Linear, Quadratic, and Cubic Forms over the Binary Field

Akihiro Munemasa

1Graduate 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

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Polynomials and Functions

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

Polynomials $\approx$ Functions

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

Functions $\approx$ Mappings

and a polynomial $f(x)$ with real coefficients can be regarded as a mapping $\mathbb{R} \rightarrow \mathbb{R}$. 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 \( f : \mathbb{R}^4 \to \mathbb{R} \) with four variables or arguments. Then \( f \) is a linear mapping:

\[
\begin{align*}
f(x + y) &= f(x) + f(y), \\
f(ax) &= af(x),
\end{align*}
\]

where \( x = (x_1, \ldots, x_4), \ y = (y_1, \ldots, y_4), \ a \in \mathbb{R}. \)

More generally, and conversely, \ldots
Linear Form as Function

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a mapping.

A theorem in elementary linear algebra says:

$f$ satisfies

\[ f(x + y) = f(x) + f(y), \]
\[ f(ax) = af(x), \]

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

\[ \iff \exists a_1, \ldots, a_n \in \mathbb{R}, \forall x = (x_1, \ldots, x_n) \in \mathbb{R}^n, \]
\[ f(x) = a_1x_1 + \cdots + a_nx_n. \]
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 $\{b_1, \ldots, b_n\}$ 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

$$f \left( \sum_{i=1}^{n} x_i b_i \right) = a_1 x_1 + \cdots + a_n x_n.$$ 

Indeed, one can define $a_i = f(b_i)$. 

Polynomial Function on Vector Space

For a function \( f : V \rightarrow \mathbb{R} \), let

\[
g(x_1, \ldots, x_n) = f\left(\sum_{i=1}^{n} x_i b_i\right)
\]

be the function with \( n \) variables defined by \( f \) and a basis \( \{b_1, \ldots, b_n\} \) of \( V \).

<table>
<thead>
<tr>
<th>( f )</th>
<th>( g ) is homogeneous of degree:</th>
<th>( f^{-1}(0) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>linear</td>
<td>1</td>
<td>hyperplane</td>
</tr>
<tr>
<td>quadratic</td>
<td>2</td>
<td>(quadratic) surface</td>
</tr>
<tr>
<td>cubic</td>
<td>3</td>
<td>(cubic) surface</td>
</tr>
</tbody>
</table>

This definition is independent of the choice of a basis.
Vector Space over $\mathbb{F}_2 = \{0, 1\}$

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

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

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

$\ell^{-1}(0) = \text{Ker } \ell$ 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

\[(1, 0, 1, 1, 0) \leftrightarrow \{1, 3, 4\} \]
\[ x \in \mathbb{F}_2^n \quad \quad S \subset \{1, \ldots, n\} \]
\[ x \rightarrow \quad \quad \text{supp}(x) \]
\[ e_S = \sum_{i \in S} e_i \quad \leftrightarrow \quad S \]
\[ \text{wt}(x) = |S| \quad \quad \text{Support} \]

Characteristic vector
Quadratic Form

On the subspace

\[ W = \text{Ker } \ell = \{ x \in \mathbb{F}_2^n \mid \text{wt}(x): \text{even} \} \]

there is a **quadratic** form

\[ q(x) = \left( \frac{\text{wt}(x)}{2} \right) \mod 2. \]

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.

\[ \text{sum} \quad \text{symmetric difference} \]
\[ x + y \leftrightarrow (\text{supp}(x) \cup \text{supp}(y)) \setminus (\text{supp}(x) \cap \text{supp}(y)) \]
\( q(x) = \left( \frac{\text{wt}(x)}{2} \right) \mod 2 \) on \( W = \text{Ker} \ell \)

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 \( \text{supp}(x + y) = \text{supp}(x) \triangle \text{supp}(y) \),

\[ \text{wt}(x + y) = \text{wt}(x) + \text{wt}(y) - 2\text{wt}(x \ast y), \]

where \( x \ast y \) denotes the entrywise product.
\[
\text{wt}(x + y) = \text{wt}(x) + \text{wt}(y) - 2 \text{wt}(x \ast y)
\]

\[
\text{wt} \left( \sum_{i=1}^{m} b_i \right) \equiv \sum_{i=1}^{m} \text{wt}(b_i) - 2 \sum_{i<j} \text{wt}(b_i \ast b_j) \pmod{4}.
\]

If \( b_i \in W = \text{Ker} \ell \), then \( 2 \mid \text{wt}(b_i) \), so

\[
\frac{1}{2} \text{wt} \left( \sum_{i=1}^{m} b_i \right) \equiv \sum_{i=1}^{m} \frac{1}{2} \text{wt}(b_i) - \sum_{i<j} \text{wt}(b_i \ast b_j) \pmod{2}.
\]

\[
q \left( \sum_{i=1}^{m} b_i \right) = \sum_{i=1}^{m} q(b_i) + \sum_{i<j} (\text{wt}(b_i \ast b_j) \pmod{2})
\]
\[
\text{wt}(x + y) = \text{wt}(x) + \text{wt}(y) - 2 \text{wt}(x \ast y)
\]

\[
\text{wt}\left(\sum_{i=1}^{m} b_i\right) \equiv \sum_{i=1}^{m} \text{wt}(b_i) - 2 \sum_{i<j} \text{wt}(b_i \ast b_j) \pmod{4}.
\]

If \( b_i \in W = \text{Ker} \ell \), then \( 2 \mid \text{wt}(b_i) \), so

\[
\frac{1}{2} \text{wt}\left(\sum_{i=1}^{m} b_i\right) \equiv \sum_{i=1}^{m} \frac{1}{2} \text{wt}(b_i) - \sum_{i<j} \text{wt}(b_i \ast b_j) \pmod{2}.
\]

\[
q\left(\sum_{i=1}^{m} x_i b_i\right) = \sum_{i=1}^{m} q(x_i b_i) + \sum_{i<j} (\text{wt}(x_i b_i \ast x_j b_j) \pmod{2})
\]

\[
= \sum_{i=1}^{m} x_i^2 q(b_i) + \sum_{i<j} x_i x_j (\text{wt}(b_i \ast b_j) \pmod{2})
\]

:homogeneous of degree 2 (Remark: \( 0^2 = 0, 1^2 = 1 \)).
\[ q(x) = \left( \frac{\text{wt}(x)}{2} \right) \mod 2 \text{ on } W = \text{Ker } \ell \]

\[
|q^{-1}(0)| = \left| \{ x \in W \mid q(x) = 0 \} \right|
= \left| \{ x \in \mathbb{F}_2^n \mid \text{wt}(x) \equiv 0 \mod 4 \} \right|
= \left| \{ S \subset \{1, \ldots, n\} \mid |S| \equiv 0 \mod 4 \} \right|
= \binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \cdots.
\]

\( \ell^{-1}(0) = \text{Ker } \ell \) 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 \( n \equiv 2, 4, 6 \mod 8 \) 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 \( \lfloor \frac{n}{2} \rfloor \).
On the subspace $W = \ker \ell = \ell^{-1}(0)$, there was a quadratic form

$$q(x) = \left( \frac{\text{wt}(x)}{2} \right) \mod 2.$$ 

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

$$c(x) = \left( \frac{\text{wt}(x)}{4} \right) \mod 2.$$ 

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).
\[ \text{wt}(x + y) = \text{wt}(x) + \text{wt}(y) - 2 \text{wt}(x \ast y) \]

\[
\text{wt}(\sum_{i=1}^{m} b_i) \equiv \sum_{i=1}^{m} \text{wt}(b_i) - 2 \sum_{i<j} \text{wt}(b_i \ast b_j) \pmod{4}. 
\]

\[
\text{wt}(\sum_{i=1}^{m} b_i) \equiv \sum_{i=1}^{m} \text{wt}(b_i) - 2 \sum_{i<j} \text{wt}(b_i \ast b_j) 
+ 4 \sum_{i<j<k} \text{wt}(b_i \ast b_j \ast b_k) \pmod{8}. 
\]

If \( b_i \in U \subset q^{-1}(0) \), then \( 4 \mid \text{wt}(b_i) \), so

\[
c(\sum_{i=1}^{m} x_i b_i) = \sum_{i=1}^{m} x_i^3 c(b_i) + \sum_{i<j} x_i x_j^2 \left( \frac{1}{2} \text{wt}(b_i \ast b_j) \mod 2 \right) 
+ \sum_{i<j<k} x_i x_j x_k \left( \text{wt}(b_i \ast b_j \ast b_k) \mod 2 \right)
\]
\[ c(\mathbf{x}) = \left( \frac{\text{wt}(\mathbf{x})}{4} \right) \text{ mod } 2 \]

\[
|c^{-1}(0)| = \left| \{ \mathbf{x} \in q^{-1}(0) \mid c(\mathbf{x}) = 0 \} \right|
\]
\[
= \left| \{ \mathbf{x} \in \mathbb{F}_2^n \mid \text{wt}(\mathbf{x}) \equiv 0 \text{ (mod 8)} \} \right|
\]
\[
= \left| \{ S \subset \{1, \ldots, n\} \mid |S| \equiv 0 \text{ (mod 8)} \} \right|
\]
\[
= \binom{n}{0} + \binom{n}{8} + \binom{n}{16} + \cdots.
\]

\(q^{-1}(0)\) 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 $\binom{6}{2} = 15$.

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

<table>
<thead>
<tr>
<th></th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>23</th>
<th>...</th>
<th>56</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>...</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>...</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>...</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>...</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>...</td>
<td>1</td>
</tr>
</tbody>
</table>

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.