PROOFS/NOTES

NIKHIL VASAN

1. Casper FFG

Definition 1.1. ***CheckPoint***: *Let $B \in \mathcal{B}$, then B is a checkpoint iff $B = B_{genesis}$ or $h(B) \equiv 0(100)$, where $h : \mathcal{B} \to \mathbb{N}$ is the height function of the block-tree*

The *(CheckpointHeight)* $\tilde{h} : \mathcal{B} \to \mathbb{Z}$, is defined as follows

$$for B \in \mathcal{B}, \tilde{h(B)} = \lfloor h(B) \rfloor \tag{1.1}$$

Let $\mathcal{V}$ be the set of validators for the chain, then $d : \mathcal{V} \to [0, 1]$ is the deposit mapping, mapping validators to their respective deposits.

Definition 1.2. ***Vote*** *: A signed message, $\langle v, s, t, h(s), h(t)\rangle$, where $s, t \in \mathcal{B}$, and $h(s) >= h(t) + 1$, $s \in child(t)$*

Notice, that when a block $b \in \mathcal{B}$ is referred, generally, one refers to the merkle root hash of the contents of the block, as communication complexity would scale rapidly with the number of messages sent / $|\mathcal{V}|$. Further definitions follow,

Definition 1.3. *We define*

supermajority link : $SL \in \mathcal{B}^2$, *where* $(a, b) \in \mathcal{B}$ *iff* $sum_{v \in \mathcal{V}_{vote(a,b)}} d(v) >= 2/3$

conflicting : $B_1, B_2 \in \mathcal{C}$ *(checkpoints) are conflicting iff,* $B_1 \notin child(B_2)$ *and* $B_2 \notin child(B_1)$

justified : $c \in \mathcal{C}$ *is justified if (1) it is the root, or there exists* $s \in SL$ *where* $s = (c', c)$, *where* c' *is justified.*

finalized : $c \in \mathcal{C}$ *is justified if (1) it is the genesis block or (2) it is justified, and there is a supermajority link* $c \to c'$ *where* c' *is a direct child of c, that is* $h(c') = h(c) + 1$

Definition 1.4 (*slashing conditions*)**.** *A validator, $v \in \mathcal{V}$, is slashed, $d(v) = 0$ if, a validator publishes two votes $\langle v, s_1, t_1, h(s_1), h(t_1)\rangle$, $\langle v, s_2, t_2, h(s_2), h(t_2)\rangle$*

(1) $h(t_1) = h(t_2)$

(2) $h(s_1) < h(2_1) < h(t_2) < h(t_1)$

2. Proof of safety and Plausible Liveness

Theorem 2.1 ((**Accountable Safety**))**.** *Two conflicting checkpoints a_m and b_n cannot both be finalized.*

2.1. Fix $a_m, b_n \in \mathcal{C}$ where both $a_m \notin chain(b_n)$ and $b_n \notin chain(a_m)$. Intending contradiction, suppose both a_m and b_n are finalized. Naturally $h(a_m) \neq h(b_n)$, thus, we may assume WLOG that $h(a_m) > h(b_n)$. Denote b_{n+1} denote the checkpoint finalizing b_n,

Date: September 2021.

where $h(b_{n+1}) = h(b_n) + 1$, a similar case follows for a_{m+1}. Denote $a' \in chain(a_n)$ to be the first ancestor of a_n where $h(a') < h(b_n)$. Naturally a'_n the block finalizing a_n satisfies $h(a'_n) > h(b_{n+1})$, violating slashin condition **II**. □

Definition 2.2. *Denote $\mathcal{DS} : \mathcal{V} \rightarrow \mathbb{Z}$, the mapping between validators and their start dynasty. Where $\mathcal{DS}(v) = d + 2$, when v has submitted a deposit message at blockc with slot 2. The mapping $\mathcal{DE}(v) : \mathcal{V} \rightarrow \mathbb{Z}$ maps validators to their end dynasty.*

3. Gasper

4. Tendermint

Concensus for each block at height h_p proceeds in rounds, $round_p$, three types of messages for each round are passed

Definition 4.1. *The messages defined are...*

(Proposal) : *$\langle PROPOSAL, h_p, round_p, proposal, validRound_p\rangle$, where $proposal$ is the value on which all nodes will come to concensus upon, given the size of the msg, to reduce message complexity of later messages, $id(v)$ a proof of fixed size is passed between nodes*

(Prevote) : *$\langle PREVOTE, h_p, round_p, id(v)\rangle$, this message type defines a vote for the corresponding value $decode_p(id(v))$, in the first round of voting,, notice $id(v) == nil$ if $isValid(v) == false$.*

(PreCommit) : *$\langle PRECOMMIT, h_p, round_p, id(v)\rangle$, this message defines the standard type for the second round of voting*

At each round a set of 5 state variables are maintained by all $correct$ processes

Definition 4.2. *These variables are reset at the beginning of each concensus instance*

(h_p) *Identifier of the current concensus instance... height*

$(round_p)$ *Round number for this concensus instance*

$(decision_p...)$: *the set of finalized blocks, where $decison_p(h_p) = Tendermint(v)$ (block to finalize at current height)*

$(lockedValue/lockedRound)$: *These values store the most recent value precommited and the round at which the pre-commit was sent at which the process p received $2f + 1$ prevotes for a value v, and the value v, that is*

```
prevotes := make([]Prevote)

if len(prevotes) >= 2 * f + 1 {
  lockedRound = curRound
  lockedValue = value
  broadcast(Precommit{
    step: PRECOMMIT,
    height: curHeight,
    round: curRound
```

```
    id: hash(curValue),
  })
}
```

$(validValue/validRound)$ *These values serve a similar purpose to the lockedRound/Value, except these values record the first value that represents a possible decision value.*

Theorem 4.3. *For all $f \geq 0$ all sets of $2f + 1$ processes, have at least $f + 1$ process in common*

Theorem 4.4. *Notice, $n = 3f + 1$, where n is the total number of processes participating in the network. Therefore,*

Proof. 2(2f + 1) = 3f + 1 + f + 1 = n + f + 1 □

therefore by the pigeonhole principle, there is at least $f + 1 - f = 1$ correct nodes in common between two sets.

Theorem 4.5. *If $f + 1$ correct processes lock value v in round r_0 then in all round $r > r_0$ they send $PREVOTE$ for $id(v)$ or nil*

Proof. The proof is by induction on i, where r_i designates the current round. For r_1, the $f + 1$ processes that had locked v, $validValue = v$, thus if they are the proposer they broadcast $\langle PREVOTE, h_p, r_1, id(v)\rangle$, if they are not the proposer, and receive a Proposal for v' where $v' \neq v$ notice $lockedRound \neq -1$ and $lockedValue \neq v'$ thus they broadcast a prevote for nil. Assuming the hypothesis holds for n, then for round r_{n+1}, $validValue = v$ and $validRound = r_0$. That is, it is impossible for $2f + 1$ Prevotes to be signed for a conflicting value v', thus, the locked value will remain the same, and by the hypothesis, all nodes will broadcast prevotes for nil or v. □

5. COSMOS FEE DISTRIBUTION

Suppose a delegator x delegates x stake to validator v at block i and withdraws at block h, then the accum is defined as follows

$$accum = x\Sigma_{k=i}^{h}\frac{f_i}{s_i} \tag{5.1}$$

where f_i represents the total tx fees each block, and s_i represents the delegated stake for the validator at each block. Notice, the delegated stake only changes whenever a delegation is changed, as such, we may desigate the periods between delegation modifications as a $period$

Definition 5.1. ***Period**: Time between a validator's stake $\mathbf{S}_v$ changing*

The new calculation is as follows

$$accum_d = \Sigma_{k=p_{init}}^{p_{final}}\frac{T_p}{S_p} \tag{5.2}$$

where T_p is the total tx fees per period, and S_p is the total stake per period. Notice, this calculation lends itself to a recursive expression

$$entry_f = entry_{f-1} + \frac{T_f}{s_f} \tag{5.3}$$

Each entry is a state object indexable by f (Period Number). The maximal number of entries stored in state is

$$curPeriod - min_{d \in \mathcal{D}}(Period(d)) \tag{5.4}$$

where $d \in \mathcal{D}$ represents iteration over all delegations. Each delegators reward earned from withdrawing may be represented as follows

$$accum = x(entry_k - entry_f) \tag{5.5}$$

6. LP Token Pricing ($xy = k$) CFMM

Consider a pool obeying the following invariant, $r_0 * r_1 = k$, where r_0 is the reserves of $asset_0$ and r_1 is the reserve of $asset_1$. Notice, in this case the prices of $asset_0$ in terms of $asset_1$, is determined as follows

$$p_0 = \frac{\Delta r_0}{\Delta r_1}, p_1 = \frac{1}{p_0} \tag{6.1}$$

notice, Δr_0 may be determined as follows,

$$(r_1 + \Delta r_1)(r_0 - \Delta r_0) = k = r_0 * r_1 \tag{6.2}$$

$$\Delta r_0 = r_0 - \frac{k}{r_1 + \Delta r_1} = \frac{r_0(r_1 + \Delta r_1)}{r_1 + \Delta r_1} - \frac{r_0 * r_1}{r_1 + \Delta r_1} \tag{6.3}$$

$$= \frac{r_0 \Delta r_1}{r_1 + \Delta r_1} \tag{6.4}$$

substituting this value into p_0, one obtains

$$p_0 = \frac{\Delta r_0}{\Delta r_1} = \frac{r_0 \Delta r_1}{r_1 + \Delta r_1} * \frac{1}{\Delta r_1} = \frac{r_0}{r_1 + \Delta r_1} \tag{6.5}$$

Let $TVL = r_0 * p_0 + r_1 * p_1$, in this case, we may parametrize TVL in terms of Δr_1 and r_0, r_1,

$$TVL = r_0 * p_0 + r_1 = r_0 * \frac{r_0}{r_1 + \Delta r_1} + r_1 \tag{6.6}$$

7. Math

Theorem 7.1. *$\forall x_1, x_2, x_1 \leq x_2 \to f(x_1) \leq f(x_2), f(f(x)) = x$ implies that, $f(x) = x$,*

Proof. □

Theorem 7.2. *Let E be a non-empty subset of an ordered set; suppose α is a lower bound of E and β is an upper bound of E. Prove that $\alpha \leq \beta$.*

Proof. Denote $\leq$ the ordering over E, that is, $\leq$ a transitive relation. As such, fix $e \in E$. Notice, as α is a lower-bound of E, it follows that $\alpha \leq e$, furthermore, $e \leq \beta$, combining the relations, and applying the transitivity of $\leq$, obtains $\alpha \leq \beta$, as was to be shown. □

Theorem 7.3. *Let A be a non-empty set of real numbers which is bounded below. Let $-A$ be the set of all numbers $-x$, where $x \in A$. It follows*

$$infA = -sup(-A) \tag{7.1}$$

Proof. The least upper bound (greatest lower bound) property of $\mathbb{R}$ indicates that $inf(A) = \alpha$ exists (A is non-empty and bound below). Furthermore, Let $l \in \mathbb{R}$ be a lower bound for A, that is, $\forall x \in A, x \geq l$, thus $\forall x \in A, -l \geq -x$, and $-l$ is an upper-bound of $-A$, as $-A$ is non-empty and bound above $sup(-A) = \beta$ exists in $\mathbb{R}$. Suppose $-\beta > \alpha$, as $-\beta$ is a lower bound of A ($\forall x \in -A, x \leq -\beta \to \forall x' = -x \in A, x \geq \beta$), this contradicts $\alpha = inf(A)$. A similar proof follows for the other direction. Thus $-\beta = \alpha$. □

Fix $b > 1$

(6a) If $m, n, p, q$are integers, $n > 0$, $q > 0$, and $r = m/n = p/q$, prove that

$$(b^m)^{1/n} = (b^p)^{1/q} \tag{7.2}$$

Proof. Notice $(b^{1/n})^m = (b^{1/q})^p = b^{m/n} = b^{p/q} = b^r$ □

(6b) Prove that $b^{r+s} = b^r b^s$ if r and s are rational.

Proof. Let $r = m/n$ and $s = p/q$, thus $b^{r+s} = b^{m/n+p/q} = b^{\frac{mq+np}{nq}} = (b^{mq}b^{np})^{\frac{1}{nq}} = b^r b^s$ □

6c If x is real, define $B(x)$ t be the set of all numbers b^t, where t is rational and $t \leq x$. Prove that

$$b^r = sup(B(r)) \tag{7.3}$$

Proof. Fix $x \in \mathbb{Q}$, thus $x = m/n$ for $m, n \in \mathbb{Z}$. Consider $B(x)$, naturally $B(x)$, is non-empty, furthermore, $B(x) \subset \mathbb{R}$, finally, $B(r)$ is bound above by b^r, and thus $\alpha = supB(x)$ exists. Suppose, $\alpha \neq b^x$. WLOG (the other direction guarantees a similar maximal / minimal element), suppose $\alpha > b^x$ Notice, the archimedian proprty of real numbers guarantees □

7d If w is such that $b^w < y$, then $b^{w+(1/n)} < y$ for sufficiently large n.

Proof. Via $7c$, it suffices to show that $\frac{b-1}{yb^{-w}-1} < n$, for some n. Thus, $b - 1 < n(yb^{-w} - 1)$, for some n. Notice, as $b, (yb^{-w} - 1) \in \mathbb{R}_{>0}$, there exists, $n \in \mathbb{Z}$, where $b - 1 < n(yb^{-w} - 1)$. □

7e If $b^w > y$,then $b^{w-1/n} > y$ for sufficiently large n.

let A be a set, then A is infinite, if A is equivalent to one of its proper subsets.

Theorem 7.4. *Every infinite subset of a countable set A is countable*

Proof. Suppose $E \subset A$. Let $f : \mathbb{N} \to E$, as follows. Denote $f(1) = e_1$, where $e_1 \in E$, and for all $e \in E, e > e_1$, set $f(i)$ to be the smallest $e_i \in E$, such that $e_i > f(i-1)$. Suppose $i, j \in \mathbb{N}$, where $i \neq j$. WLOG, $i < j$, in which case, $f(i) < f(j)$, thus $f(i) \neq f(j)$, and f is injective. Suppose $\exists e \in E \subset A$, for which, no pre-image exists in $\mathbb{N}$, this is a contradiction. □

Theorem 7.5. *Let A be a countable set, and let B_n be the set of all n-tuples of A, that is A^n.*

Proof. The hypothesis holds trivially for $n = 1$, as $A^1 = A$ which is countable. Suppose the theorem holds for $n - 1$, then $x \ inB^n, x = (b, a), b \in B^{n-1}a \in A$, notice, for all $b \in B^{n-1}$, the set $(b, a), a \in A$ is countable. Thus $B^n = \Cup_{b \in B^{n-1}}(b, a)$, this is a countable union of countable sets, and is countable by (15). Thus B^n is countable. The proof follows by induction. □

Definition 7.6. *Let A be a set, a function $f : A \to \mathbb{R}_{\geq 0}$ is a metric function if*

1 $p, q \in A, d(p, q) = 0 \iff p = q$,

2 $p, q \in A, d(p, q) = d(q, p)$,

3 $d(p, q) \leq d(p, r) + d(r, q)$

A metric space, is a tuple (A, σ), where A is a set and σ is a metric function over A

Definition 7.7. *A subset $E \subset \mathbb{R}^k$ is convex, if for all $x, y \in E$, $\lambda x + (1-\lambda)y \in E$.*

Theorem 7.8. *Balls are convex*

Proof. Fix a ball $E \subset \mathbb{R}^k$ with center $z \in \mathbb{R}^k$. Fix $x, y \in E$, fix $0 < \lambda < 1$, Thus,

$$|z - (\lambda x + (1-\lambda)y| = |\lambda(z-x) + (1-\lambda)(z-y)| \leq \lambda|z-x| + (1-\lambda)|z-y| \tag{7.4}$$

$$< \lambda r + (1-\lambda)r = r \tag{7.5}$$

Thus $(\lambda x + (1-\lambda)y) \in E$, and E is a convex set. □

Let X be a metrix space,

(a) A *neighbourhood* of p, $N_r(p) := \{q \in X : d(q, p) < r\}$

(b) A point p is a *Limit Point* of the set E if, $\forall r, \exists (q)(q \neq p) \in N_r(p), q \notin E$

(c) $p \in E$ is an *Isolated Point* of E, if p is not a limit point of E

(d) E is *closed* if every limit point p is an element of E

(e) A point $p \in E$ is an *interior* point of E, if $\exists r, N_r(p) \subset E$

(f) E is *open* if every point of E is an interior point of E

(g) The *complement* of E, $E^c := \{p \in X, p \notin E\}$

(h) E is *perfect*, if E is closed, and every point of E is a limit point of E

(i) E is *bounded* if $\exists M \in \mathbb{R}$ and $q \in X$ such that, $d(p, q) < M, \forall p \in E$

(j) E is *dense* in X if every point of $p \in X$ is a limit point of E or $p \in E$.

Theorem 7.9. *If X is a metric space, and $E \subset X$, then*

(a) $\bar{E}$ is closed

(a) $\bar{E} = E$ iff E is closed

(c) $\bar{E} \subset F$ for every closed set $F \subset X$ such that $E \subset F$.

Proof. For (a), let $p \in \bar{E}^c$, that is $p \notin E \wedge p \notin \bar{E}$, as such, $\exists r > 0 \in \mathbb{R}$, where for all $q \in N_r(p), (p \neq q), q \notin E$. If $N_r(p) \cap \bar{E} = \{x..\}$. Then $\forall r \in \mathbb{R}, \exists x \in N_r(p) \cap \bar{E}$, thus, $x \in \bar{E}$, $x \notin \bar{E}^c$. As such, $\forall x \in \bar{E}^c, \exists r \in \mathbb{R}, N_r(x) \subset \bar{E}^c$, and $\bar{E}^c$ is open, thus $\bar{E}^{c^c} = \bar{E}$

is closed.
For (b). Suppose E is closed, then $x \in E' \subset E$ implies that $x \in E$, $\bar{E} = E' \cup E = E$. Suppose $\bar{E} = E$, then suppose $x \in E' \subset \bar{E} = E$, and $x \in E$, therefore, E is closed. For (c), ☐

Definition 7.10. ***Open Cover*** *- Let X be a metric space, $E \subset X$. Then an Open Cover of E, is $\{G_\alpha\}, \forall\alpha, G_\alpha \subset \mathcal{O}(X)$, and $E \subset \cup_\alpha G_\alpha$*

Definition 7.11. ***Compactness*** *- A set E of metric space X, is Compact if every open cover of E, $\{G_\alpha\}_\alpha$, has finitely many indices $\alpha_1, \cdots, \alpha_n$, where $E \subset \cup_i, G_{\alpha_i}$*

Definition 7.12. *Suppose $K \subset Y \subset X$. THen K is compact relative to X iff K is compact relative to Y*

Proof. Suppose K is compact in X, then $K \subset \cup_{i=1...n} G_{\alpha_i}$, where $\{G_\alpha\}$ are open relative to Y. As such, $G'_\alpha \cap Y = G_\alpha$ where G'_α are open in X, and $K \subset \cup_i G'_{\alpha_i}$, as $\{G'_{\alpha_i}\}$ is an open cover of K in X, there exists $\alpha_1 ... \alpha_n$, where $K \subset G'_{\alpha_1} \cup ... \cup G'_{\alpha_n}$. As such, $K \cap Y = K \subset (G'_{\alpha_1} \cup ... \cup G'_{\alpha_n}) \cap Y = G_{\alpha_1} ... G_{\alpha_n}$, and every open cover relative to Y has a finite subcover, thus K is compact in Y.
Suppose K is compact in $Y \subset X$, then for every open cover $\{G_\alpha\}_\alpha$ in Y, there exist G'_α open in X, where $G'_\alpha \cap Y = G_\alpha$. And, $K \subset \cup_{\alpha_i} G_\alpha \subset \cup_i G'_{\alpha_i}$, and K is compact in X. ☐

Definition 7.13. *Compact subsets of metric spaces are closed.*

Proof. Let K be a compact subset of a metric sapce X. Fix $p \in K^c$, and $q \in K$, let V_q be a neighbourhood of p with $r < 1/2d(p,q)$, notice $V_q \cap W_q = \emptyset$. Notice, $K \subset \cup_{q \in K} W_q$, as K is compact, $K \subset \cup_{i=1...n} W_{q_i}$, furthermore, $V = \cap_{i=1...n} V_{q_i}$, $V \cap W = \emptyset$, and $r = min_{i=q..n}(d(p,q_i)), N_r(p) \subset V$, thus there exists $N_r(p) \subset K^c$, for all $p \in K^c$, and K^c is open. ☐

Definition 7.14. *Closed subsets of compact sets are compact*

Proof. Let, $L \subset K \subset X$, where X is a metric space, K is compact, and L is closed. Fix V_α, an open cover of K, notice $(\cup_\alpha V_\alpha) \cup L^c$ covers K, thus there exists a finite-subcover $V_{\alpha_i} \cup L^c$, as $L \not\subset L^c$, V_α has a finite subcover covering L, and L is compact. ☐

Theorem 7.15. *If F is closed and K is compact, then $F \cap K$ is compact.*

Proof. Notice, $F \cap K \subset K$ is closed, thus, $F \cap K$ is compact. ☐

Theorem 7.16. *If $\{K_\alpha\}$ is a collection of compact sets of metric space X, such that, the intersection of every finite subcollection of K_α is non-empty, then $\cap K_\alpha$ is not empty.*

Proof. Suppose $\cap_\alpha K_\alpha = \emptyset$, then $\cup_\alpha K^c_\alpha = X$, as such, there exists $K \in K_\alpha, K \subset \cup_\alpha K^c_\alpha$, notice, $\{K^c_\alpha\}$ is an open-cover of K, and $K \subset \cup_{i=1..n} K^c_{\alpha_i}$, however, $K \cap (\cap_{i=1..n} K_{\alpha_i}) \neq \emptyset$, a contradiction. ☐

Theorem 7.17. *Let $\{I_n\}$ be an infinite collection of intervals in $\mathbb{R}^1$, where $I_{n+1} \subset I_n$, then $\cap_i I_i \neq \emptyset$*

Proof. Let $I_n = [a_n, b_n]$, let $E = \{a_n \in \mathbb{R} : I_n = [a_n, b_n]\}$, then $E \subset \mathbb{R}$, and is bound above, namely by b_1. Fix $sup(E) = x$. Fix n, then $I_n = [a_n, b_n]$, naturally, $a_n \leq x$. Suppose $b_n < x$, then there exists, $a_m \in E, a_m > b_n$, and, $I_m \cap I_n = \emptyset$, this is impossible, and $x \leq b_n$, thus $x \in I_n$, and $x \in \cap_i I_i$. ☐

Theorem 7.18. *Suppose $\{I_n\}$ is a seq. of $k-cells$, where $I_{n+1} \subset I_n$, then, $\cap_i I_i \neq \emptyset$.*

Proof. For I_n, let $I_{n,i} = [a_{n,i}, b_{n,1}]$, where $I_n = \times_{1\leq i\leq k} I_{n,i}$ then, for each $\{I_{n,i}\}$, where $1 \leq i \leq k$, there exists, $x_i \in \cap_{1\leq i\leq k} I_{n,i}$, let $\vec{x} = (x_1, ..., x_k)$, then $\vec{x} \in \cap_i I_i$. □

Theorem 7.19. *Every $k-cell$ is compact*

Proof. Let $I \subset \mathbb{R}^k$, where $I = \times_{1\leq i\leq k} I_i$, where $I_i = [a_i, b_i]$. Fix

$$\delta = (\Sigma_{1\leq i\leq k}(a_i - b_i)^2)^{1/2} \tag{7.6}$$

as such, for $x, y \in I$

$$|x - y| = (\Sigma_{1\leq i\leq k}(x_i - y_i)^2)^{1/2} \leq \delta \tag{7.7}$$

Fix $c_j = (a_j + b_j)/2$, notice, $I_j \subset [a_j, c_j] \cup [c_j, b_j]$, as such, we have Q_i, a set of 2^k k-cells, where $\cup_i Q_i \supset I$. If I is not compact, then for open-cover $\{G_\alpha\}_\alpha$, there exists Q_i such that for any finite subcollection $\{G_{\alpha_i}\}_{\alpha_i}$, $\cup_i G_{\alpha_i} \not\supset Q_i$, continue this process indefinitely, and one obtains, $\{I_n\}$, where $I_n \supset I_{n+1}$ (where I_n is the k-cell obtained from the nth round of this subdvision process). Furthermore, for $x, y \in I_n$, $|x - y| \leq 1/2^n\delta$, and $I_n \not\subset \cup_{\alpha_i} G_{\alpha_i}$. Notice, that 7.18 leaves $x \in \cap_i I_i$, there exists G_α where $x \in G_\alpha$ ($\{G_\alpha\}$ is an open cover of I). For n large enough, $I_n \subset G_\alpha$ (some neighbourhood of x is contained in G_α), this is a contradiction. □

Theorem 7.20. *Any infinite subset $L \subset K$, where K is compact, must have a limit pt. $x \in K$.*

Proof. Suppose $L \subset K$ is infinite, and no limit point of L exists in K, that is, for all $k \in K$ for any neighbourhood of k, $V_k \backslash \{k\} \cap L = \emptyset$ consider the open cover of K, $\{V_k\}_{k\in K}$, no finite subcollection of $\{V_k\}$ covers $L \subset K$, a contradiction. □

Theorem 7.21 (Heine-Borel)**.** *For, metric space $X \subset \mathbb{R}^k$, and $E \subset X$ $E \subset X$ the following statements are equivalent*

(a) E is closed and bounded.

(b) E is compact.

(c) Any infinite subset of E, has a limit point in E.

Proof. For $(a) \to (c)$, if E is closed and bounded, then $E \subset I$, where I is a k-cell. As I is compact, and E is closed, it follows that E is compact. $(b) \to (c)$. For $(c) \to (a)$, suppose E is not bounded, then let $E' = \{|x_n| > n, n = 1, 2, 3, \cdots\}$, $E' \subset E$. Suppose $x \in \mathbb{R}^k$ is a limit point of E', then for all $r > 0$, $N_r(x) \cap S \neq \emptyset$, fix $n', n'+1$, where $|x_{n'}| < |x|$, and $x_{n'+1}| > |x|$, then set $r < min(|x_{n'} - r|, |x_{n'+1} - r|)$, and $N_r(x) \cap S = \emptyset$, a contradiction, thus E must be bounded. Suppose E is not closed, fix x_0 a limit pt. of E, where $x_0 \notin E$. Let $S = \{x_n \in E : |x_n - x_0| < 1/n, n \in \mathbb{N}\}$. Naturally S is infinite, furthermore if y is also a limit pt. of S, then

$$|x_0 - y| \leq |x_0 - x_n| + |x_n - y| < 1/n + |x_n - y| \tag{7.8}$$

If $|x_0 - y| = \epsilon > 0$, then for $n \in \mathbb{N}$, where $1/n < \epsilon$, $r < \epsilon - 1/n$, $N_r(y) \cap S = \emptyset$, otherwise, $|x_n - x_0| < 1/n$, and $|x_n - y| < r$, a contradiction. Thus $x_0 = y$, and E must be closed. □

Theorem 7.22. *Let P be a non-empty perfect set in $\mathbb{R}^k$. Then $\mathbb{R}^k$ is un-countable.*

Proof. P is non-empty, and has a limit-point, thus P is infinite. Suppose P is countable, label $P = \{x_1, x_2, \cdots\}$, construct neighbourhoods $\{V_n\}$, where $\overline{V}_{n+1} \subset V_n$, $x_n \notin \bar{V}_{n+1}$, and $V_n \cap P$ is non-empty, for V_1, fix some neighbourhood of x_1. Naturally, $V_1 \subset P$, and $\bar{V}_1 \subset P$, as P is closed, and $V_1 \cap P \neq \emptyset$. Suppose V_n exists where $V_n \cap P \neq \emptyset$. Notice, if $x_{n+1} \notin V_n$, let $V_{n+1} = N_{r/2}(x_n)$, where $V_n = N_r(x_n)$, otherwise, a similar (yet with diff. radius) neighbourhood can be constructed around x_{n+1}, so that, $x_n \notin V_{n+1}$.
Set $K_n = \overline{V}_n \cap P$, $\overline{V}_n$ is closed and bounded, thus compact, and K_n is the inter. of a closed and compact set, it is itself compact. Furthermore, $K_{n+1} \subset K_n$, furthermore $\bigcap_i K_i \cap P = \emptyset$, this is a contradiction. □

Definition 7.23. *The Cantor Set - A perfect set in $\mathbb{R}^1$ which contains no segment. Let $E_n = \cup_{0 \le i < \lfloor n^2/2 \rfloor} [\frac{2*i}{n^2}, \frac{2*i+1}{n^2}]$. A few properties*

(a) $E_1 \supset E_2 \supset \cdots \supset E_n$

Finally, the Cantor Set is $\cap_n E_n$

As E_1 is compact, $E_n \subset E_1$, is a closed subset of a compact set, and is itself, compact. Furthermore, as $E_i \neq \emptyset$, and the intersection of any finite collection of $\cap_i \{E_i\} = E_{i'}$, where $i' = min(j \in \mathbb{N}, E_j \in \{E_i\})$, $\cap_n E_n$ is non-empty.

Theorem 7.24. *The Cantor Set is perfect.*

Proof. The *Cantor Set* contains no segment. □

Definition 7.25. *Separated Set - Let $A, B \subset X$, where X is a metric space, then A, B are separated iff, $\overline{A} \cap B = \overline{B} \cap A = \emptyset$*

Definition 7.26. *Connected Set - $E \subset X$, a metric space. E is connected iff, E is not the union of two connected sets.*

(1) Prove that the empty set is a subset of every set.

Proof. Suppose $\emptyset \not\subset A$, in which case, $A \cap \emptyset = \emptyset$, a contradiction. □

(2) Prove that the set of *algebraic* numbers is countable.

Proof. For $n \in \mathbb{N}$, denote $A_n = \{z \in \mathbb{C} : P(z)_n = 0\}$, where $P_n(z) = a_0 z^n + \cdots + a_{n-1} z + a_n$. Notice, there are at most $|\mathbb{Z}^n|$, polynomials of degree n, as such, $\cup_n A_n \subset \cup_n P_n$, thus $\cup_n A_n$ is countable, as it is at most an infinite subset, of a *countable* set. □

(3) Prove that there exist real numbers which are not algebraic.

Proof. Suppose otherwise, then $\mathbb{R} \subset \mathbb{A}$, and $\mathbb{R}$ is countable. □

(4) Is the set of all irrational real numbers countable?

Proof. Notice, $\mathbb{R} = \mathbb{Q} \cup \mathbb{R} \backslash \mathbb{Q}$, $\mathbb{Q}$ is countable, thus $\mathbb{R} \backslash \mathbb{Q}$ is un-countable. □

(5) Construct bounded set of real numbers with exactly three limit points.

Proof. $\{0 + 1/n : n \in \mathbb{N}\} \cup \{2 + 1/n : n \in \mathbb{N}\} \cup \{4 + 1/n : n \in \mathbb{N}\}$, notice, $0, 2, 4$ are the only limit points. □

(6) Let E' be the set of all limit points of a set E. Prove that E' is closed. Prove that E and $\bar{E}$ have the same limit points. Do E and E' have the same limit points?

Proof. Let $p \in E'^c$, thus there exists $N_r(p)$, where $N_r(p) \cap E = \emptyset$. Suppose $m \in N_r(p) \cap E'$. Then $d(m,p) < r$, furthermore, for all $\epsilon_{>0}, N_\epsilon(m) \cap E = \emptyset$, denote, $p_\epsilon \in N_\epsilon \cap E$. As, $d(p,m) + d(m,p_\epsilon) > d(p,p_\epsilon)$, it follows that, $d(m,p_\epsilon) > d(p,p_\epsilon) - d(p,m)$, thus, $0 < d(p,p_\epsilon) - d(p,m) = \mu$, $d(m,p_\epsilon) > \mu$, for all ϵ. This is a contradiction, and $N_r(p) \cap E' = \emptyset$, and E'^c, is open. Thus E' is closed.

(6a.) *Proof.* Let $p \in E'$, then there exists $r > 0$, such that, $N_r(p) \cap E' \neq \emptyset$, let $p' \in N_r(p) \cap E'$, Notice, $N_r(p)$ is an isolated point, thus there exists $N_{r'}(p') \subset N_r(p)$. As $p' \in E'$, there exists $s \in E, s \neq p'$, where and $s \in N_{r'}(p') \subset N_r(p)$, and $p \in E'$, thus $E'' \subset E'$, and E' is closed. □

□

(7) Prove that E and $\overline{E}$, always have the same limit points.

Proof. Fix $p \in \overline{E}'$, as $p \in \overline{E}$ is closed, $p \in \overline{E}$, thus $p \in E$ or $p \in E'$, in either case, p is a limit point of E. Suppose $p \in E'$, then $p \in \overline{E}$, and is a limit point of $\overline{E}$. □

(8) Do E and E' always have the same limit points?

Proof. let $p \in \overline{E'}$, then $p \in E'$, and p is a limit point of E. The reverse is obvious. □

(9) Is every point of an open set $E \subset \mathbb{R}^2$ a limit point of E. What about for closed sets in $\mathbb{R}^2$.

Proof. Yes, no. □

(10) Let $A_1, A_2, \cdots, A_n$ be subsets of a metric space. If $B_n = \bigcup_n A_n$, then $\overline{B_n} = \bigcup_n \overline{A_n}$.

Proof. Notice, $B \subset \bigcup \overline{A_n}$. Suppose $p \in \bigcup \overline{A_n} \backslash \overline{B_n}$, then $p \in B_n'$, and $p \in \overline{B_n}$, thus $\bigcup \overline{A_n} \backslash \overline{B_n} = \emptyset$, and $\bigcup \overline{A_n} \subset \overline{B_n}$, furthermore, $\bigcup \overline{A_n}$ is closed. As such, $\bigcup \overline{A_n} = \overline{B_n}$. □

(11) , if $B = \bigcup_{i=1}^{\infty} A_i$, prove that $\overline{B} \supset \cup_{i=1}^{\infty} \overline{A_i}$. Show by example that the inclusion can be proper.

Proof. let $p \in \cup_{i=1}^{\infty} \overline{A_i}$, and $p \notin \overline{B}$, then there exists $\epsilon_{>0}$, where $N_\epsilon(p) \cap B \subset \{p\}$. Thus, for all i, $A_i \cap N_\epsilon(p) \cap A_i \subset \{p\}$, thus $p \notin \bigcup \overline{A_i}$, a contradiction □

(12) Show, by an example that the inclusion can be proper.

Proof. Let $A_i = [-\infty, 1 - 1/i] \cup [1 + 1/i, \infty]$, $B = \cup_i A_i$, then $1 \in \overline{B}$, is not a limit pt. of A_i □

(13) Let E^o denote the set of all interior points of a set E. Prove that E is always open.

Proof. Let $D = (E^o)^c$, suppose $p \in D'$, then for all neighbourhoods V of p, there exists $l \in D$, thus $V \not\subset E^o$, and $p \in D$, thus D is closed, and $D^c = E^o$ is open. □

(14) Prove that E is open iff $E^o = E$.

Proof. Suppose E is open, then $p \in E$ implies that $p \in E^o$, and $E \subset E^o$, that $E^o \subset E$ holds unilaterally. Suppose $E^o = E$. Then $p \in E$, means that p is an interior point, thus E is open. □

(15) If $G \subset E$ and G is open, prove that $G \subset E^o$.

Proof. Let $p \in G$, then every neighbourhood of p, $V_p \subset G \subset E$, thus $p \in E^o$. As such, $G \subset E^o$. □

(16) Prove that the complement of E^o is the closure of the complement of E.

Proof. Let $D = (E^o)^c$, notice D is closed, and $E^c \subset D$, thus $\overline{E^c} \subset D$. Suppose $p \in D$, then either, $p \in E^c$, or $p \in D \backslash E^c$, then for all neighbourhoods of p, V_p, $V_p \cap E^c \neq \emptyset$,thus $D \subset \overline{E^c}$, and $D = \overline{E^c}$. □

(17) Do E and $\overline{E}$ always have the same interiors.

Proof. It suffices to show that $\overline{E^c} = \overline{\overline{E}^c}$, naturally $\overline{\overline{E}c} \subset \overline{E^c}$. Suppose $p \in \overline{E^c}$, then $p \in E'$, or $E^c \backslash E'$, if $p \in E'$, then $p \in (\overline{E}^c)'$, and in the other case, $p \in \overline{E}^c$, thus $\overline{E^c} \subset \overline{\overline{E}^c}$, and $\overline{E^c} = \overline{\overline{E}^c}$ □

(18) Do E and E^o always have the same closures?

Proof. No, consider $\{1, 2, 3\}$, or any finite set. □

(19) Let X be an infinite set. For $p \in X$ and $q \in X$, define

$$d(p, q) = \begin{cases} 1, & (p \neq q) \\ 0, & (p = q) \end{cases} \tag{7.9}$$

Prove that this is a metric. Which subsets of the resulting metric space are open? Which are closed? Which are compact?

Proof. Consider $p, q, r \in X$, then $d(p, r) \leq 1 \leq d(p, q) + d(q, r)$, furthermore, $d(p, q) = d(q, p)$, $\cdots$. Let $E \subset X$, and E is not empty. then, E is open. To see this, fix $p \in E$, then there exists $N_r(p) \subset E$, where $r < 1$. Furthermore, for $E \subset X$, let $p \in E'$, then for all $r > 0$, $N_r(p) \cap E \backslash p \neq \emptyset$, however, for $r < 1$, this set is empty. Thus for $E \subset X$, $E' = \emptyset$. Naturally $E' \subset E$, and E is closed. Only finite sets are compact. Otherwise, if E is infinite, let $\{p_i\}$, where each $p_i \in E$ is an open-cover, and not subset of $\{p_i\}$ is an open cover of E. □

(20) Is $d(x, y) = (x - y)^2$ a metric?

Proof. No, for $x, y, z \in \mathbb{R}$, where $y > x$ and $y > z$ □

(21) $d(x, y) = \sqrt{|x - y|}$

Proof. Yes □

(22) $d(x, y) = |x^2 - y^2|$

Proof. Yes □

(23) $d(x, y) = |x - 2y|$

Proof. No □

(24) $d(x, y) = \frac{|x-y|}{1+|x-y|}$

Proof. □

(25) Let $K \subset \mathbb{R}$ consist of 0 and $1/n$, where $n = 1, 2 \cdots$. Prove K is compact from the definition.

Proof. Notice $[0, 1] \subset \mathbb{R}$ is compact, and $K \subset [0, 1]$ and is closed, thus it is compact. □

(25a) *Proof.* Fix A_i, an open cover where for $i \neq j$, $A_i \cap A_j \neq \emptyset$ (a set A_i can be obtained for every *OC* of K). Fix $0 \in A_{\alpha_0}$, then as A_{α_0} is open, let $r > 0, N_r(0) \subset A_{\alpha_0}$, then fix $min_{n \in \mathbb{N}, r < 1/n}$, subsequently, there exists A_{α_i}, where $1/n \in A_{\alpha_i}$, the process may be repeated, to obtain a finite open cover $\{A_{\alpha_i}\}$ □

(26) construct a compact set of real numbers whose limit points form a countable set.

Proof. $A = \{0\} \cup \{1/n, n \in \mathbb{N}\} \cup \{1/m + 1/n, n \in \mathbb{N}\}$, notice, $A \subset [0, 2]$, and is closed, as such, it is compact. Furthermore, its limit points are $0, 1/m, 1 + 1/m, m \in \mathbb{N}$. □

(27) Give an example of an open cover of $(0, 1)$ which has no finite subcover.

Proof. $A_i = N_{1/2i}(1 - i), i \in \mathbb{N}$ □

(28) Show that theorem 2.36, and its corollary become false if the word "compact" is replaced by "closed" or "bounded"".

Proof. *bounded*: Let $K_i = [-1/i, 0) \cup (0, 1/i]$
closed: □

(29) Regard $\mathbb{Q}$,

(30) If A and B are disjoint closed sets in some metric space X, prove that they are separated.

Proof. Notice, $\emptyset = \bar{A} \cap \bar{B} \supset \bar{A} \cap B = \emptyset$, a similar proof exists that $A \cap \bar{B} = \emptyset$. □

(31) Prove the same for disjoint open sets.

Proof. Let $A, B \subset X$, be disjoint open sets. Suppose $b \in \bar{A} \cap B$, then $b \in A' \cap B$, thus $b \in B$ and is not an interior pt. of B, a contradiction. □

(32) Fix $p \in X$, $\delta > 0$, define A to be the set of all $q \in X$ for which $d(p, q) < \delta$, define B to be the set of all l where $d(p, l) > \delta$. Prove that A and B are separated.

Proof. A, B are open sets, the proof follows from 32. □

(33) Prove that every connected metrc space with at least two points is uncountable

(35) Let A, B be separated subsets of $\mathbb{R}^k$, fix $a \in A, b \in B$, and define

$$p(t) = (1 - t)a + tb \tag{7.10}$$

where $t \in \mathbb{R}$, put $A_0 = p^{-1}(A), B_0 = p^{-1}(B)$. Prove that A_0 and B_0 are separated subsets of $\mathbb{R}$.

Proof. Let $l \in \bar{A}_0 \cap B$, then $p(l) \in B$, and, for all ϵ, $l + \epsilon \in A_0$, thus $p(l + \epsilon) = p(l) + \epsilon * (a + b) \in A$, however, there exists some $N_\delta(p(l)) \cap A = \emptyset$ as $p(l) \notin A'$, thus $d(p(l), p(l+\epsilon)) > \delta, \epsilon * \|(a+b)\| > \delta$, and $\epsilon > \delta/\|a+b\| > 0$, contradicting that $l \in \overline{A_0}$. A similar proof holds that $\bar{B}_0 \cap A_0 = \emptyset$. □

(36) Prove that there exists $t_0 \in (0, 1)$ such that $p(t_0) \notin A \cup B$