Linear, Quadratic, and Cubic Forms over the Binary Field

Akihiro Munemasa[1]

[1]Graduate School of Information Sciences
Tohoku University

October 28, 2009
POSTECH

Linear, Quadratic, and Cubic Forms over the Binary Field

Linear form is a homogeneous polynomial of degree 1:
e.g. $2x_1 - x_2 + x_3 + 3x_4$.

Quadratic Form is a homogeneous polynomial of degree 2:
e.g. $x_1^2 - x_2x_3 + 3x_4^2$.

Cubic Form is a homogeneous polynomial of degree 3:
e.g. $x_1^3 - x_2^2x_3 + 2x_1x_2x_4$.

The Binary Field is $\mathbb{F}_2 = \{0, 1\}$ with addition and multiplication defined by

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Polynomials and Functions

In high school mathematics, where polynomials are exclusively used for calculus and analytic geometry,

$$\text{Polynomials} \approx \text{Functions}$$

In abstract algebra (college level), a polynomial is a purely algebraic object,

$$\text{Functions} \approx \text{Mappings}$$

and a polynomial $f(x)$ with real coefficients can be regarded as a mapping $\mathbb{R} \to \mathbb{R}$. This means

some functions can be represented by a polynomial.

Linear Form as Polynomial

Linear form is a homogeneous polynomial of degree 1:
e.g. $f(x_1, x_2, x_3, x_4) = 2x_1 - x_2 + x_3 + 3x_4$.

f can be regarded as a polynomial in four indeterminates, or as a mapping $f : \mathbb{R}^4 \longrightarrow \mathbb{R}$ with four variables or arguments. Then f is a linear mapping:

$$f(\boldsymbol{x} + \boldsymbol{y}) = f(\boldsymbol{x}) + f(\boldsymbol{y}),$$
$$f(a\boldsymbol{x}) = af(\boldsymbol{x}),$$

where $\boldsymbol{x} = (x_1, \ldots, x_4)$, $\boldsymbol{y} = (y_1, \ldots, y_4)$, $a \in \mathbb{R}$.
More generally, and conversely,...

Linear Form as Function

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a mapping.
A theorem in elementary linear algebra says:

f satisfies

$$f(\boldsymbol{x} + \boldsymbol{y}) = f(\boldsymbol{x}) + f(\boldsymbol{y}),$$
$$f(a\boldsymbol{x}) = af(\boldsymbol{x}),$$

for all $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$ and $a \in \mathbb{R}$

$\Longleftrightarrow$

$\exists a_1, \ldots, a_n \in \mathbb{R}$, $\forall \boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$,

$$f(\boldsymbol{x}) = a_1 x_1 + \cdots + a_n x_n.$$

Vector Space over $\mathbb{R}$

Standard linear algebra deals with vector spaces over $\mathbb{R}$, not necessarily of the form $\mathbb{R}^n$, and linear mappings among them.

A vector space V is equipped with addition and scalar multiplication, and is required to satisfy certain axioms. I assume the audience is familiar with the concept of "basis" and "subspace".
If $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ is a basis of V, then $f : V \to \mathbb{R}$ is linear if and only if $\exists a_1, \ldots, a_n$ such that

$$f(\sum_{i=1}^{n} x_i \boldsymbol{b}_i) = a_1 x_1 + \cdots + a_n x_n.$$

Indeed, one can define $a_i = f(\boldsymbol{b}_i)$.

Polynomial Function on Vector Space

For a function $f : V \to \mathbb{R}$, let

$$g(x_1, \dots, x_n) = f(\sum_{i=1}^{n} x_i \boldsymbol{b}_i)$$

be the function with n variables defined by f and a basis $\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\}$ of V.

f	g is homogeneous of degree:	$f^{-1}(0)$
linear	1	hyperplane
quadratic	2	(quadratic) surface
cubic	3	(cubic) surface

This definition is independent of the choice of a basis.

Vector Space over $\mathbb{F}_2 = \{0, 1\}$

+	0	1
0	0	1
1	1	0

$$\mathbb{F}_2^n = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{F}_2\}$$

is a vector space over $\mathbb{F}_2$; it has entrywise addition and scalar (0 and 1 only!) multiplication.
All the standard concepts (basis, dimension, subspace, etc) can be carried over and work without any change.

$$\ell : \mathbb{F}_2^n \to \mathbb{F}_2, \quad \ell(x_1, \ldots, x_n) = x_1 + x_2 + \cdots + x_n$$

is a linear form. Its value is

$$\ell(x_1, \ldots, x_n) = \begin{cases} 0 & \text{if } |\{i \mid x_i = 1\}| : \text{ even,} \\ 1 & \text{if } |\{i \mid x_i = 1\}| : \text{ odd.} \end{cases}$$

$\ell^{-1}(0) = \operatorname{Ker} \ell$ is a subspace of dimension $n - 1$.

$\mathbb{F}_2^n$ as Power Set

$$|\mathbb{F}_2^n| = |\{(x_1, \ldots, x_n) \mid x_i \in \mathbb{F}_2\}| = 2^n.$$

A vector space of dimension k over $\mathbb{F}_2$ has 2^k elements.
There is a 1-1 correspondence

$$\begin{array}{ccc}
(1,0,1,1,0) & \leftrightarrow & \{1,3,4\} \\
\boldsymbol{x} \in \mathbb{F}_2^n & & S \subset \{1,\ldots,n\} \\
\boldsymbol{x} & \rightarrow & \mathrm{supp}(\boldsymbol{x}) \\
\boldsymbol{e}_S = \sum_{i \in S} \boldsymbol{e}_i & \leftarrow & S \\
\mathrm{wt}(\boldsymbol{x}) & = & |S| \\
\text{Characteristic vector} & & \text{Support}
\end{array}$$

Quadratic Form

On the subspace

$$W = \operatorname{Ker} \ell = \{\boldsymbol{x} \in \mathbb{F}_2^n \mid \mathrm{wt}(\boldsymbol{x})\colon \text{ even}\}$$

there is a quadratic form

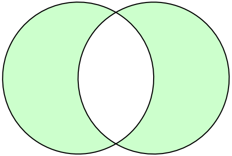
$$q(\boldsymbol{x}) = (\frac{\mathrm{wt}(\boldsymbol{x})}{2} \bmod 2).$$

Why is this a quadratic form?
(Take a basis, then express q as a polynomial function in the basis-coefficient, and see it is homogeneous of degree 2).
To do this, we need the interpretation of the addition via support-characteristic vector correspondence.

$$\begin{array}{ccc} \text{sum} & & \text{symmetric difference} \\ \boldsymbol{x} + \boldsymbol{y} & \leftrightarrow & (\mathrm{supp}(\boldsymbol{x}) \cup \mathrm{supp}(\boldsymbol{y})) \setminus (\mathrm{supp}(\boldsymbol{x}) \cap \mathrm{supp}(\boldsymbol{y})) \end{array}$$

$q(\boldsymbol{x}) = (\frac{\mathrm{wt}(\boldsymbol{x})}{2} \bmod 2)$ on $W = \operatorname{Ker} \ell$

Let $S \triangle T$ denote the symmetric difference



$$S \triangle T = (S \cup T) \setminus (S \cap T).$$

Then

$$|S \triangle T| = |S \cup T| - |S \cap T| = |S| + |T| - 2|S \cap T|.$$

Since $\mathrm{supp}(\boldsymbol{x} + \boldsymbol{y}) = \mathrm{supp}(\boldsymbol{x}) \triangle \mathrm{supp}(\boldsymbol{y})$,

$$\mathrm{wt}(\boldsymbol{x} + \boldsymbol{y}) = \mathrm{wt}(\boldsymbol{x}) + \mathrm{wt}(\boldsymbol{y}) - 2\,\mathrm{wt}(\boldsymbol{x} * \boldsymbol{y}),$$

where $\boldsymbol{x} * \boldsymbol{y}$ denotes the entrywise product.

$\times$	0	1
0	0	0
1	0	1

$$\mathrm{wt}(\boldsymbol{x}+\boldsymbol{y}) = \mathrm{wt}(\boldsymbol{x}) + \mathrm{wt}(\boldsymbol{y}) - 2\,\mathrm{wt}(\boldsymbol{x}*\boldsymbol{y})$$

$$\mathrm{wt}\Big(\sum_{i=1}^{m} \boldsymbol{b}_i\Big) \equiv \sum_{i=1}^{m} \mathrm{wt}(\boldsymbol{b}_i) - 2\sum_{i<j} \mathrm{wt}(\boldsymbol{b}_i * \boldsymbol{b}_j) \pmod 4.$$

If $\boldsymbol{b}_i \in W = \operatorname{Ker}\ell$, then $2 \mid \mathrm{wt}(\boldsymbol{b}_i)$, so

$$\frac{1}{2}\,\mathrm{wt}\Big(\sum_{i=1}^{m} \boldsymbol{b}_i\Big) \equiv \sum_{i=1}^{m} \frac{1}{2}\,\mathrm{wt}(\boldsymbol{b}_i) - \sum_{i<j} \mathrm{wt}(\boldsymbol{b}_i * \boldsymbol{b}_j) \pmod 2.$$

$$q\Big(\sum_{i=1}^{m} \boldsymbol{b}_i\Big) = \sum_{i=1}^{m} q(\boldsymbol{b}_i) + \sum_{i<j} \big(\mathrm{wt}(\boldsymbol{b}_i * \boldsymbol{b}_j) \bmod 2\big)$$

$$\mathrm{wt}(\boldsymbol{x}+\boldsymbol{y}) = \mathrm{wt}(\boldsymbol{x}) + \mathrm{wt}(\boldsymbol{y}) - 2\,\mathrm{wt}(\boldsymbol{x} * \boldsymbol{y})$$

$$\mathrm{wt}\Big(\sum_{i=1}^{m} \boldsymbol{b}_i\Big) \equiv \sum_{i=1}^{m} \mathrm{wt}(\boldsymbol{b}_i) - 2\sum_{i<j} \mathrm{wt}(\boldsymbol{b}_i * \boldsymbol{b}_j) \pmod 4.$$

If $\boldsymbol{b}_i \in W = \operatorname{Ker}\ell$, then $2 \mid \mathrm{wt}(\boldsymbol{b}_i)$, so

$$\frac{1}{2}\mathrm{wt}\Big(\sum_{i=1}^{m} \boldsymbol{b}_i\Big) \equiv \sum_{i=1}^{m} \frac{1}{2}\mathrm{wt}(\boldsymbol{b}_i) - \sum_{i<j} \mathrm{wt}(\boldsymbol{b}_i * \boldsymbol{b}_j) \pmod 2.$$

$$\begin{aligned} q\Big(\sum_{i=1}^{m} x_i\boldsymbol{b}_i\Big) &= \sum_{i=1}^{m} q(x_i\boldsymbol{b}_i) + \sum_{i<j} (\mathrm{wt}(x_i\boldsymbol{b}_i * x_j\boldsymbol{b}_j) \bmod 2) \\ &= \sum_{i=1}^{m} x_i^2 q(\boldsymbol{b}_i) + \sum_{i<j} x_i x_j (\mathrm{wt}(\boldsymbol{b}_i * \boldsymbol{b}_j) \bmod 2) \end{aligned}$$

:homogeneous of degree 2 (Remark: $0^2 = 0$, $1^2 = 1$).

$q(\boldsymbol{x}) = (\frac{\mathrm{wt}(\boldsymbol{x})}{2} \bmod 2)$ on $W = \operatorname{Ker}\ell$

$$\begin{aligned} |q^{-1}(0)| &= |\{\boldsymbol{x} \in W \mid q(\boldsymbol{x}) = 0\}| \\ &= |\{\boldsymbol{x} \in \mathbb{F}_2^n \mid \mathrm{wt}(\boldsymbol{x}) \equiv 0 \pmod 4\}| \\ &= |\{S \subset \{1, \dots, n\} \mid |S| \equiv 0 \pmod 4\}| \\ &= \binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \cdots . \end{aligned}$$

$\ell^{-1}(0) = \operatorname{Ker}\ell$ was a subspace, but $q^{-1}(0)$ is not.

- The largest dimension of subspaces contained in $q^{-1}(0)$ is $\frac{n}{2} - 1$ or $\lfloor \frac{n}{2} \rfloor$, according as $n \equiv 2, 4, 6 \pmod 8$ or not.
- Every subspace contained in $q^{-1}(0)$ is contained in such a subspace of the largest dimension.
- In particular, $q^{-1}(0)$ is a union of subspaces of dimension $\frac{n}{2} - 1$ or $\lfloor \frac{n}{2} \rfloor$.

Cubic Form

On the subspace $W = \mathrm{Ker}\,\ell = \ell^{-1}(0)$, there was a quadratic form

$$q(\boldsymbol{x}) = (\frac{\mathrm{wt}(\boldsymbol{x})}{2} \bmod 2).$$

On any subspace $U \subset q^{-1}(0)$, there is a cubic form

$$c(\boldsymbol{x}) = (\frac{\mathrm{wt}(\boldsymbol{x})}{4} \bmod 2).$$

Why is this a cubic form?
(Take a basis, then express c as a polynomial function in the basis-coefficient, and see it is homogeneous of degree 3).

$$\mathrm{wt}(\boldsymbol{x}+\boldsymbol{y}) = \mathrm{wt}(\boldsymbol{x}) + \mathrm{wt}(\boldsymbol{y}) - 2\,\mathrm{wt}(\boldsymbol{x} * \boldsymbol{y})$$

$$\mathrm{wt}(\sum_{i=1}^{m} \boldsymbol{b}_i) \equiv \sum_{i=1}^{m} \mathrm{wt}(\boldsymbol{b}_i) - 2\sum_{i<j} \mathrm{wt}(\boldsymbol{b}_i * \boldsymbol{b}_j) \pmod 4.$$

$$\mathrm{wt}(\sum_{i=1}^{m} \boldsymbol{b}_i) \equiv \sum_{i=1}^{m} \mathrm{wt}(\boldsymbol{b}_i) - 2\sum_{i<j} \mathrm{wt}(\boldsymbol{b}_i * \boldsymbol{b}_j) + 4 \sum_{i<j<k} \mathrm{wt}(\boldsymbol{b}_i * \boldsymbol{b}_j * \boldsymbol{b}_k) \pmod 8.$$

If $\boldsymbol{b}_i \in U \subset q^{-1}(0)$, then $4 \mid \mathrm{wt}(\boldsymbol{b}_i)$, so

$$c(\sum_{i=1}^{m} x_i \boldsymbol{b}_i) = \sum_{i=1}^{m} x_i^3 c(\boldsymbol{b}_i) + \sum_{i<j} x_i x_j^2 (\frac{1}{2}\mathrm{wt}(\boldsymbol{b}_i * \boldsymbol{b}_j) \bmod 2) + \sum_{i<j<k} x_i x_j x_k (\mathrm{wt}(\boldsymbol{b}_i * \boldsymbol{b}_j * \boldsymbol{b}_k) \bmod 2)$$

$$c(\boldsymbol{x}) = \left(\frac{\mathrm{wt}(\boldsymbol{x})}{4} \bmod 2\right)$$

$$\begin{aligned}
|c^{-1}(0)| &= |\{\boldsymbol{x} \in q^{-1}(0) \mid c(\boldsymbol{x}) = 0\}| \\
&= |\{\boldsymbol{x} \in \mathbb{F}_2^n \mid \mathrm{wt}(\boldsymbol{x}) \equiv 0 \pmod 8\}| \\
&= |\{S \subset \{1, \ldots, n\} \mid |S| \equiv 0 \pmod 8\}| \\
&= \binom{n}{0} + \binom{n}{8} + \binom{n}{16} + \cdots .
\end{aligned}$$

$q^{-1}(0)$ had some nice properties, but little is known for $c^{-1}(0)$.

$q^{-1}(0)$ and $c^{-1}(0)$

$q^{-1}(0)$ had some nice properties:

- The largest dimension of subspaces contained in $q^{-1}(0)$ is $\frac{n}{2} - 1$ or $\lfloor \frac{n}{2} \rfloor$, according as $n \equiv 2, 4, 6 \pmod 8$ or not.
- Every subspace contained in $q^{-1}(0)$ is contained in such a subspace of the largest dimension.

Little is known for $c^{-1}(0)$.

- What is the largest dimension of subspaces contained in $c^{-1}(0)$?
- Not every subspace contained in $c^{-1}(0)$ is contained in such a subspace of the largest dimension. That is, the dimensions of maximal subspaces contained in $c^{-1}(0)$ is not constant.
- Describe all the maximal subspaces contained in $c^{-1}(0)$.

A maximal subspace contained in $c^{-1}(0)$

Take $n = 15$. Observe $\binom{6}{2} = 15$.

$$\{1, 2, \dots, 15\} \leftrightarrow \{i, j\} \subset \{1, 2, \dots, 6\}.$$

	12	13	14	15	16	23	$\cdots$	56
12	0	1	1	1	1	1	$\cdots$	0
13	1	0	1	1	1	1	$\cdots$	0
14	1	1	0	1	1	0	$\cdots$	0
15	1	1	1	0	1	0	$\cdots$	1
16	1	1	1	1	0	0	$\cdots$	1

$$\begin{cases} 1 & |\cap| = 1 \\ 0 & |\cap| \neq 1 \end{cases}$$

The row vectors span a 4-dimensional space $U \subset c^{-1}(0)$, and this is maximal. Up to permutation of coordinates, this is the unique maximal subspace contained in $c^{-1}(0)$.

But for larger n, the situation is different.

Conclusion

- This construction of maximal subspaces using $\binom{6}{2}$ can be generalized to $\binom{4k+2}{2}$ for an arbitrary positive integer k. I will talk more about it with its connection to other mathematical objects in Friday's colloquium.
- If you are interested in "linear algebra over $\mathbb{F}_2$," try to read introductory textbook on coding theory, especially on "binary linear codes."

Thank you very much for attending my talk.