

An Exponential Improvement for Diagonal Ramsey

Lawrence C. Paulson

6 February 2026

Abstract

The (diagonal) Ramsey number $R(k)$ denotes the minimum size of a complete graph such that every red-blue colouring of its edges contains a monochromatic subgraph of size k . In 1935, Erdős and Szekeres found an upper bound, proving that $R(k) \leq 4^k$. Somewhat later, a lower bound of $\sqrt{2}^k$ was established. In subsequent improvements to the upper bound, the base of the exponent stubbornly remained at 4 until March 2023, when Campos et al. [1] sensationally showed that $R(k) \leq (4 - \epsilon)^k$ for a particular small positive ϵ .

The Isabelle/HOL formalisation of the result presented here is largely independent of the prior formalisation (in Lean) by Bhavik Mehta.

Contents

1	Background material: the neighbours of vertices	5
1.1	Preliminaries on graphs	5
1.2	Neighbours of a vertex	7
1.3	Density: for calculating the parameter p	7
1.4	Lemma 9.2 preliminaries	10
2	The book algorithm	11
2.1	Locales for the parameters of the construction	11
2.2	State invariants	18
2.3	Degree regularisation	18
2.4	Big blue steps: code	19
2.5	The central vertex	20
2.6	Red step	21
2.7	Density-boost step	22
2.8	Execution steps 2–5 as a function	23
2.9	The classes of execution steps	26
2.10	Termination proof	29
3	Big Blue Steps: theorems	31
3.1	Preliminaries	31
3.2	Preliminaries: Fact D1	32
4	Red Steps: theorems	34
4.1	Density-boost steps	34
4.1.1	Observation 5.5	34
4.1.2	Lemma 5.6	35
4.2	Lemma 5.4	35
4.3	Lemma 5.1	36
4.4	Lemma 5.3	37
5	Bounding the Size of Y	38
5.1	The following results together are Lemma 6.4	38
5.2	Towards Lemmas 6.3	39
5.3	Lemma 6.5	39
5.4	Lemma 6.2	40
5.5	Lemma 6.1	41
6	Bounding the Size of X	41
6.1	Preliminaries	41
6.2	Lemma 7.2	43
6.3	Lemma 7.3	43
6.4	Lemma 7.5	44
6.5	Lemma 7.4	45

6.6	Observation 7.7	46
6.7	Lemma 7.8	46
6.8	Lemma 7.9	46
6.9	Lemma 7.10	47
6.10	Lemma 7.11	47
6.11	Lemma 7.12	48
6.12	Lemma 7.6	48
6.13	Lemma 7.1	49
7	The Zigzag Lemma	49
7.1	Lemma 8.1 (the actual Zigzag Lemma)	49
7.2	Lemma 8.5	50
7.3	Lemma 8.6	51
8	An exponential improvement far from the diagonal	51
8.1	An asymptotic form for binomial coefficients via Stirling's formula	51
8.2	Fact D.3 from the Appendix	52
8.3	Fact D.2	53
8.4	Lemma 9.3	53
8.5	Lemma 9.5	54
8.6	Lemma 9.2	55
8.7	Theorem 9.1	57
9	An exponential improvement closer to the diagonal	58
9.1	Lemma 10.2	58
9.2	Theorem 10.1	59
10	From diagonal to off-diagonal	60
10.1	Lemma 11.2	60
10.2	Lemma 11.3	62
10.3	Theorem 11.1	62
11	The Proof of Theorem 1.1	63
11.1	The bounding functions	63
11.2	The monster calculation from appendix A	66
11.2.1	Observation A.1	66
11.2.2	Claims A.2–A.4	67
11.3	Concluding the proof	68

Acknowledgements Many thanks to Mantas Bakšys, Chelsea Edmonds, Simon Griffiths, Bhavik Mehta, Fedor Petrov and Andrew Thomason for their help with aspects of the proofs. The author was supported by the ERC

Advanced Grant ALEXANDRIA (Project 742178), funded by the European Research Council.

1 Background material: the neighbours of vertices

Preliminaries for the Book Algorithm

theory *Neighbours* **imports** *Ramsey-Bounds.Ramsey-Bounds*

begin

abbreviation *set-difference* :: [*'a set, 'a set*] \Rightarrow *'a set* (**infixl** $\langle \setminus \rangle$ 65)
where $A \setminus B \equiv A - B$

lemma *setdif-eq-iff*: $\llbracket A \subseteq C; B \subseteq C \rrbracket \Longrightarrow C \setminus A = C \setminus B \longleftrightarrow A = B$
\langle proof \rangle

1.1 Preliminaries on graphs

context *ulgraph*

begin

The set of *undirected* edges between two sets

definition *all-edges-betw-un* :: *'a set* \Rightarrow *'a set* \Rightarrow *'a set set* **where**
all-edges-betw-un $X Y \equiv \{\{x, y\} \mid x y. x \in X \wedge y \in Y\} \cap E$

lemma *all-edges-betw-un-commute1*: *all-edges-betw-un* $X Y \subseteq$ *all-edges-betw-un* $Y X$
\langle proof \rangle

lemma *all-edges-betw-un-commute*: *all-edges-betw-un* $X Y =$ *all-edges-betw-un* $Y X$
\langle proof \rangle

lemma *all-edges-betw-un-iff-mk-edge*: *all-edges-betw-un* $X Y =$ *mk-edge* ' *all-edges-between* $X Y$
\langle proof \rangle

lemma *all-uedges-betw-subset*: *all-edges-betw-un* $X Y \subseteq E$
\langle proof \rangle

lemma *all-uedges-betw-I*: $x \in X \Longrightarrow y \in Y \Longrightarrow \{x, y\} \in E \Longrightarrow \{x, y\} \in$
all-edges-betw-un $X Y$
\langle proof \rangle

lemma *all-edges-betw-un-subset*: *all-edges-betw-un* $X Y \subseteq$ *Pow* $(X \cup Y)$
\langle proof \rangle

lemma *all-edges-betw-un-empty* [*simp*]:
all-edges-betw-un $\{\} Z = \{\}$ *all-edges-betw-un* $Z \{\} = \{\}$
\langle proof \rangle

lemma *card-all-uedges-betw-le*:

assumes *finite X finite Y*
shows $\text{card } (\text{all-edges-betw-un } X Y) \leq \text{card } (\text{all-edges-between } X Y)$
<proof>

lemma *all-edges-betw-un-le:*
assumes *finite X finite Y*
shows $\text{card } (\text{all-edges-betw-un } X Y) \leq \text{card } X * \text{card } Y$
<proof>

lemma *all-edges-betw-un-insert1:*
 $\text{all-edges-betw-un } (\text{insert } v X) Y = (\{\{v, y\} \mid y. y \in Y\} \cap E) \cup \text{all-edges-betw-un } X Y$
<proof>

lemma *all-edges-betw-un-insert2:*
 $\text{all-edges-betw-un } X (\text{insert } v Y) = (\{\{x, v\} \mid x. x \in X\} \cap E) \cup \text{all-edges-betw-un } X Y$
<proof>

lemma *all-edges-betw-un-Un1:*
 $\text{all-edges-betw-un } (X \cup Y) Z = \text{all-edges-betw-un } X Z \cup \text{all-edges-betw-un } Y Z$
<proof>

lemma *all-edges-betw-un-Un2:*
 $\text{all-edges-betw-un } X (Y \cup Z) = \text{all-edges-betw-un } X Y \cup \text{all-edges-betw-un } X Z$
<proof>

lemma *finite-all-edges-betw-un:*
assumes *finite X finite Y*
shows *finite (all-edges-betw-un X Y)*
<proof>

lemma *all-edges-betw-un-Union1:*
 $\text{all-edges-betw-un } (\text{Union } \mathcal{X}) Y = (\bigcup X \in \mathcal{X}. \text{all-edges-betw-un } X Y)$
<proof>

lemma *all-edges-betw-un-Union2:*
 $\text{all-edges-betw-un } X (\text{Union } \mathcal{Y}) = (\bigcup Y \in \mathcal{Y}. \text{all-edges-betw-un } X Y)$
<proof>

lemma *all-edges-betw-un-mono1:*
 $Y \subseteq Z \implies \text{all-edges-betw-un } Y X \subseteq \text{all-edges-betw-un } Z X$
<proof>

lemma *all-edges-betw-un-mono2:*
 $Y \subseteq Z \implies \text{all-edges-betw-un } X Y \subseteq \text{all-edges-betw-un } X Z$
<proof>

lemma *disjnt-all-edges-betw-un:*

assumes *disjnt* $X Y$ *disjnt* $X Z$
shows *disjnt* (*all-edges-betw-un* $X Z$) (*all-edges-betw-un* $Y Z$)
 ⟨*proof*⟩

end

1.2 Neighbours of a vertex

definition *Neighbours* :: 'a set set \Rightarrow 'a \Rightarrow 'a set **where**
Neighbours $\equiv \lambda E x. \{y. \{x,y\} \in E\}$

lemma *in-Neighbours-iff*: $y \in \text{Neighbours } E x \iff \{x,y\} \in E$
 ⟨*proof*⟩

lemma *finite-Neighbours*:
assumes *finite* E
shows *finite* (*Neighbours* $E x$)
 ⟨*proof*⟩

lemma (**in** *fin-sgraph*) *not-own-Neighbour*: $E' \subseteq E \implies x \notin \text{Neighbours } E' x$
 ⟨*proof*⟩

context *fin-sgraph*
begin

declare *singleton-not-edge* [*simp*]

"A graph on vertex set $S \cup T$ that contains all edges incident to S "
 (page 3). In fact, S is a clique and every vertex in T has an edge into S .

definition *book* :: 'a set \Rightarrow 'a set \Rightarrow 'a set set \Rightarrow bool **where**
book $\equiv \lambda S T F. \text{disjnt } S T \wedge \text{all-edges-betw-un } S (S \cup T) \subseteq F$

Cliques of a given number of vertices; the definition of clique from Ramsey
 is used

definition *size-clique* :: nat \Rightarrow 'a set \Rightarrow 'a set set \Rightarrow bool **where**
size-clique $p K F \equiv \text{card } K = p \wedge \text{clique } K F \wedge K \subseteq V$

lemma *size-clique-smaller*: $\llbracket \text{size-clique } p K F; p' < p \rrbracket \implies \exists K'. \text{size-clique } p' K' F$
 ⟨*proof*⟩

1.3 Density: for calculating the parameter p

definition *edge-card* $\equiv \lambda C X Y. \text{card } (C \cap \text{all-edges-betw-un } X Y)$

definition *gen-density* $\equiv \lambda C X Y. \text{edge-card } C X Y / (\text{card } X * \text{card } Y)$

lemma *edge-card-empty* [*simp*]: $\text{edge-card } C \{\} X = 0$ $\text{edge-card } C X \{\} = 0$
 ⟨*proof*⟩

lemma *edge-card-commute*: $\text{edge-card } C X Y = \text{edge-card } C Y X$
 ⟨proof⟩

lemma *edge-card-le*:
assumes *finite X finite Y*
shows $\text{edge-card } C X Y \leq \text{card } X * \text{card } Y$
 ⟨proof⟩

the assumption that Z is disjoint from X (or Y) is necessary

lemma *edge-card-Un*:
assumes *disjnt X Y disjnt X Z finite X finite Y*
shows $\text{edge-card } C (X \cup Y) Z = \text{edge-card } C X Z + \text{edge-card } C Y Z$
 ⟨proof⟩

lemma *edge-card-diff*:
assumes $Y \subseteq X$ *disjnt X Z finite X*
shows $\text{edge-card } C (X \setminus Y) Z = \text{edge-card } C X Z - \text{edge-card } C Y Z$
 ⟨proof⟩

lemma *edge-card-mono*:
assumes $Y \subseteq X$ **shows** $\text{edge-card } C Y Z \leq \text{edge-card } C X Z$
 ⟨proof⟩

lemma *edge-card-eq-sum-Neighbours*:
assumes $C \subseteq E$ **and** B : *finite B disjnt A B*
shows $\text{edge-card } C A B = (\sum_{i \in B}. \text{card } (\text{Neighbours } C i \cap A))$
 ⟨proof⟩

lemma *sum-eq-card*: $\text{finite } A \implies (\sum_{x \in A}. \text{if } x \in B \text{ then } 1 \text{ else } 0) = \text{card } (A \cap B)$
 ⟨proof⟩

lemma *sum-eq-card-Neighbours*:
assumes $x \in V$ $C \subseteq E$
shows $(\sum_{y \in V \setminus \{x\}}. \text{if } \{x, y\} \in C \text{ then } 1 \text{ else } 0) = \text{card } (\text{Neighbours } C x)$
 ⟨proof⟩

lemma *Neighbours-insert-NO-MATCH*: $\text{NO-MATCH } \{ \} C \implies \text{Neighbours } (\text{insert } e C) x = \text{Neighbours } \{e\} x \cup \text{Neighbours } C x$
 ⟨proof⟩

lemma *Neighbours-sing-2*:
assumes $e \in E$
shows $(\sum_{x \in V}. \text{card } (\text{Neighbours } \{e\} x)) = 2$
 ⟨proof⟩

lemma *sum-Neighbours-eq-card*:
assumes *finite C C ⊆ E*
shows $(\sum_{i \in V}. \text{card } (\text{Neighbours } C i)) = \text{card } C * 2$

<proof>

lemma *gen-density-empty [simp]: gen-density C {} X = 0 gen-density C X {} = 0*

<proof>

lemma *gen-density-commute: gen-density C X Y = gen-density C Y X*

<proof>

lemma *gen-density-ge0: gen-density C X Y ≥ 0*

<proof>

lemma *gen-density-gt0:*

assumes *finite X finite Y {x,y} ∈ C x ∈ X y ∈ Y C ⊆ E*

shows *gen-density C X Y > 0*

<proof>

lemma *gen-density-le1: gen-density C X Y ≤ 1*

<proof>

lemma *gen-density-le-1-minus:*

shows *gen-density C X Y ≤ 1 - gen-density (E\C) X Y*

<proof>

lemma *gen-density-lt1:*

assumes *{x,y} ∈ E\C x ∈ X y ∈ Y C ⊆ E*

shows *gen-density C X Y < 1*

<proof>

lemma *gen-density-le-iff:*

assumes *disjnt X Z finite X Y ⊆ X Y ≠ {} finite Z*

shows *gen-density C X Z ≤ gen-density C Y Z ↔*

edge-card C X Z / card X ≤ edge-card C Y Z / card Y

<proof>

"Removing vertices whose degree is less than the average can only increase the density from the remaining set" (page 17)

lemma *gen-density-below-avg-ge:*

assumes *disjnt X Z finite X Y ⊆ X finite Z*

and *genY: gen-density C Y Z ≤ gen-density C X Z*

shows *gen-density C (X\Y) Z ≥ gen-density C X Z*

<proof>

lemma *edge-card-insert:*

assumes *NO-MATCH {} F and e ∉ F*

shows *edge-card (insert e F) X Y = edge-card {e} X Y + edge-card F X Y*

<proof>

lemma *edge-card-sing:*

assumes $e \in E$
shows $\text{edge-card } \{e\} U U = (\text{if } e \subseteq U \text{ then } 1 \text{ else } 0)$
 ⟨proof⟩

lemma *sum-edge-card-choose*:

assumes $2 \leq k$ $C \subseteq E$
shows $(\sum_{U \in [V]^k} \text{edge-card } C U U) = (\text{card } V - 2 \text{ choose } (k-2)) * \text{card } C$
 ⟨proof⟩

lemma *sum-nsets-Compl*:

assumes *finite* A $k \leq \text{card } A$
shows $(\sum_{U \in [A]^k} f(A \setminus U)) = (\sum_{U \in [A]^{(\text{card } A - k)}} f U)$
 ⟨proof⟩

1.4 Lemma 9.2 preliminaries

Equation (45) in the text, page 30, is seemingly a huge gap. The development below relies on binomial coefficient identities.

definition *graph-density* $\equiv \lambda C. \text{card } C / \text{card } E$

lemma *graph-density-Un*:

assumes *disjnt* $C D$ $C \subseteq E$ $D \subseteq E$
shows $\text{graph-density } (C \cup D) = \text{graph-density } C + \text{graph-density } D$
 ⟨proof⟩

Could be generalised to any complete graph

lemma *density-eq-average*:

assumes $C \subseteq E$ **and** *complete*: $E = \text{all-edges } V$
shows $\text{graph-density } C =$
 $\text{real } (\sum_{x \in V} \sum_{y \in V \setminus \{x\}} \text{if } \{x,y\} \in C \text{ then } 1 \text{ else } 0) / (\text{card } V * (\text{card } V - 1))$
 ⟨proof⟩

lemma *edge-card-V-V*:

assumes $C \subseteq E$ **and** *complete*: $E = \text{all-edges } V$
shows $\text{edge-card } C V V = \text{card } C$
 ⟨proof⟩

Bhavik's statement; own proof

proposition *density-eq-average-partition*:

assumes $k: 0 < k < \text{card } V$ **and** $C \subseteq E$ **and** *complete*: $E = \text{all-edges } V$
shows $\text{graph-density } C = (\sum_{U \in [V]^k} \text{gen-density } C U (V \setminus U)) / (\text{card } V \text{ choose } k)$
 ⟨proof⟩

lemma *exists-density-edge-density*:

assumes $k: 0 < k < \text{card } V$ **and** $C \subseteq E$ **and** *complete*: $E = \text{all-edges } V$
obtains U **where** $\text{card } U = k$ $U \subseteq V$ $\text{graph-density } C \leq \text{gen-density } C U (V \setminus U)$
 ⟨proof⟩

end

end

2 The book algorithm

theory *Book* imports

Neighbours

HOL-Library.Disjoint-Sets *HOL-Decision-Proc.Approximation*

HOL-Real-Asymp.Real-Asymp

begin

hide-const *Bseq*

2.1 Locales for the parameters of the construction

type-synonym *'a config* = *'a set* × *'a set* × *'a set* × *'a set*

locale *P0-min* =

fixes *p0-min* :: *real*

assumes *p0-min*: $0 < p0-min$ $p0-min < 1$

locale *Book-Basis* = *fin-sgraph* + *P0-min* + — building on finite simple graphs
(no loops)

assumes *complete*: $E = \text{all-edges } V$

assumes *infinite-UNIV*: *infinite* (*UNIV*::*'a set*)

begin

abbreviation $nV \equiv \text{card } V$

lemma *graph-size*: $\text{graph-size} = (nV \text{ choose } 2)$

<proof>

lemma *in-E-iff* [*iff*]: $\{v, w\} \in E \longleftrightarrow v \in V \wedge w \in V \wedge v \neq w$

<proof>

lemma *all-edges-betw-un-iff-clique*: $K \subseteq V \implies \text{all-edges-betw-un } K \iff \text{clique } K$

<proof>

lemma *clique-Un*:

assumes *clique* *A* *F* *clique* *B* *F* *all-edges-betw-un* $A \subseteq F$ $A \subseteq V$ $B \subseteq V$

shows *clique* $(A \cup B)$ *F*

<proof>

lemma *clique-insert*:

assumes *clique* *A* *F* *all-edges-betw-un* $\{x\} \subseteq F$ $A \subseteq V$ $x \in V$

shows *clique* (*insert x A*) *F*
 ⟨*proof*⟩

lemma *less-RN-Red-Blue*:

fixes *l k*
assumes *nV*: $nV < RN\ k\ l$
obtains *Red Blue* :: 'a set set
where $Red \subseteq E\ Blue = E \setminus Red \neg (\exists K. \text{size-clique } k\ K\ Red) \neg (\exists K. \text{size-clique } l\ K\ Blue)$
 ⟨*proof*⟩

end

locale *No-Cliques* = *Book-Basis* +

fixes *Red Blue* :: 'a set set
assumes *Red-E*: $Red \subseteq E$
assumes *Blue-def*: $Blue = E - Red$
 — the following are local to the program
fixes *l::nat* — blue limit
fixes *k::nat* — red limit
assumes *l-le-k*: $l \leq k$ — they should be "sufficiently large"
assumes *no-Red-clique*: $\neg (\exists K. \text{size-clique } k\ K\ Red)$
assumes *no-Blue-clique*: $\neg (\exists K. \text{size-clique } l\ K\ Blue)$

locale *Book* = *Book-Basis* + *No-Cliques* +

fixes *μ::real* — governs the big blue steps
assumes *μ01*: $0 < \mu < 1$
fixes *X0* :: 'a set **and** *Y0* :: 'a set — initial values
assumes *XY0*: $\text{disjnt } X0\ Y0\ X0 \subseteq V\ Y0 \subseteq V$
assumes *density-ge-p0-min*: $\text{gen-density } Red\ X0\ Y0 \geq p0\text{-min}$

locale *Book'* = *Book-Basis* + *No-Cliques* +

fixes *γ::real* — governs the big blue steps
assumes *γ-def*: $\gamma = \text{real } l / (\text{real } k + \text{real } l)$
fixes *X0* :: 'a set **and** *Y0* :: 'a set — initial values
assumes *XY0*: $\text{disjnt } X0\ Y0\ X0 \subseteq V\ Y0 \subseteq V$
assumes *density-ge-p0-min*: $\text{gen-density } Red\ X0\ Y0 \geq p0\text{-min}$

definition *eps* $\equiv \lambda k. \text{real } k\ \text{powr } (-1/4)$

definition *qfun-base* :: $[nat, nat] \Rightarrow \text{real}$

where $qfun\text{-base} \equiv \lambda k\ h. ((1 + \text{eps } k)^h - 1) / k$

definition *hgt-maximum* $\equiv \lambda k. 2 * \ln (\text{real } k) / \text{eps } k$

The first of many "bigness assumptions"

definition *Big-height-upper-bound* $\equiv \lambda k. qfun\text{-base } k\ (\text{nat } \lfloor \text{hgt-maximum } k \rfloor) > 1$

lemma *Big-height-upper-bound*:

shows $\forall^\infty k$. *Big-height-upper-bound* k
 \langle *proof* \rangle

context *No-Cliques*
begin

abbreviation $\varepsilon \equiv \text{eps } k$

lemma *eps-eq-sqrt*: $\varepsilon = 1 / \text{sqrt } (\text{sqrt } (\text{real } k))$
 \langle *proof* \rangle

lemma *eps-ge0*: $\varepsilon \geq 0$
 \langle *proof* \rangle

lemma *ln0*: $l > 0$
 \langle *proof* \rangle

lemma *kn0*: $k > 0$
 \langle *proof* \rangle

lemma *eps-gt0*: $\varepsilon > 0$
 \langle *proof* \rangle

lemma *eps-le1*: $\varepsilon \leq 1$
 \langle *proof* \rangle

lemma *eps-less1*:
assumes $k > 1$ **shows** $\varepsilon < 1$
 \langle *proof* \rangle

lemma *Blue-E*: $\text{Blue} \subseteq E$
 \langle *proof* \rangle

lemma *disjnt-Red-Blue*: *disjnt* $\text{Red } \text{Blue}$
 \langle *proof* \rangle

lemma *Red-Blue-all*: $\text{Red} \cup \text{Blue} = \text{all-edges } V$
 \langle *proof* \rangle

lemma *Blue-eq*: $\text{Blue} = \text{all-edges } V - \text{Red}$
 \langle *proof* \rangle

lemma *Red-eq*: $\text{Red} = \text{all-edges } V - \text{Blue}$
 \langle *proof* \rangle

lemma *disjnt-Red-Blue-Neighbours*: *disjnt* (*Neighbours* $\text{Red } x \cap X$) (*Neighbours* $\text{Blue } x \cap X'$)
 \langle *proof* \rangle

lemma *indep-Red-iff-clique-Blue*: $K \subseteq V \implies \text{indep } K \text{ Red} \iff \text{clique } K \text{ Blue}$
(proof)

lemma *Red-Blue-RN*:

fixes $X :: 'a \text{ set}$

assumes $\text{card } X \geq RN \ m \ n \ X \subseteq V$

shows $\exists K \subseteq X. \text{size-clique } m \ K \text{ Red} \vee \text{size-clique } n \ K \text{ Blue}$

(proof)

end

context *Book*

begin

lemma *Red-edges-XY0*: $\text{Red} \cap \text{all-edges-betw-un } X0 \ Y0 \neq \{\}$
(proof)

lemma *finite-X0*: *finite X0* **and** *finite-Y0*: *finite Y0*
(proof)

lemma *Red-nonempty*: $\text{Red} \neq \{\}$
(proof)

lemma *gorder-ge2*: $\text{gorder} \geq 2$
(proof)

lemma *nontriv*: $E \neq \{\}$
(proof)

lemma *no-singleton-Blue* [simp]: $\{a\} \notin \text{Blue}$
(proof)

lemma *no-singleton-Red* [simp]: $\{a\} \notin \text{Red}$
(proof)

lemma *not-Red-Neighbour* [simp]: $x \notin \text{Neighbours Red } x$ **and** *not-Blue-Neighbour*
[simp]: $x \notin \text{Neighbours Blue } x$
(proof)

lemma *Neighbours-RB*:

assumes $a \in V \ X \subseteq V$

shows $\text{Neighbours Red } a \cap X \cup \text{Neighbours Blue } a \cap X = X - \{a\}$

(proof)

lemma *Neighbours-Red-Blue*:

assumes $x \in V$

shows $\text{Neighbours Red } x = V - \text{insert } x \ (\text{Neighbours Blue } x)$

(proof)

abbreviation $red-density\ X\ Y \equiv gen-density\ Red\ X\ Y$
abbreviation $blue-density\ X\ Y \equiv gen-density\ Blue\ X\ Y$

definition $Weight :: ['a\ set,\ 'a\ set,\ 'a,\ 'a] \Rightarrow real$ **where**
 $Weight \equiv \lambda X\ Y\ x\ y. inverse\ (card\ Y) * (card\ (Neighbours\ Red\ x \cap Neighbours\ Red\ y \cap Y))$
 $- red-density\ X\ Y * card\ (Neighbours\ Red\ x \cap Y)$

definition $weight :: 'a\ set \Rightarrow 'a\ set \Rightarrow 'a \Rightarrow real$ **where**
 $weight \equiv \lambda X\ Y\ x. \sum y \in X \setminus \{x\}. Weight\ X\ Y\ x\ y$

definition $p0 :: real$
where $p0 \equiv red-density\ X0\ Y0$

definition $qfun :: nat \Rightarrow real$
where $qfun \equiv \lambda h. p0 + qfun-base\ k\ h$

lemma $qfun-eq: qfun \equiv \lambda h. p0 + ((1 + \varepsilon)^h - 1) / k$
 $\langle proof \rangle$

definition $hgt :: real \Rightarrow nat$
where $hgt \equiv \lambda p. LEAST\ h. p \leq qfun\ h \wedge h > 0$

lemma $qfun0 [simp]: qfun\ 0 = p0$
 $\langle proof \rangle$

lemma $p0-ge: p0 \geq p0-min$
 $\langle proof \rangle$

lemma $card-XY0: card\ X0 > 0\ card\ Y0 > 0$
 $\langle proof \rangle$

lemma $finite-Red [simp]: finite\ Red$
 $\langle proof \rangle$

lemma $finite-Blue [simp]: finite\ Blue$
 $\langle proof \rangle$

lemma $Red-edges-nonzero: edge-card\ Red\ X0\ Y0 > 0$
 $\langle proof \rangle$

lemma $p0-01: 0 < p0\ p0 \leq 1$
 $\langle proof \rangle$

lemma $qfun-strict-mono: h' < h \implies qfun\ h' < qfun\ h$
 $\langle proof \rangle$

lemma $qfun-mono: h' \leq h \implies qfun\ h' \leq qfun\ h$
 $\langle proof \rangle$

lemma *q-Suc-diff*: $qfun (Suc h) - qfun h = \varepsilon * (1 + \varepsilon)^h / k$
<proof>

lemma *height-exists'*:
obtains h **where** $p \leq qfun\text{-base } k h \wedge h > 0$
<proof>

lemma *height-exists*:
obtains h **where** $p \leq qfun h \wedge h > 0$
<proof>

lemma *hgt-gt0*: $hgt p > 0$
<proof>

lemma *hgt-works*: $p \leq qfun (hgt p)$
<proof>

lemma *hgt-Least*:
assumes $0 < h \leq qfun h$
shows $hgt p \leq h$
<proof>

lemma *real-hgt-Least*:
assumes $real h \leq r \wedge 0 < h \leq qfun h$
shows $real (hgt p) \leq r$
<proof>

lemma *hgt-greater*:
assumes $p > qfun h$
shows $hgt p > h$
<proof>

lemma *hgt-less-imp-qfun-less*:
assumes $0 < h < hgt p$
shows $p > qfun h$
<proof>

lemma *hgt-le-imp-qfun-ge*:
assumes $hgt p \leq h$
shows $p \leq qfun h$
<proof>

This gives us an upper bound for heights, namely *hgt 1*, but it's not explicit.

lemma *hgt-mono*:
assumes $p \leq q$
shows $hgt p \leq hgt q$

<proof>

lemma *hgt-mono'*:
 assumes $hgt\ p < hgt\ q$
 shows $p < q$
 <proof>

The upper bound of the height $h(p)$ appears just below (5) on page 9. Although we can bound all Heights by monotonicity (since $p \leq 1$), we need to exhibit a specific $o(k)$ function.

lemma *height-upper-bound*:
 assumes $p \leq 1$ **and** *big*: *Big-height-upper-bound* k
 shows $hgt\ p \leq 2 * \ln\ k / \varepsilon$
 <proof>

definition *alpha* :: $nat \Rightarrow real$ **where** $alpha \equiv \lambda h. qfun\ h - qfun\ (h-1)$

lemma *alpha-ge0*: $alpha\ h \geq 0$
 <proof>

lemma *alpha-Suc-ge*: $alpha\ (Suc\ h) \geq \varepsilon / k$
 <proof>

lemma *alpha-ge*: $h > 0 \implies alpha\ h \geq \varepsilon / k$
 <proof>

lemma *alpha-gt0*: $h > 0 \implies alpha\ h > 0$
 <proof>

lemma *alpha-Suc-eq*: $alpha\ (Suc\ h) = \varepsilon * (1 + \varepsilon) ^ h / k$
 <proof>

lemma *alpha-eq*:
 assumes $h > 0$ **shows** $alpha\ h = \varepsilon * (1 + \varepsilon) ^ (h-1) / k$
 <proof>

lemma *alpha-hgt-eq*: $alpha\ (hgt\ p) = \varepsilon * (1 + \varepsilon) ^ (hgt\ p - 1) / k$
 <proof>

lemma *alpha-mono*: $\llbracket h' \leq h; 0 < h' \rrbracket \implies alpha\ h' \leq alpha\ h$
 <proof>

definition *all-incident-edges* :: $'a\ set \Rightarrow 'a\ set\ set$ **where**
 $all-incident-edges \equiv \lambda A. \bigcup_{v \in A.} incident-edges\ v$

lemma *all-incident-edges-Un [simp]*: $all-incident-edges\ (A \cup B) = all-incident-edges\ A \cup all-incident-edges\ B$
 <proof>

end

context *Book*
begin

2.2 State invariants

definition *V-state* $\equiv \lambda(X, Y, A, B). X \subseteq V \wedge Y \subseteq V \wedge A \subseteq V \wedge B \subseteq V$

definition *disjoint-state* $\equiv \lambda(X, Y, A, B). \text{disjnt } X \ Y \wedge \text{disjnt } X \ A \wedge \text{disjnt } X \ B \wedge \text{disjnt } Y \ A \wedge \text{disjnt } Y \ B \wedge \text{disjnt } A \ B$

previously had all edges incident to A, B

definition *RB-state* $\equiv \lambda(X, Y, A, B). \text{all-edges-betw-un } A \ A \subseteq \text{Red} \wedge \text{all-edges-betw-un } A \ (X \cup Y) \subseteq \text{Red} \\ \wedge \text{all-edges-betw-un } B \ (B \cup X) \subseteq \text{Blue}$

definition *valid-state* $\equiv \lambda U. \text{V-state } U \wedge \text{disjoint-state } U \wedge \text{RB-state } U$

definition *termination-condition* $\equiv \lambda X \ Y. \text{card } X \leq RN \ k \ (\text{nat } \lceil \text{real } l \ \text{powr } (3/4) \rceil) \vee \text{red-density } X \ Y \leq 1/k$

lemma

assumes *V-state*(X, Y, A, B)

shows *finX*: *finite* X **and** *finY*: *finite* Y **and** *finA*: *finite* A **and** *finB*: *finite* B
<proof>

lemma

assumes *valid-state*(X, Y, A, B)

shows *A-Red-clique*: *clique* A *Red* **and** *B-Blue-clique*: *clique* B *Blue*
<proof>

lemma *A-less-k*:

assumes *valid*: *valid-state*(X, Y, A, B)

shows *card* $A < k$
<proof>

lemma *B-less-l*:

assumes *valid*: *valid-state*(X, Y, A, B)

shows *card* $B < l$
<proof>

2.3 Degree regularisation

definition *red-dense* $\equiv \lambda Y \ p \ x. \text{card } (\text{Neighbours } \text{Red } x \cap Y) \geq (p - \varepsilon \ \text{powr } (-1/2) * \text{alpha } (\text{hgt } p)) * \text{card } Y$

definition *X-degree-reg* $\equiv \lambda X \ Y. \{x \in X. \text{red-dense } Y \ (\text{red-density } X \ Y) \ x\}$

definition *degree-reg* $\equiv \lambda(X, Y, A, B). (\text{X-degree-reg } X \ Y, Y, A, B)$

lemma *X-degree-reg-subset*: $X\text{-degree-reg } X Y \subseteq X$

<proof>

lemma *degree-reg-V-state*: $V\text{-state } U \implies V\text{-state } (\text{degree-reg } U)$

<proof>

lemma *degree-reg-disjoint-state*: $\text{disjoint-state } U \implies \text{disjoint-state } (\text{degree-reg } U)$

<proof>

lemma *degree-reg-RB-state*: $RB\text{-state } U \implies RB\text{-state } (\text{degree-reg } U)$

<proof>

lemma *degree-reg-valid-state*: $\text{valid-state } U \implies \text{valid-state } (\text{degree-reg } U)$

<proof>

lemma *not-red-dense-sum-less*:

assumes $\bigwedge x. x \in X \implies \neg \text{red-dense } Y p x$ **and** $X \neq \{\}$ *finite* X

shows $(\sum_{x \in X}. \text{card } (\text{Neighbours Red } x \cap Y)) < p * \text{real } (\text{card } Y) * \text{card } X$

<proof>

lemma *red-density-X-degree-reg-ge*:

assumes *disjnt* $X Y$

shows $\text{red-density } (X\text{-degree-reg } X Y) Y \geq \text{red-density } X Y$

<proof>

2.4 Big blue steps: code

definition *bluish* :: $['a \text{ set}, 'a] \Rightarrow \text{bool}$ **where**

$\text{bluish} \equiv \lambda X x. \text{card } (\text{Neighbours Blue } x \cap X) \geq \mu * \text{real } (\text{card } X)$

definition *many-bluish* :: $'a \text{ set} \Rightarrow \text{bool}$ **where**

$\text{many-bluish} \equiv \lambda X. \text{card } \{x \in X. \text{bluish } X x\} \geq \text{RN } k (\text{nat } \lceil l \text{ pour } (2/3) \rceil)$

definition *good-blue-book* :: $['a \text{ set}, 'a \text{ set} \times 'a \text{ set}] \Rightarrow \text{bool}$ **where**

$\text{good-blue-book} \equiv \lambda X. \lambda (S, T). \text{book } S T \text{ Blue} \wedge S \subseteq X \wedge T \subseteq X \wedge \text{card } T \geq (\mu \wedge \text{card } S) * \text{card } X / 2$

lemma *ex-good-blue-book*: $\text{good-blue-book } X (\{\}, X)$

<proof>

lemma *bounded-good-blue-book*: $\llbracket \text{good-blue-book } X (S, T); \text{finite } X \rrbracket \implies \text{card } S \leq \text{card } X$

<proof>

definition *best-blue-book-card* :: $'a \text{ set} \Rightarrow \text{nat}$ **where**

$\text{best-blue-book-card} \equiv \lambda X. \text{GREATEST } s. \exists S T. \text{good-blue-book } X (S, T) \wedge s = \text{card } S$

lemma *best-blue-book-is-best*: $\llbracket \text{good-blue-book } X (S,T); \text{finite } X \rrbracket \implies \text{card } S \leq \text{best-blue-book-card } X$

<proof>

lemma *ex-best-blue-book*: $\text{finite } X \implies \exists S T. \text{good-blue-book } X (S,T) \wedge \text{card } S = \text{best-blue-book-card } X$

<proof>

definition *choose-blue-book* $\equiv \lambda(X,Y,A,B). @ (S,T). \text{good-blue-book } X (S,T) \wedge \text{card } S = \text{best-blue-book-card } X$

lemma *choose-blue-book-works*:

$\llbracket \text{finite } X; (S,T) = \text{choose-blue-book } (X,Y,A,B) \rrbracket$

$\implies \text{good-blue-book } X (S,T) \wedge \text{card } S = \text{best-blue-book-card } X$

<proof>

lemma *choose-blue-book-subset*:

$\llbracket \text{finite } X; (S,T) = \text{choose-blue-book } (X,Y,A,B) \rrbracket \implies S \subseteq X \wedge T \subseteq X \wedge \text{disjnt } S T$

<proof>

expressing the complicated preconditions inductively

inductive *big-blue*

where $\llbracket \text{many-bluish } X; \text{good-blue-book } X (S,T); \text{card } S = \text{best-blue-book-card } X \rrbracket \implies \text{big-blue } (X,Y,A,B) (T, Y, A, B \cup S)$

lemma *big-blue-V-state*: $\llbracket \text{big-blue } U U'; \text{V-state } U \rrbracket \implies \text{V-state } U'$

<proof>

lemma *big-blue-disjoint-state*: $\llbracket \text{big-blue } U U'; \text{disjoint-state } U \rrbracket \implies \text{disjoint-state } U'$

<proof>

lemma *big-blue-RB-state*: $\llbracket \text{big-blue } U U'; \text{RB-state } U \rrbracket \implies \text{RB-state } U'$

<proof>

lemma *big-blue-valid-state*: $\llbracket \text{big-blue } U U'; \text{valid-state } U \rrbracket \implies \text{valid-state } U'$

<proof>

2.5 The central vertex

definition *central-vertex* :: [*'a set, 'a*] \Rightarrow *bool* **where**

$\text{central-vertex} \equiv \lambda X x. x \in X \wedge \text{card } (\text{Neighbours Blue } x \cap X) \leq \mu * \text{real } (\text{card } X)$

lemma *ex-central-vertex*:

assumes $\neg \text{termination-condition } X Y \neg \text{many-bluish } X$

shows $\exists x. \text{central-vertex } X x$

<proof>

lemma *finite-central-vertex-set*: $\text{finite } X \implies \text{finite } \{x. \text{central-vertex } X x\}$
 ⟨proof⟩

definition *max-central-vx* :: [*'a set, 'a set*] \Rightarrow *real* **where**
 $\text{max-central-vx} \equiv \lambda X Y. \text{Max } (\text{weight } X Y \text{ ' } \{x. \text{central-vertex } X x\})$

lemma *central-vx-is-best*:
 $\llbracket \text{central-vertex } X x; \text{finite } X \rrbracket \implies \text{weight } X Y x \leq \text{max-central-vx } X Y$
 ⟨proof⟩

lemma *ex-best-central-vx*:
 $\llbracket \neg \text{termination-condition } X Y; \neg \text{many-bluish } X; \text{finite } X \rrbracket$
 $\implies \exists x. \text{central-vertex } X x \wedge \text{weight } X Y x = \text{max-central-vx } X Y$
 ⟨proof⟩

it's necessary to make a specific choice; a relational treatment might allow different vertices to be chosen, making a nonsense of the choice between steps 4 and 5

definition *choose-central-vx* $\equiv \lambda(X, Y, A, B). @x. \text{central-vertex } X x \wedge \text{weight } X Y x = \text{max-central-vx } X Y$

lemma *choose-central-vx-works*:
 $\llbracket \neg \text{termination-condition } X Y; \neg \text{many-bluish } X; \text{finite } X \rrbracket$
 $\implies \text{central-vertex } X (\text{choose-central-vx } (X, Y, A, B)) \wedge \text{weight } X Y (\text{choose-central-vx } (X, Y, A, B)) = \text{max-central-vx } X Y$
 ⟨proof⟩

lemma *choose-central-vx-X*:
 $\llbracket \neg \text{many-bluish } X; \neg \text{termination-condition } X Y; \text{finite } X \rrbracket \implies \text{choose-central-vx } (X, Y, A, B) \in X$
 ⟨proof⟩

2.6 Red step

definition *reddish* $\equiv \lambda k X Y p x. \text{red-density } (Neighbours \text{ Red } x \cap X) (Neighbours \text{ Red } x \cap Y) \geq p - \text{alpha } (\text{hgt } p)$

inductive *red-step*
where $\llbracket \text{reddish } k X Y (\text{red-density } X Y) x; x = \text{choose-central-vx } (X, Y, A, B) \rrbracket$
 $\implies \text{red-step } (X, Y, A, B) (Neighbours \text{ Red } x \cap X, Neighbours \text{ Red } x \cap Y, \text{insert } x A, B)$

lemma *red-step-V-state*:
assumes $\text{red-step } (X, Y, A, B) U' \neg \text{termination-condition } X Y$
 $\neg \text{many-bluish } X \text{ V-state } (X, Y, A, B)$
shows *V-state* U'
 ⟨proof⟩

lemma *red-step-disjoint-state*:

assumes *red-step* (X, Y, A, B) $U' \neg$ *termination-condition* $X Y$
 \neg *many-bluish* X *V-state* (X, Y, A, B) *disjoint-state* (X, Y, A, B)
shows *disjoint-state* U'

<proof>

lemma *red-step-RB-state*:

assumes *red-step* (X, Y, A, B) $U' \neg$ *termination-condition* $X Y$
 \neg *many-bluish* X *V-state* (X, Y, A, B) *RB-state* (X, Y, A, B)
shows *RB-state* U'

<proof>

lemma *red-step-valid-state*:

assumes *red-step* (X, Y, A, B) $U' \neg$ *termination-condition* $X Y$
 \neg *many-bluish* X *valid-state* (X, Y, A, B)

shows *valid-state* U'

<proof>

2.7 Density-boost step

inductive *density-boost*

where $\llbracket \neg$ *reddish* $k X Y$ (*red-density* $X Y$) x ; $x =$ *choose-central-vx* $(X, Y, A, B) \rrbracket$

\implies *density-boost* (X, Y, A, B) (*Neighbours Blue* $x \cap X$, *Neighbours Red* $x \cap Y$, A , *insert* $x B$)

lemma *density-boost-V-state*:

assumes *density-boost* (X, Y, A, B) $U' \neg$ *termination-condition* $X Y$
 \neg *many-bluish* X *V-state* (X, Y, A, B)

shows *V-state* U'

<proof>

lemma *density-boost-disjoint-state*:

assumes *density-boost* (X, Y, A, B) $U' \neg$ *termination-condition* $X Y$
 \neg *many-bluish* X *V-state* (X, Y, A, B) *disjoint-state* (X, Y, A, B)

shows *disjoint-state* U'

<proof>

lemma *density-boost-RB-state*:

assumes *density-boost* (X, Y, A, B) $U' \neg$ *termination-condition* $X Y$ \neg *many-bluish* X *V-state* (X, Y, A, B)

and rb : *RB-state* (X, Y, A, B)

shows *RB-state* U'

<proof>

lemma *density-boost-valid-state*:

assumes *density-boost* (X, Y, A, B) $U' \neg$ *termination-condition* $X Y$ \neg *many-bluish* X *valid-state* (X, Y, A, B)

shows *valid-state* U'

<proof>

2.8 Execution steps 2–5 as a function

definition *next-state* :: 'a config \Rightarrow 'a config **where**

next-state $\equiv \lambda(X, Y, A, B).$

if many-bluish X

then let $(S, T) = \text{choose-blue-book } (X, Y, A, B)$ *in* $(T, Y, A, B \cup S)$

else let $x = \text{choose-central-vx } (X, Y, A, B)$ *in*

if reddish $k \ X \ Y$ (*red-density* $X \ Y$) x

then $(\text{Neighbours Red } x \cap X, \text{Neighbours Red } x \cap Y, \text{insert } x \ A, B)$

else $(\text{Neighbours Blue } x \cap X, \text{Neighbours Red } x \cap Y, A, \text{insert } x \ B)$

lemma *next-state-valid*:

assumes *valid-state* $(X, Y, A, B) \neg \text{termination-condition } X \ Y$

shows *valid-state* $(\text{next-state } (X, Y, A, B))$

<proof>

primrec *stepper* :: $\text{nat} \Rightarrow$ 'a config **where**

stepper $0 = (X0, Y0, \{\}, \{\})$

| *stepper* $(\text{Suc } n) =$

$(\text{let } (X, Y, A, B) = \text{stepper } n$ *in*

if termination-condition $X \ Y$ *then* (X, Y, A, B)

else if even n *then* *degree-reg* (X, Y, A, B) *else* *next-state* (X, Y, A, B))

lemma *degree-reg-subset*:

assumes *degree-reg* $(X, Y, A, B) = (X', Y', A', B')$

shows $X' \subseteq X \wedge Y' \subseteq Y$

<proof>

lemma *next-state-subset*:

assumes *next-state* $(X, Y, A, B) = (X', Y', A', B')$ *finite* X

shows $X' \subseteq X \wedge Y' \subseteq Y$

<proof>

lemma *valid-state0*: *valid-state* $(X0, Y0, \{\}, \{\})$

<proof>

lemma *valid-state-stepper* [*simp*]: *valid-state* $(\text{stepper } n)$

<proof>

lemma *V-state-stepper*: *V-state* $(\text{stepper } n)$

<proof>

lemma *RB-state-stepper*: *RB-state* $(\text{stepper } n)$

<proof>

lemma

assumes *stepper* $n = (X, Y, A, B)$

shows *stepper-A*: $\text{clique } A \text{ Red} \wedge A \subseteq V$ **and** *stepper-B*: $\text{clique } B \text{ Blue} \wedge B \subseteq V$
 ⟨*proof*⟩

lemma *card-B-limit*:

assumes *stepper* $n = (X, Y, A, B)$ **shows** $\text{card } B < l$
 ⟨*proof*⟩

definition $Xseq \equiv (\lambda(X, Y, A, B). X) \circ \text{stepper}$

definition $Yseq \equiv (\lambda(X, Y, A, B). Y) \circ \text{stepper}$

definition $Aseq \equiv (\lambda(X, Y, A, B). A) \circ \text{stepper}$

definition $Bseq \equiv (\lambda(X, Y, A, B). B) \circ \text{stepper}$

definition $pseq \equiv \lambda i. \text{red-density } (Xseq\ i) (Yseq\ i)$

lemma *Xseq-0 [simp]*: $Xseq\ 0 = X0$

⟨*proof*⟩

lemma *Xseq-Suc-subset*: $Xseq\ (Suc\ i) \subseteq Xseq\ i$ **and** *Yseq-Suc-subset*: $Yseq\ (Suc\ i) \subseteq Yseq\ i$

⟨*proof*⟩

lemma *Xseq-antimono*: $j \leq i \implies Xseq\ i \subseteq Xseq\ j$

⟨*proof*⟩

lemma *Xseq-subset-V*: $Xseq\ i \subseteq V$

⟨*proof*⟩

lemma *finite-Xseq*: $\text{finite } (Xseq\ i)$

⟨*proof*⟩

lemma *Yseq-0 [simp]*: $Yseq\ 0 = Y0$

⟨*proof*⟩

lemma *Yseq-antimono*: $j \leq i \implies Yseq\ i \subseteq Yseq\ j$

⟨*proof*⟩

lemma *Yseq-subset-V*: $Yseq\ i \subseteq V$

⟨*proof*⟩

lemma *finite-Yseq*: $\text{finite } (Yseq\ i)$

⟨*proof*⟩

lemma *Xseq-Yseq-disjnt*: $\text{disjnt } (Xseq\ i) (Yseq\ i)$

⟨*proof*⟩

lemma *edge-card-eq-pee*:

$\text{edge-card Red } (Xseq\ i) (Yseq\ i) = pseq\ i * \text{card } (Xseq\ i) * \text{card } (Yseq\ i)$

⟨*proof*⟩

lemma *valid-state-seq*: $\text{valid-state}(Xseq\ i, Yseq\ i, Aseq\ i, Bseq\ i)$

<proof>

lemma *Aseq-less-k*: $\text{card } (Aseq\ i) < k$
<proof>

lemma *Aseq-0 [simp]*: $Aseq\ 0 = \{\}$
<proof>

lemma *Aseq-Suc-subset*: $Aseq\ i \subseteq Aseq\ (Suc\ i)$ **and** *Bseq-Suc-subset*: $Bseq\ i \subseteq Bseq\ (Suc\ i)$
<proof>

lemma
assumes $j \leq i$
shows *Aseq-mono*: $Aseq\ j \subseteq Aseq\ i$ **and** *Bseq-mono*: $Bseq\ j \subseteq Bseq\ i$
<proof>

lemma *Aseq-subset-V*: $Aseq\ i \subseteq V$
<proof>

lemma *Bseq-subset-V*: $Bseq\ i \subseteq V$
<proof>

lemma *finite-Aseq*: $\text{finite } (Aseq\ i)$ **and** *finite-Bseq*: $\text{finite } (Bseq\ i)$
<proof>

lemma *Bseq-less-l*: $\text{card } (Bseq\ i) < l$
<proof>

lemma *Bseq-0 [simp]*: $Bseq\ 0 = \{\}$
<proof>

lemma *pee-eq-p0*: $pseq\ 0 = p0$
<proof>

lemma *pee-ge0*: $pseq\ i \geq 0$
<proof>

lemma *pee-le1*: $pseq\ i \leq 1$
<proof>

lemma *pseq-0*: $p0 = pseq\ 0$
<proof>

The central vertex at each step (though only defined in some cases), $x-i$ in the paper

definition *cvx* $\equiv \lambda i. \text{choose-central-}vx\ (stepper\ i)$

the indexing of *beta* is as in the paper — and different from that of *Xseq*

definition

$beta \equiv \lambda i. let (X,Y,A,B) = stepper\ i\ in\ card(Neighbors\ Blue\ (cvx\ i) \cap X) / card\ X$

lemma *beta-eq*: $beta\ i = card(Neighbors\ Blue\ (cvx\ i) \cap Xseq\ i) / card\ (Xseq\ i)$
 ⟨proof⟩

lemma *beta-ge0*: $beta\ i \geq 0$
 ⟨proof⟩

2.9 The classes of execution steps

For R, B, S, D

datatype *stepkind* = *red-step* | *bblue-step* | *dboost-step* | *dreg-step* | *halted*

definition *next-state-kind* :: 'a config \Rightarrow *stepkind* **where**
 $next-state-kind \equiv \lambda(X,Y,A,B).$
 if *many-bluish* X then *bblue-step*
 else let $x = choose-central-vx\ (X,Y,A,B)$ in
 if *reddish* k X Y (*red-density* X Y) x then *red-step*
 else *dboost-step*

definition *stepper-kind* :: nat \Rightarrow *stepkind* **where**
 $stepper-kind\ i =$
 (let $(X,Y,A,B) = stepper\ i$ in
 if *termination-condition* X Y then *halted*
 else if even i then *dreg-step* else $next-state-kind\ (X,Y,A,B)$)

definition *Step-class* $\equiv \lambda knd. \{n. stepper-kind\ n \in knd\}$

lemma *subset-Step-class*: $\llbracket i \in Step-class\ K'; K' \subseteq K \rrbracket \Longrightarrow i \in Step-class\ K$
 ⟨proof⟩

lemma *Step-class-Un*: $Step-class\ (K' \cup K) = Step-class\ K' \cup Step-class\ K$
 ⟨proof⟩

lemma *Step-class-insert*: $Step-class\ (insert\ knd\ K) = (Step-class\ \{knd\}) \cup (Step-class\ K)$
 ⟨proof⟩

lemma *Step-class-insert-NO-MATCH*:
 $NO-MATCH\ \{\} K \Longrightarrow Step-class\ (insert\ knd\ K) = (Step-class\ \{knd\}) \cup (Step-class\ K)$
 ⟨proof⟩

lemma *Step-class-UNIV*: $Step-class\ \{red-step, bblue-step, dboost-step, dreg-step, halted\} = UNIV$
 ⟨proof⟩

lemma *Step-class-cases*:

$i \in \text{Step-class } \{\text{stepkind.red-step}\} \vee i \in \text{Step-class } \{\text{bblue-step}\} \vee$
 $i \in \text{Step-class } \{\text{dboost-step}\} \vee i \in \text{Step-class } \{\text{dreg-step}\} \vee$
 $i \in \text{Step-class } \{\text{halted}\}$
 <proof>

lemmas *step-kind-defs* = *Step-class-def stepper-kind-def next-state-kind-def*
Xseq-def Yseq-def Aseq-def Bseq-def cvx-def Let-def

lemma *disjnt-Step-class*:
 $\text{disjnt } \text{knd } \text{knd}' \implies \text{disjnt } (\text{Step-class } \text{knd}) (\text{Step-class } \text{knd}')$
 <proof>

lemma *halted-imp-next-halted*: $\text{stepper-kind } i = \text{halted} \implies \text{stepper-kind } (\text{Suc } i) =$
 halted
 <proof>

lemma *halted-imp-ge-halted*: $\text{stepper-kind } i = \text{halted} \implies \text{stepper-kind } (i+n) =$
 halted
 <proof>

lemma *Step-class-halted-forever*: $\llbracket i \in \text{Step-class } \{\text{halted}\}; i \leq j \rrbracket \implies j \in \text{Step-class}$
 $\{\text{halted}\}$
 <proof>

lemma *Step-class-not-halted*: $\llbracket i \notin \text{Step-class } \{\text{halted}\}; i \geq j \rrbracket \implies j \notin \text{Step-class}$
 $\{\text{halted}\}$
 <proof>

lemma
assumes $i \notin \text{Step-class } \{\text{halted}\}$
shows *not-halted-pee-gt*: $\text{pseq } i > 1/k$
and *Xseq-gt0*: $\text{card } (Xseq\ i) > 0$
and *Xseq-gt-RN*: $\text{card } (Xseq\ i) > RN\ k\ (\text{nat } \lceil \text{real } l\ \text{powr } (3/4) \rceil)$
and *not-termination-condition*: $\neg \text{termination-condition } (Xseq\ i)\ (Yseq\ i)$
 <proof>

lemma *not-halted-pee-gt0*:
assumes $i \notin \text{Step-class } \{\text{halted}\}$
shows $\text{pseq } i > 0$
 <proof>

lemma *Yseq-gt0*:
assumes $i \notin \text{Step-class } \{\text{halted}\}$
shows $\text{card } (Yseq\ i) > 0$
 <proof>

lemma *step-odd*: $i \in \text{Step-class } \{\text{red-step}, \text{bblue-step}, \text{dboost-step}\} \implies \text{odd } i$
 <proof>

lemma *step-even*: $i \in \text{Step-class } \{\text{dreg-step}\} \implies \text{even } i$
 ⟨proof⟩

lemma *not-halted-odd-RBS*: $\llbracket i \notin \text{Step-class } \{\text{halted}\}; \text{odd } i \rrbracket \implies i \in \text{Step-class } \{\text{red-step}, \text{bblue-step}, \text{dboost-step}\}$
 ⟨proof⟩

lemma *not-halted-even-dreg*: $\llbracket i \notin \text{Step-class } \{\text{halted}\}; \text{even } i \rrbracket \implies i \in \text{Step-class } \{\text{dreg-step}\}$
 ⟨proof⟩

lemma *step-before-dreg*:
 assumes $\text{Suc } i \in \text{Step-class } \{\text{dreg-step}\}$
 shows $i \in \text{Step-class } \{\text{red-step}, \text{bblue-step}, \text{dboost-step}\}$
 ⟨proof⟩

lemma *dreg-before-step*:
 assumes $\text{Suc } i \in \text{Step-class } \{\text{red-step}, \text{bblue-step}, \text{dboost-step}\}$
 shows $i \in \text{Step-class } \{\text{dreg-step}\}$
 ⟨proof⟩

lemma
 assumes $i \in \text{Step-class } \{\text{red-step}, \text{bblue-step}, \text{dboost-step}\}$
 shows *dreg-before-step'*: $i - \text{Suc } 0 \in \text{Step-class } \{\text{dreg-step}\}$
 and *dreg-before-gt0*: $i > 0$
 ⟨proof⟩

lemma *dreg-before-step1*:
 assumes $i \in \text{Step-class } \{\text{red-step}, \text{bblue-step}, \text{dboost-step}\}$
 shows $i - 1 \in \text{Step-class } \{\text{dreg-step}\}$
 ⟨proof⟩

lemma *step-odd-minus2*:
 assumes $i \in \text{Step-class } \{\text{red-step}, \text{bblue-step}, \text{dboost-step}\}$ $i > 1$
 shows $i - 2 \in \text{Step-class } \{\text{red-step}, \text{bblue-step}, \text{dboost-step}\}$
 ⟨proof⟩

lemma *Step-class-iterates*:
 assumes *finite* ($\text{Step-class } \{knd\}$)
 obtains n where $\text{Step-class } \{knd\} = \{m. m < n \wedge \text{stepper-kind } m = knd\}$
 ⟨proof⟩

lemma *step-non-terminating-iff*:
 $i \in \text{Step-class } \{\text{red-step}, \text{bblue-step}, \text{dboost-step}, \text{dreg-step}\}$
 $\longleftrightarrow \neg \text{termination-condition } (Xseq\ i) (Yseq\ i)$
 ⟨proof⟩

lemma *step-terminating-iff*:
 $i \in \text{Step-class } \{\text{halted}\} \longleftrightarrow \text{termination-condition } (Xseq\ i) (Yseq\ i)$

<proof>

lemma *not-many-bluish*:

assumes $i \in \text{Step-class } \{\text{red-step}, \text{dboost-step}\}$

shows $\neg \text{many-bluish } (X\text{seq } i)$

<proof>

lemma *stepper-XYseq*: $\text{stepper } i = (X, Y, A, B) \implies X = X\text{seq } i \wedge Y = Y\text{seq } i$

<proof>

lemma *cvx-works*:

assumes $i \in \text{Step-class } \{\text{red-step}, \text{dboost-step}\}$

shows $\text{central-vertex } (X\text{seq } i) (\text{cvx } i)$

$\wedge \text{weight } (X\text{seq } i) (Y\text{seq } i) (\text{cvx } i) = \text{max-central-vx } (X\text{seq } i) (Y\text{seq } i)$

<proof>

lemma *cvx-in-Xseq*:

assumes $i \in \text{Step-class } \{\text{red-step}, \text{dboost-step}\}$

shows $\text{cvx } i \in X\text{seq } i$

<proof>

lemma *card-Xseq-pos*:

assumes $i \in \text{Step-class } \{\text{red-step}, \text{dboost-step}\}$

shows $\text{card } (X\text{seq } i) > 0$

<proof>

lemma *beta-le*:

assumes $i \in \text{Step-class } \{\text{red-step}, \text{dboost-step}\}$

shows $\text{beta } i \leq \mu$

<proof>

2.10 Termination proof

Each step decreases the size of X

lemma *ex-nonempty-blue-book*:

assumes $mb: \text{many-bluish } X$

shows $\exists x \in X. \text{good-blue-book } X (\{x\}, \text{Neighbours Blue } x \cap X)$

<proof>

lemma *choose-blue-book-psubset*:

assumes $\text{many-bluish } X$ **and** $ST: \text{choose-blue-book } (X, Y, A, B) = (S, T)$

and $\text{finite } X$

shows $T \neq X$

<proof>

lemma *next-state-smaller*:

assumes $\text{next-state } (X, Y, A, B) = (X', Y', A', B')$

and $\text{finite } X$ **and** $\text{nont}: \neg \text{termination-condition } X Y$

shows $X' \subset X$

$\langle proof \rangle$

lemma *do-next-state*:

assumes $odd\ i \neg\ termination\ condition\ (Xseq\ i)\ (Yseq\ i)$
obtains $A\ B\ A'\ B'$ **where** $next\ state\ (Xseq\ i,\ Yseq\ i,\ A,\ B)$
 $=\ (Xseq\ (Suc\ i),\ Yseq\ (Suc\ i),\ A',\ B')$

$\langle proof \rangle$

lemma *step-bound*:

assumes $i:\ Suc\ (2*i) \in\ Step\ class\ \{red\ step,\ bblue\ step,\ dboost\ step\}$
shows $card\ (Xseq\ (Suc\ (2*i))) + i \leq card\ X0$

$\langle proof \rangle$

lemma *Step-class-halted-nonempty*: $Step\ class\ \{halted\} \neq \{\}$

$\langle proof \rangle$

definition *halted-point* $\equiv Inf\ (Step\ class\ \{halted\})$

lemma *halted-point-halted*: $halted\ point \in Step\ class\ \{halted\}$

$\langle proof \rangle$

lemma *halted-point-minimal*:

shows $i \notin Step\ class\ \{halted\} \longleftrightarrow i < halted\ point$

$\langle proof \rangle$

lemma *halted-point-minimal'*: $stepper\ kind\ i \neq halted \longleftrightarrow i < halted\ point$

$\langle proof \rangle$

lemma *halted-eq-Compl*:

$Step\ class\ \{dreg\ step,\ red\ step,\ bblue\ step,\ dboost\ step\} = -\ Step\ class\ \{halted\}$

$\langle proof \rangle$

lemma *before-halted-eq*:

shows $\{.. < halted\ point\} = Step\ class\ \{dreg\ step,\ red\ step,\ bblue\ step,\ dboost\ step\}$

$\langle proof \rangle$

lemma *finite-components*:

shows $finite\ (Step\ class\ \{dreg\ step,\ red\ step,\ bblue\ step,\ dboost\ step\})$

$\langle proof \rangle$

lemma

shows $dreg\ step\ finite\ [simp]: finite\ (Step\ class\ \{dreg\ step\})$

and $red\ step\ finite\ [simp]: finite\ (Step\ class\ \{red\ step\})$

and $bblue\ step\ finite\ [simp]: finite\ (Step\ class\ \{bblue\ step\})$

and $dboost\ step\ finite\ [simp]: finite\ (Step\ class\ \{dboost\ step\})$

$\langle proof \rangle$

lemma *halted-stepper-add-eq*: $stepper\ (halted\ point + i) = stepper\ (halted\ point)$

$\langle proof \rangle$

lemma *halted-stepper-eq*:
assumes $i: i \geq \text{halted-point}$
shows $\text{stepper } i = \text{stepper } (\text{halted-point})$
 $\langle \text{proof} \rangle$

lemma *below-halted-point-cardX*:
assumes $i < \text{halted-point}$
shows $\text{card } (X\text{seq } i) > 0$
 $\langle \text{proof} \rangle$

end

sublocale $\text{Book}' \subseteq \text{Book}$ **where** $\mu = \gamma$
 $\langle \text{proof} \rangle$

lemma (**in** Book) Book' :
assumes $\gamma = \text{real } l / (\text{real } k + \text{real } l)$
shows $\text{Book}' \text{ V E } p0\text{-min Red Blue } l \ k \ \gamma \ X0 \ Y0$
 $\langle \text{proof} \rangle$

end

3 Big Blue Steps: theorems

theory *Big-Blue-Steps* **imports** Book

begin

3.1 Preliminaries

A bounded increasing sequence of finite sets eventually terminates

lemma *Union-incseq-finite*:
assumes $\text{fin}: \bigwedge n. \text{finite } (A \ n)$ **and** $N: \bigwedge n. \text{card } (A \ n) < N$ **and** $\text{incseq } A$
shows $\forall_F k \text{ in sequentially. } \bigcup (\text{range } A) = A \ k$
 $\langle \text{proof} \rangle$

Two lemmas for proving "bigness lemmas" over a closed interval

lemma *eventually-all-geI0*:
assumes $\forall_F l \text{ in sequentially. } P \ a \ l$
 $\bigwedge l \ x. \llbracket P \ a \ l; a \leq x; x \leq b; l \geq L \rrbracket \implies P \ x \ l$
shows $\forall_F l \text{ in sequentially. } \forall x. a \leq x \wedge x \leq b \longrightarrow P \ x \ l$
 $\langle \text{proof} \rangle$

lemma *eventually-all-geI1*:
assumes $\forall_F l \text{ in sequentially. } P \ b \ l$
 $\bigwedge l \ x. \llbracket P \ b \ l; a \leq x; x \leq b; l \geq L \rrbracket \implies P \ x \ l$
shows $\forall_F l \text{ in sequentially. } \forall x. a \leq x \wedge x \leq b \longrightarrow P \ x \ l$

<proof>

Mehta's binomial function: convex on the entire real line and coinciding with gchoose under weak conditions

definition *mfact* $\equiv \lambda a k. \text{if } a < \text{real } k - 1 \text{ then } 0 \text{ else prod } (\lambda i. a - \text{of-nat } i) \{0..<k\}$

Mehta's special rule for convexity, my proof

lemma *convex-on-extend*:

fixes *f* :: *real* \Rightarrow *real*

assumes *cf*: *convex-on* {*k..*} *f* **and** *mon*: *mono-on* {*k..*} *f*

and *fk*: $\bigwedge x. x < k \implies f x = f k$

shows *convex-on UNIV* *f*

<proof>

lemma *convex-mfact*:

assumes *k* > 0

shows *convex-on UNIV* ($\lambda a. \text{mfact } a k$)

<proof>

definition *mbinomial* :: *real* \Rightarrow *nat* \Rightarrow *real*

where *mbinomial* $\equiv \lambda a k. \text{mfact } a k / \text{fact } k$

lemma *convex-mbinomial*: *k* > 0 \implies *convex-on UNIV* ($\lambda x. \text{mbinomial } x k$)

<proof>

lemma *mbinomial-eq-choose* [*simp*]: *mbinomial* (*real n*) *k* = *n choose k*

<proof>

lemma *mbinomial-eq-gchoose* [*simp*]: *k* \leq *a* \implies *mbinomial a k* = *a gchoose k*

<proof>

3.2 Preliminaries: Fact D1

from appendix D, page 55

lemma *Fact-D1-73-aux*:

fixes σ ::*real* **and** *m b*::*nat*

assumes σ : $0 < \sigma$ **and** *bm*: *real b* < *real m*

shows $((\sigma * m) \text{ gchoose } b) * \text{inverse } (m \text{ gchoose } b) = \sigma ^ b * (\prod_{i < b. 1 - ((1 - \sigma) * i) / (\sigma * (\text{real } m - \text{real } i))}$

<proof>

This is fact 4.2 (page 11) as well as equation (73), page 55.

lemma *Fact-D1-73*:

fixes σ ::*real* **and** *m b*::*nat*

assumes σ : $0 < \sigma \leq 1$ **and** *b*: *real b* $\leq \sigma * m / 2$

shows $(\sigma * m) \text{ gchoose } b \in \{\sigma ^ b * (m \text{ gchoose } b) * \text{exp } (- (\text{real } b)^2 / (\sigma * m)) .. \sigma ^ b * (m \text{ gchoose } b)\}$

<proof>

Exact at zero, so cannot be done entirely using the approximation method

lemma *exp-inequality-17*:

fixes $x::\text{real}$

assumes $0 \leq x \leq 1/7$

shows $1 - 4*x/3 \geq \exp(-3*x/2)$

<proof>

additional part

lemma *Fact-D1-75*:

fixes $\sigma::\text{real}$ **and** $m b::\text{nat}$

assumes $\sigma: 0 < \sigma < 1$ **and** $b: \text{real } b \leq \sigma * m / 2$ **and** $b': b \leq m/7$ **and** $\sigma': \sigma \geq 7/15$

shows $(\sigma*m) \text{ gchoose } b \geq \exp(- (3 * \text{real } b^2) / (4*m)) * \sigma^b * (m \text{ gchoose } b)$

<proof>

lemma *power2-12*: $m \geq 12 \implies 25 * m^2 \leq 2^m$

<proof>

How b and m are obtained from l

definition *b-of* **where** $b\text{-of} \equiv \lambda l::\text{nat}. \text{nat}[l \text{ powr } (1/4)]$

definition *m-of* **where** $m\text{-of} \equiv \lambda l::\text{nat}. \text{nat}[l \text{ powr } (2/3)]$

definition *Big-Blue-4-1* \equiv

$\lambda \mu l. m\text{-of } l \geq 12 \wedge l \geq (6/\mu) \text{ powr } (12/5) \wedge l \geq 15$

$\wedge 1 \leq 5/4 * \exp(- \text{real}((b\text{-of } l)^2) / ((\mu - 2/l) * m\text{-of } l)) \wedge \mu > 2/l$

$\wedge 2/l \leq (\mu - 2/l) * ((5/4) \text{ powr } (1/b\text{-of } l) - 1)$

Establishing the size requirements for 4.1. NOTE: it doesn't become clear until SECTION 9 that all bounds involving the parameter μ must hold for a RANGE of values

lemma *Big-Blue-4-1*:

assumes $0 < \mu$

shows $\forall^\infty l. \forall \mu. \mu \in \{\mu 0.. \mu 1\} \longrightarrow \text{Big-Blue-4-1 } \mu l$

<proof>

context *Book*

begin

lemma *Blue-4-1*:

assumes $X \subseteq V$ **and** *manyb*: *many-bluish* X **and** *big*: *Big-Blue-4-1* μl

shows $\exists S T. \text{good-blue-book } X(S, T) \wedge \text{card } S \geq l \text{ powr } (1/4)$

<proof>

Lemma 4.3

proposition *bblue-step-limit*:

assumes *big*: *Big-Blue-4-1* μl

shows $\text{card } (\text{Step-class } \{\text{bblue-step}\}) \leq l \text{ powr } (3/4)$

<proof>

lemma *red-steps-eq-A:*

defines $REDS \equiv \lambda r. \{i. i < r \wedge \text{stepper-kind } i = \text{red-step}\}$

shows $\text{card}(REDS\ n) = \text{card}\ (Aseq\ n)$

<proof>

proposition *red-step-eq-Aseq:* $\text{card}\ (\text{Step-class}\ \{\text{red-step}\}) = \text{card}\ (Aseq\ \text{halted-point})$

<proof>

proposition *red-step-limit:* $\text{card}\ (\text{Step-class}\ \{\text{red-step}\}) < k$

<proof>

proposition *bblue-dboost-step-limit:*

assumes *big:* $Big\text{-Blue-4-1}\ \mu\ l$

shows $\text{card}\ (\text{Step-class}\ \{\text{bblue-step}\}) + \text{card}\ (\text{Step-class}\ \{\text{dboost-step}\}) < l$

<proof>

end

end

4 Red Steps: theorems

theory *Red-Steps* **imports** *Big-Blue-Steps*

begin

Bhavik Mehta: choose-free Ramsey lower bound that's okay for very small

p

lemma *Ramsey-number-lower-simple:*

fixes $p::\text{real}$

assumes $n: n^k * p \text{ powr } (k^2 / 4) + n^l * \text{exp } (-p * l^2 / 4) < 1$

assumes $p01: 0 < p < 1$ **and** $k > 1\ l > 1$

shows $\neg \text{is-Ramsey-number } k\ l\ n$

<proof>

context *Book*

begin

4.1 Density-boost steps

4.1.1 Observation 5.5

lemma *sum-Weight-ge0:*

assumes $X \subseteq V\ Y \subseteq V\ \text{disjnt } X\ Y$

shows $(\sum x \in X. \sum x' \in X. \text{Weight } X\ Y\ x\ x') \geq 0$

<proof>

end

4.1.2 Lemma 5.6

definition *Big-Red-5-6-Ramsey* \equiv

$$\begin{aligned} & \lambda c l. \text{nat } \lceil \text{real } l \text{ powr } (3/4) \rceil \geq 3 \\ & \wedge (l \text{ powr } (3/4) * (c - 1/32) \leq -1) \\ & \wedge (\forall k \geq l. k * (c * l \text{ powr } (3/4) * \ln k - k \text{ powr } (7/8) / 4) \leq -1) \end{aligned}$$

establishing the size requirements for 5.6

lemma *Big-Red-5-6-Ramsey*:

assumes $0 < c < 1/32$

shows $\forall^\infty l. \text{Big-Red-5-6-Ramsey } c l$

<proof>

lemma *Red-5-6-Ramsey*:

assumes $0 < c < 1/32$ **and** $l \leq k$ **and** *big*: *Big-Red-5-6-Ramsey* $c l$

shows $\exp (c * l \text{ powr } (3/4) * \ln k) \leq RN k (\text{nat } \lceil l \text{ powr } (3/4) \rceil)$

<proof>

definition *ineq-Red-5-6* $\equiv \lambda c l. \forall k. l \leq k \longrightarrow \exp (c * \text{real } l \text{ powr } (3/4) * \ln k) \leq RN k (\text{nat } \lceil l \text{ powr } (3/4) \rceil)$

definition *Big-Red-5-6* \equiv

$$\lambda l. 6 + m\text{-of } l \leq (1/128) * l \text{ powr } (3/4) \wedge \text{ineq-Red-5-6 } (1/128) l$$

establishing the size requirements for 5.6

lemma *Big-Red-5-6*: $\forall^\infty l. \text{Big-Red-5-6 } l$

<proof>

lemma (in *Book*) *Red-5-6*:

assumes *big*: *Big-Red-5-6* l

shows $RN k (\text{nat } \lceil l \text{ powr } (3/4) \rceil) \geq k^6 * RN k (m\text{-of } l)$

<proof>

4.2 Lemma 5.4

definition *Big-Red-5-4* $\equiv \lambda l. \text{Big-Red-5-6 } l \wedge (\forall k \geq l. \text{real } k + 2 * \text{real } k^6 \leq \text{real } k^\gamma)$

establishing the size requirements for 5.4

lemma *Big-Red-5-4*: $\forall^\infty l. \text{Big-Red-5-4 } l$

<proof>

context *Book*

begin

lemma *Red-5-4*:

assumes $i: i \in \text{Step-class } \{\text{red-step}, \text{dboost-step}\}$
and $\text{big: Big-Red-5-4 } l$
defines $X \equiv X\text{seq } i$ **and** $Y \equiv Y\text{seq } i$
shows $\text{weight } X \ Y \ (\text{cvx } i) \geq - \text{card } X / (\text{real } k) ^5$
 $\langle \text{proof} \rangle$

lemma *Red-5-7a*: $\varepsilon / k \leq \text{alpha } (\text{hgt } p)$
 $\langle \text{proof} \rangle$

lemma *Red-5-7b*:
assumes $p \geq \text{qfun } 0$ **shows** $\text{alpha } (\text{hgt } p) \leq \varepsilon * (p - \text{qfun } 0 + 1/k)$
 $\langle \text{proof} \rangle$

lemma *Red-5-7c*:
assumes $p \leq \text{qfun } 1$ **shows** $\text{alpha } (\text{hgt } p) = \varepsilon / k$
 $\langle \text{proof} \rangle$

lemma *Red-5-8*:
assumes $i: i \in \text{Step-class } \{\text{dreg-step}\}$ **and** $x: x \in X\text{seq } (\text{Suc } i)$
shows $\text{card } (\text{Neighbours } \text{Red } x \cap Y\text{seq } (\text{Suc } i))$
 $\geq (1 - \varepsilon \text{ powr } (1/2)) * \text{pseq } i * (\text{card } (Y\text{seq } (\text{Suc } i)))$
 $\langle \text{proof} \rangle$

corollary *Y-Neighbours-nonempty-Suc*:
assumes $i: i \in \text{Step-class } \{\text{dreg-step}\}$ **and** $x: x \in X\text{seq } (\text{Suc } i)$ **and** $k \geq 2$
shows $\text{Neighbours } \text{Red } x \cap Y\text{seq } (\text{Suc } i) \neq \{\}$
 $\langle \text{proof} \rangle$

corollary *Y-Neighbours-nonempty*:
assumes $i: i \in \text{Step-class } \{\text{red-step}, \text{dboost-step}\}$ **and** $x: x \in X\text{seq } i$ **and** $k \geq 2$
shows $\text{card } (\text{Neighbours } \text{Red } x \cap Y\text{seq } i) > 0$
 $\langle \text{proof} \rangle$

end

4.3 Lemma 5.1

definition *Big-Red-5-1* $\equiv \lambda \mu l. (1 - \mu) * \text{real } l > 1 \wedge l \text{ powr } (5/2) \geq 3 / (1 - \mu)$
 $\wedge l \text{ powr } (1/4) \geq 4$
 $\wedge \text{Big-Red-5-4 } l \wedge \text{Big-Red-5-6 } l$

establishing the size requirements for 5.1

lemma *Big-Red-5-1*:
assumes $\mu 1 < 1$
shows $\forall^\infty l. \forall \mu. \mu \in \{\mu 0 .. \mu 1\} \longrightarrow \text{Big-Red-5-1 } \mu l$
 $\langle \text{proof} \rangle$

context *Book*
begin

lemma *card-cvx-Neighbours*:
assumes $i: i \in \text{Step-class } \{\text{red-step}, \text{dboost-step}\}$
defines $x \equiv \text{cvx } i$
defines $X \equiv X_{\text{seq}} i$
defines $NBX \equiv \text{Neighbours Blue } x \cap X$
defines $NRX \equiv \text{Neighbours Red } x \cap X$
shows $\text{card } NBX \leq \mu * \text{card } X$ $\text{card } NRX \geq (1-\mu) * \text{card } X - 1$
 $\langle \text{proof} \rangle$

lemma *Red-5-1*:
assumes $i: i \in \text{Step-class } \{\text{red-step}, \text{dboost-step}\}$
and $\text{Big: Big-Red-5-1 } \mu l$
defines $p \equiv p_{\text{seq}} i$
defines $x \equiv \text{cvx } i$
defines $X \equiv X_{\text{seq}} i$ **and** $Y \equiv Y_{\text{seq}} i$
defines $NBX \equiv \text{Neighbours Blue } x \cap X$
defines $NRX \equiv \text{Neighbours Red } x \cap X$
defines $NRX \equiv \text{Neighbours Red } x \cap X$
defines $NRX \equiv \text{Neighbours Red } x \cap Y$
defines $\beta \equiv \text{card } NBX / \text{card } X$
shows $\text{red-density } NRX \text{ } NRX \geq p - \text{alpha } (\text{hgt } p)$
 $\vee \text{red-density } NBX \text{ } NRX \geq p + (1 - \varepsilon) * ((1-\beta) / \beta) * \text{alpha } (\text{hgt } p) \wedge \beta$
 > 0
 $\langle \text{proof} \rangle$

This and the previous result are proved under the assumption of a sufficiently large l

corollary *Red-5-2*:
assumes $i: i \in \text{Step-class } \{\text{dboost-step}\}$
and $\text{Big: Big-Red-5-1 } \mu l$
shows $p_{\text{seq}} (\text{Suc } i) - p_{\text{seq}} i \geq (1 - \varepsilon) * ((1 - \text{beta } i) / \text{beta } i) * \text{alpha } (\text{hgt } (p_{\text{seq}} i)) \wedge$
 $\text{beta } i > 0$
 $\langle \text{proof} \rangle$

end

4.4 Lemma 5.3

This is a weaker consequence of the previous results

definition

Big-Red-5-3 \equiv
 $\lambda \mu l. \text{Big-Red-5-1 } \mu l$
 $\wedge (\forall k \geq l. k > 1 \wedge 1 / (\text{real } k)^2 \leq \mu \wedge 1 / (\text{real } k)^2 \leq 1 / (k / \text{eps } k / (1 - \text{eps } k) + 1))$

establishing the size requirements for 5.3. The one involving μ , namely $1 / (\text{real } k)^2 \leq \mu$, will be useful later with "big beta".

lemma *Big-Red-5-3*:
assumes $0 < \mu < 1$ $\mu < 1$

shows $\forall^{\infty} l. \forall \mu. \mu \in \{\mu 0.. \mu 1\} \longrightarrow \text{Big-Red-5-3 } \mu l$
 $\langle \text{proof} \rangle$

context *Book*
begin

corollary *Red-5-3*:

assumes $i: i \in \text{Step-class } \{\text{dboost-step}\}$
and $\text{big}: \text{Big-Red-5-3 } \mu l$
shows $\text{pseq } (\text{Suc } i) \geq \text{pseq } i \wedge \text{beta } i \geq 1 / (\text{real } k)^2$
 $\langle \text{proof} \rangle$

corollary *beta-gt0*:

assumes $i \in \text{Step-class } \{\text{dboost-step}\}$
and $\text{Big-Red-5-3 } \mu l$
shows $\text{beta } i > 0$
 $\langle \text{proof} \rangle$

end

end

5 Bounding the Size of Y

theory *Bounding-Y* **imports** *Red-Steps*

begin

yet another telescope variant, with weaker promises but a different conclusion; as written it holds even if $n = 0$

lemma *prod-lessThan-telescope-mult*:

fixes $f::\text{nat} \Rightarrow 'a::\text{field}$
assumes $\bigwedge i. i < n \implies f i \neq 0$
shows $(\prod i < n. f (\text{Suc } i) / f i) * f 0 = f n$
 $\langle \text{proof} \rangle$

5.1 The following results together are Lemma 6.4

Compared with the paper, all the indices are greater by one!!

context *Book*
begin

lemma *Y-6-4-Red*:

assumes $i \in \text{Step-class } \{\text{red-step}\}$
shows $\text{pseq } (\text{Suc } i) \geq \text{pseq } i - \text{alpha } (\text{hgt } (\text{pseq } i))$
 $\langle \text{proof} \rangle$

lemma *Y-6-4-DegreeReg*:

assumes $i \in \text{Step-class } \{\text{dreg-step}\}$
shows $\text{pseq } (\text{Suc } i) \geq \text{pseq } i$
 $\langle \text{proof} \rangle$

lemma *Y-6-4-Bblue*:

assumes $i: i \in \text{Step-class } \{\text{bblue-step}\}$
shows $\text{pseq } (\text{Suc } i) \geq \text{pseq } (i-1) - (\varepsilon \text{ powr } (-1/2)) * \text{alpha } (\text{hgt } (\text{pseq } (i-1)))$
 $\langle \text{proof} \rangle$

The basic form is actually *Red-5-3*. This variant covers a gap of two, thanks to degree regularisation

corollary *Y-6-4-dbooSt*:

assumes $i: i \in \text{Step-class } \{\text{dboost-step}\}$ **and** *big*: *Big-Red-5-3* μl
shows $\text{pseq } (\text{Suc } i) \geq \text{pseq } (i-1)$
 $\langle \text{proof} \rangle$

5.2 Towards Lemmas 6.3

definition *Z-class* $\equiv \{i \in \text{Step-class } \{\text{red-step}, \text{bblue-step}, \text{dboost-step}\}.$
 $\text{pseq } (\text{Suc } i) < \text{pseq } (i-1) \wedge \text{pseq } (i-1) \leq p0\}$

lemma *finite-Z-class*: *finite* (*Z-class*)
 $\langle \text{proof} \rangle$

lemma *Y-6-3*:

assumes *big53*: *Big-Red-5-3* μl **and** *big41*: *Big-Blue-4-1* μl
shows $(\sum i \in \text{Z-class}. \text{pseq } (i-1) - \text{pseq } (\text{Suc } i)) \leq 2 * \varepsilon$
 $\langle \text{proof} \rangle$

5.3 Lemma 6.5

lemma *Y-6-5-Red*:

assumes $i: i \in \text{Step-class } \{\text{red-step}\}$ **and** $k \geq 16$
defines $h \equiv \lambda i. \text{hgt } (\text{pseq } i)$
shows $h (\text{Suc } i) \geq h i - 2$
 $\langle \text{proof} \rangle$

lemma *Y-6-5-DegreeReg*:

assumes $i \in \text{Step-class } \{\text{dreg-step}\}$
shows $\text{hgt } (\text{pseq } (\text{Suc } i)) \geq \text{hgt } (\text{pseq } i)$
 $\langle \text{proof} \rangle$

corollary *Y-6-5-dbooSt*:

assumes $i \in \text{Step-class } \{\text{dboost-step}\}$ **and** *Big-Red-5-3* μl
shows $\text{hgt } (\text{pseq } (\text{Suc } i)) \geq \text{hgt } (\text{pseq } i)$
 $\langle \text{proof} \rangle$

this remark near the top of page 19 only holds in the limit

lemma $\forall^\infty k. (1 + \text{eps } k) \text{ powr } (- \text{real } (\text{nat } [2 * \text{eps } k \text{ powr } (-1/2)])) \leq 1 - \text{eps } k \text{ powr } (1/2)$

<proof>

end

definition *Big-Y-6-5-Bblue* \equiv

$\lambda l. \forall k \geq l. (1 + \text{eps } k) \text{ powr } (- \text{real } (\text{nat } \lfloor 2 * (\text{eps } k \text{ powr } (-1/2)) \rfloor)) \leq 1 - \text{eps } k \text{ powr } (1/2)$

establishing the size requirements for Y 6.5

lemma *Big-Y-6-5-Bblue*:

shows $\forall^\infty l. \text{Big-Y-6-5-Bblue } l$

<proof>

lemma (in *Book*) *Y-6-5-Bblue*:

fixes $\kappa :: \text{real}$

defines $\kappa \equiv \varepsilon \text{ powr } (-1/2)$

assumes $i: i \in \text{Step-class } \{\text{bblue-step}\}$ **and** $\text{big}: \text{Big-Y-6-5-Bblue } l$

defines $h \equiv \text{hgt } (\text{pseq } (i-1))$

shows $\text{hgt } (\text{pseq } (\text{Suc } i)) \geq h - 2 * \kappa$

<proof>

5.4 Lemma 6.2

definition *Big-Y-6-2* $\equiv \lambda \mu l. \text{Big-Y-6-5-Bblue } l \wedge \text{Big-Red-5-3 } \mu l \wedge \text{Big-Blue-4-1 } \mu l$

$\wedge (\forall k \geq l. ((1 + \text{eps } k)^2) * \text{eps } k \text{ powr } (1/2) \leq 1$
 $\wedge (1 + \text{eps } k) \text{ powr } (2 * \text{eps } k \text{ powr } (-1/2)) \leq 2 \wedge k \geq 16)$

establishing the size requirements for 6.2

lemma *Big-Y-6-2*:

assumes $0 < \mu 0 \ \mu 1 < 1$

shows $\forall^\infty l. \forall \mu. \mu \in \{\mu 0 .. \mu 1\} \longrightarrow \text{Big-Y-6-2 } \mu l$

<proof>

context *Book*

begin

Following Bhavik in excluding the even steps (degree regularisation). Assuming it hasn't halted, the conclusion also holds for the even cases anyway.

proposition *Y-6-2*:

defines $RBS \equiv \text{Step-class } \{\text{red-step}, \text{bblue-step}, \text{dboost-step}\}$

assumes $j: j \in RBS$ **and** $\text{big}: \text{Big-Y-6-2 } \mu l$

shows $\text{pseq } (\text{Suc } j) \geq p0 - 3 * \varepsilon$

<proof>

corollary *Y-6-2-halted*:

assumes $\text{big}: \text{Big-Y-6-2 } \mu l$

shows $\text{pseq halted-point} \geq p0 - 3 * \varepsilon$

<proof>

end

5.5 Lemma 6.1

context *P0-min*

begin

definition *ok-fun-61* $\equiv \lambda k. (2 * \text{real } k) * \log 2 (1 - 2 * \text{eps } k \text{ powr } (1/2) / p0\text{-min})$

lemma *ok-fun-61-works*:

assumes $p0\text{-min} > 2 * \text{eps } k \text{ powr } (1/2)$

shows $2 \text{ powr } (ok\text{-fun-61 } k) = (1 - 2 * (\text{eps } k) \text{ powr } (1/2) / p0\text{-min}) ^ (2*k)$
<proof>

lemma *ok-fun-61*: $ok\text{-fun-61} \in o(\text{real})$

<proof>

definition

Big-Y-6-1 \equiv

$\lambda \mu l. \text{Big-Y-6-2 } \mu l \wedge (\forall k \geq l. \text{eps } k \text{ powr } (1/2) \leq 1/3 \wedge p0\text{-min} > 2 * \text{eps } k \text{ powr } (1/2))$

establishing the size requirements for 6.1

lemma *Big-Y-6-1*:

assumes $0 < \mu 0 \ \mu 1 < 1$

shows $\forall^\infty l. \forall \mu. \mu \in \{\mu 0 .. \mu 1\} \longrightarrow \text{Big-Y-6-1 } \mu l$
<proof>

end

lemma (in *Book*) *Y-6-1*:

assumes *big*: *Big-Y-6-1* μl

defines *st* $\equiv \text{Step-class } \{\text{red-step}, \text{dboost-step}\}$

shows $\text{card } (Y\text{seq halted-point}) / \text{card } Y 0 \geq 2 \text{ powr } (ok\text{-fun-61 } k) * p0 ^ \text{card } st$
<proof>

end

6 Bounding the Size of X

theory *Bounding-X* imports *Bounding-Y*

begin

6.1 Preliminaries

lemma *sum-odds-even*:

fixes $f :: nat \Rightarrow 'a :: ab\text{-group-add}$
assumes $even\ m$
shows $(\sum i \in \{i. i < m \wedge odd\ i\}. f\ (Suc\ i) - f\ (i - Suc\ 0)) = f\ m - f\ 0$
 $\langle proof \rangle$

lemma *sum-odds-odd*:

fixes $f :: nat \Rightarrow 'a :: ab\text{-group-add}$
assumes $odd\ m$
shows $(\sum i \in \{i. i < m \wedge odd\ i\}. f\ (Suc\ i) - f\ (i - Suc\ 0)) = f\ (m-1) - f\ 0$
 $\langle proof \rangle$

context *Book*

begin

the set of moderate density-boost steps (page 20)

definition *dboost-star* **where**

$dboost\text{-star} \equiv \{i \in Step\text{-class}\ \{dboost\text{-step}\}. real\ (hgt\ (pseq\ (Suc\ i))) - hgt\ (pseq\ i) \leq \varepsilon\ powr\ (-1/4)\}$

definition *bigbeta* **where**

$bigbeta \equiv let\ S = dboost\text{-star}\ in\ if\ S = \{\}\ then\ \mu\ else\ (card\ S) * inverse\ (\sum i \in S. inverse\ (beta\ i))$

lemma *dboost-star-subset*: $dboost\text{-star} \subseteq Step\text{-class}\ \{dboost\text{-step}\}$

$\langle proof \rangle$

lemma *finite-dboost-star*: $finite\ (dboost\text{-star})$

$\langle proof \rangle$

lemma *bigbeta-ge0*: $bigbeta \geq 0$

$\langle proof \rangle$

lemma *bigbeta-ge-square*:

assumes $big: Big\text{-Red-5-3}\ \mu\ l$

shows $bigbeta \geq 1 / (real\ k)^2$

$\langle proof \rangle$

lemma *bigbeta-gt0*:

assumes $big: Big\text{-Red-5-3}\ \mu\ l$

shows $bigbeta > 0$

$\langle proof \rangle$

lemma *bigbeta-less1*:

assumes $big: Big\text{-Red-5-3}\ \mu\ l$

shows $bigbeta < 1$

$\langle proof \rangle$

lemma *bigbeta-le*:
assumes *big*: *Big-Red-5-3* μ l
shows *bigbeta* $\leq \mu$
 \langle *proof* \rangle

end

6.2 Lemma 7.2

definition *Big-X-7-2* $\equiv \lambda \mu l. \text{nat } \lceil \text{real } l \text{ powr } (3/4) \rceil \geq 3 \wedge l > 1 / (1-\mu)$
 establishing the size requirements for 7.11

lemma *Big-X-7-2*:
assumes $0 < \mu < 1$
shows $\forall^\infty l. \forall \mu. \mu \in \{\mu 0 .. \mu 1\} \longrightarrow \text{Big-X-7-2 } \mu l$
 \langle *proof* \rangle

definition *ok-fun-72* $\equiv \lambda \mu k. (\text{real } k / \ln 2) * \ln (1 - 1 / (k * (1-\mu)))$

lemma *ok-fun-72*:
assumes $\mu < 1$
shows *ok-fun-72* $\mu \in o(\text{real})$
 \langle *proof* \rangle

lemma *ok-fun-72-uniform*:
assumes $0 < \mu < 1$
assumes $e > 0$
shows $\forall^\infty k. \forall \mu. \mu 0 \leq \mu \wedge \mu \leq \mu 1 \longrightarrow |\text{ok-fun-72 } \mu k| / k \leq e$
 \langle *proof* \rangle

lemma (in *Book*) *X-7-2*:
defines $\mathcal{R} \equiv \text{Step-class } \{\text{red-step}\}$
assumes *big*: *Big-X-7-2* μ l
shows $(\prod_{i \in \mathcal{R}} \text{card } (X\text{seq}(Suc\ i)) / \text{card } (X\text{seq } i)) \geq 2 \text{ powr } (\text{ok-fun-72 } \mu k) * (1-\mu) \wedge \text{card } \mathcal{R}$
 \langle *proof* \rangle

6.3 Lemma 7.3

context *Book*
begin

definition *Bdelta* $\equiv \lambda \mu i. B\text{seq } (Suc\ i) \setminus B\text{seq } i$

lemma *card-Bdelta*: $\text{card } (B\text{delta } \mu\ i) = \text{card } (B\text{seq } (Suc\ i)) - \text{card } (B\text{seq } i)$
 \langle *proof* \rangle

lemma *card-Bseq-mono*: $\text{card } (B\text{seq } (Suc\ i)) \geq \text{card } (B\text{seq } i)$
 \langle *proof* \rangle

lemma *card-Bseq-sum*: $\text{card} (Bseq\ i) = (\sum j < i. \text{card} (Bdelta\ \mu\ j))$
 ⟨proof⟩

definition *get-blue-book* $\equiv \lambda i. \text{let } (X, Y, A, B) = \text{stepper } i \text{ in choose-blue-book } (X, Y, A, B)$

Tracking changes to X and B. The sets are necessarily finite

lemma *Bdelta-bblue-step*:

assumes $i \in \text{Step-class } \{\text{bblue-step}\}$

shows $\exists S \subseteq Xseq\ i. Bdelta\ \mu\ i = S$

$\wedge \text{card} (Xseq (Suc\ i)) \geq (\mu \wedge \text{card } S) * \text{card} (Xseq\ i) / 2$

⟨proof⟩

lemma *Bdelta-dboost-step*:

assumes $i \in \text{Step-class } \{\text{dboost-step}\}$

shows $\exists x \in Xseq\ i. Bdelta\ \mu\ i = \{x\}$

⟨proof⟩

lemma *card-Bdelta-dboost-step*:

assumes $i \in \text{Step-class } \{\text{dboost-step}\}$

shows $\text{card} (Bdelta\ \mu\ i) = 1$

⟨proof⟩

lemma *Bdelta-trivial-step*:

assumes $i: i \in \text{Step-class } \{\text{red-step}, \text{dreg-step}, \text{halted}\}$

shows $Bdelta\ \mu\ i = \{\}$

⟨proof⟩

end

definition *ok-fun-73* $\equiv \lambda k. - (\text{real } k \text{ powr } (3/4))$

lemma *ok-fun-73*: $ok\text{-fun-73} \in o(\text{real})$

⟨proof⟩

lemma (in *Book*) *X-7-3*:

assumes *big*: $Big\text{-Blue-4-1 } \mu\ l$

defines $\mathcal{B} \equiv \text{Step-class } \{\text{bblue-step}\}$

defines $\mathcal{S} \equiv \text{Step-class } \{\text{dboost-step}\}$

shows $(\prod i \in \mathcal{B}. \text{card} (Xseq(Suc\ i)) / \text{card} (Xseq\ i)) \geq 2 \text{ powr } (ok\text{-fun-73 } k) * \mu \wedge (l - \text{card } \mathcal{S})$

⟨proof⟩

6.4 Lemma 7.5

Small $o(k)$ bounds on summations for this section

This is the explicit upper bound for heights given just below (5) on page 9

definition *ok-fun-26* $\equiv \lambda k. 2 * \ln k / \text{eps } k$

definition *ok-fun-28* $\equiv \lambda k. -2 * \text{real } k \text{ powr } (7/8)$

lemma *ok-fun-26*: *ok-fun-26* $\in o(\text{real})$ **and** *ok-fun-28*: *ok-fun-28* $\in o(\text{real})$
(*proof*)

definition

Big-X-7-5 \equiv
 $\lambda \mu l. \text{Big-Blue-4-1 } \mu l \wedge \text{Big-Red-5-3 } \mu l \wedge \text{Big-Y-6-5-Bblue } l$
 $\wedge (\forall k \geq l. \text{Big-height-upper-bound } k \wedge k \geq 16 \wedge (\text{ok-fun-26 } k - \text{ok-fun-28 } k$
 $\leq k))$

establishing the size requirements for 7.5

lemma *Big-X-7-5*:

assumes $0 < \mu 0 \ \mu 1 < 1$

shows $\forall^\infty l. \forall \mu. \mu \in \{\mu 0 .. \mu 1\} \longrightarrow \text{Big-X-7-5 } \mu l$

(*proof*)

context *Book*

begin

lemma *X-26-and-28*:

assumes *big*: *Big-X-7-5* μl

defines $\mathcal{D} \equiv \text{Step-class } \{\text{dreg-step}\}$

defines $\mathcal{B} \equiv \text{Step-class } \{\text{bblue-step}\}$

defines $\mathcal{H} \equiv \text{Step-class } \{\text{halted}\}$

defines $h \equiv \lambda i. \text{real } (\text{hgt } (\text{pseq } i))$

obtains $(\sum i \in \{.. < \text{halted-point}\} \setminus \mathcal{D}. h (\text{Suc } i) - h (i-1)) \leq \text{ok-fun-26 } k$
 $\text{ok-fun-28 } k \leq (\sum i \in \mathcal{B}. h (\text{Suc } i) - h (i-1))$

(*proof*)

proposition *X-7-5*:

assumes $\mu: 0 < \mu \ \mu < 1$

defines $\mathcal{S} \equiv \text{Step-class } \{\text{dboost-step}\}$ **and** $\mathcal{SS} \equiv \text{dboost-star}$

assumes *big*: *Big-X-7-5* μl

shows $\text{card } (\mathcal{S} \setminus \mathcal{SS}) \leq 3 * \varepsilon \text{ powr } (1/4) * k$

(*proof*)

end

6.5 Lemma 7.4

definition

Big-X-7-4 $\equiv \lambda \mu l. \text{Big-X-7-5 } \mu l \wedge \text{Big-Red-5-3 } \mu l$

establishing the size requirements for 7.4

lemma *Big-X-7-4*:

assumes $0 < \mu 0 \ \mu 1 < 1$

shows $\forall^\infty l. \forall \mu. \mu \in \{\mu 0 .. \mu 1\} \longrightarrow \text{Big-X-7-4 } \mu l$

<proof>

definition *ok-fun-74* $\equiv \lambda k. -6 * \text{eps } k \text{ powr } (1/4) * k * \ln k / \ln 2$

lemma *ok-fun-74*: *ok-fun-74* $\in o(\text{real})$
<proof>

context *Book*
begin

lemma *X-7-4*:
 assumes *big*: *Big-X-7-4* μl
 defines $\mathcal{S} \equiv \text{Step-class } \{\text{dboost-step}\}$
 shows $(\prod i \in \mathcal{S}. \text{card } (X\text{seq } (\text{Suc } i)) / \text{card } (X\text{seq } i)) \geq 2 \text{ powr } \text{ok-fun-74 } k * \text{bigbeta} \wedge \text{card } \mathcal{S}$
<proof>

6.6 Observation 7.7

lemma *X-7-7*:
 assumes *i*: *i* $\in \text{Step-class } \{\text{dreg-step}\}$
 defines $q \equiv \varepsilon \text{ powr } (-1/2) * \text{alpha } (\text{hgt } (\text{pseq } i))$
 shows $\text{pseq } (\text{Suc } i) - \text{pseq } i \geq \text{card } (X\text{seq } i \setminus X\text{seq } (\text{Suc } i)) / \text{card } (X\text{seq } (\text{Suc } i)) * q \wedge \text{card } (X\text{seq } (\text{Suc } i)) > 0$
<proof>

end

6.7 Lemma 7.8

definition *Big-X-7-8* $\equiv \lambda k. k \geq 2 \wedge \text{eps } k \text{ powr } (1/2) / k \geq 2 / k^2$

lemma *Big-X-7-8*: $\forall^\infty k. \text{Big-X-7-8 } k$
<proof>

lemma (*in Book*) *X-7-8*:
 assumes *big*: *Big-X-7-8* k
 and *i*: *i* $\in \text{Step-class } \{\text{dreg-step}\}$
 shows $\text{card } (X\text{seq } (\text{Suc } i)) \geq \text{card } (X\text{seq } i) / k^2$
<proof>

6.8 Lemma 7.9

definition *Big-X-7-9* $\equiv \lambda k. ((1 + \text{eps } k) \text{ powr } (\text{eps } k \text{ powr } (-1/4) + 1) - 1) / \text{eps } k \leq 2 * \text{eps } k \text{ powr } (-1/4) \wedge k \geq 2 \wedge \text{eps } k \text{ powr } (1/2) / k \geq 2 / k^2$

lemma *Big-X-7-9*: $\forall^\infty k. \text{Big-X-7-9 } k$
<proof>

lemma *one-plus-powr-le*:
fixes $p::real$
assumes $0 \leq p \leq 1 \ x \geq 0$
shows $(1+x) \text{ powr } p - 1 \leq x * p$
 $\langle proof \rangle$

lemma (in *Book*) *X-7-9*:
assumes $i: i \in \text{Step-class } \{dreg\text{-step}\}$ **and** $big: \text{Big-X-7-9 } k$
defines $hp \equiv \lambda i. \text{ hgt } (pseq \ i)$
assumes $pseq \ i \geq p0$ **and** $hgt: hp \ (Suc \ i) \leq hp \ i + \varepsilon \text{ powr } (-1/4)$
shows $\text{card } (Xseq \ (Suc \ i)) \geq (1 - 2 * \varepsilon \text{ powr } (1/4)) * \text{card } (Xseq \ i)$
 $\langle proof \rangle$

6.9 Lemma 7.10

definition *Big-X-7-10* $\equiv \lambda \mu \ l. \text{Big-X-7-5 } \mu \ l \wedge \text{Big-Red-5-3 } \mu \ l$
 establishing the size requirements for 7.10

lemma *Big-X-7-10*:
assumes $0 < \mu0 \ \mu1 < 1$
shows $\forall^\infty l. \forall \mu. \mu \in \{\mu0.. \mu1\} \longrightarrow \text{Big-X-7-10 } \mu \ l$
 $\langle proof \rangle$

lemma (in *Book*) *X-7-10*:
defines $\mathcal{R} \equiv \text{Step-class } \{\text{red-step}\}$
defines $\mathcal{S} \equiv \text{Step-class } \{\text{dboost-step}\}$
defines $h \equiv \lambda i. \text{ real } (\text{hgt } (pseq \ i))$
defines $C \equiv \{i. h \ i \geq h \ (i-1) + \varepsilon \text{ powr } (-1/4)\}$
assumes $big: \text{Big-X-7-10 } \mu \ l$
shows $\text{card } ((\mathcal{R} \cup \mathcal{S}) \cap C) \leq 3 * \varepsilon \text{ powr } (1/4) * k$
 $\langle proof \rangle$

6.10 Lemma 7.11

definition *Big-X-7-11-inequalities* $\equiv \lambda k.$
 $\text{eps } k * \text{eps } k \text{ powr } (-1/4) \leq (1 + \text{eps } k) \wedge (2 * \text{nat } \lfloor \text{eps } k \text{ powr } (-1/4) \rfloor) - 1$
 $\wedge k \geq 2 * \text{eps } k \text{ powr } (-1/2) * k \text{ powr } (3/4)$
 $\wedge ((1 + \text{eps } k) * (1 + \text{eps } k) \text{ powr } (2 * \text{eps } k \text{ powr } (-1/4))) \leq 2$
 $\wedge (1 + \text{eps } k) \wedge (\text{nat } \lfloor 2 * \text{eps } k \text{ powr } (-1/4) \rfloor + \text{nat } \lfloor 2 * \text{eps } k \text{ powr } (-1/2) \rfloor - 1) \leq 2$

definition *Big-X-7-11* \equiv
 $\lambda \mu \ l. \text{Big-X-7-5 } \mu \ l \wedge \text{Big-Red-5-3 } \mu \ l \wedge \text{Big-Y-6-5-Bblue } l$
 $\wedge (\forall k. l \leq k \longrightarrow \text{Big-X-7-11-inequalities } k)$

establishing the size requirements for 7.11

lemma *Big-X-7-11*:

assumes $0 < \mu_0 \ \mu_1 < 1$
shows $\forall^\infty l. \forall \mu. \mu \in \{\mu_0.. \mu_1\} \longrightarrow \text{Big-X-7-11 } \mu \ l$
 $\langle \text{proof} \rangle$

lemma (in *Book*) *X-7-11*:

defines $\mathcal{R} \equiv \text{Step-class } \{\text{red-step}\}$
defines $\mathcal{S} \equiv \text{Step-class } \{\text{dboost-step}\}$
defines $C \equiv \{i. \text{pseq } i \geq \text{pseq } (i-1) + \varepsilon \text{ powr } (-1/4) * \text{alpha } 1 \wedge \text{pseq } (i-1) \leq p_0\}$
assumes *big*: *Big-X-7-11* $\mu \ l$
shows $\text{card } ((\mathcal{R} \cup \mathcal{S}) \cap C) \leq 4 * \varepsilon \text{ powr } (1/4) * k$
 $\langle \text{proof} \rangle$

6.11 Lemma 7.12

definition *Big-X-7-12* \equiv

$\lambda \mu \ l. \text{Big-X-7-11 } \mu \ l \wedge \text{Big-X-7-10 } \mu \ l \wedge (\forall k. l \leq k \longrightarrow \text{Big-X-7-9 } k)$

establishing the size requirements for 7.12

lemma *Big-X-7-12*:

assumes $0 < \mu_0 \ \mu_1 < 1$
shows $\forall^\infty l. \forall \mu. \mu \in \{\mu_0.. \mu_1\} \longrightarrow \text{Big-X-7-12 } \mu \ l$
 $\langle \text{proof} \rangle$

lemma (in *Book*) *X-7-12*:

defines $\mathcal{R} \equiv \text{Step-class } \{\text{red-step}\}$
defines $\mathcal{S} \equiv \text{Step-class } \{\text{dboost-step}\}$
defines $C \equiv \{i. \text{card } (X\text{seq } i) < (1 - 2 * \varepsilon \text{ powr } (1/4)) * \text{card } (X\text{seq } (i-1))\}$
assumes *big*: *Big-X-7-12* $\mu \ l$
shows $\text{card } ((\mathcal{R} \cup \mathcal{S}) \cap C) \leq 7 * \varepsilon \text{ powr } (1/4) * k$
 $\langle \text{proof} \rangle$

6.12 Lemma 7.6

definition *Big-X-7-6* \equiv

$\lambda \mu \ l. \text{Big-Blue-4-1 } \mu \ l \wedge \text{Big-X-7-12 } \mu \ l \wedge (\forall k. k \geq l \longrightarrow \text{Big-X-7-8 } k \wedge 1 - 2 * \text{eps } k \text{ powr } (1/4) > 0)$

lemma *Big-X-7-6*:

assumes $0 < \mu_0 \ \mu_1 < 1$
shows $\forall^\infty l. \forall \mu. \mu \in \{\mu_0.. \mu_1\} \longrightarrow \text{Big-X-7-6 } \mu \ l$
 $\langle \text{proof} \rangle$

definition *ok-fun-76* \equiv

$\lambda k. ((1 + 2 * \text{real } k) * \ln (1 - 2 * \text{eps } k \text{ powr } (1/4)) - (k \text{ powr } (3/4) + 7 * \text{eps } k \text{ powr } (1/4) * k + 1) * (2 * \ln k)) / \ln 2$

lemma *ok-fun-76*: *ok-fun-76* $\in o(\text{real})$

$\langle \text{proof} \rangle$

lemma (in *Book*) *X-7-6*:
assumes *big*: *Big-X-7-6* μ l
defines $\mathcal{D} \equiv \text{Step-class } \{\text{dreg-step}\}$
shows $(\prod_{i \in \mathcal{D}} \text{card}(X\text{seq}(\text{Suc } i)) / \text{card}(X\text{seq } i)) \geq 2 \text{ powr } \text{ok-fun-76 } k$
 $\langle \text{proof} \rangle$

6.13 Lemma 7.1

definition *Big-X-7-1* \equiv
 $\lambda \mu l. \text{Big-Blue-4-1 } \mu l \wedge \text{Big-X-7-2 } \mu l \wedge \text{Big-X-7-4 } \mu l \wedge \text{Big-X-7-6 } \mu l$
 establishing the size requirements for 7.11

lemma *Big-X-7-1*:
assumes $0 < \mu < 1$
shows $\forall^\infty l. \forall \mu. \mu \in \{\mu 0.. \mu 1\} \longrightarrow \text{Big-X-7-1 } \mu l$
 $\langle \text{proof} \rangle$

definition *ok-fun-71* $\equiv \lambda \mu k. \text{ok-fun-72 } \mu k + \text{ok-fun-73 } k + \text{ok-fun-74 } k + \text{ok-fun-76 } k$

lemma *ok-fun-71*:
assumes $0 < \mu < 1$
shows *ok-fun-71* $\mu \in o(\text{real})$
 $\langle \text{proof} \rangle$

lemma (in *Book*) *X-7-1*:
assumes *big*: *Big-X-7-1* μ l
defines $\mathcal{D} \equiv \text{Step-class } \{\text{dreg-step}\}$
defines $\mathcal{R} \equiv \text{Step-class } \{\text{red-step}\}$ **and** $\mathcal{S} \equiv \text{Step-class } \{\text{dboost-step}\}$
shows $\text{card}(X\text{seq halted-point}) \geq$
 $2 \text{ powr } \text{ok-fun-71 } \mu k * \mu^l * (1 - \mu)^\wedge \text{card } \mathcal{R} * (\text{bigbeta} / \mu)^\wedge \text{card } \mathcal{S} * \text{card } X0$
 $\langle \text{proof} \rangle$

end

7 The Zigzag Lemma

theory *Zigzag* imports *Bounding-X*

begin

7.1 Lemma 8.1 (the actual Zigzag Lemma)

definition *Big-ZZ-8-2* $\equiv \lambda k. (1 + \text{eps } k \text{ powr } (1/2)) \geq (1 + \text{eps } k) \text{ powr } (\text{eps } k \text{ powr } (-1/4))$

An inequality that pops up in the proof of (39)

definition *Big39* $\equiv \lambda k. 1/2 \leq (1 + \text{eps } k) \text{ powr } (-2 * \text{eps } k \text{ powr } (-1/2))$

Two inequalities that pops up in the proof of (42)

definition $Big42a \equiv \lambda k. (1 + eps\ k)^2 / (1 - eps\ k\ powr\ (1/2)) \leq 1 + 2 * k\ powr\ (-1/16)$

definition $Big42b \equiv \lambda k. 2 * k\ powr\ (-1/16) * k + (1 + 2 * \ln\ k / eps\ k + 2 * k\ powr\ (7/8)) / (1 - eps\ k\ powr\ (1/2)) \leq real\ k\ powr\ (19/20)$

definition $Big-ZZ-8-1 \equiv \lambda \mu\ l. Big-Blue-4-1\ \mu\ l \wedge Big-Red-5-1\ \mu\ l \wedge Big-Red-5-3\ \mu\ l \wedge Big-Y-6-5-Bblue\ l \wedge (\forall k. k \geq l \longrightarrow Big-height-upper-bound\ k \wedge Big-ZZ-8-2\ k \wedge k \geq 16 \wedge Big39\ k \wedge Big42a\ k \wedge Big42b\ k)$

$(16::'a) \leq k$ is for $Y-6-5-Red$

lemma $Big-ZZ-8-1$:

assumes $0 < \mu0\ \mu1 < 1$

shows $\forall^\infty l. \forall \mu. \mu \in \{\mu0.. \mu1\} \longrightarrow Big-ZZ-8-1\ \mu\ l$

$\langle proof \rangle$

lemma (in Book) $ZZ-8-1$:

assumes $big: Big-ZZ-8-1\ \mu\ l$

defines $\mathcal{R} \equiv Step-class\ \{red-step\}$

defines $sum-SS \equiv (\sum_{i \in dboost-star.} (1 - beta\ i) / beta\ i)$

shows $sum-SS \leq card\ \mathcal{R} + k\ powr\ (19/20)$

$\langle proof \rangle$

7.2 Lemma 8.5

An inequality that pops up in the proof of (39)

definition $inequality85 \equiv \lambda k. 3 * eps\ k\ powr\ (1/4) * k \leq k\ powr\ (19/20)$

definition $Big-ZZ-8-5 \equiv$

$\lambda \mu\ l. Big-X-7-5\ \mu\ l \wedge Big-ZZ-8-1\ \mu\ l \wedge Big-Red-5-3\ \mu\ l$

$\wedge (\forall k \geq l. inequality85\ k)$

lemma $Big-ZZ-8-5$:

assumes $0 < \mu0\ \mu1 < 1$

shows $\forall^\infty l. \forall \mu. \mu \in \{\mu0.. \mu1\} \longrightarrow Big-ZZ-8-5\ \mu\ l$

$\langle proof \rangle$

lemma (in Book) $ZZ-8-5$:

assumes $big: Big-ZZ-8-5\ \mu\ l$

defines $\mathcal{R} \equiv Step-class\ \{red-step\}$ **and** $\mathcal{S} \equiv Step-class\ \{dboost-step\}$

shows $card\ \mathcal{S} \leq (bigbeta / (1 - bigbeta)) * card\ \mathcal{R}$

$+ (2 / (1 - \mu)) * k\ powr\ (19/20)$

$\langle proof \rangle$

7.3 Lemma 8.6

For some reason this was harder than it should have been. It does require a further small limit argument.

definition *Big-ZZ-8-6* \equiv

$\lambda \mu l. \text{Big-ZZ-8-5 } \mu l \wedge (\forall k \geq l. 2 / (1 - \mu) * k \text{ powr } (19/20) < k \text{ powr } (39/40))$

lemma *Big-ZZ-8-6*:

assumes $0 < \mu < 1$

shows $\forall \infty l. \forall \mu. \mu \in \{\mu 0 .. \mu 1\} \longrightarrow \text{Big-ZZ-8-6 } \mu l$

<proof>

lemma (in *Book*) *ZZ-8-6*:

assumes *big*: *Big-ZZ-8-6* μl

defines $\mathcal{R} \equiv \text{Step-class } \{\text{red-step}\}$ **and** $\mathcal{S} \equiv \text{Step-class } \{\text{dboost-step}\}$

and $a \equiv 2 / (1 - \mu)$

assumes *s-ge*: $\text{card } \mathcal{S} \geq k \text{ powr } (39/40)$

shows $\text{bigbeta} \geq (1 - a * k \text{ powr } (-1/40)) * (\text{card } \mathcal{S} / (\text{card } \mathcal{S} + \text{card } \mathcal{R}))$

<proof>

end

8 An exponential improvement far from the diagonal

theory *Far-From-Diagonal*

imports *Zigzag Stirling-Formula. Stirling-Formula*

begin

8.1 An asymptotic form for binomial coefficients via Stirling's formula

From Appendix D.3, page 56

lemma *const-smallo-real*: $(\lambda n. x) \in o(\text{real})$

<proof>

lemma *o-real-shift*:

assumes $f \in o(\text{real})$

shows $(\lambda i. f(i+j)) \in o(\text{real})$

<proof>

lemma *tendsto-zero-imp-o1*:

fixes $a :: \text{nat} \Rightarrow \text{real}$

assumes $a \longrightarrow 0$

shows $a \in o(1)$

<proof>

8.2 Fact D.3 from the Appendix

And hence, Fact 9.4

definition $stir \equiv \lambda n. fact\ n / (sqrt\ (2*pi*n) * (n / exp\ 1) ^ n) - 1$

Generalised to the reals to allow derivatives

definition $stirG \equiv \lambda n. Gamma\ (n+1) / (sqrt\ (2*pi*n) * (n / exp\ 1) powr\ n) - 1$

lemma $stir-eq-stirG: n > 0 \implies stir\ n = stirG\ (real\ n)$
 $\langle proof \rangle$

lemma $stir-ge0: n > 0 \implies stir\ n \geq 0$
 $\langle proof \rangle$

lemma $stir-to-0: stir \longrightarrow 0$
 $\langle proof \rangle$

lemma $stir-o1: stir \in o(1)$
 $\langle proof \rangle$

lemma $fact-eq-stir-times: n \neq 0 \implies fact\ n = (1 + stir\ n) * (sqrt\ (2*pi*n) * (n / exp\ 1) ^ n)$
 $\langle proof \rangle$

definition $logstir \equiv \lambda n. if\ n=0\ then\ 0\ else\ log\ 2\ ((1 + stir\ n) * sqrt\ (2*pi*n))$

lemma $logstir-o-real: logstir \in o(real)$
 $\langle proof \rangle$

lemma $logfact-eq-stir-times:$
 $fact\ n = 2\ powr\ (logstir\ n) * (n / exp\ 1) ^ n$
 $\langle proof \rangle$

lemma $mono-G:$
defines $G \equiv (\lambda x::real. Gamma\ (x + 1) / (x / exp\ 1) powr\ x)$
shows $mono-on\ \{0<..\}\ G$
 $\langle proof \rangle$

lemma $mono-logstir: mono\ logstir$
 $\langle proof \rangle$

definition $ok-fun-94 \equiv \lambda k. -\ logstir\ k$

lemma $ok-fun-94: ok-fun-94 \in o(real)$
 $\langle proof \rangle$

lemma $fact-9-4:$
assumes $l: 0 < l \leq k$

defines $\gamma \equiv l / (\text{real } k + \text{real } l)$
shows $k+l \text{ choose } l \geq 2 \text{ powr } ok\text{-fun-94 } k * \gamma \text{ powr } (-l) * (1-\gamma) \text{ powr } (-k)$
 $\langle \text{proof} \rangle$

8.3 Fact D.2

For Fact 9.6

lemma *D2*:

fixes $k \ l$
assumes $t: 0 < t \leq k$
defines $\gamma \equiv l / (\text{real } k + \text{real } l)$
shows $(k+l-t \text{ choose } l) \leq \exp(-\gamma * (t-1)^2 / (2*k)) * (k / (k+l))^t * (k+l \text{ choose } l)$
 $\langle \text{proof} \rangle$

Statement borrowed from Bhavik; no $o(k)$ function

corollary *Far-9-6*:

fixes $k \ l$
assumes $t: 0 < t \leq k$
defines $\gamma \equiv l / (k + \text{real } l)$
shows $\exp(-1) * (1-\gamma) \text{ powr } (-\text{real } t) * \exp(\gamma * (\text{real } t)^2 / \text{real}(2*k)) * (k-t+l \text{ choose } l) \leq (k+l \text{ choose } l)$
 $\langle \text{proof} \rangle$

8.4 Lemma 9.3

definition $ok\text{-fun-93g} \equiv \lambda\gamma \ k. (\text{nat } \lceil k \text{ powr } (3/4) \rceil) * \log 2 \ k - (ok\text{-fun-71 } \gamma \ k + ok\text{-fun-94 } k) + 1$

lemma *ok-fun-93g*:

assumes $0 < \gamma \ \gamma < 1$
shows $ok\text{-fun-93g } \gamma \in o(\text{real})$
 $\langle \text{proof} \rangle$

definition $ok\text{-fun-93h} \equiv \lambda\gamma \ k. (2 / (1-\gamma)) * k \text{ powr } (19/20) * (\ln \gamma + 2 * \ln k) + ok\text{-fun-93g } \gamma \ k * \ln 2$

lemma *ok-fun-93h*:

assumes $0 < \gamma \ \gamma < 1$
shows $ok\text{-fun-93h } \gamma \in o(\text{real})$
 $\langle \text{proof} \rangle$

lemma *ok-fun-93h-uniform*:

assumes $\mu 0 1: 0 < \mu 0 \ \mu 1 < 1$
assumes $e > 0$
shows $\forall^\infty k. \forall \mu. \mu \in \{\mu 0 .. \mu 1\} \longrightarrow |ok\text{-fun-93h } \mu \ k| / k \leq e$
 $\langle \text{proof} \rangle$

context *P0-min*

begin

definition *Big-Far-9-3* \equiv

$\lambda \mu l. \text{Big-ZZ-8-5 } \mu l \wedge \text{Big-X-7-1 } \mu l \wedge \text{Big-Y-6-2 } \mu l \wedge \text{Big-Red-5-3 } \mu l$
 $\wedge (\forall k \geq l. p0\text{-min} - 3 * \text{eps } k > 1/k \wedge k \geq 2$
 $\wedge |\text{ok-fun-93h } \mu k / (\mu * (1 + 1 / (\text{exp } 1 * (1-\mu))))| / k \leq 0.667 -$
 $2/3)$

lemma *Big-Far-9-3*:

assumes $0 < \mu 0 \ \mu 0 \leq \mu 1 \ \mu 1 < 1$
shows $\forall^\infty l. \forall \mu. \mu \in \{\mu 0 .. \mu 1\} \longrightarrow \text{Big-Far-9-3 } \mu l$
{proof}

end

lemma $(\lambda k. (\text{nat } \lceil \text{real } k \text{ powr } (3/4) \rceil) * \log 2 k) \in o(\text{real})$
{proof}

lemma *RN34-le-2powr-ok*:

fixes $l k :: \text{nat}$
assumes $l \leq k \ 0 < k$
defines $l34 \equiv \text{nat } \lceil \text{real } l \text{ powr } (3/4) \rceil$
shows $\text{RN } k \ l34 \leq 2 \text{ powr } (\lceil k \text{ powr } (3/4) \rceil) * \log 2 k$
{proof}

Here n really refers to the cardinality of V , so actually nV

lemma (in *Book'*) *Far-9-3*:

defines $\delta \equiv \min (1/200) (\gamma/20)$
defines $\mathcal{R} \equiv \text{Step-class } \{\text{red-step}\}$
defines $t \equiv \text{card } \mathcal{R}$
assumes $\gamma 15: \gamma \leq 1/5$ **and** $p0: p0 \geq 1/4$
and $nge: n \geq \text{exp } (-\delta * \text{real } k) * (k+l \text{ choose } l)$
and $X0ge: \text{card } X0 \geq n/2$
— Because $n / 2 \leq \text{real } (\text{card } X0)$ makes the proof harder
assumes *big*: *Big-Far-9-3* γl
shows $t \geq 2*k / 3$
{proof}

8.5 Lemma 9.5

context *P0-min*

begin

Again stolen from Bhavik: cannot allow a dependence on γ

definition *ok-fun-95a* $\equiv \lambda k. \text{ok-fun-61 } k - (2 + 4 * k \text{ powr } (19/20))$

definition *ok-fun-95b* $\equiv \lambda k. \ln 2 * \text{ok-fun-95a } k - 1$

lemma *ok-fun-95a*: *ok-fun-95a* $\in o(\text{real})$

{proof}

lemma *ok-fun-95b*: $ok-fun-95b \in o(\text{real})$

<proof>

definition *Big-Far-9-5* $\equiv \lambda\mu l. \text{Big-Red-5-3 } \mu l \wedge \text{Big-Y-6-1 } \mu l \wedge \text{Big-ZZ-8-5 } \mu l$

lemma *Big-Far-9-5*:

assumes $0 < \mu 0 \ \mu 1 < 1$

shows $\forall^\infty l. \forall \mu. \mu 0 \leq \mu \wedge \mu \leq \mu 1 \longrightarrow \text{Big-Far-9-5 } \mu l$

<proof>

end

$Y0$ is an additional assumption found in Bhavik's version. (He had a couple of others). The first $o(k)$ function adjusts for the error in $n/2$

lemma (in *Book'*) *Far-9-5*:

fixes $\delta \ \eta :: \text{real}$

defines $\mathcal{R} \equiv \text{Step-class } \{\text{red-step}\}$

defines $t \equiv \text{card } \mathcal{R}$

assumes $nV: \text{real } nV \geq \text{exp } (-\delta * k) * (k+l \text{ choose } l)$ **and** $Y0: \text{card } Y0 \geq nV \text{ div } 2$

assumes $p0: 1/2 \leq 1-\gamma-\eta \ 1-\gamma-\eta \leq p0$ **and** $0 \leq \eta$

assumes *big*: *Big-Far-9-5* γl

shows $\text{card } (Y \text{seq halted-point}) \geq$

$\text{exp } (-\delta * k + \text{ok-fun-95b } k) * (1-\gamma-\eta) \text{ powr } (\gamma * t / (1-\gamma)) * ((1-\gamma-\eta)/(1-\gamma)) ^ t$

$* \text{exp } (\gamma * (\text{real } t)^2 / (2 * k)) * (k-t+l \text{ choose } l)$ (**is** - \geq ?*rhs*)

<proof>

8.6 Lemma 9.2

context *P0-min*

begin

lemma *error-9-2*:

assumes $\mu > 0 \ d > 0$

shows $\forall^\infty k. \text{ok-fun-95b } k + \mu * \text{real } k / d \geq 0$

<proof>

definition *Big-Far-9-2* $\equiv \lambda\mu l. \text{Big-Far-9-3 } \mu l \wedge \text{Big-Far-9-5 } \mu l \wedge (\forall k \geq l. \text{ok-fun-95b } k + \mu * k / 60 \geq 0)$

lemma *Big-Far-9-2*:

assumes $0 < \mu 0 \ \mu 0 \leq \mu 1 \ \mu 1 < 1$

shows $\forall^\infty l. \forall \mu. \mu 0 \leq \mu \wedge \mu \leq \mu 1 \longrightarrow \text{Big-Far-9-2 } \mu l$

<proof>

end

Used for both 9.2 and 10.2

lemma (in *Book'*) *Off-diagonal-conclusion*:
defines $\mathcal{R} \equiv \text{Step-class } \{\text{red-step}\}$
defines $t \equiv \text{card } \mathcal{R}$
assumes $Y: (k-t+l \text{ choose } l) \leq \text{card } (Y \text{seq halted-point})$
shows *False*
 $\langle \text{proof} \rangle$

A little tricky to express since the Book locale assumes that there are no cliques in the original graph (page 9). So it's a contrapositive

lemma (in *Book'*) *Far-9-2-aux*:
fixes $\delta \eta::\text{real}$
defines $\delta \equiv \gamma/20$
assumes $0: \text{real } (\text{card } X0) \geq nV/2 \text{ card } Y0 \geq nV \text{ div } 2 \text{ p}0 \geq 1-\gamma-\eta$
— These are the assumptions about the red density of the graph
assumes $\gamma: \gamma \leq 1/10$ **and** $\eta: 0 \leq \eta \leq \gamma/15$
assumes $nV: \text{real } nV \geq \exp(-\delta * k) * (k+l \text{ choose } l)$
assumes *big: Big-Far-9-2* $\gamma \ l$
shows *False*
 $\langle \text{proof} \rangle$

Mediation of 9.2 (and 10.2) from locale *Book-Basis* to the book locales with the starting sets of equal size

lemma (in *No-Cliques*) *to-Book*:
assumes $gd: \text{p}0\text{-min} \leq \text{graph-density Red}$
assumes $\mu01: 0 < \mu \ \mu < 1$
obtains $X0 \ Y0$ **where** $l \geq 2 \ \text{card } X0 \geq \text{real } nV / 2 \ \text{card } Y0 = \text{gorder div } 2$
and $X0 = V \setminus Y0 \ Y0 \subseteq V$
and $\text{graph-density Red} \leq \text{gen-density Red } X0 \ Y0$
and *Book* $V \ E \ \text{p}0\text{-min Red Blue } l \ k \ \mu \ X0 \ Y0$
 $\langle \text{proof} \rangle$

Material that needs to be proved **outside** the book locales

As above, for *Book'*

lemma (in *No-Cliques*) *to-Book'*:
assumes $gd: \text{p}0\text{-min} \leq \text{graph-density Red}$
assumes $l: 0 < l \leq k$
obtains $X0 \ Y0$ **where** $l \geq 2 \ \text{card } X0 \geq \text{real } nV / 2 \ \text{card } Y0 = \text{gorder div } 2$ **and**
 $X0 = V \setminus Y0 \ Y0 \subseteq V$
and $\text{graph-density Red} \leq \text{gen-density Red } X0 \ Y0$
and *Book'* $V \ E \ \text{p}0\text{-min Red Blue } l \ k \ (\text{real } l / (\text{real } k + \text{real } l)) \ X0 \ Y0$
 $\langle \text{proof} \rangle$

lemma (in *No-Cliques*) *Far-9-2*:
fixes $\delta \ \gamma \ \eta::\text{real}$
defines $\gamma \equiv l / (\text{real } k + \text{real } l)$
defines $\delta \equiv \gamma/20$
assumes $gd: \text{graph-density Red} \geq 1-\gamma-\eta$ **and** $\text{p}0\text{-min-OK}: \text{p}0\text{-min} \leq 1-\gamma-\eta$

assumes $\gamma \leq 1/10$ **and** $\eta: 0 \leq \eta \leq \gamma/15$
assumes $nV: \text{real } nV \geq \exp(-\delta * k) * (k+l \text{ choose } l)$
assumes *big: Big-Far-9-2* $\gamma \ l$
shows *False*
 <proof>

8.7 Theorem 9.1

An arithmetical lemma proved outside of the locales

lemma *kl-choose*:
fixes $l \ k::\text{nat}$
assumes $m < l \ k > 0$
defines $PM \equiv \prod i < m. (l - \text{real } i) / (k+l - \text{real } i)$
shows $(k+l \text{ choose } l) = (k+l-m \text{ choose } (l-m)) / PM$
 <proof>

context *P0-min*
begin

The proof considers a smaller graph, so l needs to be so big that the smaller l' will be big enough.

definition *Big-Far-9-1* $:: \text{real} \Rightarrow \text{nat} \Rightarrow \text{bool}$ **where**
Big-Far-9-1 $\equiv \lambda \mu \ l. l \geq 3 \wedge (\forall l' \ \gamma. \text{real } l' \geq (10/11) * \mu * \text{real } l \longrightarrow \mu^2 \leq \gamma \wedge \gamma \leq 1/10 \longrightarrow \text{Big-Far-9-2 } \gamma \ l')$

The proof of theorem 10.1 requires a range of values

lemma *Big-Far-9-1*:
assumes $0 < \mu \ \mu \leq 1/10$
shows $\forall^\infty l. \forall \mu. \mu \leq \mu \wedge \mu \leq 1/10 \longrightarrow \text{Big-Far-9-1 } \mu \ l$
 <proof>

The text claims the result for all k and l , not just those sufficiently large, but the $o(k)$ function allowed in the exponent provides a fudge factor

theorem *Far-9-1*:
fixes $l \ k::\text{nat}$
fixes $\delta \ \gamma::\text{real}$
defines $\gamma \equiv \text{real } l / (\text{real } k + \text{real } l)$
defines $\delta \equiv \gamma/20$
assumes $\gamma: \gamma \leq 1/10$
assumes *big: Big-Far-9-1* $\gamma \ l$
assumes *p0-min-91: p0-min* $\leq 1 - (1/10) * (1 + 1/15)$
shows $RN \ k \ l \leq \exp(-\delta * k + 1) * (k+l \text{ choose } l)$
 <proof>

end

end

9 An exponential improvement closer to the diagonal

theory *Closer-To-Diagonal*
imports *Far-From-Diagonal*

begin

9.1 Lemma 10.2

context *P0-min*
begin

lemma *error-10-2*:

assumes $\mu / \text{real } d > 1/200$

shows $\forall^\infty k. \text{ok-fun-95b } k + \mu * \text{real } k / \text{real } d \geq k/200$

<proof>

The "sufficiently large" assumptions are problematical. The proof's calculation for $(3::'a) / (20::'a) < \gamma$ is sharp. We need a finite gap for the limit to exist. We can get away with $1/300$.

definition *x320::real* **where** $x320 \equiv 3/20 + 1/300$

lemma *error-10-2-True*: $\forall^\infty k. \text{ok-fun-95b } k + x320 * \text{real } k / \text{real } 30 \geq k/200$

<proof>

lemma *error-10-2-False*: $\forall^\infty k. \text{ok-fun-95b } k + (1/10) * \text{real } k / \text{real } 15 \geq k/200$

<proof>

definition *Big-Closer-10-2* $\equiv \lambda\mu l. \text{Big-Far-9-3 } \mu l \wedge \text{Big-Far-9-5 } \mu l$

$\wedge (\forall k \geq l. \text{ok-fun-95b } k + (\text{if } \mu > x320 \text{ then } \mu*k/30 \text{ else } \mu*k/15) \geq$

$k/200)$

lemma *Big-Closer-10-2*:

assumes $1/10 \leq \mu1 \ \mu1 < 1$

shows $\forall^\infty l. \forall \mu. 1/10 \leq \mu \wedge \mu \leq \mu1 \longrightarrow \text{Big-Closer-10-2 } \mu l$

<proof>

end

A little tricky to express since the Book locale assumes that there are no cliques in the original graph (page 10). So it's a contrapositive

lemma (in *Book'*) *Closer-10-2-aux*:

assumes $0: \text{real } (\text{card } X0) \geq nV/2 \ \text{card } Y0 \geq nV \ \text{div } 2 \ p0 \geq 1 - \gamma$

— These are the assumptions about the red density of the graph

assumes $\gamma: 1/10 \leq \gamma \ \gamma \leq 1/5$

assumes $nV: \text{real } nV \geq \exp(-k/200) * (k+l \text{ choose } l)$

assumes *big*: *Big-Closer-10-2* γl

shows *False*

<proof>

Material that needs to be proved **outside** the book locales

lemma (in *No-Cliques*) *Closer-10-2*:

fixes $\gamma::\text{real}$

defines $\gamma \equiv l / (\text{real } k + \text{real } l)$

assumes nV : $\text{real } nV \geq \exp(-\text{real } k/200) * (k+l \text{ choose } l)$

assumes gd : *graph-density* $\text{Red} \geq 1-\gamma$ **and** $p0\text{-min-OK}$: $p0\text{-min} \leq 1-\gamma$

assumes big : *Big-Closer-10-2* γ l **and** $l \leq k$

assumes γ : $1/10 \leq \gamma \leq 1/5$

shows *False*

<proof>

9.2 Theorem 10.1

context *P0-min*

begin

definition *Big101a* $\equiv \lambda k. 2 + \text{real } k / 2 \leq \exp(\text{of-int}[k/10] * 2 - k/200)$

definition *Big101b* $\equiv \lambda k. (\text{real } k)^2 - 10 * \text{real } k > (k/10) * \text{real}(10 + 9*k)$

The proof considers a smaller graph, so l needs to be so big that the smaller l' will be big enough.

definition *Big101c* $\equiv \lambda \gamma 0 l. \forall l'. \gamma. l' \geq \text{nat } [2/5 * l] \longrightarrow \gamma 0 \leq \gamma \longrightarrow \gamma \leq 1/10 \longrightarrow \text{Big-Far-9-1 } \gamma l'$

definition *Big101d* $\equiv \lambda l. (\forall l'. \gamma. l' \geq \text{nat } [2/5 * l] \longrightarrow 1/10 \leq \gamma \longrightarrow \gamma \leq 1/5 \longrightarrow \text{Big-Closer-10-2 } \gamma l')$

definition *Big-Closer-10-1* $\equiv \lambda \gamma 0 l. l \geq 9 \wedge (\forall k \geq l. \text{Big101c } \gamma 0 k \wedge \text{Big101d } k \wedge \text{Big101a } k \wedge \text{Big101b } k)$

lemma *Big-Closer-10-1-upward*: $\llbracket \text{Big-Closer-10-1 } \gamma 0 l; l \leq k; \gamma 0 \leq \gamma \rrbracket \implies \text{Big-Closer-10-1 } \gamma k$

<proof>

The need for $\gamma 0$ is unfortunate, but it seems simpler to hide the precise value of this term in the main proof.

lemma *Big-Closer-10-1*:

fixes $\gamma 0::\text{real}$

assumes $\gamma 0 > 0$

shows $\forall^\infty l. \text{Big-Closer-10-1 } \gamma 0 l$

<proof>

The strange constant $\gamma 0$ is needed for the case where we consider a subgraph; see near the end of this proof

theorem *Closer-10-1*:

fixes $l k::\text{nat}$

fixes $\delta \ \gamma :: \text{real}$
defines $\gamma \equiv \text{real } l / (\text{real } k + \text{real } l)$
defines $\delta \equiv \gamma / 40$
defines $\gamma_0 \equiv \min \ \gamma \ (0.07)$ — Since $36 \leq k$, the lower bound $1 / (10::'a) - 1 / (36::'a)$ works
assumes *big: Big-Closer-10-1* $\gamma_0 \ l$
assumes $\gamma: \gamma \leq 1/5$
assumes *p0-min-101: p0-min* $\leq 1 - 1/5$
shows $RN \ k \ l \leq \exp(-\delta * k + 3) * (k+l \text{ choose } l)$
 $\langle \text{proof} \rangle$

definition *ok-fun-10-1* $\equiv \lambda \gamma \ k. \text{ if } \text{Big-Closer-10-1} \ (\min \ \gamma \ 0.07) \ (\text{nat}[(\gamma / (1-\gamma)) * k]) \text{ then } 3 \text{ else } (\gamma / 40 * k)$

lemma *ok-fun-10-1*:
assumes $0 < \gamma \ \gamma < 1$
shows *ok-fun-10-1* $\gamma \in o(\text{real})$
 $\langle \text{proof} \rangle$

theorem *Closer-10-1-unconditional*:
fixes $l \ k :: \text{nat}$
fixes $\delta \ \gamma :: \text{real}$
defines $\gamma \equiv \text{real } l / (\text{real } k + \text{real } l)$
defines $\delta \equiv \gamma / 40$
assumes $\gamma: 0 < \gamma \ \gamma \leq 1/5$
assumes *p0-min-101: p0-min* $\leq 1 - 1/5$
shows $RN \ k \ l \leq \exp(-\delta * k + \text{ok-fun-10-1 } \gamma \ k) * (k+l \text{ choose } l)$
 $\langle \text{proof} \rangle$

end

end

10 From diagonal to off-diagonal

theory *From-Diagonal*
imports *Closer-To-Diagonal*

begin

10.1 Lemma 11.2

definition *ok-fun-11-2a* $\equiv \lambda k. \lceil \text{real } k \text{ powr } (3/4) \rceil * \log 2 \ k$

definition *ok-fun-11-2b* $\equiv \lambda \mu \ k. k \text{ powr } (39/40) * (\log 2 \ \mu + 3 * \log 2 \ k)$

definition *ok-fun-11-2c* $\equiv \lambda \mu \ k. -k * \log 2 \ (1 - (2 / (1-\mu))) * k \text{ powr } (-1/40)$

definition *ok-fun-11-2* $\equiv \lambda \mu \ k. 2 - \text{ok-fun-71 } \mu \ k + \text{ok-fun-11-2a } k$

+ $\max (ok\text{-fun-11-2b } \mu k) (ok\text{-fun-11-2c } \mu k)$

lemma *ok-fun-11-2a*: $ok\text{-fun-11-2a} \in o(\text{real})$
 ⟨*proof*⟩

possibly, the functions that depend upon μ need a more refined analysis to cover a closed interval of possible values. But possibly not, as the text implies $\mu = (2::'a) / (5::'a)$.

lemma *ok-fun-11-2b*: $ok\text{-fun-11-2b } \mu \in o(\text{real})$
 ⟨*proof*⟩

lemma *ok-fun-11-2c*: $ok\text{-fun-11-2c } \mu \in o(\text{real})$
 ⟨*proof*⟩

lemma *ok-fun-11-2*:
assumes $0 < \mu < 1$
shows $ok\text{-fun-11-2 } \mu \in o(\text{real})$
 ⟨*proof*⟩

definition *Big-From-11-2* \equiv
 $\lambda \mu k. \text{Big-ZZ-8-6 } \mu k \wedge \text{Big-X-7-1 } \mu k \wedge \text{Big-Y-6-2 } \mu k \wedge \text{Big-Red-5-3 } \mu k \wedge$
 $\text{Big-Blue-4-1 } \mu k$
 $\wedge 1 \leq \mu^2 * \text{real } k \wedge 2 / (1 - \mu) * \text{real } k \text{ powr } (-1/40) < 1 \wedge 1/k < 1/2$
 $- 3 * \text{eps } k$

lemma *Big-From-11-2*:
assumes $0 < \mu < 1$ $\mu_0 \leq \mu_1 < 1$
shows $\forall^\infty k. \forall \mu. \mu \in \{\mu_0.. \mu_1\} \longrightarrow \text{Big-From-11-2 } \mu k$
 ⟨*proof*⟩

Simply to prevent issues about the positioning of the function *real*

abbreviation *ratio* $\equiv \lambda \mu s t. \mu * (\text{real } s + \text{real } t) / \text{real } s$

the text refers to the actual Ramsey number but I don't see how that could work. Theorem 11.1 will define n to be one less than the Ramsey number, hence we add that one back here.

lemma (in *Book*) *From-11-2*:
assumes $l = k$
assumes *big*: $\text{Big-From-11-2 } \mu k$
defines $\mathcal{R} \equiv \text{Step-class } \{\text{red-step}\}$ **and** $\mathcal{S} \equiv \text{Step-class } \{\text{dboost-step}\}$
defines $t \equiv \text{card } \mathcal{R}$ **and** $s \equiv \text{card } \mathcal{S}$
defines $nV' \equiv \text{Suc } nV$
assumes $0: \text{card } X0 \geq nV \text{ div } 2$ **and** $p0 \geq 1/2$
shows $\log 2 nV' \leq k * \log 2 (1/\mu) + t * \log 2 (1 / (1 - \mu)) + s * \log 2 (\text{ratio } \mu s t) + ok\text{-fun-11-2 } \mu k$
 ⟨*proof*⟩

10.2 Lemma 11.3

same remark as in Lemma 11.2 about the use of the Ramsey number in the conclusion

lemma (in *Book*) *From-11-3*:

assumes $l=k$

assumes *big*: *Big-Y-6-1* μ k

defines $\mathcal{R} \equiv \text{Step-class } \{\text{red-step}\}$ **and** $\mathcal{S} \equiv \text{Step-class } \{\text{dboost-step}\}$

defines $t \equiv \text{card } \mathcal{R}$ **and** $s \equiv \text{card } \mathcal{S}$

defines $nV' \equiv \text{Suc } nV$

assumes 0 : $\text{card } Y0 \geq nV \text{ div } 2$ **and** $p0 \geq 1/2$

shows $\log 2 nV' \leq \log 2 (\text{RN } k (k-t)) + s + t + 2 - \text{ok-fun-61 } k$

<proof>

10.3 Theorem 11.1

definition *FF* :: $\text{nat} \Rightarrow \text{real} \Rightarrow \text{real} \Rightarrow \text{real}$ **where**

$FF \equiv \lambda k x y. \log 2 (\text{RN } k (\text{nat}[\text{real } k - x * \text{real } k])) / \text{real } k + x + y$

definition *GG* :: $\text{real} \Rightarrow \text{real} \Rightarrow \text{real} \Rightarrow \text{real}$ **where**

$GG \equiv \lambda \mu x y. \log 2 (1/\mu) + x * \log 2 (1/(1-\mu)) + y * \log 2 (\mu * (x+y) / y)$

definition *FF-bound* :: $\text{nat} \Rightarrow \text{real} \Rightarrow \text{real}$ **where**

$FF\text{-bound} \equiv \lambda k u. FF k 0 u + 1$

lemma *log2-RN-ge0*: $0 \leq \log 2 (\text{RN } k k) / k$

<proof>

lemma *le-FF-bound*:

assumes x : $x \in \{0..1\}$ **and** $y \in \{0..u\}$

shows $FF k x y \leq FF\text{-bound } k u$

<proof>

lemma *FF2*: $y' \leq y \implies FF k x y' \leq FF k x y$

<proof>

lemma *FF-GG-bound*:

assumes μ : $0 < \mu < 1$ **and** x : $x \in \{0..1\}$ **and** y : $y \in \{0..\mu * x / (1-\mu) + \eta\}$

shows $\min (FF k x y) (GG \mu x y) + \eta \leq FF\text{-bound } k (\mu / (1-\mu) + \eta) + \eta$

<proof>

context *P0-min*

begin

definition *ok-fun-11-1* $\equiv \lambda \mu k. \max (\text{ok-fun-11-2 } \mu k) (2 - \text{ok-fun-61 } k)$

lemma *ok-fun-11-1*:

assumes $0 < \mu < 1$
shows *ok-fun-11-1* $\mu \in o(\text{real})$
 $\langle \text{proof} \rangle$

lemma *eventually-ok111-le- η* :
assumes $\eta > 0$ **and** $\mu: 0 < \mu < 1$
shows $\forall^\infty k. \text{ok-fun-11-1 } \mu \ k / k \leq \eta$
 $\langle \text{proof} \rangle$

lemma *eventually-powr-le- η* :
assumes $\eta > 0$
shows $\forall^\infty k. (2 / (1 - \mu)) * k \text{ powr } (-1/20) \leq \eta$
 $\langle \text{proof} \rangle$

definition *Big-From-11-1* \equiv
 $\lambda \eta \ \mu \ k. \text{Big-From-11-2 } \mu \ k \wedge \text{Big-ZZ-8-5 } \mu \ k \wedge \text{Big-Y-6-1 } \mu \ k \wedge \text{ok-fun-11-1 } \mu$
 $k / k \leq \eta/2$
 $\wedge (2 / (1 - \mu)) * k \text{ powr } (-1/20) \leq \eta/2$
 $\wedge \text{Big-Closer-10-1 } (1/101) (\text{nat}\lceil k/100 \rceil) \wedge 3 / (k * \ln 2) \leq \eta/2 \wedge k \geq 3$

In sections 9 and 10 (and by implication all proceeding sections), we needed to consider a closed interval of possible values of μ . Let's hope, maybe not here. The fact below can only be proved with the strict inequality $0 < \eta$, which is why it is also strict in the theorems depending on this property.

lemma *Big-From-11-1*:
assumes $\eta > 0$ $0 < \mu < 1$
shows $\forall^\infty k. \text{Big-From-11-1 } \eta \ \mu \ k$
 $\langle \text{proof} \rangle$

The actual proof of theorem 11.1 is now combined with the development of section 12, since the concepts seem to be inescapably mixed up.

end

end

11 The Proof of Theorem 1.1

theory *The-Proof*
imports *From-Diagonal*

begin

11.1 The bounding functions

definition *H* $\equiv \lambda p. -p * \log 2 \ p - (1 - p) * \log 2 \ (1 - p)$

definition *dH* **where** *dH* $\equiv \lambda x::\text{real}. -\ln(x)/\ln(2) + \ln(1 - x)/\ln(2)$

lemma *dH* [*derivative-intros*]:
assumes $0 < x \ x < 1$
shows (*H has-real-derivative dH x*) (*at x*)
 \langle *proof* \rangle

lemma *H0* [*simp*]: $H\ 0 = 0$ **and** *H1* [*simp*]: $H\ 1 = 0$
 \langle *proof* \rangle

lemma *H-reflect*: $H\ (1-p) = H\ p$
 \langle *proof* \rangle

lemma *H-ge0*:
assumes $0 \leq p \ p \leq 1$
shows $0 \leq H\ p$
 \langle *proof* \rangle

Going up, from 0 to 1/2

lemma *H-half-mono*:
assumes $0 \leq p' \ p' \leq p \ p \leq 1/2$
shows $H\ p' \leq H\ p$
 \langle *proof* \rangle

Going down, from 1/2 to 1

lemma *H-half-mono'*:
assumes $1/2 \leq p' \ p' \leq p \ p \leq 1$
shows $H\ p' \geq H\ p$
 \langle *proof* \rangle

lemma *H-half*: $H(1/2) = 1$
 \langle *proof* \rangle

lemma *H-le1*:
assumes $0 \leq p \ p \leq 1$
shows $H\ p \leq 1$
 \langle *proof* \rangle

Many thanks to Fedor Petrov on mathoverflow

lemma *H-12-1*:
fixes $a \ b::nat$
assumes $a \geq b$
shows $\log\ 2\ (a\ choose\ b) \leq a * H(b/a)$
 \langle *proof* \rangle

definition *gg* $\equiv GG\ (2/5)$

lemma *gg-eq*: $gg\ x\ y = \log\ 2\ (5/2) + x * \log\ 2\ (5/3) + y * \log\ 2\ ((2 * (x+y)) / (5*y))$
 \langle *proof* \rangle

definition $f1 \equiv \lambda x y. x + y + (2-x) * H(1/(2-x))$

definition $f2 \equiv \lambda x y. f1 x y - (1 / (40 * \ln 2)) * ((1-x) / (2-x))$

definition $ff \equiv \lambda x y. \text{if } x < 3/4 \text{ then } f1 x y \text{ else } f2 x y$

Incorporating Bhavik's idea, which gives us a lower bound for γ of 1/101

definition $ffGG :: real \Rightarrow real \Rightarrow real \Rightarrow real$ **where**
 $ffGG \equiv \lambda \mu x y. \max 1.9 (\min (ff x y) (GG \mu x y))$

The proofs involving *Sup* are needlessly difficult because ultimately the sets involved are finite, eliminating the need to demonstrate boundedness. Simpler might be to use the extended reals.

lemma *f1-le*:
assumes $x \leq 1$
shows $f1 x y \leq y + 2$
 $\langle proof \rangle$

lemma *ff-le4*:
assumes $x \leq 1 \ y \leq 1$
shows $ff x y \leq 4$
 $\langle proof \rangle$

lemma *ff-GG-bound*:
assumes $x \leq 1 \ y \leq 1$
shows $ffGG \mu x y \leq 4$
 $\langle proof \rangle$

lemma *bdd-above-ff-GG*:
assumes $x \leq 1 \ u \leq 1$
shows *bdd-above* $((\lambda y. ffGG \mu x y + \eta) \text{ ' } \{0..u\})$
 $\langle proof \rangle$

lemma *bdd-above-SUP-ff-GG*:
assumes $0 \leq u \ u \leq 1$
shows *bdd-above* $((\lambda x. \bigsqcup y \in \{0..u\}. ffGG \mu x y + \eta) \text{ ' } \{0..1\})$
 $\langle proof \rangle$

Claim (62). A singularity if $x = 1$. Okay if we put $\ln(0) = 0$

lemma *FF-le-f1*:
fixes $k::nat$ **and** $x y::real$
assumes $x: 0 \leq x \ x \leq 1$ **and** $y: 0 \leq y \ y \leq 1$
shows $FF k x y \leq f1 x y$
 $\langle proof \rangle$

Bhavik's *eleven-one-large-end*

lemma *f1-le-19*:
fixes $k::nat$ **and** $x y::real$
assumes $x: 0.99 \leq x \ x \leq 1$ **and** $y: 0 \leq y \ y \leq 3/4$

shows $f1\ x\ y \leq 1.9$
 ⟨proof⟩

Claim (63) in weakened form; we get rid of the extra bit later

lemma (in *P0-min*) *FF-le-f2*:
fixes $k::nat$ **and** $x\ y::real$
assumes $x: 3/4 \leq x \leq 1$ **and** $y: 0 \leq y \leq 1$
and $l: real\ l = k - x*k$
assumes *p0-min-101*: $p0-min \leq 1 - 1/5$
defines $\gamma \equiv real\ l / (real\ k + real\ l)$
defines $\gamma0 \equiv min\ \gamma\ (0.07)$
assumes $\gamma > 0$
shows $FF\ k\ x\ y \leq f2\ x\ y + ok-fun-10-1\ \gamma\ k / (k * ln\ 2)$
 ⟨proof⟩

The body of the proof has been extracted to allow the symmetry argument. And $1/12$ is $3/4 - 2/3$, the latter number corresponding to $\mu = (2::'a) / (5::'a)$

lemma (in *Book-Basis*) *From-11-1-Body*:
fixes $V :: 'a\ set$
assumes $\mu: 0 < \mu \leq 2/5$ **and** $\eta: 0 < \eta \leq 1/12$
and *ge-RN*: $Suc\ nV \geq RN\ k\ k$
and *Red*: *graph-density* $Red \geq 1/2$
and *p0-min12*: $p0-min \leq 1/2$
and *Red-E*: $Red \subseteq E$ **and** *Blue-def*: $Blue = E \setminus Red$
and *no-Red-K*: $\neg (\exists K. size-clique\ k\ K\ Red)$
and *no-Blue-K*: $\neg (\exists K. size-clique\ k\ K\ Blue)$
and *big*: *Big-From-11-1* $\eta\ \mu\ k$
shows $log\ 2\ (RN\ k\ k) / k \leq (SUP\ x \in \{0..1\}. SUP\ y \in \{0..3/4\}. ffgg\ \mu\ x\ y + \eta)$
 ⟨proof⟩

theorem (in *P0-min*) *From-11-1*:
assumes $\mu: 0 < \mu \leq 2/5$ **and** $0 < \eta \leq 1/12$
and *p0-min12*: $p0-min \leq 1/2$ **and** *big*: *Big-From-11-1* $\eta\ \mu\ k$
shows $log\ 2\ (RN\ k\ k) / k \leq (SUP\ x \in \{0..1\}. SUP\ y \in \{0..3/4\}. ffgg\ \mu\ x\ y + \eta)$
 ⟨proof⟩

11.2 The monster calculation from appendix A

11.2.1 Observation A.1

lemma *gg-increasing*:
assumes $x \leq x'$ $0 \leq x$ $0 \leq y$
shows $gg\ x\ y \leq gg\ x'\ y$
 ⟨proof⟩

Thanks to Manuel Eberl

lemma *continuous-on-x-ln*: *continuous-on* $\{0..\}$ $(\lambda x::real. x * ln\ x)$

<proof>

lemma *continuous-on-f1*: *continuous-on* {..1} ($\lambda x. f1\ x\ y$)
<proof>

definition *df1* **where** $df1 \equiv \lambda x. \log\ 2\ (2 * ((1-x) / (2-x)))$

lemma *Df1* [*derivative-intros*]:
assumes $x < 1$
shows ($\lambda x. f1\ x\ y$) *has-real-derivative* $df1\ x$ (*at* x)
<proof>

definition *delta* **where** $delta \equiv \lambda u::real. 1 / (\ln\ 2 * 40 * (2 - u)^2)$

lemma *Df2*:
assumes $1/2 \leq x < 1$
shows ($\lambda x. f2\ x\ y$) *has-real-derivative* $df1\ x + delta\ x$ (*at* x)
<proof>

lemma *antimono-on-ff*:
assumes $0 \leq y < 1$
shows *antimono-on* {1/2..1} ($\lambda x. ff\ x\ y$)
<proof>

11.2.2 Claims A.2–A.4

Called simply x in the paper, but are you kidding me?

definition *x-of* $\equiv \lambda y::real. 3*y/5 + 0.5454$

lemma *x-of*: $x-of \in \{0..3/4\} \rightarrow \{1/2..1\}$
<proof>

definition *y-of* $\equiv \lambda x::real. 5 * x/3 - 0.909$

lemma *y-of-x-of* [*simp*]: $y-of\ (x-of\ y) = y$
<proof>

lemma *x-of-y-of* [*simp*]: $x-of\ (y-of\ x) = x$
<proof>

lemma *Df1-y* [*derivative-intros*]:
assumes $x < 1$
shows ($\lambda x. f1\ x\ (y-of\ x)$) *has-real-derivative* $5/3 + df1\ x$ (*at* x)
<proof>

lemma *Df2-y* [*derivative-intros*]:
assumes $1/2 \leq x < 1$
shows ($\lambda x. f2\ x\ (y-of\ x)$) *has-real-derivative* $5/3 + df1\ x + delta\ x$ (*at* x)
<proof>

definition $Dg-x \equiv \lambda y. 3 * \log 2 (5/3) / 5 + \log 2 ((2727 + y * 8000) / (y * 12500))$
 $- 2727 / (\ln 2 * (2727 + y * 8000))$

lemma $Dg-x$ [*derivative-intros*]:

assumes $y \in \{0 < .. < 3/4\}$

shows $((\lambda y. gg (x-of y) y) \text{ has-real-derivative } Dg-x y) \text{ (at } y)$

<proof>

Claim A2 is difficult because it comes *real close*: max value = 1.999281, when $y = 0.4339$. There is no simple closed form for the maximum point (where the derivative goes to 0).

Due to the singularity at zero, we need to cover the zero case analytically, but at least interval arithmetic covers the maximum point

lemma $A2$:

assumes $y \in \{0..3/4\}$

shows $gg (x-of y) y \leq 2 - 1/2^{11}$

<proof>

lemma $A3$:

assumes $y \in \{0..0.341\}$

shows $f1 (x-of y) y \leq 2 - 1/2^{11}$

<proof>

This one also comes close: max value = 1.999271, when $y = 0.4526$. The specified upper bound is 1.99951

lemma $A4$:

assumes $y \in \{0.341..3/4\}$

shows $f2 (x-of y) y \leq 2 - 1/2^{11}$

<proof>

context $P0\text{-min}$

begin

The truly horrible Lemma 12.3

lemma 123 :

assumes $\delta \leq 1 / 2^{11}$

shows $(SUP x \in \{0..1\}. SUP y \in \{0..3/4\}. ffgG (2/5) x y) \leq 2 - \delta$

<proof>

end

11.3 Concluding the proof

we subtract a tiny bit, as we seem to need this gap

definition $\text{delta}'::\text{real}$ **where** $\text{delta}' \equiv 1 / 2^{11} - 1 / 2^{18}$

lemma *Aux-1-1*:

assumes $p0\text{-min}12$: $p0\text{-min} \leq 1/2$

shows $\forall^\infty k. \log 2 (RN\ k\ k) / k \leq 2 - \text{delta}'$

<proof>

Main theorem 1.1: the exponent is approximately 3.9987

theorem *Main-1-1*:

obtains $\varepsilon::\text{real}$ **where** $\varepsilon > 0 \ \forall^\infty k. RN\ k\ k \leq (4 - \varepsilon)^k$

<proof>

end

References

- [1] M. Campos, S. Griffiths, R. Morris, and J. Sahasrabudhe. An exponential improvement for diagonal Ramsey, 2023. arXiv, 2303.09521.