Boolean Algebra

Introduction to Logic

Some Elementary Equivalences

- Double Negation:
  - $P \Leftrightarrow \neg \neg P$
- Commutation:
  - $P \wedge Q \Leftrightarrow Q \wedge P$
  - $P \vee Q \Leftrightarrow Q \vee P$
- Association:
  - $P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \wedge R$
  - $P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$
- Idempotence:
  - $P \wedge P \Leftrightarrow P$
  - $P \vee P \Leftrightarrow P$

Some More

- DeMorgan:
  - $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
  - $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$

- Distribution:
  - $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ (Left-distribution of $\vee$ over $\wedge$)
  - $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$ (Left-distribution of $\wedge$ over $\vee$)
  - $(Q \wedge R) \vee P \Leftrightarrow (Q \vee P) \wedge (R \vee P)$ (Right-distribution of $\vee$ over $\wedge$)
  - $(Q \vee R) \wedge P \Leftrightarrow (Q \wedge P) \vee (R \wedge P)$ (Right-distribution of $\wedge$ over $\vee$)

Simplifying Statements I

- Using the principle of substitution of logical equivalents, and using the logical equivalences that we saw before (Double Negation, Association, Commutation, Idempotence, DeMorgan, Distribution, and Subsumption), we can simplify statements.

Example Simplifying Statements

- Example:

$$(A \wedge B) \wedge A$$
$$\Leftrightarrow \text{(Commutation)}$$
$$(B \wedge A) \wedge A$$
$$\Leftrightarrow \text{(Association)}$$
$$B \wedge (A \wedge A)$$
$$\Leftrightarrow \text{(Idempotence)}$$
$$B \wedge A$$

A Not so Easy One …

$$\neg A \wedge \neg\neg(\neg((A \vee B) \vee C) \wedge \neg B) \Leftrightarrow \text{(Double Negation)}$$

$$\neg A \wedge (\neg((A \vee B) \vee C) \wedge \neg B) \Leftrightarrow \text{(DeMorgan)}$$

$$\neg A \wedge ((\neg(A \vee B) \wedge \neg C) \wedge \neg B) \Leftrightarrow \text{(DeMorgan)}$$

$$\neg A \wedge (((\neg A \wedge \neg B) \wedge \neg C) \wedge \neg B) \Leftrightarrow \text{(Commutation)}$$

$$\neg A \wedge ((\neg C \wedge (\neg A \wedge \neg B)) \wedge \neg B) \Leftrightarrow \text{(Commutation)}$$

$$\neg A \wedge (\neg C \wedge ((\neg A \wedge \neg B) \wedge \neg B)) \Leftrightarrow \text{(Association)}$$

$$\neg A \wedge (\neg C \wedge (\neg A \wedge (\neg B \wedge \neg B))) \Leftrightarrow \text{(Idempotence)}$$

$$\neg A \wedge (\neg C \wedge (\neg A \wedge \neg B)) \Leftrightarrow \text{(Commutation)}$$

$$\neg A \wedge ((\neg A \wedge \neg B) \wedge \neg C) \Leftrightarrow \text{(Association)}$$

$$\neg A \wedge (\neg A \wedge (\neg B \wedge \neg C)) \Leftrightarrow \text{(Association)}$$

$$(\neg A \wedge \neg A) \wedge (\neg B \wedge \neg C) \Leftrightarrow \text{(Idempotence)}$$

$$\neg A \wedge (\neg B \wedge \neg C)$$

Generalized Conjunctions and Generalized Disjunctions

- Recall the Association equivalences:
  - $P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \wedge R$
  - $P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$

- Because of this, we'll allow to drop brackets:
  - $P \wedge Q \wedge R$
  - $P \vee Q \vee R$

- We can generalize conjunctions and disjunctions
  - A generalized conjunction (disjunction) can have any number of conjuncts (disjuncts)

Simplifying Statements II

- Many of the equivalence rules can be generalized in a completely intuitive and straightforward manner to generalized conjunctions and disjunctions.
- Example:
  - Generalized Commutation:
    - $P \wedge Q \wedge R \Leftrightarrow R \wedge P \wedge Q \Leftrightarrow Q \wedge R \wedge P \Leftrightarrow \ldots$ (swap any way!)
  - Generalized DeMorgan:
    - $\neg(P \wedge Q \wedge R) \Leftrightarrow \neg P \vee \neg Q \vee \neg R$
    - $\neg(P \vee Q \vee R) \Leftrightarrow \neg P \wedge \neg Q \wedge \neg R$

Let's do that not so easy one again:

$$\neg A \wedge \neg\neg(\neg((A \vee B) \vee C) \wedge \neg B)$$

$\Leftrightarrow$ (Double Negation)

$$\neg A \wedge (\neg((A \vee B) \vee C) \wedge \neg B)$$

$\Leftrightarrow$ (Association (drop parentheses))

$$\neg A \wedge \neg(A \vee B \vee C) \wedge \neg B$$

$\Leftrightarrow$ (Generalized DeMorgan)

$$\neg A \wedge (\neg A \wedge \neg B \wedge \neg C) \wedge \neg B$$

$\Leftrightarrow$ (Association (drop parentheses))

$$\neg A \wedge \neg A \wedge \neg B \wedge \neg C \wedge \neg B$$

$\Leftrightarrow$ (Gen'd Commutation)

$$\neg A \wedge \neg A \wedge \neg B \wedge \neg B \wedge \neg C$$

$\Leftrightarrow$ (Association (add parentheses))

$$(\neg A \wedge \neg A) \wedge (\neg B \wedge \neg B) \wedge \neg C$$

$\Leftrightarrow$ (Idempotence x 2)

$$\neg A \wedge \neg B \wedge \neg C$$

Still rather tedious …
So, I'll allow short-cuts when things are 'obvious'
E.g. No need for Commutation to 'group' terms to be combined
No need for an explicit Association to add or drop parentheses
Also, there is no need to use 'Generalized …' in justifications
So, the same problem from the previous slide can be done as:

$$\neg A \wedge \neg\neg(\neg(A \vee B \vee C) \wedge \neg B)$$
$$\Leftrightarrow \text{ (Double Negation)}$$
$$\neg A \wedge \neg(A \vee B \vee C) \wedge \neg B$$
$$\Leftrightarrow \text{ (DeMorgan)}$$
$$\neg A \wedge \neg A \wedge \neg B \wedge \neg C \wedge \neg B$$
$$\Leftrightarrow \text{ (Idempotence x 2)}$$
$$\neg A \wedge \neg B \wedge \neg C$$

Ah, that's more like it!

‘⊤’ and ‘⊥’

- A generalized conjunction is false if it has at least one false conjunct, otherwise it is true.
  - So, a generalized conjunction with 0 conjuncts cannot have a false conjunct, and hence cannot be false. Therefore, it is a tautology! We will write this as ‘⊤’.
- A generalized disjunction is true if it has at least one true disjunct, otherwise it is false.
  - Hence, a generalized disjunction with 0 disjuncts can never be true, and is therefore a contradiction! We will write this as ‘⊥’.

Some equivalences involving '$\top$' and '$\bot$'

- Complement
  - $P \wedge \neg P \Leftrightarrow \bot$
  - $P \vee \neg P \Leftrightarrow \top$
- Inverse
  - $\neg \bot \Leftrightarrow \top$
  - $\neg \top \Leftrightarrow \bot$
- Identity
  - $P \wedge \top \Leftrightarrow P$
  - $P \vee \bot \Leftrightarrow P$
- Annihilation
  - $\bot \wedge P \Leftrightarrow \bot$
  - $\top \vee P \Leftrightarrow \top$

$$\neg(\neg A \vee \neg(\neg B \wedge (\neg A \vee B)))$$

$$\Leftrightarrow \text{(DeMorgan)}$$

$$\neg\neg A \wedge \neg\neg(\neg B \wedge (\neg A \vee B))$$

$$\Leftrightarrow \text{(Double Neg. x 2)}$$

$$A \wedge \neg B \wedge (\neg A \vee B)$$

$$\Leftrightarrow \text{(Distribution)}$$

$$(A \wedge \neg B \wedge \neg A) \vee (A \wedge \neg B \wedge B)$$

$$\Leftrightarrow \text{(Complement x 2)}$$

$$(\bot \wedge \neg B) \vee (A \wedge \bot)$$

$$\Leftrightarrow \text{(Annihilation x 2)}$$

$$\bot \vee \bot$$

$$\Leftrightarrow \text{(Idempotence (or Identity))}$$

$$\bot$$

Distribution: ‘FOIL’

$$(A \wedge B) \vee (C \wedge D)$$

$$\Leftrightarrow \text{ (Distribution)}$$

$$[(A \wedge B) \vee C] \wedge [(A \wedge B) \vee D]$$

$$\Leftrightarrow \text{ (Distribution x 2)}$$

$$(A \vee C) \wedge (A \vee D) \wedge (B \vee C) \wedge (B \vee D)$$

So:

$$(A \wedge B) \vee (C \wedge D)$$

$$\Leftrightarrow \text{ (Distribution)}$$

$$(A \vee C) \wedge (A \vee D) \wedge (B \vee C) \wedge (B \vee D)$$

Generalized Distribution

The 'FOIL' principle completely generalizes to generalized conjunctions and disjunctions. Examples:

$$(A \wedge B) \vee (C \wedge D \wedge E)$$

$$\Leftrightarrow \quad \text{(Distribution)}$$

$$(A \vee C) \wedge (A \vee D) \wedge (A \vee E) \wedge (B \vee C) \wedge (B \vee D) \wedge (B \vee E)$$

$$(A \wedge B) \vee (C \wedge D) \vee (E \wedge F)$$

$$\Leftrightarrow \quad \text{(Distribution)}$$

$$(A \vee C \vee E) \wedge (A \vee C \vee F) \wedge (A \vee D \vee E) \wedge (A \vee D \vee F) \wedge$$
$$(B \vee C \vee E) \wedge (B \vee C \vee F) \wedge (B \vee D \vee E) \wedge (B \vee D \vee F)$$

Common Pitfall with Distribution

- Many students think of Distribution going only one way, i.e. as $P \vee (Q \wedge R) \Rightarrow (P \vee Q) \wedge (P \vee R)$
- As such, I often see something like this:

  $(P \vee Q) \wedge (P \vee \neg Q)$

  $\Leftrightarrow$ (Distribution)

  $(P \wedge P) \vee (P \wedge \neg Q) \vee (Q \wedge P) \vee (Q \wedge \neg Q)$

  $\Leftrightarrow$(Idempotence, Complement)

  $P \vee (P \wedge \neg Q) \vee (Q \wedge P) \vee \bot$

  $\Leftrightarrow$(Identity)

  $P \vee (P \wedge \neg Q) \vee (Q \wedge P)$

  … so you think you're making good progress …

  … but you're not!

‘Reverse’ Distribution

- Do not forget that Distribution is an *equivalence*, i.e. it goes *both* ways.
- In particular, as an instance of Distribution, you *also* have: $(P \vee Q) \wedge (P \vee R) \Rightarrow P \vee (Q \wedge R)$
- Of course, this does not *feel* like ‘distribution’ (hence, it is understandable that many students think of distribution going only one way), but more like a ‘reverse Distribution’ or ‘un-Distribution’ or ‘Collect Common Terms’
- …. But we will still call it ‘Distribution’!

Example
(same problem as before)

$(P \vee Q) \wedge (P \vee \neg Q)$
$\Leftrightarrow$ (('reverse') Distribution!)
$P \vee (Q \wedge \neg Q)$
$\Leftrightarrow$ (Complement)
$P \vee \bot$
$\Leftrightarrow$ (Identity)
P

Ha! ☺

Another Common Pitfall

$P \wedge (P \vee Q)$
$\Leftrightarrow$(Distribution)
$(P \wedge P) \vee (P \wedge Q)$
$\Leftrightarrow$(Idempotence)
$P \vee (P \wedge Q)$
$\Leftrightarrow$(Distribution)
$(P \vee P) \wedge (P \vee Q)$
$\Leftrightarrow$(Idempotence)
$P \wedge (P \vee Q)$
… back at the beginning …
… so you're going in one big circle!

Instead:

$P \wedge (P \vee Q)$

$\Leftrightarrow$ (Identity)

$(P \wedge \top) \vee (P \wedge Q)$

$\Leftrightarrow$ (Distribution)

$P \wedge (\top \vee Q)$

$\Leftrightarrow$ (Annihilation)

$P \wedge \top$

$\Leftrightarrow$ (Identity)

P

Ha! ☺

One more Nice one

$P \wedge (\neg P \vee Q)$
$\Leftrightarrow$ (Distribution)
$(P \wedge \neg P) \vee (P \wedge Q)$
$\Leftrightarrow$ (Complement)
$\bot \vee (P \wedge Q)$
$\Leftrightarrow$ (Identity)
$P \wedge Q$

Ha! ☺

Three Handy Equivalences

The three ‘nice’ equivalences we found:

- Absorption:
  - $P \wedge (P \vee Q) \Leftrightarrow P$
  - $P \vee (P \wedge Q) \Leftrightarrow P$

  (the P term ‘absorbs’ the other term)

- Reduction :
  - $P \wedge (\neg P \vee Q) \Leftrightarrow P \wedge Q$
  - $P \vee (\neg P \wedge Q) \Leftrightarrow P \vee Q$

  (in the context of P, the second term gets ‘reduced’ to a simpler term)

- Adjacency :
  - $(P \wedge Q) \vee (P \wedge \neg Q) \Leftrightarrow P$
  - $(P \vee Q) \wedge (P \vee \neg Q) \Leftrightarrow P$

  (in a K-map, the two terms form ‘adjacent’ cells and can thus be combined to one)

Exercise

- Simplify the following statement:

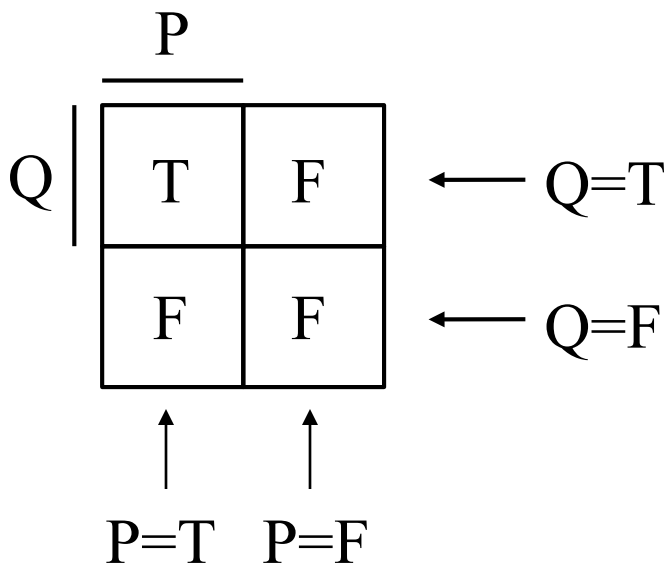
$$(\neg A \vee B) \wedge (A \vee B \vee D) \wedge \neg D$$

K-Maps

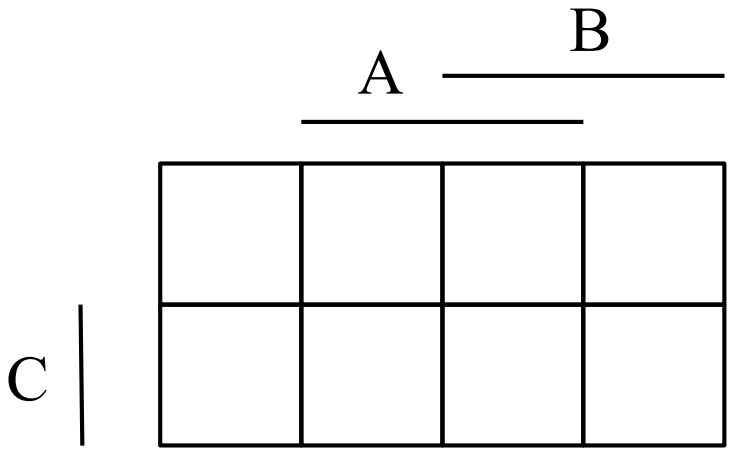
Karnaugh Map (K-Map)

A K-map is a diagrammatic way of representing a Boolean function
… it is kind of like a truth-table
… but it represents the truth-function in a ‘clever’ way so you can simplify more easily

Here is a K-map for $P \wedge Q$:

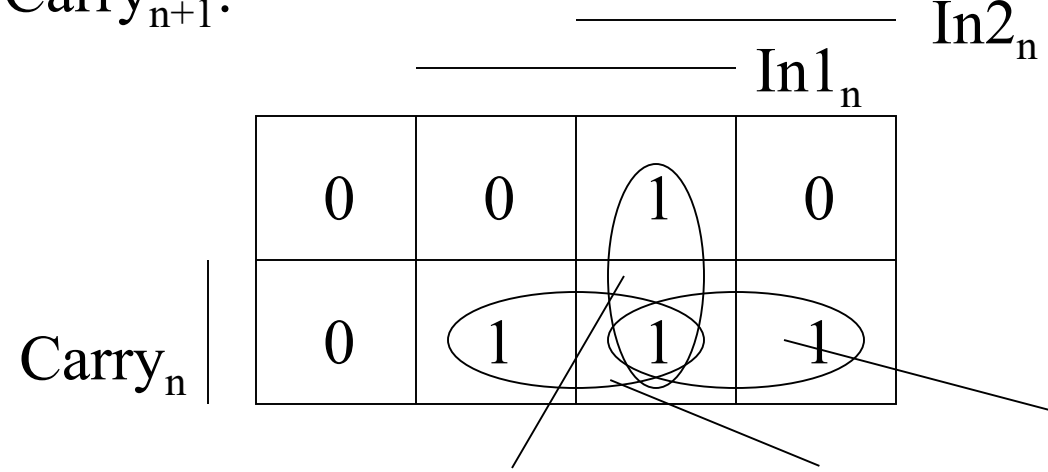


Karnaugh Maps (K-Maps)



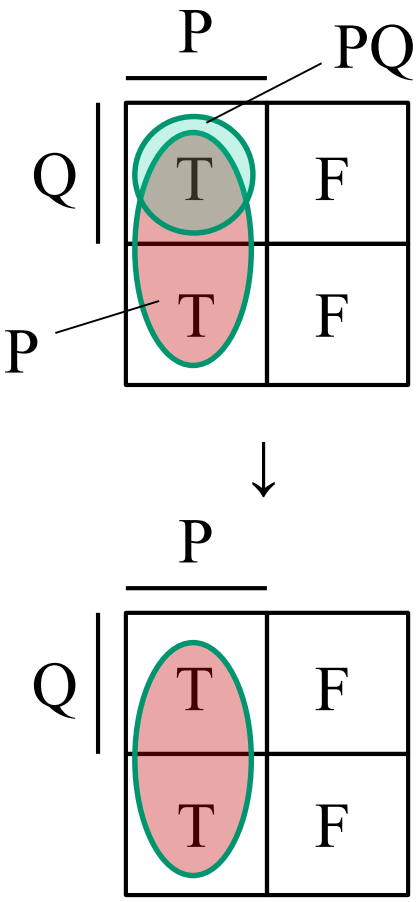
To find a small (if not ‘minimal’) expression for a function, try to ‘group’ the T’s (1’s) in groups (rectangles) of powers of two .. Those can be represented with small terms. The larger the group, the smaller the expression.

$Carry_{n+1}$:



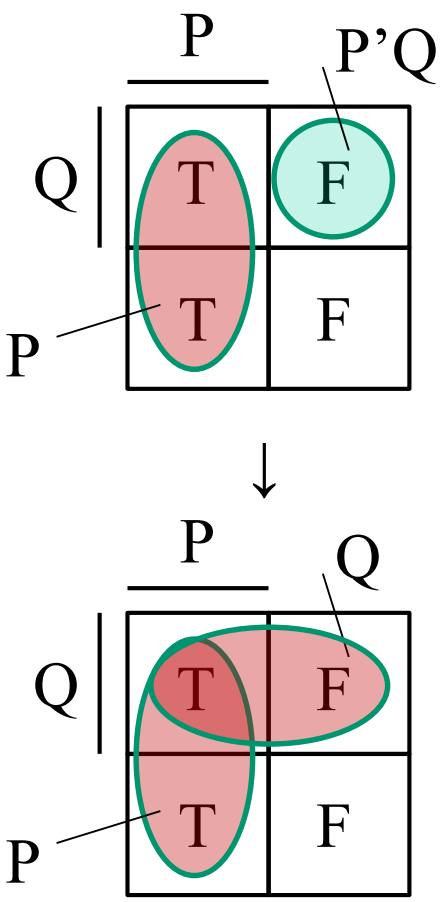
→ $Carry_{n+1} = (In1_n \wedge In2_n) \vee (In1_n \wedge Carry_n) \vee (In2_n \wedge Carry_n)$

Absorption:



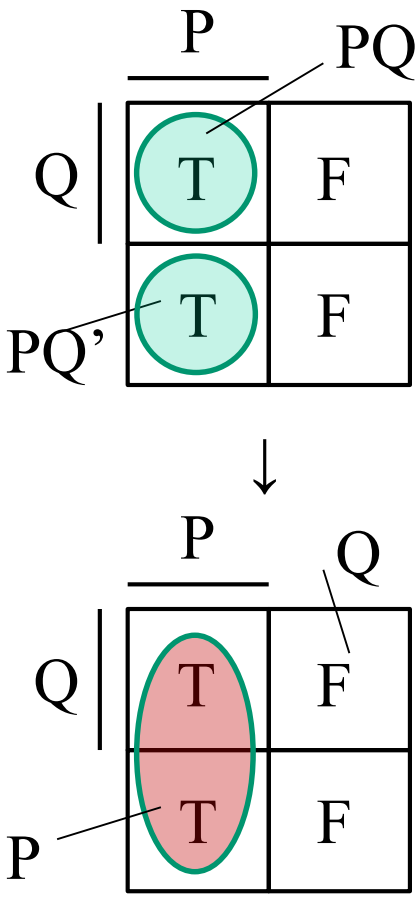
P+PQ=P

Reduction:



P+P'Q=P+Q

Adjacency:



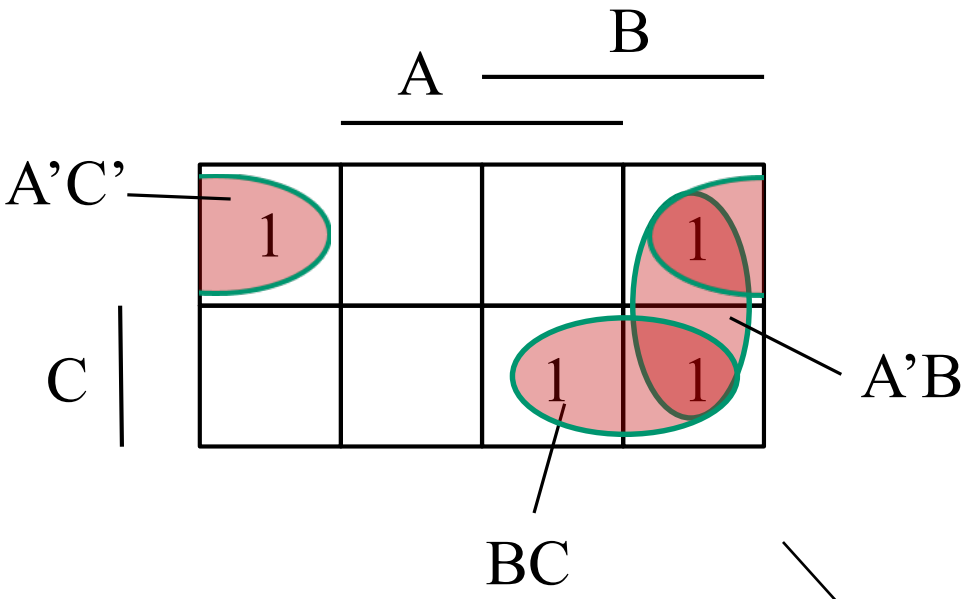
PQ+PQ'=P

Consensus Theorem

- Here is an interesting theorem:
  - $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R) \Leftrightarrow$
    $(P \wedge Q) \vee (\neg P \wedge R)$

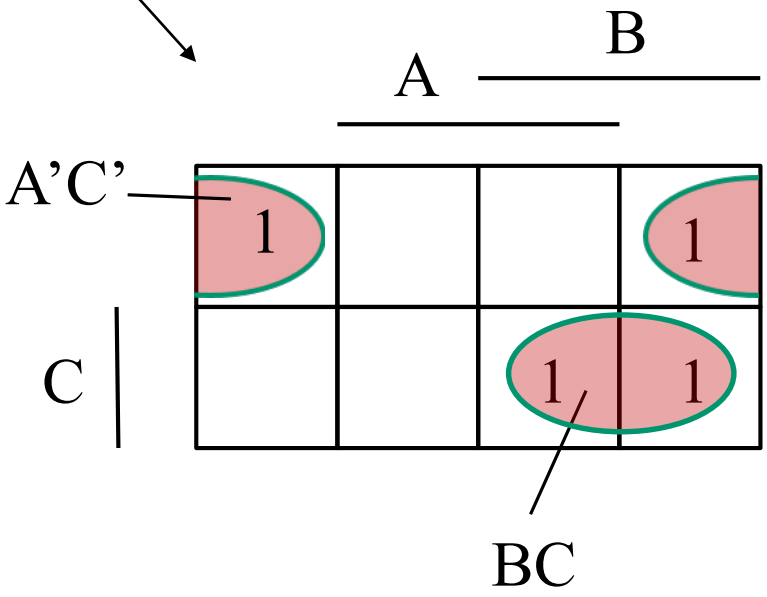
Proof:

$(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$
$\Leftrightarrow$ (Adjacency)
$(P \wedge Q) \vee (\neg P \wedge R) \vee (P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge R)$
$\Leftrightarrow$ (Absorption x 2)
$(P \wedge Q) \vee (\neg P \wedge R)$



$$A'C' + BC + A'B = A'C' + AB$$

(Consensus)



Reduction through Consensus and Absorption

$P \wedge (\neg P \vee Q)$
$\Leftrightarrow$ (Identity)
$(\bot \vee P) \wedge (\neg P \vee Q)$
$\Leftrightarrow$ (Consensus)
$(\bot \vee P) \wedge (\neg P \vee Q) \wedge (\bot \vee Q)$
$\Leftrightarrow$ (Identity x 2)
$P \wedge (\neg P \vee Q) \wedge Q$
$\Leftrightarrow$ (Absorption)
$P \wedge Q$

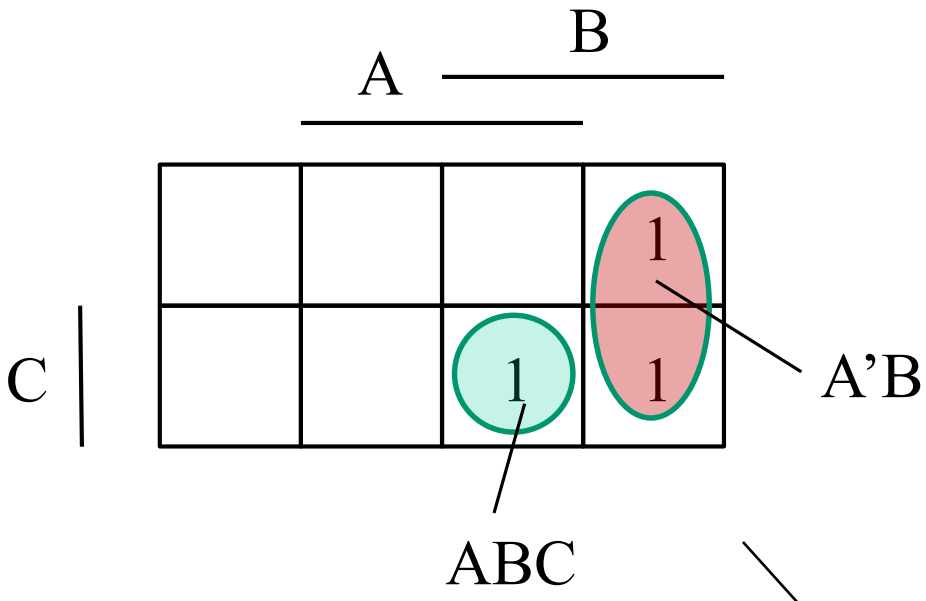
Nested Reduction

$(P \vee Q) \wedge (\neg P \vee Q \vee R)$
$\Leftrightarrow$ (Distribution)
$Q \vee (P \wedge (\neg P \vee R))$
$\Leftrightarrow$ (Reduction)
$Q \vee (P \wedge R)$
$\Leftrightarrow$ (Distribution)
$(P \vee Q) \wedge (Q \vee R)$

So:

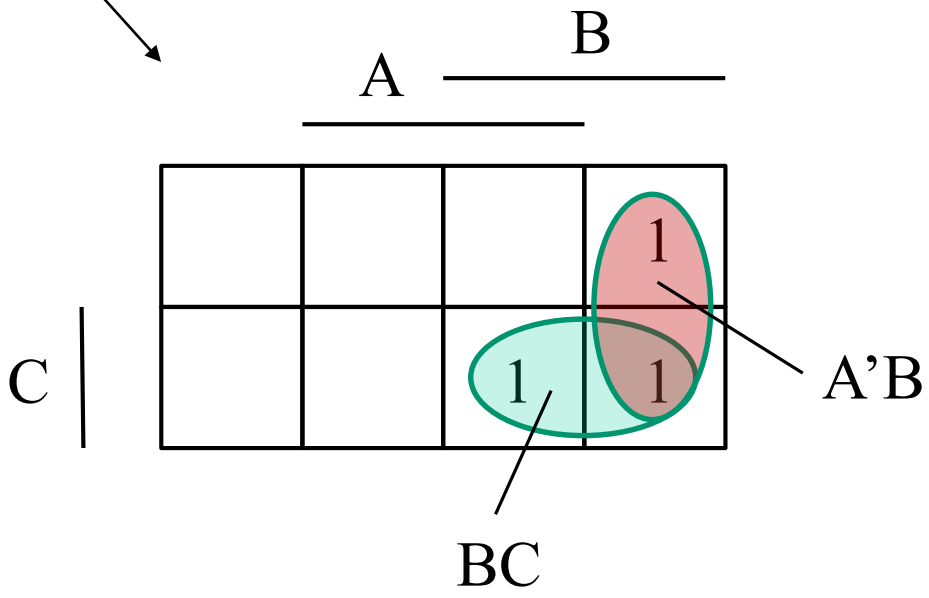
$(P \vee Q) \wedge (\neg P \vee Q \vee R) \Leftrightarrow (P \vee Q) \wedge (Q \vee R)$

We can call this Nested (or Contextualized) Reduction



So: ABC + A'B = BC + A'B

(nested Reduction)



Nested Reduction through Consensus and Absorption

$(P \vee Q) \wedge (\neg P \vee Q \vee R)$
$\Leftrightarrow$ (Consensus)
$(P \vee Q) \wedge (\neg P \vee Q \vee R) \wedge (Q \vee Q \vee R)$
$\Leftrightarrow$ (Idempotence)
$(P \vee Q) \wedge (\neg P \vee Q \vee R) \wedge (Q \vee R)$
$\Leftrightarrow$ (Absorption)
$(P \vee Q) \wedge (Q \vee R)$

Nested Consensus

$(P \wedge Q \wedge S) \vee (\neg P \wedge R \wedge S) \vee (Q \wedge R \wedge S)$
$\Leftrightarrow$ (Distribution)
$S \wedge ((P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R))$
$\Leftrightarrow$ (Consensus)
$S \wedge ((P \wedge Q) \vee (\neg P \wedge R))$
$\Leftrightarrow$ (Distribution)
$(P \wedge Q \wedge S) \vee (\neg P \wedge R \wedge S)$

So:

$(P \wedge Q \wedge S) \vee (\neg P \wedge R \wedge S) \vee (Q \wedge R \wedge S)$
$\Leftrightarrow (P \wedge Q \wedge S) \vee (\neg P \wedge R \wedge S)$

We can call this Nested (or Contextualized) Consensus

Transposition Theorem

$(A \wedge B) \vee (\neg A \wedge C)$

$\Leftrightarrow$ (FOIL)

$(A \vee \neg A) \wedge (A \vee C) \wedge (\neg A \vee B) \wedge (B \vee C)$

$\Leftrightarrow$ (Complement)

$\top \wedge (A \vee C) \wedge (\neg A \vee B) \wedge (B \vee C)$

$\Leftrightarrow$ (Identity)

$(A \vee C) \wedge (\neg A \vee B) \wedge (B \vee C)$

$\Leftrightarrow$ (Consensus)

$(A \vee C) \wedge (\neg A \vee B)$

So:

$(A \wedge B) \vee (\neg A \wedge C) \Leftrightarrow$

$(A \vee C) \wedge (\neg A \vee B)$

Transposition Theorem

Reduction through Transposition Theorem

$P \wedge (\neg P \vee Q)$
$\Leftrightarrow$ (Identity)
$(P \vee \bot) \wedge (\neg P \vee Q)$
$\Leftrightarrow$ (Transposition Theorem)
$(P \wedge Q) \vee (\neg P \wedge \bot)$
$\Leftrightarrow$ (Annihilation)
$(P \wedge Q) \vee \bot$
$\Leftrightarrow$ (Identity)
$P \wedge Q$

Equivalences Involving Conditionals

Some Important Equivalences Involving Conditionals

- Implication:
  - $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
  - $\neg(P \rightarrow Q) \Leftrightarrow P \wedge \neg Q$
- Contraposition (or Transposition):
  - $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
- Exportation:
  - $P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R$
- Equivalence:
  - $P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$
  - $P \leftrightarrow Q \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$

Some More Equivalences

- Distribution:
  - $P \rightarrow (Q \wedge R) \Leftrightarrow (P \rightarrow Q) \wedge (P \rightarrow R)$
  - $P \rightarrow (Q \vee R) \Leftrightarrow (P \rightarrow Q) \vee (P \rightarrow R)$
  - $(P \vee Q) \rightarrow R \Leftrightarrow (P \rightarrow R) \wedge (Q \rightarrow R)$
  - $(P \wedge Q) \rightarrow R \Leftrightarrow (P \rightarrow R) \vee (Q \rightarrow R)$ (this last one is a good example of the paradox of material implication!)

- Conditional Reduction:
  - $(P \rightarrow Q) \wedge P \Leftrightarrow P \wedge Q$
  - $(P \rightarrow Q) \wedge \neg Q \Leftrightarrow \neg P \wedge \neg Q$

Also:

$P \rightarrow P \Leftrightarrow \top$

$P \rightarrow \neg P \Leftrightarrow \neg P$

$P \rightarrow \bot \Leftrightarrow \neg P$

$P \rightarrow \top \Leftrightarrow \top$

$\top \rightarrow P \Leftrightarrow P$

$\bot \rightarrow P \Leftrightarrow \top$

Demonstration of Aris

The Substitution Theorem and the Replacement Theorem

Substituting Arbitrary Sentences for ‘P’ and ‘Q’

- Notice that when doing algebra, we assumed that P $\Leftrightarrow \neg \neg$ P is a general principle, i.e. that the ‘P’ could be any other sentence.
- This is why we may want to write $\varphi \Leftrightarrow \neg\neg\varphi$
- But is this more general principle the case? And how would we prove it?
- In particular, while a truth-table can easily be used to show P $\Leftrightarrow \neg \neg$ P, what if P is a complex sentence? Shouldn’t we be worried that possibly the interplay of the atomic variables can change the outcome?
  - E.g. the truth-table for ‘P’ shows that ‘P’ is a contingency. But it is false to infer that therefore any φ is a contingency!

Proving General Equivalences

- One solution is to use formal semantics
- For example, using formal semantics, we can prove $\varphi \Leftrightarrow \neg\neg\varphi$:

  Consider any φ and h. We have:

  $h \models \varphi$ iff (semantics $\neg$)

  $h \not\models \neg\varphi$ iff (semantics $\neg$)

  $h \models \neg\neg\varphi$
- OK, but do we have to do this for all equivalences?

The Substitution Theorem

- Something else we can do is to use the Substitution Theorem:
  - Where P is an atomic sentence, where $S_1(P)$ is a sentence containing P, where $S_2(P)$ another sentence containing P, and where φ is an arbitrary sentence:
    - If $S_1(P) \Leftrightarrow S_2(P)$, then $S_1(\varphi) \Leftrightarrow S_2(\varphi)$
- It turns out that the Substitution Theorem can be proven, but proving it is far from trivial! (we'll do the proof next week)

The Principle of Substitution of Logical Equivalents

- Another thing we have assumed all along is the *principle of substitution of logical equivalents*:
  - if $\varphi \Leftrightarrow \psi$, then $S(\varphi) \Leftrightarrow S(\psi)$

  Where $S(\varphi)$ is a statement that contains zero or more instances of φ as a component statement, and $S(\psi)$ the statement that results from replacing zero or more instances of φ with ψ
- This result is called the Replacement Theorem
  - *not* to be confused with the Substitution Theorem!

Proof of Replacement Theorem

- Take any φ and ψ for which $\varphi \Leftrightarrow \psi$.
- First: For any sentence $S(\varphi)$ for which $S(\varphi) = \varphi$, we have that $S(\psi) = \varphi$ (if we don't replace φ with ψ), or $S(\psi) = \psi$ (in case we do). But in either case, it is clear that $S(\varphi) \Leftrightarrow S(\psi)$
- We'll use mathematical induction over the recursive syntactical formation of sentences, that for any sentence $S(\varphi)$ that contains zero or more instances of φ as a *strict* component, we have that $S(\varphi) \Leftrightarrow S(\psi)$
  - Base: if $S(\varphi)$ = atomic, $\bot$, or $\top$, then it is impossible

Base

- If $S(\varphi)$ = atomic, $\bot$, or $\top$, then it is impossible for it to contain φ as a strict component. Thus, no substitutions are possible, and therefore $S(\psi) = S(\varphi)$, meaning that $S(\varphi) \Leftrightarrow S(\psi)$

Step

- If $S(\varphi)$ is compound, then one of the following is the case:
  - $S(\varphi) = \neg S_1(\varphi)$ for some $S_1(\varphi)$
  - $S(\varphi) = S_1(\varphi) \wedge S_2(\varphi)$ for some $S_1(\varphi)$ and $S_2(\varphi)$
  - $S(\varphi) = S_1(\varphi) \vee S_2(\varphi)$ for some $S_1(\varphi)$ and $S_2(\varphi)$
  - Etc.
- We'll now show that in each case, we have $S(\varphi) \Leftrightarrow S(\psi)$, based on the Inductive Hypothesis.

Step (Continued)

- Let's consider the case $S(\varphi) = \neg S_1(\varphi)$ for some $S_1(\varphi)$
- We need to show that for if we replace zero or instances of φ as a strict component of $S(\varphi)$, we get $S(\varphi) \Leftrightarrow S(\psi)$
- Now, for φ to be a strict component of $S(\varphi) = \neg S_1(\varphi)$, it must be a component of $S_1(\varphi)$, and hence it must also be the case that $S(\psi) = \neg S_1(\psi)$
  - In case that $S_1(\varphi) = \varphi$, we already showed that $S_1(\varphi) \Leftrightarrow S_1(\psi)$
  - And by Inductive Hypothesis, if φ is a strict component of $S_1(\varphi)$, we have $S_1(\varphi) \Leftrightarrow S_1(\psi)$
  - So, in either case, we have $S_1(\varphi) \Leftrightarrow S_1(\psi)$
- But that means that $\neg S_1(\varphi) \Leftrightarrow \neg S_1(\psi)$, meaning that $S(\varphi) \Leftrightarrow S(\psi)$

Another Case of the Step

- Suppose $S(\varphi) = S_1(\varphi) \wedge S_2(\varphi)$
- Again, for φ to be a strict component of $S(\varphi) = S_1(\varphi) \wedge S_2(\varphi)$ it must be a component of $S_1(\varphi)$ and/or $S_2(\varphi)$, and we must also have that $S(\psi) = S_1(\psi) \wedge S_2(\psi)$
  - In case that $S_1(\varphi) = \varphi$, we already showed $\Leftrightarrow S_1(\psi)$. Same for the case that $S_2(\varphi) = \varphi$
  - And by Inductive Hypothesis, if φ is a strict component of $S_1(\varphi)$, we have $S_1(\varphi) \Leftrightarrow S_1(\psi)$. Likewise, $S_2(\varphi) \Leftrightarrow S_2(\psi)$.
  - So, we have $S_1(\varphi) \Leftrightarrow S_1(\psi)$ and $S_2(\varphi) \Leftrightarrow S_2(\psi)$.
- We can show that (Lemma): if $\varphi_1 \Leftrightarrow \psi_1$ and $\varphi_2 \Leftrightarrow \psi_2$, then $\varphi_1 \wedge \varphi_2 \Leftrightarrow \psi_1 \wedge \psi_2$
  - Hence, $S(\varphi) = S_1(\varphi) \wedge S_2(\varphi) \Leftrightarrow$ (Lemma) $S_1(\psi) \wedge S_2(\psi) = S(\psi)$