THE UNIVERSITY OF SYDNEY

Sydney University Mathematical Society Problem Competition 2012

1. Alice and Bess are playing a game where Alice thinks of a number in the set $A = \{1, 2, 3, 4, 5, 6\}$ and Bess has to guess what it is. If she guesses correctly, she wins; if she guesses incorrectly, Alice increases or decreases her number by 1 (keeping it in the set A) before Bess' next guess. What is the smallest number k such that Bess can guarantee to win within k guesses?

Solution. The answer is $k = 8$. A sequence of 8 guesses which is guaranteed to win is:

$$2,\ 3,\ 4,\ 5,\ 5,\ 4,\ 3,\ 2.$$

The reason for this is as follows. Suppose first that Alice's initial number is even.

- If the first guess 2 is incorrect, Alice's number at that time is either 4 or 6, and must change to either 3 or 5.
- Then if the second guess 3 is incorrect, Alice's number at that time is 5, and must change to either 4 or 6.
- Then if the third guess 4 is incorrect, Alice's number at that time is 6, and must change to 5.
- So the fourth guess 5 is guaranteed to be correct.

Therefore, if Bess has not won within the first four guesses, it must be that Alice's initial number was odd. Since her number changes parity after each unsuccessful guess, her number will again be odd after four guesses.

- Then if the fifth guess 5 is incorrect, Alice's number at that time is either 1 or 3, and must change to either 2 or 4.
- Then if the sixth guess 4 is incorrect, Alice's number at that time is 2, and must change to either 1 or 3.
- Then if the seventh guess 3 is incorrect, Alice's number at that time is 1, and must change to 2.
- So then the eighth guess 2 is guaranteed to be correct.

There is a generalization which is just as easy to prove: if we replace 6 by a general integer $n \geq 3$, the sequence of guesses $2,\ 3,\ \cdots,\ n-1,\ n-1,\ \cdots,\ 3,\ 2$ is guaranteed to win.

Now we must show that no sequence of fewer than 8 (or, in the generalization, $2n-4$) guesses is guaranteed to win. It is enough to show that no sequence where one of the 'internal' numbers $2, 3, 4, 5$ occurs fewer than twice is guaranteed to win. Suppose that the number 2 occurs fewer than twice in the sequence of guesses (the argument for other internal numbers is analogous). Alice's numbers could conceivably alternate between 2 and one of the neighbours of 2 (that is, 1 or 3 – not necessarily the same neighbour each time). In this case, even if there is one occasion when Bess guesses 2, Alice's starting parity could have been such that she is at one of the neighbours of 2 at that time; and on any occasion when Bess guesses one of the neighbours of 2, Alice could be either at 2 or at the other neighbour of 2. So it is possible that Alice evades all of Bess' guesses.

2. Show that there exists an infinite set X of points in the plane such that no three points in X lie on a line, and the distance between any two points in X is a rational number.

Solution. One solution constructs X as a subset of the upper half of the unit circle in the complex plane, in which case it is obvious that no three points in X lie on a line. This semicircle consists of the numbers $e^{2\mathbf{i}\theta}$ where $\theta \in [0, \frac{\pi}{2}]$. Note that the distance between $e^{2\mathbf{i}\theta}$ and $e^{2\mathbf{i}\psi}$ is

$$\begin{aligned}\sqrt{(\cos 2\theta - \cos 2\psi)^2 + (\sin 2\theta - \sin 2\psi)^2} &= \sqrt{2 - 2\cos 2(\theta - \psi)} \\ &= \pm 2(\sin\theta\cos\psi - \cos\theta\sin\psi).\end{aligned}$$

So it suffices to show that there are infinitely many $\theta \in [0, \frac{\pi}{2}]$ such that $\cos\theta$ and $\sin\theta$ are both rational. This follows from the fact that there are infinitely many primitive Pythagorean triples; explicitly, we can have $\cos\theta = \frac{m^2-1}{m^2+1}$ and $\sin\theta = \frac{2m}{m^2+1}$ for any positive integer m.

If we changed "rational number" to "integer" in the statement of the problem, there would be no solution; this result is known as the Erdös–Anning Theorem. It was observed by SUMS entrant Matthew Kwan (UNSW) that any set X satisfying the requirements of the problem must be countable. Indeed, if one fixes distinct points P and Q in the plane, the set of points R such that the distances $|PR|$ and $|QR|$ are both rational is a countable set, since the set of points R such that $|PR|$ and $|QR|$ have specified rational values has at most two elements.

3. Find the largest positive real number α for which the sequence $\left(1 + \dfrac{\alpha}{n}\right)^{n+1}$ (for $n = 1, 2, 3, \cdots$) is monotonically decreasing.

Solution. One way to answer this is to consider the function $f(x) = (x+1)\ln(1 + \dfrac{\alpha}{x})$ of a positive real variable x, where α is a positive real constant. Differentiating, we obtain

$$f'(x) = \ln(1 + \frac{\alpha}{x}) + \frac{x+1}{1+\frac{\alpha}{x}} \cdot \frac{-\alpha}{x^2} = \ln(1 + \frac{\alpha}{x}) - \frac{\alpha(x+1)}{x(x+\alpha)}.$$

It is helpful to change the variable: define the function $g(y)$ of a positive real variable y by

$$g(y) = f'(\frac{\alpha}{y}) = \ln(1+y) - \frac{y(\alpha+y)}{\alpha(1+y)}.$$

Note that $\lim\limits_{y\to 0^+} g(y) = 0$. Moreover,

$$g'(y) = \frac{1}{1+y} - \frac{(\alpha+2y)(1+y) - y(\alpha+y)}{\alpha(1+y)^2} = \frac{y(\alpha-2-y)}{\alpha(1+y)^2}.$$

If $\alpha \le 2$, we conclude that $g'(y) < 0$ for all $y > 0$, so $g(y) < 0$ for all $y > 0$. This shows that $f'(x) < 0$ for all $x > 0$, so $f(x)$ is a strictly decreasing function, and hence so is $e^{f(x)} = \left(1 + \dfrac{\alpha}{x}\right)^{x+1}$. In particular, the sequence $\left(1 + \dfrac{\alpha}{n}\right)^{n+1}$ is strictly decreasing when $\alpha \le 2$.

If $\alpha > 2$, we conclude that $g'(y) > 0$ when $0 < y < \alpha - 2$, so $g(y) > 0$ when $0 < y \le \alpha - 2$. Thus $f'(x) > 0$ for all $x \ge \dfrac{\alpha}{\alpha-2}$, showing that $f(x)$ is a strictly increasing function on the domain $x \ge \dfrac{\alpha}{\alpha-2}$. In particular, the sequence $\left(1 + \dfrac{\alpha}{n}\right)^{n+1}$ is strictly increasing once $n \ge \dfrac{\alpha}{\alpha-2}$, and is therefore certainly not monotonically decreasing. So the answer is $\alpha = 2$.

Incidentally, what we have shown implies that $\lim_{n\to\infty}\left(1+\frac{\alpha}{n}\right)^{n+1}$ exists for all positive α. It is easy to see (for example, using L'Hopital's rule) that this limit equals e^α. When $\alpha = 2$, the sequence begins

$$9,\ 8,\ 7.716\cdots,\ 7.59375,\ 7.529\cdots,\ \text{converging to } e^2 = 7.389\cdots.$$

4. In this problem, a *word* means a string of letters drawn from the three-letter alphabet $\mathsf{A}, \mathsf{B}, \mathsf{C}$. Say that a word is *decent* if it does not contain two consecutive identical letters, and also does not contain AB as a consecutive substring. Find the number of decent words of length n.

Solution. Let d_n denote the number of decent words of length n. Note that $d_1 = 3$ and $d_2 = 5$. Define $d_n^{\mathsf{A}}, d_n^{\mathsf{B}}, d_n^{\mathsf{C}}$ to be the number of decent words of length n ending in those respective letters. Considering what possible second-last letters a decent word can have if its last letter is given, we see that for all $n \geq 2$,

$$\begin{aligned} d_n^{\mathsf{A}} &= d_{n-1}^{\mathsf{B}} + d_{n-1}^{\mathsf{C}}, \\ d_n^{\mathsf{B}} &= d_{n-1}^{\mathsf{C}}, \\ d_n^{\mathsf{C}} &= d_{n-1}^{\mathsf{A}} + d_{n-1}^{\mathsf{B}}. \end{aligned}$$

Hence for all $n \geq 3$,

$$\begin{aligned} d_n &= d_n^{\mathsf{A}} + d_n^{\mathsf{B}} + d_n^{\mathsf{C}} \\ &= d_{n-1}^{\mathsf{A}} + 2d_{n-1}^{\mathsf{B}} + 2d_{n-1}^{\mathsf{C}} \\ &= d_{n-1} + d_{n-1}^{\mathsf{B}} + d_{n-1}^{\mathsf{C}} \\ &= d_{n-1} + d_{n-2}^{\mathsf{C}} + d_{n-2}^{\mathsf{A}} + d_{n-2}^{\mathsf{B}} \\ &= d_{n-1} + d_{n-2}. \end{aligned}$$

This is the same recurrence relation as is satisfied by the Fibonacci sequence. Since $d_1 = F_4$ and $d_2 = F_5$ are consecutive terms of the Fibonacci sequence, we have $d_n = F_{n+3}$ for all $n \geq 1$. An exact formula for the Fibonacci sequence is well known:

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

5. In this problem, S denotes a subset of the set of real numbers.

a) Suppose that $1 \in S$, S is closed under subtraction in the sense that $a, b \in S \Rightarrow a - b \in S$, and S is closed under taking inverses in the sense that $0 \neq a \in S \Rightarrow a^{-1} \in S$. Prove that S is closed under multiplication in the sense that $a, b \in S \Rightarrow ab \in S$.

b) Show that the assumption $1 \in S$ in a) is necessary: that is, give an example of an S that is closed under subtraction and taking inverses, but not closed under multiplication.

Solution. Make the assumptions of a). Note that S contains $0 = 1 - 1$, and hence S is closed under taking negatives, since $a \in S \Rightarrow -a = 0 - a \in S$. It follows that S is closed under addition, since $a, b \in S \Rightarrow a + b = a - (-b) \in S$. (In the language of abstract algebra, S is a subgroup of the additive group $\mathbb{R}$.)

If $a \in S$ is not equal to 0 or 1, then S contains $(a-1)^{-1} - a^{-1} = (a^2-a)^{-1}$, so S contains $a^2 - a$ and hence also a^2. Thus S is closed under squaring. For any nonzero $a, b \in S$, we know that S contains $(a+b)^2 = a^2 + 2ab + b^2$ as well as a^2 and b^2, so S contains $2ab$ and hence also $((2ab)^{-1} + (2ab)^{-1})^{-1} = ab$. If either a or b is zero, it is obvious that S contains ab. So we have shown that S is closed under multiplication, as required. (This means that S is a subfield of the field $\mathbb{R}$.)

One example for part b) is $S = \{a\sqrt{2} \mid a \in \mathbb{Q}\}$. It is clear that S is closed under subtraction. Since $\sqrt{2}$ is irrational, $\sqrt{2}^2 = 2 \notin S$ which shows that S is not closed under multiplication. However, S is closed under taking inverses, because if $a \in \mathbb{Q}$ is nonzero then $(a\sqrt{2})^{-1} = \frac{1}{2a}\sqrt{2} \in S$.

6. Let x be a positive real number. Define a sequence $(a_0(x), a_1(x), a_2(x), \cdots)$ by the initial condition $a_0(x) = x$ and the recursion $a_n(x) = \dfrac{a_{n-1}(x)^2}{n}$ for all $n \geq 1$. For which x does this sequence converge?

Solution. It is obvious that, when x is positive, all terms $a_n(x)$ of the sequence are positive. Since the function $\mathbb{R}_{>0} \to \mathbb{R}_{>0} : y \mapsto \frac{y^2}{n}$ is increasing for all $n \geq 1$, the equivalence $x < y \Leftrightarrow a_n(x) < a_n(y)$ holds for all n. Moreover, x can be recovered uniquely from a specified n and a given value of $a_n(x)$.

Suppose the sequence $(a_n(x))$ converges to the real number L. We must have $L = 0$, for suppose for a contradiction that $L > 0$. Then there is some positive integer N such that $L/2 < a_n(x) < 3L/2$ for all $n \geq N$, which implies in particular that

$$\frac{L}{2} < a_{n+1}(x) = \frac{a_n(x)^2}{n+1} < \frac{9L^2}{4(n+1)} \text{ for all } n \geq N,$$

which rearranges to the absurd statement $L > \frac{2}{9}(n+1)$ for all $n \geq N$.

Now we claim that $(a_n(x))$ converges to 0 if and only if $a_m(x) \leq 1$ for some $m \geq 1$. The "only if" direction is obvious. For the "if" direction, suppose that $a_m(x) \leq 1$ for some $m \geq 1$. Then $a_{m+1}(x) \leq \frac{a_m(x)}{m+1} \leq 1$, $a_{m+2}(x) \leq \frac{a_{m+1}(x)}{m+2} \leq \frac{a_{m+1}(x)}{m+1} \leq 1$, and so forth, giving $a_n(x) \leq \frac{a_m(x)}{(m+1)^{n-m}}$ for all $n \geq m$, which clearly implies that $(a_n(x))$ converges to 0.

For any $m \geq 1$, let x_m denote the unique positive real number such that $a_m(x_m) = 1$. From what we have shown, we know that $(a_n(x))$ converges if and only if $x \leq x_m$ for some $m \geq 1$. By definition, we have

$$\begin{aligned} a_m(x_m) &= 1, \\ a_{m-1}(x_m) &= \sqrt{m}, \\ a_{m-2}(x_m) &= \sqrt{(m-1)\sqrt{m}}, \\ a_{m-3}(x_m) &= \sqrt{(m-2)\sqrt{(m-1)\sqrt{m}}}, \end{aligned}$$

leading to the formula

$$x_m = \prod_{i=1}^{m} i^{2^{-i}}, \text{ or equivalently } \log(x_m) = \sum_{i=1}^{m} \frac{\log(i)}{2^i}.$$

We have that $(a_n(x))$ converges if and only if $\log(x) \leq \log(x_m)$ for some $m \geq 1$.

Now the series $\sum_{i=1}^{\infty} \frac{\log(i)}{2^i}$ has positive terms and converges by the ratio test, since

$$\frac{\log(i+1)}{2^{i+1}} \Big/ \frac{\log(i)}{2^i} = \frac{1}{2}\frac{\log(i+1)}{\log(i)} \leq \frac{2}{3} \text{ for } i \text{ sufficiently large.}$$

Let $L = \sum_{i=1}^{\infty} \frac{\log(i)}{2^i}$. Then the sequence of partial sums $\log(x_m)$ is strictly increasing and tends to L, so the condition that $\log(x) \leq \log(x_m)$ for some $m \geq 1$ is equivalent to the condition that $\log(x) < L$. Therefore the answer is that $(a_n(x))$ converges if and only if $\log(x) < L$, or equivalently $x < e^L = \prod_{i=1}^{\infty} i^{2^{-i}}$.

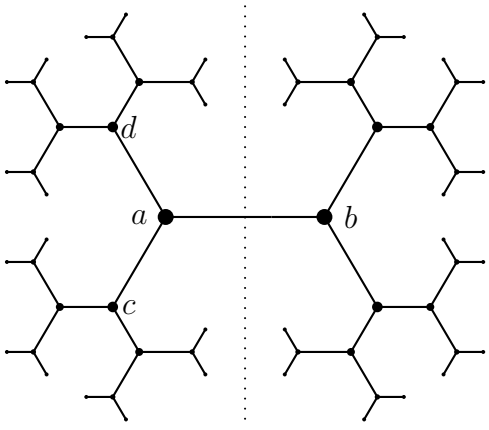
7. A *tree* is a connected simple graph with no cycles. For a tree T, let $s(T)$ denote the number of nonempty subsets X of the set of vertices of T such that for any two vertices in X, there is a path in T joining them that only passes through vertices in X. For a positive integer n, find the minimum and maximum values of $s(T)$ as T ranges over all trees with n vertices.

Solution. Clearly X is such a subset if and only if X, together with the edges of T between vertices in X, is a tree; in other words, X defines a sub-tree of T. So an alternative description of $s(T)$ is that it counts the sub-trees of T.

Any vertex of T is itself a sub-tree, so we get n singleton sub-trees. For any two distinct vertices of T, there is a unique path in T from one to the other. This path is a sub-tree, so we get $\binom{n}{2}$ sub-trees of this kind. Thus $s(T) \geq n + \binom{n}{2} = \frac{1}{2}(n^2 + n)$. Equality in this lower bound is attained exactly when T is itself a path; otherwise, T contains a vertex of degree ≥ 3 and thus contains a sub-tree (consisting of this vertex and three of its neighbours) that is not a singleton or a path.

It is well known that T has $n - 1$ edges. A non-singleton sub-tree is clearly determined by its (nonempty) set of edges, so the number of non-singleton sub-trees is bounded above by $2^{n-1} - 1$. Thus $s(T) \leq 2^{n-1} + n - 1$. Equality in this upper bound is attained exactly when T is a 'star' with one vertex adjacent to every other; otherwise, T contains two edges with no vertices in common, and these two edges do not constitute a sub-tree.

8. In this problem, let T denote a 3-regular tree ("3-regular" means that every vertex is adjacent to 3 others). The vertex set of T is infinite, but this picture gives an indication of part of it:



As shown here, T can be embedded in the plane so that the edges at each vertex are at angles of $120°$, and the whole tree is symmetric under reflection in the dotted line. That reflection σ is one example of an *automorphism* of T (a permutation of the vertices under which adjacent vertices map to adjacent vertices). Another is the 'rotation' ρ, which fixes a, sends b to c, c to d, and d to b, and rotates the direction of each edge by $120°$ clockwise, though it does not

preserve the lengths of edges. An *allowable* automorphism of T is one that may be obtained by repeatedly performing ρ and σ in some order. Show that for any two vertices v and w of T, there are exactly three allowable automorphisms that send v to w.

Solution. Since $\rho^{-1} = \rho^2$ and $\sigma^{-1} = \sigma$, the allowable automorphisms form a subgroup G of the group of automorphisms of T (the subgroup generated by ρ and σ). If V is the set of vertices of T, then G acts on V. Part of what we must show is that this action is transitive, meaning that for any vertex v of T, there is an allowable automorphism that sends v to a.

It is convenient to label vertices according to the left or right turns taken along the path from a to the vertex. For example, the string $bLRRLL$ would represent the vertex reached by starting at a, moving to b, then taking a left turn, then two right turns, then two left turns. With this convention, the labels of vertices other than a are exactly the finite strings where the first digit is either b, c, or d, and every other digit is either L or R.

The rotation ρ gives the following permutation on vertices, where X denotes any string of Ls and Rs:

$$\begin{aligned} a &\mapsto a \\ bX &\mapsto cX \\ cX &\mapsto dX \\ dX &\mapsto bX \end{aligned}$$

The reflection σ gives the following self-inverse permutation on vertices:

$$\begin{aligned} a &\leftrightarrow b \\ cX &\leftrightarrow bR\overline{X} \\ dX &\leftrightarrow bL\overline{X} \end{aligned}$$

where $\overline{X}$ denotes the string obtained from X by replacing every L with an R and vice versa.

We can then prove the transitivity statement by induction on the length of the label of v (in other words, the number of edges in the path from a to v). The base case is clear: each of b, c, d is mapped to a by some allowable automorphism. Given any vertex v different from a, b, c, d, there is an allowable automorphism that sends v to a vertex v' with a shorter label: namely, we can use some power of ρ to change the first digit to b, and then σ to reduce the length by 1. By the induction hypothesis, we can then apply some allowable automorphism to arrive at a, so the induction step is complete.

Since the action is transitive, it follows from basic results in group theory that we can assume $v = w = a$ in the more precise statement of the problem. That is, we need to show that ρ, ρ^2, and the identity $(= \rho^3)$ are the only three allowable automorphisms that fix the vertex a.

Since $\rho^3 = \sigma^2 =$ identity, any allowable automorphism other than these three can be written in the following form:

$$\rho^{i_0}\sigma\rho^{i_1}\sigma\cdots\sigma\rho^{i_{k-1}}\sigma\rho^{i_k},$$

where $k \geq 1$, $i_0, i_k \in \{0, 1, 2\}$, $i_1, \cdots, i_{k-1} \in \{1, 2\}$. Consider what happens we apply this expression (composing from right to left as usual) to the vertex a. We have $\sigma\rho^{i_k}(a) = b$. If $i \in \{1, 2\}$, then $\sigma\rho^i(bX) = b?\overline{X}$ where $?$ denotes either L or R; in particular, $\sigma\rho^i(bX) = bY$ where the length of Y is 1 more than the length of X. Consequently, $\sigma\rho^{i_1}\sigma\cdots\sigma\rho^{i_{k-1}}\sigma\rho^{i_k}(a)$ is of the form bX where X has length $k-1$. The final ρ^{i_0} may change the initial letter to c or d, but it cannot produce the vertex a.

9. For a permutation σ of $\{1, 2, 3, \cdots, n\}$, a *break* of σ is an element k of $\{1, 2, \cdots, n-1\}$ such that $\sigma(\{1, \cdots, k\}) = \{1, \cdots, k\}$. The *score* of σ is the square of the number of breaks. Show that the average score of all permutations of $\{1, 2, 3, \cdots, n\}$ tends to 0 as n tends to infinity.

Solution. Let S_n denote the set (or rather group) of permutations of $\{1, 2, \cdots, n\}$, and write $b(\sigma)$ for the number of breaks of $\sigma \in S_n$. Since $b(\sigma)^2 = b(\sigma) + 2\binom{b(\sigma)}{2}$, it suffices to show that

$$\lim_{n\to\infty} \frac{1}{n!} \sum_{\sigma\in S_n} b(\sigma) = 0 \text{ and } \lim_{n\to\infty} \frac{1}{n!} \sum_{\sigma\in S_n} \binom{b(\sigma)}{2} = 0.$$

Now $\sum_{\sigma\in S_n} b(\sigma)$ is the number of pairs (σ, k) where $\sigma \in S_n$, $k \in \{1, \cdots, n-1\}$, and k is a break of σ. Counting these pairs by k instead, we see that

$$\sum_{\sigma\in S_n} b(\sigma) = \sum_{k=1}^{n-1} k!(n-k)!.$$

The $k = 1$ and $k = n-1$ terms of this sum both equal $(n-1)!$. Every term with $2 \le k \le n-2$ satisfies $k!(n-k)! \le 2(n-2)!$, since

$$\frac{2(n-2)!}{k!(n-k)!} = \frac{(n-2)(n-3)\cdots(n-k+1)}{k(k-1)\cdots 3} = \frac{n-2}{k}\,\frac{n-3}{k-1}\cdots\frac{n-k+1}{3} \ge 1.$$

Hence for all $n \ge 3$ we have

$$\frac{1}{n!}\sum_{k=1}^{n-1} k!(n-k)! \le \frac{2(n-1)! + (n-3).2(n-2)!}{n!} = \frac{4n-8}{n(n-1)}.$$

Since this last quantity clearly tends to 0 as $n \to \infty$, we deduce the first of our desired limit statements.

The proof of the second is similar. Note that $\sum_{\sigma\in S_n} \binom{b(\sigma)}{2}$ is the number of triples (σ, i, j) where $\sigma \in S_n$, $1 \le i < j \le n-1$, and i, j are both breaks of σ. Counting these triples by i, j instead, we see that

$$\sum_{\sigma\in S_n} \binom{b(\sigma)}{2} = \sum_{1\le i<j\le n-1} i!(j-i)!(n-j)!.$$

Note that the latter sum has $\binom{n-1}{2}$ terms. There are three of these terms that are equal to $(n-2)!$, namely the $i = n-2, j = n-1$ term, the $i = 1, j = n-1$ term, and the $i = 1, j = 2$ term. We claim that every other term satisfies $i!(j-i)!(n-j)! \le 2(n-3)!$. If any of $i, j-i, n-j$ equals 1, this follows immediately from the inequality shown in the previous part; otherwise, it still follows from that inequality, via

$$\frac{2(n-3)!}{i!(j-i)!(n-j)!} = \frac{2(j-2)!}{i!(j-i)!}\,\frac{2(n-4)!}{(j-2)!(n-j)!}\,\frac{n-3}{2} > 1.$$

Hence for all $n \ge 4$ we have

$$\frac{1}{n!}\sum_{1\le i<j\le n-1} i!(j-i)!(n-j)! \le \frac{3(n-2)! + (\binom{n-1}{2} - 3).2(n-3)!}{n!} = \frac{n^2-10}{n(n-1)(n-2)}.$$

Since this last quantity clearly tends to 0 as $n \to \infty$, we deduce the second of our desired limit statements.

Generalizing this reasoning, one can show that the same result would hold if the score were defined to be any polynomial function of the number of breaks.

10. Let S denote the polynomial ring $\mathbb{C}[x_1, x_2, x_3, \cdots]$. Define a linear operator Δ on S by

$$\Delta(p) = \sum_{r\geq 0}\left(\sum_{m_1+2m_2+\cdots+rm_r=r} \frac{x_1^{m_1}x_2^{m_2}\cdots x_r^{m_r}}{1^{m_1}m_1!\,2^{m_2}m_2!\,\cdots\,r^{m_r}m_r!}\right)\frac{\partial p}{\partial x_{r+1}}.$$

Here the outer sum, over nonnegative integers r, makes sense because each $p \in S$ involves only finitely many of the variables, so $\frac{\partial p}{\partial x_{r+1}} = 0$ for sufficiently large r. The inner sum is over all r-tuples $(m_1, m_2, \cdots, m_r)$ of nonnegative integers satisfying the stated condition $m_1 + 2m_2 + \cdots + rm_r = r$. (There is an empty 0-tuple, so the $r = 0$ term is $\frac{\partial p}{\partial x_1}$.)

a) For each integer $k \geq 2$, let $p_k = 2(k-1)x_k - \sum_{i=1}^{k-1} x_i x_{k-i}$. Show that $\Delta(p_k) = 0$.

b) Show that the kernel of Δ consists exactly of the polynomials in $p_2, p_3, p_4, \cdots$.

Solution. Note first that Δ is a derivation of S, meaning that $\Delta(pq) = \Delta(p)q + p\Delta(q)$ for all $p, q \in S$. Also, for any $r \geq 0$ we have

$$\Delta(x_{r+1}) = \sum_{m_1+2m_2+\cdots+rm_r=r} \frac{x_1^{m_1}x_2^{m_2}\cdots x_r^{m_r}}{1^{m_1}m_1!2^{m_2}m_2!\cdots r^{m_r}m_r!}.$$

This gives a generating function identity

$$\sum_{r\geq 0}\Delta(x_{r+1})z^r = \prod_{s\geq 1}\exp\left(\frac{x_s}{s}z^s\right) = E(z), \text{ say.}$$

We have

$$\begin{aligned}\sum_{r\geq 0}\Delta(p_{r+2})z^r &= \sum_{r\geq 0}\Delta\left(2(r+1)x_{r+2} - \sum_{i=1}^{r+1} x_i x_{r+2-i}\right)z^r \\ &= 2\sum_{r\geq 0}(r+1)\Delta(x_{r+2})z^r - \sum_{r\geq 0}\sum_{i=1}^{r+1}\Delta(x_i)x_{r+2-i}z^r - \sum_{r\geq 0}\sum_{i=1}^{r+1} x_i\Delta(x_{r+2-i})z^r \\ &= 2E'(z) - E(z)X(z) - X(z)E(z),\end{aligned}$$

where

$$X(z) = \sum_{r\geq 0} x_{r+1}z^r.$$

But

$$\frac{E'(z)}{E(z)} = \frac{d}{dz}\log(E(z)) = \frac{d}{dz}\sum_{s\geq 1}\frac{x_s}{s}z^s = X(z),$$

so $\sum_{r\geq 0}\Delta(p_{r+2})z^r$ vanishes, implying that $\Delta(p_{r+2}) = 0$ for all $r \geq 0$. This finishes part a).

To prove part b), note that since Δ is a derivation, $\ker(\Delta)$ is not just a linear subspace of S but a subalgebra (i.e. it is closed under multiplication). So if L denotes the subalgebra generated by $p_2, p_3, \cdots$ (i.e. the set of all polynomial expressions in these polynomials), part a) implies that $L \subseteq \ker(\Delta)$. We aim to show that $\ker(\Delta) \subseteq L$.

From the definition of p_k, it is clear that x_k (for $k \geq 2$) can be expressed as a polynomial in $x_1, x_2, x_3, \cdots, x_{k-1}, p_k$. By an easy induction, one deduces that x_k (for $k \geq 2$) can be

expressed as a polynomial in $x_1, p_2, p_3, \cdots, p_k$. Hence every element of S can be expressed as a polynomial in the new variables $x_1, p_2, p_3, \cdots$.

Moreover, we claim that these new variables are algebraically independent, meaning that there is no nontrivial polynomial expression in them that equals zero. To prove this, assume for a contradiction that there is such an expression involving $x_1, p_2, p_3, \cdots, p_k$, where $k \geq 2$ is chosen to be minimal. Then we have an equation of the form

$$Q_b(x_1, p_2, \cdots, p_{k-1})p_k^b + Q_{b-1}(x_1, p_2, \cdots, p_{k-1})p_k^{b-1} + \cdots + Q_0(x_1, p_2, \cdots, p_{k-1}) = 0,$$

where $b \geq 1$ and $Q_0, \cdots, Q_b$ are some polynomials in $k-1$ variables, with Q_b being nontrivial. Now the left-hand side is a polynomial in the variables $x_1, x_2, \cdots, x_k$, where the variable x_k occurs only in the powers of p_k. So it can be rewritten in the form

$$Q_b(x_1, p_2, \cdots, p_{k-1})(2(k-1))^b x_k^b + \text{ terms involving lower powers of } x_k,$$

showing that $Q_b(x_1, p_2, \cdots, p_{k-1}) = 0$ in contradiction to the minimality of k.

It follows that every element of S can be written *uniquely* as a polynomial in $x_1, p_2, p_3, \cdots$. Hence every element of S can be written uniquely in the form

$$r_b x_1^b + r_{b-1}x_1^{b-1} + \cdots + r_0, \text{ where } b \geq 0, r_0, \cdots, r_b \in L, r_b \neq 0.$$

Since $\Delta(x_1^i) = ix_1^{i-1}$ and $L \subseteq \ker(\Delta)$, applying Δ to this element gives

$$br_b x_1^{b-1} + (b-1)r_{b-1}x_1^{b-2} + \cdots + r_1.$$

By the uniqueness of such expressions, this vanishes only when $b = 0$. Hence $\ker(\Delta) \subseteq L$ as required.