A Decision Procedure for Probability Calculus with Applications

Branden Fitelson[*]
University of California–Berkeley

04/16/08. Penultimate draft (final version to appear in the *Review of Symbolic Logic*).

Abstract. A decision procedure (PrSAT) for classical (Kolmogorov) probability calculus is presented. This decision procedure is based on an existing decision procedure for the theory of real closed fields, which has recently been implemented in *Mathematica*. A *Mathematica* implementation of PrSAT is also described, along with several applications to various non-trivial problems in the probability calculus.

Keywords: Probability, decision procedure, Tarski, Kolmogorov, CAD, Bayesian

1. Probability Calculus: Axiomatic Presentation

The standard presentation of probability calculus is that of Kolomogorov [19]. His presentation is axiomatic and couched in set-theoretic terms. I will use Kolmogorov's axioms here, but I will couch them in logical rather than set-theoretic terms. This choice is merely conventional, but it will make subsequent sections of the paper easier to digest.

I will be concerned only with finite probability models (*i.e.*, probability models over finite Boolean algebras). As such, I begin with a *sentential language* $\mathcal{L}_n$, containing n atomic sentences $\{A_1, \dots, A_n\}$, and all wffs that can be constructed from them using the standard truth-functional connectives. I will use '$\top$' ('$\bot$') to denote an arbitrary tautology (contradiction) of $\mathcal{L}_n$, '$\vDash$' to denote the metatheoretic relation of tautological entailment in $\mathcal{L}_n$ ('$\Dashv\vDash$' will denote tautological equivalence in $\mathcal{L}_n$), and lower-case italic letters $p, q, r \dots$ will be metavariables ranging over sentences of $\mathcal{L}_n$. With this background in place, we have:

[*] I would like to thank Jason Alexander and Ben Blum for their invaluable assistance with various *Mathematica* implementations of PrSAT. I would also like to thank three avid users of PrSAT: Igor Douven, Wouter Meijs, and John Pollock, who have come up with lots of interesting problems for PrSAT to solve, and also provided very useful feedback on PrSAT's performance. I would also like to thank the members of audiences (too many individuals to thank here, I'm afraid!) at the University of California–Irvine, the University of Michigan, Stanford University, the University of Bristol, the University of California–Berkeley, the University of San Francisco, San José State University, the University of Iowa, Argonne National Laboratory, Lawrence Livermore National Laboratory, and SRI International for valuable discussion and feedback on presentations and demonstrations of various versions of PrSAT. Finally, I am indebted to an anonymous referee of the *Review of Symbolic Logic*.

Definition. *A probability model* $\mathfrak{M}_n = \langle \mathcal{L}_n, \Pr \rangle$ *consists of a sentential language* $\mathcal{L}_n$*, together with a unary unconditional probability function* $\Pr(\cdot) \colon \mathcal{L}_n \mapsto \mathbb{R}$ *satisfying the following axioms of Kolmogorov [19].*

1. *For all* $p \in \mathcal{L}_n$, $\Pr(p) \geq 0$.
2. *For all* $p \in \mathcal{L}_n$*, if* $p \Dashv\vDash \top$*, then* $\Pr(p) = 1$.
3. *For all* $p, q \in \mathcal{L}_n$*, if* $p \,\&\, q \Dashv\vDash \bot$*, then* $\Pr(p \vee q) = \Pr(p) + \Pr(q)$.

Again following Kolmogorov [19], we also define a binary conditional probability function $\Pr(\cdot \mid \cdot) \colon \mathcal{L}_n \times \mathcal{L}_n \mapsto \mathbb{R}$*, in terms of* $\Pr(\cdot)$*, as follows:*

4. *For all* $p, q \in \mathcal{L}_n$*, if* $\Pr(q) \neq 0$*, then* $\Pr(p \mid q) \overset{\text{def}}{=} \dfrac{\Pr(p \,\&\, q)}{\Pr(q)}$.

In the next section, I will show how such probability models can, alternatively, be couched entirely in simple *algebraic* terms. This will be the key to our subsequent decision procedure for probability calculus.

2. Probability Calculus: Algebraic Presentation

In this section, I explain how any probability model $\mathfrak{M}_n$ can be given a simple algebraic representation using what I will call a *stochastic truth-table*. Here is a simple example. Let's take a sentential language $\mathcal{L}_3$ with three atomic sentences $\{A, B, C\}$. An ordinary truth-table for such a language has $2^3 = 8$ rows. Each row (i) of the truth table corresponds to a state description (s_i) of the language $\mathcal{L}_3$. And, every truth-functional proposition definable in terms of $\{A, B, C\}$ can be expressed as a disjunction of said state descriptions. So far, this is all just elementary classical sentential calculus, with which we are all intimately familiar. Now, a *stochastic* truth-table for $\mathfrak{M}_3 = \langle \mathcal{L}_3, \Pr \rangle$ is a truth-table with an additional column containing real numbers corresponding to the values assigned by Pr to each state description of $\mathcal{L}_3$. Thus, for $\mathfrak{M}_3$, we have:

A	B	C	State Descriptions (s_i)	$\Pr(s_i) = \mathfrak{s}_i$
T	T	T	$A \,\&\, B \,\&\, C = s_1$	$\Pr(s_1) = \mathfrak{s}_1$
T	T	F	$A \,\&\, B \,\&\, {\sim}C = s_2$	$\Pr(s_2) = \mathfrak{s}_2$
T	F	T	$A \,\&\, {\sim}B \,\&\, C = s_3$	$\Pr(s_3) = \mathfrak{s}_3$
T	F	F	$A \,\&\, {\sim}B \,\&\, {\sim}C = s_4$	$\Pr(s_4) = \mathfrak{s}_4$
F	T	T	${\sim}A \,\&\, B \,\&\, C = s_5$	$\Pr(s_5) = \mathfrak{s}_5$
F	T	F	${\sim}A \,\&\, B \,\&\, {\sim}C = s_6$	$\Pr(s_6) = \mathfrak{s}_6$
F	F	T	${\sim}A \,\&\, {\sim}B \,\&\, C = s_7$	$\Pr(s_7) = \mathfrak{s}_7$
F	F	F	${\sim}A \,\&\, {\sim}B \,\&\, {\sim}C = s_8$	$\Pr(s_8) = \mathfrak{s}_8$

Now, just as each proposition p expressible in $\mathcal{L}_3$ is equivalent to some disjunction $\bigvee_i s_i$ of state descriptions of $\mathcal{L}_3$, each unconditional probability term $\Pr(p)$ of the language of $\mathfrak{M}_3$ can be expressed as a sum $\sum_i \mathfrak{s}_i$ of the real numbers assigned by Pr to those state descriptions of $\mathcal{L}_3$ that make-up the disjunction of state descriptions which expresses p.[1] Moreover, each conditional probability term $\Pr(p\,|\,q)$ of the language of $\mathfrak{M}_3$ can be expressed as a ratio of the sums corresponding to $\Pr(p \& q)$ and $\Pr(q)$, respectively. This gives us a faithful translation from the language of $\mathfrak{M}_3$ into the language of simple real algebra (*viz.*, high-school algebra). Here are some examples of translations of probability terms in the language of $\mathfrak{M}_3$ into terms of high-school algebra:

- $\Pr(A) = \Pr(s_1 \vee s_2 \vee s_3 \vee s_4) = \mathfrak{s}_1 + \mathfrak{s}_2 + \mathfrak{s}_3 + \mathfrak{s}_4$
- $\Pr(B \,\&\, {\sim}C) = \Pr(s_2 \vee s_6) = \mathfrak{s}_2 + \mathfrak{s}_6$
- $\Pr(A\,|\,B \equiv C) = \dfrac{\Pr(A \,\&\, (B \equiv C))}{\Pr(B \equiv C)} = \dfrac{\Pr(s_1 \vee s_4)}{\Pr(s_1 \vee s_4 \vee s_5 \vee s_7)} = \dfrac{\mathfrak{s}_1 + \mathfrak{s}_4}{\mathfrak{s}_1 + \mathfrak{s}_4 + \mathfrak{s}_5 + \mathfrak{s}_7}$

Our only remaining task is to demonstrate that this procedure really does yield a general algebraic characterization of the concept of a (Kolmogorov) probability model $\mathfrak{M}_n$. There are two things that need to be shown here. First, we need to show that if we are given a *concrete* probability model (which assigns real numbers to each of the $\mathfrak{s}_i$), then the translation procedure yields an algebraic characterization of that concrete probability model. And, second, that, in the absence of specified numerical values for all the real variables $\mathfrak{s}_i$, we can use our algebraic translations to reason *generally* about probability models $\mathfrak{M}_n$.

For the first part, consider a concrete probability model $\mathfrak{M}_n$, and note that our translation procedure has two steps. First, it goes from $\Pr(p)$ to $\Pr(\bigvee_i s_i)$ where $\bigvee_i s_i$ is tautologically equivalent to p. That step is kosher, since it's a theorem of the (Kolmogorov) probability calculus (hence, true for *all* probability models) that $\Pr(p) = \Pr(q)$ if $p \dashv\vDash q$. The second step of our translation procedure goes from $\Pr(\bigvee_i s_i)$ to $\sum_i \mathfrak{s}_i$. This step is also kosher, since the s_i are mutually exclusive and finite additivity is one of the axioms of (Kolmogorov) probability calculus. Finally, since our translations of unconditional probability terms (for a concrete probability model) are Kosher, it follows that our translations of conditional probability terms will also be Kosher (for a concrete model), since translated conditional probabilities are defined in terms of translated unconditional probabilities in the appropriate way.

[1] Note added in proof: in the case where $p \dashv\vDash \bot$, the corresponding set of state descriptions will be the empty set $\varnothing$. In this degenerate case, we just stipulate that the empty disjunction gets assigned probability zero under all algebraic translations. That is, if $p \dashv\vDash \bot$, then the term $\ulcorner\Pr(p)\urcorner$ will be translated to '0'.

For the second part, no numerical values are assigned to the $\mathfrak{s}_i$, and we want to use our translations to reason *generally* about *arbitrary* probability models of size n. Here, we just need to impose two simple general algebraic constraints on the real variables $\mathfrak{s}_i$ that appear in a generic (non-numerical) stochastic truth-table for a model of size n:

- $\mathfrak{s}_1 \geq 0, \mathfrak{s}_2 \geq 0, \ldots, \mathfrak{s}_{2^n} \geq 0$.
- $\sum_{i=1}^{2^n} \mathfrak{s}_i = 1$

It is easy to verify that these two algebraic constraints ensure that the Kolmogorov axioms are respected (in general) by our translation. To see why, note that these two constraints ensure the following:

(*i*) $\Pr(p)$ will always (and for all p) get translated to a high-school algebra expression that is guaranteed (for all assignments of real numbers to the $\mathfrak{s}_i$) to be non-negative. This follows from the first constraint on the $\mathfrak{s}_i$'s (that they are all are non-negative), and the fact that $\Pr(p)$ is always translated as a sum of $\mathfrak{s}_i$'s.

(*ii*) $\Pr(\top)$ will always get translated to an expression that is algebraically identical (in high-school algebra) to the number 1. This follows from the translation set-up, and the second constraint on the $\mathfrak{s}_i$'s.

(*iii*) Provided that p and q are mutually exclusive, the terms $\Pr(p \vee q)$ and $\Pr(p) + \Pr(q)$ will always (and for all p and q) get translated to expressions that are algebraically identical (in high-school algebra). This doesn't even depend on the two constraints on the $\mathfrak{s}_i$'s. It is guaranteed by the nature of the translation scheme (and algebra).

Finally, since our translation is *generally* Kosher for unconditional probability terms, it will also be *generally* Kosher for conditional probability terms, since conditional probability translations are constructed in the appropriate way out of unconditional probability translations.[2]

With this translation technique in hand, we can now transform any set of statements in probability calculus into a corresponding set of statements in high-school algebra. By a *statement of probability calculus*, I mean an algebraically well-formed statement, which is either an equation, an inequation, or an inequality containing terms of the language of a probability model $\mathfrak{M}_n$ and/or symbols denoting real numbers (*i.e.*, real constants), where these probabilistic and/or algebraic terms can be combined using the standard algebraic operations of multiplication, division, addition, and subtraction. We also allow such simple statements of probability calculus to be combined using logical connectives. Here are a few example statements of probability calculus:

[2] See [21, pp. 13–14] for a more rigorous mathematical presentation of this algebraic representation of probability functions over sentential languages.

- $\Pr(A \mid B) \cdot \Pr(B \mid C) \geq \dfrac{\Pr(A \mid B \,\&\, C)}{\Pr(B \vee C)}$
- $\Pr(X) - \Pr(Y)^2 = \frac{1}{2}$
- $\Pr(C \mid A \vee \sim B) + 2 \cdot \Pr(B) \neq \frac{1}{\pi}$
- $\Pr(X \mid Y) > \Pr(X) \vee \Pr(X) < \Pr(Y)$

This definition of a statement of probability calculus is rather broad, but it does rule-out (in addition to statements that are not algebraically or logically well-formed) statements involving *quantification* over sentence letters and/or real variables. I enforce this restriction here because (a) it makes the presentation of our translation methods and our decision procedure much simpler, and (b) most applications of probability calculus (indeed, almost all applications with which I am familiar) do not (essentially) involve such quantification. In any event, the methods described here can be extended to this more general class of statements. But, I will not explain such extensions in this paper.

A set S of statements of probability calculus is *satisfiable* just in case there exists a concrete probability model $\mathfrak{M}$ on which all members of S are true. If S is unsatisfiable, this means that there is no such model, *i.e.*, that a contradiction can be deduced from the members of S using only the Kolmogorov axioms for probability calculus. A *decision procedure for probability calculus* is an algorithm which takes as input an arbitrary finite set S of statements of probability calculus. If S is satisfiable, then a decision procedure must output a concrete model $\mathfrak{M}$ on which all members of S are true, and if S is unsatisfiable, then a decision procedure must tell us that there are no such models. In the next section, I explain how the algebraic translation procedure described above allows us to produce a decision procedure for probability calculus, based on an existing decision procedure for high-school algebra.

3. PrSAT: A Decision Procedure for Probability Calculus

3.1. A High-Level Description of PrSAT

The first step in constructing PrSAT is writing the translation algorithm, which transforms any finite set S of statements in probability calculus into a finite set S' of statements in simple high-school algebra, in accordance with the procedure above.[3] Once this is done, we see immediately that the problem of giving a decision procedure for probability calculus is just the problem of giving a decision procedure for the satisfiability of sets of statements in high-school algebra. Specifically, the problem of deciding whether a set S of statements in probability calculus (in the language of $\mathfrak{M}_n$) is satisfiable is just the problem of deciding whether the following set of statements of high-school algebra is satisfiable:

$$S' \cup \left\{ \mathfrak{s}_1 \geq 0, \ldots, \mathfrak{s}_{2^n} \geq 0, \sum_{i=1}^{2^n} \mathfrak{s}_i = 1 \right\}$$

In other words, if we can find a procedure for deciding whether the union of our translated set S' and the set containing the pair of algebraic constraints on our $\mathfrak{s}_i$ is satisfiable, then we are done.

Happily, there is an existing decision procedure for statements of high-school algebra, and so all we need to do is use our translation algorithm, plus this existing decision procedure, and we'll have our decision procedure for probability calculus. In other words, we have:

1. Translate the set S of statements of probability calculus (in the language of $\mathfrak{M}_n$) into the set S' of high-school algebra statements, in accordance with the translation procedure described above.

2. Form the union $S' \cup C_n$, where $C_n = \{\mathfrak{s}_1 \geq 0, \ldots, \mathfrak{s}_{2^n} \geq 0, \sum_{i=1}^{2^n} \mathfrak{s}_i = 1\}$ is the set of algebraic constraints on the $\mathfrak{s}_i$, which ensures that they are basic *probabilities* corresponding to state descriptions of $\mathcal{L}_n$.

3. Consult the existing decision procedure for sets of high-school algebra statements (see below) as to the satisfiability of $S' \cup C_n$.[4]

4. If the decision procedure for high-school algebra says that $S' \cup C_n$ is unsatisfiable, then report that S is unsatisfiable. And, if the decision procedure returns a model $\mathfrak{M}'_n$ on which all members of $S' \cup C_n$ are true, then translate $\mathfrak{M}'_n$ back into the language of $\mathfrak{M}_n$, and this will yield a probability model on which all members of S are true. □

This general procedure, now known as PrSAT, has been implemented in *Mathematica* (which has the requisite decision procedure for high-school algebra as a built-in function — see below), and it has been

[3] Here, I am greatly indebted to Jason Alexander for implementing a very elegant and fully general version of this translation procedure in *Mathematica*. Before Jason came along, I had hard-coded the translation procedure in *Mathematica* for models of size $n = 2, 3, 4$ (I didn't even bother doing $n = 5$!). See [10, Appendix] for some early implementations of this kind. The new *Mathematica* implementation of PrSAT (available on my PrSAT website: http://fitelson.org/PrSAT/) uses Jason's techniques to generate (canonical) stochastic truth-tables and translations on-the-fly, from arbitrary sets S of statements in probability calculus.

[4] Actually, the latest versions of PrSAT do some other tricks at this stage of the high-level description of the procedure to simplify and optimize the input set. Also, the latest version of PrSAT contains a random-search option (implemented by Ben Blum), which can be tried before sending the problem to the decision procedure (*i.e.*, before this step). See section 5 for discussion of this added functionality.

used to solve many non-trivial problems in probability calculus. I will describe some example applications of PrSAT in the next section. But, first, I should say something about the existing decision procedure for high-school algebra (now built-in to *Mathematica*), which has been treated as a "black box" in our high-level description of PrSAT.

3.2. Decidability in the Theory of Real-Closed Fields

The theory of real closed fields (TRCF) is a vast generalization of high-school algebra. It is a first-order theory, which allows for arbitrary quantification over statements of arbitrary complexity that can be expressed using real variables and constants, the standard algebraic operations, equality and inequality signs, and logical connectives. The theory of high-school algebra is a tiny fragment of TRCF, which only involves existential (or universal) quantification over such (sets of) statements. High-school algebra does *not* involve *mixed* (∀∃ or ∃∀) quantification. This is a *significant* difference in expressive power. To get a sense of the power of full TRCF, note (*e.g.*) that the definition of a limit of any high-school algebra term can be defined in TRCF. Here is an example:

$$\lim_{x\to\infty}\frac{3x^2-5x+7}{7x^2-2x+11} \overset{\text{def}}{=} \iota\lambda\left[(\forall\epsilon>0)(\exists\delta)(\forall x>\delta)\left(-\epsilon<\frac{3x^2-5x+7}{7x^2-2x+11}-\lambda<\epsilon\right)\right]$$

Of course, we don't need the full power of the full TRCF for our present purposes. But, as it turns out, even this much more powerful theory is decidable. In the late 1920's Alfred Tarski proved that the full TRCF is decidable [7]. Tarski's quantifier elimination algorithm for TRCF was not properly published until 1951 [26]. And, even after the publication of Tarski's method, over 20 years went by before there was significant further work on the problem or any real applications of such decision procedures. One reason for this lag is that Tarski's algorithm is extremely computational complex. In general, its complexity is not bounded by any tower of exponentials.[5] In the early 70's, George Collins [5] came-up with a much more efficient decision procedure for TRCF, based on methods of Cylindrical Algebraic Decomposition (CAD). The complexity of Collins's CAD algorithm is (merely!) double-exponential in the number of real variables contained in the set of TRCF sentences. It has since been shown that double-exponential complexity in the number of real variables is a *lower-bound* for *any* general decision procedure for TRCF [6].[6] In the 1990's, various practical improvements to various parts of the CAD algorithm were developed by Hong [13, 15], McCallum [20], Brown [2, 3], and others. Ultimately, these efforts have led to the computer program QEPCAD. An up-to-date C implementation of QEPCAD is now freely available for download [16]. In 2003, *Mathematica* [27] was released with a suite of QEPCAD-like functions built-in to its main Kernel. Adam Strzebonski [24, 25] was (and still is) responsible for these *Mathematica* functions. Specifically, *Mathematica* has a function called FindInstance, which will take as input a finite set S' of statements of high-school algebra, and it will return an assignment of real numbers to all the real variables in S' on which all the members of S' are true (if there is one). If the set S' is unsatisfiable, it will return the empty set { }. This is precisely the function that PrSAT uses to decide the satisfiability of its sets $S' \cup C_n$ of high-school algebra statements (from step 3 of our high-level description of PrSAT, above). As we will see in the next section, the *Mathematica* implementation of PrSAT is quite powerful, as it is able to solve many non-trivial problems in probability calculus. But, before we get to these applications, I want to say one more thing about decision procedures for TRCF and its fragments.

Since high-school algebra only involves existential quantification over sets of simple algebraic claims, a natural question to ask is whether there are algorithms more efficient than QEPCAD for just the *pure existential fragment* of TRCF. *Theoretically*, the answer to this question is "Yes". But, *practically*, the answer is less clear. That is, theoretically, it can be shown that the complexity of the decision problem for the existential fragment of TRCF is "only" *single*-exponential, as opposed to double-exponential for the full TRCF [1]. However, when one looks at

[5] See [7] for a detailed accounting of the fascinating and complicated history of Tarskian decision procedures for TRCF. And, see [4] for all technical details about various decision procedures for TRCF and their computational complexities. The details of these methods are beyond the scope of this paper, which is primarily concerned with communicating the basic ideas behind PrSAT and its applications.

[6] Since the number of real variables in our problems grows exponentially in n (2^n), the complexity of PrSAT, using any decision procedure for the full TRCF, will be (at least) *triple* exponential in n! This means that (naïvely) solving problems of size $n > 4$ is not (generally) practical. Some heuristics for speeding-up PrSAT's model-finding are illustrated in http://fitelson.org/pm.nb, which is this paper's companion *Mathematica* notebook. There, all the problems in the final section of this paper are quickly solved using PrSAT, with the help of a simple heuristic (which serves to reduce the effective number of real variables in the problem). That heuristic technique can also be used to quickly find models for problems involving 4 or even 5 atomic sentence letters. It is crucial that today's computers are *much* more powerful than even those of the late 90's, when QEPCAD began to be applied to non-trivial problems. For instance, all of the "practically intractable" application problems reported in Brown's 1998 CAD applications paper [2] can be solved (with *Mathematica*) in under 15 minutes on today's PCs (even on our laptops!). This is one of the reasons that PrSAT is (nowadays) able to solve so many non-trivial problems. In the latest version of PrSAT, there is also a random search feature, which greatly speeds-up model finding in many (satisfiable) examples. See section 5 for further discussion.

existing implementations of these algorithms, one finds that *in practice* they tend to be *much slower* than QEPCAD, except on very large problems that are practically intractable anyway [14]. However, recently, there has been some progress on improving the implementations of these pure-exsitential decision procedures.[7] This is an interesting area for future research and development.

4. Some Applications of PrSAT

This section contains several non-trivial problems from probability calculus (some of which are also of philosophical interest) that can be solved rather easily with the *Mathematica* implementation of PrSAT.[8]

4.1. A Well-Known Problem in Probability Calculus

We begin with a well-known problem in probability calculus, which is discussed in most contemporary introductory texts on probability [8, p. 116]. Consider a language $\mathcal{L}_3$ with three atomic sentences $\{A, B, C\}$. Question: if A, B, and C are *pairwise* probabilistically independent, does it follow that they are *mutually* probabilistically independent? That is, do the statements (1)–(3) in probability calculus entail statement (4)?

1. $\Pr(A \,\&\, B) = \Pr(A) \cdot \Pr(B)$
2. $\Pr(A \,\&\, C) = \Pr(A) \cdot \Pr(C)$
3. $\Pr(B \,\&\, C) = \Pr(B) \cdot \Pr(C)$
4. $\Pr(A \,\&\, B \,\&\, C) = \Pr(A) \cdot \Pr(B) \cdot \Pr(C)$

An equivalent question is whether the set S consisting of (1), (2), (3), and the denial of (4) is *unsatisfiable*. To illustrate how our translation procedure works on a real example, we can use the stochastic truth-table for $\mathfrak{M}_3$ above to translate (1), (2), (3), and the denial of (4), into the following set S' of high-school algebra statements in terms of $\mathfrak{s}_1$–$\mathfrak{s}_8$:

1′. $\mathfrak{s}_1 + \mathfrak{s}_2 = (\mathfrak{s}_1 + \mathfrak{s}_2 + \mathfrak{s}_3 + \mathfrak{s}_4) \cdot (\mathfrak{s}_1 + \mathfrak{s}_2 + \mathfrak{s}_5 + \mathfrak{s}_6)$

2′. $\mathfrak{s}_1 + \mathfrak{s}_3 = (\mathfrak{s}_1 + \mathfrak{s}_2 + \mathfrak{s}_3 + \mathfrak{s}_4) \cdot (\mathfrak{s}_1 + \mathfrak{s}_3 + \mathfrak{s}_5 + \mathfrak{s}_7)$

3′. $\mathfrak{s}_1 + \mathfrak{s}_5 = (\mathfrak{s}_1 + \mathfrak{s}_2 + \mathfrak{s}_5 + \mathfrak{s}_6) \cdot (\mathfrak{s}_1 + \mathfrak{s}_3 + \mathfrak{s}_5 + \mathfrak{s}_7)$

4′. $\mathfrak{s}_1 \neq (\mathfrak{s}_1 + \mathfrak{s}_2 + \mathfrak{s}_3 + \mathfrak{s}_4) \cdot (\mathfrak{s}_1 + \mathfrak{s}_2 + \mathfrak{s}_5 + \mathfrak{s}_6) \cdot (\mathfrak{s}_1 + \mathfrak{s}_3 + \mathfrak{s}_5 + \mathfrak{s}_7)$

Following our procedure, we need to determine whether the set $S' \cup C_3$ is satisfiable, where C_3 is the following set of nine algebraic statements:

$$\{\mathfrak{s}_1 \geq 0, \mathfrak{s}_2 \geq 0, \mathfrak{s}_3 \geq 0, \mathfrak{s}_4 \geq 0, \mathfrak{s}_5 \geq 0, \mathfrak{s}_6 \geq 0, \mathfrak{s}_7 \geq 0, \mathfrak{s}_8 \geq 0,$$
$$\mathfrak{s}_1 + \mathfrak{s}_2 + \mathfrak{s}_3 + \mathfrak{s}_4 + \mathfrak{s}_5 + \mathfrak{s}_6 + \mathfrak{s}_7 + \mathfrak{s}_8 = 1\}$$

PrSAT can find *many* assignments to the $\mathfrak{s}_i$ on which all members of $S' \cup C_3$ are true. So, the set S is satisfiable. Hence, the answer to the question is “No” — pairwise probabilistic independence of three statements does *not* entail their *mutual* independence. Before reporting a nice model found by PrSAT, it is worth noting that all of the answers to this problem that I have seen in the textbooks — see, *e.g.*, Feller [8, p. 116] — involve models which assign probability zero to at least one state description of $\mathcal{L}_3$, owing to some kind of logical dependencies between atomic sentences. It is interesting to note that that PrSAT can easily (and automatically) find models that are *regular* — *i.e.*, that assign nonzero probability to all state descriptions of $\mathcal{L}_3$. Indeed, PrSAT can find regular models such that the $\mathfrak{s}_i$’s have equal denominators (*i.e.*, regular “urn models”). Here is a nice PrSAT model on which all members of $S' \cup C_3$ are true (think in terms of sampling from an urn containing 2000 balls, with properties A, B, C, distributed according to the $\mathfrak{s}_i$):

A	B	C	State Descriptions (s_i)	$\Pr(s_i) = \mathfrak{s}_i$
T	T	T	$A \,\&\, B \,\&\, C = s_1$	$\Pr(s_1) = \mathfrak{s}_1 = \frac{1}{2000}$
T	T	F	$A \,\&\, B \,\&\, {\sim}C = s_2$	$\Pr(s_2) = \mathfrak{s}_2 = \frac{19}{2000}$
T	F	T	$A \,\&\, {\sim}B \,\&\, C = s_3$	$\Pr(s_3) = \mathfrak{s}_3 = \frac{19}{2000}$
T	F	F	$A \,\&\, {\sim}B \,\&\, {\sim}C = s_4$	$\Pr(s_4) = \mathfrak{s}_4 = \frac{161}{2000}$
F	T	T	${\sim}A \,\&\, B \,\&\, C = s_5$	$\Pr(s_5) = \mathfrak{s}_5 = \frac{19}{2000}$
F	T	F	${\sim}A \,\&\, B \,\&\, {\sim}C = s_6$	$\Pr(s_6) = \mathfrak{s}_6 = \frac{161}{2000}$
F	F	T	${\sim}A \,\&\, {\sim}B \,\&\, C = s_7$	$\Pr(s_7) = \mathfrak{s}_7 = \frac{161}{2000}$
F	F	F	${\sim}A \,\&\, {\sim}B \,\&\, {\sim}C = s_8$	$\Pr(s_8) = \mathfrak{s}_8 = \frac{1459}{2000}$

On this model, we have the following:

[7] Galen Huntington has been working on more practically efficient decision procedures for the pure existential fragment of TRCF. Indeed, he has made significant progress on this front. He now has an algorithm that solves all of Hong’s challenge problems [14] in a matter of minutes (as opposed to *eons*, which is what previous algorithms would have taken). Galen’s work will soon appear in his thesis [17].

[8] All of the problems discussed in this section have been solved with the *Mathematica* implementation of PrSAT, which can be freely downloaded from the PrSAT website, at `http://fitelson.org/PrSAT/`. The PrSAT website also contains documentation and further examples. A *Mathematica* notebook containing all of the examples discussed here can be downloaded from `http://fitelson.org/pm.nb`. That notebook also describes a heuristic technique for speeding-up model searches, as well as Blum’s random search add-on (which often finds models very quickly), which has recently been added to PrSAT. See section 5 for discussion.

1. $\Pr(A \,\&\, B) = \frac{1}{100} = \frac{1}{10} \cdot \frac{1}{10} = \Pr(A) \cdot \Pr(B)$

2. $\Pr(A \,\&\, C) = \frac{1}{100} = \frac{1}{10} \cdot \frac{1}{10} = \Pr(A) \cdot \Pr(C)$

3. $\Pr(B \,\&\, C) = \frac{1}{100} = \frac{1}{10} \cdot \frac{1}{10} = \Pr(B) \cdot \Pr(C)$

4. $\Pr(A \,\&\, B \,\&\, C) = \frac{1}{2000} \neq \frac{1}{10} \cdot \frac{1}{10} \cdot \frac{1}{10} = \Pr(A) \cdot \Pr(B) \cdot \Pr(C)$

Next, we will discuss some examples motivated by philosophical (specifically, philosophy of science) applications of probability calculus.

4.2. Three Problems from Bayesian Confirmation Theory

According to Bayesian confirmation theory, an evidential statement E is said to *confirm* a hypothesis statement H, relative to a probability model $\mathfrak{M} = \langle \mathcal{L}, \Pr \rangle$, just in case E and H are positively correlated under the probability function Pr, *i.e.*, just in case $\Pr(H \mid E) > \Pr(H)$. Moreover, there are many Bayesian measures $\mathfrak{c}(H, E)$ of the *degree* to which E confirms H [9]. Here are a few measures that have been used:

$$\begin{aligned}
\mathsf{d}(H,E) &\overset{\text{def}}{=} \Pr(H \mid E) - \Pr(H) \\
\mathsf{l}(H,E) &\overset{\text{def}}{=} \frac{\Pr(E \mid H) - \Pr(E \mid {\sim}H)}{\Pr(E \mid H) + \Pr(E \mid {\sim}H)} \\
\mathsf{s}(H,E) &\overset{\text{def}}{=} \Pr(H \mid E) - \Pr(H \mid {\sim}E)
\end{aligned}$$

All of these measures respect the *qualitative* Bayesian definition, since they are all positive when E confirms H, negative when E disconfirms H, and zero when E and H are independent. Moreover, all three of these measures are defined on a $[-1, 1]$ scale. But, these measures disagree radically on *comparative* claims [9] of the form $\mathfrak{c}(H, E) \geq \mathfrak{c}(H', E')$. The following condition is assumed by most commentators to be a *desideratum* for Bayesian measures of degree of confirmation [18]:

($\star$) If $\Pr(H \mid E_1) \geq \Pr(H \mid E_2)$, then $\mathfrak{c}(H, E_1) \geq \mathfrak{c}(H, E_2)$.

Indeed, it was simply assumed by many that ($\star$) *must* be satisfied by *any* Bayesian measure. An early prototype of PrSAT was able to show that, while d and l satisfy ($\star$), s *violates* it [10]! This result came as a surprise to many Bayesian confirmation theorists. If you run PrSAT on the d-instance or the l-instance of ($\star$), it will tell you (correctly) that there are no models on which these instances of ($\star$) are false. However, if you run PrSAT on the s-instance of ($\star$) it will find a countermodel. Here is one such PrSAT model, which is regular and has equal denominators (think of an urn with 5120 balls and three properties E_1, E_2, and H):

E_1	E_2	H	State Descriptions (s_i)	$\Pr(s_i) = \mathfrak{s}_i$
T	T	T	$E_1 \,\&\, E_2 \,\&\, H = s_1$	$\Pr(s_1) = \mathfrak{s}_1 = \frac{669}{5120}$
T	T	F	$E_1 \,\&\, E_2 \,\&\, {\sim}H = s_2$	$\Pr(s_2) = \mathfrak{s}_2 = \frac{291}{5120}$
T	F	T	$E_1 \,\&\, {\sim}E_2 \,\&\, H = s_3$	$\Pr(s_3) = \mathfrak{s}_3 = \frac{127}{5120}$
T	F	F	$E_1 \,\&\, {\sim}E_2 \,\&\, {\sim}H = s_4$	$\Pr(s_4) = \mathfrak{s}_4 = \frac{193}{5120}$
F	T	T	${\sim}E_1 \,\&\, E_2 \,\&\, H = s_5$	$\Pr(s_5) = \mathfrak{s}_5 = \frac{1539}{5120}$
F	T	F	${\sim}E_1 \,\&\, E_2 \,\&\, {\sim}H = s_6$	$\Pr(s_6) = \mathfrak{s}_6 = \frac{1341}{5120}$
F	F	T	${\sim}E_1 \,\&\, {\sim}E_2 \,\&\, H = s_7$	$\Pr(s_7) = \mathfrak{s}_7 = \frac{225}{5120}$
F	F	F	${\sim}E_1 \,\&\, {\sim}E_2 \,\&\, {\sim}H = s_8$	$\Pr(s_8) = \mathfrak{s}_8 = \frac{735}{5120}$

Strictly speaking, Bayesian confirmation is a four-place relation, between E, H, a corpus of background knowledge K, and a probability model $\mathfrak{M} = \langle \mathcal{L}, \Pr \rangle$. So, our three measures should really be defined as:

$$\begin{aligned}
\mathsf{d}(H,E \mid K) &\overset{\text{def}}{=} \Pr(H \mid E \,\&\, K) - \Pr(H \mid K) \\
\mathsf{l}(H,E \mid K) &\overset{\text{def}}{=} \frac{\Pr(E \mid H \,\&\, K) - \Pr(E \mid {\sim}H \,\&\, K)}{\Pr(E \mid H \,\&\, K) + \Pr(E \mid {\sim}H \,\&\, K)} \\
\mathsf{s}(H,E \mid K) &\overset{\text{def}}{=} \Pr(H \mid E \,\&\, K) - \Pr(H \mid {\sim}E \,\&\, K)
\end{aligned}$$

For many results — like the ones concerning ($\star$) above — the background corpus K plays no role, and so it may be suppressed (for simplicity). But, in many cases, the background corpus plays a crucial role. One set of important results in confirmation theory depends essentially on the background corpus. These results have to do with the concept of *independent evidence* defined in [11] in the following way.

- E_1 and E_2 are said to be *confirmationally independent regarding* H, according to a measure $\mathfrak{c}$ just in case both $\mathfrak{c}(H, E_1 \mid E_2) = \mathfrak{c}(H, E_1)$ and $\mathfrak{c}(H, E_2 \mid E_1) = \mathfrak{c}(H, E_2)$. Here, $\mathfrak{c}(H, E)$ can be thought of unconditionally, as above, or it can be thought of as $\mathfrak{c}(H, E \mid \top)$.

Intuitively, if E_1 and E_2 are confirmationally independent regarding H, then they do not "interact" in the support they provide for H. Following Peirce, we have argued [11] that in such cases (provided that each of E_1 and E_2 individually confirms H), the degree to which the conjunction $E_1 \,\&\, E_2$ confirms H should be greater than the degree to which either conjunct *alone* confirms H. Specifically, we should have the following:

(†) If each of E_1 and E_2 individually confirms H, and if $\mathfrak{c}(H, E_1 \mid E_2) = \mathfrak{c}(H, E_1)$ and $\mathfrak{c}(H, E_2 \mid E_1) = \mathfrak{c}(H, E_2)$, then $\mathfrak{c}(H, E_1 \,\&\, E_2) > \mathfrak{c}(H, E_2)$.

It seems to me that (†) should be a *desideratum* for any measure of degree of confirmation $\mathfrak{c}(H, E|K)$. Interestingly (and, again, surprisingly, to my mind), an early prototype of PrSAT was able to establish that, while measures d and l satisfy (†), s *violates* it. If you run PrSAT on the d-instance or the l-instance of (†), it will tell you (correctly) that there are no models on which these instances of (†) are false. However, if you run PrSAT on the s-instance of (†) it will find a countermodel. Indeed, PrSAT is able to find a single model, which shows *both* that the s-instance of (⋆) is false *and* that the s-instance of (†) is false, *simultaneously*. We have already seen such a model: the model reported above for (⋆) *also* serves as a countermodel to the s-instance of (†). To see this, note that the following facts obtain on this model:

- $\Pr(H \mid E_1) = \frac{199}{320} > \frac{23}{40} = \Pr(H \mid E_2) > \Pr(H) = \frac{1}{2}$

- $$\begin{aligned}\mathsf{s}(H, E_1) = \Pr(H \mid E_1) - \Pr(H \mid {\sim}E_1) &= \frac{199}{320} - \frac{147}{320} = \frac{13}{80}\\ < \mathsf{s}(H, E_2) = \Pr(H \mid E_2) - \Pr(H \mid {\sim}E_2) &= \frac{23}{40} - \frac{11}{40} = \frac{3}{10}\end{aligned}$$

- $$\begin{aligned}\mathsf{s}(H, E_1 \mid E_2) = \Pr(H \mid E_1 \,\&\, E_2) - \Pr(H \mid {\sim}E_1 \,\&\, E_2) &= \frac{223}{320} - \frac{171}{320} = \frac{13}{80}\\ = \mathsf{s}(H, E_1) = \Pr(H \mid E_1) - \Pr(H \mid {\sim}E_1) &= \frac{199}{320} - \frac{147}{320} = \frac{13}{80}\end{aligned}$$

- $$\begin{aligned}\mathsf{s}(H, E_2 \mid E_1) = \Pr(H \mid E_2 \,\&\, E_1) - \Pr(H \mid {\sim}E_2 \,\&\, E_1) &= \frac{223}{320} - \frac{127}{320} = \frac{3}{10}\\ = \mathsf{s}(H, E_2) = \Pr(H \mid E_2) - \Pr(H \mid {\sim}E_2) &= \frac{23}{40} - \frac{11}{40} = \frac{3}{10}\end{aligned}$$

- $$\begin{aligned}\mathsf{s}(H, E_1 \,\&\, E_2) = \Pr(H \mid E_1 \,\&\, E_2) - \Pr(H \mid {\sim}(E_1 \,\&\, E_2)) &= \frac{223}{320} - \frac{1891}{4160} = \frac{63}{260}\\ < \mathsf{s}(H, E_2) = \Pr(H \mid E_2) - \Pr(H \mid {\sim}E_2) &= \frac{23}{40} - \frac{11}{40} = \frac{3}{10}\end{aligned}$$

Our third and final class of problems from Bayesian confirmation theory involves Hempel's infamous raven paradox. This is also a case in which non-trival new theorems and non-trivial new models were found by PrSAT. I won't get into the philosophical background behind the raven paradox here. Rather, I'll just briefly (and at a high-level) explain the purely formal part of contemporary Bayesian approaches to the paradox, and how PrSAT allowed us to discover a new-and-improved approach. See [12] for all of the philosophical and technical details. The formal part of standard Bayesian resolutions of the raven paradox rests on the following four statements of probability calculus.

1. $\Pr(B \mid R \,\&\, H) = 1$.

2. $\Pr({\sim}B) > \Pr(R)$.

3. $\Pr(B \mid H) = \Pr(B)$.

4. $\Pr(R \mid H) = \Pr(R)$.

From these assumptions, it is possible to prove the following:

5. $\Pr(H \mid R \,\&\, B) > \Pr(H \mid {\sim}R \,\&\, {\sim}B)$.

Indeed, the main formal component of Bayesian resolutions of the raven paradox involves describing sets of sufficient conditions for (5). The usual set of sufficient conditions is (1)–(4). But, these assumptions are controversial, because they have undesirable consequences, such as:

6. $\Pr(H \mid {\sim}R \,\&\, {\sim}B) > \Pr(H)$.

7. $\Pr(H \mid {\sim}R \,\&\, B) < \Pr(H)$.

So, if we could find sufficient conditions for (5) that were weaker than (1)–(4) — so that they do not entail (6) and (7) — that would be an improvement on the standard Bayesian approaches. Note: conditions (1) and (2) are non-negotiable, as they are either logically implied by the set-up of the raven paradox or they are otherwise uncontroversial. As such, the challenge is to find conditions C such that: (a) the conditions (1), (2), and C jointly entail (5), (b) C is strictly weaker than the conjunction (3) & (4), and (c) the conditions (1), (2), and C do not jointly entail either (6) or (7). James Hawthorne and I [12] have recently reported that the following condition C will serve as a replacement for (3) and (4):

(C) $\Pr(H \mid R) \geq \Pr(H \mid {\sim}B)$.

We discovered this condition by using PrSAT to examine various conditions that are strictly weaker than the conjunction (3) & (4). It is easy to see that (C) satisfies (b), since (3) & (4) entails $\Pr(H \mid R) = \Pr(H \mid {\sim}B) = \Pr(H)$, which entails (C), but (C) does not entail $\Pr(H \mid R) = \Pr(H \mid {\sim}B)$ or $\Pr(H \mid R) = \Pr(H)$ or $\Pr(H \mid {\sim}B) = \Pr(H)$. The hard part of the problem is establishing (a). PrSAT told us that (a) was true, but it took awhile for us to find an axiomatic proof (PrSAT does not output proof objects). James Hawthorne eventually discovered an axiomatic proof of (a), which is reported in [12]. As for (c), PrSAT gives us concrete models which show that (1), (2), and (C) do not entail either (6) or (7). In fact, here is a single PrSAT model that shows *both* things *simultaneously*:

B	H	R	State Descriptions (s_i)	$\Pr(s_i) = \mathfrak{s}_i$
T	T	T	$B \,\&\, H \,\&\, R = s_1$	$\Pr(s_1) = \mathfrak{s}_1 = \frac{125}{2650}$
T	T	F	$B \,\&\, H \,\&\, {\sim}R = s_2$	$\Pr(s_2) = \mathfrak{s}_2 = \frac{30}{2650}$
T	F	T	$B \,\&\, {\sim}H \,\&\, R = s_3$	$\Pr(s_3) = \mathfrak{s}_3 = \frac{80}{2650}$
T	F	F	$B \,\&\, {\sim}H \,\&\, {\sim}R = s_4$	$\Pr(s_4) = \mathfrak{s}_4 = \frac{21}{2650}$
F	T	T	${\sim}B \,\&\, H \,\&\, R = s_5$	$\Pr(s_5) = \mathfrak{s}_5 = 0$
F	T	F	${\sim}B \,\&\, H \,\&\, {\sim}R = s_6$	$\Pr(s_6) = \mathfrak{s}_6 = \frac{105}{2650}$
F	F	T	${\sim}B \,\&\, {\sim}H \,\&\, R = s_7$	$\Pr(s_7) = \mathfrak{s}_7 = \frac{51}{2650}$
F	F	F	${\sim}B \,\&\, {\sim}H \,\&\, {\sim}R = s_8$	$\Pr(s_8) = \mathfrak{s}_8 = \frac{1128}{2650}$

To see this, note that, on the above model, we have:

(1) $\Pr(B \mid R \,\&\, H) = 1$

(2) $\Pr({\sim}B) = \frac{9}{10} > \frac{1}{10} = \Pr(R)$

(C) $\Pr(H \mid R) = \frac{125}{256} = \Pr(H \mid {\sim}B)$

∼(6) $\Pr(H \mid {\sim}R \,\&\, {\sim}B) = \frac{375}{751} < \frac{1}{2} = \Pr(H)$

∼(7) $\Pr(H \mid {\sim}R \,\&\, B) = \frac{10}{17} > \frac{1}{2} = \Pr(H)$

4.3. Examples from Howard Sobel's "Lotteries and Miracles"

In his recent paper "Lotteries and Miracles", Howard Sobel [23] reports many interesting new theorems of probability calculus, which he puts to good use for the purpose of reconstructing (and critiquing) various arguments concerning testimonial evidence regarding the possibility of miracles. One important class of results (in a section devoted to a particular Humean claim about such testimony) involves the following five claims of probability calculus (using a slightly different notation):

1. $\Pr(T) < 1/2$.
2. $\Pr(T \mid W) > 1/2$.
3. $\Pr(W \mid T) > 1/2$.
4. $\Pr(T \mid {\sim}W) < \Pr(W)$.
5. $\Pr(T \mid W) - \Pr(T \mid {\sim}W) > \Pr({\sim}W) - \Pr(W)$.

Sobel's analysis led him to the following three questions:

- Do (1)–(3) entail (4)?

- Do (1)–(3) entail (5)?
- Do (1)–(3) entail the *disjunction* (4) ∨ (5)?

Sobel (email correspondence, May 2006) asked me if I could answer any of these questions. Of course, I immediately plugged them into PrSAT, and I found answers to all of these questions very quickly. The answers are "No", "No", and "Yes", respectively. That is, PrSAT found (*i*) models in which (1)–(3) are all true but (4) is false, (*ii*) models in which (1)–(3) are all true but (5) is false, and (*iii*) *no* models in which (1)–(3) are all true but the disjunction (4) ∨ (5) is false. Sobel reports the PrSAT models for (*i*) and (*ii*) in his paper. Since PrSAT does not produce *proofs* of theorems, the task remained (as in our raven paradox example above) to find an axiomatic proof of the disjunction (4) ∨ (5) from (1)–(3). And, just as in the case of our new ravens theorem, James Hawthorne (email correspondence, May 2006) was able to find an axiomatic proof.

These examples should be sufficient to illustrate to power and usefulness of PrSAT in real mathematical and philosophical applications of probability calculus. I encourage readers to try PrSAT for themselves. In the final section, I will discuss three kinds of extensions to (and/or generalizations of) PrSAT that suggest directions for future research.

5. Directions for Future Research

There are three main extensions/improvements to PrSAT that are being investigated. First, there is the extension (mentioned above) to the broader class of statements which allow for (non-trivial) *quantification* over both sentence letters and real variables of the language of probability calculus. Such an extension would allow us to work with statements which are now beyond the scope of PrSAT.

The second alteration to PrSAT involves trying out different (asymptotically single-exponential) decision procedures for the existential fragment of TRCF (on the simple class of statements considered in this paper). As I mentioned, Hong's investigation [14] of these alternatives to QEPCAD in the early 90's indicated that no practical gain in performance would be had by making such a switch (except on problems of prohibitive size). Of course, Hong did not investigate all possible decision procedures for existential TRCF. And, it now appears that there is good reason for optimism on this front.[9]

Finally, a more radical departure from the current approach would be to consider alternative *incomplete* or *nondeterministic* model finding

[9] As I mentioned above, Galen Huntington has succeeded in implementing a much more efficient algorithm for this purpose, which will be reported in his thesis [17].

(or SAT) techniques. For instance, various *local search* SAT algorithms [22] have proved to be very powerful for other sorts of SAT problems. Ben Blum has implemented a simple random search add-on for `PrSAT`, which has linear complexity in the number of state descriptions.[10]

References

1. S. Basu, R. Pollack and M.F. Roy, *On the Combinatorial and Algebraic Complexity of Quantifier Elimination*, Journal of the ACM, **43** (1996), 1002–1045.
2. C. Brown, *Simple CAD Construction and its Applications*, Journal of Symbolic Computation **31** (2001), 521–547.
3. ———, *Improved projection for cylindrical algebraic decomposition*, Journal of Symbolic Computation **32** (2001), 447-465.
4. B. Caviness and J. Johnson (eds.), *Quantifier elimination and cylindrical algebraic decomposition*, Springer-Verlag, 1998.
5. G. Collins, *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, 1975, reprinted in [4], 85–121.
6. J.H. Davenport and J. Heintz, *Real quantifier elimination is doubly exponential*, Journal of Symbolic Computation **5** (1988), 29–35.
7. A. Burdman Feferman and S. Feferman, *Alfred Tarski: Life and Logic*, Cambridge University Press, 2004.
8. W. Feller, *An introduction to probability theory and its applications*, Volume I, Third Edition, John Wiley & Sons Inc., 1968.
9. B. Fitelson, *The plurality of Bayesian measures of confirmation and the problem of measure sensitivity*, Philosophy of Science **66** (1999), S362–S378, `http://fitelson.org/psa.pdf`.
10. ———, *Studies in Bayesian confirmation theory*, Ph.D. thesis, University of Wisconsin–Madison (Philosophy), 2001, `http://fitelson.org/thesis.pdf`.
11. ———, *A Bayesian account of independent evidence with applications*, Philosophy of Science, 2001, `http://fitelson.org/psa2.pdf`.
12. Fitelson, B., and Hawthorne, J., *How Bayesian Confirmation Theory Handles the Paradox of the Ravens*, in *Probability in Science*, E. Eells and J. Fetzer (*eds.*), Open Court, to appear, 2007, `http://fitelson.org/ravens.pdf`.
13. H. Hong, *An improvement of the projection operator in cylindrical algebraic decomposition*, 1990, reprinted in [4], 166–173.
14. ———, *Comparison of Several Decision Algorithms for the Existential Theory of the Reals*, technical report 91–41, Johannes Kepler University, Linz, Austria, 1991, `http://citeseer.ist.psu.edu/hong91comparison.html`.
15. ———, *Simple solution formula construction in cylindrical algebraic decomposition based quantifier elimination*, in Proceedings of the International Symposium on Symbolic and Algebraic Computation, 1992, 177–188.

[10] While attending my probability and induction course at Berkeley in spring 2005, Ben Blum (then a first-year CS student) implemented a prototype local search add-on to our *Mathematica* implementation of `PrSAT` (as his project for the course). It is now included in the current version of `PrSAT`, which (by default) tries a few random search runs before giving up and sending the problem to the decision procedure. See the companion *Mathematica* notebook that goes along with this paper (at the following url: `http://fitelson.org/pm.nb`) for illustrations.

16. ———, *`QEPCAD` – Quantifier Elimination by Partial Cylindrical Algebraic Decomposition*, computer program website, 2006, `http://www.cs.usna.edu/~qepcad/`.
17. G. Huntington, *Decision Procedures for the Pure Existential Fragment of the Theory of Real-Closed Fields*, PhD. dissertation, Group in Logic and the Methodology of Science, UC–Berkeley, 2008 (expected).
18. J. Joyce, *Bayes's theorem*, The Stanford Encyclopedia of Philosophy, 2003, `http://plato.stanford.edu/entries/bayes-theorem/`.
19. A. Kolmogorov, *Foundations of probability*, 2nd ed., AMS Chelsea, 1956.
20. S. McCallum, An improved projection operator for cylindrical algebraic decomposition, 1998, in [4], 242–268.
21. J. Paris, *The Uncertain Reasoner's Companion: A Mathematical Perspective*, Cambridge University Press, 1995.
22. D. Schuurmans and F. Southey, *Local search characteristics of incomplete SAT procedures*. Artificial Intelligence **132** (2001), 121-150. `http://dx.doi.org/10.1016/S0004-3702(01)00151-5`.
23. J.H. Sobel, *Lotteries and Miracles*, manuscript, May 2006, `http://www.scar.utoronto.ca/~sobel/OnL_T/BigLotteries.wpd.pdf`.
24. A. Strzebonski, *Solving systems of strict polynomial inequalities*, Journal of Symbolic Computation **29** (2000), 471–480.
25. ———, *Solving algebraic inequalities with version 4*, The Mathematica Journal **7** (2000).
26. A. Tarski, *A decision method for elementary algebra and geometry*, University of California Press, 1951.
27. S. Wolfram, *The Mathematica Book*, Version 5, Wolfram Research, 2003.