CCS Discrete III	Professor: Padraic Bartlett
Lecture 1: Electrical Netwo	rks and Random Walks
Weeks 1-2	UCSB 2015

(Relevant source material: Doyle and Snell's "Random walks and electrical networks," which is available online here! Also, sections of Bollobas's text on Modern Graph Theory, various articles I've read, and probably other random things.)

Consider the following problem:

Problem. (The Drunkard's Walk.) Assume, for a moment, that we are modeling a drunkard's very simplified map of the universe:



There are in this world four possible locations: H, the drunkard's home, B, an all-devouring black hole that absorbs everything that accidentally wanders into it, and two intermediate locations x and y. A drunkard, left to its own devices, will randomly wander between these locations. Specifically: if it is at some vertex that is neither H nor B at time t, at time t+1it will choose via coinflip one of the neighboring vertices to its current location and wander there. If the drunkard ever makes it home (i.e. wanders to H,) it is safe and goes merrily to sleep. If it wanders to B, it is sucked into the black hole and never will be seen again.

Suppose the drunkard starts at x. What are the drunkard's chances of making it home? How can we model these kinds of behaviors?

1 Random Walks

For a model as simple as this one, it's remarkably simple to determine what happens! Specifically, let's consider the drunkard's chances of making it home starting from **any** vertex v, not just x: for notational convenience, denote this probability as p(v). What do we know about these values?

- p(H) = 1: if the drunkard starts at home, it's happy and safe!
- p(B) = 0: if we've accidentally left the drunkard inside of the black hole, we're not going to see it anytime soon.
- For $v \neq H, B$, we have $p(x) = \frac{1}{2}p(H) + \frac{1}{2}p(y)$, and $p(y) = \frac{1}{2}p(x) + \frac{1}{2}p(B)$. This is because a drunkard at any vertex that's neither home or the black hole will choose between the two neighbors available to it with the same probability (1/2), and then travel to that respective vertex via that edge. So, its chances of survival are $\frac{1}{2}$ its chances at the vertex to its left, plus $\frac{1}{2}$ its chances at the vertex to its right.

This gives us the following four linear equations in four unknowns:

- p(B) = 0, p(H) = 1,
- $p(x) = \frac{p(H) + p(y)}{2}$, $p(y) = \frac{p(x) + p(B)}{2}$,

Solving this system tells you that $p(y) = \frac{1}{3}$, $p(x) = \frac{2}{3}$, and thus that our specific drunkard at vertex x has a 2/3rds chance of making it home.

Let's consider a trickier version of the above problem. Suppose that instead of just a four-vertex path, we have some graph G that we want to model a drunkard's walk on, with selected vertices H and B that denote the drunkard's home / a point of no return, respectively; this lets us model things like city blocks. Also, let's attach weights w_{xy} to every edge in our graph, that denote the likelihood that our drunkard will pick that edge over the other edges available to it; this lets us distinguish between things like clean, well-light main streets and sketchy alleyways.

Under this model, if we still let p(x) denote the probability that from x we make it to H before reaching B, we have the following system:

- p(H) = 1.
- p(B) = 0.
- For $x \neq H, B$, we have

$$p(x) = \sum_{y \in (\text{neighbors of } x)} p(y) \cdot \frac{w_{xy}}{w_x},$$

where w_x is the sum of all of the weights of edges leaving x:

$$w_x = \sum_{y \in (\text{neighbors of } x)} w_{xy}$$

This is because a drunkard at any vertex that's neither home or the black hole will choose between the neighbors available to it with probabilities weighted by the values w_{xy} : i.e. the probability that we travel to a neighbor y is just w_{xy}/w_x , the weight of the edge from x to y divided by the sum of the weights of all of the possible edges leaving x. Therefore, our probability p(x) of making it to home before the black hole is just the weighted average over all of x's neighbors of the same event!

To illustrate this idea, we calculate a second example:

Problem. (The Drunkard's Walk.) Consider the following second map for a drunkard's walk:



There are in this world six possible locations: H, the drunkard's home, B, a black hole, and four intermediate locations a, b, c, d, with weighted links between them as labeled. Suppose that a drunkard starts off at one of these four locations. How likely are they to make it to the vertex H before the vertex B?

As noted above, we can turn this into a system of six linear equations in six unknowns:

- p(B) = 0, p(H) = 1,
- $p(a) = \frac{1}{2}p(H) + \frac{1}{2}p(b),$ • $p(b) = \frac{1}{2}p(a) + \frac{1}{4}p(c) + \frac{1}{4}p(B),$
- $p(c) = \frac{1}{4}p(H) + \frac{1}{4}p(a) + \frac{1}{2}p(d),$ $p(d) = \frac{1}{2}p(c) + \frac{1}{2}p(B).$

Again, we can just solve these equations by your favorite method of dealing with systems of linear equations, to get

$$p(a) = \frac{12}{19}, p(b) = \frac{5}{19}, p(c) = \frac{8}{19}, p(d) = \frac{4}{19}$$

Excellent! We have a general method for solving a problem. Let's put that aside for a second and consider a second problem that might seem unrelated at first:

2 Electrical Networks

We're going to talk about electrical circuits and networks here for a bit! If you've never ran into the concepts of voltage, current, conductance, or resistance before, that's OK. For our purposes, define these concepts as follows:

- 1. Voltage is just some function $v: V(G) \to \mathbb{R}^+$ that assigns a positive number v(x) to each vertex x. In any circuit, we will have some vertex that is grounded; this vertex has v(ground) = 0. Similarly, we will declare that some source vertex has a potential difference of 1v from ground assigned to it: this vertex has v(source) = 1.
- 2. Current is just another function $i: V(G) \times V(G) \to \mathbb{R}$ that assigns a number to each "oriented edge" (x, y). We will usually denote the resistance of an edge as i_{xy} . We ask that $i_{xy} = -i_{yx}$, which is why we have the current pay attention to the orientation of edges: we want the flow of current in one direction on an edge to be -1· the flow of current in the opposite direction. We also ask that $i_{xy} = 0$ if $\{x, y\}$ is not an edge in E(G), as there is no "wire" present in our circuit to conduct a current directly from x to y.
- 3. Resistance is a function $V(G) \times V(G) \to \mathbb{R}^+ \cup \{\infty\}$ that assigns a positive number (measured in ohms, Ω) to each "unoriented edge" $\{x, y\} \in E(G)$. We denote this as R_{xy} for shorthand, and to enforce this "unoriented" notion we ask that $R_{xy} = R_{yx}$ for all x, y. We also ask that $R_{xy} = \infty$ for any x, y such that $\{x, y\} \notin E(G)$, as the resistance on a nonexistent wire is "infinite" (as nothing can pass through a nonexistent wire.)

- 4. The conductance of an edge $\{x, y\}$ as the reciprocal of its resistance: i.e. $C_{xy} = 1/R_{xy}$.
- 5. We define the conductance of a vertex x as the sum of the conductances of the edges leaving it: i.e. $C_x = \sum_{y \in N(x)} C_{xy}$.

We ask that these functions preserve the following two properties:

• (Ohm's law:) The current across an edge $\{x, y\}$ in the direction (x, y), i_{xy} , satisfies

$$i_{xy} = \frac{v(x) - v(y)}{R_{xy}},$$

where v(x), v(y) are the voltages at x, y and R_{xy} is the resistance of the edge $\{x, y\}$.

• (Kirchoff's law:) The sum of the currents into and out of any vertex other than the grounded vertex or the "source" vertex is zero: i.e. for any vertex neither grounded nor hooked up to power, we have

$$\sum_{y \in N(x)} i_{xy} = 0.$$

With these definitions made, the following problem is a fairly natural one to consider.

Problem. Suppose that we have an **electrical circuit**: i.e. a graph G with the following structure:

- The values R_{xy} have been defined for every edge.
- Some vertex G has been declared to be grounded, while another vertex S has been declared to be a "source" with a potential difference of 1v from ground.

Can we find v(x) for every vertex in our graph?

We start by considering basically the first graph we studied in this lecture, P_4 :



Specifically: we have taken the graph P_4 we studied in our first example of random walks, and turned it into a circuit as follows:

- 1. We replaced all of P_4 's edges with resistors of unit resistance 1.
- 2. We grounded the vertex G, and created a potential difference of 1v across the vertices G and S.

The decorations on the graph above denote this transformation: i.e. attaching a vertex to \pm denotes that it is the ground vertex, $\neg \Downarrow \vdash$ tells us that the vertex on the other side of this symbol from ground is a source vertex with a potential of some number of volts defined on it, $\neg W$ - tells us that an edge is a resistor with the labeled resistance, etc.

In this setup, what happens? Well: we have that v(G) = 0, v(S) = 1, and for any vertex v not G or S,

$$\sum_{y \in N(v)} i_{vy} = 0;$$

i.e. for vertex x, we have

$$0 = \sum_{y \in N(x)} i_{x,y} = i_{xS} + i_{xy} = \frac{v(x) - v(S)}{R_{xS}} + \frac{v(x) - v(y)}{R_{xy}}$$
$$= v(x) - v(S) + v(x) - v(y),$$

which implies that $v(x) = \frac{v(S)+v(y)}{2}$; similarly, we can derive that $v(y) = \frac{v(x)+v(G)}{2}$. In other words, to find the voltages at the vertices x, y we're solving the same equations we did for our drunkard's walk earlier: i.e. v(x) is 2/3, the probability that a drunkard walking on our graph starting from x will make it to vertex S before vertex G!

3 Electrons Are Drunks

Surprisingly, this property above – that our random walk and electrical network were, in some sense, the "same" – holds for all graphs! In the following lemmas, we make this idea concrete:

Lemma. Suppose that we have a connected graph G with edges weighted by some labeling w_{xy} . Define a **drunkard's walk** starting at a vertex x in our graph as the following process:

- Initially, the drunkard starts at x.
- Every minute, if a drunkard is at some vertex z, it randomly chooses one of the elements $y \in N(z)$ with probability given by the weights on its edges- i.e. each neighbor has probability w_{zy}/w_z of being picked and goes to that vertex.

Let a, b be a pair of distinguished vertices in our graph, and p(x) be the probability that a drunkard starting at the vertex x will make it to vertex b before vertex a.

Then p(x) and v(x) are both solutions to the same set of equations, if we turn our graph G into a electrical network with a connected to ground, a unit of electrical potential sent across a and b, and replace every edge $\{x, y\}$ of G with a resistor with conductance w_{xy} .

Proof. This is pretty much identical to what we just did. Specifically: we know from Ohm's law that

$$i_{xy} = \frac{v(x) - v(y)}{R_{xy}};$$

therefore, if we plug Ohm's law into Kirchoff's law, we have that whenever $x \neq a, b$, we have

$$\begin{split} \sum_{y \in N(x)} \frac{v(x) - v(y)}{R_{xy}} &= v(x) \cdot \left(\sum_{y \in N(x)} \frac{1}{R_{xy}}\right) - \sum_{y \in N(x)} \frac{v(y)}{R_{xy}} \\ \Rightarrow \qquad v(x) \cdot \left(\sum_{y \in N(x)} \frac{1}{R_{xy}}\right) &= \sum_{y \in N(x)} \frac{v(y)}{R_{xy}} \\ \Rightarrow \qquad v(x)C_x &= \sum_{y \in N(x)} C_{xy}v(y) \\ \Rightarrow \qquad v(x) &= \sum_{y \in N(x)} \frac{C_{xy}}{C_x}v(y). \end{split}$$

But what is $\frac{C_{xy}}{C_x}$? It's the probability that a drunkard starting at x chooses to travel to the vertex y, if we're picking neighbors of x with probabilities given by the C_{xy} 's! In this specific case, where all of our resistances are 1, this is just the chance that a drunkard at vertex x will go to y in our random walk.

But this is the exact same equation we're asking p(x) to satisfy: i.e. we want

$$p(x) = \sum_{y \in N(x)} (\text{chance drunkard goes from x to y}) \cdot p(y) = \sum_{y \in N(x)} \frac{w_{xy}}{w_x} \cdot p(y)$$

The only other restrictions we have on our voltage or random walk is that v(a) = p(a) = 0, v(b) = p(b) = 1: in other words, the equations that we're asking our voltage function to satisfy are the same that we're asking our probability function to satisfy!

We have just shown that p(x) and v(x) are both solutions to the same sets of linear equations. It might feel very tempting to simply conclude from here that p(x) must equal v(x); after all, they're both solving the same sets of equations!

This, however, is not a claim we can reasonably make. For example x = 1, y = 2 and x = 14, y = -11 are both solutions to the linear equation x + y = 3, and yet they are different! As well, it's not even clear that our system of linear equations has **any** solution: i.e. the equations x + y = 3, x - z = 4, y + z = 0 have no solutions, despite being three equations in three unknowns (check it if you don't see why!)

To conclude that they are equal, then, we just have to show that there is a unique solution to these equations!

We do this by first making the following two observations:

Observation. Take any system of linear equations of the form obtained from these random

walks on a connected graph¹; i.e. a collection of equations of the form

$$p(x) = \sum_{y \in N(x)} \frac{w_{xy}}{w_x} \cdot p(y),$$

where $w_x = \sum_{y \in N(x)} w_{xy}$, along with some boundary conditions $p(b_i) = c_i$. (In this sense, the "boundary" points are the values that we're given at the start of our system, while the rest of the points are the "interior" points whose values are determined by these weighted averages of their neighbors.)

Then the maximum and minimum values of p(x) must occur on these boundary points.

Proof. This is a fairly easy proof. Suppose instead that x is a point in the interior of our graph, and that p attains its maximum at x: i.e. that $p(x) \ge p(y)$ for all $y \in V(G)$. If we apply this observation to the equation

$$p(x) = \sum_{y \in N(x)} \frac{w_{xy}}{w_x} \cdot p(y),$$

we get

$$p(x) = \sum_{y \in N(x)} \frac{w_{xy}}{w_x} \cdot p(y) \le \sum_{y \in N(x)} \frac{w_{xy}}{w_x} \cdot p(x) = p(x).$$

The equality of the far-left- and far-right-hand-sides forces the intermediate terms to be equal: i.e. we must have p(y) = p(x), for every neighbor of x! Repeated applications of this argument will eventually give us that every vertex connected to x — i.e. every vertex in our graph, because our graph is connected — is equal to p(x). In particular, this means that our boundary points have values equal to p(x) as well.

An identical argument will show that having an interior point correspond to a minimum of p(x) will force all of our vertices to be equal to that minimum as well.

Observation. Again, take any system of linear equations of the form obtained from these random walks on a connected graph; i.e. a collection of interior equations of the form

$$p(x) = \sum_{y \in N(x)} \frac{w_{xy}}{w_x} \cdot p(y),$$

where $w_x = \sum_{y \in N(x)} w_{xy}$, along with some boundary conditions $p(b_i) = c_i$.

Suppose that p(x), q(x) are a pair of solutions to these equations. Then the mapping r(x) = p(x) - q(x) is a solution to the same set of interior equations, if we replace all of the original boundary conditions with the new requirements that $r(b_i) = 0$, for all boundary points b_i .

Proof. This is an even easier proof! Simply notice that if

$$p(x) = \sum_{y \in N(x)} \frac{w_{xy}}{w_x} \cdot p(y), \qquad q(x) = \sum_{y \in N(x)} \frac{w_{xy}}{w_x} \cdot q(y),$$

¹Finding a solution to this kind of a system is the process of solving a **Dirichlet problem**, if you want a formal name for reference in your reading.

we have

$$r(x) = p(x) - q(x) = \sum_{y \in N(x)} \frac{w_{xy}}{w_x} \cdot (p(y) - q(y)) = \sum_{y \in N(x)} \frac{w_{xy}}{w_x} \cdot r(y)$$

Also, if $p(b_i) = c_i, q(b_i) = c_i$, then we have $r(b_i) = c_i - c_i = 0$.

Given these two observations, we get the following corollary for free:

Corollary. If there is a solution to a system of linear equations of the form obtained from these random walks on a connected graph, it is unique.

Proof. Suppose we have two solutions p(x), q(x) to such a system of linear equations. By our second observation, their difference p(x) - q(x) is a solution to a system of linear equations where all of the boundary values are 0. By our first observation, the maximum and minimum of this p(x) - q(x) is attained on the boundary. But this means that the maximum and minimum of p(x) - q(x) is 0: i.e. that p(x) = q(x)!

So, this tells us that a solution is unique if it exists. To finish our proof, we just need to simply note that a solution can exist! This is also not too hard, if we come up with the appropriate bits of linear algebra!

We do this here, in the following (lengthy!) section:

4 Interlude: Linear Algebra

In earlier lectures, we defined a **vector space** as follows:

Definition. A vector space V over a field F is a set V along with the two operations addition and scalar multiplication, such that the following properties hold:

- Closure(+): $\forall \vec{v}, \vec{w} \in V$, we have $v + w \in V$.
- Identity(+): $\exists \vec{0} \in V$ such that $\forall \vec{v} \in V, \ \vec{0} + \vec{v} = \vec{v}$.
- Commutativity(+): $\forall \vec{v}, \vec{w} \in V, \vec{v} + \vec{w} = \vec{w} + \vec{v}.$
- Associativity(+): $\forall \vec{u}, \vec{v}, \vec{w} \in V, (\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w}).$
- Inverses(+): $\forall \vec{v} \in V, \exists \text{ some } \vec{v} \in V$ such that $\vec{v} + (-\vec{v}) = 0$.

- Closure(·): $\forall a \in F, \vec{v} \in V$, we have $a\vec{v} \in V$.
- Identity(·): $\forall \vec{v} \in V$, we have $1\vec{v} = \vec{v}$.
- Compatibility(·): $\forall a, b \in F$, we have $a(b\vec{v}) = (a \cdot b)\vec{v}$.
- **Distributivity** $(+, \cdot)$: $\forall a \in F, \vec{v}, \vec{w} \in V, a(\vec{v} + \vec{w}) = a\vec{v} + a\vec{w}.$

A subspace S of a vector space V is any subset of V that is a vector space in its own right, when given the same field F and addition/scalar multiplication operations that V has.

We gave several examples of vector spaces at the time — the set of all polynomials with real coefficients, the collection of all $n \times n$ matrices, F^n for any field F — but the main example I want for this class is \mathbb{R}^n , the collection of all ordered *n*-tuples of real numbers.

Given a vector space V, there are a number of useful concepts we can come up with to help study V. We start with the concepts of **linear dependence and independence** here:

4.1 Linear Dependence and Independence

Definition. Let V be a vector space over some field F. A linear combination of some set of vectors S is any sum of the form

$$a_1\vec{v_1} + a_2\vec{v_2} + \dots a_n\vec{v_n},$$

where $a_1, \ldots a_n$ are all elements of our field F, and $\vec{v_1}, \ldots \vec{v_n} \in S$.

In other words, a linear combination of some set of vectors is anything we can make by scaling and adding these vectors together.

A useful thing to study, given some set $\{\vec{v_1}, \ldots, \vec{v_n}\}$ of vectors, is the following: what can we make with these vectors? In other words, what is the collection of all **linear combinations** of these vectors?

This question is sufficiently common that we have a term for its related concept: the idea of **span**!

Definition. Given any collection of vectors A, the **span** of A, denoted span(A), is the collection of all linear combinations of elements of A. In other words,

$$span(A) = \{a_1 \vec{v_1} + a_2 \vec{v_2} + \dots + a_n \vec{v_n} | n \in \mathbb{N}, a_1 \dots + a_n \in \mathbb{R}, \vec{v_1}, \dots, \vec{v_n} \in A\}.$$

A genre of questions you'll often encounter in a linear algebra class is "Given some set A of vectors, what is their span? Is some other vector \vec{w} contained within this span?"

We give an example of a calculation here:

Question. You have been hired as a deep-sea navigator. Your first task is to pilot a submarine from our ship, anchored at (0,0,0) in the diagram below, to observe a whale at (12,6,-6). Your submarine has three engines on it. The first, when ran for a cycle, moves the submarine (2,1,0) units from its current location. The second, when ran for a cycle, moves the submarine (0,2,1) units from its current location. Finally, the third, when ran for a cycle, moves the submarine (1,0,2) units from its current location. Submarine engines can be fired for fractional units of time, and when ran in reverse moves the shuttle backwards along that given vector.



Can you make it to the whale?

Answer. Essentially, our question is asking if the vector (12, 6, -6) is contained in the span of the three vectors (2, 1, 0), (0, 2, 1), (1, 0, 2).

I claim that it is! To see why, simply just start trying to combine these three vectors into (12, 6, -6). If we assume that we fire the first engine for a units, the second for b units, and the third for c units, we're essentially trying to find a, b, c such that

$$a(2,1,0) + b(0,2,1) + c(1,0,2) = (12,6,-6).$$

This gives us three equations, one for the x-coördinate, one for the y-coördinate, and a third for the z-coördinate:

$$2a + 0b + 1c = 12,$$

$$1a + 2b + 0c = 6,$$

$$0a + 1b + 2c = -6$$

Subtracting two copies of the second equation from the first gives us

$$-4b + c = 0,$$

in other words c = 4b. Plugging this into the last equation gives us

$$b + 2(4b) = -6$$

i.e. $b = -\frac{2}{3}$. This gives us then that $c = -\frac{8}{3}$, and thus that

$$2a - \frac{8}{3} = 12,$$

i.e. $a = \frac{22}{3}$.

Consequently, we've just calculated that

$$\frac{22}{3}(2,1,0) - \frac{2}{3}(0,2,1) - \frac{8}{3}(1,0,2) = (12,6,-6);$$

in other words, that (12, 6, -6) is in the span of our set of vectors, and therefore that we can get to it by using our three engines as described by a, b, c!

A fact worth noting is the following:

Proposition. Let V be a vector space over a field F and A any nonempty subset of vectors of V. The span of A, span(A), is a subspace of V.

Proof. As on Friday, we just have to check three properties:

• Closure(+): Take any two vectors $\vec{x}, \vec{y} \in \text{span}(A)$. For each of these vectors, because they're in the span of A, we can write them as some linear combination of elements of A: i.e. we can find field elements $a_1, \ldots a_n, b_1, \ldots b_m \in F$ and vectors $\vec{v_1}, \ldots, \vec{v_n}, \vec{w_1}, \ldots, \vec{w_m} \in A$ such that

$$a_1 \vec{v_1} + \dots a_n \vec{v_n} = \vec{x},$$

$$b_1 \vec{w_1} + \dots b_n \vec{w_n} = \vec{y}.$$

Then, we have that

$$a_1 \vec{v_1} + \dots + a_n \vec{v_n} + b_1 \vec{w_1} + \dots + b_n \vec{w_n} = \vec{x} + \vec{y}.$$

In other words, $\vec{x} + \vec{y}$ is a linear combination of elements in A! Therefore, $\vec{x} + \vec{y}$ is also in the span of A.

• Closure(·): Take any vector $\vec{x} \in \text{span}(A)$. Like before, because \vec{x} is in the span of A, we can write it as some linear combination of elements of A: i.e. we can find field elements $a_1, \ldots a_n \in F$ and vectors $\vec{v_1}, \ldots \vec{v_n} \in A$ such that

$$a_1\vec{v_1} + \dots a_n\vec{v_n} = \vec{x}$$

Pick any $b \in F$. We have that

$$b\vec{x} = b(a_1\vec{v_1} + \dots + a_n\vec{v_n}) = ba_1\vec{v_1} + \dots + ba_n\vec{v_n};$$

in other words, $b\vec{x}$ is a linear combination of elements of A, and is therefore in the span of A.

• Identity(+). Take any vector $\vec{v} \in A$. We know/have proven that $0\vec{v} = \vec{0}$, the additive identity, for any vector space V. Therefore, because span(A) is closed under scalar multiplication, we have just shown that $\vec{0}$ is in span(A).

Because these three properties hold, by our results on Friday (which said that given these three properties along with the fact that $\operatorname{span}(A)$ is a subset of V, the rest of the vector space properties must follow) we have just shown that this is a subspace of V!

Based off of this observation, we can make the following definition:

Definition. Suppose that $A = {\vec{v_1}, \ldots, \vec{v_n}}$ is some set of vectors, drawn from some vector space V. In the proposition above, we proved that span(A) is a subspace of the vector space V: in other words, span(A) is a vector space in its own right! Suppose that span(A) is equal to the vector space U. Then we say that A spans U.

This definition motivates a second kind of question: take some vector space V. Can we find a set A of vectors that spans V?

The answer here is clearly yes: we can just pick A to be V itself! Then the span of A is certainly V, because every vector of V is simply contained in A. Yet, this answer is also kind of dumb. While A spans V, it does so with a lot of redundancy: i.e. if V was \mathbb{R}^3 , we'd be using a set with infinitely many elements to span \mathbb{R}^3 , when we really only need the three vectors (1,0,0), (0,1,0), (0,0,1).

Here's a related question, to help us spot this kind of inefficiency: suppose we have some set A of vectors. Is it possible to remove a vector from A and still have a set with the same span as A?

This concept **also** comes up all the time in mathematics! Therefore, we have a definition for it:

Definition. Let V be some vector space over a field F, and A be a subset of V. We say that the set A is **linearly dependent** if there is some n > 0 and distinct elements $\vec{v_1}, \ldots, \vec{v_n} \in A$, field coefficients $a_1, \ldots, a_n \neq 0 \in F$ such that

$$\vec{0} = a_1 \vec{v_1} + a_2 \vec{v_2} + \dots a_n \vec{v_n}$$

In other words, a set A is linearly dependent if there is a linear combination of elements in A that sums to 0.

If no such combination exists, then we say that A is **linearly independent**.

Notice that if a set is **linearly dependent**, then there is some vector within it that we can remove without changing its span!

Lemma 1. Let V be a vector space over a field F, and S be a linearly dependent subset of V. Then there is some vector \vec{v} in S that we can remove from S without changing its span.

Proof. By definition, because S is linearly dependent, there is some n > 0 and distinct elements $\vec{v_1}, \ldots, \vec{v_n} \in A$, field coefficients $a_1, \ldots, a_n \neq 0 \in F$ such that

$$\vec{0} = a_1 \vec{v_1} + a_2 \vec{v_2} + \dots a_n \vec{v_n}.$$

Solve for $\vec{v_1}$:

$$\vec{v_1} = -\frac{a_2}{a_1}\vec{v_2} - \frac{a_3}{a_1}\vec{v_2} - \dots \frac{a_n}{a_1}\vec{v_n}.$$

This is a way to create the vector $\vec{v_1}$ without using the vector $\vec{v_1}$ itself.

Consider the set $S \setminus \{\vec{v_1}\}$, the set created by removing $\vec{v_1}$ from S. We claim that this set has the same span as S itself. To see why, take any element \vec{u} in the span of S: i.e. any linear combination of elements in S. Pick distinct vectors $\vec{w_1}, \ldots, \vec{w_m} \in S$ and scalars b_1, \ldots, b_m such that

$$\vec{u} = b_1 \vec{w_1} + \dots b_n \vec{w_n}.$$

If none of these vectors $\vec{w_1}, \ldots, \vec{w_n}$ are the vector $\vec{v_1}$, then this linear combination is also in the span of $S \setminus {\vec{v_1}}$. Otherwise, if some $\vec{w_i} = \vec{v_1}$, then we can just replace $\vec{w_i}$ with

$$-\frac{a_2}{a_1}\vec{v_2} - \frac{a_3}{a_1}\vec{v_2} - \dots \frac{a_n}{a_1}\vec{v_n}$$

This gives us a way to combine elements of $S \setminus \{\vec{v_1}\}$ in a way to create \vec{u} .

So, we've shown that any element of the span of S is also in the span of $S \setminus \{\vec{v_1}\}$! Therefore, these two sets have the same span, and we've proven our claim: there is a vector, $\vec{v_1}$, that we can remove from S without changing its span.

By repeatedly applying Lemma 1, we can get the following theorem:

Theorem 2. Any finite set of vectors S has a linearly independent subset T, such that span(S) = span(T).

Proof. Take any set S. If it is linearly independent, stop; we're done. Otherwise, repeatedly apply Lemma 1 to find an element we can remove from S without changing its span, and remove that element from S. Because our set is finite, and any set with one vector is linearly independent (prove this if you don't see why!), we know that this process will eventually stop and leave us with a linearly independent set at some stage!

So we've found a subset T of S with the same span as S, that's linearly independent. Yay! \Box

Side note. In the infinite case, things are much more complicated. In particular, the above process, of repeatedly removing elements one-by-one, isn't guaranteed to ever stop! For example, suppose you had the set $S = \{(z, 0) : z \neq 0 \in \mathbb{Z}\}$.

This is an infinite set. Moreover, because the span of this set is simply $\{(x, 0) : x \in \mathbb{R}\}$, literally any single element (z, 0) of S will have the same span as S: this is because $\frac{x}{z}(z, 0)$ is a linear combination using just (z, 0) that can generate any element in span(S).

However, suppose you were simply removing elements one-by-one from S. It is possible, through sheer bad luck, you would pick the elements $(1,0), (2,0), (3,0), (4,0), \ldots$ all in a row. This would never get you down to a linearly independent set! In particular, you'd still have all of the elements (z,0) where z is a negative integer lying around, and there are tons of linear combinations of these elements that combine to (0,0).

So the argument above doesn't work. However, the result is still true: there is a subset that is linearly independent with the same span! Proving that this always exists, though, is tricky, and requires the use of things like the axiom of choice. Look for a relevant problem on this on your homework! To illustrate how we concretely find linearly independent subsets of certain sets of vectors, we work an example:

Question. Consider the set

$$S = \{a, a+1, a+2\} : a \in \mathbb{N}, 0 < a \le 100\}.$$

Is this set linearly dependent? If it is, find a linearly independent subset of this set. If not, prove it is linearly independent.

Proof. So, it certainly seems like this set should be linearly dependent: there are a hundred vectors in the set, and it's a subset of \mathbb{R}^3 ! However, we need to actually prove this is true, which is a little tricker: where do we start?

One good tactic here is to look at some concrete elements of our set, and see what we can do with those elements. (In general, this is a useful tactic when you're presented with a large collection of objects all described using rules: make a few examples and see what those examples do!)

In particular, we know that (1, 2, 3), (2, 3, 4), (3, 4, 5), and (4, 5, 6) are all elements of our set. Is this smaller, easier-to-understand set linearly dependent?

Well: if it were, we would have to have some way of combining elements to get to (0, 0, 0). It's not obvious how to do this as written, though. One strategy here is to just algebra-bash out a solution: i.e. try to find a, b, c, d such that a(1, 2, 3) + b(2, 3, 4) + c(3, 4, 5) + d(4, 5, 6) =(0, 0, 0). This will work! But it seems tedious; solving three equations in four variables is not the most enjoyable thing in the world to do. Also, we've already given an example (earlier, when we were showing that a given vector is in the span of some set) that basically goes through this method.

An alternate strategy, that is sometimes worth pursuing, is not to just try to find combinations of (1,2,3), (2,3,4), (3,4,5), (4,5,6) that get to (0,0,0), but rather to just look for combinations that get to something **useful**! I.e. if we could make the vectors (1,0,0) or (0,1,0) or (0,0,1), that would be really useful for making (0,0,0) later, as these are relatively useful and easy-to-understand vectors!

This, we **can** do. In particular, notice that

$$(2,3,4) - (1,2,3) = (1,1,1),$$

which certainly looks like a useful vector!

In fact, it's great for generating the other vectors in this set! Notice that, for example,

$$(3,4,5) = (1,2,3) + 2(1,1,1) = (1,2,3) + 2((2,3,4) - (1,2,3)),$$

and therefore that we can write (3, 4, 5) as a linear combination of vectors in our set!

More generally, notice that

$$(a, a + 1, a + 2) = (1, 2, 3) + (a - 1)(1, 1, 1) = (1, 2, 3) + (a - 1)((2, 3, 4) - (1, 2, 3)),$$

and therefore that we can write **any** vector in our set as a linear combination of the two vectors (1, 2, 3) and (2, 3, 4)!

Therefore, we've shown that the span of our set S is just the span of the two vectors (1, 2, 3) and (2, 3, 4). These vectors are clearly linearly independent: to see why, notice that if

$$x(1,2,3) + y(2,3,4) = (0,0,0),$$

we would have to have

$$x + 2y = 0,$$

 $2x + 3y = 0,$ and
 $3x + 4y = 0.$

The first two equations tell us that x = -2y and that $x = -\frac{3}{2}y$, which can only hold if x = y = 0. Therefore, there is no nontrivial combination (i.e. no combination in which the coefficients are nonzero) of these two vectors that is equal to (0, 0, 0).

So we've created a linearly independent subset of S that has the same span as S! Yay, success. $\hfill \Box$

4.2 Basis and Dimension

This idea — of a set S that doesn't have any redundancy in it — is a valuable one in linear algebra. Accordingly, we have a term for these kinds of sets:

Definition. Take a vector space V. A **basis** B for V is a set of vectors B such that B is linearly independent, and span(B) = V.

Bases are really useful things. You're already aware of a few bases:

- The set of vectors $\vec{e_1} = (1, 0, 0 \dots 0), e_2 = (0, 1, 0 \dots 0), \dots e_n = (0, 0 \dots 0, 1)$ is a basis for \mathbb{R}^n .
- The set of polynomials $1, x, x^2, x^3, \dots$ is a basis for $\mathbb{R}[x]$.

As a quick example, we study another interesting basis:

Question. Consider the set of vectors

$$S = \{(1, 1, 1, 1), (1, 1, -1, -1), (1, -1, 1, -1), (1, -1, -1, 1)\}.$$

Show that this is a basis for \mathbb{R}^n .

Proof. Take any $(w, x, y, z) \in \mathbb{R}^4$. We want to show that there are always a, b, c, d such that

$$a(1,1,1,1) + b(1,1,-1,-1) + c(1,-1,1,-1) + d(1,-1,-1,1) = (w, x, y, z),$$

and furthermore that if (w, x, y, z) = (0, 0, 0, 0) that this forces a, b, c, d to all be 0. This proves that the span of S is all of \mathbb{R}^4 and that S is linearly independent, respectively.

We turn the equation above into four equalities, one for each coördinate in \mathbb{R}^4 :

$$a+b+c+d = u$$
$$a+b-c-d = x$$
$$a-b+c-d = y$$
$$a-b-c+d = z$$

Summing all four equations gives us

$$4a = w + x + y + z.$$

Adding the first two equations and subtracing the second two equations gives us

$$4b = w + x - y - z$$

Adding the first and third, and subtracting the second and fourth gives us

$$4c = w + y - x - z.$$

Finally, adding the first and fourth and subtracting the second and third yields

$$4d = w + z - x - y.$$

So: if (w, x, y, z) = (0, 0, 0, 0), this means that a = b = c = d = 0. Therefore, our set is linearly independent.

Furthermore, for any (w, x, y, z), we have that

$$\frac{w+x+y+z}{4}(1,1,1,1) + \frac{w+x-y-z}{4}(1,1,-1,-1) + \frac{w+y-z-z}{4}(1,-1,-1,-1) + \frac{w+z-x-y}{4}(1,-1,-1,1) = (w,x,y,z).$$

Therefore, we can combine these four elements to get any vector in \mathbb{R}^4 ; i.e. our set spans \mathbb{R}^4 .

This example is interesting because its entries satisfy the following two properties:

- Every vector is made up out of entries from ± 1 .
- The dot product of any two vectors is 0.

Finding a basis of vectors that can do this is actually an open question. We know that they exist for any \mathbb{R}^n where *n* is a multiple of 4 up to 664, but no one's found such a basis for \mathbb{R}^{668} . Find one for extra credit?

Another natural idea to wonder about is the following: given a vector space V, what is the smallest number of elements we need to make a basis? Can we have two bases with different lengths?

This is answered in the following theorem:

Theorem. Suppose that V is a vector space with two bases $B_1 = {\vec{v_1}, \ldots, \vec{v_n}}, B_2 = {\vec{w_1}, \ldots, \vec{w_m}}$ both containing finitely many elements. Then these sets have the same size: i.e. $|B_1| = |B_2|$.

Proof. HW!

Using this, we can finally define the concept of **dimension**:

Definition. Suppose that V is a vector space with a basis B containing finitely many elements. Then we say that the **dimension** of V is the number of elements in B.

For example, the dimension of \mathbb{R}^n is n, because this vector space is spanned by the vectors $\vec{e_1} = (1, 0, 0...0), e_2 = (0, 1, 0...0), \dots e_n = (0, 0...0, 1).$

We care about the idea of dimension not so much for understanding vector spaces — after all, it's not that surprising that the dimension of \mathbb{R}^n is n — but rather because it lets us study **linear maps**.

4.3 Linear Maps

Definition. A linear map from a vector space V to another vector space W, where V and W are two vector spaces over some field F, is a function $T: V \to W$ with the following properties:

- Plays well with addition: for any $\vec{v}, \vec{w} \in V$, $T(\vec{v} + \vec{w}) = T(\vec{v}) + T(\vec{w})$.
- Plays well with multiplication: for any $\vec{v} \in V$ and any $a \in \mathbb{R}$, $T(a\vec{v}) = aT(\vec{v})$.

If people are being formal, they will say that maps that satisfy the first property are "additive," while maps that satisfy the second property are "homogeneous."

Also, sometimes people call linear maps linear transformations. These are the same things.

For example, the map $id: \mathbb{R}^2 \to \mathbb{R}^2$, defined by

$$id(x,y) = (x,y)$$

is a linear map, because

- it plays well with addition: for any two vectors (a, b), (c, d), we have id((a, b) + (c, d)) = id(a + c, b + d) = (a + c, b + d). This is the same thing as id(a, b) + id(c, d) = (a, b) + (c, d) = (a + c, b + d).
- it plays well with multiplication: for any vector (a, b) and any real number λ , we have $id(\lambda(a, b)) = id(\lambda a, \lambda b) = (\lambda a, \lambda b)$. This is the same thing as $\lambda id(a, b) = \lambda(a, b) = \lambda(a, b)$.

Conversely, the map $T: \mathcal{P}_1(\mathbb{R}) \to \mathcal{P}_1(\mathbb{R})$, defined by

$$T(a+bx) = a^2$$

is not a linear map, because

• it does not play well with addition. Specifically, look at the two polynomials 2, 2 + x in $\mathcal{P}_1(\mathbb{R})$. $T(2 + (2 + x)) = T(4 + x) = 4^2 = 16$, while $T(2) + T(2 + x) = 2^2 + 2^2 = 8$.

Essentially, we care about linear maps because they're a way to take one vector space and "turn it" somehow into another vector space: i.e. it gives us a way of taking something that has addition and scalar multiplication operations and turning it into something else that has addition and scalar multiplication operations, in a way that "preserves" these two operations (because it "plays well" with addition and scalar multiplication.)

Two concepts we like to study with linear maps are the range and null space:

Definition. Pick two vector spaces U, V. Let $T : U \to V$ be a linear map from U to V. The **range** of T is the following set:

$$\operatorname{range}(T) = \{T(\vec{u}) \mid \vec{u} \in U\}$$

In other words, the range of a linear map is the collection of all possible outputs of T under all possible inputs from U. Some people call this the **image** of T, and denote this im(T). Others will denote this as T(U), the idea being that you've put "all" of U into T itself.

Definition. Pick two vector spaces U, V. Let $T : U \to V$ be a linear map from U to V. The **null space** of T is the following set:

$$\operatorname{null}(T) = \{ \vec{u} \mid T(\vec{u}) = \vec{0} \in V \}$$

In other words, the null space of a linear map is the collection of all of the elements in U that T maps to 0.

For example, consider the linear map $T : \mathbb{R}^4 \to \mathbb{R}^2$,

$$T(w, x, y, z) = (0, 0).$$

For this map,

- The image of T is the set $\{(0,0)\}$, because T outputs (0,0) on every input.
- The null space of T is all of \mathbb{R}^4 , because T sends every element of \mathbb{R}^4 to (0,0).

Similarly, consider the map $T : \mathbb{R}^4 \to \mathbb{R}$, defined such that

$$T(x, y, z) = x + y + z.$$

Thing you should do if you don't believe it: show this is a linear map. Once you've done this, then you can easily check the following:

• The **image** of T is all of \mathbb{R} . This is because on input (a, 0, 0), for any real number a, T outputs a + 0 + 0 = a. Therefore, we can get any real number as an output of T. Because T's output is restricted to \mathbb{R} , there's nothing else to worry about getting; consequently, the image of T is precisely T.

• The null space of T is the collection of all triples (a, b, c) such that T(a, b, c) = a + b + c = 0. In other words, if we solve for c in terms of the other two variables, it's the collection $\{(a, b, -a - b) : a, b \in \mathbb{R}\}$ of vectors in \mathbb{R}^3 .

Fun fact: both the range and the nullspace of any linear map are subspaces! We prove this here:

Theorem 3. The range of a linear map $T: U \to V$ is a subspace of V.

Proof. Let $T: U \to V$ be a linear map, and range(T) denote the range of T: i.e.

$$\operatorname{range}(T) = \{T(\vec{u}) \mid \vec{u} \in U\}$$

We want to show this is a subspace of the set it's contained in, V.

To do this, we recall from week 1 that we simply need to check the following three conditions:

• Closure(+): we need to take any two vectors $\vec{x}, \vec{y} \in \text{range}(T)$, and show that their sum is in the range of T.

Doing this is not very hard. If \vec{x}, \vec{y} are both in the range of T, then by definition there must be a pair of vectors \vec{a}, \vec{b} such that $T(\vec{a}) = \vec{x}, T(\vec{b}) = \vec{y}$. Therefore, the vector $T(\vec{a} + \vec{b})$ is also in the range of T, because it is something else that is an output of T. But $T(\vec{a} + \vec{b}) = T(\vec{a}) + T(\vec{b}) = \vec{x} + \vec{y}$. Therefore, given any two vectors \vec{x}, \vec{y} in the range of T, their sum is also in the range of T.

• Closure(·): we need to take any vector $\vec{x} \in \operatorname{range}(T)$, and any scalar $\lambda \in F$, and show that their product is in the range of T.

This is pretty easy, and similar to what we just did above. Again, because \vec{x} is in the range of T, there has to be some vector \vec{a} such that $T(\vec{a}) = \vec{x}$. Then, we have that $T(\lambda \vec{a})$ must also be in the range of T, because it's another possible output of T. But $T(\lambda \vec{a}) = \lambda T(\vec{a}) = \lambda \vec{x}$. Therefore, the range is closed under multiplication by scalars.

• Identity(+): Take any $\vec{a} \in U$. Because U is a vector space, we know that $-\vec{u}$ is contained within U. We know that $T(\vec{a} - \vec{a}) = T(\vec{a}) - T(\vec{a}) = \vec{0}$; therefore, $\vec{0}$ is in the range of T.

Theorem 4. The null space of a linear map $T: U \to V$ is a subspace of V.

Proof. Let $T: U \to V$ be a linear map, and null(T) denote the null space of T: i.e.

$$\operatorname{null}(T) = \{ \vec{u} \mid T(\vec{u}) = \vec{0} \in V \}$$

We want to show this is a subspace of the set it's contained in, U.

To do this, we recall from week 1 that we simply need to check the following three conditions:

• Closure(+): we need to take any two vectors $\vec{x}, \vec{y} \in \text{null}(T)$, and show that their sum is in the null space of T.

Doing this is easier than for the range! If \vec{x}, \vec{y} are both in the null space of T, then by definition $T(\vec{x}) = T(\vec{y}) = \vec{0}$. But then $T(\vec{x} + \vec{y}) = T(\vec{x}) + T(\vec{y}) = \vec{0} + \vec{0} = \vec{0}$. Therefore, given any two vectors \vec{x}, \vec{y} in the null space of T, their sum is also in the null space of T.

• Closure(·): we need to take any vector $\vec{x} \in \text{null}(T)$, and any scalar $\lambda \in F$, and show that their product is in the null space of T.

This is also easy. Again, because \vec{x} is in the null space of T, $T(\vec{x}) = \vec{0}$. Then, we have that $T(\lambda \vec{x}) = \lambda T(\vec{x}) = \lambda \vec{0} = \vec{0}$. Therefore, the null space is closed under multiplication by scalars.

• Identity(+): This is identical to the proof for range. Take any $\vec{a} \in U$. Because U is a vector space, we know that $-\vec{u}$ is contained within U. We know that $T(\vec{a} - \vec{a}) = T(\vec{a}) - T(\vec{a}) = \vec{0}$; therefore, $\vec{a} - \vec{a} = \vec{0}$ is in the null space of T.

The null space and the range are linked by perhaps the most famous theorem in any first quarter of a linear algebra class:

4.4 The Rank-Nullity Theorem

The **rank-nullity** theorem is the following result:

Theorem. Let U, V be a pair of finite-dimensional vector spaces, and let $T : U \to V$ be a linear map. Then the following equation holds:

 $\operatorname{dimension}(\operatorname{null}(T)) + \operatorname{dimension}(\operatorname{range}(T)) = \operatorname{dimension}(U).$

Before we prove this theorem, let's try to visualize what it means in a specific case. Suppose that we have the linear map $T : \mathbb{R}^2 \to \mathbb{R}$ given by $(x, y) \mapsto 2x - y$.

It is not too hard to see the following:

- 1. the null space of T is the line $\{(x, 2x) \mid x \in \mathbb{R}\}$, and
- 2. the range of this map is all of \mathbb{R} , because $(0, -x) \mapsto x$ for any x.

Moreover, we can actually make the following more specific observation:

Observation. For any $a \in \mathbb{R}$, let $T^{-1}(a)$ denote the collection of all points in \mathbb{R}^2 that map to a. This set is just a copy of the null space of T shifted by the constant (0, -a): in other words, $T^{-1}(a) = \{(0, -a) + \vec{n} \mid \vec{n} \in \text{null}(T)\}.$

We can illustrate this situation with the following picture:



Graphically, what we did here is decompose the **domain** of our linear map, \mathbb{R}^2 , into "range(T)-many" copies of the null space. If we look at the dimensions of the objects we studied here, we said that we could take a two-dimensional object (the **domain**) and break it into copies of this one dimensional object (the **null space**), with as many copies of this one-dimensional object as we have $T^{-1}(a)$'s (i.e. elements in the **range**.)

In general, we can always break the domain into copies of the null space like this: i.e. you can prove (and are asked to do so on the homework!) the following result:

Theorem 5. Let $T: U \to V$ be a linear map. Let N(T) denote the null space of T, and \vec{u}, \vec{w} be any pair of vectors from U, V respectively such that $T(\vec{u}) = \vec{v}$.

Let $T^{-1}(\vec{v})$ denote the set of all vectors in U that get mapped to \vec{v} by T: i.e.

$$A_{\vec{v}} = \{ \vec{w} \in U \mid T(\vec{w}) = \vec{v} \}.$$

Then $T^{-1}(\vec{v})$ is just N(T) translated by \vec{u} ! In other words,

 $T^{-1}(\vec{v}) = \{ \vec{w} \in U \mid \text{there is some } \vec{x} \in N(T) \text{ such that } \vec{w} = \vec{x} + \vec{u} \}$

In other words, understanding the collection of elements that all get mapped to $\vec{0}$ basically lets us understand the collection of elements that get mapped to any fixed vector \vec{v} .

This should lead you to believe that the rank-nullity theorem is true: intuitively, this result should mean that we can break the domain of T into "range-many" copies of the null space, and thus that dimension(null(T)) + dimension(range(T)) = dimension(U).

However, this might not feel a lot like a proper "proof" to some of you: there's a pretty picture here, but where is the rigor? How am I turning this decomposition into an argument about dimension (which is a statement about bases, which we're not saying anything about here?)

The point of this section is to take the above intuition, and turn it into a proper argument. We do so as follows:

4.5 The Rank-Nullity Proof: Some Useful Lemmas

First, recall the following theorem, that we proved earlier in our notes:

Theorem. The idea of "dimension" is well defined. In other words: suppose that U is a vector space with two different bases B_1, B_2 containing finitely many elements each. Then there are as many elements in B_1 as there are in B_2 .

We will need this theorem to prove the rank-nullity theorem. As well, we will also need the following: **Theorem.** Suppose that U is a *n*-dimensional vector space with basis B, and that S is a subspace of U. Then S is also finite dimensional, and in particular has dimension no greater than n.

Proof. We prove this statement by contradiction. Suppose that S is a set with dimension greater than n. Using this fact, create a set T of n + 1 linearly independent vectors in S as follows. At first, simply pick any nonzero vector $\vec{v} \in S$, and put $\vec{v} \in T$. Then, repeat the following process

- 1. Look at T. If it has no more than n vectors in it, then it cannot span S, because S has dimension greater than n. So there is some vector $\vec{w} \in S$ that is not in the span of T.
- 2. Put \vec{w} in T. Notice that if T was linearly independent before we added \vec{w} , it is still linearly independent, because \vec{w} was not in the span of T.

So: we now have a set of n + 1 linearly independent vectors in S, which means in particular we have a set of n + 1 linearly independent vectors in U! This is a problem, because U is *n*-dimensional. To see why, notice that we can "grow" this set T of n + 1 linearly independent vectors into a basis for U as follows. Start with T. If T spans U, stop. Otherwise, repeat the following process until we get a linearly independent set that spans U:

- 1. If T does not span U, then there is some element \vec{b} in the basis B of U that is not in the span of T (because otherwise, if T contained all of a basis for U in its span, it would be forced to contain all of U itself in its span!).
- 2. Add \vec{b} to T. Again, notice that if T was linearly independent before we added \vec{b} , it is still linearly independent, because \vec{b} was not in the span of T.

Eventually, this process will stop, as after n steps your set T will at the least contain **all** of the elements of B, which is a basis for U!

So this creates a linearly independent set that spans U: i.e. a basis! And in particular a basis with at least n + 1 elements, because T started with n + 1 elements and had more things potentially added to it later.

However, B is a basis for U with n elements. We've proven that dimension is well-defined: i.e. that a vector space cannot have two different bases with different sizes! Therefore, this is impossible, and we have a contradiction. Consequently, our assumption must be false: in other words, S must have dimension no greater than n.

4.6 Proving the Rank-Nullity Theorem

With these tools set up, we proceed with the main proof:

Theorem. Let U, V be a pair of finite-dimensional vector spaces, and let $T : U \to V$ be a linear map. Then the following equation holds:

$$\operatorname{dimension}(\operatorname{null}(T)) + \operatorname{dimension}(\operatorname{range}(T)) = \operatorname{dimension}(U).$$

Proof. We prove this as follows: we will create a basis for U with as many elements as dimension $(\operatorname{null}(T))$ + dimension $(\operatorname{range}(T))$, which will clearly demonstrate the above equality. We do this as follows:

- 1. By using Theorem 4.5, we can see that the null space of T is finite dimensional. Take some basis N_B for the null space of T.
- 2. Now: let B be a basis for U, and R_B be some set that is empty for now. If N_B is also a basis for U, stop. Otherwise, repeat the following process:
 - (a) Look at $N_B \cup R_B$. If it is a basis for U, stop. Otherwise, there is some vector \vec{b} that is in the basis set B, that is not in $N_B \cup R_B$. (Again, this is because if not, T would contain the entirety of a basis for U in its span, which would force it to contain U itself in its span!)
 - (b) Put \vec{b} in R_B . Notice that if $N_B \cup R_B$ was linearly independent before we added \vec{b} , it is still linearly independent, because \vec{r} was not in the span of $N_B \cup R_B$.

As before, this process will eventually end, because we only have finitely many elements in B.

- 3. At the end of this process, we have two sets R_B, N_B such that their union is a basis for U. Look at the set $T(R_B) = \{T(\vec{r}) \mid \vec{r} \in R_B\}$. We claim that $T(R_B)$ is a basis for the range of T. To prove this, we will simply show that this set spans the range, and is linearly independent.
- 4. To see that $T(R_B)$ spans the range: take any \vec{v} in the range of T. Because \vec{v} is in the range, there is some $\vec{u} \in U$ such that $T(\vec{u}) = \vec{v}$. Write \vec{u} as some linear combination of elements in our basis $R_B \cup N_B$: i.e.

$$\vec{u} = \sum_{\vec{r_i} \in R_B} \lambda_i \vec{r_i} + \sum_{\vec{n_i} \in N_B} \gamma_i \vec{n_i}.$$

Let \vec{w} be the following vector:

$$\vec{w} = \sum_{\vec{r_i} \in R_B} \lambda_i \vec{r_i}$$

In other words, \vec{w} is just \vec{u} if you get rid of all of the parts made using vectors in the null space! Now, simply observe that on one hand, \vec{w} is an element in the span of R_B ,

and on the other

$$\vec{v} = T(\vec{u}) = T\left(\sum_{\vec{r_i} \in R_B} \lambda_i \vec{r_i} + \sum_{\vec{n_i} \in N_B} \gamma_i \vec{n_i}\right)$$
$$= T\left(\sum_{\vec{r_i} \in R_B} \lambda_i \vec{r_i}\right) + T\left(\sum_{\vec{n_i} \in N_B} \gamma_i \vec{n_i}\right)$$
$$= \sum_{\vec{r_i} \in R_B} \lambda_i T(\vec{r_i}) + \sum_{\vec{n_i} \in N_B} \lambda_i T(\vec{n_i})$$
$$= \sum_{\vec{r_i} \in R_B} \lambda_i T(\vec{r_i}) + \vec{0}$$
$$= \sum_{\vec{r_i} \in R_B} \lambda_i T(\vec{r_i}),$$

because things in the null space get mapped to $\vec{0}$!

Therefore, given any \vec{v} in the range, we have expressed it as a linear combination of elements in $T(R_B)$. In other words, $T(R_B)$ spans the range of V.

5. To show that $T(R_B)$ is linearly independent: take any linear combination of vectors in $T(R_B)$ that is equal to $\vec{0}$:

$$\sum_{\vec{r_i} \in R_B} \lambda_i T(\vec{r_i}) = \vec{0}.$$

We want to show that all of the coefficients λ_i are 0. To see this, start by using the fact that T is linear:

$$\vec{0} = \sum_{\vec{r_i} \in R_B} \lambda_i T(\vec{r_i}) = T\left(\sum_{\vec{r_i} \in R_B} \lambda_i \vec{r_i}\right).$$

This means that the vector

$$\sum_{\vec{r_i} \in R_B} \lambda_i \vec{r_i}$$

is in the null space of T. Therefore, we can create a linear combination of vectors in N_B that are equal to this vector: i.e. we can find elements in N_B and constants γ_i such that

$$\sum_{\vec{r_i} \in R_B} \lambda_i \vec{r_i} = \sum_{\vec{n_i} \in N_B} \gamma_i \vec{n_i}.$$

But this means that we have

$$\sum_{\vec{r_i} \in R_B} \lambda_i \vec{r_i} - \sum_{\vec{n_i} \in N_B} \gamma_i \vec{n_i} = \vec{0},$$

which is a linear combination of elements in our basis $R_B \cup N_B$ that equals $\vec{0}$! Because this set is a basis, it is linearly independent; therefore all of the coefficients in this linear combination must be 0. In particular, this means that all of the λ_i 's are 0, which proves what we wanted: that the set $T(R_B)$ is linearly independent!

Consequently, we have created a basis for U of the form N_B and R_B , where $T(R_B)$ is a basis for the range and N_B is a basis for the null space. This means that, in particular, the dimension of U is the number of elements in N_B (i.e. the dimension of the null space) plus the number of elements in R_B (i.e. the dimension of the range.) So we're done!

This has a particularly useful corollary, that we will want for our study of circuits and random walks:

Corollary. Suppose that $A: \mathbb{R}^n \to \mathbb{R}^n$ is a linear map with dim(nullspc(A)) = 0. Then the range of A is all of \mathbb{R}^n , as the dimension n of its domain must be equal to the dimension of its range plus the dimension of the nullspace.

4.7Solutions Are Unique

We return to our original problem:

Theorem. Take a system of linear equations of the form obtained from these random walks on a connected graph, where the boundary values are 0: i.e. a collection of interior equations of the form

$$p(x) = \sum_{y \in N(x)} \frac{w_{xy}}{w_x} \cdot p(y),$$

where $w_x = \sum_{y \in N(x)} w_{xy}$, along with some boundary conditions $p(b_i) = c_i$. There is a unique solution to this system of equations.

Proof. We have already proven that there is at most one solution to these equations; therefore, it suffices to prove that there is at least one solution as well.

Let x_1, \ldots, x_n denote the *n* interior vertices and $b_1 \ldots b_m$ denote the *m* boundary vertices of our graph. Consider the following linear map $A : \mathbb{R}^n \to \mathbb{R}^n$, defined by

$$A(t_1, \dots, t_n) = \left(t_1 - \sum_{y \in N(x_1)} \frac{w_{x_1y}}{w_{x_1}} \cdot t_j, t_2 - \sum_{y \in N(x_2)} \frac{w_{x_2y}}{w_{x_2}} \cdot t_j, \dots, t_n - \sum_{y \in N(x_n)} \frac{w_{x_ny}}{w_{x_n}} \cdot t_j \right)$$

In other words, A is the map that takes a n-tuple $t_1 \dots t_n$ and "plugs it in" to our n linear equations $\sum_{y \in N(x_i)} \frac{w_{x_iy}}{w_{x_i}} \cdot t_j$. We can easily see that this map is linear in the variables $t_1, \dots t_n$, as each coordinate is

a linear combination of the t_i coefficients: so this is actually a linear map $\mathbb{R}^n \to \mathbb{R}^n$.

As such, we can consider its nullspace! We can see that there is a vector that maps to $\vec{0}$: namely, the all-zeroes vector $\vec{0}$.

We can also see that this is the **only** vector that maps to zero. To do this, notice that if \vec{t} maps to $\vec{0}$, then we have for all *i* the following equation:

$$t_i - \sum_{y \in N(x_i)} \frac{w_{x_iy}}{w_{x_i}} \cdot t_j$$
$$\Rightarrow \quad t_i = \sum_{y \in N(x_i)} \frac{w_{x_iy}}{w_{x_i}} \cdot t_j.$$

Therefore, if we let $p(x_i) = t_i$ for every *i*, and let $p(b_k) = 0$ for all *k*, we have a solution to all of our equations!

We know that any such solution is **unique**, as proved before. Therefore there is only one such solution: the all-zeroes vector $\vec{0}$.

Therefore, A is a linear map $\mathbb{R}^n \to \mathbb{R}^n$ with a dimension-zero nullspace. So the dimension of its range is n — that is, its range is all of \mathbb{R}^n !

What does this mean? Well: suppose we take **any** boundary conditions $p(b_i) = c_i$, for any collection of values $\{c_i\}_{i=1}^m$, along with our interior equations of the form

$$p(x_i) = \sum_{y \in N(x_i)} \frac{w_{x_i y}}{w_{x_i}} \cdot p(y).$$

Take any interior equation, and separate it into two parts as follows:

$$p(x_i) = \sum_{\substack{y \in N(x_i), \\ y \text{ in interior}}} \frac{w_{x_iy}}{w_{x_i}} \cdot p(y) + \sum_{\substack{y \in N(x_i), \\ y \text{ on boundary}}} \frac{w_{x_iy}}{w_{x_i}} \cdot p(y).$$

If we define

$$d_i = \sum_{\substack{y \in N(x_i), \\ y \text{ on boundary}}} c_j \cdot \frac{w_{x_i b_j}}{w_{x_i}}$$

then we can rewrite our equations as follows:

$$p(x_i) - \sum_{y \in N(x_i)} \frac{w_{x_iy}}{w_{x_i}} \cdot p(y) = d_i.$$

But this set of equations is simply the statement that

$$A(p(x_1), p(x_2), \dots, p(x_n)) = (d_1, d_2, \dots, d_n).$$

We know that A's range is all of \mathbb{R}^n , so for any \vec{d} there is some \vec{t} with $A\vec{t} = \vec{d!}$ Therefore, if we set $p(x_i) = t_i$ and $p(b_i) = c_i$, then we have a solution to our set of equations, as claimed.

Other Connections: Current $\mathbf{5}$

We now have an excellent interpretation of voltage in terms of our random walk. This might lead us to wonder if other properties, like current, also correspond nicely to properties about random walks! To establish this, we first prove the following lemma:

Lemma 6. Take a weighted graph with two distinguished vertices A, B on which we are trying to model a random walk: on this graph, a walker starts at A, and at each time step randomly (using our edge weighting) pick a neighbor of the vertex that it is currently at and wanders to that vertex. If it ever reaches B it stops; otherwise, it continues (unlike in our previous interpretation, where the walker stopped if it arrived at some other home vertex Has well.) Let u(x) denote the average number of times that a walker will wander through the vertex x before reaching B in this model.

Consider the corresponding circuit to this weighted graph, where all edges have conductance corresponding to our weights, B is grounded, and a potential of $\frac{u(A)}{C_A}$ volts is established between B and A. Then we have the following relation between v(x), the voltage, and u(x):

$$v(x) = \frac{u(x)}{C_x}.$$

Proof. Trivially, we have $v(B) = 0 = u(B)/C_B$, because B is grounded and no vertex can visit B before, um, visiting B. As well, we've specifically asked that $v(A) = u(A)/C_A$ in our problem's statement.

Finally: for any vertex $x \neq A, B$, we have

$$u(x) = \sum_{y \in N(x)} (\text{chance of going from y to x}) \cdot u(y);$$

i.e. the number of times we'll go through x is just the sum of the number of times we'll

visit any of the neighbors of x, weighted by the chances of subsequently going from y to x. By definition, we know that the chance of walking from y to x is $\frac{C_{xy}}{C_y}$. If we use this observation and do a little symbolic manipulation, we can get the following:

$$u(x) = \sum_{y \in N(x)} \frac{C_{xy}}{C_y} \cdot u(y)$$
$$= \sum_{y \in N(x)} \frac{C_{xy} \cdot C_x}{C_y \cdot C_x} \cdot u(y)$$
$$\Rightarrow \qquad \frac{u(x)}{C_x} = \sum_{y \in N(x)} \frac{C_{xy}}{C_x} \cdot \frac{u(y)}{C_y}$$

So: we've seen these linear equations before! In particular, if we replace the $\frac{u(z)}{C_z}$'s with v(z)'s, these are precisely the linear equations that we asked the voltage function v(x) to satisfy.

We proved that these equations have a **unique** solution; therefore, this forces v(x) and $\frac{u(x)}{C_x}$ to be equal, as they are both solutions to these equations. How does this relate to current? Well: in a super-simplistic sense, we can model the current flowing through an oriented edge (x, y) as the "flow" of electrons from x to y. That is, if we have electrons randomly bumbling about on our graph starting at b and wandering around until they get to a, we might hope that i_{xy} is the average number of electrons that go from x to y, minus the number that go "backwards" along this edge from y to x.

We prove this here:

Lemma 7. Let G be a graph as above, with potential difference between the ground vertex B and the source vertex A still set to $u(A)/C_A$. Then we have the following relation:

$$i_{xy} = u(x)\frac{C_{xy}}{C_x} - u(y)\frac{C_{xy}}{C_y}.$$

In other words, the current between x and y is just the average number of times a random walker "uses" the edge (x, y) to go from x to y, minus the average number of times a random walker walks backwards on said edge from y to x!

Proof. We simply calculate, using our identities:

$$i_{xy} = (v(x) - v(y)) \cdot C_{xy} = \left(\frac{u(x)}{C_x} - \frac{u(y)}{C_y}\right) C_{xy} = u(x) \frac{C_{xy}}{C_x} - u(y) \frac{C_{xy}}{C_y}.$$

Electricity! Random walks! Apparently, mostly the same. So: why mention this in a graph theory class, other than the basic underlying structure? Consider the following puzzle posed by Polya (amongst others):

Question 8. Suppose that you have placed a random walker placed at the origin of a ddimensional integer lattice \mathbb{Z}^d , and let it wander. Given enough time, will the random walker return to the origin? Or is there a nonzero chance that the random walker will wander forever without returning to the origin?

6 Circuits as Black Boxes

To attack this kind of question, it might help to introduce some new ideas. Specifically, suppose that we have a circuit with two points A, G, where we've grounded G and have a voltage of 1v established at A. If you have done this, then there is some amount of current flowing out of A. Denote this quantity as i_A , and note that i_A is given by the sum $\sum_{x \in N(A)} i_{Ax}$. Note that by Kirchoff's laws, the quantity of current that flows out of A is the same as the quantity of current that flows into G, because the sum of the currents through every vertex not A, B is equal to 0, and therefore whatever flows out of A must eventually flow into G.

Now, imagine simply covering up all of the connections and other bits between A and G with some sort of big black box. If we do this, then our circuit just looks like the following:



In this sense, we can simply "abstract" the rest of our circuit as some particularly large and bulky resistor, with effective resistance (which we denote R_{eff}) given by Ohm's law:

$$\frac{V(A) - V(G)}{i_A} = R_{\text{eff}}$$

Similarly, we can define $C_{\text{eff}} = 1/R_{\text{eff}}$.

Earlier, we noted that the current across an edge (x, y) was proportional to the expected number of paths from x to y minus the expected number of paths from y to x, up to scaling by the voltage we've established between the ground and the source. Does this idea still hold here? In other words: is there some connection between i_a and the total number of paths from A to G? Well: calculating, we have

$$i_A = \sum_{y \in N(A)} (v(A) - v(y)) \cdot C_{Ay}$$

=
$$\sum_{y \in N(A)} (v(A) - v(y)) \cdot \frac{C_{Ay}}{C_A} \cdot C_A$$

=
$$C_A \left(v(A) \sum_{y \in N(A)} \frac{C_{Ay}}{C_A} - \sum_{y \in N(A)} v(y) \frac{C_{Ay}}{C_A} \right)$$

=
$$C_A \left(v(A) - \sum_{y \in N(A)} v(y) \frac{C_{Ay}}{C_A} \right)$$

What is this quantity? Well:

- We know that v(A) is 1, by assumption.
- We also know that $\frac{C_{Ay}}{C_A}$ denotes the probability that a random walker will travel from the vertex A to the vertex y.
- Finally, we know that v(y) = p(y), the probability that a walk starting at y will make it to A before G.

So: if we're starting at A and leaving to any of A's neighbors (which we pick with probability $\frac{C_{Ay}}{C_A}$), the chances of returning to A before making it to G is just v(y). Therefore, the sum

on the right inside of our parentheses is precisely the chances of starting at A and returning there before making it to G; consequently, 1 minus this sum is precisely the likelihood that we start at A and do not return there before wandering to G. Call this event, where we start at A and wander to G without returning to A, an "escape" event, and denote the probability of such an event happening p_{esc} .

If we plug this interpretation into our formula above, we get the following fantastically useful relation:

$$\frac{i_A}{C_A} = p_{\rm esc}.$$

7 Resistance: Surprisingly Not Futile

This, basically, is almost the last tool we need to tackle Polya's problem on \mathbb{Z}^d . This is because we (for values of "we" that includes electrical engineers) know lots of techniques for finding effective resistances! In particular, suppose we have a series of resistors connected "in parallel," like in the picture below:



Then the effective resistance of the pictured circuit is the reciprocal of the sum of the reciprocals of the resistors:

$$\frac{1}{R_{\rm eff}} = \sum_{i=1}^{n} \frac{1}{R_i}$$

Alternately, you can think of this claim as the statement that the "effective conductance" of the circuit is the sum of the conductances of the circuit.

Similarly, suppose we have a circuit made of resistors linked in series, as depicted below:



Then the effective resistance of the pictured circuit is the sum of the resistors:

$$R_{\text{eff}} = \sum_{i=1}^{n} R_i.$$

It bears noting that you can deduce these properties from the two rules we've stated for electrical networks, Ohm's law and Kirchoff's law; the first property just says that the conductances sum when we have resistors in parallel, and the second says that resistances sum when we have resistors in series. We omit a formal proof here, but it's not very difficult (indeed, it's on your HW!)

The other property of electrical networks we're going to use throughout our proofs is Rayleigh's Monotonicity Theorem, which we state here:

Theorem 9. If any of the individual resistances in a circuit increase, then the overall effective resistance of the circuit can only increase or stay constant; conversely, if any of the individual resistances in a circuit decrease, the overall effective resistance of the circuit can only decrease or stay constant.

In specific, cutting wires (setting certain resistances to infinity) only increases the effective resistance, while fusing vertices together (setting certain resistances to 0) only decreases the effective resistance.

We also omit the proof of the statement here (again, it's on your HW!)

8 Random Walks in \mathbb{Z}^d

Given these tools, we are now equipped to tackle our question! Let's turn to \mathbb{Z}^1 , as a quick warm-up. Our question, then, is whether a random walker starting at some point on the integer line (say the origin) will always return to the origin, or whether there's a nonzero chance that it wanders off forever.

All of our tools, as currently formulated, only apply to finite graphs. So, to study an infinite graph like \mathbb{Z}^d , we need to do the following:

- Let x be whichever node we're designating as the origin, and $G^{(r)}$ be the graph formed by taking all of the vertices connected to x by paths of length at most r.
- Turn this into a electrical network problem by soldering all of the vertices that are distance r from x together into one big ball (i.e. identifying all of these vertices together,) grounding them, putting one unit of voltage at x, and making all of the edges resistors with resistance 1. Then, via our earlier discussions, we can talk about the probability that a drunkard starting at x will make it to this point at distance r before returning to x. Denote this quantity as $p_{esc}^{(r)}$.
- Let p_{esc} be the limit $\lim_{r\to\infty} p_{\text{esc}}^{(r)}$. If this is nonzero, then there is some nonzero chance that our walker will wander forever; if this is zero, then our walker must eventually return to the origin.
- Notice that if it must eventually return to the origin, then it must eventually make it to any vertex w in G! This is because starting from the origin, we always have some nonzero chance to make it to w, and (because we return to the origin infinitely many times) we get infinitely many tries.

If G is a graph on which we return infinitely many times to the origin, we call G recurrent; if it is a graph where there is a chance that we will never return to the origin, we call G transient.

Theorem 10. The one-dimensional lattice graph \mathbb{Z} is recurrent.

Proof. Let 0 be the origin, without any loss of generality. Using our earlier discussion, we know that

$$p_{\rm esc}^{(r)} = \frac{i_0}{C_0} = \frac{1}{C_0} \cdot \frac{v(0)}{R_{\rm eff}} = \frac{1}{C_0 R_{\rm eff}}$$

We know that the resistance of a string of r resistors in a row is r, from our earlier discussion about resistors in series. Consequently, because there are two such strings in parallel from the origin to distance r for any r, we know that their combined resistance is $\frac{1}{r} + \frac{1}{r} = \frac{r}{2}$. Therefore, because the conductance of the origin is 1 + 1 = 2, we have

$$p_{\rm esc}^{(r)} = \frac{1}{2 \cdot r/2} = \frac{1}{r}.$$

The limit as r goes to infinity of this quantity is 0; therefore, this walk is recurrent. \Box

Theorem 11. The two-dimensional lattice graph \mathbb{Z}^2 is recurrent.

Proof. Take our graph, turn it into an electrical network with origin = (0, 0), and perform the following really clever trick: for every r, let V_r be the collection of all of the vertices that are distance r from the origin under the taxicab metric (i.e. shortest length of a path.) Take our graph and **short** all of V_r 's vertices into one huge clump, for each r: i.e. take the collection of all of the vertices at distance r, and just stick them all together! In essence, we are adding wires between all of the vertices at distance r with resistance 0, which (if you think of these wires not as connecting vertices that didn't use to be connected, but rather as replacing the wires of resistance " ∞ " between such vertices) is decreasing the resistance between certain vertices. We know that this reduces the overall resistance, because of Rayleigh's principle; therefore, we know that if this graph is recurrent, \mathbb{Z}^2 must be as well.

What does this process do to the graph $(\mathbb{Z}^2)^{(r)}$? Well, it produces the following picture:



Note that there are 8n + 4 edges between the vertices at distance n and the vertices at distance n + 1, which we prove by induction:

• The base case is clearly true: there are 4 edges from the origin to the points (±1,0), (0,±1) that are distance 1 from the origin.

- Now, notice that the collection of points at distance n forms a diamond, with corners given by the points $(\pm n, 0)$, $(0, \pm n)$ and side points given by points of the form (a, b) with |a| + |b| = n. There are 4 corner points and 4(n 1) side points, an observation that you can either simply take as obviously true or as something we are proving by induction in the course of this proof.
- Each corner point has three edges connecting to points of distance n+1, and each side point has two edges connecting to points at distance n + 1. Therefore, by induction, we know that there are $3 \cdot 4 + 2 \cdot 4(n-1) = 8n + 4$ edges to points at distance n + 1! (Of these edges at distance n + 1, the new corner points each have one edge to a point at distance n, while the side points each have 2 edges to points at distance n. This, plus our observation that there are 8n + 4 edges in total, tells us that there are 4 new corner points and (8n + 4 - 4)/2 = 4n = 4((n + 1) - 1) new side points, if you were worried about that.)

What is the resistance here? Well: if there are 8n + 4 resistors between node n and node n + 1, we can regard our graph as equivalent to the path on $\{0, \ldots r\}$ where the resistance between vertices n and n + 1 is $\frac{1}{8n+4}$:



By adding these resistances together, we can finally calculate the effective resistance of this "shorted" $(\mathbb{Z}^2)^{(r)}$:

$$\sum_{i=1}^{r} \frac{1}{8i+4}$$

This sum diverges to infinity! Therefore, the current on these graphs, and thus the $p_{\text{esc}}^{(r)}$'s, must converge to 0. So $(\mathbb{Z}^2)^{(r)}$ is also recurrent.

Lemma 12. Suppose C is a circuit with two vertices x, y that are not connected by a resistor and are at the same potential: i.e. v(x) = v(y). Then shorting together x and y does not change the voltages or currents in the circuit.

Proof. Take any such circuit C, and let C' denote the same circuit where x, y are joined by a wire of resistance R_{xy} .

Initially, suppose that $R_{xy} = \infty$; then these are literally the same circuits, as we interpreted any nonexistent wire as a wire with infinite resistance.

Notice that in C', there is no current flowing from x to y, as $v(x) = v(y) \Rightarrow \frac{v(x) - v(y)}{R_{xy}} = 0$. Suppose we change R_{xy} in C' to some finite value. I claim that nothing changes.

To see why, take all of the equations for C''s circuit that we need to satisfy, and substitute in the voltage and current values from C. If we still satisfy all of these equations, then the uniqueness of our solutions implies that the currents and voltages have not changed from C to C'.

The only equations that may have changed are those that refer to R_{xy} . Of those, all of those equations are either the one instance of Ohm's law:

$$i_{xy} = \frac{v(x) - v(y)}{R_{xy}}$$

or any instance of Kirchoff's law that refers to i_{xy} .

However, the Ohm's law equation is still 0, as we're assuming that v(x) = v(y); so nothing has changed there. Therefore, in each instance of Kirchoff's law that refers to i_{xy} , nothing has changed as well; we had $i_{xy} = 0$ in C, and it's still 0 in C'.

Therefore, our voltages and currents for C satisfy all of the equations for C'; consequently, they did not change when we went from C to C'.

So: what happens in three dimensions?