Exponential blowup from conjunctive to disjunctive normal form

Wolfgang Slany
http://slany.org/wolfgang/
http://www.dbai.tuwien.ac.at/proj/pf2html/

April 23, 2002

Abstract

Printable version of a sample proof that uses Lamport's proof style [1], illustrating how structured proofs can be converted to HTML pages via LaTeX2HTML enriched with extensions for Lamport's proof style. Note that we try on purpose to carry out Lamport's rule of thumb to "expand the proof until the lowest level statements are obvious, and then continue for one more level" in order to illustrate the principles of structured proofs.

Problem (cf. [2]):

What is the disjunctive normal form of

$$(x_1 \vee y_1) \wedge (x_2 \vee y_2) \wedge \ldots \wedge (x_n \vee y_n)?$$

1 Solution 1

$$(x_1 \vee y_1) \wedge (x_2 \vee y_2) \wedge \ldots \wedge (x_n \vee y_n) \equiv \left.\begin{array}{r} (x_1 \wedge x_2 \wedge \ldots \wedge x_{n-1} \wedge x_n) \\ \vee\, (y_1 \wedge x_2 \wedge \ldots \wedge x_{n-1} \wedge x_n) \\ \vee\, (x_1 \wedge y_2 \wedge \ldots \wedge x_{n-1} \wedge x_n) \\ \vee\, (y_1 \wedge y_2 \wedge \ldots \wedge x_{n-1} \wedge x_n) \\ \vdots \\ \vee\, (y_1 \wedge y_2 \wedge \ldots \wedge y_{n-1} \wedge y_n) \end{array}\right\} 2^n \quad (1)$$

The resulting disjunctive normal form is exponentially blown up compared to the size of the original conjunctive normal form.

PROOF SKETCH: We show that the right side of Equation 1 is a disjunctive normal form of its left side. Since disjunctive normal forms are unique modulo permutations of the disjuncts and modulo the order of the literals in the disjuncts, the given disjunctive normal form cannot be reduced in size and the exponential blowup is unavoidable. The formal proof establishes that the right side of Equation 1 is a disjunctive normal form of its left side by induction on n.

PROOF:
1. CASE: $n = 1$
   The left hand side of Equation 1 is $(x_1 \vee y_1)$ which is `true` iff its right hand side $(x_1) \vee (y_1)$ is `true`.
   PROOF:

x_1	y_1	$(x_1 \vee y_1)$	$(x_1) \vee (y_1)$
`true`	`true`	`true`	`true`
`true`	`false`	`true`	`true`
`false`	`true`	`true`	`true`
`false`	`false`	`false`	`false`

   Q.E.D.
2. CASE: $n > 1$
   We proceed by showing that if Equation 1 holds for $n - 1 \geq 1$, then it also holds for n.
   LET:
   2.1. Denote the left side of Equation 1 for each n by ϕ_n.
   2.2. Denote the right side of Equation 1 for each n by φ_n.
   2.3. Denote by $b_{n,i}b_{n-1,i}\ldots b_{2,i}b_{1,i}$ with $b_{j,i} \in \{0,1\}$ and $j \in \{1,\ldots,n\}$ the binary notation of $i \in \{0,\ldots,2^n - 1\}$, such that $i = \sum_{j=1}^{n} b_{j,i}2^{j-1}$.
   2.4. Denote the $(i+1)$th disjunct of φ_n by
   $$\delta_{n,i} \stackrel{\text{def}}{=} (z_{1,b_{1,i}} \wedge z_{2,b_{2,i}} \wedge \ldots \wedge z_{n-1,b_{n-1,i}} \wedge z_{n,b_{n,i}})$$
   where $z_{j,0} \stackrel{\text{def}}{=} x_j$ and $z_{j,1} \stackrel{\text{def}}{=} y_j$.
   ASSUME:
   2.5. Equation 1 holds for $n - 1 \geq 1$ (induction hypothesis):
   $$\phi_{n-1} \equiv \varphi_{n-1} = \bigvee_{i=0}^{2^{n-1}-1} \delta_{n-1,i} \ .$$
   PROVE:
   2.6. Assumption 2.5 implies (induction step):
   $$\phi_n \equiv \varphi_n = \bigvee_{i=0}^{2^n-1} \delta_{n,i} \ .$$
   PROOF:
   2.7. $\phi_n \equiv \left(\bigvee_{i=0}^{2^{n-1}-1} (\, \delta_{n-1,i} \wedge x_n \,) \right) \vee \left(\bigvee_{i=0}^{2^{n-1}-1} (\, \delta_{n-1,i} \wedge y_n \,) \right)$.
      2.7.1. $\phi_n \equiv \phi_{n-1} \wedge (x_n \vee y_n)$.
         PROOF: By definition of ϕ_n (cf. 2.1).
      2.7.2. $\phi_n \equiv \left(\bigvee_{i=0}^{2^{n-1}-1} \delta_{n-1,i} \right) \wedge (x_n \vee y_n)$.
         PROOF: By step 2.7.1 and Assumption 2.5.

2.7.3. $\phi_n \equiv \bigvee_{i=0}^{2^{n-1}-1} \Big(\delta_{n-1,i} \wedge (x_n \vee y_n)\Big)$.

PROOF: By step 2.7.2, the distributivity of $\wedge$ over $\vee$ [2, Proposition 4.1 (7)] (cf. Table 1), and the associativity of $\vee$ [2, Proposition 4.1 (4)] (cf. Table 1), the latter two applied repeatedly.

2.7.4. $\phi_n \equiv \bigvee_{i=0}^{2^{n-1}-1} \Big((\delta_{n-1,i} \wedge x_n) \vee (\delta_{n-1,i} \wedge y_n)\Big)$.

PROOF: By step 2.7.3 and the distributivity of $\wedge$ over $\vee$ [2, Proposition 4.1 (7)] (cf. Table 1).

2.7.5. Q.E.D.

PROOF: By step 2.7.4, the commutativity of $\vee$ [2, Proposition 4.1 (1)] (cf. Table 1), and the associativity of $\vee$ [2, Proposition 4.1 (4)] (cf. Table 1), the latter two applied repeatedly.

2.8. $\delta_{n-1,i} \wedge x_n \equiv \delta_{n,i}$.

PROOF: By definition of $\delta_{n,i}$ (cf. 2.4).

2.9. $\delta_{n-1,i} \wedge y_n \equiv \delta_{n,2^{n-1}+i}$.

PROOF: By definition of $\delta_{n,i}$ (cf. 2.4).

2.10. $\varphi_n \equiv \Big(\bigvee_{i=0}^{2^{n-1}-1} (\, \delta_{n,i} \,) \Big) \vee \Big(\bigvee_{i=0}^{2^{n-1}-1} (\, \delta_{n,2^{n-1}+i} \,) \Big)$.

2.10.1. $\varphi_n \equiv \Big(\bigvee_{i=0}^{2^{n-1}-1} (\, \delta_{n,i} \,) \Big) \vee \Big(\bigvee_{i=2^{n-1}}^{2^{n}-1} (\, \delta_{n,i} \,) \Big)$.

PROOF: By definition of $\delta_{n,i}$ (cf. 2.4) and by splitting up the expression of φ_n in 2.6 into two equally sized parts, which is possible because of the associativity of $\vee$ [2, Proposition 4.1 (4)] (cf. Table 1).

2.10.2. Q.E.D.

PROOF: By shifting the offset 2^{n-1} in the second term of the right part of Equivalence 2.10.1 from the running variable i into the term expression $\delta_{n,2^{n-1}+i}$ in the second term of the right part of Equivalence 2.10.

2.11. Q.E.D.

PROOF: Substituting from left to right Equivalences 2.8 and 2.9 in Equivalence 2.7, we get Equivalence 2.10. Thus, $\phi_n \equiv \varphi_n$ (2.6) is proved.

3. Q.E.D.

PROOF: By steps 1 and 2 of the inductive argument.

Table 1: Proposition 4.1 of [2]: Let ϕ_1, ϕ_2, and ϕ_3 be arbitrary Boolean expressions. Then:

(1)	$(\phi_1 \vee \phi_2) \equiv (\phi_2 \vee \phi_1)$	(commutativity of $\vee$)
(2)	$(\phi_1 \wedge \phi_2) \equiv (\phi_2 \wedge \phi_1)$	(commutativity of $\wedge$)
(3)	$\neg\neg\phi_1 \equiv \phi_1$	(double negation is canceled)
(4)	$((\phi_1 \vee \phi_2) \vee \phi_3) \equiv (\phi_1 \vee (\phi_2 \vee \phi_3))$	(associativity of $\vee$)
(5)	$((\phi_1 \wedge \phi_2) \wedge \phi_3) \equiv (\phi_1 \wedge (\phi_2 \wedge \phi_3))$	(associativity of $\wedge$)
(6)	$((\phi_1 \wedge \phi_2) \vee \phi_3) \equiv (\phi_1 \vee \phi_3) \wedge (\phi_2 \vee \phi_3))$	(distributivity of $\vee$ over $\wedge$)
(7)	$((\phi_1 \vee \phi_2) \wedge \phi_3) \equiv (\phi_1 \wedge \phi_3) \vee (\phi_2 \wedge \phi_3))$	(distributivity of $\wedge$ over $\vee$)
(8)	$\neg(\phi_1 \vee \phi_2) \equiv (\neg\phi_1 \wedge \neg\phi_2)$	(De Morgan's law for $\vee$)
(9)	$\neg(\phi_1 \wedge \phi_2) \equiv (\neg\phi_1 \vee \neg\phi_2)$	(De Morgan's law for $\wedge$)
(10)	$\phi_1 \vee \phi_1 \equiv \phi_1$	(idempotency of $\vee$)
(11)	$\phi_1 \wedge \phi_1 \equiv \phi_1$	(idempotency of $\wedge$)

2 Solution 2

$$(x_1 \vee y_1) \wedge (x_2 \vee y_2) \wedge \ldots \wedge (x_n \vee y_n) \quad \equiv \quad \left.\begin{array}{r} (x_1 \wedge x_2 \wedge \ldots \wedge x_{n-1} \wedge x_n) \\ \vee\, (y_1 \wedge x_2 \wedge \ldots \wedge x_{n-1} \wedge x_n) \\ \vee\, (x_1 \wedge y_2 \wedge \ldots \wedge x_{n-1} \wedge x_n) \\ \vee\, (y_1 \wedge y_2 \wedge \ldots \wedge x_{n-1} \wedge x_n) \\ \vdots \\ \vee\, (y_1 \wedge y_2 \wedge \ldots \wedge y_{n-1} \wedge y_n) \end{array}\right\} 2^n \tag{2}$$

The resulting disjunctive normal form is exponentially blown up compared to the size of the original conjunctive normal form.

Proof sketch: Consider the directed graph shown in Figure 1. Observe that

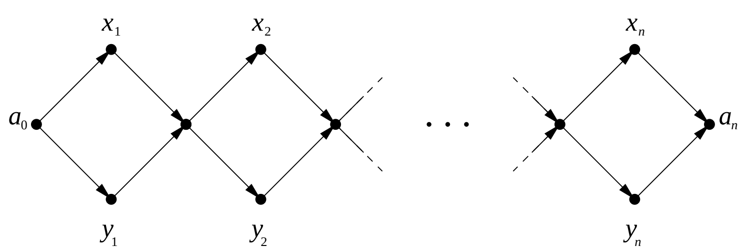

Figure 1: Visual proof of Equation 2.

paths from a_0 to a_n can be described either as going through nodes (x_1 or y_1) and (x_2 or y_2) and ... and (x_n or y_n) (cf. the conjunctive normal form), or alternatively as going through nodes (x_1 and x_2 and ... and x_{n-1} and x_n) or (x_1 and x_2 and ... and x_{n-1} and y_n) or (x_1 and x_2 and ... and y_{n-1} and x_n) or (x_1 and x_2 and ... and y_{n-1} and y_n) or ... or (y_1 and y_2 and ... and

y_{n-1} and y_n) (cf. the disjunctive normal form). The formal proof makes this precise.

LET: Denote the left side of Equation 2 by ϕ, and its right side by φ (the variable-names are reused in Figure 1 to label the top and bottom nodes).

PROVE: $\phi \equiv \varphi$.

PROOF:

1. There is a one-to-one correspondence (a bijection) between the paths from node a_0 to node a_n and the minimal satisfying truth assignments of ϕ (the conjunctive normal form).

   1.1. Every path from node a_0 to node a_n corresponds to a unique minimal satisfying truth assigment of ϕ.

   LET:

   1.1.1. Let a variable of ϕ be set to `true` whenever the path goes through a node with the same name as the variable.

   PROOF:

   1.1.2. The truth assignments induced by paths from a_0 to a_n are *satisfying* truth assigments of ϕ.

   1.1.2.1. Every path from a_0 to a_n must go through either x_i or y_i for all $i \in \{1, \ldots, n\}$.

   PROOF: Structure of the graph in Figure 1.

   1.1.2.2. Q.E.D.

   PROOF: 1.1.1, 1.1.2.1, and the stucture of ϕ.

   1.1.3. The truth assignments induced by paths from a_0 to a_n are *minimal* satisfying truth assigments of ϕ.

   1.1.3.1. Flipping any variable from `true` to `false` in such a truth assignment makes ϕ unsatisfied.

   PROOF: Structure of ϕ (every conjunct has only one variable that makes it `true` in any minimal truth assignment of ϕ).

   1.1.3.2. Q.E.D.

   PROOF: 1.1.2 and 1.1.3.1.

   1.1.4. These minimal satisfying truth assigments are *unique*.

   PROOF: 1.1.3, the structure of the graph, the structure of ϕ, and because the order of variables in truth assigments does not matter.

   1.1.5. Q.E.D.

   1.2. Conversely, every minimal satisfying truth assignment of ϕ corresponds to a unique path from node a_0 to node a_n.

   LET:

   1.2.1. Let a variable of ϕ be set to `true` whenever the path goes through a node with the same name as the variable.

   PROOF:

   1.2.2. Every minimal satisfying truth assignment of ϕ corresponds to a path from node a_0 to node a_n.

   PROOF: From the structure of ϕ, exactly one variable in each conjunct must be `true` in any minimal satisfying truth assignment of ϕ. This defines a path from node a_0 to node a_n by the structure of the graph in

Figure 1 and 1.2.1.

1.2.3. The thus induced path is *unique*.

PROOF: Structure of ϕ and the construction of the graph in Figure 1.

1.2.4. Q.E.D.

1.3. Q.E.D.

PROOF: 1.1 and 1.2.

2. There is a one-to-one correspondence between the paths from node a_0 to node a_n and the minimal satisfying truth assignments of φ (the disjunctive normal form).

2.1. Every path from node a_0 to node a_n corresponds to a unique minimal satisfying truth assigment of φ.

LET:

2.1.1. Let a variable of φ be set to `true` whenever the path goes through a node with the same name as the variable.

PROOF:

2.1.2. The truth assignments induced by paths from a_0 to a_n are *satisfying* truth assigments of φ.

2.1.2.1. Every path from a_0 to a_n must for all $i \in \{1, \ldots, n\}$ either go through x_i or y_i.

PROOF: Structure of the graph in Figure 1.

2.1.2.2. Q.E.D.

PROOF: 2.1.1, 2.1.2.1, and the stucture of φ.

2.1.3. The truth assignments induced by paths from a_0 to a_n are *minimal* satisfying truth assigments of φ.

2.1.3.1. Flipping any variable from `true` to `false` in such a truth assignment makes φ unsatisfied.

PROOF: Structure of φ (only one disjunct is made `true` by any minimal truth assignment of φ).

2.1.3.2. Q.E.D.

PROOF: 2.1.2 and 2.1.3.1.

2.1.4. These minimal satisfying truth assigments are *unique*.

PROOF: 2.1.3, the structure of the graph, the structure of φ, and because the order of variables in truth assigments does not matter.

2.1.5. Q.E.D.

2.2. Conversely, every minimal satisfying truth assignment of φ corresponds to a unique path from node a_0 to node a_n.

LET:

2.2.1. Let a variable of φ be set to `true` whenever the path traverses a node with the same name as the variable.

PROOF:

2.2.2. Every minimal satisfying truth assignment of φ corresponds to a path from node a_0 to node a_n.

PROOF: From the structure of φ, exactly one variable in each disjunct must be `true` in any minimal satisfying truth assignment of φ. This defines a path from node a_0 to node a_n by the structure of the graph in Figure 1 and 2.2.1.

2.2.3. The thus induced path is *unique*.

PROOF: Structure of φ and the construction of the graph in Figure 1.

2.2.4. Q.E.D.

2.3. Q.E.D.

PROOF: 2.1 and 2.2.

3. Q.E.D.

PROOF: Since each satisfying truth assignment of a boolean formula must contain a *minimal* satisfying truth assignment (by definition of the latter), and since by proof steps 1 and 2 there must be a one-to-one correspondence between the minimal satisfying truth assignment of ϕ and of φ, a truth assignment satisfies ϕ iff it also satisfies φ.

Acknowledgements

The help and comments of Marcus Carotta, Wolfgang Goedl, Martina Osztovits, and Helmut Veith are gratefully acknowledged.

References

[1] Leslie Lamport, 1993, How to write a proof. In *Global Analysis of Modern Mathematics*, pp. 311–321. Publish or Perish, Houston, Texas, February 1993. A symposium in honor of Richard Palais' sixtieth birthday (also published as SRC Research Report 94). http://research.microsoft.com/users/lamport /proofs/src94.ps.Z

[2] Christos H. Papadimitriou, 1994, Problem 4.4.5. In *Computational Complexity*, p. 84. Addison-Wesley.