Excursions in Computing Science:
Week 10. The laws of thought

T. H. Merrett[*]
McGill University, Montreal, Canada

May 24, 2022

I. Prefatory Notes

1. Let's take a look at a strange new algebra. We'll give it first in terms of the formal rules, or *axioms*, it obeys.

- operators +, . are
  (a) commutative
  (b) associative
- ! (c) identities: 0 for +; 1 for .; and

$$\begin{aligned} X+1 &= 1 \\ X.0 &= 0 \end{aligned}$$

- ! (d) *mutually* distributive:

$$\begin{aligned} X.(Y+Z) &= X.Y+X.Z \\ X+Y.Z &= (X+Y).(X+Z) \end{aligned}$$

- ! (e) absorptive:

$$\begin{aligned} X+X.Y &= X \\ X.(X+Y) &= X \end{aligned}$$

- ! (f) unary operator $'$ ("complement")

$$\begin{aligned} X+X' &= 1 \\ X.X' &= 0 \end{aligned}$$

From this (treating the rules formally as if for a game such as chess)

The author gratefully acknowledges support from the taxpayers of Québec and of Canada who have paid his salary and research grants while this work was developed at McGill University, and from his students and their funding agencies.

(1)

$$\begin{aligned} X+0 &= X+X.X' = X \\ X.1 &= X.(X+X') = X \end{aligned}$$

(2) if $X+Y=1$ and $X.Y=0$ then $Y=X'$:

$$\begin{aligned} Y &= Y.1 = Y.(X+X') = Y.X+Y.X' \\ &= 0+Y.X' = X.X'+Y.X' \\ &= (X+Y).X' = X' \end{aligned}$$

(2a) $Y=Y''$:
combine (2) and (f) (set $X=Y'$).

(2b)

$$\begin{aligned} (X+Y)' &= X'.Y' \\ (X.Y)' &= X'+Y' \end{aligned}$$

De Morgan's laws. These follow from (2), since:

$$\begin{aligned} (X+Y)+X'.Y' &\overset{(d)}{=} ((X+Y)+X').((X+Y)+Y') \\ &\overset{(b)}{=} (Y+X+X').(X+Y+Y') \\ &\overset{(f)}{=} (Y+1).(X+1) \\ &\overset{(c)}{=} 1.1 \\ &= 1 \\ \text{and} & \\ (X+Y).(X'.Y') &\overset{(d)}{=} X.X'.Y'+Y.X'.Y' \\ &\overset{(f),(c)}{=} 0+0 \\ &= 0 \end{aligned}$$

2. The algebra obeying these rules is "boolean algebra" [Boo54].

The simplest example has only two elements, 0 and 1.

$$\begin{array}{c|cc} 1 & 1 & 1 \\ 0 & 0 & 1 \\ \hline + & 0 & 1 \end{array} \quad \begin{array}{c|cc} 1 & 0 & 1 \\ 0 & 0 & 0 \\ \hline . & 0 & 1 \end{array} \quad \begin{array}{c|c} 1 & 0 \\ 0 & 1 \\ \hline ' & \end{array}$$

(The existence of this particular interpretation (mathematicians call it a "model") of boolean algebra proves that the axioms (a)..(f) are *consistent*. It does not show that the axioms are *complete* or *independent*, which we do not attempt here.)

From now on, I'm going to stop using '.' as an operator and just write the operands adjacent to each other, as we normally do with multiplication in algebra. Thus $X.Y$ will henceforth be XY.

For this particular, two-valued model, we can use "truth tables" to check that the axioms apply. For instance, the second distributive law:

X	Y	Z	$X+YZ$	$(X+Y)(X+Z)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

We will now interpret +, ., and ', respectively as **or**, **and** and **not**, and we will interpret 0 and 1 as **false** and **true**, respectively.

Boolean algebra now formalizes *propositional logic* (hence Boole's motivation for titling his book *The Laws of Thought*).

Here are some example propositions, each abbreviated by a suitable letter.

L "lightspeed is the same for all observers"

R "ontogeny recapitulates phylogeny"

W "water is composed of oxygen and hydrogen"

Here are the values of each of these.

$$\begin{array}{rcll} L & = & 1 & \textbf{true} \\ R & = & 0 & \textbf{false} \quad \text{"Haeckel's Lie"} \\ W & = & 1 & \textbf{true} \end{array}$$

Here are some combinations.

$$\begin{array}{rcl} L \textbf{ or } R & = & L+R: \ \textbf{true} \\ L \textbf{ and } R & = & LR: \ \textbf{false} \\ L \textbf{ and } W & = & LW: \ \textbf{true} \\ \textbf{not } R & = & R': \ \textbf{true} \end{array}$$

3. A useful but misunderstood logical operator is *implication*.

$$\begin{array}{c|cc} 1 & 0 & 1 \\ 0 & 1 & 1 \\ \hline \rightarrow & 0 & 1 \end{array} \qquad \begin{array}{c|cc} 1 & 0 & 1 \\ 0 & 1 & 1 \\ \hline \leq & 0 & 1 \end{array}$$

Note that **false** implies anything.

Using two of the above propositions,

$$\begin{array}{rcl} \textbf{if } R \textbf{ then } L & = & R \rightarrow L: \ \textbf{true} \\ \textbf{if } L \textbf{ then } R & = & L \rightarrow R: \ \textbf{false} \end{array}$$

$\rightarrow$ is not commutative. (It is *transitive*:

$$X \rightarrow Y \textbf{ and } Y \rightarrow Z \quad \text{gives} \quad X \rightarrow Z)$$

For example,

N “x is a minimum of $f()$”

S “the slope of $f()$ at x is zero”

$$\begin{aligned} \textbf{if } N \textbf{ then } S &= N \rightarrow S: \ \textbf{true} \\ \textbf{if } S \textbf{ then } N &= S \rightarrow N: \ \textbf{false} \end{aligned}$$

(x might be the maximum)

X “x is a maximum of $f()$”

$$\begin{aligned} \textbf{if } X \textbf{ then } S &= X \rightarrow S: \ \textbf{true} \\ \textbf{if } S \textbf{ then } (X \textbf{ or } N) &= S \rightarrow (X + N): \ \textbf{false} \end{aligned}$$

Can we get → from +, ., ’ (**or**, **and**, **not**)?

X	Y	$X \rightarrow Y$
0	0	1
0	1	1
1	0	0
1	1	1

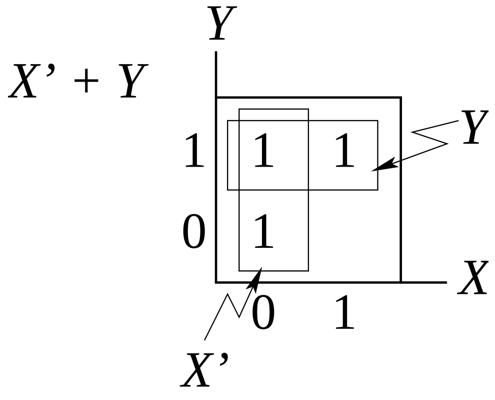
We can: for each row containing a 1 under $X \rightarrow Y$, write down the following
(if $X = 1$ then X else X')(if $Y = 1$ then Y else Y')
then take the (boolean) sum of all of these for which there was a 1 under $X \rightarrow Y$.

This gives $X \rightarrow Y$ is $X'Y' + X'Y + XY$.

We can *simplify* this using the axioms of boolean algebra.

$$\begin{aligned} X'Y' + X'Y + XY &= X'Y' + X'Y + X'Y + XY \\ &= X'(Y' + Y) + (X' + X)Y \\ &= X' + Y \end{aligned}$$

We can also simplify it visually, using a “2-cube” (a two-dimensional cube, i.e., a square).



X	Y	$X \rightarrow Y$	$X' + Y$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

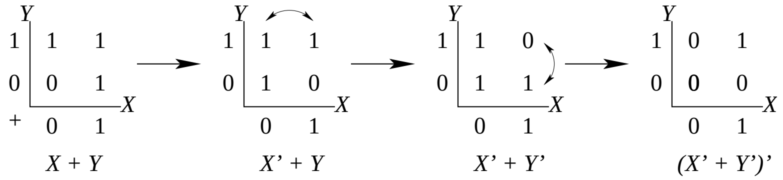
4. What is beyond →? We can find a grand total of sixteen binary operators.

false	0 0	0 0	**and**	0 1	0 0
$\not\leftarrow$ $\not\geq$	1 0	0 0	**right**	1 1	0 0
$\not\rightarrow$ $\not\leq$	0 0	0 1	**left**	0 1	0 1
xor, $\times$, $\neq$	1 0	0 1	**or**, $+$	1 1	0 1
nor	0 0	1 0	**nxor**, $=$	0 1	1 0
nleft	1 0	1 0	$\rightarrow$, $\leq$	1 1	1 0
nright	0 0	1 1	$\leftarrow$, $\geq$	0 1	1 1
nand	1 0	1 1	**true**	1 1	1 1

although six of them are not strictly binary, and only $\leq$, **xor**, **nand** and **nor** are logically interesting besides **and** and **or**. (Interpretation: e.g., X **right** $Y = Y$.

$$\begin{array}{c|cc} 1 & 1 & 1 \\ 0 & 0 & 0 \\ \hline & 0 & 1) \end{array}$$

Let's show that we don't need both **and** and **or** as basic operators, by getting **and** from **or** and **not**.



Of course, it's just de Morgan's law, but seen in a new way.

We can get unary operators from these binary ones in several ways:

fix $X = 0$ (i.e., use left column)
fix $X = 1$ (i.e., use right column)
fix $Y = 0$ (i.e., use bottom row)
fix $Y = 1$ (i.e., use top row)
fix $X = Y$ (i.e., use diagonal, bottom left to top right)

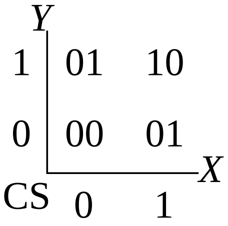
Thus X **nand** X = **not** X.

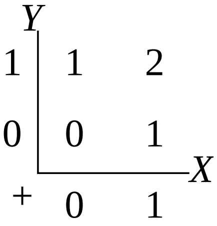
5. The two-element boolean algebra also describes *switching circuits*.

These are built from primitive elements such as **not**, **and**, **or**; or **not**, **or**; or just **nand**.
Let's build an adder out of **not**, **and**, **or**.
"Half adder", `h`, for the least significant bit; "full adder", `f`, for the other bits.

```
 fffh
 1011
+ 101
10000
```

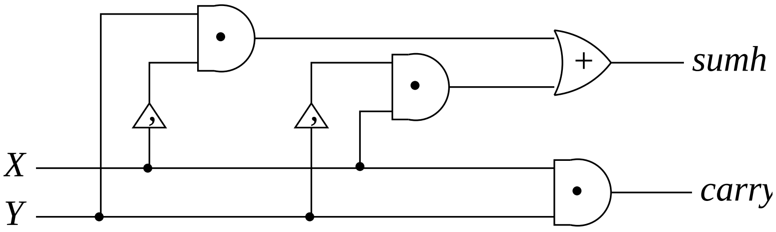
X	Y	*carry*	*sumh*
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0





This is easy:

$$\begin{aligned} carry &= XY \\ sumh &= X \textbf{ xor } Y = XY' + X'Y \end{aligned}$$



Half adder

This will do to add the first bit of each two multi-bit numbers.

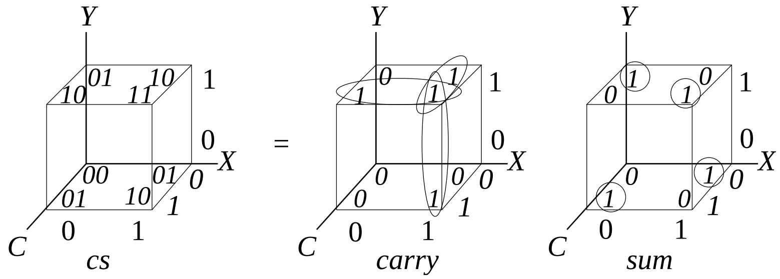
Here it is in MATLAB.

```
% function [carry,sumh] = halfadder(x,y)
% THM 060828
function [carry,sumh] = halfadder(x,y)
carry = and(x,y);
sumh  = xor(x,y);
```

To add subsequent bits requires a bunch of *full adders*

C	X	Y	*carry*	*sum*
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

(Note: *carry* $= \geq 2$ bits are on;
sum = odd # bits are on.)



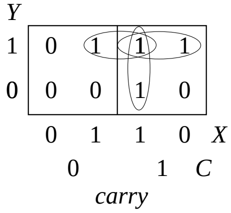
Carry is made up of three 1-dimensional pairs, each requiring only $3 - 1 = 2$ variables:

$$\textit{carry} \ = CX + CY + XY$$

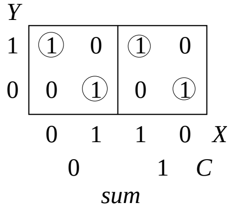
Sum is made up of four 0-dimensional pieces, so it cannot be simplified: each requires $3 - 0 = 3$ variables:

$$\textit{sum} \ = CX'Y' + C'XY' + C'X'Y + CXY$$

Since some of us are straining at these three-dimensional representations, and since four or more input variables would require four or more dimensions, where we would all have difficulty, let's look at a 2-D encoding of 3, 4, 5, .. dimensions: the *Karnaugh map.*

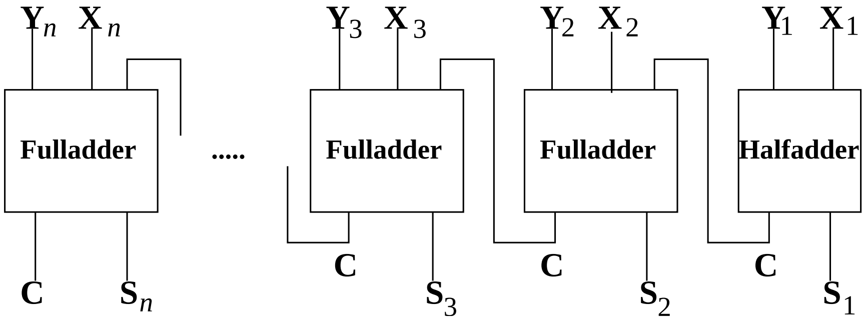


carry



sum

Once we have both halfadder and fulladder, we can add any number of bits.



6. Reversibility

None of our binary operators is reversible: given the output we cannot reconstruct the inputs. Charles Bennett showed in 1973 that a reversible calculation can be done, in principle, consuming *no* energy, so reversibility is significant.

Which of our boolean operations is reversible?

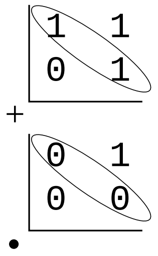
- **not**: $X'' = X$

This is a unary operator: 1 input → 1 output.

Binary operators give only 1 output for 2 inputs, so they cannot be reversible.

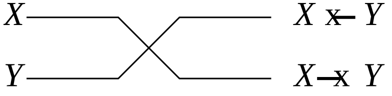
What if we combine them?

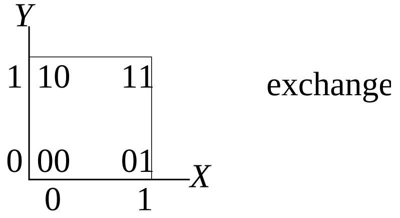
X	Y	$X+Y$	XY
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1



In the rectangle in the truth table (and the ellipses in the operator tables), $X+Y$ and XY stay the same, but give different results for X and Y: thus **or** (+) and **and** (.) cannot be combined in any way to give back X and Y.

We could invent a binary operator with two outputs which is reversible, such as *exchange.*

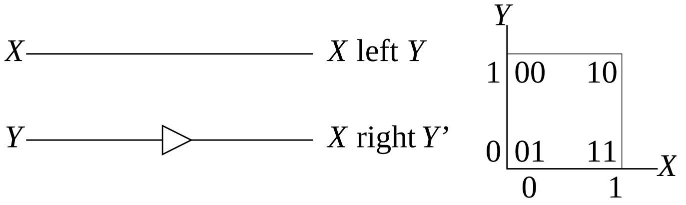




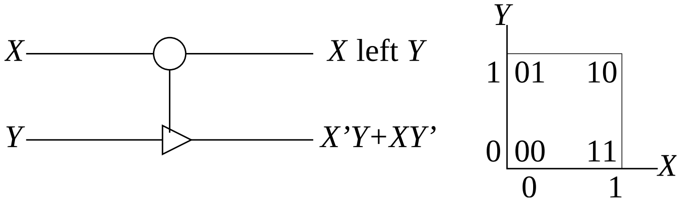
X	Y	$X \times\!-Y$	$X -\!\times Y$
0	0	0	0
0	1	1	0
1	0	0	1
1	1	1	1

but this does not at first seem interesting: we certainly cannot get **and**, **or** or **not** out of this, or any of the operators that generate a boolean algebra.

Similarly apparently trivial is



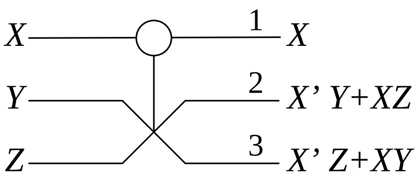
But what about a "controlled not" (**CN**)?



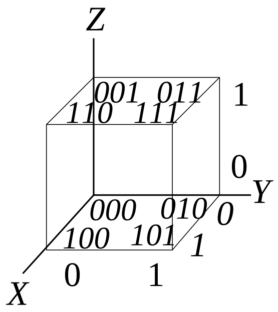
Now we're getting an **xor**: that does not generate a boolean algebra but it is at least less trivial.

How about 3 inputs and 3 outputs?

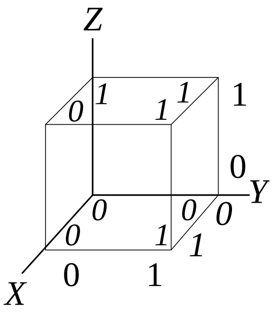
A "controlled exchange" (**CX**) operator.



Fredkin (controlled exchange)

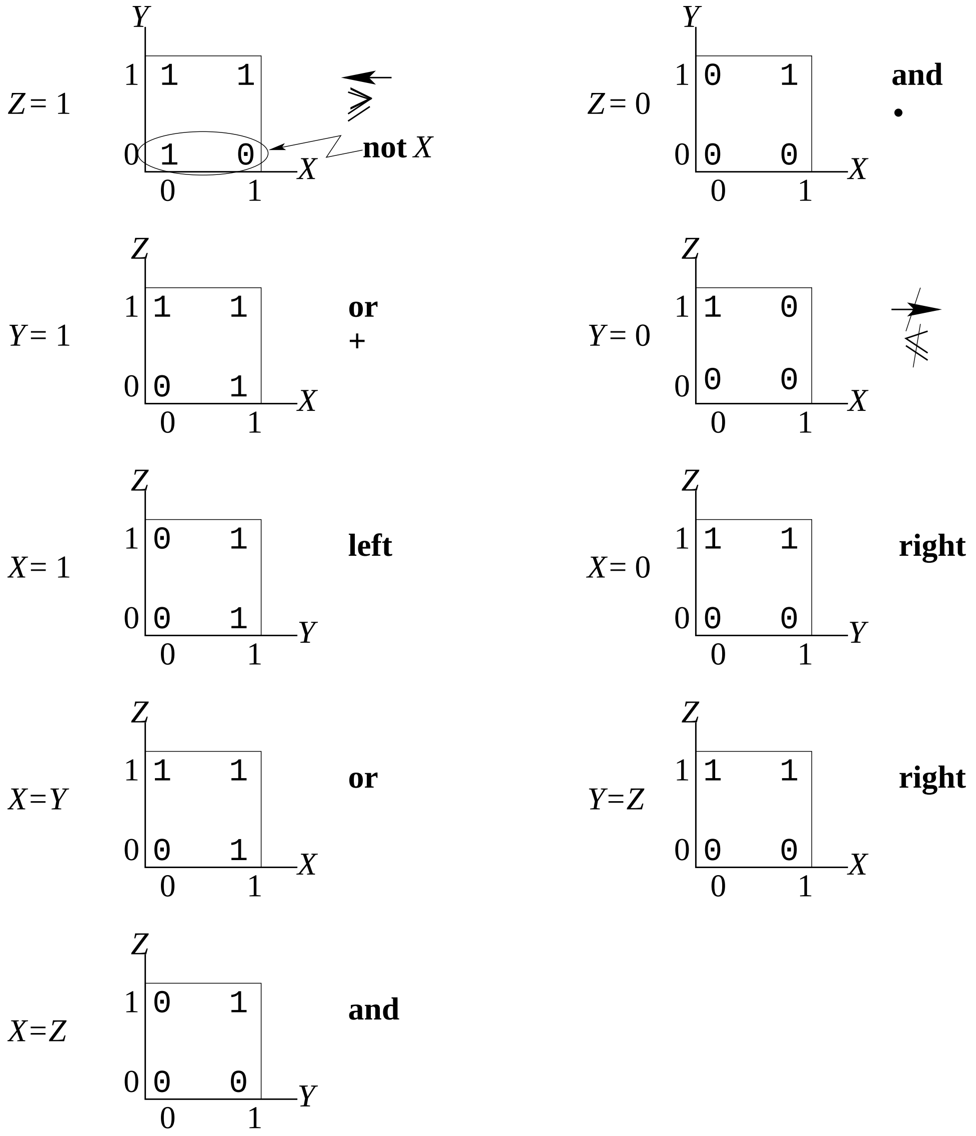


CX $\boxed{123}$



output 3

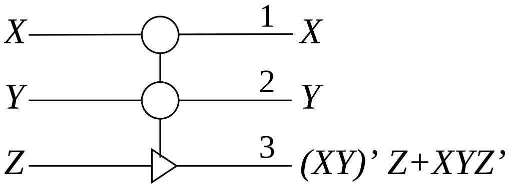
I've pulled out output 3 so that we can look at it from various points of view, which give different binary operators.



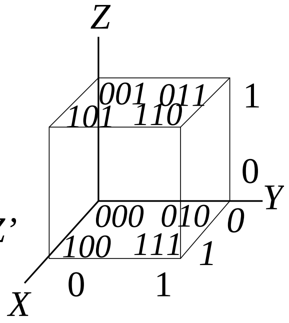
This third output can give us **or**, **and** and even **not** if we consider the 1-dimensional result for $Y = 0$ and $Z = 1$. It also gives implication and other operators.

Thus, the **CX** operator is reversible and contains all of boolean algebra. It is a reversible and *universal* operator.

Another reversible operator is "controlled controlled not" (**CCN** or Toffoli).

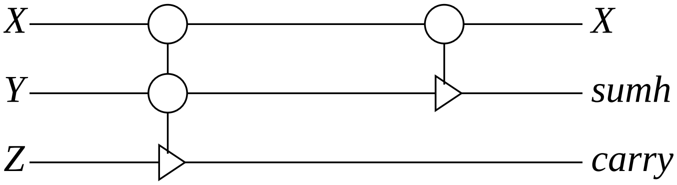


controlled controlled not



CCN

CCN and **CN** give a reversible half-adder.



7. The operator tables look like matrices in `0,1` but they're not.

Can we describe logic/switching operators as matrices?

How about $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} = \begin{pmatrix} t \\ f \end{pmatrix}$ for **not**?

$$\textbf{not not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Seems right.

So maybe **and** is

$$\begin{array}{c|cccc} \downarrow & \textbf{ff} & \textbf{ft} & \textbf{tf} & \textbf{tt} \\ \hline \textbf{f} & 1 & 1 & 1 & 0 \\ \textbf{t} & 0 & 0 & 0 & 1 \end{array}$$

No: 1) it does funny things:

$$\textbf{and} \begin{pmatrix} \textbf{ff} \\ \textbf{ft} \\ \textbf{tf} \\ \textbf{tt} \end{pmatrix} = \begin{pmatrix} \textbf{f}+\textbf{f}+\textbf{f} \\ \textbf{t} \end{pmatrix}$$

2) the matrix is not square.

Let's focus on operators with the same number of outputs as inputs.

Then the matrices could describe a *change of state* from input state to output state.

$$\textbf{CN} \quad \begin{array}{c|cccc} \downarrow & \textbf{ff} & \textbf{ft} & \textbf{tf} & \textbf{tt} \\ \hline \textbf{ff} & 1 & & & \\ \textbf{ft} & & 1 & & \\ \textbf{tf} & & & & 1 \\ \textbf{tt} & & & 1 & \end{array} \quad \overset{X_0\,Y_0}{\begin{pmatrix} \textbf{ff} \\ \textbf{ft} \\ \textbf{tf} \\ \textbf{tt} \end{pmatrix}} = \overset{X_1\,Y_1}{\begin{pmatrix} \textbf{ff} \\ \textbf{ft} \\ \textbf{tt} \\ \textbf{tf} \end{pmatrix}}$$

Let's look at this as a tensor product of matrices for X and Y (Week 6, Note 8).

$$\begin{array}{rcl} \left(\begin{array}{c|c} 1 & \\ \hline & 0 \end{array}\right)_X \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}_Y & + & \left(\begin{array}{c|c} 0 & \\ \hline & 1 \end{array}\right)_X \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}_Y = \\ \mathbf{ifnot}_X \; 1_Y & + & \mathbf{if}_X \; \mathbf{not}_Y \\ (\text{Compare } X'Y & + & XY' \end{array}$$

but that gives only one of the outputs.)

Feynman [Fey99, Chap. 6] uses this as the basis for analyzing reversible operators in a quantum computer: quantum states can be *superpositions* of pre-quantum mutually exclusive states.

8. Summary

(These notes show the trees. Try to see the forest!)

- boolean algebra
  - logic: **and**, **or**, **not**
  - logic: **if .. then ..**
    16 binary operators
- circuits: adders, boolean simplification
  - Extracting boolean expression from truth table (expression = term + term + .. + term; term = component.component. .. .component; component = variable or variable$'$)
    1. Ignore output entries of `0`. Each output entry of `1` contributes a term to the expression.
    2. Each input entry of `1` contributes that variable to the term. Each input entry of `0` contributes the negation of that variable to the term.
  - Simplifying the boolean expression (arrange the truth table as a hypercube or as a Karnaugh map, and apply the previous rules)
    1. Look for patterns of output `1`s: if any input variable contributes both `0` and `1` to output `1`s, that variable may be dropped from the corresponding terms and the terms combined into a single term. (Patterns include lines parallel to axes, squares, ..)
- reversible operators and universal operators
- matrix formulation

9. **Appendix: Binary Arithmetic**

We count on 10 fingers. Computers count on 2 electrical states.

Binary	`0`	`1`	`10`	`11`	`100`	`101`	`110`	`111`	...
Decimal	`0`	`1`	`2`	`3`	`4`	`5`	`6`	`7`	...

1	1	10	11
0	0	1	10
+	0	1	10

```
Decimal                               Binary

          825                                   101     (5)
       + 9346                                + 1101    (13)
        -----                                 -----
carry   1101                          carry   1101
sum     10171                         sum     10010    (18)

            1   10^0                              0   2^0
           70   10^1                             2    2^1
          100   10^2                           0*4    2^2
         0000   10^3                          0*8     2^3
        10000   10^4                          1*16    2^4
```

Adding least significant bits (digits) requires 2 inputs: `halfadder(x,y)`.
Adding any other pairs of bits (digits) requires 3 inputs: `fulladder(c,x,y)`.

II. The Excursions

You've seen lots of ideas. Now *do* something with them!

1. Derive $X + X = X$ and $XX = X$ from axioms (e.)
2. Run the MATLAB function

   ```
   % function OT= OperatorTableOr()
   % THM 060828
   function OT = OperatorTableOr()
   for x = 0:1
    for y = 0:1
     OT(y+1,x+1) = or(x,not(y));
    end
   end
   ```

   and write corresponding ones for **and** and **not**.
3. For a two-element boolean algebra, verify all the axioms of boolean algebra by using the truth tables for +, ., and '.
4. What are the differences between the boolean algebra on two elements, 0 and 1, and the field (see Week 4) on two elements, 0 and 1? How does binary arithmetic on two elements, 0 and 1, differ from each?
5. How do the boolean axioms change if we swap 0 ↔ 1 and + ↔ .?
6. From "nature is not indiscrete" infer that "nature is discrete".
7. Show that *if* **not** Q *then* **not** P is equivalent to *if* P *then* Q, for any propositions P and Q.
8. Use the equivalent form of implication (previous excursion) to show that if a Mersenne number is prime then its index is prime. (The Mersenne number of index n, $M_n = 2^n - 1$. Pere Marin Mersenne 1588–1648.)
   Find an example to show the converse is not true.
9. (Eugene Lehman) Eugene teaches unnecessarily advanced math extracurricularly to Abe, Ben and Chaim at Hebrew school. They are all very smart, but Ben is the brightest. However, Ben has been blind from birth.

Eugene always wears his kippah but one day all three boys forgot theirs. Ben, however, said that he knows Eugene keeps two red and three white kippahs in the closet, and said he would fetch three out. But he turned off the lights so the room was dark when he went, and did not turn them back on until all three boys each had a kippah on his head.

Ben then asked Abe if he knew what colour kippah he was wearing. Abe looked at the other boys' kippahs but not his own (because it was on his head), thought carefully (remember, Abe is very smart) and said he didn't know.

Ben then asked Chaim if he knew what colour kippah he was wearing. Chaim looked at the other boys' kippahs but not his own (because it was on his head), thought carefully (remember, Chaim is very smart) and said he didn't know either.

Ben then said that, although he could not see the other boys' kippahs, having been blind from birth, he knew what colour kippah he was wearing himself. He waved it in the air and correctly pronounced its colour.

a) What colour was Ben's kippah and how did he know? Figure this out informally before going on to the next parts of this excursion.

b) Formulate the problem in boolean algebra using

`AR` = Abe's kippah is red = **not** `AW`
`BR` = Ben's kippah is red = **not** `BW`
`CR` = Chaim's kippah is red = **not** `CW`

`AK` = Abe knows the colour of his own kippah
`CK` = Chaim knows the colour of his own kippah

c) Why is the following true?
not(`AR` **and** `BR` **and** `CR`)
d) Use boolean algebra to infer from (c)
if `BR` **and** `CR` **then** `AW`
e) Why is the following true?
`AK` = `BR` **and** `CR`
f) From **not** `AK` infer
if `BR` **then** `CW`
g) Repeating the reasoning of (d)–(f) find the expression for `CK` and infer the final answer.

10. Since **not not** X is X, boolean logic imposes the "law of the excluded middle".
This allows us to make proofs by contradiction: suppose what you want to prove is untrue, then derive an impossibility from this supposition. This is used, for instance in automated reasoning (J. A. Robinson's "resolution principle").
We'll do something simpler, which we'll need in Week 12.
Use contradiction to show that the greatest common divisor of integers x and y,
$$\gcd(x, y) = \gcd(y, x \bmod y),$$
where $x \bmod y$ is the remainder after x is divided by y. Note that $x = (x \div y)y + x \bmod y$, where $x \div y$ is the integer quotient of dividing x by$y$ y, and that if $\gcd(x, y) = g$ then $x = gp$ and $y = gq$ for some integers p and q such that $\gcd(p, q) = 1$.

11. **More than one kind of infinity**

> *When we've been there ten thousand years,*
> *Bright shining as the sun,*
> *We've no less days to sing God's praise,*
> *Than when we first begun.*
> —1790 addition to John Newton's 1779 *Amazing Grace*

a) Use contradiction to prove that there are numbers beyond the "rational" numbers, which are ratios, p/q, of integers p and q: suppose that $\sqrt{2} = p/q$, with p and q in lowest terms (i.e., $p \bmod q = 1$). Hint: show that if p is odd then p^2 must be odd (for any integer, p). (This discovery so upset Pythagoras' belief in the supremacy of integers that he reputedly had Hippasus, who made it, drowned: South Italy, 550BC.)

b) Show that the collection of all rational numbers is *countable*, i.e., ways can be found to order each rational number, p/q, in a sequence so that each number can be paired with a non-negative integer in the sequence 0, 1, 2, .. Hint: make a two-dimensional grid for p and q and find a way to draw a connected line through all the grid points.

c) Check that each rational number, p/q, can be converted to decimal form using a procedure such as the following for 1/7: for digits $a, b, c, d, e, ..$ (which can only take on the values 0, 1, 2, 3, 4, 5, 6, 7, 8 or 9)

$$\begin{aligned}
1/7 &= a/10 + b/10^2 + c/10^3 + d/10^4 + e/10^5 + .. \\
&= \frac{1}{10}(a + \frac{1}{10}(b + \frac{1}{10}(c + \frac{1}{10}(d + \frac{1}{10}(e..))))) \\
\frac{10}{7} &= a + \frac{1}{10}(b + \frac{1}{10}(c + \frac{1}{10}(d + \frac{1}{10}(e + ..))))
\end{aligned}$$

So $a = 1$.

$$\begin{aligned}
\frac{10}{7} - 1 = \frac{3}{7} &= \frac{1}{10}(b + \frac{1}{10}(c + ..)) \\
\frac{30}{7} &= b + \frac{1}{10}(c + \frac{1}{10}(d + \frac{1}{10}(e + ..)))
\end{aligned}$$

So $b = 4$.

$$\begin{aligned}
\frac{30}{7} - 4 = \frac{2}{7} &= \frac{1}{10}(c + ..) \\
\frac{20}{7} &= c + \frac{1}{10}(d + \frac{1}{10}(e + ..))
\end{aligned}$$

So $c = 2$. At this point, let's stop and look ahead. How many *different* remainders can there be, at most? How soon, at most, will we see any given remainder *again* in this process? What does this mean for the digits in the decimal form of 1/7?

Now carry on with 1/7 by finding digits $d, e, f, ..$ and see if you were right. Try it for some other fractions. Persuade yourself that the sequence of digits always repeats after a certain point. (The repetition may be of only a single digit, and this digit may even be 0: include some fractions that give these special cases in your experimenting.)

You can also use this procedure to find the "decimal" representation of a fraction in any base b: just replace all the 10s, above, by b. Here is the start for 1/7 in binary.

$$\begin{aligned}
1/7 &= a/2 + b/2^2 + c/2^3 + d/2^4 + e/2^5 + .. \\
&= \frac{1}{2}(a + \frac{1}{2}(b + \frac{1}{2}(c + \frac{1}{2}(d + \frac{1}{2}(e + ..))))) \\
\frac{2}{7} &= a + \frac{1}{2}(b + \frac{1}{2}(c + \frac{1}{2}(d + \frac{1}{2}(e + ..))))
\end{aligned}$$

where bits $a, b, c, d, e, ..$ can only take on the values 0 or 1.

d) How many numbers are there whose decimal representations contain no repetitions? Here is Cantor's argument that there are more than can even be counted. It is another argument by contradiction, the "diagonal" argument. It is sufficient to consider only fractions between 0 and 1, and to represent them in binary. Suppose we have found a sequence which includes all the infinitely-long fractions, and replace the diagonal elements by their opposites (shown in bold in the second column).

00000000...	**1**0000000...
10000000...	1**1**000000...
11111111...	11**0**11111...
01010101...	010**0**0101...
10101010...	1010**0**010...
11010110...	11010**0**10...
00110110...	001101**0**0...
10001000...	1000100**1**...

Convince yourself that the replaced bits themselves form a new infinitely-long fraction

11000001..

which is not in the sequence, contradicting our supposition that the sequence was complete. (To see that the new infinitely-long fraction does not repeat and so cannot be rational, look up www.mathpages.com/home/kmath371.htm: if it did, the rationals would be uncountable, contradicting (b), above.)
e) Cantor also showed that the *power set* (the set of all subsets) of an infinite set has a higher infinity of elements than the original set. The argument is also by contradiction and also uses a form of diagonal. Consider, for example, the (countably infinite) set of integers. Suppose we have paired off its power set with integers, so that we can count it.

$\mathcal{N}$	P($\mathcal{N}$)
1	{4,5}
2	{1,2,3}
3	{4,5,6}
4	{1,3,5}
:	:

In this example, 2 is paired with a subset that contains 2, but 1, 3 and 4 are paired with subsets that do not contain themselves. Which integer is paired with the subset, {1,3,4,..}, of all integers that are paired with subsets that do not contain themselves? Is it *not* in this subset? Then it is paired with a subset that does not contain itself, and so it is in the subset: contradiction. Conversely, if it *is* in this subset, then it is not in it: there is no escape.
This is a diagonal argument because it is asking whether, in row ? below, there is a • on the diagonal, and getting a contradiction for both alternatives.

	1	2	3	4	5	6	..
1				•	•		
2	•	•	•				
3				•	•	•	
4	•		•		•		
:							
?	•		•	•			?

So instead of writing ∞, we need more than one symbol. We could call the kind of infinity that the integers have $\aleph_0$ and the kind of infinity that the power set of the integers has $\aleph_1$. What about the power set of the power set? $\aleph_2$? Which of these is the infinity that the real numbers (rational numbers and irrationals together) have?

12. Some irrationals can be represented as periodic sequences of integers via *continued fractions.* Here is $\sqrt{2}$. $q = 1 + \sqrt{2}$ satisfies $q^2 - 2q - 1 = 0$, i.e.,

$$q \quad = \quad 2 + \frac{1}{q} = 2 + \frac{1}{2 + \frac{1}{q}} = 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{q}}} = ..$$

$$= \quad 2 + \cfrac{1}{2 + \frac{1}{2+\frac{1}{2+\frac{1}{2+..}}}}$$

So

$$\begin{aligned}\sqrt{2} &= q - 1 \\ &= 1 + \cfrac{1}{2 + \frac{1}{2+\frac{1}{2+\frac{1}{2+..}}}}\end{aligned}$$

Thus the sequence of integers for $\sqrt{2}$ is 1, 2, 2, 2, 2, ..
Show that the following sequences hold.

$$\begin{aligned}
\sqrt{3} &: \quad 1, 1, 2, 1, 2, .. \\
\sqrt{4} &: \quad 2, 0, 0, 0, .. \\
\sqrt{5} &: \quad 2, 4, 4, 4, .. \\
\sqrt{6} &: \quad 2, 2, 4, 2, 4, .. \\
\sqrt{7} &: \quad 2, 1, 1, 1, 4, 1, 1, 1, 4, .. \\
\sqrt{8} &: \quad 2, 1, 4, 1, 4, .. \\
\sqrt{9} &: \quad 3, 0, 0, 0, .. \\
\sqrt{10} &: \quad 3, 6, 6, 6, .. \\
\sqrt{11} &: \quad 3, 3, 6, 3, 6, .. \\
\sqrt{12} &: \quad 3, 2, 6, 2, 6, .. \\
\sqrt{13} &: \quad 3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, .. \\
\sqrt{14} &: \quad 3, 1, 2, 1, 6, 1, 2, 1, 6, .. \\
\sqrt{15} &: \quad 3, 1, 6, 1, 6, .. \\
\sqrt{16} &: \quad 4, 0, 0, 0, .. \\
\sqrt{17} &: \quad 4, 8, 8, 8, .. \\
\sqrt{18} &: \quad 4, 4, 8, 4, 8, .. \\
\sqrt{19} &: \quad 4, 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8, .. \\
\sqrt{20} &: \quad 4, 2, 8, 2, 8, ..
\end{aligned}$$

(Well, be careful about those 0, 0, ..)
To discover the sequence for, say, $\sqrt{3}$, use a calculator:

$$\begin{aligned}\sqrt{3} &= 1.73205.. \\ &= 1 + \frac{1}{1.3660..} \\ &= 1 + \cfrac{1}{1 + \frac{1}{2.73205..}}\end{aligned}$$

and there's the repeat.
What number is $q = 1 + 1/q$?
What about other irrationals? Cube roots?
Transcendental numbers such as π can also be represented as continued fractions, but they do not repeat.

$$\pi \quad : \quad 3,\ 7,\ 15,\ 1,\ 292$$

If we work backwards from 7 we get 22/7 as an approximation to π. If we work back from the 1 we get 355/113, an approximation which is good to six decimal places. Furthermore, it lends itself to ruler-and-compass construction (Gelder's construction) since

$$\frac{355}{113} = 3 + \frac{4^2}{8^2 + 7^2} = 3 + (\frac{1/2}{\sqrt{1 + (7/8)^2}})^2$$

How much does working back from the 292 improve the approximation?
The continued fraction representation of square roots was explored by Joseph Louis Lagrange. Where else have we encountered him?

13. What are the differences among the following three propositions?

$$X \textbf{ and } Y, \quad X \textbf{ and/or } Y, \quad X \textbf{ or } Y$$

14. Find other examples showing that implication ($X \to Y$) is not commutative. Here are three.
If she is pregnant then she is female.
If he is my son-in-law then he is my son's brother-in-law.
If $2^p - 1$ *is prime then* p *is prime.*

15. Why is it not true that
if (the slope of $f()$ at x is zero) then
(x is a maximum of $f()$ or x is a minimum of $f()$)?

16. Confirm by truth table that $X \to Y$ is $X'Y' + X'Y + XY$. Convince yourself that the sum-of-products rule that gave this equivalence works in general for any boolean combination.

17. Which of the sixteen binary boolean operators on 0 and 1 are commutative? Associative?

18. Show that X **xor** Y is $XY' + X'Y$.

19. Show that **or** can be derived from **and** and **not**.

20. Show that **or** and **and** can be derived from → and **not**.

21. Show that $X \to Y$ is $Y' \to X'$.

22. What is the relationship between → and ≤ ?

23. Show that X **xor** Y' is X' **xor** Y is $(X$ **xor** $Y)'$.

24. Show that **xor** is commutative and associative. This follows from the observation that **xor** gives the parity of the number of 1s when applied repeatedly: true if odd, false if even. Show this by induction (Note 4 of Week 12).
Here's the start (and immediately gives commutativity).

X	Y	X **xor** Y
0	0	0
0	1	1
1	0	1
1	1	0

Now consider what happens when a third variable, Z, is 0 and when it is 1. (And now you have associativity, as well as the induction step to continue forever.)
Apply this to find a simple expression for the sum result, S, of a full adder.

25. Show that $(X \textbf{ xor } Y) \textbf{ xor } XY = (X \textbf{ xor } Y) + XY = X + Y$.

26. IQ tests often check analogic reasoning, such as [Kle85]

X = Boy loves light	Z = Girl hates dark
Y = Woman hates light	?

The way we solve such a puzzle is to compare X and Y for equality on each item and then apply the result to Z. So "loves" in X and "hates" in Y are not equal; thus the verb in ? will be the opposite of "hates" in Z: "loves".

This process supposes a universe for each item: light/dark, loves/hates and boy/girl/woman/man (or female/male and adult/child). We can represent each of these pairs of opposites as a boolean

	M	C	H	D
0	female	adult	loves	light
1	male	child	hates	dark

Putting these together as vectors of booleans

$$\begin{array}{rcl} & & MCHD \\ X & = & 1100 \\ Y & = & 0010 \\ Z & = & 0111 \end{array}$$

It is easy to find out where X and Y match (1) or differ (0)

$$X \textbf{ nxor } Y = 0001$$

(where I've used **nxor** for = (see Note 4) because $X{=}Y = 0001$ is confusing to interpret). Here, **nxor** is applied in turn to each element of the two vectors.

All we have left to do is to apply the same operation to this result and Z:

$$(X \textbf{ nxor } Y)\textbf{nxor } Z = 0001\textbf{nxor } Z = 1001$$

to find out that ? = Man (male adult) loves dark.

a) Check this and explain why. Is it reasonable to translate the result of X **nxor** Y back into $MCHD$ terminology?

b) Show that **nxor** is associative and commutative. What does this say about other ways of doing the above calculation?

c) Show that

$$X = Y \textbf{ nxor } Z, Y = Z \textbf{ nxor } X \text{ and } Z = X \textbf{ nxor } Y$$

are all equivalent statements.

d) Use mathematical induction (Note 4 of Week 12) to show that

$$Z \textbf{ nxor } Y\textbf{nxor } X\textbf{nxor } .. \textbf{ nxor } A$$

is 1 (**true**) if there are an even number of 0s in $Z, Y, X, .., A$ and 0 (**false**) otherwise.

e) show that **xor** has the same (or, for (d), similar) properties and also works for the calculations of (a) and (b).

f) Look up [Kle85] for an example of a longer chain of analogic reasoning, X **nxor** Y **nxor** Z **nxor** W **nxor** P. Must the number of terms always be odd?

27. Find eight ways we can get the not operator, $'$, from the sixteen binary operators.

28. Show that **or**, **and** and **not** can all be derived from **nand**. What other single binary operator gives **or**, **and** and **not**?

29. From the table for the half adder we can see directly that

$$\mathit{carry} \ = C'XY + C(X+Y)$$

Show that this is the same as

$$\mathit{carry} \ = CX + CY + XY$$

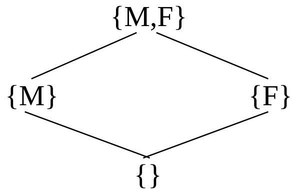
30. Draw the circuit diagram for the full adder.

31. Write the MATLAB function `[carry,sum] = fulladder(c,x,y)`. Combine it with `[carry,sumh] = halfadder(x,y)` from Note 5 to build a function which adds 2-bit numbers. Build a function which adds eight-bit numbers.

32. Which is the better way to schedule a meeting among several people next week: ask them to tell you what times they *are* available; or ask them to tell you when they are *not* available? Imagine that each person will fill out a schedule for the coming week in the form

	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00
Mon								
Tue								
Wed								
Thu								
Fri								

33. Boolean algebra can also represent sets, with the "product" standing for set intersection, the "sum" giving set union and "negation" giving the complement. *Mother* and *father* form a set of two members, $\{M, F\}$, and this set, together with all its subsets, form a four-element boolean algebra.



Here, {} is the *empty set* which is given by the intersection of $\{M\}$ and $\{F\}$. The union of $\{M\}$ and $\{F\}$ gives the full set. The complement of $\{M\}$ is $\{F\}$, and vice-versa.
a) Which of these four elements behaves as `1` and which as `0`? Invent symbols, such as `a` and `b`, for the remaining two sets.
b) Verify that the boolean axioms hold for the three operators on these elements.
c) How many boolean elements arise from a 3-member set? Draw the diagram corresponding to the diamond for the 2-member set, showing all connections between subsets (upwards for unions, downwards for intersections). To what three-dimensional figure is this diagram equivalent?

34. If we have a set, A, of apples and a set, R, of red fruit, the set AR is the red apples. (There might also be green and yellow apples, and red strawberries.) The set $A + R$ is all the fruit that is red or an apple.
    This is especially useful in assessing probabilities: the probability of a set is the number in the set divided by the total number. The intersection of two overlapping sets is assigned as probability the (arithmetic) product of the probabilities of the two sets. (What is it if the sets are disjoint?) The union of two disjoint sets is assigned the probabality that is the (arithmetic) sum. But if the sets overlap, we must use De Morgan's laws and the "not" operator: $A + R = (A'R')'$. The probability that something is not in a set is $1 -$ the probability that it is in the set, so "not", $'$, becomes subtraction from 1. Thus the probability that a fruit is an apple or red is $\text{prob}(A+R) = \text{prob}((A'R')') = 1 - \text{prob}(A'R') = 1 - (1 - \text{prob}(A))(1 - \text{prob}(R))$.
    Using the counts

	red	green	yellow	TOTALS
apples	10	6	4	20
bananas			8	8
strawberries	20			20
grapes	15	18		33
lemons			3	3
limes		2		2
TOTALS	45	26	15	85

    and assuming that this accounts for all fruit, calculate
    a) the probability that a fruit is a red apple;
    b) the probability that a fruit is not a red apple;
    c) the probability that a fruit is a red apple and a green apple;
    d) the probability that a fruit is a red apple or a green apple.
    Now suppose that you know only the probability that a fruit is an apple and the probability that a fruit is red, and calculate
    e) the probability that a fruit is a red and an apple;
    f) the probability that a fruit is a red or an apple;
    and compare these results to the actual number of fruit that satisfy the two conditions.
    g) What is the probability that an apple is red (that is, you know it is an apple, and want to know how likely it is to be red)?

35. Suppose the Earth is 70% water and suppose that 50% of the Earth is covered in clouds at any particular time. A satellite has taken pictures of all of the Earth and we want to keep only those that have neither clouds nor water. What proportion of the pictures will we keep? Check these figures and find out if clouds are associated with lakes and oceans in ways that make the calculation less simple.

36. The "birthday paradox" states that, with 23 people gathered in a room, the probability that at least two of them share a birthday is over 50%.
    a) If n people in a room take turns crossing off their birthday on a calendar of 365 days, and the $k + 1$st person finds k crosses on the calendar (none of the k predecessors shares a birthday with any other predecessor), how many ways out of the 365 can $k + 1$ place heir cross on a blank day?
    b) What is the probability that $k + 1$ does not share a birthday with the previous k?
    c) What is the probability that none of the n people share a birthday with any other. (Try this for $n < 365$. Think about it for $n \geq 365$.) What assumptions must you make to calculate this probability?
    d) From (c), what is the probability that at least two people of the n share a birthday? What must n be for this to exceed fifty-fifty? (Use MATLAB to plot the probability versus n.)

37. Children get half their genetic inheritance from each parent. In the following questions, "genetic overlap" means the probability that the genetic material is the same in two individuals: count the number of ways it can be the same relative to the (total) number of ways it can be the same or different.
a) What is the genetic overlap between siblings?
b) What is the genetic overlap between grandparent and grandchild?
c) What is the genetic overlap between first cousins? Between two first cousins who marry and their children?
d) What is the genetic overlap between yourself and your aunt or uncle? (Consider both possibilities.) What if two brothers married two sisters?
e) What is the genetic overlap between yourself and a half-sibling? A step-sibling?
f) In "haplodiploid" species such as bees, fathers have only one chromosome so that the genetic inheritance from the father is identical in each offspring: what is the genetic overlap between siblings?
g) Supposing that genes control a species' behaviour so as to maximize their own (the genes' own) survival down the generations, would a bee be more likely to risk its own life for a sibling or for an offspring?
h) Do these calculations contradict the assertion that humans share 97% of our genes with chimpanzees?

38. Show that **right**, **left**, **xor**, **nxor**, **nright** and **nleft** can be combined in any pairs, except <op> with **n**<op>, whose results can be combined in turn to give back the original inputs. E.g., $X = X$ **left** $Y, Y = (X$ **xor** $Y)$ **xor** $(X$ **left** $Y)$.

39. Show that any boolean operator can be got from the third output of the controlled exchange operator, **CX**. That is, **CX** is universal.

40. Show that the second output of **CX** gives the same collection of operators as the third output does, and thus is also universal.

41. What operators does the first output of **CX** give?

42. What is the inverse of **CX**? Give two different arguments. (Hint: write the numbers, 0, .., 7, on the cube in two ways, first labelling the inputs, second labelling the outputs.)

43. Look up Edward Fredkin, 1934– . What is the Fredkin gate? What are tries?

44. Show that **CCN**, the controlled controlled not operator, is reversible. What is its inverse? Show that it is universal.

45. Show that **CCN** and the controlled not operator, **CN**, do give a half adder. What is the inverse of the half adder?

46. Can a operator with three inputs and three outputs be reversible if one output is the full adder sum and another output is the full adder carry?

47. Construct a reversible operator, $G(X, Y, Z)$, such that the first output gives **nand** and **nor** and **not** when inputs are equated (e.g., $G_1(X, Y, Y) = X$ **nand** Y) and the second output, $G_2(X, Y, Z)$, gives the full adder sum. What is its inverse?

48. Can a operator be built which is its own inverse and which gives **nand** by setting some inputs equal to each other?

49. How many different reversible three-input operators can there be? How many of these are their own inverse?

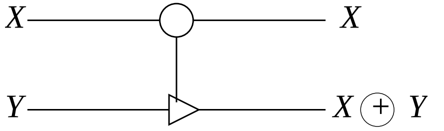
50. How can we get exchange from controlled not? Vice versa?

51. Using the matrix representation of operator, show that **CCN** is

$$(\mathbf{ifnot}_X 1_Y + \mathbf{if}_X \mathbf{ifnot}_Y)1_Z + \mathbf{if}_X \mathbf{if}_Y \mathbf{not}_Z = 1 + \mathbf{if}_X \mathbf{if}_Y (\mathbf{not}_Z - 1_Z)$$

52. **Matrix logic.** Practice making reversible boolean circuits and the corresponding matrices, using gates CN and CCN. Note that we must now think in terms of **xor** instead of **and** $(\cdot)$ and **or** $(+)$: I've used $\oplus$ in the diagrams as a symbol for **xor**.
Work out and check the following.

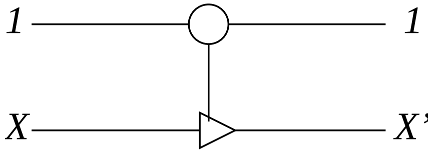
Controlled-not gives **xor**.



controlled not CN

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{pmatrix}$$

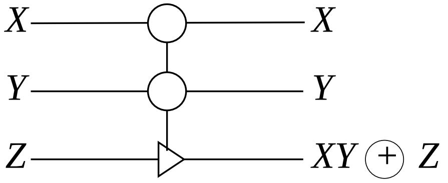
Not is a special case. (There is one less variable, so the matrix is smaller.)



$$\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$$

reversible not

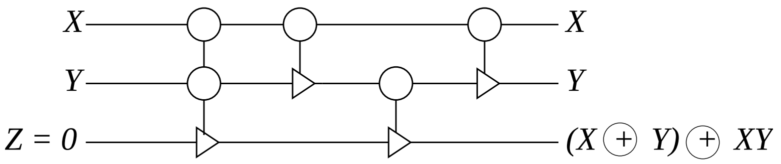
Controlled-controlled-not gives **and**. We now have three variables. (I have not set Z to 0 although that's what we need for **and**.) So the matrix is 8-by-8 and I've introduced two 2-by-2 block matrices in order to keep the sizes manageable: I the usual identity and N the above **not** matrix.



$$\begin{pmatrix} \mathrm{I} & & & \\ & \mathrm{I} & & \\ & & \mathrm{I} & \\ & & & \mathrm{N} \end{pmatrix}$$

controlled controlled not CCN

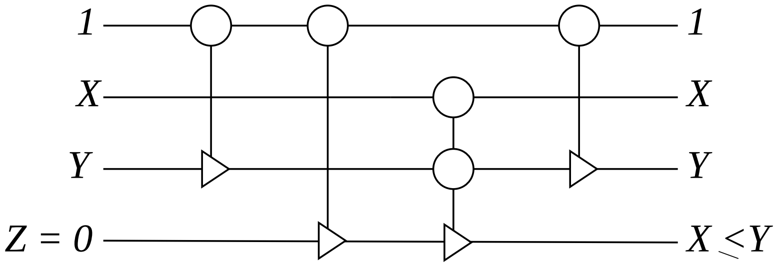
For **or** we must combine gates and we get a product of four matrices, applied, of course as usual, from right to left. Note carefully the two different variants of the CN (**xor**) gate and that **xor** is its own inverse so I've applied it a second time at the end to restore Y.
Apply the resulting matrix to the 8-by-1 vector of all possible combinations of $XYZ = \{000,001,010,011,100,101,110,111\}$ to check that the resulting value of Z is $X + Y$. (I've used the result of an earlier Excursion that $X \oplus Y \oplus XY = X + Y$.)



reversible or

$$\begin{pmatrix} I & & & \\ & I & & \\ & & & I \\ & & I & \end{pmatrix}\begin{pmatrix} I & & & \\ & N & & \\ & & I & \\ & & & N \end{pmatrix}\begin{pmatrix} I & & & \\ & I & & \\ & & & I \\ & & I & \end{pmatrix}\begin{pmatrix} I & & & \\ & I & & \\ & & I & \\ & & & N \end{pmatrix} = \begin{pmatrix} I & & & \\ & N & & \\ & & N & \\ & & & N \end{pmatrix}$$

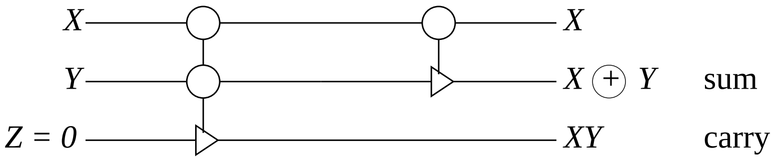
We can also express implication $X \leq Y = X \Leftarrow Y = X' + Y$. To do this I've started from an alternative implementation of **or**, using $(XY')' = X' + Y$ for implication. There are again four gates, including the repetition of CN to restore Y at the end.
What is the inverse of the resulting matrix?



reversible implies

$$\begin{pmatrix} & I & & \\ I & & & \\ & & & I \\ & & I & \end{pmatrix}\begin{pmatrix} & & I & \\ & & & I \\ I & & & \\ & I & & \end{pmatrix}\begin{pmatrix} I & & & \\ & I & & \\ & & I & \\ & & & N \end{pmatrix}\begin{pmatrix} & I & & \\ I & & & \\ & & & I \\ & & I & \end{pmatrix} = \begin{pmatrix} & & N & \\ & & & I \\ I & & & \\ & I & & \end{pmatrix}$$

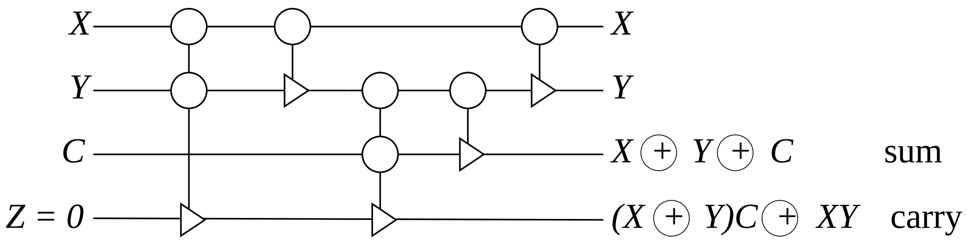
A half-adder is actually simpler then the last two because the sum is given directly by **xor**, and the carry by **and**. We need only two gates.



reversible half−adder

$$\begin{pmatrix} I & & & \\ & I & & \\ & & & I \\ & & I & \end{pmatrix}\begin{pmatrix} I & & & \\ & I & & \\ & & I & \\ & & & N \end{pmatrix} = \begin{pmatrix} I & & & \\ & I & & \\ & & & N \\ & & I & \end{pmatrix}$$

The full adder similarly uses **xor** for the sum, only twice.The carry is a little more complicated. The five gates on four lines give five 16-by-16 matrices.

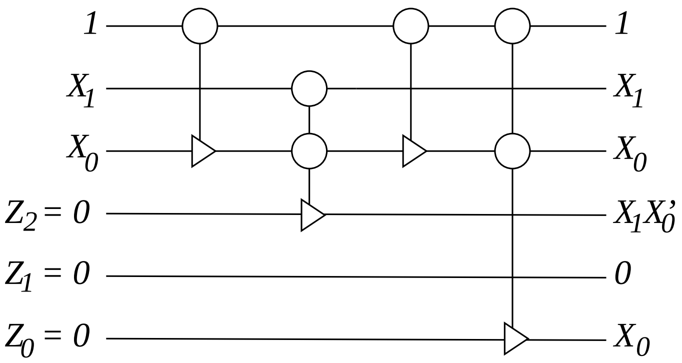


reversible full−adder

$$\left(\begin{array}{cccc|cccc} I&&&&&&& \\ &I&&&&&& \\ &&I&&&&& \\ &&&I&&&& \\ \hline &&&&&&I& \\ &&&&&&&I \\ &&&&I&&& \\ &&&&&I&& \end{array}\right)\left(\begin{array}{cccc|cccc} I&&&&&&& \\ &I&&&&&& \\ &&&I&&&& \\ &&I&&&&& \\ \hline &&&&I&&& \\ &&&&&I&& \\ &&&&&&&I \\ &&&&&&I& \end{array}\right)\left(\begin{array}{cccc|cccc} I&&&&&&& \\ &I&&&&&& \\ &&I&&&&& \\ &&&N&&&& \\ \hline &&&&I&&& \\ &&&&&I&& \\ &&&&&&I& \\ &&&&&&&N \end{array}\right)\times$$

$$\times\left(\begin{array}{cccc|cccc} I&&&&&&& \\ &I&&&&&& \\ &&I&&&&& \\ &&&I&&&& \\ \hline &&&&&&I& \\ &&&&&&&I \\ &&&&I&&& \\ &&&&&I&& \end{array}\right)\left(\begin{array}{cccc|cccc} I&&&&&&& \\ &I&&&&&& \\ &&I&&&&& \\ &&&I&&&& \\ \hline &&&&I&&& \\ &&&&&I&& \\ &&&&&&N& \\ &&&&&&&N \end{array}\right)=\left(\begin{array}{cccc|cccc} I&&&&&&& \\ &I&&&&&& \\ &&&N&&&& \\ &&I&&&&& \\ \hline &&&&&N&& \\ &&&&I&&& \\ &&&&&&I& \\ &&&&&&&I \end{array}\right)$$

Finally let's implement a circuit which calculates the square of a two-bit number: $00^2 = 000$, $01^2 = 001$, $10^2 = 100$ and $11^2 = 001$ (9 is 1 modulo 2^3, of course). There are five lines but z_1 remains 0 so we can leave it out: the four gates give four 16-by-16 matrices.



reversible square

$$\left(\begin{array}{cccc|cccc} I&&&&&&& \\ &I&&&&&& \\ &&N&&&&& \\ &&&N&&&& \\ \hline &&&&I&&& \\ &&&&&I&& \\ &&&&&&N& \\ &&&&&&&N \end{array}\right)\left(\begin{array}{cccc|cccc} &&I&&&&& \\ &&&I&&&& \\ I&&&&&&& \\ &I&&&&&& \\ \hline &&&&&&I& \\ &&&&&&&I \\ &&&&I&&& \\ &&&&&I&& \end{array}\right)\left(\begin{array}{cccc|cccc} I&&&&&&& \\ &I&&&&&& \\ &&I&&&&& \\ &&&I&&&& \\ \hline &&&&I&&& \\ &&&&&I&& \\ &&&&&&&I \\ &&&&&&I& \end{array}\right)\times$$

$$\left(\begin{array}{cccc|cccc} &&I&&&&& \\ &&&I&&&& \\ I&&&&&&& \\ &I&&&&&& \\ \hline &&&&&&I& \\ &&&&&&&I \\ &&&&I&&& \\ &&&&&I&& \end{array}\right)=\left(\begin{array}{cccc|cccc} I&&&&&&& \\ &I&&&&&& \\ &&N&&&&& \\ &&&N&&&& \\ \hline &&&&&I&& \\ &&&&I&&& \\ &&&&&&N& \\ &&&&&&&N \end{array}\right)$$

53. **xor** and **and**. a) Show that exclusive or (**xor**, $\oplus$) is commutative, associative and distributive under **and** ($x(y \oplus z) = xy \oplus xz$).
b) Show that **xor** determines if the number of on-bits ("true" answers) is odd, e.g., $z \oplus y \oplus x$ is 1 iff an odd number of z, y, x are 1.
c) Show that $0 \oplus x = x$ and $1 \oplus x =$ **not** x.
d) Show that **xor** and **and** together are universal: the 16 possible values of the combined boolean coefficients a_0, a_1, a_2 and a_3 allow $a_0 \oplus a_1 x \oplus a_2 y \oplus a_3 xy$ to express any boolean function.

y	x	0	$1 \oplus x \oplus y \oplus xy$	$x \oplus xy$	$y \oplus xy$	xy	$1 \oplus y$	$1 \oplus x$	$1 \oplus x \oplus y$	$x \oplus y$	x	y
0	0	0	1	0	0	0	1	1	1	0	0	0
0	1	0	0	1	0	0	1	0	0	1	1	0
1	0	0	0	0	1	0	0	1	0	1	0	1
1	1	0	0	0	0	1	0	0	1	0	1	1

y	x	$1 \oplus xy$	$1 \oplus y \oplus xy$	$1 \oplus x \oplus xy$	$x \oplus y \oplus xy$	1
0	0	1	1	1	0	1
0	1	1	1	0	1	1
1	0	1	0	1	1	1
1	1	0	1	1	1	1

e) Find a matrix which maps each of the column vectors above into the coefficients below.

a_0	0	1	0	0	0	1	1	1	0	0	0	1	1	1	0	1
a_1	0	1	1	0	0	0	1	1	1	1	0	0	0	1	1	0
a_2	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0
a_3	0	1	1	1	1	0	0	0	0	0	0	1	1	1	1	0

Hint. Start with finding the matrix that transforms correctly the vectors with only one 1:

$$M \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$M \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

$$M \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

$$M \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Next apply this matrix to each of the other input vectors *but* use **and** instead of multiplication and **xor** instead of addition:

$$\oplus_k M_{jk} a_k = b_j$$

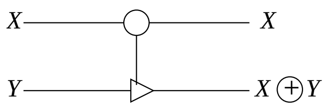
f) What matrix gives the corresponding transformation from truth table for the single bit x to coefficients of $0, 1 \oplus x, x, 1$?
g) What matrix does the same for three bits z, y, x?

z	y	x	$1 \oplus x \oplus y \oplus yx \oplus z \oplus zx \oplus zy \oplus zyx$	$x \oplus yx \oplus zx \oplus zyx$	$y \oplus yx \oplus zy \oplus zyx$	$xy \oplus zyx$
0	0	0	1	0	0	0
0	0	1	0	1	0	0
0	1	0	0	0	1	0
0	1	1	0	0	0	1
1	0	0	0	0	0	0
1	0	1	0	0	0	0
1	1	0	0	0	0	0
1	1	1	0	0	0	0

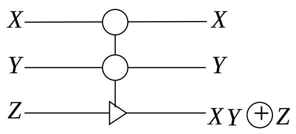
z	y	x	$z \oplus zx \oplus zy \oplus zyx$	$zx \oplus zyx$	$zy \oplus zyx$	zyx
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	0	0	0	0
1	0	0	1	0	0	0
1	0	1	0	1	0	0
1	1	0	0	0	1	0
1	1	1	0	0	0	1

NB. The coefficients here follow the order $1, x, y, yx, z, zx, zy, zyx$. See [SM13, p.6].

54. **C^{k}N circuits.** Despite my admiration for Fredkin, who also co-invented a computing data structure called *tries*, let's replace his CX gate by the CCN gate of his precedessor, Toffoli, because, like CN, CCN is a variant of **xor** and, indeed, also incorporates **and** so that we can use the systematic results of the previous Excursion.

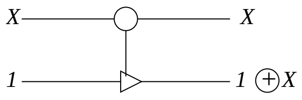


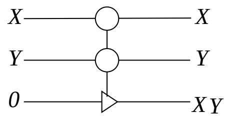
CN

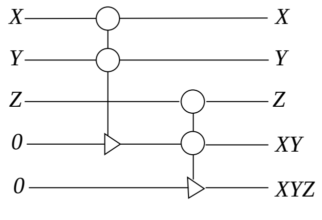


CCN

Using these two and **not** gates, or "ancilla" lines with preset initial values of 0 or 1, construct circuits to implement the **xor-and** expressions of the previous Excursion.







What is the inverse of any of these circuits? (After all, they are reversible.) How would you reset the ancilla lines to their original values without losing the results of the computation?

55. **Basic matrices for logic.** a) Show that under the vector representation of 0 (F) as $(1, 0)^T$ and 1 (T) as $(0, 1)^T$ the four basic transformations are

$$0 \to 0 \quad \text{is} \quad \begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$$

$$\begin{aligned} 0 \to 1 \quad &\text{is} \quad \begin{pmatrix} & 0 \\ 1 & \end{pmatrix} \\ 1 \to 0 \quad &\text{is} \quad \begin{pmatrix} & 1 \\ 0 & \end{pmatrix} \\ 1 \to 1 \quad &\text{is} \quad \begin{pmatrix} 0 & \\ & 1 \end{pmatrix} \end{aligned}$$

Thus the identity transformation is

$$\begin{pmatrix} 1 & \\ & 0 \end{pmatrix} + \begin{pmatrix} 0 & \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$$

and the **not** transformation is

$$\begin{pmatrix} & 0 \\ 1 & \end{pmatrix} + \begin{pmatrix} & 1 \\ 0 & \end{pmatrix} = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$$

b) To apply these to two bits we need the *tensor product* (Week 6 Note 8 but the notation is from Book 11d Part IV Note 20).
The controlled not, CN, has the truth table

x	y	x	CN
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

So the matrix form is (with the $x \to x$ transition in the first matrix of each tensor product and the $y \to cn$ transition in the second)

$$\begin{pmatrix} 1 & \\ & 0 \end{pmatrix} \overset{\leftarrow}{\times} \begin{pmatrix} 1 & \\ & 0 \end{pmatrix} + \begin{pmatrix} 1 & \\ & 0 \end{pmatrix} \overset{\leftarrow}{\times} \begin{pmatrix} 0 & \\ & 1 \end{pmatrix} + \begin{pmatrix} 0 & \\ & 1 \end{pmatrix} \overset{\leftarrow}{\times} \begin{pmatrix} & 0 \\ 1 & \end{pmatrix} + \begin{pmatrix} 0 & \\ & 1 \end{pmatrix} \overset{\leftarrow}{\times} \begin{pmatrix} & 1 \\ 0 & \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \\ & 0 \end{pmatrix} \overset{\leftarrow}{\times} \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \begin{pmatrix} 0 & \\ & 1 \end{pmatrix} \overset{\leftarrow}{\times} \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$$

c) Together with the null matrix, the four basic matrices form a closed set. Using letter abbreviations

$$\begin{array}{ccccc} 0 & A & B & C & D \\ \begin{pmatrix} 0 & \\ & 0 \end{pmatrix} & \begin{pmatrix} 1 & \\ & 0 \end{pmatrix} & \begin{pmatrix} 0 & \\ & 1 \end{pmatrix} & \begin{pmatrix} & 0 \\ 1 & \end{pmatrix} & \begin{pmatrix} & 1 \\ 0 & \end{pmatrix} \end{array}$$

we have the multiplication table

$\times$	A	B	C	D
A	A	0	0	D
B	0	B	C	0
C	C	0	0	B
D	0	D	A	0

What happens if we include

$$\begin{array}{cccc} E & F & G & H \\ \begin{pmatrix} i & \\ & 0 \end{pmatrix} & \begin{pmatrix} 0 & \\ & i \end{pmatrix} & \begin{pmatrix} & 0 \\ i & \end{pmatrix} & \begin{pmatrix} & i \\ 0 & \end{pmatrix} \end{array}$$

to form a 9-element closed set? What happens if we use the nine 3-by-3 matrices with one 1 each, together with 0, to form a 10-element set?

56. Look up George Boole's *The Laws of Thought* [Boo54]. What is the connection between logic and probability?

57. Look up Georg Ferdinand Ludwig Philipp Cantor (1845–1918) on sets and infinities.

58. Look up Richard Feynman's *Lectures on Computation* [Fey99]. What are the energy requirements for computing in principle and in current practice? How many atoms are involved in a modern transistor? What did Charles Bennett prove? What is the significance of reversible computation?

59. Look up Kee Dewdney's *The Turing Omnibus* [Dew89] or *The New Turing Omnibus* [Dew93] (call them [61] and [66], respectively) chapters 3, 13 and 20 [66] (3, 12 and 18 [61]).

60. **Euclid's Elements.** The original and classical axiom-based mathematics is Euclid's *Elements* of geometry and number theory. Joyce [Joy98] presents an annotated translation, with discussion of major subsequent developments. What makes this a classic is Euclid's spare and inexorable development of results in a direct way from minimum preliminaries. What makes it accessible is that these results are mostly already familiar to us because of the two millennia that we have collectively lived with them.
    Euclid presents five axioms (*Postulates*) for geometry and five *Common Notions* for magnitudes, based on (for Book I) 23 *Definitions*. From these he can prove 48 *Propositions* (in Book I).
    Below I have excerpted the statements of Postulates and Common Notions, and of some Definitions and Propositions from Book I by kind permission of David E. Joyce.
    (We'll restrict ourselves to Book I, but the 13 Books present a total of 468 Propositions based on the Postulates and Common Notions and on a total of 138 Definitions.)

    We need four Definitions.

    - Definition 10. When a straight line standing on a straight line makes the adjacent angles equal to one another, each of the equal angles is *right*, and the straight line standing on the other is called a *perpendicular* to that on which it stands.
    - Definition 15. A *circle* is a plane figure contained by one line such that all the straight lines falling upon it from one point among those lying within the figure equal one another.
    - Definition 20. Of trilateral figures, an *equilateral triangle* is that which has its three sides equal, an *isosceles triangle* that which has two of its sides alone equal, and a *scalene triangle* that which has its three sides unequal.
    - Definition 23. *Parallel* straight lines are straight lines which, being in the same plane and being produced indefinitely in both directions, do not meet one another in either direction.

    (These depend on five other Definitions.

    - Definition 1. A *point* is that which has no part.
    - Definition 2. A *line* is breadthless length.
    - Definition 4. A *straight line* is a line which lies evenly with the points on itself.
    - Definition 7. A *plane surface* is a surface which lies evenly with the straight lines on itself.

- Definition 19. *Rectilinear figures* are those which are contained by straight lines, *trilateral figures* being those contained by three, *quadrilateral* those contained by four, and *multilateral* those contained by more than four straight lines.

Only Definition 19 is actually useful.)

Here are the five Postulates.

- Postulate 1. To draw a straight line from any point to any point.
- Postulate 2. To produce a finite straight line continuously in a straight line.
- Postulate 3. To describe a circle with any center and radius.
- Postulate 4. That all right angles equal one another.
- Postulate 5. That, if a straight line falling on two straight lines makes the interior angles on the same side less than two right angles, the two straight lines, if produced indefinitely, meet on that side on which are the angles less than the two right angles.

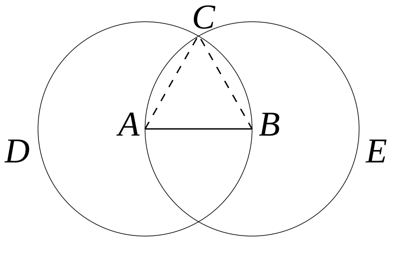
The first three Postulates are *constructions* and specify the two tools of classical geometry: the straightedge and the compass.
Note the large difference between the fifth and the first four. The fifth Postulate is not needed for the first 28 Propositions, and is used directly in Book I only by Proposition 29. These facts caused Euclid and subseqent mathematicians some uneasiness about it until alternatives to "Euclidean" geometry were discovered/invented in the 19th century.

And here are the five Common Notions.

- Common Notion 1. Things which equal the same thing also equal one another.
- Common Notion 2. If equals are added to equals, then the wholes are equal.
- Common Notion 3. If equals are subtracted from equals, then the remainders are equal.
- Common Notion 4. Things which coincide with one another equal one another.
- Common Notion 5. The whole is greater than the part.

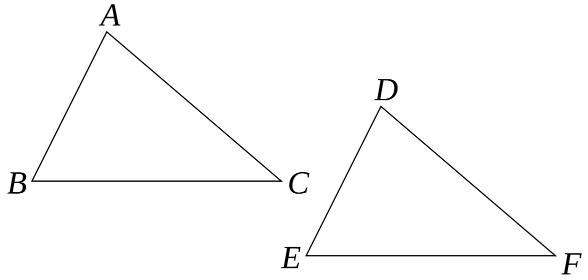
Let's see how these are used to establish first a constructive Proposition and second an assertive Proposition.

- Proposition 1. To construct an equilateral triangle on a given finite straight line.
- Proof. Let AB be the given line.



(Postulate 3.) Draw circle BCD with centre A and radius AB.
(Postulate 3.) Draw circle ACE with centre B and radius BA.
Let C be the upper point at which the circles intersect.
(Postulate 1.) Draw the straight lines CA and CB.
(Definition 5.) AC equals AB.
(Definition 5.) BC equals BA.
(Common Notion 1.) AC equals BC.
(Definition 20.) The triangle ABC is equilateral.
It has been constructed on AB as specified.

- Proposition 4. If two triangles have two sides equal to two sides respectively, and have the angles contained by the equal straight lines equal, then they also have the base equal to the base, the triangle equals the triangle, and the remaining angles equal the remaining angles respectively, namely those opposite the equal sides.
- Proof. Let ABC and DEF be two triangles having the two sides AB and AC equal to the two sides DE and DF respectively.



Superimpose ABC on DEF by placing point A on point D and line AB on line DE.
(Common Notion 4.) Point B also coincides with point E because AB equals DE.
(Common Notion 4.) Point C also coincides with point F because AC equals DF.
(Common Notion 4.) The base BC coincides with the base EF and equals it.
(Common Notion 4.) Thus triangle ABC coincides with triangle DEF and equals it, the first required result.
(Common Notion 4.) The remaining two angles also coincide with each other respectively and are respectively equal, the second required result.

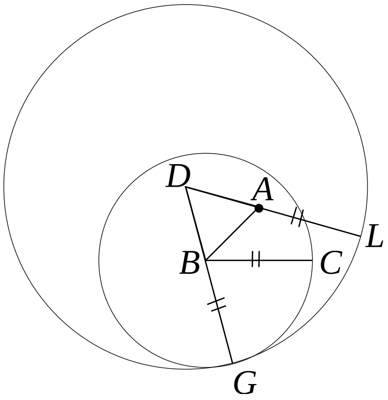
- NB. Proposition 4 is the first of three Propositions which give equality of triangles (equality in the sense of shape as well as area, a concept later called *congruity*), here from equality of two sides and their common angle. Proposition 8, below, shows equality of two triangles from equality of all three of their sides. Proposition 26, not given here, shows equality of two triangles from equality of two angles and one side.
  Propositions 4 and 8 employ the shaky notion of *superimposing* the two triangles to be compared. There are surfaces (not planes) on which we cannot move a triangle around without changing its shape.

The further propositions proceed similarly, but depend on each other, either directly or via intermediate propositions. Here is a self-contained chain selected from the forty-eight in Book I, with Proposition 4 being needed for Proposition 5 onwards.

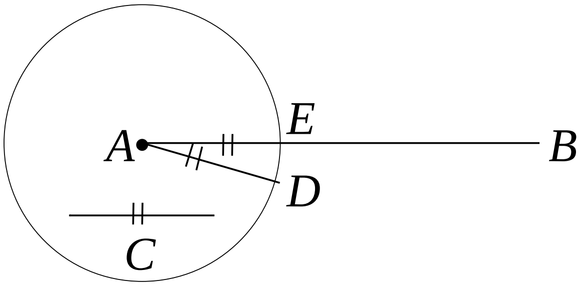
$$1 \to 2 \to 3 \to 5 \to 7 \to 8 \to 9 \to 10 \to 11 \to 13 \to 15 \to 16 \to 27 \to 28 \to 29$$

a) Here are the statements and the diagrams. Try to prove them using the Definitions, Postulates, Common Notions and preceding Propositions.

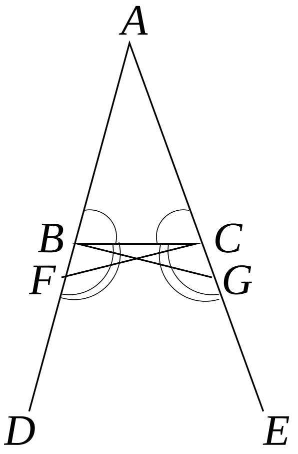
- Proposition 2. To place a straight line equal to a given straight line with one end at a given point.
- Preparation for Proof. To draw a straight line in some direction from A with length equal to that of BC. Use Proposition 1, Postulate 2 and Common Notion 3.



- NB. The purpose of Proposition 2 becomes apparent in Proposition 3.
- Proposition 3. To cut off from the greater of two given unequal straight lines a straight line equal to the less.
- Preparation for Proof. To cut off from AB a segment AE equal in length to line C. Use Proposition 2, Definition 15, Postulate 3, and Common Notion 1.

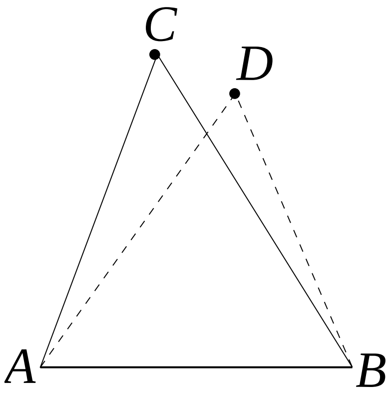


- NB. Proposition 3 is the the most extensively used of a “library” of propositions which Euclid systematically builds up for convenience.
- Proposition 5. In isosceles triangles the angles at the base equal one another, and, if the equal straight lines are produced further, then the angles under the base equal one another.
- Preparation for Proof. Show the equality of the marked angles in the isoceles triangle ABC. Use Propositions 3 and 4, Definition 20, Postulates 1 and 2, and Common Notion 3.

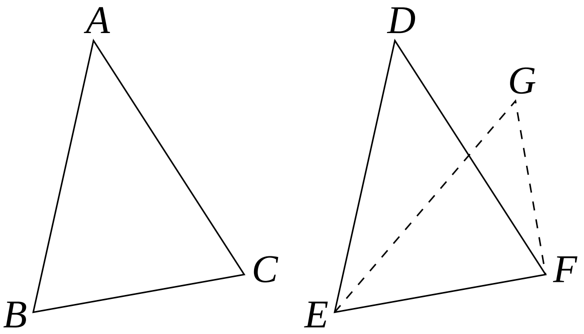


- NB. Prove that two pairs of triangles are equal rather than trying to use the notion, unsupported by Euclid, of the symmetry of the isoceles triangle: that’s why both conclusions are in the one proposition.

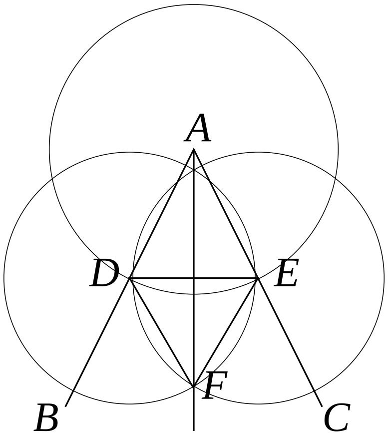
- Proposition 7. Given two straight lines constructed from the ends of a straight line and meeting in a point, there cannot be constructed from the ends of the same straight line, and on the same side of it, two other straight lines meeting in another point and equal to the former two respectively, namely each equal to that from the same end.
- Preparation for Proof. Connect the ends of the line AB to the point C: suppose the same can be done for some point D and show that $AC \neq AD$ and $BC \neq BD$. Use Proposition 5, Postulate 1 and Common Notion 5, as well as notions introduced in the *Nota Bene* below.



- NB. Proposition 7 uses *reductio ad absurdum*, or contradiction: pretend that you can do what the Proposition says you can't do and show that it leads to contradiction. (Some mathematicians do not consider this a valid way of proceeding.)
  Proposition 7 also uses ideas which, like symmetry, are unsupported by Euclid's preliminaries. The notions of greater and less than are not defined (they appear only in the Definitions, not given here, of obtuse and acute angles, and "less" appears in Postulate 5 and "greater" in Common Notion 5). So, first, the idea of *transitivity*, $x < y$ and $y < z$ means $x < z$, is not supported, nor is the related idea that $x < y$ and $y = z$ means $x < z$. Second, the idea of *trichotomy*, that $x < y$, $x = y$ and $y < x$ are complete and mutually exclusive alternatives, is also not in the preliminaries.
- Proposition 8. If two triangles have the two sides equal to two sides respectively, and also have the base equal to the base, then they also have the angles equal which are contained by the equal straight lines.
- Preparation for Proof. In triangles ABC and DEF with all sides respectively equal, show that that angles at A and D are equal so that Proposition 4 can be applied. Use Propositions 4 and 7 and Common Notion 4.

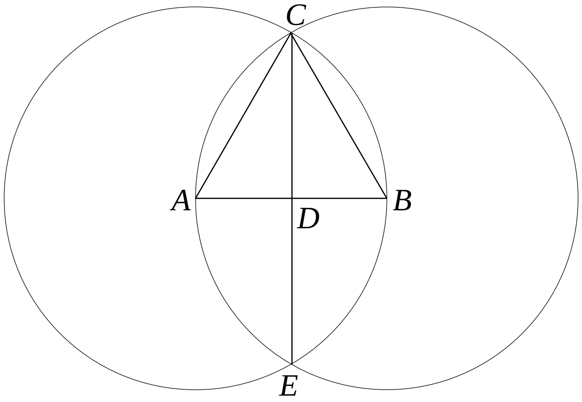


- Proposition 9. To bisect a given rectilinear angle.
- Preparation for Proof. Bisect the angle at A. Use Propositions 1, 3 and 8, Definition 20 and Postulate 1.

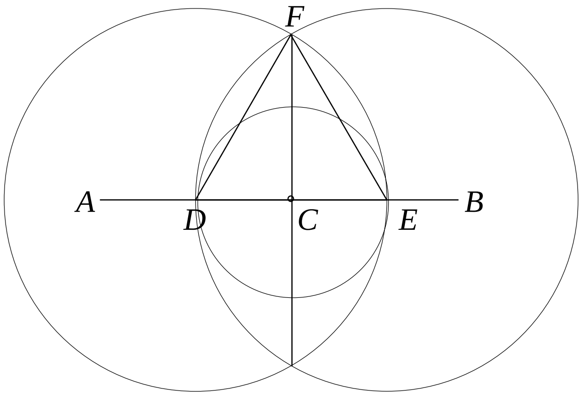


- NB. You can draw three circles directly instead of explicitly building the equilateral triangle.

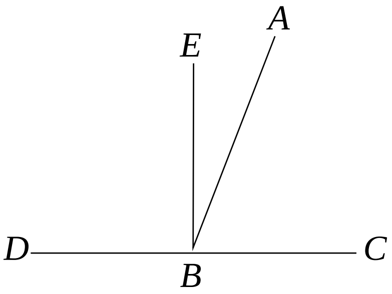
  While *bi*secting an angle is easy, *tri*secting one, in general, is impossible in Euclid's framework. A proof of this impossibility uses the fact that the ability to extract square roots does not give us cube roots: because the radius of a circle centred at $x = 0$, $y = 0$ satisfies $r = \sqrt{x^2 + y^2}$, Euclid's use of a compass is tantamount to the ability to extract square roots. But to trisect an angle is equivalent to extracting cube roots. The cube-root, square-root mismatch arises from another axiom system, the "field axioms", discussed in the Excursions for Note 7 of Week 4.
- Proposition 10. To bisect a given finite straight line.
- Preparation for Proof. Bisect line AB. Use Propositions 1 and 9 to do the construction and Proposition 4 and Definition 20 to prove it.



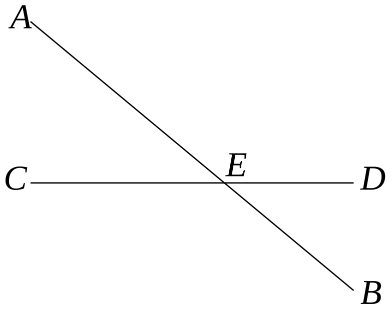
- NB. Again, there's a short cut.
- Proposition 11. To draw a straight line at right angles to a given straight line from a given point on it.
- Preparation for Proof. Draw a straight line at right angles to AB from C. Use Propositions 1, 3 and 8, Definitions 10 and 20, and Postulate 1.



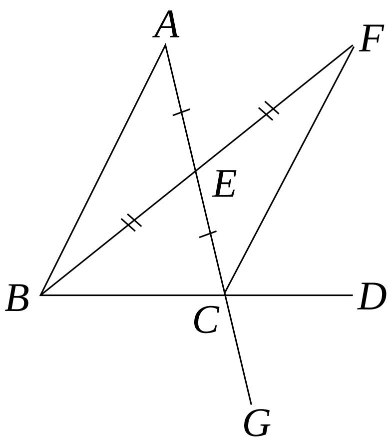
- Proposition 13. If a straight line stands on a straight line, then it makes either two right angles or angles whose sum equals two right angles.
- Preparation for Proof. Let AB be the straight line standing on straight line CD and show that $\angle CBA + \angle ABD$ equals two right angles. Use Proposition 11, Definition 10 and Common Notions 1 and 2.



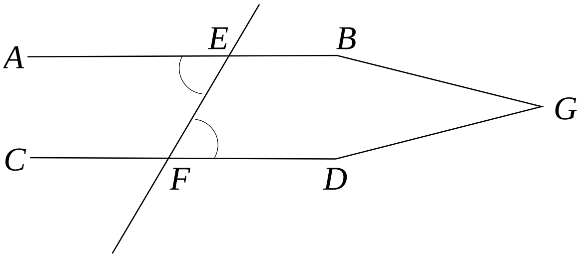
- NB. Euclid considered that the only possible “angles” must be less than two right angles, so the “sums” in Proposition 13 are formal and do not necessarily constitute angles themselves. In particular, a “straight angle” is not an admissible concept.
- Proposition 15. If two straight lines cut one another, then they make the vertical angles equal to one another.
- Preparation for Proof. If straight lines AB and CD cut each other at E, show that $\angle CEA = \angle DEB$ and $\angle BEC = \angle AED$. Use Proposition 13, Postulate 4 and Common Notions 1 and 3.



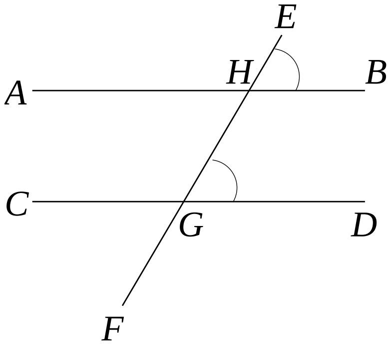
- Proposition 16. In any triangle, if one of the sides is produced, then the exterior angle is greater than either of the interior and opposite angles.
- Preparation for Proof. Let ABC be a triangle, and let one side of it BC be produced to D. Show that the exterior angle ACD is greater than either of the interior and opposite angles CBA and BAC. Use Propositions 3, 4, 10 and 15, Postulates 1 and 2, and Common Notion 5.



- Proposition 27. If a straight line falling on two straight lines makes the alternate angles equal to one another, then the straight lines are parallel to one another.
- Preparation for Proof. Let the straight line *EF* falling on the two straight lines *AB* and *CD* make the alternate angles *AEF* and *EFD* equal to one another. Show, by contradiction, that *AB* is parallel to *CD*. Use Proposition 16 and Definition 23.



- NB. This and the next Proposition establish two *sufficient* conditions on angles for lines to be parallel. Proposition 29 gives the converse of both, thus establishing the *necessity* of these conditions.
  Joyce gives a discussion in connection with Proposition 27 on logical inverses and other logical operations already familiar to us from this Week.
- Proposition 28. If a straight line falling on two straight lines makes the exterior angle equal to the interior and opposite angle on the same side, or the sum of the interior angles on the same side equal to two right angles, then the straight lines are parallel to one another.
- Preparation for Proof. Let the straight line *EF* falling on the two straight lines *AB* and *CD* make the exterior angle *EGB* equal to the interior and opposite angle *GHD*, or the sum of the interior angles on the same side, namely *BGH* and *GHD*, equal to two right angles. Show that *AB* is parallel to *CD*. Use Propositions 13, 15 and 27, Postulate 4 and Common Notions 1 and 3.



- Proposition 29. A straight line falling on parallel straight lines makes the alternate angles equal to one another, the exterior angle equal to the interior and opposite angle, and the sum of the interior angles on the same side equal to two right angles.
- Preparation for Proof. If *EF* falls on parallel lines AB and CD (see the diagram for Proposition 28), show that the alternate angles $\angle AGH = \angle GHD$, the exterior angle *EGB* equals the interior and opposite angle *GDH*, and $\angle BGH + \angle GHD$ equals two right angles. Use Propositions 13 and 15, Postulate 5, and Common Notions 1 and 2.
- NB. Proposition 29 is the first to depend on Postulate 5, and all subsequent Propositions (except Proposition 31) and especially Proposition 32, depend on Proposition 29.

b) Find a triangle on a sphere which violates Proposition 16. In spherical geometry, "straight lines" are defined as parts of great circles, which are the shortest distance between two points on a spherical surface: a *great circle* on a sphere is the intersection of the sphere with a plane containing the centre point of the sphere; it is a largest possible circle within the spherical surface. Hint: include the "north pole" and part of the "equator" in your spherical triangle. Where is the failure point in Euclid's system that allows Proposition 16 to be "proved" even though it is not valid in a different interpretation?

61. Any part of the Preliminary Notes that needs working through.

References

[Boo54] George Boole. *An Investigation of the Laws of Thought, on Which Are Founded the Mathematical Theories of Logic and Probabilities.* Dover Publications, 1858 and 1973, 1854. http://www.gutenberg.org/etext/15114.

[Dew89] A. K. Dewdney. *The Turing Omnibus: 61 Excursions in Computer Science.* Computer Science Press, Rockville, MD, 1989.

[Dew93] A. K. Dewdney. *The New Turing Omnibus: 66 Excursions in Computer Science.* Computer Science Press, Rockville, MD, 1993.

[Fey99] Richard P. Feynman. *Feynman Lectures on Computation.* Westview Press, Oxford, 1999. edited by Tony Hey and Robin W. Allen.

[Joy98] David E. Joyce. Euclid's elements. URL http://aleph0.clarku.edu/∼djoyce/java/elements/elements.html (accessed 2013/7), 1996,1997,1998.

[Kle85] Sheldon Klein. The invention of computationally plausible knowledge systems in the upper paleolithic. Technical Report 628, Computer Sciences, University of Wisconsin-Madison, Madison, WI, Dec. 1985. Presented at The World Archeological Congress, Southampton and London, 1–7 Sept. 1986, Allen and Unwin.

[SM13] Mehdi Saeedi and Igor L. Markov. Synthesis and optimization of reversible circuits—a survey. *ACM Computing Surveys*, 45(2):178–211, Feb. 2013. arXiv:1110.2574v2 [cs.ET] 20 Mar 2013, URL= https://arxiv.org/abs/1110.2574.