USAMO 2025 Solution Notes

EVAN CHEN《陳誼廷》

27 March 2025

This is a compilation of solutions for the 2025 USAMO. The ideas of the solution are a mix of my own work, the solutions provided by the competition organizers, and solutions found by the community. However, all the writing is maintained by me.

These notes will tend to be a bit more advanced and terse than the "official" solutions from the organizers. In particular, if a theorem or technique is not known to beginners but is still considered "standard", then I often prefer to use this theory anyways, rather than try to work around or conceal it. For example, in geometry problems I typically use directed angles without further comment, rather than awkwardly work around configuration issues. Similarly, sentences like "let $\mathbb{R}$ denote the set of real numbers" are typically omitted entirely.

Corrections and comments are welcome!

Contents

§0 Problems

1. Fix positive integers k and d. Prove that for all sufficiently large odd positive integers n, the digits of the base-$2n$ representation of n^k are all greater than d.

2. Let $n > k \geq 1$ be integers. Let $P(x) \in \mathbb{R}[x]$ be a polynomial of degree n with no repeated roots and $P(0) \neq 0$. Suppose that for any real numbers $a_0, \dots, a_k$ such that the polynomial $a_k x^k + \dots + a_1 x + a_0$ divides $P(x)$, the product $a_0 a_1 \dots a_k$ is zero. Prove that $P(x)$ has a nonreal root.

3. Alice the architect and Bob the builder play a game. First, Alice chooses two points P and Q in the plane and a subset $\mathcal{S}$ of the plane, which are announced to Bob. Next, Bob marks infinitely many points in the plane, designating each a city. He may not place two cities within distance at most one unit of each other, and no three cities he places may be collinear. Finally, roads are constructed between the cities as follows: each pair A, B of cities is connected with a road along the line segment AB if and only if the following condition holds:

   > For every city C distinct from A and B, there exists $R \in \mathcal{S}$ such that $\triangle PQR$ is directly similar to either $\triangle ABC$ or $\triangle BAC$.

   Alice wins the game if (i) the resulting roads allow for travel between any pair of cities via a finite sequence of roads and (ii) no two roads cross. Otherwise, Bob wins. Determine, with proof, which player has a winning strategy.

4. Let H be the orthocenter of an acute triangle ABC, let F be the foot of the altitude from C to AB, and let P be the reflection of H across BC. Suppose that the circumcircle of triangle AFP intersects line BC at two distinct points X and Y. Prove that $CX = CY$.

5. Find all positive integers k such that: for every positive integer n, the sum

   $$\binom{n}{0}^k + \binom{n}{1}^k + \dots + \binom{n}{n}^k$$

   is divisible by $n + 1$.

6. Let m and n be positive integers with $m \geq n$. There are m cupcakes of different flavors arranged around a circle and n people who like cupcakes. Each person assigns a nonnegative real number score to each cupcake, depending on how much they like the cupcake. Suppose that for each person P, it is possible to partition the circle of m cupcakes into n groups of consecutive cupcakes so that the sum of P's scores of the cupcakes in each group is at least 1. Prove that it is possible to distribute the m cupcakes to the n people so that each person P receives cupcakes of total score at least 1 with respect to P.

§1 Solutions to Day 1

§1.1 USAMO 2025/1, proposed by John Berman

Available online at https://aops.com/community/p34326777.

Problem statement

Fix positive integers k and d. Prove that for all sufficiently large odd positive integers n, the digits of the base-$2n$ representation of n^k are all greater than d.

The problem actually doesn't have much to do with digits: the idea is to pick any length $\ell \le k$, and look at the rightmost ℓ digits of n^k; that is, the remainder upon division by $(2n)^\ell$. We compute it exactly:

Claim — Let $n \ge 1$ be an odd integer, and $k \ge \ell \ge 1$ integers. Then

$$n^k \bmod (2n)^i = c(k, \ell) \cdot n^i$$

for some odd integer $1 \le c(k, \ell) \le 2^\ell - 1$.

Proof. This follows directly by the Chinese remainder theorem, with $c(k, \ell)$ being the residue class of $n^{k-i} \pmod{2^\ell}$ (which makes sense because n was odd). □

In particular, for the ℓth digit from the right to be greater than d, it would be enough that

$$c(k, \ell) \cdot n^\ell \ge (d + 1) \cdot (2n)^{\ell-1}.$$

But this inequality holds whenever $n \ge (d + 1) \cdot 2^{\ell-1}$.

Putting this together by varying ℓ, we find that for all odd

$$n \ge (d + 1) \cdot 2^{k-1}$$

we have that

- n^k has k digits in base-$2n$; and
- for each $\ell = 1, \dots, k$, the ℓ^{th} digit from the right is at least $d + 1$

so the problem is solved.

Remark. Note it doesn't really matter that $c(k, i)$ is odd *per se*; we only need that $c(k, i) \ge 1$.

§1.2 USAMO 2025/2, proposed by Carl Schildkraut

Problem statement

Let $n > k \geq 1$ be integers. Let $P(x) \in \mathbb{R}[x]$ be a polynomial of degree n with no repeated roots and $P(0) \neq 0$. Suppose that for any real numbers $a_0, \dots, a_k$ such that the polynomial $a_k x^k + \dots + a_1 x + a_0$ divides $P(x)$, the product $a_0 a_1 \dots a_k$ is zero. Prove that $P(x)$ has a nonreal root.

By considering any $k+1$ of the roots of P, we may as well assume WLOG that $n = k+1$. Suppose that $P(x) = (x+r_1)\dots(x+r_n) \in \mathbb{R}[x]$ has $P(0) \neq 0$. Then the problem hypothesis is that each of the n polynomials (of degree $n-1$) given by

$$\begin{aligned} P_1(x) &= (x+r_2)(x+r_3)(x+r_4)\dots(x+r_n) \\ P_2(x) &= (x+r_1)(x+r_3)(x+r_4)\dots(x+r_n) \\ P_3(x) &= (x+r_1)(x+r_2)(x+r_4)\dots(x+r_n) \\ &\vdots \\ P_n(x) &= (x+r_1)(x+r_2)(x+r_3)\dots(x+r_{n-1}) \end{aligned}$$

has at least one coefficient equal to zero. (Explicitly, $P_i(x) = \frac{P(x)}{x+r_i}$.) We'll prove that at least one r_i is not real.

Obviously the leading and constant coefficients of each P_i are nonzero, and there are $n-2$ other coefficients to choose between. So by pigeonhole principle, we may assume, say, that P_1 and P_2 share the position of a zero coefficient, say the x^k one, for some $1 \leq k < n-1$.

Claim — If P_1 and P_2 both have x^k coefficient equal to zero, then the polynomial

$$Q(x) = (x+r_3)(x+r_4)\dots(x+r_n)$$

has two consecutive zero coefficients, namely $b_k = b_{k-1} = 0$.

Proof. Invoking Vieta formulas, suppose that

$$Q(x) = x^{n-2} + b_{n-3}x^{n-3} + \dots + b_0.$$

(And let $b_{n-2} = 1$.) Then the fact that the x^k coefficient of P_1 and P_2 are both zero means

$$r_1 b_k + b_{k-1} = r_2 b_k + b_{k-1} = 0$$

and hence that $b_k = b_{k-1} = 0$ (since the r_i are nonzero). □

To solve the problem, we use:

Lemma

If $F(x) \in \mathbb{R}[x]$ is a polynomial with two consecutive zero coefficients, it cannot have all distinct real roots.

Here are two possible proofs of the lemma I know (there are more).

First proof using Rolle's theorem. Say x^t and x^{t+1} coefficients of F are both zero.

Assume for contradiction all the roots of F are real and distinct. Then by Rolle's theorem, every higher-order derivative of F should have this property too. However, the tth order derivative of F has a double root of 0, contradiction. □

Second proof using Descartes rule of signs. The number of (nonzero) roots of F is bounded above by the number of sign changes of $F(x)$ (for the positive roots) and the number of sign changes of $F(-x)$ (for the negative roots). Now consider each pair of consecutive nonzero coefficients in F, say $\star x^i$ and $\star x^j$ for $i > j$.

- If $i - j = 1$, then this sign change will only count for one of $F(x)$ or $F(-x)$
- If $i - j \geq 2$, then the sign change could count towards both $F(x)$ or $F(-x)$ (i.e. counted twice), but also there is at least one zero coefficient between them.

Hence if b is the number of nonzero coefficients of F, and z is the number of *consecutive runs* of zero coefficients of F, then the number of real roots is bounded above by

$$1 \cdot (b - 1 - z) + 2 \cdot z = b - 1 + z \leq \deg F.$$

However, if F has *two* consecutive zero coefficients, then the inequality is strict. □

> **Remark.** The final claim has appeared before apparently in the HUST Team Selection Test for the Vietnamese Math Society's undergraduate olympiad; see https://aops.com/community/p33893374 for citation.

§1.3 USAMO 2025/3, proposed by Carl Schildkraut

Problem statement

Alice the architect and Bob the builder play a game. First, Alice chooses two points P and Q in the plane and a subset $\mathcal{S}$ of the plane, which are announced to Bob. Next, Bob marks infinitely many points in the plane, designating each a city. He may not place two cities within distance at most one unit of each other, and no three cities he places may be collinear. Finally, roads are constructed between the cities as follows: each pair A, B of cities is connected with a road along the line segment AB if and only if the following condition holds:

> For every city C distinct from A and B, there exists $R \in \mathcal{S}$ such that $\triangle PQR$ is directly similar to either $\triangle ABC$ or $\triangle BAC$.

Alice wins the game if (i) the resulting roads allow for travel between any pair of cities via a finite sequence of roads and (ii) no two roads cross. Otherwise, Bob wins. Determine, with proof, which player has a winning strategy.

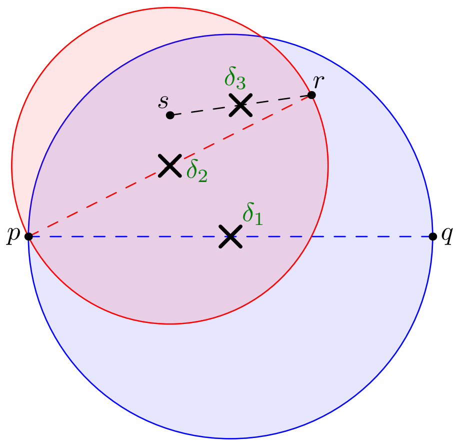
The answer is that Alice wins. Let's define a *Bob-set* V to be a set of points in the plane with no three collinear and with all distances at least 1. The point of the problem is to prove the following fact.

Claim — Given a Bob-set $V \subseteq \mathbb{R}^2$, consider the *Bob-graph* with vertex set V defined as follows: draw edge ab if and only if the disk with diameter $\overline{ab}$ contains no other points of V on or inside it. Then the Bob-graph is (i) connected, and (ii) planar.

Proving this claim shows that Alice wins since Alice can specify $\mathcal{S}$ to be the set of points outside the disk of diameter PQ.

Proof that every Bob-graph is connected. Assume for contradiction the graph is disconnected. Let p and q be two points in different connected components. Since pq is not an edge, there exists a third point r inside the disk with diameter $\overline{pq}$.

Hence, r is in a different connected component from at least one of p or q — let's say point p. Then we repeat the same argument on the disk with diameter $\overline{pr}$ to find a new point s, non-adjacent to either p or r. See the figure below, where the X'ed out dashed edges indicate points which are not only non-adjacent but in different connected components.



In this way we generate an infinite sequence of distances δ_1, δ_2, δ_3, ... among the non-edges in the picture above. By the "Pythagorean theorem" (or really the inequality for it), we have

$$\delta_i^2 \le \delta_{i-1}^2 - 1$$

and this eventually generates a contradiction for large i, since we get $0 \le \delta_i^2 \le \delta_1^2 - (i-1)$. □

Proof that every Bob-graph is planar. Assume for contradiction edges ac and bd meet, meaning $abcd$ is a convex quadrilateral. WLOG assume $\angle bad \ge 90^\circ$ (each quadrilateral has an angle at least 90°). Then the disk with diameter $\overline{bd}$ contains a, contradiction. □

Remark. In real life, the Bob-graph is actually called the Gabriel graph. Note that we never require the Bob-set to be infinite; the solution works unchanged for finite Bob-sets.

However, there are approaches that work for finite Bob-sets that don't work for infinite sets, such as the relative neighbor graph, in which one joins a and b iff there is no c such that $d(a,b) \le \max\{d(a,c), d(b,c)\}$. In other words, edges are blocked by triangles where ab is the longest edge (rather than by triangles where ab is the longest edge of a right or obtuse triangle as in the Gabriel graph).

The relative neighbor graph has fewer edges than the Gabriel graph, so it is planar too. When the Bob-set is finite, the relative distance graph is still connected. The same argument above works where the distances now satisfy

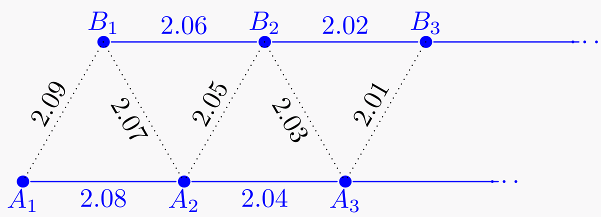
$$\delta_1 > \delta_2 > \dots$$

instead, and since there are finitely many distances one arrives at a contradiction.

However for infinite Bob-sets the descending condition is insufficient, and connectedness actually fails altogether. A counterexample (communicated to me by Carl Schildkraut) is to start by taking $A_n \approx (2n, 0)$ and $B_n \approx (2n+1, \sqrt{3})$ for all $n \ge 1$, then perturb all the points slightly so that

$$\begin{aligned} B_1A_1 &> A_1A_2 > A_2B_1 > B_1B_2 > B_2A_2 \\ &> A_2A_3 > A_3B_2 > B_2B_3 > B_3A_3 \\ &> \cdots. \end{aligned}$$

A cartoon of the graph is shown below.



In that case, $\{A_n\}$ and $\{B_n\}$ will be disconnected from each other: none of the edges A_nB_n or B_nA_{n+1} are formed. In this case the relative neighbor graph consists of the edges $A_1A_2A_3A_4\cdots$ and $B_1B_2B_3B_4\cdots$. That's why for the present problem, the inequality

$$\delta_i^2 \le \delta_{i-1}^2 - 1$$

plays such an important role, because it causes the (squared) distances to decrease appreciably enough to give the final contradiction.

§2 Solutions to Day 2

§2.1 USAMO 2025/4, proposed by Carl Schildkraut

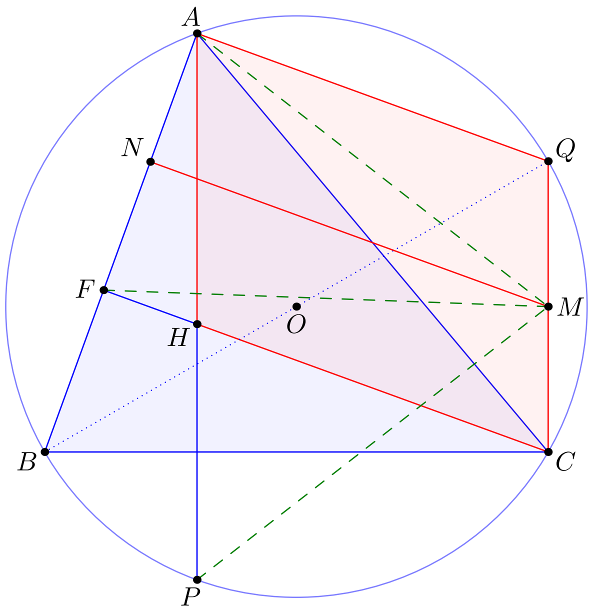
Problem statement

Let H be the orthocenter of an acute triangle ABC, let F be the foot of the altitude from C to AB, and let P be the reflection of H across BC. Suppose that the circumcircle of triangle AFP intersects line BC at two distinct points X and Y. Prove that $CX = CY$.

Let Q be the antipode of B.

Claim — $AHQC$ is a parallelogram, and $APCQ$ is an isosceles trapezoid.

Proof. As $\overline{AH} \perp \overline{BC} \perp \overline{CQ}$ and $\overline{CF} \perp \overline{AB} \perp \overline{AQ}$. □



Let M be the midpoint of $\overline{QC}$.

Claim — Point M is the circumcenter of $\triangle AFP$.

Proof. It's clear that $MA = MP$ from the isosceles trapezoid. As for $MA = MF$, let N denote the midpoint of $\overline{AF}$; then $\overline{MN}$ is a midline of the parallelogram, so $\overline{MN} \perp \overline{AF}$. □

Since $\overline{CM} \perp \overline{BC}$ and M is the center of (AFP), it follows $CX = CY$.

§2.2 USAMO 2025/5, proposed by John Berman

Available online at https://aops.com/community/p34335836.

Problem statement

Find all positive integers k such that: for every positive integer n, the sum

$$\binom{n}{0}^k + \binom{n}{1}^k + \dots + \binom{n}{n}^k$$

is divisible by $n+1$.

The answer is all even k.

Let's abbreviate $S(n) \coloneqq \binom{n}{0}^k + \dots + \binom{n}{n}^k$ for the sum in the problem.

¶ Proof that even k is necessary. Choose $n = 2$. We need $3 \mid S(2) = 2 + 2^k$, which requires k to be even.

> **Remark.** It's actually not much more difficult to just use $n = p - 1$ for prime p, since $\binom{p-1}{i} \equiv (-1)^i \pmod p$. Hence $S(p-1) \equiv 1 + (-1)^k + 1 + (-1)^k + \dots + 1 \pmod p$, and this also requires k to be even. This special case is instructive in figuring out the proof to follow.

¶ Proof that k is sufficient. From now on we treat k as fixed, and we let p^e be a prime fully dividing $n+1$. The basic idea is to reduce from $n+1$ to $(n+1)/p$ by an induction.

> **Remark.** Here is a concrete illustration that makes it clear what's going on. Let $p = 5$. When $n = p - 1 = 4$, we have
>
> $$S(4) = 1^k + 4^k + 6^k + 4^k + 1^k \equiv 1 + 1 + 1 + 1 + 1 \equiv 0 \pmod 5.$$
>
> When $n = p^2 - 1 = 24$, the 25 terms of $S(24)$ in order are, modulo 25,
>
> $$\begin{aligned} S(24) &\equiv 1^k + 1^k + 1^k + 1^k + 1^k \\ &\quad + 4^k + 4^k + 4^k + 4^k + 4^k \\ &\quad + 6^k + 6^k + 6^k + 6^k + 6^k \\ &\quad + 4^k + 4^k + 4^k + 4^k + 4^k \\ &\quad + 1^k + 1^k + 1^k + 1^k + 1^k \\ &= 5(1^k + 4^k + 6^k + 4^k + 1^k). \end{aligned}$$
>
> The point is that $S(24)$ has five copies of $S(4)$, modulo 25.

To make the pattern in the remark explicit, we prove the following lemma on each *individual* binomial coefficient.

Lemma 2.1

Suppose p^e is a prime power which fully divides $n+1$. Then

$$\binom{n}{i} \equiv \pm \binom{\frac{n+1}{p}-1}{\lfloor i/p \rfloor} \pmod{p^e}.$$

Proof of lemma. It's easiest to understand the proof by looking at the cases $\lfloor i/p \rfloor \in \{0,1,2\}$ first.

- For $0 \le i < p$, since $n \equiv -1 \mod p^e$, we have

$$\binom{n}{i} = \frac{n(n-1)\dots(n-i+1)}{1 \cdot 2 \cdot \dots \cdot i} \equiv \frac{(-1)(-2)\dots(-i)}{1 \cdot 2 \cdot \dots \cdot i} \equiv \pm 1 \pmod{p^e}.$$

- For $p \le i < 2p$ we have

$$\begin{aligned} \binom{n}{i} &\equiv \pm 1 \cdot \frac{n-p+1}{p} \cdot \frac{(n-p)(n-p-1)\dots(n-i+1)}{(p+1)(p+2)\dots i} \\ &\equiv \pm 1 \cdot \frac{\frac{n-p+1}{p}}{1} \cdot \pm 1 \\ &\equiv \pm \binom{\frac{n+1}{p}-1}{1} \pmod{p^e}. \end{aligned}$$

- For $2p \le i < 3p$ the analogous reasoning gives

$$\begin{aligned} \binom{n}{i} &\equiv \pm 1 \cdot \frac{n-p+1}{p} \cdot \pm 1 \cdot \frac{n-2p+1}{2p} \cdot \pm 1 \\ &\equiv \pm \frac{\left(\frac{n+1}{p}-1\right)\left(\frac{n+1}{p}-2\right)}{1 \cdot 2} \\ &\equiv \pm \binom{\frac{n+1}{p}-1}{2} \pmod{p^e}. \end{aligned}$$

And so on. The point is that in general, if we write

$$\binom{n}{i} = \prod_{1 \le j \le i} \frac{n-(j-1)}{j}$$

then the fractions for $p \nmid j$ are all $\pm 1 \pmod{p^e}$. So only considers those j with $p \mid j$; in that case one obtains the claimed $\binom{\frac{n+1}{p}-1}{\lfloor i/p \rfloor}$ exactly (even without having to take modulo p^e). □

From the lemma, it follows if p^e is a prime power which fully divides $n+1$, then

$$S(n) \equiv p \cdot S\left(\frac{n+1}{p}-1\right) \pmod{p^e}$$

by grouping the $n+1$ terms (for $0 \le i \le n$) into consecutive ranges of length p (by the value of $\lfloor i/p \rfloor$).

Remark. Actually, with the exact same proof (with better $\pm$ bookkeeping) one may show that

$$n+1 \mid \sum_{i=0}^{n} \left((-1)^i \binom{n}{i} \right)^k$$

holds for *all* nonnegative integers k, not just k even. So in some sense this result is more natural than the one in the problem statement.

§2.3 USAMO 2025/6, proposed by Cheng-Yin Chang and Hung-Hsun Yu

Available online at https://aops.com/community/p34335840.

Problem statement

Let m and n be positive integers with $m \geq n$. There are m cupcakes of different flavors arranged around a circle and n people who like cupcakes. Each person assigns a nonnegative real number score to each cupcake, depending on how much they like the cupcake. Suppose that for each person P, it is possible to partition the circle of m cupcakes into n groups of consecutive cupcakes so that the sum of P's scores of the cupcakes in each group is at least 1. Prove that it is possible to distribute the m cupcakes to the n people so that each person P receives cupcakes of total score at least 1 with respect to P.

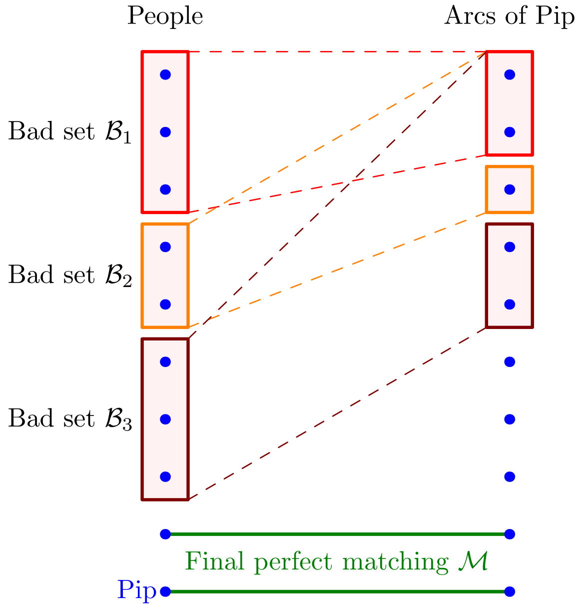
Arbitrarily pick any one person — call her Pip — and her n arcs. The initial idea is to try to apply Hall's marriage lemma to match the n people with Pip's arcs (such that each such person is happy with their matched arc). To that end, construct the obvious bipartite graph $\mathfrak{G}$ between the people and the arcs for Pip.

We now consider the following algorithm, which takes several steps.

- If a perfect matching of $\mathfrak{G}$ exists, we're done!
- We're probably not that lucky. Per Hall's condition, this means there is a *bad set* $\mathcal{B}_1$ of people, who are compatible with fewer than $|\mathcal{B}_1|$ of the arcs. Then delete $\mathcal{B}_1$ and the neighbors of $\mathcal{B}_1$, then try to find a matching on the remaining graph.
- If a matching exists now, terminate the algorithm. Otherwise, that means there's another bad set $\mathcal{B}_2$ for the remaining graph. We again delete $\mathcal{B}_2$ and the fewer than $\mathcal{B}_2$ neighbors.
- Repeat until some perfect matching $\mathcal{M}$ is possible in the remaining graph, i.e. there are no more bad sets (and then terminate once that occurs).

  Since Pip is a universal vertex, it's impossible to delete Pip, so the algorithm does indeed terminate with nonempty $\mathcal{M}$.

A cartoon of this picture is shown below.

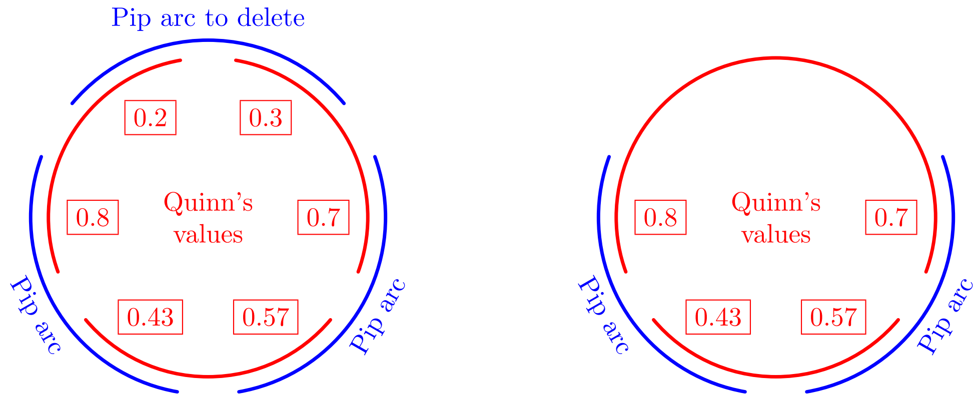


We commit to assigning each of person in $\mathcal{M}$ their matched arc (in particular if there are no bad sets at all, the problem is already solved). Now we finish the problem by induction on n (for the remaining people) by simply deleting the arcs used up by $\mathcal{M}$.

To see why this deletion-induction works, consider any particular person Quinn not in $\mathcal{M}$. By definition, Quinn is not happy with any of the arcs in $\mathcal{M}$. So when an arc $\mathcal{A}$ of $\mathcal{M}$ is deleted, it had value less than 1 for Quinn so in particular it couldn't contain entirely any of Quinn's arcs. Hence at most one endpoint among Quinn's arcs was in the deleted arc $\mathcal{A}$. When this happens, this causes two arcs of Quinn to merge, and the merged value is

$$(\geq 1) + (\geq 1) - (\leq 1) \qquad \geq \qquad 1$$

meaning the induction is OK. See below for a cartoon of the deletion, where Pip's arcs are drawn in blue while Quinn's arcs and scores are drawn in red (in this example $n = 3$).



> **Remark.** This deletion argument can be thought of in some special cases even before the realization of Hall, in the case where $\mathcal{M}$ has only one person (Pip). This amounts to saying that if one of Pip's arcs isn't liked by anybody, then that arc can be deleted and the induction carries through.

Remark. Conversely, it should be reasonable to expect Hall's theorem to be helpful even before finding the deletion argument. While working on this problem, one of the first things I said was:

> "We should let Hall do the heavy lifting for us: find a way to make n groups that satisfy Hall's condition, rather than an assignment of n groups to n people."

As a general heuristic, for any type of "compatible matching" problem, Hall's condition is usually the go-to tool. (It is much easier to verify Hall's condition than actually find the matching yourself.) Actually in most competition problems, if one realizes one is in a Hall setting, one is usually close to finishing the problem. This is a relatively rare example in which one needs an additional idea to go alongside Hall's theorem.