# 20200109

## Well-Ordering

Sometimes we can interpret a relation on a set as an **ordering** of the set ... if the pair (a,b) is in the relation, then we can say “a comes before b”. For example, the relation might be “is a biological ancestor of” on a set of people or “must be compiled before” on a set of software modules. Some sets have natural orders, such as the set of integers or the set of real numbers. For these sets of numbers, the natural order is based on our understanding of “less than” and “less than or equal”. They have the property that for any two different numbers x and y, we know that either x < y or y < x ... in other words, either (x,y) or (y,x) is in the relation. For other sets and relations there may be some pairs that are not related. For example we can easily find two persons x and y where neither one is a biological ancestor of the other.

In these notes, I will occasionally include “enrichment” material that is included for the people who are *really* interested in the topic. If you are reading these notes for the purpose of getting the essential information so you can get on with solving practice problems etc., you can skip over the extra material. Extra material will be in ***bold italic*** font and enclosed in < > braces. Like this:

***<Is “$\leq$” the only ordering we can define for the natural numbers? No! There are infinitely many others. For example we can order the natural numbers based on their prime factorization, with the primes in ascending order ( $\leq$ order) treated as a list for each number. So 20 is represented by the list (2,2,5) and 1001 is represented by the list (7,11,13). [By the way, I just explained the mental arithmetic trick I did on Day 1.] We can call these the “prime-lists” of the integers. Note that the prime-list of a prime number contains just the prime itself. Now we can define the relation $\preceq$ on $\mathbb{N}$ by***

$0 \preceq x \quad \forall x \in \mathbb{N}$

$1 \preceq x \quad \forall x \in \mathbb{N}$ except $0$

$a \preceq b$ iff $a = b$ ***or prime_list(a) comes before prime-list(b) using standard dictionary rules***[1] $\forall a, b > 1$

***This ordering looks like 0,1,2,4,8,16,...,6,18,54,...,3,9,27,....15,75,375,....5,35,245,... where each set of ... represents infinitely many integers between the groups shown. We can't write down the list, but the ordering is well defined! For any two distinct integers a and b,***

---

1 Dictionary ordering of words compares letters from left to right. If the first two letters are different, the word that starts with the earlier letter comes first. If the first two letters are the same, the comparison is based on the remaining letters. If one word is a prefix of the other (such as “cat” and “catch”) the shorter word is listed before the longer. This can easily be applied to lists of numbers. For example, (2,2,3,7) comes before (3,5) because 2 < 3, and (7,13) comes before (7,13,23)

***we can determine which comes before the other in this ordering. Math is wonderful.***

***We can also create prime-list based orderings in which shorter lists come before longer lists, with ties are broken by the actual values of the numbers. This ordering looks like this (using the same rules for 0 and 1):***
***0, 1, 2, 3, 5, 7, 11, 13 ... 4, 6, 10, 14, 22, 26 ... 9, 15, 21, 33 ... 8, 12, 20, 28 ...***

***Another way to order the integers is to use alphabetical order on their standard names in English. So "eight thousand nine hundred and forty-seven" comes before "one" etc. The interesting thing about this ordering is that even though it contains infinitely many numbers, we know exactly what the last number in the list is: zero ! The idea of an infinite ordering having a known final element is a bit of a mind-twister.***

***There are infinitely many other rules we can use to order the integers. The patterns hidden in the integers are enough to occupy us for a lifetime.***

***The*** $\preceq$ ***symbol is often used to represent an unspecified ordering – not just the one we defined here.>***

We will look at orderings in more detail later in the course. For now we will focus on **The Well-Ordering Principle**.

Definition: Suppose S is a set with a defined *anti-symmetric*[2] relation R, and S contains an element x such that $(x, y) \in R \;\; \forall y \in S$ . We say that **x is a minimum (or least) element of S, with respect to R.**

Definition: If S is a set with a defined anti-symmetric relation R, **and** it is the case that every non-empty subset of S contains a least element with respect to R, then we say that **S is well-ordered with respect to R.**

Note that not all sets are well ordered with respect to all anti-symmetric relations. For example, consider the set $\mathbb{Z}$ of all integers, and let the relation be $\leq$. The subset {-1,-2,-3,...} has no least element, so $\mathbb{Z}$ is not well-ordered with respect to $\leq$.

---

2 *Anti-symmetry* is the relation property that nobody can ever remember. Basically, saying a relation R is anti-symmetric means that when a and b are different elements, we can't have both (a,b) and (b,a) in R. When thinking about these well-ordered sets, you really can't go wrong by just thinking about $\leq$ for integers. If a and b are different integers, we can have a $\leq$ b, or we can have b $\leq$ a, but we can't have both.

Practice questions: Let S = {1,2,3,4} Which of the following relations are anti-symmetric?

1. R = {(1,1),(1,2),(2,3),(4,1),(1,3),(4,2)}
2. R = {(2,2),(3,3)}
3. R = $\emptyset$

***<Here's a great challenge: find a relation $\preceq$ such that $\mathbb{Z}$ is well-ordered with respect to $\preceq$>***

Here are a couple of useful facts about well-ordered sets:

If a set S is well-ordered with respect to a relation R, then every subset of S is also well-ordered with respect to R ... this follows directly from the definition of well-ordering.

If a set S is **not** well-ordered with respect to a relation R, then every set that contains S is also not well-ordered with respect to R. This follows directly from the first fact.

The **Well-Ordering Principle : The set of natural numbers $\mathbb{N}$ = {0, 1, 2, 3, ...} is well-ordered with respect to $\leq$**

We state this without proof ... it should be clear that in any non-empty subset of $\mathbb{N}$ there is a least element.

This may seem so obvious that you might wonder why we bother stating it and why we give it a fancy name. It's important to state it because, as mentioned above, there are useful sets of numbers for which well-ordering does not apply. For example, consider the set $S = \left\{ \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots \right\}$ . S has no least element with respect to $\leq$, so S is not well-ordered. S is a subset of $\mathbb{Q}$ (the rational numbers), so $\mathbb{Q}$ is not well-ordered with respect to $\leq$ . And since $\mathbb{Q}$ is not well-ordered with respect to $\leq$, this means that $\mathbb{R}$ (the real numbers) is not well-ordered with respect to $\leq$ either.

**<However, it is easy to define a relation for which S *is* well-ordered. Think about how you do this before you check out my answer in this footnote[3]. >**

That fact that $\mathbb{N}$ **is** well-ordered (and we usually don't bother to state the "with respect to ..." part because we all know what the relation is ... it is just $\leq$) makes it possible to prove some interesting properties of integers. Even more importantly, it lets us prove things that are much more complex than integers, but which can be placed in a one-to-one correspondence

---

[3] Remember, even though $\leq$ is the most natural ordering to use on sets of numbers, there is nothing in the definition of well-ordering that requires us to use $\leq$. So for the set S = {1/2, 1/4, 1/8, ...} we can observe that each element is of the form $1/2^k$ where k is an integer. Then we can define the relation $R^* = \{(1/2^a, 1/2^b) \mid \quad 1 \leq a \leq b\}$ ... you should satisfy yourself that S is well-ordered with respect to $R^*$ (Note that $R^*$ is just a fancy way of writing $\geq$ for this set)

with the integers. Later in the course we may have the opportunity to explore well-ordering in other contexts.

The Well-Ordering Principle lies behind a specialized form of Proof by Contradiction, known as **Proof by Minimal Counter-example**. This name is a bit misleading because it seems to be self-contradictory ... if there is a counter-example, how can there be a proof? The full name of the proof technique should probably be **Proof By Contradiction That Involves Showing That There Cannot Exist a Minimal Counter-Example**, but PBCTISTTCEMCE is just too long to be practical.

**PMCE** works like this. Suppose we want to prove some statement P about all elements of some subset $S \subseteq \mathbb{N}$. We start by assuming that P is not true for all elements of S (this is the standard PBC approach). This means that there must exist at least one counter-example in S. This means that the set of counter-examples is non-empty. This means that the set of counter-examples must contain a least element (**by the Well-Ordering Principle**). Let x be this minimum counter-example. And from there, we construct a contradiction. The details of this contradiction depend on the statement P. Sometimes we show that x is not actually a counter-example. Sometimes we show that x is not the minimum counter-example. Either of these contradicts x's status as the minimum counter-example. The contradiction shows that our assumption must be false, so P is true for all elements of S.

**Example of Proof By Minimal Counter-Example**

Claim: Every integer $\geq 2$ is either prime or can be written as the product of primes.

Proof by PMCE:
Suppose the claim is not true.
Then let x be the smallest integer $\geq 2$ such that x is neither prime nor the product of primes

(This is a collapsed version of these steps:
Claim not true => there is a counter-example
=> the set of counter-examples is non-empty
=> the set of counter-examples has a least element
Call the minimum counter-example x)

Since x is not prime, x must be composite. (This comes from the definition of prime numbers.)

x composite => x = w*z where w and z are integers and $2 \leq w < x$ and $2 \leq z < x$

Since x is the minimum counter-example and w and z are both < x, **w and z cannot be counter-examples** (*this is where we see the purpose of choosing x to be the* ***minimum*** *counter-example*). So each of w and z must either be prime or the product of primes. Either way, we can write x as the product of primes. But that contradicts our assertion that x is not the product of primes. $\otimes$ (That's the contradiction symbol I like to use.)

Our assumption that the claim is false led to a contradiction, so we conclude that the claim is true.

We'll do another example of PMCE on Monday.