Linear Block Codes

Qi Zhang

Aarhus University School of Engineering

7/02/2014

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

- **Example**:Many communication or storage systems use a parity check bit as a simple means of error detection. Let $A = \{0,\ 1,\ 2,\ 3\}$. Let each symbol a be equally probable and let $B = \{0,\ 1\}$ be a parity generator with

$$b_j = \begin{cases} 0 & \textit{if} \quad a = 0 \quad \text{or} \quad a = 3 \\ 1 & \textit{if} \quad a = 1 \quad \text{or} \quad a = 2 \end{cases}$$

what are $H(A)$, $H(B)$ and $H(A, B)$?

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

- **Solution**:
  - $H(A) = 4 \cdot 1/4 \cdot log_2(4) = 2$.
  - Likewise, the two systems in B each have probability 0.5, so $H(B) = 2 \cdot 1/2 \cdot log_2(2) = 1$
  - The conditional probabilities $p(b|a)$ are

$$\begin{array}{llll} p(0|0) = 1 & p(1|0) = 0 & p(0|1) = 0 & p(1|1) = 1 \\ p(0|2) = 0 & p(1|2) = 1 & p(0|3) = 1 & p(1|3) = 0 \end{array}$$

  - Therefore,

$$\begin{aligned} H(B|A) &= \sum_{i=0}^{3} p_i \sum_{j=0}^{1} p_{j|i} log_2(1/p_{j|i}) \\ &= 4 \times 0.25 \times (1 \cdot log_2(1) - 0 \cdot log_2(1/0)) = 0 \end{aligned}$$

  - It means that B is completely determined by A, therefore,

$$H(A, B) = H(A) + H(B|A) = 2 + 0 = 2$$

  - B contributes no information to the compound signal, i.e., source B is *redundant* info.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Error probability of repetition code

- Let's calculate the error probability of the repetition code:

$$0 \Rightarrow \underbrace{00\ldots000}_{n}$$

$$1 \Rightarrow \underbrace{11\ldots111}_{n}$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Error probability of repetition code

$$\underbrace{00\ldots000}_{n} \qquad \underbrace{11\ldots111}_{n}$$

- Assuming the error probability of Binary symmetric channel (BSC) is p, to calculate the probability that there are i errors in a word of n bits?

$$P_e(i,n) = \binom{n}{i} p^i (1-p)^{n-i} \cong \binom{n}{i} p^i \quad p \ll 1$$

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}$$

- e.g., $n = 5, i = 1, p = 0.1$, $P_e(i,n) = 5 \cdot 0.1 \cdot 0.9^4 = 0.3281$;
- e.g, $n = 5, i = 2, p = 0.1$, $P_e(i,n) = 10 \cdot 0.1^2 \cdot 0.9^3 = 0.0729$;
- e.g., $n = 5, i = 3, p = 0.1$, $P_e(i,n) = 10 \cdot 0.1^3 \cdot 0.9^2 = 0.0041$;
- the probability of having i errors is higher than having $i+1$ errors, i.e., $P_e(i,n) \gg P_e(i+1,n)$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Error probability of repetition code

- A repetition code with $n = 3$, the codeword are (111) and (000).
- As the probability of having i errors is higher than having $i + 1$ errors:
  - Error pattern (110), (101) and (011) are decoded as "1";
  - Error pattern (001), (010) and (100) are decoded as "0";
- This particular repetition code can only correct single error.
- This repetition code can detect up to two errors.
- This repetition code CANNOT detect three errors.

- Question: what is the undetectable error probability ?
- Question: what is the decoding fail probability?

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Error probability of repetition code

- Question: what is the undetectable error probability of $n = 3$ repetition code?
- A: The undetectable probability is the probability that three errors happen.

$$P = P_e(3,3) = \binom{3}{3} p^3 (1-p)^{3-3} = p^3$$

- Question: what is the decoding fail probability of $n = 3$ repetition code ?
- A: If more than one error happen, it will have decoding failure. Therefore, the decoding fail probability is the sum of probabilities that two errors and three errors happen.

$$\begin{aligned} P &= P_e(2,3) + P_e(3,3) \\ &= \binom{3}{2} p^2 (1-p)^{3-2} + \binom{3}{3} p^3 (1-p)^{3-3} \\ &= 3p^2 - 2p^3 \end{aligned}$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

What is vector space?

- Let V be a set of vectors on which a binary operation *add*, $\oplus$,and a binary operation *multiplication*, $\bullet$, are defined.
- The set V is called a *vector space* over a field F, if it satisfies the axioms listed below.
- Elements of V are called vectors, such as $\mathbf{u}, \mathbf{v}, \mathbf{w}$ below.
- Elements of F are called scalars, such as a, b below.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Axiom	**Signification**
Associativity of addition	$\mathbf{u} \oplus (\mathbf{v} \oplus \mathbf{w}) = (\mathbf{u} \oplus \mathbf{v}) \oplus \mathbf{w}$
Commutativity of addition	$\mathbf{u} \oplus \mathbf{v} = \mathbf{v} \oplus \mathbf{u}$
Identity element of addition	zero element $\mathbf{0} \in V$, $\mathbf{u} \oplus \mathbf{0} = \mathbf{u}$ for all $\mathbf{u} \in V$
Inverse element of addition	if $\mathbf{u} \in V$, there exists $\mathbf{v}$, called additive inverse of $\mathbf{u}$, such that $\mathbf{u} \oplus \mathbf{v} = \mathbf{0}$
Identity element of scalar multiplication	$1 \bullet \mathbf{u} = \mathbf{u}$, if 1 is the unit element in F
Distributivity of scalar multiplication with respect to vector addition	$a \bullet (\mathbf{u} \oplus \mathbf{v}) = a \bullet \mathbf{u} \oplus a \bullet \mathbf{v}$
Distributivity of scalar multiplication with respect to field addition	$(a \oplus b) \bullet \mathbf{u} = a \bullet \mathbf{u} \oplus b \bullet \mathbf{u}$
Compatibility of scalar multiplication with field multiplication	$a \bullet (b \bullet \mathbf{u}) = (a \bullet b) \bullet \mathbf{u}$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Field

- In abstract algebra, a **field** is an algebraic structure with notions of addition, subtraction, multiplication, and division, satisfying certain axioms.
- The most commonly used fields are the field of real numbers, the field of complex numbers.
- There is one special field called **finite fields**(also called Galois fields).
- Finite fields are fields with finite elements, for example GF(2) consists of two elements “0” and “1”.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Vector space over the binary field

- A useful vector space for block codes is vector space defined over the binary field, or Galois Field GF(2);
- Consider a sequence of n components $(a_0, a_1, \ldots, a_{n-1})$;
- Each component of the sequence a_i is an element of the field GF(2), i.e., a_i is either "0" or "1";
- This sequence is called an n-component vector;
- This vector belongs to a vector space V_n which has 2^n vectors.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Binary addition operation

- If two vectors $\mathbf{u}, \mathbf{v}$ in V_n:

$$\begin{aligned} \mathbf{u} &= (u_0, u_1, \ldots, u_{n-1}) \\ \mathbf{v} &= (v_0, v_1, \ldots, v_{n-1}) \end{aligned}$$

- then

$$\mathbf{u} \oplus \mathbf{v} = (u_0 \oplus v_0, u_1 \oplus v_1, \ldots, u_{n-1} \oplus v_{n-1})$$

  - The sum is also a vector that belongs to vector space V_n;
  - **The addition of any two vectors of a given vector space is also another vector of the same vector space.**

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Modulo-2 addition and multiplication

- Operation over the binary field are modulo-2 addition and multiplication:

Modulo-2 addition	Modulo-2 multiplication
$0 \oplus 0 = 0$	$0 \bullet 0 = 0$
$0 \oplus 1 = 1$	$0 \bullet 1 = 0$
$1 \oplus 0 = 1$	$1 \bullet 0 = 0$
$1 \oplus 1 = 0$	$1 \bullet 1 = 1$

- The all-zero vector $\mathbf{0} = (0, 0, \ldots, 0)$ in the vector space, there is

$$\mathbf{u} \oplus \mathbf{0} = (u_0 \oplus 0,\ u_1 \oplus 0,\ \ldots,\ u_{n-1} \oplus 0) = \mathbf{u}$$

$$\mathbf{u} \oplus \mathbf{u} = (u_0 \oplus u_0,\ u_1 \oplus u_1,\ \ldots,\ u_{n-1} \oplus u_{n-1}) = \mathbf{0}$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

- **Example 2.1**: The vector space of vector with four components consists of $2^4 = 16$ vectors:

$$\begin{aligned} V_4 \quad = \quad & \{(0000), (0001), (0010), (0011), (0100), (0101), (0110), (0111), \\ & (1000), (1001), (1010), (1011), (1100), (1101), (1110), (1111)\} \end{aligned}$$

  Verify that addition of any two of these vectors is another vector in the same vector space.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Vector subspace

- Vector subspace: it is possible to find a subset of vectors, S, inside the vector space V defined over field F, which can obey all the conditions for being vector space.
- The subset S is referred as a subspace of the vector space V.
- The conditions of subset, S, being a subspace of vector space V:
  - For any two vectors in S, $\mathbf{u}, \mathbf{v} \in S$, the sum vector $(\mathbf{u} + \mathbf{v}) \in S$.
  - For any element of the field $a \in F$ and any vector $\mathbf{u} \in S$, the scalar multiplication $a \bullet \mathbf{u} \in S$.
- **Example 2.2**: Verify the following subset is a subspace of the vector space V_4:

$$S = \{(0000), (1001), (0100), (1101)\}$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Linear combination

- A set of vector $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ of vector space V defined over F,
- $a_1, a_2, \ldots, a_k$ are scalar numbers of the field F,
- The sum of the expression below is called a linear combination of the vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$.

$$a_1 \bullet \mathbf{v}_1 \oplus a_2 \bullet \mathbf{v}_2 \oplus \ldots \oplus a_k \bullet \mathbf{v}_k$$

- **Property**:
  - Addition of linear combinations is also a linear combination of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$;
  - Multiplication of a linear combination by an element of the field F is also a linear combination of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

- **Theorem 2.1**: If $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ are k vectors in V defined over F, the set of all the linear combinations of $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ is a subspace S of V.
- **Example 2.3**: Verify the linear combination of the two vector (1001) and (0100) of the vector space V_4 form a subspace S.

$$S = \{(0000), (1001), (0100), (1101)\}$$

- **Solution**:

$$\begin{aligned} 0 \bullet (1001) \oplus 0 \bullet (0100) &= (0000) \\ 0 \bullet (1001) \oplus 1 \bullet (0100) &= (0100) \\ 1 \bullet (1001) \oplus 0 \bullet (0100) &= (1001) \\ 1 \bullet (1001) \oplus 1 \bullet (0100) &= (1101) \end{aligned}$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

- If

$$a_1 \bullet \mathbf{v}_1 \oplus a_2 \bullet \mathbf{v}_2 \oplus \ldots \oplus a_k \bullet \mathbf{v}_k = \mathbf{0}$$

  where $a_1, a_2, \ldots, a_k$ are not all equal to zero, then the set of k vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ is said to be *linearly dependent* .
- If the set of vectors is not linearly dependent, then the set is said to be *linearly independent*.

$$a_1 \bullet \mathbf{v}_1 \oplus a_2 \bullet \mathbf{v}_2 \oplus \ldots \oplus a_k \bullet \mathbf{v}_k \neq \mathbf{0}$$

  unless $a_1 = a_2 = \ldots = a_k = 0$
- **Example 2.4**: Check vectors (1001), (0100) and (1101) are linearly dependent.
- **Solution:**

$$1 \bullet (1001) \oplus 1 \bullet (0100) \oplus 1 \bullet (1101) = (0000)$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

- A set of vectors is said to *span* a vector space V if every vector in V is a linear combination of the vectors in the set.
- In any vector space or subspace there exists at least one set of linearly independent vectors that *span* the space.
- This set is called a *basis* (or *base*) of the vector space.
- The number of vectors in a *basis* of a vector space is called the *dimenstion* of the vector space.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

- For a given vector space V_n defined over GF(2), the following set of vectors is the set of vectors $\mathbf{e}_i$ that have a non-zero component only at position i:

$$\begin{aligned} \mathbf{e}_0 &= (1, 0, \ldots, 0) \\ \mathbf{e}_1 &= (0, 1, \ldots, 0) \\ &\vdots \\ \mathbf{e}_{n-1} &= (0, 0, \ldots, 1) \end{aligned}$$

- Any vector of the vector space can be described as a function of this set:

$$(a_0, a_1, \ldots, a_{n-1}) = a_0 \bullet \mathbf{e}_0 + a_1 \bullet \mathbf{e}_1 + \ldots + a_{n-1} \bullet \mathbf{e}_{n-1}$$

- The set of linearly independent vectors $\{\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{n-1}\}$ generates the vector space V_n

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

- The set of n linearly independent vectors $\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{n-1}$ generates a n dimension vector space V_n;
- If $k < n$, the set of k linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k$ generates a subspace S of V_n;
- S is k dimension, it consists of 2^k vectors.
- **Question**: Consider why there are 2^k vectors in subspace S.
- A: For a vector space defined over GF(2), the scalar is either "0" or "1". There are 2^k linear combinations of k vectors.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

- *Inner product* of two vectors $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ is defined as:

$$\mathbf{u} \circ \mathbf{v} = u_0 \bullet v_0 \oplus u_1 \bullet v_1 \oplus \ldots \oplus u_{n-1} \bullet v_{n-1}$$

- If $\mathbf{u} \circ \mathbf{v} = 0$, then vector $\mathbf{u}$ and $\mathbf{v}$ are orthogonal.
- **Example**: Verify vector (1001) and (0100) are orthogonal.
- **Solution**: $(1001) \circ (0100) = 1 \bullet 0 \oplus 0 \bullet 1 \oplus 0 \bullet 0 \oplus 1 \bullet 0 = 0$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Dual subspace

- **Example**: For the vector space V_4 over GF(2), the set of vectors $S = \{(0000), (0011), (0110), (0100), (0101), (0111), (0010), (0001)\}$ is a 3-dimension subspace of V_4, $S_d = \{(0000), (1000)\}$ is a 1-dimension subspace of V_4. Verify the vectors of subspace S are orthogonal with the vectors in subspace S_d.
- **Solution**:

$$\begin{aligned} (0000) \circ (1000) &= 0 \\ (0011) \circ (1000) &= 0 \\ &\vdots \\ (0001) \circ (1000) &= 0 \end{aligned}$$

- We say subspace S_d is the *dual subspace* of S. There is:

$$\dim(S) + \dim(S_d) = n$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN