Some combinatorics of imperfect information

Peter Cameron and Wilfrid Hodges

1 Introduction

We can use the compositional semantics of Hodges [8] to show that any compositional semantics for logics of imperfect information must obey certain constraints on the number of semantically inequivalent formulas. As a corollary, there is no compositional semantics for the 'independence-friendly' logic of Hintikka and Sandu (henceforth IF) in which the interpretation in a structure A of each 1-ary formula is a subset of the domain of A (Corollary 14 below proves this and more). After a fashion, this rescues a claim of Hintikka and provides the proof which he lacked:

> ... there is no realistic hope of formulating compositional truth-conditions for [sentences of IF], even though I have not given a strict impossibility proof to that effect.

(Hintikka [6] page 110ff.) One curious spinoff is that there is a structure of cardinality 6 on which the logic of Hintikka and Sandu gives nearly eight million inequivalent formulas in one free variable (which is more than the population of Finland).

We thank the referee for a sensible change of notation, and Joel Berman and Stan Burris for bringing us up to date with the computation of Dedekind's function (see section 4). Our own calculations, utterly trivial by comparison, were done with Maple V.

2 Definitions

The paper Hodges [8] (cf. [9]) gave a compositional semantics for a language with some devices of imperfect information. The language was complicated, because it allowed imperfect information both at quantifiers and at conjunctions and disjunctions. To make sense of the idea of

imperfect information at conjunctions, one needs to start by distinguishing between indexed and unindexed conjunctions; from that point onwards, everything rapidly becomes ugly. This paper will use only quantifiers of imperfect information; all our conjunctions and disjunctions will be classical.

For a structure with only a single element, there is not much point in revealing or hiding which element one has chosen. So to avoid triviality we shall generally limit ourselves to structures with at least two elements. One can extend the theorems below to structures with a single element, by resurrecting the conjunctions of imperfect information. But this is the only point where we shall lose generality by killing them off.

Syntactically the language CS ('compositional semantics' from the title of [8]) of a given signature σ is the same as the ordinary first-order language of signature σ, with logical symbols $\vee, \wedge, \sim, \forall, \exists$, apart from two changes. First, quantifiers appear only in the contexts $(\forall x/W)$, $(\exists x/W)$ where W is a finite set of variables, possibly empty, and x is a variable not in W. We abbreviate $(\forall x/\emptyset)$, $(\exists x/\emptyset)$ to the usual quantifiers $\forall x$, $\exists x$. We often write $(\forall x/y_0, \dots, y_{m-1})$ for $(\forall x/\{y_0, \dots, y_{m-1}\})$, and likewise with $\exists$. And second, if ϕ is a formula then there is a formula $\downarrow \phi$. We write $\neg$ for $\sim\downarrow$.

Free variables are defined as in ordinary first-order logic, except that occurrences of variables in W in the contexts $(\forall x/W)$, $(\exists x/W)$ are free. The operator $\downarrow$ binds no variables.

One can give intuitive meanings for at least some of the new symbols, but it is always safer to work with the mathematical definitions (as in the Appendix). In this area, intuitions can easily mislead. The 'meaning' of $(\exists x/W)$ is 'There is an element x, not depending on W, such that ... '. The 'meaning' of $(\forall x/W)$ is the dual, for which we don't know a convincing English equivalent. The 'meaning' of $(\downarrow \phi)(\bar{a})$ is: If the identity of the tuple $\bar{a}$ is made public, then this tuple satisfies ϕ.

Hintikka and Sandu [7] gave a formal semantics for IF in terms of games, and with suitable adaptations their semantics covers all sentences of CS not containing $\downarrow$.

The semantics of [8] associates to each formula $\phi(x_0, \dots, x_{n-1})$ of CS and each structure A of appropriate signature a pair of sets, the set of *trumps* of ϕ in A and the set of *cotrumps* of ϕ in A respectively. We write $|\phi|^\tau_A$ for

the set of trumps of ϕ in A, and $|\phi|^{\kappa}_{A}$ for the set of cotrumps of ϕ in A. Intuitively, a trump is a nonempty set of n-tuples of elements of A which satisfy ϕ in A uniformly, where 'uniformly' means independent of any facts which are 'hidden' by the slashed sets W in quantifiers in ϕ. By the same token, a cotrump is a nonempty set of n-tuples of A which uniformly fail to satisfy ϕ in A. We give the inductive definitions of $|\phi|^{\tau}_{A}$ and $|\phi|^{\kappa}_{A}$ in the Appendix at the end of this paper, with apologies for the brevity. A fuller account appears in [8], together with a proof that a sentence ϕ without $\downarrow$ is true in A by the adapted Hintikka-Sandu semantics if and only if ϕ has a trump in A.

The paper [8] also proves a full abstraction theorem, which says that for any two formulas $\phi(x_0, \ldots, x_{n-1})$, $\psi(x_0, \ldots, x_{n-1})$ the following are equivalent:

- ϕ and ψ have the same trumps and cotrumps as each other in every structure;
- replacing an occurrence of ϕ by ψ in a larger sentence never affects the truth-value of the larger sentence in any structure.

In short, if two formulas have different trumps or cotrumps in some structure, then the two formulas really are inequivalent.

For our purposes the language IF of Hintikka and Sandu [7] is essentially the same as the fragment of CS consisting of the formulas which meet the following two restrictions:

1. $\downarrow$ never occurs, and $\sim$ occurs only immediately in front of atomic formulas, and
2. if a quantifier $(\exists x/W)$ occurs within the scope of a quantifier $(\exists y/V)$, then $y \in W$.

Let us call this fragment HS (for Hintikka-Sandu). Apparently the purpose of the second restriction was to prevent the player $\exists$ from using her earlier choices to signal information to her later ones. It is not a reliable way of achieving this purpose: $\exists$ can sometimes work her way around this obstacle by using her choices at $\vee$ instead. A quirk of the syntax in [7] means that although there are translations between IF and HS, these translations are not compositional, so that the compositional semantics for CS doesn't automatically yield one for IF. Nevertheless one can devise a compositional semantics for IF; see [9].

We shall need to concatenate tuples. If $\bar{a}$ and $\bar{b}$ are tuples, we write $\bar{a}\bar{b}$ for the tuple consisting of $\bar{a}$ followed by $\bar{b}$. If t is a set of tuples and $\bar{b}$ is a tuple, we write $t\bar{b}$ for the set of tuples $\bar{a}\bar{b}$ with $\bar{a} \in t$. If t, u are sets of tuples, we write tu for the set of tuples $\bar{a}\bar{b}$ with $\bar{a} \in t$ and $\bar{b} \in u$.

We write m for the set $\{0, \ldots, m-1\}$. We write the set of all n-tuples of elements of m as $(m)^n$, to distinguish it from the n-th integer power of m, which is m^n.

3 Trumps in finite structures

Let A be a structure. Abusing notation, we write A^n for the n-th cartesian power of the domain of A. By an *n-suit* in A we mean a set S of nonempty subsets of A^n which is closed under nonempty subsets. By an *(m,n)-suit* we mean an n-suit in a structure whose domain is the set m. By a *double (m,n)-suit* we mean an ordered pair (S_0, S_1) where S_0, S_1 are (m,n)-suits with $\bigcup S_0$ disjoint from $\bigcup S_1$.

Our first proposition follows easily from the definitions in [8]:

Proposition 1 *Let A be a structure and $\phi(x_0, \ldots, x_{n-1})$ a formula of the signature of A. Then $S_0 = |\phi|^\tau_A$ and $S_1 = |\phi|^\kappa_A$ are n-suits in A, and $\bigcup S_0$ is disjoint from $\bigcup S_1$. In particular if A is a finite structure with the m elements $\{0, \ldots, m-1\}$, then (S_0, S_1) is a double (m,n)-suit.*

□

Theorem 3 below will show that for finite structures, Proposition 1 is best possible: for all $m \geq 2$ and n there is a formula ϕ of HS such that every possible double (m,n)-suit describes the sets of trumps and cotrumps of ϕ in a suitable m-element structure A. For simplicity we start with the case of trumps; in this case we can get by with a simpler formula.

Theorem 2 *Suppose m, n are positive integers and S is a set of nonempty subsets of $(m)^n$. Let k be such that $m^k \geq 2^{m^n}$. Then there is an $(n+k)$-ary relation R on m such that the trumps of the formula*

$$(\exists y_0/\bar{x})(\exists y_1/\bar{x}, y_0) \ldots (\exists y_{k-1}/\bar{x}, y_0, \ldots, y_{k-2}) R(\bar{x}, y_0, \ldots, y_{k-1})$$

in the structure $A = (m, R)$ are precisely the nonempty subsets of members of S.

PROOF. Since S is a set of subsets of m^n, its cardinality is at most 2^{m^n}. We can index its elements s by k-tuples of elements of m; write $\bar{b}_s$ for the k-tuple which indexes s. Let R be the relation

$$\{(\bar{a}, \bar{b}_s) : s \in S, \bar{a} \in s\}.$$

Using this relation R, write $\phi(\bar{x})$ for the formula in the theorem, and $\phi_i(\bar{x})$ for the subformula

$$(\exists y_i/\bar{x}, y_0, \ldots, y_{i-1}) \ldots (\exists y_{k-1}/\bar{x}, y_0, \ldots, y_{k-2}) R(\bar{x}, y_0, \ldots, y_{k-1}),$$

so that in particular ϕ is ϕ_0. Write $A = (m, R)$. Let t be a nonempty subset of $(m)^n$. Then by the rules in the Appendix (particularly the first and last ones):

$$t \in |\phi|_A^\tau \;\Leftrightarrow$$

$$\Leftrightarrow (\exists b_0)\ tb_0 \in |\phi_1|_A^\tau$$

$$\Leftrightarrow \ldots$$

$$\Leftrightarrow (\exists b_0, \ldots, b_{k-1})\ tb_0 \ldots b_{k-1} \subseteq R_A$$

$$\Leftrightarrow (\exists s \in S)\ t \subseteq s.$$

□

Theorem 3 *Suppose m, n are positive integers with $m \geq 2$, and S_0, S_1 are sets of nonempty subsets of $(m)^n$ with $\bigcup S_0$ disjoint from $\bigcup S_1$. Let k be such that $m^k > 2^{m^n}$. Then there is an $(n+2k)$-ary relation R on m such that, writing $\phi(\bar{x})$ for the formula*

$$(\forall y_0/\bar{x})(\forall y_1/\bar{x}, y_0) \ldots (\forall y_{k-1}/\bar{x}, y_0, \ldots, y_{k-2})$$

$$(\exists z_0/\bar{x}, \bar{y})(\exists z_1/\bar{x}, \bar{y}, z_0) \ldots (\exists z_{k-1}/\bar{x}, \bar{y}, z_0, \ldots, z_{k-2}) R(\bar{x}, \bar{y}, \bar{z})$$

and A for the structure (m, R),

- *the trumps of ϕ in A are precisely the nonempty subsets of members of S_0, and*

- *the cotrumps of ϕ in A are precisely the nonempty subsets of members of S_1.*

PROOF. As before, we choose a distinct k-tuple $\bar{c}_s$ for each set $s \in S_0 \cup S_1$. We define the $(n+2k)$-ary relation R as follows:

> If $\bar{a}, \bar{b}, \bar{c}$ are tuples of lengths n, k, k respectively, then $\bar{a}\bar{b}\bar{c} \in R$ if and only if at least one of the following holds:
>
> (i) for some $s \in S_0$, $\bar{c} = \bar{c}_s$ and $\bar{a} \in s$, or
>
> (ii) for some $s \in S_1$, $\bar{b} = \bar{c} = \bar{c}_s$ and $\bar{a} \notin s$, or
>
> (iii) $\bar{c}$ is equal to $\bar{b}$ but not to any $\bar{c}_s$ with $s \in S_1$.

Let t be a nonempty subset of $(m)^n$. Then again using the rules in the Appendix (this time the last two):

$$t \in |\phi|^\tau_A \;\Leftrightarrow$$

$$\Leftrightarrow\; t(m)^1 \in |(\forall y_1/\bar{x}, y_0) \dots (\exists z_{k-1}/\bar{x}, \bar{y}, z_0, \dots, z_{k-2}) R(\bar{x}, \bar{y}, \bar{z})|^\tau_A$$

$$\Leftrightarrow\; \dots$$

$$\Leftrightarrow\; t(m)^k \in |(\exists z_0/\bar{x}, \bar{y})(\exists z_1/\bar{x}, \bar{y}, z_0) \dots (\exists z_{k-1}/\bar{x}, \bar{y}, z_0, \dots, z_{k-2}) R(\bar{x}, \bar{y}, \bar{z})|^\tau_A$$

$$\Leftrightarrow (\exists c_0, \dots, c_{k-1})\; t(m)^k \subseteq R_A$$

$$\Leftrightarrow\; (\exists \bar{c})(\forall \bar{b})\; t\bar{b}\bar{c} \subseteq R_A.$$

Dually,

$$t \in |\phi|^\kappa_A \;\Leftrightarrow$$

$$\Leftrightarrow\; (\exists b_0, \dots, b_{k-1})\; tb_0 \dots b_{k-1} \in |(\exists z_0/\bar{x}, \bar{y})(\exists z_1/\bar{x}, \bar{y}, z_0) \dots$$

$$\dots (\exists z_{k-1}/\bar{x}, \bar{y}, z_0, \dots, z_{k-2}) R(\bar{x}, \bar{y}, \bar{z})|^\kappa_A$$

$$\Leftrightarrow\; (\exists b_0, \dots, b_{k-1})\; tb_0 \dots b_{k-1}(m)^k \in |\sim R(\bar{x}, y_0, \dots, y_{k-1}, z_0, \dots, z_{k-1})|^\tau_A$$

$$\Leftrightarrow (\exists \bar{b})(\forall \bar{c})\; t\bar{b}\bar{c} \cap R_A = \emptyset.$$

Let t be a nonempty set of n-tuples from A. There are four things to show:

1. If t is a subset of some $s \in S_0$ then t is a trump of ϕ in A.
2. If t is a trump of ϕ in A then t is a subset of some $s \in S_0$.
3. If t is a subset of some $s \in S_1$ then t is a cotrump of ϕ in A.
4. If t is a cotrump of ϕ in A then t is a subset of some $s \in S_1$.

We prove these as follows. We call a k-tuple $\bar{d}$ *dead* if it is not of the form $\bar{c}_s$ for any $s \in S_0 \cup S_1$. By the choice of k, there are at least two dead tuples.

1. If $t \subseteq s \in S_0$, then by (i) in the definition of R, $t\bar{b}\bar{c}_s \subseteq R$ for all $\bar{b}$. It follows that t is a trump of ϕ in A.
2. Suppose t is a trump of ϕ in A. Then there is some $\bar{c}$ such that for all $\bar{b}$, $t\bar{b}\bar{c} \subseteq R$. In particular let $\bar{d}$ be a dead k-tuple not equal to $\bar{c}$. Then $t\bar{d}\bar{c} \subseteq R_A$. By the definition of R this is only possible when $\bar{c} = \bar{c}_s$ and $t \subseteq s$ for some $s \in S_0$.
3. Assume $t \subseteq s \in S_1$. We show that if $\bar{a} \in t$ and $\bar{c}$ is any k-tuple, then $\bar{a}\bar{c}_s\bar{c} \notin R_A$. Clauses (i) and (iii) of the definition of R don't put it in R, since s is in S_1. Neither does clause (ii), since $\bar{a} \in s$.
4. Finally suppose t is a cotrump of ϕ_A. Then there is $\bar{b}$ such that for each $\bar{c}$, $t\bar{b}\bar{c} \cap R = \emptyset$. In particular $t\bar{b}\bar{b} \cap R = \emptyset$. So by (iii) of the definition of R, $\bar{b} = \bar{c}_s$ for some $s \in S_1$, and hence by (ii), $t \subseteq s$.

This completes the proof. □

Corollary 4 *Let m, n be positive integers with $m \geq 2$. Then there is a structure B with domain m such that the following two sets are equal:*

(a) The set of all double (m,n)-suits.

(b) The set of all sets of the form $(|\phi|^\tau_B, |\phi|^\kappa_B)$, where ϕ ranges over formulas $\phi(x_0, \ldots, x_{n-1})$ of HS.

Also the sets $|\phi|^\tau_B$ are exactly the (m,n)-suits.

PROOF. We know from [8] that every set of the form (b) is a set of the form (a) too. For the converse, let A be the structure of empty signature with domain m. Each double (m,n)-suit S gives rise to a relation R_S as in Theorem 3. Take B to be the expansion of A got by adding all the relations R_S. The last sentence follows by noting that every (m,n)-suit S occurs as the first term of a double (m,n)-suit $(S, \emptyset)$. □

4 Counting sets of trumps

Let m and n be positive integers. We define $f(m,n)$ to be the number of distinct (m,n)-suits, and $g(m,n)$ to be the number of distinct double (m,n)-suits. We write $f(m)$ for $f(m,1)$, and likewise $g(m)$ for $g(m,1)$.

By an *m-antichain* we mean a set of nonempty subsets of m, such that no two of the subsets are comparable under inclusion.

Proposition 5 *For all positive integers m, $f(m)$ is the number of distinct m-antichains.*

PROOF. The maximal sets in an m-suit form an m-antichain. Conversely if S is an m-antichain then the nonempty subsets of sets in S form an m-suit. □

The next proposition lists some easy properties of the four functions just defined.

Proposition 6 *Suppose $2 \leq m < \omega$ and $1 \leq n < \omega$.*

(a) $f(m,n) = f(m^n)$, $g(m,n) = g(m^n)$.

(b) $m < m'$ *implies* $f(m) < f(m')$ *and* $g(m) < g(m')$.

(c) $2^m < f(m) < 2^{(2^m-1)}$.

(d) $2f(m) < g(m)$.

PROOF. (a) and (b) are clear.

For the upper bound in (c), note first that every $(m,1)$-suit is a set of nonempty subsets of m; hence $f(m)$ is at most the number of such sets, which is $2^{(2^m-1)}$. But since $m \geq 2$, there is at least one set of nonempty subsets of m which is not closed under nonempty subsets. Turning to the lower bound, each set of singleton subsets of m is an $(m,1)$-suit, giving 2^m such suits. But since $m \geq 2$, there is at least one other $(m,1)$-suit, namely $\{\{0\},\{1\},\{0,1\}\}$.

For (d), note that every nonempty m-suit S contributes two to $g(m)$, namely the double m-suits $(S,\emptyset)$ and $(\emptyset,S)$. Since $m \geq 2$ there are at least three other double m-suits, for example $(\{\{0\}\},\{\{1\}\})$, $(\{\{1\}\},\{\{0\}\})$ and the empty double m-suit. □

The following refinement of Proposition 6(c) needs a subtler argument.

Proposition 7 *If $m \geq 3$ then $f(m) < 2^{(2^m - m)}$.*

PROOF. Let k be $\lfloor (m-1)/2 \rfloor$, and set

$$\beta(m) = \binom{m}{k}.$$

One easily verifies the following:

- $\beta(m)/m$ is strictly increasing on even m, and likewise on odd m, for all integers $m \geq 2$.
- $\beta(6)/6 = 2.5$ and $\beta(7)/7 = 5$.

Write A for the set of k-element subsets of m and B for the set of $(m-k)$-element subsets of m; note that A and B are disjoint. We shall use the following claim:

> For each set a in A we can choose a set a' in B with $a \subset a'$, in such a way that if $a_1 \neq a_2$ then $a_1' \neq a_2'$.

Assume the claim. Any m-antichain is determined by its characteristic function $\chi : \mathcal{P}(m) \to 2$. But if a is any set in A, the restriction of χ to $\{a, a'\}$ must be one of only three possible functions, because $a \subset a'$. It follows that $f(m)$, the number of m-antichains, is at most

$$\left(\frac{3}{4}\right)^{|A|} .2^{2^m} \;=\; \left(\frac{3}{4}\right)^{\beta(m)} .2^{2^m}.$$

So it suffices to show that

$$\left(\frac{3}{4}\right)^{\beta(m)} < \left(\frac{1}{2}\right)^{m},$$

or taking logs,

$$\beta(m) > \frac{m \log 2}{\log 4/3} = m \times 2.409\ldots .$$

As we have seen, this holds for all $m \geq 6$.

Now we prove the claim. Define a bipartite graph on A and B by putting an edge from a to b if and only if $a \subset b$. We note that each vertex has valency $\gamma = \binom{m-k}{m-2k}$. For each subset X of A let $X^\star$ be $\{b \in B : b$ is joined to some vertex in $X\}$. Hall's Marriage Theorem ([5] p.

89) tells us that a sufficient condition for the claim to hold is that for every subset X of A,

$$|X^\star| \geq |X|.$$

We show that this holds. Count the number of edges incident with vertices in X in two ways. First, starting from A, the number is $\gamma|X|$. Second, starting from B the number is $\sum_{b \in X^\star} \gamma_b$, where for each b in $X^\star$, γ_b is the number of vertices in X joined to b. Clearly each γ_b is at most γ, and it follows at once that $|X^\star| \geq |X|$ as required. □

To find sharper results, we start by noting another way of counting m-suits. We write $F(m)$ for the number of elements of the free distributive lattice on m generators.

Proposition 8 *For every $m \geq 1$, $F(m) = f(m) - 1$.*

PROOF. This is an observation of Skolem from 1913. One can find a proof and discussion in Birkhoff [1] Chapter IX section 10. (Dedekind first raised the problem of calculating $F(m)$.) □

In a moment Proposition 8 will allow us to calculate $f(m)$ from known values of $F(m)$. (Note that several writers prefer to give values of $F(m) + 2$, which is the number of elements of the free distributive lattice on m generators with new top and bottom elements adjoined.) But first we introduce an auxiliary function that will give us $g(m)$ too. We define $h(m)$ to be the number of m-suits S such that $\bigcup S = m$. The definitions immediately yield:

Proposition 9 *For every $m \geq 0$,*

$$f(m) = \sum_{k=0}^{m} \binom{m}{k} h(k),$$

$$g(m) = \sum_{k=0}^{m} \binom{m}{k} h(k) f(m-k).$$

□

Using Proposition 9 and some values for F from Lunnon [12] (for $m \leq 6$), Berman and Köhler [3] (for $m = 7$) and Wiedemann [13] (for $m = 8$), we

have the following table. (The number $h(n)$ is the number of essentially n-ary term operations in the variety of distributive lattices with 1; cf. Berman [2].)

	2^m	$h(m)$	$f(m)$	$g(m)$	2^{2^m}
$m=0$	1	1	1	1	2
$m=1$	2	1	2	3	4
$m=2$	4	2	5	11	16
$m=3$	8	9	19	55	256
$m=4$	16	114	167	489	65,536
$m=5$	32	6,894	7,580	17,279	4,294,967,296
$m=6$	64	7,785,062	7,828,353	15,758,603	$\sim 2\times 10^{19}$
$m=7$	128	2,414,627, 396,434	2,414,682, 040,997	4,829,474, 397,415	$\sim 3\times 10^{38}$
$m=8$	256	56,130,437, 209,370,320, 359,966	56,130,437, 228,687,557, 907,787	112,260,874, 496,010,913, 723,317	$\sim 1\times 10^{77}$

(Wiedemann [13] reports that the calculation of $f(8)$ took 200 hours on a Cray-2.)

One can think of the ratio of $g(m)$ to 2^m as measuring the expressive strength of CS compared with ordinary first-order logic—always bearing in mind that CS may have a rather unorthodox notion of what is worth expressing.

Proposition 10 *For all $m \geq 1$, $g(m) < 2^{2^m}$.*

PROOF. If (S_0, S_1) is a double m-suit then $S_0 \cup S_1$ is an m-suit and the pair (S_0, S_1) is recoverable from the pair

$$(S_0 \cup S_1, \bigcup S_0).$$

So $g(m) \leq f(m).2^m$, and it suffices to show that $f(m) < 2^{2^m}/2^m$. For all $m \geq 6$ we have this by Proposition 7. For the remaining values of m, use the table above to check the proposition directly. □

5 An asymptotic result

In fact as m rises, $g(m)$ falls so far short of 2^{2^m} that it soon settles down very near $2f(m)$. The table above illustrates this already for quite low values of m. In this section we prove it in the limit.

We write

$$\alpha(m) = \binom{m}{\lfloor m/2 \rfloor}.$$

Thus $\alpha(m)$ is the highest of the binomial coefficients $\binom{m}{i}$. The following facts are known.

Proposition 11 *(a) There are positive constants c, c' such that*

$$(1 + ce^{-m/4})\alpha(m) \leq \log_2 f(m) \leq \left(1 + \frac{c' \ln m}{\sqrt{m}}\right) \alpha(m).$$

(b)

$$\frac{2^m}{\sqrt{\pi \lfloor m/2 \rfloor}} < \alpha(m) < \frac{2^m}{\sqrt{\pi \lfloor m/2 \rfloor}} \left(1 + \frac{1}{8\lfloor m/2 \rfloor}\right).$$

PROOF. (a) is due to Kleitman [11], and (b) is direct from Stirling's formula. □

We remark that Sperner's Theorem ([5] p. 101) and a calculation in [4] give the bound

$$f(m) \leq \left(\frac{e2^m}{\alpha(m)}\right)^{\alpha(m)},$$

though we shall not need this.

Proposition 12 $\frac{g(m)}{f(m)} \to 2$ *as* $m \to \infty$.

PROOF. From Proposition 6 we have that $g(m) \geq 2f(m)$. In the other direction, using Proposition 9,

$$g(m) = f(m) + mf(m-1) + \sum_{k=2}^{m-2} \binom{m}{k} h(k) f(m-k) + mh(m-1) + h(m)$$

$$\leq 2f(m) + 2mf(m-1) + 2^m . f(m-2)^2.$$

It suffices to show that

$$2mf(m-1) = o(f(m)) \text{ as } m \to \infty$$

and

$$2^m.f(m-2)^2 = o(f(m)) \text{ as } m \to \infty.$$

Or taking logs, we must show that if

$$\beta(m) = \log_2(f(m)) - \log_2(f(m-1)) - 1 - \log_2(m),$$

$$\gamma(m) = \log_2(f(m)) - 2\log_2(f(m-2)) - m,$$

then $\beta(m)$ and $\gamma(m)$ both tend to ∞ as $m \to \infty$. Now Kleitman's bounds (Proposition 11(a)) tell us that for all large enough m,

$$\beta(m) \geq \alpha(m) - 1.1\alpha(m-1) - 1 - \log_2(m).$$

By Stirling's formula, $1 + \log_2(m) = o(\alpha(m-1))$ as $m \to \infty$, so that for all large enough m,

$$\beta(m) \geq \alpha(m) - 1.2\alpha(m-1).$$

Then by Stirling again,

$$\beta(m) \geq \frac{2^m}{\sqrt{\pi m/2}} - 1.3\frac{2^{m-1}}{\sqrt{\pi(m-1)/2}}$$

$$= \frac{2^{m-1}}{\sqrt{\pi(m-1)/2}}\left(2\sqrt{\frac{m-1}{m}} - 1.3\right)$$

which clearly tends to ∞ as $m \to \infty$. Likewise for all large enough m,

$$\gamma(m) \geq \alpha(m) - 2.1\alpha(m-2),$$

so

$$\gamma(m) \geq \frac{2^{m-2}}{\sqrt{\pi(m-2)/2}}\left(4\sqrt{\frac{m-2}{m}} - 2.1\right).$$

□

6 Impossible semantics

By an *adequate semantics* for CS we mean a function which assigns to each pair (ϕ, A), where ϕ is a formula of CS and A is a structure whose signature includes that of ϕ, an interpretation $|\phi|_A$ with the following two properties:

(a) There is a distinguished value, call it $TRUE$, such that if ϕ is a sentence of CS then $|\phi|_A = TRUE$ if and only if ϕ is true in A under the semantics of [8].

(b) Suppose ϕ, ψ are formulas and χ is a sentence of CS, and A is a structure whose signature contains those of ϕ, ψ and χ. If $|\phi|_A = |\psi|_A$, and χ' comes from χ by replacing an occurrence of ϕ in χ by an occurrence of ψ, then $|\chi|_A = TRUE$ if and only if $|\chi'|_A = TRUE$.

One can define 'adequate semantics for HS' similarly.

Condition (a) says, in the case of HS, that the semantics agrees with that of Hintikka and Sandu on sentences. Condition (b) is a weak version of compositionality: the meaning of a complex formula can be recovered from the meanings of its parts and the way they are arranged. Thus an adequate semantics is, roughly speaking, a compositional semantics which extends the Hintikka-Sandu semantics. Under some technical assumptions which are met here, one can show that there is a smallest adequate semantics, in the sense that if any adequate semantics makes two formulas ϕ and ψ equivalent, then this one does. It happens that this smallest adequate semantics is the trump-cotrump semantics. So the number of semantic equivalence classes is a minimum for the trump-cotrump semantics. The paper [10] sets out these background facts more rigorously. (But note that what we have called the smallest semantics, because it has fewest synonymy classes, is called maximal in [10] because its synonymy relation is maximal.)

Here we shall give a direct proof of the same consequences for CS and HS, without appealing to the machinery of [10]

Theorem 13 *If $|.|$ is an adequate semantics for HS, then for each integer $m \geq 2$ there is a structure A with m elements, such that there are at least $f(m)$ distinct interpretations $|\phi(x)|_A$ as $\phi(x)$ ranges over the formulas of HS with one free variable x. If $|.|$ is an adequate semantics for CS, then the same holds with g in place of f.*

PROOF. The semantics in this paragraph is that of [8]; we shall move on to $|.|$ in the next paragraph. Fix m. In Theorem 2 let n be 1 and choose k as stated in the theorem. There are $f(m)$ distinct m-suits; number them from 0 to $f(m)-1$. If S is the i-th m-suit, let R_i be the relation defined in terms of S in the theorem. Let the structure A have domain m, labelled relations R_i $(i < f(m))$, and for each subset t of m a 1-ary relation symbol P_t naming t. For each $i < f(m)$, let $\psi_i(x)$ be the formula defined in the statement of Theorem 2 for the i-th m-suit S. By Theorem 2, if $i \neq i'$ then ψ_i and $\psi_{i'}$ have different trumps. Suppose for example that t is a trump of ψ_i in A but not a trump of $\psi_{i'}$ in A. Then there is a sentence $\chi_{ii'}$ with subformula ψ_i, whose truth value in A changes when ψ_i is replaced by $\psi_{i'}$. In fact we can take $\chi_{ii'}$ to be the sentence

$$\forall \bar{x}\ (\sim P_t(\bar{x}) \vee \psi_i(\bar{x})),$$

as in the proof of full abstraction (Theorem 7.6) in [8].

Now we turn to the adequate semantics $|.|$. Since this semantics agrees with that of [8] on sentences, if $i \neq i'$ then the value $|\chi_{ii'}|_A$ changes when we replace ψ_i in $\chi_{ii'}$ by $\psi_{i'}$. So by the second clause in the definition of adequacy, the interpretations $|\psi_i|_A$ $(i < f(m))$ must all be distinct.

The same argument works for CS with appropriate changes. □

Of course this proof is grotesquely extravagant. All we need for A is a set of cardinality m with constants to name all the elements of m; then the relations R_i and the sets X are all definable by quantifier-free formulas.

It follows at once by Proposition 6(c) that there is no adequate semantics $|.|$ for HS in which each interpretation $|\phi(x)|_A$ is a subset of the domain of A. One might be tempted to try using a pair of subsets instead of a single set. The following corollary puts paid to any such hope.

Corollary 14 *Let λ be any positive integer. Then there is no adequate semantics $|.|$ for HS in which each interpretation $|\phi(x)|_A$ is a set of ordered λ-tuples of elements of A. The same holds a fortiori for CS.*

PROOF. By Theorem 13 it suffices to find $m \geq 2$ such that

$$2^{m^\lambda} < f(m).$$

Using Kleitman's lower bound (Proposition 11(a) above) and the lower bound on $\alpha(m)$ given by Stirling's formula, a sufficient condition for this is

that

$$m^\lambda < \frac{2^m}{\sqrt{\pi\lfloor m/2 \rfloor}}.$$

Since 2^m climbs much faster than $m^\lambda\sqrt{\lfloor m/2 \rfloor}$, it is clear that such m exist. □

There is no clear analogue of the proof of Corollary 14 if we restrict to infinite structures. Suppose κ is an infinite cardinal, and we consider interpretations in the semantics of [8]. Then we can bound the number of possible interpretations of formulas $\phi(x)$ of CS in a structure A of cardinality κ as follows. Without loss we can suppose there are no function or constant symbols. Call two formulas of CS *congruent* if they differ only in the choice of relation symbols. Then there are ω congruence classes of formulas. The interpretation in A of a formula ϕ is determined by its congruence class and the assignment to relation symbols in ϕ of relations on the domain of A; the number of such relations is 2^κ. Thus the total number of distinct interpretations of formulas of CS in A, using the semantics of [8], is $\omega.2^\kappa = 2^\kappa$. But this is also the number of subsets of the domain of A.

Common sense suggests that there is no sensible semantics for CS on infinite structures A, using subsets of the domain of A as interpretations for formulas with one free variable. But we don't know a sensible theorem along these lines.

Appendix: The definition of trumps and cotrumps

If $\phi(v_0, \ldots, v_{n-1})$ is a formula of the language of CS for signature σ, and A is a structure of signature σ, the interpretation of ϕ in A consists of two sets of nonempty sets of n-tuples of elements of A, viz. the set $|\phi|^\tau_A$ of trumps for ϕ in A and the set $|\phi|^\kappa_A$ of cotrumps for ϕ in A. The definitions of trumps and cotrumps are by induction on the complexity of ϕ, as follows. In the definitions we use the notation of section 2. The variables s, t, u range over sets of tuples of elements of A; *we always assume that t is nonempty* (but s, u can be empty). The set W is assumed to be a subset of $\{v_0, \ldots, v_{n-1}\}$. If $\bar{a}, \bar{b}$ are respectively the n-tuples $(a_0, \ldots, a_{n-1}), (b_0, \ldots, b_{n-1})$ of elements of A, we write $\bar{a} \simeq_W \bar{b}$ to mean that $a_i = b_i$ whenever $v_i \notin W$. Then $\simeq_W$ is an equivalence relation; we say t is a $\simeq_W$-*set* if t is a subset of a single equivalence class of $\simeq_W$.

- Suppose ϕ is atomic.
  Then $t \in |\phi|^\tau_A$ if and only if every tuple in t satisfies ϕ in A;
  $t \in |\phi|^\kappa_A$ if and only if no tuple in t satisfies ϕ in A.

- Suppose ϕ is $\sim \psi(v_0, \ldots, v_{n-1})$.
  Then $t \in |\phi|^\tau_A$ if and only if $t \in |\psi|^\kappa_A$;
  $t \in |\phi|^\kappa_A$ if and only if $t \in |\psi|^\tau_A$.

- Suppose ϕ is $\psi(v_0, \ldots, v_{n-1}) \wedge \chi(v_0, \ldots, v_{n-1})$.
  Then $|\phi|^\tau_A = |\psi|^\tau_A \cap |\chi|^\tau_A$;
  $t \in |\phi|^\kappa_A$ if and only if there are $s \in |\psi|^\kappa_A$ and $u \in |\chi|^\kappa_A$ such that $t \subseteq s \cup u$.

- Suppose ϕ is $\psi(v_0, \ldots, v_{n-1}) \vee \chi(v_0, \ldots, v_{n-1})$.
  Then $t \in |\phi|^\tau_A$ if and only if there are $s \in |\psi|^\tau_A$ and $u \in |\chi|^\tau_A$ such that $t \subseteq s \cup u$;
  $|\phi|^\kappa_A = |\psi|^\kappa_A \cap |\chi|^\kappa_A$.

- Suppose ϕ is $(\forall v_n/W)\psi(v_0, \ldots, v_n)$.
  Then $t \in |\phi|^\tau_A$ if and only if $tA^1 \in |\psi|^\tau_A$;
  $t \in |\phi|^\kappa_A$ if and only if there is $u \in |\psi|^\kappa_A$ such that for each $\simeq_W$-set $s \subseteq t$ there is an element b of A for which $sb \subseteq u$.

- Suppose ϕ is $(\exists v_n/W)\psi(v_0, \ldots, v_n)$.
  Then $t \in |\phi|^\tau_A$ if and only if there is $u \in |\psi|^\tau_A$ such that for each $\simeq_W$-set $s \subseteq u$ there is an element b of A for which $sb \subseteq u$;
  $t \in |\phi|^\kappa_A$ if and only if $tA^1 \in |\psi|^\kappa_A$.

- Suppose ϕ is $\downarrow \psi(v_0, \ldots, v_{n-1})$.
  Then $t \in |\phi|^\tau_A$ if and only if $t \subseteq \bigcup |\psi|^\tau_A$;
  $t \in |\phi|^\kappa_A$ if and only if $t \cap \bigcup |\psi|^\tau_A = \emptyset$.

- Suppose $\phi(v_0, \ldots, v_{n-1})$ is $\psi(v_0, \ldots, v_{n-2})$.
  Then $t \in |\phi|^\tau_A$ if and only if for every element b of A the set $\{\bar{a} : \bar{a}b \in t\}$ is either empty or in $|\psi|^\tau_A$;
  $t \in |\phi|^\kappa_A$ if and only if for every element b of A the set $\{\bar{a} : \bar{a}b \in t\}$ is either empty or in $|\psi|^\kappa_A$.

In the paper we use the quantifier cases where $W = \{v_0, \ldots, v_{n-1}\}$. In these cases the quantifier clauses reduce to:

- Suppose ϕ is $(\forall v_n/W)\psi(v_0, \ldots, v_n)$.
  Then $t \in |\phi|^\tau_A$ if and only if $tA^1 \in |\psi|^\tau_A$;
  $t \in |\phi|^\kappa_A$ if and only if there is an element b of A for which $tb \in |\psi|^\kappa_A$.

- Suppose ϕ is $(\exists v_n/W)\psi(v_0, \ldots, v_n)$.
  Then $t \in |\phi|^\tau_A$ if and only if there is an element b of A for which $tb \in |\psi|^\tau_A$;
  $t \in |\phi|^\kappa_A$ if and only if $tA^1 \in |\psi|^\kappa_A$.

References

[1] Birkhoff, G.: Lattice theory. American Mathematical Society, Providence RI 1961.

[2] Berman, J.: Algebraic properties of k-valued logics. Proceedings of Tenth International Symposium on Multiple-Valued Logic, Evanston, Illinois 1980.

[3] Berman, J. and Köhler, P.: Cardinalities of finite distributive lattices. Mitteilungen aus dem Mathem. Seminar Giessen **121** (1976) 103–124.

[4] Blumer, A., Ehrenfeucht, A., Haussler, D., Warmuth, M. K.: Learnability and the Vapnik-Chervonenkis dimension. J. Assoc. Comp. Mach. **36** (1989) 929–965.

[5] Cameron, P. J.: Combinatorics. Cambridge University Press 1994.

[6] Hintikka, J.: The principles of mathematics revisited. Cambridge University Press, Cambridge 1996.

[7] Hintikka, J., Sandu, G.: Game-theoretical semantics. Handbook of logic and language, ed. van Benthem, J., ter Meulen, A., Elsevier 1996, pp. 361–410.

[8] Hodges, W.: Compositional semantics for a language of imperfect information. Logic Journal of the IGPL **5** (1997) 539–563, `http://www.oup.co.uk/igpl/Volume_05/Issue_04/`.

[9] Hodges, W.: Some strange quantifiers. Structures in logic and computer science, ed. Mycielski, J. et al., Lecture Notes in Computer Science 1261, Springer, Berlin 1997, pp. 51–65.

[10] Hodges, W.: Formal features of compositionality. Journal of Logic, Language and Information (to appear).

[11] Kleitman, D.: On Dedekind's problem: the number of monotone boolean functions. Proc. Amer. Math. Soc. **21** (1969) 677–682.

[12] Lunnon, F.: The *IU* function: the size of a free distributive lattice. Combinatorial mathematics and its applications, ed. Welsh, D. J. A., Academic Press, London 1971, pp. 173–181.

[13] Wiedemann, D.: A computation of the eighth Dedekind number. Order **8** (1991) 5–6.