Matroids

Jonas Keinholz

March 17, 2025

Abstract

This article defines combinatorial structures known as *Independence Systems* and *Matroids* and provides basic concepts and theorems related to them. These structures play an important role in combinatorial optimisation, e. g. greedy algorithms such as Kruskal's algorithm. The development is based on Oxley's 'What is a Matroid?' [1].

Contents

1 Independence systems

theory *Indep-System*
  imports *Main*
begin

lemma *finite-psubset-inc-induct*:
  assumes $\mathit{finite}\ A\ X \subseteq A$
  assumes $\bigwedge X.\ (\bigwedge Y.\ X \subset Y \Longrightarrow Y \subseteq A \Longrightarrow P\ Y) \Longrightarrow P\ X$
  shows $P\ X$
⟨*proof*⟩

An *independence system* consists of a finite ground set together with an independence predicate over the sets of this ground set. At least one set of the carrier is independent and subsets of independent sets are also independent.

locale *indep-system* =
  fixes $\mathit{carrier} :: {}'a\ \mathit{set}$
  fixes $\mathit{indep} :: {}'a\ \mathit{set} \Rightarrow \mathit{bool}$
  assumes *carrier-finite*: *finite carrier*
  assumes *indep-subset-carrier*: $\mathit{indep}\ X \Longrightarrow X \subseteq \mathit{carrier}$
  assumes *indep-ex*: $\exists X.\ \mathit{indep}\ X$
  assumes *indep-subset*: $\mathit{indep}\ X \Longrightarrow Y \subseteq X \Longrightarrow \mathit{indep}\ Y$
begin

lemmas *psubset-inc-induct* [*case-names carrier step*] = *finite-psubset-inc-induct*[*OF carrier-finite*]
lemmas *indep-finite* [*simp*] = *finite-subset*[*OF indep-subset-carrier carrier-finite*]

The empty set is independent.

lemma *indep-empty* [*simp*]: *indep* {}
  ⟨*proof*⟩

1.1 Sub-independence systems

A subset of the ground set induces an independence system.

definition *indep-in* **where** $\mathit{indep\text{-}in}\ \mathcal{E}\ X \longleftrightarrow X \subseteq \mathcal{E} \wedge \mathit{indep}\ X$

lemma *indep-inI*:
  assumes $X \subseteq \mathcal{E}$
  assumes $\mathit{indep}\ X$
  shows $\mathit{indep\text{-}in}\ \mathcal{E}\ X$
  ⟨*proof*⟩

lemma *indep-in-subI*: $\mathit{indep\text{-}in}\ \mathcal{E}\ X \Longrightarrow \mathit{indep\text{-}in}\ \mathcal{E}'\ (X \cap \mathcal{E}')$
  ⟨*proof*⟩

lemma *dep-in-subI*:
  assumes $X \subseteq \mathcal{E}'$

shows ¬ *indep-in* $\mathcal{E}'$ X $\Longrightarrow$ ¬ *indep-in* $\mathcal{E}$ X
⟨*proof*⟩

lemma *indep-in-subset-carrier*: *indep-in* $\mathcal{E}$ X $\Longrightarrow$ $X \subseteq \mathcal{E}$
⟨*proof*⟩

lemma *indep-in-subI-subset*:
assumes $\mathcal{E}' \subseteq \mathcal{E}$
assumes *indep-in* $\mathcal{E}'$ X
shows *indep-in* $\mathcal{E}$ X
⟨*proof*⟩

lemma *indep-in-supI*:
assumes $X \subseteq \mathcal{E}'$ $\mathcal{E}' \subseteq \mathcal{E}$
assumes *indep-in* $\mathcal{E}$ X
shows *indep-in* $\mathcal{E}'$ X
⟨*proof*⟩

lemma *indep-in-indep*: *indep-in* $\mathcal{E}$ X $\Longrightarrow$ *indep* X
⟨*proof*⟩

lemmas *indep-inD* = *indep-in-subset-carrier indep-in-indep*

lemma *indep-system-subset* [*simp*, *intro*]:
assumes $\mathcal{E} \subseteq$ *carrier*
shows *indep-system* $\mathcal{E}$ (*indep-in* $\mathcal{E}$)
⟨*proof*⟩

We will work a lot with different sub structures. Therefore, every definition 'foo' will have a counterpart 'foo_in' which has the ground set as an additional parameter. Furthermore, every result about 'foo' will have another result about 'foo_in'. With this, we usually don't have to work with **interpretation** in proofs.

context
fixes $\mathcal{E}$
assumes $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *indep-system* $\mathcal{E}$ *indep-in* $\mathcal{E}$
⟨*proof*⟩

lemma *indep-in-sub-cong*:
assumes $\mathcal{E}' \subseteq \mathcal{E}$
shows $\mathcal{E}$.*indep-in* $\mathcal{E}'$ X $\longleftrightarrow$ *indep-in* $\mathcal{E}'$ X
⟨*proof*⟩

lemmas *indep-in-ex* = $\mathcal{E}$.*indep-ex*
lemmas *indep-in-subset* = $\mathcal{E}$.*indep-subset*
lemmas *indep-in-empty* = $\mathcal{E}$.*indep-empty*

end

1.2 Bases

A *basis* is a maximal independent set, i. e. an independent set which becomes dependent on inserting any element of the ground set.

definition *basis* **where** $basis\ X \longleftrightarrow indep\ X \wedge (\forall\, x \in carrier - X.\ \neg\ indep\ (insert\ x\ X))$

lemma *basisI*:
  assumes $indep\ X$
  assumes $\bigwedge x.\ x \in carrier - X \Longrightarrow \neg\ indep\ (insert\ x\ X)$
  shows $basis\ X$
  ⟨*proof*⟩

lemma *basis-indep*: $basis\ X \Longrightarrow indep\ X$
  ⟨*proof*⟩

lemma *basis-max-indep*: $basis\ X \Longrightarrow x \in carrier - X \Longrightarrow \neg\ indep\ (insert\ x\ X)$
  ⟨*proof*⟩

lemmas *basisD* = *basis-indep basis-max-indep*
lemmas *basis-subset-carrier* = *indep-subset-carrier*[*OF basis-indep*]
lemmas *basis-finite* [*simp*] = *indep-finite*[*OF basis-indep*]

lemma *indep-not-basis*:
  assumes $indep\ X$
  assumes $\neg\ basis\ X$
  shows $\exists\, x \in carrier - X.\ indep\ (insert\ x\ X)$
  ⟨*proof*⟩

lemma *basis-subset-eq*:
  assumes $basis\ B_1$
  assumes $basis\ B_2$
  assumes $B_1 \subseteq B_2$
  shows $B_1 = B_2$
⟨*proof*⟩

definition *basis-in* **where**
  $basis\text{-}in\ \mathcal{E}\ X \longleftrightarrow indep\text{-}system.basis\ \mathcal{E}\ (indep\text{-}in\ \mathcal{E})\ X$

lemma *basis-iff-basis-in*: $basis\ B \longleftrightarrow basis\text{-}in\ carrier\ B$
⟨*proof*⟩

context
  fixes $\mathcal{E}$
  assumes $\mathcal{E} \subseteq carrier$
begin

interpretation $\mathcal{E}$: *indep-system* $\mathcal{E}$ *indep-in* $\mathcal{E}$
  ⟨*proof*⟩

lemma *basis-inI-aux*: $\mathcal{E}$.*basis* $X \Longrightarrow$ *basis-in* $\mathcal{E}$ X
  ⟨*proof*⟩

lemma *basis-inD-aux*: *basis-in* $\mathcal{E}$ $X \Longrightarrow \mathcal{E}$.*basis* X
  ⟨*proof*⟩

lemma *not-basis-inD-aux*: $\neg$ *basis-in* $\mathcal{E}$ $X \Longrightarrow \neg$ $\mathcal{E}$.*basis* X
  ⟨*proof*⟩

lemmas *basis-inI* = *basis-inI-aux*[*OF* $\mathcal{E}$.*basisI*]
lemmas *basis-in-indep-in* = $\mathcal{E}$.*basis-indep*[*OF basis-inD-aux*]
lemmas *basis-in-max-indep-in* = $\mathcal{E}$.*basis-max-indep*[*OF basis-inD-aux*]
lemmas *basis-inD* = $\mathcal{E}$.*basisD*[*OF basis-inD-aux*]
lemmas *basis-in-subset-carrier* = $\mathcal{E}$.*basis-subset-carrier*[*OF basis-inD-aux*]
lemmas *basis-in-finite* = $\mathcal{E}$.*basis-finite*[*OF basis-inD-aux*]
lemmas *indep-in-not-basis-in* = $\mathcal{E}$.*indep-not-basis*[*OF - not-basis-inD-aux*]
lemmas *basis-in-subset-eq* = $\mathcal{E}$.*basis-subset-eq*[*OF basis-inD-aux basis-inD-aux*]

end

context
  fixes $\mathcal{E}$
  assumes $*$: $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *indep-system* $\mathcal{E}$ *indep-in* $\mathcal{E}$
  ⟨*proof*⟩

lemma *basis-in-sub-cong*:
  assumes $\mathcal{E}' \subseteq \mathcal{E}$
  shows $\mathcal{E}$.*basis-in* $\mathcal{E}'$ $B \longleftrightarrow$ *basis-in* $\mathcal{E}'$ B
⟨*proof*⟩

end

1.3 Circuits

A *circuit* is a minimal dependent set, i. e. a set which becomes independent on removing any element of the ground set.

definition *circuit* **where** *circuit* $X \longleftrightarrow X \subseteq$ *carrier* $\wedge \neg$ *indep* $X \wedge (\forall x \in X.$ *indep* $(X - \{x\}))$

lemma *circuitI*:
  assumes $X \subseteq$ *carrier*
  assumes $\neg$ *indep* X

assumes $\bigwedge x.\ x \in X \Longrightarrow$ *indep* $(X - \{x\})$
shows *circuit* X
⟨*proof*⟩

lemma *circuit-subset-carrier*: *circuit* $X \Longrightarrow X \subseteq$ *carrier*
⟨*proof*⟩
lemmas *circuit-finite* [*simp*] = *finite-subset*[*OF circuit-subset-carrier carrier-finite*]

lemma *circuit-dep*: *circuit* $X \Longrightarrow \neg$ *indep* X
⟨*proof*⟩

lemma *circuit-min-dep*: *circuit* $X \Longrightarrow x \in X \Longrightarrow$ *indep* $(X - \{x\})$
⟨*proof*⟩

lemmas *circuitD* = *circuit-subset-carrier circuit-dep circuit-min-dep*

lemma *circuit-nonempty*: *circuit* $X \Longrightarrow X \neq \{\}$
⟨*proof*⟩

lemma *dep-not-circuit*:
assumes $X \subseteq$ *carrier*
assumes $\neg$ *indep* X
assumes $\neg$ *circuit* X
shows $\exists x \in X.\ \neg$ *indep* $(X - \{x\})$
⟨*proof*⟩

lemma *circuit-subset-eq*:
assumes *circuit* C_1
assumes *circuit* C_2
assumes $C_1 \subseteq C_2$
shows $C_1 = C_2$
⟨*proof*⟩

definition *circuit-in* **where**
circuit-in $\mathcal{E}$ $X \longleftrightarrow$ *indep-system.circuit* $\mathcal{E}$ (*indep-in* $\mathcal{E}$) X

context
fixes $\mathcal{E}$
assumes $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *indep-system* $\mathcal{E}$ *indep-in* $\mathcal{E}$
⟨*proof*⟩

lemma *circuit-inI-aux*: $\mathcal{E}$.*circuit* $X \Longrightarrow$ *circuit-in* $\mathcal{E}$ X
⟨*proof*⟩

lemma *circuit-inD-aux*: *circuit-in* $\mathcal{E}$ $X \Longrightarrow \mathcal{E}$.*circuit* X
⟨*proof*⟩

lemma *not-circuit-inD-aux*: $\neg$ *circuit-in* $\mathcal{E}$ $X \Longrightarrow \neg$ $\mathcal{E}$.*circuit* X
⟨*proof*⟩

lemmas *circuit-inI* = *circuit-inI-aux*[*OF* $\mathcal{E}$.*circuitI*]

lemmas *circuit-in-subset-carrier* = $\mathcal{E}$.*circuit-subset-carrier*[*OF circuit-inD-aux*]
lemmas *circuit-in-finite* = $\mathcal{E}$.*circuit-finite*[*OF circuit-inD-aux*]
lemmas *circuit-in-dep-in* = $\mathcal{E}$.*circuit-dep*[*OF circuit-inD-aux*]
lemmas *circuit-in-min-dep-in* = $\mathcal{E}$.*circuit-min-dep*[*OF circuit-inD-aux*]
lemmas *circuit-inD* = $\mathcal{E}$.*circuitD*[*OF circuit-inD-aux*]
lemmas *circuit-in-nonempty* = $\mathcal{E}$.*circuit-nonempty*[*OF circuit-inD-aux*]
lemmas *dep-in-not-circuit-in* = $\mathcal{E}$.*dep-not-circuit*[*OF - - not-circuit-inD-aux*]
lemmas *circuit-in-subset-eq* = $\mathcal{E}$.*circuit-subset-eq*[*OF circuit-inD-aux circuit-inD-aux*]

end

lemma *circuit-in-subI*:
assumes $\mathcal{E}' \subseteq \mathcal{E}$ $\mathcal{E} \subseteq$ *carrier*
assumes *circuit-in* $\mathcal{E}'$ C
shows *circuit-in* $\mathcal{E}$ C
⟨*proof*⟩

lemma *circuit-in-supI*:
assumes $\mathcal{E}' \subseteq \mathcal{E}$ $\mathcal{E} \subseteq$ *carrier* $C \subseteq \mathcal{E}'$
assumes *circuit-in* $\mathcal{E}$ C
shows *circuit-in* $\mathcal{E}'$ C
⟨*proof*⟩

context
fixes $\mathcal{E}$
assumes $*$: $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *indep-system* $\mathcal{E}$ *indep-in* $\mathcal{E}$
⟨*proof*⟩

lemma *circuit-in-sub-cong*:
assumes $\mathcal{E}' \subseteq \mathcal{E}$
shows $\mathcal{E}$.*circuit-in* $\mathcal{E}'$ $C \longleftrightarrow$ *circuit-in* $\mathcal{E}'$ C
⟨*proof*⟩

end

lemma *circuit-imp-circuit-in*:
assumes *circuit* C
shows *circuit-in carrier* C
⟨*proof*⟩

1.4 Relation between independence and bases

A set is independent iff it is a subset of a basis.

lemma *indep-imp-subset-basis*:
  assumes *indep X*
  shows $\exists B.\ basis\ B \wedge X \subseteq B$
  ⟨*proof*⟩

lemmas *subset-basis-imp-indep* = *indep-subset*[*OF basis-indep*]

lemma *indep-iff-subset-basis*: $indep\ X \longleftrightarrow (\exists B.\ basis\ B \wedge X \subseteq B)$
  ⟨*proof*⟩

lemma *basis-ex*: $\exists B.\ basis\ B$
  ⟨*proof*⟩

context
  fixes $\mathcal{E}$
  assumes $*$: $\mathcal{E} \subseteq carrier$
begin

interpretation $\mathcal{E}$: *indep-system* $\mathcal{E}$ *indep-in* $\mathcal{E}$
  ⟨*proof*⟩

lemma *indep-in-imp-subset-basis-in*:
  assumes *indep-in* $\mathcal{E}$ X
  shows $\exists B.$ *basis-in* $\mathcal{E}\ B \wedge X \subseteq B$
  ⟨*proof*⟩

lemmas *subset-basis-in-imp-indep-in* = *indep-in-subset*[*OF* $*$ *basis-in-indep-in*[*OF* $*$]]

lemma *indep-in-iff-subset-basis-in*: *indep-in* $\mathcal{E}\ X \longleftrightarrow (\exists B.$ *basis-in* $\mathcal{E}\ B \wedge X \subseteq B)$
  ⟨*proof*⟩

lemma *basis-in-ex*: $\exists B.$ *basis-in* $\mathcal{E}\ B$
  ⟨*proof*⟩

lemma *basis-in-subI*:
  assumes $\mathcal{E}' \subseteq \mathcal{E}$ $\mathcal{E} \subseteq carrier$
  assumes *basis-in* $\mathcal{E}'\ B$
  shows $\exists B' \subseteq \mathcal{E} - \mathcal{E}'.$ *basis-in* $\mathcal{E}\ (B \cup B')$
⟨*proof*⟩

lemma *basis-in-supI*:
  assumes $B \subseteq \mathcal{E}'$ $\mathcal{E}' \subseteq \mathcal{E}$ $\mathcal{E} \subseteq carrier$
  assumes *basis-in* $\mathcal{E}\ B$
  shows *basis-in* $\mathcal{E}'\ B$

⟨*proof*⟩

end

1.5 Relation between dependence and circuits

A set is dependent iff it contains a circuit.

lemma *dep-imp-supset-circuit*:
  assumes $X \subseteq$ *carrier*
  assumes $\neg$ *indep* X
  shows $\exists C.$ *circuit* $C \wedge C \subseteq X$
  ⟨*proof*⟩

lemma *supset-circuit-imp-dep*:
  assumes *circuit* $C \wedge C \subseteq X$
  shows $\neg$ *indep* X
  ⟨*proof*⟩

lemma *dep-iff-supset-circuit*:
  assumes $X \subseteq$ *carrier*
  shows $\neg$ *indep* $X \longleftrightarrow (\exists C.$ *circuit* $C \wedge C \subseteq X)$
  ⟨*proof*⟩

context
  fixes $\mathcal{E}$
  assumes $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *indep-system* $\mathcal{E}$ *indep-in* $\mathcal{E}$
  ⟨*proof*⟩

lemma *dep-in-imp-supset-circuit-in*:
  assumes $X \subseteq \mathcal{E}$
  assumes $\neg$ *indep-in* $\mathcal{E}$ X
  shows $\exists C.$ *circuit-in* $\mathcal{E}$ $C \wedge C \subseteq X$
  ⟨*proof*⟩

lemma *supset-circuit-in-imp-dep-in*:
  assumes *circuit-in* $\mathcal{E}$ $C \wedge C \subseteq X$
  shows $\neg$ *indep-in* $\mathcal{E}$ X
  ⟨*proof*⟩

lemma *dep-in-iff-supset-circuit-in*:
  assumes $X \subseteq \mathcal{E}$
  shows $\neg$ *indep-in* $\mathcal{E}$ $X \longleftrightarrow (\exists C.$ *circuit-in* $\mathcal{E}$ $C \wedge C \subseteq X)$
  ⟨*proof*⟩

end

1.6 Ranks

definition *lower-rank-of* :: *'a set* ⇒ *nat* **where**
lower-rank-of carrier' ≡ *Min* {*card B* | *B*. *basis-in carrier' B*}

definition *upper-rank-of* :: *'a set* ⇒ *nat* **where**
upper-rank-of carrier' ≡ *Max* {*card B* | *B*. *basis-in carrier' B*}

lemma *collect-basis-finite*: *finite* (*Collect basis*)
⟨*proof*⟩

context
fixes $\mathcal{E}$
assumes ∗: $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *indep-system* $\mathcal{E}$ *indep-in* $\mathcal{E}$
⟨*proof*⟩

lemma *collect-basis-in-finite*: *finite* (*Collect* (*basis-in* $\mathcal{E}$))
⟨*proof*⟩

lemma *lower-rank-of-le*: *lower-rank-of* $\mathcal{E} \leq$ *card* $\mathcal{E}$
⟨*proof*⟩

lemma *upper-rank-of-le*: *upper-rank-of* $\mathcal{E} \leq$ *card* $\mathcal{E}$
⟨*proof*⟩

context
fixes $\mathcal{E}'$
assumes ∗∗: $\mathcal{E}' \subseteq \mathcal{E}$
begin

interpretation $\mathcal{E}'_1$: *indep-system* $\mathcal{E}'$ *indep-in* $\mathcal{E}'$
⟨*proof*⟩
interpretation $\mathcal{E}'_2$: *indep-system* $\mathcal{E}'$ $\mathcal{E}$.*indep-in* $\mathcal{E}'$
⟨*proof*⟩

lemma *lower-rank-of-sub-cong*:
shows $\mathcal{E}$.*lower-rank-of* $\mathcal{E}'$ = *lower-rank-of* $\mathcal{E}'$
⟨*proof*⟩

lemma *upper-rank-of-sub-cong*:
shows $\mathcal{E}$.*upper-rank-of* $\mathcal{E}'$ = *upper-rank-of* $\mathcal{E}'$
⟨*proof*⟩

end

end

end

end

2 Matroids

theory *Matroid*
  imports *Indep-System*
begin

lemma *card-subset-ex*:
  assumes *finite A* $n \leq$ *card A*
  shows $\exists B \subseteq A$. *card B* $= n$
⟨*proof*⟩

locale *matroid* = *indep-system* +
  assumes *augment-aux*:
    indep X $\Longrightarrow$ *indep Y* $\Longrightarrow$ *card X* = *Suc* (*card Y*) $\Longrightarrow \exists x \in X - Y$. *indep* (*insert x Y*)
begin

lemma *augment*:
  assumes *indep X indep Y card Y* < *card X*
  shows $\exists x \in X - Y$. *indep* (*insert x Y*)
⟨*proof*⟩

lemma *augment-psubset*:
  assumes *indep X indep Y* $Y \subset X$
  shows $\exists x \in X - Y$. *indep* (*insert x Y*)
  ⟨*proof*⟩

2.1 Minors

A subset of the ground set induces a matroid.

lemma *matroid-subset* [*simp*, *intro*]:
  assumes $\mathcal{E} \subseteq$ *carrier*
  shows *matroid* $\mathcal{E}$ (*indep-in* $\mathcal{E}$)
  ⟨*proof*⟩

context
  fixes $\mathcal{E}$
  assumes $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *matroid* $\mathcal{E}$ *indep-in* $\mathcal{E}$
  ⟨*proof*⟩

lemmas *augment-aux-indep-in* = $\mathcal{E}$.*augment-aux*

lemmas *augment-indep-in* = $\mathcal{E}$.*augment*
lemmas *augment-psubset-indep-in* = $\mathcal{E}$.*augment-psubset*

end

2.2 Bases

lemma *basis-card*:
  assumes *basis* B_1
  assumes *basis* B_2
  shows *card* B_1 = *card* B_2
⟨*proof*⟩

lemma *basis-indep-card*:
  assumes *indep* X
  assumes *basis* B
  shows *card* $X \leq$ *card* B
⟨*proof*⟩

lemma *basis-augment*:
  assumes *basis* B_1 *basis* B_2 $x \in B_1 - B_2$
  shows $\exists\, y \in B_2 - B_1$. *basis* (*insert* y ($B_1 - \{x\}$))
⟨*proof*⟩

context
  fixes $\mathcal{E}$
  assumes $*$: $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *matroid* $\mathcal{E}$ *indep-in* $\mathcal{E}$
  ⟨*proof*⟩

lemmas *basis-in-card* = $\mathcal{E}$.*basis-card*[*OF* *basis-inD-aux*[*OF* $*$] *basis-inD-aux*[*OF* $*$]]
lemmas *basis-in-indep-in-card* = $\mathcal{E}$.*basis-indep-card*[*OF* - *basis-inD-aux*[*OF* $*$]]

lemma *basis-in-augment*:
  assumes *basis-in* $\mathcal{E}$ B_1 *basis-in* $\mathcal{E}$ B_2 $x \in B_1 - B_2$
  shows $\exists\, y \in B_2 - B_1$. *basis-in* $\mathcal{E}$ (*insert* y ($B_1 - \{x\}$))
  ⟨*proof*⟩

end

2.3 Circuits

lemma *circuit-elim*:
  assumes *circuit* C_1 *circuit* C_2 $C_1 \neq C_2$ $x \in C_1 \cap C_2$
  shows $\exists\, C_3 \subseteq (C_1 \cup C_2) - \{x\}$. *circuit* C_3
⟨*proof*⟩

lemma *min-dep-imp-supset-circuit*:
  assumes *indep X*
  assumes *circuit C*
  assumes $C \subseteq$ *insert x X*
  shows $x \in C$
⟨*proof*⟩

lemma *min-dep-imp-ex1-supset-circuit*:
  assumes $x \in$ *carrier*
  assumes *indep X*
  assumes ¬ *indep* (*insert x X*)
  shows $\exists!C$. *circuit C* ∧ $C \subseteq$ *insert x X*
⟨*proof*⟩

lemma *basis-ex1-supset-circuit*:
  assumes *basis B*
  assumes $x \in$ *carrier* − *B*
  shows $\exists!C$. *circuit C* ∧ $C \subseteq$ *insert x B*
  ⟨*proof*⟩

definition *fund-circuit* :: *'a* ⇒ *'a set* ⇒ *'a set* **where**
  fund-circuit x B ≡ (*THE C*. *circuit C* ∧ $C \subseteq$ *insert x B*)

lemma *circuit-iff-fund-circuit*:
  circuit C ⟷ (∃ *x B*. $x \in$ *carrier* − *B* ∧ *basis B* ∧ *C* = *fund-circuit x B*)
⟨*proof*⟩

lemma *fund-circuitI*:
  assumes *basis B*
  assumes $x \in$ *carrier* − *B*
  assumes *circuit C*
  assumes $C \subseteq$ *insert x B*
  shows *fund-circuit x B* = *C*
  ⟨*proof*⟩

definition *fund-circuit-in* **where** *fund-circuit-in* $\mathcal{E}$ *x B* ≡ *matroid.fund-circuit* $\mathcal{E}$ (*indep-in* $\mathcal{E}$) *x B*

context
  fixes $\mathcal{E}$
  assumes ∗: $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *matroid* $\mathcal{E}$ *indep-in* $\mathcal{E}$
  ⟨*proof*⟩

lemma *fund-circuit-inI-aux*: $\mathcal{E}$.*fund-circuit x B* = *fund-circuit-in* $\mathcal{E}$ *x B*
  ⟨*proof*⟩

lemma *circuit-in-elim*:
  assumes *circuit-in* $\mathcal{E}$ C_1 *circuit-in* $\mathcal{E}$ C_2 $C_1 \neq C_2$ $x \in C_1 \cap C_2$
  shows $\exists\, C_3 \subseteq (C_1 \cup C_2) - \{x\}$. *circuit-in* $\mathcal{E}$ C_3
  ⟨*proof*⟩

lemmas *min-dep-in-imp-supset-circuit-in* = $\mathcal{E}$.*min-dep-imp-supset-circuit*[*OF* - *circuit-inD-aux*[*OF* ∗]]

lemma *min-dep-in-imp-ex1-supset-circuit-in*:
  assumes $x \in \mathcal{E}$
  assumes *indep-in* $\mathcal{E}$ X
  assumes $\neg$ *indep-in* $\mathcal{E}$ (*insert* x X)
  shows $\exists!C$. *circuit-in* $\mathcal{E}$ $C \wedge C \subseteq$ *insert* x X
  ⟨*proof*⟩

lemma *basis-in-ex1-supset-circuit-in*:
  assumes *basis-in* $\mathcal{E}$ B
  assumes $x \in \mathcal{E} - B$
  shows $\exists!C$. *circuit-in* $\mathcal{E}$ $C \wedge C \subseteq$ *insert* x B
  ⟨*proof*⟩

lemma *fund-circuit-inI*:
  assumes *basis-in* $\mathcal{E}$ B
  assumes $x \in \mathcal{E} - B$
  assumes *circuit-in* $\mathcal{E}$ C
  assumes $C \subseteq$ *insert* x B
  shows *fund-circuit-in* $\mathcal{E}$ x $B = C$
  ⟨*proof*⟩

end

context
  fixes $\mathcal{E}$
  assumes ∗: $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *matroid* $\mathcal{E}$ *indep-in* $\mathcal{E}$
  ⟨*proof*⟩

lemma *fund-circuit-in-sub-cong*:
  assumes $\mathcal{E}' \subseteq \mathcal{E}$
  assumes $x \in \mathcal{E}' - B$
  assumes *basis-in* $\mathcal{E}'$ B
  shows $\mathcal{E}$.*fund-circuit-in* $\mathcal{E}'$ x B = *fund-circuit-in* $\mathcal{E}'$ x B
⟨*proof*⟩

end

2.4 Ranks

abbreviation *rank-of* **where** *rank-of* ≡ *lower-rank-of*

lemmas *rank-of-def* = *lower-rank-of-def*
lemmas *rank-of-sub-cong* = *lower-rank-of-sub-cong*
lemmas *rank-of-le* = *lower-rank-of-le*

context
  fixes $\mathcal{E}$
  assumes ∗: $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *matroid* $\mathcal{E}$ *indep-in* $\mathcal{E}$
  ⟨*proof*⟩

lemma *lower-rank-of-eq-upper-rank-of*: *lower-rank-of* $\mathcal{E}$ = *upper-rank-of* $\mathcal{E}$
⟨*proof*⟩

lemma *rank-of-eq-card-basis-in*:
  assumes *basis-in* $\mathcal{E}$ *B*
  shows *rank-of* $\mathcal{E}$ = *card B*
⟨*proof*⟩

lemma *rank-of-indep-in-le*:
  assumes *indep-in* $\mathcal{E}$ *X*
  shows *card X* ≤ *rank-of* $\mathcal{E}$
⟨*proof*⟩

end

lemma *rank-of-mono*:
  assumes $X \subseteq Y$
  assumes $Y \subseteq$ *carrier*
  shows *rank-of X* ≤ *rank-of Y*
⟨*proof*⟩

lemma *rank-of-insert-le*:
  assumes $X \subseteq$ *carrier*
  assumes $x \in$ *carrier*
  shows *rank-of* (*insert x X*) ≤ *Suc* (*rank-of X*)
⟨*proof*⟩

lemma *rank-of-Un-Int-le*:
  assumes $X \subseteq$ *carrier*
  assumes $Y \subseteq$ *carrier*
  shows *rank-of* $(X \cup Y)$ + *rank-of* $(X \cap Y)$ ≤ *rank-of X* + *rank-of Y*
⟨*proof*⟩

lemma *rank-of-Un-absorbI*:

assumes $X \subseteq$ *carrier* $Y \subseteq$ *carrier*
assumes $\bigwedge y.\ y \in Y - X \Longrightarrow$ *rank-of* (*insert* y X) = *rank-of* X
shows *rank-of* $(X \cup Y)$ = *rank-of* X
⟨*proof*⟩

lemma *indep-iff-rank-of*:
assumes $X \subseteq$ *carrier*
shows *indep* $X \longleftrightarrow$ *rank-of* X = *card* X
⟨*proof*⟩

lemma *basis-iff-rank-of*:
assumes $X \subseteq$ *carrier*
shows *basis* $X \longleftrightarrow$ *rank-of* X = *card* $X \wedge$ *rank-of* X = *rank-of carrier*
⟨*proof*⟩

lemma *circuit-iff-rank-of*:
assumes $X \subseteq$ *carrier*
shows *circuit* $X \longleftrightarrow X \neq \{\} \wedge (\forall x \in X.$ *rank-of* $(X - \{x\})$ = *card* $(X - \{x\})$ $\wedge$ *card* $(X - \{x\})$ = *rank-of* $X)$
⟨*proof*⟩

context
fixes $\mathcal{E}$
assumes $*$: $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *matroid* $\mathcal{E}$ *indep-in* $\mathcal{E}$
⟨*proof*⟩

lemma *indep-in-iff-rank-of*:
assumes $X \subseteq \mathcal{E}$
shows *indep-in* $\mathcal{E}$ $X \longleftrightarrow$ *rank-of* X = *card* X
⟨*proof*⟩

lemma *basis-in-iff-rank-of*:
assumes $X \subseteq \mathcal{E}$
shows *basis-in* $\mathcal{E}$ $X \longleftrightarrow$ *rank-of* X = *card* $X \wedge$ *rank-of* X = *rank-of* $\mathcal{E}$
⟨*proof*⟩

lemma *circuit-in-iff-rank-of*:
assumes $X \subseteq \mathcal{E}$
shows *circuit-in* $\mathcal{E}$ $X \longleftrightarrow X \neq \{\} \wedge (\forall x \in X.$ *rank-of* $(X - \{x\})$ = *card* $(X - \{x\})$ $\wedge$ *card* $(X - \{x\})$ = *rank-of* $X)$
⟨*proof*⟩

end

2.5 Closure

definition *cl* :: *'a set* ⇒ *'a set* **where**
$cl\ X \equiv \{x \in carrier.\ rank\text{-}of\ (insert\ x\ X) = rank\text{-}of\ X\}$

lemma *clI*:
assumes $x \in carrier$
assumes $rank\text{-}of\ (insert\ x\ X) = rank\text{-}of\ X$
shows $x \in cl\ X$
⟨*proof*⟩

lemma *cl-altdef*:
assumes $X \subseteq carrier$
shows $cl\ X = \bigcup\{Y \in Pow\ carrier.\ X \subseteq Y \wedge rank\text{-}of\ Y = rank\text{-}of\ X\}$
⟨*proof*⟩

lemma *cl-rank-of*: $x \in cl\ X \Longrightarrow rank\text{-}of\ (insert\ x\ X) = rank\text{-}of\ X$
⟨*proof*⟩

lemma *cl-subset-carrier*: $cl\ X \subseteq carrier$
⟨*proof*⟩

lemmas *clD* = *cl-rank-of cl-subset-carrier*

lemma *cl-subset*:
assumes $X \subseteq carrier$
shows $X \subseteq cl\ X$
⟨*proof*⟩

lemma *cl-mono*:
assumes $X \subseteq Y$
assumes $Y \subseteq carrier$
shows $cl\ X \subseteq cl\ Y$
⟨*proof*⟩

lemma *cl-insert-absorb*:
assumes $X \subseteq carrier$
assumes $x \in cl\ X$
shows $cl\ (insert\ x\ X) = cl\ X$
⟨*proof*⟩

lemma *cl-cl-absorb*:
assumes $X \subseteq carrier$
shows $cl\ (cl\ X) = cl\ X$
⟨*proof*⟩

lemma *cl-augment*:
assumes $X \subseteq carrier$
assumes $x \in carrier$

assumes $y \in cl\ (insert\ x\ X) - cl\ X$
shows $x \in cl\ (insert\ y\ X)$
⟨*proof*⟩

lemma *clI-insert*:
assumes $x \in carrier$
assumes *indep X*
assumes $\neg\ indep\ (insert\ x\ X)$
shows $x \in cl\ X$
⟨*proof*⟩

lemma *indep-in-carrier* [*simp*]: *indep-in carrier* = *indep*
⟨*proof*⟩

context
fixes *I*
defines $I \equiv (\lambda X.\ X \subseteq carrier \wedge (\forall x \in X.\ x \notin cl\ (X - \{x\})))$
begin

lemma *I-mono*: *I Y* **if** $Y \subseteq X$ *I X* **for** *X Y* :: *'a set*
⟨*proof*⟩

lemma *clI'*:
assumes *I X* $x \in carrier$ $\neg I\ (insert\ x\ X)$
shows $x \in cl\ X$
⟨*proof*⟩

lemma *matroid-I*: *matroid carrier I*
⟨*proof*⟩

end

definition *cl-in* **where** *cl-in* $\mathcal{E}$ *X* = *matroid.cl* $\mathcal{E}$ (*indep-in* $\mathcal{E}$) *X*

lemma *cl-eq-cl-in*:
assumes $X \subseteq carrier$
shows *cl X* = *cl-in carrier X*
⟨*proof*⟩

context
fixes $\mathcal{E}$
assumes $*$: $\mathcal{E} \subseteq carrier$
begin

interpretation $\mathcal{E}$: *matroid* $\mathcal{E}$ *indep-in* $\mathcal{E}$
⟨*proof*⟩

lemma *cl-inI-aux*: $x \in \mathcal{E}.cl\ X \Longrightarrow x \in cl\text{-}in\ \mathcal{E}\ X$

⟨*proof*⟩

lemma *cl-inD-aux*: $x \in$ *cl-in* $\mathcal{E}$ $X \Longrightarrow x \in \mathcal{E}.cl\ X$
⟨*proof*⟩

lemma *cl-inI*:
assumes $X \subseteq \mathcal{E}$
assumes $x \in \mathcal{E}$
assumes *rank-of* (*insert* x X) = *rank-of* X
shows $x \in$ *cl-in* $\mathcal{E}$ X
⟨*proof*⟩

lemma *cl-in-altdef*:
assumes $X \subseteq \mathcal{E}$
shows *cl-in* $\mathcal{E}$ $X = \bigcup\{Y \in Pow\ \mathcal{E}.\ X \subseteq Y \wedge$ *rank-of* $Y =$ *rank-of* $X\}$
⟨*proof*⟩

lemma *cl-in-subset-carrier*: *cl-in* $\mathcal{E}$ $X \subseteq \mathcal{E}$
⟨*proof*⟩

lemma *cl-in-rank-of*:
assumes $X \subseteq \mathcal{E}$
assumes $x \in$ *cl-in* $\mathcal{E}$ X
shows *rank-of* (*insert* x X) = *rank-of* X
⟨*proof*⟩

lemmas *cl-inD* = *cl-in-rank-of cl-in-subset-carrier*

lemma *cl-in-subset*:
assumes $X \subseteq \mathcal{E}$
shows $X \subseteq$ *cl-in* $\mathcal{E}$ X
⟨*proof*⟩

lemma *cl-in-mono*:
assumes $X \subseteq Y$
assumes $Y \subseteq \mathcal{E}$
shows *cl-in* $\mathcal{E}$ $X \subseteq$ *cl-in* $\mathcal{E}$ Y
⟨*proof*⟩

lemma *cl-in-insert-absorb*:
assumes $X \subseteq \mathcal{E}$
assumes $x \in$ *cl-in* $\mathcal{E}$ X
shows *cl-in* $\mathcal{E}$ (*insert* x X) = *cl-in* $\mathcal{E}$ X
⟨*proof*⟩

lemma *cl-in-augment*:
assumes $X \subseteq \mathcal{E}$
assumes $x \in \mathcal{E}$
assumes $y \in$ *cl-in* $\mathcal{E}$ (*insert* x X) − *cl-in* $\mathcal{E}$ X

shows $x \in$ *cl-in* $\mathcal{E}$ (*insert* y X)
⟨*proof*⟩

lemmas *cl-inI-insert* = *cl-inI-aux*[*OF* $\mathcal{E}$.*clI-insert*]

end

lemma *cl-in-subI*:
assumes $X \subseteq \mathcal{E}'$ $\mathcal{E}' \subseteq \mathcal{E}$ $\mathcal{E} \subseteq$ *carrier*
shows *cl-in* $\mathcal{E}'$ $X \subseteq$ *cl-in* $\mathcal{E}$ X
⟨*proof*⟩

context
fixes $\mathcal{E}$
assumes $*$: $\mathcal{E} \subseteq$ *carrier*
begin

interpretation $\mathcal{E}$: *matroid* $\mathcal{E}$ *indep-in* $\mathcal{E}$
⟨*proof*⟩

lemma *cl-in-sub-cong*:
assumes $X \subseteq \mathcal{E}'$ $\mathcal{E}' \subseteq \mathcal{E}$
shows $\mathcal{E}$.*cl-in* $\mathcal{E}'$ X = *cl-in* $\mathcal{E}'$ X
⟨*proof*⟩

end
end
end

References

[1] J. Oxley. What is a matroid?, 2003.