Fachbereich Informatik und Mathematik

Institut für Mathematik

. . . . . .

Das zufällige Erfüllbarkeitsproblem

Masterarbeit

vorgelegt von

Piravean Chandirakanthan

geboren am 11.08.1986 in Hünfeld

Matrikelnummer: 3477669

Erstprüfer und Betreuer: Prof. Dr. Ralph Neininger

Zweitprüfer: Prof. Dr. Amin Coja-Oghlan

Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, dass alle Stellen der Arbeit, die wörtlich oder sinngemäß aus anderen Quellen übernommen wurden, als solche kenntlich gemacht sind und dass die Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegt wurde.

Hünfeld, den 2. Juli 2012 Unterschrift

Inhaltsverzeichnis

1 Einleitung

Eine Formel des Erfüllbarkeitsproblems wird über n Boolesche Variablen, d.h. Variablen, die die Werte '*wahr*' oder '*falsch*' annehmen, definiert. Sie besteht aus der logischen *UND*-Verknüpfung von sogenannten Klauseln, die ihrerseits logische *ODER*-Verknüpfungen von Variablen oder deren Negierungen sind.
Formal betrachten wir für $i \in \{0, \ldots, n\}$ die Variablen $x_i \in \{0, 1\}$ (1=*wahr*, 0=*falsch*). Die Negierung von x_i ist $\bar{x}_i := 1 - x_i$ und wir bezeichnen eine Variable x_i oder ihre Negierung $\bar{x}_i$ als ein Literal. Eine Klausel c der Länge k_c ist dann die logische *ODER*-Verknüpfung von k_c Literalen. Geschrieben wird die *ODER*-Verknüpfung mit dem Symbol $\vee$. Wir sagen c ist 'erfüllt', falls mindestens eines der k_c Literale in c den Wert 1 hat und damit auch der gesamte logische Ausdruck c. Die Klausel c wird durch genau eines der 2^{k_c} möglichen Besetzungen der k_c beteiligten Variablen nicht erfüllt, nämlich die Besetzung die allen in c auftretenden Literalen den Wert 0 zuordnet. Zum Beispiel wird die Klausel $c = (x_3 \vee \bar{x}_5 \vee x_{17} \vee \bar{x}_{49})$ nur durch die Wahl $x_3 = 0$, $x_5 = 1$, $x_{17} = 0$ und $x_{49} = 1$ nicht erfüllt.
Eine Formel F des Erfüllbarkeitsproblems ist nun die logische *UND*-Verknüpfung von m Klauseln $c_1, \ldots, c_m$, die wir $F = c_1 \wedge \cdots \wedge c_m$ schreiben. Die Formel heißt 'erfüllt', falls der gesamte logische Ausdruck F den Wert 1 hat, d.h. falls alle Klauseln $c_1, \ldots, c_m$ erfüllt sind.
In dieser Masterarbeit betrachten wir ausschließlich den Spezialfall, in dem alle Klauseln $c_1, \ldots, c_m$ die gleiche Länge haben, d.h. wir gehen nun davon aus, dass $k_{c_1} = k_{c_2} = \ldots = k_{c_m} =: k \geq 2$ gilt und nennen dann F eine k-SAT-Formel. Die Klauselläng k ist im folgenden stets fest, wobei wir in Kapitel 2.4 kurz den Fall $k = k(n)$ betrachten.
Hat man eine k-SAT-Formel F gegeben, dann beschäftigt uns die Frage, ob es eine Besetzung der Variablen $x_1, \ldots, x_n$ gibt, sodass F erfüllt wird. Falls eine solche 'erfüllende' Besetzung existiert, sagen wir, dass F 'erfüllbar' (oder auch kurz SAT für *satisfiable*) ist. Die Untersuchung dieser Fragestellung ist allgemein bekannt als Erfüllbarkeits- oder SAT-Problem, und wurde schnell bekannt als das erste NP-vollständige Problem. Speziell hat Cook in [12] gezeigt, dass das k-SAT-Problem für $k \geq 3$ NP-vollständig ist, wohingegen für $k = 2$ das Problem in polynomieller Zeit gelöst werden kann.
Die Lösbarkeit des SAT–Problems ist abhängig von der ausgehenden Formel. Man unterscheidet insbesondere zwischen 'leichten' und 'schweren' Formeln. Unter leichten Formeln kann man sich Formeln vorstellen, die viele erfüllende Besetzungen haben und dadurch (relativ) schnell eine Lösung gefunden werden kann. Schwere Formeln haben wenige beziehungsweise keine erfüllende Besetzungen. Wenn man nun das Problem mit Algorithmen oder anderen Heuristiken untersucht, ist für die Aussagekraft der Ergebnisse u.a. auch entscheident, dass man bei der Wahl der Ausgangsformel leichte Formeln nicht bevorzugt, sondern Resultate für 'typische' Formeln angeben kann. Das interessanteste Modell, um solche typischen Formeln zu generieren, ist das zufällige k-SAT-Modell, wobei Formeln nach einer gewissen Wahrscheinlichkeitsverteilung gewählt werden. Uns wird in dieser Masterarbeit ausschließlich folgende drei Vorgehensweisen zur Generierung von zufälligen Formeln begegnen: Wegen der Ähnlichkeit der Modelle (siehe die Diskussion unten) verwenden wir im folgenden identische Bezeichnungen für sich entsprechende Größen.

- *$F_{n,m}$-Modell*:
    1. Bezeichne $C_n(k)$ die Menge der $N := 2^k\binom{n}{k}$ möglichen Klauseln, in denen keine Variablen mehrfach auftreten. Dann unterscheidet man zwischen zwei Varianten:

(i) Die zufällige Formel $F_k(n,m)$ wird dadurch generiert, dass aus der Menge $C_n(k)$ m Klauseln uniform, unabhängig und mit Zurücklegen gezogen werden. Die Menge der verschiedenen Formeln, die durch diese Weise erzeugt werden können, sei mit $Form(n,m,k)$ bezeichnet. Es gilt $|Form(n,m,k)| = N^m$ und für alle $f \in Form(n,m,k)$

$$\mathbb{P}(F_k(n,m) = f) = \frac{1}{N^m}. \tag{1}$$

(ii) Die zufällige Formel $F_k(n,m)$ wird dadurch generiert, dass aus der Menge $C_n(k)$ m Klauseln uniform, unabhängig und ohne Zurücklegen gezogen werden. Die Menge der verschiedenen Formeln, die durch diese Weise erzeugt werden können, sei mit $Form(n,m,k)$ bezeichnet. Es gilt $|Form(n,m,k)| = \binom{N}{m}$ und für alle $f \in Form(n,m,k)$

$$\mathbb{P}(F_k(n,m) = f) = \frac{1}{\binom{N}{m}}. \tag{2}$$

2. Bezeichne $C_n(k)$ die Menge der $N := (2n)^k$ möglichen Klauseln, in denen nun auch Literale mehrfach auftreten können. Die zufällige Formel $F_k(n,m)$ wird dadurch generiert, dass aus der Menge $C_n(k)$ m Klauseln uniform, unabhängig und mit Zurücklegen gezogen werden. Die Menge der verschiedenen Formeln, die durch diese Weise erzeugt werden können, sei mit $Form(n,m,k)$ bezeichnet. Es gilt $|Form(n,m,k)| = (2n)^{km}$ und für alle $f \in Form(n,m,k)$

$$\mathbb{P}(F_k(n,m) = f) = \frac{1}{N^m}. \tag{3}$$

- *$F_{n,p}$-Modell*: Bezeichne $C_n(k)$ die Menge der $N := 2^k\binom{n}{k}$ möglichen Klauseln, in denen keine Variable mehrfach auftreten. In diesem Modell ist bei einer zufälligen Formel $F_k(n,p)$ jede der N möglichen Klauseln unabhängig mit Wahrscheinlichkeit

$$p := \frac{m}{N} \tag{4}$$

vorhanden. Da die Anzahl der Klauseln in der zufälligen Formel $F_k(n,p)$ $Bin(N,p)$-verteilt ist, ist die erwartete Anzahl an Klauseln in der Formel m.

Wir werden uns überwiegend für asymptotische Aussagen für das zufällige k-SAT-Problem interessieren. Dabei ist gemeint, dass wir das zufällige Problem für wachsende Variablenanzahl n betrachten. Die Aussagen folgender Art werden eine wichtige Rolle spielen.

Definition 1. *Sei $(E_n)_{n\in\mathbb{N}}$ eine Folge von Ereignissen. Wir sagen E_n tritt mit hoher Wahrscheinlichkeit ein, falls*

$$\lim_{n\to\infty} \mathbb{P}(E_n) = 1 \tag{5}$$

gilt und E_n tritt mit (uniform) positiver Wahrscheinlichkeit ein, falls

$$\liminf_{n\to\infty} \mathbb{P}(E_n) > 0 \tag{6}$$

gilt.

Für Eigenschaften, die mit hoher Wahrscheinlichkeit gelten, wurde in [1] und [4] gezeigt, dass all die oben vorgestellten Modell für das zufällige k-SAT äquivalent sind, und zwar in dem Sinne, dass jede Eigenschaft, die mit hoher Wahrscheinlichkeit in einem dieser Modelle gilt, auch mit hoher Wahrscheinlichkeit in den anderen Modellen gilt.
Bei der Untersuchung des zufälligen k-SAT-Problems stellt sich heraus, dass der Parameter

$$r := \frac{m}{n}, \tag{7}$$

welcher als Klausel-zu-Variablen Rate oder Klauseldichte bezeichnet wird, eine wichtige Rolle spielt. Wir werden im folgenden für die Anzahl der Klauseln einer zufälligen Formel $m = rn$ schreiben, sodass die Klauseldichte stets konstant (also unabhängig von der Variablenanzahl n) ist. In dieser Masterarbeit werden wir den Schwerpunkt auf den sogenannten Phasenübergang des zufälligen k-SAT setzen. Experimente zeigen, dass die Wahrscheinlichkeit, dass eine zufällige k-SAT-Formel $F_k(n, rn)$ erfüllbar ist, mit wachsender Klauseldichte r von nahe 1 schnell auf nahe 0 fällt. Man geht stark davon aus, dass dieser Phasenübergang mit wachsender Variablenanzahl n sich um einen gewissen festen Wert für die Klauseldichte, den sogenannten Threshold r_k, abspielt:
Die SAT-Threshold-Behauptung. *Für $k \geq 2$ existiert eine Konstante $r_k > 0$, so dass für alle $\varepsilon > 0$*

$$\lim_{n\to\infty} \mathbb{P}\left(F_k(n, rn) \text{ erfüllbar}\right) = \begin{cases} 1 & \text{, falls } r = (1-\varepsilon)r_k \\ 0 & \text{, falls } r = (1+\varepsilon)r_k. \end{cases}$$

gilt.
Wir werden in Kapitel 2 zunächst die Ergebnisse aus [10] und [19] vorstellen, die für den Fall $k = 2$ nicht nur die Existenz der Konstanten r_2 aus obiger Behauptung nachweisen, sondern sogar zeigen, dass $r_2 = 1$ gilt. Für $k \geq 3$ ist die Behauptung noch offen, aber man kann ein Intervall angeben, in dem r_k, falls sie existiert, liegen muss. Wir werden hierzu das Ergebnis aus [5] betrachten und zeigen, dass für $k \geq 3$ und eine passende Nullfolge β_k

$$2^k \ln 2 - 2(k+1)\ln 2 - 1 - \beta_k \leq r_k \leq 2^k \ln 2$$

gilt.
In Kapitel 3 werden wir Resultate bezüglich der Schärfe des Phasenübergangs anschauen ([9],[26]) und in Kapitel 4 die Menge der erfüllenden Besetzungen genauer betrachten ([1],[2],[6],[25]). Im abschließendem Kapitel stellen wir einen einfachen randomisierten Algorithmus aus [24] für k-SAT vor, der für eine erfüllbare k-SAT-Formel eine erfüllende Besetzung findet. Wir werden zeigen, dass die erwartete Laufzeit des Algorithmus echt kleiner ist als die Komplexität des naiven Verfahrens, bei dem man die 2^n möglichen Besetzungen bei der Formel testet, bis man eine erfüllende Besetzung gefunden hat, welches eine Worst-Case-Laufzeit von 2^n hat.

2 Die Thresholds für das zufällige k-SAT-Problem

Das zufällige k-SAT-Problem erlebt mit wachsender Variablenzahl n einen Phasenübergang. Dabei ist gemeint, dass die Wahrscheinlichkeit, mit der eine zufällige k-SAT-Formel erfüllbar ist, um einen kritischen Wert r_k für die Klauseln-zu-Variablen Rate r von 1 für $r < r_k$ schnell auf 0 für $r > r_k$ fällt. Die Existenz und der genaue Wert des Thresholds r_k wurde bisher nur für den Fall $k = 2$ gezeigt ([10],[16],[19]). Für den Fall $k \geq 3$ sind derzeit nur obere und untere Schranken für den Threshold bekannt. Einen großen Schritt hat dabei Friegut [17] gemacht, in dem er folgendes Theorem zeigen konnte.

Theorem 1. *(Theorem 1.3 in [17])*
Für jedes $k \geq 2$ existiert eine Folge $r_k(n)$, so dass für alle $\varepsilon > 0$

$$\lim_{n\to\infty} \mathbb{P}\left(F_k(n, rn) \text{ erfüllbar}\right) = \begin{cases} 1, & \text{falls } r = (1-\varepsilon)r_k(n) \\ 0, & \text{falls } r = (1+\varepsilon)r_k(n). \end{cases}$$

Folgerung 1. *Sei $k \geq 2$. Ist $F_k(n, rn)$ mit positiver Wahrscheinlichkeit erfüllbar, dann ist $r_k \geq r$, d.h. $F_k(n, rn)$ ist mit hoher Wahrscheinlichkeit erfüllbar.*

Im folgenden werden wir uns zunächst den Beweis des Thresholds für den Fall $k = 2$ anschauen und dann für den Fall $k \geq 3$ das wichtige Ergebnis aus [5] betrachten. Dazwischen werden wir einige Ergebnisse aus [3] zu dem sog. zufälligen $(2 + p)$-SAT-Problem vorstellen, welches als eine Art Interpolation zwischen 2-SAT und 3-SAT verstanden werden kann (siehe [22]).

2.1 Das zufällige 2-SAT-Problem

In diesem Abschnitt wollen wir uns den Phasenübergang bei wachsender Variablenanzahl n für das zufällige Erfüllbarkeitsproblem mit $m = rn$ Klauseln der Länge 2 betrachten. Nur für den Fall $k = 2$ ist der genaue Threshold für den Phasenübergang von SAT zu UNSAT einer zufälligen uniformen Formel bekannt. Im foldenden wollen wir zeigen, dass

$$r_2 = 1$$

gilt. Dabei werden wir uns an den Arbeiten von Goerdt [19] und Chvátal und Reed [10] halten. Eine 2-SAT Formel F kann man durch ihren korrespondierenden Formelgraphen darstellen.

Definition 2. *(Formelgraph)*
Ein Formelgraph über n Variablen ist ein gerichteter Graph $G = (V, E)$ mit

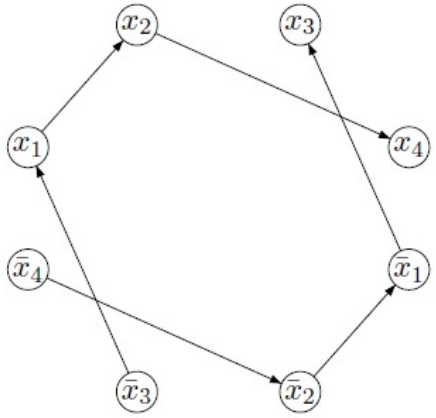
(i) $V = \{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$ *und*

(ii) für $l_i, l_j \in V$ mit $i \neq j$, gilt

$$(l_i, l_j) \in E \iff (\bar{l}_j, \bar{l}_i) \in E.$$

Ist $(v \vee w)$ eine Klausel in F, dann entspricht dieser Klausel in dem korrespondierenden Graphen G_F genau das Paar von komplementären Kanten $((\bar{v}, w), (\bar{w}, v))$. Da wir uns für die Erfüllbarkeit von Klauseln interessieren, sollen für die Klausel $(v \vee w)$ die Kanten $(\bar{v}, w)$ und $(\bar{w}, v)$ im Formelgraphen implizieren, dass im Falle $\bar{v} = 1$ $w = 1$ gelten muss damit die

Klausel erfüllt ist und umgekehrt, falls $\bar{w} = 1$, muss dann entprechend $v = 1$ gelten. Dies bedeutet, dass eine Besetzung der Variablen $x_1, \ldots, x_n$ genau dann erfüllend ist, wenn sie alle Implikationen im Formelgraphen erfüllt. Aus diesem Grund nennt man einen Formelgraphen G_F einer Formel F auch Implikationsgraphen. Für $n = 4$ beispielsweise ist der Formelgraph für die Formel $F = (x_1 \vee x_3) \wedge (\bar{x}_2 \vee x_4) \wedge (\bar{x}_1 \vee x_2)$ gegeben durch Die Abbildung, die eine Formel



auf einen Formelgraphen abbildet, ist bijektiv. Damit ist der zufällige Formelgraph einer auf der Menge $Form(n, m, 2)$ uniform verteilten Formel $F_2(n, m)$ ebenfalls uniform verteilt, nun auf der Menge der Formelgraphen, die wir mit $FG(n, m)$ bezeichnen.
Wir müssen noch einige Definitionen und Notationen einführen.

Definition 3.

- *Für einen Teilgraphen $H = (U, W)$ eines Formelgraphen, ist der Komplementärgraph $\bar{H} = (\bar{U}, \bar{W})$ definiert durch*

$$\bar{U} = \{\bar{l} \mid l \in U\} \text{ und } \bar{F} = \{(\bar{l}, \bar{k}) \mid (k, l) \in W\}.$$

- *Für $H = (U, W)$ ist*

$$Paar\ H = \{(l, k), (\bar{k}, \bar{l}) \mid (l, k) \in W\} \text{ und } Lit\ H = U.$$

- *Ein widerprüchlicher Kreis in einem Formelgraphen ist ein Kreis, der die Knoten l und $\bar{l}$ für ein Literal l enthält.*

Um das Ergebnis zum Threshold zu beweisen, werden wir die schon länger bekannte Beobachtung in [7] verwenden.

Proposition 1.
Eine 2-SAT Formel F ist genau dann UNSAT, wenn der zu F gehörige Formelgraph G_F einen widersprüchlichen Kreis enthält.

Wir wollen die Behauptung mithilfe des sog. UC-Verfahrens (UC=„unit clause“) zeigen (siehe [21]). Das Verfahren beruht darauf, einzelnen Literalen, die in der Formel auftauchen, zunächst einen Wert zuzuweisen und zu notieren, welche Implikationen diese für die Werte anderer Literale in der Formel haben. Betrachtet man eine Klausel $(l_i \vee l_j)$ und fixiert z.B. l_i, dann kann je nachdem welchen Wert wir l_i geben, folgendes passieren:

- Fixiert man $l_i = 1$, dann ist die Klausel $(l_i \vee l_j)$ also erfüllbar und wir können diese aus der Formel wegstreichen.
- Fixiert man $l_i = 0$, dann wird die Klausel $(l_i \vee l_j)$ zu der 1-Klausel (l_j) und die einzige Möglichkeit für die Erfüllbarkeit dieser Klausel ist die Wahl $l_j = 1$.

Für eine gegebene 2-SAT Formel starten wir mit einem beliebigen x_i, $i \in \{1, \ldots, n\}$, und wählen zunächst $x_i = 0$. Wir wenden dann obige Regel auf die Klauseln an, die x_i oder $\bar{x}_i$ enthalten und fixieren die Literale in den dadurch entstehenden 1-Klauseln. Diese Prozedur kann durch folgende zwei Situationen zum stoppen kommen:

(i) Die reduzierte Formel hat keine 1-Klauseln.

(ii) Die reduzierte Formel enthält die 1-Klauseln (z) und $(\bar{z})$ für ein Literal z.

Im Falle von (i) hat man eine Besetzung von einem Teil der Variablen gefunden, sodass keine Klausel in der Formel verletzt wird. Man beachte, dass solch eine Teilbesetzung der Variablen genau dann zu einer kompletten erfüllenden Besetzung erweitert werden kann, wenn die Formel SAT ist. Nun kann man das Verfahren mit dem Fixieren einer neuen Variable x_j fortsetzen.
Im Falle von (ii) kann die gefundene Teilbesetzung der Variablen nicht zu einer kompletten erfüllenden Besetzung erweitert werden. Deshalb löscht man die Besetzung und startet erneut mit der Wahl $x_i = 1$. Endet nun das Verfahren durch (i), dann fährt man wie oben erwähnt fort. Ist aber (ii) der Fall, dann ist die Formel UNSAT. Dieses Verfahren kann man nun mit dem Formelgraphen verbinden um Proposition 1 zu zeigen.

Beweis. Sei F eine beliebige 2-SAT Formel und G_F der dazugehörige Formelgraph.
G_F enthalte zunächst einen widersprüchlichen Kreis, d. h. es existiert ein $i \in \{1, \ldots, n\}$, sodass die Pfade

$$x_i \to \cdots \to \bar{x}_i \text{ und } \bar{x}_i \to \cdots \to x_i$$

in G_F enthalten sind. Wendet man nun das UC-Verfahren auf die Formel F an und wählt dabei $x_i = 0$, dann folgt wegen der Existenz des Pfades $\bar{x}_i \to \cdots \to x_i$ in G_F, dass das Verfahren wegen (ii) stoppt. Wählt man dann $x_i = 1$, dann folgt das gleiche wegen der Existenz des Pfades $x_i \to \cdots \to \bar{x}_i$ und die Formel ist damit UNSAT.
Nehmen wir nun an, dass die Formel F UNSAT ist, d. h. es existiert ein $i \in \{1, \ldots, n\}$, sodass beim UC-Verfahren folgendes passiert:

1. Die Wahl $x_i = 0$ führt zu (ii) und die gefundene Besetzung wird gelöscht.
2. Aber auch die Wahl $x_i = 1$ führt zu (ii).

Aus 1. folgt, dass für ein Literal v der Formelgraph G_F die Pfade

$$\bar{x}_i \to \cdots \to v \text{ und } \bar{x}_i \to \cdots \to \bar{v}$$

enthält. Da aber nach Definition des Formelgraphen mit diesen beiden Pfaden auch ihre Komplementärpfade in G_F sind, können wir also z.B. den Pfad

$$\bar{x}_i \to \cdots \to v \to \cdots x_i$$

in G_F finden. Analog folgt aus 2., dass auch ein Pfad

$$\bar{x}_i \to \cdots \to z \to \cdots x_i,$$

für ein Literal z, existieren muss. Zusammen erhalten wir einen widersprüchlichen Kreis in G_F. □

Das Threshold-Theorem sieht foldermaßen aus.

Theorem 2.
Sei $F_2(n, m)$ eine zufällige uniforme Formel mit $m = rn$ Klauseln der Länge zwei über n Variablen. Dann gilt für n gegen unendlich:
(i) Falls $r < 1$, dann ist $F_2(n, m)$ mit Wahrscheinlichkeit $1 - o(1)$ erfüllbar,
(ii) falls $r > 1$, dann ist $F_2(n, m)$ mit Wahrscheinlichkeit $1 - o(1)$ nicht erfüllbar.

Beweis. Teil (i).
Für diesen Teil werden wir uns an den Beweis von Goerdt halten. Das Ziel wird sein zu zeigen, dass für den Fall $r < 1$ ein uniform gewählter Formelgraph mit rn Paaren von komplementären Kanten mit hoher Wahrscheinlichkeit keinen widersprüchlichen Kreis enthält. Wie schon in der Einleitung zu diesem Abschnitt erwähnt, folgt dann, dass die zugehörige zufällige Formel mit hoher Wahrscheinlichkeit erfüllbar ist.
Dazu führen wir folgende Normalform für widersprüchliche Kreise ein.

Definition 4. *(Kreise vom Typ a, b, c)*
Seien a, b und c natürliche Zahlen mit $a \geq 1$, $b \geq a$ und $c \geq 0$. Ein Kreis π ist vom Typ a, b, c, falls π folgendermaßen geschrieben werden kann:

$$\pi = \begin{array}{ccccccccc} & S_1 & \to & U_1 & \to & \cdots & \to & S_a & \to & U_a \\ & \uparrow & & & & & & & & \downarrow \\ & V_a & \leftarrow & \bar{S}_a & \leftarrow & \cdots & \leftarrow & V_1 & \leftarrow & \bar{S}_1 \end{array},$$

wobei die S_i nicht-leere Pfade und die U_i und V_i möglicherweise leere Pfade sind, sodass:

- *Für alle Paare l und $\bar{l}$ in π gibt es exakt ein i mit*

$$l \in S_i \text{ und } \bar{l} \in \bar{S}_i.$$

- *Die Anzahl widersprüchlicher Paare in π ist b:*

$$\sum_i |Lit\ S_i| = b.$$

- *Die Anzahl der Literale l in π, sodass das Komplement $\bar{l}$ nicht in π enthalten ist, ist c:*

$$\sum_i (|Lit\ U_i| + |Lit\ V_i|) = c.$$

Bemerkung 1. *Für einen Kreis π vom Typ a, b, c folgt per Definition $|Paar\ \pi| = a + b + c$ und length $\pi := |\{l \mid l \in \pi\}| = 2b + c$.*

Jeder Formelgraph mit einem widersprüchlichen Kreis, enthält einen Kreis vom Typ a, b, c. Betrachtet man beispielsweise folgenden widersprüchlichen Kreis

$$\pi^* = \begin{array}{ccccccc} u & \to & v & \to & w & \to & x \\ \uparrow & & & & & & \downarrow \\ z & \leftarrow & \bar{u} & \leftarrow & y & \leftarrow & \bar{w} \end{array}$$

in einem Formelgraphen, dann ist π^* selbst kein Kreis vom Typ a, b, c, aber da in einem Formelgraphen per Definition mit dem Pfad $u \to v \to w$ auch der Pfad $\bar{w} \to \bar{v} \to \bar{u}$ vorhanden sein muss, wissen wir, dass der Kreis

$$\pi = \begin{array}{ccccccc} u & \to & v & \to & w & \to & x \\ \uparrow & & & & & & \downarrow \\ z & \leftarrow & \bar{u} & \leftarrow & \bar{v} & \leftarrow & \bar{w} \end{array}$$

auch in dem Formelgraphen enthalten ist. π ist nun ein Kreis vom Typ $1, 3, 2$ mit $S_1 = u \to v \to w$, $U_1 = x$, $\bar{S}_1 = \bar{w} \to \bar{v} \to \bar{u}$ und $V_1 = z$.

Im folgenden werden wir sehen, dass die erwartete Anzahl von Kreisen in Normalform in einem uniform aus der Menge $FG(n, m)$ gewählten Formelgraphen G für n gegen unendlich gegen null geht. Aus Bemerkung 1 folgt dann, dass dieser Formelgraph mit hoher Wahrscheinlichkeit keinen widersprüchlichen Kreis enthält.

Lemma 1. *Sei $X_{a,b,c}$ die Anzahl Kreise vom Typ a, b, c in einem uniformen Formelgraphen G mit rn Paare komplementärer Kanten und X die Anzahl aller Kreise in Normalform in G. Dann gilt:*

(a) $\mathbb{E}[X_{a,b,c}] \leq \binom{b-1}{a-1}\binom{c+2a-1}{c}\left(\frac{1}{n}\right)^a r^{a+b+c}(1 + o(1))$.

(b) *Falls $r < 1$, dann gilt $\mathbb{E}[X] \to 0$ für $n \to \infty$.*

Beweis. von Lemma 1:
Teil (a):
Bezeichne $\mu_{a,b,c}$ die Anzahl der Kreise vom Typ a, b, c im vollständigen Formelgraphen über n Variablen. Dann gilt

$$\mu_{a,b,c} \leq \binom{n}{b} \cdot b! \cdot 2^b \cdot \binom{n-b}{c} \cdot c! \cdot 2^c \cdot \binom{b-1}{a-1} \cdot \binom{c+2a-1}{c} \cdot \frac{1}{2a}.$$

Denn wir können jeden Kreis π vom Typ a, b, c auf genau $2a$ Weise folgendermaßen erhalten:

(1) Wähle den Pfad $S = S_1 \to S_2 \to \cdots \to S_a$ aus. Dazu wähle man zunächst b aus den n Variablen, ordnet sie zu einem gerichteten Pfad und entscheidet schließlich ob man die Variablen negiert oder nicht. Es gibt also $\binom{n}{b} \cdot b! \cdot 2^b$ Möglichkeiten für den Pfad S an sich ohne die Aufteilung der Variablen auf die einzelnen S_i zu berücksichtigen.

(2) Wähle den Pfad $U = U_1 \to U_2 \to \cdots \to U_a \to V_1 \to \cdots \to V_a$ aus. Analog zu (1) gibt es hier $\binom{n-b}{c} \cdot c! \cdot 2^c$ Möglichkeiten für U.

(3) Gegeben den Pfad S, teile nun die Literale auf die S_i auf, sodass $S_i \neq \emptyset$ gilt. Die Anzahl der möglichen Aufteilungen kann man dadurch zählen, indem man zählt wieviele Möglichkeiten es gibt von den $b-1$ Kanten in S genau $a-1$ rauszunehmen. Da gibt es $\binom{b-1}{a-1}$ Möglichkeiten. Dies ist gerade die Anzahl von Vektoren $(m_1, \ldots, m_a)$ mit $m_1 + \ldots + m_a = b$ und $m_i \in \mathbb{N}$.

(4) Gegeben den Pfad U, teile die Literale auf die U_i und V_i auf, wobei dieses mal leere Pfade erlaubt sind. Um wieder die Anzahl der Möglichkeiten zu zählen, schaut man sich an wieviele Vektoren $(m_1, \ldots, m_{2a})$ es gibt, mit $m_1 + \ldots + m_{2a} = c$ und $m_i \in \mathbb{N}_0$. Dies entspricht der Anzahl von Vektoren $(y_1, \ldots, y_{2a})$ mit $y_1 + \ldots + y_{2a} = c + 2a$ und $y_i \in \mathbb{N}$ (denn wähle $y_i = m_i + 1$). Dann folgt aus der Überlegung in (3) und der Tatsache, dass falls $a = 1$, $U_1, V_1 \neq \emptyset$ gelten muss, dass es höchstens $\binom{c+2a-1}{2a-1} = \binom{c+2a-1}{c}$ mögliche Aufteilungen des Pfades U gibt (siehe [23]).

(5) Da nun aber der gleiche Kreis durch (1)-(4) auf $2a$ Weise konstruiert werden kann, muss man die bisherige Gesamtanzahl noch durch $2a$ teilen und es folgt die behauptete Schranke.

Mit $|Paar\ \pi| = a + b + c$ für einen Kreis π vom Typ a, b, c folgt

$$\begin{aligned}
\mathbb{E}[X_{a,b,c}] &= \mathbb{E}\left[\sum_{i=1}^{\mu_{a,b,c}} \mathbb{1}_{\{\pi_i \in G\}}\right] = \mu_{a,b,c} \cdot \frac{\binom{2n(n-1)-(a+b+c)}{rn-(a+b+c)}}{\binom{2n(n-1)}{rn}} \\
&\leq \binom{n}{b} \cdot b! \cdot 2^b \cdot \binom{n-b}{c} \cdot c! \cdot 2^c \cdot \binom{b-1}{a-1} \cdot \binom{c+2a-1}{c} \cdot \frac{1}{2a} \cdot \frac{\binom{2n(n-1)-(a+b+c)}{rn-(a+b+c)}}{\binom{2n(n-1)}{rn}} \\
&= \binom{b-1}{a-1} \cdot \binom{c+2a-1}{c} \cdot \frac{1}{2a} \cdot \prod_{i=0}^{b+c-1} (n-i) \cdot 2^{b+c} \cdot \prod_{i=0}^{a+b+c-1} \frac{rn-i}{2n(n-1)-i} \\
&\overset{(*)}{\leq} \binom{b-1}{a-1} \cdot \binom{c+2a-1}{c} \cdot \frac{1}{2a} \cdot \frac{n}{n-1} \cdot \prod_{i=1}^{b+c-1} \frac{(n-i)}{(n-1)} \cdot \frac{1}{(2(n-1))^a} \cdot r^{a+b+c} \\
&\leq \binom{b-1}{a-1} \cdot \binom{c+2a-1}{c} \cdot \left(\frac{1}{n}\right)^a \cdot r^{a+b+c} \cdot (1 + o(1)),
\end{aligned}$$

wobei bei $(*)$ benutzt wurde, dass $\frac{rn-i}{2n(n-1)-i} \leq \frac{rn}{2n(n-1)}$ für $i \geq 0$ gilt.
Teil (b): Sei jetzt $r < 1$, dann ist

$$\begin{aligned}
\mathbb{E}[X] &= \sum_{a,b,c} \mathbb{E}[X_{a,b,c}] \\
&\overset{(a)}{\leq} \sum_{a=1}^{\infty} \sum_{b=a}^{\infty} \sum_{c=0}^{\infty} \binom{b-1}{a-1} \cdot \binom{c+2a-1}{2a-1} \cdot \frac{1}{2a} \cdot \frac{1}{(2(n-1))^a} \cdot r^{a+b+c} \\
&\leq \sum_{a=1}^{\infty} \frac{1}{(2(n-1))^a} \cdot r^a \sum_{b=a}^{\infty} \binom{b-1}{a-1} \cdot r^b \sum_{c=0}^{\infty} \binom{c+2a-1}{2a-1} \cdot r^c \\
&\leq \sum_{a=1}^{\infty} \frac{1}{(2(n-1))^a} \cdot r \sum_{b-1=a-1}^{\infty} \binom{b-1}{a-1} \cdot r^{b-1} \sum_{c=0}^{\infty} \binom{c+2a-1}{2a-1} \cdot r^c \\
&= \sum_{a=1}^{\infty} \frac{1}{(2(n-1))^a} \cdot \frac{r^{a-1}}{(1-r)^a} \cdot \frac{1}{(1-r)^{2a}} \text{ ([20], Formeln (5.56) und (5.57))} \\
&= \sum_{a=0}^{\infty} \left(\frac{r}{2(n-1)(1-r)^3}\right)^a - 1 \\
&= \frac{1}{1 - \frac{r}{2(n-1)(1-r)^3}} - 1 \to 0 \text{ für } n \to \infty.
\end{aligned}$$

□

D.h. der Formelgraph einer uniformen Formel $F_2(n,m)$ mit $m = rn$ Klauseln, $r < 1$, hat mit hoher Wahrscheinlichkeit keine Kreise in Normalform und wegen Bemerkung 1 erst recht keine widersprüchlichen Kreise. Daher ist $F_2(n,m)$ mit hoher Wahrscheinlichkeit erfüllbar und Theorem 2 (i) folgt. □

Beweis. Teil (ii).
Für Teil (ii) von Theorem 2 folgen wir dem Beweis von Chvátal und Reed [10]. Dazu wählen wir zunächst eine von n abhängige natürliche Zahl $t = t(n)$, sodass

$$\frac{t}{\log n} \to \infty \text{ und } \frac{t}{n^{1/9}} \to 0 \tag{8}$$

für n gegen unendlich gilt.

Definition 5. *(Schlangen)*
Eine Schlange ist eine Folge von Literalen $A = (l_1, \ldots, l_s)$, $l_i \neq l_j$ und $l_i \neq \bar{l}_j$ für alle $i \neq j$, mit $s = 2t - 1$. Für eine Schlange $A = (l_1, \ldots, l_s)$ sei

$$F_A = \{\left(\bar{l}_i \vee l_{i+1}\right) \mid 0 \leq i \leq s,\ l_0 = l_{s+1} = \bar{l}_t\}.$$

Bemerkung 2. *Eine Formel F, die die Menge F_A für eine Schlange $A = (l_1, \ldots, l_s)$ enthält, ist nicht erfüllbar, da dieser Menge im Formelgraphen G_F von F folgende zwei widersprüchliche Kreise entsprechen:*

$$\pi_1 = \begin{array}{ccccccc} \bar{l}_t & \to & l_1 & \to & \cdots & \to & l_{t-1} \\ \uparrow & & & & & & \downarrow \\ l_s & \leftarrow & \cdots & \leftarrow & l_{t+1} & \leftarrow & l_t \end{array}$$

und

$$\pi_2 = \begin{array}{ccccccc} l_t & \to & \bar{l}_s & \to & \cdots & \to & \bar{l}_{t+1} \\ \uparrow & & & & & & \downarrow \\ \bar{l}_1 & \leftarrow & \cdots & \leftarrow & \bar{l}_{t-1} & \leftarrow & \bar{l}_t \end{array} .$$

Nach Definition 3 sind diese Kreise vom Typ $1, 1, 2(t-1)$.

Unser Ziel wird nun sein zu zeigen, dass für $m = rn$, $r > 1$, eine zufällige uniforme 2-SAT Formel $F_2(n,m)$ mit Wahrscheinlichkeit $1 - o(1)$ alle Klauseln einer Menge F_A enthält. Es ist zu erwähnen, dass Chvátal und Reed im Gegensatz zu Goerdt die Version 1.(i) aus unsere Definition des $F_{n,m}$-Modell aus der Einleitung verwenden, d.h. eine Klausel kann unter den m Klauseln einer Formel mehrfach vorkommen.
Sei nun

$$X = \sum_A X_A$$

mit

$$X_A = \begin{cases} 1 & \text{, falls } F_A \text{ genau einmal in } F_2(n,m) \text{ enthalten ist} \\ 0 & \text{, sonst.} \end{cases}$$

Wir werden zeigen, dass $\mathbb{E}\left[X^2\right] \leq (1 + o(1)) \cdot \mathbb{E}\left[X\right]^2$ gilt. Dann folgt die Behauptung aus folgendem Lemma.

Lemma 2. *(Second Moment Method)*
Für jede nichtnegative Zufallsvariable X gilt

$$\mathbb{P}(X > 0) \geq \frac{\mathbb{E}[X]^2}{\mathbb{E}[X^2]}.$$

Beweis. Da $X \geq 0$, gilt mit der Cauchy-Schwarz Ungleichung

$$\begin{aligned} \mathbb{E}[X]^2 &= \mathbb{E}\left[X \cdot \mathbb{1}_{\{X>0\}}\right]^2 \\ &\leq \mathbb{E}\left[X^2\right] \cdot \mathbb{E}\left[\mathbb{1}^2_{\{X>0\}}\right] \\ &= \mathbb{E}\left[X^2\right] \cdot \mathbb{P}(X > 0). \end{aligned}$$

□

Für beliebige Schlangen A und B gilt

$$\mathbb{E}[X_A] = \binom{m}{2t} \cdot (2t)! \cdot \left(\frac{1}{2n(n-1)}\right)^{2t} \cdot \left(1 - \frac{2t}{2n(n-1)}\right)^{m-2t} \tag{9}$$

und für den Fall, dass F_A und F_B genau i Klauseln gemeinsam haben

$$\mathbb{E}[X_A \cdot X_B] = \binom{m}{4t-i} \cdot (4t-i)! \cdot \left(\frac{1}{2n(n-1)}\right)^{4t-i} \cdot \left(1 - \frac{4t-i}{2n(n-1)}\right)^{m-4t+i}. \tag{10}$$

Mit

$$f(x) = \binom{m}{x} \cdot x! \cdot \left(\frac{1}{2n(n-1)}\right)^{x} \cdot \left(1 - \frac{x}{2n(n-1)}\right)^{m-x},$$

ist also $\mathbb{E}[X_A] = f(2t)$ und $\mathbb{E}[X_A \cdot X_B] = f(4t-i)$ und man kann zeigen, dass für $x = O(n^\alpha)$, $\alpha < \frac{1}{2}$,

$$f(x) = (1 + o(1)) \cdot \left(\frac{m}{2n(n-1)}\right)^{x}$$

gilt. Da nach (8) $t = O(n^{\frac{1}{9}})$, können wir für alle $1 \leq i \leq 2t$ also schreiben:

$$\begin{aligned} \frac{f(4t-i)}{f(2t)^2} &= (1 + o(1)) \cdot \left[\frac{\left(\frac{m}{2n(n-1)}\right)^{4t-i}}{\left(\left(\frac{m}{2n(n-1)}\right)^{2t}\right)^2}\right] \\ &= (1 + o(1)) \cdot \left(\frac{2n(n-1)}{m}\right)^{i}. \end{aligned} \tag{11}$$

Bezeichne $p_i(n)$ die Wahrscheinlichkeit, dass für eine feste Schlange A und eine Schlange B, die uniform aus der Menge aller Schlangen gewählt wird, die Mengen F_A und F_B genau i Klauseln gemeinsam haben und weiter sei K die Anzahl aller Schlangen im vollständigen

Formelgraphen. Es folgt dann für das zweite Moment von X

$$\begin{aligned}
\mathbb{E}\left[X^2\right] &= \sum_{A,B} \mathbb{E}\left[X_A \cdot X_B\right] \\
&= \sum_{A,B} \mathbb{P}\left(X_A = 1, X_B = 1\right) \\
&= \sum_{A,B} \mathbb{P}\left(X_A = 1\right) \cdot \mathbb{P}\left(X_B = 1 \mid X_A = 1\right) \\
&= \sum_{A} \left(\mathbb{P}\left(X_A = 1\right) \sum_{B} \mathbb{P}\left(X_B = 1 \mid X_A = 1\right) \right) \\
&= \left(\sum_{A} \mathbb{P}\left(X_A = 1\right) \right) \cdot \left(\sum_{B} \mathbb{P}\left(X_B = 1 \mid X_A = 1\right) \right) \\
&= \mathbb{E}\left[X\right] \cdot \sum_{B} \sum_{i=0}^{2t} p_i(n) \cdot \frac{f(4t-i)}{f(2t)} \\
&= \mathbb{E}\left[X\right] \cdot K \cdot f(2t) \cdot \sum_{i=0}^{2t} p_i(n) \cdot \frac{f(4t-i)}{f(2t)^2} \\
&= (1+o(1))\, \mathbb{E}\left[X\right]^2 \cdot \sum_{i=0}^{2t} p_i(n) \cdot \left(\frac{2n(n-1)}{m} \right)^i . \qquad (12)
\end{aligned}$$

Um den Ausdruck in (12) weiter zu behandeln, müssen wir die dort auftauchende Summe weiter abschätzen. Dazu wollen wir folgendes Lemma aus [10] verwenden.

Lemma 3. *Für $p_i(n)$ wie oben definiert gilt*

1. $p_i(n) < \frac{1300t^9}{n} \cdot \left(\frac{1}{2n}\right)^i$ *für* $1 \le i \le t-1$ *und*
2. $p_i(n) < 18tn \cdot \left(\frac{1}{2n}\right)^i$ *für* $1 \le i \le 2t$.

Dieses Lemma und die Tatsache wie $t = t(n)$ in (8) gewählt wurde liefert dann zunächst für den ersten Teil der Summe in (12)

$$\begin{aligned}
\sum_{i=1}^{t-1} p_i(n) \cdot \left(\frac{2n(n-1)}{rn} \right)^i &< \frac{1300t^9}{n} \sum_{i=1}^{t-1} \left(\frac{n-1}{rn} \right)^i \\
&= 1300 \cdot \left(\frac{t}{n^{\frac{1}{9}}} \right)^9 \cdot \sum_{i=1}^{t-1} \left(\frac{n-1}{rn} \right)^i \qquad (13) \\
&= o(1). \qquad (14)
\end{aligned}$$

Dabei verwenden wir um (14) zu erhalten, dass der zweite Faktor in (13) für n gegen unendlich gegen 0 geht und der letzte Faktor wegen $r > 1$ beschränkt ist.
Für den zweiten Teil der Summe gilt

$$\begin{aligned}
\sum_{i=t}^{2t} p_i(n) \cdot \left(\frac{2n(n-1)}{rn} \right)^i &< 18tn \cdot \sum_{i=t}^{2t} \left(\frac{n-1}{rn} \right)^i \\
&= 18tn \sum_{i=t}^{2t} \left(\frac{n-1}{rn} \right). \qquad (15)
\end{aligned}$$

Wählt man beispielsweise $t = n^{\frac{1}{10}}$, dann ist $18tn = O\left(n^{\frac{11}{10}}\right)$. Der größte Term in der Geometrischen Reihe ist allerdings $\left(\frac{n-1}{rn}\right)^{n^{\frac{1}{10}}}$, da $r > 1$, d.h. der gesamte Ausdruck konvergiert für n gegen unendlich gegen 0.
Insgesamt folgt

$$\mathbb{E}\left[X^2\right] \leq (1 + o(1)) \cdot \mathbb{E}\left[X\right]^2. \tag{16}$$

Also folgt aus Lemma 2 für n gegen unendlich

$$\begin{aligned} \mathbb{P}\left(F_2(n,m) \text{ nicht erfüllbar}\right) &\geq \mathbb{P}\left(X > 0\right) \\ &\geq \frac{\mathbb{E}\left[X\right]^2}{\mathbb{E}\left[X^2\right]} \\ &\geq \frac{\mathbb{E}\left[X\right]^2}{(1 + o(1)) \cdot \mathbb{E}\left[X\right]^2} \\ &= 1 - o(1) \end{aligned} \tag{17}$$

und daraus Teil (ii) von Theorem 2. □

2.2 Das zufällige $(2 + p)$-SAT-Problem

In diesem kurzen Abschnitt wollen wir einige Ergebnisse zum sogenannten $(2+p)$-SAT-Modell zusammenstellen. Dieses Modell betrachtet Formeln, die eine Mischung sind aus 2-Klauseln und 3-Klauseln, und wurde von Monasson et al in [22] zum ersten Mal eingeführt. Motiviert war das Modell durch das Interesse zu untersuchen, was eigentlich „zwischen“ 2-SAT und 3-SAT passiert. Eines der Ergebnisse, die man versucht hat zu erklären, war der Unterschied in der „Ordnung“ des Phasenübergangs von 2-SAT und k-SAT für $k \geq 3$. Dabei ist folgendes gemeint: Zunächst einmal bezeichnen wir eine Variable x *fest* in einer SAT-Formel F, falls x in allen erfüllenden Besetzungen von F den gleichen Wert hat. Nun wird als Ordnungsparameter der Anteil an festen Variablen betrachtet. Für $r > r_k$ hat eine zufällige k-SAT Formel $F_k(n, rn)$ mit hoher Wahrscheinlichkeit $f_k(r)n + o(n)$ feste Variablen. Mit dem oben angesprochenen Unterschied ist dann gemeint, dass für $k = 2$

$$\lim_{r \to r_2^+} f_2(r) = 0$$

gilt, wohingegen für $k \geq 3$

$$\lim_{r \to r_k^+} f_k(r) > 0$$

gilt.
Die Ergebnisse von Monasson et al. beruhen auf der sogenannten Replica-Methode aus der statistischen Mechanik. Da aber diese Methode auf noch nicht bewiesene Annahmen aufbaut, haben nun Achlioptas et al. einige Behauptungen zum $(2+p)$-SAT in [3] mathematisch rigorous bewiesen.
Kommen wir nun zur Definition des zufälligen $(2+p)$-SAT-Modells. Sei $p \in [0, 1]$. Eine zufällige $(2+p)$-SAT-Formel $F_{2+p}(n, m)$ ist eine zufällige Formel über n Variablen und mit m Klauseln, wobei von diesen pm Klauseln aus der Menge aller Klauseln der Länge 3 und $(1-p)m$ Klauseln aus der Menge der Klauseln der Länge 2 jeweils uniform und unabhängig (mit Zurücklegen)

gewählt werden. Wie man sieht, definiert dies für $p = 0$ eine 2-SAT-Formel und für $p = 1$ eine 3-SAT-Formel (Monasso et al sehen in diesem Modell auch eine Art Interpolation zwischen 2-SAT und 3-SAT). Nun ist $F_{2+p}(n, m)$ erfüllt, falls ihre 2-SAT Teilformel und ihre 3-SAT Teilformel unabhängig voneinander erfüllt sind. Das erste wichtige Theorem ist eine Version von Friedgut's Theorem für den $(2 + p)$-SAT:

Theorem 3. *(Theorem 2 in [3])*
Für jedes $p \in [0, 1]$ existiert ein kritischer Wert $r_p(n)$, sodass für alle $\varepsilon > 0$

$$\lim_{n\to\infty} \mathbb{P}\left(F_{2+p}(n, r_p(n)n - \varepsilon) \text{ ist erfüllbar}\right) = 1 \tag{18}$$

und

$$\lim_{n\to\infty} \mathbb{P}\left(F_{2+p}(n, r_p(n)n + \varepsilon) \text{ ist erfüllbar}\right) = 0 \tag{19}$$

gelten.

Für bestimmte Werte für p konnten Achlioptas et al. den Grenzwert von $r_p(n)$ exakt bestimmen:

Theorem 4. *(Theorem 3 in [3])*
Sei $p \in [0, 2/5]$. Dann ist der Threshold des zufälligen $(2 + p)$-SAT gegeben durch

$$r_p = \frac{1}{1-p}. \tag{20}$$

Bemerkung 3. *Da eine zufällige $(2 + p)$-SAT-Formel $F_{2+p}(n, rn)$ per Definition $r(1 - p)n$ Klauseln der Länge 2 enthält, muss $r_p(1 - p) \leq r_2 = 1$ gelten. D.h. für alle $p \in [0, 1]$ ist der Threshold r_p nach oben beschränkt durch $1/(1 - p)$.*
Sei $F_2(n, (1 - \varepsilon)n)$ eine zufällige 2-SAT-Formel. Dann wissen wir bereits aus Theorem 2, dass diese für alle $\varepsilon > 0$ mit hoher Wahrscheinlichkeit erfüllbar ist. Nun können wir aus den beiden letzten Theoremen folgern, dass wenn wir zu $F_2(n, (1 - \varepsilon)n)$ $(2/3)n$ zufällige Klauseln der Länge 3 anhängen, die dadurch entstehende neue zufällige Formel immernoch mit hoher Wahrscheinlichkeit erfüllbar ist.

Für den Fall $p > 2/5$ konnten die Autoren in [3] r_p nicht exakt bestimmen, aber ein Intervall angeben, in dem der kritische Wert liegt:

Theorem 5. *Sei $p \in (2/5, 1]$. Dann gilt*

$$\frac{24p}{(p+2)^2} \leq r_p \leq \min\left(\frac{1}{1-p}, r^*\right), \tag{21}$$

wobei r^* die Lösung der Gleichung

$$\left(\frac{7}{6}\right)^{rp} \left(\frac{3}{4}\right)^{r} \left(2 - \exp\left(-r\left(\frac{2}{3} - \frac{5p}{21}\right)\right)\right) = 1$$

ist.

2.3 Das zufällige k-SAT-Problem, $k \geq 3$

In diesem Abschnitt wollen wir eine obere und eine untere Schranke für den Threshold für $k \geq 3$ herleiten. Hier werden wir das Modell mit Wiederholungen verwenden. Also bezeichne wieder $C_n(k)$ die Menge der $2^k n^k$ möglichen k-Klauseln auf $\{x_1, \ldots, x_n\}$. Eine zufällige k-SAT Formel $F_k(n, m)$ erhalten wir dann durch das uniforme, unabhängige Auswählen von $m = rn$ Klauseln $c_1, \ldots, c_m$ aus $C_n(k)$ und dann die UND-Verknüpfung diese (siehe Einleitung). Wir interessieren uns nun für die Größen

$$r_k^{sup} := \sup \{r \ : \ F_k(n, rn) \text{ ist m. h. W. erfüllbar}\} \tag{22}$$

und

$$r_k^{inf} := \inf \{r \ : \ F_k(n, rn) \text{ ist m. h. W. nicht erfüllbar}\} \tag{23}$$

Es gilt offenbar $r_k^{sup} \leq r_k^{inf}$. Wie bereits erwähnt, ist die Gleichheit nur im Fall $k = 2$ bewiesen. Eine obere Schranke für r_k^{inf} lässt sich in diesem Modell durch die sogenannte First-Moment-Methode herleiten. Hat man eine Zufallsvariable X mit Werten in $\mathbb{N}_0$, dann ist die Wahrscheinlichkeit, dass X strikt positiv ist, nach oben abgeschätzt durch ihren Erwartungswert.

Proposition 2. *Es gilt*

$$r_k^{inf} \leq 2^k \log 2. \tag{24}$$

Beweis. Sei X die Anzahl erfüllender Besetzungen einer zufälligen Formel $F_k(n, rn)$. Falls eine erfüllende Besetzung existiert, d.h. falls $X > 0$ gilt, dann ist $F_k(n, rn)$ erfüllbar. Die Wahrscheinlichkeit für das Ereignis kann man durch den Erwartungswert von X nach oben abschätzen. Bezeichne B die Menge aller Besetzungen und $S(F) \subset B$ die zufällige Menge der Besetzungen, die die Formel F erfüllen. Es gilt

$$\begin{aligned} \mathbb{E}[X] &= \mathbb{E}\left[\sum_{\sigma \in B} \mathbb{1}_{\{\sigma \in S(F)\}}\right] \\ &= 2^n \cdot \mathbb{P}(\sigma \text{ erfüllt } F_k(n, rn)) \\ &= 2^n \cdot \left(1 - 2^{-k}\right)^{rn} = \left(2\left(1 - 2^{-k}\right)^r\right)^n. \end{aligned} \tag{25}$$

Der letzte Ausdruck ist für $r \geq 2^k \log 2$ kleiner 1 und deshalb konvergiert der Erwartungswert von X für $n \to \infty$ gegen 0. Damit folgt schließlich

$$\mathbb{P}(F_k(n, rn) \text{ erfüllbar}) \leq \mathbb{P}(X > 0) \leq \mathbb{E}[X] \to 0, \tag{26}$$

für $n \to \infty$ und alle $r \geq 2^k \log 2$. □

Eine untere Schranke für r_k^{sup} leiten Achlioptas und Peres in [5] mithilfe der Second-Moment-Methode (Lemma 2) her. Eine naive Anwendung von Lemma 2 auf die zueben betrachtete Zufallsvariable X liefert jedoch keine brauchbare untere Schranke für $\mathbb{P}(X > 0)$. Berechnet man nämlich das zweite Moment von X, dann erhält man zunächst in diesem Wahrscheinlichkeitsmodell

$$\begin{aligned} \mathbb{E}\left[X^2\right] &= \mathbb{E}\left[\sum_{\sigma, \tau \in B} \mathbb{1}_{\{\sigma, \tau \in S(F)\}}\right] \\ &= \sum_{\sigma, \tau \in B} \prod_{c_i} \mathbb{E}\left[\mathbb{1}_{\{\sigma, \tau \in S(c_i)\}}\right]. \end{aligned} \tag{27}$$

Für ein Paar von Besetzungen (σ, τ) sei $z = \alpha n$ die Anzahl gleicher Werte unter σ und τ und $\mathbb{P}\left(\sigma, \tau \in S(c_i)\right) = 1 - 2^{1-k} + 2^{-k}\alpha^k =: f(\alpha)$. Dann lässt sich (27) weiter schreiben als

$$\mathbb{E}\left[X^2\right] = 2^n \cdot \sum_{z=0}^{n} \binom{n}{z} f(\alpha)^{rn}.$$

Und mithilfe der Approximation

$$\binom{n}{\alpha n} = \left(\alpha^\alpha (1-\alpha)^{1-\alpha}\right)^{-n} \times poly(n)$$

folgt

$$\begin{aligned} \mathbb{E}\left[X^2\right] &\leq 2^n \cdot \left(\max_{0\leq\alpha\leq 1} \left\{ \frac{f(\alpha)^r}{\alpha^\alpha (1-\alpha)^{1-\alpha}} \right\}\right)^n \times poly(n) \\ &=: \max_{0\leq\alpha\leq 1} \Lambda(\alpha)^n \times poly(n). \end{aligned} \tag{28}$$

Andererseits gilt für das Quadrat des Erwartungswertes

$$\begin{aligned} \mathbb{E}\left[X\right]^2 &= \left(\left(2(1-2^{-k})^r\right)^n\right)^2 = 4^n f\left(\frac{1}{2}\right)^{rn} \\ &= \Lambda\left(\frac{1}{2}\right)^n. \end{aligned} \tag{29}$$

Solange das Maximum von Λ nicht bei $\alpha = 1/2$ angenommen wird, ist die durch die Second-Moment-Methode resultierende untere Schranke für $\mathbb{P}(X > 0)$ exponentiell (in n) klein und daher scheitert das Vorgehen mit der Zufallsvariable X. Da man die Second-Moment-Methode auf jede Zufallsvariable Y mit der Eigenschaft, dass aus $Y > 0$ folgt, dass die Menge der erfüllenden Besetzungen $S(F)$ nichtleer ist, anwenden kann, kam man auf die Idee, $X = \sum_{\sigma\in B} \mathbb{1}_{\{\sigma\in S(F)\}}$ durch eine gewichtete Anzahl $\bar{X} := \sum_{\sigma\in B} w(\sigma, F)$, mit $w(\sigma, F) = 0$ für $\sigma \notin S(F)$, zu ersetzen. Die Motivation hierfür kam u.a. auch aus [14], in der Peres et al die Erdős-Taylor-Vermutung von 1960 (siehe [15]) mit Hilfe dieser Idee beweisen.

Betrachten wir nun also die Zufallsvariable

$$\bar{X} = \sum_{\sigma\in B} \prod_{i=1}^{m} w(\sigma, c_i).$$

Dann gilt in unserem Modell zunächst für jede Funktion w

$$\begin{aligned} \mathbb{E}[\bar{X}] &= \sum_{\sigma\in B} \prod_{i=1}^{m} \mathbb{E}[w(\sigma, c_i)] \\ &= 2^n \cdot \left(\mathbb{E}[w(\sigma, c_1)]\right)^m \end{aligned} \tag{30}$$

und

$$\begin{aligned} \mathbb{E}[\bar{X}^2] &= \sum_{\sigma,\tau\in B} \prod_{i=1}^{m} \mathbb{E}[w(\sigma, c_i) w(\tau, c_i)] \\ &= \sum_{\sigma,\tau\in B} \left(\mathbb{E}[w(\sigma, c_1) w(\tau, c_1)]\right)^m. \end{aligned} \tag{31}$$

Da in dem Fall von unabhängig und uniform gewählten Klauseln die Variablenindices irrelevant sind, soll für jede Besetzung σ und jede Klausel $c = l_1, \cdots, l_k$ $w(\sigma, c) = w(v)$ sein, wobei für $1 \leq i \leq k$

$$v_i = \begin{cases} +1 & \text{, falls } l_i = 1 \text{ unter } \sigma \\ -1 & \text{, falls } l_i = 0 \text{ unter } \sigma \end{cases}$$

ist. Mit $A = \{+1, -1\}^k$ folgt

$$\mathbb{E}[w(\sigma, c_1)] = \mathbb{E}[w(V)] = \sum_{v \in A} w(v) 2^{-k}$$

und für jedes Paar von Besetzungen σ, τ mit $z = \alpha n$ übereinstimmenden Belegungen

$$\begin{aligned} \mathbb{E}[w(\sigma, c_1) w(\tau, c_1)] &= \sum_{u,v \in A} w(u) w(v) 2^{-k} \prod_{i=1}^{k} \left(\alpha^{\mathbb{1}_{u_i = v_i}} \cdot (1-\alpha)^{\mathbb{1}_{u_i \neq v_i}} \right) \\ &=: f_w(\alpha). \end{aligned}$$

Damit folgt analog zu (28)

$$\begin{aligned} \mathbb{E}[\bar{X}^2] &= \sum_{\sigma, \tau \in B} f_w(\alpha)^m \\ &= 2^n \cdot \sum_{z=0}^{n} \binom{n}{z} f_w(z/n)^m \\ &\leq 2^n \cdot \left(\max_{0 \leq \alpha \leq 1} \left\{ \frac{f_w(\alpha)^r}{\alpha^\alpha (1-\alpha)^{1-\alpha}} \right\} \right)^n \times poly(n) \\ &=: \left(\max_{0 \leq \alpha \leq 1} \Lambda_w(\alpha) \right)^n \times poly(n) \end{aligned} \tag{32}$$

und

$$\mathbb{E}[\bar{X}]^2 = \Lambda_w(1/2)^n.$$

Um sicherzustellen, dass die Second-Moment-Methode in diesem Fall nicht scheitert, verlangen wir, dass die Abbildung Λ_w ihr globales Maximum bei $\alpha = 1/2$ annimmt. Die notwendige Bedingung dafür ist $\Lambda'_w(1/2) = 0$. Da die Entropiefunktion $E(\alpha) = \alpha^\alpha (1-\alpha)^{1-\alpha}$ ihr Maximum bei $\alpha = 1/2$ annimmt, ist die notwendige Bedingung also genau dann erfüllt, falls $f'_w(1/2) = 0$ ist. Berechnet man die erste Ableitung von f_w an der Stelle $\alpha = 1/2$ und setzt diese gleich 0, dann erhalten wir folgende Bedingung:

$$f'_w(1/2) = 0 \;\Leftrightarrow\; \sum_{v \in A} w(v) v = 0. \tag{33}$$

Gesucht ist nun eine Abbildung w, welche die Bedingung (33) erfüllt, und durch welche man nahe wie möglich an die Anzahl X herankommt. Achlioptas und Peres lösen dieses Problem durch die Betrachtung folgender Zufallsvariable:

$$\bar{X} := \sum_{\sigma \in B} \gamma^{H(\sigma, F)} \mathbb{1}_{\{\sigma \in S(F)\}}, \tag{34}$$

wobei $\gamma \in (0,1]$ und $H(\sigma, F)$ für $\sigma \in \{0,1\}^n$ die Differenz der Anzahl der durch σ erfüllter Literale (=: $L(\sigma, F)$) in F und der Anzahl der durch σ nicht erfüllten Literale in F bezeichnet, also

$$H(\sigma, F) := \sum_{i=1}^{km} \mathbb{1}_{\{\sigma \in S(l_i)\}} - \sum_{i=1}^{km} \mathbb{1}_{\{\sigma \notin S(l_i)\}} = \left(2 \cdot \sum_{i=1}^{km} \mathbb{1}_{\{\sigma \in S(l_i)\}}\right) - km = 2L(\sigma, F) - km.$$

Man sieht, dass durch diese Wahl von Gewichten erfüllende Besetzungen, die relativ viele Literale in der Formel verfüllen, schwächer gewichtet werden als erfüllende Besetzungen, die die Formel gerade so noch erfüllen.
Diese Zufallsvariable (34) ist nun der wichtige Ausgangspunkt für den Beweis für die folgende untere Schranke für r_k^{sup}:

Theorem 6. *Es existiert eine Nullfolge $(\beta_k)_{k\geq 1}$, sodass für alle $k \geq 3$*

$$r_k^{sup} \geq 2^k \log 2 - 2(k+1)\log 2 - 1 - \beta_k. \tag{35}$$

Beweis. Wir müssen zeigen, dass

$$\lim_{n\to\infty} \mathbb{P}\left(F_k(n, rn) \text{ erfüllbar}\right) = 1$$

für alle $r \leq 2^k \log 2 - 2(k+1)\log 2 - 1 - \beta_k$. Für $\bar{X}$, wie in (34) definiert, gilt, dass die zufällige Formel $F_k(n, rn)$ genau dann erfüllbar ist, wenn $\bar{X} > 0$. Wir werden im folgenden zeigen, dass für die in Theorem 6 geforderten Werte für r und einer Konstanten $C > 0$ $\mathbb{E}[\bar{X}^2] < C \cdot \mathbb{E}[\bar{X}]^2$ gilt, was uns die erfolgreiche Anwendung der Second-Moment-Methode ermöglicht.
Zunächst erinnern wir uns daran, dass in der zufälligen k-SAT Formel $F = F_k(n, m)$ die $m = rn$ Klauseln $\{c_1, \ldots, c_m\}$ unabhängige und identisch verteilte Zufallsvariablen sind, wobei die c_i logische ODER-Verknüpfungen von k unabhängigen und identisch uniform verteilten Zufallsvariablen $\{l_1^i, \ldots, l_k^i\}$ sind.
Damit gilt für den Erwartungswert von $\bar{X}$

$$\begin{aligned}
\mathbb{E}[\bar{X}] &= \mathbb{E}\left[\sum_{\sigma\in B} \gamma^{H(\sigma,F)} \mathbb{1}_{\{\sigma\in S(F)\}}\right] \\
&= \sum_{\sigma\in B} \prod_{i=1}^{m} \mathbb{E}\left[\gamma^{H(\sigma,c_i)} \mathbb{1}_{\{\sigma\in S(c_i)\}}\right] \\
&= \left(2\mathbb{E}\left[\gamma^{H(\sigma,c_1)} \mathbb{1}_{\{\sigma\in S(c_1)\}}\right]^r\right)^n =: \left(2\psi(\gamma)^r\right)^n .
\end{aligned} \tag{36}$$

Für $0 < \gamma \leq 1$ ist $\psi(\gamma)$ gegeben durch

$$\begin{aligned}
\psi(\gamma) &= \mathbb{E}\left[\gamma^{H(\sigma,c_1)} \left(1 - \mathbb{1}_{\{\sigma\notin S(c_1)\}}\right)\right] \\
&= \mathbb{E}\left[\gamma^{H(\sigma,c_1)}\right] - (2\gamma)^{-k} \\
&= \mathbb{E}\left[\prod_{j=1}^{k} \gamma^{H(\sigma,l_j^1)}\right] - (2\gamma)^{-k} \\
&= \left(\frac{\gamma + \gamma^{-1}}{2}\right)^k - (2\gamma)^{-k}.
\end{aligned} \tag{37}$$

Das zweite Moment von $\bar{X}$ lässt sich zunächst schreiben als

$$\begin{aligned}\mathbb{E}[\bar{X}^2] &= \mathbb{E}\left[\left(\gamma^{H(\sigma,F)}\mathbb{1}_{\{\sigma\in S(F)\}}\right)^2\right] \\ &= \sum_{\sigma,\tau\in B}\mathbb{E}\left[\gamma^{H(\sigma,F)+H(\tau,F)}\mathbb{1}_{\{\sigma,\tau\in S(F)\}}\right] \\ &= \sum_{\sigma,\tau\in B}\mathbb{E}\left[\gamma^{H(\sigma,c_1)+H(\tau,c_1)}\mathbb{1}_{\{\sigma,\tau\in S(c_1)\}}\right]^{rn}. \end{aligned} \tag{38}$$

Schauen wir uns den Erwartungswert in (38) genauer an. Da für feste Besetzungen σ und τ die Gleichheit $\mathbb{1}_{\{\sigma,\tau\in S(c_1)\}} = 1 - \mathbb{1}_{\{\sigma\notin S(c_1)\}} - \mathbb{1}_{\{\tau\notin S(c_1)\}} + \mathbb{1}_{\{\sigma,\tau\notin S(c_1)\}}$ gilt, folgt für σ,τ mit $z = \alpha n$ übereinstimmenden Belegungen

$$\begin{aligned}\mathbb{E}\left[\gamma^{H(\sigma,c_1)+H(\tau,c_1)}\mathbb{1}_{\{\sigma,\tau\in S(c_1)\}}\right] &= \mathbb{E}\left[\prod_{j=1}^{k}\gamma^{H(\sigma,l_j^1)+H(\tau,l_j^1)}\right] \\ &\quad -2\cdot\mathbb{E}\left[\left(\prod_{j=1}^{k}\gamma^{H(\sigma,l_j^1)+H(\tau,l_j^1)}\right)\mathbb{1}_{\{\sigma\notin S(c_1)\}}\right] \\ &\quad +\mathbb{E}\left[\left(\prod_{j=1}^{k}\gamma^{H(\sigma,l_j^1)+H(\tau,l_j^1)}\right)\mathbb{1}_{\{\sigma,\tau\notin S(c_1)\}}\right] \\ &= \left(\alpha\left(\frac{\gamma^2+\gamma^{-2}}{2}\right)+1-\alpha\right)^k - 2\left(\frac{1-\alpha}{2}+\gamma^{-2}\cdot\frac{\alpha}{2}\right)^k \\ &\quad +\left(\gamma^{-2}\cdot\frac{\alpha}{2}\right)^k.\end{aligned}$$

Mit $\gamma^2 =: 1-\varepsilon$ gilt dann

$$\begin{aligned}\mathbb{E}\left[\gamma^{H(\sigma,c_1)+H(\tau,c_1)}\mathbb{1}_{\{\sigma,\tau\in S(c_1)\}}\right] &= \frac{\left(2-2\varepsilon+\alpha\varepsilon^2\right)^k - 2\left(1-\varepsilon+\alpha\varepsilon\right)^k+\alpha^k}{2^k\left(1-\varepsilon\right)^k} \\ &=: \frac{f(\alpha)}{2^k(1-\varepsilon)^k}.\end{aligned} \tag{39}$$

Einsetzen in (38) liefert schließlich

$$\mathbb{E}[\bar{X}^2] = 2^n\sum_{z=0}^{n}\binom{n}{z}\left(\frac{f(z/n)}{2^k(1-\varepsilon)^k}\right)^{rn}. \tag{40}$$

Da die Funktion f^r für jedes feste ε reellwertig, positiv und zweimal differenzierbar ist, können wir folgendes technisches Lemma aus [4] verwenden, um die Summe in (40) abzuschätzen.

Lemma 4. *Sei Φ eine reelle, positive, zweimal differenzierbare Funktion auf $[0,1]$ und*

$$S_n = \sum_{z=0}^{n}\binom{n}{z}\Phi(z/n)^n. \tag{41}$$

Sei weiter g auf $[0,1]$ definiert durch

$$g(\alpha) = \frac{\Phi(\alpha)}{\alpha^\alpha(1-\alpha)^{1-\alpha}} \tag{42}$$

mit der Konvention $0^0 = 1$.
Falls ein $\alpha_{max} \in (0,1)$ *existiert, so dass* $g(\alpha_{max}) =: g_{max} > g(\alpha)$ *für alle* $\alpha \neq \alpha_{max}$ *und* $g''(\alpha_{max}) < 0$*, dann existieren Konstanten* $C > 0$*, so dass für genügend große Werte für* n *gilt*

$$S_n < C \cdot g_{max}^n. \tag{43}$$

Beweis. Lemma 4:
Der Beweis beruht darauf, die Summe durch ein Integral abzuschätzen um dann die Laplace-Methode für asymptotische Integrale [13] zu verwenden.
Vorher leiten wir zwei obere Schranken für den z-ten Term der Summe S_n her. Mit der Stirling-Approximation

$$\sqrt{2\pi n} < \frac{n!}{(n/e)^n} < \sqrt{2\pi n}\left(1 + \frac{1}{n}\right)$$

erhalten wir für $\alpha \in [\delta, 1-\delta]$, $\delta > 0$ fest,

$$\begin{aligned} \binom{n}{z}\Phi(z/n)^n &= \frac{n!}{z!(n-z)!}\left(g(\alpha)\alpha^\alpha(1-\alpha)^{1-\alpha}\right)^n \\ &< \frac{1}{\sqrt{2\pi\alpha(1-\alpha)n}} g(\alpha)^n \left(1 + \frac{1}{n}\right). \end{aligned} \tag{44}$$

Aus der Analysis kennt man aber auch folgende Ungleichung für den Binomialkoeffizienten, die für alle $0 \leq z \leq n$ gilt

$$\binom{n}{z} \leq \frac{n^n}{z^z(n-z)^{n-z}}.$$

Damit erhalten wir eine zweite obere Schranke für den z-ten Term der Summe S_n

$$\begin{aligned} \binom{n}{z}\Phi(z/n)^n &\leq \frac{n^n}{z^z(n-z)^{n-z}} g(\alpha)^n \left(\left(\frac{z}{n}\right)^{z/n}\left(1 - \frac{z}{n}\right)^{1-z/n}\right)^n \\ &= g(\alpha)^n \end{aligned} \tag{45}$$

Nun gehen wir davon aus, dass ein $\alpha_{max} \in (0,1)$ existiert mit $g_{max} = g(\alpha_{max}) > g(\alpha)$ für alle $\alpha \neq \alpha_{max}$. Sei $I_\varepsilon := [\alpha_{max} - \varepsilon, \alpha_{max} + \varepsilon]$ die abgeschlossene ε-Umgebung von α_{max} in $\mathbb{R}$. Dann existiert für jedes $\varepsilon > 0$ eine Konstante $g_\varepsilon < g_{max}$, so dass $g(\alpha) < g_\varepsilon$ für alle $\alpha \notin I_\varepsilon$.
Seien weiter $z_\varepsilon^- := \lfloor(\alpha_{max} - \varepsilon)n\rfloor$, $z_\varepsilon^+ := \lceil(\alpha_{max} + \varepsilon)n\rceil$ und

$$S_n^{(\varepsilon)} := \sum_{z=z_\varepsilon^-}^{z_\varepsilon^+} \binom{n}{z}\Phi(z/n)^n. \tag{46}$$

Teilt man die Summe S_n auf in $S_n^{(\varepsilon)}$ und den restlichen Termen und benutzt (44) um die Summanden in $S_n^{(\varepsilon)}$ abzuschätzen und (45) um die verbleibenden Summanden abzuschätzen, dann erhalten wir für jedes $\varepsilon > 0$

$$S_n < (C_\varepsilon n)^{-1/2} \cdot \sum_{z=z_\varepsilon^-}^{z_\varepsilon^+} g(z/n)^n \tag{47}$$

mit einer Konstanten $C_\varepsilon > 2\pi \min\{(\alpha_{max} - \varepsilon)(1 - (\alpha_{max} - \varepsilon)), (\alpha_{max} + \varepsilon)(1 - (\alpha_{max} + \varepsilon))\}$.
Bevor wir fortfahren, wollen wir definieren, wann eine Funktion unimodal heißen soll.

Definition 6. *(Unimodale Funktion)*
Sei ψ eine zweimal differenzierbare Funktion. ψ heißt unimodal auf dem Interval $[a,b]$, falls ψ' eine eindeutige Nullstelle $c \in (a,b)$ hat und $\psi''(c) < 0$ ist.

Von der Funktion g wissen wir, dass sie zweimal differénzierbar ist und ein $\alpha_{max} \in (0,1)$ existiert, so dass $g'(\alpha_{max}) = 0$ und $g''(\alpha_{max}) < 0$. Nun können wir ε so klein wählen, dass g unimodal auf I_ε ist. Damit sind dann auch $\ln g$ und, für $n \geq 1$, g^n unimodal auf I_ε.
Die Idee war die Summe durch ein Integral abzuschätzen. Dazu verwenden wir die Tatsache, dass für jede nichtnegative und auf einem Intervall $[a,b]$ unimodale Funktion ψ, deren eindeutiges Maximum in $[a,b]$ wir mit ψ_{max} bezeichnen wollen,

$$\sum_{z=\lfloor an \rfloor}^{\lceil bn \rceil} \psi(z/n) \leq \int_a^b \psi(x)dx + \psi_{max} \tag{48}$$

gilt. Damit erhalten wir in unserem Fall

$$\sum_{z=z_\varepsilon^-}^{z_\varepsilon^+} g(z/n)^n \leq n \int_{I_\varepsilon} g(x)dx + g_{max}. \tag{49}$$

Nun können wir folgendes Lemma aus [13], welches aus der sogenannte Laplace-Methode für asymptotische Integrale folgt, verwenden.

Lemma 5. *Sei $h(x)$ unimodal auf $[a,b]$ und c die eindeutige Nullstelle von h' auf (a,b). Dann gilt*

$$\int_a^b e^{nh(x)}dx \sqrt{\frac{2\pi}{n|h''(c)|}} \cdot e^{nh(c)}. \tag{50}$$

Wählen wir $h = \ln g$ und $c = \alpha$, dann erhalten wir mit obigem Lemma

$$\begin{aligned} S_n &< (C_\varepsilon n)^{-1/2} \left(\int_{I_\varepsilon} g(\alpha)^n d\alpha + g_{max} \right) \\ &< C \cdot g_{max} \end{aligned} \tag{51}$$

mit einer von n unabhängigen Konstanten $C > 0$. □

Definieren wir in unserem Fall die Funktion $g =: g_r$ durch

$$g_r(\alpha) := \frac{f(\alpha)^r}{\alpha^\alpha (1-\alpha)^{1-\alpha}} \tag{52}$$

und sei weiter

$$s_k := 2^k \log 2 \log 2(k+1) - 1 - 3/k. \tag{53}$$

Nun erlaubt uns folgender Hilfssatz die Verwendung von Lemma 4 mit der Funktion g_r.

Lemma 6. *Sei $\varepsilon \in (0,1)$ so gewählt, dass die Gleichung*

$$\varepsilon(2-\varepsilon)^{k-1} = 1 \tag{54}$$

erfüllt ist. Für alle $k \geq 22$ gilt dann, falls $r \leq s_k$, $g_r(1/2) > g_r(\alpha)$ für alle $\alpha \neq 1/2$ und $g_r''(1/2) < 0$.

Bevor wir dieses wichtige Lemma beweisen, wollen wir sehen, wie nun aus Lemma 4 die Behauptung in Theorem 6 mithilfe der Second-Moment-Methode folgt.
Seien dazu r, k und ε wie in Lemma 6 gefordert. Dann folgt aus Lemma 4 zunächst für das zweite Moment von $\bar{X}$

$$\begin{aligned}\mathbb{E}[\bar{X}^2] &= 2^n \sum_{z=0}^{n} \binom{n}{z} \left(\frac{f(z/n)}{2^k(1-\varepsilon)^k}\right)^{rn} \\ &= 2^n \left(\frac{1}{2}^k (1-\varepsilon)^k\right)^{rn} \sum_{z=0}^{n} \binom{n}{z} (f(z/n)^r)^n \\ &< C \cdot \left(\frac{2g_r(1/2)}{(2(1-\varepsilon))^{rk}}\right)^n \end{aligned} \tag{55}$$

mit einer von n unabhängigen Konstante $C = C(k)$. Das Quadrat des Erwartungswertes lässt sich mit (36), (37), $\gamma^2 = 1-\varepsilon$ und f wie in (39) folgendermaßen schreiben

$$\begin{aligned}\mathbb{E}[\bar{X}]^2 &= 4^n \left(\psi(\gamma)^2\right)^{rn} \\ &= \left(\frac{4f(1/2)^r}{(2(1-\varepsilon))^{rk}}\right)^n. \end{aligned} \tag{56}$$

Da nach Definition $2f(1/2)^r = g_r(1/2)$, folgt

$$\mathbb{E}[\bar{X}]^2 = \left(\frac{2g_r(1/2)}{(2(1-\varepsilon))^{rk}}\right)^n. \tag{57}$$

Für r, k und ε wie in Lemma 6 gilt daher

$$\mathbb{E}[\bar{X}^2] < C \cdot \left(\frac{2g_r(1/2)}{(2(1-\varepsilon))^{rk}}\right)^n = C \cdot \mathbb{E}[\bar{X}]^2. \tag{58}$$

Jetzt sind wir in der Situation, wo wir die Second-Moment-Methode (Lemma 2) erfolgreich anwenden können. Mit Lemma 2 erhalten wir nämlich für eine zufällige uniforme Formel $F_k(n, rn)$

$$\mathbb{P}\left(F_k(n, rn) \text{ erfüllbar}\right) = \mathbb{P}(\bar{X} > 0) > 1/C.$$

Mit Friedgut's Theorem wissen wir dann, dass $r_k^{sup} \geq r$ sein muss für alle $r \leq s_k$, was die Behauptung in Theorem 6 impliziert.

Nun müssen wir versuchen das entscheidende Lemma 6 zu beweisen. Dies wird in [5] in mehreren Schritten gemacht:
Das folgende Lemma erlaubt es uns nur auf die $\alpha \in (1/2, 1]$ zu beschränken.

Lemma 7. *Für alle $\varepsilon, x > 0$ gilt $g_r(1/2 + x) > g_r(1/2 - x)$.*

Und anschließend zeigen wir, dass die Behauptung in Lemma 6 zunächst einmal für $\alpha \in (1/2, 4/5]$ gilt. Da die Funktion g_r eine weitere Maximalstelle bei 1 hat, müssen wir dann noch den Fall $\alpha \in (4/5, 1]$ separat behandeln:

Lemma 8. *Erfülle $\varepsilon \in (0, 1)$ die Gleichung (54). Für alle $k \geq 22$ gilt, falls $r \leq 2^k \log 2$, $g_r(1/2) > g_r(\alpha)$ für alle $\alpha \in (1/2, 4/5]$ und $g_r''(1/2) < 0$.*

Lemma 9. *Erfülle $\varepsilon \in (0,1)$ die Gleichung (54). Für alle $k \geq 22$ gilt, falls $r \leq s_k$, $g_r(1/2) > g_r(\alpha)$ für alle $\alpha \in (4/5, 1]$.*

Bevor wir diese drei Lemmata beweisen, zeigen wir folgendes Lemma, welches uns Auskunft darüber gibt, durch welche Schranken diejenigen $\varepsilon \in (0,1)$, die die Gleichung (54) erfüllen, beschränkt sind.

Lemma 10. *Sei $k \geq 3$ und erfülle $\varepsilon \in (0,1)$ die Gleichung (54). Dann gilt*

$$2^{1-k} + k4^{-k} < \varepsilon < 2^{1-k} + 3k4^{-k}. \tag{59}$$

Beweis. Lemma 10:
Als erstes stellen wir fest, dass die Ableitung für die in der Gleichung (54) auftauchende Funktion $q(x) := x(2-x)^{k-1}$ gegeben ist durch $q'(x) = (2-x)^{k-2}(2-kx)$ und dass $q(1) = 1$ ist. D.h. im Intervall $(0,1)$ gibt es genau einen Wert x_0, so dass $q(x_0) = 1$ gilt.
Seien nun $\theta := \varepsilon 2^{k-1}$ und $s(x) := x(1 - x/2^k)^{k-1}$. Damit lässt sich die Gleichung (54) also umschreiben in $s(\theta) = 1$. Seien weiter $\theta_1 := 1 + k/2^{k+1}$ und $\theta_2 := 1 + 3k/2^{k+1}$. Wenn wir zeigen können, dass $s(\theta_1) < 1$ und $s(\theta_2) > 1$ gilt, dann würde $\theta_1 < \theta < \theta_2$ folgen, welches die behaupteten Grenzen impliziert.
Zeigen wir zunächst, dass $s(\theta_1) < 1$ ist:

$$\begin{aligned} s(\theta_1) &= \left(1 + \frac{k}{2^{k+1}}\right)\left(1 - \frac{\left(1 + k/2^{k+1}\right)}{2^k}\right)^{k-1} \\ &< \left(1 + \frac{1}{2^k}\right)^{k-1}\left(1 - \frac{1}{2^k}\right)^{k-1} \qquad (60) \\ &= \left(1 - \left(\frac{1}{2^k}\right)^2\right)^{k-1} \\ &< 1. \end{aligned}$$

Dabei haben wir bei (60) benutzt, dass

$$\begin{aligned} \left(1 + \frac{1}{2^k}\right)^{k-1} &= \sum_{i=0}^{k-1} \binom{k-1}{i} \left(\frac{1}{2^k}\right)^i \\ &= 1 + \frac{k-1}{2^k} + \sum_{i=2}^{k-1} \binom{k-1}{i} \left(\frac{1}{2^k}\right)^i \\ &> 1 + \frac{k-1}{2^k} \\ &> 1 + \frac{k}{2^{k+1}} \qquad (61) \end{aligned}$$

gilt, wobei man die letzte Abschätzung einfach durch Induktion über alle $k \geq 3$ zeigen kann. Dann bleibt uns noch zu zeigen, dass $s(\theta_2) > 1$ ist. Für $k \in \{3,4,5,6\}$ kann man die Behauptung schnell per Einsetzen und Nachrechnen zeigen.
Sei nun $k \geq 7$. Dann liefert wieder die aus dem Binomischen Lehrsatz für alle $x > -1$ folgende

Ungleichung $(1+x)^j > 1+jx$

$$\begin{aligned} s(\theta_2) &= \theta_2\left(1-\frac{\theta_2}{2^k}\right)^{k-1} \\ &> \theta_2\left(1-\frac{(k-1)\theta_2}{2^k}\right) \\ &=: \tau(k). \end{aligned} \tag{62}$$

Was wir haben wollen, ist

$$\tau(k) = \left(1+\frac{3k}{2^{k+1}}\right)\left(1-\frac{(k-1)\left(1+3k/2^{k+1}\right)}{2^k}\right) \stackrel{!}{>} 1 \tag{63}$$

für $k \geq 7$. Diese Bedingung lässt sich äquivalent umformen in

$$(k-1)\left(1+\frac{3k}{2^{k+1}}\right)\left(2^{k+1}+3k\right) - 3k2^k \stackrel{!}{<} 0. \tag{64}$$

Da $\left(1+\frac{3k}{2^{k+1}}\right)$ für $k \geq 7$ echt kleiner als 1.4 ist, lässt sich (64) vereinfachen zu

$$4.2(k^2-k) - 2^k(0.2k+2.8) \stackrel{!}{<} 0. \tag{65}$$

(65) ist offensichtich für $k \geq 7$ erfüllt. Es folgt $s(\theta_2) > 1$ und zusammen mit $s(\theta_1) < 1$ die Behauptung in Lemma 10. □

Kommen wir nun zum Beweis der drei Lemmata, die zusammen Lemma 6 implizieren.

Beweis. Lemma 7:
Erinnern wir uns zunächst einmal, dass g_r definiert war durch

$$g_r(\alpha) = \frac{f(\alpha)^r}{\alpha^\alpha(1-\alpha)^{1-\alpha}}.$$

Da nun die Entropiefunktion $E(\alpha) = \alpha^\alpha(1-\alpha)^{1-\alpha}$ symmetrisch ist um $1/2$, d.h. $h(1/2+x) = h(1/2-x)$, gilt die Behauptung in Lemma 7 genau dann, wenn für alle $x > 0$

$$f(1/2+x) > f(1/2-x) \tag{66}$$

gilt. Dazu beobachten wir zunächst folgende Gleichheit für jedes $x \neq 0$

$$\begin{aligned} 2^k f(1/2+x) &= \left((2-\varepsilon)^2+2x\varepsilon^2\right)^k - 2\left(2-\varepsilon+2x\varepsilon\right)^k + (1+2x)^k \\ &= \sum_{j=0}^{k}\binom{k}{j}\left[(2-\varepsilon)^{2(k-j)}(2x\varepsilon^2)^j - 2(2-\varepsilon)^{k-j}(2x\varepsilon)^j + (2x)^j\right] \\ &= \sum_{j=0}^{k}\binom{k}{j}(2x)^j\left[\left((2-\varepsilon)^{k-j}\varepsilon^j\right)-1\right]^2. \end{aligned} \tag{67}$$

Also folgt mit (67) für alle $x > 0$

$$\begin{aligned} f(1/2+x) - f(1/2-x) &= 2^{-k} \sum_{j=0}^{k} \binom{k}{j} \left[\left((2-\varepsilon)^{k-j} \varepsilon^j \right) - 1 \right]^2 2^j \left(x^j - (-x)^j \right) \\ &= 2^{-k} \sum_{j=0}^{k} \binom{k}{j} \left[\left((2-\varepsilon)^{k-j} \varepsilon^j \right) - 1 \right]^2 2^{j+1} x^j. \end{aligned} \tag{68}$$

Da nun $\left[\left((2-\varepsilon)^{k-j} \varepsilon^j \right) - 1 \right]^2$ für $j = 0$ wegen (54) gleich 0 und für $j > 0$ echt größer 0 ist, folgt somit $f(1/2+x) - f(1/2-x) > 0$. □

Mit Lemma 7 können wir uns nun auf die $\alpha \in (1/2, 1]$ beschränken und zeigen zunächst Lemma 8:

Beweis. Lemma 8:
Wir wollen zeigen, dass g_r für alle $k \geq 22$ und $r \leq 2^k \log 2$ im Intervall $(1/2, 4/5]$ streng monoton fallend ist. Dazu betrachten wir zunächst die erste Ableitung von g_r. Die Ableitung der Entropiefunktion $E(\alpha) = \alpha^\alpha (1-\alpha)^{1-\alpha}$ ist wegen $x^x = e^{x \log x}$ gegeben durch

$$\begin{aligned} E'(\alpha) &= (\log \alpha + 1)\alpha^\alpha (1-\alpha)^{1-\alpha} + \alpha^\alpha (-\log(1-\alpha) + 1)(1-\alpha)^{1-\alpha} \\ &= \alpha^\alpha (1-\alpha)^{1-\alpha} \left(\log \alpha - \log(1-\alpha) \right). \end{aligned} \tag{69}$$

Damit ist

$$\begin{aligned} g_r'(\alpha) &= \frac{r f(\alpha)^{r-1} f'(\alpha) E(\alpha) - f(\alpha)^r E'(\alpha)}{E(\alpha)^2} \\ &= \frac{f(\alpha)^{r-1} \left(r f'(\alpha) + f(\alpha)(\log(1-\alpha) - \log \alpha) \right)}{\alpha^\alpha (1-\alpha)^{1-\alpha}} \end{aligned} \tag{70}$$

mit

$$f'(\alpha) = k \left((2 - 2\varepsilon - \alpha\varepsilon^2)^{k-1} \varepsilon^2 - 2(1 - \varepsilon + \alpha\varepsilon)^{k-1} \varepsilon - \alpha^{k-1} \right). \tag{71}$$

Da ε die Bedingung (54) erfüllt, sehen wir, dass

$$\begin{aligned} f'(1/2) &= k 2^{1-k} \left[(2-\varepsilon)^{k-1} \varepsilon - 1 \right]^2 \\ &= 0 \end{aligned} \tag{72}$$

und dadurch auch $g_r'(1/2) = f(1/2)^{r-1} f'(1/2) = 0$ gilt.
Um nun zu zeigen, dass g_r im Intervall $(1/2, 4/5]$ streng monoton fallend ist, reicht es, wegen $g_r'(1/2) = 0$ und $f(\alpha) > 0$ für alle $\alpha > 1/2$, zu zeigen, dass die erste Ableitung von

$$h(\alpha) := r f'(\alpha) + f(\alpha)(\log(1-\alpha) - \log \alpha) \tag{73}$$

im Intervall $(1/2, 4/5]$ negativ ist.
Die Ableitung von h ist

$$\begin{aligned} h'(\alpha) &= r f''(\alpha) + f'(\alpha) \left(\log(1-\alpha) - \log \alpha \right) \\ &\quad - f(\alpha) \left(\frac{1}{1-\alpha} + \frac{1}{\alpha} \right). \end{aligned} \tag{74}$$

Mit Hilfe von (67) sehen wir, dass f im gesamten Intervall $[1/2, 1]$ nichtfallend ist und, da $\log(1-\alpha) \leq \log\alpha$ für $\alpha \in [1/2, 1]$, haben wir also

$$f'(\alpha)\left(\log(1-\alpha) - \log\alpha\right) \leq 0. \tag{75}$$

D.h. h' ist im Intervall $(1/2, 4/5]$ negativ, falls

$$rf''(\alpha) - f(\alpha)\left(\frac{1}{1-\alpha} + \frac{1}{\alpha}\right) \leq 0 \tag{76}$$

gilt. Leiten wir zunächst eine obere Schranke für $f''(\alpha)$ für $\alpha \in (1/2, 4/5]$ her. Da für α, $\varepsilon \in (0,1)$ offenbar die Ungleichung $\alpha\varepsilon^2 \leq 2\varepsilon$ gilt, erhalten wir für alle $\alpha \in (1/2, 4/5]$

$$\begin{aligned} f''(\alpha) &= k(k-1)\left(\left(2-2\varepsilon+\alpha\varepsilon^2\right)^{k-2}\varepsilon^4 - 2(1-\varepsilon+\alpha\varepsilon)^{k-2}\varepsilon^2 + \alpha^{k-2}\right) \\ &\leq k^2\left(2^{k-2}\varepsilon^4 + \left(\frac{4}{5}\right)^{k-2}\right). \end{aligned} \tag{77}$$

Außerdem folgt für die Funktion $m(\alpha) := \frac{1}{1-\alpha} + \frac{1}{\alpha}$, da sie im Intervall $(1/2, 4/5]$ monoton wachsend ist, dass $m(\alpha) \geq m(1/2) = 4$ gilt und wie oben schon erwähnt, gilt $f(\alpha) \geq f(1/2) = 2^{-k}\left((2-\varepsilon)^k - 1\right)^2$ für alle $\alpha \in [1/2, 1]$. Fasst man dies nun zusammen, so erhalten wir folgende obere Schranke für den linken Ausdruck in (76)

$$\begin{aligned} rf''(\alpha) - f(\alpha)\left(\frac{1}{1-\alpha} + \frac{1}{\alpha}\right) &\leq rk^2\left(2^{k-2}\varepsilon^4 + \left(\frac{4}{5}\right)^{k-2}\right) \\ &\quad -4\cdot 2^{-k}\left((2-\varepsilon)^k - 1\right)^2 \end{aligned} \tag{78}$$

Nun reicht es zu zeigen, dass für die obere Schranke $\varepsilon_o = 2^{1-k} + 3k4^{-k}$ für ε aus Lemma 10 und $r = 2^k \log 2$ der rechte Ausdruck von (78) für $k \geq 22$ negativ ist. Für $k = 22$ rechnet man dies einfach nach und für $k > 22$ sieht man leicht durch Identifizieren der entscheidenden Terme, dass der erste Ausdruck der Differenz in (78) 'langsamer' wächst als der zweite Term und somit für große k (78) tatsächlich negativ ist.
Mit dem, was wir uns für den Beweis der ersten Behauptung von Lemma 8 erarbeitet haben, lässt sich die zweite Behauptung, dass $g_r''(1/2) < 0$ gilt, auch sehr schnell zeigen. Es gilt

$$g_r''(\alpha) = \frac{\left[(r-1)f(\alpha)^{r-2}f'(\alpha)F(\alpha) + f(\alpha)^{r-1}F'(\alpha)\right]E(\alpha) - f(\alpha)^{r-1}F(\alpha)E'(\alpha)}{E(\alpha)^2}.$$

Nun wissen wir bereits, dass $f(1/2) > 0$ und $f'(1/2) = 0$ gelten. Und wenn man oben genauer hinschaut, dann sieht man, dass wir nicht nur gezeigt haben, dass $F'(\alpha)$ für alle $\alpha \in (1/2, 4/5]$ strikt negativ ist, sondern auch für $\alpha = 1/2$. Mit diesen Ergebnissen folgt damit, dass $g_r''(1/2) < 0$ gilt. □

Nun wollen wir noch die Aussage für die $\alpha \in (4/5, 1]$ beweisen.

Beweis. Lemma 9:
Zunächst beobachten wir, dass die Ungleichung $g_r(1/2) > g_r(\alpha)$ mit Hilfe der Definition der Funktion g_r äquivalent in die Ungleichung

$$\left(\frac{f(\alpha)}{f(1/2)}\right)^r < 2\alpha^\alpha(1-\alpha)^{1-\alpha} \tag{79}$$

umgeformt werden kann. Logarithmiert man noch diese Ungleichung auf beiden Seiten, dann erhalten wir

$$r \log\left(\frac{f(\alpha)}{f(1/2)}\right) < \log 2 - H(\alpha), \tag{80}$$

wobei die Funktion H definiert ist durch $H(\alpha) := -\log(E(\alpha)) = -\alpha\log\alpha - (1-\alpha)\log(1-\alpha)$. Die linke Seite von (80) können wir schreiben als

$$r \log\left(\frac{f(\alpha)}{f(1/2)}\right) = r \log\left(1 + \frac{f(\alpha) - f(1/2)}{f(1/2)}\right). \tag{81}$$

Nun sei daran erinnert, dass f im Intervall $(1/2, 1]$ monoton wachsend ist, und dass damit insbesondere der Ausdruck $f(\alpha) - f(1/2)$ für alle $\alpha \in (1/2, 1]$ strikt positiv ist. Die Anwendung der für alle $x \geq 0$ geltenden Ungleichung $\log(1+x) \leq x$ liefert dann aus (81)

$$r \log\left(\frac{f(\alpha)}{f(1/2)}\right) \leq r\left(\frac{f(\alpha) - f(1/2)}{f(1/2)}\right). \tag{82}$$

Insgesamt folgt damit, dass die behauptete Ungleichung $g_r(1/2) > g_r(\alpha)$ gilt, falls wir zeigen können, dass

$$r < (\log 2 - H(\alpha)) \cdot \left(\frac{f(1/2)}{f(\alpha) - f(1/2)}\right) \tag{83}$$

gilt.
Schauen wir aber, ob wir (83) noch weiter vereinfachen können. Als erstes leiten wir eine untere Schranke für $f(1/2)$ her. Verwendet man aus Lemma 10, dass $\varepsilon < 2^{1-k} + 3k4^{-k}$ gilt, dann erhalten wir

$$\begin{aligned} f(1/2) &= \left(2 - 2\varepsilon + \varepsilon^2/2\right)^k - 2(1-\varepsilon/2)^k + (1/2)^k \\ &> (2(1-\varepsilon))^k - 2 \\ &> 2^k(1 - k\varepsilon) - 2 \\ &> 2^k\left(1 - k\left(2^{1-k} + 3k4^{-k}\right)\right) - 2 \\ &= 2^k - 2k - 2 + 3k^2 2^{-k}. \end{aligned} \tag{84}$$

Außerdem gilt für $f(\alpha)$ mit $\alpha = 1/2 + x$, $x > 0$, wegen (67) und der Tatsache, dass ε so gewählt wurde, dass die Bedingung (54) erfüllt ist, zunächst

$$\begin{aligned} f(1/2+x) &= 2^{-k}\sum_{j=0}^{k}\binom{k}{j}(2x)^j\left[\left((2-\varepsilon)^{k-j}\varepsilon^j\right) - 1\right]^2 \\ &= 2^{-k}\left((2-\varepsilon)^k - 1\right)^2 + 2^{-k}\sum_{j=2}^{k}\binom{k}{j}(2x)^j\left[\left((2-\varepsilon)^{k-j}\varepsilon^j\right) - 1\right]^2. \end{aligned} \tag{85}$$

Da nun ebenfalls wegen (54) für alle $j > 1$

$$\begin{aligned} 0 < (2-\varepsilon)^{k-j}\varepsilon^j &= \varepsilon(2-\varepsilon)^{k-1}(2-\varepsilon) - j + 1\varepsilon^{j-1} \\ &= \left(\frac{\varepsilon}{2-\varepsilon}\right)^{j-1} < 1. \end{aligned} \tag{86}$$

gilt, lässt sich (85) weiter abschätzen und wir erhalten

$$\begin{aligned} f(1/2+x) &\leq f(1/2) + 2^{-k} \sum_{j=0}^{k} \binom{k}{j} (2x)^j \\ &= f(1/2) + 2^{-k}(1+2x)^k \\ &= f(1/2) + \alpha^k. \end{aligned} \tag{87}$$

Damit ist der Ausdruck $f(\alpha) - f(1/2)$ kleiner als α^k für alle $\alpha \in (1/2, 1]$. Deshalb gilt die Ungleichung (83), solange

$$\begin{aligned} r &\leq \frac{\log 2 - H(\alpha)}{\alpha^k} \cdot f(1/2) \\ &=: \Phi(\alpha) \cdot f(1/2) \end{aligned} \tag{88}$$

gilt. Fortfahren wollen wir mit der Herleitung einer unteren Schranke für $\Phi(\alpha)$ für alle $\alpha \in (1/2, 1]$. Zunächst halten wir fest, dass wir mit $y := 1 - \alpha$ für alle $0 < y \leq 1/2$

$$\begin{aligned} -H(\alpha) &= -H(1-y) \\ &= (1-y)\log(1-y) + y \log y \\ &> \log(1-y) + y \log y \\ &> -y - y^2 + y \log y \end{aligned} \tag{89}$$

erhalten. Dabei haben wir im letzten Schritt verwendet, dass für alle $x \in (-1, 1]$ $\log(1+x)$ die Reihendarstellung

$$\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n \tag{90}$$

hat. Weiter beobachten wir, dass für $0 < y \leq 1/2$

$$\frac{1}{(1-y)^k} > (1+y)^k > 1 + ky \tag{91}$$

gilt. Damit sehen wir, dass $\Phi(\alpha)$ für alle $\alpha \in [1/2, 1)$ folgendermaßen nach unten beschränkt ist:

$$\begin{aligned} \Phi(\alpha) = \Phi(1-y) &= \frac{\log 2 - H(1-y)}{(1-y)^k} \\ &> (1+ky)\left(\log 2 - y(1 + y - \log y)\right). \end{aligned} \tag{92}$$

Diesen Ausdruck wollen wir weiter bearbeiten und führen zunächst die Substitution $y = d/2^k$ durch. Es gilt

$$\begin{aligned} \Phi(\alpha) &> (1 + kd2^{-k}) \left(\log 2 - d2^{-k}\left(1 + d2^{-k} - \log(d2^{-k})\right)\right) \\ &= \log 2 + d2^{-k}(\log d - 1) - d^2 4^{-k}\left(1 + k\left(1 + d2^{-k} - \log(d2^{-k})\right)\right) \\ &\geq \log 2 - 2^{-k} - d^2 4^{-k}\left(1 + k\left(1 + d2^{-k} - \log(d2^{-k})\right)\right) \qquad (93) \\ &= \log 2 - 2^{-k} - (1-\alpha)^2\left(1 + k\left(2 - \alpha - \log(1-\alpha)\right)\right) \\ &=: b(\alpha). \qquad (94) \end{aligned}$$

Dabei haben wir bei (93) benutzt, dass $d(\log d - 1)$ stets größer -1 ist. Diese Behauptung ist richtig, da man sehr leicht nachrechnen kann, dass das Minimum der Funktion $d(\log d - 1) = 2^k y \log y + 2^k(k \log 2 - 1)y$ gerade -1 ist.
Um nun zu ermitteln, wie die Funktion Φ im Intervall $(4/5, 1]$ beschränkt ist, reicht es die Werte $\Phi(4/5)$, $\Phi(1)$ und die diejenigen Werte $\Phi(\alpha)$, für die $\Phi'(\alpha) = 0$ gilt, zu kennen. Die erste Ableitung von Φ ist dabei gegeben durch

$$\Phi'(\alpha) = \frac{\alpha \log \alpha - \alpha \log(1-\alpha) - k \log 2 + kH(\alpha)}{\alpha^{k+1}}. \tag{95}$$

Was wir als erstes durch Einsetzen sehen, ist dass $\Phi'(4/5)$ für $k \geq 6$ strikt negativ ist. Für den Endpunkt des Intervalls gilt

$$\lim_{\alpha \to 1} \frac{\Phi'(\alpha)}{\log(1-\alpha)} = -1, \tag{96}$$

d.h. Φ strebt gegen ∞ für α gegen 1. Damit können wir uns auf das Intervall $(4/5, 1)$ beschränken.
Setzt man nun $\Phi'(\alpha)$ gleich 0, dann erhalten wir

$$\log(1-\alpha) = \log \alpha - \frac{k \log 2 - kH(\alpha)}{\alpha}, \tag{97}$$

und dadurch wegen $1/2 < \alpha < 1$ die Ungleichung

$$\log(1-\alpha) \leq -k(\log 2 - H(\alpha)). \tag{98}$$

Da nun $\log 2 - H(4/5) \approx 0.1927 > 1/6$ gilt, folgt mit (98) für alle k

$$\log(1-\alpha) \leq -k/6 \quad \text{bzw.} \quad \alpha > 1 - e^{-k/6}. \tag{99}$$

Dies ermöglicht uns nun die obere Schranke für die Funktion H aus (89) weiter abzuschätzen:

$$\begin{aligned} H(\alpha) &= H(1-y) \\ &< y + y^2 - y \log y \\ &< e^{k/6}\left(1 + e^{-k/6} + k/6\right) \\ &< e^{-k/6}(2 + k/6) =: Q(k). \end{aligned} \tag{100}$$

Wenn wir nun dieses Ergebnis in (98) einsetzen und nach α auflösen, dann erhalten wir

$$\alpha > 1 - e^{-k(\log 2 - Q(k))} =: \alpha_k^*. \tag{101}$$

Da nun für $k \geq 22$

$$\begin{aligned} \alpha_k^* &= 1 - \exp\left(-k\left(\log 2 - \exp(-k/6)/2 + k/6\right)\right) \\ &= 1 - 2^{-k} e^{e^{-k/6}(2k+6)} \\ &< \frac{4}{5}, \end{aligned} \tag{102}$$

muss Φ für $k \geq 22$ im Intervall $(4/5, \alpha_k^*]$ monoton fallend sein.
Außerdem sehen wir, dass die Funktion b, welche Φ von unten beschränkt, monoton wachsend ist. Damit folgt für alle $\alpha \in (4/5, 1]$

$$\begin{aligned} \Phi(\alpha) &> \Phi(\alpha_k^*) \\ &> b(\alpha_k^*) \\ &= \log 2 - 2^{-k} - (1-\alpha_k^*)^2 \left(1 + k\left(2 - \alpha_k^* - \log(1-\alpha_k^*)\right)\right). \end{aligned} \tag{103}$$

Da nun für $k \geq 22$

$$(1-\alpha_k^*)^2 \left(1 + k\left(2 - \alpha_k^* - \log(1-\alpha_k^*)\right)\right) < \frac{2}{k2^k}$$

gilt, folgt für $k \geq 22$ und $\alpha \in (4/5, 1]$

$$\Phi(\alpha) > \log 2 - 2^{-k} - \frac{2}{k2^k}. \tag{104}$$

Jetzt wollen die Teile zusammensetzen: Es sei erinnert, dass die zu beweisende Behauptung richtig ist, falls (88) gilt, d.h. falls für $k \geq 22$ und $r \leq s_k = 2^k \log 2 - 2(k+1)\log 2 - 1 - 3/k$

$$r \leq \Phi(\alpha) \cdot f(1/2)$$

gilt. Nun haben wir für $\Phi(\alpha)$ und $f(1/2)$ die untere Schranke (104) und (84) hergeleitet und damit ist obige Ungleichung erfüllt, falls für $k \geq 22$ und $r \leq s_k$ die Ungleichung

$$r < \left(\log 2 - 2^{-k} - \frac{2}{k2^k}\right) \cdot \left(2^k - 2k - 2 + 3k^2 2^{-k}\right) \tag{105}$$

gilt. Multipliziert man das Produkt auf der rechten Seite von (105) aus, so erhält man

$$\left(\log 2 - 2^{-k} - \frac{2}{k2^k}\right) \cdot \left(2^k - 2k - 2 + 3k^2 2^{-k}\right) = s_k + a_k \tag{106}$$

mit einer Folge a_k. Nun kann man leicht zeigen, dass a_k für $k \geq 22$ größer als 0 ist. Damit ist wegen $r \leq s_k$ (105) erfüllt und es folgt die Behauptung des Lemmas. □

Damit haben wir Lemma 6 bewiesen, welches, wie wir bereits gesehen haben, die behauptete Schranke aus Theorem 6 impliziert. □

2.4 Das zufällige $k(n)$-SAT-Problem

Bisher haben wir uns in diesem Kapitel mit dem Threshold r_k für das k-SAT Problem mit festem k beschäftigt und erwähnt, dass die Existenz von r_k noch nicht vollständig bewiesen ist, aber Friedgut's Theorem dies sehr nahelegt. Nun haben sich zunächst Frieze und Wormald gefragt, ob sich das Problem vereinfacht, wenn man jetzt, statt feste Werte für k zu betrachten, k von n abhängig macht. Die Antwort darauf ist positiv. In [18] zeigen die Autoren folgendes Theorem:

Theorem 7. *Angenommen,* $\omega := k - \log_2 n \to \infty$ *für* $n \to \infty$.
Seien nun

$$m_0 := \frac{n \ln 2}{\ln(1-2^{-k})} = \left(2^k + O(1)\right) n \ln 2, \tag{107}$$

so dass $2^n\left(1-1/2^k\right)^{m_0}=1$ *und* $\varepsilon=\varepsilon(n)>0$*, so dass* $\varepsilon n\to\infty$*. Für die zufällige uniforme k-SAT Formel* $F_k(n,m)$ *über* n *Variablen und mit* m *Klauseln gilt dann*

$$\lim_{n\to\infty}\mathbb{P}\left(F_k(n,m)\ \textit{erfüllbar}\right)=\begin{cases}1, & \textit{falls } m\le(1-\varepsilon)m_0\\ 0, & \textit{falls } m\ge(1+\varepsilon)m_0.\end{cases}$$

Mit diesem Theorem kann man die Behauptung der Existenz des Thresholds r_k für sehr große, aber feste k unterstützen. Man sieht, dass für den Threshold c_k hier $c_k\sim 2^k\ln 2$ gilt.
Wir wollen im folgenden eine Verschärfung der Aussage in Theorem 7 zeigen. Coja-Oghlan und Frieze haben in [11] gezeigt, dass unter etwas verschärften Bedingungen als in Theorem 7 sogar folgendes gilt:

Theorem 8. *Angenommen,* $\omega:=k-\log_2 n\to\infty$*, aber* $\omega=o(\ln n)$*.*
Sei $m=2^k(n\ln n+c)$ *für eine Konstante c. Für die zufällige uniforme k-SAT Formel* $F_k(n,m)$ *über* n *Variablen und mit* m *Klauseln gilt dann*

$$\lim_{n\to\infty}\mathbb{P}(F_k(n,m)\ \textit{erfüllbar})=1-e^{-e^{-c}}. \tag{108}$$

Hier wird also behauptet, dass die Anzahl erfüllender Besetzungen für $F_k(n,m)$ asymptotisch Poisson ist.

Beweis. Sei nun X_m die Anzahl der erfüllenden Besetzungen für die zufällige uniforme Formel $F_k(n,m)$ über n Variablen $V=\{x_1,\dots,x_n\}$ und mit m Klauseln $C_1,\dots,C_m$ der Länge $k=k(n)$. Im folgenden verwenden wir das Modell (siehe $2.F_{n,m}$-Modell in der Einleitung), in dem jedes Literal in C_i unabhängig und uniform aus der Menge $V\cup\bar{V}$ gewählt wird, wobei $\bar{V}$ die Menge der negierten Variablen $\bar{x}_1,\dots,\bar{x}_n$ bezeichnet.
Nehmen wir nun an, dass $k=\log_2 n+\omega$ gilt und seien weiter $m_0\sim 2^k n\ln 2$ wie in (107) und $m_1=m_0-2^k\gamma$, wobei $\gamma=\ln\omega$. Für zwei Besetzungen σ_1 und σ_2 der Variablen V bezeichne $h(\sigma_1,\sigma_2)$ den Hammingabstand dieser beiden Besetzungen, d.h. $h(\sigma_1,\sigma_2)$ bezeichnet die Anzahl der Indices $i\in\{1,\dots,n\}$, für welche $\sigma_1(i)\neq\sigma_2(i)$ gilt. Nun gelten folgende zwei Lemmata.

Lemma 11. ***E1****:*
Es gilt mit hoher Wahrscheinlichkeit

$$X_{m_1}\sim\mathbb{E}[X_{m_1}]\sim 2^n(1-2^{-k})^{m_1}=e^{\gamma}.$$

Lemma 12. ***E2****:*
Sei Z_t *die Anzahl von Paaren erfüllender Besetzungen* σ_1,σ_2 *mit* $h(\sigma_1,\sigma_2)=t$*. Dann gilt für* $0<t<0.49n$ *mit hoher Wahrscheinlichkeit* $Z_t=0$*.*

Lemma 12 sagt also aus, dass der Hammingabstand zweier erfüllender Besetzungen (asymptotisch) mindestens $n/2$ ist, d.h die erfüllenden Besetzungen liegen in der Menge aller Besetzungen sehr isoliert voneineinder. Wie dies im Falle des k-SAT's (festes k) aussieht, sprechen wir in Kapitel 4 an.
Bevor wir diese beiden Lemmata beweisen, wollen wir sehen, wie nun damit Theorem 8 folgt. Stellen wir uns die Formel $F_k(n,m)$ in zwei Schritten generiert vor. Als erstes generieren wir die Formel $F_k(n,m_1)$ und fügen dann die $m-m_1$ zufälligen Klauseln $J=\{C_1,\dots,C_{m-m_1}\}$ an $F_k(n,m_1)$ an. Nun können wir zunächst einmal die erfüllenden Besetzungen von $F_k(n,m_1)$

betrachten, die wir mit $\sigma_1 \ldots, \sigma_r$ bezeichnen wollen. Nach Lemma 11 gilt dann $X_{m_1} = r \sim e^{\gamma}$. Nachdem wir nun die zufälligen Klauseln J angehängt haben, ist dann die Anzahl der erfüllenden Besetzungen $Y = Y_n$ von $F_k(n, m)$ gegeben durch die Anzahl derjenigen Besetzungen aus unserer Menge $\{\sigma_1, \ldots, \sigma_r\}$, die auch alle Klauseln in J erfüllen.
Wir wollen zeigen, dass Y asymptotisch poissonverteilt ist mit Parameter e^{-c}. Dazu verwenden wir die sogenannte Momenten-Methode, die ein Werkzeug ist um Konvergenz in Verteilung zu zeigen. Die Aussage ist, dass eine Folge von Zufallsvariablen Y_n in Verteilung gegen eine Zufallsvariable X konvergiert, falls für alle $t \in \mathbb{N}$ das t-te Moment von Y_n gegen das t-te Moment von X konvergiert und dabei die Verteilung von X komplett und eindeutig durch die Folge ihrer Momente bestimmt ist. In unserem Fall ist X eine Poisson-verteilte Zufallsvariable. Dass dann die Momenten-Folge von X eindeutig der Poissonverteilung zugeordnet werden kann, lässt sich leicht durch Carleman's Bedingung verifizieren:
Sei $(m_t)_{t \in \mathbb{N}_o}$ die Momenten-Folge von X. Falls nun

$$\sum_{t=1}^{\infty} m_{2t}^{-\frac{1}{2t}} = \infty \tag{109}$$

gilt, ist die Verteilung von X die einzige mit Momenten-Folge m_t. Im Falle einer Poisson-Verteilung mit Parameter $\lambda > 0$ ist $m_t = \lambda^t$ und damit

$$\sum_{t=1}^{\infty} m_{2t}^{-\frac{1}{2t}} = \sum_{t=1}^{\infty} \left(\lambda^{2t}\right)^{-\frac{1}{2t}} = \sum_{t=1}^{\infty} \frac{1}{\lambda} = \infty. \tag{110}$$

Eine Variante dieser Methode ist statt der Konvergenz der t-ten Momente, die Konvergenz der t-ten faktoriellen Momente zu zeigen. Dabei ist das t-te faktorielle Moment der Erwartungswert von $Y_{(t)} := \prod_{j=0}^{t-1} (Y - j)$. Da für die Poissonverteilung mit Parameter λ das t-te faktorielle Moment gegeben ist durch λ^t, zeigen wir im folgenden, dass für jede feste natürliche Zahl t

$$\mathbb{E}\left[Y_{(t)}\right] \sim e^{-ct} \tag{111}$$

gilt. Sei also $t \in \mathbb{N}$. Dann gilt wegen der Unabhängigkeit der Klauseln $C_1, \ldots, C_{m-m_1}$

$$\begin{aligned} \mathbb{E}[Y_{(t)}] &= \mathbb{E}\left[\prod_{j=0}^{t-1}(Y - j)\right] \\ &= r_{(t)}\mathbb{P}(\sigma_1, \ldots, \sigma_t \text{ erfüllen } J) \\ &= r_{(t)} \left(\mathbb{P}(\sigma_1, \ldots, \sigma_t \text{ erfüllen } C_1)\right)^{m-m_1}, \end{aligned} \tag{112}$$

wobei man

$$\mathbb{P}(\sigma_1, \ldots, \sigma_t \text{ erfüllen } C_1) = 1 - \mathbb{P}\left(\exists 1 \leq i \leq t : \sigma_i \text{ erfüllt } C_1 \text{ nicht}\right) \tag{113}$$

schreiben kann. Nun gilt einerseits wegen Subadditivität

$$\begin{aligned} \mathbb{P}\left(\exists 1 \leq i \leq t : \sigma_i \text{ erfüllt } C_1 \text{ nicht}\right) &\leq t\mathbb{P}(\sigma_1 \text{ erfüllt } C_1 \text{ nicht}) \\ &= \frac{t}{2^k} \end{aligned} \tag{114}$$

und mit der Inklusion-/Exklusionsformel andererseits

$$\begin{aligned}\mathbb{P}\left(\exists 1 \leq i \leq t : \sigma_i \text{ erfüllt } C_1 \text{ nicht}\right) &= \sum_{k=1}^{t}(-1)^{k-1} \sum_{1\leq i_1<\cdots<i_k\leq t} \mathbb{P}(\sigma_{i_1},\ldots,\sigma_{i_t} \text{ erfüllen } C_1 \text{ nicht}) \\ &\geq t\mathbb{P}(\sigma_1 \text{ erfüllt } C_1 \text{ nicht}) \\ &\quad - \sum_{1\leq i<j\leq t} \mathbb{P}(\sigma_i,\sigma_j \text{ erfüllen } C_1 \text{ nicht}). \end{aligned} \tag{115}$$

Nun kann man für ein Paar von Besetzungen (σ_i, σ_j) mit Hammingabstand $h(\sigma_i, \sigma_j) = \tau$ die Wahrscheinlichkeit, dass dieses Paar die zufällige Klausel nicht erfüllt, folgendermaßen abschätzen:

$$\begin{aligned}\mathbb{P}(\sigma_i,\sigma_j \text{ erfüllen } C_1 \text{ nicht}) &= \mathbb{P}(\sigma_i,\sigma_j \text{ erfüllen } C_1 \text{ nicht}|\mathbf{E2})\mathbb{P}(\mathbf{E2}) \\ &\quad +\mathbb{P}(\sigma_i,\sigma_j \text{ erfüllen } C_1 \text{ nicht}|\neg\mathbf{E2})\mathbb{P}(\neg\mathbf{E2}) \\ &= \left(\frac{n-\tau}{2n}\right)^k + o(1) \\ &\leq \frac{1}{3^k}. \end{aligned} \tag{116}$$

Zusammensetzen der Ergebnisse liefert uns für das t-te faktorielle Moment von Y zum einen die untere Schranke

$$\begin{aligned}\mathbb{E}[Y_{(t)}] &= r_{(t)}\left(1-\mathbb{P}\left(\exists 1 \leq i \leq t : \sigma_i \text{ erfüllt } C_1 \text{ nicht}\right)\right)^{m-m_1} \\ &\geq r_{(t)}\left(1-\frac{t}{2^k}\right)^{m-m_1} \end{aligned} \tag{117}$$

und zum anderen die obere Schranke

$$\mathbb{E}[Y_{(t)}] \leq r_{(t)}\left(1-\frac{t}{2^k}+\frac{t^2}{3^k}\right)^{m-m_1}. \tag{118}$$

Da nun aufgrund unserer Voraussetzungen

$$t^2(m-m_1) = O(m-m_1) = O(\omega 2^k) = o(3^k)$$

gilt, erhalten wir asymptotisch für $n \to \infty$

$$\begin{aligned}\mathbb{E}[Y_{(t)}] &\sim r_{(t)}\left(1-\frac{t}{2^k}\right)^{m-m_1} \\ &\sim e^{t\gamma}\left(1-\frac{t}{2^k}\right)^{m-m_1} \\ &\sim e^{t\gamma}\left(\left(1-\frac{t}{2^k}\right)^{2^k}\right)^{c+\gamma} \\ &\sim e^{t\gamma}e^{-t(c+\gamma)} \\ &= e^{-c} \end{aligned}$$

und somit folgt dann die Behauptung (108).
Kommen wir nun zum Beweis der beiden Lemmata.

Beweis. Lemma 11:
Sei σ eine feste Besetzung und C eine zufällige Klausel der Länge k. Wir haben bereits gezeigt (vgl. (25)), dass dann

$$\mathbb{E}[X_{m_1}] = 2^n \left(1 - 2^{-k}\right)^{m_1}$$

gilt. Nun verwenden wir das entscheidende Ergebnis von Frieze und Wormald. Die Autoren in [18] haben nämlich gezeigt, dass für $n \to \infty$

$$\mathbb{E}[X_{m_1}^2] \sim \mathbb{E}[X_{m_1}]^2$$

gilt. Mit Chebysheff's Ungleichung folgt damit asymptotisch in n

$$X_{m_1} \sim \mathbb{E}[X_{m_1}].$$

Der Rest der Behauptung in Lemma 11 folgt schließlich wegen

$$\begin{aligned}
\mathbb{E}[X_{m_1}] &= 2^n \left(1 - 2^{-k}\right)^{m_1} \\
&= 2^n \left(1 - 2^{-k}\right)^{m_0 - 2^k \gamma} \\
&\sim 2^n \left(1 - 2^{-k}\right)^{-2^k(\gamma - n \ln 2)} \\
&\sim 2^n e^{\gamma - n \ln 2} \\
&= e^{\gamma}.
\end{aligned}$$

□

Beweis. Lemma 12:
Seien σ_1 und σ_2 zwei Besetzungen mit Hammingabstand $h(\sigma_1, \sigma_1) = t$. Dann ist eine zufällige Klausel C der Länge k durch mindestens einer dieser beiden Besetzungen mit folgender Wahrscheinlichkeit nicht erfüllt:

$$\begin{aligned}
\mathbb{P}(\sigma_1 \text{ oder } \sigma_2 \text{ erfüllt } C \text{ nicht}) &= \mathbb{P}(\sigma_1 \text{ erfüllt } C \text{ nicht}) + \mathbb{P}(\sigma_2 \text{ erfüllt } C \text{ nicht}) \\
&\quad - \mathbb{P}(\sigma_1, \sigma_2 \text{ erfüllen } C \text{ nicht}) \\
&= 2^{1-k} - \left(\frac{n-t}{2n}\right)^k \\
&= 2^{1-k} - 2^{-k} \left(1 - \frac{t}{n}\right)^k. \qquad (119)
\end{aligned}$$

Sei nun $F(t) := \mathbb{E}[Z_t]$ die erwartete Anzahl von Paaren σ_1, σ_2 mit Hammingabstand $h(\sigma_1, \sigma_2) = t$, die die zufällige Formel $F_k(n, m_1)$ erfüllen. Wegen (119) folgt mit
$A := \{\sigma_1, \sigma_2 : h(\sigma_1, \sigma_2) = t\}$

$$\begin{aligned}
F(t) &= \mathbb{E}[Z_t] \\
&= \mathbb{E}\left[\sum_A \mathbb{1}_{\{\sigma_1, \sigma_2 \text{ erfüllen } F_k(n, m_1)\}}\right] \\
&= \sum_A \mathbb{P}(\sigma_1, \sigma_2 \text{ erfüllen } C)^{m_1} \\
&= 2^n \binom{n}{t} \left(1 - 2^{1-k} + 2^{-k} \left(1 - \frac{t}{n}\right)^k\right)^{m_1}. \qquad (120)
\end{aligned}$$

Setzen wir nun $\rho := m_1/n = 2^k(\ln 2 - \gamma/n) + O(1/n)$, $\tau := t/n$ und betrachten die Funktion

$$\begin{aligned} f(\tau) &:= n^{-1}\ln(F(t)) \\ &= \ln 2 + \rho\ln(1 - 2^{1-k} + 2^{-k}(1-\tau)^k) + n^{-1}\ln\binom{n}{t}. \end{aligned} \tag{121}$$

Da nun mithilfe von Stirlings Approximationsformel $n^{-1}\ln(\binom{n}{t}) \leq -\tau\ln\tau - (1-\tau)\ln(1-\tau) + O(\tau/n)$ gilt, erhalten wir für f die obere Schranke

$$\begin{aligned} f(\tau) &\leq \ln 2 + \rho\ln(1 - 2^{1-k} + 2^{-k}(1-\tau)^k) - \tau\ln\tau - (1-\tau)\ln(1-\tau) + O(\tau/n) \\ &\leq \ln 2 - \tau\ln\tau - (1-\tau)\ln(1-\tau) - 2^{-k}\rho(2 - (1-\tau)^k) + O(\tau/n) \\ &= \ln 2 - \tau\ln\tau - (1-\tau)\ln(1-\tau) - (\ln 2 - \gamma/n)(2 - (1-\tau)^k) \\ &\quad + O((\tau + 2^{-k})/n). \end{aligned} \tag{122}$$

Wir wollen zeigen, dass für n gegen unendlich $\sum_{1\leq t\leq 0.49n} F(t) = o(1)$ gilt. Dazu unterscheiden wir drei Fälle:
Fall 1: $n^{-1} \leq \tau \leq \ln^{-1.1} n$.
Zunächst beobachten wir folgende Eigenschaften:

- Mit dem Binomischen Lehrsatz folgt

$$(1-\tau)^k = 1 - k\tau + O(k^2\tau^2).$$

- Es gilt

$$-(1-\tau)\ln(1-\tau) \leq \tau.$$

- Aufgrund der Wahl von k gilt

$$k\ln 2 = \ln 2\omega + \log_2 n \ln 2 = \ln n + \omega\ln 2.$$

Mit diesen Ergebnissen und der oberen Schranke (122) folgt dann für hinreichend große n

$$\begin{aligned} f(\tau) &\leq \tau\left(1 - \ln\tau - k\ln 2(1 - O(k\tau)) + \frac{2\gamma}{n\tau}\right) \\ &= \tau\left(1 - \ln n - (\ln n + \omega\ln 2) + o(1)\right) \\ &= \tau(1 - \omega\ln 2 + o(1)) \\ &\leq -\frac{\tau\omega}{2}. \end{aligned} \tag{123}$$

Damit ist

$$\begin{aligned} \sum_{1\leq t\leq n\ln^{-1.1} n} F(t) &= \sum_{1\leq t\leq n\ln^{-1.1} n} \exp\left(nf(t/n)\right) \\ &\leq \sum_{1\leq t\leq n\ln^{-1.1} n} \exp(-t\omega/2) \\ &= o(1). \end{aligned} \tag{124}$$

Fall 2: $\ln^{-1.1} n < \tau \leq k^{-1}\ln\ln n$.
Wieder wollen wir die obere Schranke für $f(\tau)$ in (122) weiter geeignet abschätzen. Dazu

beobachten wir zunächst, dass für hinreichend große Werte für n folgende Abschätzungen gelten

$$\begin{aligned} -\tau\ln\tau-(1-\tau)\ln(1-\tau) &= -\tau\ln\tau-\ln(1-\tau)+\tau\ln(1-\tau)\\ &\le \tau(1-\ln\tau)\\ &\le k^{-1}\ln\ln n(1+\ln\ln n)\\ &\le k^{-1}\ln\ln n(1+\ln k)\\ &\le \ln^{-0.5} n. \end{aligned} \tag{125}$$

Desweiteren können wir für hinreichend große Werte für n folgende obere Schranke für $(1-\tau)^k$ finden:

$$\begin{aligned} (1-\tau)^k &\le \exp(-k\tau)\\ &\le \exp(-k\ln^{-1.1} n)\\ &\le 1-\ln^{-0.1} n. \end{aligned} \tag{126}$$

Mit diesen beiden Ergebnissen folgt dann mit (122)

$$\begin{aligned} f(\tau) &\le \ln 2+\ln^{-0.5} n-\ln 2(2-(1-\ln^{-0.1} n))\\ &= (\ln^{-0.4}-\ln 2)\ln^{-0.1} n. \end{aligned} \tag{127}$$

Da nun für sehr große n der Faktor $\ln^{-0.4}-\ln 2$ kleiner ist als -0.5 folgt also

$$f(\tau)\le -0.5\ln^{-0.1} n. \tag{128}$$

Deshalb gilt auch in diesem Fall

$$\begin{aligned} \sum_{n\ln^{-1.1} n<t\le nk^{-1}\ln\ln n} F(t) &= \sum_{n\ln^{-1.1} n<t\le nk^{-1}\ln\ln n} \exp\left(nf(t/n)\right)\\ &\le \sum_{n\ln^{-1.1} n<t\le nk^{-1}\ln\ln n} \exp(-0.5n\ln^{-0.1} n)\\ &= o(1). \end{aligned} \tag{129}$$

Kommen wir dann zum letzten Fall.
Fall 3: $k^{-1}\ln\ln n<\tau\le 0.49$.
Wir sehen, dass in diesem Fall $(1-\tau)^k\le(1-\ln\ln n/k)^k=o(1)$ gilt und daher $(\ln 2-\gamma/n)(2-(1-\tau)^k)\sim 2\ln 2$ folgt. Da nun die Funktion $H(a)=-a\ln a-(1-a)\ln(1-a)$ im Intervall $[0,1/2]$ monoton wachsend ist, erhalten wir

$$\begin{aligned} \ln 2-\tau\ln\tau-(1-\tau)\ln(1-\tau) &\le \ln 2-0.49\ln(0.49)-0.51\ln(0.51)\\ &\le 1.3861\le 1.9998\ln 2. \end{aligned} \tag{130}$$

Damit folgt also

$$\begin{aligned} f(\tau) &\le 1.9998\ln 2-2\ln 2\\ &\le -0.0001 \end{aligned} \tag{131}$$

und schließlich

$$\begin{aligned}\sum_{nk^{-1}\ln\ln n<t\leq 0.49n} F(t) &\leq \sum_{nk^{-1}\ln\ln n<t\leq 0.49n} \exp(-0.0001n)\\ &= o(1). \end{aligned} \tag{132}$$

□

Dies vervollständigt den Beweis von Theorem 8. □

3 Der kritische Exponent des zufälligen k-SAT

In Kapitel 2 haben wir gesehen, dass bei wachsender Variablenanzahl n der zufällige k-SAT einen scharfen Phasenübergang von erfüllbar zu nicht-erfüllbar durchmacht. Die Schärfe eines solchen Phasenübergangs wird durch den sogenannten kritischen Exponenten $\nu = \nu_k$ charakterisiert. Es gilt: je kleiner ν desto schärfer der Übergang.
Im folgenden stellen wir einige Ergebnisse aus [9] und [26] vor. Sei $F_k(n,m)$ eine zufällige Formel und sei wieder $m = rn$. Für $0 < \delta < 1$ wollen wir nun wissen, um welchen Betrag man r erhöhen muss, damit die Wahrscheinlichkeit, dass die entsprechende zufällige Formel $F_k(n, rn)$ erfüllbar ist, von $1-\delta$ auf δ fällt. Betrachten wir folgende zwei Größen

$$r_-(n,\delta) := \sup\{r \geq 2 : \mathbb{P}(F_k(n,rn) \text{ erfüllbar}) > 1-\delta\} \tag{133}$$

und

$$r_+(n,\delta) := \sup\{r \geq 2 : \mathbb{P}(F_k(n,rn) \text{ erfüllbar}) < \delta\}. \tag{134}$$

Dann bezeichnet man mit dem Skalierungsfenster des Phasenübergangs das Intervall

$$W_k(n,\delta) := (r_-(n,\delta), r_+(n,\delta)). \tag{135}$$

Für eine zufällige Formel $F_k(n,rn)$ mit $r \in W_k(n,\delta)$ liegt also die Wahrscheinlickeit, dass diese erfüllbar ist, gerade zwischen δ und $1-\delta$ (insbesondere verschieden von 0). Uns interessiert nun die Länge dieses Intervalls, wo der eigentliche Phasenübergang stattfindet. Bezeichne Δ die Länge von $W_k(n,\delta)$. Von dieser wird ausgegangen, dass sie von der Ordnung

$$\Delta = \Theta\left(n^{-1/\nu}\right) \tag{136}$$

ist, wobei die Konstante in $\Theta()$ von δ abhängt, der kritische Exponent ν aber nicht. Durch Experimente ging man davon aus, dass $\nu_3 = 1.5 \pm 0.1$, $\nu_4 = 1.1 \pm 0.05$ und $\nu_5 = 1.05 \pm 0.05$ gilt und durch heuristische Argumentationen sogar, dass für k gegen ∞ der kritische Exponent gegen 1 konvergiert. Diese Behauptungen wurden dann von Wilson widerlegt. Dieser zeigt in [26], dass für alle $k \geq 2$ der kritische Exponent (falls er wohldefiniert ist) mindestens 2 ist:

Theorem 9. *(Korollar 4 in [26])*
Seien p_1 und p_2 reelle Zahlen mit $1 > p_1 > p_2 > 0$. Angenommen, eine zufällige k-SAT Formel über n Variablen und $r_1 n$ Klauseln ist mit Wahrscheinlichkeit $\geq p_1$ erfüllbar und eine zufällige k-SAT Formel über n Variablen und $r_2 n$ Klauseln ist mit Wahrscheinlichkeit $\leq p_2$ erfüllbar. Dann gilt

$$r_2 - r_1 \geq (p_1 - p_2) \cdot \Theta\left(\sqrt{n}\right). \tag{137}$$

Wie bei der Untersuchung des kritischen Wertes r_k, ist auch hier im Falle $k = 2$ mehr bekannt als für $k \geq 3$. In [9] zeigen Bollabas et al., dass $\nu_2 = 3$ ist, wohingegen wir für $k \geq 3$ aus vorherigem Theorem von Wilson nur wissen, dass $\nu_k \geq 2$ gilt.
In [9] wird viel mehr bewiesen. Wir betrachten 2-SAT-Formeln mit $m = (1 + \varepsilon)n$ Klauseln und machen zunächst einmal ε abhängig von n. Es stellt sich heraus, dass $\varepsilon = \lambda_n n^{-1/3}$ die angemessene Skalierung dafür ist. Nun unterscheidet man drei Fälle. Einmal den Fall, dass λ_n beschränkt ist und des weiteren die Fälle, dass λ_n gegen ∞ bzw. $-\infty$ konvergiert. Bollabas et al. zeigen folgendes Theorem.

Theorem 10. *(Theorem 1.1 in [9])*
Es existieren Konstanten ε_0 und λ_0 mit $0 < \varepsilon_0 < 1$ und $0 < \lambda_0 < \infty$, so dass

$$\mathbb{P}\left(F_2(n,m) \text{ erfüllbar }\right) = \begin{cases} 1 - \Theta\left(\frac{1}{|\lambda_n|^3}\right), & \text{falls } -\varepsilon_0 n^{1/3} \leq \lambda_n \leq -\lambda_0, \\ \Theta(1), & \text{falls } -\lambda_0 \leq \lambda_n \leq \lambda_0, \\ \exp\left(-\Theta((\lambda_n^3)\right), & \text{falls } \lambda_0 \leq \lambda_n \leq \varepsilon_0 n^{1/3}. \end{cases}$$

Dieses Theorem liefert die exakte Form des Skalierungsfensters für das zufällige 2-SAT.

Folgerung 2. *Für alle ausreichend kleine $\delta > 0$ ist das Skalierungsfenster für den zufälligen 2-SAT von der Form*

$$W_2(n,\delta) = \left(1 - \Theta\left(n^{-1/3}\right), 1 + \Theta\left(n^{-1/3}\right)\right). \tag{138}$$

Bemerkung 4. *Theorem 10 gibt uns auch Auskunft darüber, mit welcher Rate die Wahrscheinlichkeit, dass eine zufällige 2-SAT-Formel mit $rn = (1 + \varepsilon)n$ Klauseln für $(1 + \varepsilon)$ nahe an der oberen Grenze von $W_2(n, \delta)$ aus Folgerung 2 erfüllbar ist, gegen 0 geht. Es gilt für positives ε*

$$\mathbb{P}\left(F_2(n,(1+\varepsilon)n) \text{ erfüllbar}\right) = \exp\left(-\Theta(\varepsilon^3 n)\right). \tag{139}$$

4 Die Menge der erfüllenden Besetzungen einer zufälligen k-SAT-Formel

In diesem Kapitel wollen wir uns die zufällige Menge $S(F_k(n, rn))$ der erfüllenden Besetzungen einer zufälligen Formel $F_k(n, rn)$ etwas näher betrachten. Wir werden sehen, dass die Mächtigkeit dieser Menge, eine Zufallsvariable in $\mathbb{N}_0$, um einen gewissen Wert konzentriert ist. Desweiteren konnte man sehr interessante Eigenschaften der Struktur von $S(F_k(n, rn))$ herausfinden, von denen wir hier einige vorstellen werden.

4.1 Konzentration der Anzahl erfüllender Besetzungen

Betrachtet man eine zufällige k-SAT-Formel F, dann ist die Anzahl der Besetzungen, die F erfüllen, die wir $Z(F)$ bezeichnen, eine Zufallsvariable mit Werten in $\{0, \ldots, 2^n\}$. Abbe und Montanari haben kürzlich in ihrer Arbeit [1] gezeigt, dass unter bestimmten Vorrausetzungen die Größe $(1/n)\log_2(Z(F))$ Konzentration um einen gewissen Wert aufweisst. Die entscheidenden Behauptungen wurden dabei mit einer Interpolationsmethode bewiesen, welche in der statistischen Physik ihre Entstehung hat. Schon lange davor hat Sharell [25] für das zufällige 2-SAT-Problem ähnliche Konzentrationseigenschaften bewiesen. Sharell benutzt dabei die

Azuma-Hoeffding-Ungleichung, ein wichtiges Mittel um Konzentrationsungleichungen herzuleiten. Wir wollen die genauen Ergebnisse dieser Arbeiten nun vorstellen und beginnen mit dem allgemeinen Fall.
Für den allgemeinen Fall in [1] werden wir im folgenden zufällige Formeln $F_k(n,r)$ betrachten, die nach dem $F_{n,p}$-Modell, welches wir in unserer Einleitung vorgestellt haben, generiert wurden. Und wie bereits erwähnt bezeichnen wir mit $Z(F_k(n,r))$ die zufällige Anzahl erfüllender Besetzungen für $F_k(n,r)$ und mit

$$P_{k,n}(r,\phi) := \mathbb{P}(Z(F_k(n,rn) < 2^{n\phi}) \tag{140}$$

die Wahrscheinlichkeit, dass $F_k(n,rn)$ weniger als $2^{n\phi}$ erfüllende Besetzungen hat. Wie man sieht, ist $P_{n,k}(r,0)$ gerade die Wahrscheinlichkeit, dass $F_k(n,r)$ nicht erfüllbar ist und im folgenden wird die Zahl

$$r^* := \sup\Big\{r \ : \ P_{n,k}(r,0) = O((1/(\log n)^{1+\delta}),\ \text{für ein } \delta > 0\Big\} \tag{141}$$

eine Rolle spielen.

Bemerkung 5. *Für $k \geq 2$ ist $r^* \geq 1$. Für $k = 2$ und $r < r_2 = 1$ wissen wir nämlich schon aus vorherigem Kapitel, dass*

$$P_{n,2}(r,0) = \mathbb{P}(Z_2(F_2(n,rn)) = 0) = O(1/n)$$

gilt. Da wir nun für $k \geq 3$ die Wahrscheinlichkeit $P_{n,k}(r,0)$ durch

$$P_{n,k}(r,0) = \mathbb{P}(Z_k(F_k(n,rn)) = 0) \leq \mathbb{P}(Z_2(F_2(n,rn)) = 0)$$

abschätzen können, erhalten wir $r^* \geq 1$.

Kommen nun zum Hauptresultat von Abbe und Montanari zur Konzentration von $Z(F)$.

Theorem 11. *(Theorem 1 in [1]):*
Es existiert eine abzählbare Menge $C \subset \mathbb{R}$ und eine Funktion $\phi_s : [0,r^*) \to [0,1]$, sodass für jedes $r \in [0,r^*)\backslash C$ und jedes $\varepsilon > 0$

$$\lim_{n\to\infty} P_{n,k}(r, \phi_s(r) - \varepsilon) = 0 \tag{142}$$

und

$$\lim_{n\to\infty} P_{n,k}(r, \phi_s(r) + \varepsilon) = 1 \tag{143}$$

gilt.

Dieses Theorem besagt also, dass die Zufallsvariable $(1/n)\log(Z(F(_k(n,r)))$ für $r < r^*$ mit hoher Wahrscheinlichkeit in dem Intervall $[\phi_s(r) - \varepsilon, \phi_s(r) + \varepsilon]$ liegt.

Bemerkung 6. *Wegen Bemerkung 5 haben wir also im Falle des zufälligen 2-SAT-Problems obige Konzentrationseigenschaft für jedes r, sodass $F_2(n,r)$ mit hoher Wahrscheinlichkeit erfüllbar ist, gegeben (bis auf abzählbar viele Ausnahmen). Für $k \geq 3$ lassen die bisherigen Ergenisse keine genauen Schlüsse über die UNSAT-Wahrscheinlichkeit zu, sodass wir nicht in der Lage sind zu entscheiden, ob r_k in $[0,r^*)$ liegt.*

Bemerkung 7. *Um diesen Phasenübergang in $\phi_s(r)$ (r hier fest!) zu erhalten, zeigen die Autoren zunächst, dass das Ereignis $\{Z(F_k(n,r)) > 2^{n\phi}\}$ (ϕ fest!) einen Phasenübergang in r durchmacht. Genauer gesagt zeigen sie, dass für jedes $\varepsilon > 0$ und jedes $\phi \in [0,1)$ eine Folge $(r_n(\phi))_{n\in\mathbb{N}}$ existiert, sodass*

$$\lim_{n\to\infty} P_{n,k}(r_n(\phi) - \varepsilon, \phi) = 0 \tag{144}$$

und

$$\lim_{n\to\infty} P_{n,k}(r_n(\phi) + \varepsilon, \phi) = 1 \tag{145}$$

gelten. Was wir sehen können ist, dass für $\phi = 0$ wir gerade Friedgut's Theorem (Theorem 1) erhalten.

Die in Theorem 11 auftretende Funktion ϕ_s ist folgendermaßen charakterisiert.

Theorem 12. *(Theorem 3 in [1]):*
Sei

$$\beta_n(r) := \frac{1}{n}\mathbb{E}\left[\log Z(F_k(n,r)) | Z(F_k(n,r)) \geq 1\right]. \tag{146}$$

Dann konvergiert für jedes $r < r^*$ $\beta_n(r)$ für n gegen unendlich gegen einen Grenzwert $\phi_s(r)$.

4.1.1 Eine Konzentrationsungleichung für das zufällige 2-SAT-Problem

In [16] wird geschildert, was Sharell in seinem Manuskript [25] über die Konzentration der Anzahl erfüllender Besetzungen einer zufälligen uniformen Formel $F_2(n, rn)$ schreibt. Im folgenden verlangen wir, dass die Klauseldichte $\frac{m}{n} = r$ stets echt kleiner als dem Threshold $r_2 = 1$ und fest ist. Die Menge erfüllender Besetzungen für die zufällige Formel $F_2(n, rn)$ bezeichnen wir mit $S(F_2(n, rn))$ und ihre Mächtigkeit wieder mit $Z(F_2(n, rn))$. Dann gilt folgende Konzentrationsungleichung.

Theorem 13. *(Sharell)*
Sei $0 < r < 1$ fest und $X_n = \log_2(Z(F_2(n, rn)))$. Dann gilt

$$\mathbb{P}\left(|X_n - \mathbb{E}[X_n]| \leq n^{\frac{1}{2}} \log^2 n\right) = 1 - o(1). \tag{147}$$

Bemerkung 8. *X_n ist also in einem Bereich der Größenordnung $n^{\frac{1}{2}} \log^2 n$ um ihren Erwartungswert konzentriert. Es ist jedoch noch nicht bekannt, wie $\mathbb{E}[X_n]$ berechnet werden kann.*

Beweis. Theorem 2:
Wir werden uns hier nur die grundsätzliche Vorgehensweise anschauen und verweisen für die Beweise einiger verwendeter Ergbnisse auf [25]. Die grungsätzliche Idee von Sharell ist es, einen Formelprozess $(F_i)_{0\leq i\leq m}$ zu verwenden um die zufällige Formel $F_2(n, rn)$ zu generieren. Dabei ist F_0 die leere Formel und für jedes $0 \leq i \leq m-1$ entsteht F_{i+1} durch das Hinzufügen einer zufälligen Klausel C_i an F_i. Das Ziel wird sein, die Azuma-Hoeffding Ungleichung aus [8] in folgender Version zu benutzen um die behauptete Konzentration zu zeigen.

Theorem 14. *(Azuma-Hoeffding Ungleichung)*
Sei X eine integriebare Zufallsvariable, für die Zufallsvariablen $T_1, \ldots, T_n$ existieren, sodass

$$\sigma(X) \subset \sigma(T_1, \ldots, T_n).$$

Falls für jedes $i \in \{1, \ldots, n\}$ Konstanten b_i existieren mit

$$|\mathbb{E}[X|T_1, \ldots, T_{i+1}] - \mathbb{E}[X|T_1, \ldots, T_i]| \leq b_i,$$

dann gilt

$$\mathbb{P}(|X - \mathbb{E}[X]| > t) \leq 2\exp\left(-\frac{t^2}{2\sum_{i=1}^n b_i^2}\right). \tag{148}$$

Sei $F_2(n, rn) = \bigwedge_{i=1}^m C_i$ für zufällige Klauseln C_i. Dann wollen wir Theorem 14 für $X = X_n = \log_2(\#Z(F_2(n, rn)))$ mit $T_i = C_i$ für $i = 1, \ldots, n$ zu verwenden. Was wir zeigen müssen ist, dass

$$Y_k := \mathbb{E}[X|C_1, \ldots, C_{k+1}] - \mathbb{E}[X|C_1, \ldots, C_k]$$

betragsmäßig für jedes $1 \leq k \leq m-1$ durch eine Konstante b_k beschränkt ist. Die entscheidende Information gibt uns folgendes Lemma von Sharell, wodurch man die Größenordnung der Schranken ableiten kann. Bevor wir zum Lemma kommen, brauchen wir noch einige Definitionen, die Sharell verwendet.

Definition 7.

- *Der Grad $d(c_1, \ldots, c_k)$ einer Menge von Klauseln $\{c_1, \ldots, c_k\}$ ist die maximale Anzahl von Erscheinungen eines Literals in dieser Menge.*
- *Eine Variable heißt „forced" in einer erfüllbaren Formel, falls der Wert der Variable unter allen erfüllenden Besetzungen der Formel gleich ist. Für Klauseln $c_1, \ldots, c_k$ bezeichne $\#forced(c_1, \ldots, c_k)$ die Anzahl der forced variablen in $\{c_1, \ldots, c_k\}$.*

Lemma 13. *(Sharell)*
Sei $X = \log_2(Z(F_2(n, rn)))$, wobei $F_2(n, rn) = \bigwedge_{1 \leq i \leq m} C_i$ die zufällige 2-SAT Formel bezeichnet, die durch die Folge von zufälligen Klauseln $\mathcal{C} := \{C_1, \ldots, C_m\}$ entsteht. Sei weiter Y_k, $0 \leq k \leq m-1$, wie oben definiert. Dann gilt:

- $|Y_k| \leq d(C_1, \ldots, C_{m-1}) + \frac{1}{4n} \cdot \#forced(C_1, \ldots, C_{m-1})^2$.
- *Für jede natürliche Zahl l und $0 \leq k \leq m-1$ gilt*

$$\begin{aligned} |Y_k| \quad \leq \quad & \mathbb{E}[d(\mathcal{C})|C_1, \ldots, C_k] + \frac{2n(m-k)}{M} \cdot \binom{l+1}{2} + 2n \cdot \mathbb{P}(d(\mathcal{C}) > r|C_1, \ldots, C_k) \\ & + \frac{1}{4n} \cdot \#forced(C-1, \ldots, C_{k-1}). \end{aligned}$$

Beweis. Siehe Sharell [25]. □

Fernandez d. l. Vega zeigt in [16] dann weiter von welcher Größenordnung diese Schranken sind. Es stellt sich heraus, dass die $|Y_k|$ für jedes $0 \leq k \leq m-1$ mit Wahrscheinlichkeit $1-o(1)$ von der Größenordnung $O\left(\sqrt{n}\log n\right)$ sind.
Wählt man nun in Theorem 14 für alle $1 \leq i \leq n$ die $b_i = O\left(\sqrt{n}\log n\right)$, dann folgt für eine Konstante $L > 0$

$$\begin{aligned}
\mathbb{P}\left(|X_n - \mathbb{E}\left[X_n\right]| \leq t\right) &= 1 - \mathbb{P}\left(|X_n - \mathbb{E}\left[X_n\right]| > t\right) \\
&\geq 1 - 2\exp\left(-\frac{t^2}{2\sum_{i=1}^n b_i^2}\right) \\
&\geq 1 - 2\exp\left(-\frac{t^2}{2\sum_{i=1}^n \left(L\sqrt{n}\log n\right)^2}\right) \\
&= 1 - 2\exp\left(-\frac{t^2}{2L^2 \cdot n^2 \log^2 n}\right).
\end{aligned}$$

Mit der Wahl $t = \sqrt{n}\log^2 n$ folgt dann die Behauptung in Theorem 13. □

4.2 Die Struktur von $S(F)$ als Teilgraph des Hammingwürfels

In diesem Abschnitt wollen wir uns die Ergebnisse aus [2] und [6] anschauen, in der Achlioptas, Coja-Oghlan und Tersenghi die Struktur der Menge $S(F)$ aller erfüllenden Besetzungen einer k-SAT-Formel F mit $m = rn$ Klauseln, betrachtet als Teilgraph des Hammingwürfels, untersuchen. Motiviert waren die Überlegungen u.a. durch die Frage, warum ein signifikanter Unterschied existiert zwischen den größten theoretischen Wert r', für die eine erfüllende Besetzung existiert und dem größten bekannten Wert r'', für die ein Algorithmus in polynomieller Zeit eine erfüllende Besetzung finden kann. Die Autoren finden heraus, dass $S(F)$ als Teilgraph schon für Werte r weit unterhalb des Thresholds r_k in exponentiell viele Zusammenhangskomponenten zerfällt. Die genauen Ergebnisse dazu werden wir nun vorstellen.
Im folgenden betrachten wir zufällige k-SAT-Formeln $F = F_k(n, rn)$ definiert über n Variablen $x_1, \ldots, x_n$ und bezeichnen wieder mit $S(F) \subseteq \{0,1\}^n$ die zufällige Menge der Besetzungen der Variablen $x_1, \ldots, x_n$, die F erfüllen. Zunächst führen wir noch ein paar Definitionen ein.

Definition 8.

- *Sei $X \subseteq \{0,1\}^n$ eine beliebige Menge. Dann ist ihr Durchmesser definiert als*

$$diam(X) := \min_{x,y \in X} d_H(x,y),$$

  wobei d_H den Hammingabstand bezeichnet.
  Seien $X, Y \subseteq \{0,1\}^n$ zwei beliebige Mengen. Dann ist der Abstand zwischen X und Y definiert als

$$d(X,Y) := \min_{x \in X, y \in Y} d_H(x,y).$$

- *Zwei Elemente $x, y \in \{0,1\}^n$ heißen adjacent oder benachbart, falls $d_H(x,y) = 1$. Dann bezeichnen wir mit Clustern der Formel F die Zusammenhangskomponenten von $S(F)$ und mit einer Cluster-Region eine nichtleere Menge von Clustern.*

Eines der Resultate von Achlioptas, Coja-Oghlan und Tersenghi ist nun das folgende Theorem.

Theorem 15. *(Theorem 2 in [2])*
Für jedes $k \geq 8$ existieren ein Wert $r < r_k$ und Konstanten $\alpha_k < \beta_k < 1/2$ und $\varepsilon_k < 0$, so dass die Menge der erfüllenden Besetzungen $S(F)$ von $F = F_k(n, rn)$ mit hoher Wahrscheinlichkeit aus $2^{\varepsilon_k n}$ Cluster-Regionen besteht, die folgende Eigenschaften erfüllen:

1. *Jede dieser Cluster-Regionen hat einen Durchmesser von höchstens $\alpha_k n$.*
2. *Der Abstand zwischen je zwei dieser Cluster-Regionen ist mindestens $\beta_k n$.*

Das Theorem besagt also, dass für $k \geq 8$ und einen Wert unterhalb des Thresholds r_k die zufällige Lösungsmenge $S(F_k(n, rn))$ für ausreichend große n in exponentiell viele Zusammenhangskomponenten zerfällt, wobei jede dieser Komponenten kleinen Durchmesser hat und gut von anderen Komponenten separiert ist. Dies wird noch deutlicher für große Werte für k. Für ausreichend große k und r nahe am Threshold r_k werden die Cluster-Regionen beliebig klein und maximal voneinander entfernt. Dies wird durch folgendes Theorem nun beschrieben.

Theorem 16. *(Theorem 3 in [2])*
Für jedes $0 < \delta < 1/3$, falls $r = (1-\delta)2^k \ln 2$, gilt für alle $k \geq k_0(\delta)$ Theorem XY mit

$$\alpha_k = \frac{1}{k}, \quad \beta_k = \frac{1}{2} - \frac{5}{6}\sqrt{\delta}, \quad \varepsilon_k = \frac{\delta}{2} - 3k^{-2}.$$

Nun kann man sich fragen, was genau innerhalb der einzelnen Cluster passiert. Dieser Frage gehen Achlioptas und Tersenghi in [6] u.a. auch nach. Bevor wir ihr Ergebnis dazu vorstellen können, müssen wir noch ein paar Definitionen einführen.

Definition 9. *Die Projektion einer Variable x_i in einer Menge $C \subseteq S(F)$ ist die Menge der Werte, die durch die Besetzungen in C für x_i vorgesehen sind. Diese Menge sei mit $\Pi_i(C)$ bezeichnet. Falls $\Pi_i(C) \neq \{0, 1\}$ gilt, dann sagen wir, dass x_i fest in C ist.*

Theorem 17. *(Theorem 4 in [6])*
Für jedes $\alpha > 0$ und alle $k \geq k_0(\alpha)$ existiert $c_k^\alpha < r_k$, so dass für alle $r \geq c_k^\alpha$ mit hoher Wahrscheinlichkeit jeder Cluster von $F_k(n, rn)$ mindestens $(1-\alpha)n$ feste Variablen hat. Es gilt

$$\lim_{k\to\infty} \frac{c_k^\alpha}{2^k \ln 2} = \frac{1}{1 + \alpha(1-\alpha)}. \tag{149}$$

Für zum Beispiel $\alpha = 1/2$ folgt aus diesem Theorem, dass für hinreichend großes k jeder Cluster schon eine Mehrheit an festen Variablen hat, falls $r = (4/5 + \delta_k)2^k \ln 2$ gilt, mit $\delta_k \to 0$ für $k \to \infty$

5 Ein randomisierter Algorithmus für k-SAT

Für das k-SAT-Problem, insbesondere 3-SAT und 4-SAT, wurden in letzter Zeit sehr viele Algorithmen untersucht. Viele von ihnen hatten den Zweck für $k = 3, 4, ...$ Schranken für den Threshold r_k aus Kapitel 1 zufinden oder bekannte Schranken zu verbessern. In diesem Kapitel wollen wir uns mit einem einfachen randomisierten Algorithmus von Schöning [24] beschäftigen und zeigen, dass die Laufzeit des Algorithmus, um eine erfüllende Besetzung

für die Formel zu finden, von der Größenordnung $(2(1-1/k))^n$ ist, was eine Verbesserung gegenüber der naiven Vorgehensweise ist, bei der man alle 2^n Besetzungen ausprobiert. Der Algorithmus sieht folgendermaßen aus:

EINGABE: Eine k-SAT Formel über n Variablen:
Wähle eine Startbesetzung $a \in \{0,1\}^n$ zufällig und uniform aus den 2^n möglichen.
Wiederhole $3n$ mal:
FALLS: a erfüllt die Formel:
Stop und akzeptiere a als erfüllende Besetzung.
ANDERNFALLS: Sei C eine Klausel, die durch a nicht erfüllt wird:
Wähle eines der k Literale in C zufällig und uniform
und ändere den Wert der entsprechenden Variable in a.

Sei nun F eine k-SAT-Formel über n Variablen und a^* eine feste erfüllende Besetzung. Nun kann man sich fragen, mit welcher Wahrscheinlickeit dieser randomisierte Algorithmus a^* (oder eine andere erfüllende Besetzung) findet. Diese Wahrscheinlichkeit wollen wir mit p bezeichnen. Wenn der Algorithmus nach $3n$ Schritten abbricht ohne eine erfüllende Besetzung gefunden zu haben, wird der Algorithmus wiederholt. Da wir dies unabhängig machen, ist die Anzahl von unabhängigen Wiederholungen T des Algorithmus bis eine erfüllende Besetzung befunden wird eine $Geom(p)$-verteilte Zufallsvariable mit Erwartungswert $1/p$. Die Wahrscheinlichkeit, dass nach t unabhängigen Wiederholungen der Algorithmus keine erfüllende Besetzung findet (dieses Ereignis sei mit A bezeichnet), ist nach oben abgeschätzt durch

$$\begin{aligned} \mathbb{P}(A) &= (1-p)^t \\ &\leq e^{-pt}. \end{aligned} \tag{150}$$

$\mathbb{P}(A)$ wird als Error-Wahrscheinlichkeit bezeichnet. Will man, dass der Algorithmus eine Error-Wahrscheinlichkeit von e^{-20} erreicht, so muss man nach (150) $t = 20/p$ wählen. Die Anzahl der Wiederholungen t wird auch als Komplexität des Algorithmus bezeichnet. Auf jeden Fall weiss man, dass die Komplexität des Algorithmus ein polynomielles Vielfaches von der erwarteten Anzahl an Wiederholungen $1/p$ ist. Wir wollen nun dieses p genauer charakterisieren, wodurch wir dann in der Lage sind die Komplexität zu bestimmen.
Sei nun $a^* \in \{0,1\}^n$, wie oben definiert, eine feste erfüllende Besetzung und $a \in \{0,1\}^n$ eine zufällige, uniforme Besetzung. Dann bezeichnen wir mit

$$X := \sum_{i=1}^{n} \mathbb{1}_{\{a_i \neq a_i^*\}} \tag{151}$$

den Hamming-Abstand von a und a^*. X ist als Summe von n unabhängigen $Bern(1/2)$-verteilten Zufallsvariablen $Bin(n,1/2)$-verteilt und wir halten fest, dass dann für $j = 0, \ldots, n$

$$\mathbb{P}(X = j) = \binom{n}{j} 2^{-n} \tag{152}$$

gilt. Haben a und a^* den Hamming-Abstand j, dann ist dies die Anzahl der Variablen, die geflippt werden müssen, damit $a = a^*$ gilt (vorrausgesetzt man wählt die richtigen Literale zum Flippen). Nun kann man folgende Markovkette betrachten, welche eine einfache Irrfahrt ist.

Es gibt einen Startwert X_0 und die Zustände $0, 1, \ldots, n$, die die Hamming-Abstände zwischen a und a^* während der Durchführung des obigen Algorithmus darstellen sollen. Der Startwert X_0 ist uniformverteilt auf der Menge $\{0, \ldots, n\}$, da die Startbesetzung a uniform auf $\{0,1\}^n$ verteilt ist. Die Übergangswahrscheinlichkeit von X_0 nach $j \in \{0, \ldots, n\}$ ist nach (152) gegeben durch $\binom{n}{j}2^{-n}$. Der Zustand 0 bedeutet, dass der Algorithmus die erfüllende Besetzung a^* gefunden hat und damit ist dieser ein absorbierender Zustand. Man beachte hier, dass der Algorithmus eine erfüllende Besetzung $a' \neq a^*$ finden kann bevor die Kette den Zustand 0 erreicht, aber dies würde die Akzeptanzwahrscheinlichkeit nur größer machen.
Sei C nun eine Klausel, die durch a nicht erfüllt wird, d.h. in C gibt es mindestens ein Literal, bei dem das Flippen des entsprechenden Wertes in a dazu führt, dass der Hamming-Abstand zu a^* um eins kleiner wird. Dies liegt daran, dass unter den k Literalen in C durch a^* mindestens eines davon den Wert 1 bekommt, wohingegen unter a alle den Wert 0 haben. Da im Algorithmus das Literal, welches geflippt werden soll, zufällig und uniform gewählt wird, bedeutet dies, dass die Übergangswahrscheinlichkeit von j nach $j-1$ mindestens $1/k$ ist. Entsprechend ist dann die Übergangswahrscheinlichkeit von j nach $j+1$ höchstens $1 - 1/k = (k-1)/k$.
Angenommen, der Prozess befindet sich im Zusatnd j, dann bezeichnen wir mit q_j die Wahrscheinlichkeit den absorbierenden Zustand 0 zu erreichen. Klar ist, dass dazu mindestens j Schritte nötig sind. Betrachtet man den Fall, dass der Prozess i Schritte in die 'falsche' Richtung macht (die Irrfahr macht i Schritte nach oben), dann braucht man insgesamt also $j+2i$ Schritte um die 0 zu erreichen. Um q_j zu berechnen, müssen wir die Anzahl c der Pfade bestimmen, die von j nach 0 gehen mit genau i Aufwärtsbewegungen. Mit einem Spiegelungstrick kann man zeigen, dass es

$$\binom{2s}{s+t} - \binom{2s}{s+t+1}$$

nichtnegative Pfade gibt, die von $2t$ in genau $2s$ Schritten 0 erreichen. Da in unserem Fall die 0 nach $j+2i$ Schritten zum ersten Mal erreicht werden soll, wählen wir also $2s = j+2i-1$ und $2t = j-1$ und erhalten

$$\begin{aligned} c &= \binom{j+2i-1}{j+i-1} - \binom{j+2i-1}{j+i} \\ &= \binom{j+2i}{i} \cdot \frac{j}{j+2i}. \end{aligned} \tag{153}$$

Damit folgt mit obigen Vorüberlegungen

$$\begin{aligned} q_j &\geq \sum_{i=0}^{j} \binom{j+2i}{i} \cdot \frac{j}{j+2i} \cdot \left(\frac{k-1}{k}\right)^i \cdot \left(\frac{1}{k}\right)^{i+j} \\ &\geq \frac{1}{3} \sum_{i=0}^{j} \binom{j+2i}{i} \cdot \left(\frac{k-1}{k}\right)^i \cdot \left(\frac{1}{k}\right)^{i+j}. \end{aligned} \tag{154}$$

Wir verwenden nun die Tatsache, dass für $n \in \mathbb{N}$ und $\alpha \in (0,1)$

$$\begin{aligned} \binom{n}{\alpha n} &\sim 2^{E(\alpha)n} \\ &= \left(\frac{1}{\alpha}\right)^{\alpha n} \left(\frac{1}{1-\alpha}\right)^{(1-\alpha)n} \end{aligned} \tag{155}$$

gilt, wobei $E(\alpha) = -\alpha \log_2 \alpha - (1-\alpha)\log_2(1-\alpha)$ die binäre Entropiefunktion ist. Nun kann man die Summe in (154) nach unten abschätzen durch den Summanden für $i = \alpha j$ und dann (155) verwenden, wodurch man folgende Abschätzung bekommt

$$\begin{aligned} q_j &\geq \binom{(1+2\alpha)j}{\alpha j} \cdot \left(\frac{k-1}{k}\right)^{\alpha j} \cdot \left(\frac{1}{k}\right)^{(1+\alpha)j} \\ &\geq \left[\left(\frac{1+2\alpha}{\alpha}\right)^{\alpha} \cdot \left(\frac{1+2\alpha}{1+\alpha}\right)^{1+\alpha} \cdot \left(\frac{k-1}{k}\right)^{\alpha} \cdot \left(\frac{1}{k}\right)^{1+\alpha}\right]^j, \end{aligned} \tag{156}$$

wobei die letzte Abschätzung bis auf einen polynomiellen Faktor gültig ist. Mit der Wahl $\alpha = 1/(k-2)$ erhalten wir

$$q_j \geq \left(\frac{1}{k-1}\right)^j. \tag{157}$$

Nun können wir die Wahrscheinlichkeit $p = \mathbb{P}(A)$ abschätzen durch

$$\begin{aligned} p &\geq \mathbb{P}(\text{Algorithmus findet } a^*) \\ &= \sum_{j=0}^{n} \binom{n}{j} \left(\frac{1}{2}\right)^n q_j \\ &\geq \left(\frac{1}{2}\right)^n \sum_{j=0}^{n} \binom{n}{j} \left(\frac{1}{k-1}\right)^j \\ &= \left(\frac{1}{2}\left(1 + \frac{1}{k-1}\right)\right)^n. \end{aligned} \tag{158}$$

Damit folgt für die Laufzeit/Komplexität des Algorithmus

$$\begin{aligned} \mathbb{E}[T] &= \tfrac{1}{p} \\ &\leq \left(2\left(1 - \frac{1}{k}\right)\right)^n. \end{aligned} \tag{159}$$

Für jede erfüllbare k-SAT-Formel über n Variablen muss dieser Algorithmus im Mittel 'nur' t mal wiederholt werden, um eine erfüllende Besetzung zu finden, wobei t ein polynomielles Vielfaches von $\left(2\left(1-\frac{1}{k}\right)\right)^n < 2^n$ ist.

6 Literaturverzeichnis

[1] Abbe, Emmanuel; Montanari, Andrea
On the concentration of the number of solutions of random satisfiability formulas.
arXiv:1006.3786v1 [cs.DM] (2010).

[2] Achlioptas, Dimitris; Coja-Oghlan, Amin; Ricci-Tersenghi, Federico
On the solution-space geometry of random constraint satisfaction problems.
Random Struct. Algorithms 38, No. 3, 251–268 (2011).

[3] Achlioptas, D.; Kirousis, L.M.; Kranakis, E.; Krizanc, D.
Rigorous results for random $(2 + p)$-SAT.
Theor. Comput. Sci. 265, No.1–2, 109–129 (2001).

[4] Achlioptas, Dimitris; Moore, Cristopher
Random k-SAT: Two moments suffice to cross a sharp threshold.
SIAM J. Comput. 36, No. 3, 740–762 (2006).

[5] Achlioptas, Dimitris; Peres, Yuval
The threshold for random k-SAT is $2^k \log 2 - O(k)$.
J. Am. Math. Soc. 17, No. 4, 947–973 (2004).

[6] Achlioptas, Dimitris; Ricci-Tersenghi, Federico
Random formulas have frozen variables.
SIAM J. Comput. 39, No. 1, 260–280 (2009).

[7] Aspvall, Bengt; Plass, Michael F.; Tarjan, Robert Endre
A linear-time algorithm for testing the truth of certain quantified Boolean formulas.
Inf. Process. Lett. 8, 121–123 (1979).

[8] Azuma, K.
Weighted sums of certain dependent random variables.
Tohoku Math. J., II. Ser. 19, 357–367 (1967).

[9] Bollobás, Béla; Borgs, Christian; Chayes, Jennifer T.; Kim, Jeong Han; Wilson, David B.
The scaling window of the 2-SAT transition.
Random Struct. Algorithms 18, No.3, 201–256 (2001).

[10] Chvátal, V.; Reed, B.
Mick gets some (the odds are on his side).
33rd annual symposium on Foundations of computer science (FOCS), IEEE Computer Society Press, 620–627 (1992).

[11] Coja-Oghlan, Amin; Frieze, Alan
Random k-sat: the limiting probability for satisfiability for moderately growing k.
Electron. J. Comb. 15, No. 1, Research Paper N2, 6 p. (2008).

[12] Cook, Stephen A.
The complexity of theorem-proving procedures.
ACM, Proc. 3rd ann. ACM Sympos. Theory Computing, Shaker Heights, Ohio 1971, 151–158 (1971).

[13] de Bruijn, N.G.
Asymptotic methods in analysis.
New York: Dover Publications, Inc. XII, 200 p. (1981).

[14] Dembo, Amir; Peres, Yuval; Rosen, Jay; Zeitouni, Ofer
Thick points for planar Brownian motion and the Erdös-Taylor conjecture on random walk.
Acta Math. 186, No.2, 239–270 (2001).

[15] Erdős, Pál; Taylor, S.J.
Some problems concerning the structure of random walk paths.
Acta Math. Acad. Sci. Hung. 11, 137–162 (1960).

[16] Fernandez de la Vega, W.
Random 2-SAT: Results and problems.
Theor. Comput. Sci.265, No.1–2, 131–146 (2001).

[17] Friedgut, Ehud
Sharp thresholds of graph properties, and the k-SAT problem (with an appendix by Jean Bourgain).
J. Am. Math. Soc. 12, No. 4, 1017–1054 (1999).

[18] Frieze, Alan; Wormald, Nicholas C.
Random k-SAT: A tight threshold for moderately growing k.
Combinatorica 25, No. 3, 297–305 (2005).

[19] Goerdt, Andreas
A threshold for unsatisfiability.
J. Comput. Syst. Sci. 53, No.3, 469–486 (1996).

[20] Graham, Ronald L.; Knuth, Donald E.; Patashnik, Oren
Concrete Mathematics.
Addison-Wesley, Reading, Massachusetts (1988).

[21] Mézard, Marc; Montanari, Andrea
Information, physics, and computation.
Oxford Graduate Texts. Oxford University Press, Oxford, xiv+569 pp (2009).

[22] Monasson, R.; Zecchina, R.
Statistical mechanics of the random K-satisfiability model.
Phys. Rev. E 56 (2) 1357–1370 (1997).

[23] Ross, Sheldon
A first course in probability.
Macmillan, New York (1976).

[24] Schöning, Uwe
A Probabilistic Algorithm for k-SAT and Constraint Satisfaction Problems.
FOCS, 410–414 (1999).

[25] Sharell, A.
Concentration of the number of solutions to a random 2-CNF formula.
Manuscript (2000).

[26] Wilson, David B.
On the critical exponents of random k-SAT.
Random Struct. Algorithms 21, No.2, 182–195 (2002).