Projects Offered by Robin Chapman

These are brief descriptions of the projects I'm officially offering for 2006–2007. If you're interested please email me. I'm also willing to offer other topics in most branches of mathematics, especially in number theory, algebra, combinatorics, geometry and topology. If there's any aspect of your courses so far that you'd like to continue in a project, please let me know. I give a list of possible alternative titles (not exhaustive!) at the end.

Level 3 projects

Generating functions Generating functions are a method used for solving recurrence relations and in combinatorial problems. For instance consider the recurrence for the sequence $a_0, a_1, a_2, \ldots$ given by

$$a_n = \begin{cases} 0 & \text{if } n = 0, \\ 2a_{n-1} + 1 & \text{if } n = 1, 2, 3, \ldots. \end{cases} \qquad (*)$$

To solve this recurrence we introduce the *generating function* for the sequence:

$$A(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n + \cdots = \sum_{n=0}^{\infty} a_n X^n.$$

Using the recurrence $(*)$ we get

$$\begin{aligned} A(X) &= 0 + (2a_0 + 1)X + (2a_1 + 1)X^2 + (2a_2 + 1)X^3 + \cdots \\ &= 2(a_0 X + a_1 X^2 + a_2 X^3 + \cdots) + (X + X^2 + X^3 + \cdots) \\ &= 2XA(X) + \frac{X}{1 - X} \end{aligned}$$

which solves to give

$$A(X) = \frac{X}{(1 - X)(1 - 2X)}.$$

Expanding in partial fractions gives

$$\begin{aligned} A(X) &= \frac{1}{1 - 2X} - \frac{1}{1 - X} \\ &= (1 + 2X + 2^2 X^2 + \cdots + 2^n X^n + \cdots) \\ &\quad -(1 + X + X^2 + \cdots + X^n + \cdots) \\ &= 0 + (2 - 1)X + (2^2 - 1)X^2 + \cdots + (2^n - 1)X^n + \cdots \end{aligned}$$

and we get the formula $a_n = 2^n - 1$.

Generating functions are also used in a variety of combinatorial problems, for instance counting partitions, derangements and other types of permutation.

Reading: Wilf, *generatingfunctionology*,
`http://www.math.upenn.edu/~wilf/DownldGF.html`

Quaternions Quaternions are "hypercomplex" numbers of the form $t+xi+yj+zk$ where t, x, y and z are real. The "numbers" i, j and k satisfy $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. The quaternions form a noncommutative division ring.

Quaternions have applications in geometry: they can be used to model rotating coordinate frames. They are used in computer graphics, in particular the Tomb Raider games. Quaternions are also used in number theory: they can be used to prove that each positive integer is the sum of at most four squares.

Reading:
`http://pages.cpsc.ucalgary.ca/~mario/587/2-orientation/papers/quaternions_01.pdf`

Fourier Series and Transforms Fourier series and their generalizations Fourier transforms are ubiquitous in mathematics and its applications. The Fourier series of a function f on say $[0, 2\pi]$ has coefficients

$$c_n = \frac{1}{2\pi} \int_0^{2\pi} f(t) e^{-int}\, dt$$

and we expect that

$$f(x) = \sum_{n=-\infty}^{\infty} c_n e^{inx}.$$

However this series may not even converge, and even when it does it may converge maddeningly slowly (even for familiar functions like $f(x) = x$.) The Fourier transform of a function g on $\mathbf{R}$ is defined by

$$\hat{g}(t) = \int_{-\infty}^{\infty} g(x) e^{-itx}\, dx$$

(if this makes sense!), and if f is nice enough then

$$g(x) = \int_{-\infty}^{\infty} \hat{g}(t) e^{itx}\, dt.$$

The many applications of Fourier series and transforms include differential equations (the heat equation), probability theory (the central limit theorem) and number theory (primes in arithmetic progressions).

Reading: Körner, *Fourier Analysis* & *Exercises in Fourier Analysis*.

Design theory A design is a type of finite "geometry". For instance suppose we have a "plane" with seven points A, B, C, D, E, F and G and we have seven "lines" each containing three points namely:

$$\begin{aligned} L_1 &= \{A, B, D\} \\ L_2 &= \{B, C, E\} \\ L_3 &= \{C, D, F\} \\ L_4 &= \{D, E, G\} \\ L_5 &= \{A, E, F\} \\ L_6 &= \{B, F, G\} \\ L_7 &= \{A, C, G\}. \end{aligned}$$

The we can check that, as in familiar Euclidean geometry, every pair of distinct points is contained in exactly one line. (Exercise: find a similar "geometry" with 9 points and 12 lines with 3 points on each line. This is one of the basic examples of a design. In general a design with parameters v, k t and λ (or a t-(v, k, λ) design) is a set $\mathcal{P} = \{P_1, P_2, \ldots, P_v\}$ of v "points" and a set $\mathcal{B}$ of "blocks" (instead of lines); each block being a k-element subset of $\mathcal{P}$. These have to satisfy the condition that every t-element subset of $\mathcal{P}$ is contained in exactly λ blocks. Hence our example of a finite geometry is a 2-(7,3,1) design (and the exercise is to find a 2-(9,3,1) design).

There are many ways of constructing designs, and designs are used in group theory, in the construction of error-correcting codes and in the design of experiments.

Reading: Anderson, *A First Course in Combinatorial Mathematics*; Hughes & Piper, *Design Theory*.

Sphere packings Given a large box and a lot of small spheres of equal size (say ball-bearings or marbles) how can we fit as many in the box as possible? This is a pretty hard problem in general so mathematicians simplify by asking instead how densely can we pack spheres in all of 3-dimensional space. As a start we can fill a layer with spheres by putting 6 spheres about a given one in a hexagonal arrangement and filling the plane by building up larger and larger hexagons. Then we build a lot of similar layers and stack them up as snugly as possible. By doing this we fill a proportion of $\pi/\sqrt{18} = 0 \cdot 740 \cdots$ of space. It is conjectured (but not proved) that this is the best possible. If we restrict to a certain class of regular packings called lattice packings then it is the best. We can also consider the problem of packing n-dimensional hyperspheres in n-dimensional space. In particular there are some exceptionally dense packings in 8 and 24-dimensional spaces called the E_8 lattice and the Leech lattice.

Reading: Sloane, 'The packing of spheres', in *Scientific American*, vol. 250, no. 1, pp. 116–125, 1984; Conway & Sloane, *Sphere Packings, Lattices and Groups* (in particular chapter 1).

Level 4 projects

Quaternary Codes In coding theory one mainly studies binary codes where one takes the alphabet as $Z_2 = \{0, 1\}$. It is convenient to study codes over Z_p for p prime at the same time, as much of their theory is the same. It is also convenient to study linear codes. However there are some important nonlinear codes over Z_2 such as the Nordstrom-Robinson, Kerdock and Preparata codes which are for their parameters more efficient than any linear codes. Also these codes have weight enumerators similar to binary codes: they satisfy the MacWilliams identities.

In the 1990s this phenomenon was explained. Researchers studied linear quaternary codes. These are codes over Z_4, which is not a field. One can translate from quaternary codes of length n to binary codes of length $2n$. The nonlinear binary codes mentioned above all come from linear quaternary codes, and in this way the MacWilliams identities were explained.

Reading: Wan *Quaternary codes.*

The Distribution of Prime Numbers How many prime numbers are there? Obviously the answer is infinitely many, but how are they distributed? If we look at a table of prime numbers they obviously thin out, but at what rate. To study this problem we let $\pi(x)$ denote the number of primes up to the number x. While there is no simple formula for $\pi(x)$, the crucial result is that $\pi(x)$ is approximately equal (is asymptotic to) the function $x/\log x$ for large x. This is the celebrated Prime Number Theorem.

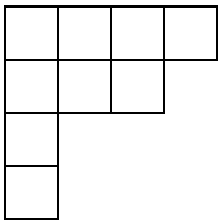
More generally we can study primes having other properties. Examining table of prime numbers we see that there seem to be roughly as many primes ending in 1 as there are ending in 3, or in 7 or in 9. In fact there are infinitely many primes ending in each of these digits, and these four classes are "equidistributed" in an appropriate sense. This is a particular case of Dirichlet's Theorem on primes in arithmetic progressions.

The easiest proofs of these results involve complex analysis, involving functions such as the Riemann ζ-function is defined by

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots.$$

Reading: Serre, *A Course in Arithmetic*, Jameson, *The Prime Number Theorem.*

Young Tableaux A Young diagram is an array of boxes like:



If we have a Young diagram with n boxes, then a standard Young tableau is a way of writing in the numbers 1 to n in the boxes so that each row and column is increasing, for instance:

1	3	4	7
2	6	9	
5			
8			

One basic question we might ask is how many standard Young tableaux are there on a given Young diagram. The answer is given by the remarkable Hook Length Formula. One can then study more general tableaux. For instance in a semistandard Young tableau we can use any numbers, more than once if we like, but have the rows weakly increasing and the columns strictly increasing, for instance:

1	1	3	3
2	3	5	
4			
7			

Young tableaux have surprising applications in group theory.

Reading: Fulton, *Young Tableaux*, Stanley, *Enumerative Combinatorics 2*.

Elliptic Functions and Curves The exponential function $z \mapsto e^z$ is periodic: $e^{z+2\pi i} = e^z$. Elliptic function are meromorphic complex functions which are periodic in two independent ways: they satisfy $f(z+a) = f(z) = f(z+b)$

for two constants a and b with nonreal ratio. The Weierstrass $\wp$-function defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{m,n} \left(\frac{1}{(z - ma - nb)^2} - \frac{1}{(ma + nb)^2} \right)$$

is an elliptic function (the summation is over all pairs (m, n) of integers apart from $(0, 0)$).

The $\wp$-function satisfies a differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

This is related to the equation

$$y^2 = 4x^3 - g_2x - g_3.$$

This latter equation defines a curve in the plane — an elliptic curve. Thus elliptic curves are parametrized by elliptic functions. Elliptic functions and curves have a wide array of applications, from physics to number theory. For instance Wiles's proof of Fermat's Last Theorem relies on deep properties of elliptic curves.

Reading: McKean and Moll, *Elliptic Curves*.

The Golay codes and the Mathieu groups The Golay codes are certain error-correcting codes. The codes defined by Golay are $\mathcal{G}_{23}$ which is a perfect $[23, 12, 7]$-linear code over Z_2 and $\mathcal{G}_{11}$ which is a perfect $[11, 6, 5]$-linear code over Z_3. Apart from the Hamming codes they are the only nontrivial perfect error-correcting codes. In practice it is more convenient to study the extended Golay codes; these are $\mathcal{G}_{24}$ which is a $[24, 12, 8]$-linear code over Z_2 and $\mathcal{G}_{12}$ which is a $[12, 6, 6]$-linear code over Z_3.

The Golay codes are very symmetric. Their symmetry groups are the Mathieu groups which are of central importance in the theory of finite groups.

Reading: Conway & Sloane, *Sphere Packings, Lattices and Groups*.

Other possible titles:

- Finite sets (combinatorics)
- Ordered sets and lattices (combinatorics, algebra)
- Algorithms in number theory (number theory)
- Character sums (number theory)
- p-adic numbers (number theory)
- Algebraic numbers (number theory)
- The classical groups (algebra)
- Categories and functors (algebra, topology)
- Differential geometry (geometry)
- Projective geometry (geometry)
- Geometry of triangles (geometry)
- Tilings (geometry)
- Regular polyhedra and polytopes (geometry)
- Generalized functions (analysis)
- Wavelets (analysis)
- The fundamental group (topology)
- The Brouwer fixed point theorem (topology)
- Recursive functions and computability (logic)

and many others!

RJC, March 2006