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
\[(x_1 \lor y_1) \land (x_2 \lor y_2) \land \ldots \land (x_n \lor y_n)\]?

1 Solution 1

\[
(x_1 \lor y_1) \land (x_2 \lor y_2) \land \ldots \land (x_n \lor y_n) \equiv \begin{array}{l}
(x_1 \land x_2 \land \ldots \land x_{n-1} \land x_n) \\
\lor (y_1 \land x_2 \land \ldots \land x_{n-1} \land x_n) \\
\lor (x_1 \land y_2 \land \ldots \land x_{n-1} \land x_n) \\
\lor (y_1 \land y_2 \land \ldots \land x_{n-1} \land x_n) \\
\vdots \\
\lor (y_1 \land y_2 \land \ldots \land y_{n-1} \land y_n)
\end{array} \quad (1)
\]

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 $(x_1 \lor y_1)$ which is true if its right hand side $(x_1) \lor (y_1)$ is true.

   **Proof:**

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$y_1$</th>
<th>$(x_1 \lor y_1)$</th>
<th>$(x_1) \lor (y_1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
</tbody>
</table>

   **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 $\varphi_n$.
   2.2. Denote the right side of Equation 1 for each $n$ by $\varphi_n$.
   2.3. Denote by $b_{n,i}$ the binary notation of $i \in \{0, 1, \ldots, 2^{n-1}\}$, such that $i = \sum_{j=1}^{n} b_{j,i} 2^{j-1}$.
   2.4. Denote the ($i + 1$)th disjunct of $\varphi_n$ by

   $\delta_{n,i} \text{ def } = (z_{1,b_{1,i}} \land z_{2,b_{2,i}} \land \ldots \land z_{n-1,b_{n-1,i}} \land z_{n,b_{n,i}})$

   where $z_{j,0} \text{ def } = x_j$ and $z_{j,1} \text{ def } = y_j$.

   **Assume:**

   2.5. Equation 1 holds for $n - 1 \geq 1$ (induction hypothesis):

   $\varphi_{n-1} = \bigvee_{i=0}^{2^{n-1}-1} \delta_{n-1,i}$.

   **Prove:**

   2.6. Assumption 2.5 implies (induction step):

   $\varphi_n = \bigvee_{i=0}^{2^n-1} \delta_{n,i}$.

   **Proof:**

   2.7. $\varphi_n \equiv \left( \bigvee_{i=0}^{2^n-1} (\delta_{n-1,i} \land x_n) \right) \lor \left( \bigvee_{i=0}^{2^n-1} (\delta_{n-1,i} \land y_n) \right)$.

   2.7.1. $\varphi_n \equiv \varphi_{n-1} \land (x_n \lor y_n)$.

   **Proof:** By definition of $\varphi_n$ (cf. 2.1).

   2.7.2. $\varphi_n \equiv \left( \bigvee_{i=0}^{2^n-1} \delta_{n-1,i} \right) \land (x_n \lor y_n)$.

   **Proof:** By step 2.7.1 and Assumption 2.5.
2.7.3. $\phi_n \equiv 2^n - 1 \bigvee_{i=0}^{2^n-1-1} \left( \delta_{n-1,i} \land (x_n \lor y_n) \right)$.

**Proof**: By step 2.7.2, the distributivity of $\land$ over $\lor$ [2, Proposition 4.1 (7)] (cf. Table I), and the associativity of $\lor$ [2, Proposition 4.1 (4)] (cf. Table I), the latter two applied repeatedly.

2.7.4. $\phi_n \equiv 2^n - 1 \bigvee_{i=0}^{2^n-1-1} \left( \left( \delta_{n-1,i} \land x_n \right) \lor \left( \delta_{n-1,i} \land y_n \right) \right)$.

**Proof**: By step 2.7.3 and the distributivity of $\land$ over $\lor$ [2, Proposition 4.1 (7)] (cf. Table I).

2.7.5. Q.E.D.

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

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

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

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

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

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

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

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

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 $\phi_1$, $\phi_2$, and $\phi_3$ be arbitrary Boolean expressions. Then:

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

2 Solution 2

\[
(x_1 \lor y_1) \land (x_2 \lor y_2) \land \ldots \land (x_n \lor y_n) \equiv \left\{ \begin{array}{l}
(x_1 \land x_2 \land \ldots \land x_{n-1} \land x_n) \\
\lor (y_1 \land x_2 \land \ldots \land x_{n-1} \land x_n) \\
\lor (x_1 \land y_2 \land \ldots \land x_{n-1} \land x_n) \\
\lor (y_1 \land y_2 \land \ldots \land x_{n-1} \land x_n) \\
\vdots \\
\lor (y_1 \land y_2 \land \ldots \land y_{n-1} \land y_n)
\end{array} \right\} 2^n (2)
\]

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 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 $y_{n-1}$ 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 $y_n$).
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 \( \phi \) and its right side by \( \varphi \) (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 \( \phi \) (the conjunctive normal form).
   1.1. Every path from node \( a_0 \) to node \( a_n \) corresponds to a unique minimal satisfying truth assignment of \( \phi \).
      **LET:**
      1.1.1. Let a variable of \( \phi \) 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 assignments of \( \phi \).
         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 \( \phi \).
      1.1.3. The truth assignments induced by paths from \( a_0 \) to \( a_n \) are **minimal** satisfying truth assignments of \( \phi \).
         1.1.3.1. Flipping any variable from **true** to **false** in such a truth assignment makes \( \phi \) unsatisfied.
         **PROOF:** Structure of \( \phi \) (every conjunct has only one variable that makes it **true** in any minimal truth assignment of \( \phi \)).
      1.1.3.2. Q.E.D.
      **PROOF:** 1.1.2 and 1.1.3.1.
      1.1.4. These minimal satisfying truth assignments are **unique**.
      **PROOF:** 1.1.3, the structure of the graph, the structure of \( \phi \), and because the order of variables in truth assignments does not matter.
      1.1.5. Q.E.D.
   1.2. Conversely, every minimal satisfying truth assignment of \( \phi \) corresponds to a unique path from node \( a_0 \) to node \( a_n \).
      **LET:**
      1.2.1. Let a variable of \( \phi \) 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 \( \phi \) corresponds to a path from node \( a_0 \) to node \( a_n \).
      **PROOF:** From the structure of \( \phi \), exactly one variable in each conjunct must be **true** in any minimal satisfying truth assignment of \( \phi \). 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 $\phi$ 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 $\varphi$ (the disjunctive normal form).

2.1. Every path from node $a_0$ to node $a_n$ corresponds to a unique minimal satisfying truth assignment of $\varphi$.

**Let:**

2.1.1. Let a variable of $\varphi$ 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 assignments of $\varphi$.

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 structure of $\varphi$.

2.1.3. The truth assignments induced by paths from $a_0$ to $a_n$ are *minimal* satisfying truth assignments of $\varphi$.

2.1.3.1. Flipping any variable from *true* to *false* in such a truth assignment makes $\varphi$ unsatisfied.

**Proof:** Structure of $\varphi$ (only one disjunct is made *true* by any minimal truth assignment of $\varphi$).

2.1.3.2. Q.E.D.

**Proof:** 2.1.2 and 2.1.3.1.

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

**Proof:** 2.1.3, the structure of the graph, the structure of $\varphi$, and because the order of variables in truth assignments does not matter.

2.1.5. Q.E.D.

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

**Let:**

2.2.1. Let a variable of $\varphi$ 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 $\varphi$ corresponds to a path from node $a_0$ to node $a_n$.

**Proof:** From the structure of $\varphi$, exactly one variable in each disjunct must be *true* in any minimal satisfying truth assignment of $\varphi$. 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 $\varphi$ and the construction of the graph in Figure II

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 $\phi$ and of $\varphi$, a truth assignment satisfies $\phi$ if and only if it also satisfies $\varphi$.

**Acknowledgements**

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

**References**
