

# Error Correcting Codes: Mathematical Prerequisites

Henry D. Pfister  
Duke University

January 8th, 2025

## 1 Book: “Proofs and Fundamentals” by Ethan Bloch

- Chapter 1: Logic
  - Notation/Terminology for propositions:  $P, Q$ 
    - \* **Negation:** the proposition  $P$  is not true is denoted  $\neg P$
    - \* **Implication:**  $P \rightarrow Q$  is the proposition that “ $P$  implies  $Q$ ”
    - \* **Equivalence:**  $P \leftrightarrow Q$  is the proposition that  $P$  is true iff (if and only if)  $Q$  is true
    - \* **Conjunction:** “ $P$  and  $Q$ ” is denoted  $P \wedge Q$  ( $\wedge$  is also used for minimum)
    - \* **Disjunction:** “ $P$  or  $Q$ ” is denoted  $P \vee Q$  ( $\vee$  also used for maximum)
    - \* **Tautology:** A statement that is always true
    - \* **Contradiction:** A statement that is always false
    - \* **Provable Inference:** An tautological implication such as  $(P \rightarrow Q) \wedge P \Rightarrow Q$
    - \* **Provable Identity:** An tautological equivalence such as  $\neg(\neg P) \Leftrightarrow P$
  - First-Order Predicate Logic
    - \* Proposition:  $P(x)$  is true or false for each  $x$
    - \* Example:  $P(x)$  = “ $x$  is even” for  $x \in \mathbb{Z}$  is true for all even numbers
  - Quantifiers: Universal  $\forall x P(x)$  versus Existential  $\exists x P(x)$ 
    - \* Example: “ $x$  is even” is existentially true, but not universally
  - **De Morgan’s Laws:**  $\neg(P \wedge Q) = (\neg P \vee \neg Q)$  and  $\neg(P \vee Q) = (\neg P \wedge \neg Q)$ 
    - \* Proof via enumeration of all cases
- Chapter 2: Proofs
  - By **contrapositive:**  $P \rightarrow Q$  is equivalent to  $\neg Q \rightarrow \neg P$ 
    - \* Example: Prove “If  $n^2$  is odd, then  $n$  is odd”  
via “If  $n$  is even, then  $n = 2m$  and  $n^2 = 4m^2 = 2(2m^2)$  is even”
  - By **contradiction:** Assume  $P$  true, find  $P \rightarrow Q$  with  $Q$  false, this implies  $P$  false
    - \* Example: Prove “ $\sqrt{2}$  is irrational” by supposing  $\sqrt{2}$  is rational  
“If  $\sqrt{2} = a/b$  with  $\gcd(a, b) = 1$ , then  $a^2 = 2b^2$  and  $a$  is even”  
“Therefore,  $a = 2c$  and  $4c^2 = 2b$  which implies  $b$  is even and  $\gcd(a, b) \geq 2$ ”
- Chap 3-5 = Sets, Functions, and Relations
  - Formal definitions of common mathematical structures
  - Relations: Equality, Greater, Less than, etc...
  - Sections 7.1-7.3: Binary operations, groups, morphisms
  - Sections 7.6-7.7: Counting and Combinatorics

## 2 Set Theory

- Sets are often denoted by calligraphic letters:  $\mathcal{X}, \mathcal{Y}, \mathcal{S}$
- Standard sets are defined by blackboard bold
  - The natural numbers:  $\mathbb{N} = \{0, 1, 2, \dots\}$
  - The integers:  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
  - The positive integers:  $\mathbb{Z}^+ = \{1, 2, \dots\}$
  - The real numbers:  $\mathbb{R}$
- Standard set notation
  - **Membership:**  $x \in \mathcal{X}$  means “element  $x$  is a member of set  $\mathcal{X}$ ” or “ $\mathcal{X}$  contains  $x$ ”
    - \*  $x \notin \mathcal{X}$  means “element  $x$  is not a member of set  $\mathcal{X}$ ”
  - **Cardinality:**  $|\mathcal{X}|$  gives the “number of elements in  $\mathcal{X}$ ”
    - \* In this class, we define  $|\mathcal{X}| = \infty$  if  $\mathcal{X}$  is not finite
  - **Subset:**  $\mathcal{X} \subseteq \mathcal{Y}$  means “Every element of set  $\mathcal{X}$  is in set  $\mathcal{Y}$ ”
  - **Set Equality:**  $\mathcal{X} = \mathcal{Y}$  means “set  $\mathcal{X}$  contains exactly the same elements as set  $\mathcal{Y}$ ”
  - **Proper Subset:**  $\mathcal{X} \subset \mathcal{Y}$  means  $\mathcal{X} \subseteq \mathcal{Y}$  but  $\mathcal{X} \neq \mathcal{Y}$
  - Subset with some property:  $\mathcal{X} = \{x \mid P(x) \text{ is true}\}$ 
    - \* Example: set builder notation  $\mathcal{X} = \{2x \mid x \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid x \text{ is even}\}$
  - **Union:**  $\mathcal{X} \cup \mathcal{Y}$  means “the set of elements that are contained in either  $\mathcal{X}$  or  $\mathcal{Y}$ ”
  - **Intersection:**  $\mathcal{X} \cap \mathcal{Y}$  means “the set of elements that are contained in both  $\mathcal{X}$  and  $\mathcal{Y}$ ”
  - **Set Difference:**  $\mathcal{Y} - \mathcal{X} = \mathcal{Y} \setminus \mathcal{X} \triangleq \{y \in \mathcal{Y} \mid y \notin \mathcal{X}\}$  means “elements in  $\mathcal{Y}$  not in  $\mathcal{X}$ ”
  - **Complement:**  $\mathcal{X}^c = \mathcal{U} - \mathcal{X}$  where  $\mathcal{U}$  is the implied universal set
  - **De Morgan’s Laws:** (for  $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{U}$ )
    - \*  $(\mathcal{X} \cup \mathcal{Y})^c = \mathcal{X}^c \cap \mathcal{Y}^c$  (proved via  $\neg((x \in \mathcal{X}) \vee (y \in \mathcal{Y}))$ )
    - \*  $(\mathcal{X} \cap \mathcal{Y})^c = \mathcal{X}^c \cup \mathcal{Y}^c$  (proved via  $\neg((x \in \mathcal{X}) \wedge (y \in \mathcal{Y}))$ )
- Product sets: pairs, tuples, and general products
  - An **ordered pair:**  $\mathcal{X} \times \mathcal{Y} = \{(x, y) \mid x \in \mathcal{X}, y \in \mathcal{Y}\}$
  - The set of 2-tuples:  $\mathcal{X}^2 = \mathcal{X} \times \mathcal{X} = \{(x_1, x_2) \mid x_1 \in \mathcal{X}, x_2 \in \mathcal{X}\}$
  - General **product set:**  $\mathcal{X}_1 \times \mathcal{X}_2 \times \dots \times \mathcal{X}_n = \{(x_1, x_2, \dots, x_n) \mid x_i \in \mathcal{X}_i \text{ for } i = 1, 2, \dots, n\}$

## 3 Functions

- A **function** (or **mapping**)  $f$  from  $\mathcal{X}$  to  $\mathcal{Y}$  is denoted  $f : \mathcal{X} \rightarrow \mathcal{Y}$ 
  - It assigns to each element  $x \in \mathcal{X}$  a single element in  $\mathcal{Y}$ 
    - \* Evaluation at  $x$  is denoted, as usual, by  $f(x)$
  - The set  $\mathcal{X}$  is called the **domain** of the function and the set  $\mathcal{Y}$  is called the **codomain**
  - Two functions are equal if they have the same domain, codomain, and value for all  $x \in \mathcal{X}$
  - The **range** of the function is subset of  $\mathcal{Y}$  achieved by some  $x$  or  $\{f(x) \mid x \in \mathcal{X}\}$ .
  - **Identity function** on  $\mathcal{X}$  is denoted  $1_{\mathcal{X}} : \mathcal{X} \rightarrow \mathcal{X}$  and satisfies  $1_{\mathcal{X}}(x) = x$  for all  $x \in \mathcal{X}$
- The **composition** of  $f : \mathcal{X} \rightarrow \mathcal{Y}$  and  $g : \mathcal{Y} \rightarrow \mathcal{Z}$  maps  $\mathcal{X} \rightarrow \mathcal{Z}$  and is denoted  $g \circ f$ 
  - Evaluating the composition gives  $(g \circ f)(x) = g(f(x))$
- Properties of a function  $f : \mathcal{X} \rightarrow \mathcal{Y}$ 
  - The function is called **one-to-one** or **injective** iff  $f(x) = f(x') \implies x = x'$
  - The function is called **onto** or **surjective** iff  $\mathcal{Y} = \{f(x) \mid x \in \mathcal{X}\}$
  - $f$  is called a **one-to-one correspondence** or **bijective** if it is both one-to-one and onto
    - \* Has a well-defined bijective **inverse**  $f^{-1} : \mathcal{Y} \rightarrow \mathcal{X}$  s.t.  $f^{-1} \circ f = 1_{\mathcal{X}}$  and  $f \circ f^{-1} = 1_{\mathcal{Y}}$

## 4 Relations

- A **relation** (e.g.,  $=, \leq, <$ ) on a set  $\mathcal{X}$  is a logical question about pairs
  - Defined as a subset  $\mathcal{R} \subseteq \mathcal{X} \times \mathcal{X}$
  - For  $x, x' \in \mathcal{X}$ , the statement  $x \succeq x'$  is true iff  $(x, x') \in \mathcal{R}$
- Properties of a relation on  $\mathcal{X}$  defined by  $\mathcal{R} \subseteq \mathcal{X} \times \mathcal{X}$ 
  - A relation is **reflexive** if  $(x, x) \in \mathcal{R}$  for all  $x \in \mathcal{X}$ 
    - \* Example:  $x = x$  and  $x \geq x$  are both true
  - A relation is **symmetric** if  $(x, x') \in \mathcal{R}$  implies  $(x', x) \in \mathcal{R}$ 
    - \* Example:  $x = y$  is true implies  $y = x$  is true
  - A relation is **transitive** if  $(x, y) \in \mathcal{R}, (y, z) \in \mathcal{R}$  implies  $(x, z) \in \mathcal{R}$ 
    - \* Example:  $x \geq y$  and  $y \geq z$  implies  $x \geq z$
- An **equivalence relation** is reflexive, symmetric, and transitive
  - An equivalence relation **partitions** the set into disjoint **equivalence classes**
  - Example:  $\mathcal{X} = \mathbb{R}^2$  and  $\mathcal{R} = \{((w, x), (y, z)) \mid w^2 + x^2 = y^2 + z^2\}$ 
    - \* Points at the same distance from the origin are equivalent
    - \* Equivalence classes decompose all of  $\mathbb{R}^2$  into concentric circles

## 5 Natural Numbers

- Every non-empty subset of  $\mathbb{N}$  contains a least element
  - In particular, 0 is the least element of  $\mathbb{N}$
- Mathematical **induction**: Assume 0 is the least element in  $\mathcal{S} \subseteq \mathbb{N}$ 
  - (i) If  $n \in \mathcal{S}$  implies  $n + 1 \in \mathcal{S}$ , then  $\mathcal{S} = \mathbb{N}$
  - (ii) If  $m \in \mathcal{S}$  for all  $0 \leq m \leq n$  implies  $n + 1 \in \mathcal{S}$ , then  $\mathcal{S} = \mathbb{N}$
  - This formalizes the idea of proof by induction
- The **integers**  $\mathbb{Z}$  should be well-known and have the following laws:
  - **Associative** laws:  $(a + b) + c = a + (b + c)$  and  $(ab)c = a(bc)$
  - **Commutative** laws:  $a + b = b + a$  and  $ab = ba$
  - **Distributive** laws:  $a(b + c) = ab + ac$  and  $(a + b)c = ac + bc$
  - **Identity** elements:  $a + 0 = a$  and  $a1 = a$
  - Additive inverses: For each  $a \in \mathbb{Z}$ , there is a  $-a$  such that  $a + (-a) = 0$
  - Cancellation:  $ab = 0$  implies  $a = 0$  or  $b = 0$
  - Invariance under shift:  $a < b$  implies  $a + c < b + c$  for all  $c \in \mathbb{Z}$ 
    - \* Same for  $=, \leq, >, \geq$
  - Invariance under scale:  $a < b$  implies  $ca < cb$  for all  $c \in \mathbb{Z}^+$ 
    - \* Same for  $=, \leq, >, \geq$
  - **Absolute value**:  $|a|$  equals  $a$  if  $a \geq 0$  and  $-a$  if  $a < 0$
- For integers  $a, b, c \in \mathbb{Z} \setminus \{-1, 0, 1\}$ , we say  $c$  is **composite** if it can be written as  $c = ab$ 
  - More abstractly, we say that  $c$  is **reducible**

- We say an integer  $d \in \mathbb{Z} \setminus \{0\}$  **divides**  $a \in \mathbb{Z}$  iff  $a = dq$  for some  $q \in \mathbb{Z}$ . This is denoted  $d \mid a$ 
  - If  $d$  does not divide  $a$ , then we write  $d \nmid a$ .
  - If , for positive  $a, d \in \mathbb{Z}^+$ ,  $d \mid a$ , then  $d \leq a$
- The **division** of  $a \in \mathbb{Z}$  by  $d \in \mathbb{Z} \setminus \{0\}$  results in a unique **quotient**  $q \in \mathbb{Z}$  and **remainder**  $r \in \mathbb{Z}$  that satisfy  $a = qd + r$  and  $0 \leq r < |d|$ 
  - Proof: First, we note that  $q = q'$  implies  $r = a - qd = a - q'd = r'$ . So any counterexample to uniqueness must have  $q \neq q'$ . Suppose there is another pair  $(q', r')$  with  $q' > q$  (wolog) which also satisfies  $a = q'd + r'$  and  $0 \leq r' < |d|$ . Then,  $|r - r'| = |q' - q| |d| \geq |d|$ . But, the bounds on  $r$  and  $r'$  imply that  $|r - r'| \leq |d| - 1$  and the contradiction eliminates the possibility of a counterexample.
  - Used to define the **modulo** operation  $a \bmod d \triangleq r$  and the remainder function  $R_d[a] \triangleq r$
- An integer  $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$  is **prime** if it is not composite
  - Since a prime cannot be written as a product, it is only divisible by  $\pm 1$  and  $\pm p$
  - The abstract definition is that  $p$  is prime iff  $p \mid ab$  implies  $p \mid a$  or  $p \mid b$ 
    - \* For integers, this is known as Euclid's Lemma (proof via Euclidean algorithm)
- The **greatest common divisor** of  $a_1, \dots, a_n \in \mathbb{Z}$  is the largest  $d \in \mathbb{Z}^+$  s.t.  $d \mid a_i$  for  $i = 1, \dots, n$ 
  - This element is denoted  $\gcd(a_1, \dots, a_n)$
  - If the  $\gcd(a, b) = 1$ , then  $a, b$  are **relatively prime**
- The **least common multiple** of  $a_1, \dots, a_n \in \mathbb{Z}$  is the smallest  $m \in \mathbb{Z}^+$  s.t.  $a_i \mid m$  for  $i = 1, \dots, n$ 
  - This element is denoted  $\text{lcm}(a_1, \dots, a_n)$

## 6 Matrices and Vector Spaces

- Let  $\mathbb{R}$  be the set of real numbers
  - Real numbers obey all laws that the integers do
  - In addition, every non-zero  $x \in \mathbb{R}$ , has a mult. inverse  $x^{-1} \in \mathbb{R}$  such that  $x^{-1} \cdot x = 1$
- Let  $V = \mathbb{R}^n$  be the set of  $n$ -dimensional column vectors of real numbers
  - Vectors denoted  $\underline{v} = (v_1, \dots, v_n) \in V$  (and written horizontally for ease)
  - **Scalar multiplication** (SM):  $\alpha \cdot \underline{v} \triangleq (\alpha v_1, \dots, \alpha v_n)$  for  $\alpha \in \mathbb{R}$
  - **Vector addition** (VA):  $\underline{u} + \underline{v} \triangleq (u_1 + v_1, \dots, u_n + v_n)$  for  $\underline{u}, \underline{v} \in V$
  - The **standard basis vectors** are  $\underline{e}_i = (\underbrace{0, \dots, 0}_{i-1 \text{ ZEROS}}, 1, \underbrace{0, \dots, 0}_{n-i \text{ ZEROS}})$  for  $i = 1, \dots, n$
- A real **vector space**  $V$  satisfies, for  $\underline{u}, \underline{v}, \underline{w} \in V$ ,  $\alpha, \beta \in \mathbb{R}$ :
  - **Closure** under SM, VA:  $\alpha \underline{u} + \beta \underline{v} \in V$
  - **Commutative** law for VA:  $\underline{u} + \underline{v} = \underline{v} + \underline{u}$
  - **Associative** law for VA:  $(\underline{u} + \underline{v}) + \underline{w} = \underline{u} + (\underline{v} + \underline{w})$
  - **Identity** element for VA:  $\underline{u} + \underline{0} = \underline{0} + \underline{u} = \underline{u}$
  - **Distributive** law for SM over VA:  $\alpha \cdot (\underline{u} + \underline{v}) = \alpha \cdot \underline{u} + \alpha \cdot \underline{v}$
  - **Distributive** law for VA over SM:  $(\alpha + \beta) \cdot \underline{u} = \alpha \cdot \underline{u} + \beta \cdot \underline{u}$
  - **Associative** law for SM:  $(\alpha\beta) \cdot \underline{u} = \alpha(\beta \cdot \underline{u})$

- **Identity** element for SM:  $1 \cdot \underline{u} = \underline{u}$
- Consider a set of  $m$  vectors  $G = \{\underline{v}_1, \underline{v}_2, \dots, \underline{v}_m\}$ 
  - $G$  **spans**  $V$  if, for any  $\underline{v} \in V$ , there exist  $\alpha_1, \dots, \alpha_m \in \mathbb{R}$  such that  $\underline{v} = \sum_{i=1}^m \alpha_i \underline{v}_i$ 
    - \* Where the sum denotes vector addition
    - \* For example,  $\{(1, 0, 0), (1, 1, 0), (0, 1, 1), (1, 1, 1)\}$  spans  $\mathbb{R}^3$
  - $G$  is **linearly independent** iff  $\sum_{i=1}^m \alpha_i \underline{v}_i = 0$  implies  $\alpha_1 = \dots = \alpha_m = 0$
  - $G$  is **linearly dependent** iff  $G$  is not linearly independent
  - $G$  is a **basis** for  $V$  if  $G$  is linearly independent and  $G$  spans  $V$ 
    - \* For example,  $\{(1, 1, 0), (0, 1, 1), (1, 1, 1)\}$  is a basis for  $\mathbb{R}^3$
    - \* The **canonical basis** for  $\mathbb{R}^n$  is given by  $\{\underline{e}_1, \underline{e}_2, \dots, \underline{e}_n\}$
  - The **dimension**  $\dim(V)$  is the number of vectors in any basis of  $V$
- A **subspace**  $U$  is a subset  $U \subseteq V$  which is also a vector space
  - For  $V = \mathbb{R}^n$ , the **dual space**  $U^\perp$  is  $\{\underline{v} \in V \mid \sum_{i=1}^n u_i \cdot v_i = 0 \text{ for all } \underline{u} \in U\}$
- Let  $\mathbb{R}^{m \times n}$  be the set of real  $m \times n$  matrices
  - Rows can be viewed as  $m$  row vectors in  $\mathbb{R}^n$ 
    - \* The **row space** is the vector space spanned by the rows
  - Columns can be viewed as  $n$  row vectors in  $\mathbb{R}^m$ 
    - \* The **column space** is the vector space spanned by the columns
  - The row/column space is unchanged by **elementary** row/column operations
    - \* Interchange any two rows/columns
    - \* Multiply any any row/column by a scalar
    - \* Add a scalar multiple of any row/column to another row/column
  - Matrices are denoted by underlined capital letters  $\underline{A} \in \mathbb{R}^{m \times n}$ 
    - \* Element in  $i$ th row,  $j$ th column is denoted  $[\underline{A}]_{ij}$
    - \* The transpose  $\underline{A}^T$  is a  $n \times m$  matrix defined by  $[\underline{A}^T]_{ij} = [\underline{A}]_{ji}$
  - The dimension of the row space and the column space are equal
    - \* and called the the **rank** of the matrix  $\text{rank}(\underline{A})$
    - \* A matrix  $\underline{A} \in \mathbb{R}^{m \times n}$  is **full rank** if  $\text{rank}(\underline{A}) = \min(m, n)$
  - Scalar multiplication:  $\alpha \cdot \underline{A}$  for  $\underline{A} \in \mathbb{R}^{m \times n}$  and  $\alpha \in \mathbb{R}$ 
    - \* defined by  $[\alpha \cdot \underline{A}]_{ij} \triangleq \alpha \cdot [\underline{A}]_{ij}$
    - \* Easy to verify that it inherits all the mult. properties of  $\mathbb{R}$
  - Matrix addition:  $\underline{A} + \underline{B}$  for  $\underline{A} \in \mathbb{R}^{m \times n}$  and  $\underline{B} \in \mathbb{R}^{m \times n}$ 
    - \* defined by  $[\underline{A} + \underline{B}]_{ij} \triangleq [\underline{A}]_{ij} + [\underline{B}]_{ij}$
    - \* Easy to verify that it inherits all the additive properties of  $\mathbb{R}$
  - Matrix multiplication:  $\underline{A} \cdot \underline{B}$  for  $\underline{A} \in \mathbb{R}^{m \times n}$  and  $\underline{B} \in \mathbb{R}^{n \times p}$ 
    - \* defined by  $[\underline{A} \cdot \underline{B}]_{ik} \triangleq \sum_{j=1}^n [\underline{A}]_{ij} \cdot [\underline{B}]_{jk}$
    - \* Easy to verify it inherits associative and distributive properties from  $\mathbb{R}$
  - The **null space** of  $\underline{A} \in \mathbb{R}^{m \times n}$  is  $\{\underline{v} \in \mathbb{R}^n \mid \underline{A} \cdot \underline{v} = \underline{0}\}$ 
    - \* Equivalent to the dual space of the row space of  $\underline{A}$
    - \* Proof: Let  $U$  be the row space of  $\underline{A}$ , then  $U = \{\underline{w}^T \cdot \underline{A} \mid \underline{w} \in \mathbb{R}^m\}$ . So the dual space is

$$U^\perp = \{\underline{v} \in \mathbb{R}^n \mid \underline{w}^T \cdot \underline{A} \cdot \underline{v} = 0 \text{ for all } \underline{w} \in \mathbb{R}^m\},$$

but  $\underline{w}^T \cdot \underline{A} \cdot \underline{v} = 0$  for all  $\underline{w} \in \mathbb{R}^m$  iff  $\underline{A} \cdot \underline{v} = \underline{0}$ . So,  $U^\perp$  is null space of  $\underline{A}$ .