# Excursions in Computing Science: Week 1. Polarized Light

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

August 1, 2021

## I. Prefatory Notes

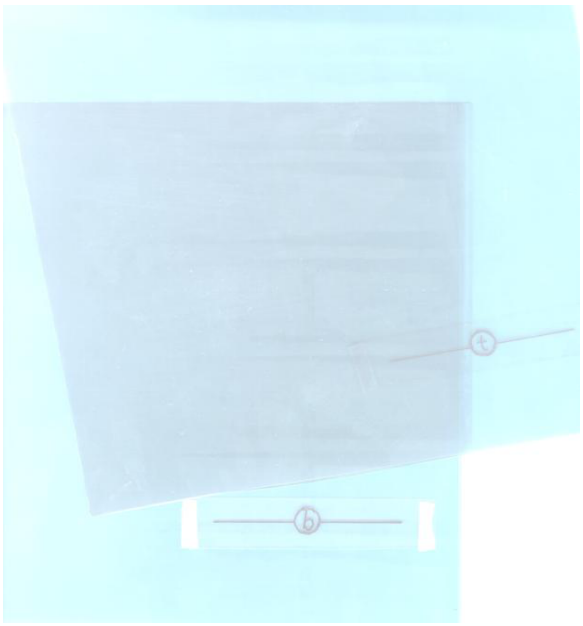
1. Here is a polarizing filter on a source of light, showing the direction of polarization.

The Bottom Polarizing Filter

 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.

The amount of light getting through does not depend on the angle of this direction of polarization.

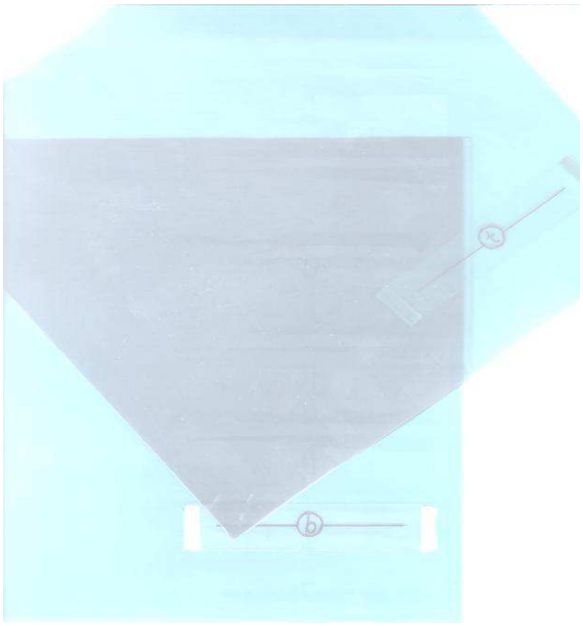
2. Here are two polarizing filters, with the top one, t, at an angle of 0.17 radians to the original, now bottom, one, b.




Top and Bottom Polarizing Flters at $10^{0}$

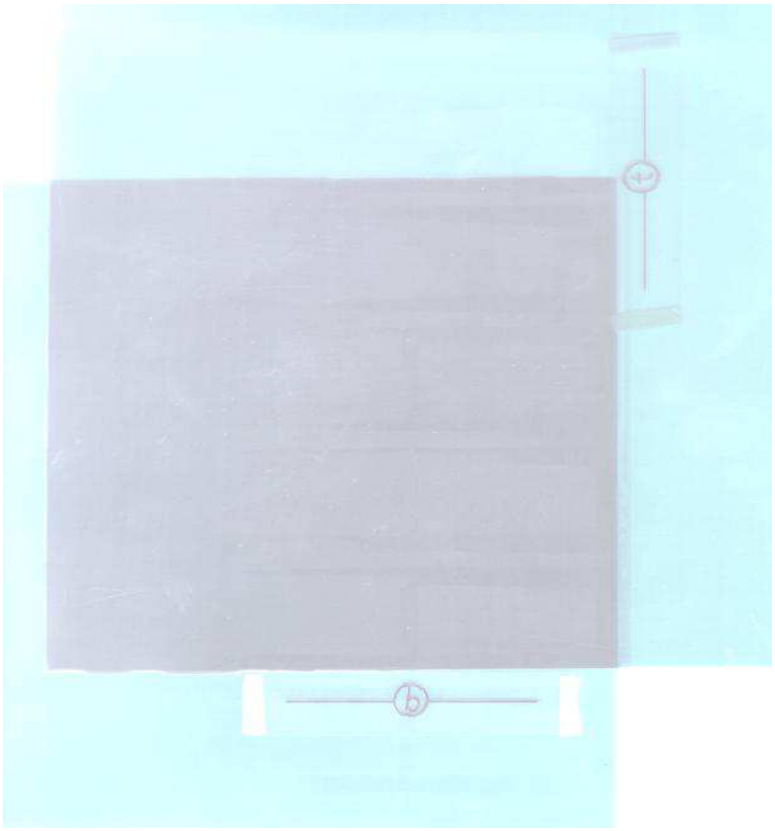
The amount of light getting through decreases as the angle between the two increases:

Here are two polarizing filters, with the top one, t, at an angle of 0.60 radians to the bottom, one, b. Less light gets through than at 0.17 radians.




Top and Bottom Polarizing Filters at $35^{0}$

Finally, here they are with t at angle $\pi/2$ to b: no light gets through.




Top and Bottom Polarizing Filters at $90^0$

3. Can we make a theory for this?

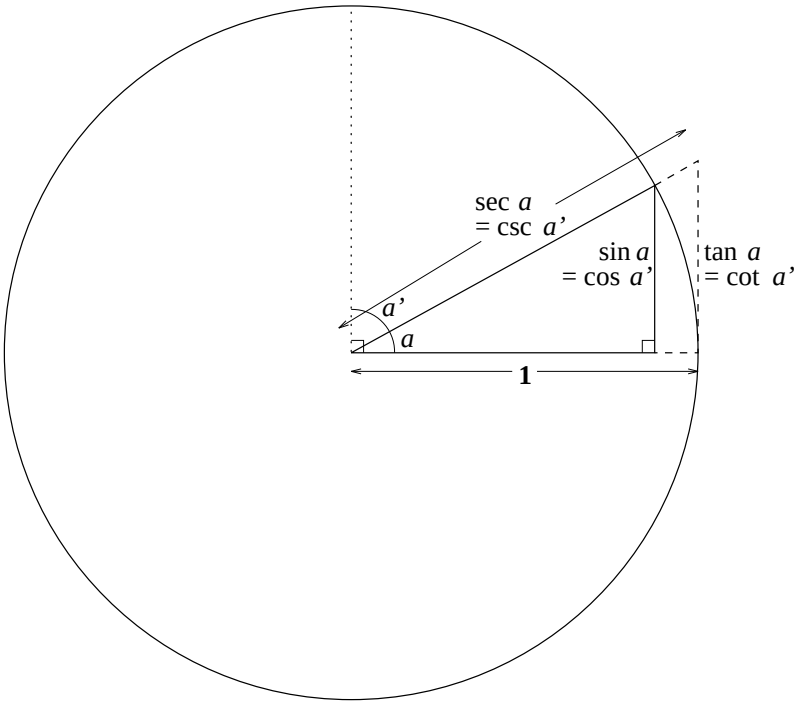
A theory should:

- be falsifiable;
- enable calculation.

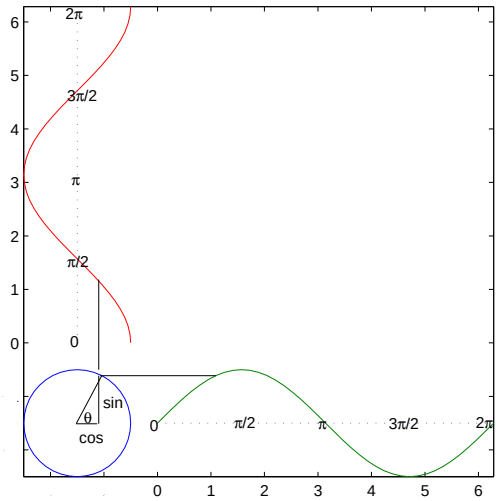
These are related: a theory which leads to deductions in the form of precise numbers can easily be proved wrong by measurements which give different numbers. A theory which survives determined attempts to prove it wrong is good science.

Since we are concerned with angles between directions of polarization, we should revisit trigonometry.

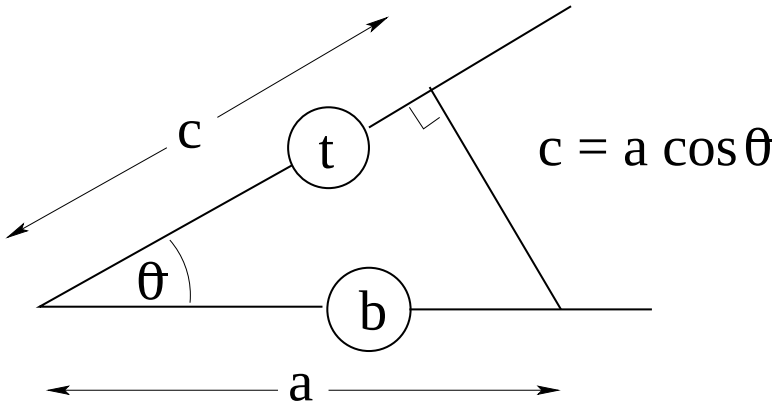
All of trig:




Let's focus on sine and cosine.

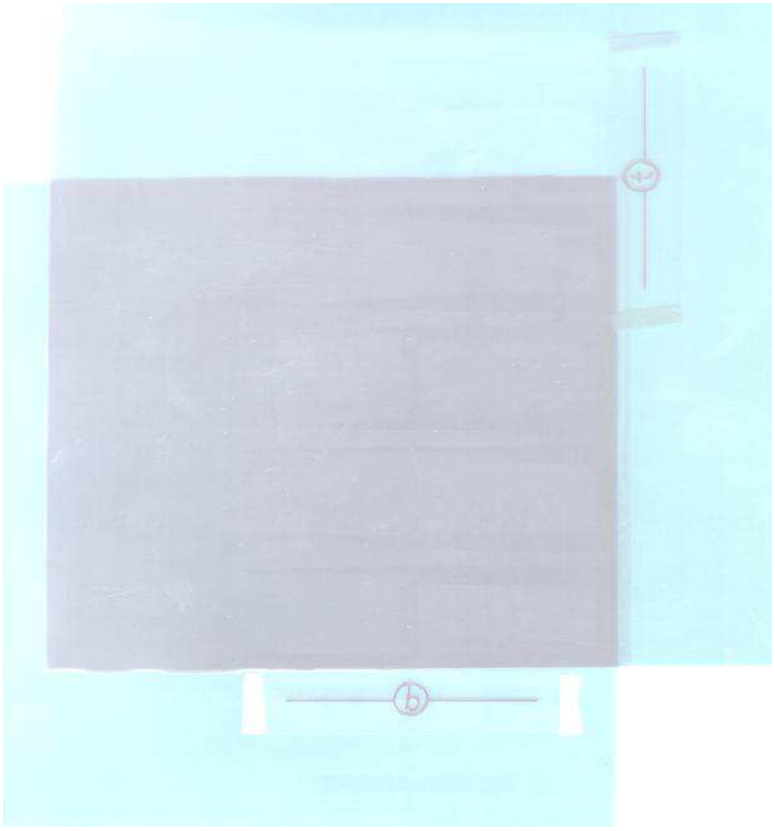



4. Which trig function diminishes to 0 as the angle increases to $\pi/2$? Let's try cosine as a theory.




($a$ is the *amplitude* of the light through the bottom polarizing filter.)

5. Theories should predict (this is part of being falsifiable). Let's predict what will happen with a third polarizing filter. Here are the top and bottom filters at right angles.

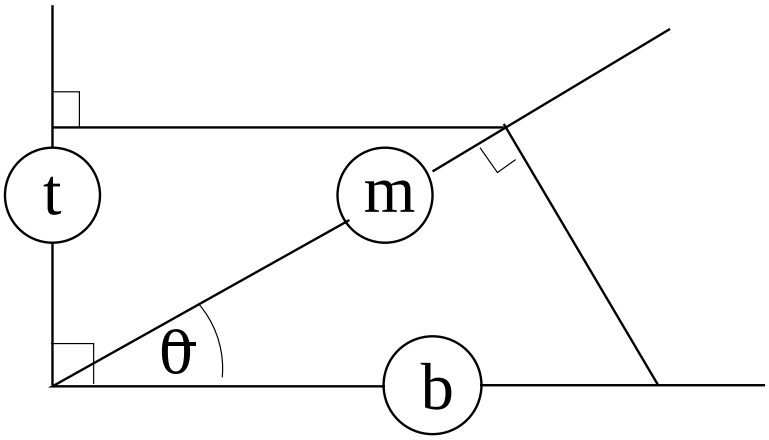


Top and Bottom Polarizing Filters at 90°

What will happen if a third polarizing filter is put on top of them?

What will happen if the third polarizing filter is put in between them?

6. Here's what our theory says about putting it in between.




$$\begin{aligned} a_m &= a_b \cos\theta \\ a_t &= a_m \cos(\pi/2 - \theta) \\ &= a_b \cos\theta \cos(\pi/2 - \theta) \\ &= a_b \cos\theta \sin\theta \end{aligned}$$

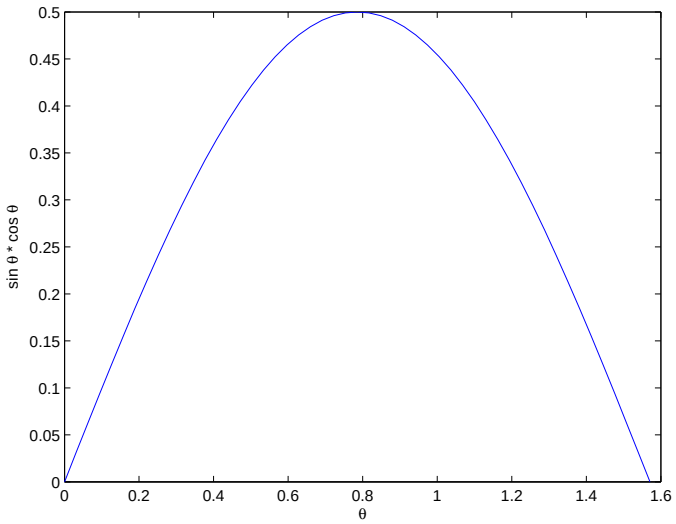
MATLAB can tell us what this is for, say $\theta = \pi/4$:

```
cos(pi/4) * sin(pi/4)

ans =

    0.5000
```

This is non-zero: light gets through! Does it? Let's try the three polarizing filters at $\pi/4$.. MATLAB can give us a plot.



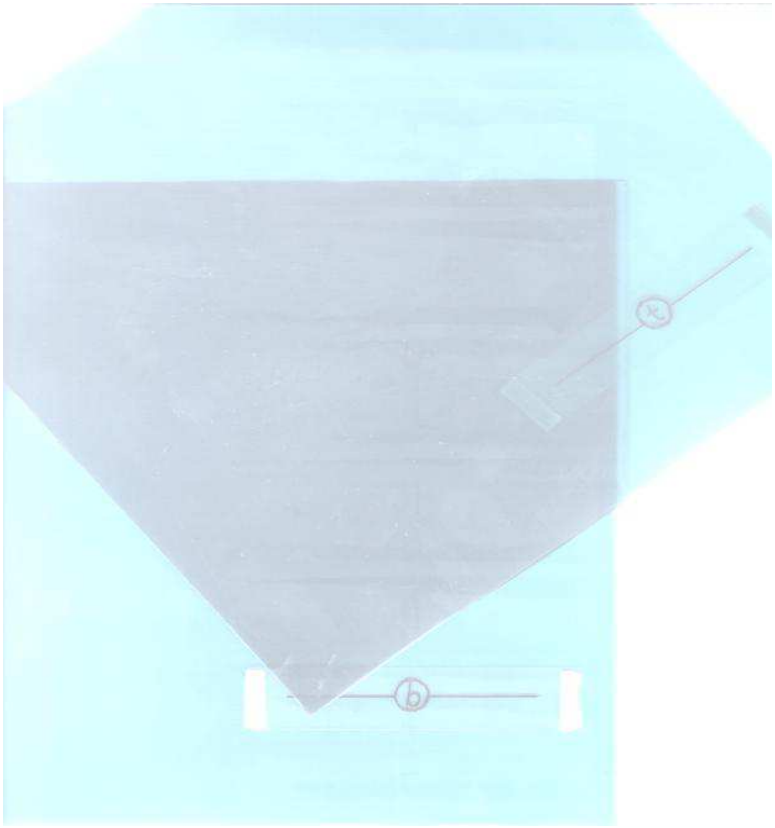
```
theta = [0:pi/100:pi/2];
cs = cos(theta) .* sin(theta);
plot(theta,cs)
xlabel('\theta'), ylabel('sin \theta * cos \theta')
```

This predicts the transmitted light will go from 0 at angle 0 through a maximum of 0.5 at $\pi/4$ and back down to zero at $\pi/2$. Does it? Let's rotate the middle polarizing filter, m.

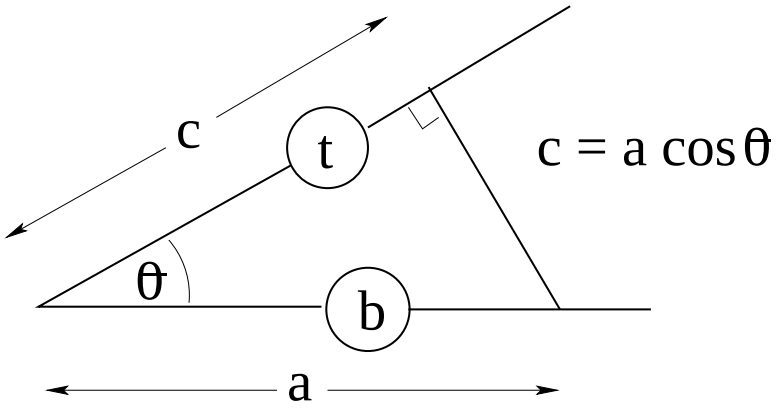
7. As far as we can tell—qualitatively, not quantitatively: without measuring the light strengths—the theory makes the right predictions.

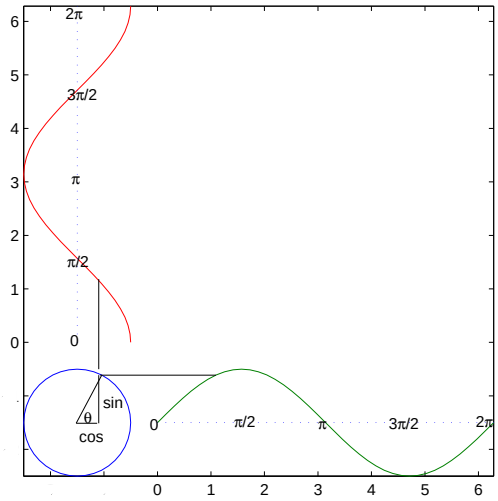
Does it make any wrong predictions?

8. Let's go back to two polarizing filters.



Top and Bottom Polarizing Filters at 35°




Cosine goes negative!

What does negative light strength mean?

How would we force it to be positive?

9. To test it properly, we really need to make the measurements. But this is not a course on how to measure light strength, so let's go to history.

In 1810, Etienne Louis Malus, in Paris, found

$$I_t \quad = \quad I_b \cos^2(\theta)$$

$I$ is the *intensity*.

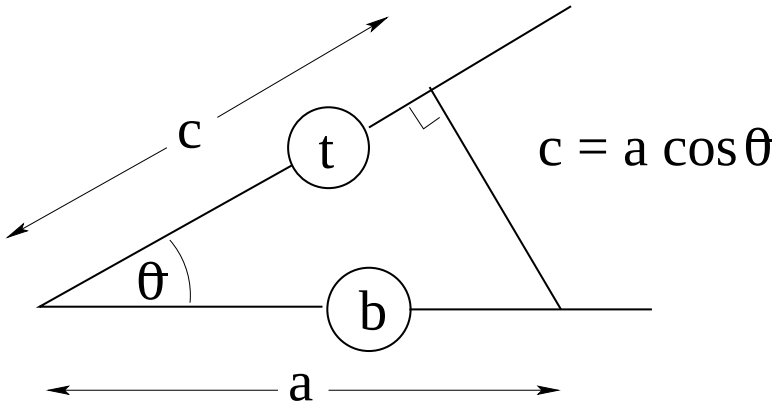
So we take the square.

Do we do this before we work out the three-filter result, or afterwards?

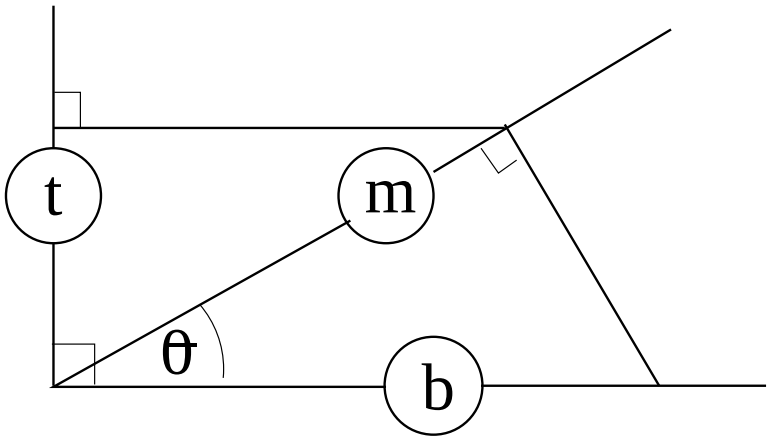
When we look at quantum theory, we'll find out why we do the calculations before squaring, then square to compare with the measurements.

10. So we'll just square our results.

Two polaroids: $I \times (\cos(\theta))^2$




Three polaroids: $I \times (\cos(\theta)\sin(\theta))^2$




## 11. **Algorithm for scientific theories.**

1. Invent a theory (imagination)
2. Make a prediction (deduction/calculation)
3. Test prediction against observation (measurement/experiment)
4. If it's wrong, goto 1; else goto 2 (falsification)

(The longer we loop from (2) the better the theory.)

## 12. **Summary**

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

We have

- explained two polarizing filters and three polarizing filters
  - light has a direction of polarization (angle of line)
  - light has a brightness ("amplitude/intensity") (length of line)
  - polarization in one direction has components in any other direction, except the direction at right angles to it

- reviewed trigonometry
- introduced MATLAB
- begun an understanding of scientific theories

# II. The Excursions

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

1. **Quantitative thinking is important.** (Eugene Lehman) Eugene wrapped a belt all the way around the Earth's equator, floating it across the surfaces of the oceans and tunnelling through hills and mountains at sea level, for all 40075 *kilo*meters. In the dark of night, Tim cut the belt and inserted an extra length of $\pi$ *meters*.
   a) Guess whether, on a sea-level beach: an ant could now squeeze under the extended belt; a toy car could be pushed under the belt; Tim could ride a bike under the belt; Tim could drive a car under the belt; or a building could be built under the belt.
   b) Use the relationship between diameter and circumference of a circle to see how much higher than sea level the extended belt would be, if kept a circle centered at the centre of the Earth.
   c) How much could this be increased by moving the belt but keeping it circular?
   d) How much could it be increased by allowing the belt to be flexible?

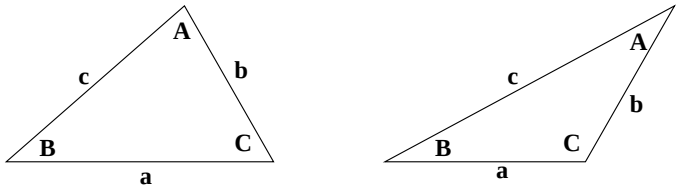
2. Get hold of three pairs of polaroid glasses (or two pairs, if you're allowed to break one in half) and repeat all the experiments.

3. **Measuring angles.** Angles can be measured using various units, and we pick one convention throughout. We use "radians" as the unit. A radian is the angle we must turn through to draw a circular arc whose length equals the radius. Since the ratio of circumference to radius is $2\pi$, a full cycle is $2\pi$ radians. There are some important reasons for choosing radians, which we will see later, notably in Book 8c.
   Draw a hexagon inside a circle of radius 1 to see that a radian is just less than the angle inside an equilateral triangle.
   Other units could be "cycles" or "degrees". Angles measured in cycles would be some fraction of 1, with 1 being the angle of a full cycle.
   Degrees provide a way of writing the most frequently used angles as integers. 360 degrees make a full cycle, and 360 has many divisors.
   We must also adopt a convention for the direction of an angle. This convention is that counterclockwise angles are positive and clockwise angles are negative. Unless stated, or negative, angles are assumed counterclockwise.
   Write in radians, cycles and degrees the following angles: a right angle, a clockwise right angle (don't use a minus sign for this one), the angle that reverses direction, half a right angle, one fifth, one sixth and one twelfth of a full cycle.

4. Use MATLAB to plot both cos and $\cos^2$ in the same plot for a full period, $0..2\pi$ What does this mean for two polarizing filters at relative angle between 0 and $\pi/2$? Why do we use $\pi(\pi/2, \pi, 2\pi, ..)$ and not degrees (90, 180, 360, ..)?

5. Use MATLAB to plot both sin(t) and $\cos(\pi/2 - t)$ in the same plot for a full period, $0..2\pi$ Give a simple argument why they should be the same.

6. (Trig. and triangles) a) On MATLAB plots, show that $\cos(-t) = \cos(t)$ and $\sin(-t) = -\sin(t)$. What are the relationships between $\cos(\pi - t)$ and $\cos(t)$? $\sin(\pi - t)$ and $\sin(t)$?
   b) In both of the triangles shown, why is $b\sin(C) = c\sin(B)$?

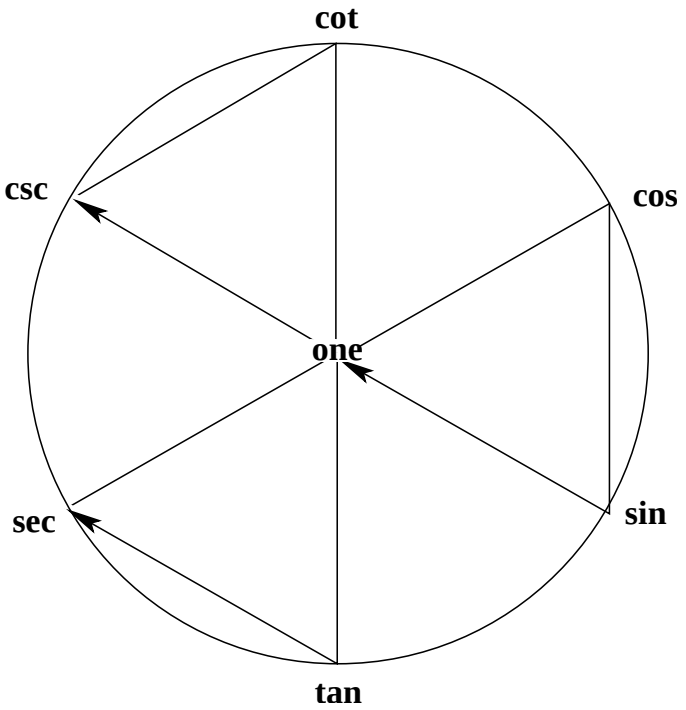



   c) Use symmetry to show that $a\sin(C) = c\sin(A)$ and $b\sin(A) = a\sin(B)$, and hence

$$\frac{a}{\sin(A)} = \frac{b}{\sin(B)} = \frac{c}{\sin(C)}.$$

   d) Going back to the triangles and the relationship of (b), and Pythagoras' theorem, show that $2ab\cos(C) = a^2 + b^2 - c^2$. By symmetry, show that $2bc\cos(A) = b^2 + c^2 - a^2$ and $2ca\cos(B) = c^2 + a^2 - b^2$.

7. Eugene's Clock (Eugene Lehman) is constructed by writing "cos, sin, tan" clockwise in alphabetical order on one side of a circle, then writing their inverses, "sec, csc, cot" diagonally opposite. Construct directed triangles, as in the radioactivity symbol, for each pair and the centre, starting cos–sin–centre, with the arrow showing the end of each loop always pointing in the same direction.

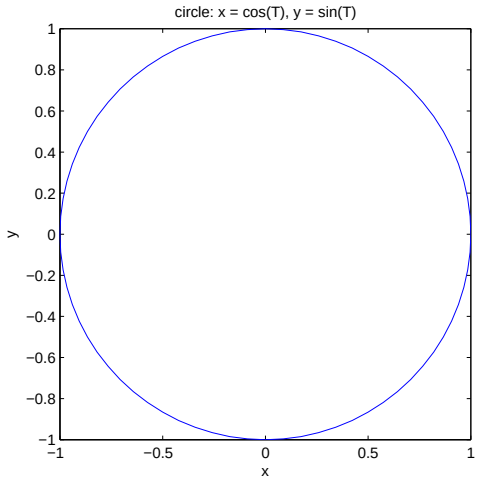



   a) Show that the sum of the squares on the first two vertices of each triangle equals the square on the third vertex, with the centre vertex being 1. (Is it the same whether

you go in or against the direction of the arrow?)
b) Show that each of the six triples, $a, b, c$, as you go clockwise around the circumference of the circle, satisfies $a = b/c$. Can you make a pattern for multiplying instead of dividing?
c) What happens in (b) as you go counterclockwise? What about across any diagonal?

8. **Celtic knots and other fun with cos and sin.** What happens if we plot cos() and sin() against each other?

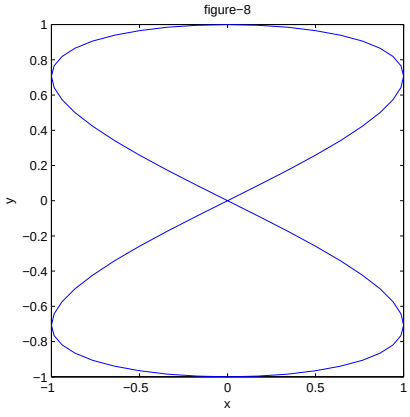
```
% function circle          THM          1
function circle
T = 0:5:360;      % angle parameter in de
ang = T*pi/180;   % angle parameter in ra
plot(cos(ang),sin(ang))
title('circle: x = cos(T), y = sin(T)')
xlabel('x')
ylabel('y')
axis square
```

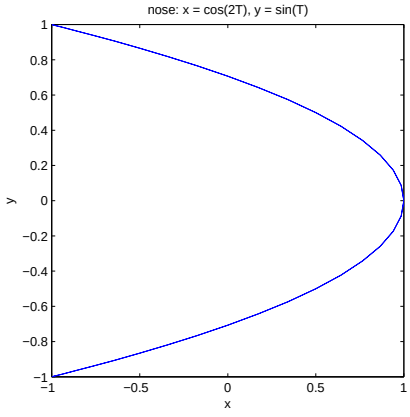



How does this work? Let's calculate $x$ (cos($T$)) and $y$ (sin($T$)) for a few angles $T$ (in degrees, for familiarity). Note that .7 is really $1/\sqrt{2}$: how does this arise?

| $T$ | 0 | 45 | 90 | 135 | 180 | 225 | 270 | 315 | 360 |
|---|---|---|---|---|---|---|---|---|---|
| $x$=cos($T$) | 1 | .7 | 0 | −.7 | −1 | −.7 | 0 | .7 | 1 |
| $y$=sin($T$) | 0 | .7 | 1 | .7 | 0 | −.7 | −1 | −.7 | 0 |

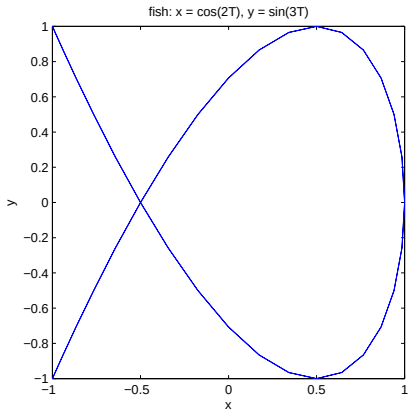
a) Trace the positions of each of these points on the circle. What would happen if we swapped the cos and the sin: $x = \sin(T)$, $y = \cos(T)$?

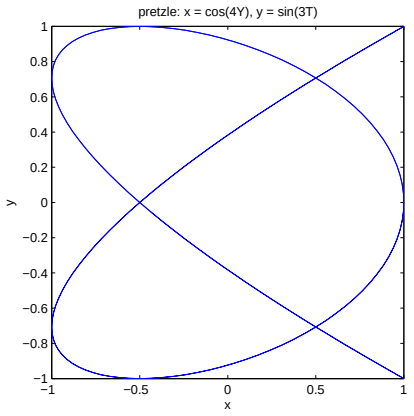


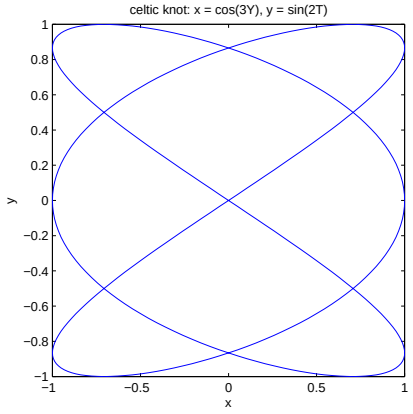

b) How would you make a figure-8? Hint: the drawing starts at the top; write down a sequence of points such as $(x, y)$ = (0,1), (1,.7), (0,0), .. and see if you can figure out

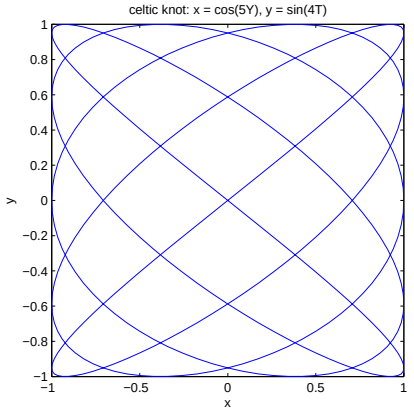
how to generate these with sin() and cos(). After you've figured it out, then modify the program and try it.
c) How would you turn the figure-8 into a bow-tie? Turning the figure-8 into a bow tie incorrectly might result in a "nose" (above). Notice the "free ends". What is the condition that generates such free ends? Here are some more.



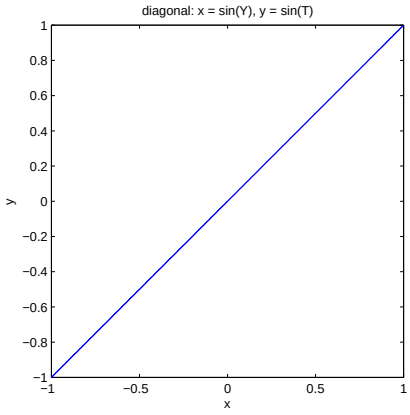



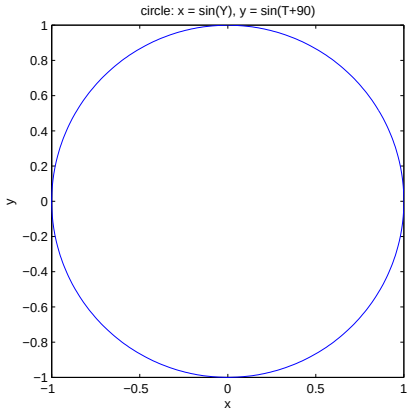

d) The prettiest pictures you can probably get are "Celtic knots". Here are two. Find some more.



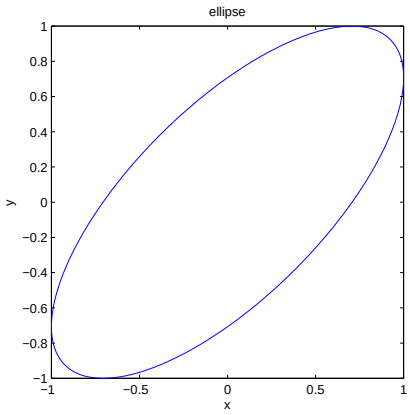



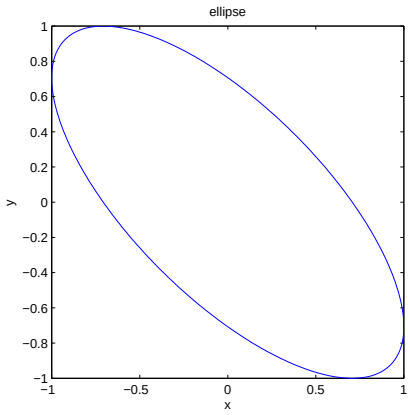

e) What can you say about the common denominator of $m$ and $n$ in a figure drawn by, say $x = \cos(mT)$ and $y = \sin(nT)$?
What happens if you use only sin()? Here are a diagonal line and a circle.



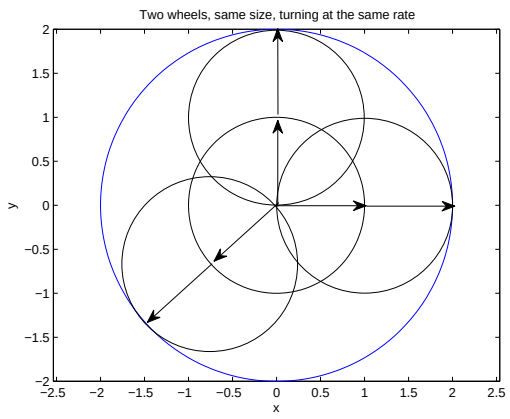

f) How would you make an ellipse? (Hint: it's "in between" a diagonal line and a circle.) How would you make the ellipse tilt the other way? How many different ways can you do this?

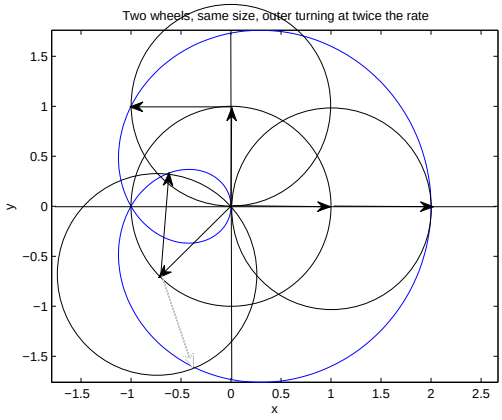


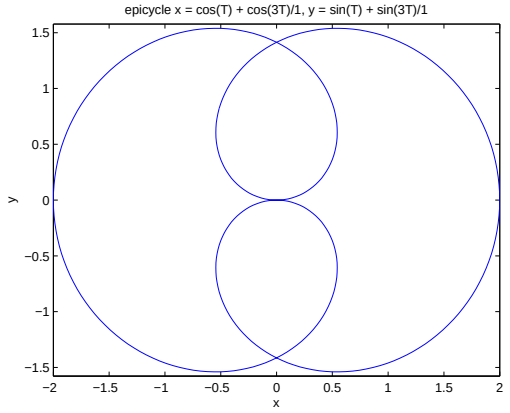

g) How would you make a skinnier ellipse? A really skinny ellipse? A fatter ellipse?

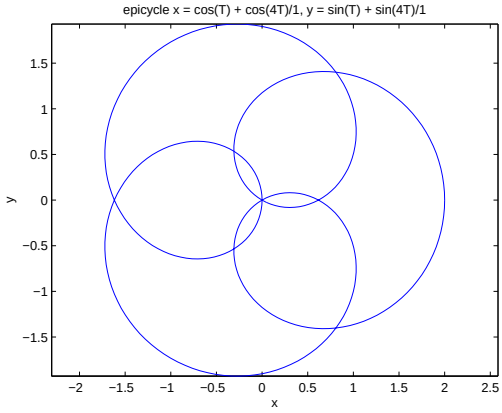
Since we can draw Celtic knots, how about a shamrock? This requires something new: *two* circles, one revolving around the other.
Let's start simply. Imagine a wheel with a pen on its rim, attached by its axle to another wheel. If both wheels are rotating at the same rate the pen will draw a circle. But if the outer wheel is turning twice as fast as the one it's attached to, the pen will do a loop.



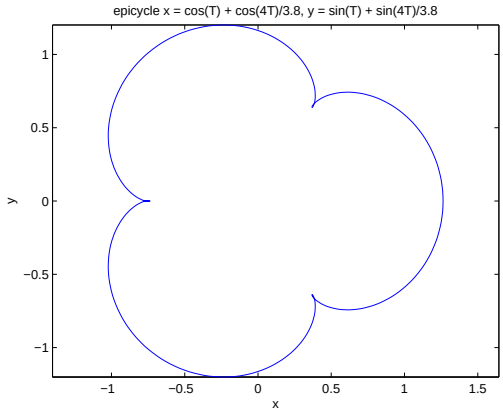




h) How would you change the program to draw (the blue part of) these two pictures? Hint: $x$ will involve two cosines, $\cos(T)$ being one, and since when $T = 0$ the pen is at $x = 2$, these cosines must be added.
i) Now we observe that since *one* loop is made by rotating the outer wheel *twice* as fast as the inner, we can get more loops by speeding up the outer rotation. Reproduce the following.




j) Now you should be able to adjust to get the following sort-of shamrock. How would you improve it?



9. Use MATLAB to draw $\cos(t)\sin(t)$ for a full period, $0..2\pi$ Give a simple argument why it is positive in the first quadrant, except for two places where it is zero. What else is needed to explain the behaviour of three polarizing filters, two at $\pi/2$ from each other and the third in between at relative angle between 0 and $\pi/2$?

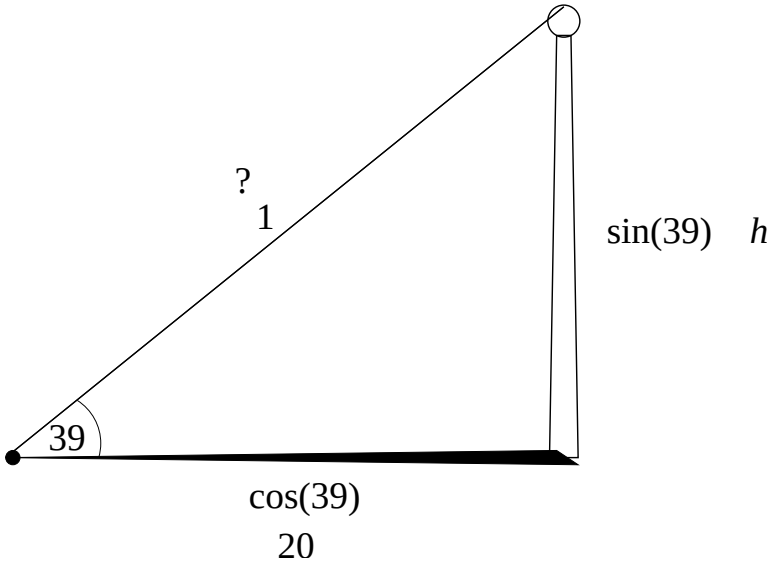
10. Use MATLAB to draw $(\cos(t))^2$ and $\text{abs}(\cos(t))$ on the same plot, for comparison. Do the same for $(\cos(t)*\sin(t))^2$ and $\text{abs}(\cos(t)*\sin(t))$. Why should we not take the absolute value of the cosine to repair our theory, instead of squaring it?

11. Look up the uses of "polarizing filters". How can you tell if the "polaroid" sunglasses at a store really are polarizing filters? Look through polarizing glasses, at various angles, at: daylight reflected off a mirror, off a puddle and off a sunny highway. Which direction do you think the light is polarized in that is passed by polarizing glasses worn in the normal way? If you are walking along the bottom of a smooth and shiny wet cliff, wearing polarizing sunglasses, and suddenly the angle of the sun produces a tremendous glare off the cliff, what should you do?

12. Take a pair of polarizing sunglasses outside on a sunny day and see if you can see that sunlight has a strong component of polarization in directions that form a circle around the sun. *Do not look directly at, or near, the sun.*
    Look up Karl von Frisch and the waggle dance of bees (1947) and discuss the bees' sense of direction in terms of this polarization of sunlight.

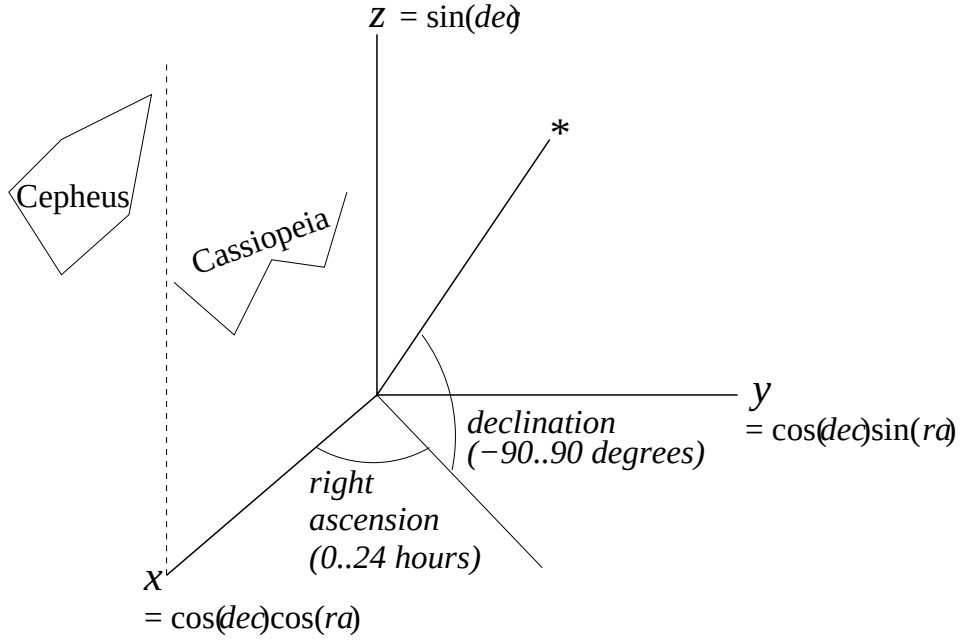
13. Hold, at the middle of two opposite sides, a rectangular piece of cardboard horizontally under a lamp so its shadow is on the floor or on a desk. Rotate the cardboard about the line across the middle. Make a theory about how the shape and area of the shadow changes. Can you find a way to make some measurements to see if your theory is wrong?

14. **Useful cos and sin.** Suppose we have an unclimbable flagpole whose height we must measure. It is perpendicular and standing in a level, horizontal plaza.
    At a certain time of day, the shadow of the flagpole is 20 meters long (say), which we can measure along the ground. The sun casting this shadow is 39 degrees up in the sky (say). If the triangle made by pole and shadow were a trig triangle—namely with hypotenuse 1—then its base (corresponding to the shadow) would be cos(39) and its height (corresponding to the pole) would be sin(39). We don't know the hypotenuse of the flagpole triangle, and don't want to know it, so we call it "?". We do know the base: 20. And we don't know, but would like to know, the height, which we call $h$.
    Since the trig triangle and the flagpole triangle have the common angle of 39 degrees they are similar and we can draw them on top of each other but with two sets of lengths.




The inner set of numbers are for the trig triangle. The outer set of numbers and symbols give the flagpole triangle.
Use a calculator to find cos(39) and sin(39), remembering that the 39 is *degrees*. From this, use the diagram to figure out how to find the height $h$.

15. Trigonometry can help us locate the stars. Using sin() and cos() we can convert to $x, y$ and $z$ from the astronomical coordinates of *right ascension* (measured eastwards in hours, minutes and seconds) and *declination* (measured northwards in degrees, minutes and seconds, and southward with the negative of these) as shown. (The zero of right ascension is the "vernal equinox", part of the line where the plane that the earth's equator lies in intersects the plane of the Earth's orbit around the Sun. This puts it between the easily identifiable constellations of Cassiopeia and Cepheus. (Look up the mythology of these constellations!))
(Look up "spherical coordinates": how do they differ from astronomical coordinates?)

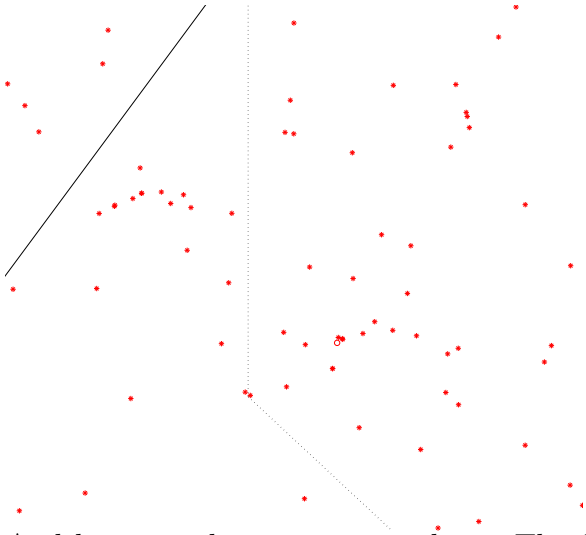


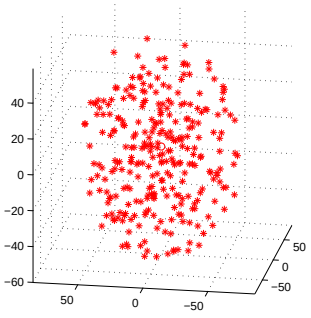
a) Inspect the following code, which is a slightly roundabout MATLAB way to extract data from a file, in this case the Yale Bright Star Catalog of the 9110 brightest stars, yale.txt, which is stored on the SOCS teaching computers at the location indicated. Run it with $n = 5$ and print the resulting data for the brightest five and the closest five stars. Run it, without printing, for $n = 300$, in preparation for part (b).

```
% function [brightest,closest] = selectStars(n)
% THM 070502 in file selectStars.m
function [brightest,closest] = selectStars(n)
yaleBSC = textread('/home/course/cs199/yale.txt','%s','delimiter','\n','whitespace','
for k = 1:size(yaleBSC)
   StarNo(k) = str2double(yaleBSC{k}(1:4)); % number in the Yale BSC
   RA19h(k) = str2double(yaleBSC{k}(53:54)); % right ascension, 1900: h, m, s
   RA19m(k) = str2double(yaleBSC{k}(56:57));
   RA19s(k) = str2double(yaleBSC{k}(59:62));
   DEC19sgn(k) = yaleBSC{k}(64); % declination, 1900: +-, d, m, s
   DEC19d(k) = str2double(yaleBSC{k}(65:66));
   DEC19m(k) = str2double(yaleBSC{k}(68:69));
   DEC19s(k) = str2double(yaleBSC{k}(71:72));
   RA20h(k) = str2double(yaleBSC{k}(74:75)); % right ascension, 2000: h, m, s
   RA20m(k) = str2double(yaleBSC{k}(77:78));
   RA20s(k) = str2double(yaleBSC{k}(80:83));
   DEC20sgn(k) = yaleBSC{k}(85); % declination, 1900: +-, d, m, s
   DEC20d(k) = str2double(yaleBSC{k}(86:87));
   DEC20m(k) = str2double(yaleBSC{k}(89:90));
   DEC20s(k) = str2double(yaleBSC{k}(92:93));
   vMag(k) = str2double(yaleBSC{k}(109:113)); % visual magnitude("brightness")
   annMoRA(k) = str2double(yaleBSC{k}(156:161));% annual motion of rt ascension
   annMoDEC(k) = str2double(yaleBSC{k}(163:168));% annual motion of declination
   parx(k) = str2double(yaleBSC{k}(171:174)); % parallax (seconds)
   rankB(k) = k; % rank for sorting brightness
   rankC(k) = k;
end
magrank = sortrows([vMag',rankB']); % ascending by visual magnitude
nearank = sortrows([parx',rankC'],-1); % descending by parallax
for k = 1:n % n brightest, closest
   bk = magrank(k,2); % select in order of brightness
   brightest(k,1) = StarNo(bk);
   brightest(k,2) = RA19h(bk);
   brightest(k,3) = RA19m(bk);
   brightest(k,4) = RA19s(bk);
   brightest(k,5) = DEC19sgn(bk);
   brightest(k,6) = DEC19d(bk);
   brightest(k,7) = DEC19m(bk);
   brightest(k,8) = DEC19s(bk);
   brightest(k,9) = RA20h(bk);
   brightest(k,10) = RA20m(bk);
   brightest(k,11) = RA20s(bk);
   brightest(k,12) = DEC20sgn(bk);
   brightest(k,13) = DEC20d(bk);
```

```
   brightest(k,14) = DEC20m(bk);
   brightest(k,15) = DEC20s(bk);
   brightest(k,16) = vMag(bk);
   brightest(k,17) = annMoRA(bk);
   brightest(k,18) = annMoDEC(bk);
   brightest(k,19) = parx(bk);
   ck = nearank(k,2); % select in order of closeness
   closest(k,1) = StarNo(ck);
   closest(k,2) = RA19h(ck);
   closest(k,3) = RA19m(ck);
   closest(k,4) = RA19s(ck);
   closest(k,5) = DEC19sgn(ck);
   closest(k,6) = DEC19d(ck);
   closest(k,7) = DEC19m(ck);
   closest(k,8) = DEC19s(ck);
   closest(k,9) = RA20h(ck);
   closest(k,10) = RA20m(ck);
   closest(k,11) = RA20s(ck);
   closest(k,12) = DEC20sgn(ck);
   closest(k,13) = DEC20d(ck);
   closest(k,14) = DEC20m(ck);
   closest(k,15) = DEC20s(ck);
   closest(k,16) = vMag(ck);
   closest(k,17) = annMoRA(ck);
   closest(k,18) = annMoDEC(ck);
   closest(k,19) = parx(ck);
end
```

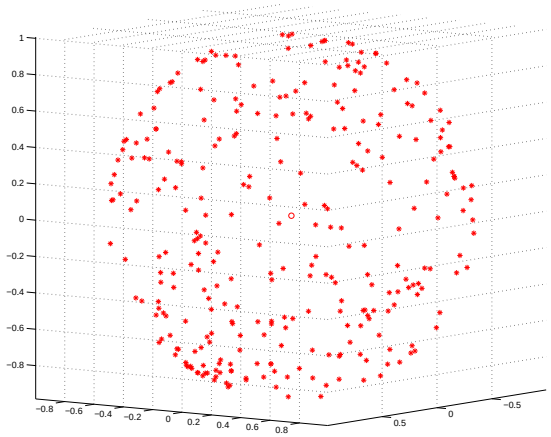
b) Write a MATLAB program to display stars represented in arrays such as `brightest` and `closest` in 3D. (Distance in light years is 3.26 times the distance in parsecs, and distance in parsecs is 1/parallax (sec).) (Use `quiver3()`, and note that the arguments `U, V` and `W` of `quiver3()` can in this case just be arrays of zeros. The seventh argument of `quiver3()` can be 0 and the eighth could be `'r*'` to show the stars as red asterisks.) How would you also display our Sun, in the middle of all these stars, as a red circle? Here are snapshots of the pictures you might get. First, the brightest 300 and the closest 300 stars. (The axis units are light years.)

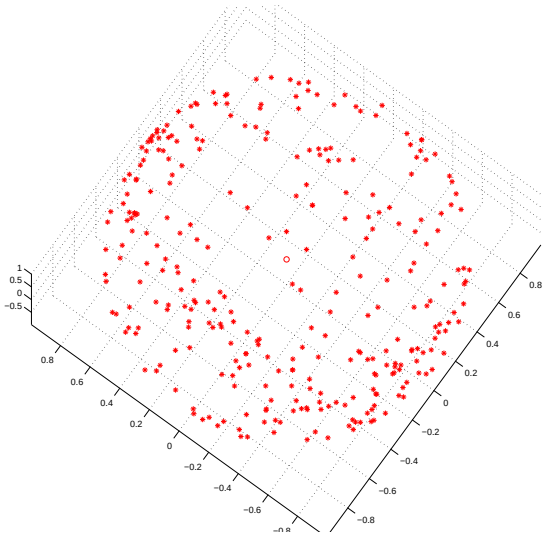


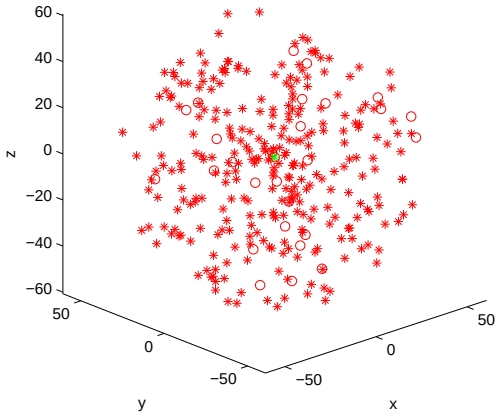



And here are three more snapshots. The first two are of the brightest 300 stars with distances all set to 1 light-year, so that we can see them as on a sphere—the "celestial sphere" seen from outside!. Can you make out the belt and sword of Orion, and the shape of the Little Dipper?

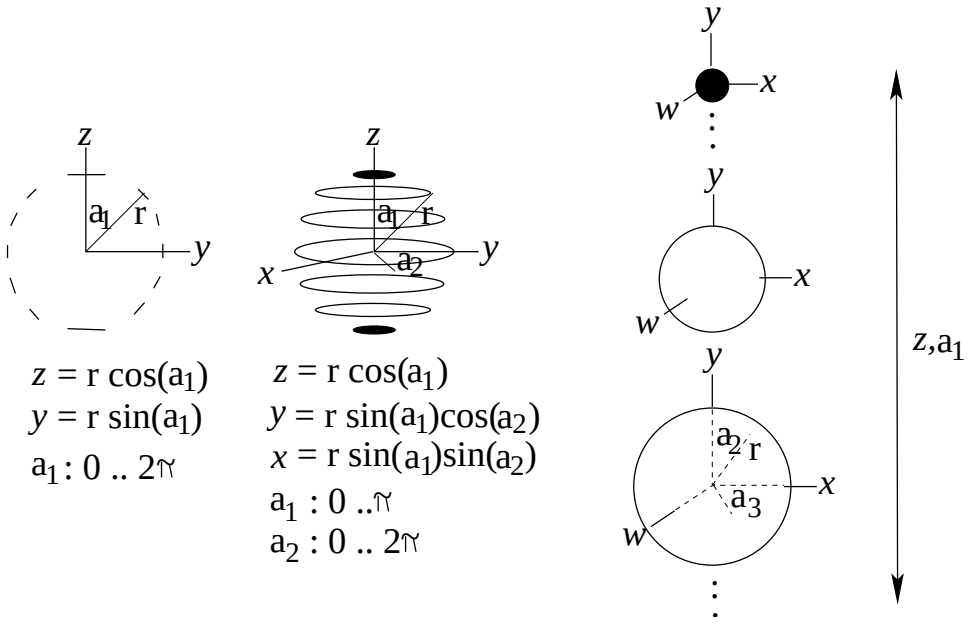
The third shows the 300 closest stars, augmented (red circles) by the closest 27 of the 168 stars so far known to have planets of their own. These stars are stored in the file /home/course/cs199/exoplanetStars, with entries for RA 2000 (starting at position 28), Dec 2000 (starting at position 44) and distance in parsecs (positions 76–80). If you write and run programs to select and display these together with the closest 300 stars, you can use MATLAB's Camera Toolbar to Orbit the camera and to move the camera Forward/Back for better views. How many of the 27 closest stars known to have "exoplanets" coincide with any of the 300 closest stars from the Bright Star Catalog? What is the probability that a star has observable planets (at least from this sample of closest stars)? Look up "exoplanets"!








16. **Hyperspheres**. If you are systematic, you can begin to think about coordinates for spheres in higher dimensions—*hyperspheres*. Note how a circle can be built up from point-pairs at an angle $a_1$ from the $z$-axis, with solid "caps" at top and bottom; how a sphere can be built up from circles at an angle $a_1$ from the $z$-axis, with solid "caps" at top and bottom; how a 4-dimensional hypersphere can be built up from spheres at an angle $a_1$ from the $z$-axis, with solid "caps" at top and bottom; etc.




a) Convince yourself that the general coordinates for a $d$-dimensional hypersphere are

$$\begin{aligned} z_1 &= r\cos(a_1) \\ z_2 &= r\sin(a_1)\cos(a_2) \\ z_3 &= r\sin(a_1)\sin(a_2)\cos(a_3) \end{aligned}$$

$$
\begin{aligned}
&\vdots \\
z_{d-1} &= r\sin(a_1)\sin(a_2)..\cos(a_{d-1}) \\
z_d &= r\sin(a_1)\sin(a_2)..\sin(a_{d-1})
\end{aligned}
$$

where all the angles range from 0 to $\pi$ except the last which is from 0 to $2\pi$.
b) Work out expressions for $r$ and the angles $a_i, i = 1..d-1$ supposing the Cartesian coordinates $z_1, .., z_d$ are given.

17. Look up Etienne Louis Malus, 1775-1812: why did he get interested in polarized light? what was then known about polarized light? what did he do in his career?

18. Look up "photometer" to see if you can devise the experiment needed to measure the light intensity as a top filter, $t$, is rotated above a bottom filter, $b$, or as a middle filter, $m$, is rotated between $t$ and $b$ placed at right angles to each other.

19. **Can quantum physics be made more complete?** Quantum physics says that light, which we have discussed as passing through polarizing filters, is made up of indivisible parts ("quanta") called *photons*. Thus it is not an issue of *some* of the light passing through a filter but rather of individual photons *somehow deciding* whether or not to pass through. We can ask if each photon possesses part of a set of "keys", one for each filter "gate" such that, if it has the key for a particular gate then it gets through, otherwise not. Quantum physics is not aware of any such keys, but they may be there, waiting for a more complete physics theory.
a) Consider three polarizing filters, $A$, $B$, $C$, as in Note 6, but angled $\pi/6$ to each other, with, say, $A$ oriented at 0 radians, $B$ at $\pi/6$ radians and $C$ at $\pi/3$. Starting with light that has passed through $A$, the proportion of this light that gets through $B$ is, by Malus' law, $\cos^2(\pi/6) = (\sqrt{3}/2)^2 = 3/4$, and the proportion that does not get through is $\sin^2(\pi/6) = 1/4$. For an individual photon, then, the *probability* that it gets through is $3/4$ and that it does not get through is $1/4$.
Similarly, if a photon has got through $B$, the probability that it then gets through $C$ is $3/4$ and that it does not get through is $1/4$.
If, on the other hand, we *removed* the middle filter, $B$, allowing a photon to proceed directly from $A$ to $C$, the probability that it then gets through $C$ is $\cos^2(\pi/3) = (1/2)^2 = 1/4$ and the probability that it does not get through is $3/4$.
Let's pull out of this math three probabilities, and consider the relationship among them. Let $A$, $B$ or $C$ stand for the photon getting through the corresponding filter and $A'$, $B'$ and $C'$ for the photon not getting through. If the letter does not appear, the filter is irrelevant or not there.

$$
\begin{aligned}
\text{prob}(AC') &= 3/4 \\
\text{prob}(AB') &= 1/4 \\
\text{prob}(BC') &= 1/4
\end{aligned}
$$

That's what quantum physics says.
b) Now consider a more complete theory in which the photons are given keys, or not, for each of the three filters. There are $2^3 = 8$ possibilities. If we have $N$ photons we can break them up into eight groups

$$N = N(ABC)+N(ABC')+N(AB'C)+N(AB'C')+N(A'BC)+N(A'BC')+N(A'B'C)+N(A'B'C')$$

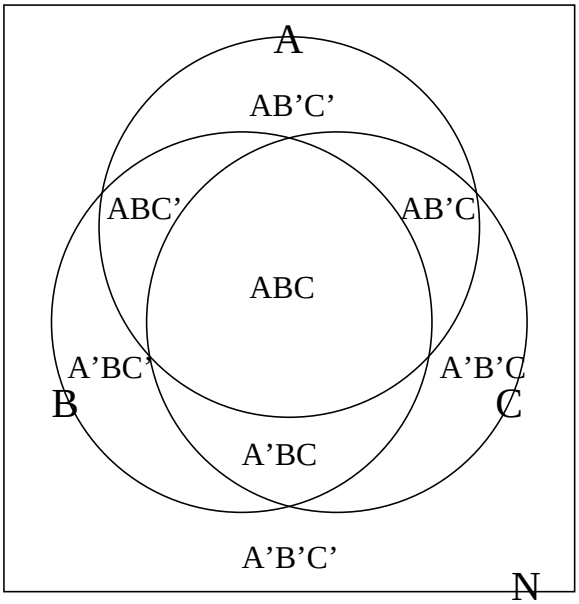
where $N(ABC)$ is the number of photons with keys for all three filters, $N(ABC')$ is the number of photons with keys for filters $A$ and $B$ but not $C$, and so on. The corresponding probabilities are $\text{prob}(ABC) = N(ABC)/N$, $\text{prob}(ABC') = N(ABC')/N$, and so on.
From the quantum theory of part (a) above, let's suppose we know $\text{prob}(AB')$ and $\text{prob}(BC')$. We can expand these in terms of the eight basic probabilities above by noting that, for instance, $C$ and $C'$ are disjoint sets, so $N(AB') = N(AB'C) + N(AB'C')$. Thus

$$\begin{aligned}
\text{prob}(AB') &= \text{prob}(AB'C) + \text{prob}(AB'C') \\
\text{prob}(BC') &= \text{prob}(ABC') + \text{prob}(A'BC') \\
\text{prob}(AC') &= \text{prob}(ABC') + \text{prob}(AB'C') \\
&= \text{prob}(BC') - \text{prob}(A'BC') + \text{prob}(AB') - \text{prob}(AB'C) \\
&\leq \text{prob}(BC') + \text{prob}(AB')
\end{aligned}$$

The third of these, $\text{prob}(AC')$, is the probability that photons getting through filter $A$ are stopped by filter $C$ with *no* filter $B$ in between. The inequality arises because no probability can be negative and we have subtracted two probabilities from $\text{prob}(AB') + \text{prob}(BC')$.
But the quantum theory violates this inequality.
c) The "complete" theory disagrees with the quantum theory. But all experiments performed so far agree with the quantum theory.
d) Unfortunately, the "complete" theory discussed here is a weak straw man. The major hole is that there might ba a connection between filters, say between $B$ and $C$, such as a key for $B$ also (sometimes) opening $C$. This can be circumvented by exploiting the second remarkable property of quantum physics, namely *quantum entanglement*, by means of which the two filters can operate on opposite parts of a quantum state combining two photons, and can be placed so far apart that they cannot communicate with each other unless the communication can travel faster than light—see Week 3,
All this was put together in a watertight way by John Stuart Bell in 1964: a "complete" theory without faster-than-light communication makes predictions (about inequalities) that have been falsified by experiment. Quantum theory wins. It cannot be made more "complete". We'll look at this in Book 11d.
The inequality in key theory (part (b)) is an example of a "Bell inequality"—or would be once entanglement is incorporated; the contradiction (part (c)) with quantum theory is an example of "Bell's theorem".
e) Play with the predictions of quantum theory for different angles between the filters. You will see that the relationship does not always disagree with the key theory. But the fact that it does *sometimes* is crucial.
You may want to do this by plotting

$$\begin{aligned}
\text{prob}(AC') - \text{prob}(AB') - \text{prob}(BC') &= \sin^2 AC - \sin^2 AB - \sin^2 BC \\
&= s_2^2 - 2s^2 \\
&= 1 - c_2^2 - 2(1 - c^2) \\
&= 1 - c_2^2 + 2c^2 - 2 \\
&= 1 - c_2^2 + c_2 - 1 \\
&= c_2 - c_2^2 \\
&= c_2(1 - c_2)
\end{aligned}$$

and assuming that the angle between $A$ and $B$ is $\theta$ and the same as the angle between $B$ and $C$, which is what allowed me to use $s = \sin\theta$ and $s_2 = \sin 2\theta$ in the second line above. The remaining lines above are just to facilitate using some advanced math ($c = \cos\theta$ and $c_2 = \cos 2\theta$) to help study the shape of the curve, but you can use a calculator to plot it to the same end.
Does $\theta = \pi/8$ also contradict the key theory? See [RS17]. What about $\theta = \pi/3$? What about the example of Note 6 where $\theta = \pi/4$?
f) Here is a "Venn diagram" showing the eight regions $ABC$, $ABC'$, etc and indicating the number $N$ of all photons. Change the circles to illustrate the probabilities for $\theta = \pi/4$. What about $\theta = \pi/3$?




20. **Quantum key distribution.** Polarized photons can be used to guarantee secure communication. Suppose Adams wants to send to Bell the 1-byte message "42" (00101010 in binary) ("The Ultimate Answer to Life, the Universe and Everything is...42!": Douglas Adams) without anyone else able to intercept it (although Bell could at her discretion forward it to Copernicus, Dirac, Einstein, Feynman, Gauss and so on).
To do this, Adams must generate a *key*, communicate it to Bell, and then use it to *encrypt* the message, which Bell will *decrypt* using the same key. We'll first discuss generating and communicating the key, then how it might be used to encrypt and decrypt.
Adams can send photons to Bell and they both have two sets of polarizers:
set 0 represents 0 as horizontal polarization and 1 as vertical;
set 1 represents 0 as 45-degree polarization and 1 as 135-degree.
a) Adams first generates a random string of 0s and 1s four times as long as the message.

```
p4 = floor(rand(1,4*8)+0.5)
0 0 1 0 1 0 0 0 0 1 0 1 0 0 1 0 1 1 0 1 1 0 0 1 0 1 0 0 1 1 0 1
```

For each "bit" in this string, Adams will select one of the sets at random to polarize a photon before sending, and Bell will also select one of the two sets at random to detect it on receipt. They have a 50% chance of selecting the same set (either both set 0 or both set 1) and agreeing on the bit represented by that photon. If they select different sets, Bell will have equal probabilities of seeing a 0 or a 1 if Adam sent a

photon representing, say, 1: $\cos^2\pi/4 = 1/2 = \sin^2\pi/4$.
So Adams generates another random string, the same length as the first, where now 0 represents polarizer set 0 and 1 represents polarizer set 1:

```
codeA = floor(rand(1,4*8)+0.5)
0 0 0 0 0 1 0 0 1 0 1 1 0 0 1 1 0 0 1 0 1 1 1 0 1 0 1 1 0 1 0 1
```

Meanwhile Bell does the same for her polarizer sets:

```
codeB = floor(rand(1,4*8)+0.5)
1 1 0 1 1 0 0 1 0 1 1 0 1 0 1 1 1 1 1 1 1 1 1 0 1 1 1 0 1 0 1 0
```

Now Adam uses `codeA` to transmit `p4` to Bell, which Bell interprets using `codeB`. Bell should get about half of the bits of `p4` right, as we said above, but *which* bits? Adam and Bell can find out where their coding systems agree, `codeA==codeB`, by sharing them via a second channel which can be classical.
(So the whole scheme has two channels, a quantum (photon) channel which is one-way from Adams to Bell, and a regular, two-way channel which is not necessarily secure.)

```
AeqB = codeA==codeB
0 0 1 0 0 0 1 0 0 0 1 0 0 1 1 1 0 0 1 0 1 1 1 1 1 0 1 0 0 0 0 0
```

Now the whole point is that this insecure communication happens *after* the crucial `p4` has been transmitted optically, so that any eavesdropper trying to listen in cannot go back and use it to interpret the photons the way Bob did. And a "no-cloning" theorem states that it is impossible for the eavesdropper to make a copy, at the time, of the quantum states of those photons so as to check up on them later. We'll come back to the eavesdropper shortly. For now we continue to suppose Adams and Bell are communicating wit no eavesdropper.
So, using `AeqB`, Bell determines which half of the bits she has correctly interpreted. In this example there are 13 (of 32):
(Code to extract bits of `p4`, and their positions, for which `AeqB`.)

```
? ? 1 ? ? ? 0 ? ? ? 0 ? ? 0 1 0 ? ? 0 ? 1 0 0 1 0 ? 0 ? ? ? ? ?
```

Of these 13 bits, about half—well, here, 8 to be exact—will be needed for the key to encode the intended message "42". So 5 of the 13 can be used to check if there has been an eavesdropper. Bell uses the classical channel to send a random five of them to Adam.

```
xpose = floor(rand(1,5)*13+0.5)
 5 9 11 10 0
```

(Well, I was lucky; they're all different: this was not very good programming.)
Here is Adam's confirmation that all five are correct and there has been no interference:

```
- - y - - - - - - - - - - - - - y - - - - - - y y y - - - - - - -
```

So now Adams can use the remaining eight bits to encrypt the message. A way to do this is by addition modulo 2 (which is the same as the exclusive-or operator `XOR`) applied to each corresponding pair of bits:

```
(0 0 1 0 1 0 1 0) XOR (0 0 0 1 0 1 0 0) = (0 0 1 1 1 1 1 0)
```

And the neat thing is that Bell can decrypt it by the same operation:

```
(0 0 1 1 1 1 1 0) XOR (0 0 0 1 0 1 0 0) = (0 0 1 0 1 0 1 0)
```

Why did the initial `p4` need to be 4 times the length of the key ("one-time pad") finally used?
Why must this one-time pad never be re-used for a later message?
b) Now let's repeat the whole operation in (a) but with an eavesdropper, Eve.
Adams generates `p4` and `codeA` as before. But now Eve generates her own `codeE`:

```
codeE = floor(rand(1,4*8)+0.5)
1 1 1 0 0 0 1 0 0 1 0 0 0 0 0 1 1 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0
```

Eve interprets Adams' `p4` bits according to `codeE` and immediately relays them to Bell but encoded with her own `codeE`. Eve then intercepts Adam's (non-quantum) message to Bell and can compare coding systems:

```
AeqE = codeA==codeE
0 0 0 1 1 0 0 1 0 0 0 0 1 1 0 1 0 1 0 1 1 0 0 1 0 0 0 0 1 0 1 0
```

This tells Eve that she received 12 bits correctly from Adams:

```
? ? ? 0 1 ? ? 0 ? ? ? ? 0 0 ? 0 ? 1 ? 1 1 ? ? 1 ? ? ? ? 1 ? 0 ?
```

Meanwhile, Bell has generated `codeB` as before, and tested `AeqB = codeA==codeB`, going on as before to think she has received 13 bits of `p4`, where `AeqB`, except that 10 of them have been garbled by Eve:

```
? ? ! ? ? ? ! ? ? ? ! ? ? ! ! 0 ? ? ! ? 1 ! ! 1 ! ? ! ? ? ? ? ?
```

Then Bell and Adams do the eavesdropper test by `xpose`ing 5 bits as before:

```
- - ? - - - - - - - - - - - - - y - - - - - - ? y ? - - - - - - -
```

where about half of the `?` will *not* be OK, revealing to Adams and Bell that there has been an eavesdropper, and warning them off using the remaining 8 bits as a key for the message, and so alerting Adams not to send the message, at least through *this* channel.

c) The above protocol ("BB84" for Bennett and Brassard in 1984) repeatedly generates random numbers between 0 and 1. All classical random number generators, including MATLAB's `rand()`, have regularities that prevent the results from being truly random. How can we use quantum physics to generate truly random numbers?

21. Look up Karl Popper's "The Logic of Scientific Discovery": is there a summary on the Web? What is "the logic of scientific discovery"? How can the statement "The sun rises every morning" be proved? Disproved? How does science differ from technology, mathematics or philosophy?

22. Wolfgang Pauli (1900–1958) was known to have dismissed poor work by saying "It is not even wrong". Comment, in the light of Popper's characterization of science as falsification.

23. Why is astrology not a science? What change in approach might make astrology scientific?

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

# References


[RS17] Henry Reich and Grant Sanderson. Bell's theorem: The quantum Venn diagram paradox. minutePhysics and 3Blue1Brown URL https://www.youtube.com/watch?v=zcqZHYo7ONs..[incomplete] last accessed 18/7/8, Sept. 2017.