A Sound and Complete Calculus for Probability Inequalities

Matthew Doty

December 9, 2023

Abstract

We give a sound an complete multiple-conclusion calculus $\$ \vdash$ for finitely additive probability inequalities. In particular, we show

$$\sim\!\Gamma \$ \vdash \sim\!\Phi \equiv \forall \mathcal{P} \in \mathit{probabilities}. \sum \phi \leftarrow \Phi.\ \mathcal{P}\phi \leq \sum \gamma \leftarrow \Gamma.\ \mathcal{P}\gamma$$

...where $\sim \Gamma$ is the negation of all of the formulae in Γ (and similarly for $\sim \Phi$). We prove this by using an abstract form of *MaxSAT*. We also show

$$\mathit{MaxSAT}(\sim\!\Gamma \mathbin{@} \Phi) + c \leq \mathit{length}\, \Gamma \equiv \forall \mathcal{P} \in \mathit{probabilities}. \left(\sum \phi \leftarrow \Phi.\ \mathcal{P}\phi\right) + c \leq \sum \gamma \leftarrow \Gamma.\ \mathcal{P}\gamma$$

Finally, we establish a *collapse theorem*, which asserts that $(\sum \phi \leftarrow \Phi.\ \mathcal{P}\phi) + c \leq \sum \gamma \leftarrow \Gamma.\ \mathcal{P}\gamma$ holds for all probabilities $\mathcal{P}$ if and only if $(\sum \phi \leftarrow \Phi.\ \delta\phi) + c \leq \sum \gamma \leftarrow \Gamma.\ \delta\gamma$ holds for all binary-valued probabilities δ.

Contents

Chapter 1

Introduction

theory *Probability-Inequality-Completeness*
  imports
    Suppes-Theorem.Probability-Logic
begin

no-notation *FuncSet.funcset* (**infixr** $\rightarrow$ *60*)

We introduce a novel logical calculus and prove completeness for probability inequalities. This is a vast generalization of *Suppes' Theorem* which lays the foundation for this theory.

We provide two new logical judgements: *measure deduction* ($\$\vdash$) and *counting deduction* ($\#\vdash$). Both judgements capture a notion of *measure* or quantity. In both cases premises must be partially or completely *consumed* in sense to prove multiple conclusions. That is to say, a portion of the premises must be used to prove each conclusion which cannot be reused. Counting deduction counts the number of times a particular conclusion can be proved (as the name implies), while measure deduction includes multiple, different conclusions which must be proven via the premises.

We also introduce an abstract notion of MaxSAT, which is the maximal number of clauses in a list of clauses that can be simultaneously satisfied.

We show the following are equivalent:

- $\sim \Gamma \ \$\vdash \ \sim \Phi$
- $(\sim \Gamma \ @ \ \Phi) \ \#\vdash \ (\textit{length}\ \Phi)\ \bot$
- $\textit{MaxSAT}\ (\sim \Gamma \ @ \ \Phi) \leq \textit{length}\ \Gamma$
- $\forall\ \delta \in \textit{dirac-measures}.\ (\sum \varphi \leftarrow \Phi.\ \delta\ \varphi) \leq (\sum \gamma \leftarrow \Gamma.\ \delta\ \gamma)$
- $\forall\ \mathcal{P} \in \textit{probabilities}.\ (\sum \varphi \leftarrow \Phi.\ \mathcal{P}\ \varphi) \leq (\sum \gamma \leftarrow \Gamma.\ \mathcal{P}\ \gamma)$

In the special case of MaxSAT, we show the following are equivalent:

- $\mathit{MaxSAT}\ (\sim \Gamma\ @\ \Phi) + c \leq \mathit{length}\ \Gamma$
- $\forall\ \delta \in \mathit{dirac\text{-}measures}.\ (\sum \varphi \leftarrow \Phi.\ \delta\ \varphi) + c \leq (\sum \gamma \leftarrow \Gamma.\ \delta\ \gamma)$
- $\forall\ \mathcal{P} \in \mathit{probabilities}.\ (\sum \varphi \leftarrow \Phi.\ \mathcal{P}\ \varphi) + c \leq (\sum \gamma \leftarrow \Gamma.\ \mathcal{P}\ \gamma)$

Chapter 2

Measure Deduction and Counting Deduction

2.1 Definition of Measure Deduction

To start, we introduce a common combinator for modifying functions that take two arguments.

definition *uncurry* :: $('a \Rightarrow 'b \Rightarrow 'c) \Rightarrow 'a \times 'b \Rightarrow 'c$
  where *uncurry-def* [*simp*]: *uncurry* $f = (\lambda\ (x,\ y).\ f\ x\ y)$

Our new logical calculus is a recursively defined relation ($\$\vdash$) using *list deduction* ($:\vdash$).

We call our new logical relation *measure deduction*:

primrec (**in** *classical-logic*)
  measure-deduction :: $'a\ list \Rightarrow 'a\ list \Rightarrow bool$ (**infix** $\$\vdash$ *60*)
  where
    $\Gamma\ \$\vdash\ [] = True$
  $|\ \Gamma\ \$\vdash\ (\varphi\ \#\ \Phi) =$
      $(\exists\ \Psi.\ mset\ (map\ snd\ \Psi) \subseteq\#\ mset\ \Gamma$
          $\wedge\ map\ (uncurry\ (\sqcup))\ \Psi\ :\vdash\ \varphi$
          $\wedge\ map\ (uncurry\ (\rightarrow))\ \Psi\ @\ \Gamma \ominus (map\ snd\ \Psi)\ \$\vdash\ \Phi)$

Let us briefly analyze what the above definition is saying.

From the above we must find a special list-of-pairs Ψ, which we refer to as a *witness*, in order to establish $\Gamma\ \$\vdash\ \varphi\ \#\ \Phi$.

We may motivate measure deduction as follows. In the simplest case we know $\mathcal{P}\ \varphi \leq \mathcal{P}\ \psi + \Sigma$ if and only if $\mathcal{P}\ (\ \chi \sqcup \varphi\ ) + \mathcal{P}\ (\ \sim \chi \sqcup \varphi\ ) \leq \mathcal{P}\ \psi + \Sigma$, or equivalently $\mathcal{P}\ (\ \chi \sqcup \varphi\ ) + \mathcal{P}\ (\ \chi \rightarrow \varphi\ ) \leq \mathcal{P}\ \psi + \Sigma$. So it suffices to prove $\mathcal{P}\ (\ \chi \sqcup \varphi\ ) \leq \mathcal{P}\ \psi$ and $\mathcal{P}\ (\ \chi \rightarrow \varphi\ ) \leq \Sigma$. Here $[(\chi,\varphi)]$ is like the *witness* in our recursive definition, which reflects the $\exists\ \Psi.\ \ldots$ formula is our definition. The fact that measure deduction reflects proving theorems in the theory of inequalities of probability logic is the elementary intuition behind the soundness theorem we will ultimately prove in §2.12.

A key difference from the simple motivation above is that, as in the case of Suppes' Theorem where we prove $\sim \Gamma :\vdash \sim \varphi$ if and only if $\mathcal{P}\ \varphi \leq (\sum\ \gamma \leftarrow \Gamma\ .\ \mathcal{P}\ \gamma)$ for all $\mathcal{P}$, soundness in this context means $\sim \Gamma\ \$\vdash\ \sim \Phi$ implies $\forall\ \mathcal{P}.\ (\sum \gamma{\leftarrow}\Gamma.\ \mathcal{P}\ \gamma) \geq (\sum \varphi{\leftarrow}\Phi.\ \mathcal{P}\ \varphi)$.

Another way of thinking about measure deduction is to think of Γ and Σ as bags of balls of soft clay and $\Gamma\ \$\vdash\ \Sigma$ meaning that we have shown Γ is *heavier than* Σ (ignoring, for the moment, that $(\$\vdash)$ is not totally ordered). We have a scale $(:\vdash)$ that lets us weigh several things on the left and one thing on the right at a time. We go through each clay ball σ in Σ one at a time without replacement, putting σ on the right of the scale. Then, we take a bunch of clay balls from Γ, cut them up as necessary (that is the $\psi \sqcup \gamma$ trick using the witness Ψ), and show they are heavier using our scale. We take the parts $\psi \to \gamma$ that we didn't use and put them back in our bag Γ. We will be able to reuse them later. If we can do this trick for every element σ in Σ successively using combinations of split leftovers in Γ, then we can show Γ is heavier than Σ (i.e., $\Gamma\ \$\vdash\ \Sigma$).

2.2 Definition of the Stronger Theory Relation

We next turn to looking at a subrelation of $(\$\vdash)$, which we call the *stronger theory* relation $(\preceq)$. Here we construe a *theory* as a list of propositions. We say theory Γ is *stronger than* Σ where, for each element σ in Σ, we can take an element γ of Γ *without replacement* such that $\vdash \gamma \to \sigma$.

To motivate this notion, let's reuse the metaphor that Γ and Σ are bags of balls of clay, and we need to show Γ is heavier without simply weighing the two bags. A sufficient (but incomplete) approach is to take each ball of clay σ in Σ and find another ball of clay γ in Γ (without replacement) that is heavier. This simple approach avoids the complexity of iteratively cutting up balls of clay.

definition (**in** *implication-logic*)
  stronger-theory-relation :: *'a list* $\Rightarrow$ *'a list* $\Rightarrow$ *bool* (**infix** $\preceq$ *100*)
  where
    $\Sigma \preceq \Gamma =$
      $(\exists\ \Phi.\ \mathit{map\ snd}\ \Phi = \Sigma$
        $\wedge\ \mathit{mset}\ (\mathit{map\ fst}\ \Phi) \subseteq\#\ \mathit{mset}\ \Gamma$
        $\wedge\ (\forall\ (\gamma,\sigma) \in \mathit{set}\ \Phi.\ \vdash \gamma \to \sigma))$

abbreviation (**in** *implication-logic*)
  stronger-theory-relation-op :: *'a list* $\Rightarrow$ *'a list* $\Rightarrow$ *bool* (**infix** $\succeq$ *100*)
  where
    $\Gamma \succeq \Sigma \equiv \Sigma \preceq \Gamma$

2.3 The Stronger Theory Relation is a Preorder

Next, we show that $(\preceq)$ is a preorder by establishing reflexivity and transitivity.

We first prove the following lemma with respect to multisets and stronger theories.

lemma (**in** *implication-logic*) *msub-stronger-theory-intro*:
  assumes *mset* $\Sigma \subseteq\#$ *mset* Γ
  shows $\Sigma \preceq \Gamma$
⟨*proof*⟩

The *reflexive* property immediately follows:

lemma (**in** *implication-logic*) *stronger-theory-reflexive* [*simp*]: $\Gamma \preceq \Gamma$
  ⟨*proof*⟩

lemma (**in** *implication-logic*) *weakest-theory* [*simp*]: $[] \preceq \Gamma$
  ⟨*proof*⟩

lemma (**in** *implication-logic*) *stronger-theory-empty-list-intro* [*simp*]:
  assumes $\Gamma \preceq []$
  shows $\Gamma = []$
  ⟨*proof*⟩

Next, we turn to proving transitivity. We first prove two permutation theorems.

lemma (**in** *implication-logic*) *stronger-theory-right-permutation*:
  assumes $\Gamma \rightleftharpoons \Delta$
    and $\Sigma \preceq \Gamma$
   shows $\Sigma \preceq \Delta$
⟨*proof*⟩

lemma (**in** *implication-logic*) *stronger-theory-left-permutation*:
  assumes $\Sigma \rightleftharpoons \Delta$
    and $\Sigma \preceq \Gamma$
   shows $\Delta \preceq \Gamma$
⟨*proof*⟩

lemma (**in** *implication-logic*) *stronger-theory-transitive*:
  assumes $\Sigma \preceq \Delta$ **and** $\Delta \preceq \Gamma$
   shows $\Sigma \preceq \Gamma$
⟨*proof*⟩

2.4 The Stronger Theory Relation is a Subrelation of of Measure Deduction

Next, we show that $\Gamma \succeq \Sigma$ implies $\Gamma \ \$\!\vdash \Sigma$. Before doing so we establish several helpful properties regarding the stronger theory relation ($\succeq$).

lemma (**in** *implication-logic*) *stronger-theory-witness*:
  assumes $\sigma \in \mathit{set}\ \Sigma$
    shows $\Sigma \preceq \Gamma = (\exists\ \gamma \in \mathit{set}\ \Gamma.\ \vdash \gamma \to \sigma \wedge (\mathit{remove1}\ \sigma\ \Sigma) \preceq (\mathit{remove1}\ \gamma\ \Gamma))$
⟨*proof*⟩

lemma (**in** *implication-logic*) *stronger-theory-cons-witness*:
  $(\sigma \# \Sigma) \preceq \Gamma = (\exists\ \gamma \in \mathit{set}\ \Gamma.\ \vdash \gamma \to \sigma \wedge \Sigma \preceq (\mathit{remove1}\ \gamma\ \Gamma))$
⟨*proof*⟩

lemma (**in** *implication-logic*) *stronger-theory-left-cons*:
  assumes $(\sigma \# \Sigma) \preceq \Gamma$
  shows $\Sigma \preceq \Gamma$
⟨*proof*⟩

lemma (**in** *implication-logic*) *stronger-theory-right-cons*:
  assumes $\Sigma \preceq \Gamma$
  shows $\Sigma \preceq (\gamma \# \Gamma)$
⟨*proof*⟩

lemma (**in** *implication-logic*) *stronger-theory-left-right-cons*:
  assumes $\vdash \gamma \to \sigma$
    and $\Sigma \preceq \Gamma$
  shows $(\sigma \# \Sigma) \preceq (\gamma \# \Gamma)$
⟨*proof*⟩

lemma (**in** *implication-logic*) *stronger-theory-relation-alt-def*:
  $\Sigma \preceq \Gamma = (\exists \Phi.\ \mathit{mset}\ (\mathit{map}\ \mathit{snd}\ \Phi) = \mathit{mset}\ \Sigma\ \wedge$
        $\mathit{mset}\ (\mathit{map}\ \mathit{fst}\ \Phi) \subseteq\#\ \mathit{mset}\ \Gamma\ \wedge$
        $(\forall (\gamma, \sigma) {\in} \mathit{set}\ \Phi.\ \vdash \gamma \to \sigma))$
⟨*proof*⟩

lemma (**in** *implication-logic*) *stronger-theory-deduction-monotonic*:
  assumes $\Sigma \preceq \Gamma$
    and $\Sigma :\vdash \varphi$
  shows $\Gamma :\vdash \varphi$
⟨*proof*⟩

lemma (**in** *classical-logic*) *measure-msub-left-monotonic*:
  assumes $\mathit{mset}\ \Sigma \subseteq\#\ \mathit{mset}\ \Gamma$
    and $\Sigma \ \$\!\vdash \Phi$
  shows $\Gamma \ \$\!\vdash \Phi$
⟨*proof*⟩

lemma (**in** *classical-logic*) *witness-weaker-theory*:
  assumes *mset* (*map snd* Σ) $\subseteq\#$ *mset* Γ
  shows *map* (*uncurry* ($\sqcup$)) $\Sigma \preceq \Gamma$
$\langle$*proof*$\rangle$

lemma (**in** *implication-logic*) *stronger-theory-combine*:
  assumes $\Phi \preceq \Delta$
    and $\Psi \preceq \Gamma$
   shows $(\Phi @ \Psi) \preceq (\Delta @ \Gamma)$
$\langle$*proof*$\rangle$

We now turn to proving that $(\succeq)$ is a subrelation of $(:\vdash)$.

lemma (**in** *classical-logic*) *stronger-theory-to-measure-deduction*:
  assumes $\Gamma \succeq \Sigma$
  shows Γ $\$\vdash$ Σ
$\langle$*proof*$\rangle$

2.5 Measure Deduction is a Preorder

We next show that measure deduction is a preorder.

Reflexivity follows immediately because $(\preceq)$ is a subrelation and is itself reflexive.

theorem (**in** *classical-logic*) *measure-reflexive*: Γ $\$\vdash$ Γ
  $\langle$*proof*$\rangle$

Transitivity is complicated. It requires constructing many witnesses and involves a lot of metatheorems. Below we provide various witness constructions that allow us to establish $[\![\Gamma \;\$\vdash\; \Lambda;\ \Lambda \;\$\vdash\; \Delta]\!] \Longrightarrow \Gamma \;\$\vdash\; \Delta$.

primrec (**in** *implication-logic*)
  first-component :: $('a \times 'a)$ *list* $\Rightarrow$ $('a \times 'a)$ *list* $\Rightarrow$ $('a \times 'a)$ *list* ($\mathfrak{A}$)
  where
   $\mathfrak{A}\ \Psi\ [] = []$
  | $\mathfrak{A}\ \Psi\ (\delta \# \Delta) =$
     (*case find* ($\lambda\ \psi$. (*uncurry* ($\rightarrow$)) ψ = *snd* δ) Ψ *of*
        None $\Rightarrow \mathfrak{A}\ \Psi\ \Delta$
       | *Some* $\psi \Rightarrow \psi\ \#\ (\mathfrak{A}$ (*remove1* $\psi\ \Psi$) Δ))

primrec (**in** *implication-logic*)
  second-component :: $('a \times 'a)$ *list* $\Rightarrow$ $('a \times 'a)$ *list* $\Rightarrow$ $('a \times 'a)$ *list* ($\mathfrak{B}$)
  where
   $\mathfrak{B}\ \Psi\ [] = []$
  | $\mathfrak{B}\ \Psi\ (\delta \# \Delta) =$
     (*case find* ($\lambda\ \psi$. (*uncurry* ($\rightarrow$)) ψ = *snd* δ) Ψ *of*
        None $\Rightarrow \mathfrak{B}\ \Psi\ \Delta$
       | *Some* $\psi \Rightarrow \delta\ \#\ (\mathfrak{B}$ (*remove1* $\psi\ \Psi$) Δ))

lemma (**in** *implication-logic*) *first-component-second-component-mset-connection*:
$mset\ (map\ (uncurry\ (\rightarrow))\ (\mathfrak{A}\ \Psi\ \Delta)) = mset\ (map\ snd\ (\mathfrak{B}\ \Psi\ \Delta))$
$\langle proof \rangle$

lemma (**in** *implication-logic*) *second-component-right-empty* [*simp*]:
$\mathfrak{B}\ []\ \Delta = []$
$\langle proof \rangle$

lemma (**in** *implication-logic*) *first-component-msub*:
$mset\ (\mathfrak{A}\ \Psi\ \Delta) \subseteq\#\ mset\ \Psi$
$\langle proof \rangle$

lemma (**in** *implication-logic*) *second-component-msub*:
$mset\ (\mathfrak{B}\ \Psi\ \Delta) \subseteq\#\ mset\ \Delta$
$\langle proof \rangle$

lemma (**in** *implication-logic*) *second-component-snd-projection-msub*:
$mset\ (map\ snd\ (\mathfrak{B}\ \Psi\ \Delta)) \subseteq\#\ mset\ (map\ (uncurry\ (\rightarrow))\ \Psi)$
$\langle proof \rangle$

lemma (**in** *implication-logic*) *second-component-diff-msub*:
assumes $mset\ (map\ snd\ \Delta) \subseteq\#\ mset\ (map\ (uncurry\ (\rightarrow))\ \Psi\ @\ \Gamma \ominus (map\ snd\ \Psi))$
shows $mset\ (map\ snd\ (\Delta \ominus (\mathfrak{B}\ \Psi\ \Delta))) \subseteq\#\ mset\ (\Gamma \ominus (map\ snd\ \Psi))$
$\langle proof \rangle$

primrec (**in** *classical-logic*)
$merge\text{-}witness :: ('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list\ (\mathfrak{J})$
where
$\mathfrak{J}\ \Psi\ [] = \Psi$
$|\ \mathfrak{J}\ \Psi\ (\delta\ \#\ \Delta) =$
$(case\ find\ (\lambda\ \psi.\ (uncurry\ (\rightarrow))\ \psi = snd\ \delta)\ \Psi\ of$
$None \Rightarrow \delta\ \#\ \mathfrak{J}\ \Psi\ \Delta$
$|\ Some\ \psi \Rightarrow (fst\ \delta \sqcap fst\ \psi,\ snd\ \psi)\ \#\ (\mathfrak{J}\ (remove1\ \psi\ \Psi)\ \Delta))$

lemma (**in** *classical-logic*) *merge-witness-right-empty* [*simp*]:
$\mathfrak{J}\ []\ \Delta = \Delta$
$\langle proof \rangle$

lemma (**in** *classical-logic*) *second-component-merge-witness-snd-projection*:
$mset\ (map\ snd\ \Psi\ @\ map\ snd\ (\Delta \ominus (\mathfrak{B}\ \Psi\ \Delta))) = mset\ (map\ snd\ (\mathfrak{J}\ \Psi\ \Delta))$
$\langle proof \rangle$

lemma (**in** *classical-logic*) *second-component-merge-witness-stronger-theory*:
$(map\ (uncurry\ (\rightarrow))\ \Delta\ @\ map\ (uncurry\ (\rightarrow))\ \Psi \ominus map\ snd\ (\mathfrak{B}\ \Psi\ \Delta)) \preceq$
$map\ (uncurry\ (\rightarrow))\ (\mathfrak{J}\ \Psi\ \Delta)$
$\langle proof \rangle$

lemma (**in** *classical-logic*) *merge-witness-msub-intro*:

assumes $mset\ (map\ snd\ \Psi) \subseteq\#\ mset\ \Gamma$
and $mset\ (map\ snd\ \Delta) \subseteq\#\ mset\ (map\ (uncurry\ (\rightarrow))\ \Psi\ @\ \Gamma \ominus (map\ snd\ \Psi))$
shows $mset\ (map\ snd\ (\mathfrak{J}\ \Psi\ \Delta)) \subseteq\#\ mset\ \Gamma$
$\langle proof \rangle$

lemma (**in** *classical-logic*) *right-merge-witness-stronger-theory*:
$map\ (uncurry\ (\sqcup))\ \Delta \preceq map\ (uncurry\ (\sqcup))\ (\mathfrak{J}\ \Psi\ \Delta)$
$\langle proof \rangle$

lemma (**in** *classical-logic*) *left-merge-witness-stronger-theory*:
$map\ (uncurry\ (\sqcup))\ \Psi \preceq map\ (uncurry\ (\sqcup))\ (\mathfrak{J}\ \Psi\ \Delta)$
$\langle proof \rangle$

lemma (**in** *classical-logic*) *measure-empty-deduction*:
$[]\ \$\vdash\ \Phi = (\forall\ \varphi \in set\ \Phi.\ \vdash \varphi)$
$\langle proof \rangle$

lemma (**in** *classical-logic*) *measure-stronger-theory-left-monotonic*:
assumes $\Sigma \preceq \Gamma$
and $\Sigma\ \$\vdash\ \Phi$
shows $\Gamma\ \$\vdash\ \Phi$
$\langle proof \rangle$

lemma (**in** *classical-logic*) *merge-witness-measure-deduction-intro*:
assumes $mset\ (map\ snd\ \Delta) \subseteq\#\ mset\ (map\ (uncurry\ (\rightarrow))\ \Psi\ @\ \Gamma \ominus (map\ snd\ \Psi))$
and $map\ (uncurry\ (\rightarrow))\ \Delta\ @\ (map\ (uncurry\ (\rightarrow))\ \Psi\ @\ \Gamma \ominus map\ snd\ \Psi) \ominus map\ snd\ \Delta\ \$\vdash\ \Phi$
(**is** $?\Gamma_0\ \$\vdash\ \Phi$)
shows $map\ (uncurry\ (\rightarrow))\ (\mathfrak{J}\ \Psi\ \Delta)\ @\ \Gamma \ominus map\ snd\ (\mathfrak{J}\ \Psi\ \Delta)\ \$\vdash\ \Phi$
(**is** $?\Gamma\ \$\vdash\ \Phi$)
$\langle proof \rangle$

lemma (**in** *classical-logic*) *measure-formula-right-split*:
$\Gamma\ \$\vdash\ (\psi \sqcup \varphi\ \#\ \psi \rightarrow \varphi\ \#\ \Phi) = \Gamma\ \$\vdash\ (\varphi\ \#\ \Phi)$
$\langle proof \rangle$

primrec (**in** *implication-logic*)
X-witness :: $('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list\ (\mathfrak{X})$
where
$\mathfrak{X}\ \Psi\ [] = []$
$|\ \mathfrak{X}\ \Psi\ (\delta\ \#\ \Delta) =$
$(case\ find\ (\lambda\ \psi.\ (uncurry\ (\rightarrow))\ \psi = snd\ \delta)\ \Psi\ of$
$None \Rightarrow \delta\ \#\ \mathfrak{X}\ \Psi\ \Delta$
$|\ Some\ \psi \Rightarrow (fst\ \psi \rightarrow fst\ \delta,\ snd\ \psi)\ \#\ (\mathfrak{X}\ (remove1\ \psi\ \Psi)\ \Delta))$

primrec (**in** *implication-logic*)
X-component :: $('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list\ (\mathfrak{X}_\bullet)$

where
  $\mathfrak{X}_\bullet\ \Psi\ []\ =\ []$
| $\mathfrak{X}_\bullet\ \Psi\ (\delta\ \#\ \Delta) =$
    $($*case find* $(\lambda\ \psi.\ (uncurry\ (\rightarrow))\ \psi = snd\ \delta)\ \Psi$ *of*
      None $\Rightarrow \mathfrak{X}_\bullet\ \Psi\ \Delta$
    | *Some* $\psi \Rightarrow (fst\ \psi \rightarrow fst\ \delta,\ snd\ \psi)\ \#\ (\mathfrak{X}_\bullet\ (remove1\ \psi\ \Psi)\ \Delta))$

primrec (**in** *implication-logic*)
  Y-witness :: $('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list\ (\mathfrak{Y})$
  where
  $\mathfrak{Y}\ \Psi\ []\ =\ \Psi$
| $\mathfrak{Y}\ \Psi\ (\delta\ \#\ \Delta) =$
    $($*case find* $(\lambda\ \psi.\ (uncurry\ (\rightarrow))\ \psi = snd\ \delta)\ \Psi$ *of*
      None $\Rightarrow \mathfrak{Y}\ \Psi\ \Delta$
    | *Some* $\psi \Rightarrow (fst\ \psi,\ (fst\ \psi \rightarrow fst\ \delta) \rightarrow snd\ \psi)\ \#$
        $(\mathfrak{Y}\ (remove1\ \psi\ \Psi)\ \Delta))$

primrec (**in** *implication-logic*)
  Y-component :: $('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list\ (\mathfrak{Y}_\bullet)$
  where
  $\mathfrak{Y}_\bullet\ \Psi\ []\ =\ []$
| $\mathfrak{Y}_\bullet\ \Psi\ (\delta\ \#\ \Delta) =$
    $($*case find* $(\lambda\ \psi.\ (uncurry\ (\rightarrow))\ \psi = snd\ \delta)\ \Psi$ *of*
      None $\Rightarrow \mathfrak{Y}_\bullet\ \Psi\ \Delta$
    | *Some* $\psi \Rightarrow (fst\ \psi,\ (fst\ \psi \rightarrow fst\ \delta) \rightarrow snd\ \psi)\ \#$
        $(\mathfrak{Y}_\bullet\ (remove1\ \psi\ \Psi)\ \Delta))$

lemma (**in** *implication-logic*) *X-witness-right-empty* [*simp*]:
  $\mathfrak{X}\ []\ \Delta = \Delta$
  $\langle proof \rangle$

lemma (**in** *implication-logic*) *Y-witness-right-empty* [*simp*]:
  $\mathfrak{Y}\ []\ \Delta = []$
  $\langle proof \rangle$

lemma (**in** *implication-logic*) *X-witness-map-snd-decomposition*:
  $mset\ (map\ snd\ (\mathfrak{X}\ \Psi\ \Delta)) = mset\ (map\ snd\ ((\mathfrak{A}\ \Psi\ \Delta)\ @\ (\Delta \ominus (\mathfrak{B}\ \Psi\ \Delta))))$
$\langle proof \rangle$

lemma (**in** *implication-logic*) *Y-witness-map-snd-decomposition*:
  $mset\ (map\ snd\ (\mathfrak{Y}\ \Psi\ \Delta)) = mset\ (map\ snd\ ((\Psi \ominus (\mathfrak{A}\ \Psi\ \Delta))\ @\ (\mathfrak{Y}_\bullet\ \Psi\ \Delta)))$
$\langle proof \rangle$

lemma (**in** *implication-logic*) *X-witness-msub*:
  assumes $mset\ (map\ snd\ \Psi) \subseteq\#\ mset\ \Gamma$
    and $mset\ (map\ snd\ \Delta) \subseteq\#\ mset\ (map\ (uncurry\ (\rightarrow))\ \Psi\ @\ \Gamma \ominus (map\ snd$
$\Psi))$
  shows $mset\ (map\ snd\ (\mathfrak{X}\ \Psi\ \Delta)) \subseteq\#\ mset\ \Gamma$
$\langle proof \rangle$

lemma (**in** *implication-logic*) *Y-component-msub*:
$mset\ (map\ snd\ (\mathfrak{Y}_\bullet\ \Psi\ \Delta)) \subseteq\#\ mset\ (map\ (uncurry\ (\rightarrow))\ (\mathfrak{X}\ \Psi\ \Delta))$
⟨*proof*⟩

lemma (**in** *implication-logic*) *Y-witness-msub*:
assumes $mset\ (map\ snd\ \Psi) \subseteq\#\ mset\ \Gamma$
and $mset\ (map\ snd\ \Delta) \subseteq\#\ mset\ (map\ (uncurry\ (\rightarrow))\ \Psi\ @\ \Gamma \ominus (map\ snd\ \Psi))$
shows $mset\ (map\ snd\ (\mathfrak{Y}\ \Psi\ \Delta)) \subseteq\#$
$mset\ (map\ (uncurry\ (\rightarrow))\ (\mathfrak{X}\ \Psi\ \Delta)\ @\ \Gamma \ominus map\ snd\ (\mathfrak{X}\ \Psi\ \Delta))$
⟨*proof*⟩

lemma (**in** *classical-logic*) *X-witness-right-stronger-theory*:
$map\ (uncurry\ (\sqcup))\ \Delta \preceq map\ (uncurry\ (\sqcup))\ (\mathfrak{X}\ \Psi\ \Delta)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *Y-witness-left-stronger-theory*:
$map\ (uncurry\ (\sqcup))\ \Psi \preceq map\ (uncurry\ (\sqcup))\ (\mathfrak{Y}\ \Psi\ \Delta)$
⟨*proof*⟩

lemma (**in** *implication-logic*) *X-witness-second-component-diff-decomposition*:
$mset\ (\mathfrak{X}\ \Psi\ \Delta) = mset\ (\mathfrak{X}_\bullet\ \Psi\ \Delta\ @\ \Delta \ominus \mathfrak{B}\ \Psi\ \Delta)$
⟨*proof*⟩

lemma (**in** *implication-logic*) *Y-witness-first-component-diff-decomposition*:
$mset\ (\mathfrak{Y}\ \Psi\ \Delta) = mset\ (\Psi \ominus \mathfrak{A}\ \Psi\ \Delta\ @\ \mathfrak{Y}_\bullet\ \Psi\ \Delta)$
⟨*proof*⟩

lemma (**in** *implication-logic*) *Y-witness-right-stronger-theory*:
$map\ (uncurry\ (\rightarrow))\ \Delta \preceq map\ (uncurry\ (\rightarrow))\ (\mathfrak{Y}\ \Psi\ \Delta \ominus (\Psi \ominus \mathfrak{A}\ \Psi\ \Delta)\ @\ (\Delta \ominus \mathfrak{B}\ \Psi\ \Delta))$
⟨*proof*⟩

lemma (**in** *implication-logic*) *xcomponent-ycomponent-connection*:
$map\ (uncurry\ (\rightarrow))\ (\mathfrak{X}_\bullet\ \Psi\ \Delta) = map\ snd\ (\mathfrak{Y}_\bullet\ \Psi\ \Delta)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *xwitness-ywitness-measure-deduction-intro*:
assumes $mset\ (map\ snd\ \Psi) \subseteq\#\ mset\ \Gamma$
and $mset\ (map\ snd\ \Delta) \subseteq\#\ mset\ (map\ (uncurry\ (\rightarrow))\ \Psi\ @\ \Gamma \ominus (map\ snd\ \Psi))$
and $map\ (uncurry\ (\rightarrow))\ \Delta\ @\ (map\ (uncurry\ (\rightarrow))\ \Psi\ @\ \Gamma \ominus map\ snd\ \Psi) \ominus map\ snd\ \Delta\ \$\vdash \Phi$
(**is** $?\Gamma_0\ \$\vdash \Phi$)
shows $map\ (uncurry\ (\rightarrow))\ (\mathfrak{Y}\ \Psi\ \Delta)\ @$
$(map\ (uncurry\ (\rightarrow))\ (\mathfrak{X}\ \Psi\ \Delta)\ @\ \Gamma \ominus map\ snd\ (\mathfrak{X}\ \Psi\ \Delta)) \ominus$
$map\ snd\ (\mathfrak{Y}\ \Psi\ \Delta)\ \$\vdash \Phi$
(**is** $?\Gamma\ \$\vdash \Phi$)

⟨*proof*⟩

lemma (**in** *classical-logic*) *measure-cons-cons-right-permute*:
assumes Γ $⊢ ($\varphi$ # ψ # Φ)
shows Γ $⊢ ($\psi$ # φ # Φ)
⟨*proof*⟩

lemma (**in** *classical-logic*) *measure-cons-remove1*:
assumes $\varphi \in$ *set* Φ
shows Γ $⊢ Φ = Γ $⊢ ($\varphi$ # (*remove1* φ Φ))
⟨*proof*⟩

lemma (**in** *classical-logic*) *witness-stronger-theory*:
assumes *mset* (*map snd* Ψ) ⊆# *mset* Γ
shows (*map* (*uncurry* ($\rightarrow$)) Ψ @ $\Gamma \ominus$ (*map snd* Ψ)) $\preceq \Gamma$
⟨*proof*⟩

lemma (**in** *classical-logic*) *measure-msub-weaken*:
assumes *mset* Ψ ⊆# *mset* Φ
and Γ $⊢ Φ
shows Γ $⊢ Ψ
⟨*proof*⟩

lemma (**in** *classical-logic*) *measure-stronger-theory-right-antitonic*:
assumes $\Psi \preceq \Phi$
and Γ $⊢ Φ
shows Γ $⊢ Ψ
⟨*proof*⟩

lemma (**in** *classical-logic*) *measure-witness-right-split*:
assumes *mset* (*map snd* Ψ) ⊆# *mset* Φ
shows Γ $⊢ (*map* (*uncurry* ($\sqcup$)) Ψ @ *map* (*uncurry* ($\rightarrow$)) Ψ @ $\Phi \ominus$ (*map snd* Ψ)) = Γ $⊢ Φ
⟨*proof*⟩

primrec (**in** *classical-logic*)
submerge-witness :: ($'a \times 'a$) *list* $\Rightarrow$ ($'a \times 'a$) *list* $\Rightarrow$ ($'a \times 'a$) *list* ($\mathfrak{E}$)
where
$\mathfrak{E}$ Σ [] = *map* (λ σ. ($\bot$, (*uncurry* ($\sqcup$)) σ)) Σ
| $\mathfrak{E}$ Σ (δ # Δ) =
(*case find* (λ σ. (*uncurry* ($\rightarrow$)) σ = *snd* δ) Σ *of*
None $\Rightarrow$ $\mathfrak{E}$ Σ Δ
| *Some* σ $\Rightarrow$ (*fst* σ, (*fst* δ $\sqcap$ *fst* σ) $\sqcup$ *snd* σ) # ($\mathfrak{E}$ (*remove1* σ Σ) Δ))

lemma (**in** *classical-logic*) *submerge-witness-stronger-theory-left*:
map (*uncurry* ($\sqcup$)) $\Sigma \preceq$ *map* (*uncurry* ($\sqcup$)) ($\mathfrak{E}$ Σ Δ)
⟨*proof*⟩

lemma (**in** *classical-logic*) *submerge-witness-msub*:

$mset\ (map\ snd\ (\mathfrak{E}\ \Sigma\ \Delta)) \subseteq\#\ mset\ (map\ (uncurry\ (\sqcup))\ (\mathfrak{J}\ \Sigma\ \Delta))$
⟨proof⟩

lemma (**in** *classical-logic*) *submerge-witness-stronger-theory-right*:
$map\ (uncurry\ (\sqcup))\ \Delta$
$\preceq (map\ (uncurry\ (\rightarrow))\ (\mathfrak{E}\ \Sigma\ \Delta)\ @\ map\ (uncurry\ (\sqcup))\ (\mathfrak{J}\ \Sigma\ \Delta) \ominus map\ snd\ (\mathfrak{E}\ \Sigma\ \Delta))$
⟨proof⟩

lemma (**in** *classical-logic*) *merge-witness-cons-measure-deduction*:
assumes $map\ (uncurry\ (\sqcup))\ \Sigma :\vdash \varphi$
and $mset\ (map\ snd\ \Delta) \subseteq\#\ mset\ (map\ (uncurry\ (\rightarrow))\ \Sigma\ @\ \Gamma \ominus map\ snd\ \Sigma)$
and $map\ (uncurry\ (\sqcup))\ \Delta\ \$\vdash\ \Phi$
shows $map\ (uncurry\ (\sqcup))\ (\mathfrak{J}\ \Sigma\ \Delta)\ \$\vdash\ (\varphi\ \#\ \Phi)$
⟨proof⟩

primrec (**in** *classical-logic*)
$recover\text{-}witness\text{-}A :: ('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list\ (\mathfrak{P})$
where
$\mathfrak{P}\ \Sigma\ []= \Sigma$
$|\ \mathfrak{P}\ \Sigma\ (\delta\ \#\ \Delta) =$
$(case\ find\ (\lambda\ \sigma.\ snd\ \sigma = (uncurry\ (\sqcup))\ \delta)\ \Sigma\ of$
$None \Rightarrow \mathfrak{P}\ \Sigma\ \Delta$
$|\ Some\ \sigma \Rightarrow (fst\ \sigma \sqcup fst\ \delta,\ snd\ \delta)\ \#\ (\mathfrak{P}\ (remove1\ \sigma\ \Sigma)\ \Delta))$

primrec (**in** *classical-logic*)
$recover\text{-}complement\text{-}A :: ('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list\ (\mathfrak{P}^C)$
where
$\mathfrak{P}^C\ \Sigma\ [] = []$
$|\ \mathfrak{P}^C\ \Sigma\ (\delta\ \#\ \Delta) =$
$(case\ find\ (\lambda\ \sigma.\ snd\ \sigma = (uncurry\ (\sqcup))\ \delta)\ \Sigma\ of$
$None \Rightarrow \delta\ \#\ \mathfrak{P}^C\ \Sigma\ \Delta$
$|\ Some\ \sigma \Rightarrow (\mathfrak{P}^C\ (remove1\ \sigma\ \Sigma)\ \Delta))$

primrec (**in** *classical-logic*)
$recover\text{-}witness\text{-}B :: ('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list \Rightarrow ('a \times 'a)\ list\ (\mathfrak{Q})$
where
$\mathfrak{Q}\ \Sigma\ [] = []$
$|\ \mathfrak{Q}\ \Sigma\ (\delta\ \#\ \Delta) =$
$(case\ find\ (\lambda\ \sigma.\ (snd\ \sigma) = (uncurry\ (\sqcup))\ \delta)\ \Sigma\ of$
$None \Rightarrow \delta\ \#\ \mathfrak{Q}\ \Sigma\ \Delta$
$|\ Some\ \sigma \Rightarrow (fst\ \delta,\ (fst\ \sigma \sqcup fst\ \delta) \rightarrow snd\ \delta)\ \#\ (\mathfrak{Q}\ (remove1\ \sigma\ \Sigma)\ \Delta))$

lemma (**in** *classical-logic*) *recover-witness-A-left-stronger-theory*:
$map\ (uncurry\ (\sqcup))\ \Sigma \preceq map\ (uncurry\ (\sqcup))\ (\mathfrak{P}\ \Sigma\ \Delta)$
⟨proof⟩

lemma (**in** *classical-logic*) *recover-witness-A-mset-equiv*:
assumes $mset\ (map\ snd\ \Sigma) \subseteq\#\ mset\ (map\ (uncurry\ (\sqcup))\ \Delta)$

shows $mset$ (map snd ($\mathfrak{P}$ Σ Δ @ $\mathfrak{P}^C$ Σ Δ)) = $mset$ (map snd Δ)
⟨*proof*⟩

lemma (**in** *classical-logic*) *recover-witness-B-stronger-theory*:
assumes $mset$ (map snd Σ) $\subseteq\#$ $mset$ (map ($uncurry$ ($\sqcup$)) Δ)
shows (map ($uncurry$ ($\rightarrow$)) Σ @ map ($uncurry$ ($\sqcup$)) Δ $\ominus$ map snd Σ)
$\preceq$ map ($uncurry$ ($\sqcup$)) ($\mathfrak{Q}$ Σ Δ)
⟨*proof*⟩

lemma (**in** *classical-logic*) *recover-witness-B-mset-equiv*:
assumes $mset$ (map snd Σ) $\subseteq\#$ $mset$ (map ($uncurry$ ($\sqcup$)) Δ)
shows $mset$ (map snd ($\mathfrak{Q}$ Σ Δ))
= $mset$ (map ($uncurry$ ($\rightarrow$)) ($\mathfrak{P}$ Σ Δ) @ map snd Δ $\ominus$ map snd ($\mathfrak{P}$ Σ Δ))
⟨*proof*⟩

lemma (**in** *classical-logic*) *recover-witness-B-right-stronger-theory*:
map ($uncurry$ ($\rightarrow$)) Δ $\preceq$ map ($uncurry$ ($\rightarrow$)) ($\mathfrak{Q}$ Σ Δ)
⟨*proof*⟩

lemma (**in** *classical-logic*) *recoverWitnesses-mset-equiv*:
assumes $mset$ (map snd Δ) $\subseteq\#$ $mset$ Γ
and $mset$ (map snd Σ) $\subseteq\#$ $mset$ (map ($uncurry$ ($\sqcup$)) Δ)
shows $mset$ (Γ $\ominus$ map snd Δ)
= $mset$ ((map ($uncurry$ ($\rightarrow$)) ($\mathfrak{P}$ Σ Δ) @ Γ $\ominus$ map snd ($\mathfrak{P}$ Σ Δ)) $\ominus$ map snd ($\mathfrak{Q}$ Σ Δ))
⟨*proof*⟩

theorem (**in** *classical-logic*) *measure-deduction-generalized-witness*:
Γ \$⊢ (Φ @ Ψ) = ($\exists$ Σ. $mset$ (map snd Σ) $\subseteq\#$ $mset$ Γ $\wedge$
map ($uncurry$ ($\sqcup$)) Σ \$⊢ Φ $\wedge$
(map ($uncurry$ ($\rightarrow$)) Σ @ Γ $\ominus$ (map snd Σ)) \$⊢ Ψ)
⟨*proof*⟩

lemma (**in** *classical-logic*) *measure-list-deduction-antitonic*:
assumes Γ \$⊢ Ψ
and Ψ :⊢ φ
shows Γ :⊢ φ
⟨*proof*⟩

Finally, we may establish that (\$⊢) is transitive.

theorem (**in** *classical-logic*) *measure-transitive*:
assumes Γ \$⊢ Λ
and Λ \$⊢ Δ
shows Γ \$⊢ Δ
⟨*proof*⟩

2.6 Measure Deduction Cancellation Rules

In this chapter we go over how to cancel formulae occurring in measure deduction judgements.

The first observation is that tautologies can always be canceled on either side of the turnstile.

lemma (**in** *classical-logic*) *measure-tautology-right-cancel*:
  assumes $\vdash \varphi$
  shows Γ $\vdash $(\varphi \# \Phi) = \Gamma$ $\vdash Φ
$\langle proof \rangle$

lemma (**in** *classical-logic*) *measure-tautology-left-cancel* [*simp*]:
  assumes $\vdash \gamma$
  shows $(\gamma \# \Gamma)$ $\vdash $\Phi = \Gamma$ $\vdash Φ
$\langle proof \rangle$

lemma (**in** *classical-logic*) *measure-deduction-one-collapse*:
  Γ $\vdash $[\varphi] = \Gamma :\vdash \varphi$
$\langle proof \rangle$

Split cases, which are occurrences of $\psi \sqcup \varphi \# \psi \rightarrow \varphi \# \ldots$, also cancel and simplify to just $\varphi \# \ldots$. We previously established Γ $\vdash $\psi \sqcup \varphi \# \psi \rightarrow \varphi \# \Phi = \Gamma$ $\vdash $\varphi \# \Phi$ as part of the proof of transitivity.

lemma (**in** *classical-logic*) *measure-formula-left-split*:
  $\psi \sqcup \varphi \# \psi \rightarrow \varphi \# \Gamma$ $\vdash $\Phi = \varphi \# \Gamma$ $\vdash Φ
$\langle proof \rangle$

lemma (**in** *classical-logic*) *measure-witness-left-split* [*simp*]:
  assumes *mset* (*map snd* Σ) $\subseteq\#$ *mset* Γ
  shows (*map* (*uncurry* $(\sqcup)$) Σ @ *map* (*uncurry* $(\rightarrow)$) Σ @ $\Gamma \ominus$ (*map snd* Σ)) $\vdash
$\Phi = \Gamma$ $\vdash Φ
  $\langle proof \rangle$

We now have enough to establish the cancellation rule for ($\vdash).

lemma (**in** *classical-logic*) *measure-cancel*: $(\Delta @ \Gamma)$ $\vdash $(\Delta @ \Phi) = \Gamma$ $\vdash Φ
$\langle proof \rangle$

lemma (**in** *classical-logic*) *measure-biconditional-cancel*:
  assumes $\vdash \gamma \leftrightarrow \varphi$
  shows $(\gamma \# \Gamma)$ $\vdash $(\varphi \# \Phi) = \Gamma$ $\vdash Φ
$\langle proof \rangle$

2.7 Measure Deduction Substitution Rules

Just like conventional deduction, if two formulae are equivalent then they may be substituted for one another.

lemma (**in** *classical-logic*) *right-measure-sub*:
  assumes $\vdash \varphi \leftrightarrow \psi$
  shows $\Gamma \ \$\!\vdash (\varphi \ \# \ \Phi) = \Gamma \ \$\!\vdash (\psi \ \# \ \Phi)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *left-measure-sub*:
  assumes $\vdash \gamma \leftrightarrow \chi$
  shows $(\gamma \ \# \ \Gamma) \ \$\!\vdash \Phi = (\chi \ \# \ \Gamma) \ \$\!\vdash \Phi$
⟨*proof*⟩

2.8 Measure Deduction Sum Rules

We next establish analogues of the rule in probability that $\mathcal{P}\ \alpha + \mathcal{P}\ \beta = \mathcal{P}\ (\alpha \sqcup \beta) + \mathcal{P}\ (\alpha \sqcap \beta)$. This equivalence holds for both sides of the ($\$\!\vdash$) turnstile.

lemma (**in** *classical-logic*) *right-measure-sum-rule*:
  $\Gamma \ \$\!\vdash (\alpha \ \# \ \beta \ \# \ \Phi) = \Gamma \ \$\!\vdash (\alpha \sqcup \beta \ \# \ \alpha \sqcap \beta \ \# \ \Phi)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *left-measure-sum-rule*:
  $(\alpha \ \# \ \beta \ \# \ \Gamma) \ \$\!\vdash \Phi = (\alpha \sqcup \beta \ \# \ \alpha \sqcap \beta \ \# \ \Gamma) \ \$\!\vdash \Phi$
⟨*proof*⟩

2.9 Measure Deduction Exchange Rule

As we will see, a key result is that we can move formulae from the right hand side of the ($\$\!\vdash$) turnstile to the left.

We observe a novel logical principle, which we call *exchange*. This principle follows immediately from the split rules and cancellation rules.

lemma (**in** *classical-logic*) *measure-exchange*:
  $(\gamma \ \# \ \Gamma) \ \$\!\vdash (\varphi \ \# \ \Phi) = (\varphi \to \gamma \ \# \ \Gamma) \ \$\!\vdash (\gamma \to \varphi \ \# \ \Phi)$
⟨*proof*⟩

The exchange rule allows us to prove an analogue of the rule in classical logic that $\Gamma \ {:}\!\vdash \varphi = (\sim \varphi \ \# \ \Gamma) \ {:}\!\vdash \bot$ for measure deduction.

theorem (**in** *classical-logic*) *measure-negation-swap*:
  $\Gamma \ \$\!\vdash (\varphi \ \# \ \Phi) = (\sim \varphi \ \# \ \Gamma) \ \$\!\vdash (\bot \ \# \ \Phi)$
⟨*proof*⟩

2.10 Definition of Counting Deduction

The theorem $\Gamma \ \$\!\vdash \varphi \ \# \ \Phi = \sim \varphi \ \# \ \Gamma \ \$\!\vdash \bot \ \# \ \Phi$ gives rise to another kind of judgement: *how many times can a list of premises* Γ *prove a formula* φ*?*. We call this kind of judgment *counting deduction*. As with measure deduction, bits of Γ get "used up" with each dispatched conclusion.

primrec (**in** *classical-logic*)
  counting-deduction :: *'a list* ⇒ *nat* ⇒ *'a* ⇒ *bool* (- #⊢ - - [*60*,*100*,*59*] *60*)
  where
    Γ #⊢ *0* φ = *True*
  | Γ #⊢ (*Suc n*) φ = (∃ Ψ. *mset* (*map snd* Ψ) ⊆# *mset* Γ ∧
                map (*uncurry* (⊔)) Ψ :⊢ φ ∧
                map (*uncurry* (→)) Ψ @ Γ ⊖ (*map snd* Ψ) #⊢ *n* φ)

2.11 Converting Back and Forth from Counting Deduction to Measure Deduction

We next show how to convert back and forth from counting deduction to measure deduction.

First, we show that trivially counting deduction is a special case of measure deduction.

lemma (**in** *classical-logic*) *counting-deduction-to-measure-deduction*:
  Γ #⊢ *n* φ = Γ $⊢ (*replicate n* φ)
  ⟨*proof*⟩

We next prove a few helpful lemmas regarding counting deduction.

lemma (**in** *classical-logic*) *counting-deduction-tautology-weaken*:
  assumes ⊢ φ
  shows Γ #⊢ *n* φ
⟨*proof*⟩

lemma (**in** *classical-logic*) *counting-deduction-weaken*:
  assumes *n* ≤ *m*
    and Γ #⊢ *m* φ
  shows Γ #⊢ *n* φ
⟨*proof*⟩

lemma (**in** *classical-logic*) *counting-deduction-implication*:
  assumes ⊢ φ → ψ
    and Γ #⊢ *n* φ
  shows Γ #⊢ *n* ψ
⟨*proof*⟩

Finally, we use Γ $⊢ φ # Φ = ∼ φ # Γ $⊢ ⊥ # Φ to prove that measure deduction reduces to counting deduction.

theorem (**in** *classical-logic*) *measure-deduction-to-counting-deduction*:
  Γ $⊢ Φ = (∼ Φ @ Γ) #⊢ (*length* Φ) ⊥
⟨*proof*⟩

2.12 Measure Deduction Soundess

The last major result for measure deduction we have to show is *soundness*. That is, judgments in measure deduction of lists of formulae can be translated into tautologies for inequalities of finitely additive probability measures over those same formulae (using the same underlying classical logic).

lemma (**in** *classical-logic*) *negated-measure-deduction*:
$\sim \Gamma \ \$\vdash \ (\varphi \ \# \ \Phi) =$
$(\exists \ \Psi. \ mset \ (map \ fst \ \Psi) \subseteq\# \ mset \ \Gamma \ \wedge$
$\sim (map \ (uncurry \ (\backslash)) \ \Psi) \ :\vdash \ \varphi \ \wedge$
$\sim (map \ (uncurry \ (\sqcap)) \ \Psi \ @ \ \Gamma \ominus (map \ fst \ \Psi)) \ \$\vdash \ \Phi)$
$\langle proof \rangle$

lemma (**in** *probability-logic*) *measure-deduction-soundness*:
assumes $\sim \Gamma \ \$\vdash \ \sim \Phi$
shows $(\sum \varphi \leftarrow \Phi. \ \mathcal{P} \ \varphi) \leq (\sum \gamma \leftarrow \Gamma. \ \mathcal{P} \ \gamma)$
$\langle proof \rangle$

Chapter 3

MaxSAT

We turn now to showing that counting deduction reduces to MaxSAT, the problem of finding the maximal number of satisfiable clauses in a list of clauses.

3.1 Definition of Relative Maximal Clause Collections

Given a list of assumptions Φ and formula φ, we can think of those maximal sublists of Φ that do not prove φ. While in practice we will care about $\varphi = \bot$, we provide a general definition in the more general axiom class *implication-logic*.

definition (**in** *implication-logic*) *relative-maximals* :: *'a list* $\Rightarrow$ *'a* $\Rightarrow$ *'a list set* ($\mathcal{M}$)
  where
    $\mathcal{M}\ \Gamma\ \varphi =$
      $\{\ \Phi.\ \mathit{mset}\ \Phi \subseteq\#\ \mathit{mset}\ \Gamma$
        $\wedge\ \neg\ \Phi :\vdash \varphi$
        $\wedge\ (\forall\ \Psi.\ \mathit{mset}\ \Psi \subseteq\#\ \mathit{mset}\ \Gamma \longrightarrow \neg\ \Psi :\vdash \varphi \longrightarrow \mathit{length}\ \Psi \leq \mathit{length}\ \Phi)\ \}$

lemma (**in** *implication-logic*) *relative-maximals-finite*: *finite* ($\mathcal{M}\ \Gamma\ \varphi$)
$\langle$*proof*$\rangle$

We know that φ is not a tautology if and only if the set of relative maximal sublists has an element.

lemma (**in** *implication-logic*) *relative-maximals-existence*:
  $(\neg \vdash \varphi) = (\exists\ \Sigma.\ \Sigma \in \mathcal{M}\ \Gamma\ \varphi)$
$\langle$*proof*$\rangle$

lemma (**in** *implication-logic*) *relative-maximals-complement-deduction*:
  assumes $\Phi \in \mathcal{M}\ \Gamma\ \varphi$
    and $\psi \in \mathit{set}\ (\Gamma \ominus \Phi)$
  shows $\Phi :\vdash \psi \to \varphi$

$\langle proof \rangle$

lemma (**in** *implication-logic*) *relative-maximals-set-complement* [*simp*]:
  assumes $\Phi \in \mathcal{M}\ \Gamma\ \varphi$
  shows $set\ (\Gamma \ominus \Phi) = set\ \Gamma - set\ \Phi$
$\langle proof \rangle$

lemma (**in** *implication-logic*) *relative-maximals-complement-equiv*:
  assumes $\Phi \in \mathcal{M}\ \Gamma\ \varphi$
    and $\psi \in set\ \Gamma$
   shows $\Phi :\vdash \psi \to \varphi = (\psi \notin set\ \Phi)$
$\langle proof \rangle$

lemma (**in** *implication-logic*) *maximals-length-equiv*:
  assumes $\Phi \in \mathcal{M}\ \Gamma\ \varphi$
    and $\Psi \in \mathcal{M}\ \Gamma\ \varphi$
   shows $length\ \Phi = length\ \Psi$
  $\langle proof \rangle$

lemma (**in** *implication-logic*) *maximals-list-subtract-length-equiv*:
  assumes $\Phi \in \mathcal{M}\ \Gamma\ \varphi$
    and $\Psi \in \mathcal{M}\ \Gamma\ \varphi$
   shows $length\ (\Gamma \ominus \Phi) = length\ (\Gamma \ominus \Psi)$
$\langle proof \rangle$

We can think of $\Gamma :\vdash \varphi$ as saying "the relative maximal sublists of Γ are not the entire list".

lemma (**in** *implication-logic*) *relative-maximals-max-list-deduction*:
  $\Gamma :\vdash \varphi = (\forall\ \Phi \in \mathcal{M}\ \Gamma\ \varphi.\ 1 \leq length\ (\Gamma \ominus \Phi))$
$\langle proof \rangle$

3.2 Definition of MaxSAT

We next turn to defining an abstract form of MaxSAT, which is largest the number of simultaneously satisfiable propositions in a list of propositions.

Unlike conventional MaxSAT, we don't actually work at the *semantic* level, i.e. constructing a model for the Tarski truth relation $\models$. Instead, we just count the elements in a maximal, consistent sublist (i.e., a maximal sub list Σ such that $\neg\ \Sigma :\vdash \bot$) of the list of assumptions Γ we have at hand.

Because we do not work at the semantic level, computing if $MaxSAT\ \Gamma \leq n$ is not in general CoNP-Complete, as it is classically classified [1]. In the special case that the underlying logic is the *classical propositional calculus*, then the complexity is CoNP-Complete. But we could imagine the underlying logic to be linear temporal logic or even first order logic. In such cases the complexity class would be higher in the complexity hierarchy.

definition (**in** *implication-logic*) *relative-MaxSAT* :: $'a$ *list* $\Rightarrow$ $'a$ $\Rightarrow$ *nat* ($(|\ \text{-}\ |_{\text{-}}$ [*45*]))
  where
    $(|\ \Gamma\ |_{\varphi}) = (\mathit{if}\ \mathcal{M}\ \Gamma\ \varphi = \{\}\ \mathit{then}\ 0\ \mathit{else}\ \mathit{Max}\ \{\ \mathit{length}\ \Phi\ |\ \Phi.\ \Phi \in \mathcal{M}\ \Gamma\ \varphi\ \})$

abbreviation (**in** *classical-logic*) *MaxSAT* :: $'a$ *list* $\Rightarrow$ *nat*
  where
    $\mathit{MaxSAT}\ \Gamma \equiv |\ \Gamma\ |_{\bot}$

definition (**in** *implication-logic*) *complement-relative-MaxSAT* :: $'a$ *list* $\Rightarrow$ $'a$ $\Rightarrow$ *nat* ($(\|\ \text{-}\ \|_{\text{-}}$ [*45*]))
  where
    $(\|\ \Gamma\ \|_{\varphi}) = \mathit{length}\ \Gamma - |\ \Gamma\ |_{\varphi}$

lemma (**in** *implication-logic*) *relative-MaxSAT-intro*:
  assumes $\Phi \in \mathcal{M}\ \Gamma\ \varphi$
  shows $\mathit{length}\ \Phi = |\ \Gamma\ |_{\varphi}$
⟨*proof*⟩

lemma (**in** *implication-logic*) *complement-relative-MaxSAT-intro*:
  assumes $\Phi \in \mathcal{M}\ \Gamma\ \varphi$
  shows $\mathit{length}\ (\Gamma \ominus \Phi) = \|\ \Gamma\ \|_{\varphi}$
⟨*proof*⟩

lemma (**in** *implication-logic*) *length-MaxSAT-decomposition*:
  $\mathit{length}\ \Gamma = (|\ \Gamma\ |_{\varphi}) + \|\ \Gamma\ \|_{\varphi}$
⟨*proof*⟩

3.3 Reducing Counting Deduction to MaxSAT

Here we present a major result: counting deduction may be reduced to MaxSAT.

primrec *MaxSAT-optimal-pre-witness* :: $'a$ *list* $\Rightarrow$ ($'a$ *list* $\times$ $'a$) *list* ($\mathfrak{V}$)
  where
    $\mathfrak{V}\ [] = []$
  $|\ \mathfrak{V}\ (\psi\ \#\ \Psi) = (\Psi,\ \psi)\ \#\ \mathfrak{V}\ \Psi$

lemma *MaxSAT-optimal-pre-witness-element-inclusion*:
  $\forall\ (\Delta,\delta) \in \mathit{set}\ (\mathfrak{V}\ \Psi).\ \mathit{set}\ (\mathfrak{V}\ \Delta) \subseteq \mathit{set}\ (\mathfrak{V}\ \Psi)$
  ⟨*proof*⟩

lemma *MaxSAT-optimal-pre-witness-nonelement*:
  assumes $\mathit{length}\ \Delta \geq \mathit{length}\ \Psi$
  shows $(\Delta,\delta) \notin \mathit{set}\ (\mathfrak{V}\ \Psi)$
  ⟨*proof*⟩

lemma *MaxSAT-optimal-pre-witness-distinct*: $\mathit{distinct}\ (\mathfrak{V}\ \Psi)$
  ⟨*proof*⟩

lemma *MaxSAT-optimal-pre-witness-length-iff-eq*:
$\forall\ (\Delta,\delta) \in set\ (\mathfrak{V}\ \Psi).\ \forall\ (\Sigma,\sigma) \in set\ (\mathfrak{V}\ \Psi).\ (length\ \Delta = length\ \Sigma) = ((\Delta,\ \delta) = (\Sigma,\sigma))$
$\langle proof \rangle$

lemma *mset-distinct-msub-down*:
assumes $mset\ A \subseteq\#\ mset\ B$
and $distinct\ B$
shows $distinct\ A$
$\langle proof \rangle$

lemma *mset-remdups-set-sub-iff*:
$(mset\ (remdups\ A) \subseteq\#\ mset\ (remdups\ B)) = (set\ A \subseteq set\ B)$
$\langle proof \rangle$

lemma *range-characterization*:
$(mset\ X = mset\ [0..<length\ X]) = (distinct\ X \wedge (\forall\ x \in set\ X.\ x < length\ X))$
$\langle proof \rangle$

lemma *distinct-pigeon-hole*:
fixes $X :: nat\ list$
assumes $distinct\ X$
and $X \neq []$
shows $\exists\ n \in set\ X.\ n + 1 \geq length\ X$
$\langle proof \rangle$

lemma *MaxSAT-optimal-pre-witness-pigeon-hole*:
assumes $mset\ \Sigma \subseteq\#\ mset\ (\mathfrak{V}\ \Psi)$
and $\Sigma \neq []$
shows $\exists\ (\Delta,\ \delta) \in set\ \Sigma.\ length\ \Delta + 1 \geq length\ \Sigma$
$\langle proof \rangle$

abbreviation (**in** *classical-logic*)
$MaxSAT\text{-}optimal\text{-}witness :: 'a \Rightarrow 'a\ list \Rightarrow ('a \times 'a)\ list\ (\mathfrak{W})$
where $\mathfrak{W}\ \varphi\ \Xi \equiv map\ (\lambda(\Psi,\psi).\ (\Psi :\rightarrow \varphi,\ \psi))\ (\mathfrak{V}\ \Xi)$

abbreviation (**in** *classical-logic*)
$disjunction\text{-}MaxSAT\text{-}optimal\text{-}witness :: 'a \Rightarrow 'a\ list \Rightarrow 'a\ list\ (\mathfrak{W}_{\sqcup})$
where $\mathfrak{W}_{\sqcup}\ \varphi\ \Psi \equiv map\ (uncurry\ (\sqcup))\ (\mathfrak{W}\ \varphi\ \Psi)$

abbreviation (**in** *classical-logic*)
$implication\text{-}MaxSAT\text{-}optimal\text{-}witness :: 'a \Rightarrow 'a\ list \Rightarrow 'a\ list\ (\mathfrak{W}_{\rightarrow})$
where $\mathfrak{W}_{\rightarrow}\ \varphi\ \Psi \equiv map\ (uncurry\ (\rightarrow))\ (\mathfrak{W}\ \varphi\ \Psi)$

lemma (**in** *classical-logic*) *MaxSAT-optimal-witness-conjunction-identity*:
$\vdash \bigsqcap\ (\mathfrak{W}_{\sqcup}\ \varphi\ \Psi) \leftrightarrow (\varphi \sqcup \bigsqcap\ \Psi)$
$\langle proof \rangle$

lemma (**in** *classical-logic*) *MaxSAT-optimal-witness-deduction*:

$\vdash \mathfrak{W}_{\sqcup}\ \varphi\ \Psi :\rightarrow \varphi \leftrightarrow \Psi :\rightarrow \varphi$
⟨*proof*⟩

lemma (**in** *classical-logic*) *optimal-witness-split-identity*:
$\vdash (\mathfrak{W}_{\sqcup}\ \varphi\ (\psi\ \#\ \Xi)) :\rightarrow \varphi \rightarrow (\mathfrak{W}_{\rightarrow}\ \varphi\ (\psi\ \#\ \Xi)) :\rightarrow \varphi \rightarrow \Xi :\rightarrow \varphi$
⟨*proof*⟩

lemma (**in** *classical-logic*) *disj-conj-impl-duality*:
$\vdash (\varphi \rightarrow \chi \sqcap \psi \rightarrow \chi) \leftrightarrow ((\varphi \sqcup \psi) \rightarrow \chi)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *weak-disj-of-conj-equiv*:
$(\forall\, \sigma \in set\ \Sigma.\ \sigma :\vdash \varphi) = \vdash \bigsqcup\ (map\ \bigsqcap\ \Sigma) \rightarrow \varphi$
⟨*proof*⟩

lemma (**in** *classical-logic*) *arbitrary-disj-concat-equiv*:
$\vdash \bigsqcup\ (\Phi\ @\ \Psi) \leftrightarrow (\bigsqcup\ \Phi \sqcup \bigsqcup\ \Psi)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *arbitrary-conj-concat-equiv*:
$\vdash \bigsqcap\ (\Phi\ @\ \Psi) \leftrightarrow (\bigsqcap\ \Phi \sqcap \bigsqcap\ \Psi)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *conj-absorption*:
assumes $\chi \in set\ \Phi$
shows $\vdash \bigsqcap\ \Phi \leftrightarrow (\chi \sqcap \bigsqcap\ \Phi)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *conj-extract*: $\vdash \bigsqcup\ (map\ ((\sqcap)\ \varphi)\ \Psi) \leftrightarrow (\varphi \sqcap \bigsqcup\ \Psi)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *conj-multi-extract*:
$\vdash \bigsqcup\ (map\ \bigsqcap\ (map\ ((@)\ \Delta)\ \Sigma)) \leftrightarrow (\bigsqcap\ \Delta \sqcap \bigsqcup\ (map\ \bigsqcap\ \Sigma))$
⟨*proof*⟩

lemma (**in** *classical-logic*) *extract-inner-concat*:
$\vdash \bigsqcup\ (map\ (\bigsqcap \circ (map\ snd \circ (@)\ \Delta))\ \Psi) \leftrightarrow (\bigsqcap\ (map\ snd\ \Delta) \sqcap \bigsqcup\ (map\ (\bigsqcap \circ map\ snd)\ \Psi))$
⟨*proof*⟩

lemma (**in** *classical-logic*) *extract-inner-concat-remdups*:
$\vdash \bigsqcup\ (map\ (\bigsqcap \circ (map\ snd \circ remdups \circ (@)\ \Delta))\ \Psi) \leftrightarrow$
$(\bigsqcap\ (map\ snd\ \Delta) \sqcap \bigsqcup\ (map\ (\bigsqcap \circ (map\ snd \circ remdups))\ \Psi))$
⟨*proof*⟩

lemma (**in** *classical-logic*) *optimal-witness-list-intersect-biconditional*:
assumes $mset\ \Xi \subseteq\#\ mset\ \Gamma$
and $mset\ \Phi \subseteq\#\ mset\ (\Gamma \ominus \Xi)$
and $mset\ \Psi \subseteq\#\ mset\ (\mathfrak{W}_{\rightarrow}\ \varphi\ \Xi)$

shows $\exists\ \Sigma.\ \vdash ((\Phi\ @\ \Psi) :\to \varphi) \leftrightarrow (\bigsqcup\ (\mathit{map} \bigsqcap\ \Sigma) \to \varphi)$
$\wedge\ (\forall\ \sigma \in \mathit{set}\ \Sigma.\ \mathit{mset}\ \sigma \subseteq\#\ \mathit{mset}\ \Gamma \wedge \mathit{length}\ \sigma + 1 \geq \mathit{length}\ (\Phi\ @\ \Psi))$
$\langle \mathit{proof} \rangle$

lemma (**in** *classical-logic*) *relative-maximals-optimal-witness*:
assumes $\neg \vdash \varphi$
shows $0 < (\|\ \Gamma\ \|_\varphi)$
$= (\exists\ \Sigma.\ \mathit{mset}\ (\mathit{map}\ \mathit{snd}\ \Sigma) \subseteq\#\ \mathit{mset}\ \Gamma\ \wedge$
$\mathit{map}\ (\mathit{uncurry}\ (\sqcup))\ \Sigma :\vdash \varphi\ \wedge$
$1 + (\|\ \mathit{map}\ (\mathit{uncurry}\ (\to))\ \Sigma\ @\ \Gamma \ominus \mathit{map}\ \mathit{snd}\ \Sigma\ \|_\varphi) = \|\ \Gamma\ \|_\varphi)$
$\langle \mathit{proof} \rangle$

primrec (**in** *implication-logic*)
$\mathit{MaxSAT\text{-}witness} :: ('a \times 'a)\ \mathit{list} \Rightarrow 'a\ \mathit{list} \Rightarrow ('a \times 'a)\ \mathit{list}\ (\mathfrak{U})$
where
$\mathfrak{U}$ - [] = []
$|\ \mathfrak{U}\ \Sigma\ (\xi\ \#\ \Xi) = (\mathit{case}\ \mathit{find}\ (\lambda\ \sigma.\ \xi = \mathit{snd}\ \sigma)\ \Sigma\ \mathit{of}$
$\mathit{None} \Rightarrow \mathfrak{U}\ \Sigma\ \Xi$
$|\ \mathit{Some}\ \sigma \Rightarrow \sigma\ \#\ (\mathfrak{U}\ (\mathit{remove1}\ \sigma\ \Sigma)\ \Xi))$

lemma (**in** *implication-logic*) *MaxSAT-witness-right-msub*:
$\mathit{mset}\ (\mathit{map}\ \mathit{snd}\ (\mathfrak{U}\ \Sigma\ \Xi)) \subseteq\#\ \mathit{mset}\ \Xi$
$\langle \mathit{proof} \rangle$

lemma (**in** *implication-logic*) *MaxSAT-witness-left-msub*:
$\mathit{mset}\ (\mathfrak{U}\ \Sigma\ \Xi) \subseteq\#\ \mathit{mset}\ \Sigma$
$\langle \mathit{proof} \rangle$

lemma (**in** *implication-logic*) *MaxSAT-witness-right-projection*:
$\mathit{mset}\ (\mathit{map}\ \mathit{snd}\ (\mathfrak{U}\ \Sigma\ \Xi)) = \mathit{mset}\ ((\mathit{map}\ \mathit{snd}\ \Sigma) \cap \Xi)$
$\langle \mathit{proof} \rangle$

lemma (**in** *classical-logic*) *witness-list-implication-rule*:
$\vdash (\mathit{map}\ (\mathit{uncurry}\ (\sqcup))\ \Sigma :\to \varphi) \to \bigsqcap\ (\mathit{map}\ (\lambda\ (\chi, \xi).\ (\chi \to \xi) \to \varphi)\ \Sigma) \to \varphi$
$\langle \mathit{proof} \rangle$

lemma (**in** *classical-logic*) *witness-relative-MaxSAT-increase*:
assumes $\neg \vdash \varphi$
and $\mathit{mset}\ (\mathit{map}\ \mathit{snd}\ \Sigma) \subseteq\#\ \mathit{mset}\ \Gamma$
and $\mathit{map}\ (\mathit{uncurry}\ (\sqcup))\ \Sigma :\vdash \varphi$
shows $(|\ \Gamma\ |_\varphi) < (|\ \mathit{map}\ (\mathit{uncurry}\ (\to))\ \Sigma\ @\ \Gamma \ominus \mathit{map}\ \mathit{snd}\ \Sigma\ |_\varphi)$
$\langle \mathit{proof} \rangle$

lemma (**in** *classical-logic*) *relative-maximals-counting-deduction-lower-bound*:
assumes $\neg \vdash \varphi$
shows $(\Gamma\ \#\!\vdash\ n\ \varphi) = (n \leq \|\ \Gamma\ \|_\varphi)$
$\langle \mathit{proof} \rangle$

As a brief aside, we may observe that φ is a tautology if and only if counting deduction can prove it for any given number of times. This follows immediately from $\neg \vdash \varphi \Longrightarrow \Gamma \ \#\!\vdash \ n \ \varphi = (n \leq \| \ \Gamma \ \|_{\varphi})$.

lemma (**in** *classical-logic*) *counting-deduction-tautology-equiv*:
$(\forall \ n. \ \Gamma \ \#\!\vdash \ n \ \varphi) = \vdash \varphi$
$\langle proof \rangle$

theorem (**in** *classical-logic*) *relative-maximals-max-counting-deduction*:
$\Gamma \ \#\!\vdash \ n \ \varphi = (\forall \ \Phi \in \mathcal{M} \ \Gamma \ \varphi. \ n \leq \mathit{length} \ (\Gamma \ominus \Phi))$
$\langle proof \rangle$

lemma (**in** *consistent-classical-logic*) *counting-deduction-to-maxsat*:
$(\Gamma \ \#\!\vdash \ n \ \bot) = (\mathit{MaxSAT} \ \Gamma + n \leq \mathit{length} \ \Gamma)$
$\langle proof \rangle$

Chapter 4

Inequality Completeness For Probability Logic

4.1 Limited Counting Deduction Completeness

The reduction of counting deduction to MaxSAT allows us to first prove completeness for counting deduction, as maximal consistent sublists allow us to recover maximally consistent sets, which give rise to Dirac measures.

The completeness result first presented here, where all of the propositions on the left hand side are the same, will be extended later.

lemma (**in** *probability-logic*) *list-probability-upper-bound*:
$(\sum \gamma \leftarrow \Gamma.\ \mathcal{P}\ \gamma) \leq \mathit{real}\ (\mathit{length}\ \Gamma)$
$\langle \mathit{proof} \rangle$

theorem (**in** *classical-logic*) *dirac-limited-counting-deduction-completeness*:
$(\forall\ \mathcal{P} \in \mathit{dirac\text{-}measures}.\ \mathit{real}\ n * \mathcal{P}\ \varphi \leq (\sum \gamma \leftarrow \Gamma.\ \mathcal{P}\ \gamma)) = \sim \Gamma\ \#\!\vdash\ n\ (\sim \varphi)$
$\langle \mathit{proof} \rangle$

4.2 Measure Deduction Completeness

Since measure deduction may be reduced to counting deduction, we have measure deduction is complete.

lemma (**in** *classical-logic*) *dirac-measure-deduction-completeness*:
$(\forall\ \mathcal{P} \in \mathit{dirac\text{-}measures}.\ (\sum \varphi \leftarrow \Phi.\ \mathcal{P}\ \varphi) \leq (\sum \gamma \leftarrow \Gamma.\ \mathcal{P}\ \gamma)) = \sim \Gamma\ \$\!\vdash\ \sim \Phi$
$\langle \mathit{proof} \rangle$

theorem (**in** *classical-logic*) *measure-deduction-completeness*:
$(\forall\ \mathcal{P} \in \mathit{probabilities}.\ (\sum \varphi \leftarrow \Phi.\ \mathcal{P}\ \varphi) \leq (\sum \gamma \leftarrow \Gamma.\ \mathcal{P}\ \gamma)) = \sim \Gamma\ \$\!\vdash\ \sim \Phi$
$\langle \mathit{proof} \rangle$

4.3 Counting Deduction Completeness

Leveraging our measure deduction completeness result, we may extend our limited counting deduction completeness theorem to full completness.

lemma (**in** *classical-logic*) *measure-left-commute*:
$(\Phi\ @\ \Psi)\ \$\vdash\ \Xi = (\Psi\ @\ \Phi)\ \$\vdash\ \Xi$
⟨*proof*⟩

lemma (**in** *classical-logic*) *stronger-theory-double-negation-right*:
$\Phi \preceq \sim (\sim \Phi)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *stronger-theory-double-negation-left*:
$\sim (\sim \Phi) \preceq \Phi$
⟨*proof*⟩

lemma (**in** *classical-logic*) *counting-deduction-completeness*:
$(\forall\ \mathcal{P} \in \textit{dirac-measures}.\ (\sum \varphi \leftarrow \Phi.\ \mathcal{P}\ \varphi) \leq (\sum \gamma \leftarrow \Gamma.\ \mathcal{P}\ \gamma)) = (\sim \Gamma\ @\ \Phi)\ \#\vdash (\textit{length}\ \Phi)\ \bot$
⟨*proof*⟩

4.4 Collapse Theorem For Probability Logic

We now turn to proving the collapse theorem for probability logic. This states that any inequality holds for all finitely additive probability measures if and only if it holds for all Dirac measures.

theorem (**in** *classical-logic*) *weakly-additive-completeness-collapse*:
$(\forall\ \mathcal{P} \in \textit{probabilities}.\ (\sum \varphi \leftarrow \Phi.\ \mathcal{P}\ \varphi) \leq (\sum \gamma \leftarrow \Gamma.\ \mathcal{P}\ \gamma))$
$= (\forall\ \mathcal{P} \in \textit{dirac-measures}.\ (\sum \varphi \leftarrow \Phi.\ \mathcal{P}\ \varphi) \leq (\sum \gamma \leftarrow \Gamma.\ \mathcal{P}\ \gamma))$
⟨*proof*⟩

The collapse theorem may be strengthened to include an arbitrary constant term c. This will be key to characterizing MaxSAT completeness in §4.5.

lemma (**in** *classical-logic*) *nat-dirac-probability*:
$\forall\ \mathcal{P} \in \textit{dirac-measures}.\ \exists\, n :: \textit{nat}.\ \textit{real}\ n = (\sum \varphi \leftarrow \Phi.\ \mathcal{P}\ \varphi)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *dirac-ceiling*:
$\forall\ \mathcal{P} \in \textit{dirac-measures}.$
$((\sum \varphi \leftarrow \Phi.\ \mathcal{P}\ \varphi) + c \leq (\sum \gamma \leftarrow \Gamma.\ \mathcal{P}\ \gamma))$
$= ((\sum \varphi \leftarrow \Phi.\ \mathcal{P}\ \varphi) + \lceil c \rceil \leq (\sum \gamma \leftarrow \Gamma.\ \mathcal{P}\ \gamma))$
⟨*proof*⟩

lemma (**in** *probability-logic*) *probability-replicate-verum*:
fixes $n :: \textit{nat}$
shows $(\sum \varphi \leftarrow \Phi.\ \mathcal{P}\ \varphi) + n = (\sum \varphi \leftarrow (\textit{replicate}\ n\ \top)\ @\ \Phi.\ \mathcal{P}\ \varphi)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *dirac-collapse*:
$(\forall\ \mathcal{P} \in \textit{probabilities}.\ (\sum\varphi\leftarrow\Phi.\ \mathcal{P}\ \varphi) + c \leq (\sum\gamma\leftarrow\Gamma.\ \mathcal{P}\ \gamma))$
$= (\forall\ \mathcal{P} \in \textit{dirac-measures}.\ (\sum\varphi\leftarrow\Phi.\ \mathcal{P}\ \varphi) + \lceil c \rceil \leq (\sum\gamma\leftarrow\Gamma.\ \mathcal{P}\ \gamma))$
⟨*proof*⟩

lemma (**in** *classical-logic*) *dirac-strict-floor*:
$\forall\ \mathcal{P} \in \textit{dirac-measures}.$
$((\sum\varphi\leftarrow\Phi.\ \mathcal{P}\ \varphi) + c < (\sum\gamma\leftarrow\Gamma.\ \mathcal{P}\ \gamma))$
$= ((\sum\varphi\leftarrow\Phi.\ \mathcal{P}\ \varphi) + \lfloor c \rfloor + \mathit{1} \leq (\sum\gamma\leftarrow\Gamma.\ \mathcal{P}\ \gamma))$
⟨*proof*⟩

lemma (**in** *classical-logic*) *strict-dirac-collapse*:
$(\forall\ \mathcal{P} \in \textit{probabilities}.\ (\sum\varphi\leftarrow\Phi.\ \mathcal{P}\ \varphi) + c < (\sum\gamma\leftarrow\Gamma.\ \mathcal{P}\ \gamma))$
$= (\forall\ \mathcal{P} \in \textit{dirac-measures}.\ (\sum\varphi\leftarrow\Phi.\ \mathcal{P}\ \varphi) + \lfloor c \rfloor + \mathit{1} \leq (\sum\gamma\leftarrow\Gamma.\ \mathcal{P}\ \gamma))$
⟨*proof*⟩

4.5 MaxSAT Completeness For Probability Logic

It follows from the collapse theorem that any probability inequality tautology, include those with *constant terms*, may be reduced to a bounded MaxSAT problem. This is not only a key computational complexity result, but suggests a straightforward algorithm for *computing* probability identities.

lemma (**in** *classical-logic*) *relative-maximals-verum-extract*:
assumes $\neg \vdash \varphi$
shows $(|\ \textit{replicate}\ n\ \top\ @\ \Phi\ |_{\varphi}) = n + (|\ \Phi\ |_{\varphi})$
⟨*proof*⟩

lemma (**in** *classical-logic*) *complement-MaxSAT-completeness*:
$(\forall\ \mathcal{P} \in \textit{dirac-measures}.\ (\sum\varphi\leftarrow\Phi.\ \mathcal{P}\ \varphi) \leq (\sum\gamma\leftarrow\Gamma.\ \mathcal{P}\ \gamma)) = (\textit{length}\ \Phi \leq \|\ \sim\Gamma\ @\ \Phi\ \|_{\bot})$
⟨*proof*⟩

lemma (**in** *classical-logic*) *relative-maximals-neg-verum-elim*:
$(|\ \textit{replicate}\ n\ (\sim\top)\ @\ \Phi\ |_{\varphi}) = (|\ \Phi\ |_{\varphi})$
⟨*proof*⟩

lemma (**in** *classical-logic*) *dirac-MaxSAT-partial-completeness*:
$(\forall\ \mathcal{P} \in \textit{dirac-measures}.\ (\sum\varphi\leftarrow\Phi.\ \mathcal{P}\ \varphi) \leq (\sum\gamma\leftarrow\Gamma.\ \mathcal{P}\ \gamma)) = (\textit{MaxSAT}\ (\sim\Gamma\ @\ \Phi\ ) \leq \textit{length}\ \Gamma)$
⟨*proof*⟩

lemma (**in** *consistent-classical-logic*) *dirac-inequality-elim*:
fixes $c :: \textit{real}$
assumes $\forall\ \mathcal{P} \in \textit{dirac-measures}.\ (\sum\varphi\leftarrow\Phi.\ \mathcal{P}\ \varphi) + c \leq (\sum\gamma\leftarrow\Gamma.\ \mathcal{P}\ \gamma)$
shows $(\textit{MaxSAT}\ (\sim\Gamma\ @\ \Phi) + c \leq \textit{length}\ \Gamma)$
⟨*proof*⟩

lemma (**in** *classical-logic*) *dirac-inequality-intro*:
fixes c :: *real*
assumes $MaxSAT$ ($\sim$ Γ @ Φ) + $c \leq$ *length* Γ
shows $\forall$ $\mathcal{P} \in$ *dirac-measures*. ($\sum \varphi \leftarrow \Phi$. $\mathcal{P}$ φ) + $c \leq$ ($\sum \gamma \leftarrow \Gamma$. $\mathcal{P}$ γ)
⟨*proof*⟩

lemma (**in** *consistent-classical-logic*) *dirac-inequality-equiv*:
($\forall$ $\delta \in$ *dirac-measures*. ($\sum \varphi \leftarrow \Phi$. δ φ) + $c \leq$ ($\sum \gamma \leftarrow \Gamma$. δ γ))
= ($MaxSAT$ ($\sim$ Γ @ Φ) + (c :: *real*) $\leq$ *length* Γ)
⟨*proof*⟩

theorem (**in** *consistent-classical-logic*) *probability-inequality-equiv*:
($\forall$ $\mathcal{P} \in$ *probabilities*. ($\sum \varphi \leftarrow \Phi$. $\mathcal{P}$ φ) + $c \leq$ ($\sum \gamma \leftarrow \Gamma$. $\mathcal{P}$ γ))
= ($MaxSAT$ ($\sim$ Γ @ Φ) + (c :: *real*) $\leq$ *length* Γ)
⟨*proof*⟩

no-notation *first-component* ($\mathfrak{A}$)
no-notation *second-component* ($\mathfrak{B}$)
no-notation *merge-witness* ($\mathfrak{J}$)
no-notation *X-witness* ($\mathfrak{X}$)
no-notation *X-component* ($\mathfrak{X}_\bullet$)
no-notation *Y-witness* ($\mathfrak{Y}$)
no-notation *Y-component* ($\mathfrak{Y}_\bullet$)
no-notation *submerge-witness* ($\mathfrak{E}$)
no-notation *recover-witness-A* ($\mathfrak{P}$)
no-notation *recover-complement-A* ($\mathfrak{P}^C$)
no-notation *recover-witness-B* ($\mathfrak{Q}$)
no-notation *relative-maximals* ($\mathcal{M}$)
no-notation *relative-MaxSAT* (| - |_ [*45*])
no-notation *complement-relative-MaxSAT* (‖ - ‖_ [*45*])
no-notation *MaxSAT-optimal-pre-witness* ($\mathfrak{V}$)
no-notation *MaxSAT-optimal-witness* ($\mathfrak{W}$)
no-notation *disjunction-MaxSAT-optimal-witness* ($\mathfrak{W}_\sqcup$)
no-notation *implication-MaxSAT-optimal-witness* ($\mathfrak{W}_\rightarrow$)
no-notation *MaxSAT-witness* ($\mathfrak{U}$)

notation *FuncSet.funcset* (**infixr** $\rightarrow$ *60*)

end

Bibliography

[1] M. R. Garey, D. S. Johnson, and L. Stockmeyer. Some simplified NP-complete graph problems. *Theoretical Computer Science*, 1(3):237–267, Feb. 1976.