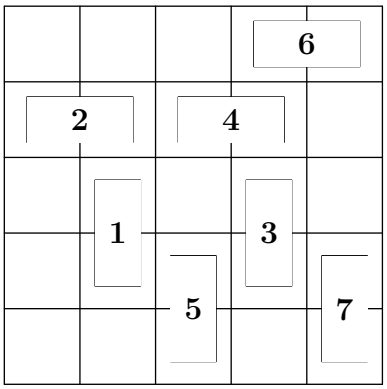
PROJECT IDEAS

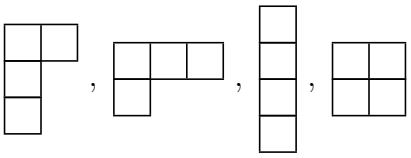
MARK WILDON

I am happy to supervise projects in any area of combinatorics or algebra. Here are some ideas. Most have already been successful projects for at least one student, and could be used as either a 3rd year, 4th year or M.Sc. project. You can read this document online `http://www.ma.rhul.ac.uk/~uvah099/teaching.html`.

Combinatorial game theory. In the game of *Domineering* the two players are called Horizontal and Vertical. In each turn, Vertical places a domino vertically on the board, and then Horizontal places a domino horizontally on the board. The first player who is unable to move loses. For example, the diagram below shows a position with Horizontal to play.



The aim of a project in this area would be to explain the remarkable connection between numbers and games that makes it possible to assign numerical values to Domineering positions, and so to decide optimal moves in even quite complicated positions. For example, of the boards



the first three have values $1/2$, $-1/2$ and 2 respectively. The fourth has a value $\star$ that lies outside the real number system. The theory can also be applied to many other games, including Nim, Dots-and-Boxes and *go*; any of these games could be used as an example in a project. For an undergraduate level introduction see [2].

Date: February 13, 2020

`mark.wildon@rhul.ac.uk`.

Poker. It is possible to use game theory to give a complete analysis of some simplified poker games. For instance, in the AKQ-game, a pack consisting of the ace, king and queen of spades is shuffled, and each player is given one card. After a round of betting either one player folds, or there is a showdown and the player with the higher card wins. The optimal strategy for this game shows many techniques used by good poker players in real games, for example, bluffing on weak hands, and slow-playing on strong hands.

The aim of a project in this area could to give a mathematical analysis of the AKQ-game or a more complicated variant. Alternatively, or in addition, some of the literature on five-card draw could be surveyed: see for example [33]. I can supply some computer code that can simulate different strategies in the AKQ-game and five-card draw and related games.

See [12] for an introduction to this area (written more for poker-players than for mathematicians).

Derangements. Let σ be a permutation of the set $\{1, 2, \ldots, n\}$, i.e. σ is a bijective function from $\{1, 2, ..., n\}$ to itself. A *fixed point* of σ is an element $k \in \{1, 2, \ldots, n\}$ such that $\sigma(k) = k$. A permutation is said to be a *derangement* if it has no fixed points. Let $r_n(k)$ be the number of permutations of $\{1, 2, \ldots, n\}$ with exactly k fixed points and let $d_n = r_n(0)$.

There are a number of interesting combinatorial bijections involving derangements. For example, Wilf [32] gives a bijective proof that

$$r_n(0) - r_n(1) = (-1)^n.$$

Remmel [28] gives a bijective proof that

$$dn = nd_{n-1} + (-1)^n.$$

A more recent paper by Diaconis, Fulman, Guralnick [18] proves a number of statistical results on the numbers $r_n(k)$. For many more open problems on derangements, see Peter Cameron's notes: `www.maths.qmul.ac.uk/~pjc/slides/beamer/triangle1.pdf`.

Stirling numbers. Given n, $k \in \mathbf{N}_0$, the Stirling number of the second kind $\left\{ {n \atop k} \right\}$ is defined to be the number of set partitions of $\{1, 2, \ldots, n\}$ into k non-empty subsets. For example, $\big\{\{1, 4\}, \{2\}, \{3, 5, 6\}\big\}$ is one of the set partitions contributing to $\left\{ {6 \atop 3} \right\}$.

The aim of this project would be to explore some of the many different settings in which Stirling numbers appear, some of the many

combinatorial identities they satisfy, and to say something about their asymptotic behaviour for large n and k. See [20, §6.1] for an introduction to the subject and further examples.

Estimates for the number of partitions of n. A partition of a natural number is a way to write that number as a sum of smaller numbers. For example there are five partitions of 4, namely 4 itself, 3+1, 2+2, 2+1+1 and 1+1+1+1. In 1918, G. H. Hardy and S. Ramanujan [22] proved an amazing asymptotic formula for the number of partitions of n. The early sections of their paper give some easier combinatorial argument that it would be interested to survey. A later paper by Erdös [19] gives some other nice elementary arguments. (Here 'elementary' means not using complex analysis: some real analysis will be required!)

The RSK-correspondence. If m, $n \in \mathbf{N}$, then any sequence of $mn+1$ distinct real numbers has either an increasing subsequence of length $m+1$, or a decreasing subsequence of length $n+1$. One proof of this fact uses the RSK-correspondence.

The RSK-correspondence is a bijective map between permutations of $\{1, 2, \ldots, n\}$ and pairs of tableaux of the type shown below. For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 3 & 4 & 2 \end{pmatrix} \longleftrightarrow \left(\begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 4 \\ \hline 6 \\ \cline{1-1} \end{array} \, , \, \begin{array}{|c|c|c|} \hline 1 & 2 & 4 \\ \hline 3 & 6 \\ \cline{1-2} 5 \\ \cline{1-1} \end{array} \right).$$

A possible project in this area would explain how the correspondence works, prove some its (quite remarkable) combinatorial properties (this could lead to Knuth's relations on words and/or shadow diagrams), and give some applications, such as the finite Bolzano–Weierstrass theorem mentioned earlier or the Cauchy–Frobenius identity in symmetric polynomials. See [11, Chapter 13] for an introduction to the RSK-correspondence.

Card shuffling. Suppose that we shuffle a pack of n cards by choosing uniformly at random two numbers from 1 up to n. If the numbers are the same, we do nothing; otherwise we swap the cards in the indicated positions. This is not a particularly efficient shuffle, so it is perhaps surprising that after a bit more than $\frac{1}{2}n \log n$ shuffles, it is very likely than the pack will be well-mixed.

The first aim of a project in this area would be to understand the definition and properties of *total variation distance*, which gives a way

to measure how well a shuffle mixes a pack. Then it should try to explain the sharp 'cut-off' phenomenon: that the amount of mixing after k shuffles is low until k is near to $\frac{1}{2}n \log n$, at which point it rapidly increases so that the shuffle becomes indistinguishable from a random permutation.

A mixture of probabilistic and algebraic arguments will be required, and it is likely that this project would be found quite demanding. Diaconis' book [17] is an excellent source. See Chapter 28 of [1] for an introduction.

Hook Formula. The Hook Formula is a remarkable combinatorial formula for the number of standard tableaux of a given shape. For instance, there are 5 standard $(3, 2)$-tableaux, as shown below:

$$\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4&5\\\cline{1-2}\end{array}\,,\quad \begin{array}{|c|c|c|}\hline 1&2&4\\\hline 3&5\\\cline{1-2}\end{array}\,,\quad \begin{array}{|c|c|c|}\hline 1&2&5\\\hline 3&4\\\cline{1-2}\end{array}\,,\quad \begin{array}{|c|c|c|}\hline 1&3&4\\\hline 2&5\\\cline{1-2}\end{array}\,,\quad \begin{array}{|c|c|c|}\hline 1&3&5\\\hline 2&4\\\cline{1-2}\end{array}\,.$$

A project in this area might survey some of the different ways to prove the formula (suitable proofs include those by Greene–Nijenhuis–Wilf [21], Bandlow [3] and Novelli–Pak–Stoyanovskii [25]) and look at applications to enumerative combinatorics. For example, the formula for the Catalan Numbers $C_n = \frac{1}{n+1}\binom{2n}{n}$ follows from the Hook Formula for tableaux of shape (n, n).

Knights and spies. In a room there are 100 people, numbered from 1 to 100. A person is either a knight or a spy. Knights always tell the truth, but spies may tell the truth or lie as they see fit. Every person in the room knows the identity of everyone else. It is given that strictly more knights than spies are present.

Asking only questions of the form

'Person i, what is the identity of person j?',

what is the minimum number of questions which will guarantee to find everyone's true identity?

The aim of a project in this area would be to survey the literature on this and related problems, and maybe consider applications to social networks or look at some related unsolved problems. See [6], [31] and the references in [10] for an introduction.

Secret-sharing schemes. Suppose we want any three of five people to be able to decode a message encoded using a key k. Any two of them working together should not be able to learn anything. This can be achieved by splitting k into five shares, using ideas from coding theory.

The original scheme, due to Shamir [29], and lectured in the MT5462 Cipher Systems course, uses polynomial interpolation. It is related to the Reed–Solomon codes studied in MT5461 Error Correcting Codes. Other schemes are due to Brickell [8] and [5]. See [26] for a recent result that leads to a new coding theory bound. A useful survey article is [30]. The recent book [14] gives a formal computational framework and goes into a lot of detail on the algebra of secret sharing.

You could concentrate on the algebra and combinatorics, or go more into the cryptography by considering what happens when people start cheating. For instance, the people could be cloud computing providers, and cheating could mean that one or more lies (deliberately or accidentally) about their share.

Other ideas. Here are some brief ideas for other possible projects (not yet taken by a student). Please see me for more details.

- **Do bookmakers profit from the wisdom of crowds?** The book [23] could be a useful source for several different projects with a practical slant.
- **Hall's Marriage Theorem and related results**: there is a circle of interesting combinatorial theorems all of which can be used to prove one another: Hall's Marriage Theorem, König's Lemma, the Maxflow-mincut Theorem, Gale–Ryser Theorem, ... The aim of this project would be to prove one of these theorems, and explore the circle of implications and some applications of the theorems.
- **Cop and robber games**: graph searching problems. There is a recent book by Bonato and Nowakowski [7] that is a good introduction. A related search game was the subject of a popular question on a stackexchange cite: see `https://tinyurl.com/yx9q8vyq`; see [9] for some further results.
- **Weighing pennies**: given 12 pennies, one of which *might* be counterfeit have a different weight to the others, how many weighings does it take to locate the counterfeit penny and determine whether it is light or heavy, or be sure that all the coins are genuine? This problem has a close connection with coding

theory and has a non-adaptive optimal solution (i.e. the weighings can be specified in advance). A project could survey work on this problem and its many generalizations, for example: multiple counterfeit coins, restrictions on how many coins can be placed on the balance, adaptive versus non-adaptive solutions.

- **How to find and decode asymptotically good binary codes.** Very roughly, this project would be about binary codes of long length that have high rate and high minimum distance. The Gilbert–Varshamov bound shows that such codes must exist, but it doesn't give any effective way to find them. Try searching for 'concatenated codes', 'Expander codes', and 'LDPC codes' to see some modern constructions and decoders.

  One possible aim of a project in this area would be to understand the definition of (bipartite) expander graphs and the probabilistic proof that they exist. It should then explain how bipartite graphs can be used to define asymptotically good codes. There are now some notes appearing on the web aimed at advanced undergraduates. See `http://www.cs.washington.edu/education/courses/cse533/06au/lecnotes/lecture13.pdf` for an introduction. It might be very interesting to do some simulations of encoding and decoding for a randomly constructed expander code. Some programming would be required.

- **Counting combinatorial objects using sign-reversing involutions.** A typical example is the 'Matrix Tree Theorem' which expresses the number of spanning trees in a graph as a determinant. In particular, this theorem implies that there are n^{n-2} distinct trees on the vertex set $\{1, 2, \ldots, n\}$. There is a very nice introductory paper [4]. This could also form part of a project on symmetric polynomials: the final chapter of [24] gives a very nice account of some arguments that until recently were only available in the research literature. The article [27] has some nice bijective and involutive proofs.

- **Ramsey Theory, builder–painter games**. See [13] for a recent paper with some new results and background references. (If this area sounds interesting you should certainly also talk to Dr Gerke.)

- **Binomial identities**. Very rich and can be very deep. Gould's tables, Knuth convolution polynomials, Wilf–Zeilberger method ...

- **Voting theory**. One basic result is Arrow's Theorem: subject to some apparently reasonable axioms characteristing fairness, the only fair voting system for an election with three or more candidates is a dictatorship! That is, there is a single elector whose preferences are the only ones that matter. There are also connections with the representation theory of the symmetric group (my main research area): see [16] or [15] for an introduction.

References

[1] Aigner, M., and Ziegler, G. M. *Proofs from THE BOOK*, 3rd ed. Springer, 2010.

[2] Albert, M. H., Nowakowski, R. J., and Wolfe, D. *Lessons in play: An introduction combinatorial game theory*. A K Peters, 2007.

[3] Bandlow, J. An elementary proof of the hook formula. *Electron. J. Combin. 15*, 1 (2008), Research paper 45, 14.

[4] Benjamin, A. T., and Cameron, N. T. Counting on determinants. *Amer. Math. Monthly 112*, 6 (2005), 481–492.

[5] Blakley, G. R. Safeguarding cryptographic keys. In *AFIPS Conference Proceedings* (1979), vol. 48, pp. 313–317.

[6] Blecher, P. M. On a logical problem. *Discrete Math. 43*, 1 (1983), 107–110.

[7] Bonato, A., and Nowakowski, R. J. *The Game of Cops of Robbers on Graphs*. American Mathematical Society, 2011.

[8] Brickell, E. F. Some ideal secret sharing schemes. In *Advances in cryptology—EUROCRYPT '89 (Houthalen, 1989)* (1990), vol. 434 of *Lecture Notes in Comput. Sci.*, Springer, Berlin, pp. 468–475.

[9] Britnell, J. R., and Wildon, M. Finding a princess in a palace: a pursuit-evasion problem. *Elec. J. Combinat. 20* (2013), #25.

[10] Britnell, J. R., and Wildon, M. The majority game with an arbitrary majority. *Disc. Appl. Math 208* (2016), 1–6.

[11] Cameron, P. J. *Combinatorics: Topics, Techniques, Algorithms*. CUP, 1994.

[12] Chen, B., and Ankenman, J. *The Mathematics of Poker*. ConJelCo LLC, 2006.

[13] Conlon, D., Fox, J., and Sudakov, B. Essays in extremal combinatorics. *arXiv:1212.1300,* `http://arxiv.org/abs/1212.1300`.

[14] Cramer, R., Damgård, I. B., and Nielsen, J. B. *Secure multiparty secret sharing*. Cambridge University Press, 2015.

[15] Crisman, K.-D., and Orrison, M. E. Representation theory of the symmetric group in voting theory and game theory. In *Algebraic and geometric methods in discrete mathematics*, vol. 685 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 2017, pp. 97–115.

[16] Daugherty, Z., Eustis, A. K., Minton, G., and Orrison, M. E. Voting, the symmetric group, and representation theory. *Amer. Math. Monthly 116*, 8 (2009), 667–687.

[17] Diaconis, P. *Group Representations in Probability and Statistics*, vol. 11 of *Lecture Notes — Monograph Series*. Institute of Mathematical Statistics, 1988.

[18] Diaconis, P., Fulman, J., and Guralnick, R. On fixed points of permutations. *J. Algebraic Combin. 28*, 1 (2008), 189–218.

[19] Erdős, P. On an elementary proof of some asymptotic formulas in the theory of partitions. *Ann. of Math. (2) 43* (1942), 437–450.

[20] Graham, R. L., Knuth, D. E., and Patashnik, O. *Concrete Mathematics*. Addison Wesley, 1994.

[21] Greene, C., Nijenhuis, A., and Wilf, H. A probabilistic proof of a formula for the number of Young tableaux of a given shape. *Adv. Math. 31* (1979), 104–109.

[22] Hardy, G. H., and Ramanujan, S. Asymptotic formulae in combinatorial analysis. *Proc. London Math. Soc. (2) 17* (1917), 75–113.

[23] Körner, T. W. *Naive decision making*. Cambridge University Press, Cambridge, 2008. Mathematics applied to the social world.

[24] Loehr, N. A. *Bijective combinatorics*. Discrete Mathematics and its Applications (Boca Raton). CRC Press, Boca Raton, FL, 2011.

[25] Novelli, J. C., Pak, I. M., and Stoyanovskii, A. V. A direct bijective proof of the hook-length formula. *Discrete Math. Theoret. Computer Science 1* (1997), 53–67.

[26] Paterson, M. B., and Stinson, D. R. A simple combinatorial treatment of constructions and threshold gaps of ramp schemes. *Cryptogr. Commun. 5*, 4 (2013), 229–240.

[27] Quinn, J. J. Tonight! epic math battles: counting versus matching. *Math Horizons 18* (2015), 5–9.

[28] Remmel, J. B. A note on a recursion for the number of derangements. *European J. Combin. 4*, 4 (1983), 371–374.

[29] Shamir, A. How to share a secret. *Comm. ACM 22*, 11 (1979), 612–613.

[30] Stinson, D. R. An explication of secret sharing schemes. *Des. Codes Cryptogr. 2*, 4 (1992), 357–390.

[31] Wildon, M. Knights, spies, games and ballot sequences. *Discrete Math. 310*, 21 (2010), 2974–2983.

[32] Wilf, H. S. A bijection in the theory of derangements. *Mathematics Magazine 57* (1984), 37–40.

[33] Zadeh, N. Computation of optimal poker strategies. *Operations Res. 25*, 4 (1977), 541–562.