Vector space $\mathbb{F}_2^n$

Ralf Pöppel
mailto:ralf@poeppel-familie.de

2026-01-12

Abstract

This article is a supplemental documentation to the package gf2vs. It descibes the vector space $\mathbb{F}_2^n$ based on the finite field of order 2 or Galois field $GF(2)$ of size n. [2]

Field $\mathbb{F}_2$

The finite field of order 2 has 2 elements $\mathbb{F}_2 = \{0, 1\}$ and the operations addition $+$ and multiplication $\cdot$. For the definition see equation (1).

$$\begin{aligned} + : \quad & 0+0=0, \quad 0+1=1, \quad 1+0=1, \quad 1+1=0, \\ \cdot : \quad & 0\cdot 0=0, \quad 0\cdot 1=0, \quad 1\cdot 0=0, \quad 1\cdot 1=1. \end{aligned} \tag{1}$$

We may use the notation ab instead of $a \cdot b$ omitting the multiplication sign if there is no ambiguity.

Each of the 2 operations of the field $\mathbb{F}_2$ satisfy the group axioms [3] for the groups $G_+ : (\mathbb{F}_2, +)$ and $G_\cdot : (\mathbb{F}_2, \cdot)$. For reference the group axioms are repeated here. We use the symbol $\circ$ to denote the binary operations $+, \cdot$.

Associativity
$\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$.

Identity element e
$\exists e \in G, \forall a \in G : e \circ a = a$ and $a \circ e = a$, e is unique.

Inverse element a^{-1}
$\forall a \in G \;\; \exists b \in G : a \circ b = e$ and $b \circ a = e, e$ identity element, b is unique $\forall a$, notation $b = a^{-1}$.

We can look at the field from an algebraic point of view or from a logic view. In logic the field can be seen as the boolean variables $F = 0$ and $T = 1$. The boolean operations are disjunction $\vee$ [6], contravalence $\oplus$ [1] and conjunction $\wedge$ [5] the definition is repeated in equation (2).

$$\begin{aligned} \vee : \quad & 0\vee 0=0, \quad 0\vee 1=1, \quad 1\vee 0=1, \quad 1\vee 1=1, \\ \oplus : \quad & 0\oplus 0=0, \quad 0\oplus 1=1, \quad 1\oplus 0=1, \quad 1\oplus 1=0, \\ \wedge : \quad & 0\wedge 0=0, \quad 0\wedge 1=0, \quad 1\wedge 0=0, \quad 1\wedge 1=1. \end{aligned} \tag{2}$$

Please note the operations $\oplus$ and $\wedge$ are identically defined as $+$ and $\cdot$ and hence satisfy the group axioms. But the operation $\vee$ does not satisfy the group axioms, there is no inverse element. In the remaining chapters we will use the notation $+, \cdot$ for the operations only.

Vector Space $\mathbb{F}_2^n$

We define the vector space $\mathbb{F}_2^n$ over the field $\mathbb{F}_2$ as set V of vectors v of n elements of the field together with the binary operation addition $u + v = w,\ \ u, v, w \in V$ and the binary function scalar multiplication $a \cdot v = w,\ \ a \in \mathbb{F}_2, v, w \in V$. We apply the addition element-wise and we multiply the scalar with each element of the vector. This definition is similar to the definition in [7].

We use the notation $v = (x_i)$ for the vector v with the components x_i .

In addition we define 2 constants:

Zeros
: $\mathbb{0}$ Zero vector were all components are 0.

Ones
: $\mathbb{1}$ Vector were all components are 1.

The axioms of a vector space are satisfied [7]:

Associativity of vector addition
: $u + (v + w) = (u + v) + w, \forall u, v, w \in \mathbb{F}_2^n$.

Commutativity of vector addition
: $u + v = v + u, \forall u, v \in \mathbb{F}_2^n$.

Identity element of vector addition
: $\exists \mathbb{0} \in \mathbb{F}_2^n : v + \mathbb{0} = v, \forall v \in \mathbb{F}_1^n$.

Inverse elements of vector addition
: $\forall v \in \mathbb{F}_2^n\ \ \exists - v \in \mathbb{F}_2^n : v + (-v) = \mathbb{0}, -v = v,$ each vector is its own additive inverse.

Compatibility of scalar multiplication with field multiplication
: $a(bv) = (ab)v,\ \ a, b \in \mathbb{F}_2, v \in \mathbb{F}_2^n$.

Identity element of scalar multiplication
: $1v = v,\ \ 1 \in \mathbb{F}_2, v \in \mathbb{F}_2^n,$ 1 is the multiplicative identity of $\mathbb{F}_2$.

Distributivity of scalar multiplication with respect to vector addition
: $a(u + v) = au + av,\ \ a \in \mathbb{F}_2, u, v \in \mathbb{F}_2^n$.

Distributivity of scalar multiplication with respect to field addition
: $(a + b)v = av + bv,\ \ a, b \in \mathbb{F}_2, v \in \mathbb{F}_2^n$.

We use some more definitions:

Unit vector
: We define the unit vectors e_i of the vector space as the vectors where all elements except the ith element x_i are 0 and $x_i = 1$.
$e_i = (x_i) : x_i = 1 \wedge x_j = 0, i \neq j, x_i, x_j \in \mathbb{F}_2, e_i \in \mathbb{F}_2^n$.

Generating system
: We define the subspace $\mathbb{E} = \{e_i\}$, $\mathbb{E} =\subset \mathbb{F}_2^n$. The vectors e_i form a generating system. Obviously each vector v of $\mathbb{F}_2^n$ is a linear combination of the scalars a_i and the e_i.
$\forall v \in BF_2^n : v = \sum_{i=1}^{n} a_i e_i,\ \ a_i \in \mathbb{F}_2, e_i \in \mathbb{E}$. So the $\mathbb{E}$ is a span of $\mathbb{F}_2^n$. In this vector space it is the only span. And the decomposition of a vector v in a linear combination of unit vectors e_i is unique.

Basis
: The subspace $\mathbb{E}$ is the one and only basis of the vector space $\mathbb{F}_2^n$.

Index

We name i of e_i the index of a unit vector in the basis.

Norm

We define the Norm $|v|$ of a vector $v \in \mathbb{F}_2^n$ to be its Hamming weight [4]. In this case the count of ones of the vector.

References

[1] Wikipedia contributors. *Exclusive or — Wikipedia, The Free Encyclopedia.* https://en.wikipedia.org/w/index.php?title=Exclusive_or&oldid=1316886803. [Online; accessed 12-January-2026]. 2025.

[2] Wikipedia contributors. *Finite field — Wikipedia, The Free Encyclopedia.* https://en.wikipedia.org/w/index.php?title=Finite_field&oldid=1330855394. [Online; accessed 12-January-2026]. 2026.

[3] Wikipedia contributors. *Group (mathematics) — Wikipedia, The Free Encyclopedia.* https://en.wikipedia.org/w/index.php?title=Group_(mathematics)&oldid=1330839314. [Online; accessed 12-January-2026]. 2026.

[4] Wikipedia contributors. *Hamming weight — Wikipedia, The Free Encyclopedia.* https://en.wikipedia.org/w/index.php?title=Hamming_weight&oldid=1306107874. [Online; accessed 13-January-2026]. 2025.

[5] Wikipedia contributors. *Logical conjunction — Wikipedia, The Free Encyclopedia.* https://en.wikipedia.org/w/index.php?title=Logical_conjunction&oldid=1324909528. [Online; accessed 12-January-2026]. 2025.

[6] Wikipedia contributors. *Logical disjunction — Wikipedia, The Free Encyclopedia.* https://en.wikipedia.org/w/index.php?title=Logical_disjunction&oldid=1317551960. [Online; accessed 12-January-2026]. 2025.

[7] Wikipedia contributors. *Vector space — Wikipedia, The Free Encyclopedia.* https://en.wikipedia.org/w/index.php?title=Vector_space&oldid=1326882436. [Online; accessed 12-January-2026]. 2025.