekt (die neu gepflanzten Birken haben wirklich je zehn Lärchen um sich herum) und auch ausführbar (wir müssen dafür sorgen, daß keine zwei Bäume auf die gleiche Stelle kopiert oder gepflanzt werden, das ist möglich, da wir die X_i auf dem Umfang beliebig wählen können, verboten sind aber höchstens endlich viele Punkte.)

Für die Anzahl der Lärchen L_k im Wald W_k gilt offenbar $L_k = 10^k$. Die Anzahl der Birken B_k berechnet sich nach

$$B_1 = 1, B_{k+1} = 10B_k + L_k$$

mit der Lösung $B_k = k \cdot 10^{k-1}$.

Daraus folgt, daß W_{11} die Lösung ist, denn dort gilt $L_{11} = 10^{11} < 11 \cdot 10^{10} = B_{11}$.

Wie groß ist der Wald? Die Verschiebungspfeile haben die Gesamtlänge $\leq$ 100 m, also stehen auf etwa 200 m im Quadrat insgesamt $2.1 \cdot 10^{11}$ Bäume.

4.2 Das Happy–End–Problem

20. April

Klassisch ist die folgende Frage von Erdös/Klein/Szekeres: Für alle n: existiert m: jede ebene Anordnung von m Punkten in allgemeiner Lage (d. h. keine drei auf einer Geraden) enthält n Punkte, die ein konvexes Polygon bilden.

Siehe [Hof98], Seite 74ff (zitiert in [Win00]).

Man muß sich elementargeometrisch diese Sachverhalte klarmachen:

- Die Punkte $X = \{x_1, \ldots, x_n\}$ liegen konvex $\iff$ alle Vierermengen $\subseteq X$ konvex liegen.
- Jede Fünfermenge enthält ein konvexes Viereck.

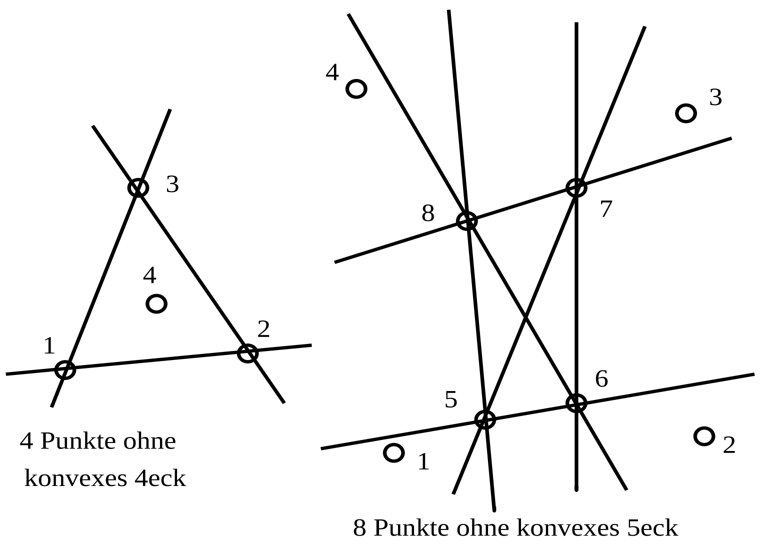
Dann reduziert sich die Aufgabe auf $m \leq R_4(5, n)$. Warum? Wir haben dann entweder 5 Punkte ohne konvexes Unterviereck (verboten) oder n Punkte mit lauter konvexen Untervierecken (also liegen die Punkte selbst konvex).

Für $n = 5$ braucht man demnach $m \leq R_4(5,5) \leq 1 + R_3(R_4(4,5), R_4(5,4)) = 1 + R_3(5,5) \leq 1 + 1 + R_2(R_3(4,5), R_3(5,4)) = 2 + R_2(6782, 6782)$. Nach Abschätzung $R_2(a,a) \leq 2^{2a-3}$ folgt $m \leq 2 + 2^{13561}$. Eine beachtliche Zahl, und tatsächlich viel zu groß. (Der wahre Wert ist 9, siehe später.)

Interessant sind auch untere Schranken, d. h. Anordnungen von möglichst vielen Punkten, die *kein* konvexes Fünfeck enthalten.

Es besteht die Vermutung, daß die minimale erfolderliche Punktzahl für ein konvexes n–Eck genau $2^{n-2} + 1$ ist.

Das stimmt für $n = 4$ und $n = 5$ mit den Tatsachen überein, aber für $n = 6$ ergibt das 17 Punkte. Die schärfste derzeit bekannte obere Schranke ist 37.



27. April

Warum ist die $R_4(5,n)$–Abschätzung so furchtbar zu groß? Wir tun dabei so, als hinge alles nur von den Vierermengen ab. Tatsächlich ist aber Konvexität eine Aussage über Dreiecke: Das Polygon $(x_1,\ldots,x_n)$ ist konvex $\iff$ für alle Teilmengen $\{a,b,c\} \subseteq \{1,\ldots,n\}$ mit $a<b<c$ die Vorzeichen der orientierten Flächeninhalte der $\Delta x_a x_b x_c$ übereinstimmen.

Es geht also tatsächlich um 2–Färbungen (nämlich plus oder minus) von Dreiermengen (Flächeninhalten). Die angegebene Konfiguration der vier Punkte ohne konvexes Viereck ist: $\Delta 123 > 0, \Delta 124 > 0, \Delta 134 < 0, \Delta 234 > 0$.

Wir stellen leicht fest, daß von den 16 denkbaren 2–Färbungen des vollständigen 3–Graphen auf 4 Punkten (d. h. der Unter–Dreiecke eines Vierecks) nur 14 geometrisch realisierbar sind. Beispiel: die folgende ist es nicht: $\Delta 123 > 0, \Delta 124 < 0, \Delta 134 > 0, \Delta 234 < 0$.

Ramseytheoretisch passiert folgendes: wir suchen einen einfarbigen Teilgraphen bestimmter Form (nämlich ein konvexes n–Eck), aber wir wissen dabei schon, daß der Ausgangsgraph nicht beliebig gefärbt ist, sondern bereits gewisse Randbedingungen erfüllt. Das sollte hier die Ramseyzahl deutlich verkleinern.

Schreibe ein Programm, das zu einer gegeben 2–Färbung eines vollständigen 3–Graphen auf n Ecken die Realisierbarkeit entscheidet. Ist die Bedingung "jede Vierermenge ist realisierbar" auch hinreichend für die Realisierbarkeit der gesamten Färbung? Wie findet man dann eine Realisierung (d. h. mögliche Koordinaten der Punkte)?

Dabei könnte diese Idee helfen: Es läßt sich leicht ablesen, ob drei Punkte ein leeres Dreieck bilden. Wir fixieren ein solches. Jetzt suchen wir (für jede seiner Seiten xy) einen Punkt z, so daß Δxyz ebenfalls leer ist, usw. Das ergibt eine Triangulierung mit Baumstruktur, in der schließlich alle Punkte vorkommen. Diesen Baum müssen wir dann hoffentlich "nur noch" geeignet verformen.

Eine naheliegende Frage ist die nach der Existenz von *leeren* konvexen n–Ecken. Man kann zeigen: jede genügend große Punktmenge enthält ein leeres Fünfeck, aber es gibt eine Anordnung von unendliche vielen Punkten *ohne* leeres Siebeneck. Für Sechsecke ist die Frage offen.

4.3 Euklidische Ramsey–Theorie

11. Mai

(Literatur: [Bol79], [Gra97] in [GO97].)

Definition: Für eine Punktmenge P schreiben wir

$$\mathbb{R}^m \to (P)_c,$$

wenn jede c–Färbung des $\mathbb{R}^m$ ein einfarbiges P' enthält, das kongruent zu P ist.

Satz: $P =$ zwei Punkte im Abstand 1. Dann

$$\mathbb{R}^2 \to (P)_3, \text{ aber } \mathbb{R}^2 \not\to (P)_7$$

Beweis: (Zwei Bilder.)

Der größte Wert c, für den $\mathbb{R}^2 \to (P)_c$, ist nicht bekannt.

Satz: Für $T =$ die Ecken eines gleichseitigen Dreicks (der Seitenlänge 1): $\mathbb{R}^2 \not\to (T)_2$

Beweis: Färbung der Ebene durch halboffene Streifen $\{(x, y) \mid 2m \leq x < 2m+1, y \in \mathbb{R}\}$. Streifendicke stimmt nicht?

Vermutung: für jedes nicht gleichseitige Dreieck T gilt $\mathbb{R}^2 \to (T)_2$.

Satz: Für $Q =$ die Ecken eines Einheitsquadrats: $\mathbb{R}^2 \not\to (Q)_2$.

Beweis: gleiche Streifenfärbung wie eben.

Satz: $Q =$ die vier Ecken eines Einheitsquadrats. Dann

$$\mathbb{R}^6 \to (Q)_2$$

Beweis: betrachte die 15 Punkte $x_{12}, x_{12}, \ldots, x_{56} \in \mathbb{R}^6$ mit den Koordinaten

$$x_{ijk} = \text{wenn } k = i \vee k = j \text{ dann } 1/\sqrt{2} \text{ sonst } 0$$

Das sind alle 15 Möglichkeiten, zweimal die $1/\sqrt{2}$ und viermal die 0 auf die 6 Koordinaten zu verteilen.

Übung: berechne die Abstände und Winkel zwischen diesen Punkten.

Antwort: Zwei dieser Vektoren unterscheiden sich wie x_{12}, x_{13} an zwei, oder wie x_{12}, x_{34} an 4 Koordinaten. Die Abstände sind $\sqrt{2 \cdot 1/\sqrt{2}^2} = 1$ bzw. $\sqrt{4 \cdot 1/\sqrt{2}^2} = \sqrt{2}$. Das sind die Seiten bzw. die Diagonalen von Einheitsquadraten, denn für alle a, b, c, d gilt: $x_{ab}x_{bc}$ steht senkrecht auf $x_{bc}x_{cd}$. (Beweis: Skalarprodukt ausrechnen.)

Wir finden darunter vier gleichfarbige Ecken eines Einheitsquadrates, wie folgt:

Wir wollen einen klassischen Ramsey–Satz für Graphen benutzen. Dort geht es aber um Kantenfärbungen. Wir müssen uns also aus der (Punkt-)Färbung dieser 15 Punkte des $\mathbb{R}^6$ eine Kantenfärbung eines geeigneten Graphen basteln. So etwas ähnliches passierte beim Beweis des Satzes von Schur.

Wir bauen einen K_6 auf den Knoten $v_1, \ldots, v_6$ und färben die Kante v_iv_j mit der Farbe des Punktes x_{ij}.

Wegen $R(C_4, C_4) = 6$ gibt es einen roten C_4, oBdA über die Knoten $v_1v_2v_3v_4$. Wir sehen, daß $x_{12}, x_{23}, x_{34}, x_{14}$ dann ein rotes Einheitsquadrat bilden.

Kompaktheit

11. Mai

Satz: $X \to (P)_c \iff$ es existiert eine endliche Menge $Y \subseteq X$ mit $Y \to (P)_c$.

(Das ist anschaulich klar aus den vorigen Beispielen: wir haben das gesuchte einfarbige P aus einer geeignet konstruierten endlichen Menge ausgewählt.)

Beweis: Wenn nicht, dann gibt es für jede endliche Menge $Y \subseteq X$ eine "schlechte" Färbung (ohne einfarbiges P). Wir können daraus eine schlechte Färbung für ganz X basteln.

Wir betrachten die Menge B aller schlechten Färbungen von Teilmengen von X. Sie ist halbgeordnet durch

$$f \leq g \iff \operatorname{domain} f = F \subseteq G = \operatorname{domain} g \wedge f = g|_F$$

Jede Kette (linear geordnete Menge von Färbungen) besitzt ein Supremum, das selbst wieder in B liegt. Nach dem Zornschen Lemma enthält dann B ein maximales Element. Das muß aber eine Färbung für ganz X sein, die schlecht ist.

Bemerkung: Solche Schlüsse trifft man öfter, zum Beispiel bei Endlichkeitssätzen in der Logik: eine Formelmenge ist erfüllbar $\iff$ jede endliche Teilmenge ist erfüllbar. Es heißt Kompaktheits–Argument, denn der "wahre" Grund ist der Satz von Tychonov: Das Produkt kompakter topologischer Räume ist kompakt.

Wo ist hier ein topologischer Raum? Wir haben die Menge $C = \{1, \ldots, c\}$ der Farben, und geben ihr die diskrete Topologie. Die Menge der c–Färbungen von X ist C^X und bekommt die Produkttopologie.

Ramsey–Mengen im $\mathbb{R}^n$

Wir können die Frage auch andersrum stellen (c festhalten und nach der Dimension fragen):

Definition: Eine Punktmenge P heißt Ramsey–Menge, wenn für jedes c ein m existiert, so daß

$$\mathbb{R}^m \to (P)_c$$

Satz: Jede Zweipunkt–Menge (die Enden eine Strecke) ist Ramsey.

Beweis: Betrachte einen Einheits–Simplex im $\mathbb{R}^c$.

(zur Erinnerung: Das sind $c+1$ Punkte mit allen paarweisen Abständen $= 1$. Anders gesagt: Ein 0–dimensionaler Simplex ist ein Punkt. Für $d > 0$: ein d–dimensionaler Simplex hat $d+1$ Eckpunkte und $d+1$ Seiten. Jede Seite ist ein $(d-1)$–dimensionaler Simplex.)

Definition: Für Mengen $A \subseteq \mathbb{R}^a, B \subseteq \mathbb{R}^b$ bedeutet 11. Mai

$$A \times B = \{(x_1, \dots, x_a, y_1, \dots, y_b) \mid (x_1, \dots, x_a) \in A \wedge (y_1, \dots, y_b) \in B\}$$

Satz: Wenn A und B Ramsey sind, dann auch $A \times B$.

Beweis: Gegeben ist die Farbzahl c. Wir müssen m finden, so daß $\mathbb{R}^m \to (A \times B)_c$.

Weil B Ramsey ist, gibt es ein b mit $\mathbb{R}^b \to (B)_c$. Nach obigem Satz existiert dann bereits eine endliche Teilmenge $Y \subseteq \mathbb{R}^b$ mit $Y \to (B)_c$. Die Anzahl der Elemente von Y ist y.

Nun ist auch A Ramsey, deswegen gibt es eine Zahl a mit $\mathbb{R}^a \to (A)_{c^y}$.

Wir setzen $m = a + b$. Betrachte eine beliebige Färbung f von $\mathbb{R}^m$. Definiere eine Färbung g des $\mathbb{R}^a$ durch

$$g(x_1, \dots, x_a) = [f(x_1, \dots, x_a, y_1, \dots, y_b) \mid \vec{y} \in Y]$$

D. h. g bildet einen Punkt $\vec{x}$ ab auf eine Liste (der Länge y) von Farben aus $\{1, \dots, c\}$. Das gibt c^y mögliche Farben.

Nach der Wahl von a enthält dann g eine einfarbige kongruente Kopie K von A.

Nach Konstruktion erhalten wir durch Einschränkung der Färbung f auf die Menge $K \times Y$ eine c–Färbung von Y.

Weiter enthält Y eine einfarbige kongruente Kopie L von B. Dann ist $K \times L$ die gesuchte Menge.

Definition: Für beliebige $a_i > 0$ nennen wir jedes kongruente Bild der Menge

$$\{(e_1 a_1, \dots, e_m a_m) \mid e_i \in \{0, 1\}$$

einen *Block* im $\mathbb{R}^m$.

Offensichtlich ist jeder Block ein Produkt von eindimensionalen Blöcken. Das sind aber Zweiermengen, und die sind Ramsey. Es folgt:

Satz: Jeder Block ist Ramsey.

Satz: Jede Teilmenge eines Blocks ist Ramsey.

Anwendung: Ein regulärer Tetrader ist Ramsey. Beweis: weil er in einen Würfel gelegt werden kann. (Läßt sich das verallgemeinern?)

Sphärische Mengen

18. Mai

Definition: Eine Menge $P \subseteq \mathbb{R}^m$ heißt *sphärisch*, wenn sie Teilmenge einer Kugeloberfläche ist.

Satz: Jede Ramsey–Menge ist sphärisch.

(Vermutung: Jede sphärische Menge ist Ramsey.)

Beweis: durch diese drei Aufgaben [Bol79].

18. Eine Menge $X = \{x_0, x_1, \ldots, x_l\} \in \mathbb{R}^n$ ist nicht sphärisch gwd. c_i existieren mit

$$\sum_1^l c_i(x_i - x_0) = 0$$

$$\sum_1^l c_i(|x_i|^2 - |x_0|^2) = b \neq 0$$

Lösung: Diese Aussagen sind äquivalent:

1. l Punkte liegen im $\mathbb{R}^n$ auf einer Kugel
2. beliebige $n+2$ davon liegen auf einer Kugel, wir nennen diese $x_0, x_1, \ldots, x_{n+1}$
3. die $n+1$ Mittel–Ebenen $M_1, \ldots, M_{n+1}$ mit $M_i = \{y \mid |y - x_0| = |y - x_i|\}$ haben einen Punkt m gemeinsam (vergleiche beim Dreieck die Mittelsenkrechten)

Für den Kugelmittelpunkt m gilt für alle i:

$$\langle m - (x_i + x_0)/2, (x_i - x_0)/2 \rangle = 0$$

Das schreiben wir als

$$\langle m, 2(x_i - x_0) \rangle = |x_i|^2 - |x_0|^2$$

Das ist ein System von $n+1$ Gleichungen für n Unbekannte (nämlich die Koordinaten von m). Das ist aus Dimensionsgründen "eigentlich nicht" lösbar, sondern gdw. seine Determinante $= 0$ ist.

Nehmen wir an, die x_* liegen nicht alle auf einer Kugel. Dann ist eines dieser Gleichungssysteme nicht lösbar, d. h. hat eine Determinante $\neq 0$.

Falls für alle $(c_1, \ldots, c_{n+1})$ mit $\sum c_i(x_i - x_0) = 0$ gilt, daß auch $\sum c_i(|x_i|^2 - |x_0|^2) = 0$, dann sind die Zeilen nicht linear unabhängig, also wird die Determinante doch 0.

Deswegen muß es $(c_1, \ldots, c_{n+1})$ geben, die die Forderung erfüllen. (Beachte: wir haben $n+2$ aus den l Vektoren ausgewählt. Die c_i der nicht ausgewählten setzen wir 0.

19. Für beliebige $b, c_1, \ldots, c_l \in \mathbb{R}$ mit $b \neq 0$, finde k und eine k–Färbung f von $\mathbb{R}^1$, so daß die Gleichung

$$\sum_1^l c_i(x_i - x_0) = b$$

keine Lösung hat, bei der $\{x_0, \ldots, x_l\}$ gleichfarbig sind.

Lösung: Wir bemerken, daß $x_0 = x_1 = \ldots = x_l$ niemals Lösung der Gleichung ist. Die Lösungsmenge liegt auf einer $(l-1)$–dimensionalen Hyperebene im $\mathbb{R}^l$, die die Gerade $x_0 = x_1 = \ldots = x_l$ nicht schneidet (also parallel zu ihr ist).

Für einfache Beispiele können wir die Lösung direkt hinschreiben. Beispiel: $1/4\ (x_1 - x_0) + 1/4\ (x_2 - x_0) = 1/2$.

Wir setzen 4 Farben an, mit Farbe $0 \leq i \leq 3$ für die Vereinigung der halboffenen Intervalle $\bigcup_{z\in\mathbb{Z}}[4z + i, 4z + (i + 1))$.

Dann ist für gleichfarbige x_i immer

$$\begin{aligned} 1/4\ (x_1 - x_0) &\in \mathbb{Z} + (-1/4, 1/4) \\ 1/4\ (x_2 - x_0) &\in \mathbb{Z} + (-1/4, 1/4) \\ 1/4\ (x_1 - x_0) + 1/4\ (x_2 - x_0) &\in \mathbb{Z} + (-1/2, 1/2) \end{aligned}$$

das ist ist aber disjunkt mit $\mathbb{Z} + 1/2$.

Das klappt immer, solange alle c_i und b rational sind (weil wir den Hauptnenner bilden). und wenn nicht?

20. Zeige: P ist nicht sphärisch $\Rightarrow$ P ist nicht Ramsey. Definiere dazu eine k–Färbung g für den $\mathbb{R}^n$ durch

$$g : \mathbb{R}^n \ni x \mapsto f(|x|^2)$$

Lösung. Das ist nach den Vorbereitungen klar. Falls g doch eine einfarbige kongruente Kopie $(y_0, \ldots, y_l)$ von P enthält, dann wäre das eine (in f) einfarbige Lösung der Gleichung $\sum c_i(z_i - z_0) = b$, und zwar mit $z_i = |y_i|^2$. Begründung:

Es gibt eine Matrix $A \in SO(n)$ mit $y_i = Ax_i + s$ d. h. wird drehen x_i um A und verschieben dann um $s \in \mathbb{R}^n$. Wir benutzen, daß A Längen erhält: $|Ax| = |x|$.

$$\begin{aligned} \sum c_i(|y_i|^2 - |y_0|^2) = \sum c_i(|Ax_i + s|^2 - |Ax_0 + s|^2) &= \\ \sum c_i(|Ax_i|^2 + |s|^2 + 2\langle Ax_i, s\rangle - |Ax_0|^2 - |s|^2 - 2\langle Ax_0, s\rangle) &= \\ \sum c_i(|x_i|^2 + |s|^2 + 2\langle Ax_i, s\rangle - |x_0|^2 - |s|^2 - 2\langle Ax_0, s\rangle) &= \\ \sum c_i(|x_i|^2 - |x_0|^2 + 2\langle A(x_i - x_0), s\rangle) &= \\ \sum c_i(|x_i|^2 - |x_0|^2 + 2\langle x_i - x_0, A^T s\rangle) &= \end{aligned}$$

$$\sum c_i(|x_i|^2 - |x_0|^2) + 2\left\langle \sum c_i(x_i - x_0), A^T s\right\rangle = \sum c_i(|x_i|^2 - |x_0|^2) = b$$

Beispiel: Wir setzen $X = \{x_0, x_1, x_2\} = \{1, 0, 2\}$ = drei Punkte im Abstand 1 (ein entartetes Dreick mit Seiten 1,1,2). Wir haben: X ist nicht sphärisch (weil dieses Dreieck keinen Umkreis hat) also sollte gelten (nach dem Satz): X ist nicht Ramsey. Welche Färbungen belegen das?

Es gilt

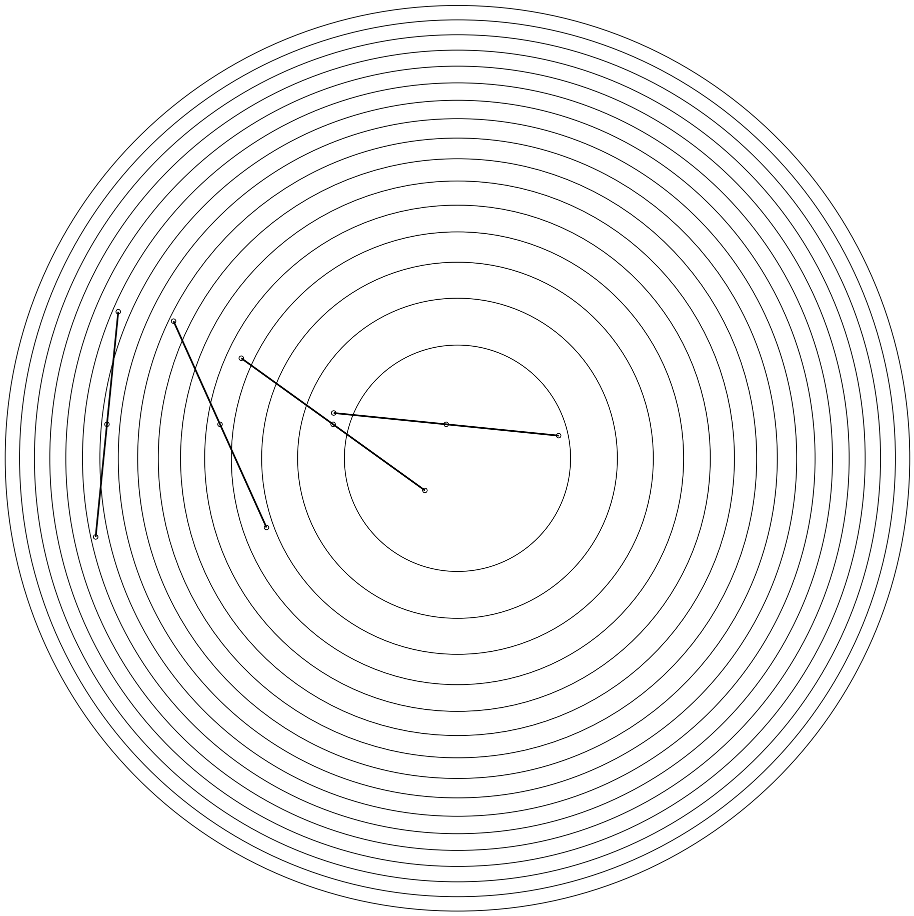
$$1/4\ (x_1 - x_0) + 1/4\ (x_2 - x_0) = -1/4 + 1/4 = 0,$$

aber

$$1/4\ (x_1^2 - x_0^2) + 1/4\ (x_2^2 - x_0^2) = -1/4 + 3/4 = 1/2 \neq 0.$$

Mit $c_1 = 1/4, c_2 = 1/4, b = 1/2$ werden also die Voraussetzungen obiger Sätze erfüllt. Die entsprechende Färbung f für den $\mathbb{R}^1$ ist genau die angegebene (mit 4 Farben). Daraus folgt, für jedes n, eine X–freie Färbung g für den $\mathbb{R}^n$, durch Kugelschalen (im $\mathbb{R}^2$ Kreisringe) mit Radien $\sqrt{1}, \sqrt{2}, \sqrt{3}, \sqrt{4}, \sqrt{5}, \ldots$

Übung: Man mache sich für den $\mathbb{R}^2$ klar, daß die Menge X weder radial noch tangential (relative zu den Kreisringen) einfarbig paßt. Siehe Bild.



Die Kurzschreibweise für das Resultat ist

$$\forall n : \quad \mathbb{R}^n \not\rightarrow (0, 1, 2)_4$$

Für beliebige $a, b > 0$ gilt

$$\forall n : \quad \mathbb{R}^n \not\rightarrow (0, a, a + b)_{16}$$

Es ist offen, ob sich die 4 oder die 16 durch eine kleinere Zahl ersetzen lassen [Gra97].

4.4 Arithmetische Folgen

18. Mai

Satz (Baudet, van der Waerden): Für alle l, c: Jede c–Färbung der natürlichen Zahlen $\mathbb{N}$ enthält eine einfarbige arithmetische Teilfolge der Länge l.

Kompakte Darstellung in [Bol79]. Ausführliche Beschreibung "Wie der Beweis gefunden wurde" in [vdW98] (online!) . Beweisidee: Induktion nach l. Induktionsanfang ($l = 2$) ist Schubfachschluß.

In [Gra97] finden wir diese Zahlenwerte für 2 Farben

l	1	2	3	4	5
$W(l, 2)$	1	3	9	35	178

Aus Spaß hier eine 3–Färbung ohne 3–Folgen (für 26 Zahlen) (demnach ist $3^3 \leq W(3, 3)$, ein Zufall?):

$$[3, 3, 1, 1, 3, 3, 1, 2, 1, 2, 2, 3, 2, 3, 3, 1, 3, 1, 1, 2, 3, 2, 2, 1, 2, 1]$$

und hier eine 2–Färbung ohne 4–Folgen (für 34 Zahlen):

$$[2, 2, 1, 2, 2, 2, 1, 1, 1, 2, 1, 1, 2, 1, 2, 2, 2, 1, 1, 1, 2, 1, 1, 2, 1, 2, 2, 2, 1, 1, 1, 2, 1, 1]$$

Die längste 2–Färbung ohne 5–Folge, die ich gefunden habe (einige Stunden Rechenzeit) hat erstmal nur 176 Stellen:

```
2221211122 2212222122 2211121222 1211211112 1121222121
1121221222 2122221112 1222121121 1112112122 2121112222
1222212212 1112122212 1121111211 2122212111 2222122221
2222111212 2211112111 121111
```

und hier noch eine 3–Färbung ohne 4–Folgen der Länge 127, also $W(4, 3) \geq 2^8$:

```
3133131312 2233133112 2332211121 1312123132 2233232322
3213311131 3311122311 1211222331 2323233232 3321221113
1133322212 1113222111 2112111
```

Ein explizites unteres Resultat ist für Primzahlen p

$$p \cdot 2^p \leq W(p + 1, 2)$$

(Berlekamp, 1990?) und andererseits gibt es die obere Schranke

$$W(m, 2) < A(4, m)$$

(Shelah, 1988?) wobei A eine Ackermann–Funktion ist:

$$\begin{array}{rl} m \geq 1 & A(m, 2) = 4 \\ n \geq 2 & A(1, n) = 2^n \\ m \geq 2, n \geq 3 & A(m + 1, n + 1) = A(m, A(m + 1, n)) \end{array}$$

Der original van der Waerdensche Beweis liefert eine Schranke von $A(m, m)$, also nicht primitiv rekursiv.

Graham (1970?) vermutet, daß man den "Ackermann–Exponenten" noch drücken kann: $W(m, 2) \leq A(3, m)$

Vergleichen wir diese Aussage mit den euklidischen Ramsey–Resultaten: damals durften wir *Kongruenz*abbildungen anwenden (drehen, verschieben, spiegeln), jetzt geht es um *homothetische* Abbildungen (zentrisch strecken und verschieben, aber nicht drehen) (das heißt, multiplizieren mit einer Diagonalmatrix, und Vektor addieren). Eine arithmetische Folge der Länge l ist ein homothetisches Bild der Menge $\{1, 2, \ldots, l\}$.

Tatsächlich gilt im allgemeinen dieser Satz (von Gallai): für alle endlichen Mengen M: für alle n, r: jede r–Färbung des $\mathbb{R}^n$ enthält ein homothetisches einfarbiges Bild von M.

(Bezüglich Homothetien ist also jede Menge "Ramsey".)

Es liegt nahe, die folgende Verschärfung des eben bewiesenen Satzes auszusprechen: Für alle l, c gibt es eine Zahl w, so daß jede c–Färbung der Zahlen $\{1, \ldots, w\}$ eine einfarbige arithemtische Folge der Länge l enthält, *und zwar in der Farbe, die insgesamt am häufigsten vorkommt.*

Das ist äquivalent zu einer Vermutung von Erdös und Turan (von 1940?): Jede Teilmenge M der natürlichen Zahlen mit positiver oberer Dichte, d. h.

$$\limsup \frac{|M \cap \{1..n\}|}{n} > 0$$

enthält beliebig lange arithmetische Folgen, die 1975 von E. Szemeredi bewiesen wurde.

Offen ist diese Vermutung von Erdös: Jede Teilmenge $M \subseteq \mathbb{N}$ mit

$$\sum_{m \in M} 1/m = \infty$$

enthält beliebig lange arithmetische Folgen.

Bemerkung: Die Summe der Reziproken der Primzahlen ist divergent. Wie findet man lange arithmetische Folgen von Primzahlen?

Für höhere Dimensionen vermutet Graham: Jedes $A \subseteq \mathbb{N}^2$ mit

$$\sum_{(x,y) \in A} 1/(x^2 + y^2) = \infty$$

enthält die Ecken eines achsenparallelen Quadrates, oder sogar, für alle k, ein homothetisches Bild von $\{1, 2, \ldots, k\}^2$.

Teil II

Kombinatorik auf Wörtern

Plan:

25. Mai	Einführung, Zerlegungssätze (Lyndon)
1. Juni	(Ausfall, Himmelfahrt)
8. Juni	(vermeidbare) Muster, Fixpunkte von Morphismen (Thue, Morse)
15. Juni	(Ausfall, Pfingsten?)
22. Juni	Sturmsche Wörter, mechanische Wörter
29. Juni	Halbgruppen, Gruppen, Burnside–Probleme

4.5 Wörter

25. Mai

Literatur: steht alles hier

- [Lot97b] Kapitel 1 (gibts online)
- [Lot97a] Kapitel 1 (auch online)
- [dLV99] Kapitel 1
- [CK97] = Kapitel 6 in [RS97] (Bibliothek)

4.5.1 endliche Wörter

Ein *Alphabet* ist eine (meistens endliche) Menge Σ.

Ein *Wort* w über dem Alphabet Σ ist eine endliche Folge $(w_1, \dots, w_n)$ von Elementen aus Σ. Die Zahl n heißt *Länge* des Wortes w, geschrieben $|w| = n$.

Es gibt genau ein Wort der Länge 0, das heißt *leeres Wort* und bekommt den Namen ϵ (oder 1, weil es das Einselement in Monoid ist).

Die Menge *aller* Wörter über Σ heißt Σ^*. Die Menge aller *nichtleeren* Wörter über Σ heißt Σ^+.

Auf Wörtern gibt es die binäre Operation *Verkettung* (Hintereinanderschreiben),

$$(u_1, \dots, u_m) \cdot (v_1, \dots, v_n) = (u_1, \dots, u_m, v_1, \dots, v_n)$$

Wir lassen den Punkt oft weg.

Das *Spiegelbild* eines Wortes $w = (w_1, \dots, w_n)$ ist

$$\tilde{w} = (w_n, \dots, w_1)$$

Ein Wort w mit $w = \tilde{w}$ heißt *Palindrom*.

4.5.2 Halbgruppen und Monoide

Eine *Halbgruppe* ist eine Menge M und darauf eine assoziative Operation. Das Paar $(\Sigma^+, \cdot)$ ist eine Halbgruppe.

Ein *Monoid* ist eine Halbgruppe $(M, \cdot)$ mit einem Element $e \in M$, für das

$$\forall x \in M: \; x \cdot e = e = e \cdot x$$

Das Tupel $(\Sigma^*, \cdot, 1)$ ist ein Monoid.

Ein *Homomorphismus* vom Monoid $(M, \cdot_M, 1_M)$ zum Monoid $(N, \cdot_N, 1_N)$ ist eine Abbildung $f : M \to N$ mit

$$\forall u, v \in M: \; f(u) \cdot_N f(v) = f(u \cdot_M v)$$

Daraus folgt auch $f(1_M) = 1_N$.

Die Abbildung "Wortlänge" ist ein Homomorphismus von $(\Sigma^*, \cdot, 1)$ nach $(\mathbb{N}, +, 0)$.

Die Identität ist ein Homomorphismus, und Hintereinanderausführung von Homomorphismen ist Homomorphismus, deswegen haben wir eine Kategorie mit den Monoiden als Objekten und den Homomorphismen als Pfeilen. In dieser Kategorie sind die Σ^* *initiale* Objekte (?) (genaue Definition hinschreiben) und heißen deswegen *freie* Monoide. (Beispiel: das Monoid $\mathbb{Z}/p\mathbb{Z}$ ist nicht frei.)

4.5.3 Halbordnungen

Ein Wort v ist *Faktor* eines Wortes w, geschrieben $v \subseteq w$, wenn $\exists x, y \in \Sigma^* : \; xvy = w$. Das Wort v ist *echter Faktor* von w, geschrieben $v \subset w$, wenn $v \subseteq w$ und $v \neq w$.

Ein Wort v ist *linker Faktor* oder *Präfix* von w, geschrieben $v \subseteq_L w$, wenn $\exists y \in \Sigma^* : \; vy = w$.

Enstprechend *rechter Faktor* oder *Suffix*, geschrieben $\subseteq_R$.

Ein Wort $v = (v_1, \ldots, v_m)$ ist *Teilwort* vom Wort $w = (w_1, \ldots, w_n)$, geschrieben $v \leq w$, wenn

$$\exists y_0 \in \Sigma^*, \ldots, y_m \in \Sigma^* : \; y_0 v_1 y_1 v_2 \ldots v_m y_m = w$$

Eine Halbordnung ist *Noethersch* oder *wohlfundiert*: es gibt keine unendliche echt absteigende Kette.

Beobachtung: Alle $\subseteq, \subseteq_L, \subseteq_R, \leq$ sind noethersche Halbordnungen auf Σ^*.

Eine Halbordnung $(M, \leq)$ ist ein *unterere Halbverband* (engl.: lower semilattice),

$$\forall x, y \in M : \exists i \in M : \; i \leq x \wedge i \leq y \wedge \forall j \in M : j \leq x \wedge j \leq y \rightarrow j \leq i$$

das heißt, je zwei Elemente x, y haben eine größte untere Schranke i (das *Infimum*). Sie ist dann sogar eindeutig, und heißt $\inf(x, y)$ oder $x \wedge y$.

(Entsprechend *oberer Halbverband*, *Supremum* oder $x \vee y$.)

Ein *Verband* ist gleichzeitig oberer und unterer Halbverband.

Beobachtung: $(\Sigma^*, \subseteq_L)$ ist ein unterer Halbverband, aber kein Verband.

4.5.4 Satz von Fine und Wilf

25. Mai

Eine *Potenz* entsteht durch iteriertes Anhängen, $x^n = x \cdot \ldots \cdot x$.

Satz: Für Wörter x und y mit $|x| = n, |y| = m$, setze $d = \gcd(n, m)$. Wenn ein Wort p sowie Zahlen r, s existieren mit

$$p \subseteq_L x^r \wedge p \subseteq_L y^s \wedge |p| \geq n + m - d,$$

dann sind x und y Potenzen des gleichen Worts, d. h. $\exists z, a, b : x = z^a \wedge y = z^b$.

Beweis: Zunächst können wir uns auf $d = 1$ beschränken. Wenn $\gcd(n, m) = d > 1$, dann nehmen wir immer d Buchstaben zusammen (betrachten also das Alphabet Σ^d).

Nun zeigen wir für $d = 1$, daß x und auch y unär sind (d. h. $|z| = 1$). Wir setzen o.B.d.A. $n > m$. (Falls $n = m$, ist die Behauptung sowieso klar, und falls $n < m$, tauschen wir x mit y.)

Der gemeinsame Präfix von x^r und y^s ist $p = (p_1, \ldots, p_{n+m-1})$. Wir wählen irgendein $i_0 \in \{1, \ldots, m\}$. Falls $i_0 + n < n + m$, gilt

$$y_{i_0} = x_{i_0} = x^r_{i_0+n} = y^s_{i_0+n} = y_{i_0+n \bmod m}$$

Wir nennen $i_1 = i_0 + n \bmod m$, und setzen fort. Das erzeugt eine Folge $(i_0, i_1, \ldots)$ mit $i_k = i + kn \bmod m$, und es gilt $y_{i_0} = y_{i_1} = \ldots$. Die Folge bricht ab, wenn $i_k + n = n + m$, also $i_k = m$. Es ist möglich, die i_0 so zu wählen, daß die Folge von i_0 bis i_{m-1} geht, weil die Kongruenz

$$i_0 + (m-1)n \equiv 0 \pmod{m}$$

wegen der Teilerfreiheit von m und n immer lösbar ist. Damit ist $\{i_0, \ldots, i_{m-1}\} = \{1, \ldots, m\}$ und deswegen stimmen alle Buchstaben von y überein, und natürlich alle Buchstaben von x ebenfalls.

Beispiel: Die angegebene Schranke $n + m - \gcd(n, m)$ ist scharf, wie wir hier sehen:

$$x = abaababa, |x| = 8, y = abaab, |y| = 5$$

d. h. x und y sind *nicht* Potenzen ein und desselben Wortes. Der längste gemeinsame Präfix von x^ω und y^ω ist

$$z = abaababaaba \subseteq_L \begin{array}{lcl} abaababa\ abaababa\ \ldots & = & x^\omega \\ abaab\ abaab\ abaab\ \ldots & = & y^\omega \end{array}$$

mit $|z| = 11 = 8 + 5 - 2$.

4.5.5 Lexikographische Ordnung

In diesem Abschnitt fixieren wir irgendeine lineare Ordnung $<$ auf Σ, beispielsweise $a < b < c < \ldots$ und $0 < 1 < ldots$.

Ein Wort u ist *lexikographisch kleiner* als ein Wort v, geschrieben $u <_{\text{lex}} v$, wenn

$$u \subset_L v \ \vee \ \exists w \in \Sigma^*, a, b \in \Sigma, x, y \in \Sigma^* : u = wax \wedge v = wby \wedge a < b$$

In diesem Abschnitt lassen wir den Index in $u <_{\text{lex}} v$ weg und schreiben $u < v$.

Beobachtung: $(\Sigma^*, \leq)$ ist eine lineare Ordnung, aber keine wohlfundierte.

Satz: Wenn $x, y, z \in \Sigma^*$ und $y \leq z$, dann auch $xy \leq xz$.

Satz: Wenn $x, y, u, v \in \Sigma^*$ und $x < y$ und $x \not\subseteq_L y$, dann $xu < yv$.

4.5.6 Konjugation

Zwei Wörter $u, v \in \Sigma^*$ heißen *konjugiert*, geschrieben $u \sim v$, wenn

$$\exists x, y \in \Sigma^* : u = xy \wedge yx = v.$$

Warum heißt das so? In der Gruppentheorie ist v konjugiert zu u, wenn $\exists w: \ v = w^{-1}uw$. Also gilt $v = (w^{-1}u)w$ und $u = w(w^{-1}u) = (ww^{-1})u$. Das sieht also so ähnlich aus. In Monoiden haben wir keine Inversen, darum die andere Formulierung.

Beispiele: vollständige Konjugationsklassen sind $abaab \sim baaba \sim aabab \sim ababa \sim babaa$ sowie $010101 \sim 101010$.

Satz: Zwei Wörter $x, y \in \Sigma^+$ sind konjugiert gdw.

$$\exists z \in \Sigma^* : \ xz = zy.$$

In diesem Fall gilt sogar

$$\exists u, v \in \Sigma^* : \ x = uv, y = vu, z \in u(vu)^*.$$

Beweis: Wenn $x = uv, y = vu, z = u(vu)^k$, dann folgt $xz = zy$ sofort. Andere Richtung: wenn $xz = zy$, dann $\forall k \geq 0 : x^k z = zy^k$. (Beweis durch Induktion: Anfang klar, Schritt: $x^{k+1}z = x^k xz = x^k zy = zy^k y = zy^{k+1}$.) Wir setzen $k = \lfloor |z|/|x| \rfloor$. Dann gilt $z = x^k u, x = uv, vz = y^{k+1}$. Damit ist $y^{k+1} = vz = vx^k u = v(uv)^k u = (vu)^{k+1}$. Deswegen gilt $y = vu$, und damit die Behauptung.

4.5.7 Lyndon–Wörter

Definition: ein Wort ist *prim* (oder *primitiv*), wenn es keine Potenz (mit Exponent > 1) eines anderen Wortes ist. 25. Mai

Beispiel: $abaab$ ist prim, $010101 = (01)^3$ ist nicht prim.

Definition: Ein Wort heißt *Lyndon–Wort*, wenn es prim ist und lexikographisch minimal in seiner Konjugationsklasse. Die Menge aller Lyndon–Wörter heißt L.

Beispiele: $aabab \in L$. Ist $0110101 \in L$? Nein. Sein Konjugat $(0101)(011)$ ist lexikographisch kleiner.

Satz: Ein Wort w ist Lyndon, genaudann, wenn es lexikographisch kleiner als jeder echte rechte Faktor von w ist.

Beweis: Sei $w = xy$ eine echte Zerlegung eines Lyndon–Wortes w. Wir haben $w < yx$. Wenn wir zeigen können, daß $y \not\subseteq_L w$, dann folgt $w < y$.

Falls also doch $y \subseteq_L w$, dann $\exists z : yz = w = xy$. Dann gilt $x \sim z$, und $\exists u, v, k : x = uv, z = vu, y \in u(vu)^k = (uv)^k u$. Es folgt $w = xy = (uv)^{k+1}u$.

Weil w prim ist, gilt $u \neq \epsilon$. Weil w kleiner als jedes Konjugat ist, gilt $w < u(uv)^{k+1}$. Wir kürzen den gemeinsamen Präfix u (wegen $a < b \leftrightarrow ua < ub$) und erhalten $(vu)^{k+1} < (uv)^{k+1}$. Diese Wörter sind gleichlang, also ist das linke kein Präfix vom rechten (falls doch, wäre $u = v$ und damit w nicht prim). Nach Eigenschaft der lexikographischen Ordnung dürfen wir von rechts mit u multiplizieren: $(vu)^{k+1}u < (uv)^{k+1}u = w$. Damit haben wir ein kleineres, zu w konjugiertes Wort gefunden, also war w nicht Lyndon.

Lemma: Wenn $y \in L$ und $x < y$, dann $xy < y$.

Beweis: Wenn $x \not\subseteq_L y$, dann folgt aus $x < y$ bereits $xy < y$. Also bleibt der Fall $x \subseteq_L y$. Wenn $x = y$, dann $xy = yy > y$. Deswegen $x \subset_L y$. Dann haben wir diese Zerlegung $y = xz$. Damit ist $xy = xxz$, und $xy < y$ ist äquivalent zu $y = xz < z$. Nun ist z ein echter Rechtsfaktor von y, und die Behauptung folgt wegen $y \in L$.

Satz: Wenn $x, y \in L$ und $x < y$, dann $xy \in L$.

Beweis: Wir zeigen, daß jeder echte rechte Faktor f von xy lexikographisch größer als xy ist:

Fall 1: $y \supset_R f$. Wegen $y \in L$ folgt $y < f$. Aus $x < y$ folgt (nach Lemma) $xy < y$, und daraus durch Transitivität $xy < y < f$.

Fall 2: $y = f$. Wie eben folgt $xy < y = f$.

Fall 3: $f = gy$ mit $x \supset_R g$. Wegen $x \in L$ ist $x < g$ und daraus sofort $xy < gy = f$.

Satz: $w \in \Sigma^+$ ist Lyndon, genaudann, wenn $|w| = 1$ oder $\exists x, y \in L$ mit $w = xy$ und $x < y$.

Bemerkung: das gibt eine rekursive Definition für L. Beachte, daß die dabei entstehenden Zerlegungen nicht eindeutig sind:

$$aabb = (aab)(b) = (a)(abb)$$

Beweis: Übung.

Theorem: Jedes Wort $w \in \Sigma^+$ besitzt genau eine Zerlegung als (nicht notwendig streng) monoton fallendes Produkt von Lyndon–Wörtern

$$w = l_1 l_2 \dots l_n,\ l_i \in L,\ l_1 \geq l_2 \geq \dots \geq l_n$$

Diese Zerlegung heißt *kanonisch*.

Existenzbeweis: Es gibt sicher Zerlegungen in Lyndon–Wörter, wenigstens die in einbuchstabige. Enthält eine Zerlegung zwei Faktoren mit $l_i < l_{i+1}$, dann können wir diese (nach Lemma) durch das Wort $l_i l_{i+1}$ ersetzen, das ebenfalls Lyndon ist.

Eindeutigkeit: Wir müssen noch zeigen, daß das Resultat nicht von der Reihenfolge dieser Operationen abhängt. Wenn

$$w = l_1 \dots l_n = k_1 \dots k_m$$

zwei verschiedene monotone Zerlegungen sind, die sich (von links gesehen) zum ersten mal an der Stelle i unterscheiden, dann ist o.B.d.A. $l_i \subset_L k_i$, und wir haben eine Zerlegung

$$l_i = k_i k_{i+1} \dots k_j r$$

für ein $r \subseteq_L k_{j+1}$. Dann folgt der Widerspruch $l_i < r \leq k_{j+1} \leq k_i < l_i$.

Konstruktion: Wir wählen l_n als den lexikografisch kleinsten rechten Faktor von w, (der ist immer ein Lyndon–Wort, beweisen wir gleich) und zerlegen den Rest weiter.

Beispiel: $w = 01011010011101$. Der kleinste rechte Faktor ist 0011101. Der Rest ist 0101101. Dessen kleinster rechter Faktor ist 01. Rest 01011. Kleinster rechter Faktor ist 01011 (das ganze Wort). Die Zerlegung ist also

$$01011\ 01\ 0011101.$$

Beweis der Konstruktion: Für ein $w \in \Sigma^+$ ist $w = xy$ mit y als dem lexikographisch kleinsten nichtleeren Rechtsfaktor von w. Wir müssen $y \in L$ zeigen. Nach Konstruktion gilt aber für jeden $f \subset_R y$, daß $y < f$.

4.6 Vermeidbare Muster

4.6.1 Muster

8. Juni

Definition: ein Wort $w \in \Sigma^*$ *enthält* ein Muster $m \in \Gamma^*$, geschrieben $m \ll w$, wenn Σ und Γ disjukte Alphabete sind und ein Morphismus $s : \Gamma \to \Sigma^+$ existiert mit $s(m) \subset w$.

Beispiel: Das Wort

$$01001010010010100101001001$$

enthält das Muster xxx, wegen des Morphismus $x \mapsto 010$.

Definition: das Muster m heißt *unvermeidbar* über dem Alphabet Σ, wenn jedes genügend lange Wort das Muster enthält:

$$\exists l : \forall w : |w| \geq l : m \ll w$$

Die kleinste solche Zahl l nennen wir $R_s(m)$, wobei $s = |\Sigma|$. Falls m in Σ vermeidbar ist, setzen wir $R_s(m) = \infty$.

Das ist also wieder die typische Ramsey–Form: genügend groß $\to$ enthält gewünschte Teilstruktur.

4.6.2 Unvermeidbare Muster

8. Juni

Definition: das Muster m heißt *unvermeidbar*, wenn es über *jedem* Alphabet unvermeidbar ist.

Typische Beispiele unvermeidbarer Muster sind $x, xyx, xyxzxyx$.

Satz: $m \in \Gamma^+$ unvermeidbar ist, und die Variable x nicht in m vorkommt, dann ist mxm unvermeidbar.

Beweis: Wir wählen $l = R_s(m)$ und betrachten ein Wort der Länge $(s^l+1)(l+1)-1 = s^l(l+1)+l$ Das können wir uns vorstellen als s^l+1 Stück von Wörtern der Länge l, die durch je einen Buchstaben getrennt sind.

$$(1,\ldots,l),(l+2,\ldots,2l+1),\ldots,(k(l+1)+1,\ldots k(l+1)+l),\ldots$$

Da es nur s^l verschiedene Wörter in Σ^l gibt, befinden sich unter diesen s^l+1 wenigstens zwei gleiche, und diese sind durch wenigstens einen Buchstaben getrennt. Jedes der beiden enthält zudem die gleiche Instant von m. Daraus folgt

$$R_s(m \cdot x \cdot m) \leq s^l(l+1)+l \quad \text{mit} \quad l = R_s(m)$$

Definition: die *Zimin–Muster* sind

$$Z_0 = \epsilon \qquad Z_k = Z_{k-1}x_kZ_{k-1}$$

Beispiel: $Z_3 = x_1x_2x_1x_3x_1x_2x_1$

Satz: Alle Z_k sind unvermeidbar.

Beispiel: Offensichtlich ist $R_2(Z_0) = 0$ und $R_2(Z_1) = 1$. Nach unserem Beweis ist $R_2(Z_2) \leq 2^1(1+1)+1 = 5$, und das ist auch exakt. Weiter ist $R_2(Z_3) \leq 2^5(5+1)+5 = 197$, aber durch tatsächliches Absuchen findet man $R_2(Z_3) = 29$.

4.6.3 Binäre Muster

8. Juni

Für den Fall, daß $|\Gamma| = |\Sigma| = 2$, ist die Vermeidbarkeit durch Arbeiten von Cassaigne (199?) vollständig geklärt.

Diese Muster sind unvermeidbar:

m	x	xy	x^2	x^2y	xyx	x^2yx	xy^2x	x^2y^2	$xyxy$	x^2yx^2	x^2yxy
$R_2(m)$	1	2	4	5	5	10	11	12	19	19	39

Beispiel: $x^2yxy \not\leq$ 10101010110011100011110000111000110010 (Länge 38).

Alle längeren binären Muster sind über zwei Buchstaben vermeidbar.

Wir werden sehen, daß xx über drei Buchstaben vermeidbar wird.

4.6.4 Entscheidbarkeiten

8. Juni

Die Frage

- gegeben $m \in \Gamma^+$
- gefragt: existiert ein s, so daß $R_s(m) = \infty$

ist entscheidbar (und nicht allzu kompliziert).

Die Entscheidbarkeit des Problems

- gegeben $m \in \Gamma^+$ und $s \in \mathbb{N}^+$
- gefragt: gilt $R_s(m) = \infty$

ist bis heute offen.

Es ist beispielsweise offen, ob $xxyyzz$ über zwei Buchstaben vermeidbar ist. Übungsaufgabe: schreibe ein Programm, das in kurzer Zeit ein möglichst langes Wort $w \in \{0,1\}^*$ ohne $xxyyzz$ berechnet. Die Größenordung von eine Minute für eine Million Stellen sollte erreichbar sein. Man muß das Wort ja nicht komplett ausgeben. Wähle eine geeignete Kodierung.

Definition: der *Index* eines Musters m ist die Zahl

$$I(m) \quad = \quad \min\{s \mid R_s(m) = \infty\}$$

Beispiele: $I(xx) = 3, I(abwbcxcaybazac) = 4$. Muster mit größerem (endlichen) Index sind nicht bekannt. Unvermeidbare Muster haben unendlichen Index: $I(xyx) = \infty$.

4.6.5 Unendliche Wörter

8. Juni

Die Unvermeidbarkeit eines Musters kann man ja durch vollständiges Absuchen feststellen. Wie ist es mit der Vermeidbarkeit? Dann müßte man einen Algorithmus angeben, der für jede Länge l ein Wort w herstellen kann, das das Muster nicht enthält.

Statt einer Menge immer längerer Wörter können wir auch ein einziges unendliches Wort betrachten.

Definition: Ein einseitig unendliches Wort über einem Alphabet Σ ist eine Abbildung $w : \mathbb{N} \to \Sigma$. Die Menge aller dieser Wörter ist Σ^ω. Wir bezeichnen $\Sigma^\infty = \Sigma^* \cup \Sigma^\omega$.

Die Operation $\cdot$ (Verkettung) dehnen wir aus auf den Typ $\Sigma^* \times \Sigma^\omega \to \Sigma^\omega$. Beachte: das linke Argument ist immer endlich. $(\Sigma^\omega, \cdot)$ ist damit kein Monoid mehr, denn das Produkt von zwei unendlichen Wörtern existiert nicht. Wenn wir unbedingt wollen, setzen wir für $u \in \Sigma^\omega$ immer $u \cdot v = u$. (Übung: ist es dann doch ein Monoid?)

4.6.6 Metrik

Wir erklären eine Abbildung $\rho : \Sigma^\infty \times \Sigma^\infty \to \mathbb{R}^+$ durch

$$\rho(u, v) = \text{ if } u = v \text{ then } 0 \text{ else } 2^{-l} \text{ where } l = \max\{|w| : w \subseteq_L u \wedge w \subseteq_L v\}$$

Satz: (Σ^∞, ρ) ist ein metrischer Raum.

Wir haben nicht nur die Dreiecksungleichung

$$\forall x, y, z \in \Sigma^* : \; \rho(x, y) + \rho(y, z) \geq \rho(x, z),$$

sondern sogar die *ultrametrische* Ungleichung

$$\forall x, y, z \in \Sigma^* : \; \max(\rho(x, y), \rho(y, z)) \geq \rho(x, z).$$

Satz: Der Raum (Σ^∞, ρ) ist kompakt.

Erinnerung: folgenkompakt: jede unendliche Folge hat einen Häufungspunkt; überdeckungskompakt: aus jeder unendlichen Überdeckung können wir eine endliche Teilüberdeckung auswählen.

Satz: Jede Folge $(w_0, w_1, \ldots)$ mit $w_i \in \Sigma^*$ und

$$\forall i < k : w_i \subset_L w_k$$

besitzt einen eindeutig bestimmten Grenzewert $w \in \Sigma^\omega$.

4.6.7 Faktoren von unendlichen Wörtern

Die Begriffe Faktor und linker Faktor übertragen wir direkt auf Σ^ω. Was ist mit rechten Faktoren? Wir könnten in $w = xy$ mit $w \in \Sigma^\omega, x \in \Sigma^*$ den linken Faktor x und den rechten Faktor y nennen, dann sind linke Faktoren eines unendlichen Wortes immer endlich, und rechte Faktoren immer unendlich. (Das brauchen wir aber nie.)

Definition: Für ein $w \in \Sigma^\infty$ bezeichnet $F(w)$ die Menge der Faktoren von w. Wir dehnen diese Bezeichnung auf Mengen von Wörtern aus:

$$F(M) \quad = \quad \{u \mid w \in M, u \subset w\}$$

Definition: eine Menge $M \subseteq \Sigma^*$ heißt *faktoriell*, wenn $F(M) \subseteq M$. (D. h. wenn sie alle ihre Faktoren enthält.)

Beispiel: für jedes $w \in \Sigma^\infty$ ist $F(w)$ faktoriell.

Satz: Zu jeder unendlichen faktoriellen Menge von Wörtern $M \subset \Sigma^*$ gibt es ein Wort $w \in \Sigma^\omega$ mit

$$F(w) \subseteq F(M)$$

Anwendung: Wenn es beliebig lange Wörter ohne ein Muster m gibt, dann sind das unendlich viele. Diese nehmen wir als M. Das nach Satz existierende Wort w hat nur Faktoren, die schon in M vorkommen, und enthält deswegen das Muster m auch nicht.

Beweis: Wir nehmen $F(M)$ als Knotenmenge eines Graphen. Wir ziehe eine gerichtete Kante $u \to v$, wenn es ein $x \in \Sigma$ sowie Zerlegung von einem $m \in M$ gibt, für die $ux = v \subset m$.

Dieser Graph ist

- Kreisfrei: wenn $u \to^+ v$, dann $|u| < |v|$,
- zusammenhängend: zu jedem $u = u_1 \dots u_n$ gibt es einen Pfad $\epsilon \to u_1 \to u_1 u_2 \to \dots \to u$.
- unendlich: M ist unendlich, und $M \subseteq F(M)$
- von endlichem Grad: Das Alphabet Σ ist endlich, also hat jeder Knoten $\leq |\Sigma|$ Nachfolger (und sowieso, bis auf ϵ, genau einen Vorgänger).

Nach dem Lemma von König gibt es dann in diesem Graphen einen unendlichen Pfad. Die Wörter (Faktoren) entlang dieses Pfades sind Präfixe voneineander, und bestimmen so ein unendliches Wort w mit den geforderten Eigenschaften.

4.6.8 Fixpunkte von Morphismen

8. Juni

Unsere Motivation ist, Vermeidbarkeit von Mustern m zu zeigen, indem wir ein unendliches m–freies Wort w direkt angeben. Eine Art, das zu tun, benutzt Fixpunkte von monotonen Morphismen.

Definition: Ein Morphismus $h : \Sigma \to \Sigma^*$ heißt *nichtlöschend*, wenn $\forall a \in \Sigma : 0 < |h(a)|$. Dann gilt auch $\forall w \in \Sigma^* : |w| < |h(w)|$.

Definition: $h : \Sigma \to \Sigma^*$ heißt *monoton in* $a \in \Sigma$, wenn $a \subseteq_L h(a)$, und *streng* monoton in a, falls $a \subset_L h(a)$.

Satz: Wenn $h : \Sigma \to \Sigma^*$ nichtlöschend und streng monoton in $a \in \Sigma$ ist, dann hat die Folge

$$w_0 = a, w_1 = h(a), \ldots, w_k = h^k(a), \ldots$$

einen Grenzwert $w \in \Sigma^\omega$.

Beweis: Wir setzen $h(a) = av$. Beachte, daß nach Definition der strengen Monotonie $v \in \Sigma^+$, und weil nicht gelöscht wird, $0 < |h^k(v)|$.

Dann gilt

$$w_k = h^k(a) = avh(v)h^2(v)\ldots h^{k-1}(v)$$

(Beweis: $h^{k+1}(a) = h(h^k(a)) = h(a)h(v)\ldots h(h^{k-1}(v)) = avh(v)\ldots h^k(v)$.)

insbesondere

$$\forall i < k : \qquad h^i(a) \subset_L h^k(a)$$

Somit existiert der Grenzwert.

Beispiel: Der Morphismus

$$\phi : 0 \mapsto 01, 1 \mapsto 0$$

ist nichtlöschend und monoton in 0. Also existiert $f = \phi^\omega(0)$. Wir rechnen die ersten Approximationen aus

$$\begin{aligned} f_0 &= 0 \\ f_1 &= \phi(0) = 01 \\ f_2 &= \phi(01) = 010 \\ f_3 &= \phi(010) = 01001 \\ f_4 &= \phi(01001) = 01001010 \\ f_5 &= \phi(01001010) = 0100101001001 \end{aligned}$$

Wir sehen $f_i \subset_L f_{i+1}$, in diesem Fall gilt sogar $f_i f_{i-1} = f_{i+1}$, wie man leicht durch Induktion bestätigt. Deswegen heißt f das Fibonacci–Wort.

4.6.9 Das Wort von Thue

8. Juni

Wir wollen zeigen, daß xx über drei Buchstaben vermeidbar ist. Wir konstruieren zunächst ein Wort $t \in \Sigma^\omega$, das xxx über zwei Buchstaben vermeidet.

Wir setzen t als den Limes $\tau^\omega(a)$ mit

$$\tau : a \mapsto ab, b \mapsto ba$$

Das Wort fängt so an

$$t = abbabaabbaababbabaababbaabbabaabbaababba\dots$$

Bemerkung: wir können, ähnlich wie beim Fibonacci–Wort, eine Zerlegung direkt angeben: für die Präfixe des Thue–Wortes $t_k = \tau^k(a)$ gilt

$$\begin{aligned} t_0 &= a, & u_0 &= b \\ t_{k+1} &= t_k u_k, & u_{k+1} &= u_k t_k \end{aligned}$$

Bemerkung: eine weitere äquivalente Darstellung ist: in $t = x_0 x_1 x_2 \dots$ gilt:

$$x_k = a \iff \text{die Binärdarstellung von } k \text{ enthält eine gerade Anzahl von 1}$$

Satz: t vermeidet *overlaps*. d. h. das Muster $xyxyx$, wobei ausnahmsweise y auch durch das leere Wort ersetzt werden darf.

Folgerung: t vermeidet xxx.

Beweis: Angenommen, t enthält overlaps $xyxyx$, Wir nehmen davon den kürzesten und am weitesten links liegenden. Es gibt dann ein k, so daß das Muster bereits in $t_k = \tau^k(a)$ liegt. Es genügt, wenn wir uns auf den Fall $|x| = 1$ beschränken (d. h. zeigen, daß dieser unmöglich ist).

Wir beachten, daß für die Buchstaben x_i von t immer gilt

$$x_i = x_{2i} \neq x_{2i+i}.$$

Die Buchstaben auf den geraden Plätzen folgen also aus denen auf ihren unmittelbaren rechten Nachbarn. Deswegen brauchen wir nur Muster zu betrachten, die auf einer geraden Position beginnen (die ungeraden können wir um eins nach links schieben).

Wenn *alle* x des Musters auf einer geraden Position sitzen dann finden wir das Muster bereits in t_{k-1} (d. h. eine Iteration früher). Es kann also die Länge von y keine ungerade Zahl sein.

Nehmen wir an, das Muster beginnt beim Index $2i$, O.B.d.A. ist $x_{2i} = a$. Die Mitte des Musters ist bei Index $2(i + d) + 1$ (dort steht also auch ein a).

Auf Position $2i + 1$ muß ein b stehen, dann aber auf $2(i + d) + 2$ ebenfalls (weil sich dort das y aus dem Muster wiederholt). Daraus folgt ein a an $2(i + d) + 3$, das erscheint auch an $2i + 2$, danaben auf $2i + 3$ wieder ein b, usw. Wiederholen wir das genügend oft, finden wir auf $2i + 2d + 1$ ein b, im Widerspruch zur Annahme.

4.6.10 Das Wort von Morse

8. Juni

Das ist ein unendliches Wort m über drei Buchstaben, das das Muster xx vermeidet. Es ist der Limes $\mu^\omega(0)$ des Morphismus

$$\mu \quad : \quad 0 \mapsto 012, 1 \mapsto 02, 2 \mapsto 1$$

und beginnt so

$$m = 012021012102012021020121012021012102\ldots$$

Satz: m ist *quadratfrei*, d. h. vermeidet das Muster xx.

Beweis: t ist ein homomorphes Bild von m. Wir zeigen: ein Quadrat in m ergibt dann einen overlap in t, dort sind aber keine.

Lemma: Für das Thue–Wort t und das Morse–Wort m:

$$t = h(m) \quad \text{mit} \quad h : 0 \mapsto abb, 1 \mapsto ab, 2 \mapsto a$$

Beweis: Wir müssen dazu diese Diagramme verifizieren:

$$\begin{array}{ccc} 0 & \xrightarrow{\mu} & 012 \\ h\downarrow & & h\downarrow \\ abb & \xrightarrow{\tau} & abbaba \end{array} \qquad \begin{array}{ccc} 1 & \xrightarrow{\mu} & 02 \\ h\downarrow & & h\downarrow \\ ab & \xrightarrow{\tau} & abba \end{array} \qquad \begin{array}{ccc} 2 & \xrightarrow{\mu} & 1 \\ h\downarrow & & h\downarrow \\ a & \xrightarrow{\tau} & ab \end{array}$$

Lemma: Wenn m das Muster xx enthält, dann enthält t einen overlap.

Beweis: Also gilt $m = uxxv$. Dann ist $t = h(u)h(x)h(x)h(v)$. Beachte, daß $h(x)$ und $h(v)$ in jedem Fall mit a beginnen.

Aufgabe 3.1.5** aus [Lot97a] Wenn ein Muster vermeidbar ist, dann wird es durch ein homomorphe Bild des Fixpunktes eines geeigneten Morphismus vermieden. (Vergleiche Aufgabe 3.1.4: ohne hom. Bild geht es nicht.)

Eine Motivation für die Betrachtung quadrat– und kubikfreier Wörter war eine Turnierschach–Regel (zu Anfang dieses Jahrhunderts): wenn eine Folge von Zügen zum dritten mal direkt hintereinander auftritt, wird die Partie abgebrochen. Nun gibt es aber kubikfreie Wörter (bereits auf 2 Buchstaben), also gibt es nach dieser Regel unendliche Spiele, bei denen sich trotzdem nur wenige Züge abwechseln.

Eine andere Motivation ist die Untersuchung diskreter dynamischer Systeme: die Beschreibungsgrößen sind im einfachsten fall schließlich konstant, oder sie oszillieren, oder sie folgen keinem offensichtlichen Muster. Vielleicht vermeiden sie dann "offensichtlich" ein Muster, weil sie (die Folge ihrer Werte) Fixpunkte von Morphismen sind.

Zu Morphismen müßte man noch viel mehr sagen. Ihre Untersuchung bildet einen eigenen Teil der Theorie formaler Sprachen. (siehe Postsches Korrespondenzproblem, (H)D0L–Systeme, Lösbarkeit von Wortgleichungen, Baumgleichungen, Unifizieren und Matching höherer Ordnung). Dort geht es immer hübsch knapp an der Unentscheidbarkeit vorbei.

4.7 Sturmsche Wörter

4.7.1 Die Struktur des Fibonacci–Worts

22. Juni

Zur Erinnerung. Definition:

$$\phi : 0 \mapsto 01, 1 \mapsto 0, f_n = \phi^n(0), f = \lim f_n$$

Satz:

$$f_0 = 0, f_1 = 01, f_{n+2} = f_{n+1} \cdot f_n$$

Beweis durch Induktion. Anfang durch Ausrechnen. Schritt:

$$\begin{aligned} f_{n+2} &= \phi f_{n+1} = \phi(f_n \cdot f_{n-1}) \\ &= \phi f_n \cdot \phi f_{n-1} = f_{n+1} \cdot f_n \end{aligned}$$

Definition (nur für diesen Abschnitt): für $n \geq 1$:

$$f_n = g_n \cdot t_n \text{ wobei } |t_n| = 2$$

Satz:

1. $t_n =$ wenn $2|n$ dann 10 sonst 01
2. $n \geq 1 : \; g_{n+2} = f_n g_{n+1} = f_{n+1} g_n$
3. g_n ist ein Palindrom
4. $g_{n+2} = g_{n-1} \tilde{f}_n \tilde{f}_n$

Beweis: Teil 1: $\phi(01) = 010 \supset_R 10$ und $\phi(10) = 001 \supset_R 01$.

Teil 2: Wegen $f_{n+2} = f_{n+1} f_n$ und der Definition gilt für $|f_n| \geq 2$

$$g_{n+2} = f_{n+1} g_n$$

Also ist

$$\begin{aligned} g_{n+3} &= f_{n+2} g_{n+1} = f_{n+2} f_{n-1} g_n \\ &= f_{n+1} f_n f_{n-1} g_n = f_{n+1} f_{n+1} g_n = f_{n+1} g_{n+2} \end{aligned}$$

Teil 3:

$$\begin{aligned} \widetilde{g_{n+2}} &= \widetilde{f_n g_{n+1}} = \widetilde{g_{n+1}} \widetilde{f_n} \\ &= g_{n+1} \widetilde{g_n t_n} = g_{n+1} \widetilde{t_n} \widetilde{g_n} \\ &= g_{n+1} t_{n+1} g_n = f_{n+1} g_n = g_{n+2} \end{aligned}$$

Teil 4:

$$\begin{aligned} g_{n+2} = \widetilde{g_{n+2}} &= \widetilde{f_n g_{n+1}} = \widetilde{g_{n+1}} \widetilde{f_n} \\ &= \widetilde{f_n g_{n-1}} \widetilde{f_n} = \widetilde{g_{n-1}} \widetilde{f_n} \widetilde{f_n} = g_{n-1} \widetilde{f_n} \widetilde{f_n} \end{aligned}$$

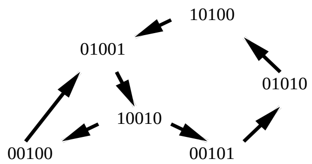
4.7.2 Faktorgraphen

22. Juni

Definition: Der *Faktorgraph* $F_n(w)$ der Länge n eines Wortes $w \in \Sigma^\omega$ besteht aus

- Knoten $\{u \mid u \subset w, |u| = n\}$
- gerichteten Kanten $u \to v$ falls $\exists x, y \in \Sigma$ mit $ux = yv$.

Beispiel: Der Graph $F_5(f)$ für das Fibonacci–Wort



Satz: Jeder Knoten hat wenigstens einen Nachfolger.

Beweis: das Wort w ist unendlich.

Satz: Der Graph ist zusammenhängend. Für beliebige u, v gilt entweder $u \to^+ v$ oder $v \to^+ u$.

Beweis: Eine beliebige Instanz von u steht rechts oder links von einer beliebigen Instanz von v.

Definition: die *Komplexität* $P_n(w)$ eines Wortes $w \in \Sigma^\omega$ ist die Knotenzahl des Faktorgraphen $F_n(w)$.

4.7.3 Periodische Wörter

Definition: ein Wort $w \in \Sigma^\omega$ heißt *schließlich periodisch*, wenn $\exists u, w \in \Sigma^* : \ w = uv^\omega$. Alle anderen Wörter aus Σ^ω heißen *aperiodisch*.

Satz: Ein Wort $w \in \{0,1\}^\omega$ ist periodisch $\iff \exists n : P_n(w) \le n$.

Beweis: $\Rightarrow$: Wenn $w = uv^\omega$, dann $\forall n : P_n(w) \le |uv|$.

$\Leftarrow$: Wir haben sicher $P_1(w) = 2$ (sonst bestünde das Wort nur aus einem Buchstaben und wäre sofort periodisch).

Weiter ist $\forall n : P_n(w) \le P_{n+1}(w)$, weil jeder Faktor der Länge n ein Präfix eines Faktors der Länge $n+1$ ist.

Nach Voraussetzung soll $\exists n : P_n(w) \le n$. Dann $\exists m : P_m(w) = P_{m+1}(w)$. Falls nicht, wäre $\forall m : P_m(w) < P_{m+1}(w)$, und deswegen $\forall m : m < P_m(w)$.

Jedes $u \in F_m(w)$ ist Präfix von wenigstens einem $v \in F_{m+1}(w)$. Da beide Graphen gleichgroße Knotenmengen haben, ist jedes $u \in F_m(w)$ Präfix von *genau einem* $v \in F_{m+1}(w)$. Das bedeutet, daß in $F_m(w)$ jeder Knoten *genau einen* Nachfolger hat.

Damit sind aber die starken Zusammenhangskomponenten Kreise, und jedes unendliche Wort muß in so einem Kreis "landen". Damit hat es die Form uv^ω.

Die "einfachsten" aperiodischen Wörter haben also lineare Komplexität. Die periodischen haben beschränkte, und dazwischen gibts nichts. Deswegen heißt das "Gap–Theorem".

4.7.4 Aperiodische Wörter minimaler Komplexität

22. Juni

Definition: ein unendliches Wort w heißt *Sturmsches Wort*, wenn es für jedes n genau $n+1$ Faktoren der Länge n hat.

$$\forall n \geq 0 \qquad P_n(w) = n+1$$

Folgerung: dann gibt es genau zwei Faktoren der Länge eins, das sind aber Buchstaben, d. h. das Alphabet hat genau die Größe 2, wir nehmen meist $\Sigma = \{0, 1\}$.

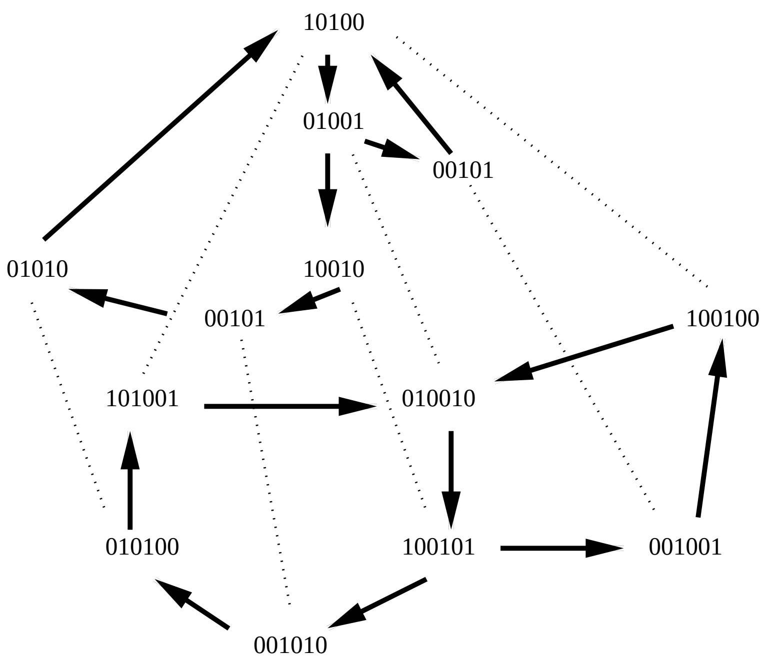
Beispiel: das Fibonacci–Wort ist Sturm (Beweis folgt)

Definition: ein Faktor u eines binären Wortes $w \in \Sigma^\omega$ heißt *rechtsverzweigt*, wenn auch $u0 \subseteq w$ und $u1 \subseteq w$. Alle anderen Faktoren heißen *rechtseindeutig*.

Im Faktorgraphen haben die rechtseindeutigen Faktoren genau einen Nachfolger, die rechtsverzweigten zwei.

Satz: w ist Sturm $\iff$ w enthält von jeder Länge genau einen rechtsverzweigten Faktor (r.v.F.)

Beweis: betrachte die Relation $\subset_L$ zwischen den Knoten von $F_n(w)$ und $F_{n+1}(w)$. Vorsicht, das Bild stimmt nicht



Um zu zeigen daß das Fibonacci–Wort ein Sturmsches Wort ist, benötigen wir zwei Resultate (*wenigstens* einen und *höchstens* einen r.v.F.) Das eine geht jetzt schon, für das andere brauchen wir einen neuen Abschnitt (über Balance).

Satz: Das Fibonacci–Wort f enthält für jedes n wenigstens einen r.v.F. der Länge n

Beweis: Da jeder Suffix eines r.v.F. selbst r.v.F. ist, genügt es, beliebig lange r.v.F. zu finden. Die Folge der gespiegelten Fibonacci–Wörter liefert diese! Im vorigen Abschnitt hatten wir die Zerlegung $g_{n+2} = g_{n-1}\tilde{f}_n\tilde{f}_n$, also

$$f_{n+2} = g_{n-1}\tilde{f}_n\tilde{f}_n t_{n+2}$$

Weil sich die Anfangsbuchstaben von $t_{n+2} = t_n$ und $\tilde{f}_n$ immer unterscheiden, ist $\tilde{f}_n$ ein r.v.F.

4.7.5 Balancierte Wörter

22. Juni

Definition: die *Höhe* $h(w)$ eines Wortes $w \in \{0,1\}^*$ ist die Anzahl der 1 in w.

Definition: die *Balance* $\delta(x,y)$ zweier binärer Wörter $x, y \in \{0,1\}^*$ ist

$$\delta(x,y) \quad = \quad |h(x) - h(y)|$$

Definition: eine Menge M von Wörtern ist *balanciert*, wenn

$$\forall x, y \in M : |x| = |y| \to \delta(x,y) \leq 1$$

Definition: ein Wort $w \in \{0,1\}^\omega$ ist *balanciert*, wenn die Menge $F(w)$ seiner Faktoren balanciert ist.

Satz: Für jede faktorielle Menge $M \subseteq \{0,1\}^*$ gilt:

$$M \text{ ist nicht balanciert} \quad \iff \quad \exists w : w = \widetilde{w} \wedge 0w0 \in M \wedge 1w1 \in M$$

Beweis: Die Richtung $\Leftarrow$ ist klar, weil $|0w0| = |1w1|$ und $\delta(0w0, 1w1) = 2$.

Für Richtung $\Rightarrow$: betrachte ein kürzestes Paar $x, y \in M$ mit $|x| = |y|$ und $\delta(x,y) > 1$. (Wir nennen solche (x,y) ein *schiefes Paar*.)

Die Wörter x und y haben keinen gemeinsamen Präfix (sonst könnten wir ihn weglassen und hätten ein kürzeres schiefes Paar) und aus dem gleichen Grund keinen gemeinsamen Suffix.

Damit bleiben die Möglichkeiten $(0u0, 1v1), (0u1, 1v0)$ sowie vertauschte. Der zweite Fall kann aber nicht eintreten: wegen $2 \leq \delta(0u1, 1v0) = \delta(u,v)$ ist (u,v) ein kürzeres schiefes Paar. Also gilt o.B.d.A. $x = 0u0, y = 1v1$. Die zu zeigende Behauptung folgt, wenn wir $u = v$ und $u = \tilde{v}$ nachweisen können.

beachte: $u = v$ und $u = \tilde{v}$

Nehmen wir an, daß $u \neq \tilde{v}$. Da beide Wörter gleichlang sind, haben sie einen gemeinsamen Präfix p und unterscheiden sich in den dann folgenden Buchstaben

$$\begin{array}{ll} \exists p \in \{0,1\}^*; a, b \in \{0,1\}, a \neq b; r, s \in \{0,1\}^* \qquad & u = par, \quad \tilde{v} = pbs \\ & x = 0par0, \quad y = 1\tilde{s}b\tilde{p}1 \end{array}$$

Falls nun $a = 0, b = 1$, dann haben wir mit $(0p0, 1\tilde{p}1)$ ein kürzeres schiefes Paar.

Deswegen ist $a = 1, b = 0$. Daraus folgt aber $\delta(r0, 1\tilde{s}) = \delta(0par0, 1\tilde{s}b\tilde{p}1) \geq 2$ wiederum ein kürzeres schiefes Paar.

(Der Beweis für $u = v$ geht ganz genauso. Aus beiden zusammen folgt $u = \tilde{u}$, und damit die Behauptung.)

29. 6.

Lemma: Für das Fibonacci–Wort f gilt

$$\nexists w \in \Sigma^* \qquad 0w0 \subset f \wedge 1w1 \subset f$$

Beweis (durch Induktion nach $|w|$): Für $|w| = 0$, also $w = \epsilon$ ist das klar, denn $11 \not\subset f$.

Für $|w| = 1$: Falls $w = 0$: wir zeigen $000 \not\subset f$: Falls doch $f = u \cdot 000 \cdot \ldots$, dann muß $f = \phi(u') \cdot \phi(11) \cdot \ldots$ sein, aber $11 \not\subset f$.

Falls $w = 1$: wir haben schon $11 \not\subset f$, also erst recht $111 \not\subset f$.

Induktionsschritt: Nimm an, w ist ein kürzestes Wort mit $0w0 \subset f$ und $1w1 \subset f$.

Aus $1w1 \subset f$ und $11 \not\subset f$ folgt $w = 0x0$. Wegen $0w0 \subset f$ folgt $00x00 \subset f$. Aus $000 \not\subset f$ folgt $x = 1y1$. Wir haben also diese beiden Faktoren

$$0w0 = 001y100 \subset f, \qquad 1w1 = 101y101 \subset f$$

Wegen $11 \not\subset f$ können wir rechts sogar schreiben $0101y101 \subset f$.

Betrachten wir die 1 nach dem y. Wegen der Struktur von ϕ muß diese aus $0 \mapsto 01$ entstanden sein. Die beiden Faktoren haben diese Zerlegung

$$\begin{array}{rl}
0w0 = 0\ 01\ y1\ 0\ 0 \subset f & 01w1 = 01\ 01\ y1\ 01 \subset f \\
0w0 = \phi(1)\ \phi(0)\ \phi(z)\ \phi(1)\ 0 \subset f & 01w1 = \phi(0)\ \phi(0)\ \phi(z)\ \phi(0) \subset f \\
0w0 = \phi(10z1)\ 0 \subset f & 01w1 = \phi(00z0) \subset f
\end{array}$$

wobei wir $\phi(z) = y1$ gesetzt haben. Nun sehen wir, daß für das Wort $w' = 0z$ ebenfalls $0z0 \subset f$ und $1z1 \subset f$ gilt. Es ist aber $|w'| = 1 + |z| \leq 1 + |\phi(z)| = |y1| < |1y1| = |x| < |w|$, also war w nicht das kürzeste Wort mit der gesuchten Eigenschaft.

Satz: Das Fibonacci–Wort ist balanciert.

Beweis: Wenn f nicht balanciert wäre, gäbe es ein Palindrom w mit $0w0 \subset f$ und $1w1 \subset f$. Das ist aber nach vorigem Satz (nicht nur für Palindrome) unmöglich.

Satz: Für alle balancierten Wörter $w \in \{0,1\}^\omega$ gilt: w enthält zu jeder Länge höchstens einen rechtsverzweigten Faktor.

Beweis (indirekt): Falls x und y gleichlange, verschiedene rechtsverzweigte Faktoren sind dann gibt es eine Zerlegung $x = uaw, y = vbw$ mit $a \neq b$ (w ist der längste gemeinsame Suffix). Dann haben wir aber die vier verschiedenen Faktoren $0w0, 0w1, 1w0, 1w1$ von f. Die Faktoren $0w0$ und $1w1$ können aber nicht beide in einem balancierten Wort auftreten.

Folgerung: Das Fibonacci–Wort ist ein Sturmsches Wort.

4.7.6 Sturmsche Wörter als balancierte aperiodische

29. Juni

Satz: Die folgenden Bedingungen sind äquivalent

- w ist Sturmsches Wort
- w ist balanciert und aperiodisch

Beweis "$\Leftarrow$": Wenn w aperiodisch ist, dann $\forall n : P_n(w) \geq n+1$. Wenn w balanciert ist, dann zeigen wir $P_n(w) \leq n+1$. Daraus folgt $P_n(w) = n+1$, also die Behauptung.

(Falls nicht: sei n die kleinste Zahl, für die $P_n(w) > n+1$. Betrachte $Y = F_{n-1}(w)$ und $Z = F_n(w)$. Dann ist $|Y| \leq n$ und $|Z| \geq n+2$. Jeder Suffix der Länge $n-1$ eines Wortes aus Z ist in Y. Nach Schubfachschluß gibt es Wörter $y \neq y' \in Y$, so daß $0y, 0y', 1y, 1y' \in Z$, denn in jedes Schubfach (Wort in Y) passen nur zwei Wörter (aus Z) — es müssen also zwei Fächer überfüllt sein. Weil $y \neq y'$ und gleichlang, gibt es x, so daß $x0$ und $x1$ Präfixe von y und y' sind. Damit haben wir $0x0$ und $1x1$ in Z, also w nicht balanciert.)

Beweis "$\Rightarrow$": Zu zeigen ist Sturm $\to$ aperiodisch (das ist einfach: nach Definition gilt Sturm $\to \neg\exists n : P_n(w) \leq n$) und Sturm $\to$ Balance. Wir dürfen dabei sogar schon die Aperiodizität verwenden.

Für einen indirekten Beweis nehmen wir an, w ist Sturm und nicht balanciert. Wir müssen nachweisen, daß dann w periodisch ist:

Nach Voraussetzung enthält w Faktoren $0x0, 1x1$ mit x Palindrom. Deswegen ist x rechtsverzweigend. Weil w Sturm ist, hat es genau einen rechtsverzweigenden Faktor jeder Länge, also auch der Länge $1+|x|$. Dieser ist entweder $0x$ oder $1x$. O.B.d.A. ist es $0x$. Dann sind dieses Faktoren von w, und jener nicht:

$$0x0, 0x1, 1x1 \subset w, \qquad 1x0 \not\subset w$$

Wir setzen $n = |1x|$ und betrachten irgendein Vorkommen von $1x1$ sowie das Wort y aus den $(n-1)$ direkt nachfolgenden Buchstaben

$$v \;=\; 1x1y \subset w$$

Wir zeigen $0x \not\subset v$ (indirekt). Falls doch, dann hätten wir eine Zerlegung

$$\begin{array}{rcccccl}
1| & & x & & |1| & & y \\ \hline
1| & a & |0| & b & |1| & c| & \\ \hline
 & & |0| & & x & & |
\end{array}$$

Durch Abzählen finden wir, daß $|a| = |c|$. Nach Voraussetzunng ist x ein Palindrom, das ergibt einen Widerspruch für den Buchstaben nach a, d. h. vor c.

Da w ein Sturmsches Wort ist, besitzt es genau $n+1$ Faktoren der Länge n. Einer davon, nämlich $0x$, kommt in v nicht vor. Alle, die doch in v vorkommen, sind demnach höchstens n Stück, und alle sind rechtseindeutig. (Denn $0x$ ist der einzige rechtsverzweigte.) Nun ist $|v| = 2n$, also kommt einer dieser Faktoren in v sogar doppelt vor. Damit liegt aber auch die weitere Fortsetzung (in w) fest, und w ist schließlich periodisch.

4.7.7 Steigung von unendlichen Wörtern

29. Juni

Definition: Der *Anstieg* eines Wortes $w \in \{0,1\}^+$ ist

$$\pi(w) = \frac{h(w)}{|w|}$$

Beispiel: Für das k–te Fibonacci–Wort $f_k = \phi^k(0)$ gilt

$$|f_k| = F_{k+1}, \qquad h(f_k) = F_{k-1}$$

wobei F_n die Fibonacci–Zahlen sind:

$$\begin{aligned} (F_0, F_1, \ldots) &= (0,1,1,2,3,5,8,\ldots) \\ F_0 = 0, F_1 = 1, &\quad F_{n+2} = F_{n+1} + F_n \\ F_n = \frac{1}{\sqrt{5}}(\tau^n - (-\tau)^{-n}) &\quad \text{mit} \quad \tau = (1+\sqrt{5})/2 \end{aligned}$$

($\tau = 1.618\ldots$ ist der Goldene Schnitt.) Der Anstieg des k–ten Fibonacci–Worts ist F_{k-1}/F_{k+1}.

Satz: Eine faktorielle Wortmenge M ist balanciert genau dann, wenn

$$\forall v, w \in M \setminus \{\epsilon\} \qquad |\pi(v) - \pi(w)| < \frac{1}{|v|} + \frac{1}{|w|}$$

Beispiel: Wir nehmen v als f_4 ohne den letzten Buchstaben, $v = 0100101$, und w als f_3 ohne den letzten Buchstaben, $w = 0100$.

$$|\pi(v) - \pi(w)| = |3/7 - 1/4| = 5/28 < 11/28 = 1/7 + 1/4 = \frac{1}{|v|} + \frac{1}{|w|}$$

Beweis: "$\Leftarrow$": Zu zeigen ist $|v| = |w| \to |h(v) - h(w)| \le 1$. Nach Voraussetzung ist

$$|\pi(v) - \pi(w)| = \frac{|h(v) - h(w)|}{|v|} < \frac{2}{|v|}$$

das ist direkt die Behauptung.

"$\Rightarrow$": durch Induktion nach $|v| + |w|$.

Anfang: $|v| = |w| = l$. Das ist einfach die Umkehrung der vorigen Zeile.

Schritt: o.B.d.A. ist $|v| < |w|$. Dann zerfällt $w = v' \cdot z$ mit $|v'| = |v|$. Es ist

$$\begin{aligned} |w|h(v) - |v|h(w) &= (|v| + |z|)h(v) - |v|(h(v') + h(z)) \\ &= |v|(h(v) - h(v')) + |z|h(v) - |v|h(z) \\ |w|h(v) - |v|h(w) &\le |v| \cdot 1 + (|z| + |v|) = |v| + |w| \end{aligned}$$

Beachte: diese Induktion enstpricht dem Euklidischen Algorithmus: wir ziehen die kleinere Zahl (Wortlänge) von der größeren ab, solange, bis beide gleichgroß sind.

Folgerung: Für eine unendliches Wort $w \in \{0,1\}^\omega$ bezeichnet w_k den Präfix der Länge k. Dann existiert der Grenzwert

$$\alpha = \lim_{k\to\infty} \pi(w_k)$$

Definition: Diese Zahl α heißt *Anstieg* $\pi(w)$.

Offensichtlich genügt es, den Limes über eine beliebige Folge von Faktoren steigender Länge zu nehmen (das sind nach obigem Satz alles Cauchy–Folgen).

Beispiel: das Fibonacci–Wort f enthält die Faktoren $f_1, f_2, \ldots$. Wir haben

$$\pi(f) = \lim \pi(f_k) = \lim F_{k-1}/F_{k+1} = \tau^{-2} = 0.381966\ldots$$

Satz: Für jedes unendliche balancierte Wort w mit Anstieg $\alpha = \pi(w)$:

$$\forall u \subset w : \qquad |\pi(u) - \alpha| \leq \frac{1}{|u|}$$

Beispiel: Wir nehmen den Faktor $u = 100101001$ des Fibonacci–Worts. Es gilt $\pi(u) = 4/9 = 0.4444\ldots$ und $\pi(u) - \alpha = 0.4444\ldots - 0.381966\ldots = 0.06\ldots < 1/9$.

Beweis: Die Behauptung folgt aus dem folgenden

Lemma: Es gilt genau eine der beiden Zeilen

$$\begin{array}{ll} \forall u \subset w : & \alpha|u| - 1 < h(u) \leq \alpha|u| + 1 \\ \forall u \subset w : & \alpha|u| - 1 \leq h(u) < \alpha|u| + 1 \end{array}$$

Beweis: (zunächst für $\leq$ auf beiden Seiten) Betrachte ein $u \cdot v \subset w$. Wir zeigen

$$\frac{h(u) - 1}{|u|} < \frac{h(u) + h(v)}{|u| + |v|}$$

(Falls nicht, wäre

$$\begin{aligned} \frac{h(u) - 1}{|u|} &\geq \frac{h(u) + h(v)}{|u| + |v|} \\ (|u| + |v|)(h(u) - 1) &\geq |u|(h(u) + h(v)) \\ |v|h(u) - (|u| + |v|) &\geq |u|h(v) \\ |v|h(u) - |u|h(v) &\geq |u| + |v| \end{aligned}$$

Das ist ein Widerspruch zu früherem Satz.) Jetzt lassen wir v immer länger werden. Dann gilt die Ungleichung im Limes immer noch (aber möglicherweise mit $\leq$). Der Limes rechts ist aber $\alpha = \pi(w)$, daraus folgt eine Seite der Behauptung. (Die andere symmetrisch.)

Falls nun sowohl $\exists u \subset w : \alpha|u| - 1 = h(u)$ als auch $\exists v \subset w : \alpha|v| + 1 = h(v)$, dann ergibt sich dieser Widerspruch

$$\begin{aligned} \alpha - \frac{1}{|u|} = \frac{h(u)}{|u|} \;&\wedge\; \alpha + \frac{1}{|v|} = \frac{h(u)}{|v|} \\ \frac{h(u)}{|v|} - \frac{h(u)}{|u|} &= \frac{1}{|v|} + \frac{1}{|u|} \end{aligned}$$

4.7.8 Rationalität und Periodizität

29. Juni

Satz: Für jedes unendliche balancierte Wort w:

$$\pi(w) \text{ ist rational} \iff w \text{ ist schließlich periodisch}$$

Beweis: "$\Leftarrow$": falls $w = uv^\omega$, dann können wir $\pi(w)$ als Limes einer beliebigen wachsenden Folge von Faktoren bestimmen, also auch von v^k.

$$\pi(w) = \lim \pi(v^k) = \lim \frac{k \cdot h(v)}{k \cdot |v|} = \frac{h(v)}{|v|} \in \mathbb{Q}$$

"$\Rightarrow$": Wir nehmen an, daß $\pi(w) = p/q \in \mathbb{Q}$. Im Fall $\forall u \subset w : \alpha|u| - 1 < h(u) \leq \alpha|u| + 1$ (der andere ist symmetrisch dazu) gilt für $|u| = q$, daß $p \leq h(u) \leq p + 1$.

Faktoren der Länge q mit Höhe $p + 1$ können aber nicht überlappungsfrei in w vorkommen. (Falls doch: es sind x und z solche Faktoren. Dann ist $xzy \subset w$. Wir berechnen den Anstieg von xyz:

$$\begin{aligned}
(p+1) + h(y) + (p+1) = h(xyz) &\leq \frac{p}{q}(q + |y| + q) + 1 \\
2 + 2p + h(y) &\leq 2p + \alpha|y| + 1 \\
h(y) &\leq \alpha|y| - 1
\end{aligned}$$

im Widerspruch zur Annahme.) Also gibt es nur endliche viele Faktoren der Länge q mit Höhe $p + 1$, und einen Suffix w' von w, in dem alle Faktoren der Länge q die Höhe p haben.

Betrachte einen Faktor $ayb \subset w'$ mit a, b Buchstaben und $|ayb| = q + 1$. Wir haben $h(ay) = h(yb) = p$, also $a = b$. Das heißt, daß der Buchstabe (a) an Position i identisch ist zu dem Buchstaben (b) an Position $i + q$, also ist w' periodisch, und w schließlich periodisch.

4.7.9 Mechanische Wörter

29. Juni

Definition: Für relle Zahlen $0 \leq \alpha \leq 1$ und β beliebig erklären wir zwei unendliche Wörter $w(\alpha, \beta), w'(\alpha, \beta) \in \{0,1\}^\omega$ durch (hierbei $g(n) = \alpha \cdot n + \beta$)

$$\begin{aligned} w'(\alpha,\beta): &\quad n \mapsto \lceil g(n+1) \rceil - \lceil g(n) \rceil \\ w(\alpha,\beta): &\quad n \mapsto \lfloor g(n+1) \rfloor - \lfloor g(n) \rfloor \end{aligned}$$

Wir nennen w das *untere* und w' das *obere mechanische Wort* zu den Parametern (α, β). Die Wörter heißten *rational*, wenn α rational ist, und *irrational* sonst.

weggelassen am 29. Juni

Wenn die Gerade g durch *keine* Gitterpunkt geht, dann stimmen oberes und unteres Wort überein.

Wenn α irrational ist, dann geht g durch höchstens einen Gittepunkt. In der Umgebung dieses Punktes lautet das obere Wort 01, und das untere 10; anderswo stimmen die Wörter überein. (Wir betrachten deswegen im folgenden o.B.d.A. nur noch untere mechanische Wörter.)

Folgerung/Definition: Ist α irrational und $\beta = 0$, dann ist $w' = 1v$ und $w = 0v$ für ein $w \in \{0,1\}^\omega$. Dieses v heißt *charakteristisches Wort* für α.

Satz: Das Fibonacci–Wort ist charakteristisch für $\alpha = 2 - \tau = 0.381966\ldots$.

Beweis: wir zeichnen das charakteristische Wort mit diesem Anstieg, und beweisen, daß es unter dem Fibonacci–Homomorphismus ϕ in sich selbst übergeht.

Wir benutzen: Scherung entlang x–Achse (oben nach links), Treppen abschneiden, Scherung entlang y–Achse (rechts nach unten) und schließlich Spiegelung.

Satz: Jedes mechanische Wort ist balanciert.

Beweis: Wie gesagt betrachten wir untere Wörter. Die Höhe eines $u \subset w$, das an der Position i bis $i + l - 1$ steht, ist

$$h(u) \quad = \quad \lfloor g(i+l) \rfloor - \lfloor g(i) \rfloor = \lfloor \alpha(i+l) + \beta \rfloor - \lfloor \alpha i + \beta \rfloor$$

Wir benutzen das Lemma $a - b - 1 < \lfloor a \rfloor - \lfloor b \rfloor < a - b + 1$ und erhalten

$$\alpha l - 1 < h(u) < \alpha l + 1$$

Fixieren wir $l = |u|$, kann $h(u)$ nur zwei verschiedene Werte annehmen. Deswegen sind die Faktoren der Länge l balanciert. Da l beliebig war, ist w balanciert.

Satz: Jedes mechanische Wort mit Parametern (α, β) hat den Anstieg α.

Beweis: Aus dem vorigen Beweis sehen wir $|\pi(u) - \alpha| < \dfrac{1}{|u|}$ Damit konvergiert $\pi(u)$ (als oder Anstieg im Sinne des vorigen Kapitels.) gegen α (den Parameter des mechanischen Wortes).

Theorem (Hauptsatz über Sturmsche Wörter): Die folgenden Bedingungen sind äquivalent:

- w ist Sturmsches Wort
- w ist balanciert und aperiodisch
- w ist irrational mechanisch

4.7.10 Potenzen als Faktoren des Fibonacci–Wortes

29. Juni

Eine äquivalente Definition mechanischer Wörter ergibt sich durch Rotationen, das sind Verschiebungen modulo 1.

Definition: Für relle Zahlen $0 < a < 1, 0 \leq \beta < 1$ erklären wir eine Abbildung

$$h : [0,1) \to [0,1) : z \mapsto (z+\alpha) \bmod 1$$

und ein unendliches Wort

$$w : \mathbb{N} \to \{0,1\} : n \mapsto \text{ wenn } h^n(0) \in [0,\beta) \text{ dann } 0 \text{ sonst } 1$$

Satz: Dieses Wort *ist* das untere mechanische Wort zu den Parametern (α, β). ???

Beispiel: Für das Fibonacci–Wort ist $\alpha = 1/\tau^2 = (3-\sqrt{5})/2 = \tau - 1$.

Beweis: TODO (Bild).

Einen Faktor eines mechanischen Wortes erkennen wir als Streckenzug. Ist der Faktor eine Potenz (beispiel ein Kubus), besteht der Streckenzug aus 3 gleichen, aneinandergesetzten, Teilen.

Satz (Three–Distance–Theorem): Für eine beliebige irrationale Zahl α ist $z_n = (n\alpha) \bmod 1$. Für jedes n teilt die Menge $\{z_0, z_1, \ldots, z_n\}$ das Intervall $[0,1)$ in gewisse Teil–Intervalle. Diese Teile haben nur drei verschiedene Längen, und der Punkt z_{n+1} fällt in eines der größten Intervalle.

Der Beweis ist (in [Knu98]) benutzt die Kettenbruch–Entwicklung von α.

Satz: Insbesondere gilt für $\alpha \in \{\tau - 1, 2 - \tau\}$: der Punkt z_{n+1} teil das Intervall, in das er fällt, im Goldenen Schnitt.

Der Beweis (ebenfalls in [Knu98]) erfolgt dadurch, daß für diese speziellen α alle Koeffizienten der Kettenbruchentwicklung gleich 1 sind.

Beispiel: TODO (Bild)

Satz: Das Fibonacci–Wort enthält keine Biquadrate (= vierten Potenzen).

Beweis (Bild): Falls doch ein Faktor $u = v^4 \subset f$, betrachte das erste Vorkommen des ersten u. Seine Bounding Box überdeckt nicht $[0,1)$, sondern läßt noch Platz, aber höchstens soviel, wie das (derzeit) breiteste der Teilintervalle.

Bis zum vierten Auftreten des u verschieben wir den Streckenzug (und damit seine Bounding Box) dreimal, und zwar jedesmal wenigstens um die (anfangs) kleinste vorkommende Intervallbreite.

Nach dem Satz verhalten sich aber größte zu kleinste Breite wie $\tau^2 : 1 = (3 + \sqrt{5})/2 = 2.618\ldots < 3$. Das bedeutet, daß spätestens die dritte Verschiebung gar nicht ausführbar ist.

Diese Idee läßt sich verallgemeinern zu:

Satz: Hat die Kettenbruchentwicklung der irrationalen Zahl α beschränkte Koeffizienten, dann enthält das mechanische Wort mit Anstieg α keine beliebig hohen Potenzen als Faktoren.

4.7.11 Das Burnside–Problem (für Gruppen)

weggelassen am 29. Juni

William Burnside fragte 1902:

> Wie sehen Gruppen aus, die durch endlich viele Generatoren erzeugt sind, und in denen jedes Element von endlicher Ordnung ist — insbesondere: können solche Gruppen unendlich sein?

Nennen wir die Anzahl der Generatoren m, und diese selbst $g_1, \ldots, g_m$. "Erzeugt" heißt dann, daß jedes Gruppenelement eine Darstellung als Produkt $g_{i_1}^{a_1} \cdot g_{i_2}^{a_2} \cdots g_{i_k}^{a_k}$ hat, wobei $i_j \in \{1, \ldots, m\}$ und $a_j \in \mathbb{Z}$ (negative Exponenten brauchen wir schon).

Die Ordnung der Gruppe ist n, das heißt $\forall x : x^n = 1$.

Für $m = 1$ und beliebige n haben wir genau die zyklische Gruppe der Ordnung n.

(Für $n = 1$ ist die Gruppe trivial.)

Für $n = 2$ kann man leicht nachrechnen, daß die Gruppe kommutativ ist, und damit auch endlich (und hat 2^m Elemente).

Für $n = 3$ sind die Gruppen nicht kommutativ, aber immer noch endlich (das war Burnsides Resultat). Übungsaufgabe: untersuche das für $m = 2$ oder $m = 3$.

Daher stammt die Vermutung, daß Burnsidegruppen für beliebige n auch endlich sind. Das ist ein schweres Problem, dessen Lösung man erst in den letzten 10, 20 Jahren nähergekommen ist (1994 hat Efim Zelmanov dafür die Fields-Medaille erhalten, das entspricht etwas dem Nobelpreis der Mathematiker).

1.) Es gibt eine Zahl N (etwa 1000), so daß für alle $n \geq N$ unendliche Burnside-Gruppen existieren.

2.) Es gibt eine Funktion $f(m, n)$ mit: Wenn G eine Burnside-Gruppe zu (m, n) ist, dann ist $|G| \leq f(m, n)$ oder $|G| = \infty$. Das sind aber astronomische Schranken im Sinne von

$$f(m, n) = \underbrace{m^{m^{m^{\cdots m}}}}_{n^{n^n}}$$

.

Obwohl es diese Schranken gibt, ist **für kleine n unbekannt,** ob es unendliche Burnside-Gruppen gibt. Bewiesen ist nur: für $n = 2, 3, 4, 6$ nicht. Der erste ungelöste Fall ist also $n = 5$.

4.7.12 Das Burnside–Problem (für Monoide)

Wir können die Frage nach der Endlichkeit ebenso für endlich erzeugte Monoide stellen.

In einem endlich erzeugtes Monoid mit m Generatoren $\{g_1, \ldots, g_m\}$ hat jedes Element eine Darstellung als Produkt $g_{i_1}^{a_1} \cdot g_{i_2}^{a_2} \cdots g_{i_k}^{a_k}$, wobei $i_j \in \{1, \ldots, m\}$ und diesmal $a_j \in \mathbb{N}^+$ (weil es ein Monoid ist, gibt es keine negativen Exponenten, es gibt ja keine Inversen).

Die *freien* endlich erzeugten Monoide kennen wir aber, das sind nämlich genau die $(\Sigma^*, \cdot)$ mit $|\Sigma| = m$.

Mit unseren Kenntnissen über potenzfreie unendliche Wörter können wir leicht unendliche Burnside–Monoide angeben: Wir nehmen $\Sigma = \{0, 1, 2\}$ und als M die Menge aller (endlichen) Faktoren des Morse–Wortes, sowie ein neues Symbol $\top$, das kein Wort ist. Die Monoid–Operation $\circ$ definieren wir so:

$$\begin{aligned} x \circ y \quad = \quad & \text{wenn } x \neq \top \wedge y \neq \top \wedge z \text{ quadratfrei dann } z \text{ sonst } \top \\ & \text{wobei } z = x \cdot y \end{aligned}$$

Die Struktur $(M, \circ)$ bildet ein Monoid (mit Eins–Element $\top$) und ist endlich erzeugt (durch drei Generatoren $\{0, 1, 2\}$). Offensichtlich hat jedes Element die Ordnung 2. M ist andererseits unendlich, da das Morse–Wort unendlich ist.

Es gibt also ein unendliches Burnside–Monoid mit drei Generatoren zur Ordnung 2.

Es wäre schön, wenn man solche formalsprachlichen Methoden auf das ursprüngliche Burnsideproblem (für Gruppen) anwenden könnte. Natürlich besteht zunächst wenig Hoffnung, dadurch die dort benutzten hochkomplizierten algebraischen Methoden einzusparen.

Teil III

Wohl–Quasi–Ordnungen

4.8 Definitionen

4.8.1 QO, PO

Definition: Eine *Quasi–Ordnung* (QO) auf einer Menge M ist eine transitive und reflexive Relation $\lesssim$ auf M

$$\begin{array}{rl} \forall x & x \lesssim x \\ \forall x, y, z & x \lesssim y \wedge y \lesssim z \rightarrow x \lesssim z \end{array}$$

Definition: Eine *Halbordnung* (PO) $\leq$ auf M ist eine antisymmetrische QO auf M.

$$\forall x, y \qquad x \leq y \wedge y \leq x \rightarrow x = y$$

Definition: Zu jeder QO $\lesssim$ auf M setzen wir

$$x \sim y \quad :\Longleftrightarrow \quad x \lesssim y \wedge y \lesssim x$$

Dann ist $\sim$ eine Äquivalenzrelation auf M.

(Ist $\lesssim$ eine PO, dann ist $\sim$ die Identität.)

Definition: Der *strikte Teil* einer QO $\lesssim$ auf M ist die Relation $<$ mit

$$x < y \quad :\Longleftrightarrow \quad x \lesssim y \wedge x \not\sim y$$

Definition: Eine *Kette* in einer QO $(M, \lesssim)$ ist eine Menge $A \subseteq M$ von paarweise vergleichbaren Elementen

$$\forall x, y \in A : \qquad x \lesssim y \vee y \lesssim x$$

Definition: Eine QO $\lesssim$ auf M ist *wohlfundiert* oder *Noethersch*, wenn es keine unendliche strikt absteigende Kette gibt, d. h. keine unendliche Folge der Form

$$x_0 > x_1 > \ldots > x_n > \ldots$$

Beispiel: Die Relation $\subseteq$ (Faktor von) ist wohlfundiert auf Σ^*.

Die vorigen Kapitel über Wörter behandelten ausführlich Eigenschaften der Relation $\subseteq$.

4.8.2 WQO, Einbettungen

Definition: Eine *Antikette* in einer QO $(\lesssim, M)$ ist eine Menge A von paarweise unvergleichbaren Elementen:

$$\forall x, y \in A : \quad x \neq y \to x \not\lesssim y \land y \not\lesssim x$$

Definition: Eine QO $\lesssim$ auf M heißt *Wohl–Quasi–Ordnung*, wenn sie wohlfundiert ist und keine unendlichen Antiketten enthält.

Beispiel: $A = \{00, 010, 0110, \dots, 01^n0, \dots\}$ ist eine unendliche Antikette für $\subseteq$. Also ist $\subseteq$ keine WQO.

Das ist manchmal ein Nachteil. Im folgenden behandeln wir deswegen eine Relation auf Σ^*, die WQO ist, nämlich

Definition: Das Wort v ist *(verstreutes) Teilwort* des Wortes w, geschrieben $v \leq w$, wenn gilt

$$\exists v_1, \dots \in \Sigma^*, w_0, w_1, \dots \in \Sigma^* \qquad v = v_1 v_2 \dots v_n \land w = w_0 v_1 w_1 v_2 \dots v_n w_n$$

Beispiel: $010 = 01 \cdot 0 \leq 01 \cdot 1 \cdot 0 = 0110$.

Der Beweis dafür, daß $\leq$ eine WQO ist, ist nicht offensichtlich, und erfolgt im nächsten Abschnitt. Tatsächlich beweisen wir die Aussage dann für eine Erweiterung dieses Begriffs von Wörtern auf Bäume. Schließlich lassen sich die Resultate auch auf Graphen übertragen, das wird ein Teil des Vortrags über Baumweite.

4.9 Minimale Mengen in WQOs

Satz: Wenn $\lesssim$ eine WQO auf M ist, dann gilt für beliebige $A \subseteq M$: die Menge $\min A$ der minimalen Elemente von A

$$\min A = \{x \mid x \in A, \nexists y \in A : y < x\}$$

ist endlich.

Beweis: Die Menge der minimalen Elemente ist eine Antikette, nach Definition der WQO kann diese nicht unendlich sein.

Satz: Ist A regulär, dann sind auch diese Sprachen regulär

$$A^{\leq} = \{v \mid v \in \Sigma^*, \exists w \in A : w \leq v\}$$
$$A^{<} = \{v \mid v \in \Sigma^*, \exists w \in A : w < v\}$$

Beweis: wir konstruieren aus einem endlichen Automaten für A einen Automaten für $A^{\leq}$ dadurch, daß wir an jedem Zustand q für jeden Buchstaben $b \in \Sigma$ eine Schleife $q \xrightarrow{b} q$ anfügen.

Einen Automaten C für $A^{<}$ erhalten wir so: wir schreiben zwei Exemplare B, B' der eben konstruierten Automaten für $A^{\leq}$ nebeneinander. Für jeden Zustand $q \in B$ und jeden Buchstaben $b \in \Sigma$ schreiben wir eine Regel $q \xrightarrow{b} q'$ (von B nach B'). Die Startzustände von C sind die von B, die Endzustände von C die von B'.

Satz: Wenn ein endlicher Automat für A gegeben ist, dann ist $\min A$ konstruierbar.

Beweis: $\min A = A \setminus A^{<}$.

4.9.1 Beispiel: Primzahlen

Es ist eine höchst mühevolle Bastelaufgabe, für gegebenes A die Menge $\min A$ zu bestimmen.

Als Beispiel wählen wir das Alphabet $\Sigma = \{0, \ldots, 9\}$ und als A die Menge der Dezimaldarstellungen aller Primzahlen. (Das ist natürlich nicht reguläre.)

Durch direktes Aufzählen erhalten wir zunächst die Menge $A_0 \subset \min A$

$A_0 = \{2, 3, 5, 7, 11, 19, 41, 61, 89, 409, 449, 499, 881, 991, 6469, 6949, 9001, 9049, 9649, 9949, 60649\}$

Für jedes $w \in A_0$ ist die Menge $w^{\leq}$ die reguläre Sprache

$$(w_1 \ldots w_n)^{\leq} = \Sigma^* w_1 \Sigma^* \ldots \Sigma^* w_n \Sigma^*$$

Somit ist auch $A_0^{\leq} = \bigcup_{w \in A_0} w^{\leq}$ regulär, und der noch fehlende Teil von $\min A$ liegt in $\Sigma^* \setminus A_0^{\leq}$, ebenfalls eine reguläre Sprache. Zum Glück können wir diese explizit angeben:

$$46^*9 \cup 6^*0^*49$$

Durch direktes Absuchen dieser Sprache finden wir die darin minimalen Primzahlen

$$A_1 = \{666649, 66600049, 66000049, 60000049\}$$

4.9.2 Beispiel: Quadratzahlen

Versuchen wir das gleiche Spiel für $B =$ die Menge der Dezimaldarstellungen von Quadratzahlen > 0. Direktes Aufzählen liefert

$$\begin{aligned} B_0 &= \{1, 4, 9, 25, 36, 576, 676, 7056, 80656, 665856, 2027776, \\ &\quad 2802276, 22282727076, 77770707876, 78807087076, 7888885568656, 8782782707776\} \end{aligned}$$

Aber danach ist die Struktur der Menge $\Sigma^* \setminus B_0^{\leq}$ nicht so einfach zu überschauen.

Man kann versuchen, die Menge der noch zu untersuchenden Zahlen einzuschränken, einerseits durch Restklassenrechnungen modulo geeigneter Zehnerpotenzen, andererseits "von vorn" durch Betrachtungen möglicher Startziffernfolgen.

Restklassenrechnungen liefern diese weiteren minimalen Elemente:

72822772707876,
555006880085056, 782280288087076, 827702888070276, 888288787822276,
2282820800707876, 7880082008070276,
80077778877070276, 88778000807227876,
782828878078078276, 872727072820287876,
2707700770820007076, 7078287780880770276, 7808287827720727876, 8008002202002207876,
27282772777702807876, 70880800720008787876, 72887222220777087876,
80028077888770207876, 80880700827207270276, 87078270070088278276,
88002002000028027076

aber damit ist noch nicht Schluß (denke ich).

4.9.3 Gute und schlechte Folgen

Definition: Gegeben ist eine QO $(M, \lesssim)$. Eine unendliche Folge $(x_1, x_2, \ldots)$ heißt *gut*, wenn $\exists i < j : x_i \lesssim x_y$; sonst *schlecht*.

Satz: Eine QO $(M, \lesssim)$ ist eine WQO $\iff$ jede unendliche Folge ist gut.

Beweis: "$\Leftarrow$": Falls $\lesssim$ keine WQO, dann kann das einerseits an unendlichen strikt absteigenden Ketten liegen (das wäre aber eine unendliche schlechte Folge) oder an unendlichen Antiketten (so etwas ist auch eine schlechte Folge).

"$\Rightarrow$": Angenommen, wir haben doch eine schlechte Folge $(x_1, \ldots)$ in einer WQO. Wir färben die Kanten des vollständigen Graphen über $\{1, \ldots\}$ so: Für $i < j$ wird die Kante ij rot, falls x_i und x_j vergleichbar sind $(x_i \lesssim x_j \vee x_j \lesssim x_i)$, ansonsten ($x_i$ und x_j unvergleichbar) blau.

Nach dem unendlichen Satz von Ramsey gibt es einen vollständigen einfarbigen unendlichen Teilgraphen, das ist also eine Teilfolge $(y_1, \ldots) \subset (x_1, \ldots)$.

Ist diese Teilfolge blau verbunden, bildet sie eine unendliche Anitkette im Widerspruch zur Voraussetzung.

Ist die Teilfolge $(y_1, \ldots)$ komplett rot verbunden, sind alle Elemente paarweise vergleichbar. Gibt es $i < j$ mit $y_i \lesssim y_j$, war die Folge $(x_1, \ldots)$ nicht schlecht. Gibt es kein $i < j$ mit $y_i \lesssim y_j$, gilt für alle $i < j \to y_i > y_j$. Das ist aber eine unendliche absteigende Kette, im Widerspruch zur Wohlfundiertheit.

Eine gute Folge enthält nach Definition *ein* Paar $(x_i \lesssim x_j)$. Tatsächlich ist in einer WQO in guten Folgen noch viel mehr drin:

Satz: In jeder WQO $(M, \lesssim)$ gilt: jede unendliche Folge $(x_1, \ldots)$ enthält eine unendliche (nicht notwendig streng) aufsteigende Teilfolge

$$y_1 \lesssim y_1 \lesssim \ldots \quad , \quad (y_1, y_2, \ldots) \subseteq (x_1, x_2, \ldots)$$

Beweis: Für die Folge $(x_1, x_2, \ldots)$: wir nennen den Index i *terminal*, wenn $\neg \exists j : i < j \wedge x_i \lesssim x_j$. Es gibt nur endlich viele terminale Indizes. (Falls nicht, bilden die terminalen x_i eine unendliche schlechte Folge, das ist aber in einer WQO verboten.)

Wir betrachten die Folge der x *nach* dem letzten terminalen Index. Für diese Teilfolge gilt sogar

$$\forall i \exists j : \qquad i < j \wedge x_i \lesssim x_j$$

(und nicht nur $\exists i \exists j \ldots$). Das heißt, daß wir von einem beliebigen Element aus eine unendliche aufsteigende Kette konstruieren können.

4.10 Satz von Kruskal für Wörter

Theorem: Die Relation $\leq$ (verstreutes Teilwort) ist eine WQO auf Σ^*.

Zu zeigen ist: jede unendliche Folge ist gut. Wir machen das indirekt: wir wählen ein kleinstes Gegenbeispiel, und führen das zum Widerspruch.

Also gibt es nach Annahme unendliche schlechte Folgen. Unter allen diesen betrachten wir die, deren erste Elemente am kürzesten sind, und unter diesen alle, deren zweiten Elemente, usw. Dieser Prozeß liefert eine schlechte Folge $(x_1, x_2, \ldots)$.

Nach Konstruktion kann es *keine* schlechte Folge y geben, deren zugeordnete Folge der Wortlängen lexikografische echt kleiner als die Wort–Längen–Folge von x ist.

Wir interessieren uns nun für die Menge S aller Wörter, die aus x_i entstehen, wenn man die ersten Buchstaben löscht.

$$S \;=\; \{s \mid i \leftarrow [1, \ldots], x_i = a \cdot s, |a| = 1\}$$

und behaupten: $(S, \lesssim)$ ist eine WQO.

Der Beweis erfolgt wiederum indirekt. Falls es doch eine unendliche schlechte Folge $(s_1, s_2, \ldots)$ in S gibt, dann $\exists k \in \mathbb{N}, a \in \Sigma : as_1 = x_k$. Wir streichen aus (s_i) alle Elemente, die zu x_j gehören mit $j < k$. Das sind nur endlich viele. (Falls unendliche, dann wären darunter nach Schubfachschluß welche gleich, also die Folge nicht schlecht.) Es entsteht die unendliche schlechte Teilfolge $(s'_1, s'_2, \ldots) \subseteq (s_1, s_2, \ldots)$.

Wir betrachten die Folge

$$(x_1, \ldots, x_{k-1}, s'_1, s'_2, \ldots)$$

Wegen $|s'_1| = |s_1| < |x_k|$ und der Voraussetzung muß das eine gute Folge sein. Wo kann die dann existierende Einbettung liegen? Falls $x_i \lesssim x_j$, dann war (x) selbst bereits gut. Falls $s'_i \lesssim s'_j$, dann war (s') und damit (s) nicht schlecht. Falls $x_i \lesssim s'_j$, dann gibt es ein l mit $x_i \lesssim s'_j < as'_j = x_l$, also ist (x) gut. Wir erhalten in jedem Fall einen Widerspruch, damit ist $(S, \lesssim)$ eine WQO.

Jetzt zeigen wir, daß die angenommene schlechte Folge (x) nicht existiert. Weil Σ endlich ist, enthält (x) nach Schubfachschluß eine unendliche Teilfolge (z), deren Anfangsbuchstaben übereinstimmen. Wir löschen in (z) alle Anfangsbuchstaben und erhalten damit eine Folge (z') in S. Weil $(S, \lesssim)$ WQO, ist (z') gut, enthält also $z'_i \lesssim z'_j$. Dann gilt auch $z_i = az'_i \lesssim az'_j = z_j$, das heißt, wir haben eine Einbettung in (z) und damit in (x) gefunden.

4.11 Satz von Kruskal für Bäume

Die vorangegangenen Definitionen, Sätze und Beweise lassen sich direkt von Wörtern auf Bäume (Elemente einer endlich erzeugten freien Algebra) übertragen. Die Erweiterung besteht darin, daß jetzt Funktionssymbole mehrere "Nachfolger" haben (bei Wörtern sind in diesem Sinne alle Symbole — bis auf das leere Wort — einstellig). Wir müssen deswegen im Beweis die Menge S anpassen.

Definition: Für eine endliche Signatur $\Sigma = (\Sigma_0, \Sigma_1, \dots, \Sigma_n)$, wobei Σ_k die Funktionssymbole der Stelligkeit j enthält, ist Term(Σ) die Menge der Terme über Σ.

Definition: Die Relation $\leq$ (verstreuter Teilterm) auf Term(Σ) ist definiert durch das Ersetzungssystem mit den Regeln

$$\forall k : \forall f \in \Sigma_k : \forall i : 1 \leq i \leq k : \qquad x_i \to f(x_1, x_2, \dots, x_k)$$

(Bei manchen Autoren ist das gar nicht erlaubt, weil rechts Variablen erscheinen, die links nicht vorkommen. Die Interpretation ist aber klar: diese dürfen durch ganz beliebige Grundterme ersetzt werden.)

Beispiel: $g(a, f(b)) < g(f(a), f(g(c, b)))$.

Theorem (Kruskal): Für endliche Σ gilt: Die Relation (Term(Σ), $\leq$) ist WQO.

Beweis: wie für Wörter, mit einem Umweg.

Wir nehmen wieder eine kleinste (elementweise nach Termgröße) schlechte Folge (x), und als S die Menge aller Teilbäume von x_i, die direkt unter der Wurzel hängen:

$$S \;=\; \{s_{i,j} \mid i \leftarrow [1, \dots], x_i = f(s_{i,1}, \dots, s_{i,k})\}$$

Wir zeigen wie gewohnt, daß $(S, \leq)$ eine WQO ist.

Im zweiten Teil des Beweises bemerken wir, daß es ein Funktionssymbol f gibt, das unendlich oft in der Wurzel der x_i steht. Dieses f hat Stelligkeit k. Dann benötigen wir die Aussage, daß $(S^k, \leq^k)$ wohlgeordnet ist, und daraus folgt das Theorem.

Es bleibt also zu definieren und zu zeigen:

Definition: Für eine Folge von QOs $(M_i, \lesssim_i)$ erklären wir $\lesssim = \lesssim_1 \times \ldots \times \lesssim_n$ auf $M_1 \times \ldots \times M_n$ durch

$$(x_1, \dots, x_n) \lesssim (y_1, \dots, y_n) \quad \iff \quad x_1 \lesssim_1 y_1 \wedge \ldots \wedge x_n \lesssim_n y_n$$

Satz: Wenn $(M_1, \lesssim_1), \dots, (M_n, \lesssim_n)$ WQOs sind, dann ist $(M_1 \times \ldots \times M_n, \lesssim_1 \times \ldots \times \lesssim_n)$ auch WQO.

Beweis: (Induktion nach n). Anfang $n = 1$ ist klar. Schritt:

Betrachte eine unendliche schlechte Folge von $x_i \in M_1 \times \ldots \times M_n$. Weil $(M_1, \lesssim_1)$ WQO, gibt es eine unendliche Teilfolge $(y) \subset (x)$, die in den ersten Komponenten aufsteigend ist. Nach Induktion ist die Folge der zugeordneten Suffixe $y'_i = (y_{i,2}, y_{i,3}, \dots, y_{i,k})$ eine gute Folge, das heißt, es existieren $i < j$ mit $y'_i \lesssim' y'_j$, wobei $\lesssim' = \lesssim_2 \times \ldots \times \lesssim_n$. Für diese i, j gilt aber $y_i \lesssim y_j$, und daraus folgt die Behauptung.

4.12 Anwendungen von WQOs bei Terminationsbeweisen

WQOs finden wesentliche Anwendung bei Terminationsbeweisen von (Term–)Ersetzungs–Systemen. Das ist zunächst überraschend, denn für Termination reicht ja Wohlfundiertheit. Wozu brauchen wir die Antikettenbedingung?

Definition: Die QO $\lesssim_2$ auf M ist eine *Erweiterung* der QO $\lesssim_1$ auf M, wenn

$$\forall x, y \in M : \qquad x \lesssim_1 y \rightarrow x \lesssim_2 y$$

Satz: Wenn $\lesssim_2$ eine Erweiterung von $\lesssim_1$ ist, und $\lesssim_2$ wohlfundiert ist, dann ist auch $\lesssim_1$ wohlfundiert.

Beweis: eine unendliche absteigende Kette in $\lesssim_1$ ist auch eine unendliche absteigende Kette in $\lesssim_2$.

Folgerung: Eine Methode für Terminationsbeweise (für eine Relation $\lesssim_1$, die durch ein Ersetzungssystem gegeben ist) besteht darin, die QO $\lesssim_1$ geschickt so zu erweitern, daß wir eine wohlfundierte Ordnung $\lesssim_2$ erhalten. Wir nehmen dazu (als Kandidaten für $\lesssim_2$) am besten ein Klasse von QOs, die von vornherein wohlfundiert sind — nämlich WQOs.

Satz: Für jede WQO $(M, \lesssim_1)$ gilt: Jede Erweiterung $\lesssim_2$ von $\lesssim_1$ ist selbst WQO.

Beweis des Satzes: Wir haben zu zeigen, daß jede unendliche Folge (x) in M bezüglich $\lesssim_2$ gut ist. Weil $(M, \lesssim_1)$ bereits WQO ist, ist die Folge bezüglich $\lesssim_1$ gut, das heißt, es gibt $i < j$ mit $x_i \lesssim_1 x_j$. Nun ist $\lesssim_2$ eine Erweiterung von $\lesssim_1$, also folgt sofort $x_i \lesssim_2 x_j$, fertig.

Folgerung: also ist $\lesssim_2$ auch wohlfundiert. Auf genau diese Weise funktionieren Simplifikations–Ordnungen (Definition und Beispiele siehe Vorlesung Termersetzung, Dr. Hartwig, oder [BN98]). Wir beginnen mit der Relation "homöomorphe Einbettung" (d. h. "verstreuter Teilbaum"), die bereits eine WQO ist, und erweitern diese solange, bis sie auch eine Erweiterung der gebenen Ersetzungsrelation R ist. Falls das geht, haben wir R als wohlfundiert, also terminierend, nachgewiesen.

(Nicht–)Beispiel für den Satz: man mache sich klar, daß es wohlfundierte Ordnungen gibt, die nicht–wohlfundierte Erweiterungen besitzen: Wir ordnen die positiven natürlichen Zahlen durch die Relation "ist Teiler von". Sicher sind alle strikt absteigenden Ketten endlich. In dieser Ordnung bilden die Primzahlen eine unendliche Antikette (es ist also keine WQO). Wenn wir eine Ordnung erweitern, können wir Antiketten beliebig ordnen, also wählen wir $2 > 3 > 5 > 7 > \dots$ und erhalten eine unendliche absteigende Kette.

4.13 WQO für Graphen

Definition: Ein Graph H ist *Teilgraph* eines Graphen G, geschrieben $H \subseteq G$, wenn wir H aus (einer isomorphen Kopie von) G durch eine Folgen von Kanten– und Knotenlöschungen erhalten können.

Beobachtung: Diese Relation ist offensichtlich wohlfundiert, aber nicht WQO: Die Menge aller Kreise $\{C_3, C_4, \ldots\}$ bildet eine uendliche Antikette (= schlechte Folge).

Nun fragt man sich, gibt es denn eine vernünftige WQO auf Graphen. Die (durch Vergleich zu Termen und Wörtern) naheliegende Definition ist:

Definition: Der Graph H ist *homöomorph eingebettet in* (oder: *ist Minor von*) G, geschrieben $H \leq G$, wenn wir H aus G durch eine Folgen von Teilgraph–Bildungen und Kanten–Kontraktionen erhalten können. Eine *Kontraktion* einer Kante uv in G erzeugt den Graphen G' mit der Knotenmenge $V(G) \setminus \{u,v\} \cup \{n\}$, wobei n ein "neuer Knoten" ist, und der Kantenmenge

$$E(G') = E(G\mid_{V(G)\setminus\{u,v\}}) \cup \{nx \mid x \in V(G) \setminus \{u,v\}, xu \in E(G) \vee xv \in E(G)\}$$

Beispiel: Durch Kontraktion einer Kante sehen wir $C_n < C_{n+1}$.

Beispiel: Die Graphen G mit $K_3 = C_3 \not\leq G$ sind genau die kreisfreien, also Bäume (bzw. Wälder).

Aufgabe: wie sehen Graphen ohne eingebetteten K_4 aus?

Theorem (Robertson/Seymour): Die Minor–Relation ist eine Wohlquasiordung auf der Menge der Graphen.

Beweis: Der Beweis erfordert einen Riesen–Aufwand. Die Autoren veröffentlichten ihn in einer Artikelserie, die über mehrer hunderte Seiten und Jahrzehnte reicht. Eine lesbare Einführung und Übersicht ist in [Die96].

Wir wollen ntürlich zum Beweis den Satz von Kruskal für Bäume benutzen, können das aber nicht direkt, weil ein Graph eben kein Baum ist. Wir definieren "Baumweite" als Maß für die Baum–Ähnlichkeit eines Graphen, und arbeiten uns von dort vor.

4.14 Verbotene Minoren

Definition: Für eine Relation $(M, \lesssim)$: eine Menge (Eigenschaft) $N \subseteq M$ heißt *erblich*, wenn

$$\forall x \in N : \forall y : y \lesssim x \to y \in N$$

Beispiel: die Menge der planaren Graphen ist erblich.

Planar heißt plättbar. Haben wir eine ebene Zeichnung eines Graphen G, dann können wir daraus leicht eine ebene Zeichnung jedes Minoren von G gewinnen. Diese sind also alle auch planar.

Beispiel: die Menge der Graphen mit Hamiltonkreis ist nicht erblich.

Aufgabe: Für festes c: ist die Menge der c–färbbaren Graphen erblich? (Nein.)

Satz: Wenn $(M, \lesssim)$ WQO und $N \subseteq M$ erblich, dann existiert eine *endliche* Menge $F \subseteq M$ mit

$$\forall x \in M \qquad x \in N \iff \forall y \in F : y \not\lesssim x$$

Das F heißt Menge der *verbotenen Minoren.*

Beispiel (Satz von Kuratowski):
Für $N =$ Menge der planaren Graphen ist $F = \{K_5, K_{3,3}\}$.

Beweis: $F = \min(M \setminus N)$. Nach früherem Satz ist das endlich. Wir zeigen, daß F die passende Menge ist:

Wegen $F = \min(M \setminus N) \subseteq M \setminus N$ gilt $y \in F \to y \notin N$. Falls weiter $y \lesssim x$, dann wegen der Erblichkeit auch $x \notin N$.

Falls andererseits $x \notin N$, dann $x \in M \setminus N$ und $\exists y \in \min(M \setminus N)$ mit $y \lesssim x$.

Bemerkung: das ist ein reiner Existenzbeweis, aus dem zunächst *überhaupt nichts* über das Aussehen oder die Größe von F folgt. Zum Beispiel ist damit der Satz von Kuratowski überhaupt noch nicht bewiesen.