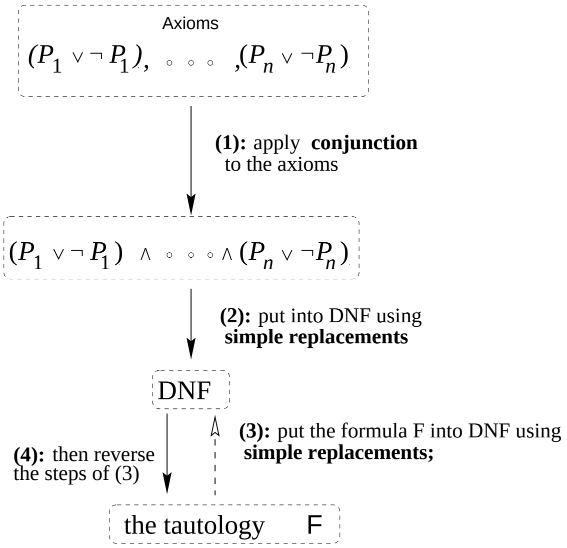
Notes prepared by
Stanley Burris
February 10, 1997

An algorithm to find derivations of tautologies

The proof of the completeness of PC given in Theorem II.9.9 of LMCS actually provides us with a straightforward algorithm to find derivations of tautologies. If we are given a tautology $F(P_1, \ldots, P_n)$ then we diagram the algorithm as follows:



How to find a derivation

Thus we see the three key parts of the algorithm:

1. find a derivation of the tautology $(P_1 \vee \neg P_1) \wedge \cdots \wedge (P_n \vee \neg P_n)$ using the conjunction rule;

2. derive the disjunctive normal form of this tautology using simple replacements based on the distributive, commutative and associative laws;

3. use simple replacements to transform $F(P_1,\ldots,P_n)$ into (the same) disjunctive normal form;
4. then reverse the order of the steps of (3), to transform the disjunctive normal form into the tautology $F(P_1,\ldots,P_n)$.

The first part requires $2n-1$ steps, namely

$$
\begin{array}{rll}
1: & P_1 \vee \neg P_1 & \text{axiom} \\
 & \vdots & \\
\text{n}: & P_n \vee \neg P_n & \text{axiom} \\
\text{n+1}: & (P_1 \vee \neg P_1) \wedge (P_2 \vee \neg P_2) & \text{C: 1,2} \\
 & \vdots & \\
\text{2n-1}: & (\cdots(P_1 \vee \neg P_1) \wedge \cdots) \wedge (P_n \vee \neg P_n) & \text{C: n,2n-2}
\end{array}
$$

For the second part one needs at least $2^{n+1}-n-3$ steps (just to apply the distributive laws). We illustrate for the case $n=2$. At this point our current notation becomes difficult to read, so for the rest of this subsection we switch to an abbreviated notation, namely we will use FG for $F \wedge G$, and $\overline{F}$ for $\neg F$. Also we will (for the time being) say $\wedge$ has higher precedence than $\vee$, so $FG \vee H$ means $(F \wedge G) \vee H$. This will allow us to dispense with many parentheses.

$$
\begin{array}{rll}
1: & P_1 \vee \overline{P}_1 & \text{axiom} \\
2: & P_2 \vee \overline{P}_2 & \text{axiom} \\
3: & (P_1 \vee \overline{P}_1)(P_2 \vee \overline{P}_2) & \text{C: 1,2} \\
4: & (P_1 \vee \overline{P}_1)P_2 \vee (P_1 \vee \overline{P}_1)\overline{P}_2 & \text{SR: 3 (9)} \\
5: & P_2(P_1 \vee \overline{P}_1) \vee (P_1 \vee \overline{P}_1)\overline{P}_2 & \text{SR: 4 (4)} \\
6: & P_2(P_1 \vee \overline{P}_1) \vee \overline{P}_2(P_1 \vee \overline{P}_1) & \text{SR: 5 (4)} \\
7: & (P_2P_1 \vee P_2\overline{P}_1) \vee \overline{P}_2(P_1 \vee \overline{P}_1) & \text{SR: 6 (9)} \\
8: & (P_2P_1 \vee P_2\overline{P}_1) \vee (\overline{P}_2P_1 \vee \overline{P}_2\overline{P}_1) & \text{SR: 7 (9)}
\end{array}
$$

So we needed the first 3 steps to obtain $(P_1 \vee \overline{P}_1)(P_2 \vee \overline{P}_2)$, the first part of the procedure, and then 5 steps to put this into disjunctive normal form. Of course one may want to rewrite this so that one has the DNF-constituents ordered according to the usual ordering of the rows of a truth table, and left associated, namely as

$$((P_1P_2 \vee P_1\overline{P}_2) \vee \overline{P}_1P_2) \vee \overline{P}_1\overline{P}_2.$$

After all, to have a DNF one needs to specify the order in which the DNF constituents are written, and how they are parenthesized. To go from line (8) above to this form will require 8 additional steps, applying commutativity and associativity (as simple replacement rules):

9:	$(P_1P_2 \vee P_2\overline{P}_1) \vee (\overline{P}_2P_1 \vee \overline{P}_2\overline{P}_1)$	SR: 8 (4)
10:	$(P_1P_2 \vee \overline{P}_1P_2) \vee (\overline{P}_2P_1 \vee \overline{P}_2\overline{P}_1)$	SR: 9 (4)
11:	$(P_1P_2 \vee \overline{P}_1P_2) \vee (P_1\overline{P}_2 \vee \overline{P}_2\overline{P}_1)$	SR: 10 (4)
12:	$(P_1P_2 \vee \overline{P}_1P_2) \vee (P_1\overline{P}_2 \vee \overline{P}_1\overline{P}_2)$	SR: 11 (4)
13:	$((P_1P_2 \vee \overline{P}_1P_2) \vee P_1\overline{P}_2) \vee \overline{P}_1\overline{P}_2$	SR: 12 (5)
14:	$(P_1P_2 \vee (\overline{P}_1P_2 \vee P_1\overline{P}_2)) \vee \overline{P}_1\overline{P}_2$	SR: 13 (5)
15:	$(P_1P_2 \vee (P_1\overline{P}_2 \vee \overline{P}_1P_2)) \vee \overline{P}_1\overline{P}_2$	SR: 14 (3)
16:	$((P_1P_2 \vee P_1\overline{P}_2) \vee \overline{P}_1P_2) \vee \overline{P}_1\overline{P}_2$	SR: 15 (5)

For larger n the second part of the algorithm explodes in the amount of work one needs to do because of the exponential lower bound $2^{n+1} - n - 3$ on the number of steps given above. For $n = 5$ variables this is already 56 steps, i.e., at least a page of work. And we still have the third part to worry about. This can be the wild card. If F is almost in DNF then there will not be much work to do. But it can be the most tedious part of the algorithm.

Let us return to the two examples that we presented after defining the notion of derivation (on page 76) and apply the above algorithm to them, and compare the results with our earlier derivations.

EXAMPLE 1 (See Example II.9.5) The following uses the above algorithm to derive $P \to (P \to P)$.

1:	$P \vee \neg P$	axiom
2:	$\neg P \vee P$	SR: 1 (3)
3:	$(\neg P \vee \neg P) \vee P$	SR: 2 (1)
4:	$\neg P \vee (\neg P \vee P)$	SR: 3 (5)
5:	$\neg P \vee (P \to P)$	SR: 4 (20)
6:	$P \to (P \to P)$	SR: 5 (20)

This compares quite favorably to the derivation in Example II.9.5, requiring only 1 more step. Part 1 and part 2 of the algorithm collapse into the first step above. Reading steps 1 through 6, in reverse order, we see the procedure for putting step 6 into its disjunctive normal form.

EXAMPLE 2 (See Example II.9.6) The following uses the algorithm to derive $P \to (Q \to P)$.

1:	$P \vee \overline{P}$	axiom
2:	$Q \vee \overline{Q}$	axiom
3:	$(P \vee \overline{P})(Q \vee \overline{Q})$	C: 1,2
4:	$(P \vee \overline{P})Q \vee (P \vee \overline{P})\overline{Q}$	SR: 3 (9)
5:	$Q(P \vee \overline{P}) \vee (P \vee \overline{P})\overline{Q}$	SR: 4 (4)
6:	$Q(P \vee \overline{P}) \vee \overline{Q}(P \vee \overline{P})$	SR: 5 (4)
7:	$(QP \vee Q\overline{P}) \vee \overline{Q}(P \vee \overline{P})$	SR: 6 (9)
8:	$(QP \vee Q\overline{P}) \vee (\overline{Q}P \vee \overline{Q}\,\overline{P})$	SR: 7 (9)
9:	$(PQ \vee Q\overline{P}) \vee (\overline{Q}P \vee \overline{Q}\,\overline{P})$	SR: 8 (4)
10:	$(PQ \vee \overline{P}Q) \vee (\overline{Q}P \vee \overline{Q}\,\overline{P})$	SR: 9 (4)
11:	$(PQ \vee \overline{P}Q) \vee (P\overline{Q} \vee \overline{Q}\,\overline{P})$	SR: 10 (4)
12:	$(PQ \vee \overline{P}Q) \vee (P\overline{Q} \vee \overline{P}\,\overline{Q})$	SR: 11 (4)
13:	$((PQ \vee \overline{P}Q) \vee P\overline{Q}) \vee \overline{P}\,\overline{Q}$	SR: 12 (5)
14:	$(PQ \vee (\overline{P}Q \vee P\overline{Q})) \vee \overline{P}\,\overline{Q}$	SR: 13 (5)
15:	$(PQ \vee (P\overline{Q} \vee \overline{P}Q)) \vee \overline{P}\,\overline{Q}$	SR: 14 (3)
16:	$(PQ \vee P\overline{Q}) \vee (\overline{P}Q \vee \overline{P}\,\overline{Q})$	SR: 15 (5)
17:	$(PQ \vee P\overline{Q}) \vee (\overline{P}Q \vee (\overline{P}\,\overline{Q} \vee \overline{P}\,\overline{Q}))$	SR: 16 (1)
18:	$(PQ \vee P\overline{Q}) \vee ((\overline{P}Q \vee \overline{P}\,\overline{Q}) \vee \overline{P}\,\overline{Q})$	SR: 17 (5)
19:	$(PQ \vee (P\overline{Q} \vee P\overline{Q})) \vee ((\overline{P}Q \vee \overline{P}\,\overline{Q}) \vee \overline{P}\,\overline{Q}$	SR: 18 (1)
20:	$((PQ \vee P\overline{Q}) \vee P\overline{Q}) \vee ((\overline{P}Q \vee \overline{P}\,\overline{Q}) \vee \overline{P}\,\overline{Q}))$	SR: 19 (5)
21:	$(PQ \vee P\overline{Q}) \vee (P\overline{Q} \vee ((\overline{P}Q \vee \overline{P}\,\overline{Q}) \vee \overline{P}\,\overline{Q}))$	SR: 20 (5)
22:	$(PQ \vee P\overline{Q}) \vee ((P\overline{Q} \vee (\overline{P}Q \vee \overline{P}\,\overline{Q})) \vee \overline{P}\,\overline{Q})$	SR: 21 (5)
23:	$(PQ \vee P\overline{Q}) \vee (((\overline{P}Q \vee \overline{P}\,\overline{Q}) \vee P\overline{Q}) \vee \overline{P}\,\overline{Q})$	SR: 22 (3)
24:	$(PQ \vee P\overline{Q}) \vee ((\overline{P}Q \vee \overline{P}\,\overline{Q}) \vee (P\overline{Q} \vee \overline{P}\,\overline{Q})$	SR: 23 (5)
25:	$(PQ \vee P\overline{Q}) \vee ((\overline{P}Q \vee \overline{P}\,\overline{Q}) \vee (P\overline{Q} \vee \overline{Q}\,\overline{P}))$	SR: 24 (4)
26:	$(PQ \vee P\overline{Q}) \vee ((\overline{P}Q \vee \overline{P}\,\overline{Q}) \vee (\overline{Q}P \vee \overline{Q}\,\overline{P}))$	SR: 25 (4)
27:	$(PQ \vee P\overline{Q}) \vee ((\overline{P}Q \vee \overline{P}\,\overline{Q}) \vee \overline{Q}(P \vee \overline{P}))$	SR: 26 (9)
28:	$(PQ \vee P\overline{Q}) \vee ((\overline{P}Q \vee \overline{P}\,\overline{Q}) \vee \overline{Q}1)$	SR: 27 (11)
29:	$(PQ \vee P\overline{Q}) \vee ((\overline{P}Q \vee \overline{P}\,\overline{Q}) \vee \overline{Q})$	SR: 28 (15)
30:	$(PQ \vee P\overline{Q}) \vee (\overline{P}(Q \vee \overline{Q}) \vee \overline{Q})$	SR: 29 (9)
31:	$(PQ \vee P\overline{Q}) \vee (\overline{P}1 \vee \overline{Q})$	SR: 30 (11)

32:	$(PQ \vee P\overline{Q}\,) \vee (\overline{P} \vee \overline{Q}\,))$	SR: 31 (15)
33:	$P(Q \vee \overline{Q}\,) \vee (\overline{P} \vee \overline{Q}\,)$	SR: 32 (9)
34:	$P1 \vee (\overline{P} \vee \overline{Q}\,)$	SR: 33 (11)
35:	$P \vee (\overline{P} \vee \overline{Q}\,)$	SR: 34 (15)
36:	$(\overline{P} \vee \overline{Q}\,) \vee P$	SR: 35 (3)
37:	$\overline{P} \vee (\overline{Q} \vee P)$	SR: 36 (5)
38:	$\overline{P} \vee (Q \to P)$	SR: 37 (20)
39:	$P \to (Q \to P)$	SR: 38 (20)

This is rather painful when compared to the 7 line derivation in Example II.9.6. Looking over the steps we see that part 1 is steps 1–3, part 2 is steps 3–13, part 3 is steps 42–13, and part 4 is steps 13–42. In this case we see that part 3 is the most demanding of our resources.

So the moral of this section is: yes, we do have a straightforward algorithm to find derivations. But it is probably a much better idea to look for a short derivation taking advantage of the many rules available in PC. That is why we have so many more rules than are needed to prove completeness.