

# USA IMO TST 2018 Solutions

## United States of America — IMO Team Selection Tests

EVAN CHEN

59<sup>th</sup> IMO 2018 Romania

### Contents

<b>1 Solutions to Day 1</b>	<b>2</b>
1.1 Solution to TST 1, by Ashwin Sah . . . . .	2
1.2 Solution to TST 2, by Michael Kural and Yang Liu . . . . .	3
1.3 Solution to TST 3, by Evan Chen . . . . .	5
<b>2 Solutions to Day 2</b>	<b>10</b>
2.1 Solution to TST 4, by Josh Brakensiek . . . . .	10
2.2 Solution to TST 5, by Evan Chen . . . . .	11
2.3 Solution to TST 6, by Mark Sellke . . . . .	13

## §1 Solutions to Day 1

### §1.1 Solution to TST 1, by Ashwin Sah

Let  $n \geq 2$  be a positive integer, and let  $\sigma(n)$  denote the sum of the positive divisors of  $n$ . Prove that the  $n^{\text{th}}$  smallest positive integer relatively prime to  $n$  is at least  $\sigma(n)$ , and determine for which  $n$  equality holds.

The equality case is  $n = p^e$  for  $p$  prime and a positive integer  $e$ . It is easy to check that this works.

**First solution** In what follows, by  $[a, b]$  we mean  $\{a, a + 1, \dots, b\}$ . First, we make the following easy observation.

**Claim** — If  $a$  and  $d$  are positive integers, then precisely  $\varphi(d)$  elements of  $[a, a + d - 1]$  are relatively prime to  $d$ .

Let  $d_1, d_2, \dots, d_k$  denote the divisors of  $n$  in some order. Consider the intervals

$$\begin{aligned} I_1 &= [1, d_1], \\ I_2 &= [d_1 + 1, d_1 + d_2] \\ &\vdots \\ I_k &= [d_1 + \dots + d_{k-1} + 1, d_1 + \dots + d_k]. \end{aligned}$$

of length  $d_1, \dots, d_k$  respectively. The  $j$ th interval will have exactly  $\varphi(d_j)$  elements which are relatively prime to  $d_j$ , hence at most  $\varphi(d_j)$  which are relatively prime to  $n$ . Consequently, in  $I = \bigcup_{j=1}^k I_j$  there are at most

$$\sum_{j=1}^k \varphi(d_j) = \sum_{d|n} \varphi(d) = n$$

integers relatively prime to  $n$ . On the other hand  $I = [1, \sigma(n)]$  so this implies the inequality.

We see that the equality holds for  $n = p^e$ . Assume now  $p < q$  are distinct primes dividing  $n$ . Reorder the divisors  $d_i$  so that  $d_1 = q$ . Then  $p, q \in I_1$ , and so  $I_1$  should contain strictly fewer than  $\varphi(d_1) = q - 1$  elements relatively prime to  $n$ , hence the inequality is strict.

**Second solution (Ivan Borsenco and Evan Chen)** Let  $n = p_1^{e_1} \dots p_k^{e_k}$ , where  $p_1 < p_2 < \dots$ . We are going to assume  $k \geq 2$ , since the  $k = 1$  case was resolved in the very beginning, and prove the strict inequality.

For a general  $N$ , the number of relatively prime integers in  $[1, N]$  is given exactly by

$$f(N) = N - \sum_i \left\lfloor \frac{N}{p_i} \right\rfloor + \sum_{i < j} \left\lfloor \frac{N}{p_i p_j} \right\rfloor - \dots$$

according to the inclusion-exclusion principle. So, we wish to show that  $f(\sigma(n)) < n$  (as  $k \geq 2$ ). Discarding the error terms from the floors (noting that we get at most 1 from

the negative floors) gives

$$\begin{aligned}
 f(N) &< 2^{k-1} + N - \sum_i \frac{N}{p_i} + \sum_{i<j} \frac{N}{p_i p_j} - \dots \\
 &= 2^{k-1} + N \prod_i (1 - p_i^{-1}) \\
 &= 2^{k-1} + \prod_i (1 - p_i^{-1}) (1 + p_i + p_i^2 + \dots + p_i^{e_i}) \\
 &= 2^{k-1} + \prod_i (p_i^{e_i} - p_i^{-1}).
 \end{aligned}$$

The proof is now divided into two cases. If  $k = 2$  we have

$$\begin{aligned}
 f(N) &< 2 + (p_1^{e_1} - p_1^{-1}) (p_2^{e_2} - p_2^{-1}) \\
 &= 2 + n - \frac{p_2^{e_2}}{p_1} - \frac{p_1^{e_1}}{p_2} + \frac{1}{p_1 p_2} \\
 &\leq 2 + n - \frac{p_2}{p_1} - \frac{p_1}{p_2} + \frac{1}{p_1 p_2} \\
 &= n + \frac{1 - (p_1 - p_2)^2}{p_1 p_2} \leq n.
 \end{aligned}$$

On the other hand if  $k \geq 3$  we may now write

$$\begin{aligned}
 f(N) &< 2^{k-1} + \left[ \prod_{i=2}^{k-1} (p_i^{e_i}) \right] (p_1^{e_1} - p_1^{-1}) \\
 &= 2^{k-1} + n - \frac{p_2^{e_2} \dots p_k^{e_k}}{p_1} \\
 &\leq 2^{k-1} + n - \frac{p_2 p_3 \dots p_k}{p_1}.
 \end{aligned}$$

If  $p_1 = 2$ , then one can show by induction that  $p_2 p_3 \dots p_k \geq 2^{k+1} - 1$ , which implies the result. If  $p_1 > 2$ , then one can again show by induction  $p_3 \dots p_k \geq 2^k - 1$  (since  $p_3 \geq 7$ ), which also implies the result.

## §1.2 Solution to TST 2, by Michael Kural and Yang Liu

Find all functions  $f: \mathbb{Z}^2 \rightarrow [0, 1]$  such that for any integers  $x$  and  $y$ ,

$$f(x, y) = \frac{f(x-1, y) + f(x, y-1)}{2}.$$

---

We claim that the only functions  $f$  are constant functions. (It is easy to see that they work.)

**First solution (hands-on)** First, iterating the functional equation relation to the  $n$ th level shows that

$$f(x, y) = \frac{1}{2^n} \sum_{i=0}^n \binom{n}{i} f(x-i, y-(n-i)).$$

In particular,

$$\begin{aligned} |f(x, y) - f(x - 1, y + 1)| &= \frac{1}{2^n} \left| \sum_{i=0}^{n+1} f(x - i, y - (n - i)) \cdot \left( \binom{n}{i} - \binom{n}{i-1} \right) \right| \\ &\leq \frac{1}{2^n} \sum_{i=0}^{n+1} \left| \binom{n}{i} - \binom{n}{i-1} \right| \\ &= \frac{1}{2^n} \cdot 2 \binom{n}{\lfloor n/2 \rfloor} \end{aligned}$$

where we define  $\binom{n}{n+1} = \binom{n}{-1} = 0$  for convenience. Since

$$\binom{n}{\lfloor n/2 \rfloor} = o(2^n)$$

it follows that  $f$  must be constant.

**Remark.** A very similar proof extends to  $d$  dimensions.

**Second solution (random walks, Mark Sellke)** We show that if  $x + y = x' + y'$  then  $f(x, y) = f(x', y')$ . Let  $Z_n, Z'_n$  be random walks starting at  $(x, y)$  and  $(x', y')$  and moving down/left. Then  $f(Z_n)$  is a martingale so we have

$$\mathbb{E}[f(Z_n)] = f(x, y), \quad \mathbb{E}[f(Z'_n)] = f(x', y').$$

We'll take  $Z_n, Z'_n$  to be independent until they hit each other, after which they will stay together. Then

$$|\mathbb{E}[f(Z_n) - f(Z'_n)]| \leq \mathbb{E}[|f(Z_n) - f(Z'_n)|] \leq 2p_n$$

where  $p_n$  is the probability that  $Z_n, Z'_n$  never collide. But the distance between  $Z_n, Z'_n$  is essentially a 1-dimensional random walk, so they will collide with probability 1, meaning  $\lim_{n \rightarrow \infty} p_n = 0$ . Hence

$$|f(x, y) - f(x', y')| = |\mathbb{E}[f(Z_n) - f(Z'_n)]| = o(1)$$

as desired.

**Remark.** If the problem were in  $\mathbb{Z}^d$  for large  $d$ , this solution wouldn't work as written because the independent random walks wouldn't hit each other. However, this isn't a serious problem because  $Z_n, Z'_n$  don't have to be independent before hitting each other. Indeed, if every time  $Z_n, Z'_n$  agree on a new coordinate we force them to agree on that coordinate forever, we can make the two walks individually have the distribution of a coordinate-decreasing random walk but make them intersect eventually with probability 1. The difference in each coordinate will be a 1-dimensional random walk which gets stuck at 0.

**Third solution (martingales)** Imagine starting at  $(x, y)$  and taking a random walk down and to the left. This is a martingale. As  $f$  is bounded, this martingale converges with probability 1. Let  $X_1, X_2, \dots$  each be random variables that represent either down moves or left moves with equal probability. Note that by the Hewitt-Savage 0-1 law, we have that for any real numbers  $a < b$ ,

$$\Pr \left[ \lim_{n \rightarrow \infty} f((x, y) + X_1 + X_2 + \dots + X_n) \in [a, b] \right] \in \{0, 1\}.$$

Hence, there exists a single value  $v$  such that with probability 1,

$$\Pr \left[ \lim_{n \rightarrow \infty} f((x, y) + X_1 + X_2 + \cdots + X_n) = v \right] = 1.$$

Obviously, this value  $v$  must equal  $f(x, y)$ . Now, we show this value  $v$  is the same for all  $(x, y)$ . Note that any two starting points have a positive chance of meeting. Therefore, we are done.

### §1.3 Solution to TST 3, by Evan Chen

At a university dinner, there are 2017 mathematicians who each order two distinct entrées, with no two mathematicians ordering the same pair of entrées. The cost of each entrée is equal to the number of mathematicians who ordered it, and the university pays for each mathematician's less expensive entrée (ties broken arbitrarily). Over all possible sets of orders, what is the maximum total amount the university could have paid?

In graph theoretic terms: we wish to determine the maximum possible value of

$$S(G) \stackrel{\text{def}}{=} \sum_{e=vw} \min(\deg v, \deg w)$$

across all graphs  $G$  with 2017 edges. We claim the answer is  $63 \cdot \binom{64}{2} + 1 = 127009$ .

**First solution (combinatorial, Evan Chen)** First define  $L_k$  to consist of a clique on  $k$  vertices, plus a single vertex connected to exactly one vertex of the clique. Hence  $L_k$  has  $k + 1$  vertices,  $\binom{k}{2} + 1$  edges, and  $S(L_k) = (k - 1)\binom{k}{2} + 1$ . In particular,  $L_{64}$  achieves the claimed maximum, so it suffices to prove the upper bound.

#### Lemma

Let  $G$  be a graph such that either

- $G$  has  $\binom{k}{2}$  edges for some  $k \geq 3$  or
- $G$  has  $\binom{k}{2} + 1$  edges for some  $k \geq 4$ .

Then there exists a graph  $G^*$  with the same number of edges such that  $S(G^*) \geq S(G)$ , and moreover  $G^*$  has a universal vertex (i.e. a vertex adjacent to every other vertex).

*Proof.* Fix  $k$  and the number  $m$  of edges. We prove the result by induction on the number  $n$  of vertices in  $G$ . Since the lemma has two parts, we will need two different base cases:

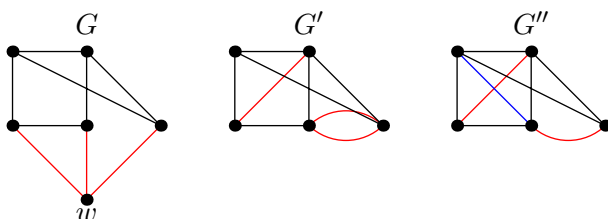
1. Suppose  $n = k$  and  $m = \binom{k}{2}$ . Then  $G$  must be a clique so pick  $G^* = G$ .
2. Suppose  $n = k + 1$  and  $m = \binom{k}{2} + 1$ . If  $G$  has no universal vertex, we claim we may take  $G^* = L_k$ . Indeed each vertex of  $G$  has degree at most  $k - 1$ , and the average degree is

$$\frac{2m}{n} = \frac{k^2 - k + 1}{k + 1} < k - 1$$

using here  $k \geq 4$ . Thus there exists a vertex  $w$  of degree  $1 \leq d \leq k - 2$ . The edges touching  $w$  will have label at most  $d$  and hence

$$\begin{aligned} S(G) &\leq (k-1)(m-d) + d^2 = (k-1)m - d(k-1-d) \\ &\leq (k-1)m - (k-2) = (k-1) \binom{k}{2} + 1 = S(G^*). \end{aligned}$$

Now we settle the inductive step. Let  $w$  be a vertex with minimal degree  $0 \leq d < k - 1$ , with neighbors  $w_1, \dots, w_d$ . By our assumption, for each  $w_i$  there exists a vertex  $v_i$  for which  $v_i w_i \notin E$ . Now, we may delete all edges  $w w_i$  and in their place put  $v_i w_i$ , and then delete the vertex  $w$ . This gives a graph  $G'$ , possibly with multiple edges (if  $v_i = w_j$  and  $w_j = v_i$ ), and with one fewer vertex.



We then construct a graph  $G''$  by taking any pair of double edges, deleting one of them, and adding any missing edge of  $G''$  in its place. (This is always possible, since when  $m = \binom{k}{2}$  we have  $n - 1 \geq k$  and when  $m = \binom{k}{2} + 1$  we have  $n - 1 \geq k + 1$ .)

Thus we have arrived at a simple graph  $G''$  with one fewer vertex. We also observe that we have  $S(G'') \geq S(G)$ ; after all every vertex in  $G''$  has degree at least as large as it did in  $G$ , and the  $d$  edges we deleted have been replaced with new edges which will have labels at least  $d$ . Hence we may apply the inductive hypothesis to the graph  $G''$  to obtain  $G^*$  with  $S(G^*) \geq S(G'') \geq S(G)$ .  $\square$

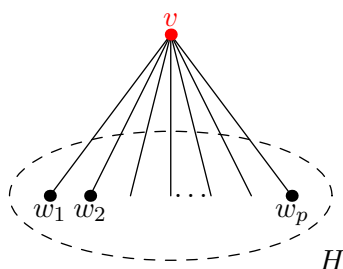
The problem then is completed once we prove the following:

**Claim** — For any graph  $G$ ,

- If  $G$  has  $\binom{k}{2}$  edges for  $k \geq 3$ , then  $S(G) \leq \binom{k}{2} \cdot (k - 1)$ .
- If  $G$  has  $\binom{k}{2} + 1$  edges for  $k \geq 4$ , then  $S(G) \leq \binom{k}{2} \cdot (k - 1) + 1$ .

*Proof.* We prove both parts at once by induction on  $k$ , with the base case  $k = 3$  being plain (there is nothing to prove in the second part for  $k = 3$ ). Thus assume  $k \geq 4$ . By the earlier lemma, we may assume  $G$  has a universal vertex  $v$ . For notational convenience, we say  $G$  has  $\binom{k}{2} + \varepsilon$  edges for  $\varepsilon \in \{0, 1\}$ , and  $G$  has  $p + 1$  vertices, where  $p \geq k - 1 + \varepsilon$ .

Let  $H$  be the subgraph obtained when  $v$  is deleted. Then  $m = \binom{k}{2} + \varepsilon - p$  is the number of edges in  $H$ ; from  $p \geq k - 1 + \varepsilon$  we have  $m \leq \binom{k-1}{2}$  and so we may apply the inductive hypothesis to  $H$  to deduce  $S(H) \leq \binom{k-1}{2} \cdot (k - 2)$ .



Now the labels of edges  $vw_i$  have sum

$$\sum_{i=1}^p \min(\deg_G v, \deg_G w_i) = \sum_{i=1}^p \deg_G w_i = \sum_{i=1}^p (\deg_H w_i + 1) = 2m + p.$$

For each of the edges contained in  $H$ , the label on that edge has increased by exactly 1, so those edges contribute  $S(H) + m$ . In total,

$$\begin{aligned} S(G) &= 2m + p + (S(H) + m) = (m + p) + 2m + S(H) \\ &\leq \binom{k}{2} + \varepsilon + 2 \binom{k-1}{2} + \binom{k-1}{2} (k-2) = \binom{k}{2} (k-1) + \varepsilon. \quad \square \end{aligned}$$

**Second solution (algebraic, submitted by contestant James Lin)** We give a different proof of  $S(G) \leq 127009$ . The proof proceeds using the following two claims, which will show that  $S(G) \leq 127010$  for all graphs  $G$ . Then a careful analysis of the equality cases will show that this bound is not achieved for any graph  $G$ . Since the example  $L_{64}$  earlier has  $S(L_{64}) = 127009$ , this will solve the problem.

**Lemma (Combinatorial bound)**

Let  $G$  be a graph with 2017 edges and let  $d_1 \geq d_2 \geq \dots \geq d_n$  be the degree sequence of the graph (thus  $n \geq 65$ ). Then

$$S(G) \leq d_2 + 2d_3 + 3d_4 + \dots + 63d_{64} + d_{65}.$$

*Proof.* Let  $v_1, \dots, v_n$  be the corresponding vertices. For any edge  $e = \{v_i, v_j\}$  with  $i < j$ , we consider associating each edge  $e$  with  $v_j$ , and computing the sum  $S(G)$  indexing over associated vertices. To be precise, if we let  $a_i$  denote the number of edges associated to  $v_i$ , we now have  $a_i \leq i - 1$ ,  $\sum a_i = 4034$ , and

$$S(G) = \sum_{i=1}^n a_i d_i.$$

The inequality  $\sum a_i d_i \leq d_2 + 2d_3 + 3d_4 + \dots + 63d_{64} + d_{65}$  then follows for smoothing reasons (by “smoothing” the  $a_i$ ), since the  $d_i$  are monotone. This proves the given inequality.  $\square$

Once we have this property, we handle the bounding completely algebraically.

**Lemma (Algebraic bound)**

Let  $x_1 \geq x_2 \geq \dots \geq x_{65}$  be any nonnegative integers such that  $\sum_{i=1}^{65} x_i \leq 4034$ . Then

$$x_2 + 2x_3 + \dots + 63x_{64} + x_{65} \leq 127010.$$

Moreover, equality occurs if and only if  $x_1 = x_2 = x_3 = \dots = x_{64} = 63$  and  $x_{65} = 2$ .

*Proof.* Let  $A$  denote the left-hand side of the inequality. We begin with a smoothing argument.

- Suppose there are indices  $1 \leq i < j \leq 64$  such that  $x_i > x_{i+1} \geq x_{j-1} > x_j$ . Then replacing  $(x_i, x_j)$  by  $(x_i - 1, x_j + 1)$  strictly increases  $A$  preserving all conditions. Thus we may assume all numbers in  $\{x_1, \dots, x_{64}\}$  differ by at most 1.

- Suppose  $x_{65} \geq 4$ . Then we can replace  $(x_1, x_2, x_3, x_4, x_{65})$  by  $(x_1 + 1, x_2 + 1, x_3 + 1, x_4 + 1, x_{65} - 4)$  and strictly increase  $A$ . Hence we may assume  $x_{65} \leq 3$ .

We will also tacitly assume  $\sum x_i = 4034$ , since otherwise we can increase  $x_1$ . These two properties leave only four sequences to examine:

- $x_1 = x_2 = x_3 = \cdots = x_{63} = 63$ ,  $x_{64} = 62$ , and  $x_{65} = 3$ , which gives  $A = 126948$ .
- $x_1 = x_2 = x_3 = \cdots = x_{63} = x_{64} = 63$  and  $x_{65} = 2$ , which gives  $A = 127010$ .
- $x_1 = 64$ ,  $x_2 = x_3 = \cdots = x_{63} = x_{64} = 63$  and  $x_{65} = 1$ , which gives  $A = 127009$ .
- $x_1 = x_2 = 64$ ,  $x_3 = \cdots = x_{63} = x_{64} = 63$  and  $x_{65} = 0$ , which gives  $A = 127009$ .

This proves that  $A \leq 127010$ . To see that equality occurs only in the second case above, note that all the smoothing operations other than incrementing  $x_1$  were strict, and that  $x_1$  could not have been incremented in this way as  $x_1 = x_2 = 63$ .  $\square$

This shows that  $S(G) \leq 127010$  for all graphs  $G$ , so it remains to show equality never occurs. Retain the notation  $d_i$  and  $a_i$  of the combinatorial bound now; we would need to have  $d_1 = \cdots = d_{64} = 63$  and  $d_{65} = 2$  (in particular, deleting isolated vertices from  $G$ , we may assume  $n = 65$ ). In that case, we have  $a_i \leq i - 1$  but also  $a_{65} = 2$  by definition (the last vertex gets all edges associated to it). Finally,

$$\begin{aligned} S(G) &= \sum_{i=1}^n a_i d_i = 63(a_1 + \cdots + a_{64}) + a_{65} \\ &= 63(2017 - a_{65}) + a_{65} \leq 63 \cdot 2015 + 2 = 126947 \end{aligned}$$

completing the proof.

**Remark.** Another way to finish once  $S(G) \leq 127010$  is note there is a unique graph (up to isomorphism and deletion of universal vertices) with degree sequence  $(d_1, \dots, d_{65}) = (63, \dots, 63, 2)$ . Indeed, the complement of the graph has degree sequence  $(1, \dots, 1, 63)$ , and so it must be a 63-star plus a single edge. One can then compute  $S(G)$  explicitly for this graph.

### Some further remarks

**Remark.** Interestingly, the graph  $C_4$  has  $\binom{3}{2} + 1 = 4$  edges and  $S(C_4) = 8$ , while  $S(L_3) = 7$ . This boundary case is visible in the combinatorial solution in the base case of the first claim. It also explains why we end up with the bound  $S(G) \leq 127010$  in the second algebraic solution, and why it is necessary to analyze the equality cases so carefully; observe in  $k = 3$  the situation  $d_1 = d_2 = d_3 = d_4 = 2$ .

**Remark.** Some comments about further context for this problem:

- The obvious generalization of 2017 to any constant was resolved in September 2018 by Mehtaab Sawhney and Ashwin Sah. The relevant paper is *On the discrepancy between two Zagreb indices*, published in *Discrete Mathematics*, Volume 341, Issue 9, pages 2575-2589. The arXiv link is <https://arxiv.org/pdf/1801.02532.pdf>.
- The quantity

$$S(G) = \sum_{e=vw} \min(\deg v, \deg w)$$

in the problem has an interpretation: it can be used to provide a bound on the number of triangles in a graph  $G$ . To be precise,  $\#E(G) \leq \frac{1}{3}S(G)$ , since an edge  $e = vw$  is



part of at most  $\min(\deg v, \deg w)$  triangles.

- For *planar* graphs it is known  $S(G) \leq 18n - 36$  and it is conjectured that for  $n$  large enough,  $S(G) \leq 18n - 72$ . See <https://mathoverflow.net/a/273694/70654>.

**Authorship comments** I came up with the quantity  $S(G)$  in a failed attempt to provide a bound on the number of triangles in a graph, since this is natural to consider when you do a standard double-counting via the edges of the triangle. I think the problem was actually APMO 1989, and I ended up not solving the problem (the solution is much simpler), but the quantity  $S(G)$  stuck in my head for a while after that.

Later on that month I was keeping Danielle company while she was working on art project (flower necklace), and with not much to do except doodle on tables I began thinking about  $S(G)$  again. I did have the sense that  $S(G)$  should be maximized at a graph close to a complete graph. But to my frustration I could not prove it for a long time. Finally after many hours of trying various approaches I was able to at least show that  $S(G)$  was maximized for complete graphs if the number of edges was a triangular number.

I had come up with this in March 2016, which would have been perfect since 2016 is a triangular number, but it was too late to submit it to any contest (the USAMO and IMO deadlines were long past). So on December 31, 2016 I finally sat down and solved it for the case 2017, which took another few hours of thought, then submitted it to that year's IMO. To my dismay it was rejected, but I passed it along to the USA TST after that, thus making it just in time for the close of the calendar year.

## §2 Solutions to Day 2

### §2.1 Solution to TST 4, by Josh Brakensiek

Let  $n$  be a positive integer and let  $S \subseteq \{0, 1\}^n$  be a set of binary strings of length  $n$ . Given an odd number  $x_1, \dots, x_{2k+1} \in S$  of binary strings (not necessarily distinct), their *majority* is defined as the binary string  $y \in \{0, 1\}^n$  for which the  $i^{\text{th}}$  bit of  $y$  is the most common bit among the  $i^{\text{th}}$  bits of  $x_1, \dots, x_{2k+1}$ . (For example, if  $n = 4$  the majority of 0000, 0000, 1101, 1100, 0101 is 0100.)

Suppose that for some positive integer  $k$ ,  $S$  has the property  $P_k$  that the majority of any  $2k + 1$  binary strings in  $S$  (possibly with repetition) is also in  $S$ . Prove that  $S$  has the same property  $P_k$  for all positive integers  $k$ .

Let  $M$  denote the majority function (of any length).

**First solution (induction)** We prove all  $P_k$  are equivalent by induction on  $n \geq 2$ , with the base case  $n = 2$  being easy to check by hand. (The case  $n = 1$  is also vacuous; however, the inductive step is not able to go from  $n = 1$  to  $n = 2$ .)

For the inductive step, we proceed by contradiction; assume  $S$  satisfies  $P_\ell$ , but not  $P_k$ , so there exist  $x_1, \dots, x_{2k+1} \in S$  whose majority  $y = M(x_1, \dots, x_k)$  is not in  $S$ . We contend that:

**Claim** — Let  $y_i$  be the string which differs from  $y$  only in the  $i^{\text{th}}$  bit. Then  $y_i \in S$ .

*Proof.* For a string  $s \in S$  we let  $\hat{s}$  denote the string  $s$  with the  $i^{\text{th}}$  bit deleted (hence with  $n - 1$  bits). Now let

$$T = \{\hat{s} \mid s \in S\}.$$

Since  $S$  satisfies  $P_\ell$ , so does  $T$ ; thus by the induction hypothesis on  $n$ ,  $T$  satisfies  $P_k$ .

Consequently,  $T \ni M(\hat{x}_1, \dots, \hat{x}_{2k+1}) = \hat{y}$ . Thus there exists  $s \in S$  such that  $\hat{s} = \hat{y}$ . This implies  $s = y$  or  $s = y_i$ . But since we assumed  $y \notin S$  it follows  $y_i \in S$  instead.  $\square$

Now take any  $2\ell + 1$  copies of the  $y_i$ , about equally often (i.e. the number of times any two  $y_i$  are taken differs by at most 1). We see the majority of these is  $y$  itself, contradiction.

**Second solution (circuit construction)** Note that  $P_k \implies P_1$  for any  $k$ , since

$$M(\underbrace{a, \dots, a}_k, \underbrace{b, \dots, b}_k, c) = M(a, b, c)$$

for any  $a, b, c$ .

We will now prove  $P_1 + P_k \implies P_{k+1}$  for any  $k$ , which will prove the result. Actually, we will show that the majority of any  $2k + 3$  strings  $x_1, \dots, x_{2k+3}$  can be expressed by 3 and  $(2k + 1)$ -majorities. WLOG assume that  $M(x_1, \dots, x_{2k+3}) = 0 \dots 0$ , and let  $\odot$  denote binary AND.

**Claim** — We have  $M(x_1, x_2, M(x_3, \dots, x_{2k+3})) = x_1 \odot x_2$ .

*Proof.* Consider any particular bit. The result is clear if the bits are equal. Otherwise, if they differ, the result follows from the original hypothesis that  $M(x_1, \dots, x_{2k+3}) = 0 \dots 0$  (removing two differing bits does not change the majority).  $\square$

By analogy we can construct any  $x_i \odot x_j$ . Finally, note that

$$M(x_1 \odot x_2, x_2 \odot x_3, \dots, x_{2k+1} \odot x_{2k+2}) = 0 \dots 0,$$

as desired. (Indeed, if we look at any index, there were at most  $k + 1$  1's in the  $x_i$  strings, and hence there will be at most  $k$  1's among  $x_i \odot x_{i+1}$  for  $i = 1, \dots, 2k + 1$ .)

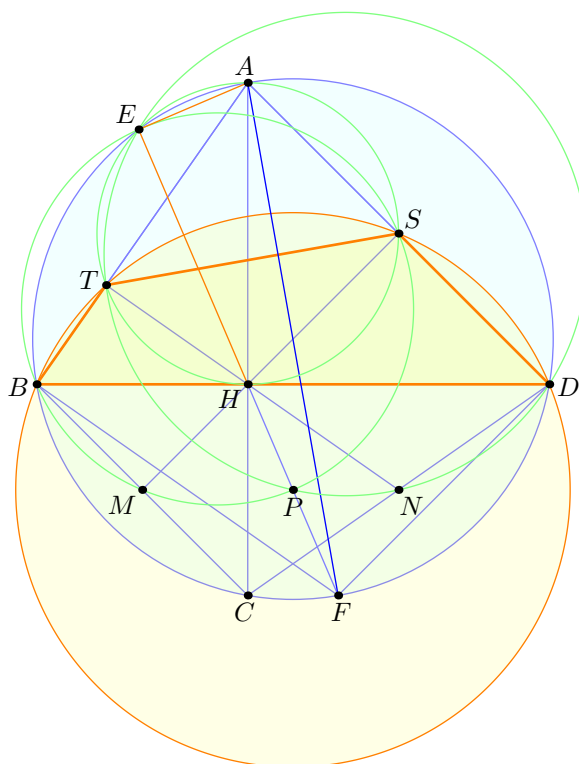
**Remark.** The second solution can be interpreted in circuit language as showing that all “ $2k + 1$ -majority gates” are equivalent. See also <https://cstheory.stackexchange.com/a/21399/48303>, in which Valiant gives a probabilistic construction to prove that one can construct  $(2k + 1)$ -majority gates from a *polynomial* number of 3-majority gates. No explicit construction is known for this.

## §2.2 Solution to TST 5, by Evan Chen

Let  $ABCD$  be a convex cyclic quadrilateral which is not a kite, but whose diagonals are perpendicular and meet at  $H$ . Denote by  $M$  and  $N$  the midpoints of  $\overline{BC}$  and  $\overline{CD}$ . Rays  $MH$  and  $NH$  meet  $\overline{AD}$  and  $\overline{AB}$  at  $S$  and  $T$ , respectively. Prove there exists a point  $E$ , lying outside quadrilateral  $ABCD$ , such that

- ray  $EH$  bisects both angles  $\angle BES$ ,  $\angle TED$ , and
- $\angle BEN = \angle MED$ .

The main claim is that  $E$  is the intersection of  $(ABCD)$  with the circle with diameter  $\overline{AH}$ .



The following observation can be quickly made without reference to  $E$ .

### Lemma

We have  $\angle HSA = \angle HTA = 90^\circ$ . Consequently, quadrilateral  $BTSD$  is cyclic.

*Proof.* This is direct angle chasing. In fact,  $\overline{HM}$  passes through the circumcenter of  $\triangle BHC$  and  $\triangle HAD \sim \triangle HCB$ , so  $\overline{HS}$  ought to be the altitude of  $\triangle HAD$ .  $\square$

From here it follows that  $E$  is the Miquel point of cyclic quadrilateral  $BTSD$ . Define  $F$  to be the point diametrically opposite  $A$ , so that  $E, H, F$  are collinear,  $\overline{CF} \parallel \overline{BD}$ . By now we already have

$$\angle BEH = \angle BEF = \angle BAF = \angle CAD = \angle HAS = \angle HES$$

so  $\overline{EH}$  bisects  $\angle BES$ , and  $\angle TED$ . Hence it only remains to show  $\angle BEM = \angle NED$ ; we present several proofs below.

**First proof (original solution)** Let  $P$  be the circumcenter of  $BTSD$ . The properties of the Miquel point imply  $P$  lies on the common bisector  $\overline{EH}$  already, and it also lies on the perpendicular bisector of  $\overline{BD}$ , hence it must be the midpoint of  $\overline{HF}$ .

We now contend quadrilaterals  $BMPS$  and  $DNPT$  are cyclic. Obviously  $\overline{MP}$  is the external angle bisector of  $\angle BMS$ , and  $PB = PS$ , so  $P$  is the arc midpoint of  $(BMS)$ . The proof for  $DNPT$  is analogous.

It remains to show  $\angle BEN = \angle MED$ , or equivalently  $\angle BEM = \angle NED$ . By properties of Miquel point we have  $E \in (BMPS) \cap (TPND)$ , so

$$\angle BEM = \angle BPM = \angle PBD = \angle BDP = \angle NPD = \angle NED$$

as desired.

**Second proof (2011 G4)** By 2011 G4, the circumcircle of  $\triangle EMN$  is tangent to the circumcircle of  $ABCD$ . Hence if we extend  $\overline{EM}$  and  $\overline{EN}$  to meet  $(ABCD)$  again at  $X$  and  $Y$ , we get  $\overline{XY} \parallel \overline{MN} \parallel \overline{BD}$ . Thus  $\angle BEM = \angle BEX = \angle YED = \angle NED$ .

**Third proof (involutions, submitted by contestant Daniel Liu)** Let  $G = \overline{BN} \cap \overline{MD}$  denote the centroid of  $\triangle BCD$ , and note that it lies on  $\overline{EHF}$ .

Now consider the dual of Desargues involution theorem on complete quadrilateral  $BNMDCG$  at point  $E$ . We get

$$(EB, EN), \quad (ED, EM), \quad (EC, EG)$$

form an involutive pairing.

However, the bisector of  $\angle BED$ , say  $\ell$ , is also the angle bisector of  $\angle CEF$  (since  $\overline{CF} \parallel \overline{BD}$ ). So the involution we found must coincide with reflection across  $\ell$ . This means  $\angle MEN$  is bisected by  $\ell$  as well, as desired.

**Authorship comments** This diagram actually comes from the inverted picture in IMO 2014/3 (which I attended). I had heard for many years that one could solve this problem quickly by inversion at  $H$  afterwards. But when I actually tried to do it during an OTIS class years later, I ended up with the picture in the TST problem, and couldn't see why it was true! In the process of trying to reconstruct this rumored solution, I ended up finding most of the properties that ended up in the January TST problem (but were overkill for the original IMO problem).

Let us make the equivalence explicit by deducing the IMO problem from our work.

Let rays  $EM$  and  $EN$  meet the circumcircles of  $\triangle BHC$  and  $\triangle BNC$  again at  $X$  and  $Y$ , with  $EM < EX$  and  $EN < EY$ . As above we concluded  $EM/EX = EN/EY$  and so  $\overline{MN} \parallel \overline{XY} \implies \overline{XY} \perp \overline{AHC}$ .

Now consider an inversion at  $H$  which swaps  $B \leftrightarrow D$  and  $A \leftrightarrow C$ . The point  $E$  goes to  $E^*$  diametrically opposite  $A$ . Points  $X$  and  $Y$  go to points on  $X^* \in \overline{AD}$  and  $Y^* \in \overline{AB}$ . Since the reflection of  $E$  across  $\overline{PX}$  is supposed to lie on  $(BAE)$ , it follows that the circumcenter of  $\triangle HX^*E^*$  lies on  $\overline{AD}$ . Consequently  $X^*$  plays the role of point “ $T$ ” in the IMO problem. Then  $Y^*$  plays the role of point “ $S$ ” in the IMO problem.

Now the fact that  $(HX^*Y^*)$  is tangent to  $\overline{BD}$  is equivalent to  $\overline{XY} \perp \overline{AHC}$  which we already knew.

### §2.3 Solution to TST 6, by Mark Sellke

Alice and Bob play a game. First, Alice secretly picks a finite set  $S$  of lattice points in the Cartesian plane. Then, for every line  $\ell$  in the plane which is horizontal, vertical, or has slope  $+1$  or  $-1$ , she tells Bob the number of points of  $S$  that lie on  $\ell$ . Bob wins if he can then determine the set  $S$ .

Prove that if Alice picks  $S$  to be of the form

$$S = \{(x, y) \in \mathbb{Z}^2 \mid m \leq x^2 + y^2 \leq n\}$$

for some positive integers  $m$  and  $n$ , then Bob can win. (Bob does not know in advance that  $S$  is of this form.)

Clearly Bob can compute the number  $N$  of points.

The main claim is that:

**Claim** — Fix  $m$  and  $n$  as in the problem statement. Among all sets  $T \subseteq \mathbb{Z}^2$  with  $N$  points, the set  $S$  is the *unique* one which maximizes the value of

$$F(T) := \sum_{(x,y) \in T} (x^2 + y^2)(m + n - (x^2 + y^2)).$$

*Proof.* Indeed, the different points in  $T$  do not interact in this sum, so we simply want the points  $(x, y)$  with  $x^2 + y^2$  as close as possible to  $\frac{m+n}{2}$  which is exactly what  $S$  does.  $\square$

As a result of this observation, it suffices to show that Bob has enough information to compute  $F(S)$  from the data given. (There is no issue with fixing  $m$  and  $n$ , since Bob can find an upper bound on the magnitude of the points and then check all pairs  $(m, n)$  smaller than that.) The idea is that he knows the full distribution of each of  $X$ ,  $Y$ ,  $X + Y$ ,  $X - Y$  and hence can compute sums over  $T$  of any power of a single one of those linear functions. By taking linear combinations we can hence compute  $F(S)$ .

Let us make the relations explicit. For ease of exposition we take  $Z = (X, Y)$  to be a uniformly random point from the set  $S$ . The information is precisely the individual distributions of  $X$ ,  $Y$ ,  $X + Y$ , and  $X - Y$ . Now compute

$$\begin{aligned} \frac{F(S)}{N} &= \mathbb{E} [(m + n)(X^2 + Y^2) - (X^2 + Y^2)^2] \\ &= (m + n) (\mathbb{E}[X^2] + \mathbb{E}[Y^2]) - \mathbb{E}[X^4] - \mathbb{E}[Y^4] - 2\mathbb{E}[X^2Y^2]. \end{aligned}$$

On the other hand,

$$\mathbb{E}[X^2Y^2] = \frac{\mathbb{E}[(X + Y)^4] + \mathbb{E}[(X - Y)^4] - 2\mathbb{E}[X^4] - 2\mathbb{E}[Y^4]}{12}.$$

Thus we have written  $F(S)$  in terms of the distributions of  $X$ ,  $Y$ ,  $X - Y$ ,  $X + Y$  which completes the proof.

**Remark** (Mark Sellke). • This proof would have worked just as well if we allowed arbitrary  $[0, 1]$ -valued weights on points with finitely many weights non-zero. There is an obvious continuum generalization one can make concerning the indicator function for an annulus. It's a simpler but fun problem to characterize when just the vertical/horizontal directions determine the distribution.

- An obstruction to purely combinatorial arguments is that if you take an octagon with points  $(\pm a, \pm b)$  and  $(\pm b, \pm a)$  then the two ways to pick every other point (going around clockwise) are indistinguishable by Bob. This at least shows that Bob's task is far from possible in general, and hints at proving an inequality.
- A related and more standard fact (among a certain type of person) is that given a probability distribution  $\mu$  on  $\mathbb{R}^n$ , if I tell you the distribution of *all* 1-dimensional projections of  $\mu$ , that determines  $\mu$  uniquely. This works because this information gives me the Fourier transform  $\hat{\mu}$ , and Fourier transforms are injective.

For the continuum version of this problem, this connection gives a much larger family of counterexamples to any proposed extension to arbitrary non-annular shapes. Indeed, take a fast-decaying smooth function  $f: \mathbb{R}^2 \rightarrow \mathbb{R}$  which vanishes on the four lines

$$x = 0, y = 0, x + y = 0, x - y = 0.$$

Then the Fourier transform  $\hat{f}$  will have mean 0 on each line  $\ell$  as in the problem statement. Hence the positive and negative parts of  $\hat{f}$  will not be distinguishable by Bob.