Duality theory in linear optimization and its extensions—formally verified

1 Introduction

A basic knowledge from linear algebra is that a system of linear equalities has a solution if and only if we cannot obtain a contradiction by taking a linear combination of the equalities. We state this theorem as follows.

Theorem (basicLinearAlgebra): Let I and J be finite types. Let F be a linearly ordered field. Let A be a matrix of type $(I \times J) \to F$. Let b be a vector of type $I \to F$. Exactly one of the following exists:

- vector $x : J \to F$ such that $A \cdot x = b$

- vector $y : I \to F$ such that $A^T \cdot y = 0$ and $b \cdot y \neq 0$

This theorem can be given in much more general settings. Here, however, this is the only version we provide. This special case of the Fredholm alternative is not our main focus but a byproduct of the other theorems we prove. In particular, we obtain basicLinearAlgebra as an immediate corollary of the following theorem.

Theorem (basicLinearAlgebra_lt): Let I and J be finite types. Let F be a linearly ordered field. Let A be a matrix of type $(I \times J) \to F$. Let b be a vector of type $I \to F$. Exactly one of the following exists:

- vector $x : J \to F$ such that $A \cdot x = b$

- vector $y : I \to F$ such that $A^T \cdot y = 0$ and $b \cdot y < 0$

The way we state the theorem exemplifies certain patterns that permeate through our work. Our results are phrased as "there are two systems of (in)equalities; exactly one of them has a solution". This goes hand-in-hand with our decision to focus mostly on "symmetric" Farkas-like theorems. Note that it must be impossible to satisfy the second system by $y = 0$. Had it been allowed, we would have said nothing about the first system as it would have to lead to a contradiction every time. The constraint $b \cdot y < 0$ disqualifies the zero solution in most of our theorems. Intuitively, it should make sense that one of the systems is always "strict" (to easily see why, consider I and J singletons), which also means that our two systems will never be "fully symmetric".

Farkas (TODO citation) gave a similar characterization for systems of linear equalities with nonnegative variables. We state his theorem as follows.

Theorem (equalityFarkas): Let I and J be finite types. Let F be a linearly ordered field. Let A be a matrix of type $(I \times J) \to F$. Let b be a vector of type $I \to F$. Exactly one of the following exists:

- nonnegative vector $x : J \to F$ such that $A \cdot x = b$

- vector $y : I \to F$ such that $A^T \cdot y \geq 0$ and $b \cdot y < 0$

We prove basicLinearAlgebra_lt by applying equalityFarkas to the matrix $(A \mid -A)$. However, equalityFarkas will be proved later, from a more general theorem.

Minkowski (TODO citation) similarly established that a system of linear inequalities has a nonnegative solution if and only if we cannot obtain a contradiction by taking a nonnegative linear combination of the inequalities. For reasons that will be apparent later, we give two versions of this theorem.

Theorem (inequalityFarkas): Let I and J be finite types. Let F be a linearly ordered field. Let A be a matrix of type $(I \times J) \to F$. Let b be a vector of type $I \to F$. Exactly one of the following exists:

- nonnegative vector $x : J \to F$ such that $A \cdot x \leq b$

- nonnegative vector $y : I \to F$ such that $A^T \cdot y \geq 0$ and $b \cdot y < 0$

Theorem (inequalityFarkas_neg): Let I and J be finite types. Let F be a linearly ordered field. Let A be a matrix of type $(I \times J) \to F$. Let b be a vector of type $I \to F$. Exactly one of the following exists:

- nonnegative vector $x : J \to F$ such that $A \cdot x \leq b$

- nonnegative vector $y : I \to F$ such that $(-A^T) \cdot y \leq 0$ and $b \cdot y < 0$

Obviously, inequalityFarkas_neg is an immediate corollary of inequalityFarkas. We prove inequalityFarkas by applying equalityFarkas to the matrix $(1 \mid A)$ where 1 is the identity matrix of type $(I \times I) \to F$.

The next theorem generalizes equalityFarkas to structures where multiplication does not have to be commutative. Furthermore, it supports infinitely many equations.

Theorem (coordinateFarkas): Let I be any type. Let J be a finite type. Let R be a linearly ordered division ring. Let A be an R-linear map from from $(I \to R)$ to $(J \to R)$. Let b be an R-linear map from from $(I \to R)$ to R. Exactly one of the following exists:

- nonnegative vector $x : J \to R$ such that, for all $w : I \to R$, we have $\sum_{j:J} (A\ w)_j \bullet x_j = b\ w$

- vector $y : I \to R$ such that $A\ y \geq 0$ and $b\ y < 0$

In the next generalization, we replace the partially ordered module $I \to R$ by a general R-module W.

Theorem (scalarFarkas): Let J be a finite type. Let R be a linearly ordered division ring. Let W be an R-module. Let A be an R-linear map from from W to $(J \to R)$. Let b be an R-linear map from from W to R. Exactly one of the following exists:

- nonnegative vector $x : J \to R$ such that, for all $w : W$, we have $\sum_{j:J} (A\ w)_j \bullet x_j = b\ w$

- vector $y : W$ such that $A\ y \geq 0$ and $b\ y < 0$

In the most general theorem, stated below, we replace certain occurrences of R by a linearly ordered R-module V whose order respects order on R. This result origins from TODO.

Theorem (fintypeFarkasBartl): Let J be a finite type. Let R be a linearly ordered division ring. Let W be an R-module. Let V be a linearly ordered R-module. We furthermore require monotonicity of scalar multiplication by nonnegative elements on the left. Let A be an R-linear map from W to $(J \to R)$. Let b be an R-linear map from W to V. Exactly one of the following exists:

- nonnegative vector family $x : J \to V$ such that, for all $w : W$, we have $\sum_{j:J} (A\ w)_j \bullet x_j = b\ w$

- vector $y : W$ such that $A\ y \geq 0$ and $b\ y < 0$

In the last branch, $A\ y \geq 0$ uses the partial order on $(J \to R)$ whereäs $b\ y < 0$ uses the linear order on V. Note that fintypeFarkasBartl subsumes scalarFarkas (as well as the other versions based on equality), since R can be viewed as a linearly ordered module over itself.

2 Extensions

Until now, we have talked about known results. What follows is a new extension of the theory.

Definition: Let F be a linearly ordered field. We define an **extended** linearly ordered field F_∞ as $F \cup \{\bot, \top\}$ with the following properties. Let p and q be numbers from F. We have $\bot < p < \top$. We define addition, scalar action, and negation on F_∞ as follows:

+	$\bot$	q	$\top$
$\bot$	$\bot$	$\bot$	$\bot$
p	$\bot$	$p+q$	$\top$
$\top$	$\bot$	$\top$	$\top$

$\bullet$	$\bot$	q	$\top$
0	$\bot$	0	0
$p > 0$	$\bot$	$p \cdot q$	$\top$

$-$	$\bot$	q	$\top$
	$\top$	$-q$	$\bot$

When we talk about elements of F_∞, we say that values from F are **finite**.

Informally speaking, $\top$ represents the positive infinity, $\bot$ represents the negative infinity, and we say that $\bot$ is "stronger" than $\top$ in all arithmetic operations. The surprising parts are $\bot + \top = \bot$ and $0 \bullet \bot = \bot$. Because of them, F_∞ is not a field. In fact, F_∞ is not even a group. However, F_∞ is still a densely linearly ordered abelian monoid with characteristic zero.

Theorem (extendedFarkas): Let I and J be finite types. Let F be a linearly ordered field. Let A be a matrix of type $(I \times J) \to F_\infty$. Let b be a vector of type $I \to F_\infty$. Assume that A does not have $\bot$ and $\top$ in the same row. Assume that A does not have $\bot$ and $\top$ in the same column. Assume that A does not have $\top$ in any row where b has $\top$. Assume that A does not have $\bot$ in any row where b has $\bot$. Exactly one of the following exists:

- nonnegative vector $x : J \to F$ such that $A \cdot x \leq b$

- nonnegative vector $y : I \to F$ such that $(-A^T) \cdot y \leq 0$ and $b \cdot y < 0$

Note that extendedFarkas looks pretty much like equalityFarkas_neg and, in certain sense, generalizes it.

Next we define an extended notion of linear program, i.e., linear programming over extended linearly ordered fields. The implicit intention is that the linear program is to be minimized.

Definition: Let I and J be finite types. Let F be a linearly ordered field. Let A be a matrix of type $(I \times J) \to F_\infty$, let b be a vector of type $I \to F_\infty$, and c be a vector of type $J \to F_\infty$ such that the following six conditions hold:

- A does not have $\bot$ and $\top$ in the same row

- A does not have $\bot$ and $\top$ in the same column

- b does not contain $\bot$

- c does not contain $\bot$

- A does not have $\top$ in any row where b has $\top$

- A does not have $\bot$ in any column where c has $\top$

We say that $P = (A, b, c)$ is a **linear program** over F_∞ whose constraints are indexed by I and variables are indexed by J. We say that a nonnegative vector $x : J \to R$ is a **solution** to P if and only if $A \cdot x \leq b$. We say that P **reaches** an objective value r if and only if there exists x such that x is a solution to P and $c \cdot x = r$. We say that P is **feasible** if and only if P reaches a finite[1] value. We say that P is **bounded by** a finite value r if and only if, for every value p reached by P, we have $r \leq p$. We say that P is **unbounded** if and only if there is no finite value r such that P is bounded by r. We say that the linear program $(-A^T, c, b)$ is the **dual** of P.

Theorem (weakDuality): Let F be a linearly ordered field. Let P be a linear program over F_∞. If P reaches p and the dual of P reaches q, then $p + q \geq 0$.

Definition: Let F be a linearly ordered field. Let P be a linear program over F_∞. We define the **optimum** of P as follows. If P is feasible and unbounded, its optimum is $\bot$. If P is not feasible, its optimum is $\top$. In all other cases, we ask whether P reaches a finite value r such that P is bounded by r. If so, its optimum is r. Otherwise, P does not have optimum.[2]

Theorem (strongDuality):[3] Let F be a linearly ordered field. Let P be a linear program over F_∞. If P or its dual is feasible (at least one of them), then there exists p in F_∞ such that P has optimum p and the dual of P has optimum $-p$.

---

[1] It would be perhaps more natural to say that P reaches a value different from $\top$. However, since $\bot$ cannot be reached because of the way linear programming is defined, it is equivalent to our definition by reaching a finite value.

[2] By the end of the paper, we will have proved that optimum always exists, i.e., it cannot happen that the set of objective values reached by P has a finite infimum that is not attained. However, because we do not have the theorem now, the optimum is defined as a partial function from linear programs to F_∞.

[3] For simplicity, we rephrased the theorem without mentioning partial functions. Also note that it would be incorrect to say the following: P has optimum p, the dual of P has optimum q, and $p + q = 0$. It would fail for unbounded linear programs because the arithmetics of F_∞ defines $\top + \bot = \bot$.