

Matroids

Jonas Keinholz

June 6, 2026

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	3
1.1	Sub-independence systems	3
1.2	Bases	5
1.3	Circuits	6
1.4	Relation between independence and bases	9
1.5	Relation between dependence and circuits	10
1.6	Ranks	11
2	Matroids	12
2.1	Minors	12
2.2	Bases	13
2.3	Circuits	13
2.4	Ranks	16
2.5	Closure	18

1 Independence systems

```
theory Indep-System
  imports Main
begin
```

```
lemma finite-psubset-inc-induct:
  assumes finite  $A$   $X \subseteq A$ 
  assumes  $\bigwedge X. (\bigwedge Y. X \subset Y \implies Y \subseteq A \implies P Y) \implies P X$ 
  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 carrier :: 'a set
  fixes indep :: 'a set  $\Rightarrow$  bool
  assumes carrier-finite: finite carrier
  assumes indep-subset-carrier: indep  $X \implies X \subseteq$  carrier
  assumes indep-ex:  $\exists X. \textit{indep } X$ 
  assumes indep-subset: indep  $X \implies Y \subseteq X \implies \textit{indep } Y$ 
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 *indep-in* $\mathcal{E} X \longleftrightarrow X \subseteq \mathcal{E} \wedge \textit{indep } X$

```
lemma indep-inI:
  assumes  $X \subseteq \mathcal{E}$ 
  assumes indep  $X$ 
  shows indep-in  $\mathcal{E} X$ 
  <proof>
```

```
lemma indep-in-subI: indep-in  $\mathcal{E} X \implies \textit{indep-in } \mathcal{E}' (X \cap \mathcal{E}')$ 
  <proof>
```

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

shows $\neg \text{indep-in } \mathcal{E}' X \implies \neg \text{indep-in } \mathcal{E} X$
<proof>

lemma *indep-in-subset-carrier*: $\text{indep-in } \mathcal{E} X \implies X \subseteq \mathcal{E}$
<proof>

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

lemma *indep-in-supI*:
assumes $X \subseteq \mathcal{E}' \mathcal{E}' \subseteq \mathcal{E}$
assumes $\text{indep-in } \mathcal{E} X$
shows $\text{indep-in } \mathcal{E}' X$
<proof>

lemma *indep-in-indep*: $\text{indep-in } \mathcal{E} X \implies \text{indep } X$
<proof>

lemmas $\text{indep-in}D = \text{indep-in-subset-carrier } \text{indep-in-indep}$

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

interpretation \mathcal{E} : $\text{indep-system } \mathcal{E} \text{ indep-in } \mathcal{E}$
<proof>

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

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

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** $\text{basis } X \longleftrightarrow \text{indep } X \wedge (\forall x \in \text{carrier} - X. \neg \text{indep } (\text{insert } x \ X))$

lemma *basisI*:

assumes $\text{indep } X$

assumes $\bigwedge x. x \in \text{carrier} - X \implies \neg \text{indep } (\text{insert } x \ X)$

shows $\text{basis } X$

$\langle \text{proof} \rangle$

lemma *basis-indep*: $\text{basis } X \implies \text{indep } X$

$\langle \text{proof} \rangle$

lemma *basis-max-indep*: $\text{basis } X \implies x \in \text{carrier} - X \implies \neg \text{indep } (\text{insert } x \ X)$

$\langle \text{proof} \rangle$

lemmas $\text{basisD} = \text{basis-indep } \text{basis-max-indep}$

lemmas $\text{basis-subset-carrier} = \text{indep-subset-carrier}[\text{OF } \text{basis-indep}]$

lemmas $\text{basis-finite} [\text{simp}] = \text{indep-finite}[\text{OF } \text{basis-indep}]$

lemma *indep-not-basis*:

assumes $\text{indep } X$

assumes $\neg \text{basis } X$

shows $\exists x \in \text{carrier} - X. \text{indep } (\text{insert } x \ X)$

$\langle \text{proof} \rangle$

lemma *basis-subset-eq*:

assumes $\text{basis } B_1$

assumes $\text{basis } B_2$

assumes $B_1 \subseteq B_2$

shows $B_1 = B_2$

$\langle \text{proof} \rangle$

definition *basis-in* **where**

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

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

$\langle \text{proof} \rangle$

context

fixes \mathcal{E}

assumes $\mathcal{E} \subseteq \text{carrier}$

begin

interpretation \mathcal{E} : *indep-system* \mathcal{E} *indep-in* \mathcal{E}

<proof>

lemma *basis-inI-aux*: $\mathcal{E}.basis\ X \implies basis-in\ \mathcal{E}\ X$

<proof>

lemma *basis-inD-aux*: $basis-in\ \mathcal{E}\ X \implies \mathcal{E}.basis\ X$

<proof>

lemma *not-basis-inD-aux*: $\neg basis-in\ \mathcal{E}\ X \implies \neg \mathcal{E}.basis\ X$

<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 $\bigwedge x. x \in X \implies \text{indep } (X - \{x\})$
shows *circuit* X
 $\langle \text{proof} \rangle$

lemma *circuit-subset-carrier*: *circuit* $X \implies X \subseteq \text{carrier}$
 $\langle \text{proof} \rangle$

lemmas *circuit-finite* [*simp*] = *finite-subset*[*OF circuit-subset-carrier carrier-finite*]

lemma *circuit-dep*: *circuit* $X \implies \neg \text{indep } X$
 $\langle \text{proof} \rangle$

lemma *circuit-min-dep*: *circuit* $X \implies x \in X \implies \text{indep } (X - \{x\})$
 $\langle \text{proof} \rangle$

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

lemma *circuit-nonempty*: *circuit* $X \implies X \neq \{\}$
 $\langle \text{proof} \rangle$

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

lemma *circuit-subset-eq*:
assumes *circuit* C_1
assumes *circuit* C_2
assumes $C_1 \subseteq C_2$
shows $C_1 = C_2$
 $\langle \text{proof} \rangle$

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

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

interpretation \mathcal{E} : *indep-system* \mathcal{E} *indep-in* \mathcal{E}
 $\langle \text{proof} \rangle$

lemma *circuit-inI-aux*: $\mathcal{E}.\text{circuit } X \implies \text{circuit-in } \mathcal{E} X$
 $\langle \text{proof} \rangle$

lemma *circuit-inD-aux*: *circuit-in* $\mathcal{E} X \implies \mathcal{E}.\text{circuit } X$
 $\langle \text{proof} \rangle$

lemma *not-circuit-inD-aux*: $\neg \text{circuit-in } \mathcal{E} X \implies \neg \mathcal{E}.\text{circuit } X$

<proof>

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

lemmas *circuit-in-subset-carrier* = $\mathcal{E}.\text{circuit-subset-carrier}$ [*OF* *circuit-inD-aux*]

lemmas *circuit-in-finite* = $\mathcal{E}.\text{circuit-finite}$ [*OF* *circuit-inD-aux*]

lemmas *circuit-in-dep-in* = $\mathcal{E}.\text{circuit-dep}$ [*OF* *circuit-inD-aux*]

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

lemmas *circuit-inD* = $\mathcal{E}.\text{circuitD}$ [*OF* *circuit-inD-aux*]

lemmas *circuit-in-nonempty* = $\mathcal{E}.\text{circuit-nonempty}$ [*OF* *circuit-inD-aux*]

lemmas *dep-in-not-circuit-in* = $\mathcal{E}.\text{dep-not-circuit}$ [*OF* - - *not-circuit-inD-aux*]

lemmas *circuit-in-subset-eq* = $\mathcal{E}.\text{circuit-subset-eq}$ [*OF* *circuit-inD-aux* *circuit-inD-aux*]

end

lemma *circuit-in-subI*:

assumes $\mathcal{E}' \subseteq \mathcal{E}$ $\mathcal{E} \subseteq \text{carrier}$

assumes *circuit-in* $\mathcal{E}' C$

shows *circuit-in* $\mathcal{E} C$

<proof>

lemma *circuit-in-supI*:

assumes $\mathcal{E}' \subseteq \mathcal{E}$ $\mathcal{E} \subseteq \text{carrier}$ $C \subseteq \mathcal{E}'$

assumes *circuit-in* $\mathcal{E} C$

shows *circuit-in* $\mathcal{E}' C$

<proof>

context

fixes \mathcal{E}

assumes *: $\mathcal{E} \subseteq \text{carrier}$

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 $\mathcal{E}.\text{circuit-in } \mathcal{E}' C \longleftrightarrow \text{circuit-in } \mathcal{E}' C$

<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 $\exists B. \text{basis } B \wedge X \subseteq B$
 <proof>

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

lemma *indep-iff-subset-basis*: $\text{indep } X \longleftrightarrow (\exists B. \text{basis } B \wedge X \subseteq B)$
 <proof>

lemma *basis-ex*: $\exists B. \text{basis } B$
 <proof>

context
 fixes \mathcal{E}
 assumes $*$: $\mathcal{E} \subseteq \text{carrier}$
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 $\exists B. \text{basis-in } \mathcal{E} B \wedge X \subseteq B$
 <proof>

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

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

lemma *basis-in-ex*: $\exists B. \text{basis-in } \mathcal{E} B$
 <proof>

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

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

assumes $\neg \text{indep } X$

shows $\exists C. \text{circuit } C \wedge C \subseteq X$

<proof>

lemma *supset-circuit-imp-dep:*

assumes $\text{circuit } C \wedge C \subseteq X$

shows $\neg \text{indep } X$

<proof>

lemma *dep-iff-supset-circuit:*

assumes $X \subseteq \text{carrier}$

shows $\neg \text{indep } X \longleftrightarrow (\exists C. \text{circuit } C \wedge C \subseteq X)$

<proof>

context

fixes \mathcal{E}

assumes $\mathcal{E} \subseteq \text{carrier}$

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 $\neg \text{indep-in } \mathcal{E} X$

shows $\exists C. \text{circuit-in } \mathcal{E} C \wedge C \subseteq X$

<proof>

lemma *supset-circuit-in-imp-dep-in:*

assumes $\text{circuit-in } \mathcal{E} C \wedge C \subseteq X$

shows $\neg \text{indep-in } \mathcal{E} X$

<proof>

lemma *dep-in-iff-supset-circuit-in:*

assumes $X \subseteq \mathcal{E}$

shows $\neg \text{indep-in } \mathcal{E} X \longleftrightarrow (\exists C. \text{circuit-in } \mathcal{E} C \wedge C \subseteq X)$

<proof>

end

1.6 Ranks

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

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

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

context
fixes \mathcal{E}
assumes *: $\mathcal{E} \subseteq \text{carrier}$
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 ≤ card A*
 shows $\exists B \subseteq A. \text{card } B = n$
 $\langle \text{proof} \rangle$

locale *matroid = indep-system +*
 assumes *augment-aux*:
 $\text{indep } X \implies \text{indep } Y \implies \text{card } X = \text{Suc } (\text{card } Y) \implies \exists x \in X - Y. \text{indep } (\text{insert } x Y)$
 $\langle \text{insert } x Y \rangle$
begin

lemma *augment*:
 assumes *indep X indep Y card Y < card X*
 shows $\exists x \in X - Y. \text{indep } (\text{insert } x Y)$
 $\langle \text{proof} \rangle$

lemma *augment-psubset*:
 assumes *indep X indep Y Y ⊂ X*
 shows $\exists x \in X - Y. \text{indep } (\text{insert } x Y)$
 $\langle \text{proof} \rangle$

2.1 Minors

A subset of the ground set induces a matroid.

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

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

interpretation \mathcal{E} : *matroid* \mathcal{E} (*indep-in* \mathcal{E})
 $\langle \text{proof} \rangle$

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 $card\ B_1 = card\ B_2$
 $\langle proof \rangle$

lemma *basis-indep-card*:
assumes *indep* X
assumes *basis* B
shows $card\ X \leq card\ B$
 $\langle proof \rangle$

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

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

interpretation \mathcal{E} : *matroid* \mathcal{E} *indep-in* \mathcal{E}
 $\langle proof \rangle$

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 $\exists y \in B_2 - B_1. basis-in\ \mathcal{E}\ (insert\ y\ (B_1 - \{x\}))$
 $\langle proof \rangle$

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 $\exists C_3 \subseteq (C_1 \cup C_2) - \{x\}. circuit\ C_3$
 $\langle proof \rangle$

lemma *min-dep-imp-supset-circuit*:

assumes *indep X*

assumes *circuit C*

assumes $C \subseteq \text{insert } x \ X$

shows $x \in C$

<proof>

lemma *min-dep-imp-ex1-supset-circuit*:

assumes $x \in \text{carrier}$

assumes *indep X*

assumes $\neg \text{indep } (\text{insert } x \ X)$

shows $\exists! C. \text{circuit } C \wedge C \subseteq \text{insert } x \ X$

<proof>

lemma *basis-ex1-supset-circuit*:

assumes *basis B*

assumes $x \in \text{carrier} - B$

shows $\exists! C. \text{circuit } C \wedge C \subseteq \text{insert } x \ B$

<proof>

definition *fund-circuit* :: 'a \Rightarrow 'a set \Rightarrow 'a set **where**

fund-circuit $x \ B \equiv (\text{THE } C. \text{circuit } C \wedge C \subseteq \text{insert } x \ B)$

lemma *circuit-iff-fund-circuit*:

circuit $C \longleftrightarrow (\exists x \ B. x \in \text{carrier} - B \wedge \text{basis } B \wedge C = \text{fund-circuit } x \ B)$

<proof>

lemma *fund-circuitI*:

assumes *basis B*

assumes $x \in \text{carrier} - B$

assumes *circuit C*

assumes $C \subseteq \text{insert } x \ B$

shows $\text{fund-circuit } x \ B = C$

<proof>

definition *fund-circuit-in* **where** *fund-circuit-in* $\mathcal{E} \ x \ B \equiv \text{matroid.fund-circuit } \mathcal{E}$

(indep-in $\mathcal{E}) \ x \ B$

context

fixes \mathcal{E}

assumes *: $\mathcal{E} \subseteq \text{carrier}$

begin

interpretation \mathcal{E} : *matroid* \mathcal{E} *indep-in* \mathcal{E}

<proof>

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

<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* \equiv *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 $*$: $\mathcal{E} \subseteq \text{carrier}$

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* $X \leq$ *rank-of* \mathcal{E}

<proof>

end

lemma *rank-of-mono*:

assumes $X \subseteq Y$

assumes $Y \subseteq \text{carrier}$

shows *rank-of* $X \leq$ *rank-of* Y

<proof>

lemma *rank-of-insert-le*:

assumes $X \subseteq \text{carrier}$

assumes $x \in \text{carrier}$

shows *rank-of* (*insert* x X) \leq *Suc* (*rank-of* X)

<proof>

lemma *rank-of-Un-Int-le*:

assumes $X \subseteq \text{carrier}$

assumes $Y \subseteq \text{carrier}$

shows *rank-of* ($X \cup Y$) + *rank-of* ($X \cap Y$) \leq *rank-of* X + *rank-of* Y

<proof>

lemma *rank-of-Un-absorbI*:

assumes $X \subseteq \text{carrier } Y \subseteq \text{carrier}$
assumes $\bigwedge y. y \in Y - X \implies \text{rank-of } (\text{insert } y \ X) = \text{rank-of } X$
shows $\text{rank-of } (X \cup Y) = \text{rank-of } X$
 <proof>

lemma *indep-iff-rank-of*:
assumes $X \subseteq \text{carrier}$
shows $\text{indep } X \longleftrightarrow \text{rank-of } X = \text{card } X$
 <proof>

lemma *basis-iff-rank-of*:
assumes $X \subseteq \text{carrier}$
shows $\text{basis } X \longleftrightarrow \text{rank-of } X = \text{card } X \wedge \text{rank-of } X = \text{rank-of } \text{carrier}$
 <proof>

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

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

interpretation \mathcal{E} : *matroid \mathcal{E} indep-in \mathcal{E}*
 <proof>

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

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

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

end

2.5 Closure

definition $cl :: 'a \text{ set} \Rightarrow 'a \text{ set}$ **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 $x \in cl\ X$

$\langle proof \rangle$

lemma $cl\text{-altdef}$:

assumes $X \subseteq carrier$

shows $cl\ X = \bigcup \{Y \in Pow\ carrier. X \subseteq Y \wedge rank\text{-of}\ Y = rank\text{-of}\ X\}$

$\langle proof \rangle$

lemma $cl\text{-rank-of}$: $x \in cl\ X \implies rank\text{-of}\ (insert\ x\ X) = rank\text{-of}\ X$

$\langle proof \rangle$

lemma $cl\text{-subset-carrier}$: $cl\ X \subseteq carrier$

$\langle proof \rangle$

lemmas $clD = cl\text{-rank-of}\ cl\text{-subset-carrier}$

lemma $cl\text{-subset}$:

assumes $X \subseteq carrier$

shows $X \subseteq cl\ X$

$\langle proof \rangle$

lemma $cl\text{-mono}$:

assumes $X \subseteq Y$

assumes $Y \subseteq carrier$

shows $cl\ X \subseteq cl\ Y$

$\langle proof \rangle$

lemma $cl\text{-insert-absorb}$:

assumes $X \subseteq carrier$

assumes $x \in cl\ X$

shows $cl\ (insert\ x\ X) = cl\ X$

$\langle proof \rangle$

lemma $cl\text{-cl-absorb}$:

assumes $X \subseteq carrier$

shows $cl\ (cl\ X) = cl\ X$

$\langle proof \rangle$

lemma $cl\text{-augment}$:

assumes $X \subseteq carrier$

assumes $x \in carrier$

assumes $y \in \text{cl} (\text{insert } x X) - \text{cl } X$
shows $x \in \text{cl} (\text{insert } y X)$
 $\langle \text{proof} \rangle$

lemma *clI-insert*:

assumes $x \in \text{carrier}$
assumes $\text{indep } X$
assumes $\neg \text{indep} (\text{insert } x X)$
shows $x \in \text{cl } X$
 $\langle \text{proof} \rangle$

lemma *indep-in-carrier [simp]*: $\text{indep-in carrier} = \text{indep}$
 $\langle \text{proof} \rangle$

context

fixes I

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

begin

lemma *I-mono*: $I Y$ **if** $Y \subseteq X$ **I** X **for** $X Y$ **::** 'a set
 $\langle \text{proof} \rangle$

lemma *clI'*:

assumes $I X$ $x \in \text{carrier}$ $\neg I (\text{insert } x X)$
shows $x \in \text{cl } X$
 $\langle \text{proof} \rangle$

lemma *matroid-I*: $\text{matroid carrier } I$
 $\langle \text{proof} \rangle$

end

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

lemma *cl-eq-cl-in*:

assumes $X \subseteq \text{carrier}$
shows $\text{cl } X = \text{cl-in carrier } X$
 $\langle \text{proof} \rangle$

context

fixes \mathcal{E}

assumes $*$: $\mathcal{E} \subseteq \text{carrier}$

begin

interpretation \mathcal{E} : $\text{matroid } \mathcal{E}$ $\text{indep-in } \mathcal{E}$
 $\langle \text{proof} \rangle$

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

<proof>

lemma *cl-inD-aux*: $x \in \text{cl-in } \mathcal{E} X \implies x \in \mathcal{E}.cl X$
<proof>

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

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

lemma *cl-in-subset-carrier*: $\text{cl-in } \mathcal{E} X \subseteq \mathcal{E}$
<proof>

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

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

lemma *cl-in-subset*:
assumes $X \subseteq \mathcal{E}$
shows $X \subseteq \text{cl-in } \mathcal{E} X$
<proof>

lemma *cl-in-mono*:
assumes $X \subseteq Y$
assumes $Y \subseteq \mathcal{E}$
shows $\text{cl-in } \mathcal{E} X \subseteq \text{cl-in } \mathcal{E} Y$
<proof>

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

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

```

shows  $x \in \text{cl-in } \mathcal{E} \text{ (insert } y \ X)$ 
   $\langle \text{proof} \rangle$ 

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

end

lemma  $\text{cl-in-subI}$ :
  assumes  $X \subseteq \mathcal{E}' \ \mathcal{E}' \subseteq \mathcal{E} \ \mathcal{E} \subseteq \text{carrier}$ 
  shows  $\text{cl-in } \mathcal{E}' \ X \subseteq \text{cl-in } \mathcal{E} \ X$ 
   $\langle \text{proof} \rangle$ 

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

interpretation  $\mathcal{E}$ : matroid  $\mathcal{E}$  indep-in  $\mathcal{E}$ 
   $\langle \text{proof} \rangle$ 

lemma  $\text{cl-in-sub-cong}$ :
  assumes  $X \subseteq \mathcal{E}' \ \mathcal{E}' \subseteq \mathcal{E}$ 
  shows  $\mathcal{E}.\text{cl-in } \mathcal{E}' \ X = \text{cl-in } \mathcal{E}' \ X$ 
   $\langle \text{proof} \rangle$ 

end
end
end

```

References

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