

A Compositional Model of MOS Circuits

by

Glynn Winskel

University of Cambridge,
Computer Laboratory,
Corn Exchange Street,
Cambridge CB2 3QG
England.

1. Introduction.

This paper describes a compositional model for MOS circuits. Following Bryant in [1] it covers some effects of capacitance and resistance used frequently in designs. Bryant's model has formed the basis of several hardware simulators. From the point of view of verification, however, it suffers the inadequacy that it is not compositional, an expression which will be explained further. This makes it hard to use the model to reason in a structured way.

In this paper we shall restrict our attention to the static behaviour of circuits. Roughly, a circuit's behaviour will be represented as the set of possible steady (or stable) states the circuit can settle into, ignoring oscillatory behaviour. Certainly a good understanding of such static behaviour is necessary in order to treat sequential circuits where the clock is taken to be slow enough so that one circuit settles into a steady state between changes. Because sequential circuits often use capacitance to precharge isolated parts of a circuit we shall include a treatment of charge sources due to capacitance in our analysis of static behaviour. Unfortunately while the model appears to generalise well to sequential circuits when all the memory is dynamic, there are difficulties describing static memory correctly. This problem is discussed in the concluding section. Note that Bryant can avoid this problem because a simulator need only produce one possible sequence of steady states of a circuit. The difficulty comes in accounting for *all* possible behaviours. While the model introduced here owes a great deal to Bryant's work, the reader is warned that we have not stuck closely to Bryant's development or terminology.

We take the view that it is useful to have a language to describe the construction of circuits. A term in the language describes a circuit and the term's structure can be used to direct reasoning about the circuit's behaviour. Naturally there should be atomic terms for basic components like transistors and then these are composed together using operations.

As a guide in choosing the operations, we borrow ideas from CCS and CSP [7, 5]. A circuit can be viewed as a process which communicates with its environment at its connection points. Assuming the connection points are named we can compose two circuits by connecting them at those points with names in common. In this way we can construct large circuits from smaller ones. Often once a connection point has been used to connect circuits we no

longer want to connect to it, so remove its name, and in effect hide, or insulate, the point.

To summarise and make this more precise, a circuit is to be associated with a set of connection points which are named; the set of such points we shall call the *sort* of the circuit. There is an operation of *composition* on circuits. Two circuits are composed by connecting those points which share the same name. The sort of composition is thus the union of the sorts of its two constituent circuits. There is an operation of *hiding*; we can cease regarding a point of a circuit as a connecting point and remove its name. The sort of the resulting circuit is thus the sort of the original circuit with the name of the hidden point removed. These two operations, with atomic terms for basic components, will generate a language whose terms describe circuits.

To define the language, we assume a countably infinite set of *point names* Π , ranged over by $\alpha, \beta, \gamma, \dots$, and a set of capacitance strengths K , with typical element k , and conductance strengths G , with typical element g . Strengths will give a qualitative measure of the relative sizes of basic devices in a way to be explained. The syntax of the language is given by:

$$\begin{aligned}
 c ::= & Pow(\alpha) \mid Gnd(\alpha) \mid \\
 & cap_{kH}(\alpha) \mid cap_{kL}(\alpha) \mid \\
 & pt(\alpha) \mid wre(\alpha, \beta) \mid res_g(\alpha, \beta) \mid \\
 & ntran(\alpha, \beta, \gamma) \mid ptran(\alpha, \beta, \gamma) \mid \\
 & c \bullet c \mid c \setminus \alpha.
 \end{aligned}$$

In the terms $wre(\alpha, \beta)$, $res_g(\alpha, \beta)$, $ntran(\alpha, \beta, \gamma)$, and $ptran(\alpha, \beta, \gamma)$ we insist that the points α, β, γ are distinct; so in these basic devices names are associated with unique connection points, a property that is inherited by any circuit described a compound term. Circuits are built up by composition; the term $c_0 \bullet c_1$ represents the composition of the circuits represented by c_0 and c_1 . Hiding a point α in a circuit described by c is represented by the term $c \setminus \alpha$. The atomic term $Pow(\alpha)$ stands for a power source connected to the point α , while $Gnd(\alpha)$ stands a connection to ground at α . We shall draw these as

$$Pow(\alpha) : \alpha \bullet \textcircled{H} \qquad Gnd(\alpha) : \alpha \bullet \textcircled{L}$$

where the H signifies that power provides a high value of voltage and L that ground provides a low value. Another kind of source arises through charge storage. The term $cap_{kH}(\alpha)$ represents a capacitance of strength k , charged high, connected to point α at one end and to ground at the other. The term $cap_{kL}(\alpha)$ is a similar capacitance but charged low. They are drawn as:

$$cap_{kH}(\alpha) : \alpha \bullet \begin{array}{c} H \\ | \\ | \\ | \\ k \end{array} \qquad cap_{kL}(\alpha) : \alpha \bullet \begin{array}{c} L \\ | \\ | \\ | \\ k \end{array}$$

Note that all the capacitance terms we consider are associated with only one connection point because they are to be used simply as a sources of charge.

The terms $pt(\alpha)$, $wre(\alpha, \beta)$ and $res_g(\alpha, \beta)$ are various forms of connectors. The simplest is $pt(\alpha)$, a point named α . The term $wre(\alpha, \beta)$ represents a wire connecting points α and β while the term $res_g(\alpha, \beta)$ stands for a resistance with conductance strength $g \in G$ connecting points α and β —it is intended to model components like d-type transistors or be included in situations where resistance effects may count. We shall draw points, wires and resistances as:

$$pt(\alpha) : \bullet\alpha \qquad wre(\alpha, \beta) : \alpha \text{---} \bullet\beta \qquad res_g(\alpha, \beta) : \alpha \text{---} \sqrt{g} \text{---} \bullet\beta$$

The term $ntran(\alpha, \beta, \gamma)$ stands for an n-type transistor with a gate γ which when it is high connects points α and β with perfect conductance. The term $ptran(\alpha, \beta, \gamma)$ stands for a p-type transistor with a gate γ which connects points α and β , again with perfect conductance, when the gate γ is low. We draw transistors as:

$$ntran(\alpha, \beta, \gamma) : \alpha \text{---} \begin{array}{c} \gamma \\ | \\ \text{---} \\ | \\ \bullet\beta \end{array} \qquad ptran(\alpha, \beta, \gamma) : \alpha \text{---} \begin{array}{c} \gamma \\ | \\ \text{---} \\ | \\ \bullet\beta \end{array}$$

Should the effect of resistance be significant we can insert a suitable resistance between α and β , and, should the capacitance of the gate be significant, capacitances can be connected to model this. This is an idealised model of a transistor. It treats transistors as switches and ignores the fact that in reality transistors have thresholds (see section 4).

We explain the idea of qualitative strength on which Bryant's model and ours, which follows his, are based. The capacitance strengths K are assumed to form a finite totally ordered set, to which we adjoin a least element 0,

$$0 < k_1 < k_2 < \dots < k_m.$$

(It seems most MOS designs can be described with $m = 3$.) The capacitances in a design are assigned a strength which says how they combine with other capacitances. The value 0 corresponds to negligible capacitance. The meaning of $k < k'$ in the strength order is that a capacitance assigned strength k is negligible with respect to one assigned strength k' . More exactly, the assumption made of the strength order can be stated: if a capacitance of strength k is combined with one of strength k' the result is equivalent to a capacitance of strength the maximum of k and k' . Accordingly, if a capacitance of strength k is charged low and connected to one of strength k' charged high, the result is, in effect, a capacitance of strength k' charged high. Accompanying this, if neither of two capacitances can be guaranteed to override the other, they are assigned the same strength.

Of course, a problem arises with this somewhat naive explanation. Two capacitances of the same strength k should combine to give a capacitance of strength k ; the capacitance of one alone is not negligible relative to that of the combination. But if we combine many capacitances of the same strength k the result may not be a capacitance of strength k ; it may not be negligible relative to one of strength k' even though $k < k'$. Still, for any particular

circuit term, the number of such combinations is bounded. It follows that, with respect to a particular circuit term, we can interpret capacitance strengths so that when capacitance of strength k combines with one of strength k' the result is a capacitance of strength the maximum of k and k' . In more detail, there is a small number $\epsilon < 1$, dependent on the circuit term, so that we can interpret the capacitance strengths as intervals of positive real numbers (capacitance values)

$${}^{\circ}0^{\circ}, {}^{\circ}k_1^{\circ}, \dots, {}^{\circ}k_i^{\circ}, \dots, {}^{\circ}k_{i+i}^{\circ}, \dots, {}^{\circ}k_m^{\circ},$$

where ${}^{\circ}k^{\circ}$ represents an interval $({}^{\circ}k, k^{\circ})$ with end points ${}^{\circ}k < k^{\circ}$, so

$$\frac{k_i^{\circ}}{{}^{\circ}k_{i+1}^{\circ}} < \epsilon$$

for $0 \leq i < m$. With respect to this interpretation a capacitance value C has strength k if $C \in {}^{\circ}k^{\circ}$. By taking the intervals ${}^{\circ}k^{\circ}$ wide enough and the number ϵ small enough there are choices of capacitances for the basic components $cap_k(\alpha)$ which ensure the assumptions of the strength order are never invalidated by compositions in the term.

To see how capacitances compose, assume a capacitance of size C , charged low to a voltage v with charge Q , is connected to a capacitance C' , charged high to voltage v' with charge Q' . From the equation $Q = vC$, relating charge to voltage and capacitance, we see

$$v_{res} = \frac{Q + Q'}{C + C'}.$$

If now we assume C has strength k , and C' strength k' with $k < k'$ we know $C/C' < \epsilon$. By Taylor's theorem we derive

$$v_{res} = v' - (v' - v)\left(\frac{C}{C'} - \left(\frac{C}{C'}\right)^2 + \text{higher order terms}\right).$$

Hence v_{res} is to within $\epsilon(v' - v)$ of v' . We cannot conclude, in general, that if v' is high then v_{res} is high also. However, because the number of compositions of capacitances in a term is bounded, we can choose ϵ small enough so that whenever such a composition occurs in the circuit described by the term the resultant voltage is high.

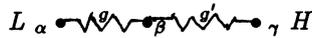
There is a similar strength order on conductances G of resistances, again assumed finite, to which is adjoined a maximum element ∞ ,

$$g_1 < g_2 < \dots < g_n < \infty.$$

(For most MOS designs $n = 3$ appears to be sufficient). Resistances are assigned a conductance strength so that a resistance of strength g' , with $g < g'$, is negligible with respect to one of strength g . Wires are assumed to have perfect

conductance and are given the special conductance strength ∞ , which we take to dominate all other conductances.

Consider the situation



where a point β is connected both to ground at α via a resistance of conductance strength g and to power at γ via a resistance of strength g' . Then $g < g'$ means the value through the stronger conductance will dominate so the resulting value will be high. A simple application of Ohm's law explains how this can arise. Suppose the resistance of strength g has value R ohms and that of strength g' is relatively small, of value r ohms say. Let $v_\alpha, v_\beta, v_\gamma$ be the voltages at the corresponding points. By Ohm's law

$$\frac{v_\gamma - v_\beta}{v_\beta - v_\alpha} = \frac{Ir}{IR} = \frac{r}{R}.$$

Ensuring R is large relative to r ensures $v_\gamma - v_\beta$ is small enough so that v_β is close to the voltage v_γ and so high. Taking R large relative to r corresponds to R being associated with a conductance strength g , r with g' , and $g < g'$. Similar arguments using Ohm's law give the conductance strengths of resistances in series and in parallel. If two resistances R and R' of strength g and g' are connected in series the resulting resistance $R + R'$ should be assigned conductance strength the *minimum* of g and g' . This is because, for example, if R'/R is very small then so is $R'/(R + R')$. Connected in parallel their resulting resistance, $RR'/(R + R')$, should be assigned strength the *maximum* of g and g' .

Such simplistic arguments suggest that if we connect arbitrarily many resistances of the same conductance strength g in parallel, or in series, the result will be equivalent to a resistance of strength g . This is clearly unrealistic in general, but with respect to any particular circuit term the number of such compositions is bounded so the assumptions needed for the strength order can be met. More precisely, with respect to the particular circuit term, the conductance strengths can be interpreted as intervals of resistance values so the properties required of the strength order hold in the circuit. The method is similar to that sketched for capacitances.

As we have explained, these qualitative orders of strengths are to be understood abstractly. The orders of capacitance and conductance strengths are only to be interpreted as referring to particular intervals of real numbers when the circuit description has been completed. The simple, seemingly naive, assumptions of the strength orders, on which the design is based, can be realised. Design, simulation and reasoning at the more abstract qualitative level postpones consideration of the exact sizes of capacitances and resistances, though, of course, they have to be dealt with at some stage before layout. It is a formidable research problem to bring these physical aspects within the domain of hardware verification. The difficulty is perhaps not so much that of not being able to solve a particular differential equation, as that of finding techniques

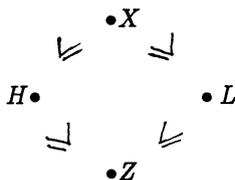
which bridge between different levels of description. These are necessary to fulfil the ultimate goal and make the verification of real devices feasible, based only on the assumption that the layout is done correctly.

Our aim is to build a model for the behaviour of circuits described by our language so that the behaviour of a term $c_0 \bullet c_1$ is derived solely from the behaviours of c_0 and c_1 , and similarly the behaviour of $c \setminus \alpha$ is derived solely from that of c . The advantage of a model like this is that proving a property of $c_0 \bullet c_1$, for instance, reduces to proving properties of c_0 and c_1 ; proof is directed by the algebraic structure of the terms. On such a compositional model it is possible to build a compositional proof system, a goal realised in [10]. Such an approach should be distinguished from that in [1]; the model and simulators of Bryant use a graphical representation of the whole circuit. Obtaining a compositional model is surprisingly involved. It rests on a detailed analysis of the idea of state necessary to support compositionality, and leads to the definition of a static configuration of a circuit.

2. Static Configurations.

A circuit computes by imposing a relation between the voltage values at its points, values which can often be assumed to be high (abbreviated to H) or low (abbreviated to L). A point takes the value H if it is only connected to sources of positive charge, like a power source or a positively charged capacitance, perhaps through resistances. It takes the value L if it is only connected to sources of negative charges. Sometimes, however, a point may take a voltage value which cannot be classified as H or L . For example, a point may be connected to both a power source and ground through resistances of roughly the same magnitude, or perhaps to two capacitances of roughly the same size but initially charged with opposite polarities. In either case the point cannot be assumed to have value H or L and so instead we take it to have the value X . It is useful to consider another case, that in which a point is not connected to any significant sources of charge. To such an isolated point we associate the value Z .

It may be helpful to think of the value X as the set $\{high, low\}$ because the value X results from a point being simultaneously connected to a source of high and low. Accordingly the value H can be identified with the singleton set $\{high\}$, similarly L with $\{low\}$, and Z with the empty set \emptyset (Z is the value due to not being connected to any source at all). With this representation the inclusion order induces the following lattice \mathbf{V} of values.



Thus X is the least upper bound of H and L with respect to the order \leq . We shall write $w_0 + w_1$ for the least upper bound of a pair of values w_0 and w_1 and, in general, we shall use ΣW for the least upper bound of a set of values W .

As has been said, the behaviour of a circuit will be represented as the set of steady states it can adopt. Because we wish to derive the behaviour of the composition $c_0 \bullet c_1$ of two circuits c_0, c_1 from the behaviour of c_0 and c_1 we cannot consider just those steady states which arise from the circuit in isolation, but must also take account of the steady states which can arise in composition with other circuits—clearly the behaviour of a transistor depends on what its gate is connected to. We shall use the expression “steady state” of a circuit to mean a stable state which the circuit can adopt in some environment. We are left with the task of formalising the notion of *static configuration*, where a static configuration consists of those attributes of a steady state which are relevant, in a sense we now make precise.

In its formalisation, the choice of those attributes which are relevant will be guided by the operations, composition and hiding, which we wish to perform on circuits. For composition, we require that the static configurations of a composition $c_0 \bullet c_1$ of two circuit should be determined by the static configurations of c_0 and c_1 . For hiding, we require that the static configurations of the circuit $c \setminus \alpha$ formed by hiding the point α in the circuit c are determined by the static configurations of c .

At first sight it might appear that a static configuration of a circuit of sort Λ should be simply a *value function* $V : \Lambda \rightarrow \mathbf{V}$ giving the values of a steady state in some environment. However, not surprisingly, this fails to account for differences in behaviour due to effects of capacitance and conductance strength. A connection to a positively charged capacitance and another to a power source, have the same value functions and yet behave differently in the same context. Consider the two forms of sources

$$s_0 \equiv cap_{kL}(\gamma) \quad \text{and} \quad s_1 \equiv (Gnd(\delta) \bullet res_g(\delta, \gamma)) \setminus \delta,$$

where k is a capacitance strength and g a conductance strength. (We use the relation \equiv to mean syntactic equality, so *e.g.* s_0 abbreviates the term to its right.) Both sources can be put in environments leading to values H, L, X at the point γ , and hence they are associated with the same value functions. But placing both in the same context,

$$C[-] \equiv (- \bullet ntran(\alpha, \beta, \gamma) \bullet res_g(\gamma, \epsilon) \bullet Pow(\epsilon)) \setminus \epsilon \setminus \gamma, \quad (*)$$

we obtain circuits $C[s_0]$ and $C[s_1]$ which have different value functions.



The transistor in $C[s_1]$ may be disconnecting because it has the value X on its gate so there is a steady state of the circuit which has a value function V with $V(\alpha) = L$ and $V(\beta) = H$; the transistor in $C[s_0]$ must be connecting in any steady state because the power source will override the stored charge and this ensures $V(\alpha) = V(\beta)$, ruling out the possibility of $V(\alpha) = L$ and $V(\beta) = H$, for the value function of any steady state.

This example shows that static configurations should consist of further attributes in addition to just value functions; only then can it be possible to derive the value functions, and so the static configurations, of a compound circuit from those of its components. Furthermore, it shows there is a need for an attribute which expresses the degree to which values are secured at points. It motivates the introduction of a *strength function* $S : A \rightarrow \mathbf{S}$, where \mathbf{S} is a set of strengths got by adjoining two elements 0 and ∞ to K and G . This is an attribute of the steady state of a circuit of sort A . A point α of a circuit in a steady state is not only associated with a value $V(\alpha)$ but is also associated with a strength $S(\alpha)$. If the point α has value $V(\alpha) = Z$ then it is assigned strength $S(\alpha) = 0$. Otherwise it either receives its value from capacitances of strength k or from power and ground via paths of conductance strength g (including ∞). It cannot receive contributions to its value $V(\alpha)$ from capacitances of different strengths or via paths of different conductance strengths by the assumptions of the strength orders. Nor can it receive contributions from both capacitances and power or ground, because then in a steady state the stored charge would drain away or be overridden. Hence the point α is associated with a unique strength in $K \cup G \cup \{0, \infty\}$, and this we take to be $S(\alpha)$.

It is useful to incorporate both the order on capacitances and that on conductances into a single order to reflect the fact that whenever a charged capacitance is connected to power or ground through even a fairly weak conductance the finite charge stored on the capacitance is eventually overridden, and makes no contribution to the values in a steady state. We arrive at the concept of the *strength order*

$$0 < k_1 < \dots < k_m < g_1 < \dots < g_n < \infty.$$

which contains 0 , the zero strength, to stand for the strength of a negligible capacitance or negligible conductance, and ∞ , the strength of a perfect conductance. As notation for later, we shall use $s \cdot s'$ for the minimum and $s + s'$ for the maximum of two strengths s and s' . Now, for example, we can say that the strength of the point β in $cap_{kH}(\alpha) \bullet res_g(\alpha, \beta) \setminus \alpha$ will be $S(\beta) \geq k$ in any steady state. It is possible to have a steady state in which $S(\beta) = k$ if it is not connected to any stronger source in the environment, while it is possible that $S(\beta) > k$ for a steady state in an environment where β is connected to a stronger capacitance, or source of power or ground via a conductance. In all the steady states of $Pow(\alpha) \bullet res_g(\alpha, \beta) \setminus \alpha$, the point β will have strength $S(\beta) \geq g$. If it is connected to a source in the environment via a conductance of strength greater than g it will have strength $S(\beta) > g$.

Are the attributes of value function and strength function enough? Unfortunately not. To see this first define an “X-source”

$$x \equiv cap_{kH}(\epsilon) \bullet cap_{kL}(\epsilon)$$

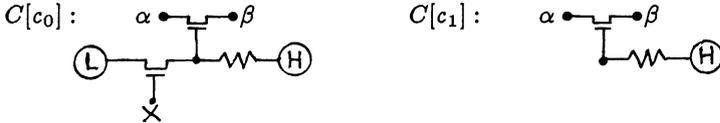
which standing alone gives rise to value X at the point ϵ . If we compose x with a transistor with gate ϵ and then hide ϵ there are two possibilities; the transistor may be connecting or disconnecting. Hence in the term

$$c_0 \equiv (Gnd(\delta) \bullet ntran(\delta, \gamma, \epsilon) \bullet x) \setminus \delta \setminus \epsilon$$

the single unhidden point γ may or may not be connected to ground. Consequently the value and strength functions of steady states of the circuit c_0 in an environment coincide with those of the simple circuit

$$c_1 \equiv pt(\gamma)$$

consisting of a single point. However c_0 and c_1 behave differently in the context $C[-]$ given by (*) above.



In the circuit $C[c_0]$ there is the possibility that the point γ will be pulled low, disconnecting α and β ; it is therefore possible for their values to be different in the same steady state. In the circuit $C[c_1]$ there is no such possibility and the points α and β must be connected and so share a common value.

This example highlights the need for a further attribute which distinguishes the circuits c_0 and c_1 . Of course c_0 has an internal source while c_1 does not. An extra attribute called the *internal-value function* marks the contribution to the value function which is due to paths of conductance from internal sources. A steady state of a circuit of sort Λ has an internal-value function $I : \Lambda \rightarrow \mathbf{V}$ which to a point α in Λ associates the part $I(\alpha)$ of the value $V(\alpha)$ which is maintained by sources built into the circuit; so naturally $I(\alpha) \leq V(\alpha)$.

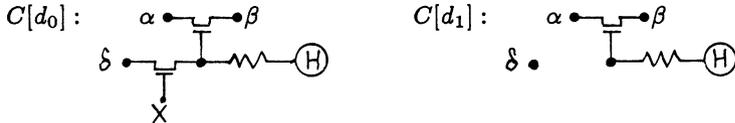
A further attribute is necessary. There are two circuits whose steady states are identical as far as their attributes of value, strength and internal-value are concerned, and yet behave differently in the same context. Let

$$d_0 \equiv (ntran(\delta, \gamma, \epsilon) \bullet x) \setminus \epsilon,$$

which connects the X -source x to the gate of a transistor. So d_0 may behave like a wire between δ and γ , or two disconnected points δ and γ . Let d_1 consist just of two disconnected points, so

$$d_1 \equiv pt(\delta) \bullet pt(\gamma).$$

Consider a steady state of d_0 . There are no internal sources in d_0 so its internal-value function will satisfy $I(\delta) = I(\gamma) = Z$. If the transistor is connecting the strength and value function will have to be the same and otherwise not. Hence for any steady state of d_0 there will be a steady state of d_1 with the same attributes. Conversely, any such attributes of a steady state of d_1 will be shared by a steady state of d_0 . With respect to the three attributes we have introduced so far the circuits d_0 and d_1 are the same. But they behave differently in the context $C[-]$ given by (*) above.



The argument is similar to that for introducing the internal-value function. In the circuit $C[d_0]$ there is the possibility that the point γ will be pulled low through the circuit being placed in an environment where δ is connected directly to ground. This would disconnect α and β so that their values can be different. In the circuit $C[d_1]$ there is no such possibility and the points α and β must be connected and their values the same.

The final attribute we introduce is one to express a generalised form of connectivity. It is the fact that in the two circuits d_0 has the possibility that δ and γ are connected and d_1 not, which accounts for their different behaviour in the same context. However, because of strengths, values do not effect one another symmetrically across a resistance, so the relation \rightsquigarrow we introduce will not be symmetric in general, although it will be reflexive and transitive.

To motivate the relation \rightsquigarrow , consider how values effect eachother across a resistance $res_g(\alpha, \beta)$. First note that in any steady state

$$S(\alpha) \cdot g \leq S(\beta).$$

If $S(\alpha) = k$, a capacitance strength, then α receives its value from capacitances of strength k and cannot be linked to power or ground. The point β is connected to α by the resistance and so receives its value from the same capacitances. Its strength, $S(\beta)$ is equal to k too. In this case $S(\alpha) \cdot g \leq S(\beta)$. If $S(\alpha) = g'$, a conductance strength, then α must receive its value from power or ground via paths of conductance strength g' . In series with the resistance from α to β these form paths of conductance strength $g \cdot g'$. Hence $S(\alpha) \cdot g = g' \cdot g \leq S(\beta)$ in this case. The relation $\alpha \rightsquigarrow_1 \beta$ is taken to hold for a steady state of $res_g(\alpha, \beta)$ iff

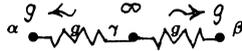
$$S(\alpha) \cdot g = S(\beta).$$

If $S(\alpha) \cdot g = S(\beta)$ the value at α effects the value at β so $V(\alpha) \leq V(\beta)$ and $I(\alpha) \leq I(\beta)$, whereas if $S(\alpha) \cdot g < S(\beta)$ it is overridden. More generally, we shall take the $\alpha \rightsquigarrow \beta$ to be true in a steady state of any circuit if the points α and β are equal or connected by any path

$$\alpha \rightsquigarrow_1 \gamma_1 \rightsquigarrow_1 \dots \rightsquigarrow_1 \gamma_u \rightsquigarrow_1 \beta.$$

A steady state of a circuit of sort Λ has a flow relation $\rightsquigarrow: \Lambda \times \Lambda$ which, when it relates two points $\alpha \rightsquigarrow \beta$, ensures that values at α contribute to those at β so that $V(\alpha) \leq V(\beta)$, and also $I(\alpha) \leq I(\beta)$.

Example. Consider a steady state of $res_g(\alpha, \gamma) \bullet res_g(\gamma, \beta)$ in which $S(\alpha) = S(\beta) = g$ and $S(\gamma) = \infty$. Then we have $\gamma \rightsquigarrow \alpha$ and $\gamma \rightsquigarrow \beta$ but not $\alpha \rightsquigarrow \gamma$ or $\beta \rightsquigarrow \gamma$.



This shows that conducting paths, in the sense of paths conducting values, are not just chains of resistances according to this model; here there is a chain of conductances between α and β and yet no flow relation between them. In Bryant's words the path is "blocked" through the point γ having a higher strength than the endpoints α and β . Despite the chain of resistances linking α to β they are effectively disconnected, and the value at one point does not effect the value at the other. Connecting two resistances in series between two points, without hiding the connection point, is not equivalent to, nor does it imply, the effect of putting a resistance between them (a phenomenon analogous to that due to interruption points in parallel programs). It is partly for this reason that the model is based on the relation \rightsquigarrow rather than on conductance matrices.

All these arguments suggest the form of a static configuration of a circuit of sort Λ ; it should consist of a strength, value function, internal-value function and a flow relation. Of course it remains to detail the axioms which relate the different attributes, and later to demonstrate that the attributes are sufficient to give a compositional model for the static behaviour of circuits.

Definition. Let Λ be a set of points in Π . A static configuration of sort Λ is a structure

$$\langle S, V, I, \rightsquigarrow \rangle$$

where

- $S: \Lambda \rightarrow \mathbf{S}$ (the strength function),
- $V: \Lambda \rightarrow \mathbf{V}$ (the value function),
- $I: \Lambda \rightarrow \mathbf{V}$ (the internal value function) and
- \rightsquigarrow is a reflexive, transitive relation on Λ (the flow relation),

which satisfy

- (i) $S(\alpha) = 0 \leftrightarrow V(\alpha) = \emptyset$,
- (ii) $I(\alpha) \leq V(\alpha)$,
- (iii) $\alpha \rightsquigarrow \beta \rightarrow S(\alpha) \geq S(\beta)$,
- (iv) $\alpha \rightsquigarrow \beta \rightarrow I(\alpha) \leq I(\beta) \wedge V(\alpha) \leq V\beta$,
- (iii) $\alpha \rightsquigarrow \beta \wedge S(\beta) \in K \cup \{0\} \rightarrow S(\alpha) = S(\beta)$,
- (vi) $\alpha \rightsquigarrow \beta \wedge S(\alpha) = S(\beta) \rightarrow \beta \rightsquigarrow \alpha$.

for any points α, β in Λ .

Write $\text{sort}(\sigma)$ for the sort of a configuration σ . Write $\text{Sta}[\Lambda]$ for the set of static configurations of sort Λ , and Sta for the set of all static configurations.

Most of the properties have appeared in the earlier discussion, but it is worth commenting on why they hold again. Property (i) says a signal of no

strength has value Z and *vice versa*; this fits the interpretations of 0 as minimum strength and Z as negligible value. Naturally the contribution to the value from internal sources cannot exceed the resultant value—property (ii). Property (iii) says flow cannot go from a point at weaker strength to a point at greater strength. This is clear by considering how a relation $\alpha \rightsquigarrow \beta$ is built out of a chain of relations $\alpha \rightsquigarrow_1 \dots \rightsquigarrow_1 \beta$ and noting (iii) holds across each single step \rightsquigarrow_1 . Property (iv) formalises the idea that \rightsquigarrow represents the direction in which values at points contribute to values at other points. The property (v) states that if $\alpha \rightsquigarrow \beta$ and $S(\beta)$ is a capacitance strength then $S(\alpha)$ is the same strength. This follows as capacitance strengths are always ranked below those of conductance in the strength order. Assume $\alpha \rightsquigarrow_1 \beta$ and $S(\beta) \in K$. Then $S(\alpha) \cdot g = S(\beta)$ for some conductance strength g for which $S(\beta) \leq g$. This can only occur with $S(\alpha) = S(\beta)$. The property follows when $\alpha \rightsquigarrow \beta$ because this relation is built out of steps \rightsquigarrow_1 . Property (vi) follows in a similar way. It expresses the fact that if $\alpha \rightsquigarrow \beta$ and α and β are at the same strength then $\beta \rightsquigarrow \alpha$, so α and β are connected. To justify (vi) assume that $\alpha \rightsquigarrow_1 \beta$ and $S(\alpha) = S(\beta)$. Then $\alpha \rightsquigarrow_1 \beta$ arises iff there is a conductance, of strength g say, between α and β so that $S(\alpha) \cdot g = S(\beta)$. Hence $S(\beta) \cdot g = S(\alpha)$ too making $\beta \rightsquigarrow_1 \alpha$.

There are sufficiently many axioms, and the idea of static configuration sufficiently complicated, to raise the question of their completeness—do static configurations all share some property that does not follow from the axioms (i)–(vi)? We have argued for their soundness. To show completeness we need an argument showing that there are no properties shared by all static configurations of circuit terms which do not follow from those written down in the definition. Later, we shall show that every structure $\langle S, V, I, \rightsquigarrow \rangle$ on a finite set of points which satisfies all the axioms (i)–(vi) can be realised as the static configuration of a circuit built-up from resistances and sources connected to those points. Then any property of structures $\langle S, V, I, \rightsquigarrow \rangle$ which holds of all static configurations of circuits must also hold of all finite structures satisfying the definition above.

In a static configuration, two points α and β may be both in the relation $\alpha \rightsquigarrow \beta$ and $\beta \rightsquigarrow \alpha$. In this case the points α and β must have the same S, V and I values. Sometimes neither $\alpha \rightsquigarrow \beta$ nor $\beta \rightsquigarrow \alpha$, *i.e.* the two points are incomparable with respect to the flow relation \rightsquigarrow . This means that the points are effectively disconnected. We introduce notation to describe these circumstances.

Definition. Let $\sigma = \langle S, V, I, \rightsquigarrow \rangle$ be a static configuration of sort Λ . For $\alpha, \beta \in \Lambda$ define

$$\begin{aligned} \alpha \sim \beta &\equiv \alpha \rightsquigarrow \beta \wedge \beta \rightsquigarrow \alpha \\ \alpha \parallel \beta &\equiv \neg(\alpha \rightsquigarrow \beta) \wedge \neg(\beta \rightsquigarrow \alpha). \end{aligned}$$

In the special case where the effects of resistance are ignored there is only one perfect conductance strength ∞ , the flow relation \rightsquigarrow coincides with

the equivalence relation \sim . In this situation any two points are either connected or disconnected.

Proposition. *Assume a static configuration σ has the property that for all points x in the sort of σ , either $S(x) = 0$ or $S(x) = \infty$. Then in σ the relation \rightsquigarrow is symmetric and so an equivalence relation on points with $x \rightsquigarrow y$ iff $x \sim y$ for all points x, y of σ .*

Proof. The proof is a little exercise in using the axioms which define a static configuration. ■

Now we present the obvious first-order syntax for describing static configurations. Static configurations are structures $\sigma = \langle S, V, I, \rightsquigarrow \rangle$. As such they can be described by predicates based on the functions S, V, I , relation \rightsquigarrow together with relations of equality. The axioms for static configurations are examples of the kind of predicate we have in mind. Also, for example, the predicate

$$(V(\gamma) = H) \rightarrow (\alpha \rightsquigarrow \beta \wedge \beta \rightsquigarrow \alpha)$$

which is true of all those static configurations where if the point γ is high then the points α and β are connected. As this predicate suggests, such assertions will be useful for giving the meaning of circuit terms as sets of static configurations and for specifying their behaviour. The treatment is a little different from that usual for predicate calculus because we shall allow point names in assertions which apply to static configurations where the names do not appear in the sort. However variables bound by quantifiers only range over points in the sort. Actually we are presenting a simple example of a “free logic” where terms need not necessarily denote; it is of the kind discussed in [8] for instance.

Notation. Because we shall work with partial functions, mathematical expressions may sometimes be undefined. We indicate a mathematical expression e is defined by writing $e \downarrow$.

We first present the formal syntax of the language.

The syntax of assertions: *Variables:* We assume a set of variables Var which range over points Π , and have typical members x, y, z, \dots .

Value terms: Terms, denoting values in $\{H, L, Z, X\}$ have the form

$$t ::= H \mid L \mid Z \mid X \mid V(\pi) \mid I(\pi),$$

where π is a point term, *i.e.* an element of Π or a variable in Var .

Strength terms: Terms, denoting values in $\mathbf{S} = K \cup G \cup \{0, \infty\}$ have the form

$$e ::= s \mid S(\pi) \mid e \cdot e \mid e + e$$

where $s \in \mathbf{S}$, and π is a point term.

Assertions for static configurations: The set of assertions is generated by

$$\begin{aligned} \phi ::= & \pi_0 = \pi_1 \mid \pi_0 \rightsquigarrow \pi_1 \mid \\ & t_0 = t_1 \mid t_0 \leq t_1 \mid \\ & e_0 = e_1 \mid e_0 \leq e_1 \mid \\ & \text{tt} \mid \text{ff} \mid \phi \wedge \phi \mid \phi \vee \phi \mid \neg \phi \mid \\ & \exists x. \phi \mid \forall x. \phi \end{aligned}$$

where π_0, π_1 are point terms, t_0, t_1 are value terms and e_0, e_1 are strength terms. We shall regard $\phi \rightarrow \theta$ as abbreviating $\neg\phi \vee \theta$ and $\phi \leftrightarrow \theta$ as abbreviating $\phi \rightarrow \theta \wedge \theta \rightarrow \phi$, and use previously introduced abbreviations like $x \sim y$ for $x \rightsquigarrow y \wedge y \rightsquigarrow x$.

The semantics of assertions: We give the semantics of closed assertions. For brevity, assume a static configuration σ has the form $\langle S_\sigma, V_\sigma, I_\sigma, \rightsquigarrow_\sigma \rangle$. First we treat value terms which are denoted by partial functions $\text{Sta} \rightarrow \mathbf{V}$, as follows:

$$\begin{aligned} \llbracket H \rrbracket \sigma &= H \text{ for all } \sigma \in \text{Sta} \\ \llbracket L \rrbracket \sigma &= L \text{ for all } \sigma \in \text{Sta} \\ \llbracket Z \rrbracket \sigma &= Z \text{ for all } \sigma \in \text{Sta} \\ \llbracket X \rrbracket \sigma &= X \text{ for all } \sigma \in \text{Sta} \\ \llbracket V(\alpha) \rrbracket \sigma &= \begin{cases} V_\sigma(\alpha) & \text{if } \sigma \in \text{Sta} \text{ and } \alpha \in \text{sort}(\sigma), \\ \text{undefined} & \text{otherwise,} \end{cases} \\ \llbracket I(\alpha) \rrbracket \sigma &= \begin{cases} I_\sigma(\alpha) & \text{if } \sigma \in \text{Sta} \text{ and } \alpha \in \text{sort}(\sigma), \\ \text{undefined} & \text{otherwise.} \end{cases} \end{aligned}$$

Strength terms are denoted by partial functions $\text{Sta} \rightarrow \mathbf{S}$, as follows:

$$\begin{aligned} \llbracket s \rrbracket \sigma &= s \text{ for all } \sigma \in \text{Sta} \\ \llbracket S(\alpha) \rrbracket \sigma &= \begin{cases} S_\sigma(\alpha) & \text{if } \sigma \in \text{Sta} \text{ and } \alpha \in \text{sort}(\sigma), \\ \text{undefined} & \text{otherwise,} \end{cases} \\ \llbracket e_0 \cdot e_1 \rrbracket \sigma &= \begin{cases} s_0 \cdot s_1 & \text{if } \llbracket e_0 \rrbracket \sigma = s_0 \text{ and } \llbracket e_1 \rrbracket \sigma = s_1 \\ \text{undefined} & \text{otherwise,} \end{cases} \\ \llbracket e_0 + e_1 \rrbracket \sigma &= \begin{cases} s_0 + s_1 & \text{if } \llbracket e_0 \rrbracket \sigma = s_0 \text{ and } \llbracket e_1 \rrbracket \sigma = s_1 \\ \text{undefined} & \text{otherwise.} \end{cases} \end{aligned}$$

Each assertion is denoted by the subset of static configurations at which it is true, defined by the following induction on the length of assertions:

$$\begin{aligned} \llbracket \alpha_0 = \alpha_1 \rrbracket &= \{ \sigma \in \text{Sta} \mid \alpha_0 \in \text{sort}(\sigma) \text{ and } \alpha_1 \in \text{sort}(\sigma) \text{ and } \alpha_0 = \alpha_1 \} \\ \llbracket \alpha_0 \rightsquigarrow \alpha_1 \rrbracket &= \{ \sigma \in \text{Sta} \mid \alpha_0 \in \text{sort}(\sigma) \text{ and } \alpha_1 \in \text{sort}(\sigma) \text{ and } \alpha_0 \rightsquigarrow_\sigma \alpha_1 \} \\ \llbracket t_0 = t_1 \rrbracket &= \{ \sigma \in \text{Sta} \mid \llbracket t_0 \rrbracket \sigma \downarrow \text{ and } \llbracket t_1 \rrbracket \sigma \downarrow \text{ and } \llbracket t_0 \rrbracket \sigma = \llbracket t_1 \rrbracket \sigma \} \\ \llbracket t_0 \leq t_1 \rrbracket &= \{ \sigma \in \text{Sta} \mid \llbracket t_0 \rrbracket \sigma \downarrow \text{ and } \llbracket t_1 \rrbracket \sigma \downarrow \text{ and } \llbracket t_0 \rrbracket \sigma \leq \llbracket t_1 \rrbracket \sigma \} \\ \llbracket e_0 = e_1 \rrbracket &= \{ \sigma \in \text{Sta} \mid \llbracket e_0 \rrbracket \sigma \downarrow \text{ and } \llbracket e_1 \rrbracket \sigma \downarrow \text{ and } \llbracket e_0 \rrbracket \sigma = \llbracket e_1 \rrbracket \sigma \} \\ \llbracket e_0 \leq e_1 \rrbracket &= \{ \sigma \in \text{Sta} \mid \llbracket e_0 \rrbracket \sigma \downarrow \text{ and } \llbracket e_1 \rrbracket \sigma \downarrow \text{ and } \llbracket e_0 \rrbracket \sigma \leq \llbracket e_1 \rrbracket \sigma \} \\ \llbracket \text{tt} \rrbracket &= \text{Sta}, \quad \llbracket \text{ff} \rrbracket = \emptyset \\ \llbracket \phi_0 \wedge \phi_1 \rrbracket &= \llbracket \phi_0 \rrbracket \cap \llbracket \phi_1 \rrbracket \text{ and } \llbracket \phi_0 \vee \phi_1 \rrbracket = \llbracket \phi_0 \rrbracket \cup \llbracket \phi_1 \rrbracket \\ \llbracket \neg \phi \rrbracket &= (\text{Sta} \setminus \llbracket \phi \rrbracket) \\ \llbracket \exists x. \phi \rrbracket &= \{ \sigma \mid \exists \alpha \in \text{sort}(\sigma). \sigma \in \llbracket \phi[\alpha/x] \rrbracket \} \\ \llbracket \forall x. \phi \rrbracket &= \{ \sigma \mid \forall \alpha \in \text{sort}(\sigma). \sigma \in \llbracket \phi[\alpha/x] \rrbracket \} \end{aligned}$$

This completes our formal language for describing static configurations. We shall write $\sigma \models \phi$ iff $\sigma \in \llbracket \phi \rrbracket$. In fact, because of the completeness theorem for such (free) predicate calculi, there is a proof system very like that for ordinary predicate calculus so that $\phi_0 \vdash \phi_1$ (i.e. ϕ_1 can be proved from ϕ_0) iff $\llbracket \phi_0 \rrbracket \subseteq \llbracket \phi_1 \rrbracket$ (i.e. ϕ_0 entails ϕ_1)—see [10] for more details.

3. The Static Behaviour of Circuits.

It remains to give a semantics to circuit terms. Each circuit term is to be denoted by the set of static configurations it can be in. This depends on being able to characterise the static configurations of a circuit $c_0 \bullet c_1$ in terms of those of c_0 and c_1 , and the static configurations of a circuit $c \setminus \alpha$ in terms of those of c . The static configurations of c are its steady states in any environment. Hence a static configuration σ of $c_0 \bullet c_1$ should be obtained as a composition, call it $\sigma_0 \bullet \sigma_1$, of static configurations σ_0 of c and σ_1 of c_1 . We cannot expect all such compositions $\sigma_0 \bullet \sigma_1$ to make sense. Afterall, quite possibly σ_0 and σ_1 may disagree on the value $V(\alpha)$ or strength $S(\alpha)$ at a point in common to both their sorts. Similarly, a static configuration σ of $c \setminus \alpha$ should be obtained by restricting a static configuration ρ of c to sort $\text{sort}(\sigma) \setminus \{\alpha\}$ but only in the case where in ρ there is no essential contribution to the value $V(\alpha)$ through the point α . This motivates the introduction of partial functions of type

$$\begin{aligned} \bullet &: \text{Sta} \times \text{Sta} \rightarrow \text{Sta}, \\ \setminus \alpha &: \text{Sta} \rightarrow \text{Sta}, \end{aligned}$$

for any $\alpha \in \Pi$. The denotation of $c_0 \bullet c_1$ and $c \setminus \alpha$ will be derived from them.

Notation. Let $\Lambda \subseteq \Pi$. Write $\Lambda \setminus \alpha$ for $\Lambda \setminus \{\alpha\}$. Let $f : \Lambda \rightarrow U$ be a function on Λ . Write $f \setminus \alpha$ for $f \upharpoonright (\Lambda \setminus \alpha)$, the function restricted to $\Lambda \setminus \{\alpha\}$. Let $R \subseteq \Lambda \times \Lambda$ be a relation. Write $R \setminus \alpha$ for the restriction $R \cap (\Lambda \setminus \alpha)^2$.

Assume σ_0 is a static configuration of a circuit c_0 and σ_1 is a static configuration of a circuit c_1 . When can σ_0 and σ_1 be composed to give a static configuration of c_0 and c_1 ? When their strengths and values agree at common points; only then do σ_0 and σ_1 make consistent assumptions about the environment. Then the resulting flow relation should be the transitive closure of the flow relations in the components and the internal-value function should be spread out accordingly.

Definition. Let $\sigma_0 = \langle S_0, V_0, I_0, \rightsquigarrow_0 \rangle$ be a static configuration of sort Λ_0 and $\sigma_1 = \langle S_1, V_1, I_1, \rightsquigarrow_1 \rangle$ be a static configuration of sort Λ_1 . Define their *composition* to be

$$\sigma_0 \bullet \sigma_1 = \begin{cases} \langle S, V, I, \rightsquigarrow \rangle & \text{if } S_0 \upharpoonright \Lambda_1 = S_1 \upharpoonright \Lambda_0 \text{ and} \\ & V_0 \upharpoonright \Lambda_1 = V_1 \upharpoonright \Lambda_0 \\ \text{undefined} & \text{otherwise} \end{cases}$$

where

$$\begin{aligned} S &= S_0 \cup S_1, \\ V &= V_0 \cup V_1, \\ \rightsquigarrow &= (\rightsquigarrow_0 \cup \rightsquigarrow_1)^* \quad \text{and} \\ I(\alpha) &= \Sigma\{I_0(\beta) \mid \beta \in \Lambda_0 \text{ and } \beta \rightsquigarrow \alpha\} + \\ &\quad \Sigma\{I_1(\beta) \mid \beta \in \Lambda_1 \text{ and } \beta \rightsquigarrow \alpha\} \end{aligned}$$

for any $\alpha \in \Lambda_0 \cup \Lambda_1$.

Suppose σ is a static configuration of a circuit c . When does σ restrict to a configuration of the circuit $c \setminus \alpha$ in which the point α has been hidden? When the value (and strength) at α result from the combined effect of internal sources and the contribution from the unhidden points $\Lambda \setminus \alpha$, more precisely when

$$V(\alpha) = I(\alpha) + \Sigma\{V(\beta) \mid \beta \in \Lambda \setminus \alpha \text{ and } \beta \rightsquigarrow \alpha\}.$$

Then the hiding of α makes no difference. Of course hiding a point α can make no difference to a circuit which does not have α in its sort and we take care of this case too in the following definition.

Definition. Let $\sigma = \langle S, V, I, \rightsquigarrow \rangle$ be a static configuration of sort Λ and α a point in Π . Define *hiding*

$$\sigma \setminus \alpha = \langle S \setminus \alpha, V \setminus \alpha, I \setminus \alpha, \rightsquigarrow \setminus \alpha \rangle$$

if $\alpha \notin \Lambda$ or $V(\alpha) = I(\alpha) + \Sigma\{V(\beta) \mid \beta \in \Lambda \setminus \alpha \text{ and } \beta \rightsquigarrow \alpha\}$, and to be undefined otherwise.

We take the behaviour of a circuit term to be the set of possible static configurations it can settle into in some static environment.

The semantics of circuit terms:

It is convenient to use $\{\sigma \mid \phi\}$ where ϕ is an assertion on static configurations to mean $\{\sigma \mid \sigma \models \phi\}$. Define the semantic function $\llbracket \cdot \rrbracket$ from circuit terms to $P(\text{Sta})$ to be the map defined by the following structural induction.

$$\llbracket Pow(\alpha) \rrbracket = \{\sigma \in Sta[\alpha] \mid S(\alpha) = \infty \wedge I(\alpha) = H\}$$

$$\llbracket Gnd(\alpha) \rrbracket = \{\sigma \in Sta[\alpha] \mid S(\alpha) = \infty \wedge I(\alpha) = L\}$$

$$\llbracket cap_{kU}(\alpha) \rrbracket = \{\sigma \in Sta[\alpha] \mid S(\alpha) \geq k \wedge (S(\alpha) = k \rightarrow I(\alpha) = U) \wedge (S(\alpha) > k \rightarrow I(\alpha) = Z)\}$$

$$\llbracket pt(\alpha) \rrbracket = \{\sigma \in Sta[\alpha] \mid I(\alpha) = Z\}$$

$$\llbracket wre(\alpha, \beta) \rrbracket = \{\sigma \in Sta[\alpha, \beta] \mid I(\alpha) = Z \wedge I(\beta) = Z \wedge \alpha \sim \beta\}$$

$$\llbracket res_g(\alpha, \beta) \rrbracket = \{\sigma \in Sta[\alpha, \beta] \mid I(\alpha) = Z \wedge I(\beta) = Z \wedge S(\alpha) \cdot g \leq S(\beta) \wedge S(\beta) \cdot g \leq S(\alpha) \wedge (S(\alpha) \cdot g = S(\beta) \leftrightarrow \alpha \rightsquigarrow \beta) \wedge (S(\beta) \cdot g = S(\alpha) \leftrightarrow \beta \rightsquigarrow \alpha)\}$$

$$\llbracket ntran(\alpha, \beta, \gamma) \rrbracket = \{\sigma \in Sta[\alpha, \beta, \gamma] \mid I(\alpha) = Z \wedge I(\beta) = Z \wedge I(\gamma) = Z \wedge \gamma \parallel \alpha \wedge \gamma \parallel \beta \wedge (\alpha \parallel \beta \vee \alpha \sim \beta) \wedge (V(\gamma) = H \rightarrow \alpha \sim \beta) \wedge (V(\gamma) = L \rightarrow \alpha \parallel \beta)\}$$

$$\llbracket ptran(\alpha, \beta, \gamma) \rrbracket = \{\sigma \in Sta[\alpha, \beta, \gamma] \mid I(\alpha) = Z \wedge I(\beta) = Z \wedge I(\gamma) = Z \wedge \gamma \parallel \alpha \wedge \gamma \parallel \beta \wedge (\alpha \parallel \beta \vee \alpha \sim \beta) \wedge (V(\gamma) = L \rightarrow \alpha \sim \beta) \wedge (V(\gamma) = H \rightarrow \alpha \parallel \beta)\}$$

$$\llbracket c \bullet d \rrbracket = \{\sigma \bullet \rho \mid \sigma \in \llbracket c \rrbracket \text{ and } \rho \in \llbracket d \rrbracket \text{ and } \sigma \bullet \rho \downarrow\}$$

$$\llbracket c \setminus \alpha \rrbracket = \{\sigma \setminus \alpha \mid \sigma \in \llbracket c \rrbracket \text{ and } \sigma \setminus \alpha \downarrow\}.$$

As the reader will notice, even capacitance sources have fairly complicated behaviours involving conditional assertions, in order to cope with strengths and the fact that they can be overridden. Sources of power and ground have simpler definitions because they cannot be overridden. Resistances introduce the flow relation in a manner dependent on strengths, as we explained when introducing the flow relation. The behaviour of wires is got as a special case, by assuming perfect conductance. We stipulate that a transistor either connects or disconnects according to the voltage on the gate. Notice for both kinds of transistors a value of X on the gate can be associated with a static configuration where it is connecting or with one where it is disconnecting. The denotations of compositions and hiding of terms are obtained in a pointwise fashion.

Further terms can be defined. For instance, we can define a general source $sce_{sU}(\alpha)$, at α , of strength s and value $U \in \mathbf{V}$ where $s = 0$ iff $U = Z$, to have denotation

$$\llbracket sce_{sU}(\alpha) \rrbracket = \{ \sigma \in \text{Sta}[\alpha] \mid S(\alpha) \geq s \wedge (S(\alpha) = s \rightarrow I(\alpha) = U) \wedge (S(\alpha) > s \rightarrow I(\alpha) = \emptyset) \}$$

Such a source only makes a contribution at α if the strength of α is exactly s . If s is a capacitance strength k then such a weakened source with value $U = H$ or L can be realised by the charged capacitance $cap_{kU}(\alpha)$. Similarly, if s is a conductance strength g it can be realised by passing signals from ground or power through a resistance of strength g . Sources with value X can be got by connecting two sources with values H and L at a common point. Writing $c = c'$ iff $\llbracket c \rrbracket = \llbracket c' \rrbracket$, for circuit terms c, c' , we have

$$\begin{aligned} sce_{kH}(\alpha) &= cap_{kH}(\alpha), & sce_{kL}(\alpha) &= cap_{kL}(\alpha), \\ sce_{gH}(\alpha) &= (Pow(\beta) \bullet res_g(\beta, \alpha)) \setminus \beta, & sce_{gL}(\alpha) &= (Gnd(\beta) \bullet res_g(\beta, \alpha)) \setminus \beta, \\ sce_{gX}(\alpha) &= sce_{gH}(\alpha) \bullet sce_{gL}(\alpha). \end{aligned}$$

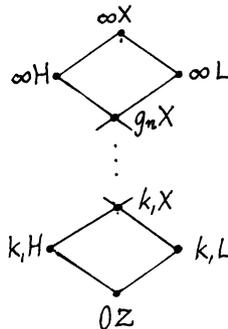
These are examples of some basic equivalences between circuit terms, which can be proved from the denotational semantics. Of course, such ideas were used informally in motivating the definition of static configuration. The one remaining case, $sce_{0Z}(\alpha)$ can be realised as a single connection point standing alone, *i.e.*

$$sce_{0Z}(\alpha) = pt(\alpha).$$

To explain the way sources combine, it is helpful to use an ordering between pairs sU , where $s \in \mathbf{S}$ and $U \in \mathbf{V}$ and $s = 0$ iff $U = Z$. On such pairs define

$$sU \leq s'U' \text{ iff } s < s' \text{ or } (s = s' \text{ and } U \leq U').$$

This forms a finite distributive lattice (meet \cdot and join $+$), mentioned in Bryant's thesis and Hayes work [4], which may be drawn as:



The way sources compose can now be summarised by:

$$sce_{sU}(\alpha) \bullet sce_{s'U'}(\alpha) = sce_{sU+s'U'}(\alpha).$$

As further examples of equivalences on terms which follow from the semantics we look at composing resistances in series and parallel:

$$\begin{aligned} (res_g(\alpha, \beta) \bullet res_{g'}(\beta, \gamma)) \setminus \beta &= res_{g \cdot g'}(\alpha, \gamma). \\ (res_g(\alpha, \beta) \bullet res_{g'}(\alpha, \beta)) &= res_{g+g'}(\alpha, \beta). \end{aligned}$$

In other words combined in series two resistances yield a resistance of conductance strength the minimum of the strengths of the components, while combined in parallel they are equivalent to one of strength the join. Again this agrees with the informal explanation given earlier but this time it follows from the general definition of the semantics of circuit terms.

Some equivalences highlight problems with the model. For example, according to the model we could produce a wire by sealing in a source to the gate of a transistor:

$$\begin{aligned} wre(\alpha, \beta) &= (Pow(\alpha) \bullet ntran(\alpha, \beta, \gamma)) \setminus \gamma \\ &= (Gnd(\alpha) \bullet ptran(\alpha, \beta, \gamma)) \setminus \gamma. \end{aligned}$$

A first complaint is that this is unrealistic because transistors have significant resistance. But this objection can be catered for simply by building in resistances. More importantly it indicates how effects caused by transistors having thresholds are ignored by the model, a topic we shall return to in the final section.

Earlier we pointed out the problem of knowing whether or not we had written down sufficient axioms for static configurations. It is sufficient to show every finite static configuration can be realised as a static configuration of a circuit term. This is established in the following proposition.

Proposition. *Any static configuration σ of sort Λ a finite subset of Π is the static configuration of some circuit c i.e. $\sigma \in \llbracket c \rrbracket$.*

Proof. Given σ , the idea is to define the required circuit to be the composition of the following finite set of components:

$$\begin{aligned} \{sce_{S(\alpha)U}(\alpha) \mid \alpha \in \Lambda \text{ and } I(\alpha) = U \neq Z\} \cup \\ \{res_g(\alpha, \beta) \mid \alpha \rightsquigarrow \beta \text{ and } g \in G \text{ is the least s.t. } S(\alpha) \cdot S(\beta) \leq g\}. \end{aligned}$$

This uses our knowledge of how to build all sources $sce_{S(\alpha)U}(\alpha)$ as circuits. From the definition of sources, resistances and composition, it follows that $\sigma \in \llbracket c \rrbracket$.

■

We would like a language of assertions with which to specify properties of circuits. A circuit denotes a subset of static configurations Sta . A circuit specification $Spec$ should pick out the subsets of circuits which satisfy it, and so semantically should denote a subset $\llbracket Spec \rrbracket \subseteq P(Sta)$ of the powerset of static configurations. We have already introduced assertions ϕ describing static configurations and, like circuits, they denote subsets $\llbracket \phi \rrbracket \subseteq Sta$, so as they stand they do not have the right type to be taken as circuit specifications. However, there is a standard way to take assertions of type Sta and make them into

assertions of type $P(\text{Sta})$. For ϕ an assertion about static configurations, define $\diamond \phi$ and $\square \phi$ to be circuit specifications with denotations

$$\begin{aligned} \llbracket \diamond \phi \rrbracket &= \{C \in P(\text{Sta}) \mid C \cap \llbracket \phi \rrbracket \neq \emptyset\}, \\ \llbracket \square A \rrbracket &= \{C \in P(\text{Sta}) \mid C \subseteq \llbracket \phi \rrbracket\}. \end{aligned}$$

A circuit term c satisfies $\diamond \phi$ iff $\llbracket c \rrbracket \in \llbracket \diamond \phi \rrbracket$, i.e. $\exists \sigma \in \llbracket c \rrbracket. \sigma \models \phi$, while c satisfies $\square \phi$ iff $\llbracket c \rrbracket \subseteq \llbracket \phi \rrbracket$, i.e. $\forall \sigma \in \llbracket c \rrbracket. \sigma \models \phi$. Thus a circuit satisfies $\diamond \phi$ means it can satisfy ϕ , whereas it satisfies $\square \phi$ means it must satisfy ϕ , which is consistent with the way these two words were used informally in section 2. Compound specifications may be made by combining these basic specifications using the usual logical operations. The operators \diamond and \square are then each definable from the other as $\diamond \phi$ is equivalent to $\neg \square \neg \phi$ (i.e. they are both satisfied by the same things), and $\square \phi$ is equivalent to $\neg \diamond \neg \phi$. However both \diamond and \square specifications characterise circuit behaviour in the sense of the following proposition. A circuit specification $Spec$ denotes a subset $\llbracket S \rrbracket \subseteq P(\text{Sta})$, and, for a circuit term c , we define

$$c \models Spec \Leftrightarrow \llbracket c \rrbracket \in \llbracket Spec \rrbracket,$$

when we say a circuit term c satisfies $Spec$.

Proposition. *Let c and c' be a circuit terms. Define*

$$\begin{aligned} c \preceq_{can} c' &\Leftrightarrow \forall \text{ assertions } \phi. c \models \diamond \phi \Rightarrow c' \models \diamond \phi, \text{ and} \\ c \preceq_{must} c' &\Leftrightarrow \forall \text{ assertions } \phi. c \models \square \phi \Rightarrow c' \models \square \phi. \end{aligned}$$

Then

$$\begin{aligned} c \preceq_{can} c' &\Leftrightarrow \llbracket c \rrbracket \subseteq \llbracket c' \rrbracket, \text{ and} \\ c \preceq_{must} c' &\Leftrightarrow \llbracket c' \rrbracket \subseteq \llbracket c \rrbracket. \end{aligned}$$

Hence if two circuit terms c, c' satisfy the same specifications $\diamond \phi$, or the same specifications $\square \phi$, then $c = c'$ (i.e. they have the same denotation).

Proof. The proof use the fact that any finite configuration σ is a characterised by an assertion A_σ in the sense that

$$\rho \models A_\sigma \Leftrightarrow \rho = \sigma.$$

Suppose $c \preceq_{can} c'$. If $\sigma \in \llbracket c \rrbracket$ then $c \models \diamond A_\sigma$ so $c' \models \diamond A_\sigma$, whence $\sigma \in \llbracket c' \rrbracket$. Hence $c \preceq_{can} c' \Rightarrow \llbracket c \rrbracket \subseteq \llbracket c' \rrbracket$, and the converse is obvious.

Suppose $c \preceq_{must} c'$. Clearly $c \models \square \bigvee_{\sigma \in \llbracket c \rrbracket} A_\sigma$. It follows that $c' \models \square \bigvee_{\sigma \in \llbracket c \rrbracket} A_\sigma$. If $\rho \in \llbracket c' \rrbracket$ then $\rho \models \bigvee_{\sigma \in \llbracket c \rrbracket} A_\sigma$ which implies $\rho = \sigma$ for some $\sigma \in \llbracket c \rrbracket$. Hence $c \preceq_{must} c' \Rightarrow \llbracket c' \rrbracket \subseteq \llbracket c \rrbracket$, and the converse is obvious. ■

Now we see how to give a specification of the NMOS inverter. The specification takes account of the fact that the strengths of its outputs are not the same. Its circuit is constructed by the term

$$c \equiv (ntran(\alpha, \beta, \gamma) \bullet res_g(\beta, \delta) \bullet Pow \delta \bullet Gnd(\alpha)) \setminus \alpha \setminus \delta.$$

Informally, its output β behaves like a direct connection to ground when its input γ is high and like a weakened power source when γ is low. Formally, if we define

$$\begin{aligned} Scc_{sU}(x) &\equiv s \leq S(x) \wedge \\ &\quad s = S(x) \rightarrow I(x) = U \wedge \\ &\quad s < S(x) \rightarrow I(x) = Z, \end{aligned}$$

then we can say c satisfies the specification

$$\begin{aligned} \square (V(\gamma) = H \rightarrow Scc_{\infty L}(\beta) \wedge \\ V(\gamma) = L \rightarrow Scc_{gH}(\beta)). \end{aligned}$$

We would like a proof system in which to demonstrate that a circuit meets a specification. In [10] a complete proof system is presented for proving a circuit term satisfies a specification of the form $\square \phi$. A proof system incorporating specifications $\diamond \phi$ will most likely follow similar lines, though it has not been done yet.

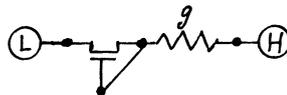
To conclude this section, we note an inadequacy which arises if we restrict to specifications of the form $\square \phi$. A related difficulty appears in the model of [2, 3] where terms like $Pow(\alpha) \bullet Gnd(\alpha)$ cause problems because they denote the empty relation and satisfy any specification. We have

$$\llbracket Pow(\alpha) \bullet Gnd(\alpha) \rrbracket \neq \emptyset,$$

and so, when we come to the logic, the circuit $Pow(\alpha) \bullet Gnd(\alpha)$ will not satisfy $\square \text{ff}$. However, there are other circuit terms which do denote \emptyset and so will satisfy $\square \text{ff}$, and indeed any specification $\square \phi$. These are terms which represent circuits whose only possible behaviour is to oscillate. For example the term

$$c \equiv (ntran(\alpha, \beta, \gamma) \bullet res_g(\beta, \delta) \bullet Pow \delta \bullet Gnd \gamma \bullet wre(\gamma, \beta)) \setminus \alpha \setminus \beta \setminus \gamma \setminus \delta$$

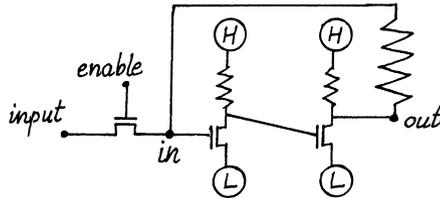
with g a conductance strength strictly between 0 and ∞ , “ties-back” the output of an NMOS inverter to its input, and then insulates all points from the environment. It can be drawn as:



The circuit c denotes the emptyset, $\llbracket c \rrbracket = \emptyset$. The circuit is a little peculiar in that it has an empty sort. However composing it with any circuit with nonempty sort yields a circuit with nonempty sort which denotes \emptyset . For this reason the proof system for circuits in [10], where all specifications have the form $\square \phi$, is akin to the logic of partial correctness assertions (Hoare logic); there a purely oscillating circuit satisfies $\square \phi$ for any assertion ϕ just as a diverging program satisfies all partial correctness assertions. However, a purely oscillating circuit like that above will not satisfy $\diamond \text{true}$, so a proof system extended to include specifications $\diamond \phi$ would not have this inadequacy.

4. Problems.

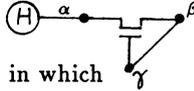
A compositional model for the static behaviour of MOS circuits has been presented. Certainly such a model is necessary for a satisfactory treatment of dynamically changing circuits. Their behaviour can often be viewed as going through a sequence of static configurations as data changes in synchrony with one or several clocks. The data and the clock pulses are held long enough for the circuit to settle into a static configuration. It seems obvious therefore to represent a possible history for such a circuit as a sequence of static configurations. Copying the approach in [2] we could try to extend our work to the dynamic case by simply including a time parameter t , a natural number, and associating devices with assertions expressing time dependencies between static configurations at different times. For example, then we could express facts like a capacitance would contribute a charge at time $t + 1$ if it was precharged at time t . While this works reasonably well for circuits with purely dynamic memory there is a hard problem in modelling static memory accurately. The main difficulty, it seems, is that short-term capacitance effects influence the physical behaviour but are not captured easily in any extension of our model. The strength orders we use assume that the environment is stable long enough for sources of current to override charges stored by capacitance. This assumption breaks down in some stages needed to explain the behaviour of devices like the following register:



When *enable* is high, a strong signal at *in* overrides that already present, and its value is established, after two inversions, at *out*. When *enable* becomes low the value is preserved at *out* (the input value is stored). Speaking loosely, the latter stage relies on capacitance to maintain the value at *in* until the feedback loop takes over. This occurs over a very short time when the assumptions behind the strength order are violated. I cannot, at present, see how to extend the model to account for effects over such a short time. Through failing to cope adequately with such short-term effects, the obvious model I have sketched allows more possibilities than are physically possible. By the way, the work of Bryant does not address this problem; a simulator need only generate one possible course of behaviour and Bryant does this by making a unit-delay assumption. (In his simulators all transistors switch with the same delay after their gates change.)

Even for just static behaviour there are inadequacies in the model. Chief among them, it seems, is that it fails to cope with the fact that transistors do not behave purely as switches which connect or disconnect according to the voltage on the gate. An n-type transistor $ntran(\alpha, \beta, \gamma)$ only connects when the difference between the voltage on its gate γ and the minimum of that on α and

β exceeds a certain positive threshold. This is ignored in switch level models like those of [1] and the model here. Consequently the model we have described allows certain static configurations which are not physically feasible. Consider the term $Pow(\alpha) \bullet ntran(\alpha, \beta, \gamma) \bullet wre(\alpha, \beta)$.



It has a static configuration in which

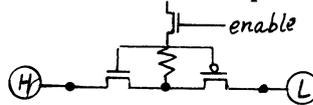
$$I(\alpha) = I(\beta) = V(\alpha) = V(\beta) = H \text{ and } \alpha \sim \beta.$$

This is not possible for a real n-type transistor. The gate γ and the source β have the same voltage so the difference in their voltages cannot exceed the positive threshold necessary for α and β to connect. Similarly the term $Pow(\alpha) \bullet ntran(\alpha, \beta, \gamma) \bullet wre(\alpha, \beta) \bullet Gnd(\beta)$ has a static configuration in which

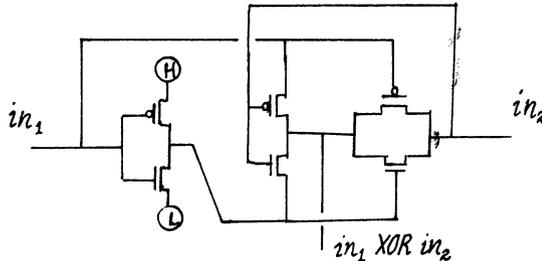
$$I(\alpha) = I(\beta) = V(\alpha) = V(\beta) = X \text{ and } \alpha \sim \beta.$$

Again this is not realistic.

Such inaccuracies can lead to an incorrect circuit being proved correct and a correct circuit being proved incorrect. For example according to the model presented the circuit



can store high and low, though showing it acts like a register encounters the same problems as for the real register above. It will not in reality because of thresholds. The following diagram describes a circuit which does compute exclusive-or (it is taken from [9], Figure 8.7, page 317).



However, according to the model when both inputs in_1 , and in_2 are high not only may the output be low, as required but also X —a possibility that is ruled out in reality because of thresholds.

Interestingly, although the model is inaccurate, we could not prove the design incorrect according to the model if we just use specifications of the form $\square \phi$. Certainly if the design satisfies $\square \phi$ according to the model then it will in reality, because the model allows more static configurations than are really possible. We could not prove it correct either. There is a \diamond -assertion which

holds of the circuit according to our model, *viz.* $\diamond A_\sigma$ where A_σ is the assertion characterising the unrealistic static configuration we have described, which does not hold of the real design.

It looks as if the model can be extended to cope with thresholds while keeping the same qualitative style. It appears to need another attribute to be attached to static configurations—a measure at each point of how strongly the value has been degraded. N-type transistors can transmit high values. But they do so at the cost of degrading the voltage to that of roughly the gate voltage minus the threshold. The measure of degradation would count the number of such degradations. The idea needs to be worked through more carefully however, and a decision taken as to how to manage different thresholds values and their relationship to each other.

Much needs to be done. Extending the model to sequential circuits with static memory seems hard. Coping with thresholds to give a more accurate treatment of static behaviours seems more tractable. Dealing with it will surely press home the need for a more careful analysis of the relationship between qualitative models of the kind here and explanations based more closely on the physics of devices. Some work, [6] and [11], has been done on the relationship between different models of hardware. But the development of a general framework in which to carry out the verification of hardware at all stages in its development, from logical design to layout, calls for a spectrum of models at different levels of abstraction with formal relations between them. We cannot claim to have anything like this at present.

Acknowledgements.

I would like to thank the members of the Hardware Verification Group here in Cambridge for help and encouragement and especially Mike Gordon for laying bare some of the issues in modelling and verifying hardware which led to this work. Mark Greenstreet helped explain the difficulties which arise from ignoring switching thresholds in transistors. Randy Bryant has been encouraging. Finally many thanks to Graham Birtwistle for his organisation and encouragement.

References.

- [1] Bryant, R.E., "A switch-level model and simulator for MOS digital systems", *IEEE Transactions on Computers* C-33 (2) pp. 160-177, February 1984.
- [2] Camilleri, A., Gordon, M., and Melham, T., "Hardware verification using higher order logic", To appear in the proceedings of the IFIP International working conference, Grenoble, France, September 1986. Also available as a report 91 of the Computer Laboratory, University of Cambridge, 1986.
- [3] Gordon, M.J.C., "Why higher order logic is a good formalism for specifying and verifying hardware", in "Formal aspects of VLSI design: Proceedings of the 1985 Edinburgh Conference on VLSI", G.J.Milne and P.A.Subrahmanyam, eds., North-Holland, Amsterdam, 1986.
- [4] Hayes, J., "A unified switching theory with applications to VLSI design", *Proc. IEEE* 70 (10) pp. 1140-1155 Oct. 1982.
- [5] Hoare, C.A.R., "Communicating sequential processes", Prentice-Hall, 1985.
- [6] Melham, T.F., "Abstraction Mechanisms for Hardware Verification" in: *VLSI Specification, Verification and Synthesis* G.M. Birtwistle and P.A. Subrahmanyam, eds, (this volume).
- [7] Milner, R., *A Calculus of Communicating Systems*. Springer Lecture Notes in Comp. Sc. vol. 92, 1980.
- [8] Scott, D.S., Identity and existence in intuitionistic logic. In proc. of Durham conference on Applications of Sheaves 1977, Lecture notes in Math., Springer-Verlag, 1979.
- [9] Weste, N., and Eshraghian, K., "Principles of CMOS VLSI Design", Addison Wesley Publishing Company, 1985.
- [10] Winskel, G., "Lectures on models and logic of MOS circuits", Proceedings for the Marktoberdorf Summer School, July 1986. Being published by Springer.
- [11] Winskel, G., "Relating two models of hardware", Submitted to the conference "Category theory and computer science", Edinburgh, September 1987.