1. In which of the following Die Hard scenarios does Bruce survive? Justify your answer.

   (a) Target 14ℓ, jug capacities 35ℓ and 63ℓ.
   (b) Target 7ℓ, jug capacities 12ℓ, 18ℓ, and 30ℓ.
   (c) Target ½ℓ, jug capacities 8½ℓ and 14½ℓ.

Solution:

   (a) Since gcd(35, 63) = 7 divides the amount of water in each jug, Bruce survives.
   (b) Bruce dies. We will argue that the amount of water in each jug is a multiple of 6. The proof is essentially identical to the one we gave for Lemma 2 in Lecture 4. Initially, every jug is empty so the amount is a multiple of 6. This property is preserved by the pouring steps because not only is the amount in each jug is a multiple of 6, but so is the remaining capacity. Since every step completely fills a jug, completely empties a jug, or transfers an amount equal to the remaining capacity of one of the jugs, the amounts will be multiples of 6 after the transition. Since 7 is not a multiple of 6, Bruce must die.
   (c) We can change the measuring unit to ½ℓ. Bruce is targeting 2 units with jug capacities 33 units and 57 units. Since gcd(33, 57) = 3 and 3 does not divide 2, he dies.

2. Do the following graphs exist? If yes, give an example. If no, prove that it doesn’t.

   (a) A graph with 14 vertices of degree 3 and 3 vertices of degree 7.
   (b) A graph with 10 vertices of degree 2 and 2 vertices of degree 9.
   (c) A graph with 10 vertices of degree 4 and 9 vertices of degree 14.

Solution:

   (a) No. The sum of the prescribed degrees is 14 · 3 + 3 · 7 = 63, which is an odd number. This violates Lemma 1 from Lecture 5, which says that the sum of the degrees must equal twice the number of edges, and is therefore always an even number.
   (b) Yes. In the following diagram the vertices $a_1, \ldots, a_{10}$ have degree 2 and vertices $b_1, b_2$ have degree 9.

   (c) No. Let $A$ be the set of all vertices of degree 4, and $B$ be the set of all vertices of degree 14. Assume for contradiction that $|A| = 10$ and $|B| = 9$. On the one hand, the number of edges between vertices in $A$ and vertices in $B$ is at most $4 \cdot 10 = 40$. On the other hand, every vertex in $B$ has at least $14 - 8 = 6$ neighbors in $A$, so the number of edges between vertices in $B$ and vertices in $A$ is at least $6 \cdot 9 = 54$. We conclude that 40 is at least as large as 54, a contradiction.
3. A summer camp has children from Hong Kong, Shanghai, and Tokyo. The table entry in row $i$ and column $j$ gives the average number of friends from city $j$ that children from city $i$ report to have. Find the missing entry. Justify your answer.

<table>
<thead>
<tr>
<th></th>
<th>H</th>
<th>S</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>2</td>
<td>?</td>
<td>4</td>
</tr>
<tr>
<td>S</td>
<td>3</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>T</td>
<td>6</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

Solution: Let $x$ be the missing number and let $H$, $M$, and $T$ be the sets of Hong Kong, Mumbai, and Tokyo children in the camp. If we look at the bipartite graph of friendships between sets $H$ and $T$, by the handshaking lemma from Lecture 5 we get that $6|T| = 4|H|$ (both are equal to the total number of edges between $H$ and $T$). By the same reasoning applied to the other two pairs we get that $|S| = 2|T|$ and $|H| = 3|S|$. Multiplying both sides of these equations we obtain that $6|T| |S| |H| = 4|H| 2|T| 3|S|$, from where $x = 4 \cdot 2 \cdot 3 / 6 = 4$.

4. Calculate the following numbers in modular arithmetic. Justify your answers.

(a) What is $9^{-1}$ (mod 23)?

(b) Suppose $5x + 7y \equiv 17 \pmod{19}$ and $4x + 11y \equiv 13 \pmod{19}$. What are $x$ and $y$?

(c) What is $1^1 + 2^2 + \cdots + 99^{99}$ (mod 3)?

Solution:

(a) We look for integers $s$ and $t$ such that $9s + 23t = 1$. A run of extended Euclid’s algorithm gives the solution $s = -5$ and $t = 2$, so $9^{-1} \pmod{23} = -5 \pmod{23} = 18$.

(b) We want to eliminate one of the variables, say $x$. We can do this systematically by multiplying the two equations by the multiplicative inverses of 4 and 5 and then subtracting both sides. This gives

$$5 \cdot 11y - 4 \cdot 7y \equiv 5 \cdot 13 - 4 \cdot 17 \pmod{19},$$

which, after simplifying, is the same as $27y \equiv -3 \pmod{19}$, or $8y \equiv 16 \pmod{19}$. We can now look for the multiplicative inverse of 8 and so on, but in this case we are lucky because $8 \cdot 2 = 16$, so $y$ must equal 2. Plugging $y$ into the first equation, we get that $5x \equiv 17 - 7 \cdot 2 \equiv 3 \pmod{19}$. The multiplicative inverse of 5 is 4, so we get that $x \equiv 3 \cdot 4 \equiv 12 \pmod{19}$, so the solution is $x = 12$, $y = 2$.

(c) We can write

$$1^1 + 2^2 + 3^3 + 4^4 + 5^5 + \cdots + 99^{99} \equiv 1^1 + (-1)^2 + 0^3 + 1^4 + (-1)^5 + 0^6 + \cdots + 0^{99} \pmod{3}$$

by the rule for multiplying modular equations. This expression has 33 values of the form $0^n$ all of which equal zero and 33 values of the form $1^n$ all of which equal one so their sum modulo 3 is congruent to zero. What remains is

$$(-1)^2 + (-1)^5 + \cdots + (-1)^{98} \pmod{3}$$

Since the powers of $-1$ alternate between even and odd, this expression is congruent to $1 + (-1) + 1 + (-1) + \cdots + 1 \pmod{3}$

which evaluates to 1 modulo 3.
5. Which of the following graphs $G = (V, E)$ has a perfect matching? If a graph has a perfect matching, describe it. If not, prove that a perfect matching does not exist.

(a) The vertices are the squares of a 9 by 9 chessboard with the top left corner removed. The edges are pairs of vertices that are adjacent along a row or column.

(b) Same as part (a), but now the chessboard is 10 by 10, and both the top left and bottom right corners are removed.

(c) The vertices are all integers between 53 and 97 inclusively. The edges are those $\{x, y\}$ for which $3x + 4y > 500$.

(d) The vertices are all integers between $-23$ and 23 inclusively except for 0. The edges are those $\{x, y\}$ for which $-144 \leq x \cdot y < 0$.

**Solution:**

(a) Yes. In the first row, 2st, 4rd, 6th and 8th squares are matched with 3nd, 5th, 7th and 9th squares. In the other rows, 2st, 4rd, 6th and 8th row’s squares are matched with 3nd, 5th, 7th and 9th row’s squares, respectively.

(b) No. Let $B$ and $W$ be the black and white squares of the chessboard. The graph is bipartite with partition $(B, W)$. The squares that were removed were both black so $|B| = 48$ and $|W| = 50$. Therefore not all vertices in $W$ can be matched.

(c) A perfect matching does not exist because there are $97 - 53 + 1 = 45$ vertices, which is an odd number.

(d) The edges $\{\{n - 24, n\} : 1 \leq n \leq 23\}$ form a perfect matching of this graph. For every $1 \leq n \leq 23$, since $n - 24 < 0$ and $n > 0$, we have $n(n - 24) < 0$. Since $n(n - 24) = n^2 - 24n = (n - 12)^2 - 144 \geq -144$, all edges are present.

6. Consider the following procedure:

**Procedure P:**

input: $k$ positive integers $a_1, a_2, \ldots, a_k$.

1. Assign the value $a_i$ to variable $x_i$ for all $i$ between 1 and $k$.
2. While there exists a pair $x_i < x_j$ such that $x_i$ does not divide $x_j$:
   - Replace $x_i$ and $x_j$ by $\gcd(x_i, x_j)$ and $x_i \cdot x_j / \gcd(x_i, x_j)$, respectively.
3. Output the largest number among $x_1, x_2, \ldots, x_k$.

(a) What are the possible outputs of $P(6, 10, 15)$? (The output might depend on the choice of $x_i$ and $x_j$ in step 2.)

(b) Show that the output of $P$ must divide the product $a_1a_2\cdots a_k$ by formulating and proving a suitable invariant.

(c) Show that for positive $a, b, c$, if $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$ then $\gcd(ab, c) = 1$.
   
   **(Hint:** Use the connection between gcds and integer combinations.)

(d) Use part (c) to show that if $\gcd(a_i, a_j) = 1$ for all $i \neq j$ then the output of $P$ must equal $a_1a_2\cdots a_k$.

(e) Show that the output of $P$ cannot equal $a_1a_2\cdots a_k$ unless $\gcd(a_i, a_j) = 1$ for all $i \neq j$.

(f) **(Extra credit)** Show that $P$ always terminates.

**Solution:**
(a) Initially, \((x_1, x_2, x_3) = (6, 10, 15)\). At step 2, we can choose \((x_i, x_j) = (6, 10)\), \((x_i, x_j) = (6, 15)\), or \((x_i, x_j) = (10, 15)\).

**Case 1:** Assume \((6, 10)\) is chosen. After step 3, \((x_1, x_2, x_3) = (2, 30, 15)\). Back to step 2, we can only choose \((x_i, x_j) = (2, 15)\). So, we have \((x_1, x_2, x_3) = (1, 30, 30)\). Then, \(P\) outputs 30.

**Case 2:** Assume \((6, 15)\) is chosen. After step 3, \((x_1, x_2, x_3) = (3, 10, 30)\). Back to step 2, we can only choose \((x_i, x_j) = (3, 10)\). So, we have \((x_1, x_2, x_3) = (1, 30, 30)\). Then, \(P\) outputs 30.

**Case 3:** Assume \((10, 15)\) is chosen. After step 3, \((x_1, x_2, x_3) = (6, 5, 30)\). Back to step 2, we can only choose \((x_i, x_j) = (5, 6)\). So, we have \((x_1, x_2, x_3) = (30, 1, 30)\). Then, \(P\) outputs 30.

(b) We show that the predicate \(x_1 x_2 \cdots x_k = a_1 a_2 \cdots a_k\) is an invariant. Initially, \(x_i = a_i\) for all \(i\), so \(x_1 x_2 \cdots x_k = a_1 a_2 \cdots a_k\). Now suppose that \(x_1 x_2 \cdots x_k = a_1 a_2 \cdots a_k\) before a transition. After the transition, \(x_i\) and \(x_j\) are replaced by \(\gcd(x_i, x_j)\) and \(x_i \cdot x_j / \gcd(x_i, x_j)\), so the product \(x_1 x_2 \cdots x_k\) stays the same.

In particular, the largest number among \(x_1, x_2, \ldots, x_k\) must divide the product \(a_1 \cdots a_k\), so the output of \(P\) divides \(a_1 a_2 \cdots a_k\).

(c) Assume \(\gcd(a, c) = 1\) and \(\gcd(b, c) = 1\). Then, \(ap + cq = 1\) and \(br + cs = 1\) for some integers \(p, q, r, s\). We can write

\[
(ap)(br) = (1 - cq)(1 - cs) = 1 + c(-q - s + csq).
\]

So \(1 = ab(pr) + c(q + s - csq)\) is an integer combination of \(ab\) and \(c\). By Lemma 3 from Lecture 4, \(\gcd(ab, c)\) divides 1, so it must equal 1.

(d) We show that under this assumption \(\gcd(x_i, x_j) = 1\) for all \(i \neq j\) is an invariant. It is true initially by the assumption on the \(a_i\)'s. Assume it is true before a transition and the transition replaces \(x_i, x_j\) by \(x_i', x_j'\). Since \(\gcd(x_i, x_j) = 1\) we must have \(x_i' = 1\) and \(x_j' = x_i x_j\) and so \(\gcd(x_i', x_j') = 1\). For every \(k\) other than \(i\) and \(j\), \(\gcd(x_k, x_i') = \gcd(x_k, x_j') = 1\), and \(\gcd(x_k, x_j') = \gcd(x_k, x_i x_j) = 1\) by part (c). It follows that all pairwise \(\gcd's\) are equal to one after the transition.

As long as at least there exists a pair \(x_i > 1\) and \(x_j > 1\), \(P\) cannot terminate because \(\gcd(x_i, x_j) = 1\) so they do not divide one another. Therefore at termination at most one of the \(x_i\)'s can be greater than one. By part (b) this \(x_i\) must equal \(a_1 a_2 \cdots a_k\).

(e) We show that under this assumption \(\gcd(x_i, x_j) > 1\) for some pair \(i \neq j\)" is an invariant. It is initially true by assumption. Assume that \(\gcd(x_i, x_j) > 1\) before a transition. The transition replaces \(x_m, x_n\) by \(x_m', x_n'\) for some \(m, n\). We consider three cases. If \(m, n\) are both distinct from \(i, j\) then the invariant is clearly preserved. If \(\gcd(x_m, x_n) > 1\) then \(\gcd(x_m, x_n)\) divides \(\gcd(x_m', x_n')\), so \(\gcd(x_m', x_n') > 1\) and the invariant is preserved again.

Otherwise, \(\gcd(x_m, x_n) = 1\) but \(m, n\) are not both distinct from \(i, j\). We may assume that \(m = i\) and \(n\) is distinct from both \(i\) and \(j\). Then \(\gcd(x_m', x_j) = \gcd(x_i x_n, x_j) > 1\). It follows that the invariant is preserved in all cases.

It follows from the invariant that \(x_i > 1\) and \(x_j > 1\) must hold for at least two distinct \(i, j\) throughout the execution. Because \(x_1 x_2 \cdots x_k = a_1 a_2 \cdots a_k\), no single \(x_i\) can ever equal \(a_1 a_2 \cdots a_k\) and this output is impossible to obtain.

(f) We show that \(x_1 + \cdots + x_k\) increases in every transition. Since \(x_1 \cdots x_k = a_1 \cdots a_k\), \(x_1 + \cdots + x_k\) is bounded by \(ka_1 \cdots a_k\) and \(P\) must terminate in this many steps.

When in step 3 \(x_i\) and \(x_j\) are replaced by \(g\) and \(x_i x_j / g\), where \(g = \gcd(x_i, x_j)\), the inequality

\[
\frac{1}{g} (x_i - g)(x_j - g) > 0
\]
must be satisfied: The left-hand side is always non-negative, and it can only be zero when $g = x_i$ or $g = x_j$, namely when $x_i$ divides $x_j$. We can rewrite this inequality as

$$g + \frac{x_i x_j}{g} > x_i + x_j$$

and so the sum of the $x_i$ increases.
1. The vertices are the integers from 0 to 1023, and \( \{u, v\} \) is an edge if \( \log_2|u - v| \) is an integer.

2. The vertices are the integers from 1 to 100, and \( \{u, v\} \) is an edge if and only if \( u \) is the largest number less than \( v \) that divides \( v \). This is the part induced by vertices 1 to 10:

![Graph Diagram]

3. The vertices are four-symbol strings \( x_1x_2x_3x_4 \), where each \( x_i \) is 0, 1, 2, 3, or 4. The pair \( \{x_1x_2x_3x_4, y_1y_2y_3y_4\} \) is an edge if and only if for every \( i \), \( x_i - y_i \) is 0, 1, or 4 modulo 5.

Describe your solution clearly. Explain how it compares to the best possible. If you used a computer program to calculate the vertex cover explain how it works.

Solution:

1. The set of all numbers between 0 and 1023 that are not divisible by 3. There are 682 of them.

   This is a vertex cover because if \( u \) and \( v \) are not in the set, \( |u - v| \) is a multiple of 3 so \( \{u, v\} \) cannot be an edge.

   We argue this is the best possible. Consider the 341 disjoint subsets of vertices \( \{0, 1, 2\} \), \( \{3, 4, 5\} \), up to \( \{1020, 1021, 1022\} \). Each of these subsets \( \{x, y, z\} \) is a triangle; namely, \( \{x, y\} \), \( \{y, z\} \), and \( \{x, z\} \) are all edges in the graph. Since the vertex cover must cover all three, it must contain at least two vertices per subset, for a total of \( 2 \cdot 341 = 682 \) vertices.

   The complement of a vertex cover is called an independent set: For any two vertices \( x, y \) in the independent set there must not be an edge between \( x \) and \( y \).

2. We describe a recursive procedure that calculates the smallest possible vertex cover of a tree. We designate a special vertex \( r \) as the root. We calculate two vertex covers: A minimum vertex cover and a minimum vertex cover that must include \( r \). If \( r \) has no neighbors (it is a leaf) these are the sets \( \emptyset \) and \( \{r\} \), respectively. Otherwise, we remove \( r \) and its outgoing edges to \( v_1, \ldots, v_d \) and recursively calculate the two vertex covers for the remaining \( d \) components, with the \( i \)-th component being rooted at \( v_i \). The minimum vertex cover that includes \( r \) is the union of the minima for all the components plus \( r \) itself. The minimum vertex cover that does not include \( r \) is the union of all the covers of the components that do include their respective roots. The minimum vertex cover is the smaller one of these two, breaking ties arbitrarily.

   Implementing this procedure gives the cover

   \[
   1 \ 4 \ 6 \ 9 \ 10 \ 11 \ 13 \ 14 \ 15 \ 16 \ 17 \ 19 \ 21 \ 24 \ 25 \ 27 \ 29 \ 31 \ 33 \ 35 \ 36 \ 40 \ 44 \ 46 \ 49 \ 52 \\
   56 \ 60 \ 64 \ 68 \ 69 \ 74 \ 76 \ 78 \ 82 \ 84 \ 86 \ 90 \ 94 \ 96 \ 100
   \]

   of size 41.
3. It is easier to describe the complement set $\overline{C}$:

$$ \overline{C} = \{ x_1x_2x_3x_4 : x_1x_2 \in P \text{ and } x_3x_4 \in S \} $$

where $P = \{00, 12, 24, 31, 42\}$.

The set $C$ has size $5^4 - 5^2 = 600$. We argue that $\overline{C}$ is an independent set (so all edges must involve some vertex in $C$). Let $x = x_1x_2x_3x_4$ and $y = y_1y_2y_3y_4$ be any distinct pair of vertices in $\overline{C}$. Then $x_1x_2$ must be distinct from $y_1y_2$, or else $x_3x_4$ is distinct from $y_3y_4$. Without loss of generality, let us assume the first case holds. By the definition of $P$, $x_2 \equiv 2x_1 \pmod{5}$ and $y_2 \equiv 2y_1 \pmod{5}$. Therefore $(x_2 - x_1) \equiv 2(y_1 - x_1) \pmod{5}$. This rules out $y_1 - x_1 \equiv 0 \pmod{5}$ because then $x_1y_1$ and $x_2y_2$ are identical. If $y_1 - x_1$ is 1 or 4 modulo 5, then $y_2 - x_2$ is 2 or 3 modulo 5, so there is no edge between $x$ and $y$.

It turns out that there is no independent set of size 26, so there can be no vertex cover of size 599 (or less). To find out why, keep reading.

Reliable communication*

Let’s consider the following communication scenario. Alice wants to send a message to Bob who lives some distance apart. There are five possible messages, which we represent by the numbers 0, 1, 2, 3, and 4. They both have access to some global clock which ticks in one-second intervals. Alice and Bob agree on the following protocol: To send message $x$, send a signal at time $x/5$ after the next clock tick. So message 0 would be sent at the time of a clock tick, message 1 at an offset of 0.2 seconds after a clock tick, and so on.

This system would work wonders in a flawless world. In the real world, communication may be disrupted by various sources of noise owing to imprecisions in the equipment, imperfect coordination, and so on. Even though Alice intends to emit her signal at 0.2 seconds past the clock tick, it may end up going out say at the 0.24th second, get delayed and Bob may register receiving it at time 0.32 and incorrectly deduce that Alice had sent him a 2 instead of a 1.

This is an example of a noisy communication channel. Graphs provide one possible model of noisy communication: The vertices represent the possible signals that Alice can send — called codewords in coding theory — and edges describe possible corruptions. The following graph $G$ may be a reasonable model of the above scenario:

![Diagram of a graph](image)

For example, the channel may corrupt codeword 1 into a 0 or a 2 but not into a 3 or a 4. If Alice wants to ensure that Bob detects possible errors in the transmission reliably, then they are limited to not five but two possible messages, for instance using the codewords 0 and 2 to represent them. Bob is then assured to receive the message that was intended for him, or else detect a corruption in transmission (in case he receives a 1, a 3, or a 4). Should they try to pack three codewords there will always be a possibility of erroneous reception, as two out of these three codewords will be represented by an edge in $G$. 
Now suppose Alice and Bob upgrade their communication equipment so that Alice can send two different signals to Bob, perhaps by using two copies of the same device tuned at different frequencies. The codewords can now be described as pairs of numbers \(x_1,x_2\), with \(x_1, x_2\) each taking values 0, 1, 2, 3, or 4, giving a total of 25 possibilities. How should we model the corruptions? In this scenario, it may be reasonable to assume that the corruptions are “independent” of one another, so for example codeword 12 may be corrupted to any one of the following possibilities: 01, 02, 03, 11, 13, 21, 22, 23. The model graph \(G^2\) has vertices \(x_1x_2\) for all \(x_1, x_2\) in 0, 1, 2, 3, 4 and edges \(\{x_1x_2, y_1y_2\}\) if and only if \(y_1 - x_1\) and \(y_2 - x_2\) are both congruent to 0, 1, or \(-1\) modulo 5. This is beginning to look familiar:

In this diagram, the right side wraps back to the left and the top one to the bottom.

Alice and Bob can achieve reliable communication if they apply both devices independently. Namely, Alice sends signal 0 or a 2 on device 1 and signal 0 or 2 on device 2 separately. This results in four codewords: 00, 02, 20, and 22. Reliability is captured by the fact that vertices 00, 02, 20, and 22 form an independent set in the graph \(G^2\). If Alice and Bob want to communicate more messages with the same equipment, they should look for a larger independent set in \(G^2\). The graph \(G^2\) has, in fact, an independent set of size 5 consisting of the vertices 00, 12, 24, 31, and 43:

If Alice and Bob now use four devices instead of two, they can achieve an even greater advantage by pairing up the devices and using this protocol separately on each pair. The number of possible codewords for reliable communication is then \(5^2 = 25\). If they used each of the four devices independently, the best they can do is \(2^4 = 16\) codewords. This is a fairly significant gain. Can they do even better? It turns out that the answer is no.

**Theorem.** The graph \(G^4\) does not have an independent set of size larger than 25.
Here, $G^4$ is the graph from part 3(c) of the mini-project, which models exactly the communication problem we are interested in.

The proof of this theorem is extremely ingenious. To warm up towards it, let us reprove something that we already know: That the graph $G$ itself does not have any independent set of size larger than $\sqrt{5}$.

**A detour into geometry** To show this we need to recall some facts from geometry of 3-dimensional space. An orthonormal basis of this space consists of three vectors $b_1$, $b_2$, $b_3$ of unit length that are mutually orthogonal:

$$
\|b_1\|^2 = \|b_2\|^2 = \|b_3\|^2 = 1 \quad \text{and} \quad b_1 \cdot b_2 = b_1 \cdot b_3 = b_2 \cdot b_3 = 0.
$$

Here, $v \cdot w$ is the dot product of $v$ and $w$ and $\|v\| = \sqrt{v \cdot v}$ is the length of $v$. One example of an orthonormal basis are the vectors $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$, but there are many others. If $b_1$, $b_2$, and $b_3$ form an orthonormal basis, then the length of any vector can be calculated using Pythagoras’ theorem:

$$
\|v\|^2 = (v \cdot b_1)^2 + (v \cdot b_2)^2 + (v \cdot b_3)^2.
$$

For the basis $e_1, e_2, e_3$, this equation restates the familiar fact that the square length of the vector is the sum of the squares of its coordinates. Since changes of orthonormal basis preserve lengths (in mathematics, such transformations are called *isometries*), the same relation holds with respect to any orthonormal basis.

We are now ready to explain why $G$ does not have independent sets of size larger than $\sqrt{5}$. To do this, we represent each vertex $x$ of $G$ by a unit length vector $x$ in 3-dimensional space as in the following diagram.

![Diagram](image)

This diagram looks like a five-pronged umbrella whose handle points in the direction $e_1 = (1, 0, 0)$. The umbrella is opened just the right amount so that the pair of vectors $\{0, 2\}$ becomes orthogonal, i.e. $0 \cdot 2 = 0$. By symmetry, the pairs $\{1, 3\}$, $\{2, 4\}$, $\{3, 0\}$, and $\{4, 1\}$ will also be orthogonal. So every pair of vertices that do not form an edge are represented by an orthogonal pair of vectors.

The dot product $x \cdot e_1$ (which is the same for all vertices $x$) determines the opening angle of the umbrella. Some elementary but tedious geometric calculation shows that the orthogonality requirement is satisfied precisely when $x \cdot e_1 = 1/\sqrt{5}$.

Now comes the proof. Suppose, for contradiction, that $G$ contained an independent set $\{x, y, z\}$ of size 3. Then the vectors $x, y, z$ form an orthonormal basis of 3-dimensional space. By Pythagoras’ theorem, we can calculate the length of $e_1 = (1, 0, 0)$ in this basis as

$$
\|e_1\|^2 = (e_1 \cdot x)^2 + (e_1 \cdot y)^2 + (e_1 \cdot z)^2 = \frac{1}{\sqrt{5}} + \frac{1}{\sqrt{5}} + \frac{1}{\sqrt{5}} = \frac{3}{\sqrt{5}}
$$
which is impossible as we know that $e_1$ has length 1!

So far we have given a complicated proof of the simple fact that $G$ does not have an independent set of size 3. The power of this proof technique becomes apparent when we work with the graph $G^2$. To apply it, we need to come up with a unit vector representation of the 25 vertices of $G^2$ with similar requirements (pairs that are not edges are orthogonal, and the first coordinate of every vector is small).

Such a representation is tricky to construct from scratch. Fortunately, we can use the representation of $G$ to construct one for $G^2$. Recall that each vertex $x_1x_2$ in $G^2$ describes a pair of vertices $x_1, x_2$ of $G$. The vertex $x_1x_2$ will be represented by the tensor product of the vectors $x_1$ and $x_2$, which is denoted by $x_1 \otimes x_2$. The tensor product of two 3-dimensional vectors is a 9-dimensional vector calculated by the following rule

$$(a, b, c) \otimes (a', b', c') = (aa', ab', ac', ba', bb', bc', ca', cb', cc').$$

Tensor products and dot products are very nice to one another. The dot product of tensor products is the scalar product of the dot products (try saying this quickly)

$$(x_1 \otimes x_2) \cdot (y_1 \otimes y_2) = (x_1 \cdot y_1)(x_2 \cdot y_2).$$

This formula ensures that the vectors representing $G^2$ inherit the desired properties, in particular:

- The vectors $x_1 \otimes x_2$ representing the vertices of $G^2$ are of unit length because

$$\|x_1 \otimes x_2\|^2 = (x_1 \otimes x_2) \cdot (x_1 \otimes x_2) = (x_1 \cdot x_1)(x_2 \cdot x_2) = \|x_1\|^2\|x_2\|^2 = 1.$$

- If $\{x_1x_2, y_1y_2\}$ is not an edge in $G^2$ then $(x_1 \otimes x_2) \cdot (y_1 \otimes y_2) = 0$ because at least one of the pairs $\{x_1, y_1\}$ or $\{x_2, y_2\}$ is not an edge of $G$ so at least one of the dot products $x_1 \cdot y_1$, $x_2 \cdot y_2$ must be zero.

- The first coordinate of $x_1 \otimes x_2$ equals $(1/\sqrt{5})^2 = 1/\sqrt{5}$ for all representatives.

We can now use the same strategy to argue that $G^2$ has no independent set of size 6. If such a set existed then there would be six distinct vertex representatives that are orthonormal to one another. The dot product of the vector $e_1 = (1, 0, 0, 0, 0, 0, 0, 0, 0)$ with each of these representatives is $1/\sqrt{5}$. By Pythagoras’ theorem it follows that the square length of $e_1$ must be at least $6 \cdot (1/\sqrt{5})^2 = 1.2$, which is a contradiction.

More generally, by taking $n$ tensor products, this reasoning extends to show that for every positive integer $n$, the graph $G^n$ cannot have independent sets of size larger than $\sqrt{5}^n$. In particular $G^4$ cannot have an independent set of size larger than 25. This was discovered by Laszlo Lovasz in 1979.