Shortest Axiomatizations of Implicational S4 and S5

Zachary Ernst
Philosophy Department, University of Wisconsin–Madison, and
Mathematics & Computer Science Division, Argonne National Laboratory

Branden Fitelson
Philosophy Department, University of Wisconsin–Madison,
Mathematics & Computer Science Division, Argonne National Laboratory

Kenneth Harris
Mathematics & Computer Science Division, Argonne National Laboratory

Larry Wos
Mathematics & Computer Science Division, Argonne National Laboratory

August 6, 2001

Abstract. Shortest possible axiomatizations for the implicational fragments of the modal logics S4 and S5 are reported. Among these axiomatizations is included a shortest single axiom for implicational S4 (which is unprecedented in the literature), and several new shortest single axioms for implicational S5. A variety of automated reasoning techniques were essential to our discoveries.

Keywords: axiomatization, modal logic, implication, single axiom

1. Some Background and Conventions

The implicational fragments of the modal logics S4 and S5 have been studied quite extensively over the years (see, for instance, [8], [7], [1], [5], and [13], just to name a few). Following tradition, we will use the labels "C4" and "C5" to denote the implicational fragments of S4 and S5, respectively. Prior [16, Appendix I] reports a variety of Hilbert-style axiomatizations for C4 and C5. All such axiomatizations presuppose detachment as their sole rule of inference (as will ours). We will also follow the convention of writing implicational formulae in polish notation (*i.e.*, instead of the infix '$p \to q$', we will use the Polish 'Cpq'). When we report our deductions, we will use Meredith's D-notation (as explained in Prior's [16, Appendix II]). That is, the notation '$D.a.b$' (appearing to the left of each line in our deductions) is used to denote the most general possible result of detachment (*i.e.*, the *condensed* detachment [6]) with a, or some substitution in a, for the major premise $C\alpha\beta$, and with b, or some substitution in b, for the minor premise α. All proofs reported below were discovered with the assistance of the automated reasoning program OTTER [12]. The extensive role of automated reasoning in the present research is discussed in § 4.

2. Axiomatic C4

2.1. A Brief History of Axiomatic C4

The axiomatization of C4 has an interesting history. As far as we can tell, the first time an axiomatization for C4 appeared explicitly in print was in Anderson & Belnap's 1962 paper [1]. Anderson & Belnap report the following 3-axiom basis for C4, which we will adopt as our "reference" C4 axiomatization (the detachment rule, as always, is presupposed to be the sole rule of inference of the systems):

$$\begin{array}{c} Cpp \\ CCpqCrCpq \\ CCpCqrCCpqCpr \end{array} \tag{1}$$

Anderson & Belnap credit Kripke's 1959 discussion [7] with providing the original insight on how to axiomatize C4. However, according to Curry [3] and Hacking [5], similar work was concurrently being done independently across the Atlantic by Hacking & Smiley. The work of Hacking & Smiley was not published until 1963 [5], but their work on C4 was available in mimeograph form several years before this [3].

Other 3-axiom bases were later discovered for C4 (see [16, Appendix I]). But, as far as we know, no 2-axiom bases for C4 were ever reported in the literature. Moreover, no single axiom for C4 has been discovered (this is stated as an open problem in [2, page 83]). Indeed, the only axiomatizations of C4 that we have seen are the two 3-axiom bases reported in [16, Appendix I]. Each of these bases contains 3 axioms, 25 symbols (total), and 11 occurrences of the implication connective C.[1]

2.2. Shortest Axiomatizations of C4

Using a variety of automated reasoning techniques (see § 4 below for more on these techniques), we have discovered many new 2-axiom bases for C4. The most elegant of these include the following 2-basis, which contains only 20 symbols, and 9 occurrences of C:

$$\begin{array}{c} CpCqq \\ CCpCqrCCpqCsCpr \end{array} \tag{2}$$

[1] The other C4 3-basis reported in Prior's [16, Appendix I] is: $\{CpCqq, CCpqCCqrCpr, CCpCpqCpq\}$. Ulrich [18] shows that C4 is also the implicational fragment of each modal logic between S4 and S4.3 (so, our bases are also new, and shortest bases for the implicational fragments of these extensions of S4 as well).

So far, we have found six such 2-bases, and we know that there are at most eight such 2-bases (we suspect there are *exactly* six).[2]

Moreover, we have been able to show that these are the *shortest possible* bases for C4. That is, no other basis for C4 (with any number of axioms) contains fewer symbols (or occurrences of C) than the above 2-basis.[3] Our automated reasoning techniques also yielded the following new 21-symbol (10-C) single axiom for C4:

$$CCpCCqCrrCpsCCstCuCpt \tag{3}$$

To our knowledge, no single axiom for C4 has previously been reported. Indeed, this has been a long-standing open problem in the axiomatics of modal logic [2, page 83]. We have ruled-out all shorter single axiom candidates (see § 4, below, for more on the techniques used to eliminate and discover single-axiom candidates). Therefore, (3) is a *shortest possible* single axiom for C4. In fact, (3) is *the* shortest C4 single axiom (all other 21-symbol candidates have been eliminated).

With a circle of three deductions, we will now establish that each of (2) and (3) is necessary and sufficient for (1). This will suffice to show that both (2) and (3) are *bases* for C4. First, we prove (1) $\Rightarrow$ (3):

	1.	Cpp
	2.	$CCpqCrCpq$
	3.	$CCpCqrCCpqCpr$
$D.3.3$	4.	$CCCpCqrCpqCCpCqrCpr$
$D.2.3$	5.	$CpCCqCrsCCqrCqs$
$D.3.5$	6.	$CCpCqCrsCpCCqrCqs$
$D.6.2$	7.	$CCpqCCrpCrq$
$D.3.7$	8.	$CCCpqCrpCCpqCrq$
$D.7.2$	9.	$CCpCqrCpCsCqr$
$D.7.8$	10.	$CCpCCqrCsqCpCCqrCsr$
$D.7.9$	11.	$CCpCqCrsCpCqCtCrs$
$D.9.2$	12.	$CCpqCrCsCpq$
$D.12.1$	13.	$CpCqCrr$
$D.9.13$	14.	$CpCqCrCss$
$D.4.13$	15.	$CCpCCqqrCpr$
$D.4.14$	16.	$CCpCCqCrrsCps$

[2] We have eliminated all other 2-bases of this complexity, except for the following two candidates, whose status remains open: $\{CpCqCrr,\ CCpqCCqCqrCpr\}$ and $\{CpCqq,\ CCpqCrCCqCqsCps\}$. We suspect these are *not* bases for C4.

[3] The proof of this result (omitted due to space limitations), which proceeds by exhaustion of all other possible candidate bases, requires the use of only 20 distinct logical matrices of size ≤ 4. In § 4, below, we will say a bit more about how this exhaustion was achieved and how the matrices and bases were discovered.

$D.6.16$	17.	$CCpCCqCrrCstCCpsCpt$
$D.15.17$	18.	$CCpCCqCrrCpsCps$
$D.9.18$	19.	$CCpCCqCrrCpsCtCps$
$D.10.19$	20.	$CCpCCqCrrCpsCCstCpt$
$D.11.20$	21.	$CCpCCqCrrCpsCCstCuCpt^{*}$

Next, we prove that (3) $\Rightarrow$ (2):

	1.	$CCpCCqCrrCpsCCstCuCpt$
$D.1.1$	2.	$CCCpCqqrCsCCpCCtCuuCpvr$
$D.2.1$	3.	$CpCCqCCrCssCqtCCCuuvCwCqv$
$D.3.3$	4.	$CCpCCqCrrCpsCCCttuCvCpu$
$D.1.3$	5.	$CCCpCqrsCtCCCuurs$
$D.5.1$	6.	$CpCCCqqCrsCCstCuCrt$
$D.6.6$	7.	$CCCppCqrCCrsCtCqs$
$D.4.6$	8.	$CCCppqCrCCstq$
$D.1.6$	9.	$CCCpCqrsCtCCqrs$
$D.1.8$	10.	$CCpqCrCCCsspq$
$D.9.7$	11.	$CpCCqrCCrsCtCqs$
$D.7.10$	12.	$CCCCCppqqrCsCtr$
$D.7.11$	13.	$CCCCpqCrCsqtCuCCspt$
$D.1.12$	14.	$CCpqCrCCCCCssttpq$
$D.12.14$	15.	$CpCqCrCCCCCssttCCuuvv$
$D.15.15$	16.	$CpCqCCCCCrrssCCttuu$
$D.16.16$	17.	$CpCCCCCqqrrCCsstt$
$D.17.17$	18.	$CCCCCppqqCCrrss$
$D.13.18$	19.	$CpCCqCCrrsCqs$
$D.18.12$	20.	$CpCqq^{*}$
$D.19.19$	21.	$CCpCCqqrCpr$
$D.21.13$	22.	$CCCCpqCrCsqtCCspt$
$D.21.1$	23.	$CCpCCqCrrCpsCtCps$
$D.22.21$	24.	$CCpqCCqrCpr$
$D.24.24$	25.	$CCCCpqCrqsCCrps$
$D.25.25$	26.	$CCpCqrCCsqCpCsr$
$D.24.26$	27.	$CCCCpqCrCpstCCrCqst$
$D.27.21$	28.	$CCCppCqrCCsqCsr$
$D.25.28$	29.	$CCpqCCrpCrq$
$D.28.7$	30.	$CCpCqrCpCsCqr$
$D.24.30$	31.	$CCCpCqCrstCCpCrst$
$D.31.23$	32.	$CCpCpqCrCpq$
$D.29.32$	33.	$CCpCqCqrCpCsCqr$
$D.27.33$	34.	$CCpCqrCCpqCsCpr^{*}$

Finally, we prove that (2) $\Rightarrow$ (1), which completes the circle:

	1.	$CpCqq$
	2.	$CCpCqrCCpqCsCpr$
$D.1.1$	3.	Cpp^*
$D.2.2$	4.	$CCCpCqrCpqCsCCpCqrCtCpr$
$D.2.1$	5.	$CCpqCrCpq^*$
$D.4.1$	6.	$CpCCqCqrCsCqr$
$D.6.6$	7.	$CCpCpqCrCpq$
$D.7.7$	8.	$CpCCqCqrCqr$
$D.2.8$	9.	$CCpCqCqrCsCpCqr$
$D.9.2$	10.	$CpCCqCrsCCqrCqs$
$D.10.10$	11.	$CCpCqrCCpqCpr^*$ $\square$

The above circle of proofs (1) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1) has the additional benefit of being *pure* — in the sense of [19] and [20]. That is, (*i*) the proof of (1) $\Rightarrow$ (3) does not make use of (2), (*ii*) the proof of (3) $\Rightarrow$ (2) does not make use of (1), and (*iii*) the proof of (2) $\Rightarrow$ (1) does not make use of (3). We think this circle of pure proofs provides an especially elegant demonstration that (2) and (3) are bases of C4.

3. Axiomatic C5

3.1. A Brief History of Axiomatic C5

The problem of axiomatizing the implicational fragment of S5 was solved in 1956 by Lemmon, Meredith, Meredith, Prior, and Thomas. In their seminal paper [8], Lemmon *et. al.* report several bases for C5, including 4, 3, 2, and 1-axiom bases. We will adopt the following 3-axiom basis from [8] as our "reference" axiomatization of C5.[4]

$$\begin{array}{c} CqCpp \\ CCpqCCqrCpr \\ CCCCpqrCpqCpq \end{array} \tag{4}$$

Since the late 50's, and until now, the shortest known bases for C5 have been the 2-axiom bases (v) and (vi) of Lemmon *et. al.* [8, page 227].

[4] (4) is basis (ii) from Lemmon *et. al.* [8, page 227]. This basis is C.A. Meredith's simplification of Lemmon's original 4-axiom basis for C5 — see [13].

These bases contain 20 symbols (9 C's).[5] Interestingly, Carew Meredith was able to find the following 21-symbol (10-C) single axiom for C5.[6]

$$CCCCCppqrCutCCtqCsCuq \tag{5}$$

3.2. Shortest Axiomatizations of C5

Applying our automated reasoning techniques to C5 (see § 4), we have discovered several new (and maximally elegant) 2-axiom bases for C5, including the following 18-symbol, 8-C basis:

$$\begin{array}{c} Cpp \\ CCpqCCCCqrurCpr \end{array} \tag{6}$$

By exhausting all other possible shorter bases (with any number of axioms), we have established that (6) is a *shortest possible* basis for C5. Furthermore, we have ruled-out all other 2-bases of this complexity. Therefore, (6) is *the* shortest basis for C5. It is a corollary of this result, of course, that there is no single axiom for C5 shorter than Meredith's (5). There are, however, at least six other single axioms of length 21. We have discovered six such axioms, including the following:

$$CCCCpqrCCuuqCCqtCsCpt \tag{7}$$

As we did in the case of C4, we will now present a circle of three pure proofs (this time, using (4) as our reference basis) which establishes that (6) and (7) are both bases for C5. First, we prove that (6) $\Rightarrow$ (4):

	1.	$CCpqCCCCqrurCpr$
	2.	Cpp
D·1·1	3.	$CCCCCCCCpqrqCuqtstCCupt$
D·1·2	4.	$CCCCpqrqCpq$
D·3·3	5.	$CCpCqrCCuqCpCur$
D·5·2	6.	$CCpqCCqrCpr^*$
D·5·1	7.	$CCpCCCqrurCCtqCpCtr$
D·6·6	8.	$CCCCpqCrquCCrpu$

[5] Meredith & Prior's [13] seems to be "the last word" on this matter — until now.

[6] What makes this interesting is that — as far as we know — Meredith *failed* to find a single axiom for C4. This is surprising, since Meredith was responsible for finding (shortest) single axioms for just about every system (that has one) which he studied. We sometimes wonder whether the 21-symbol C4 single axiom we reported above had been previously discovered (but never published) by Meredith.

D·6·8	9.	$CCCCpqruCCCCqtCptru$
D·8·4	10.	$CCpCqCprCqCpr$
D·7·9	11.	$CCpCqrCCCCuqtCurCpCur$
D·6·10	12.	$CCCpCqruCCqCpCqru$
D·12·7	13.	$CCCCpqrCuCCCpqrqCCtpCuCtq$
D·4·13	14.	$CCpqCCrpCuCrq$
D·14·2	15.	$CCpqCrCpq$
D·15·2	16.	$CpCqq^*$
D·11·16	17.	$CCCCpqrCpqCuCpq$
D·6·17	18.	$CCCpCqruCCCCqrtCqru$
D·17·18	19.	$CpCCCCqruCqrCqr$
D·19·19	20.	$CCCCpqrCpqCpq^*$

Next, we show that (4) $\Rightarrow$ (7):

	1.	$CCpqCCqrCpr$
	2.	$CCCCpqrCpqCpq$
	3.	$CpCqq$
D·1·1	4.	$CCCCpqCrquCCrpu$
D·1·3	5.	$CCCppqCrq$
D·4·4	6.	$CCpCqrCCuqCpCur$
D·4·2	7.	$CCpCpqCpq$
D·6·4	8.	$CCpCqrCCCCruCqutCpt$
D·6·3	9.	$CCpqCrCpq$
D·4·7	10.	$CCCpqpCCpqq$
D·1·9	11.	$CCCpCqruCCqru$
D·11·10	12.	$CCpqCCCpqrr$
D·6·12	13.	$CCpCCqruCCqrCpu$
D·1·5	14.	$CCCpqrCCCuuqr$
D·11·13	15.	$CCCpqrCCpqCur$
D·1·13	16.	$CCCCpqCrutCCrCCpqut$
D·16·2	17.	$CCpCCCpqrqCpq$
D·14·17	18.	$CCCppCCCqrurCqr$
D·16·18	19.	$CCCCpqrCCuuqCpq$
D·8·19	20.	$CCCCpqCrquCCCCrptCCsspu$
D·20·15	21.	$CCCCpqrCCuuqCCqtCsCpt^*$

Finally, we complete the circle by showing that (7) $\Rightarrow$ (6):

	1.	$CCCCpqrCCuuqCCqtCsCpt$
D·1·1	2.	$CCCpCqruCtCCqru$
D·2·1	3.	$CpCCCqqrCCruCtCsu$
D·3·3	4.	$CCCppqCCqrCuCtr$
D·1·3	5.	$CCCCCppqCrCuqtCsCt6t$
D·2·4	6.	$CpCCqrCCCqruCtCsu$
D·1·5	7.	$CCCpCqruCtCCCssru$
D·4·6	8.	$CCCCpqCCCpqrCuCtrsCt6Ct7s$
D·1·7	9.	$CCCCCppqqrCuCtr$
D·1·8	10.	$CCCCCpqrCuCtrsCt6CCpqs$
D·1·9	11.	$CCCpqrCuCCCttCpqr$
D·1·10	12.	$CCCCpqCrutCsCCCpqut$
D·9·11	13.	$CpCqCrCCCuuCCttss$
D·12·1	14.	$CpCCCCqrurCCrtCsCqt$
D·13·13	15.	$CpCqCCCrrCCuutt$
D·14·14	16.	$CCCCpqrqCCquCtCpu$
D·15·15	17.	$CpCCCqqCCrruu$
D·16·16	18.	$CCCCpqCrCuqtCsCCupt$
D·17·17	19.	$CCCppCCqqrr$
D·1·18	20.	$CCCCpqCpruCtCCqru$
D·19·19	21.	Cpp^*
D·19·20	22.	$CCpqCCrpCrq$
D·9·22	23.	$CpCqCCrCCuutCrt$
D·19·23	24.	$CCpCCqqrCpr$
D·22·24	25.	$CCpCqCCrruCpCqu$
D·25·16	26.	$CCCCpqrqCCquCpu$
D·26·26	27.	$CCCCpqCrquCCrpu$
D·24·26	28.	$CCCCpqrqCpq$
D·27·27	29.	$CCpCqrCCuqCpCur$
D·29·28	30.	$CCpqCCCCqrurCpr^*$ $\square$

4. The Role of Automated Reasoning in Our Research

Throughout our investigations into axiomatic C4 and C5, automated reasoning techniques played a crucial role. In particular, we relied heavily on William McCune's automated reasoning program OTTER [12], H. Zhang and J. Zhang's model-finder SEM [22], as well as John Slaney's model-finder MAGIC [17]. In the final section of this paper, we outline the techniques used to derive these results.

In our search for single axioms for C4 and C5, we used the following procedure.

1. First, we wrote computer programs to generate a large list of candidate formulas which were to be tested as axioms. For most problems, it was practical to generate an exhaustive list of all formulas with up to twenty-one symbols.

2. All the formulas in the list were tested (using matrices) to see which were likely to be tautologies in the system in question.[7]

3. We immediately eliminated large numbers of formulas by applying known results about axiomatizations in the various systems. For example, as reported by Lemmon et. al., every axiomatization for C5 must contain a formula with Cpp as a (possibly improper) subformula [8]. Another useful result is the Diamond-McKinsey theorem that no Boolean algebra can be axiomatized by formulas containing less than three distinct propositional letters [2, p. 83].

4. A set of formulas was selected from the list at random. Using either SEM or a program written by the authors, we found a matrix model that respects modus ponens, invalidates a known axiom-basis for the system, but validates the formulas selected from the list. Such a model suffices to show that the formulas are not single axioms for the system.

5. All the remaining formulas in the list were tested against that matrix. Every formula validated by that matrix would be eliminated.

6. Steps 4 and 5 were repeated until the list of candidate formulas was down to a small number, or eliminated entirely.

7. Finally, we used OTTER to attempt to prove a known axiom basis from each of the remaining candidates.

Obvious changes were made when we searched for axiom-bases with more than a single formula.

Upon implementing the above procedure, we were surprised to discover that even a small number of simple matrix models was capable of eliminating a very large proportion of candidate formulas. For example, it is possible to show that no formula with nineteen symbols is a single axiom for C5 by using ten (and possibly fewer) matrices, none

[7] We say 'likely to be tautologies' because C4 and C5 do not have finite characteristic matrices. Thus, we used matrices which validate all tautologies for the system, but also validate a small percentage of contingent formulas.

of which have more than five elements. Because of the efficiency of this procedure, we were able to complete all of our searches using ordinary consumer-grade computers, with no esoteric hardware.

We believe that this technique for finding axiom-bases in Hilbert-style systems could be used for a wide variety of logics, with equal success. For instance, the authors have used the same technique to discover the shortest known basis for the implicational fragment of the logic RM (first axiomatized by Meyer and Parks [14], [15]) [4], while McCune and Veroff have independently used a very similar technique to search for axioms in lattice theory [11].[8]

At the present time, this procedure is prohibitively time-consuming when applied to logics with a more complete vocabulary of sentential connectives. For not only are there exponentially more formulas of any particular length when additional connectives are added to the language, but the matrices and proofs tend to be larger and more complex. Currently, it is difficult, and sometimes impossible, to discover large matrices or extremely complex condensed-detachment proofs for some problems, although progress is being made on both of these fronts.[9] We believe that further results regarding axiomatizations for more complex logics await future advances in automated reasoning.[10]

References

1. Alan Ross Anderson and Nuel D. Belnap, Jr. The pure calculus of entailment. *J. Symbolic Logic*, 27:19–52, 1962.
2. Alan Ross Anderson and Nuel D. Belnap, Jr. *Entailment.* Princeton University Press, Princeton, N. J., 1975. Volume I: The logic of relevance and necessity.
3. H.B. Curry. Review of Hacking's "What is strict implication?". *Mathematical Reviews*, 31: #4717, 1963.
4. Z. Ernst, B. Fitelson, K. Harris, and L. Wos. A concise axiomatization for the implicational fragment of *RM*. Under consideration for *The Bulletin of the Section of Logic.*
5. Ian Hacking. What is strict implication? *J. Symbolic Logic*, 28:51–71, 1963.
6. J. A. Kalman. Condensed detachment as a rule of inference. *Studia Logica*, 42(4):443–451 (1984), 1983.
7. Saul A. Kripke. The problem of entailment. *J. Symbolic Logic*, 24:324, 1959.

[8] McCune has used different automated reasoning techniques to solve axiomatization problems for the left group and right group calculi. See [9] and [10].

[9] See [21] for a information on the solution of challenge problems using OTTER, as well as for open problems.

[10] We wish to thank Michael Byrd and Ted Ulrich for extremely helpful discussions.

8. E. J. Lemmon, C. A. Meredith, D. Meredith, A. N. Prior, and I. Thomas. *Calculi of pure strict implication*. Philosophy Department, Canterbury University College, Christchurch, New Zealand, 1957.
9. William McCune. Automated discovery of new axiomatizations of the left group and right group calculi. *J. Automat. Reason.*, 9(1):1–24, 1992.
10. William McCune. Single axioms for the left group and right group calculi. *Notre Dame Journal of Formal Logic*, 34(1):132–139, 1993.
11. William McCune and Robert Veroff. Available at the following URL: http://www.mcs.anl.gov/˜mccune/award-2001.
12. William W. McCune. OTTER 3.0 Reference Manual and Guide. Tech. Report ANL-94/6, Argonne National Laboratory, Argonne, IL, 1994.
13. C. A. Meredith and A. N. Prior. Investigations into implicational S5. *Z. Math. Logik Grundlagen Math.*, 10:203–220, 1964.
14. Robert K. Meyer and R. Zane Parks. Independent axioms for the implicational fragment of Sobociński's three-valued logic. *Zeitschrift für Mathematische Logik Grundlagen Mathematik*, 18:291–295, 1972.
15. R. Zane Parks. A note on R-Mingle and Sobociński's three-valued logic. *Notre Dame Journal of Formal Logic*, XIII(2):227–228, 1972.
16. A. N. Prior. *Formal logic*. Clarendon Press, Oxford, 1962.
17. John Slaney. MAGIC, matrix generator for implication connectives. Tech. Report TR-ARP-11-95, Research School of Information Science and Engineer and Centre for Information Science Research, Australian National University, 1995.
18. Dolph Ulrich. Strict implication in a sequence of extensions of S4. *Z. Math. Logik Grundlag. Math.*, 27(3):201–212, 1981.
19. Larry Wos. Searching for circles of pure proofs. *J. Automat. Reason.*, 15(3):279–315, 1995.
20. Larry Wos. OTTER and the Moufang identity problem. *J. Automat. Reason.*, 17(2):215–257, 1996.
21. Larry Wos and Gail W. Pieper. *A Fascinating Country in the World of Computing: Your Guide to Automated Reasoning*. World Scientific Publishing Company, 2000.
22. J. Zhang and H. Zhang. SEM: A system for enumerating models. *Proc. of International Joint Conference on Artificial Intelligence*, 1995.